

Hybrid image encryption scheme based on hyperchaotic map with spherical attractors

Zhitang Han(韩智堂), Yinghong Cao(曹颖鸿), Santo Banerjee, and Jun Mou(牟俊)

Citation: Chin. Phys. B, 2025, 34 (**3**): 030503. DOI: 10.1088/1674-1056/ada7db
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Bifurcation analysis and control study of improved full-speed differential model in connected vehicle environment

Wen-Huan Ai(艾文欢), Zheng-Qing Lei(雷正清), Dan-Yang Li(李丹洋), Dong-Liang Fang(方栋梁), and Da-Wei Liu(刘大为)
Chin. Phys. B, 2024, 33 (**7**): 070503. DOI: 10.1088/1674-1056/ad3b80

Effects of asymmetric coupling and boundary on the dynamic behaviors of a random nearest neighbor coupled system

Ling Xu(徐玲) and Lei Jiang(姜磊)
Chin. Phys. B, 2024, 33 (**6**): 060503. DOI: 10.1088/1674-1056/ad3b86

A color image encryption algorithm based on hyperchaotic map and DNA mutation

Xinyu Gao(高昕瑜), Bo Sun(孙博), Yinghong Cao(曹颖鸿), Santo Banerjee, and Jun Mou(牟俊)
Chin. Phys. B, 2023, 32 (**3**): 030501. DOI: 10.1088/1674-1056/ac8cdf

A novel hyperchaotic map with sine chaotification and discrete memristor

Qiankun Sun(孙乾坤), Shaobo He(贺少波), Kehui Sun(孙克辉), and Huihai Wang(王会海)
Chin. Phys. B, 2022, 31 (**12**): 120501. DOI: 10.1088/1674-1056/ac8f3a

A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations

Li-Min Zhang(张立民), Ke-Hui Sun(孙克辉), Wen-Hao Liu(刘文浩), Shao-Bo He(贺少波)
Chin. Phys. B, 2017, 26 (**10**): 100504. DOI: 10.1088/1674-1056/26/10/100504

Hybrid image encryption scheme based on hyperchaotic map with spherical attractors

Zhitang Han(韩智堂)[1], Yinghong Cao(曹颖鸿)[1,†], Santo Banerjee[2], and Jun Mou(牟俊)[1,‡]

[1] *School of Information Science and Engineering, Dalian Polytechnic University, Dalian* 116034, *China*
[2] *Department of Mathematical Sciences, Giuseppe Luigi Lagrange, Politecnico di Torino, Corso Duca degli Abruzzi* 24, *Torino, Italy*

(Received 1 December 2024; revised manuscript received 19 December 2024; accepted manuscript online 9 January 2025)

Existing chaotic encryption schemes primarily focus on single types of images, making the design of hybrid image encryption schemes more suitable for practical applications. In this paper, a hyperchaotic map with a spherical attractor is proposed, which is constructed using spherical coordinates. Dynamical analyses reveal that the hyperchaotic map exhibits global hyperchaos and high complexity, making it capable of generating more complex chaotic sequences suitable for image encryption. A hybrid encryption scheme based on a hyperchaotic map is proposed for two-dimensional (2D) images, three-dimensional (3D) models, and 3D point clouds. Firstly, the pixels of 2D image and the coordinate data of 3D image are fused into a plaintext cube, which is combined with Hash-512 to obtain the initial value of the hyperchaotic map. Chaotic sequences are utilized for cube space internal confusion and dynamic cross-diffusion. The encrypted images demonstrate high information entropy, and the test results show that the encryption scheme effectively protects the images. The proposed hybrid image encryption scheme provides an efficient solution for securing various types of images.

Keywords: hyperchaotic map, spherical attractor, global hyperchaos, hybrid image encryption

PACS: 05.45.–a, 05.45.Gg

DOI: 10.1088/1674-1056/ada7db **CSTR:** 32038.14.CPB.ada7db

1. Introduction

Advancements in information technology have positioned image data as a crucial component in information exchange, owing to its powerful visual presentation ability.[1,2] Among them, two-dimensional (2D) images mainly express flat information, three-dimensional (3D) models can provide 3D information and 3D point clouds can show high-precision point information.[3] Due to the above characteristics, 2D images, 3D models and 3D point clouds are prevalent across a variety of fields, such as medical images,[4–6] remote sensing images,[7–9] engineering models,[10] laser scanning,[11] and so on.[12] Due to the involvement of personal privacy, commercial secrets, and military intelligence, image data are vulnerable to unauthorized access and leakage during transmission over the network,[13–15] so it is important to encrypt the data before transmission.

The emergence of chaotic systems has brought new ideas for image encryption.[16–18] Chaotic systems are suitable for cryptography due to their pseudorandom, sensitivity to initial conditions and unpredictability.[19–22] Since Robert combined chaos and image encryption in 1989, chaotic image encryption has emerged as a novel research topic.[23] A significant number of image encryption schemes have been proposed based on low-dimensional chaotic systems.[24–27] However, with the improvement of mathematical theories and the limitation of computer accuracy, the simple chaotic orbits and small key space of low-dimensional chaotic systems bring hidden dangers to the encryption schemes.[28–30] The hyperchaotic system solves this drawback of low-dimensional chaotic systems due to its stronger chaotic properties and better resistance to degradation.[30–32] Therefore, the construction of hyperchaotic systems with higher complexity and higher Lyapunov exponent is favorable for the development of chaotic image encryption. This paper constructs a hyperchaotic map with spherical attractors based on the spherical coordinate, with verification conducted on the DSP. The hyperchaotic map exhibits global hyperchaos and high complexity, and the complex dynamical properties make the encryption process more unpredictable and reduce the risk of information leakage.

Due to the rapid growth of 3D technology, 3D images are widely used in diverse fields, and researchers are also working on encrypting 3D images with sensitive information.[33–35] Gao *et al*. used the chaotic system and semi-tensor product theory for 3D model encryption. Encrypting the integer and fractional parts of the model increases the time cost, although encrypting twice brings higher security.[36] Xian *et al*. proposed an iterative method for vectors of fractal characteristics and implemented simultaneous confusion–diffusion encryption. The test results demonstrate the scheme has good encryption effect.[37] Zhao *et al*. encrypted 3D models based on the chaotic system and XOR permutation, and the scheme not only has low time cost but also achieves hierarchical decryption.[38]

†Corresponding author. E-mail: caoyinghong@dlpu.edu.cn
‡Corresponding author. E-mail: moujun@dlpu.edu.cn

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

However, existing encryption techniques mainly focus on a single type of image, making it difficult to effectively protect hybrid images.[39,40]

To meet the needs of practical applications, the encryption scheme for hybrid image is proposed based on the constructed hyperchaotic system. Firstly, the relevant data of images are fused into the plaintext cube, and the plaintext cube is confusion by combining chaotic sequences and cube space internal confusion. Dynamic cross-diffusion is used next, the modulo operation is applied to even faces and the XOR operation is applied to odd faces. The results demonstrate that the proposed encryption scheme is effective in safeguarding the hybrid image. The following are the main contributions of this paper:

(I) The 3D hyperchaotic map with spherical attractors is constructed.

(II) Dynamical analyses show that the hyperchaotic map exhibits global hyperchaos and high complexity.

(III) The hybrid image encryption scheme is proposed for 2D images, 3D models, and 3D point clouds.

(IV) Testing shows encryption scheme effectively protects information in the hybrid image.

2. Chaotic map with spherical attractors

A hyperchaotic map is proposed based on the spherical coordinate and dynamical analysis and digital circuit implementation are carried out.

2.1. Construction of chaotic map

Spherical coordinates are one type of coordinate system for locating points in three-dimensional space as shown in Fig. 1. r is the length of OP, θ is the angle between OP and the positive direction of the z-axis, and φ is the angle between the projection of OP on the x–y plane and the positive direction of the x-axis. The spherical coordinate (r, θ, φ) can be converted to the rectangular coordinate by the following equation:

$$\begin{cases} x = r\sin\theta\cos\varphi, \\ y = r\sin\theta\sin\varphi, \\ z = r\cos\theta. \end{cases} \tag{1}$$

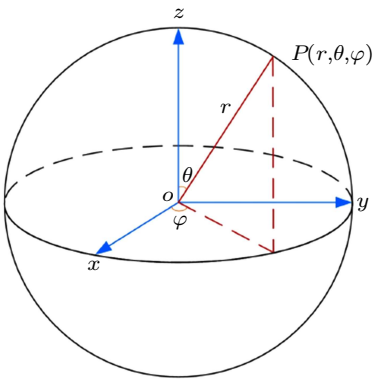


Fig. 1. Spherical coordinate system.

To obtain chaotic sequences between $-r$ and r, therefore multiply $\sin(c/x)$ in each term of Eq. (1). And replace θ with $a\pi y$ and φ with $b\pi z$, thus constructing a chaotic map with spherical attractor as follows:

$$\begin{cases} x_{n+1} = r\sin(a\pi y_n)\cos(b\pi z_n)\sin(c/x_n), \\ y_{n+1} = r\sin(a\pi y_n)\sin(b\pi z_n)\sin(c/x_n), \\ z_{n+1} = r\cos(a\pi y_n)\sin(c/x_n), \end{cases} \tag{2}$$

where a, b, c as parameters and r as the radius can control the size of the spherical attractor. The chaotic attractors obtained when the initial value is (1, 1, 1) and the parameters $a = 10$, $b = 5$, $c = 1$ are a sphere of radius r as shown in Fig. 2.

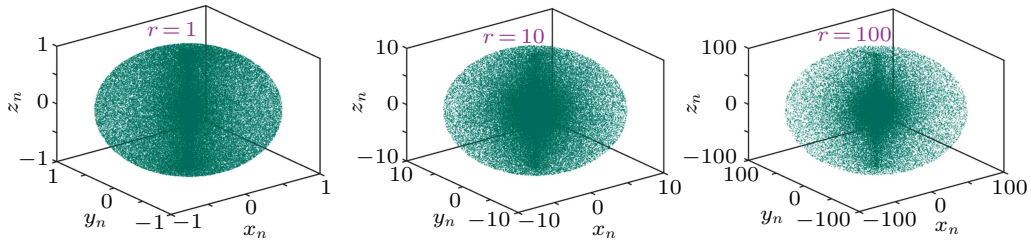


Fig. 2. Spherical attractors of different r.

2.2. LEs and bifurcation diagram

With the help of LEs and bifurcation diagrams, it is possible to quantitatively evaluate the chaotic properties and the variation of the system state concerning the parameters. The system is chaotic if it has one LE greater than 0, and hyperchaotic if it has two or more LEs greater than 0. Keeping the initial values constant, the LEs and bifurcation diagrams of the hyperchaotic map with respect to its four parameters are shown in Fig. 3.

The existence of three positive LEs for the map, when all the parameters are varied within the chosen range, means that it has the property of global hyperchaos. The parameters are more flexible when the map is applied to image encryption. In Fig. 3, LE1 is generally larger and increases with increasing parameters, indicating that the two neighboring chaotic orbits of the system separate faster, implying that the system has stronger chaotic properties. The bifurcation diagram in Fig. 3(d) shows that the parameter r can control the range of chaotic sequences well, which can provide more options for engineering applications.

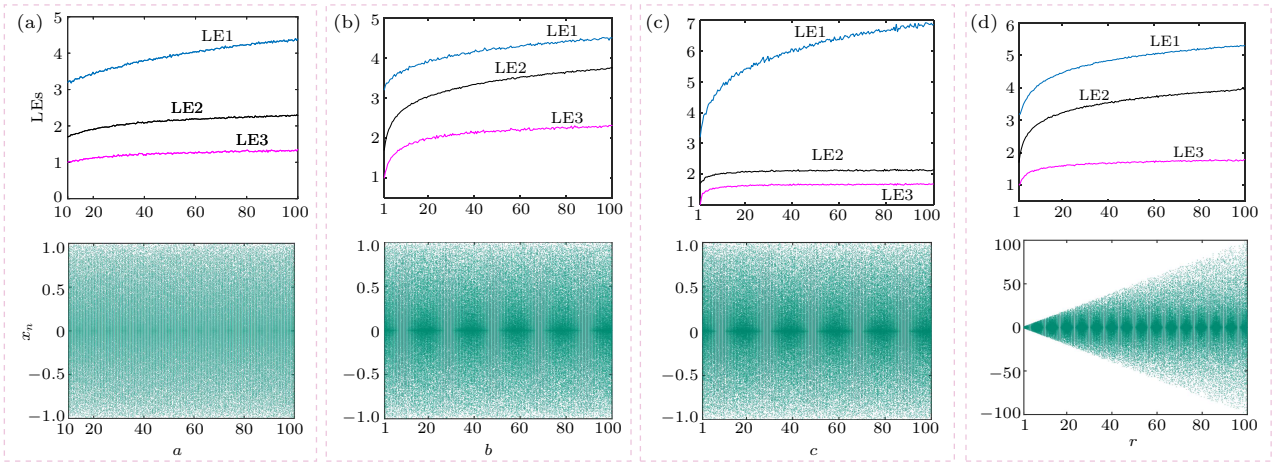


Fig. 3. Impact of parameters on the performance of the hyperchaotic map at initial values (1, 1, 1): (a) $b = c = r = 1$, $a \in (10, 100)$; (b) $a = 10$, $c = r = 1$, $b \in (1, 100)$; (c) $a = 10$, $b = r = 1$, $c \in (1, 100)$; (d) $a = 10$, $b = c = 1$, $r \in (1, 100)$.

2.3. Spectral entropy

Spectral entropy (*SE*) complexity is used to quantify the complexity of the chaotic sequence.[41] When *SE* is larger it means that the system is more complex and the generated sequence is closer to the random sequence. Keeping the initial values (1, 1, 1), the *SE* about parameters a and b when parameter $c = 5$, $r = 5$ is shown in Fig. 4(a), and the analysis shows that the *SE* is between 0.9463 and 0.9537, its mean value is 0.9504. Similarly, the *SE* with respect to parameters a and c when parameter $b = 5$, $r = 1$ is shown in Fig. 4(b), where the *SE* was between 0.9466 and 0.9538, the mean value is 0.9503. As a whole the *SE* values are large within fixed range of parameters and the corresponding chaotic sequences can satisfy the randomness requirements of image encryption.

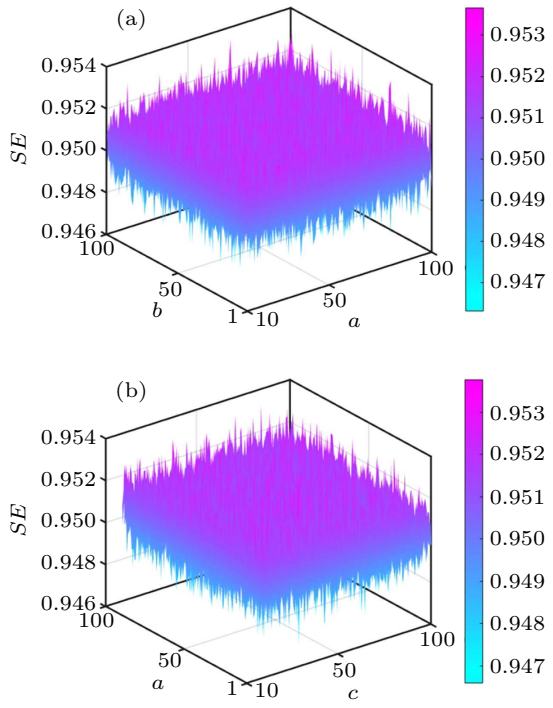


Fig. 4. *SE* complexity varies with the parameters at an initial value (1, 1, 0.1): (a) $a \in (10, 100)$ and $b \in (1, 100)$; (b) $a \in (10, 100)$ and $c \in (1, 100)$.

2.4. DSP implementation

Hyperchaotic systems can be used in the signal processing field to generate pseudorandom signals due to their highly unstable and complex dynamical properties. TMS320F28335 is chosen as the main chip. The maximum operating frequency is up to 150 MHz, providing efficient data processing capability. The verification process is shown in Fig. 5, where the digital signals processed by the chip are processed into analog signals by the DA converter (DAC8552), and the final result is output by oscilloscope. The hyperchaotic map is successfully implemented on digital circuit and provides the reference for practical applications.

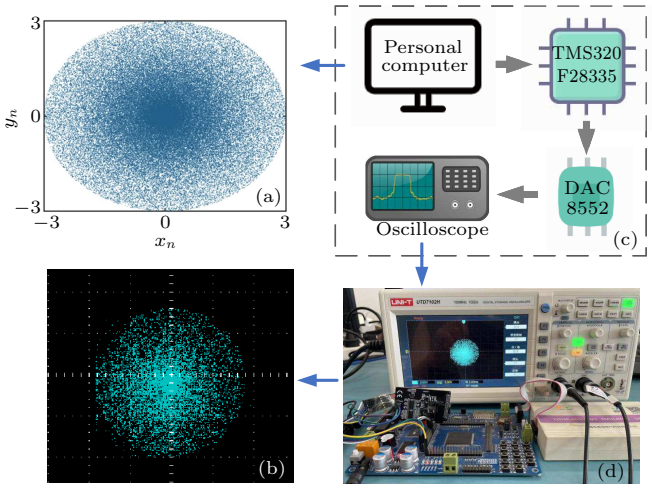


Fig. 5. The hyperchaotic map is validated on DSP platform: (a) simulation results on Matlab, (b) simulation results on oscillosope, (c) DSP hardware connection diagram, (d) physical hardware.

2.5. Randomness test

The security of an encryption algorithm relies not only on the algorithm itself but also on the quality of the random sequence used for encryption. The effectiveness and reliability of chaotic sequences in practical applications are demonstrated by performing NIST tests on them. A chaotic sequence of length 18 millions is generated using the parameters $r = 3$,

$a = 10$, $b = 5$, $c = 1$, and initial values (1, 1, 1). The corresponding binary data serves as the test sample. The results, presented in Table 1, show that all parameters satisfy the criteria of P-value ≥ 0.01 and pass rate $T \geq 0.9628$, confirming that the chaotic sequence can be used for image encryption.

Table 1. NIST test results.

No.	Test	P-value	Pass pate
01	frequency	0.2133	1.00
02	block frequency	0.0428	0.97
03	cum. sums* (F)	0.5749	1.00
	cum. sums* (R)	0.3838	0.98
04	runs	0.3041	1.00
05	longest runs	0.0757	0.99
06	rank	0.4943	0.99
07	FFT	0.9114	0.99
08	non-Ovla. Temp.*	0.9780	1.00
09	over. Temp	0.9240	0.99
10	universal	0.8513	0.97
11	appr. entropy	0.9357	1.00
12	ran. Exc.*	0.1816	1.00
13	ran. Exc. Var.*	0.8677	1.00
14	serial (1st)	0.9357	0.99
	serial (2nd)	0.8165	0.99
15	liner complexity	0.4190	0.99
	success No.	15/15	15/15

3. Encryption and decryption scheme

Hybrid image encryption improves image management, and data security. In this section, an encryption scheme for 2D images, 3D models, and 3D point clouds are proposed.

3.1. Encryption and decryption scheme

The encryption scheme first preprocesses different types of image data and fuses them into a vector then encrypts the resulting vector. The encryption flowchart is shown in Fig. 6. The detailed process outlined below.

Step 1 The 3D model and 3D point cloud are recorded in coordinates, so the coordinate data is first converted to [0, 255], which is consistent with the pixel values of the 2D image.

Step 2 All coordinate data and pixel data are fused into a vector of length b, which is converted into cube $A_{m\times n\times h}$ (m is the length of A, n is the width of A, and h is the height of A. $m = 256$, $n = 256$, $h = \text{ceil}\,(b/(mn))$).

Step 3 A is used as an input to Hash-512 where the resulting Hash sequence can be used for obtaining the initial value of the hyperchaotic map.

Step 4 The chaotic sequence used for encryption becomes the pseudorandom integer.

$$\begin{cases} x = \text{floor}(\,\text{mod}\,(x \times 10^{16}, m)) + 1, \\ y = \text{floor}(\,\text{mod}\,(y \times 10^{16}, n)) + 1, \\ z = \text{floor}(\,\text{mod}\,(z \times 10^{16}, h)) + 1, \end{cases} \tag{3}$$

where mod(·) is a modulo operation and floor(·) is a downward rounding operation.

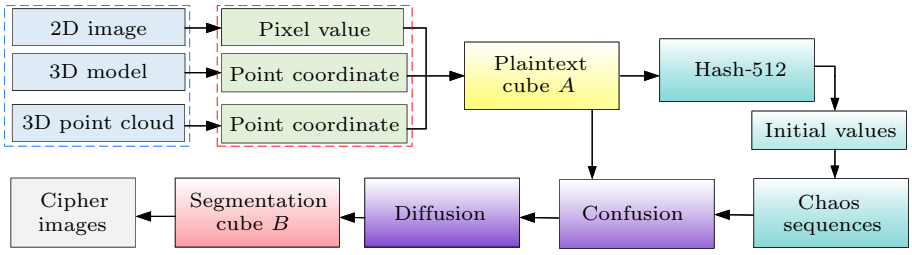


Fig. 6. The encryption flowchart.

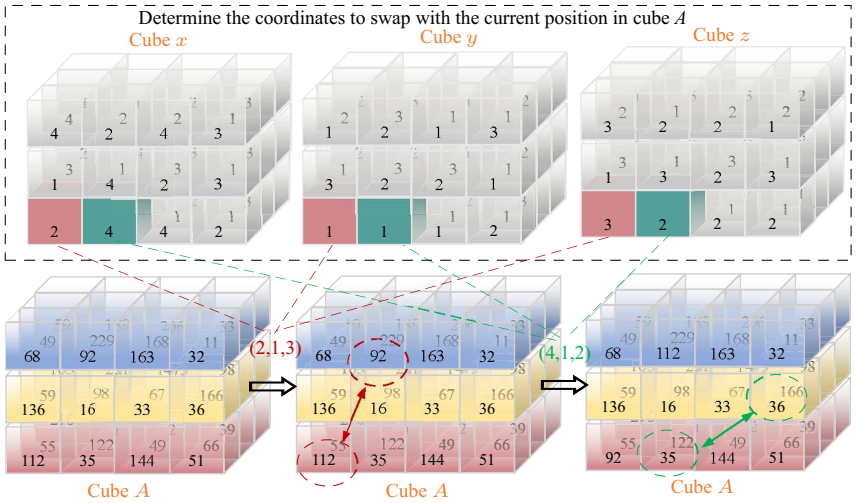


Fig. 7. The example of cube space internal confusion.

Step 5 (Cube space internal confusion) Find a random point in A using the chaotic sequence x, y, z, and swap it with the current value. Two points were chosen as examples as shown in Fig. 7. Swapping the value in coordinates (1, 1, 1) in A with the value in coordinates (2, 1, 3), the next step is to swap the value in (2, 1, 1) with (4, 1, 2). The same operation is done for each point in A as shown in Eq. (4).

$$\begin{cases} P = A(t_1,t_2,t_3), \\ A(t_1,t_2,t_3) = A(x(t_1,t_2,t_3),y(t_1,t_2,t_3),z(t_1,t_2,t_3)), \\ A(x(t_1,t_2,t_3),y(t_1,t_2,t_3),z(t_1,t_2,t_3)) = P, \end{cases} \tag{4}$$

where $t_1 = [1:m]$, $t_2 = [1:n]$, $t_3 = [1:h]$, and P is the variable that stores the current value of A.

Step 6 (Dynamic cross-diffusion) Modulo operation is applied to even faces as shown in Eq. (5) and the XOR operation is applied to odd faces as shown in Eq. (6), and the ciphertext cube B is obtained after the diffusion process is completed.

$$B(t_1,t_2,t_3) = \begin{cases} \mathrm{mod}\,(A(t_1,t_2,t_3)+u(t_1,t_2,t_3),256), & t_1 = 1, \\ \mathrm{mod}\,((\mathrm{mod}\,(A(t_1,t_2,t_3)+u(t_1,t_2,t_3),256)+A(t_1-1,t_2,t_3)),256), & t_1 \neq 1, \end{cases} \quad t_3 = 2,4,6,\ldots, \tag{5}$$

$$B(t_1,t_2,t_3) = \begin{cases} A(t_1,t_2,t_3) \oplus u(t_1,t_2,t_3), & t_1 = 1, \\ (A(t_1,t_2,t_3) \oplus u(t_1,t_2,t_3)) \oplus A(t_1-1,t_2,t_3), & t_1 \neq 1, \end{cases} \quad t_3 = 1,3,5,\ldots, \tag{6}$$

where u is the pseudorandom sequence for diffusion obtained by $u = (x+y+z)/3$.

Step 7 Segmenting the ciphertext cube B into corresponding individual ciphertext images based on the recorded image size.

3.2. Decryption scheme

Decryption is reverting the encrypted data to the original data, matching the encryption process. The original pseudorandom sequence is obtained by inputting parameter values and initial values. The cube B is reduced to cube A by inverse diffusion and inverse confusion, and then A is segmented into individual images according to the size. Figure 8 is the corresponding decryption flowchart.

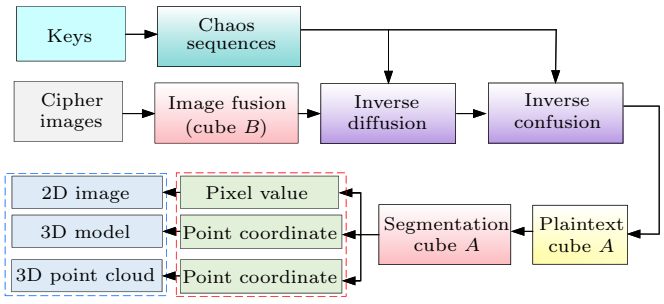


Fig. 8. The decryption process.

3.3. Simulation results

To test the encryption scheme, two 2D images, two 3D models, and two 3D point clouds are inputted. These are "5.1.14", "airplane", "hummer", "banana", "chair", and "skull" are shown in Figs. 9(a)–9(f). The data are fused into the cube A as shown in Fig. 9(g). Confusion and diffusion are applied to cube A to obtain the ciphertext cube B, which is segmented into individual images as in Fig. 10(a). The decrypted image is Fig. 10(b). The simulation results indicate that the encryption scheme effectively conceals the information contained in the images.

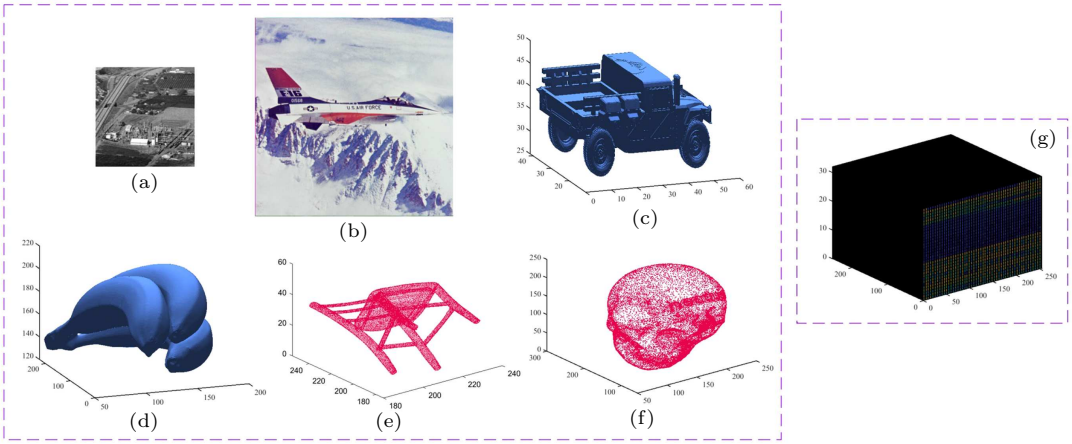


Fig. 9. Original images and cube B: (a) 5.1.14, (b) airplane, (c) hummer, (d) banana, (e) chair, (f) skull, (g) cube A.

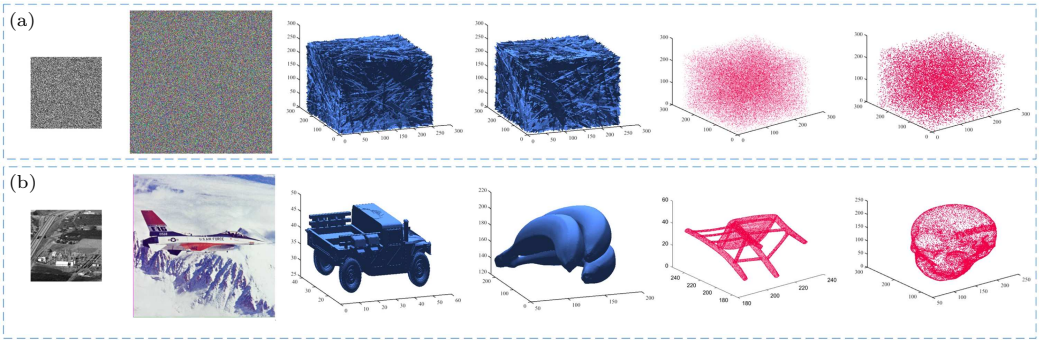


Fig. 10. Cipher images and corresponding decrypted images: (a) cipher images, (b) decrypted images.

4. Security analysis

4.1. Key space

It is important for an encryption scheme to have the ability to prevent brute force attacks. The difficulty of breaking it by brute force increases with a larger key space. In general, encryption schemes with a key space of more than 2^{100} are considered to be effective against brute force attacks.[42] The key space of the scheme consists of three initial values and four parameters of the hyperchaotic map. The key space is calculated by slightly changing each key based on whether the image can be successfully reverted or not. The total key space shown in Table 2 is 2^{358}. It takes a lot of time and strong arithmetic power to brute force break this encryption algorithm. Table 3 presents other encryption schemes, revealing that this scheme has a larger key space in comparison.

Table 2. Key space.

Keys	a, b, c, r	x_0, y_0, z_0	Total
Space	10^{15}	10^{16}	$10^{108} \approx 2^{358}$

Table 3. Key spaces of different schemes.

Scheme	Ref. [43]	Ref. [44]	Ref. [45]	Ref. [46]	Proposed
Key space	2^{212}	2^{186}	2^{196}	2^{289}	2^{358}

4.2. Key sensitivity

Key sensitivity refers to the effect of key changes on the cipher image. In encryption schemes characterized by high key sensitivity, even a minor alteration in the key can result in a considerable change in the cipher image, making the key more difficult to crack. Keeping the remainder of keys unchanged, add 10^{-15} to key c. The cipher images obtained by inputting keys c and $c+10^{-15}$ are denoted as $F1$ and $F2$, respectively. The image "airplane", as an example, is shown in Fig. 11. The difference between cipher images is measured by $F = |F1 - F2|$. F was calculated for "5.1.14", "airplane", "hummer", "banana ", "chair", and "skull". The histogram of F is displayed in Fig. 12, with fewer zeros indicating that $F1$ and $F2$ differ from each other and that the encryption scheme has higher key sensitivity.

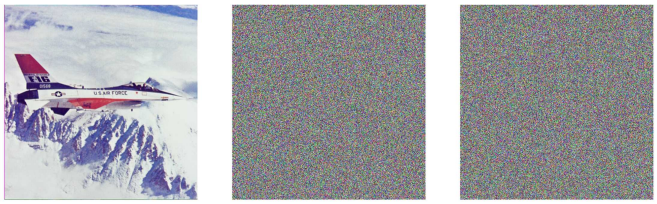


Fig. 11. Image "airplane" plaintext image and cipher image: (a) plaintext image, (b) cipher image $F1$, (c) cipher image $F2$.

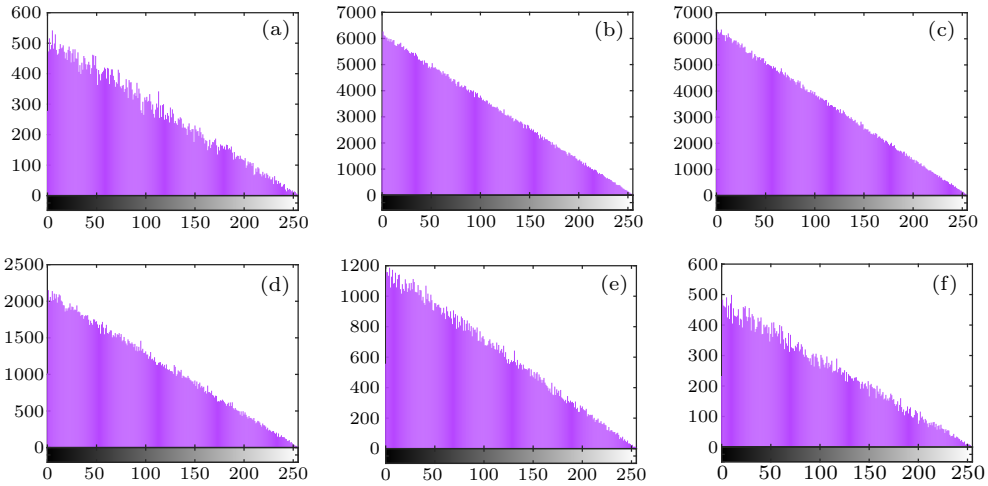


Fig. 12. Histograms for different F: (a) 5.1.14, (b) airplane, (c) hummer, (d) banana, (e) chair, (f) skull.

4.3. Information entropy

Information entropy (IE) serves as a measure of the uncertainty associated with a random variable. The larger IE in an image means fewer visual cues. Comparing the IE of the original image and the cipher image provides a method for evaluating the security. When calculating the IE, the data corresponding to all images are processed between [0, 255], and the maximum value of IE is 8 from Eq. (7).[47] It can be seen from Table 4 that the IE of all the ciphertext images is closer to 8 compared to the IE of the original images, which indicates that the information of the cipher images has greater randomness. It is difficult to infer the content of the original images from the statistical features.

$$H = \sum_{i=0}^{255} p(i)\log_2 \frac{1}{p(i)}, \tag{7}$$

where $p(i)$ is the probability of the i occurring.

Table 4. Information entropy.

	5.1.14	Airplane	Hummer	Banana	Chair	Skull
Original image	7.3424	6.6639	5.3113	7.4669	6.6153	7.7552
Cipher image	7.9969	7.9992	7.9992	7.9988	7.9984	7.9964

4.4. Histograms

The pixel data of the 2D images and the coordinate data of the 3D images can be plotted in a histogram to visually determine whether they are uniformly distributed or not. The histogram of the original images shows the clear tendency of concentration in Fig. 13. From the histogram of the cipher images, it can be seen that the number of occurrences of each value is close to each other, and the histogram is more uniformly distributed. The information of the original images will not be leaked by the histogram of the cipher images.

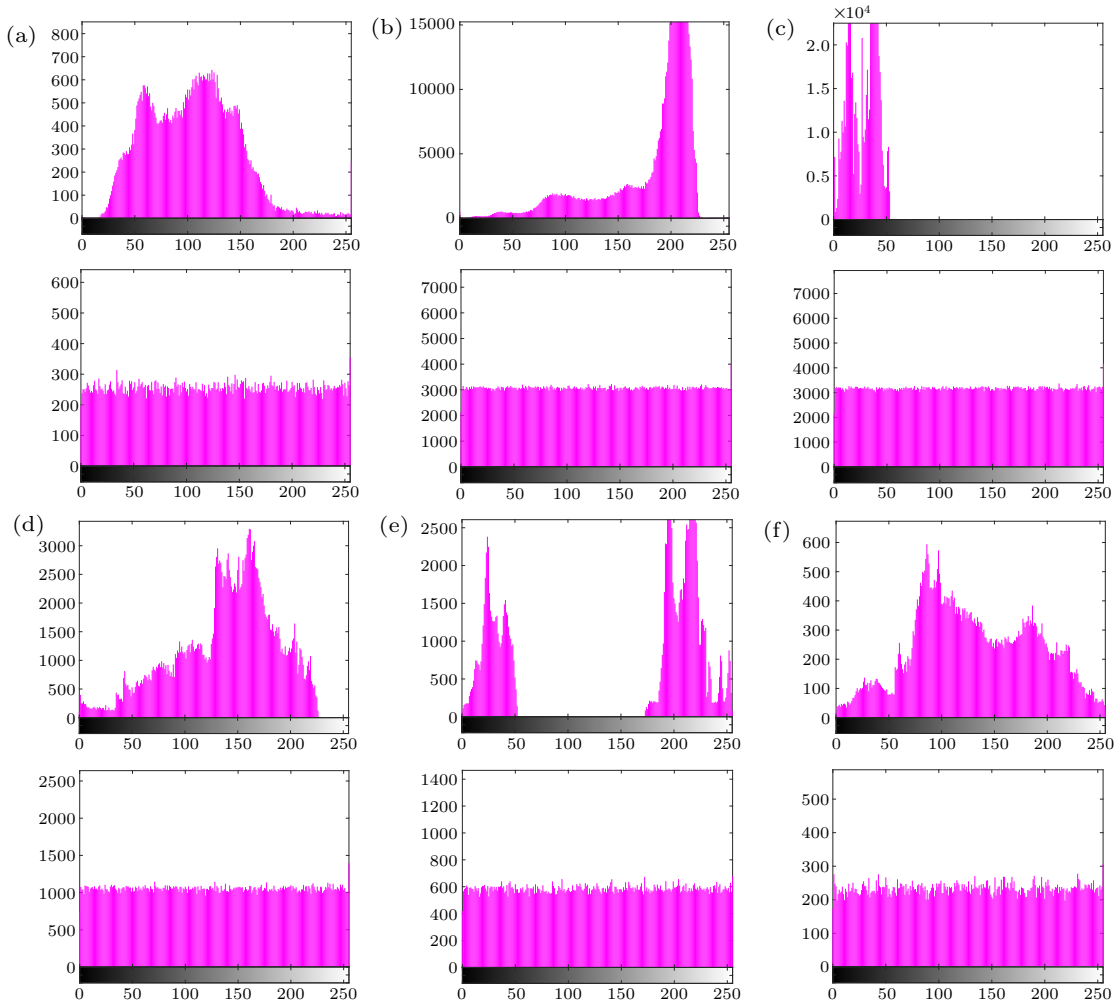


Fig. 13. Histogram of original images and cipher images: (a) 5.1.14, (b) airplane, (c) hummer, (d) banana, (e) chair, (f) skull.

4.5. Correlation

Correlation reflects the relatedness of adjacent pixels/coordinates in an image. Encryption schemes focus more on correlation reduction to prevent attackers from getting the original image data. The "5.1.14" and "chair" are chosen as test objects. The adjacent pixels/coordinates are tested as displayed in Fig. 14. The adjacent pixels/coordinates of the original images are very dense around the line with slope 1 as shown in Figs. 14(a) and 14(c), showing the strong correlation. The adjacent pix-

els/coordinates of the cipher images are randomly distributed over the whole graph as in Figs. 14(b) and 14(d). The results show that the proposed encryption scheme greatly reduces the correlation between adjacent pixels/coordinates.

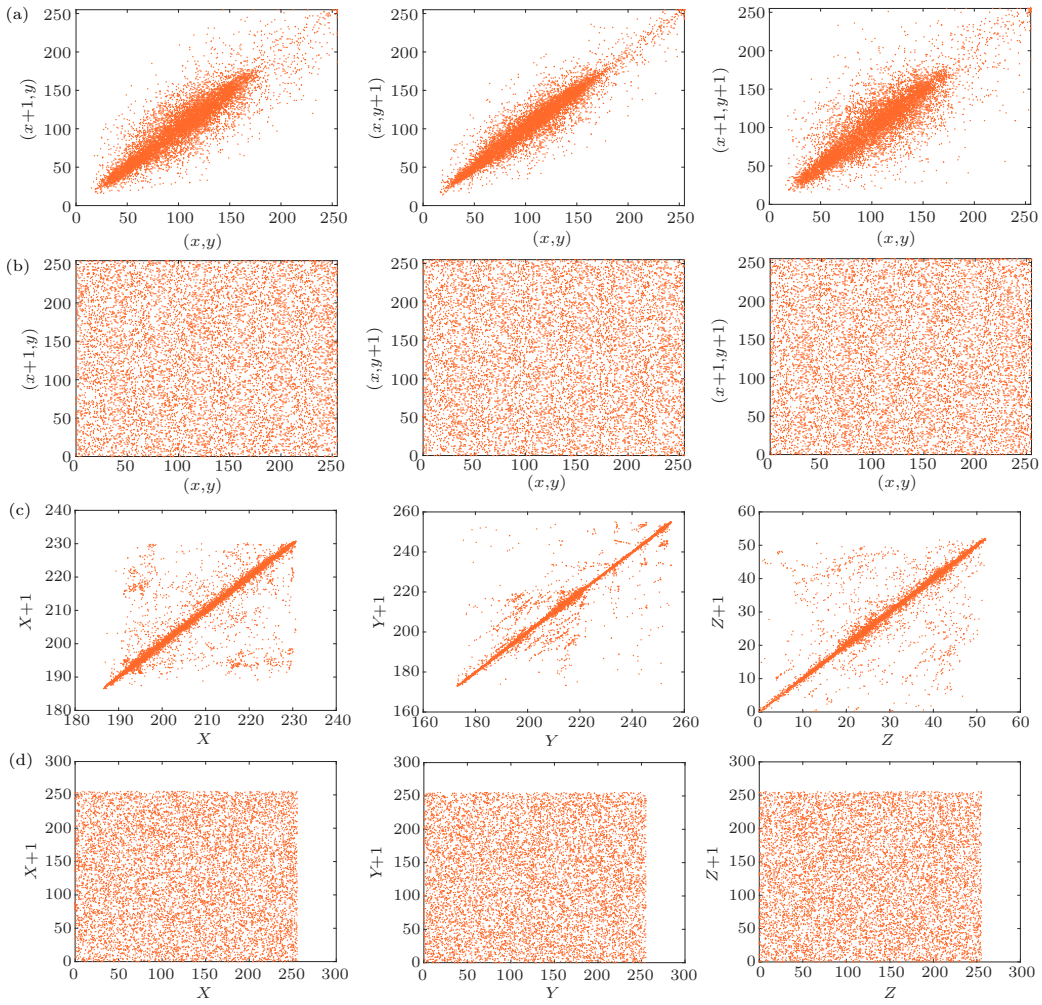


Fig. 14. Correlation analysis of "5.1.14" and "chair": (a) 5.1.14, plaintext; (b) 5.1.14, cipher; (c) chair, plaintext; (d) chair, cipher.

4.6. Differential attack

When the plaintext is modified, trying to break the encryption scheme based on the different information of the corresponding cipher image is called differential attack. If small changes of the plain image have significant effects on the cipher image, the encryption scheme is considered to be resistant to differential attacks. The difference between both cipher images is quantified by NPCR and UACI respectively, which are typically 99.6094% and 33.4635%.[48] The test results are displayed in Table 5.

Table 5. Differential attack.

	5.1.14	Airplane	Hummer	Banana	Chair	Skull	Mean
NPCR (%)	99.6201	99.6070	99.6175	99.6089	99.6170	99.6334	99.6173
UACI (%)	33.4547	33.4516	33.4639	33.4636	33.4616	33.4608	33.4594

By comparing its average value with other encryption schemes, as illustrated in Table 6, it is evident that the NPCR is higher and the UACI is closer to the theoretical value. This indicates that the differences between the two cipher images are more pronounced. The above analysis shows that it is difficult for an attacker to break the encryption scheme from a large number of different messages.

Table 6. Comparison of differential attacks.

Scheme	NPCR (%)	UACI (%)
Ref. [44]	99.6127	33.4765
Ref. [49]	99.6000	33.4500
Ref. [50]	99.6060	33.5126
Ref. [51]	99.6067	33.4467
Ref. [52]	99.5084	33.4824
Proposed	99.6116	33.4612

5. Conclusion

In this paper, a hyperchaotic map with spherical attractors is constructed based on spherical coordinates. Dynamical analysis reveals that, when the parameters are varied within the selected range, three LEs are greater than 0. The parameter r can control the size of the chaotic attractor. In addition, it is also found that the system has global hyperchaos and high complexity, which can be used for image encryption not only with flexible parameter selection but also with enhanced security. Therefore, a hybrid encryption scheme is proposed with this chaotic system, aiming to solve the security protection problem of 2D images, 3D models, and 3D point clouds. The images are encrypted using cube space internal confusion and dynamic cross-diffusion. Statistical attacks are analyzed and the results show that the encryption scheme can well destroy the visual representation ability of the original image. The large key space and key sensitivity enable the encryption scheme to cope with exhaustive attacks. The results of the differential attack show that it is difficult for an attacker to break the encryption scheme from a large amount of differential information. This paper presents a novel and effective method for encrypting hybrid images. Future work could explore the use of varying encryption strengths for different types of images, enabling more efficient resource utilization and simplifying operations.

Acknowledgements

Project supported by the Basic Scientific Research Projects of Department of Education of Liaoning Province, China (Grant No. LJ212410152049), and the Technological Innovation Projects in the field of artificial intelligence of Liaoning Province, China (Grant No. 2023JH26/10300011).

References

[1] Wang R and Ji W 2020 *IEEE Transactions on Emerging Topics in Computational Intelligence* **4** 616
[2] Mou J, Zhang Z, Banerjee S and Zhang Y 2024 *IEEE Internet of Things Journal* **11** 33565
[3] Gong M, Chai X, Lu Y and Zhang Y 2024 *IEEE Transactions on Circuits and Systems for Video Technology* **34** 7628
[4] Zhang Z, Tang J, Zhang F, Huang T and Lu M 2024 *IEEE Transactions on Circuits and Systems for Video Technology* **34** 9250
[5] Zhang Z, Zhou N, Sun B, Banerjee S and Mou J 2024 *Journal of the Franklin Institute* **361** 106844
[6] Tan L, Cao Y, Banerjee S and Mou J 2025 *The Journal of Supercomputing* **81** 96
[7] Li Z, Wang Y, Zhang N, Zhang Y, Zhao Z, Xu D, Ben G and Gao Y 2022 *Remote Sensing* **14** 2385
[8] Cai C, Wang Y, Cao Y, Sun B and Mou J 2024 *Applied Intelligence* **54** 5944
[9] Tian J, Jin S, Zhang X, Yang S and Shi D 2024 *Chin. Phys. B* **33** 050502
[10] Ma Z and Liu S 2018 *Advanced Engineering Informatics* **37** 163
[11] Nurunnabi A, West G and Belton D 2015 *Pattern Recognition* **48** 1404
[12] Kedzierski M and Fryskowska A 2015 *Measurement* **74** 221
[13] Cao Y, Tan L, Xu X and Li Bo 2024 *Mathematics* **12** 1990
[14] Mou J, Zhang Z, Zhou N, Zhang Y and Cao Y 2024 *IEEE Internet of Things Journal* **2024** 1
[15] Su J, Hong Y, Fang S and Wen Y 2024 *Chin. Phys. B* **33** 070502
[16] Zhu J, Cao Y, Mou J and Banerjee S 2024 *International Journal of Bifurcation and Chaos* **34** 2450140
[17] Chen Y, Cao Y, Mou, J, Sun B and Banerjee S 2024 *International Journal of Bifurcation and Chaos* **34** 2450069
[18] Cai C, Cao Y, Jahanshahi H, Mou J and Sun B 2024 *Journal of the Franklin Institute* **361** 106874
[19] Ma T, Mou J, Banerjee S and Cao Y 2023 *Chaos, Solitons and Fractals* **176** 114113
[20] Shi F, Cao Y, Banerjee S, Ahmad A M and Mou J 2024 *Chaos, Solitons and Fractals* **189** 115723
[21] Feng W, Yang J, Zhao X, Qin Z Zhang J, Zhu Z, Wen H and Qian K 2024 *Mathematics* **12** 3917
[22] Cao H, Cao Y, Xu X and Mou J 2024 *Physica Scripta* **99** 085226
[23] Matthews R 1989 *Cryptologia* **13** 29
[24] Zhou Y, Bao L and Chen C P 2014 *Signal Processing* **97** 172
[25] Cheng Z, Wang W, Dai Y and Li L 2022 *Complexity* **2022** 1720842
[26] Cao H, Cao Y, Qin L and Mou J 2025 *Chaos, Solitons and Fractals* **191** 115857
[27] Wang L, Banerjee S, Cao Y, Mou J and Sun B 2024 *Nonlinear Dyn.* **112** 8637
[28] Chen L, Li C and Li C 2022 *Journal of Visual Communication and Image Representation* **83** 103424
[29] Wu X, Hu H and Zhang B 2004 *Chaos, Solitons and Fractals* **22** 359
[30] Liu S, Li C and Hu Q 2021 *IEEE MultiMedia* **29** 74
[31] Feng W, Zhang J, Chen Y, Qin Z, Zhang Y, Ahmad M and Woźniak M 2024 *Expert Systems with Applications* **246** 123190
[32] Ma Y, Mou J, Jahanshahi H Alkhateeb A F and Bi X 2024 *Chaos, Solitons and Fractals* **173** 113708
[33] Lima V S, Madeiro F and Lima J B 2020 *Computers in Biology and Medicine* **121** 103772
[34] Raghunandan K, Dodmane R, Bhavya K, Rao N K and Sahu A K 2022 *IEEE Access* **11** 3545
[35] Yang W, Huang J, He X and Wen S 2024 *Neural Networks* **172** 106089
[36] Gao S, Wu R, Wang X, Wang J, Li Q, Wang C and Tang X 2023 *Signal Processing* **202** 108745
[37] Xian, Y, Wang X, Teng L, Yan X, Li Q and Wang X 2022 *Information Sciences* **596** 304
[38] Zhao R, Zhang Y, Li S, Wen W, Yi S and Lan R 2024 *Expert Systems with Applications* **238** 122140
[39] Zhang Z Y, Mou J, Banerjee S and Cao Y H 2024 *Chin. Phys. B* **33** 020503
[40] Zhang H, Hu H and Ding W 2024 *Information Sciences* **665** 120332
[41] Mou J, Cao H, Zhou N and Cao Y 2024 *IEEE Transactions on Cybernetics* **54** 7333
[42] Zhang Z, Mou J, Zhou N, Banerjee S and Cao Y 2022 *Nonlinear Dyn.* **112** 5727
[43] Cun Q, Tong X, Wang Z and Zhang M 2023 *The Visual Computer* **39** 6589
[44] Xu M 2023 *Optics and Laser Technology* **167** 109746
[45] Kumar C M, Vidhya R and Brindha M 2022 *Applied Intelligence* **52** 2556
[46] Xian Y, Wang X, Zhang Y, Yan X and Leng Z 2023 *Multimedia Tools and Applications* **82** 407
[47] Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan J P and Natarajan P 2013 *Information Sciences* **222** 323
[48] Ye G, Wu H, Huang X and Tan S 2023 *Chin. Phys. B* **32** 030504
[49] Zhou S, Wang X, Zhang Y, Ge B, Wang M and Gao S 2022 *Multimedia Systems* **28** 95
[50] Zhang X and Hu Y 2021 *Optics and Laser Technology* **141** 107073
[51] Zhou Z, Xu X, Yao Y, Jiang Z and Sun K 2023 *Chaos, Solitons and Fractals* **173** 113630
[52] Zhang L and Zhang X 2020 *Multimedia Tools and Applications* **79** 20753