




An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding

Qingfeng Li¹ · Lei Chen¹ 

Received: 28 February 2022 / Revised: 5 November 2022 / Accepted: 19 April 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Image encryption algorithm based on chaos has been widely used in various industries, but many image encryption algorithms based on low-dimensional chaos, resulting in the security of these encryption algorithms can not meet the requirements. In order to address the challenge, this paper proposes an image encryption algorithm based on 6D high-dimensional chaotic system and DNA encoding technique. First, the original image sequences is diffused and shuffled by several random chaos sequences. Second the generated sequences are diffused and shuffled by different chaos sequences on DNA level. At last, the different encoded sequences are combined into an encrypted image. The experimental results show that compared with the reference, the proposed algorithm has certain advantages in image entropy(value infinitely close to 8), pixel correlation and image complexity(key space larger than 2^{300}), and also has good robustness against geometric and cut-off attacks.

Keywords 6D hyper chaos · Color image encryption · DNA encoding · Correlation analysis · Shear attack

1 Introduction

With the rapid development of communication, billions of images are transmitted over the public network. Many applications like medical imaging system, military image databases, etc., require more reliable, faster security system to store and transmit digital images [1–3]. Therefore, protecting the security of digital images have become vital issues. Under the circumstances, three methods including encryption, steganography and watermarking [4] have been proposed. Among these three methods, as it has higher level security, the encryption

✉ Lei Chen
clei@xatu.edu.cn

Qingfeng Li
descosmos@163.com

¹ Xi'an Technological University Xi'an, 710021, Shaanxi Province, China

has become one of the primary tools. In last few decades, many image encryption techniques have proposed by using various methods [5]. Among them, plenty of ciphers exist like AES, DES, IDEA, RSA etc. have been adopted for the encryption. Nonetheless, the majority of these methods only work on the textual information. Not use for the image encryption for the reason is that the image has the properties of images like well-built inter-pixel correlation, great volume and high redundancy. In order to address the issue, some scholars have been proposed a variety of encryption schemes [5–9]. Among these methods, the encryption algorithm based on chaos is paid more attention than other encryption algorithms because chaos is sensitive to initial conditions and system parameters, which results in better performance of chaos than traditional encryption algorithms in terms of non-periodicity, randomness and unpredictability [10, 11]. For the above reasons, chaos-based encryption algorithm has been developed rapidly. In general, chaotic cryptosystem uses the sequences to shuffle the position of each pixel of the original image. Additionally, apply diffusion operation in chaotic sequences is also a universal method in image encryption.

In general, chaotic system has two categories including low-dimensional chaotic system and high-dimensional chaotic system. The first type of chaotic system usually generates one or two chaotic streams, in contrast, high-dimensional system usually generates three or more chaotic streams. In 1991, Habustu, et al. proposed an image encryption algorithm based on chaos theory [12], which enhanced the development of chaos-based image encryption algorithm. After that, many image encryption algorithms have been proposed. For instance, Hua Z presented an image encryption algorithm [13] based on "2D Logistic-Sine coupling map", the algorithm is based one of the typical coupling map combining the Logistic and Sine map; Pareek.N proposed an image encryption using one-dimensional chaotic logistic map, the algorithm is different by the secret key is modified after encrypting each block of sixteen pixels of the image [1]. Chanil Pak proposed a color image encryption using combination of the new 1D chaotic map [14], the experimental results of algorithm proposed by Chanil has better performance than most low-dimensional chaos-based image encryption algorithms. Except these, many image encryption algorithms based on various low-dimensional chaotic system have developed [15–17]. However, with the rapid development of modern communication, low-dimensional encryption cannot meet the requirements due to security problems, for which, high-dimensional encryption methods have been developed rapidly. Guarnong proposed a symmetric image encryption scheme based on 3D chaotic Cat maps [2], the algorithm is the one of the milestones in the development of hyper-chaotic based image encryption algorithm. Mao YB proposed a fast image encryption scheme based on 3D baker map [9, 10], comparing with other algorithms listed in his paper, the algorithm has better performance in time complexity. Adrian-Viorel Diaconu presented a color image scrambling technique through Transposition of Pixels between RGB Channels Using Knight's Moving Rules and Digital Chaotic [18]. Gao Xiaohong proposed a color image encryption based on an improved Hénon map [19], comparing with classical Hénon map, the improved Hénon map has more rich chaotic behaviors and better complexity, which leading the algorithm has better performance. Except these, other researchers also proposed many image encryption algorithm based on high-dimensional chaotic system [20–22]. Recent years, many encrypt methods based on hyper-chaotic and DNA encoding have been proposed, according to the characteristic of DNA computing, such as huge storage, ultra-low power consumption and large scale parallelism [15–17, 22]. Meantime, due to the superiority of bit-level permutation, several image encryption algorithms adopt it to disturb the relationship among pixels [19, 23, 24]. Besides, several algorithms combine the low chaotic system with other methods also make a great performance. [25] proposed a method based

on chaotic system and Sub-block Spiral Scans and Matrix Multiplication in 2022, [26] also implemented a fast image encryption algorithm based on single-channel encryption and chaotic system.

The methods proposed in the above papers are either based on low-dimensional chaotic systems, which leads to insufficient complexity, or based on DNA coding, which leads to easy cracking. To overcome these weakness, in this paper, we introduced a color image encryption algorithm based on 6D hyper-chaotic system and DNA encoding. The contributions and novelty of this paper are introduced in the following. First, we take a more complex 6D hyper-chaotic system as the random stream generator, the system generates six different chaotic streams with key and the characteristics of original image. Then, this paper separate the six streams into two groups which are used to permute and diffuse respectively. For the efficiency and security of permutation, this paper pixel-level and DNA-level permutations are implemented, which ensure the relationship of pixels between the original image and encrypted image is weak enough. Obviously, the two permutation processes make the image encryption algorithm can resist shear-attack efficiently. Since the permutation does not change the distribution and average of pixels, this paper carry out the pixel-level and DNA-level diffusion operations on the chaotic images after the permutation. In order to verify the algorithm, this paper adopts key space, key intensity, histogram, correlation and other analysis to evaluate the proposed algorithm. The results demonstrate that the algorithm has better performance against state-of-arts methods.

Among the remaining sections of this paper, Section 2 reviews the 6D hyper-chaotic system and DNA computing technology. Section 3 describes the detail of the encryption and decryption algorithm. Section 4 gives our experimental results, including qualitative illustration and qualitative analysis and comparison to the state-of-arts. Section 5 conclude the paper and purpose future work.

2 Building blocks

2.1 Chaotic system

Nowadays, many researchers proposed image encryption algorithms based on chaos. Some of them use low-dimensional chaotic system to generate pseudo-random sequences to encrypt the original image, the other apply the hyper-chaotic system to the cryptosystem. As a classical chaotic system, Lorenz chaotic system has been implemented in many chaos-based encryption algorithms. The formula of Lorenz chaotic system is proposed in 1963 and illustrated as formula 1 [27]. In the formula 1, x , y and z are the system values, while a , b and c are system parameters.

$$D(x) = \begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - y - xz \\ \dot{z} = -bz + xy \end{cases} \quad (1)$$

As time went by, due to the complexity of the classical Lorenz chaotic system cannot meet the increasing needs of security in communication, more and more higher-dimension chaotic system has been proposed. In 2009, after introduced a linear feedback controller and non-liner feedback controller to the classical Lorenz system, the subsequent 5D

hyper-chaotic system is derived [28].

$$D(x) = \begin{cases} \dot{x} = \sigma(y - x) + u \\ \dot{y} = rx - y - xz - v \\ \dot{z} = -\beta z + xy \\ \dot{u} = k_1 u - xz \\ \dot{v} = k_2 \end{cases} \quad (2)$$

In the 5D hyper chaotic system σ , r , k_1 , β and k_2 are system control parameters, where $k_1 > 0$ and $k_2 > 0$. There are one equilibrium and a hyper chaotic attractor with three positive Lyapunov exponents can be generated by the system. Generally, the more hyper-chaotic attractor the chaotic system has, the more complex the chaotic system will be. Therefore, it is no doubt that the 5D hyper chaotic system performance much more complex behavior than the classical Lorenz system.

However, the requirement of security is never limited, in order to make the chaotic system more complex and unpredictable, the 6D hyper-chaotic system was proposed. In this paper, algorithm adopt the 6D hyper-chaotic system which is proposed by [29]. The 6D hyper-chaotic system can be generated by coupling a 1D linear system and a 5D hyper-chaotic system, as show formula 3.

$$D(x) = \begin{cases} \dot{x} = \sigma(y - x) + u \\ \dot{y} = cx - y - xz + v \\ \dot{z} = -bz + xy \\ \dot{u} = du - xz \\ \dot{v} = -ky \\ \dot{w} = hw + ly \end{cases} \quad (3)$$

The 6D hyper chaotic system has 13 terms, which contains six system values x , y , z , u , v , w and seven parameters a , b , c , d , h , k , l , where $a, b, h, k, l \neq 0$, a, b, c and h are constant parameters, l is the coupling parameter, d and k are two control parameters, which affect the system behavior and bifurcations of system. Different from the 5D hyper-chaotic system, the 6D hyper-chaotic system has six Lyapunov exponents. Four of them are positive, which means that the 6D hyper-chaotic system has better performance in complexity and unpredictability than the 5D hyper-chaotic system. According to the paper of Qigui Yang [29], a, b, c and h are the constant parameters, the range of other parameters are $k \in [7.3, 60.5]$, $d \in [1.12, 1.99]$, $l \in [-14.61, 22.9]$.

2.2 DNA encoding

A typical DNA molecule has two anti-parallel strands, which consists four types of bases including adenine(A), thymine(T), cytosine(C) and guanine(G). These strands/bases have a complementary relationship described as A only bonding to T and G only bonding to C. The encryption based on DNA technology is called biological cryptology [30]. Traditional biological cryptography is limited by high cost and high requirements on laboratory environment, so pseudo DNA technology has become an important aspect of cryptography. [31]. As shown in Table 1, there are 8 rules following the Watson-Crick complementary rules out of the $4 \neq 24$ kinds of encoding merely. The various binary operations of DNA bases, such as addition, subtraction, and XOR, are shown in Table 2.

In this paper, only XOR operation is implemented. Two functions $DNA_{encoding}$ and $DNA_{decoding}$ has been defined and used in the encryption and decryption respectively. As the name demonstrates that, the function $DNA_{encoding}$ transforms the given image

Table 1 DNA paring rules

Rule	1	2	3	4	5	6	7	8
00	A	A	T	T	G	G	C	C
01	C	G	G	C	A	T	A	T
10	G	C	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

pixel into its reciprocal DNA base equivalent. On the contrary, the function $DNA_{decoding}$ performs the reverse procedure. Based on ASCII [24], for instance:

$dna_encoding(45, 1) = AGTC$

$dna_encoding(8, 3) = TTCT$

$dna_decoding(AGTC, 1) = 45$

$dna_decoding(TTCT, 1) = 8$.

Consequently, $XOR(AGTC, TTCT) = TCGG$ for the DNA XOR operation.

3 Proposed image encryption and decryption systems

This paper proposed a color image encryption scheme designed by the 6D hyper chaotic system and DNA encoding. Digital color image consists of three primary color matrices R, G, B. Accordingly, the digital color image is encrypted via encrypt R, G, B primary colors. In this paper, digital color image encryption scheme is illustrated in Fig. 1.

3.1 Encryption algorithm system

The flow chart of the encryption is demonstrated in Fig. 1. Given an $M * N * 3$ plain color image P, corresponding matrix A_1 , the encryption steps are shown as follows:

Step1: Calculate the size of matrix A_1 and obtaining the length M and width N .

Step2: Obtain the initial values including system values x, y, z, u, v, w . And we take system interference and system threshold as *key*. After that, system parameters a, b, c, d, h, k, l and *key* are generated by a random number generator which implemented in Monte Carlo method. The seed of the random number generator is UNIX timestamp, which ensures the randomness of the generator to the greatest extent.

Step3: Direct the key and the size of A_1 to 6D hyper chaotic system, iterating $(threshold + max(M, N))$ times to generate the chaotic sequences consist of x, y, z, u, v, w . Meantime, add interference to the 6D hyper chaotic system by using

Table 2 DNA XOR operation

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

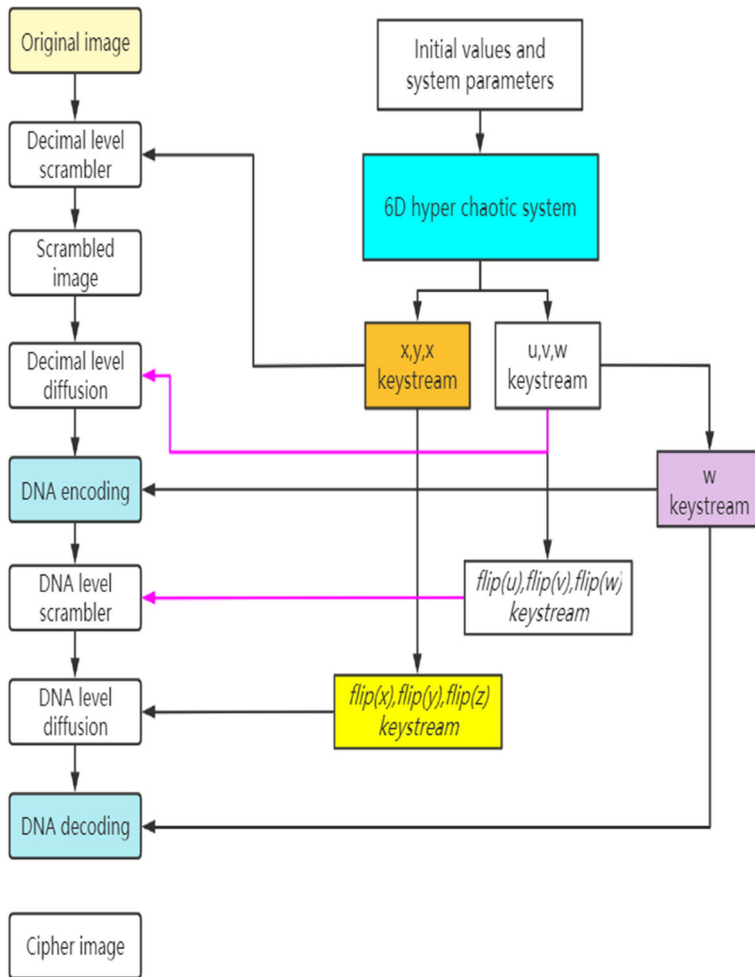


Fig. 1 image encryption scheme

$value = value + interference * \sin(value)$ as system values, the interference makes the chaotic sequences more complex.

Step4: Six chaotic sequences are derived by formula 4:

$$\begin{cases} x(t) = \text{mod}(x(t-1) + i * (\sin(x(t-1))), p) \\ y(t) = \text{mod}(y(t-1) + i * \sin(y(t-1)) * \sin(x(t-1)), p) \\ z(t) = \text{mod}(z(t-1) + i * \sin(z(t-1)) * \sin(y(t-1)) * \sin(x(t-1)), p) \\ u(t) = \text{mod}(u(t-1) + i * \sin(u(t-1)), p) \\ v(t) = \text{mod}(v(t-1) + i * \sin(v(t-1)) * \sin(u(t-1)), p) \\ w(t) = \text{mod}(w(t-1) + i * \sin(w(t-1)) * \sin(v(t-1)) * \sin(u(t-1)), p) \end{cases} \quad (4)$$

Step5: Separate the six chaotic sequences into two matrices $S_1(x, y, z)$ and $S_2(u, v, w)$ the size of S_1 and S_2 are $M * N * 3$. After that, transform the type of chaotic matrices

from *double* to *uint8*.

$$\begin{cases} S_1(t) = \text{mod}(\text{floor}(S_1, M * N) + 1, t \in [1, M * N * 3]) \\ S_2(t) = \text{mod}(\text{floor}(S_2, M * N) + 1, t \in [1, M * N * 3]) \end{cases} \quad (5)$$

Step6: Decimal permutation:

1. Initialize a zero matrix of size $M * N * 3$ as scrambled image named as $A_2(M * N * 3)$.
2. Each pixel of A_1 is disturbed by S_1 in A_2 . In this step, S_1 is divided into three parts including $S_1 1$, $S_1 2$ and $S_1 3$, which are used to take scrambling operation with three dimensions (R, G, B) of plain matrix A_1 .

$$\begin{cases} \text{Swap}(A_1 1(t), A_1 2(S_1 1(t)), t \in [1, M * N]) \\ \text{Swap}(A_1 2(t), A_1 2(S_1 2(t)), t \in [M * N, 2 * M * N]) \\ \text{Swap}(A_1 2(t), A_1 3(S_1 3(t)), t \in [2 * M * N, 3 * M * N]) \end{cases} \quad (6)$$

$$A_2(t) = A_1(t), t \in [1, M * N * 3] \quad (7)$$

Where, the matrix A_2 is the image after Decimal permutation operation. This Step depends on the randomness of chaotic matrix S_1 , for that, the 6D hyper chaotic system ensure the randomness.

Step7: Decimal Diffusion: Initialize a zero matrix as diffused image named $A_3(M * N * 3)$. Each pixel of A_2 is taken bit XOR operation of chaotic matrix S_2 .

$$A_3 = \text{bitxor}(A_2(t), S_2(t)), t \in [1, M * N * 3] \quad (8)$$

Step8: Performed DNA encoding according step by coding rules Table 1 and obtain matrix A_4 :

$$A_4 = \text{DNA}_{\text{encoding}}(A_3, w_i), w_i \in [1, 8] \cap i \in [1, 3 * M * N] \quad (9)$$

Function *DNA_encoding* transforms the decimal matrix A_3 into DNA matrix A_4 , where w_i is the one of eight legal combinations in Table 1. Finally, the function return the DNA encoded sequences or matrixes, which corresponding to the specific rule w_i . It is to be noted that the chaotic sequence w is implemented to generate the rules through $\text{mod}(\text{floor}(w), 8) + 1$, every decimal pixel is divided into four DNA bases $(w_i)_{i=1}^{3MN} = 1$.

Step9: In this step, the DNA encoding matrix is implemented to take *DNA_scrambler*, *flip(u)*, *flip(v)* and *flip(w)* are keystreams after iterating four times by itself. Combine *flip(u)*, *flip(v)* and *flip(w)* as S_3 , S_3 , which is used to scramble the position of every DNA bases of A_4 .

$$\text{Swap}(A_4(t), A_4(S_4(t))), t \in [1, M * N * 3] \quad (10)$$

$$A_5(t) = A_4(t), t \in [1, M * N * 3] \quad (11)$$

Step10: Iterate four times of x, y, z and obtaining the three sequences *flip(x)*, *flip(y)* and *flip(z)* respectively. Combine *flip(x)*, *flip(y)* and *flip(z)* as S_4 . The DNA level diffusion operation is carried out between the DNA matrix A_5 and DNA diffusion sequence S_4 . The DNA XOR rules are defined in Table 2, and the effect as follows:

$$A_6(t) = \text{dnaxor}(A_5(t), S_4(t)), t \in [1, M * N * 3] \quad (12)$$

Step11: By decimal matrix generated by chaotic sequence w and decoding rules, decode the diffused DNA matrix A_6 into a . Assume C as the encrypted image.

$$C = DNA_{decoding}(A_6, w_i), w_i \in [1, 8] \cap i \in [1, 3 * M * N] \quad (13)$$

where w_i represents the eight legal combinations rules in Table 1. Finally, the function returns the decoded decimal sequence or matrix, which is the encrypted image.

3.2 Decryption algorithm description

The decryption procedure is reverse to the encryption procedure. At first, input key to the hyper chaotic system and obtain the chaotic sequences. Afterwards, encode the cipher image to DNA sequence, via taking diffusion, permutation and decoding operations to the DNA sequence, obtaining the decimal matrix. Then, carry out the inverse operation of *Decimaldiffusion* and *Decimalpermutation*, obtaining the plain image P.

4 Algorithm performance analysis

After a lot of experimental verification, we adopted we took the *Key* : [$a = 10, b = 8/3, c = 28, d = 2, h = 8.8, k_1 = 1, k_2 = 0.9, x = 4, y = 4, z = 3, u = 4, v = 5, w = -2$]. Except these, the threshold ,interference and primer number are 700, 0.02 and 982451653 respectively. Encryption and decryption of the color images with a size of 512×512 pixels are shown in Fig. 2.

4.1 Speed performance

No matter what kind of application scenario, running speed is an important measure for an image encryption algorithm. The proposed algorithm has been implemented using Matlab, and speed performance has been measured on a personal computer with Intel Core i5-6300H CPU@2.38 GHz, with 12GB RAM, Windows 10 as the operating system.

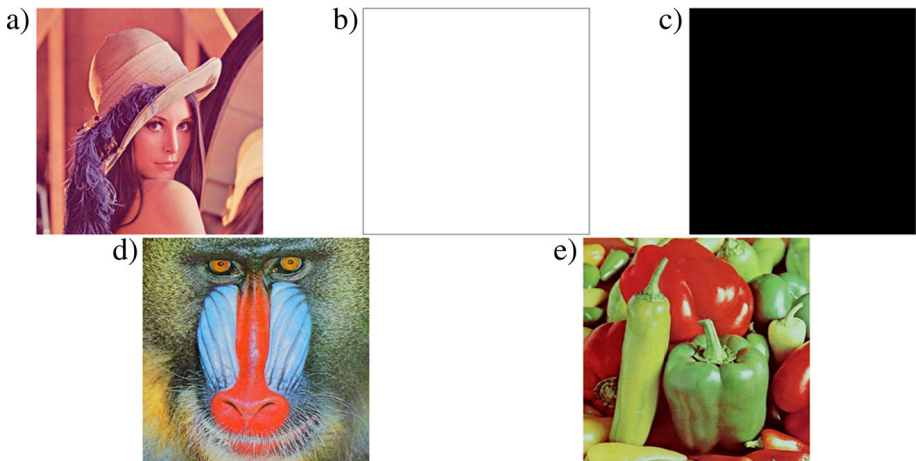


Fig. 2 From left to right, are the plain images. a(Lena), b(White), c(Black), d(Baboon), e(Pepper)

According to refs [18, 32] are 117.028, 193.502 (KB/s) respectively, the cost of proposed algorithm is 149.304 (KB/s) on image arrays of size 512×512 . Considering that the algorithm proposed in this paper is more complex, as well as some other objective factors such as computer configuration, it is very rare that the algorithm proposed in this paper can achieve such a result while greatly increasing the image security. With such a speed, illustrating that the proposed algorithm has made the balance between security and efficiency.

4.2 Key space

Key space is the set of all valid, possible, distinct keys of a given cryptosystem. The security of a cryptosystem is proportional to the size of the key space. An intercepted message with a larger key space is more resistant to attack since an attacker will try to brute force the message with all possible key combinations.

All of the possible secret keys form the key space. The secret key in the cryptosystem for images contains six initial values and seven system parameters. As the precision is 10^{-15} by computer with accuracy, the initial key space is shown as formula (14).

$$keyspace = \prod_{t=1}^{13} 10_t^{15} \quad (14)$$

The result of formula (14) is 10^{195} , which is much larger than 2^{300} . For a secure color image encryption algorithm, its key space is sufficient, has better performance than the majority of algorithms [19, 33, 34], which are 2^{160} , 2^{256} and 10^{70} . Thus, the key space of the proposed system is sufficient to frustrate an exhaustive attack.

4.3 Key sensitivity

An encryption algorithm should be sensitive to its *key*. If the cipher text cannot reflect key, then the sensitivity is very weak. In general, the *keystream* generated by chaotic system should be changed when hackers use the slightest changes of any *key* to decrypt the cipher-image. For evaluating the key sensitivity of the proposed scheme, this paper randomly select four slightly different test keys to encrypt and decrypt images. The results are shown in Fig. 3. The experiment indicates that the proposed color image encryption algorithm has high enough key sensitivity, and it is impossible to decrypt the encrypted image by imprecise key parameters.

4.4 Information entropy analysis

Information entropy is a very important indicator of randomness which measures the uncertainty of random variable in information theory. If encryption does not produce enough disorder at the output, the cryptosystem can be the subject of entropy attack. Ideally, the perfect information entropy of any RGB component image is 8. The definition of the entropy $H(m)$ of an image m can be calculated as follows:

$$H(m) = - \sum_{i=0}^{2^N-1} p(m_i) \log_2(p(m_i)) \quad (15)$$

where N is the number of bits of message m , 2^N are all possible values, $p(m_i)$ means the possibility of m_i , \log_2 represents the base two logarithm, and the entropy is expressed in

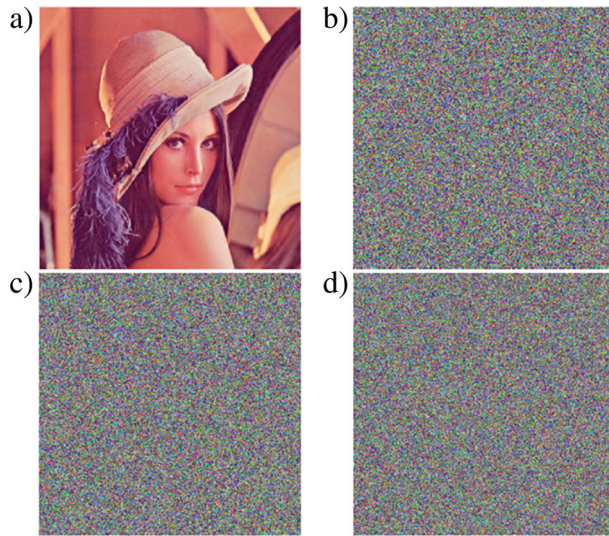


Fig. 3 Key sensitivity. From left to right are a) The original image; b) the encrypted image with $key1(a = 10, b = 8/3, c = 28, d = 2, h = 8.8, k_1 = 1, k_2 = 0.9, x = 4, y = 4, z = 3, u = 4, v = 5, w = -2)$; c) The encrypted image with $key2(a = 10, b = 8/3, c = 28, d = 2, h = 8.8, k_1 = 1, k_2 = 0.9, x = 4.001, y = 4.002, z = 3.01, u = 3.84, v = 5, w = -2.003)$; d) The decrypted Lena encrypted by key1 and decrypted by key2

bits. Some entropy statue of Liberty 512×512 RGB plain images are shown in Table 3. The information entropy of image Lena via different encryption algorithm is shown in Table 4.

Obviously, from the formula of information entropy, the average measure of information entropy values of these six selected RGB images is very close to the ideal value 8. Therefore, the proposed scheme is immune to the entropy attack. From Table 4, the value of last cipher image is 7.999 which is better than [23, 35, 36].

4.5 Histogram analysis

The histogram of the cipher image describes the distribution of pixel values, which is also an important indicator to show whether the encryption algorithm can resist the attack of statistical analysis. Statistical analysis attack refers to the attacker obtains the statistical characteristics of encrypted images through statistical analysis. The selective cipher text attack is made possible by the statistics of characteristic information. From Fig. 4, the R,G,B three components histogram of cipher images are much smooth than before, which means

Table 3 Information entropy of the different cipher images

Images	Lena	White	Black	Baboon	Pepper
Cipher image	7.999	7.994	7.993	7.997	7.999
R primary color	7.993	7.994	7.994	7.993	7.999
G primary color	7.992	7.993	7.994	7.999	7.999
B primary color	7.994	7.994	7.994	7.999	7.999

Table 4 Information entropy of Lena with different algorithm

Images	This paper	[35]	[23]	[19]	[36]
Cipher image	7.999	7.992	7.981	7.999	7.997
R primary color	7.993	7.994	7.979	7.997	7.997
G primary color	7.992	7.992	7.980	7.997	7.997
B primary color	7.994	7.990	7.982	7.996	7.997

the characteristics of encrypted images is not possible be found by attacker. As a result, the cipher image is more uniform and more resistant to statistical attacks.

The paper selected 3 different images “Lena”, “White” and “Pepper” to be encrypted. The experimental results are shown in Fig. 4. From the results, it is obvious that the histogram of each of the plain images is uneven before encryption, and the corresponding histogram of the encrypted image becomes plane.

4.6 Correlation analysis

The pixels of an image have a strong correlation, and this correlation makes the image easier to crack. In particular, the correlation of adjacent pixels, this describes the horizontal, vertical or diagonal relationship between adjacent pixels. It is important for the encrypted image to break the correlation between adjacent pixels in the source image. Ideally, the correlation of the cipher image is zero, but this is not usually achieved.

In this paper, 10000 pairs of adjacent pixels have been selected randomly. We selected all the three directions and obtained encrypted images. The mathematical formula is used to calculate correlation coefficient as follows:

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (16)$$

$$\rho_{X, Y} = \text{corr}(X, Y) = \frac{\text{cov}(X, Y)}{\sigma_X \sigma_Y} = \frac{E[(X - \beta_X)(Y - \beta_Y)]}{\sigma_X \sigma_Y} \quad (17)$$

where x and y are rgb-scale values of two adjacent pixels in the image. The following discrete formulas were used:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (18)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (19)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (20)$$

The correlation distribution of the plain images and the encrypted images has been drawn in Fig. 5. Table 5 shows the values of correlation coefficient between the two adjacent pixels, which indicates that the adjacent pixels have almost nil correlation with each other. Table 6 shows the correlation values of “Lena” images encrypted by different encryption algorithms.

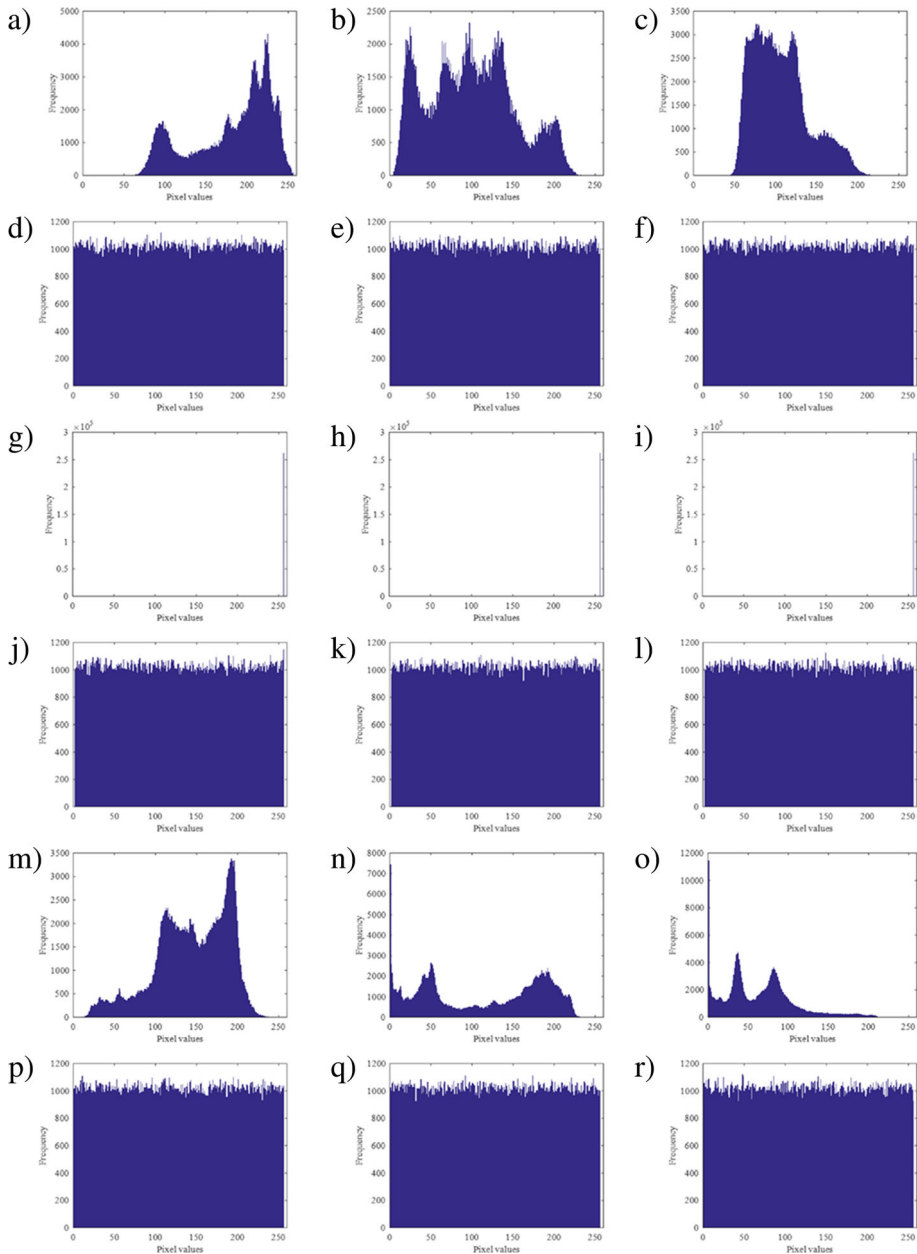


Fig. 4 Histograms. From left to right are a),b),c) Histograms of the three primary colors of original Lena; d),e),f) Histograms of the three primary colors of encrypted Lena; j),h),k) Histograms of the three primary colors of original White; g),k),l) Histograms of the three primary colors of encrypted White; m),n),o) Histograms of the three primary colors of original Pepper; p),q),r) Histograms of the three primary colors of encrypted Pepper

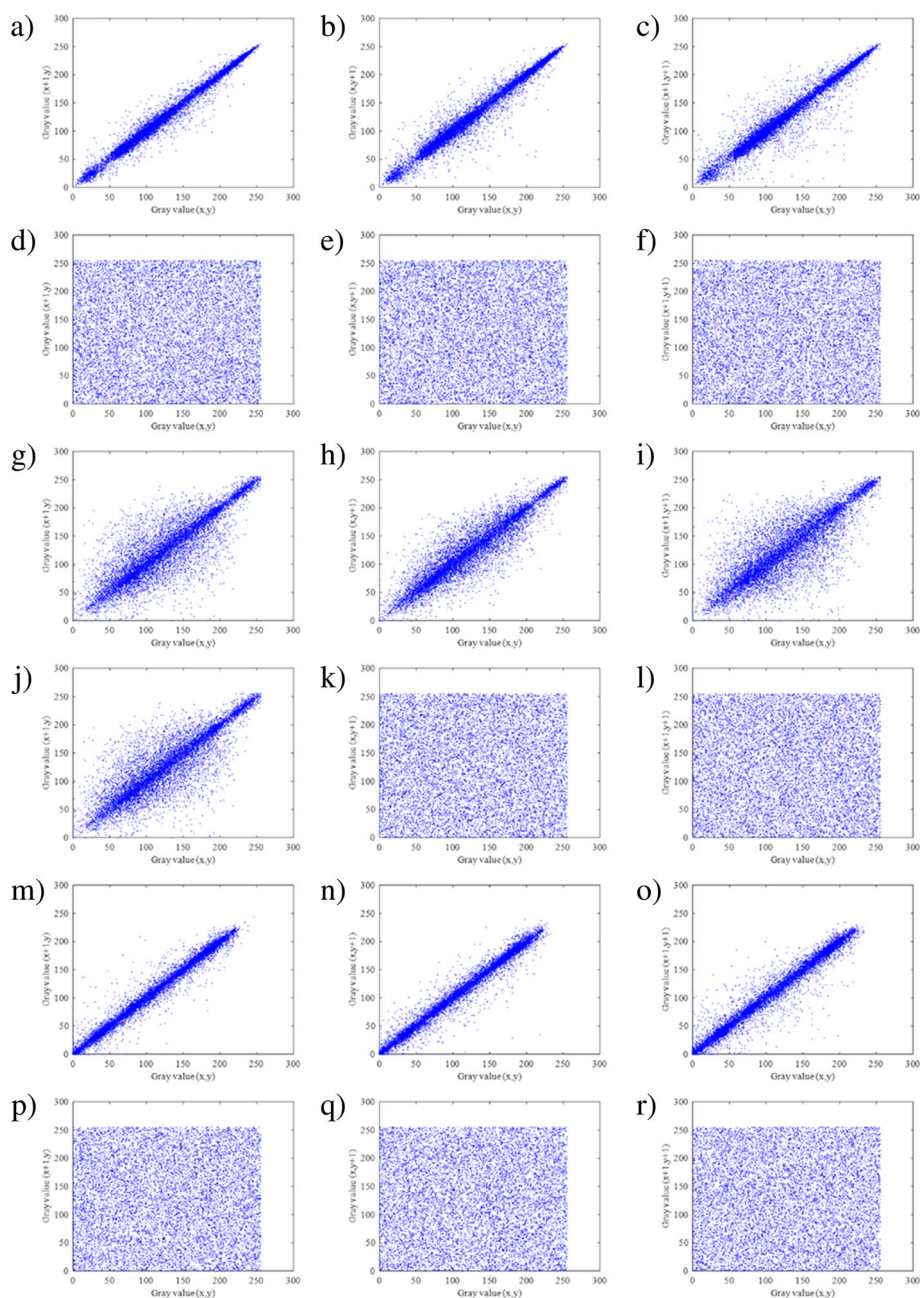


Fig. 5 Correlation analysis. From left to right are a),b),c) The three primary colors of original Lena; d),e),f) The three primary colors of encrypted Lena; j),h),i) The three primary colors of original Baboon; g),k),l) The three primary colors of encrypted Baboon; m),n),o) The three primary colors of original Pepper; p),q),r) The three primary colors of encrypted Pepper

Table 5 Correlation coefficient of different encrypted images

Images	Directions	Original image			Cipher image		
		R	G	B	R	G	B
Fig. 2(a)	H	0.9892	0.9814	0.9565	-0.0014	-0.0012	-0.0058
	V	0.9794	0.9695	0.9331	0.0011	-0.0097	0.0063
	D	0.9714	0.9547	0.9175	-0.0019	-0.0045	-0.0047
Fig. 2(b)	H	NaN	NaN	NaN	-0.0015	-0.0015	0.0052
	V	NaN	NaN	NaN	0.0030	-0.0016	0.0048
	D	NaN	NaN	NaN	0.0036	0.0079	0.0042
Fig. 2(c)	H	NaN	NaN	NaN	-0.0045	0.0036	-0.0011
	V	NaN	NaN	NaN	0.0184	-0.0038	-0.0017
	D	NaN	NaN	NaN	-0.0189	-0.0071	-0.0046
Fig. 2(d)	H	0.8563	0.8005	0.8845	0.0067	-0.0011	0.0019
	V	0.9304	0.8950	0.9363	0.0090	0.0005	0.0056
	D	0.8472	0.7702	0.8629	-0.0023	-0.0015	-0.0002
Fig. 2(e)	H	0.9760	0.9891	0.9739	-0.0091	0.0039	0.0073
	V	0.9770	0.9884	0.9759	-0.0059	0.0010	-0.0067
	D	0.9630	0.9819	0.9601	-0.0011	-0.0079	0.0047

From Table 5, it can be seen from Fig. 5 that the pixel correlation of each image is very obvious before encryption, but after encryption, this value is almost close to 0. This shows that our encryption algorithm greatly disrupts the relationship between pixels.

It can be seen from Fig. 6 that the values obtained by our algorithm are more average than those obtained by [18, 35, 36], which means that our algorithm is more stable. Especially in horizontal green part and diagonal red part, the proposed algorithm has the best performance in disturbing the pixel correlation. Therefore, the result indicates that adjacent pixels in the horizontal direction in the cipher image have almost no correlation.

4.7 Shear attack

Because the encrypted image may lose information by cutting attack during transmission, this means that the encrypted image is difficult to restore to the original image. In this paper,

Table 6 Correlation coefficient of encrypted Lena with different algorithms

Directions	Primary color	This Paper	[35]	[18]	[19]	[36]
H	R	-0.0014	0.0060	0.0063	0.0007	-0.0052
	G	-0.0012	0.0060	0.0110	-0.0035	-0.0052
	B	-0.0058	0.0060	0.0104	0.0015	-0.0052
V	R	0.0011	-0.0209	0.0004	-0.0004	0.0086
	G	-0.0097	-0.0209	-0.0064	0.0023	0.0086
	B	0.0063	-0.0209	0.003	0.0028	0.0086
D	R	-0.0019	0.0055	-0.0020	0.0039	-0.0020
	G	-0.0045	0.0055	0.0166	-0.0079	-0.0020
	B	-0.0047	0.0055	0.0049	0.0010	-0.0020

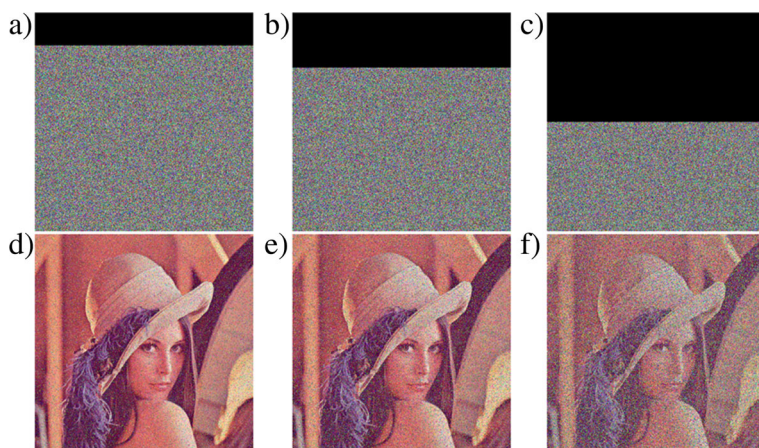


Fig. 6 Shear attack. From left to right are a) cut 15 % of encrypted image; b) cut 25 % of encrypted image; c) cut 50 % of encrypted image; d) cut 15 % of original image; e) cut 25 % of original image; f) cut 50 % of original image

simulation shear tests of 15 %, 25 % and 50 % Lena image occlusion are shown in Fig. 6. The results show that the algorithm has a strong ability to resist shear attack.

4.8 Noisy attack

The encryption algorithm will inevitably be disturbed by some unknown noises, so the ability to resist the noise attack is also a very important aspect of the encryption algorithm. In this paper, Salt and Pepper noise with different intensities was added into the encrypted image. After that, recover the encrypted image into original. The experimental results are shown in Fig. 7. After added noise into encrypted image, the results indicate that the original image can be basically recovered after decrypted the cipher image, which means that the proposed encryption algorithm has superb ability in resisting noisy attack.

5 Conclusion

Recent years, hundreds of image encryption algorithms based on chaotic system have been proposed. As the same time, the pseudo-DNA technology has developed faster and faster in cryptosystem. However, the majority of these are based on low-dimensional chaotic system, which does not fulfill the demands in randomness and robustness. To address this problem, the paper a digital color image encryption algorithm based on 6D hyper-chaotic system and DNA encoding technology. The 6D hyper chaotic system has hyper chaotic attractor with four positive Lyapunov exponents for a wide range of k . The encryption algorithm realized by pixel level diffusion, permutation and DNA level diffusion, permutation. Through pixel level and DNA level permutation, the position of original image is distributed, furthermore, after diffusion process, the relationship between the original image and encrypted image is very weak. In order to evaluate the encryption algorithm, this paper carry out several experiments, including key space, key intensity, information entropy analysis, histogram analysis, correlation analysis, differential attack analysis, quality analysis, shear attack and noisy attack. Consequently, those experiments result indicate that the proposed color image

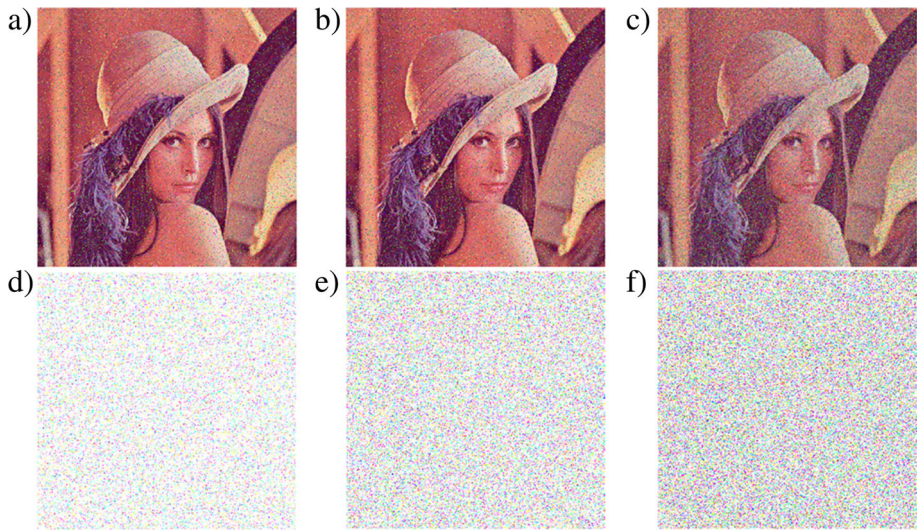


Fig. 7 Noisy attack analysis. From left to right are a), b) and c) are the decrypted image after added noise density 0.1, 0.2 and 0.3 to the original Lena; d), e) and f) are the decrypted image after added noise density 0.1, 0.2 and 0.3 to the original White

encryption algorithm has great performance in resisting the majority type of attacks. In addition, chaotic systems also have good performance in bifurcation analysis and equilibrium stability. In a word, the 6D hyper chaotic is suitable to be implemented in crypt-system. In this paper, a new digital color image encryption algorithm based on 6D hyper-chaotic system and DNA encoding technology was proposed. The encryption algorithm realized by pixel level diffusion, permutation and DNA level diffusion, permutation. Through pixel level and DNA level permutation, the position of original image is distributed, furthermore, after diffusion process, the relationship between the original image and encrypted image is very weak. In order to evaluate the encryption algorithm, this paper carry out several experiments, including key space, key intensity, information entropy analysis, histogram analysis, correlation analysis, differential attack analysis, quality analysis, shear attack and noisy attack. Consequently, those experiments result indicate that the proposed color image encryption algorithm has great performance in resisting the majority type of attacks.

The image encryption system proposed in this paper is applicable to most fields, but the performance of the 6D hyper-chaotic system of the crypt-graphic system still has the potential to improve. Limited by the hardware and MATLAB performance, the encryption speed of the algorithm is still not fast. Now, We are working on ways to make the algorithm faster and more complex. In the future, the algorithm will be optimized to improve the performance of the algorithm, and effective methods will be researched to resist the attack of supercomputer or quantum computer.

Data Availability Same as many papers in the same research direction, we also use the standard 512×512 image RGB image, the Lena is available at [Lena](#), Pepper is available at [Pepper](#) and the Baboon is available at [Baboon](#).

Declarations

Conflict of Interests The authors declare no conflict of interest.

References

- Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. *Image Vis Comput* 24(9):926–934
- Guanrong C, Yaobin M, Chui CK (2004) A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos Solitons Fractals* :21
- Furht B, Kirovski D (2004) *Multimedia security handbook* CRC press
- Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. *Signal Process* 90(3):727–752
- Hussain UN, Chithralekha T (2011) Review of dna cryptology. *Netw Commun Eng* 3(13):843–849
- Chang HK-C, Liu J-L (1997) A linear quadtree compression scheme for image encryption. *Signal Process Image Commun* 10(4):279–290
- Chen G, Ueta T (1999) Yet another chaotic attractor. *Int J Bifurcation Chaos* 9(07):1465–1466
- Bourbakis N, Alexopoulos C (1992) Picture data encryption using scan patterns. *Pattern Recogn* 25(6):567–581
- Geetha S, Punithavathi P, Infanteena AM, Sindhu SSS (2018) A literature review on image encryption techniques. *Int J Inf Secur Privacy (IJISP)* 12(3):42–83
- Mao Y, Chen G, Lian S (2004) A novel fast image encryption scheme based on 3d chaotic baker maps. *Int J Bifurcation Chaos* 14(10):3613–3624
- Mao Y, Chen G (2005) Chaos-based image encryption. In: *Handbook of geometric computing*, Springer, pp 231–265
- Habutsu T, Nishio Y, Sasase I, Mori S (1991) A secret key cryptosystem by iterating a chaotic map. In: *Workshop on the theory and application of cryptographic techniques*, Springer, pp 127–140
- Hua Z, Jin F, Xu B, Huang H (2018) 2d logistic-sine-coupling map for image encryption. *Signal Process* 149:148–161
- Murillo-Escobar MA, Meranza-Castillón MO, López-Gutiérrez RM, Cruz-Hernández C (2019) Suggested integral analysis for chaos-based image cryptosystems. *Entropy* 21(8):815
- Babaei M (2013) A novel text and image encryption method based on chaos theory and dna computing. *Natural Comput* 12(1):101–107
- Jain A, Rajpal N (2016) A robust image encryption algorithm resistant to attacks using dna and chaotic logistic maps. *Multimed Tools Appl* 75(10):5455–5472
- Zhang Q, Liu L, Wei X (2014) Improved algorithm for image encryption based on dna encoding and multi-chaotic maps. *AEU-Int J Electr Commun* 68(3):186–192
- Diaconu A-V, Costea A, Costea M-A (2014) Color image scrambling technique based on transposition of pixels between rgb channels using knight's moving rules and digital chaotic map. *Math Probl Eng* :2014
- Gao X (2021) A color image encryption algorithm based on an improved hénon map. *Physica Scripta* 96(6):065203
- Zhang W, Yu H, Zhao Y-L, Zhu Z-L (2016) Image encryption based on three-dimensional bit matrix permutation. *Signal Process* 118:36–50
- Li XW, Cho SJ, Kim ST (2014) A 3d image encryption technique using computer-generated integral imaging and cellular automata transform. *Optik* 125(13):2983–2990
- Zhu Z-L, Zhang W, Wong K-w, Yu H (2011) A chaos-based symmetric image encryption scheme using a bit-level permutation. *Inf Sci* 181(6):1171–1186
- Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt Commun* 284(16–17):3895–3903
- Pyle I (1967) Format effectors in iso7 and ascii. *Commun ACM* 10(3):137
- Xian Y, Wang X, Wang X, Li Q, Ma B (2022) A chaotic image encryption algorithm based on sub-block spiral scans and matrix multiplication. In: *International conference on artificial intelligence and security*, Springer, pp 309–322
- Gao X, Mou J, Xiong L, Sha Y, Yan H, Cao Y (2022) A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. *Nonlinear Dyn* 108(1):613–636
- Lorenz EN (1963) Deterministic nonperiodic flow. *J Atmos Sci* 20(2):130–141
- Hu G (2009) Generating hyperchaotic attractors with three positive lyapunov exponents via state feedback control. *Int J Bifurcation Chaos* 19(02):651–660
- Yang Q, Osman WM, Chen C (2015) A new 6d hyperchaotic system with four positive lyapunov exponents coined. *Int J Bifurcation Chaos* 25(04):1550060
- Shalon D, Smith SJ, Brown PO (1996) A dna microarray system for analyzing complex dna samples using two-color fluorescent probe hybridization. *Genome Res* 6(7):639–645

31. Verma A, Dave M, Joshi R (2008) Dna cryptography: a novel paradigm for secure routing in mobile ad hoc networks (manets). *J Discret Math Sci Cryptogr* 11(4):393–404
32. Wu Y, Agaian SS, Noonan JP (2012)
33. Seyedzadeh SM, Mirzakuchaki S (2012) A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. *Signal Process* 92(5):1202–1215
34. Liang Z, Qin Q, Zhou C, Wang N, Xu Y, Zhou W (2021) Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation. *PloS ONE* 16(11):0260014
35. Shakiba A (2019) A randomized cpa-secure asymmetric-key chaotic color image encryption scheme based on the chebyshev mappings and one-time pad. *Journal of King Saud University-Computer and Information Sciences*
36. Iqbal N, Hanif M, Abbas S, Khan MA, Rehman ZU (2021) Dynamic 3d scrambled image based rgb image encryption scheme using hyperchaotic system and dna encoding. *J Inf Secur Appl* 58:102809

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.