Preprints.org

Article

Not peer-reviewed version

A New Hyperchaotic Image Encryption Scheme Based on DNA Computing and SHA-512

Shuliang Sun * and Xiping Wang

Posted Date: 30 August 2024

doi: 10.20944/preprints202408.2216.v1

Keywords: hyperchaotic system; DNA computing; SHA-512

Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

A New Hyperchaotic Image Encryption Scheme Based on DNA Computing and SHA-512

Shuliang Sun [1,*] and Xiping Wang [2]

[1] College of Computer and Electrical Engineering, Hunan University of Arts and Science, Changde 415000, China; tjussl_07@126.com
[2] College of Economics and Management, Hunan University of Arts and Science, Changde 415000, China; 32698799@qq.com
* Correspondence: tjussl_07@126.com; Tel.: (optional; include country code; if there are multiple corresponding authors, add author initials)

Abstract: With the fast growth of smartphones and digital cameras, massive images are generated every day in the world. They are easily transmitted on the insecure channel-Internet. It has been a hot spot for protecting sensitive images during communication. A new cryptosystem is proposed using a six dimensional (6D) hyperchaotic system and DNA computing. The hash value is obtained with the function of SHA-512. It keeps the encrypted result closely connected with the original image. The initial values of the cryptosystem are produced with the hash value and the secret key. The pixel is divided into four parts, and a large matrix is formed. Scrambling is performed on the new image. DNA coding, modern DNA complementary rules, DNA computing, and DNA decoding are performed on the new image. Diffusion is also executed, and ciphered image is achieved finally. The experimental result reveals the outcome of the proposed algorithm. Security analysis shows that the designed algorithm has a huge secret key space, low correlation, and high sensitivity. It also signifies that the designed algorithm could protect against common attacks and is more secure than some existing methods.

Keywords: hyperchaotic system; DNA computing; SHA-512

1. Introduction

With the rapid growth of smartphones and digital cameras, massive images are generated every day in the world. They are easily transmitted on the Internet, which is an insecure channel. It is extremely important to protect sensitive images from hacker attacks during communication. Steganographic algorithms [1-2], watermarking techniques [3-5], and encryption methods [6-10] are three important techniques in terms of protecting private images. Images are famous for special characteristics: data redundancy, high correlation, large storage space, and uneven energy distributions.Traditional text-based encryption algorithms could not be used to encrypt the image, such as AES [11], DES [12], and RSA [13].

Chaos has some special merits: ergodicity, pseudo randomness, and sensibility to initial states. It is widely applied for image encryption [14-20]. Many encryption schemes have been proven to be insufficiently secure and have been cracked [21-28]. The hyperchaotic system has some special characteristics. It has more system variables and parameters, more complicated structures, and better dynamic behaviors than the low-dimensional chaotic system. [29, 30]. Huang et al. [9] proposed a chaotic image encryption method that was based on the game of life and plaintext. Two scrambling matrices were constructed to scramble the plain image. A 4D hyperchaotic system and the game of life were employed to diffuse the image. Musanna and Kuma [14] proposed a novel image encryption method based on a fractional order chaotic system. The chaotic sequences were produced with the 3D chaotic system and the Fisher-Yates method. The plain image was segmented into different blocks of the same size. A 3D hyperchaotic system was employed to scramble the image. The generated

© 2024 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

chaotic sequences were adopted to diffuse the shuffling image. Fisher-Yates was applied to generate a chaotic matrix. Sun and Chen [18] designed a new cryptosystem based on SHA-256 and chaotic theory. Noise-like pixels were randomly inserted into the plaintext image and generated a hash value with SHA-256.The authors proposed a segmented coordinate descent scheme.

DNA molecules have some special characteristics, such as huge storage space, high parallelism, strong adaptability, and low power consumption. The DNA technique is very suitable for encrypting the image [31-36]. Mansoor et al. [31] presented an image encryption scheme based on chaos theory and DNA computing. The plain image was scrambled with the logistic map and the tent map. DNA computing was performed to encrypt the plain image. Chai et al. [35] introduced an image encryption scheme that was based on the DNA technique and the chaotic technique. The hash value was calculated on the basis of the plain image and applied to compute the initial states and system parameters. The DNA matrix was produced with chaotic sequences. A color image encryption method was designed in Ref. [36]. It adopted a hyperchaotic system and DNA computing. Firstly, four chaotic sequences were produced with a 2D hyperchaotic system. Then an image cube was constructed using image blocks. Finally, DNA operations were applied to the plain image.

Section 2 introduces related techniques. Chaotic sequences are generated in Section 3. Section 4 displays the proposed scheme. The simulation results are shown in Section 5. The security test is discussed in Section 6. Section 7 concludes the manuscript.

2. Related Techniques

2.1. Six-Dimensional Hyperchaotic System

In the manuscript the chaotic sequences are produced with hyperchaotic system. The dimension of the system is six. It is defined as [37]:

$$\begin{cases} \dot{x}_1 = \delta_1(x_2 - x_1) + x_4 \\ \dot{x}_2 = \delta_2 x_1 - x_1 x_3 + x_4 \\ \dot{x}_3 = x_1 x_2 - x_3 - x_4 \\ \dot{x}_4 = -\delta_3(x_1 + x_2) + x_5 \\ \dot{x}_5 = -x_2 - \delta_4 x_5 + x_6 \\ \dot{x}_6 = -\delta_5(x_1 + x_5) \end{cases} \tag{1}$$

where δ_1, δ_2, δ_3, δ_4, and δ_5 are the system parameters.

Its Lyapunov exponents (LE) are 1.4620, 0.1433, 0.0725, 0.0449, 0 and -12.0700 if (δ_1, δ_2, δ_3, δ_4, δ_5) = (10,76,3,0.2,0.1) . There are four positive LEs in system (1), and it is a hyperchaotic system. The bifurcation diagram of system (1) is shown as Figure 1.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

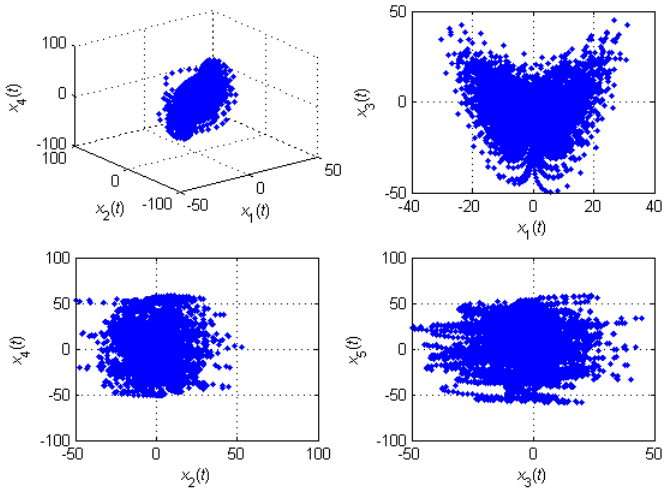


Figure 1. The bifurcation diagram of the system (1).

2.2. DNA Coding Rules

There are four nucleic acid bases in a DNA sequence. They are C (cytosine), A (adenine), T (thymine), and G (guanine). Watson and Crick proposed the DNA pairing rules [32]. A and C are complementary to T and G. Two binaries11, 10, 01 and 00 can be adopted to encode four bases. There are eight DNA coding rules, which are presented in Table 1. These coding rules could be used to encode and decode DNA sequences.

Table 1. DNA coding rules.

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

Suppose a pixel value is 156 and its binary is 10011100. If the encoding and decoding rules are 3 and 7 respectively, then the encoding and decoding results are shown in Figure 2.

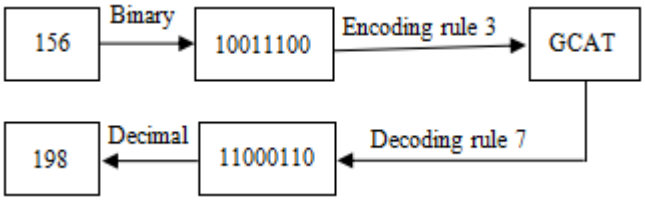


Figure 2. DNA encoding and decoding results.

2.3. Modern Dna Complementary Rules

The modern DNA complementary rules are satisfied as [33]:

$$\begin{cases} y \neq W(y) \neq W(W(y)) \neq W(W(W(y))) \\ y = W(W(W(W(y)))) \end{cases} \quad (2)$$

where W(y) represents a base pair of y and is different from y.

Six modern DNA complementary rules are displayed [35]:

Rule 1. T→A , A→G , G→C , C→T

Rule 2. T→A , A→C , C→G , G→T

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

Rule 3. T→C , C→A , A→G , G→T
Rule 4. T→C , C→G , G→A , A→T
Rule 5. T→G , G→A , A→C , C→T
Rule 6. T→G , G→C , C→A , A→T

2.4. DNA Computing

Some algebraic and biology operations are proposed for DNA computing. There are DNA addition operation, DNA subtraction operation, and DNA XOR operation. Due to the existence of eight DNA coding rules, there are eight DNA addition, DNA subtraction, and DNA XOR rules. They are shown respectively in Tables 2, 3 and 4.

Table 2. DNA addition rule.

+	G	T	A	C
G	G	T	A	C
T	T	A	C	G
A	A	C	G	T
C	C	G	T	A

Table 3. DNA subtraction rule.

-	G	T	A	C
G	G	C	A	T
T	T	G	C	A
A	A	T	G	C
C	C	A	T	G

Table 4. DNA addition rule.

⊕	G	T	A	C
G	G	T	A	C
T	T	G	C	A
A	A	C	G	T
C	C	A	T	G

3. Generation of Chaotic Sequences

The plain image with size $M \times N$ is computed with SHA-512, and the hash value W with 512-bit is generated. If an image is changed one bit and a new image is generated, then they will produce totally different hash values [38]. The initial states of system (1) are calculated using secret keys and the hash value W. W is split into many 8-bit data blocks. Each one is changed into a decimal number and is represented as $w_1, w_2, \ldots, w_{64}$.

The initial values will be achieved as follows:

$$wv_i = \mathrm{mod}(w_{9i-8} + w_{9i-7} + w_{9i-6} + w_{9i-5} + w_{9i-4} + w_{9i-3} + w_{9i-2} + w_{9i-1} + w_{9i}, 256) \quad (3)$$

$$x_1(0) = \frac{wv_1}{255} + \frac{\sum_{l=55}^{64} w_l}{10 \times 255} + sk_1 \quad (4)$$

$$x_j(0) = \frac{wv_j}{255} + x_{j-1}(0) + sk_j \quad (5)$$

where sk_i is the secret key, $i \in \{1, 2, 3, 4, 5, 6\}$; $j \in \{2, 3, 4, 5, 6\}$.

2. First iterate system (1) 600 times.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

3. Continue to perform $4MN$ iterations.
4. New sequences z_1, z_2, z_3, z_4, z_5, z_6 and z_7 are achieved.

$$z_1(j) = \mathrm{mod}((abs(100x_1(j)) - floor(abs(100x_1(j))))\times 10^{12}, 4MN) \quad (6)$$

$$z_2(j) = \mathrm{mod}((abs(100x_2(j)) - floor(abs(100x_2(j))))\times 10^{12}, 8) + 1 \quad (7)$$

$$z_3(j) = \mathrm{mod}(floor(abs(x_3(j))\times 10^{15}), 4) \quad (8)$$

$$z_4(j) = \mathrm{mod}(floor(abs(x_4(j))\times 10^{15}), 6) + 1 \quad (9)$$

$$z_5(j) = \mathrm{mod}(floor(abs(x_5(j))\times 10^{15}), 3) + 1 \quad (10)$$

$$z_6(j) = \mathrm{mod}((abs(x_5(j)) - floor(abs(x_5(j))))\times 10^{15}, 8) + 1 \quad (11)$$

$$z_7(j) = \mathrm{mod}(floor(abs(x_6(j))\times 10^{15}), 256) \quad (12)$$

where j=1, 2, …, $4MN$; *abs* means an absolute function; mod symbols a modulus function; *floor*(z) receives an integer equal to or less than z.

4. Generation of Chaotic Sequences

1. Divide the plain image with an 8-bit pixel into four 2-bit parts. It becomes a new image P_1 with size $M \times 4N$. $P_1(i, j) \in \{0, 1, 2, 3\}$, $1 \le i \le M$ and $1 \le j \le 4N$.
2. Exchange pixel $P_1(i, j)$ with pixel $P_1(i', j')$.

$$i' = floor(z_1(i, j) / 4N) + 1 \quad (13)$$

$$j' = z_1(i, j) \bmod 4N + 1 \quad (14)$$

where $1 \le i \le M$ and $1 \le j \le 4N$.
3. Convert the matrix P_1 into a binary sequence $Q = [Q(1), Q(2), \ldots, Q(4MN)]$.
4. Encode binary sequences Q and z_3 into DNA sequences U and z_3 according to the chaotic sequence z_2.
5. Modern DNA complementary rules are performed on the DNA sequence U.

$$G(i) = \begin{cases} Rule1(U(i)) & if\ z_4(i) = 1 \\ Rule2(U(i)) & if\ z_4(i) = 2 \\ Rule3(U(i)) & if\ z_4(i) = 3 \\ Rule4(U(i)) & if\ z_4(i) = 4 \\ Rule5(U(i)) & if\ z_4(i) = 5 \\ Rule6(U(i)) & if\ z_4(i) = 6 \end{cases} \quad (15)$$

where i = 1, 2, …, $4MN$.
6. DNA computation is executed on the DNA sequences G and z_3. The sequence H is decided by the chaotic sequence z_5.

$$H(j) = \begin{cases} G(j) + z_3(j) & if\ z_5(j) = 1 \\ G(j) - z_3(j) & if\ z_5(j) = 2 \\ G(j) \oplus z_3(j) & if\ z_5(j) = 3 \end{cases} \quad (16)$$

where j = 1, 2, …, $4MN$.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

Decode the DNA sequence H into binary sequences J and convert J to the decimal sequence K. Diffuse the sequence K and obtain the sequence C.

$$C(l)=\begin{cases} K(l)\oplus \mathrm{mod}(\sum_{i=1}^{MN} \mathrm{P}(i),256)\oplus \mathrm{mod}(\sum_{j=1}^{64} w(j),256)\oplus z_7(l) & if\ \ l=1 \\ K(l)\oplus \mathrm{mod}(\sum_{t=1}^{6} sk_t\times 10^{15},256)\oplus C(l-1)\oplus z_7(l) & if\ \ l=2 \\ K(l)\oplus C(l-1)\oplus C(l-2)\oplus z_7(l) & if\ \ l\in[3,MN] \end{cases} \tag{17}$$

Sequence C is converted into matrix D and finally the encrypted image is obtained. The procedure of the presented scheme is briefly described in Figure 3.

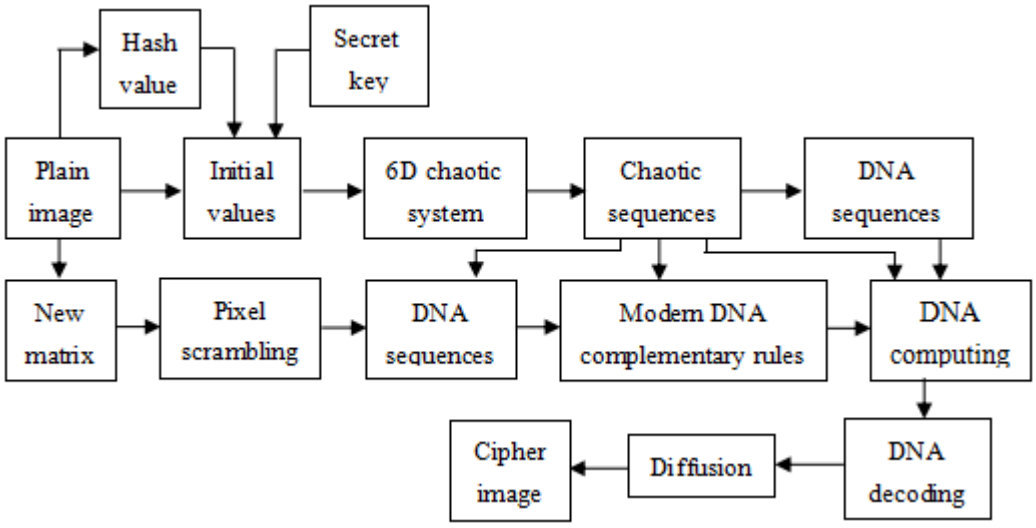


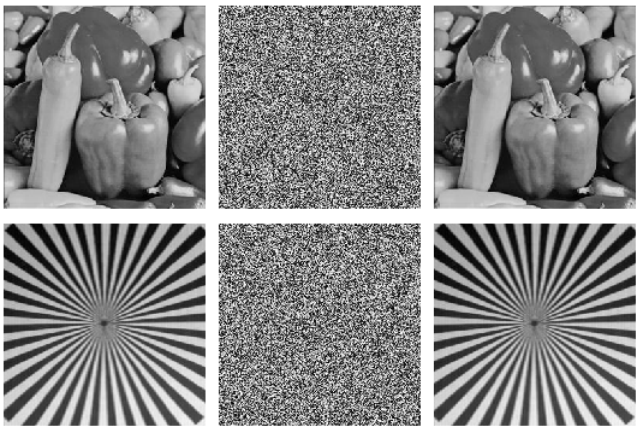
Figure 3. The procedure of the proposed scheme.

The decryption method is the opposite of the encryption procedure. It is not discussed in detail.

5. Simulation Results

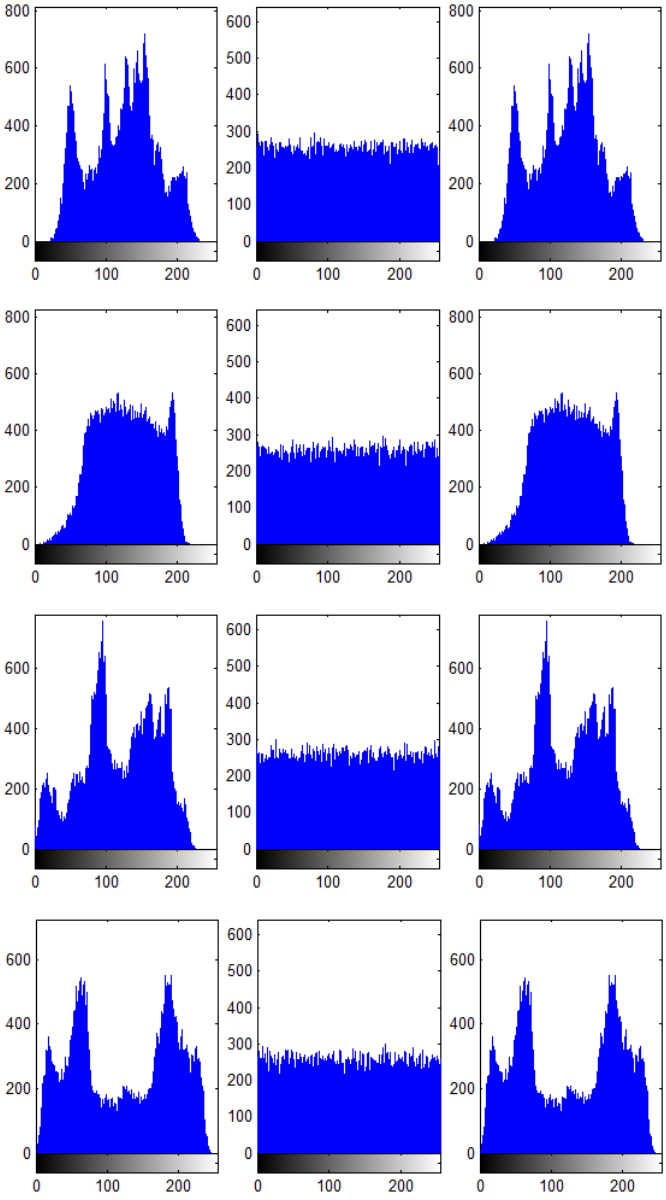
The proposed algorithm runs on MATLAB, 16G of RAM, 3.2 GHz CPU. The experimental images are 'Lena', 'Baboon', 'Peppers' and 'Testpat' with size 256×256. The simulation results are displayed in Figure 4. Their histograms are revealed in Figure 5.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1



(a) (b) (c)

Figure 4. Simulation results: (a) original image, (b) encrypted image, (c) decrypted image.



(a) (b) (c)

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

Figure 5. Histograms of plain, encrypted, and decrypted images: (a) plain, (b) encrypted, (c) decrypted.

6. Security Test

6.1. Key Space Test

If the key space of an encryption scheme is more than 2^{100}, then it will be able to withstand exhaustive attacks [38]. In this manuscript, the secret key is composed of the hash value W and the given values sk_i, i=1, 2, …, 6. Supposing the computation accuracy of 10^{-15} [39], the key space is almost $2^{256}\times(10^{15})^6 \approx 2^{256}\times 2^{299} = 2^{555}$. It is far more than 2^{100} and the designed algorithm could withstand exhaustive attack.

6.2. Histogram Test

The theoretical histogram of an encrypted image is flat and noise-like. Attackers could not find anything from the histogram. Figure 5 shows the uniform and flat pixel value distribution in encrypted image. It represents that the proposed algorithm could withstand count attack. The Chi square distribution [40] is usually used for histogram analysis. It is defined as:

$$\chi^2 = \sum_{l=0}^{255} \frac{(F_l - A)^2}{A} \tag{18}$$

$$A = \frac{M \times N}{256} \tag{19}$$

where F_l is the rate of the gray level l.

If the confidence level is set as 0.05 and the value of χ^2 is less than $\chi^2_{0.05}(255)$ =293.25 [41], then the distribution of the histogram will be very consistent. The result of the Chi square distribution is shown in Table 5.

Table 5. The Chi square distribution.

Image	Lena	Baboon	Peppers	Testpat
$\chi^2_{0.05}(255)$	293.25	293.25	293.25	293.25
χ^2	250.04	242.55	242.14	266.71
Decision	Yes	Yes	Yes	Yes

From Table 5, it reveals that four images can pass the Chi-square examination. Therefore, the histogram distribution of the encrypted image is different from that of the plain image. The designed algorithm is capable of resisting the histogram analysis attack.

6.3. Key Sensitive Test

Key sensitive test plays an important role in security analysis. The hash value W is produced with a plain image. Since the initial conditions of the cryptosystem are generated with hash value and secret keys, the encrypted result is tightly connected with the original image. The Baboon image is used to display the simulation performances. A bit is changed in W and forms a new W_1.

One of the keys is marginally revised (γ=10^{-15}) and the other keys remain the same. The new key is applied to encrypt and decrypt the image

From Figs. 6 and 7, it shows that even if there is a tiny discrepancy between two images or secret keys, the obtained results will be diverse. The discrepancy of the encrypted images C1 and C2 is about 99.6%. Figure 8 reveals that the incorrect key could not correctly decrypt the image. It proves that the proposed scheme could withstand sensitive analysis.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

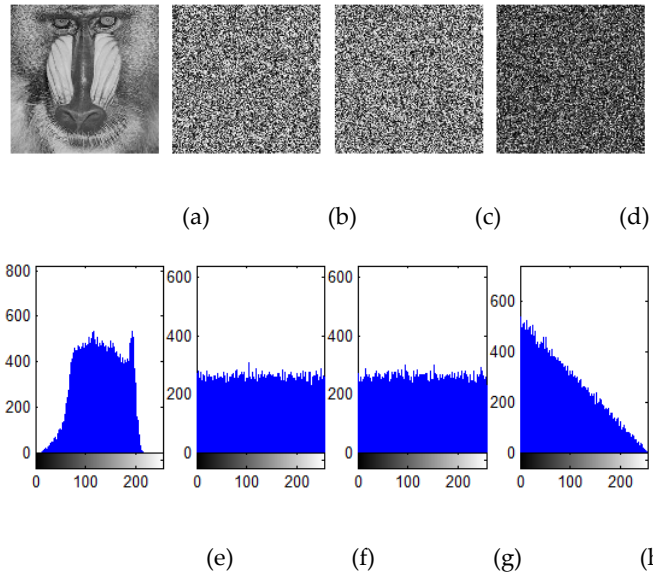


Figure 6. Sensitive analysis to the hash value in the encryption process: (a) plain image, (b) encrypted image C1, (c) encrypted image C2, (d) |C1-C2|, (e) - (h) are the corresponding histograms of (a) - (d).

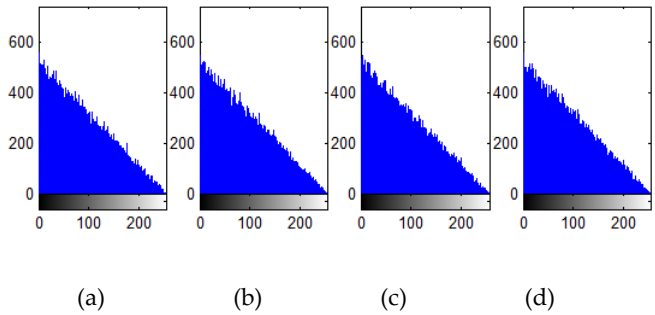


Figure 7. Sensitive analysis of the keys (γ=10^{-15}) in the encryption procedure: (a) |Enc(sk_1+γ)-C1|, (b) |Enc(sk_3-γ)-C1|; (c) |Enc(sk_5+γ)-C1|, (d) |Enc(sk_6-γ)-C1|.

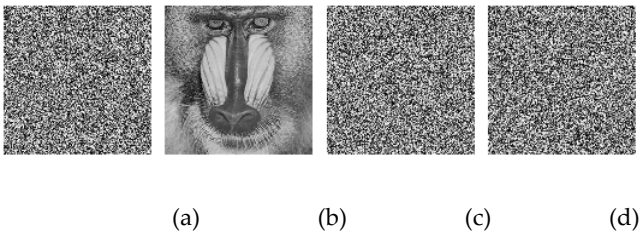


Figure 8. Sensitive analysis of secret keys (γ=10^{-15}) in the decryption procedure: (a) encrypted image C1, (b) the right decrypted result, (c) |Dec(C1, sk_1-γ)|, (d) |Dec(C1, sk_3+γ)|.

6.4. Correlation Test

The correlation coefficient (CR) can be defined as [35]:

$$CR_{AB} = \frac{\sum_{i=1}^{L}(A_i - E(A))(B_i - E(B))}{\sqrt{(\sum_{i=1}^{L}(A_i - E(A))^2)(\sum_{i=1}^{L}(B_i - E(B))^2)}} \quad (20)$$

where A_i and B_i represents the adjacent pixel; L is the total number of pixels.

Some neighboring pixel pairs are randomly chosen to compute the CR values in vertical (V), horizontal (H), and diagonal (D) directions. Figure 9 illustrates the correlation of adjacent pixels in the Baboon image and the corresponding encrypted image. Table 6 shows the CR values in three directions, and Table 7 presents comparisons of the CR values using different algorithms.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

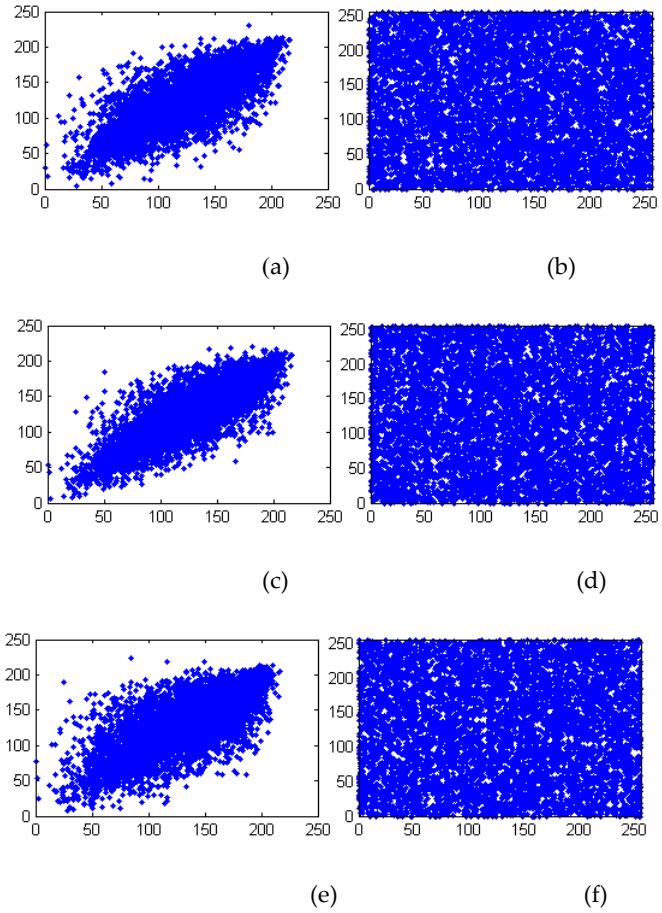


Figure 9. Correlation coefficients of Baboon: (a), (c), (e) are vertical, horizontal, and diagonal directions of the plain image, and (b), (d), (f) are three directions of the corresponding encrypted image.

Table 6. Correlation of four encrypted images.

Image	H	V	D
Lena	0.0018	0.0021	-0.0026
Baboon	0.0012	0.0015	-0.0008
Peppers	0.0014	-0.0029	-0.0003
Testpat	0.0036	0.0078	0.0015

Table 7. Comparisons of CR values.

Scheme	H	V	D
Ref. [10]	0.0065	0.0337	0.0244
Ref. [41]	0.0077	0.0013	0.0006
Ref. [43]	-0.0122	-0.0032	0.0406
Ref. [44]	0.0064	0.0024	0.0043
Ref. [45]	0.0143	0.0103	0.0103
Proposed	0.0012	0.0015	0.0008

Table 6 reveals that the correlation of neighboring pixels in three directions is approaching 0. It symbols that the proposed scheme could effectively defend on the correlation analysis attack. Table 7 indicates that the suggested scheme is more effective than some existing methods.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

6.5. Shannon Entropy Test

The global Shannon entropy (GSE) is often applied to test randomness. It can be computed as follows:

$$\mathrm{GS}E(n) = -\sum_{j=0}^{255} p(n_j)\log_2 p(n_j) \tag{21}$$

where n_j means the j-th information source; $p(n_j)$ symbolises the probability of n_j. For an 8-bit grayscale image, the theoretical value of GSE is 8.

The local Shannon entropy (LSE) is proposed by Wu et al. [46] and adopted to measure randomness from a local perspective. It is calculated as

$$LSE_{r,L}(B) = \sum_{i=1}^{r} \frac{GIE(B_i)}{r} \tag{22}$$

where B_i is a randomly chosen and non-overlapped data block. There are L pixels in each block. In this paper, (r, L) is appointed to (30,1936). If the LSE value lies within the interval [v_{left}^{α}, v_{right}^{α}], then the proposed algorithm will pass the Shannon entropy test [15]. The GSE and LSE values are organized in Table 8.

Table 8. Comparisons of CR values.

Image	GSE	LSE	$v_{left}^{0.001}$ = 7.9015 $v_{right}^{0.001}$ = 7.9034	$v_{left}^{0.01}$ = 7.9017 $v_{right}^{0.01}$ = 7.9032	$v_{left}^{0.05}$ =7.9019 $v_{right}^{0.05}$ =7.9030
			0.001-level	0.01-level	0.05-level
Lena	7.9975	7.9026	pass	pass	no
Baboon	7.9972	7.9028	pass	pass	pass
Peppers	7.9970	7.9021	pass	pass	pass
Testpat	7.9969	7.9018	pass	pass	no

Table 8 indicates that the average value of GSE is about 7.9971. Most LSE values could pass three kinds of tests. It reveals that the designed scheme effectively resists Shannon entropy analysis.

6.6. Differential Attack Test

UACI and NPCR are often used for the differential attack test [34].

$$NPCR = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N} D(x,y) \times 100\% \tag{23}$$

$$UACI = \frac{1}{M \times N}\sum_{x=1}^{M}\sum_{y=1}^{N} \frac{|E_1(x,y) - E_2(x,y)|}{255} \times 100\% \tag{24}$$

$$D(x,y) = \begin{cases} 0, & if \quad E_1(x,y) = E_2(x,y) \\ 1, & else \end{cases} \tag{25}$$

where E_1 and E_2 are two encrypted images.

33.4635% and 99.6094% are the theoretical values of UACI and NPCR [7]. Table 9 reveals that the values of two indicators are close to the ideal values. This means that the designed algorithm is capable of resisting differential attacks.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

Table 9. Comparisons of CR values.

Work	Indicator	Lena	Baboon	Peppers	Testpat
Proposed	NPCR (%)	99.61	99.60	99.62	99.63
	UACI (%)	33.45	33.44	33.45	33.49
Ref. [10]	NPCR (%)	99.61	99.59	99.60	99.62
	UACI (%)	33.42	33.46	33.43	33.49
Ref. [44]	NPCR (%)	99.56	99.60	99.61	99.63
	UACI (%)	33.32	33.45	33.47	33.58
Ref. [45]	NPCR (%)	99.60	99.62	99.61	99.57
	UACI (%)	33.45	33.44	33.45	33.40

6.7. Encryption Quality Test

ID and DUH can be used to measure encryption image quality [8]. Encryption quality will be much better if the values of ID and DUH are smaller. They can be obtained as [47]:

$$H_D = abs(H_P - H_C) \tag{26}$$

$$M_D = \frac{1}{256}\sum_{l=0}^{255} H_D(l) \tag{27}$$

$$ID = \sum_{k=0}^{255} | H_D(k) - M_D | \tag{28}$$

$$DUH = \frac{\sum_{j=0}^{255} | H_C(j) - M \times N / 256 |}{M \times N} \tag{29}$$

where H_C and H_P represent the histograms of encrypted image C and plain image P.

The DUH and ID values are listed in Table 10. It shows that the designed method produces smaller values of two indicators than the existing schemes. It reveals that the proposed algorithm has high encryption quality.

Table 10. Encryption quality test.

Work (Peppers)	**ID**	**DUH**
Proposed	11652	0.0493
Ref. [17]	23863	0.0522
Ref. [47]	28963	0.0782
Ref. [48]	35088	0.0917

6.8. Texture Test

Homogeneity, contrast, and energy are three indexes which are used for texture test [8]. They are defined as follows:

$$Homogeneity = \sum_{u,v} \frac{GLCM(u,v)}{1+|u-v|} \tag{30}$$

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

$$Contrast = \sum_{u,v} |u-v|^2 \; GLCM(u,v) \tag{31}$$

$$Energy = \sum_{u,v} GLCM(u,v)^2 \tag{32}$$

where GLCM(u, v) means the gray-level co-occurrence matrix.

The lower values of homogeneity and energy denote a higher security, and the higher value of contrast will be much better.

Three values are listed in Table 11.

Table 11. Texture test.

Image	Homogeneity	Contrast	Energy
Lena	0.4062	10.5312	0.0166
Baboon	0.4053	10.5417	0.0162
Peppers	0.4068	10.5409	0.0158
Testpat	0.4074	10.5138	0.0173

As shown in Table 11, the designed algorithm performs well. It proves that the proposed method will be able to withstand the texture test.

6.9. Robustness Test

6.9.1. Cropping attack test

Images may be subject to noise or data loss attacks during transmission. Robustness reflects the ability of a scheme to resist interference. The encrypted image of Baboon is cropped 3.125%, 6.25%, 12.5%, and 25% data. The decrypted results are shown in Figure 10.

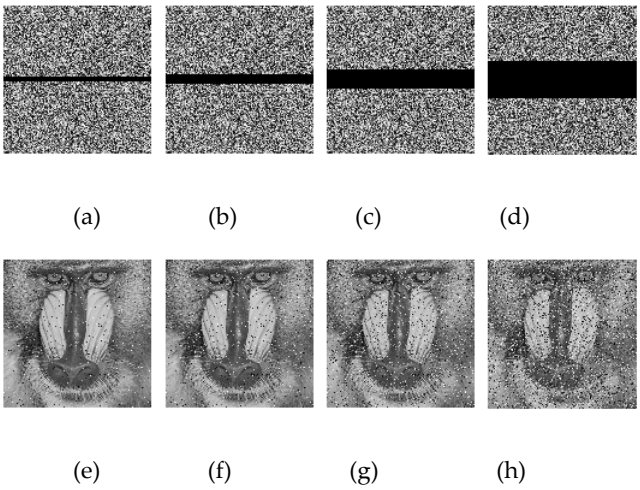


Figure 10. Robustness against cropping attack: (a)-(d) are the encrypted images with 3.125%, 6.25%, 12.5% and 25% data loss, and (e)-(h) are the decrypted images of (a)-(d). .

Figure 10 shows that even if there is a lot of noise in the decrypted result, it is still identifiable. It reveals that the designed algorithm passes the cropping attack test.

6.9.2. Noise attack test

The encrypted image of Baboon is suffered from noise attack. The densities of salt & pepper noise are 0.5%, 2%, 10%, and 30%. Figure11 shows the decrypted images. It means that the recovered

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

images are able to be recognized. It symbolises that the proposed scheme is robust enough to pass noise attack test.

(a) (b) (c) (d)

Figure 11. Robustness against noise attack: (a)-(d) are the decrypted images with 0.5%, 2%, 10%, and 30% noise.

7. Discussion

In the manuscript a novel hyperchaotic image encryption scheme is proposed. Chaotic sequences are generated with 6D chaotic systems. The encrypted result is closely related to the plain image with SHA-512. The initial values are produced with a hash value and a secret key. Each pixel is divided into four equal segments. Permutation is performed based on chaotic sequences. DNA coding, modern DNA complementary rules, DNA computing and DNA decoding are executed on the new image with size M × 4N. The image is performed on diffusion operation, and encrypted image is achieved finally. The experimental results display the effects of the proposed scheme. Secure test shows that the designed method possesses a huge key space, low pixel correlation, high encryption quality, and sensitivity. It also concludes that the designed algorithm could resist common attacks and is much better than some existing methods.

Author Contributions: Conceptualization, S.S. and X.W.; methodology, S.S.; software, S.S.; validation, S.S. and X.W.; formal analysis, S.S.; investigation, S.S.; data curation, S.S.; writing—original draft preparation, S.S.; writing—review and editing, X.W.; funding acquisition, S.S and X.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Hunan Province of China, grant number 2024JJ7310, 2024JJ7317 and the Startup Project for Doctorate Scientific Research of Hunan University of Arts and Science of China grant number 22BSQD07, 22BSQD32.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang X.; Wang S. Steganography using multiple-base notational system and human vision sensitivity. *IEEE Signal Proc. Let.* **2004**, *12*, 67-70.
2. Dash S.; Behera D. K.; Swetanisha S.; Das M. High payload image steganography using DNN classification and adaptive difference expansion. *Wireless Pers. Commun.* **2024**, *134*,1349-1366.
3. Qiao L.; Nahrstedt K. Watermarking schemes and protocols for protecting rightful ownership and customer's rights. *J. Vis. Commun. Image R.* **1998**, *9*, 194-210.
4. Wu S.; Huang J.; Huang D.; Shi Y. Efficiently self-synchronized audio watermarking for assured audio data transmission. *IEEE T. Broadcast.* **2005**, *51*, 69-76.
5. Fernandez J. J.; Nithyanandam P. Protection of online images against theft using robust multimodal biometric watermarking and T-norms. *Multimed. Tools Appl.* **2024**, *83*, 52405-52431.
6. Gao Z. A new chaotic system. *J. Hunan Uni. Art. Sci.* **2011**, *23*, 34-47.
7. Sun S.; Guo Y. A new hyperchaotic image encryption algorithm based on stochastic signals. *IEEE Access* **2021**, *9*, 144035- 144045.
8. Sun S. A new image encryption scheme based on 6D hyperchaotic system and random signal insertion. *IEEE Access* **2023**, *11*, 66009- 66016.
9. Huang H.; Chen Y.; Chen D. Plaintext-related image encryption scheme based on chaos and game of life. *J. Electron. Imaging* **2022**, *31*, 013031.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

10. Hosny K. M.; Kamal S. T.; Darwish M. M.; Papakostas G. A. New image encryption algorithm using hyperchaotic system and fibonacci q-matrix. *Electronics* **2021**,*10*, 1066.
11. Czapski M.; Nikodem M. Error detection and error correction procedures for the advanced encryption standard. *Design. Code. Cryptogr.* **2008**, *49*, 217-232.
12. Orceyre M.; Heller R. An approach to secure voice communication based on the data encryption standard. *IEEE Commun. Society Mag.* **1978**, *16*, 41-50.
13. Rahman M. M.; Sana T. K.; Bhuiyan A. A. Implementation of RSA algorithm for speech data encryption and decryption. *Int. J. Comput. Sci. Net.* **2012**, *12*, 74-82.
14. Musanna F.; Kumar S. A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3-D cat map. *Multimed. Tools Appl.* **2019**, *78*, 14867-14895.
15. Wang X.; Liu C.; Jiang D. A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Syst. Appl.* **2022**, *209*, 118426.
16. Lai Q.; Hu G.; Erkan U.; Toktas A. A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Syst. Appl.* **2023**, *213*, 118845.
17. Alawida M.; A. Samsudin A.; The J. S.; Alkhawaldeh R. S. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* **2019**, *160*, 45-58.
18. Sun X.; Chen Z. Novel chaotic image encryption algorithm based on coordinate descent and SHA-256. *IEEE Access* **2022**, *10*, 114597-114611.
19. Shukur A. A.; AlFallooji M. A.; Pham V. T. Asymmetrical novel hyperchaotic system with two exponential functions and an application to image encryption. *Nonlinear Eng.* **2024**, *13*, 1-12.
20. Zareimani E.; Parvaz R. Secure multiple-image transfer by hybrid chaos system: encryption and visually meaningful images. *Mathematics* **2024**, *12*, 1176.
21. Wang X.; Teng L.; Qin X. A novel colour image encryption algorithm based on chaos. *Signal Process.* **2012**, *92*, 1101-1108.
22. Li C.; Zhang L.; Rong O.; Wong K. W.; Shi S. Breaking a novel colour image encryption algorithm based on chaos. *Nonlinear Dynam.* **2012**, *70*, 2383-2388.
23. Liu Z.; Pun C. Reversible data-hiding in encrypted images by redundant space transfer. *Inform. Sciences* **2018**, *433*, 188-203.
24. Xiang Y.; Xiao D.; Zhang R.; Liang J.; Liu R. Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. *Inform. Sciences* **2021**, *545*, 188-206.
25. Wu X.; Zhu B.; Hu Y.; Ran Y. A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. *IEEE Access* **2017**, *5*, 6429-6436.
26. Zhu C.; Sun K. Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic Tent maps. *IEEE Access* **2018**, *6*, 18759-18770.
27. Anwar S.; Meghana S. A pixel permutation based image encryption technique using chaotic map. *Multimed. Tools Appl.* **2019**, *78*, 27569-27590.
28. Mokhnache A.; Ziet L. Cryptanalysis of a pixel permutation based image encryption technique using chaotic map. *Trait. Signal* **2020**, *37*, 95-100.
29. Chen H.; Bai E.; Jiang X.; Wu Y. Fast image encryption algorithm based on improved 6-D hyper-chaotic system. *IEEE Access* **2022**, *10*, 116031-116044.
30. Man Z.; Zhang Y.; Zhou Y.; Lu X.; Wang Z. Bit level image encryption algorithm based on hyperchaotic system. *Optoelectron. Lett.* **2023**, *19*, 186-192.
31. Mansoor S.; Parah S. A. HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. *Multimed. Tools Appl.* **2023**, *82*, 28769-28796.
32. Watson J. D.; Crick F. H. C. Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid. *Nature* **1953**, *4356*, 737-738.
33. Wang X.; Zhang Y.; Bao X. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Laser. Eng.* **2015**, *73*, 53-61.
34. Zhu S.; Deng X.; Zhang W.; Zhu C. Image encryption scheme based on newly designed chaotic map and parallel DNA coding. *Mathematics* **2023**, *11*, 231.
35. Chai X.; Gan Z.; Yuan K.; Chen Y.; Liu X. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Comput. Appl.* **2019**, *31*, 219-237.
36. Wang Q.; Zhang X.; Zhao X. Color image encryption algorithm based on novel 2D hyperchaotic system and DNA crossover and mutation. *Nonlinear dynam.* **2023**, *111*, 22679-22705.
37. Benkouider K.; Bouden T.; Yalcin M. E.; Vaidyanathan S. A new family of 5D, 6D, 7D and 8D hyperchaotic systems from the 4D hyperchaotic Vaidyanathan system, the dynamic analysis of the 8D hyperchaotic system with six positive Lyapunov exponents and an application to secure communication design. *Int. J. Model. Identif.* **2022**, *35*, 241-257.
38. Alvarez G.; Li S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcat. Chaos* **2006**, *16*, 2129-2151.
39. IEEE standard for binary floating-point arithmetic. *IEEE Standard* **1985**, 754.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 30 August 2024 doi:10.20944/preprints202408.2216.v1

40. Wang J.; Zhang Y.; Wang F.; Ni R.; Hu Y. Color-image encryption scheme based on channel fusion and spherical diffraction. *Chines. Phys. B* **2022**, *31*, 034205.
41. Cao C.; Sun K.; Liu W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *Signal Process.* **2018**, *143*, 122-133.
42. Biban G.; Chugh R.; Panwar A. Image encryption based on 8D hyperchaotic system using Fibonacci Q-Matrix. *Chaos Soliton. Fract.* **2023**, *170*, 113396.
43. Zang H.; Tai M.; Wei X. Image encryption schemes based on a class of uniformly distributed chaotic systems. *Mathematics*, **2022**, *10*, 1027.
44. Mathivanan P.; Maran P.; Color image encryption based on novel kolam scrambling and modifed 2D logistic cascade map. *J. Supercomput.* **2024**, *80*, 2164-2195.
45. Zhao J.; Zhang T.; Jiang J.; Fang T.; Ma H. Color image encryption scheme based on alternate quantum walk and controlled Rubik's Cube. *Scientifc Rep.* **2022**, *12*, 14253.
46. Wu Y.; Zhou Y.; Saveriades G.; Agaian S.; Noonan J. P.; Natarajan P. Local Shannon entropy measure with statistical tests for image randomness. *Inform. Sciences* **2013**, *222*, 323-342.
47. Zhu S.; Zhu C. Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. *IEEE Access* **2019**, *7*, 147106-147118.
48. Belazi A.; El-Latif A. A. A.; Belghith S. A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process. 2016, 128, 155-170.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.