MJPAS Vol. 1, No. 1 (2023) 68-79

Mustansiriyah Journal of Pure and Applied Sciences
https://mjpas.uomustansiriyah.edu.iq
Print ISSN: 2957-9910 Online ISSN: 2957-9929

A New Method for Color Image Encryption Using Chaotic System and DNA Encoding

Huda R. Shakir[1], Sadiq A. Mehdi[2], Anwar A. Hattab

[1,3] Department of Computer Science, College of Education, Mustansiryah University, Baghdad, Iraq,

[2] Department of Mathematics, College of Education, Mustansiryah University, Baghdad, Iraq ([1]hudarashid@uomustansiriyah.edu.iq, [2]sadiqmehdi71@uomustansiriyah .edu .iq,

[3] hudarashid@uomustansiriyah.edu.iq)

A B S T R A C T

Image encryption is an essential area of visual cryptography that helps protect images when they are shared over the internet. There are many cryptography algorithms applied for many years in encrypting images. In recent years, techniques from chaotic systems have been combined with DNA coding to help encrypt images and protect them from unauthorized use. In this study, we proposed a new method for image encryption based on a new four-dimensional chaotic system and DNA encoding. The proposed method consists of two stages: the pixel positions are scrambled depending on which chaotic sequences are generated from the new chaotic system; and then, an XOR operation is performed on the image scrambled by using the DNA encoding sequence to get the final encryption image. Analyses such as entropy, NPCR, UACI, and key space are used to evaluate the algorithm's performance. The algorithm attains average entropy of 7.99, which is close to the ideal value of 8 with NPCR and UACI of 99.64 and 33.02, respectively. In addition, the key space is 2^{627}. The simulation results show that the proposed method offers high security, good encryption, and is resistant to many types of attacks

Keywords: *Chaotic system, DNA encoding, scramble, Image encryption*

1. Introduction

With the fast growth of multimedia data like images and their transmission across unsecured communication channels, security is becoming increasingly important to prevent risks and data loss [1]. Image encryption is the most common approach for protecting the confidentiality of image data [2]. Due to the characteristics of digital image data, like large storage capacity, high redundancy, and significant correlation between neighboring pixels [3], several traditional data encryption algorithms, such as AES, RSA, and DES, are not well-suited to digital image encryption [4], [5].

Corresponding auth: Huda R. Shakir
E-mail address: hudarashid@uomustansiriyah.edu.iq
,

Therefore, the trend was to other theories and algorithms to provide high encryption and security specifications for the digital image. Chaos theory is one of them. Chaos theory is utilized in the field of encryption due to its advantages and its close relationship with cryptography, which is characterized by randomness, unpredictability, ergodicity, and high sensitivity to initial states [6], [7], [8]. Fridrich, in 1998, introduced the first general architecture for image encryption that relies on chaos, which is made up of confusion and diffusion [9]. After a few years, the integration of this chaos theory with the use of DNA encoding for building effective encryption algorithms, due to properties of DNA coding such as large information storage capacity, powerful parallel computing ability, and ultra-low power consumption. For these reasons, it is widely used in encryption systems [10], [11].

There are many researches on image encryption algorithms built on chaotic systems and DNA. Q. Liu and L. Liu, [9], Presented a bit-level DNA computation and a double-chaos system as the basis for a color image encryption technique. The Arnold method was used to scramble the three colors of the original image, and then the improved double-chaos system was employed for the diffusion process. Afterwards, the final ciphertext image was created by employing DNA coding and DNA computing to spread the three sets of images. The tests show that the algorithm is safe and can withstand many different kinds of attacks.

M. Malik et al., [11], proposed a novel method that combines a hyperchaotic dynamical system and DNA computing. The channels are initially diffused at a decimal level. They are then permuted. Additionally, DNA encoding is carried out on these channels. In addition, DNA level diffusion is applied to increase the unpredictability of the image. The final encryption image is produced by converting the DNA-encoded image into decimal. The results of the experiments, as well as the security analysis, show the robustness of the proposed method. F. Masood *et al.*, [12] proposed a method that uses DNA sequencing, Arnold transformation (AT), and a chaotic system to secure sensitive information within images. The results demonstrate that the presented system is highly resistant to a variety of attacks. Additionally, demonstrate the effectiveness of the suggested algorithm.

The motivation for this paper is to design a new scheme for image encryption by exploiting the good features of chaotic systems, such as randomlike behavior, ergodic behavior, and sensitivity to initial states, as well as the advantages of DNA computing, like strong parallel processing, very low power consumption, and large data storage capacity. So, in this paper we introduced a new approach by combining a new 4-D chaotic system and DNA encoding for image encryption, which includes two phases: The chaotic sequences were used to scramble the three color bands of the original image, and then the XOR DNA operations were employed for the diffusion phase to get the encrypted image.

2. Theoretical Background

2.1. DNA encoding

In 1994, Adelman was the first to apply DNA computing in cryptography to address the Hamiltonian path issue instead of traditional cryptography. DNA is a molecule that has the genetic information required for the growth, evolution, and reproduction of all living organisms. A(adenine), G(guanine), C(cytosine), and T(thymine) are the four nucleic acid bases found in DNA sequences. Following the principle of complementary pairing, these are the nucleotides Adenine and Thymine, Guanine and Cytosine. While the letters A, C, G, and T represent numbers, they can also denote the decimal digits 0, 1, 2, and 3. These four decimal digits correspond to the binary values 00, 01, 10, and 11, indicating that each nucleotide can contain two bits of data. This coding employs 4! = 24 different encoding approaches [13], [14]. Table 1 shows only eight different types of encoding schemes that correspond to the complimentary pairing requirement. Table 2 also provides exclusive-or DNA operations.

Table 1. DNA rules [14].

Rules	1	2	3	4	5	6	7	8
0	A	A	C	C	G	G	T	T
1	G	C	T	A	T	A	G	C
2	C	G	A	T	A	T	C	G
3	T	T	G	G	C	C	A	A

Table 2. The X-or DNA operations [14].

(Xor)	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	A	C

2.2 Construction of the New Chaotic System

A new 4D-Hyper Chaotic System is constructed using a system model represented by the following differential equation:

$$\frac{dx}{dt} = -a\,x - b\,w + c\,y\,z + z\,e^{y} \quad (1)$$
$$\frac{dy}{dt} = d\,y + e\,x - f\,x\,z - x\,e^{z}$$
$$\frac{dz}{dt} = -\,g\,z + h\,x\,y$$
$$\frac{dw}{dt} = -b\,w + i\,x\,z + j\,y\,z$$

Where x, y, z, and w called the states of system, t $\in\Re$ and $a, b, c, d, e, f, g, h, i, and\ j$ are positive parameters of the system(1) shows a chaotic

attractor in a new four-dimensional chaotic system with parameter values of: *a*=3.1, *b*=2.1, *c*=15.8, *d*=1.1, *e*=16.5, *f*=1.5, g=2.4, h=26.6, i=5.1, and j=12.9, and the initial states of : x(0)=0.2, y(0)=0.4, z(0)=1.5, and w(0)=0.8.

Lyapunov exponents & Lyapunov-dimension

Calculating the Lyapunov exponent, according to nonlinear dynamical theory, is a quantitative measure of the sensitive dependency on the initial values. It's the average rate at which two adjacent trajectories diverge (or converge). When the system's parameters(1) are chosen as: (a=3.1, b=2.1, c=15.8, d=1.1, e=16.5, f=1.5,g=2.4, h=26.6, i=5.1, and j=12.9), as well as the initial values as follows: LE1= 4.05761, LE2= 0.347562, LE3= -3.94257 and LE4= -6.61896. It could be seen that the maximum Lyapunov exponent is positive; pointing to that the system contains chaotic properties. We see two positive Lyapunov exponents are LE1 and LE2, and the other two are negative As a result, the Kaplan-Yorke dimension is calculated utilizing Lyapunov exponents, the fractal dimension is a feature of chaos, and DKY is defined as follows:

$$D_{KY} = j + \frac{1}{|L_{j+1}|}\sum_{i=1}^{j} L_i \qquad (2)$$

Where J namely, is the first Lyapunov exponent, and j is the largest value of the i values that satisfy both $\sum_{i=1}^{j} L_i > 0$ and, $\sum_{i=1}^{j+1} L_i < 0$ at the same time. Lyapunov exponents may be used to show us that the Li is in descending order, and DKY is our upper bound for system information dimension. For this new chaotic system, because the values of Lyapunov exponents is ten, so the j value is ten, and the Kaplan-Yorke dimension can be calculated from the above equation because L1+L2+ L3 +L4<0 ,and L1+L2+L3>0, the Lyapunov-dimension of a novel chaotic system will be as follows:

$$D_{KY} = 3 + \frac{1}{|L_{j+1}|}\sum_{i=1}^{3} L_i = 3 + \frac{L_1+L_2+L_3}{L4} \qquad (3)$$

$$= 3 + \frac{4.05761+0.347562\pm3.94257}{6.61891}$$

=3.06989

This means that the system (1) has a fractional Lyapunov-dimension, the novel system contains non-periodic orbits, and its neighboring paths diverge. Hence, the non-linear system is chaotic.

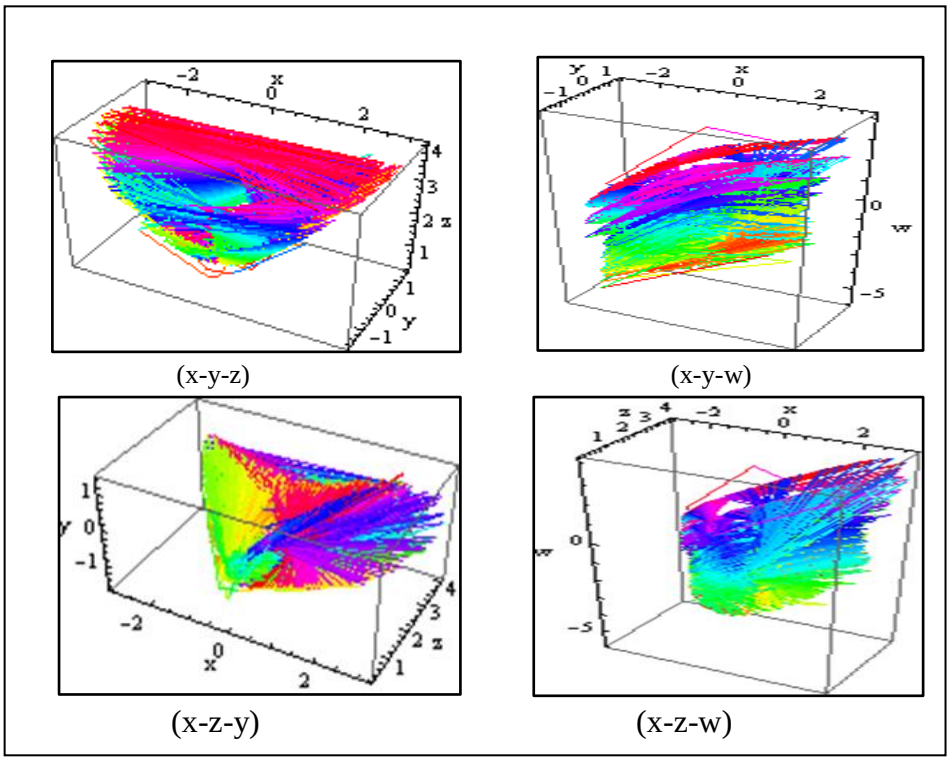

Figure 1. Chaotic attractors, 3-D view

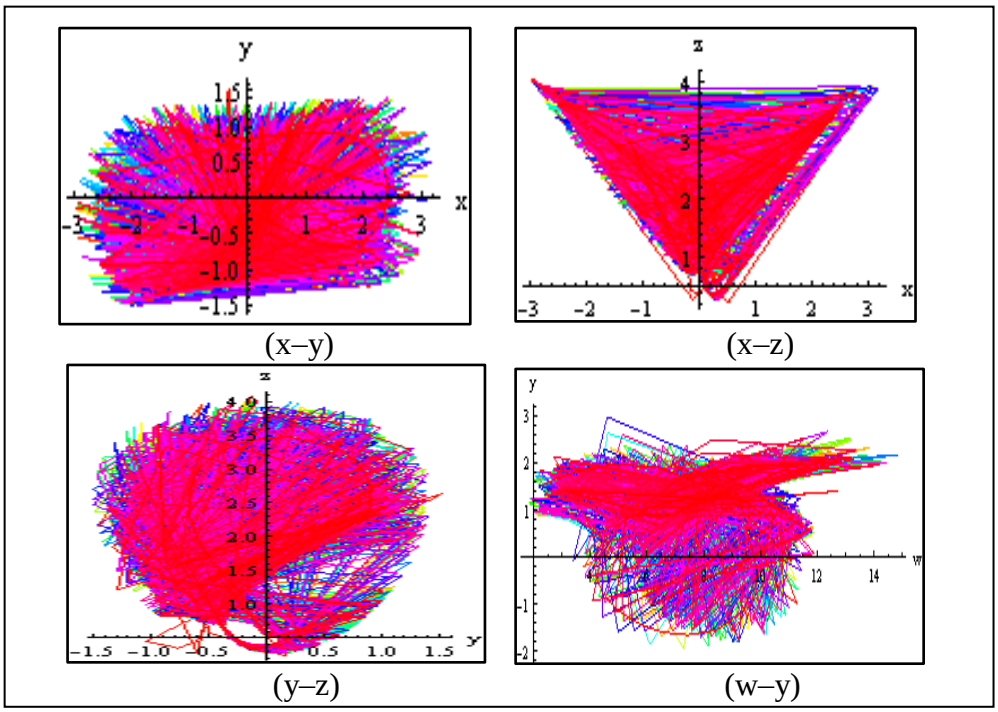

Figure 2. Chaotic attractors, 2-D view

3. The Proposed Algorithm

In the encoding stage, a new four-dimensional chaotic system was proposed to encode the original image using four chaotic sequences (xi, yi, zi, and wi) generated by the system (1). In the first stage, the three chaotic sequences (xi, yi, and zi) were used to combination the three color bands (RGB) by sorting the sequences in ascending order and obtaining the index sequences (xi, yi, and zi) to produce sequences (k1, k2, k3), so that the first sequence (k1) is used to scramble the red vector (Vr), the second sequence (k2) scrambles the green vector (Vg), and the third sequence (k3) scrambles the green vector (Vb). Then, the resulting scramble image from the previous step and the fourth sequence k4 are encoded into the DNA sequence based on Table 1, and DNA xor operations (based on Table 2) are applied between them to get the final encryption image, which is shown in Figure 2. In the decryption algorithm, the previous stages will be reversed to retrieve the plain image. Algorithm (1) describes the steps of the encryption process.

3.1. Encryption Algorithm (1)

Input: original image (OI) of size h×w×3, initial conditions(x0,y0,z0, and
w0) and parameters (a, b, c, d, e, f, g, h, I, j)
Output: encrypted image (En)
Begin
step1: read (OI) image
step2: split (OI) image into three color bands R, G, and B
step3: assign h←height of OI
assign w←width of OI
Calculate S← h×w
step4: Reshape bands R, G, and B into three vectors Vr, Vg, and Vb
step5: Generate four chaotic sequences x, y, z, and w by applying eq.1, size of sequences ≥ S
step6: Scrambling step:
- Sort the sequence xi ascending and generate the index of the sequence
xi as (k1) to scramble the vector red (Vr) and produce Vr1.
- Sort the sequence yi ascending and generate the index of the sequence
yi as (k2) to scramble the vector red (Vg) and produce Vg1.
- Sort the sequence xi ascending and generate the index of the sequence
zi as (k3) to scramble the vector red (Vb) and produce Vb1.
step7: combine three vectors Vr1, Vg1, and Vb1 into one vector Vrgb
step8: Encode the vector Vrgb into a DNA sequence according to Table1 to get
the vector $Vrgb_{DNA}$
step9: Ecode the vector k4 into DNA sequence according to Table1 to get the

Vector $k4_{DNA}$

step10: apply xor DNA operation between $Vrgb_{DNA}$ and $k4_{DNA}$ based on Table 2 to produce V_{RGB}

step11: Decode DNA sequence (V_{RGB}) and divide it into three vectors vR,vG,vB and reshape each vector into matrices (MR, MG, and MB)

step12: concatenate (MR, MG, and MB) to obtained 3D matrix encrypted image (En)

End Algorithm

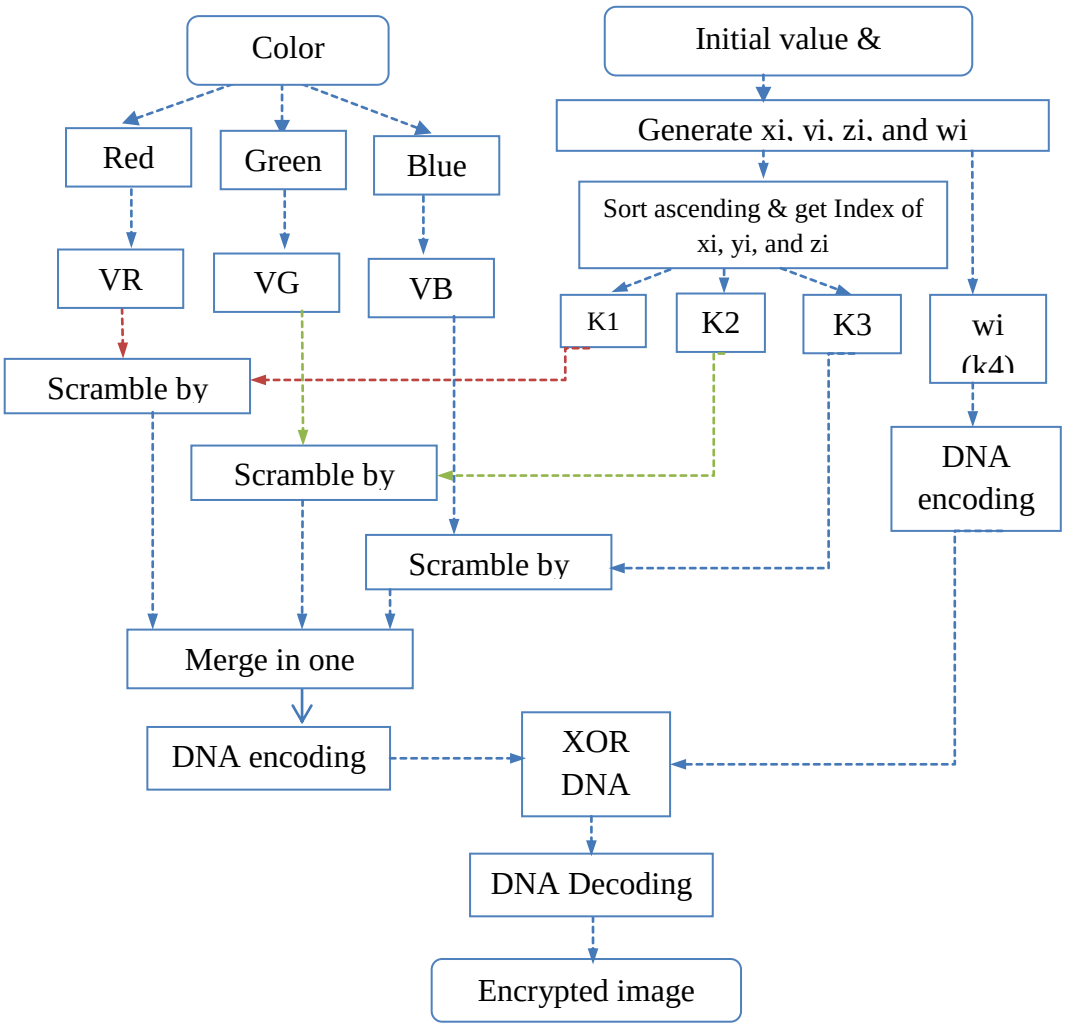

Figure 3. The general framework of encryption stage

3.2. Security Analysis and Results

We evaluate the performance of the suggested image encryption scheme in this section, by using three standard color images with a size of 256 × 256 × 3.

3.3. Key space analysis

The key space of an effective image encryption technique must be sufficiently large to withstand an exhaustive attack. To avoid brute-force attacks, the key space of a cryptosystem must be at least 2^{128} [15]. The key space of the proposed algorithm is obtained from the initial states and parameters of a four-dimensional hyper-chaotic system, which is (14) value; hence, the key space equals $(10^{196}) = 2^{627}$. Therefore, the value of the key space is enormous to withstand brute force attacks.

4. Histogram Analysis

A robust image encryption system should produce an image histogram that is uniform regardless of the nature of the original image [16]. Figure 4 demonstrates the histograms of three tested images before and after encryption: Lena, the Palace, and the garden. From the figures, you can see that the histogram of the encrypted image is fairly uniform and very diverse from that of the original image.

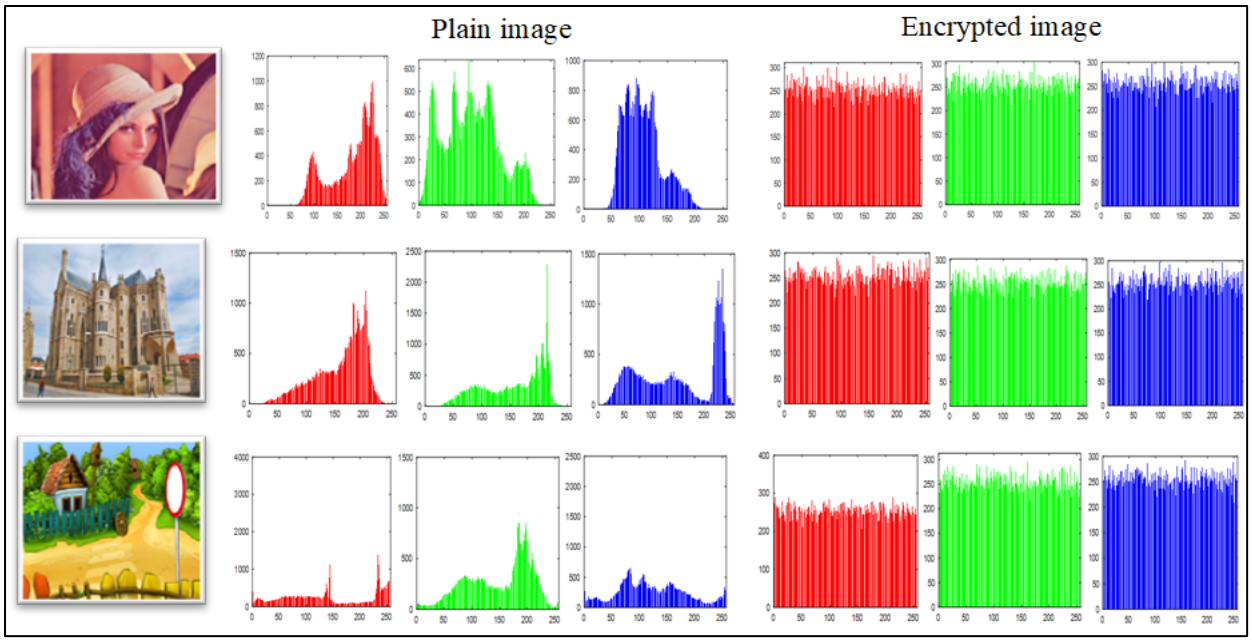

Figure 4. Histogram of RGB bands of the Plain Images and Encrypted Images

5. Information Entropy Analysis

Information entropy was first introduced by Shannon in 1948, utilizing the thermodynamic concept of entropy to identify the association between probability and information redundancy in mathematical terms. A perfectly random image has an information entropy of 8 [17], [18]. The information entropy of a random information sequence X can be calculated with formula (4):

$$Entropy\ E(X) = -\sum_{i=1}^{2*n} p(X_i)\log p(X_i) \quad (4)$$

In table (3), the results indicate that the information entropy of the cipher images is close to 8 bits. This indicates that the system is capable of resisting entropy attacks.

Table 3. The entropy test of images

Image	**Palace**
Lena	7.9987
Palace	7.9981
Garden	7.9991

6. **Differential Attack Analysis**

Differential attack measures like the Unified Average Changing Intensity and the Number of Pixels Change Rate can be used to evaluate how susceptible the original data is to even small modifications. Assume the cipher images are C and C' before and after modifying a single pixel in a plain image. The following is the formula:

$$NPCR = \frac{\sum_{ij} D(i,j)}{W * H} \times 100\% \quad (5)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (6)$$

W represents the image's width, while H represents the image's height; C1 and C2 indicate the encrypted images before and after a single pixel change in the original image, respectively [19], [20]. In Table (4), it indicates that the suggested algorithm's values are nearer to the theoretical value. Therefore, the suggested algorithm is much better able to withstand differential attacks.

Table 4. The NPCR and UCAI test

Image	NPCR	UCAI
Lena	99.6436	33.0203
Palace	99.6298	33.9346
Garden	99.6173	34.9185

7. Comparison with other proposed method

In order to evaluate the encryption algorithm, the comparative results of the entropy, UACI, and NPCR tests of Lena image between the proposed method and the relevant studies [9], [11], are shown in table (5). Based on the results in Table 5, our proposed method is more secure against differential and statistical attacks than the methods used in related studies [9], [11].

Table 5. Comparison of results from tests of Lena image with other methods

Lena encrypted image	Entropy	NPCR	UCAI
Proposed method	7.9987	99.6436	33.0203
Ref. [9]	7.9896	99.61	32.20
Ref. [11]	7.9972	99.6300	33.5269

8. Conclusion

A new 4-D hyper chaotic system and DNA encoding have been presented to encrypt color images and achieve high security levels. The simulation experiment and security tests indicate that the presented algorithm is efficient where it contains a large key space equivalent to 2627 keys, the histogram is fairly uniform, while the entropy is near to the ideal value of (8); moreover, the NPCR and UACI values are close to the ideal values of (99.99%) and (33.33%), respectively. All of this indicates that this algorithm has a high level of efficiency, good encryption effectiveness, and a robust ability to withstand various attacks.

9. References

[1] M. Liu and G. Ye, “A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm,” *Math. Biosci. Eng.*, vol. 18, no. 4, pp. 3887–3906, 2021, doi: 10.3934/mbe.2021194.

[2] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, “Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding,” *IEEE Access*, vol. 7, no. c, pp. 36667–

36681, 2019, doi: 10.1109/ACCESS.2019.2906292.
[3] G. Cui, L. Wang, X. Zhang, and Z. Zhou, *An Image Encryption Algorithm Based on Dynamic DNA Coding and Hyper-chaotic Lorenz System*. Springer Singapore, 2018.
[4] D. Keji and D. Xuebao, "Image Encryption Using Chaotic Maps and DNA Encoding," *J. Xidian Univ.*, vol. 14, no. 4, 2020, doi: 10.37896/jxu14.4/206.
[5] S. Suri and R. Vijay, "A synchronous intertwining logistic map-DNA approach for color image encryption," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 6, pp. 2277–2290, 2019, doi: 10.1007/s12652-018-0825-0.
[6] L. Li and L. Kong, "A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding," *Xitong Fangzhen Xuebao / J. Syst. Simul.*, vol. 30, no. 3, pp. 954–961, 2018, doi: 10.16182/j.issn1004731x.joss.201803023.
[7] S. A. Mehdi and A. A. Kadhim, "Image Encryption Algorithm Based on a New Five Dimensional Hyperchaotic System and Sudoku Matrix," *Proc. 5th Int. Eng. Conf. IEC 2019*, pp. 188–193, 2019, doi: 10.1109/IEC47844.2019.8950560.
[8] S. Zhu and C. Zhu, "Secure image encryption algorithm based on hyperchaos and dynamic DNA coding," *Entropy*, vol. 22, no. 7, 2020, doi: 10.3390/e22070772.
[9] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," *IEEE Access*, vol. 8, pp. 83596–83610, 2020, doi: 10.1109/ACCESS.2020.2991420.
[10] H. Wen, S. Yu, and J. Lü, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 21, no. 3, pp. 1–18, 2019, doi: 10.3390/e21030246.
[11] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020, doi: 10.1109/ACCESS.2020.2990170.
[12] F. Masood *et al.*, "A new color image encryption technique using DNA computing and Chaos-based substitution box," *Soft Comput.*, vol. 0123456789, 2021, doi: 10.1007/s00500-021-06459-w.
[13] D. H. Elkamchouchi, H. G. Mohamed, and K. H. Moussa, "A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion," *Entropy*, vol. 22, no. 2, 2020, doi: 10.3390/e22020180.
[14] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, 2018, doi: 10.1007/s11042-018-5902-z.
[15] S. A. M. and A. A. Hattab, "Image Encryption Depend on DNA Encoding and a Novel Chaotic System," no. April 2018, 2019.
[16] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process. Image Commun.*, vol. 80, no. June 2019, p. 115670, 2020, doi: 10.1016/j.image.2019.115670.
[17] B. Bouteghrine, C. Tanougast, and S. Sadoudi, "Novel image encryption algorithm based on new 3-d chaos map," *Multimed. Tools Appl.*, vol. 80, no. 17, pp. 25583–25605, 2021, doi: 10.1007/s11042-021-10773-8.
[18] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt. Laser Technol.*, vol. 135, no. February 2020, p. 106610, 2021, doi: 10.1016/j.optlastec.2020.106610.
[19] K. Ma, L. Teng, X. Wang, and J. Meng, "Color image encryption scheme based on the

combination of the fisher-yates scrambling algorithm and chaos theory," *Multimed. Tools Appl.*, vol. 80, no. 16, pp. 24737–24757, 2021, doi: 10.1007/s11042-021-10847-7.

[20] M. Roy and S. Chakraborty, "A robust image encryption framework based on DNA computing and chaotic environment," *Microsyst. Technol.*, vol. 0, 2021, doi: 10.1007/s00542-020-05120-0.