Optica Applicata, Vol. LV, No. 1, 2025
DOI: 10.37190/oa/200662

A robust color image encryption scheme for optical applications using a novel zigzag technique and 3D fractional-order chaotic system

Ismail Haddad[1,*], Djamel Herbadji[2], Aissa Belmeguenai[1]

[1]Electronics Research Laboratory, University 20 August 1955, Skikda 21000, Algeria

[2]Signals and Systems Laboratory, Institute of Electrical and Electronic Engineering, University M'Hamed BOUGARA of Boumerdes Boumerdes, Algeria

[*]Corresponding author: i.haddad@univ-skikda.dz

In this paper, we present a novel image encryption approach tailored for optical imaging encryption, leveraging fractional-order chaotic systems and an innovative zigzag technique. The proposed scheme employs various zigzag patterns to simultaneously scramble the positions of image pixels, ensuring robust security. The zigzag process is dynamically controlled by a fractional-order chaotic system, which introduces unpredictability and significantly enhances the scheme's resistance to attacks. The encryption key is derived from the initial values and fractional-order parameters of the chaotic system, offering a substantial improvement over traditional methods that rely on integer-order chaotic systems. This advancement not only expands the key space but also increases the complexity of the encryption process, making it highly secure.

The experimental results and security analysis demonstrate the scheme's effectiveness in thwarting various types of attacks, including brute-force and statistical attacks, particularly in the context of optical imaging systems. These findings highlight the technique's reliability and suitability for protecting sensitive data in optical imaging applications, where security and precision are paramount. The proposed method represents a significant step forward in securing optical imaging data, providing a robust and efficient solution for modern encryption needs.

Keywords: fractional-order chaotic systems, zigzag technique, key space, security analysis, statistical attacks, optical imaging encryption.

1. Introduction

With the increasing exchange of multimedia data across communication networks, it has become vital to investigate new methods to avoid the leak of their privacy and illicit manipulations, especially since hack applications proliferate in our modern era [1-2]. Traditional encryption techniques such as DES, RSA and AES no longer satisfy the criteria for encrypting media data such as images and audio. It takes a long time and

high consumption of computer resources due to the distinctive characteristics of these media compared to texts [3-5]. As a result, it became essential to explore other encryption techniques, which led to the appearance of many approaches based on various concepts, including DNA [6-8], quantum theory [9-10], and the chaos [11-19]. This technique offers increased speed and security, making it useful in the field of encryption applications.

Chaotic systems have demonstrated impressive outcomes in encryption applications such as secure communication and image encryption. Which is due to its distinct qualities such as sensitivity to initial values, pseudo randomness and unpredictability. It can also withstand dynamic deterioration [20]. These systems can be examined from two separate perspectives, which are integer-order systems and fractional-order systems. Chaotic systems with integer order have lower parameters and a basic structure, making them easily cracked. Otherwise, fractional chaotic systems have more complicated dynamic properties as well as more parameters that may be utilized as key in the encryption scheme, increasing the key space and the complexity, which make the encryption more secure.

Several image encryption techniques utilizing chaos have been proposed in the literature. LI *et al*. [21] create an image encryption approach using a hyper-chaos with fractional-order and computing DNA, where they integrated the chaos map with the complementary DNA base to get the ciphered image. KAUR *et al*. [22] developed a novel approach that employs chaos and a fractional Hartley transform that controlled by another chaotic map to give excellent encryption system security. LAI *et al*. [23] developed the "pixel-split" technique for image encryption. This approach employs a pixel exchange mechanism that may modify both the location and value of pixels at the same time. CHAI *et al*. [24] proposed an enhanced scheme that first applies sparse processing to the plain image, followed by zigzag scrambling. Then, the compressed sensing (CS) technique is employed to simultaneously compress and encrypt the scrambled image. In their approach to image encryption, YOUSIF *et al*. [25] utilized various chaotic maps with the aim of enhancing security while ensuring that processing performance remains at a high level. MUHAMMAD *et al*. [26] offered an enhanced technique that made use of the DES algorithm and eight S-box structures to augment their complexity. When combined with zigzag, this approach provides especially strong security for picture encryption. WANG *et al*. [27] employed the 3D zigzag transformation to permute the plain image and compared its effectiveness with other transformations, including Arnold, circular shift, and standard zigzag. The comparison showed that the 3D zigzag transformation produced a better permutation effect. However, certain image encryption schemes based on chaos have notable drawbacks, such as limited sensitivity to the plain image, which implies that they are vulnerable to some assaults, such as chosen-plaintext and know-plaintext attacks. DOU *et al*. [28] determine that the encryption scheme described in [29] is vulnerable to a chosen plaintext attack since it is unrelated to the plain image. According to [30], the encryption approach described in [31] has been cracked by a chosen-plaintext attack. Similarly, scheme [32] was vulnerable to a chosen plaintext attack [33] since the encryption key was unrelated to the plain image.

ABDELJAWAD *et al*. [34] presented tempered fractional difference equations employing time scale calculus in order to improve image encryption methods and investigated their use in examining chaotic behavior in discrete systems while taking into consideration the impact of short memory. In [35] the authors developed an ingenious method by introducing variable-order fractional chaotic systems with short memory. These approaches are critical in block image encryption, leading to major advances in security and a huge increase in encryption performance. MOHAMED *et al*. [36] improved encryption performance by using mathematical analysis, statistical testing, and FPGA implementation. The method involved extending a memristive chaotic system with transcendental nonlinearities into the fractional-order domain, incorporating it into an image encryption approach, and achieving improved encryption results. KAMAL *et al*. [37] investigated a fractional order Rössler blinking system with short memory, which verifies the presence of ghost attractors. It also presents an image encryption method that takes use of the chaotic time series created by the ghost attractor, proving its efficacy and resilience to various forms of attacks.

The purpose of this research is to solve the major issue with all forms of zigzag methods seen in existing cryptography systems. These methods exhibit a continuous nature, treating pixels as a sequential chain that uniformly moves in a fixed direction with constant pixel shifting values. While this is considered a drawback and is difficult to execute, it may be addressed by enhancing the existing zigzag approach to make it distinct and capable of going along different pixel locations. To achieve this goal, our research makes a significant contribution by employing a unique zigzag technique and leveraging a three-dimensional chaotic system with a fractional order to overcome the limitations of existing cryptography systems. Our strategy involves the simultaneous utilization of various zigzag variations. Resulting in extremely unexpected patterns controlled by a 3D fractional chaotic system. This system's integration seeks to greatly increase the algorithm's complexity, hence increasing overall security and boosting its resilience against different attacks. This research establishes a foundation for stronger and more secure encryption systems that effectively address the shortcomings of current methods, meeting the growing demands of data protection. Additionally, employing the SHA-512 hash value of the original image to determine initial values for the fractional order chaotic system plays a vital role in thwarting chosen plaintext attacks.

The increasing reliance on optical imaging systems in fields such as medical diagnostics, remote sensing, and secure communications has created a pressing need for advanced encryption techniques tailored to optical data. This paper introduces a novel color image encryption scheme combining a new zigzag technique and a 3D fractional -order chaotic system, specifically designed for optical applications. The proposed method enhances security through dynamic pixel scrambling and chaotic randomness, ensuring robust protection against unauthorized access. By addressing the unique challenges of optical image encryption, this work contributes to the development of secure and efficient solutions for modern optical systems.

This paper is structured as follows: in Section 2, we provide an analysis of the fractional-order chaotic system. Section 3 presents the proposed image encryption

algorithm in detail. The suggested scheme evaluation and simulation results are summarized in Section 4. Finally, Section 5 provides the conclusion.

2. Analyses of fractional order chaotic system

There are various definitions for the fractional derivative of order $q > 0$, but the Caputo's formulation is the most widely employed in modeling fractional order systems. The initial value problem (IVP) of a fractional order system is defined using the Caputo's derivative as follows [38]:

$$D_*^q x(t) = f(x(t)), \quad t \in [0, T] \tag{1}$$

where x_0 is the initial condition, f is a Lipschitz continuous nonlinear function and D_*^q is the Caputo's differential operator of order $0 < q < 1$. Then system (1) is described as having commensurate order; otherwise, it is described as having non-commensurate order. D_*^q is given by [38]:

$$D_*^q x(t) = \frac{1}{\Gamma(m-q)} \int_0^t \frac{x^{(m)}(\tau)}{(t-\tau)^{q+1-m}} \, \mathrm{d}\tau, \quad m-1 < q < m \tag{2}$$

where m is the smallest integer greater than q, $x^{(m)}$ is the normal m-order derivative, and Γ is Euler's Gamma function. To evaluate the fractional differential Eq. (1), numerical approximation methods such as Grünwald–Letnikov, Riemmann–Liouville and predictor-corrector Adams–Bashforth–Moulton (ABM) can be used.

In order to increase the complexity of the encryption system, we used the fractional order Chen system as a random number generator. It is characterized by more complex and rich dynamics compared to its integer-order counterpart. It is described by [38]:

$$\begin{cases} D_*^{q1} x(t) = a(y-x) \\ D_*^{q2} y(t) = (c-a)x - xz + cy \\ D_*^{q3} z(t) = xy - bz \end{cases} \tag{3}$$

where D_*^q denotes the Caputo's differential operator, x, y, and z denote the system dependent variables; and a, b, and c denote the system parameters.

2.1. Bifurcation diagram

The bifurcation diagram is a useful tool for evaluating visually the qualitative behavior of chaotic systems. It demonstrates how a qualitative control parameter affects the system's behavior. The bifurcation diagram of Chen system with fractional order is shown in Fig. 1(a)-(c). The dotted region in the diagram signifies that the system is in a state of chaos, whereas the blank zone demonstrates that the behavior of the system is not chaotic. By setting $q_1 = q_2 = 1$, $q_3 = 0.8$, $b = 3$, and $c = 28$, and then varying the value

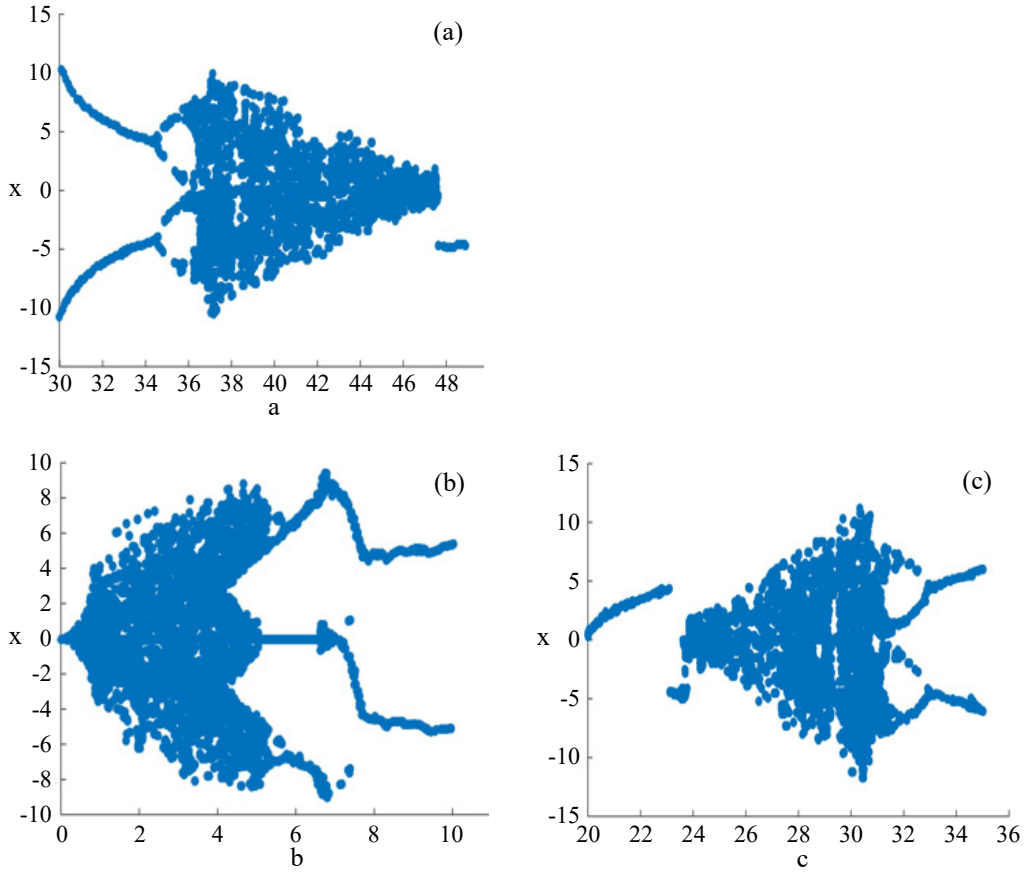


Fig. 1. The bifurcation diagram of fractional Chen system. (a) $q_1 = q_2 = 1$, $q_3 = 0.8$, $b = 3$, and $c = 28$, (b) $q_1 = q_2 = 1$, $q_3 = 0.8$, $a = 40$, and $c = 28$, and (c) $q_1 = q_2 = 1$, $q_3 = 0.8$, $b = 3$, and $a = 40$.

of a, the bifurcation diagram of the system is illustrated in Fig. 1(a). As the diagram shows, it can be seen that chaotic behavior may occur in the system when $a \in [36, 47]$. By choosing $q_1 = q_2 = 1$, $q_3 = 0.8$, $a = 40$, and $c = 28$, and then adjusting b, the bifurcation diagram is displayed in Fig. 1(b). The examination of Fig. 1(b) reveals that the system may behave chaotically when $b \in [0.8, 5]$. By setting $q_1 = q_2 = 1$, $q_3 = 0.8$, $b = 3$, and $a = 40$, and then changing the value of c, the bifurcation diagram of the system is presented in Fig. 1(c), As seen in Fig. 1(a), it can be inferred that when $c \in [23, 32]$, chaotic behavior may manifest in the system.

2.2. Lyapunov exponent

Lyapunov exponent is a crucial instrument in comprehending the intricacies of chaos. It provides insight into the level of chaos in dynamic systems. Positive values of the Lyapunov exponent signify chaos in the system, which will eventually lead to full unpredictability. The formula for the Lyapunov exponent is presented as follows [39]:

$$\mathrm{Ly} = \lim_{n \to +\infty} \frac{1}{n} \sum_{i=1}^{N} \ln \left| f'(x_i) \right| \tag{4}$$

where $f'(x_i)$ represents the derivative function of the chaotic system. The Lyapunov exponent of the Chen system with fractional order is depicted in Fig. 2. The fractional -order Chen system features three Lyapunov exponents (Ly_1 (blue), Ly_2 (green), and Ly_3 (red)) that quantify the rates of divergence or convergence of trajectories in distinct phase space directions. The Lyapunov exponent Ly_1 determines the system's behavior, which is the largest in magnitude. Positive Ly_1 suggests chaos and sensitivity to initial conditions, whereas negative Ly_1 denotes stability and trajectory convergence. The remaining Lyapunov exponents (Ly_2 and Ly_3) provide insight into local dynamics and the expansion/contraction behavior in additional phase space directions.

The Lyapunov exponent spectra depicted in Fig. 2 are in good agreement with the bifurcation diagrams. Based on the analysis above, it can be concluded that the fractional-order Chen system exhibits desirable chaotic behavior.

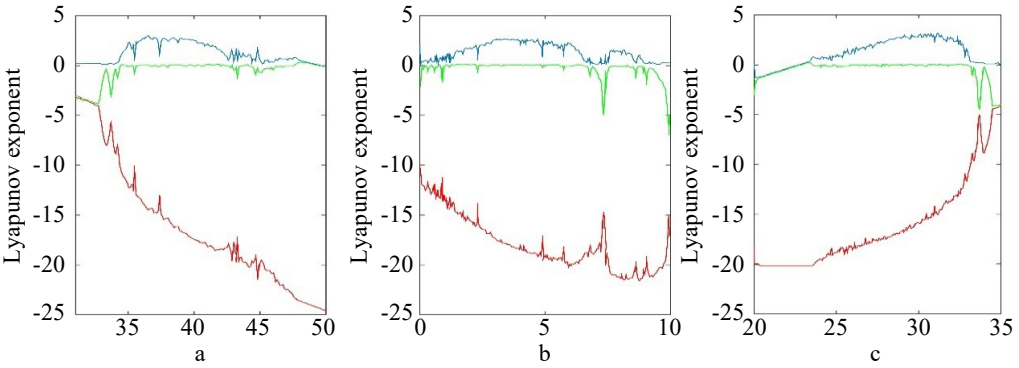


Fig. 2. The Lyapunov exponent of the fractional Chen system.

2.3. Randomness testing

The randomness quality of chaotic systems is rigorously assessed using the TestU01 suite, a comprehensive statistical testing framework. This suite includes three progressively demanding test batteries: SmallCrush, Crush, and BigCrush. The performance of a system in these tests is inversely related to the number of failures it incurs—fewer

T a b l e 1. TestU01 failures for statistical testing.

Gain		10^{13}	10^{14}	10^{15}	10^{16}
CQM(x)	SmallCrush	6	4	4	4
	Crush	107	114	102	101
FOCS(x, y, z)	SmallCrush	(2, 3, 2)	(1, 2, 1)	(1, 1, 1)	(0, 1, 0)
	Crush	(5, 6, 5)	(4, 5, 4)	(3, 4, 3)	(2, 2, 3)
	BigCrush	(8, 9, 9)	(7, 8, 8)	(6, 6, 7)	(5, 5, 6)

failures indicate stronger randomness and higher suitability for cryptographic applications [40]. In this study, we evaluate the randomness of two chaotic systems: the classic quadratic map (CQM) and the fractional-order Chen system (FOCS), across gain levels ($g = 10^{13},10^{14},10^{15},10^{16}$). Using the TestU01 suite, we find that FOCS outperforms CQM, exhibiting fewer failures in SmallCrush, Crush, and BigCrush tests—especially at higher gains ($g = 10^{15},10^{16}$), as shown in Table 1. This is due to FOCS's fractional-order dynamics and three-dimensional structure, which enhance chaotic behavior and sensitivity, making it more suitable for cryptographic applications.

3. Proposed cryptosystem

This section introduces a novel encryption scheme tailored for optical imaging systems, combining a three-dimensional fractional-order chaotic system with an innovative zigzag-based permutation technique. The proposed approach generates multiple sets of zigzag patterns driven by the fractional-order chaotic system, dynamically rearranging the pixel positions within the image. By leveraging diverse zigzag patterns in conjunction with the inherent randomness of the chaotic system, the encryption process achieves high levels of unpredictability and security. This design significantly strengthens the system's resistance to various attacks, including statistical and differential attacks, which are critical challenges in optical data security.

To further enhance robustness, the SHA-512 hash value of the input image is used to compute the initial conditions of the fractional-order chaotic system, introducing an additional layer of security and making the algorithm highly sensitive to the input image. Figure 3 provides a visual representation of the algorithm's structure and

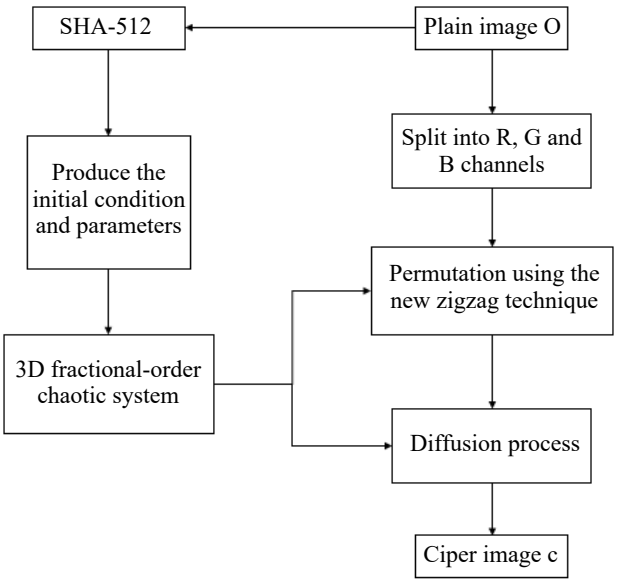


Fig. 3. The flowchart of the proposed encryption scheme.

workflow. The detailed steps outline the encryption process, emphasizing its suitability for optical imaging systems that demand both high security and computational efficiency.

This scheme is particularly well-suited for securing high-resolution optical images, such as those used in medical imaging, remote sensing, and secure optical communications. It offers a reliable and efficient solution for protecting sensitive visual data in applications where data confidentiality and integrity are of utmost importance.

3.1. Input

Plain-color image O with an arbitrary size of $L = m \times n \times 3$, the total number of encryptions rounds n, and the SHA-512 hash value of O used to compute the initial conditions (x_0, y_0, z_0) and fractional-order parameters (q_1, q_2, q_3) of the fractional-order Chen system. For larger images, small perturbations derived from the hash value are injected during iteration to prevent dynamical degradation [41].

3.2. Output

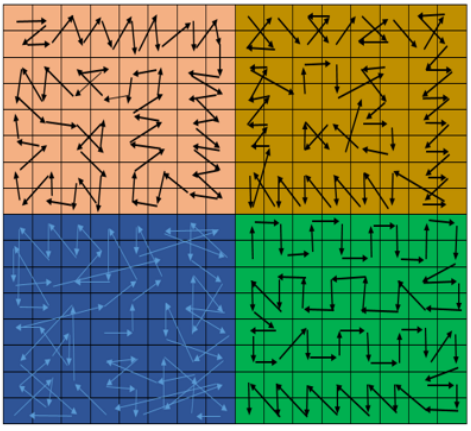
The encrypted color image C, having the same dimensions. This is accomplished through the following steps:

Step 1: The plain image O with a size of $m \times n \times 3$ is read, and then it is partitioned into three constituent parts (R, G, and B).

Step 2: We apply Eq. (3) using the parameters a, b, c, the initial conditions x_0, y_0, and z_0, as well as the fractional-order parameters q_1, q_2, and q_3 to generate three sequences of random values denoted by x, y, and z of size $m \times n$. The initial conditions are created through the SHA-512 hash.

0.1	0.2	0.35	0.4	0.42	0.46	0.5	0.52	0.1	0.14	0.17	0.16	0.19	0.22	0.25	0.24
0.25	0.3	0.38	0.41	0.44	0.5	0.51	0.52	0.13	0.12	0.15	0.18	0.21	0.2	0.23	0.26
0.92	0.9	0.88	0.88	0.85	0.84	0.55	0.53	0.6	0.58	0.62	0.65	0.68	0.67	0.27	0.28
0.93	0.91	0.89	0.87	0.86	0.83	0.6	0.58	0.57	0.56	0.61	0.66	0.9	0.7	0.29	0.3
1.23	0.94	0.94	0.96	0.82	0.81	0.61	0.6	0.55	0.54	0.82	0.75	0.71	0.72	0.31	0.32
1.22	1.21	0.96	0.95	0.8	0.75	0.63	0.62	0.53	0.52	0.8	0.85	0.74	0.73	0.33	0.34
1.2	1	0.98	0.97	0.74	0.7	0.64	0.64	0.5	0.48	0.46	0.44	0.42	0.4	0.35	0.36
1.05	0.99	0.99	0.98	0.72	0.71	0.65	0.64	0.51	0.49	0.47	0.45	0.43	0.41	0.37	0.38
0.88	0.86	0.84	0.8	0.15	0.18	0.2	0.17	0.12	0.14	0.17	0.18	0.21	0.22	0.25	0.26
0.91	0.87	0.85	0.83	0.16	0.95	0.21	0.19	0.10	0.15	0.16	0.19	0.20	0.23	0.24	0.27
0.92	0.93	0.82	0.81	0.79	0.14	0.24	0.22	0.66	0.6	0.5	0.37	0.36	0.33	0.28	0.30
0.89	0.9	0.61	0.78	0.12	0.33	0.3	0.25	0.67	0.65	0.45	0.4	0.35	0.34	0.32	0.31
0.76	0.75	0.73	0.1	0.11	0.34	0.23	0.31	0.70	0.68	0.75	0.8	0.82	0.91	0.92	0.94
0.62	0.72	0.74	0.46	0.47	0.37	0.32	0.35	0.71	0.73	0.77	0.78	0.85	0.9	0.93	0.95
0.71	0.67	0.6	0.5	0.51	0.45	0.41	0.53	1.5	1.3	1.24	1.21	1.2	0.99	0.96	0.96
0.66	0.7	0.63	0.55	0.52	0.36	0.4	0.38	1.6	1.4	1.25	1.22	1.21	1	0.98	0.97

Sequence X



Matrix I

Fig. 4. Creating various zigzag patterns: a numerical example.

Step 3: We transform the random sequence x into matrix I, which is further divided into 8×8 blocks. We then sort the elements of each block in ascending order to create a variety of zigzag patterns. Figure 4 illustrates an example of this process.

Step 4: We use the sequences Y and Z to create a new sequence with a size equal to the number of blocks in matrix I. Next, we transform this sequence into matrix J and arrange its elements in ascending order to form a new zigzag.

Step 5: We partition the channels (R, G, and B) of the original image O into blocks of size 8×8.

Step 6: By utilizing the various zigzag patterns generated from the matrix I, we change the pixel locations in each block of the R, G, and B channels. This process involves applying the zigzag patterns to each channel to modify the placement of individual pixels. An example of this process is shown in Fig. 5.

Step 7: We use the zigzag patterns created from the matrix J to alter the placement of blocks in each of the R′, G′, and B′ channels. The resulting modified R, G, and B channels are referred to as scrambled channels (R_s, G_s, and B_s). Figure 6 provides an example of this procedure.

Step 8: We obtain three keys by applying Eq. (3) with the initial values of (a, b, c), (q_1, q_2, q_3), and (x_0, y_0, z_0). Once we obtain these keys, we transform them into integers.

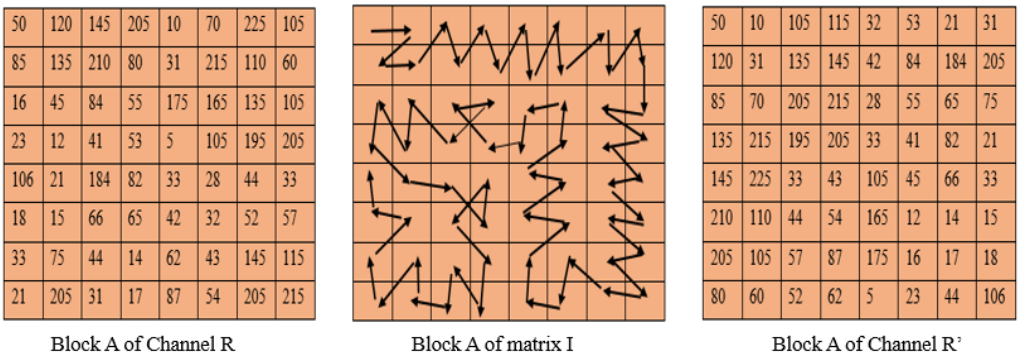


Fig. 5. Permutation process using various zigzag patterns.

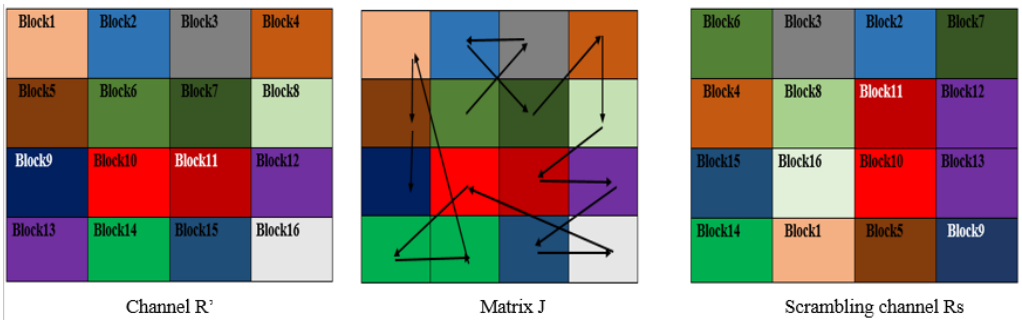


Fig. 6. Blocks permutation process.

$$\begin{cases} \text{key1} = \text{floor}(X(i) \times 10^{15}) \bmod 256 \\ \text{key2} = \text{floor}(Y(i) \times 10^{15}) \bmod 256 \\ \text{key3} = \text{floor}(Z(i) \times 10^{15}) \bmod 256 \end{cases} \tag{5}$$

Step 9: We convert the scrambled channels (R_s, G_s, and B_s) into vectors and then perform an XOR operation between the keys and scrambled vectors to obtain encrypted vectors as follows:

$$\begin{cases} R_e(i) = R_{s1d}(i) \oplus \text{key1}(i) \oplus R_s(i-1) \\ G_e(i) = G_{s1d}(i) \oplus \text{key2}(i) \oplus G_s(i-1) \\ B_e(i) = B_{s1d}(i) \oplus \text{key3}(i) \oplus B_s(i-1) \end{cases} \tag{6}$$

where R_e, G_e, and B_e are the cipher vectors.

Step 10: Once we obtain the cipher vectors R_e, G_e, and B_e, we convert them back to matrices. We can then use these matrices to construct the encrypted image.

4. Simulation experiment and analysis

Our test setup included a machine with 8 GB of memory and an Intel(R) Core(TM) i7-7500u CPU running at 2.90 GHz. The software used was MATLAB R2021a. We tested

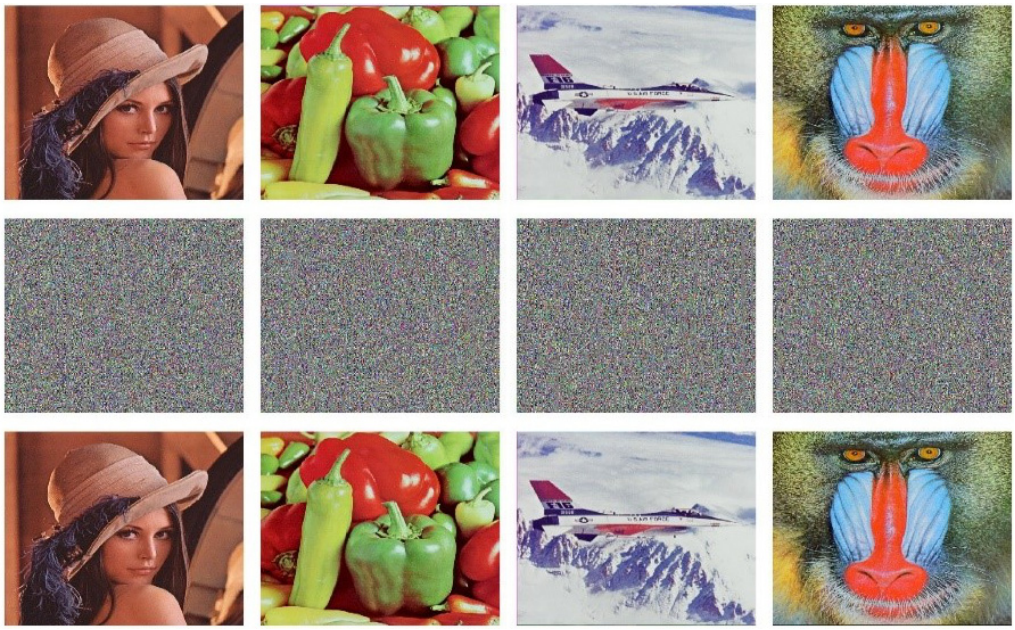


Fig. 7. Encryption and decryption results (*Lena*, *peppers*, *plane*, *baboon*).

the performance of our suggested method on four image data sets having $512 \times 512 \times 3$ dimensions. To demonstrate the effectiveness of our method, we compared our results with those of other encryption schemes in the literature. Figure 7 illustrates the results of the image encryption and decryption procedure.

4.1. Key space analysis

The size of the key space is a measure of an encryption algorithm's ability to resist violent attacks. Generally, an effective encryption method should have a key space of at least 2^{100} [42]. The key of our encryption scheme is built on sub-keys in its main structure, which are based on initial conditions, control parameters, and fractional-order parameters of the chaotic system. Different sub-key values have been implemented in both the permutation and diffusion processes. Therefore, the key of our scheme comprises a total of 18 elements, as follows:

1) The initial conditions (x_0, y_0, z_0) and (x_1, y_1, z_1).
2) Control parameters (a_0, b_0, c_0) and (a_1, b_1, c_1).
3) Fractional-order parameters (q_1, q_2, q_3) and (q_1', q_2', q_3').

Based on our experimental results, each element in the key space has a size of approximately 10^{15}. So, the suggested encryption algorithm's full key space is $10^{15 \times 18 = 270}$. As illustrated in Table 2, our encryption scheme has a sufficiently large key space, making it extremely difficult for hackers to launch brute-force attacks and compromise the system's security.

T a b l e 2. Key space analysis.

	Our method	Ref. [2]	Ref. [6]	Ref. [11]	Ref. [45]
Key space	2^{795}	2^{412}	2^{536}	2^{261}	2^{399}

4.2. Key sensitivity analysis

Ensuring secure encryption and decryption requires that every encryption method must provide high sensitivity to the encryption key. Even a minor alteration in any of the key components can render the decrypted image completely invisible, resulting in a decryption failure. We evaluated the sensitivity of our key by modifying the value

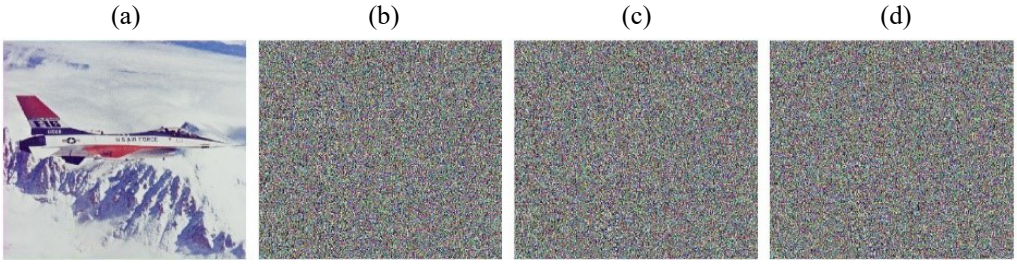


Fig. 8. The key sensitivity test of the decrypted image (a) correct key, (b) wrong q_1, (c) wrong b, and (d) wrong x_0.

of one key elements by a small percentage of 10^{-15}. The resulting outcomes are illustrated in Fig. 8. As clearly evidenced by the decrypted image, it provides no useful information about the original image, demonstrating the high sensitivity of the suggested technique to the encryption key. This makes it very difficult for attackers to decipher the original image, as even the slightest deviation from the correct key will result in a completely different, decrypted image, rendering their efforts useless.

4.3. Histogram analysis

A histogram provides a visual representation of the distribution of pixels in an image. When the histogram of a cipher image is not uniform, it can expose patterns to attackers, making the image susceptible to statistical attacks. Therefore, having a flat (uniform) histogram is essential for a secure encryption system. To ensure the security of the images, we conducted a thorough analysis of the histograms of both the original and encrypted images. Figure 9 shows the histograms of the *peppers* image and its cipher image. Figure 9 clearly illustrates that the histogram of the encrypted image is uniformly distributed and remarkably distinct from that of the original image. This indicates that our proposed approach effectively prevents attackers from obtaining any statistical information that could be used to launch statistical attacks. and make it impossible to determine the connection between the pixel distribution of the original image and the encrypted image.

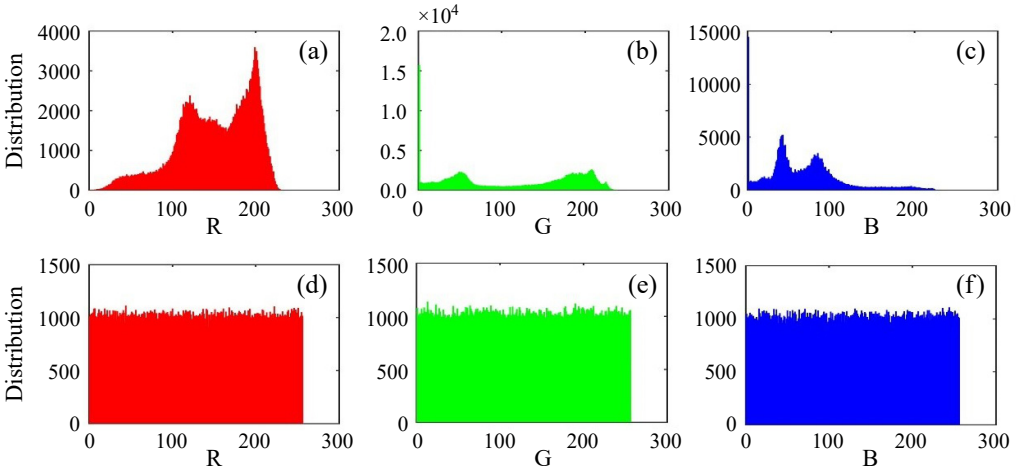


Fig. 9. Histogram of *peppers* image and cipher image (a)–(c) histogram of R, G, B channels of plain image, and (d)–(f) histogram of R, G, B channels of cipher image.

4.4. Entropy analysis

Information entropy is a vital metric in evaluating the security of an encryption method, as it quantifies the average information content of a digital image. In addition, it pro-

T a b l e 3. Entropy results.

Image	Plain image	Our method	Ref. [12]	Ref. [15]	Ref. [19]	Ref. [44]	Ref. [45]
Lena	7.4767	7.9998	7.9996	7.9992	7.99746	7.9984	7.9993
Peppers	7.6698	7.9997	7.9995	7.9912	7.99423	7.9355	7.9993
Plane	6.7174	7.9998	7.9998	7.9996	7.99664	/	/
Baboon	7.7705	7.9997	7.9997	7.9974	7.99494	7.9859	7.9994

vides insight into the randomness and unpredictability of the encrypted image. The following formula is used to determine the entropy of image [42]:

$$h(m) = -\sum_{i=0}^{2^n} p(m_i) \log_2(p(m_i)) \tag{7}$$

where $p(m_i)$ represents the probability of m_i. The information entropy value that is acquired through the encryption approach should be as near to eight as possible. The closer the obtained value is to eight, the more secure the encryption scheme performs. Table 3 displays the entropy findings of our method. Table 3 clearly demonstrates that the information entropy for all encrypted images is remarkably high, with values approaching the theoretical maximum of eight. Furthermore, we compared the information entropy of our proposed algorithm with several other established algorithms. Our proposed approach exhibited a higher information entropy value, indicating superior performance and a higher level of security.

4.5. Correlation coefficient

Correlation analysis is a crucial metric used to evaluate the performance of image encryption methods. It is widely recognized that pixels in an image are highly correlated horizontally, vertically, and diagonally with each other. As a result, strong encryption algorithms are required to break this association between pixels. The correlation coefficient can be defined as [42]:

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \tag{8}$$

$$\operatorname{cov}(x, y) = E([x - E(x)][y - E(y)]) \tag{9}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x)]^2 \tag{11}$$

where x and y are two adjacent pixels, N is the total number of pixels, $\operatorname{cov}(x, y)$ denotes the covariance between x and y, and $E(x)$ and $E(y)$ represent the means of x and y, re-

T a b l e 4. Correlation coefficient results.

	Images	Red			Green			Blue		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Our method	*Lena*	0.0009	–0.0007	–0.0015	–0.0019	0.0012	–0.0021	0.0001	–0.0002	–0.0017
	Peppers	–0.0027	0.0041	–0.0004	0.0022	–0.0005	–0.0001	0.0021	–0.0009	–0.0001
	Plane	0.0037	0.0012	0.0002	–0.0030	0.0014	–0.0007	0.0026	0.0012	–0.0010
	Baboon	–0.0022	–0.0018	0.0048	0.0042	0.0018	–0.0004	0.0012	–0.0012	0.0019
Ref. [6]	*Lena*	–0.0002	–0.0023	–0.0021	–0.00029	–0.0043	0.007	0.0074	–0.0010	–0.0007
	Peppers	–0.0008	–0.0067	–0.0069	0.0007	0.0072	–0.0048	0.0006	–0.0043	–0.0007
	Plane	–0.0032	–0.0053	0.0047	–0.0008	–0.0021	–0.0002	0.0030	–0.0006	0.0015
	Baboon	–0.0045	–0.0002	0.0014	0.005	0.0029	0.0005	0.0006	0.0001	0.0022
Ref. [11]	*Lena*	–0.0022	0.0009	0.0013	0.0057	–0.0041	0.0017	0.0007	0.0004	0.0104
	Peppers	–0.0038	–0.0026	–0.0187	0.0014	0.0038	0.0058	–0.0094	0.0035	0.0035
	Plane	0.0006	0.0013	0.0023	0.0023	0.0010	–0.0057	0.0009	–0.0017	0.0083
	Baboon	0.0049	0.0006	0.0021	–0.0026	–0.010	0.0147	0.0068	0.0038	–0.0040
Ref. [46]	*Lena*	0.0028	0.0019	–0.0011	–0.0001	–0.0013	0.0024	0.0022	–0.0006	–0.0010
	Peppers	–0.0004	0.0003	–0.009	–0.009	0.0023	0.0016	0.0021	0.006	0.0022
	Plane	0.0016	–0.0006	–0.002	0.0013	0.0017	0.0013	–0.0013	–0.001	0.0034
	Baboon	0.0011	0.0021	0.0024	–0.0002	0.006	–0.0034	–0.0024	0.0012	–0.0023
Ref. [47]	*Lena*	–0.0012	0.0012	–0.0011	0.0025	0.0019	–0.0011	0.0003	0.0025	–0.0004
	Peppers	0.0027	0.0016	–0.003	0.0017	0.0010	0.0015	0.0014	–0.005	–0.0004
	Plane	/	/	/	/	/	/	/	/	/
	Baboon	0.0002	0.0012	0.003	0.0013	–0.008	0.0011	–0.0019	–0.0015	0.001

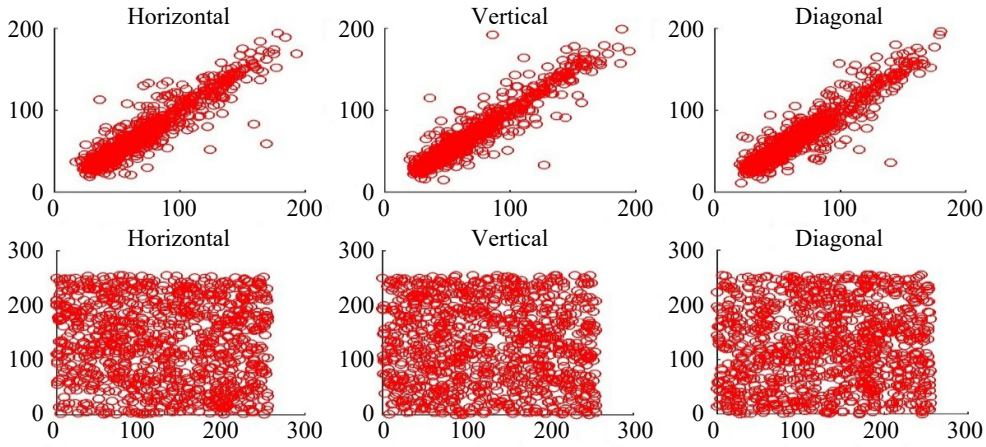


Fig. 10. Neighboring pixel distribution of *peppers* in different directions.

spectively. Table 4 compares the correlation coefficient findings acquired from our algorithms to those obtained from other encryption methods discussed in the literature. Table 4 demonstrates that the encrypted image has much lower correlation values in all directions. Additionally, in terms of correlation coefficient values, our proposed encryption technique surpasses the reference methods. This implies that our method is more robust at preventing statistical attacks. Figure 10 displays the correlations of adjacent pixels in the plain and encrypted images, visible across the vertical, diagonal, and horizontal axes.

4.6. Resistance to differential attack

The differential attack is widely recognized as a highly successful strategy among various types of attacks. Attackers often use this method to discern the relationship between an original and encrypted image by evaluating the rate of change of each pixel in an encrypted image. To prevent such assaults, an image encryption scheme must be able to resist differential attacks. To assess the robustness of encryption methods to differential attacks, number of pixel change rate (NPCR) and uniform average change intensity (UACI) are broadly applied. When comparing two encrypted pictures with slightly varying inputs, NPCR reveals the proportion of pixels that change, whereas UACI measures the average difference in pixel values. The formulas used to calculate NPCR and UACI are as follows:

$$\text{NPCR} = \frac{1}{L}\sum_{i,j} D(i,j) \times 100\% \tag{12}$$

$$\text{UACI} = \frac{1}{L}\sum_{i,j} \frac{\left|c_1(i,j) - c_2(i,j)\right|}{255} \times 100\% \tag{13}$$

T a b l e 5. NPCR and UACI of *Lena*, *peppers*, *plane* and *baboon* with just one pixel adjustment.

	Images	UACI	NPCR
Our method	*Lena*	33.44	99.60
	Peppers	33.46	99.60
	Plane	33.48	99.61
	Baboon	33.44	99.60
Ref. [19]	*Lena*	33.56	99.645
	Peppers	33.58	99.61
	Plane	33.61	99.583
	Baboon	33.547	99.627
Ref. [11]	*Lena*	33.43	99.615
	Peppers	33.43	99.61
	Plane	33.48	99.61
	Baboon	33.44	99.61
Ref. [44]	*Lena*	33.4550	99.7540
	Peppers	33.7350	99.2455
	Plane	/	/
	Baboon	33.2510	99.8335
Ref. [46]	*Lena*	33.46	99.61
	Peppers	33.46	99.61
	Plane	33.43	99.61
	Baboon	33.47	99.62

where L represent the total count of pixels, c_1 and c_2 are the initial and modified pixel values, respectively. The following rules must be followed to determine $D(i,j)$:

$$\begin{cases} D(i,j) = 1 & \text{if} \quad c_1(i,j) \neq c_2(i,j) \\ D(i,j) = 0 & \text{otherwise} \end{cases} \tag{14}$$

The literature indicates that the most desirable values for NPCR and UACI are 99.6094 and 33.4635, respectively [43]. To assess whether our method works against differential attacks, we made a small modification to the original images by altering a single pixel and computed the subsequent NPCR and UACI values. Table 5 displays the outcomes of the test. The findings of our scheme demonstrate that the proposed encryption scheme performs significantly better than other algorithms in the literature. Based on the analysis of NPCR and UACI results, our scheme has demonstrated a level of performance that is much closer to recommended values, which means that the scheme is able to withstand differential attacks.

4.7. Data loss and noise attacks

Inevitably, during the transmission of an image through a channel, it may encounter noise interference or data loss [48]. To test the suggested encryption algorithm's capacity to withstand such disturbances. We introduced salt-and-pepper noise at varying levels of 1%, 5%, and 10% to the encrypted images. We then examined the decrypted images' quality and showed our findings in Fig. 11. In addition, we conducted a test where the encrypted image was clipped at different sizes and decrypted using the correct key. Figure 12 depicts the outcomes of this test. These experiments assisted us in determining the encryption algorithm's ability to handle image corruption caused by noise and data loss. Our findings indicate that even if a significant amount of noise is injected into the encrypted image or some data is lost during transmission. Our scheme

Fig. 11. Process of decryption using different level of salt-and-pepper nose.

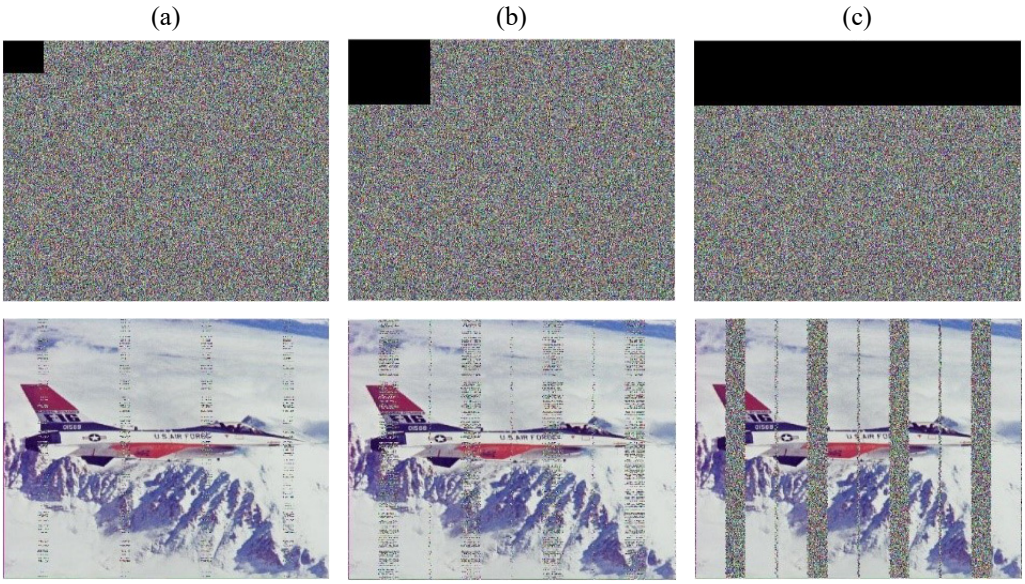


Fig. 12. Data loss attack analysis (a) 64×64 data loss, (b) 128×128 data loss, and (c) 128×512.

can effectively retrieve the essential information of the original image from the decrypted image. The findings show that our techniques are extremely adaptive to a variety of real-world situations in which data may be susceptible to various sorts of interference. Our algorithms, in fact, are resistant to noise attacks and data loss, making them ideal for applications requiring data security and integrity.

5. Conclusion

In this research, we propose an innovative image encryption strategy specifically designed for optical imaging systems. The method integrates fractional-order chaotic systems with a novel zigzag permutation technique to enhance security and unpredictability. The permutation process utilizes dynamically controlled zigzag patterns governed by the fractional-order chaotic system, ensuring efficient and robust pixel

scrambling suitable for high-resolution optical images. The encryption key is derived from the system's initial values and fractional-order parameters, significantly expanding the key space and increasing the algorithm's complexity.

Performance evaluations reveal that the proposed method exhibits outstanding features, including a large key space, high sensitivity to key variations, and low pixel correlation, making it highly resilient to statistical and differential attacks. These characteristics are essential for ensuring the security of optical data.

From an academic standpoint, this study contributes significantly to the field of optical data security by presenting a novel encryption approach that combines fractional-order dynamics with advanced permutation techniques. It addresses key challenges in encrypting optical images, such as high pixel correlation and large data volumes, bridging theoretical advancements with practical applications. This work provides a foundation for further research on the use of fractional-order systems in optical imaging and related data security domains, encouraging the development of more sophisticated encryption methods to meet the increasing demands for secure optical communication and storage.

To address potential limitations, future research could focus on optimizing the algorithm for real-time applications, such as medical imaging and remote sensing, and extending its applicability to other optical data formats, including hyperspectral and 3D imaging. Additionally, exploring quantum-resistant enhancements and hybridizing the approach with other cryptographic methods could further strengthen its security and efficiency. Such advancements would enhance the practical deployment of the proposed scheme in real-world optical imaging scenarios.

References

[1] HERBADJI D., DEROUICHE N., BELMEGUENAI A., TAHAT N., BOUMERDASSI S., *A new colour image encryption approach using a combination of two 1D chaotic map*, International Journal of Electronic Security and Digital Forensics **12**(4), 2020: 337-356. https://doi.org/10.1504/IJESDF.2020.110649

[2] SINGH K.N., SINGH O.P., BARANWAL N., SINGH A.K., *An efficient chaos-based image encryption algorithm using real-time object detection for smart city applications*, Sustainable Energy Technologies and Assessments **53**, 2022: 102566. https://doi.org/10.1016/j.seta.2022.102566

[3] HERBADJI D., BELMEGUENAI A., DEROUICHE N., LIU H., *Colour image encryption scheme based on enhanced quadratic chaotic map*, IET Image Processing **14**(1), 2020: 40-52. https://doi.org/10.1049/iet-ipr.2019.0123

[4] RAMADAN N., AHMED H.E.H., ELKHAMY S.E., ABD EL-SAMIE F.E., *Chaos-based image encryption using an improved quadratic chaotic map*, American Journal of Signal Processing **6**(1), 2016: 1-13. https://doi.org/10.5923/j.ajsp.20160601.01

[5] BEKKOUCHE T., BOUGUEZEL S., *Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform*, Journal of Electronic Imaging **27**(2), 2018: 023033. https://doi.org/10.1117/1.JEI.27.2.023033

[6] ZHANG Q., HAN J., *A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding*, Multimedia Tools and Applications **80**, 2021: 13841-13864. https://doi.org/10.1007/s11042-020-10437-z

[7] KANG X., GUO Z., *A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system*, Signal Processing: Image Communication **80**, 2020: 115670. https://doi.org/10.1016/j.image.2019.115670

[8] Iqbal N., Hanif M., Abbas S., Khan M.A., Rehman Z.U., *Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding*, Journal of Information Security and Applications **58**, 2021: 102809. https://doi.org/10.1016/j.jisa.2021.102809
[9] Li C., Yang X., *An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos*, Optik **260**, 2022: 169042. https://doi.org/10.1016/j.ijleo.2022.169042
[10] Su Y., Wang X., *A robust visual image encryption scheme based on controlled quantum walks*, Physica A: Statistical Mechanics and its Applications **587**, 2022: 126529. https://doi.org/10.1016/j.physa.2021.126529
[11] Li Z., Peng C., Tan W., Li L., *A novel chaos-based color image encryption scheme using bit-level permutation*, Symmetry **12**(9), 2020: 1497. https://doi.org/10.3390/sym12091497
[12] Alghafis A., Munir N., Khan M., *An encryption scheme based on chaotic Rabinovich-Fabrikant system and S_8 confusion component*, Multimedia Tools and Applications **80**, 2021: 7967-7985. https://doi.org/10.1007/s11042-020-10142-x
[13] Yavuz E., *A new parallel processing architecture for accelerating image encryption based on chaos*, Journal of Information Security and Applications **63**, 2021: 103056. https://doi.org/10.1016/j.jisa.2021.103056
[14] Chen L., Yin H., Huang T., Yuan L., Zheng S., Yin L., *Chaos in fractional-order discrete neural networks with application to image encryption*, Neural Networks **125**, 2020: 174-184. https://doi.org/10.1016/j.neunet.2020.02.008
[15] Shakir H.R., *Implementing digital image security framework with hybrid approach of chaotic map and singular-value decomposition*, Chaos, Solitons & Fractals: X **8**, 2022: 100075. https://doi.org/10.1016/j.csfx.2022.100075
[16] Pourasad, Y., Ranjbarzadeh R., Mardani A., *A new algorithm for digital image encryption based on chaos theory*, Entropy **23**(3), 2021: 341. https://doi.org/10.3390/e23030341
[17] Ghazvini M., Mirzadi M., Parvar N., *A modified method for image encryption based on chaotic map and genetic algorithm*, Multimedia Tools and Applications **79**, 2020: 26927-26950. https://doi.org/10.1007/s11042-020-09058-3
[18] Wang X., Su Y., *Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform*, Scientific Reports **10**, 2020: 18556. https://doi.org/10.1038/s41598-020-75562-z
[19] Ahmad M., Doja M.N., Beg M.M.S., *Security analysis and enhancements of an image cryptosystem based on hyperchaotic system*, Journal of King Saud University - Computer and Information Sciences **33**(1), 2021: 77-85. https://doi.org/10.1016/j.jksuci.2018.02.002
[20] Wang X., Chen X., *An image encryption algorithm based on dynamic row scrambling and Zigzag transformation*, Chaos, Solitons & Fractals **147**, 2021: 110962. https://doi.org/10.1016/j.chaos.2021.110962
[21] Li T., Yang M., Wu J., Jing X., *A novel image encryption algorithm based on a fractional-order hyperchaotic system and DNA computing*, Complexity, Vol. 2017, 2017: 9010251. https://doi.org/10.1155/2017/9010251
[22] Kaur G., Agarwal R., Patidar V., *Color image encryption system using combination of robust chaos and chaotic order fractional Hartley transformation*, Journal of King Saud University - Computer and Information Sciences **34**(8), 2022: 5883-5897. https://doi.org/10.1016/j.jksuci.2021.03.007
[23] Lai Q., Hu G., Erkan U., Toktas A., *A novel pixel-split image encryption scheme based on 2D Salomon map*, Expert Systems with Applications **213**, 2023: 118845. https://doi.org/10.1016/j.eswa.2022.118845
[24] Chai X., Gan Z., Chen Y., Zhang Y., *A visually secure image encryption scheme based on compressive sensing*, Signal Processing **134**, 2017: 35-51. https://doi.org/10.1016/j.sigpro.2016.11.016
[25] Yousif B., Khalifa F., Makram A., Takieldeen A., *A novel image encryption/decryption scheme based on integrating multiple chaotic maps*, AIP Advances **10**(7), 2020: 075220. https://doi.org/10.1063/5.0009225

[26] MUHAMMAD Z.M.Z., ÖZKAYNAK F., *An image encryption algorithm based on chaotic selection of robust cryptographic primitives*, IEEE Access **8**, 2020: 56581-56589. https://doi.org/10.1109/ACCESS.2020.2982827

[27] WANG X., LIU C., JIANG D., *A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT*, Information Sciences **574**, 2021: 505-527. https://doi.org/10.1016/j.ins.2021.06.032

[28] DOU Y., LIU X., FAN H., LI M., *Cryptanalysis of a DNA and chaos based image encryption algorithm*, Optik **145**, 2017: 456-464. https://doi.org/10.1016/j.ijleo.2017.08.050

[29] JAIN A., RAJPAL N., *A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps*, Multimedia Tools and Applications **75**, 2016: 5455-5472. https://doi.org/10.1007/s11042-015-2515-7

[30] BECHIKH R., HERMASSI H., ABD EL-LATIF A.A., RHOUMA R., BELGHITH S., *Breaking an image encryption scheme based on a spatiotemporal chaotic system*, Signal Processing: Image Communication **39**, 2015: 151-158. https://doi.org/10.1016/j.image.2015.09.006

[31] SONG C.-Y., QIAO Y.-L., ZHANG X.-Z., *An image encryption scheme based on new spatiotemporal chaos*, Optik **124**(18), 2013: 3329-3334. https://doi.org/10.1016/j.ijleo.2012.11.002

[32] ZHANG Q., GUO L., WEI X., *A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system*, Optik **124**(18), 2013: 3596-3600. https://doi.org/10.1016/j.ijleo.2012.11.018

[33] ZHANG Y., *Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system*, Optik **126**(2), 2015: 223-229. https://doi.org/10.1016/j.ijleo.2014.08.129

[34] ABDELJAWAD T., BANERJEE S., WU G.-C., *Discrete tempered fractional calculus for new chaotic systems with short memory and image encryption*, Optik **218**, 2020: 163698. https://doi.org/10.1016/j.ijleo.2019.163698

[35] WU G.-C., DENG Z.-G., BALEANU D., ZENG D.-Q., *New variable-order fractional chaotic systems for fast image encryption*, Chaos: An Interdisciplinary Journal of Nonlinear Science **29**(8), 2019: 083103. https://doi.org/10.1063/1.5096645

[36] MOHAMED S.M., SAYED W.S., MADIAN A.H., RADWAN A.G., SAID L.A., *An encryption application and FPGA realization of a fractional memristive chaotic system*, Electronics **12**(5), 2023: 1219. https://doi.org/10.3390/electronics12051219

[37] KAMAL F.M., ELSAID A., ELSONBATY A., *Ghost attractor in fractional order blinking system and its application*, Nonlinear Dynamics **108**, 2022: 4471-4497. https://doi.org/10.1007/s11071-022-07391-w

[38] NUÑEZ-PEREZ J.-C., ADEYEMI V.-A., SANDOVAL-IBARRA Y., PEREZ-PINAL F.-J., TLELO-CUAUTLE E., *Maximizing the chaotic behavior of fractional order Chen system by evolutionary algorithms*, Mathematics **9**(11), 2021: 1194. https://doi.org/10.3390/math9111194

[39] LIU X., TONG X., WANG Z., ZHANG M., *A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption*, Chaos, Solitons & Fractals **154**, 2022: 111693. https://doi.org/10.1016/j.chaos.2021.111693

[40] LIU H., KADIR A., XU C., *Cryptanalysis and constructing S-box based on chaotic map and backtracking*, Applied Mathematics and Computation **376**, 2020: 125153. https://doi.org/10.1016/j.amc.2020.125153

[41] LIU H., KADIR A., LIU J., *Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system*, Optics and Lasers in Engineering **122**, 2019: 123-133. https://doi.org/10.1016/j.optlaseng.2019.05.027

[42] HERBADJI D., DEROUICHE N., BELMEGUENAI A., HERBADJI A., BOUMERDASSI S., *A tweakable image encryption algorithm using an improved logistic chaotic map*, Traitement du Signal **36**(5), 2019: 407-417. https://doi.org/10.18280/ts.360505

[43] ZHAN K., WEI D., SHI J., YU J., *Cross-utilizing hyperchaotic and DNA sequences for image encryption*, Journal of Electronic Imaging **26**(1), 2017: 013021. https://doi.org/10.1117/1.JEI.26.1.013021

[44] Jawad L.M., *A new scan pattern method for color image encryption based on 3D-Lorenzo chaotic map method*, Multimedia Tools and Applications **80**, 2021: 33297-33312. https://doi.org/10.1007/s11042-021-11295-z

[45] Liu J., Chang H., Ran W., Wang E., *Research on improved DNA coding and multidirectional diffusion image encryption algorithm*, Entropy **25**(5), 2023: 746. https://doi.org/10.3390/e25050746

[46] Man X., Song Y., *Encryption of color images with an evolutionary framework controlled by chaotic systems*, Entropy **25**(4), 2023: 631. https://doi.org/10.3390/e25040631

[47] Li D., Li J., Di X., Li B., *Design of cross-plane colour image encryption based on a new 2D chaotic map and combination of ECIES framework*, Nonlinear Dynamics **111**, 2023: 2917-2942. https://doi.org/10.1007/s11071-022-07949-8

[48] Herbadji D., Herbadji A., Haddad I., Kahia H., Belmeguenai A., Derouiche N., *An enhanced logistic chaotic map based tweakable speech encryption algorithm*, Integration **97**, 2024: 102192. https://doi.org/10.1016/j.vlsi.2024.102192

Received January 11, 2025
in revised form January 27, 2025