STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **12**, May 2024, pp 697–712.
Published online in International Academic Press (www.IAPress.org)

Securing Color Images with an Innovative Hybrid Method Combining DNA Computing and Chaotic Systems

Hanaa Mansouri [1,*], Nawal El ghouate [1], Mohamed Amine Tahiri [1], Ahmed Bencherqui [1], Hassane Moustabchir [1], Hassan Qjidaa [2], Mhamed Sayyouri [1]

[1] *Engineering, Systems, and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah-Fez University, Fez, Morocco*
[2] *Electronic Signals and Information Systems Laboratory, Faculty of Science, Sidi Mohamed Ben Abdellah-Fez University, Fez, Morocco*

Abstract Modern cryptography is a key element of data security, ensuring the confidentiality and integrity of information. In an increasingly digital world, cryptography remains crucial for the protection of sensitive data. In this context, we propose a novel hybrid security system for encrypted color images using a DNA model, chaotic systems, and SHA256-MD5 hash functions as a basis. The proposed hybrid system includes DNA permutation and diffusion. In DNA permutation, we unpredictably rearrange the location of DNA image elements by using the logistic map of low computational complexity. In DNA diffusion, we diffuse the permuted image of DNA with the DNA image key generated by a 5D hyper-chaotic system, using a variety of algebraic operators such as the circular offset in both directions. Considering the experimental outcomes and security evaluation, we can infer that the proposed hybrid security system demonstrates a high level of security, resistance to existing attacks, and practical application suitability while maintaining speed.

Keywords Color image encryption, DNA computing, Chaotic system

AMS 2010 subject classifications 68P25, 94A60 34C28, 37D45, 49N30, 93C21

DOI: 10.19139/soic-2310-5070-1952

1. Introduction

The fast advancement of computer and network technology has drawn the attention of many people to multimedia communication services, especially digital images [1, 2, 3]. Since digital images include a wealth of confidential personal and private information, protecting them from misuse and unauthorized access during transmission has become critical [4, 5]. Image encryption is the most important technology for maintaining the security and confidentiality of image data. Traditional encryption methods such as Advanced Encryption Standard Critical and Digital Signature Algorithms [43] are available. Still, they are unsuitable for image encryption because their security is principally focused on high computational cost, whereas images are distinguished by massive data capacity and good correlation between adjacent pixels. Therefore, all researchers became interested in developing an efficient, effective, and secure image encryption method [36, 37, 38, 6, 7].

Several image encryption methods have been proposed based on chaotic systems, which exhibit properties such as sensitivity to initial conditions and unpredictability, and on DNA computing, which has large memory capacity, extensive parallelism, and minimal power consumption [8, 9, 10]. However, it was noted that the using

[*] Correspondence to: Hanaa Mansouri (Email: hanaa.mansouri@usmba.ac.ma). Engineering, Systems, and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah-Fez University. Avenue My Abdallah Km 5, Route d'Imouzzer, Fez BP 72, Morocco.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

of DNA-based image encryption in isolation is not secure enough [26, 27]. As a result, researchers have integrated DNA computing with chaotic systems to enhance image encryption security, resulting in a body of work that spans several references [28]. Despite these efforts, limitations in the use of DNA computing and chaotic systems for image encryption continue to exist, including the creation of cryptographic keys from simple images by transforming the information contained in the image into a complex and unique sequence of bits. Additionally, the security vulnerabilities associated with low-dimensional chaos, such as increased predictability, sensitivity to initial conditions, possible low entropy, and susceptibility to brute force attacks. Finally, the relatively slow encryption velocity [34, 35, 36, 37, 38, 39]. This motivates our proposal for an innovative hybrid security system for color image encryption, which provides an integrated solution that overcomes the specific challenges of cryptographic key generation by using the hash functions of the simple image. In addition, the specific challenges related to the security of low-dimensional chaotic systems, by using a high-dimensional system in the broadcast process to obtain a more efficient diffusion of the bits of the original image throughout the encrypted message. This contributes to a more robust dispersion of information, thereby strengthening the security of the encryption.

The main contributions of the proposed scheme are as follows:

- Combination of SHA256 and MD5 hashes, in conjunction with information extracted from the simple image and a randomly generated key to produce initial and control values for chaotic systems.
- The proposed encryption scheme benefits from the lower computational complexity of a 1D chaotic system to achieve faster encryption times. The encoding and decoding rules, based on this chaotic system, are applied to each pixel of the simple image, and the inclusion of a random key enhances the method's resistance to potential attacks, making it a robust method for image encryption.
- In DNA permutation, we unpredictably rearrange the locations of DNA image elements by using the logistic map. This process is used to diminish the elevated correlation observed among neighboring pixel values.
- In DNA diffusion, we employ diverse algebraic operations to diffuse the permuted DNA image with a key generated through a 5D hyperchaotic system known for its robust confidentiality and significant key space, aiming to minimize simulation time and enhance the security of the encryption method.
- Utilizing the five chaotic sequences derived from the 5D hyperchaotic map, we perform the selection of DNA rules and execute seven operations.

The ensuing sections of the paper are presented as follows. Section 2 clarifies the basic concepts, encompassing DNA computing, and chaotic systems. Section 3 explains our proposed image encryption method. Section 4 is devoted to Simulation and performance evaluation outcomes. Lastly, Section 5 provides a brief summary and conclusion.

2. Preliminaries

The differences between textual data and digital images make text encryption techniques inapplicable to image encryption. The first difference concerns the size, the quantity of information stored in the image is much bulky than the stored information in the textual data. In addition, the second difference concerns the loss of data when a compression technique is applied. Image encryption techniques are classified according to several concepts: spatial, transform, optical, and compressive sensing (see Fig. 1) [5].

2.1. Deoxyribonucleic acid sequence (DNA) computing

DNA computing utilizes a two-step methodology: encoding/decoding and employing algebraic operations on DNA sequences.

DNA encoding/decoding. The extensive utilization of deoxyribonucleic acid (DNA) in biological science and various applied fields, including biotechnology, diagnostics, and forensics, underscores its utmost importance for scientists [30]. The four types of nucleic acids—adenine (A), guanine (G), cytosine (C), and thymine (T)—compose

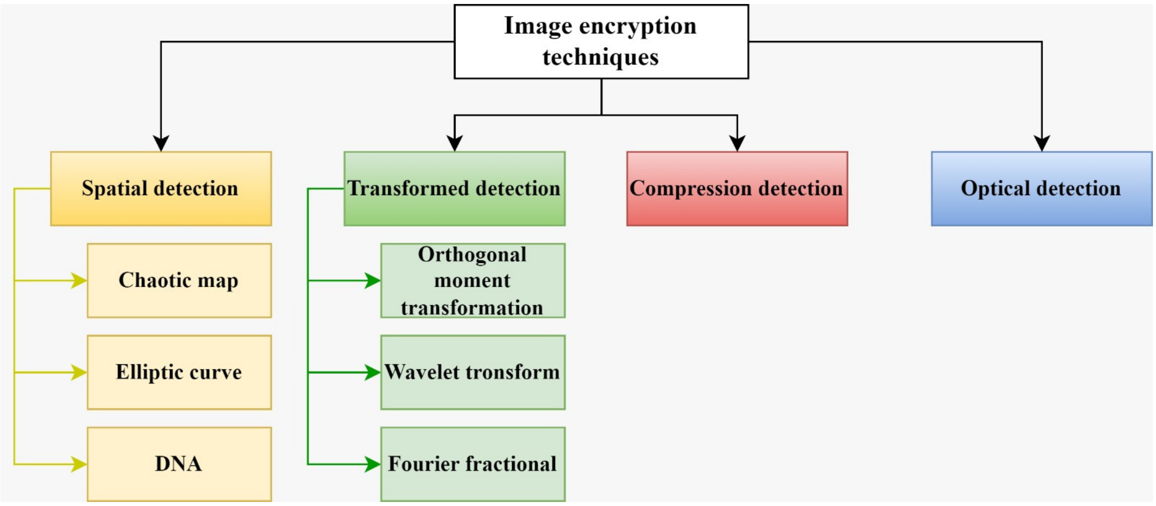


Figure 1. Image encryption techniques.

the DNA sequence. An important rule in base pairing dictates that A and T bases pair together, as do C and G [7]. These relations are known as Watson–Crick base pairing rules [31]. According to these rules of complementarity, Within the set of 24 codes, a discerning analysis reveals that merely 8 of them align with the prescribed rule. In the quaternary numbering system, 0 and 3 bases pair together, as do 1 and 2. Considering quaternary coding, the four-digit quaternary numbers 0, 1, 2, and 3 can be coded to a four-letter DNA sequence—A, C, G, and T—using one of the rules, as demonstrated in Table 1 [11, 12, 13]. In the context of color images, where each pixel is generally represented by three channels (R, G, B), quaternary coding can be applied separately to each channel. This retains the complexity of the pixel information while simplifying the representation using a four-symbol coding system.

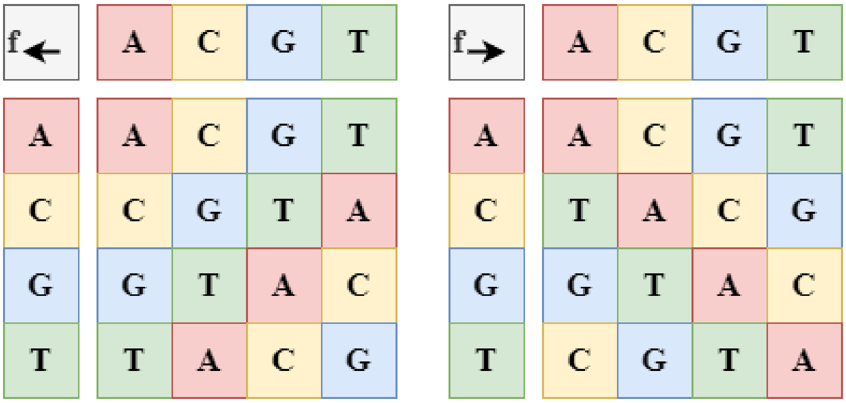
Table 1. DNA coding rules.

Quaternary coding	Rul1	Rul2	Rul3	Rul4	Rul5	Rul6	Rul7	Rul8
0	G	C	T	T	G	A	A	C
1	A	G	C	A	C	T	C	T
2	T	T	G	G	T	C	G	A
3	C	A	A	C	A	G	T	G

DNA Algebraic Operations. Since the development of DNA computing, researchers have proposed using the algebraic operation of DNA sequence to replace the traditional computational algebraic operation [12, 32, 33]. In this article, different operations for DNA sequences have been used like addition, subtraction, multiplication, Xor, Xnor, and right circular shift, which moves the final entry to the first position and left circular shift, which moves the initial entry to the final position, as shown in Fig. 2. These operations facilitate the diffusion process between the DNA image and the key, which enhances security by making it difficult for attackers to predict changes, identify patterns, or perform cryptanalysis on the encrypted image.

2.2. Chaotic systems

In cryptography, a chaotic system is a deterministic yet unpredictable dynamic system, marked by sensitivity to initial conditions (S2IC). The unpredictability of chaotic trajectories makes it difficult to predict encrypted pixel



f←	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

f→	A	C	G	T
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C
T	C	G	T	A

Figure 2. DNA operations.

values without precise knowledge of keys and initial conditions, while the S2IC ensures that slight variations produce entirely different results. These properties make chaotic systems a robust choice, providing substantial protection against cryptographic attacks and ensuring visual data privacy. Chaotic systems are chosen for their ability to improve the security of encryption systems through their complex, nonlinear, and difficult-to-reverse nature [8, 14, 15, 16].

Afterward, we will use a 1-dimensional chaotic system, which is the logistic map, and a 5-dimensional hyperchaotic system defined in (1):

$$\begin{cases} \dot{x}_1 &= -a_1 + a_1 x_2 \\ \dot{x}_2 &= a_2 x_1 + a_2 x_2 + x_5 - x_1 x_3 x_4 \\ \dot{x}_3 &= -a_3 x_2 - a_4 x_3 - a_5 x_4 + x_1 x_2 x_4 \\ \dot{x}_4 &= -a_6 x_4 + x_1 x_2 x_3 \\ \dot{x}_5 &= -a_7 x_1 - a_7 x_2 \end{cases} \tag{1}$$

Where x_1, x_2, x_3, x_4, x_5 are the state variables and $a_i (1 \leq i \leq 7)$ are the control values. To verify the quantitative behavior of the 5-D system, we will study the Lyapunov exponent values and phase portraits in different planes and spaces [44].

Lyapunov exponents. With the control values configured as $a_i = [30, 10, 15.7, 5, 2.5, 4.45, 38.5]$, the Lyapunov exponents computed for system (1) are presented as $\lambda_1 = 4.9018, \lambda_2 = 0.3846, \lambda_3 = 0, \lambda_4 = -15.8628, \lambda_5 = -31.9095$. These values confirm the presence of hyper-chaos, as evidenced by the existence of two positive exponents and a negative sum of the first five exponents, $\sum_{i=1}^{5} \lambda_i = -42.4859 < 0$. The larger positive Lyapunov exponent indicates that the system trajectories exhibit more pronounced variation in phase space. This complexity of the system results in increased sensitivity to initial conditions, Increasing the level of difficulty for attackers. predict or accurately reproduce specific steps in the encryption process without precise knowledge of the initial conditions. This feature helps to enhance the protection and security of our system.

Phase portraits. Fig. 3 and Fig. 4 show the results of phase portrait studies.

3. Proposed Color Image Encryption/Decryption approach

Fig. 5 shows a diagram of the image encryption approach employing a 5-D hyper-chaotic system and DNA computing, while Fig. 6 briefly outlines the general steps of this approach.

The use of DNA computing and chaotic systems for image encryption results in limitations, including the creation of cryptographic keys from simple images by transforming the information contained in the image into a complex and unique sequence of bits. Additionally, the security vulnerabilities associated with low-dimensional

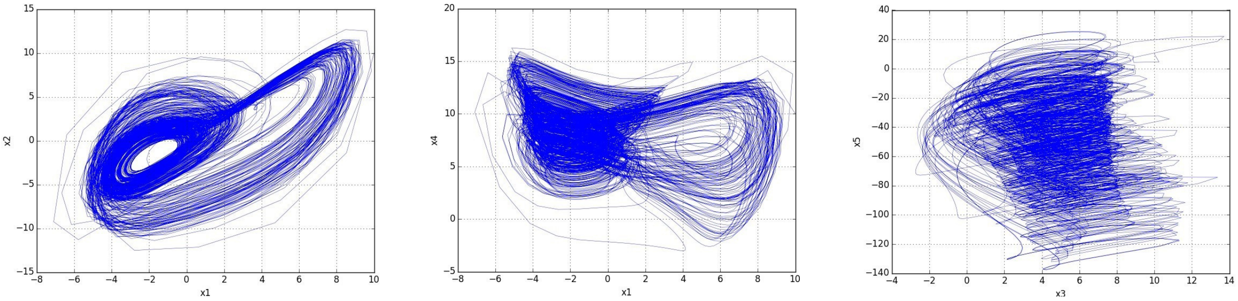


Figure 3. System Phase portraits in 2-D planes.

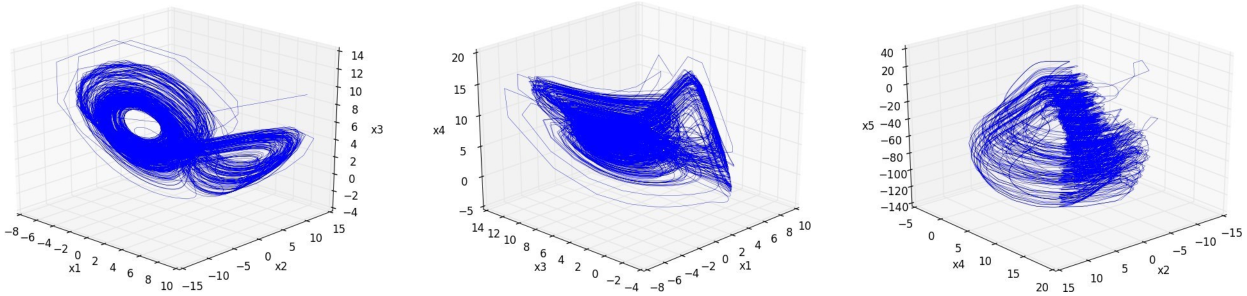


Figure 4. System Phase portraits in 3-D view spaces.

chaos, such as increased predictability, sensitivity to initial conditions, possible low entropy, and susceptibility to brute force attacks. Finally, the relatively slow encryption velocity [26, 29]. This motivates our proposal for an innovative hybrid security system for color image encryption, which provides an integrated solution that overcomes the specific challenges of cryptographic key generation by using the hash functions of the simple image. In addition, the specific challenges related to the security of low-dimensional chaotic systems, using a high-dimensional system in the broadcast process to obtain a more efficient diffusion of the bits of the original image throughout the encrypted message. This contributes to a more robust dispersion of information, thereby strengthening the security of the encryption.

The decryption operation is essentially the mirror image of the encryption operation; it restores the cipher image to its original state. To achieve this transformation, the decryption process must use the same encryption key. A key element to emphasize is that the final decrypted image must be a replica of the original image.

4. Experimental findings and performance analysis

The proposed algorithm's ability to withstand various types of attacks and its high level of security and robustness must be demonstrated to validate the promised effectiveness. In this section, the evaluation of the proposed algorithm is conducted using a Lena color image of size 512×512 through Matlab2021 on an Intel® Core™i5 computer. Hence, this section is divided into seven analyses: 1) histogram, 2) entropy, 3) correlation, 4) differential attack, 5) cropping attack, 6) Execution time, and 7) Key security [17, 18].

The experimental findings in Fig. 7 indicate that the suggested image encryption method renders the encrypted image notably noisy, effectively preventing any meaningful information about the base image from being discerned. This noise serves as a robust defense, making visual analysis and reverse engineering challenging for unauthorized entities and ensuring the confidentiality of sensitive information.

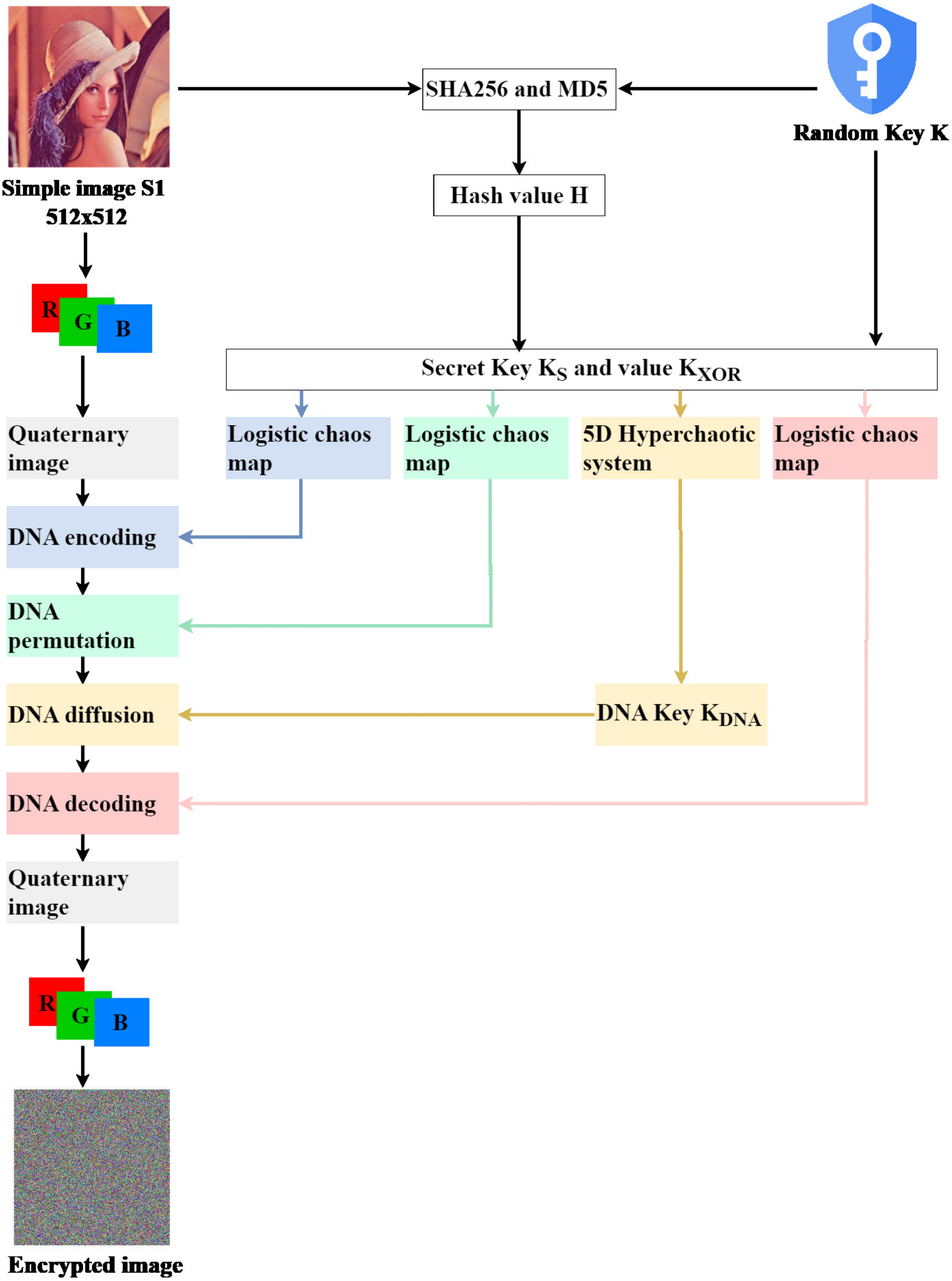
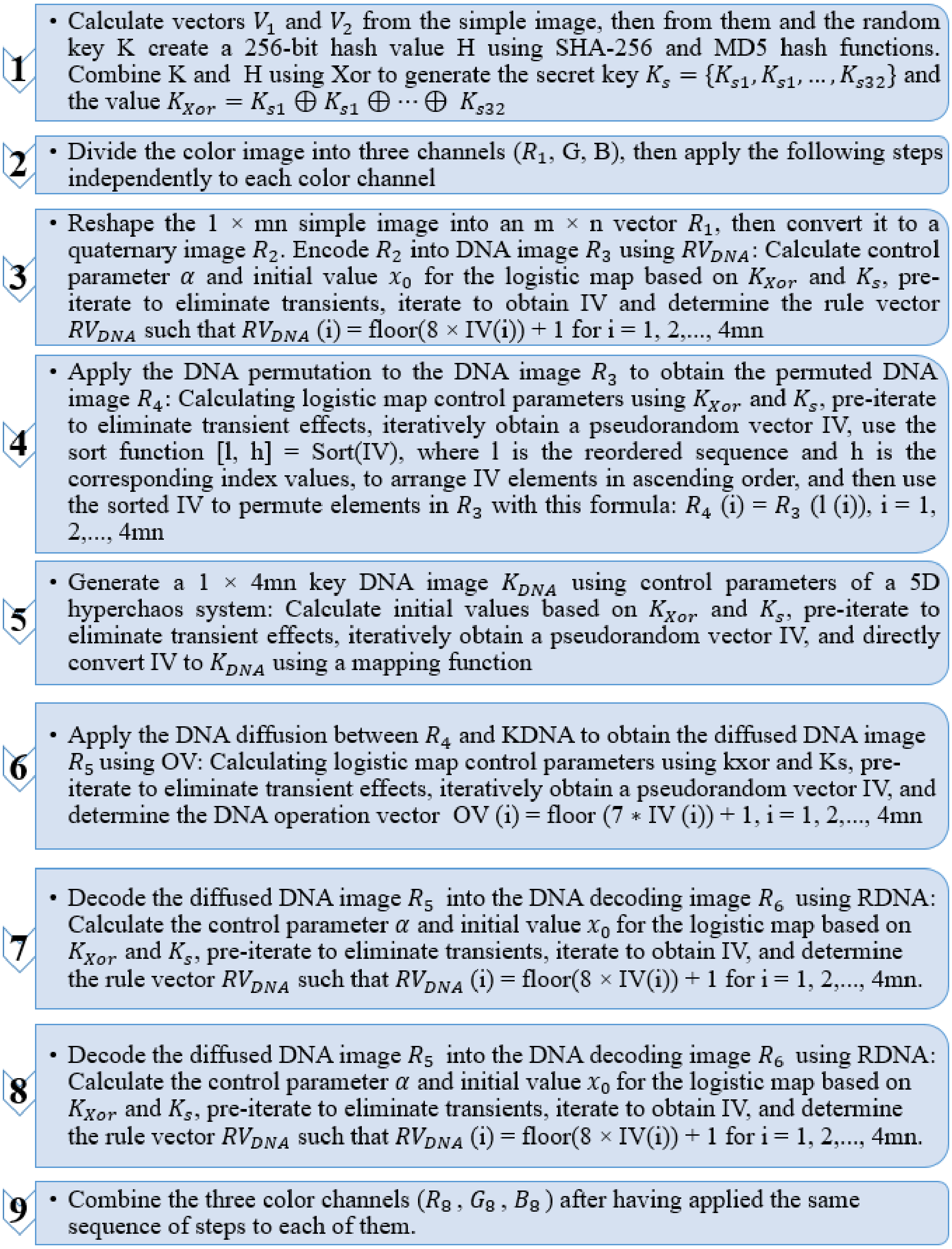


Figure 5. Diagram of the encryption method.



1 - Calculate vectors V_1 and V_2 from the simple image, then from them and the random key K create a 256-bit hash value H using SHA-256 and MD5 hash functions. Combine K and H using Xor to generate the secret key $K_s = \{K_{s1}, K_{s1}, \ldots, K_{s32}\}$ and the value $K_{Xor} = K_{s1} \oplus K_{s1} \oplus \cdots \oplus K_{s32}$

2 - Divide the color image into three channels (R_1, G, B), then apply the following steps independently to each color channel

3 - Reshape the 1 × mn simple image into an m × n vector R_1, then convert it to a quaternary image R_2. Encode R_2 into DNA image R_3 using RV_{DNA}: Calculate control parameter α and initial value x_0 for the logistic map based on K_{Xor} and K_s, pre-iterate to eliminate transients, iterate to obtain IV and determine the rule vector RV_{DNA} such that RV_{DNA} (i) = floor(8 × IV(i)) + 1 for i = 1, 2,..., 4mn

4 - Apply the DNA permutation to the DNA image R_3 to obtain the permuted DNA image R_4: Calculating logistic map control parameters using K_{Xor} and K_s, pre-iterate to eliminate transient effects, iteratively obtain a pseudorandom vector IV, use the sort function [l, h] = Sort(IV), where l is the reordered sequence and h is the corresponding index values, to arrange IV elements in ascending order, and then use the sorted IV to permute elements in R_3 with this formula: R_4 (i) = R_3 (l (i)), i = 1, 2,..., 4mn

5 - Generate a 1 × 4mn key DNA image K_{DNA} using control parameters of a 5D hyperchaos system: Calculate initial values based on K_{Xor} and K_s, pre-iterate to eliminate transient effects, iteratively obtain a pseudorandom vector IV, and directly convert IV to K_{DNA} using a mapping function

6 - Apply the DNA diffusion between R_4 and KDNA to obtain the diffused DNA image R_5 using OV: Calculating logistic map control parameters using kxor and Ks, pre-iterate to eliminate transient effects, iteratively obtain a pseudorandom vector IV, and determine the DNA operation vector OV (i) = floor (7 ∗ IV (i)) + 1, i = 1, 2,..., 4mn

7 - Decode the diffused DNA image R_5 into the DNA decoding image R_6 using RDNA: Calculate the control parameter α and initial value x_0 for the logistic map based on K_{Xor} and K_s, pre-iterate to eliminate transients, iterate to obtain IV, and determine the rule vector RV_{DNA} such that RV_{DNA} (i) = floor(8 × IV(i)) + 1 for i = 1, 2,..., 4mn.

8 - Decode the diffused DNA image R_5 into the DNA decoding image R_6 using RDNA: Calculate the control parameter α and initial value x_0 for the logistic map based on K_{Xor} and K_s, pre-iterate to eliminate transients, iterate to obtain IV, and determine the rule vector RV_{DNA} such that RV_{DNA} (i) = floor(8 × IV(i)) + 1 for i = 1, 2,..., 4mn.

9 - Combine the three color channels (R_8 , G_8 , B_8) after having applied the same sequence of steps to each of them.

Figure 6. Image encryption steps.

4.1. Statical attack analysis

Histogram analysis. The histogram for an image depicts how pixel values are spread throughout it. For a simple image, the histogram should exhibit a non-uniform pattern, showing variations in pixel intensity levels [9, 19, 20].

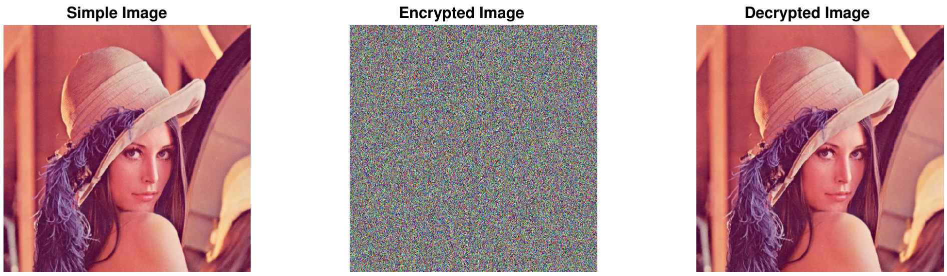


Figure 7. Experimental findings of our method.

In contrast, we ideally expect the histogram of the encrypted image to display a uniform, flat distribution, as depicted in Fig. 8.

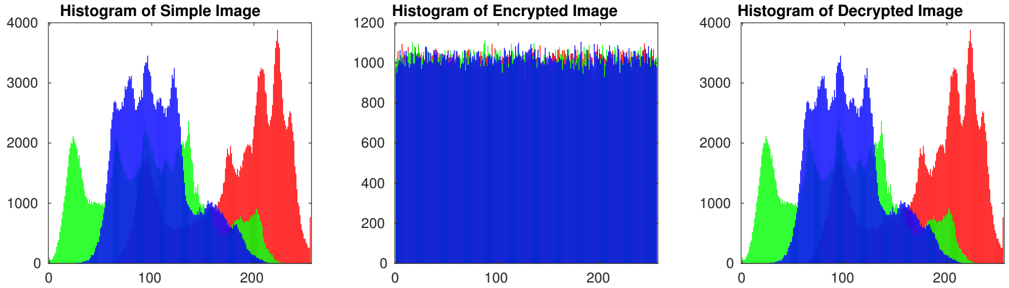


Figure 8. Histogram analysis of Lena's image.

The uniform histogram of the cipher image poses a significant challenge to statistical attacks, as it eliminates discernible patterns and prevents adversaries from extracting meaningful information through statistical analysis. This characteristic enhances the robustness of the encryption method by thwarting attempts to exploit pixel intensity distributions for unauthorized decryption.

Information entropy analysis. The entropy is established for the express purpose of assessing the degree of unpredictability or astonishment linked to an information source, and it can be determined as follows (2):

$$H(s) = -\sum_{i=0}^{2^n-1} p(s_i) \times \log_2 p(s_i) \tag{2}$$

Table 2 compares the three-channel entropy data for the simple image and its encryption against ref [7, 21].

Table 2. Entropy results

Method	Image	Entropy		
		R	G	B
Proposed	Lena	7.9993	7.9993	7.9991
[7]	Lena	7.9978	7.9982	7.9988
[21]	Lena	7.9972	7.9973	7.9972

The observation that all entropy values for the encrypted image consistently hover around eight underscores the method's remarkable ability to maintain a uniform and random distribution of information. This uniformity is crucial in cryptographic strength, indicating that the suggested method generates highly entropic cipher images. The entropy values approaching eight signify a near-maximum level of disorder and unpredictability, making it exceedingly challenging for adversaries to discern any patterns or exploit regularities within the encrypted data. This inherent randomness and uniformity serve as a robust defense against attacks that leverage entropy analysis, as the method effectively masks the underlying structure of the encrypted content. Consequently, the suggested encryption method not only prioritizes security through the preservation of high entropy but also showcases a noteworthy resilience against attempts to compromise the system through entropy-based attacks.

Correlations of the neighboring pixel analysis. A good encryption method minimizes the correlations of the neighboring pixels in the diagonally, horizontally, and vertically directions of the cipher image. The ideal correlation value is zero and is calculated by Eq. (3) [22, 23]:

$$r_{x,y} = \frac{Cov(X,Y)}{\sqrt{D(X) \times D(Y)}} \tag{3}$$

As depicted in Fig. 9, Fig. 10, and Table 3, the simple image exhibits a high correlation between two adjacent pixels in the R, G, and B canals, while the cipher image notably decreases this correlation.

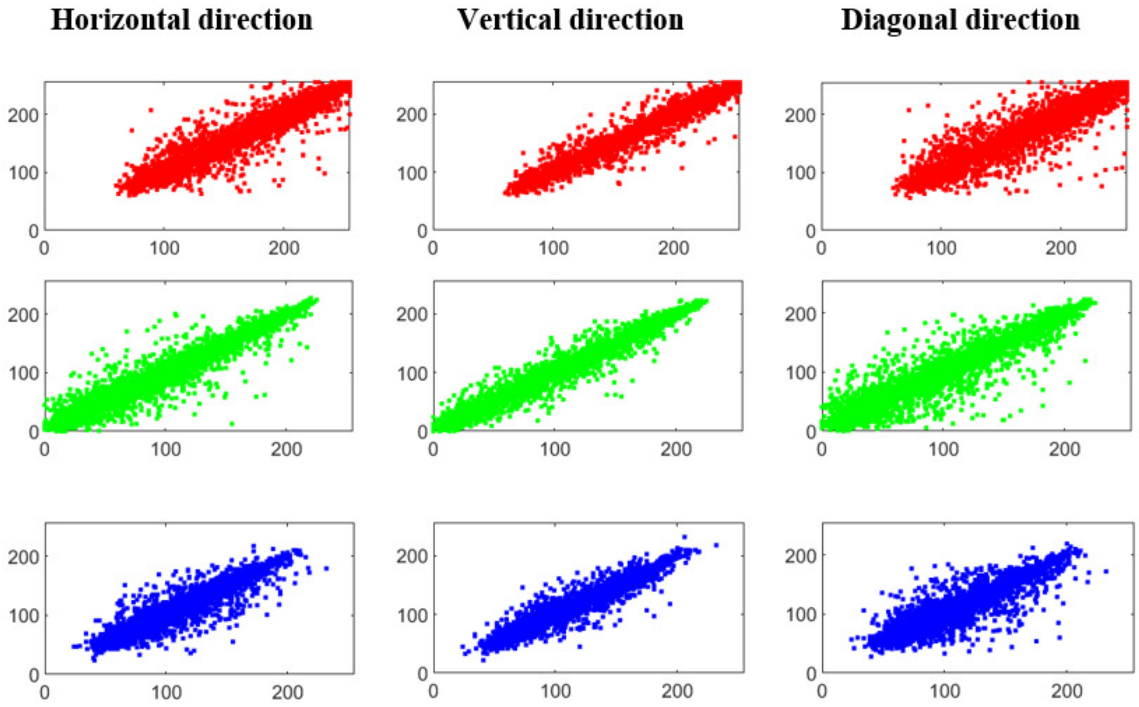


Figure 9. Correlation results of the R, G, and B canals of the simple Lena image.

The correlation coefficient comparison findings with ref. [6] and [7] in Table 3 demonstrate that the suggested encryption approach outperforms the other two approaches. A higher correlation coefficient implies a stronger resistance to linear relationships or patterns in the encrypted data, and in this context, it signifies the enhanced ability of the suggested encryption method to break away from predictability. This robust performance is particularly noteworthy in cryptographic applications where mitigating correlations is pivotal for thwarting attacks. The findings affirm that the suggested encryption approach stands as a more resilient solution, demonstrating its efficacy in achieving heightened security and a superior capability to resist correlation-based attacks compared to the alternatives outlined in the referenced literature.

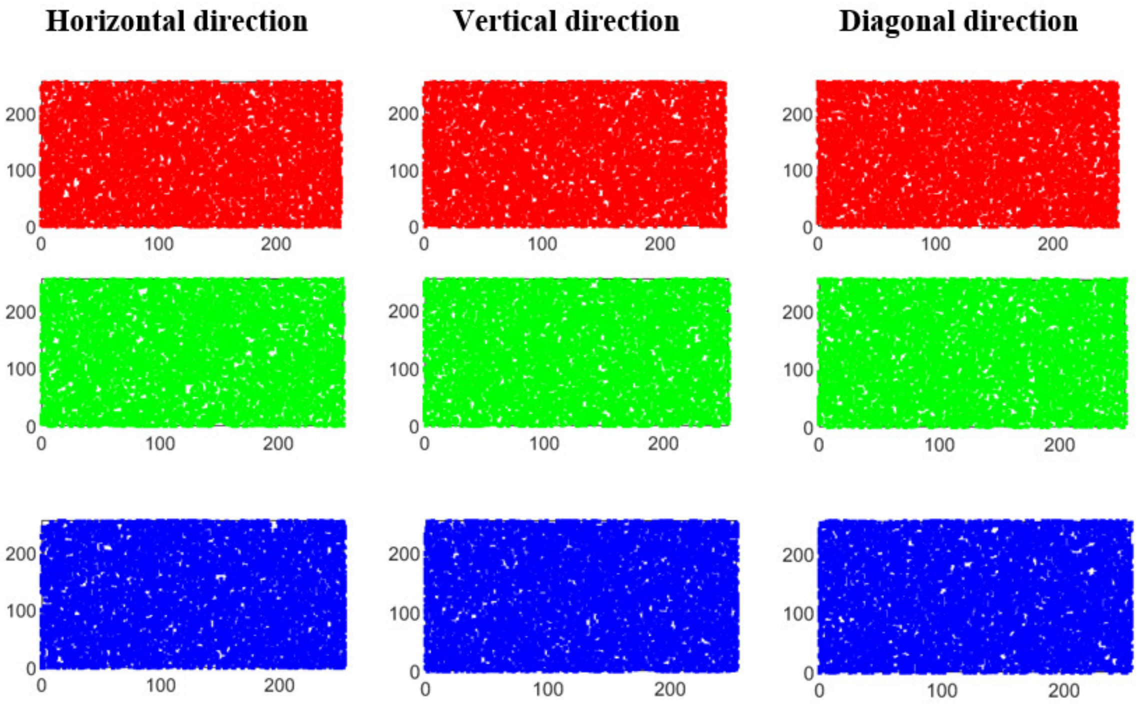


Figure 10. Correlation results of R, G, and B canals of encrypted image Lena.

Table 3. Correlation coefficient analysis.

Method	Image	Direction	Simple image			Encrypted image		
			R	G	B	R	G	B
Proposed	Lena	Horizontal	0.9696	0.9769	0.9414	0.0015	0.0008	0.0018
		Vertical	0.9844	0.9869	0.9642	-0.0033	0.0024	0.0004
		Diagonal	0.9576	0.9675	0.9068	0.0023	0.0040	0.0002
[6]	Lena	Horizontal	0.9813	0.9691	0.9455	0.0092	0.0002	0.0076
		Vertical	0.9803	0.9594	0.9294	0.0203	-0.0025	0.0006
		Diagonal	0.9668	0.9433	0.9099	0.0073	-0.0131	0.0111
[7]	Lena	Horizontal	0.9817	0.9747	0.9598	0.0018	0.0034	0.0028
		Vertical	0.9747	0.9500	0.9333	0.0055	0.0056	0.0011
		Diagonal	0.9598	0.9284	0.9072	0.0036	0.0059	0.0001

4.2. *Differential attack analysis*

An encryption method is resilient against differential attacks when even a minor alteration in a pixel of the simple image leads to an important change in the encrypted image. To assess the effectiveness of this resistance, we use the NPCR and the UACI defined by (4 and 5) [8, 24].

$$NPCR(C_1, C_2) = \frac{1}{K \times L} \sum_{i=1}^{K} \sum_{j=1}^{L} D(i,j) \times 100 \tag{4}$$

$$UACI(C_1, C_2) = \frac{1}{K \times L} \sum_{i=1}^{K} \sum_{j=1}^{L} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \tag{5}$$

The NPCR value and the UACI value must be equal to 99.6094% and 33.4635%, respectively. Table 4 presents the outcomes of a differential attack analysis, where a single pixel within the simple image undergoes random alteration, and these results are compared to the references [4, 25].

Table 4. NPCR and UACI results for a single pixel alteration in the simple image.

Method	Image	Direction	Simple image			Encrypted image		
			R	G	B	R	G	B
Proposed	Lena	Horizontal	0.9696	0.9769	0.9414	0.0015	0.0008	0.0018
[4]	Lena	Vertical	0.9844	0.9869	0.9642	-0.0033	0.0024	0.0004
[25]	Lena	Diagonal	0.9576	0.9675	0.9068	0.0023	0.0040	0.0002

The NPCR and UACI achieved by the suggested encryption method show great results, surpassing the efficacy of the other two encryption approaches. A high NPCR indicates a substantial change in pixel values between the original and encrypted images, enhancing the resistance against cryptographic attacks. Meanwhile, a superior UACI score signifies a balanced and uniform distribution of pixel intensity changes, contributing to the overall quality of the encrypted output. The superiority of the suggested encryption method in these metrics affirms its ability to introduce significant alterations while maintaining a uniform and balanced distribution of pixel changes, thereby ensuring robust security and surpassing the efficacy of alternative encryption approaches.

4.3. *Robustness analysis*

To analyze the robustness of the suggested image encryption method, we use the cutting attack. The MSE and PSNR between the simple image and the decrypted image are essential for assessing the decrypted image, and they are calculated as (6) and (7) [8, 19, 24].

$$MSE = \frac{1}{K \times L} \sum_{i=1}^{K} \sum_{j=1}^{L} (P(i,j) - D(i,j))^2 \tag{6}$$

$$PSNR = 10 \times \log_{10} \left(\frac{MAX^2}{MSE} \right) \tag{7}$$

Cutting operations on encrypted images are executed at various positions, with rates of 1/4 and 1/2. Subsequently, decryption is carried out, and the outcomes are shown in Fig. 11. Remarkably, even when the cut ratio reaches 1/2, the primary contents of the images remain recognizable. Table 5 indicates the PSNR values.

Table 5. PSNR results.

Image	Crop	PSNR		
		R	G	B
Lena	1/2	11.7183	12.3950	13.3491
Lena	1/4	13.6948	14.3880	15.3461

The empirical findings demonstrate that even if half of the pixels in the cipher image are lost, successful reconstruction of the image is achievable. This highlights the resilience of the suggested image encryption method against cutting attacks.

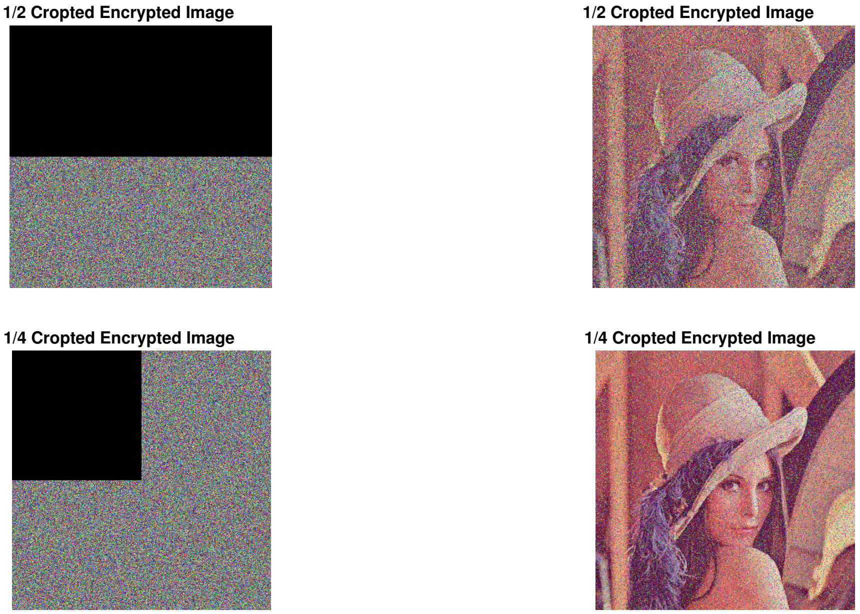

1/2 Cropted Encrypted Image
1/2 Cropted Encrypted Image
1/4 Cropted Encrypted Image
1/4 Cropted Encrypted Image

Figure 11. Cutting attack results.

4.4. *Execution time analysis*

We can also test the time complexity of the encryption process as another important measure of algorithmic performance. The color image ”Lena” of different sizes 128 x 128, 256 x 256, and 512 x 512 is implemented 10 times using Matlab2021. Table 6 illustrates the total average processing time of the encryption and decryption methods.

Table 6. Execution time results.

Image	Operation	Proposed	[4]
Lena 512x512	Encryption	2.6199	9.0016
	Decryption	3.8244	9.1095
Lena 256x256	Encryption	0.7312	2.2234
	Decryption	0.9485	2.3218
Lena 128x128	Encryption	0.1957	0.6296
	Decryption	0.2548	0.6594

The findings illustrate that as the image size rises, the processing time for each encryption method also rises. In comparison with other ref. [4], we can see that the suggested encryption method is faster.

4.5. *Key security analysis*

To prove the effectiveness of the suggested image encryption method, we performed a key security analysis, which included key space and key sensitivity analysis.

Keyspace. In the suggested image encryption method, we used a secret key with a space size of 2^{100}, which significantly surpasses the space size of $2^{100}(\approx 10^{30})$. Consequently, the suggested encryption method boasts a substantial key space, enhancing its security level and making it more resilient against exhaustive attacks.

Key sensitivity. We randomly alter one bit of the secret key K_1 [7] to acquire a new modified key, K_2. Then, using secret keys K_1 and K_2, we encrypt the simple image, generating two encrypted versions. These encrypted images are then decrypted using secret keys K_1 and K_2, respectively (see Fig. 12).

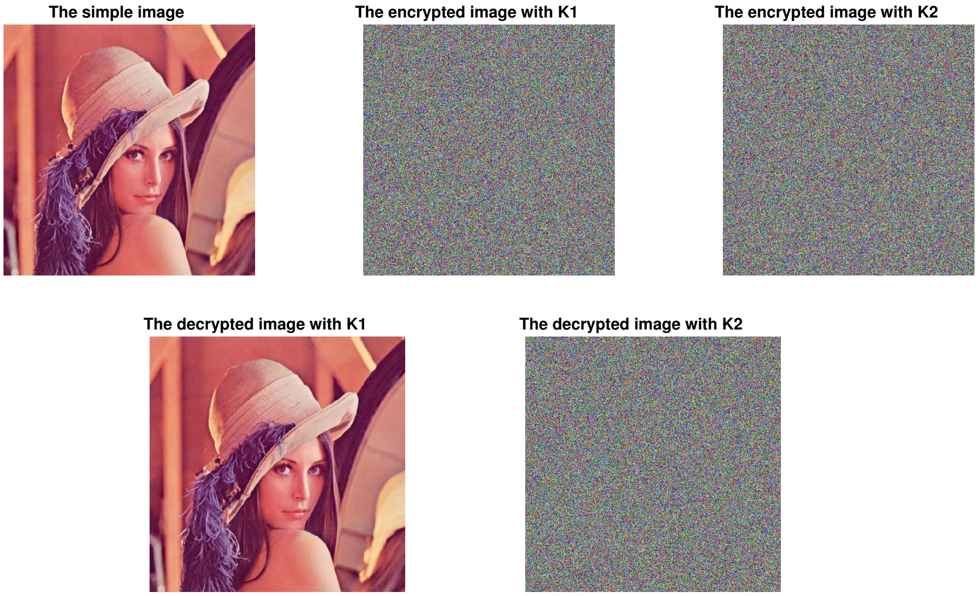

The simple image
The encrypted image with K1
The encrypted image with K2
The decrypted image with K1
The decrypted image with K2

Figure 12. Key sensitivity results.

The findings illustrate that a slight alteration in the key causes a different encryption outcome. Hence, the suggested encryption method exhibits a high level of sensitivity to the secret key.

5. Discussion

The proposed encryption scheme makes significant contributions through a combination of DNA model, Chaotic systems, and SHA256-MD5 hush functions. In the context of DNA computing, DNA coding stands out for its remarkable ability to store a massive amount of information in a small amount of material. This approach uses DNA sequences to represent data, considering each nucleotide as a bit of information, thereby achieving extremely high storage density. In addition, DNA computing is characterized by its ability to resolve the strong correlation between neighboring pixels. Sequences generated by DNA computing are inherently unpredictable due to the complexity of molecular interactions. This unpredictability helps enhance the robustness of the encryption process, making DNA-derived keys particularly effective against decryption attempts based on pre-existing patterns. For the chaotic systems, the 1-D system is employed for the encoding and decoding rules applied to every pixel of the basic image, ensuring faster encryption times without compromising overall security. The 5-D hyper-chaotic system is used specifically to generate the DNA image key, leveraging its attributes of strong confidentiality and a large key space. This strategic use contributes to reducing simulation time and bolstering the security of our method. The 1D logistic map, known for its lower computational complexity compared to higher-dimensional chaotic systems like the 5D hyper-chaotic map, is chosen to optimize efficiency in real-world applications, particularly those requiring real-time processing. While a 5D hyper-chaotic system could offer additional complexity, it comes at the expense of increased computational overhead. Minimizing computational complexity is crucial in practical deployments. The selection of a 1D chaotic sequence strikes a balance between maintaining robust security and ensuring operational efficiency, whereas the use of a 5D chaotic sequence, specifically for DNA image key generation, enhances the encryption scheme's resistance to cryptographic attacks. Finally, the hush function makes another big difference in our method through the creation of cryptographic keys from simple images by transforming the information contained in the image into a complex and unique sequence of bits.

Our proposed method extends the evaluation analysis of several existing techniques, encompassing statistical attacks analysis, differential attacks analysis, and sensitivity analysis. In [40], the integration of a DNA algorithm with a spatiotemporal chaotic system encrypts color images through the concealment of distribution information using three levels of DNA matrices. Meanwhile, in [41], a Chaos-based color image encryption technique employs a 3D histogram equalization method for optimal confusion and diffusion of image data. Hoi et al. [42] propose a medical image encryption algorithm involving two phases: pixel value alteration using the Combined Cellular Automata algorithm followed by iterative movement in a 3D generalized chaotic cat map, ensuring enhanced security by randomizing pixel values and protecting against deliberate damage or accidental transmission. Our method builds upon these advancements, providing an extended and comprehensive evaluation framework to ensure robust image security across various attack scenarios, the comparative overview is illustrated in Table 7.

Table 7. Comparative overview.

Methods	**Histogram**	**Correlation**			**NPCR**	**UACI**	**Entropy**	**Key space**
		Horizontal	**Vertical**	**Diagonal**				
Proposed	Highly uniform	R 0.0015 G 0.0008 B 0.0018	R -0.0033 G 0.0024 B 0.0004	R 0.0023 G -0.0040 B 0.0002	99.61	33.46	7.9993	2^{512}
DNA Encoding and spatiotemporal chaotic system [40]	Uniform	R 0.0092 G 0.0002 B 0.0076	R 0.0203 G -0.0025 B 0.0006	R -0.0073 G -0.0131 B 0.0111	99.65	33.457	7.9983	2^{213}
3D Piecewise-Henon map [41]	Uniform	0.0012	-0.0027	-0.0033	99.609	33.463	7.9979	2^{216}
3D Generalized chaotic cat map and combined cellular automata [42]	Good	0.0019	0.0048	-0.0048	99.62	33.608	7.9983	2^{416}

The fusion of DNA computing and chaotic systems in the proposed image encryption scheme not only offers a robust response to real-world challenges but also showcases practicality across various applications. The parallel processing capabilities of DNA computing enhance computational efficiency, catering to the intricate demands of image security processing, particularly in sectors like telemedicine and sensitive government communications. Employing DNA sequences for cryptographic keys ensures resilient key management, adding intricacy to key generation, distribution, and rotation. This adaptable design, influenced by chaotic systems, seamlessly integrates with diverse systems, accommodating different image formats and processing workflows. The scheme's success in remote consultations underscores its tangible utility in maintaining the confidentiality of sensitive medical data during transmission. The dynamic nature of chaotic systems aids continuous monitoring and anomaly detection, ensuring adaptability to evolving challenges, a crucial trait in information and communication technologies. In essence, the integration of DNA computing and chaotic systems positions the proposed encryption scheme as a sophisticated, secure, and responsive solution applicable to a range of real-world scenarios.

6. Conclusion

In this research paper, we provide a novel hybrid security system for the encryption of color images using a DNA model, chaotic systems, and hash functions as a basis. We combined the SHA256-MD5 irreversible hash of the simple image and the random key to eliminate the independence of the key generation process from the simple image and to generate the unique key, which makes our method resistant to various simple image and encrypted image attacks. The security and performance analysis show that the proposed method has a better encryption effect, a larger secret key space, and a higher sensitivity to the secret key, as well as good resistance to differential, statistical, and cropping attacks. The empirical findings reveal that our method not only outperforms other prominent image encryption methods in terms of security but also exhibits a high level of speed for various applications. Although the execution time analysis showed that the proposed method is competitive in terms of speed, future research could focus on specific optimization techniques aimed at further reducing encryption and decryption, especially in contexts where processing speed is crucial, such as in applications requiring rapid and secure exchange of images. Furthermore, the initial design for image encryption opens the way for potential extensions to other domains such as video, audio, and even general data transmission. Future research could thus explore the transfer-ability and adaptability of this approach to various application contexts, promising further development and diversification of the benefits of this innovative method. Our next steps involve implementing this method in embedded systems, emphasizing platforms like Raspberry Pi and FPGA. This aligns with the demand for efficient processing in resource-constrained environments, paving the way for broader applications and advancements.

Acknowledgement

The authors would like to thank the anonymous referees for their valuable comments and suggestions.

REFERENCES

1. H. Chang, E. Wang, J. Liu, *Research on Image Encryption Based on Fractional Seed Chaos Generator and Fractal Theory*, Fractal Fract, vol. 7, no. 3, 2023.
2. D. Mata-Mendoza, M. Cedillo-Hernandez, F. Garcia-Ugalde, A. Cedillo-Hernandez, M. Nakano-Miyatake, H. Perez-Meana, *Secured telemedicine of medical imaging based on dual robust watermarking*, The Visual Computer, vol. 38, no. 108, 2022.
3. W. Huang, N. R. Zhou, *Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion*, Optics and Laser Technology, vol. 149, no. July 2021, p. 107879, 2022.
4. Y. Q. Zhang, Y. He, P. Li, X. Y. Wang, *A new color image encryption scheme based on 2DNLCML system and genetic operations*, Optics and Lasers in Engineering, vol. 128, no. September 2019, p. 106040 (2020).
5. M. Kaur, S. Singh, M. Kaur, *Computational Image Encryption Techniques: A Comprehensive Review*, Mathematical Problems in Engineering, vol. 2021, no. 6, 2021
6. D. Liu, Q. Su, Z. Yuan, X. Zhang, *A color watermarking scheme in frequency domain based on quaternary coding*, Vis. Comput, vol. 37, no. 8, pp. 2355–2368, 2021.
7. S. Mansoor, S. A. Parah, *A hybrid adaptive image encryption algorithm using Chaos and DNA computing*, Multimedia Tools and Applications, vol. 82, no. 19, pp. 28769–28796, 2023.
8. Q. Liu, L. Liu, *Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System*, IEEE Access, vol. 8, pp. 83596–83610, 2020.
9. K. M. Hosny, S. T. Kamal, M. M. Darwish, *Novel encryption for color images using fractional-order hyperchaotic system*, J. Ambient Intell. Hum. Comput, vol. 13, no. 2, pp. 973–988, 2022.
10. N. Iqbal, M. M. Hanif, Z. U. Rehman, M. Zohair, *On the novel image encryption based on chaotic system and DNA computing*, Multimedia Tools and Applications, vol. 81, no. 1, 2022.
11. A. P. Kari, A. H. Navin, A. M. Bidgoli, M. Mirnia, *A new image encryption scheme based on hybrid chaotic maps*, Multimedia Tools and Applications, vol. 80, no. 2, pp. 2753–2772, 2021.
12. H. Li, L. Zhang, H. Cao, Y. Wu, *Hash Based DNA Computing Algorithm for Image Encryption*, Applied Sciences, vol. 13, no. 14, 2023.
13. Y. Zhang, A. Chen, W. Chen, *The unified image cryptography algorithm based on finite group*, Expert Systems with Applications, vol. 212, no. July 2021, p. 118655, 2023.
14. A. Ibrahim, S. Mohammed, H. A. Ali, S. E. Hussein, *Breast Cancer Segmentation from Thermal Images Based on Chaotic Salp Swarm Algorithm*, IEEE Access, vol. 8, pp. 122121–122134, 2020.

15. T. S. Ali, R. Ali, *A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map*, IEEE Access, vol. 8, pp. 71974–71992, 2020.
16. H. Wen, et al, *Secure Optical Image Communication Using Double Random Transformation and Memristive Chaos*, IEEE Photonics Journal, vol. PP, no. 99, 1–11, 2023.
17. M. A. Tahiri, H. Karmouni, M. Sayyouri, H. Qjidaa, *2D and 3D image localization, compression and reconstruction using new hybrid moments*, Multidimensional Systems and Signal Processing , vol. 33, no. 4, 769–806, 2022.
18. M. A. Tahiri, A. Bencherqui, H. Karmouni, M. O. Jamil, M. Sayyouri, H. Qjidaa, *Optimal 3D object reconstruction and classification by separable moments via the Firefly algorithm*, 2022 International Conference on Intelligent Systems and Computer Vision, pp. 1–8, 2022.
19. J. R. De Oliveira Neto, J. B. Lima, D. Panario, *The Design of a Novel Multiple-Parameter Fractional Number-Theoretic Transform and Its Application to Image Encryption*, IEEE Transactions on Circuits and Systems for Video Technolog, vol. 30, no. 8, pp. 2489–2502, 2020.
20. Q. Li, et al, *A novel grayscale image steganography scheme based on chaos encryption and generative adversarial networks*, IEEE Access, vol. 8, pp. 168166–168176, 2020.
21. N. R. Zhou, L. J. Tong, W. P. Zou, *Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation*, Signal Processing, vol. 211, no. 2, 2023.
22. H. Karmouni, M. A. Tahiri, I. Dagal, H. Amakdouf, M. O. Jamil, H. Qjidaa, M. Sayyouri, *Secure and Optimized Satellite Image Sharing based on Chaotic $e\pi$ Map and Racah Moments*, Expert Systems with Applications, vol. 236, no. 14, 2023.
23. M. A. Tahiri, H. Karmouni, A. Bencherqui, A. Daoui, M. Sayyouri, H. Qjidaa, K. Hosny, *New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations*, The Visual Computer, vol. 39, no. 8, 2022.
24. M. Kaur, V. Kumar, *A Comprehensive Review on Image Encryption Techniques*, Archives of Computational Methods in Engineering, vol. 27, pp. 15–43, 2020.
25. T. Hai-jiang, L. Peng,W. Yong, *Image encryption algorithm based on chaos and dynamic DNA coding*, Journal of Jilin University (Engineering Edition), vol. 44, no. 3, pp. 801–806, 2014.
26. Y. Wu, L. Zhang, S. Berretti, S. Wan, *Medical Image Encryption by Content-Aware DNA Computing for Secure Healthcare*, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, vol. 19, no. 2, 2023.
27. G. Cui, Y. Liu, X. Zhang, Z. Zhou, *A new image encryption algorithm based on DNA dynamic encoding and hyper-chaotic system*, In: International Conference on Bio-Inspired Computing: Theories and Applications. Springer, New York, pp. 286–303, 2017.
28. E. Z. Zefreh, *An image encryption scheme based on a hybrid model of DNA computing, chaotic systems, and hash functions*, Multimedia Tools and Applications, vol. 79, no. 5187, pp. 24993–25022, 2020.
29. X. Chai, Z. Gan, K. Yuan, Y. Chen, X. Liu, *A novel image encryption scheme based on DNA sequence operations and chaotic systems*, Neural Comput Applic, vol. 31, no. 1, pp. 219–237, 2019.
30. R. Enayatifar, A. Abdullah, I. F. Isnin, *Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence*, Opt Lasers Eng, vol. 56, no. 5, pp. 83–93, 2014.
31. X. Wu, H. Kan, J. Kurths, *A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps*, Applied Soft Computing, vol. 37, pp. 4–39, 2015. .
32. M. Alawida, J. S. Teh, W. H. Alshoura, *A New Image Encryption Algorithm Based on DNA State Machine for UAV Data Encryption*, Drones, vol. 7, no. 1, 2023.
33. M. Roy, S. Chakraborty, K. Mali, D. Roy, S. Chatterjee, *A robust image encryption framework based on DNA computing and chaotic environment*, Microsystem Technologies, vol. 27, no. 10, pp. 1–11, 2021.
34. S. Das, M. K. Sanyal, J. Mandal, *Secure Colour Image Encryption Based on Dynamic DNA Coding and Different Chaotic Maps*, Journal of Scientific Research, vol. 65, no. 5, pp. 1–10, 2021.
35. P. K. Naskar, S. Bhattacharyya, K. C. Mahatab, K. G. Dhal, A. Chaudhuri, *An efficient block-level image encryption scheme based on multichaotic maps with DNA encoding*, Nonlinear Dynamics, vol. 105, pp. 3673–3698, 2021.
36. A. Laghrib, L. Afraites, M. Nachaoui, A. Ghazdali, *Special Issue: Recent Developments of Optimization and Computational Mathematics*, Statistics, Optimization and Information Computing, vol. 11, no. 1, pp. 1–1, 2023.
37. H. Moussaoui, N. El Akkad, M. Benslimane, *A Hybrid Skin Lesions Segmentation Approach Based on Image Processing Methods*, Statistics, Optimization and Information Computing, vol. 11, no. 1, pp. 95–105, 2023.
38. I. Harrade, A. Daoui, Z. Chalh, M. Sayyouri, *Visual Servoing of a 3R Robot by Metaheuristic Algorithms*, Statistics, Optimization and Information Computing, vol. 11, no. 1, pp. 11624–1, 2023.
39. C. Bonini, A. Rey, D. Otero, A. Amadio, M. G. Blesa, W. Legnani, *An Alternative Computation of the Entropy of 1D Signals Based on Geometric Properties*, Statistics, Optimization and Information Computing, vol. 10, no. 4, pp. 998–1020, 2022.
40. K. Xuejing, G. Zihui, *A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system*, Signal Processing: Image Communication, Vol. 80, 2020.
41. C. Liu, Q. Ding, *A Color Image Encryption Scheme Based on a Novel 3D Chaotic Mapping*, Complexity, Vol. 2020, 2020.
42. U. S. Choi, S. J. Cho, S. W. Kang, *New Color Image Encryption for Medical Images Based on Three Dimensional Generalized Chaotic Cat Map and Combined Cellular Automata*, Advances in Science, Technology and Engineering Systems Journal, Vol. 5, no. 2, pp. 104–110, 2020.
43. N. Khalil, A. M. Sarhan, M. A. M. Alshewimy, *An efficient color/grayscale image encryption scheme based on hybrid chaotic maps*, Optics and Laser Technology, Vol. 143, 2021.
44. Y. Niu, Z. Zhou, X. Zhang, *An image encryption approach based on chaotic maps and genetic operations*, Multimed Tools Appl, Vol. 79, no. 35, pp. 25613–25633, 2020.