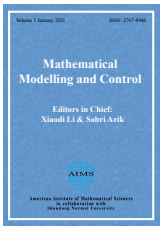
Mathematical Modelling and Control

https://www.aimspress.com/journal/mmc



MMC, 6(1): 14–28.
DOI: 10.3934/mmc.2026002
Received: 18 February 2025
Revised: 01 July 2025
Accepted: 23 July 2025
Published: 02 March 2026

Research article

Multidirectional chaos-based encryption scheme using the ABC fractional derivative for secure multimedia data transmission

Najeeb Alam Khan[1,*], **Saeed Akbar**[1,2], **Saif Ullah**[3] **and Muhammad Ayaz**[1]

[1] Department of Mathematics, University of Karachi, Karachi 75270, Pakistan

[2] Department of Electrical and Computer Engineering, Mohammad Ali Jinnah University, Karachi, Sindh 75400, Pakistan

[3] Department of Mathematics, Government College University Lahore, 54000, Pakistan

* **Correspondence:** Email: njbalam@yahoo.com.

Abstract: In this work, we studied a non-equilibrium point chaotic system with single signum function nonlinearity and multidirectional parameters under the Atangana-Baleanu-Caputo (ABC) fractional derivative. The control parameters were used to generate chaotic signals in multiple directions, such as a 1D line, 2D lattice, and 3D grid. The dynamical properties of the system were analyzed by graphical results, phase plots, and bifurcation plots. The ABC fractional analog circuit was designed using resistors, capacitors, operational amplifiers, and frequency domain approximations in the sense of ABC to ensure the system's feasibility. Random numbers were generated to evaluate the randomness of the system. These numbers were verified by the NIST test suite, and the test results established the strong unpredictability of the system. Text, video, and image files were the components that made up multimedia data, and as the usage of multimedia data sent over the internet continues to grow, so does the need for secure multimedia data. A significant topic in information security is the merging of chaos theory with encryption. For this purpose, we suggested a nonlinear 3D multidirectional chaos-based simple encryption scheme, in which a 3D multidirectional chaotic system was employed for position and value transformation. The proposed image encryption scheme employs a multidirectional chaotic system to enhance randomness and security, beginning with histogram equalization to uniformly distribute pixel intensities. This is followed by sequential row and column rotations and a final exclusive OR (XOR) operation, effectively achieving strong confusion and diffusion in the encrypted image. We computed several metrics to assess the quality of an image, including mean square error (MSE), peak signal-to-noise ratio (PSNR), entropy, the correlation coefficient, and image distance. NPCR (number of pixels change rate) and UACI (unified average change intensity) are standard statistical measures used to evaluate the effectiveness of image encryption, particularly in resisting differential attacks.

Keywords: chaotic system; Atangana-Baleanu-Caputo fractional derivative; electronic circuit; cryptography; fractional calculus

1. Introduction

The well-established field of fractional calculus (FC) has seen a revival in recent decades. Many physical phenomena can now be modeled mathematically using FC—capabilities that were previously unattainable with classical calculus. In the context of non-integer-order calculus, problems exhibiting memory effects—whether in space, time, or both—such as anomalous diffusion in heterogeneous media, can be elegantly described. As a result, FC has become a vibrant area of mathematical science, exploring the application of fractional differential and integral operators to extend classical concepts in mathematics and engineering [1, 2]. Fractional derivatives are broadly categorized as either local or nonlocal. Of these, nonlocal derivatives have attracted considerable interest due to their ability to capture memory and hereditary effects, which are essential for accurately modeling a wide range of physical and engineering phenomena. Several formulations of fractional derivatives involving singular kernels have

been introduced in the literature. Among the most prominent are the Grünwald–Letnikov, Riemann–Liouville, and Caputo definitions [3–6]. Certain fractional derivatives, such as the ABC fractional derivative, have recently been defined in terms of non-singular kernels [7, 8]. Fractional derivatives with non-singular kernels are important because certain systems of dissipative processes cannot be properly represented by conventional fractional derivatives [9, 10].

Equilibrium points (EPs) in a chaotic dynamical system play a critical part in analyzing its nonlinear dynamic behavior. Maximum described systems have limited EPs, such as the Rössler system [11], Lorenz system [12], and Chen system [13], etc. Chaos in these systems may be verified by way of the usage of conventional Shilnikov conditions wherein, as a minimum, one unstable EP for the appearance of chaos is necessary. Lately, some chaotic systems without EPs or with one stable EP have been seen. Here, we give some references for a no-EP chaotic system, such as: [14] proposed a five-term three dimension non-EP chaotic approach with two square nonlinear terms. According to the Sprott A system, a unique, non-EP hyperchaotic system of four dimensions was created [15]. The system involves nine terms, five of which are nonlinear. Then, using a computer search technique, they developed three-dimensional, no-EP chaotic signals with square terms [16]. A no-equilibrium, four-dimensional hyperchaotic technique with eight square nonlinear terms was achieved in [17]. In 2015, Shahzad et al. designed a three-dimensional no-EP chaotic approach with square nonlinearity and two square terms [18]. Then they presented a recent chaotic structure with no EP that was produced by inserting a few fixed disturbance terms into a chaotic technique with a one-dimensional line EP, and the equations contain three square terms. After that, a three-dimensional chaotic system with no EP, ten expressions, and five square nonlinearities was presented. Researchers discovered a five-dimensional no-EP system having two square nonlinearities in the same year. Later, there was a non-EP, three-dimensional chaotic system with six terms, absolute nonlinearity, and two square terms. A non-EP, four-dimensional chaotic method with two nonlinear terms followed closely after, using a controller with linear state feedback [19]. Meanwhile, Wang et al. devised a novel, three-dimensional chaotic technique with no EP but two square terms and a cubic term [20]. Researchers have suggested a simple chaotic system of three dimensions with a square term and square nonlinearity that does not have EPs [21].

Chaos-based cryptography is an emerging field in secure communication that leverages the unpredictability and sensitivity to initial conditions of chaotic systems for data encryption. Unlike traditional cryptographic methods that depend on mathematical complexity, chaos-based schemes exploit the deterministic yet seemingly random behavior of nonlinear dynamical systems, making them ideal for high-speed, lightweight applications such as multimedia and internet of things (IoT) devices. Their strong sensitivity to initial conditions ensures high confusion and diffusion, preventing unauthorized access without exact system parameters. These systems generate complex pseudo-random sequences that serve as keys or control shuffling mechanisms in image encryption, providing resilience against brute-force and statistical attacks while maintaining computational efficiency. Particularly effective in encrypting multimedia content, chaos-based methods handle high redundancy and large data volumes better than conventional algorithms, often enabling simultaneous compression and encryption. Additionally, hybrid approaches that combine chaos with traditional cryptographic techniques enhance both security and performance. Despite their advantages, careful design is essential to mitigate vulnerabilities such as low key sensitivity or periodic behavior in digital implementations, underscoring the need for continued research to align chaos-based cryptography with modern security standards [22–24].

All chaotic non-equilibrium systems discussed above exhibit at least one quadratic nonlinearity, leading to complicated algebraic structures. This will make circuit implementation more difficult. A multiplier is often used to implement a quadratic term in a chaotic system. While the multiplier increases power consumption and size of the analog circuit, it not only trashes circuit resources but is also detrimental to the initial state design. A simple and dependable analog circuit for producing chaotic signals is required for real-world engineering applications. As a result, finding a low-dimension, non-EP chaotic system

with a fundamental algebraic structure and circuit design is critical. Inspired by the analysis given above, the aim of this research is to propose a three-dimensional, non-EP chaotic system with only one signum nonlinear function with the ABC fractional derivative. The ABC fractional differential operator seems to provide meaningful findings, visual depictions, and simulated outcomes for the non-EP chaotic behaviors. By changing the multidirectional parameters, this system can also be turned into a chaotic 1D line, 2D lattice, and 3D grid. The ABC analog circuit is designed for feasibility and also random numbers are generated to check the randomness. For image encryption, we suggest a nonlinear 3D chaos-based simple encryption scheme in which 3D chaos is employed for position and value transformation.

2. Representation of a multidirectional chaotic system in ABC

In this section, we represent the non-equilibrium point's multidirectional chaotic system in the ABC fractional derivative.

Definition 2.1. Let $X \in C^1(a,b)$ and $\gamma \in (0,1)$. The ABC fractional derivative with order γ may be found as follows:

$$ {}^{ABC}D_t^{\gamma} X(t) = \frac{g(\gamma)}{1-\gamma} \int_0^t \dot{X}(z) E_{\gamma}\left(\frac{-\gamma}{1-\gamma}(t-z)^{\gamma}\right) dz, \quad (1)$$

where $g(\gamma) = 1 - \gamma + \frac{\gamma}{\Gamma(\gamma)}$, and $E_{\gamma}[.]$ is the Mittag-Leffler function.

Definition 2.2. Let $X \in C^1(a,b)$ and $\gamma \in (0,1)$. The ABC fractional integral with order γ may be found as follows:

$$ {}^{ABC}I_t^{\gamma} X(t) = \frac{1-\gamma}{g(\gamma)} X(t) + \frac{\gamma}{g(\gamma)\Gamma(\gamma)} \int_0^t X(z)(t-z)^{\gamma-1} dz. \quad (2)$$

Now we consider a non-equilibrium point's multidirectional chaotic system under the ABC fractional operator described in [25]. The model consists of three differential equations, as shown below:

$$\begin{aligned} {}^{ABC}D_t^{\gamma} x(t) &= a\,\mathrm{Sign}(y(t)) + bz(t), \\ {}^{ABC}D_t^{\gamma} y(t) &= d + z(t), \\ {}^{ABC}D_t^{\gamma} z(t) &= -c\,x(t) - z(t), \end{aligned} \quad (3)$$

where a, b, c, d are fixed parameters, $x(t)$, $y(t)$, $z(t)$ are the system variables, and $(x(0), y(0), z(0)) = (0, 1, 0.1)$ are the initial states. $\mathrm{Sign}(y(t))$ denotes the signum function defined as:

$$ \mathrm{Sign}(y(t)) = \begin{cases} 1, & y(t) > 0, \\ 0, & y(t) = 0, \\ -1, & y(t) < 0. \end{cases} \quad (4)$$

The problem has attracted more attention recently due to the new interest and motivated structure of system (3). If one can master these parameters in a chaotic dynamic system, it is controllable, and it will lead to a modification of the behavior of the chaotic signals it generates. It is worth noting that the system under consideration contains three controllable parameters, which indicates that the resultant chaotic attractor may be transmitted on a 1D line, 2D lattice, and 3D grid. System (3) may be altered by adding three new controlled parameters $\eta, \omega,$ and κ.

$$\begin{aligned} {}^{ABC}D_t^{\gamma} x(t) &= a\,\mathrm{Sign}(y(t)+\eta) + b(z(t)+\kappa), \\ {}^{ABC}D_t^{\gamma} y(t) &= d + (z(t)+\kappa), \\ {}^{ABC}D_t^{\gamma} z(t) &= -c\,(x(t)+\omega) - (z(t)+\kappa). \end{aligned} \quad (5)$$

In the concept of the specific varieties of relevant values for the system parameters along with the Sign $y(t)$ function, system (3) has no equilibrium point (EP). Here, we have taken the value of the fixed parameters $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, which does not give any equilibrium point.

3. Numerical simulations

This part is devoted to simulated results of the multidirectional chaotic system under consideration in the current work. The numerical approaches provided here have been applied with fractional order γ. All the figures are created by provided numerical algorithms under the Atangana–Baleanu–Caputo fractional operators [7], where the chaotic dynamic performance is obvious in each graphic attained with γ. By setting $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, initial state $(0, 1, 0.1)$, and $\gamma = 0.99$, system (3) exhibits one-scroll chaotic signals. Figure 1(a–c) shows the phase plots of system (3). Figure 1(a) shows the phase plot of the $(x(t), y(t))$-plane, Figure 1(b) shows the phase plot of the

$(x(t), z(t))$-plane, and Figure 1(c) shows the phase plot of the $(y(t), z(t))$-plane.

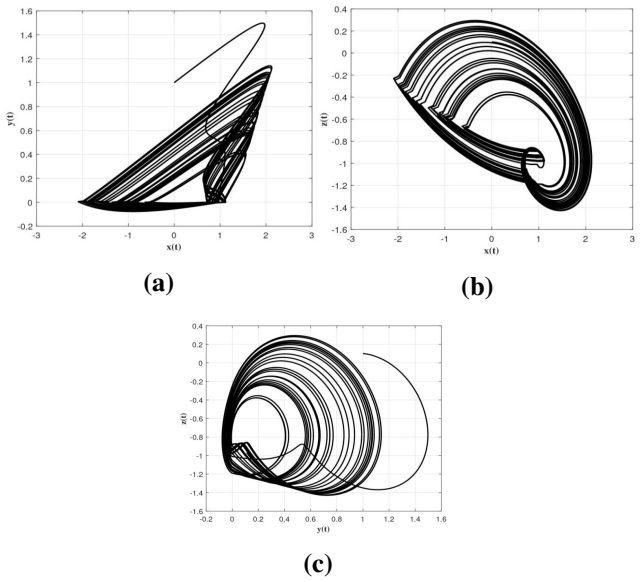


Figure 1. Phase plots of system (3): **(a)** $(x(t), y(t))$-plane, **(b)** $(x(t), z(t))$-plane, and **(c)** $(y(t), z(t))$-plane at fractional order $\gamma = 0.99$.

Behavior of the control parameters in the chaotic system

If one of the parameters of a nonlinear, dynamic chaotic system is the controller, then the divergence of the chaotic signals generated from it is enhanced. It is exciting to note that this system has inclusive magnetism and three control parameters, indicating that the calculating chaotic attractor can be scattered in a 1D line, 2D lattice, and 3D grid. By utilizing $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, initial state $(0, 1, 0.1)$, $\gamma = 0.99$, and the controlling parameters η, κ, ω in system (5), we get the following three cases of distribution of the chaotic signals.

Case A: Distribution of chaotic signals in a 1D line

By taking the control parameters $\eta = \kappa = 0$ and changing $\omega = (0, \pm 5)$, we get the line-distributed chaotic signals transmitted on the x-axis of the variables $(x(t), y(t))$ as presented in Figure 2(a). By taking the control parameters $\eta = \kappa = 0$ and changing $\omega = (0, \pm 5)$, we get the line-distributed chaotic signals transmitted on the x-axis of the variables $(x(t), z(t))$ as presented in Figure 2(b). By taking the control parameters $\kappa = \omega = 0$ and changing $\eta = (0, \pm 2)$, we get the line-distributed chaotic signals transmitted on the y-axis of the variables $(y(t), z(t))$ as presented in Figure 2(c). By taking the control parameters $\eta = \omega = 0$ and changing $\kappa = (0, \pm 3)$, we get the line-distributed chaotic signals transmitted on the z-axis of the variables $(z(t), y(t))$ as presented in Figure 2(d).

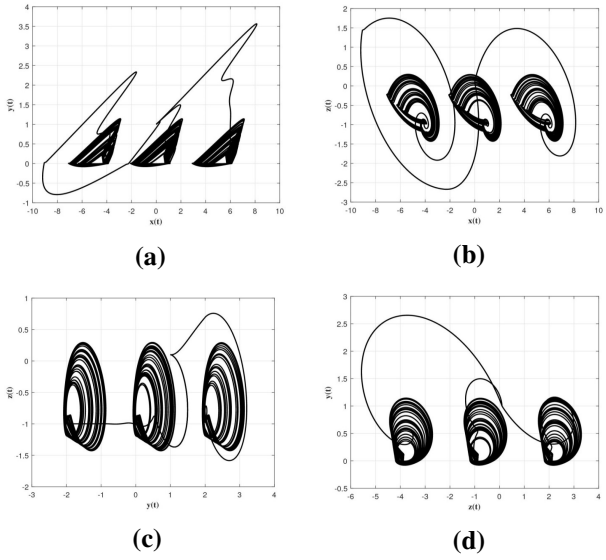
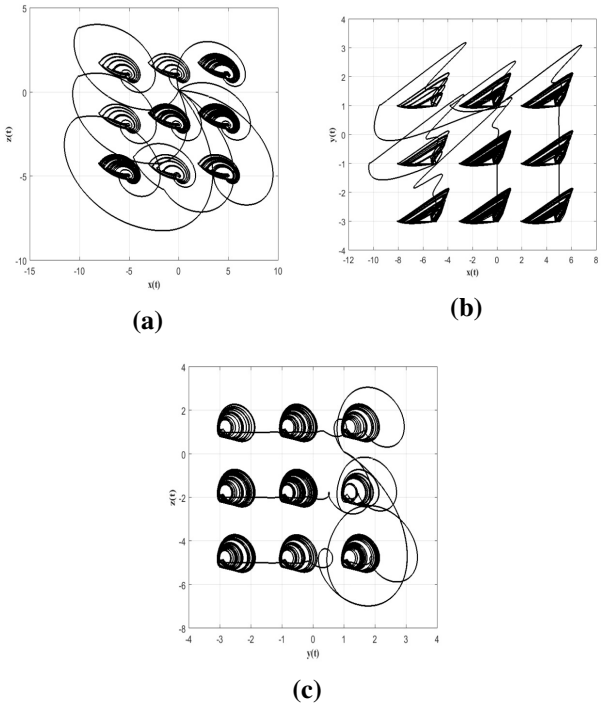


Figure 2. Phase plots of system (5): **(a)** $(x(t), y(t))$-plane, **(b)** $(x(t), z(t))$-plane, **(c)** $(y(t), z(t))$-plane, and **(d)** $(z(t), y(t))$-plane at fractional order $\gamma = 0.99$.

Case B: Distribution of chaotic signals in a 2D lattice

By taking the one control parameter $\eta = 0$ and changing two variables κ and ω simultaneously, we get the 2D-lattice distributed chaotic signals transmitted on the $(x(t), z(t))$-plane as presented in Figure 3(a). By taking the one control parameter $\kappa = 0$ and changing two variables η and ω simultaneously, we get the 2D-lattice distributed chaotic signals transmitted on the $(x(t), y(t))$-plane as presented in Figure 3(b). By taking the one control parameter $\omega = 0$ and changing two variables η and κ simultaneously, we get the 2D-lattice distributed chaotic signals transmitted on the $(y(t), z(t))$-plane as presented in Figure 3(c). All the control parameter values used in Figure 3(a–c) are tabulated in Table 1.



(a) **(b)** **(c)**

Figure 3. Phase plots of system (5): **(a)** $(x(t), y(t))$-plane, **(b)** $(x(t), z(t))$-plane, and **(c)** $(y(t), z(t))$-plane at fractional order $\gamma = 0.99$.

Table 1. Control parameter ω, κ, and η values used in Figure 4.

ω, κ, η	ω, κ, η	ω, κ, η
(1, 1, 0)	(1, 0, 1)	(0, 1, 1)
(6, 1, 0)	(-4, 0, 1)	(0, 3, 1)
(-4, 1, 0)	(6, 0, 1)	(0, -1, 1)
(1, 4, 0)	(1, 0, -1)	(0, 1, -2)
(1, -2, 0)	(1, 0, 3)	(0, 1, 4)
(6, 4, 0)	(-4, 0, -1)	(0, -1, -2)
(6, -2, 0)	(-4, 0, 3)	(0, -1, 4)
(-4, -2, 0)	(6, 0, 3)	(0, 3, 4)
(-4, 4, 0)	(6, 0, -1)	(0, 3, -2)

Case C: Distribution of chaotic signals in a 3D grid

By changing all the control parameters simultaneously, we induce complex and unpredictable behavior in the system, leading to the generation of 3D grid-distributed chaotic signals transmitted on the $(x(t), y(t), z(t))$-plane, as represented in Figure 4. This chaotic signal pattern results from the intricate interplay of variables and their sensitivity to parameter variations, demonstrating the nonlinear dynamics and emergent phenomena inherent in the system. The $(x(t), y(t), z(t))$-plane serves as the canvas for this chaotic transmission, revealing the intricate structure and dynamics that emerge from the underlying mathematical equations.

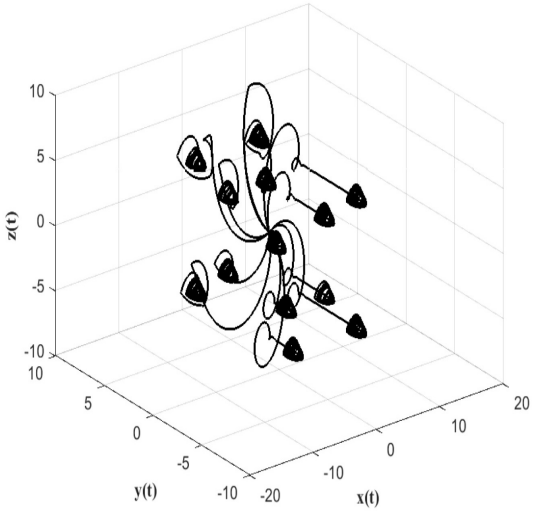
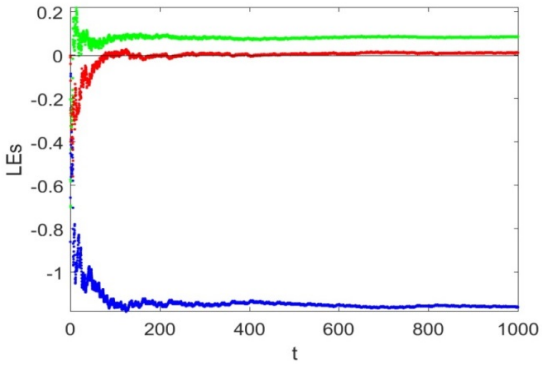


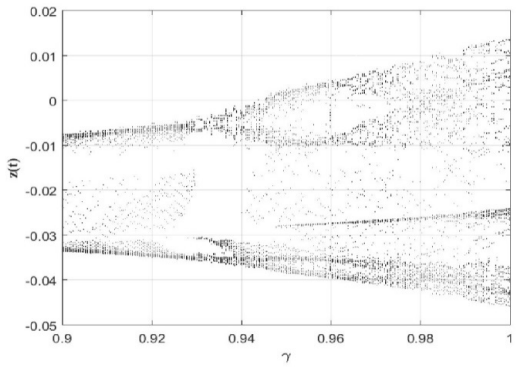
Figure 4. 3D grid plot of system (5) at $\gamma = 0.99$.

4. Dynamical properties of a multidirectional chaotic system

According to the theory, neighboring chaotic attractor routes have shown a propensity toward reciprocal expansion, and Lyapunov exponents (LEs) are a mathematical representation of the mutual repulsion and attraction that exists between route pairs. When determining whether or not a system is chaotic, the LEs of the system are a key characteristic to look at. The calculated LEs of system (3) are $L_1 = 0.0859$, $L_2 = 0.0128$, $L_3 = -1.1619$ at parameters $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, initial state $(0, 1, 0.1)$, and fractional order $\gamma = 0.99$. Graphically, LEs are presented in Figure 5(a).



(a)



(b)

Figure 5. **(a)** Lyapunov exponents (LEs) and **(b)** bifurcation plot at fractional order $\gamma = 0.99$.

The Kaplan-Yorke dimension [26], which depicts attractor convolution, is defined as:

$$D_{KY} = j + \frac{1}{|L_{j+1}|}\sum_{i=1}^{j} L_i, \tag{6}$$

where j is the largest integer satisfying $\sum_{i=1}^{j} L_i \geq 0$ and $\sum_{i=1}^{j+1} L_i \leq 0$. The Kaplan-Yorke dimension of system (3) for $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, initial state $(0, 1, 0.1)$, and fractional order $\gamma = 0.99$ is $D_{KY} = 2.08495$, which shows that the system has a fractal dimension and it has been proved to be chaotic.

Bifurcation in chaotic systems refers to the occurrence of qualitative variations in the chaotic performance of a system as a parameter or fractional order is diverse. The system variable $z(t)$ is plotted with fractional order γ. Figure 5(b) clearly shows that system (3) is chaotic under the ABC fractional derivative with order $\gamma = 0.99$.

5. Circuit implementation

The circuit implementation of the nonlinear chaotic dynamical system not only confirms the correctness of the theoretical model but also makes a notable contribution to the field of nonlinear dynamics through its potential for practical, chaos-based applications. The design serves to bridge the gap between numerical simulations and physical realization, ensuring consistency between mathematical analysis and circuital execution.

The Laplace transform and an approximate transfer function of the ABC fractional derivative

In this section, we obtain the transfer function approximation for the ABC fractional derivative. The Laplace transform of the ABC fractional derivative is given as:

$$L\left\{{}^{ABC}D_t^{\gamma}\left(f(t)\right)\right\} = \frac{g(\gamma)F(s)s^{\gamma} - s^{\gamma-1}f(0)}{(1-\gamma)\left(s^{\gamma} + \frac{\gamma}{(1-\gamma)}\right)}, \tag{7}$$

where $g(\gamma) = 1 - \gamma + \frac{\gamma}{\Gamma(\gamma)}$ and $f(0) = 0$. We consider an approximate fractional-order transfer function, defined in [27], for $s^{-0.99}$ and given as:

$$\frac{1}{s^{0.99}} = \frac{1.3537(s + 1.123 \times 10^8)}{(s + 1.417 \times 10^8)(s + 0.01123)}. \tag{8}$$

Replacing Eq (8) in Eq (7), at the resultant, we obtained Eq (9):

$$\frac{1}{s^{0.99}} = \frac{0.0100581(s + 106.222)(s + 1.417 \times 10^8)}{(s + 0.01123)(s + 1.417 \times 10^8)}. \tag{9}$$

$$H_{0.99}(s) = R_0 + \frac{R_a}{sR_aC_a + 1} + \frac{R_b}{sR_bC_b + 1}. \tag{10}$$

The following is the transfer function between nodes A and B:

We set $C_0 = 1nF$. Since $H(s) = s^{-0.99}$, at $R_0 = 0.0100581\Omega$, we can reach a fractional capacitor as shown in Figure 6, where $R_a = 95127.3M\Omega$, $C_a = 0.936084nF$, $R_b = 1.97371\Omega$ and $C_b = 0.357559nF$.

For the sake of accuracy and simplicity, we have designed an analog circuit using cooperative components, including operational amplifiers (TL082CD), fractional-order capacitors, resistors, and a DC source. The circuit

consists of eight operational amplifiers, fourteen resistors, three fractional-order capacitors, and a -0.8V DC source, along with power supplies. The designed circuit is presented in Figure 7 and its oscilloscopic results are presented in Figure 8(a–c). Comparing Figure 1(a–c) and Figure 8(a–c), it is evident that the oscilloscopic results closely match the numerical results.

$$\begin{aligned} D_t^{0.99} x(t) &= \frac{a\,\mathrm{Sign}(y(t))}{R_1} + \frac{b\,z(t)}{R_2}, \\ D_t^{0.99} y(t) &= \frac{d}{R_3} + \frac{z(t)}{R_4}, \\ D_t^{0.99} z(t) &= \frac{-c\,x(t)}{R_5} - \frac{z(t)}{R_6}. \end{aligned} \tag{11}$$

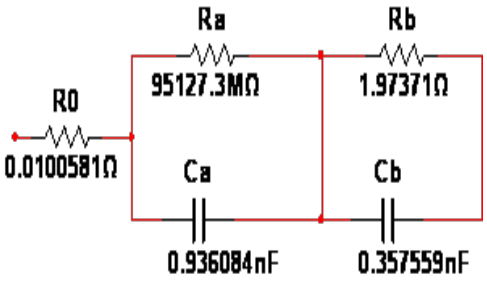


Figure 6. Fractional capacitors of the ABC fractional derivative.

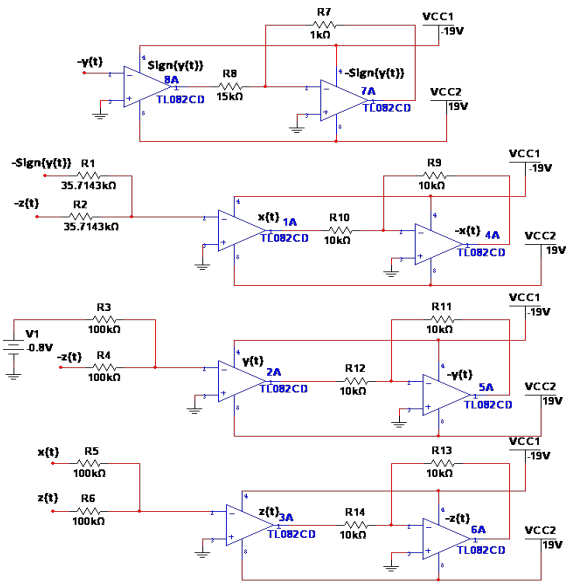


Figure 7. Analog circuit of system (3).

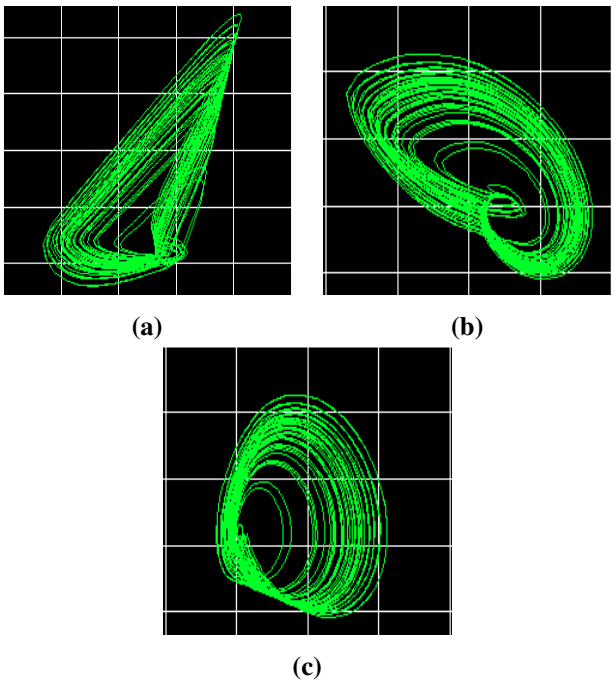


Figure 8. Oscilloscopic results of system (3): **(a)** $(x(t), y(t))$-plane, **(b)** $(x(t), z(t))$-plane, and **(c)** $(y(t), z(t))$-plane at fractional order $\gamma = 0.99$.

6. Application in random number generators (RNGs), image encryption, statistical analysis, and differential attacks

6.1. Random number generators (RNGs)

In the field of secure communication and data enhancement, the chaos-based, random number generator plays an important role because its randomness is potent enough to ensure a safe presentation. National Institute of standards and Technology (NIST) statistical test is effective to implement the conformation of the randomness of the chaotic sequences. To generate the random number, system (3) is numerically simulated by inserting parameter values and an initial condition. The generated numerical values were transformed to 32-bit binary values and then transformed to 10 least significant bits (LSBs) from each value. After that, these LSBs are arranged in an array for each variable for large data and then passed to the NIST test suite to check randomness. The randomness level, if P-values are greater than 0.001, calculates the adoption of the hypothesis concept of randomness for

the listed arrangement. P-values of $x(t), y(t)$, and $z(t)$ are recorded in Table 2, which clearly shows that all the P-values are successful and larger than 0.001, indicating good randomness is found in the chaotic system.

Table 2. P-values for system (3) at fractional order $\gamma = 0.99$.

Statistical test	P-Value			Results
	$x(t)$	$y(t)$	$z(t)$	
Monobit	0.9186	0.1220	0.6839	✓
Block	0.9784	0.1699	0.5691	✓
Runs	0.2486	0.7563	0.2091	✓
Longest Runs	0.3706	0.0451	0.2083	✓
Rank	0.2427	0.2358	0.4707	✓
Spectral	0.0691	0.2135	0.1496	✓
Non-overlapping	0.5779	0.1414	0.8625	✓
Overlapping	0.4139	0.1079	0.1942	✓
Maurer's	0.7041	0.3155	0.6724	✓
Entropy	0.0778	0.7443	0.8472	✓
Serial 1	0.6353	0.7833	0.2869	✓
Serial 2	0.7639	0.9694	0.0111	✓
Complexity	0.5833	0.8735	0.1893	✓
Cumulative Sums	0.7760	0.1370	0.6744	✓
Excursions	0.9987	0.9520	0.6077	✓
Variant	0.3768	0.7230	0.6812	✓

6.2. *Image encryption*

Chaos-based image encryption is a good solution because it is sensitive to the conditions at the beginning, does not repeat itself, and does not converge. Such encryption techniques offer greater security and resilience to cryptographic assaults by harnessing chaotic behavior, making them suited for securing sensitive visual information. Also, chaos-based algorithms provide a large key space and may be computationally inexpensive, making them an appealing alternative for image encryption applications. The entire encryption procedure is explained step by step and also shown in Figure 9. The pseudo-codes for the image encryption and decryption processes are presented in Tables 3 and 4, respectively.

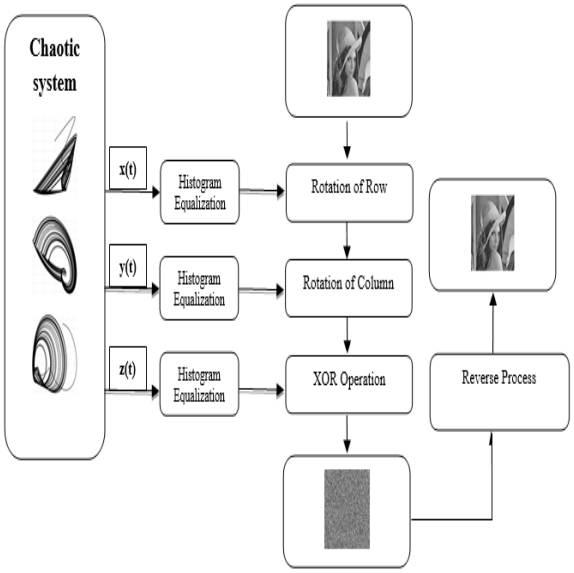


Figure 9. The encryption technique using the multidirectional chaotic system under the ABC.

Table 3. Pseudo-code for image decryption using the proposed system.

Step	Description
1)	**Read encrypted image:** Load the encrypted image and get row and column.
2)	**XOR decryption:** Flatten the encrypted image. XOR with the same chaotic sequence $m(j)$ used in the encryption. Reshape into a 2D matrix.
3)	**Reverse column rotation:** For each column: if $l(j)$ is even → shift column down by $l(j)$; otherwise, shift column up by $l(j)$.
4)	**Reverse row rotation:** For each row: if $k(j)$ is even → shift row left by $k(j)$; otherwise, shift right by $k(j)$.
5)	Reshape back into 2D as the decrypted image.

Table 4. Pseudo-code for image encryption using the proposed system.

Step	Description
1)	**Initialize parameters:** Set initial values $x(0), y(0), z(0)$ and constants a, b, c, d. Define image dimensions and iterations (e.g., 70,000), where $X = [x, y, z]$.
2)	**Generate chaotic sequences:** Iterate the system $X(i+1)$ using the proposed sysrem for $i = 1$ to 70,000.
3)	**Histogram equalization:** Normalize chaotic values using: $X = \text{ceil}(\text{mod}(X \times 100000, 256))$.
4)	**Read and convert image:** Convert input image to grayscale and get its dimensions (rows, columns).
5)	**Generate rotation keys:** Use sequences x, y, z to generate $k(j), l(j), m(j)$.
6)	**Row-wise rotation:** If $k(j)$ is even, shift row right by $k(j)$; otherwise, shift left.
7)	**Column-wise rotation:** If $l(j)$ is even, shift column up; otherwise, shift down.
8)	**XOR encryption:** Flatten image to 1D and XOR each pixel with corresponding $m(j)$.
9)	**Reshape:** Convert 1D XOR array back to 2D as the encrypted image.

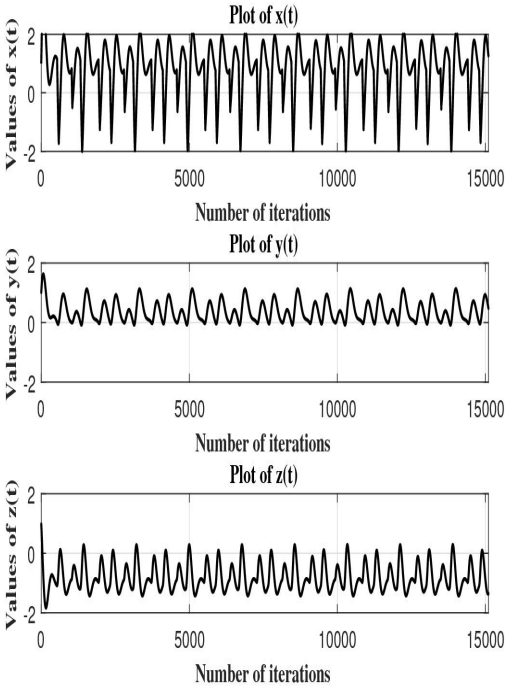


Figure 10. Time series plots of $x(t)$, $y(t)$, and $z(t)$ of system (3) at $\gamma = 0.99$.

6.2.1. Multidirectional chaotic system encryption

Equation (3) exhibits chaotic performance for the parameter values $(a, b, c, d) = (2.8, 2.8, 1, 0.8)$, initial state $(0, 1, 0.1)$, and fractional order $\gamma = 0.99$ under the ABC fractional derivative. Figure 10 shows the generated time series chaotic structures of $x(t)$, $y(t)$, and $z(t)$, respectively.

6.2.2. Equalization of the histogram

We can easily observe that the histogram of $x(t)$, $y(t)$, and $z(t)$ has a non-uniform distribution by looking at Figure 11. We need to equalize the histogram in order to achieve greater levels of security. If a grayscale image has the sizes $M \times N$, where N is the number of columns and M is the number of rows, then the following formulas may be used to determine whether or not the histogram is equal:

$$\begin{aligned} x(t) &= (I(x(t) \times N2)) \mod N, \\ y(t) &= (I(y(t) \times N4)) \mod M, \\ z(t) &= (I(z(t) \times N6)) \mod 256, \end{aligned} \tag{12}$$

where I indicates the integer and $N2$, $N4$, and $N6$ are huge random numbers, usually more than 10,000. For instance, we take $N2 = N4 = N6 = 100,000$. The equalized histogram is shown in Figure 12.

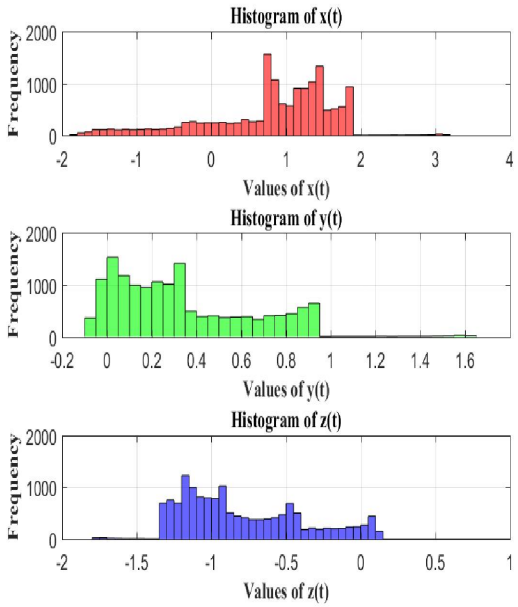


Figure 11. Histogram plots of $x(t)$, $y(t)$, and $z(t)$ of system (3) at $\gamma = 0.99$.

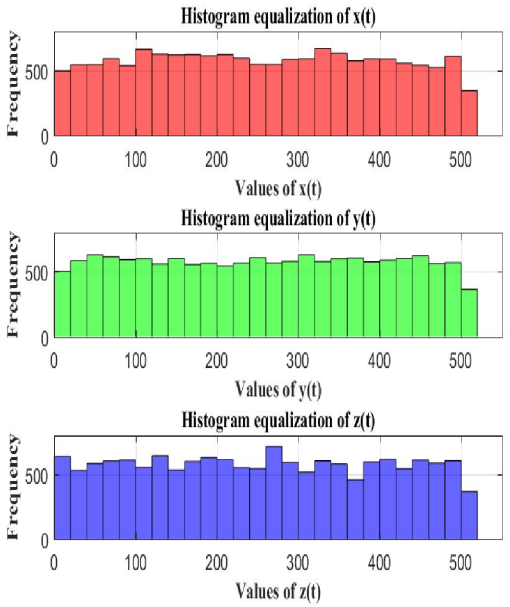


Figure 12. Equalized histogram plots $x(t)$, $y(t)$, and $z(t)$ of system (3) at $\gamma = 0.99$.

6.2.3. Rotation of a row

As part of the task of pixel transformation, we used a technique called the rotation of a row column [15]. This technique is the same as a padlock on a briefcase; the only difference is the direction. For rotation, we take an image in a grayscale with size $M \times N$, and we will need to choose M numbers from the chaotic sequence. Firstly, a very big random number, $N1$, is generated. Next, M numbers of chaotic values are selected. When the value is even, $N1$ and the rows are rotated based on the need to shift $x(t)$ in Eq 3. If the value is even, we rotate left, and when the chaotic value is odd, we rotate right. This is done for increased safety.

6.2.4. Rotation of a column

The process of rotating a column is identical to that of rotating a row. In order to rotate a row in a grayscale with dimensions of $M \times N$, we will need to choose an appropriate number of chaotic sequences. To begin, a very big random number $N3$ is generated. Next, N numbers of chaos are chosen, beginning with the index $N3$, and each column is rotated based on the value of the chaos variable $y(t)$ of Eq (3). When the chaotic value is even, we rotate up, and when it is odd, we rotate down, so that we may improve the level of security. After the rows and columns have been rotated, the image will be encrypted; nevertheless, the histogram will remain intact, which leaves it vulnerable to a histogram attack. We need one more step that will modify the pixel value of the image in order to oppose this attack.

6.2.5. XOR operation

The XOR operation is the final stage in this encryption procedure. The XOR operation will transform the pixel value to a new value, and this change cannot be undone even with knowledge of the chaos key. The first thing that we do is produce a very huge random number called $N5$, and then we turn $M \times N$ dimension into a $1 \times MN$ row vector form. Following that, we XOR the chaos (beginning at index $N5$) and the row-column shifted image, and then eventually we have the encrypted image.

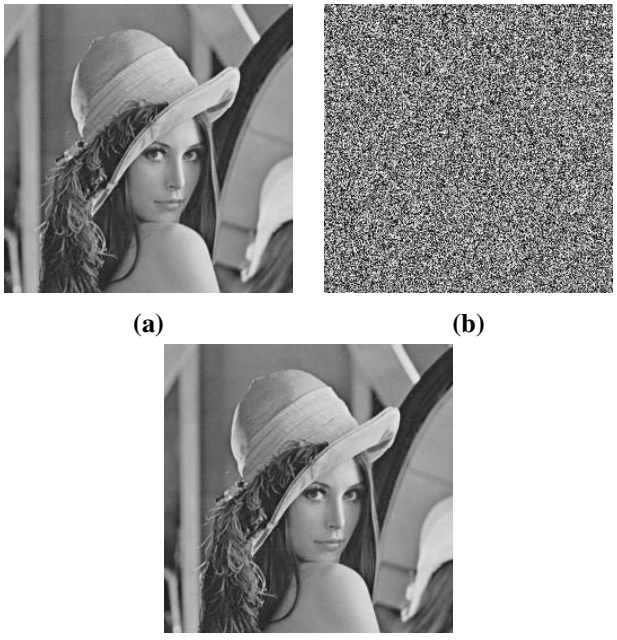
In order to simulate the results of our encryption process, we make use of a Lena image that has a resolution of 256 pixels on each side. The experiment has been carried out

in order to demonstrate that the algorithm is reliable. We establish an image with a size of 256×256, and set its initial keys as follows:

$$(x(0), y(0), z(0)) = (0, 1, 0.1), N1 = 5000, N3 = 6000,$$
$$N5 = 7000, N2 = N4 = N6 = 100000,$$
$$(a, b, c, d) = (2.8, 2.8, 1, 0.8).$$

The encryption can be seen in Figure 13(a–c). There is an original Lena image, an encrypted version of the original Lena, and the decrypted version of the original Lena. It is clear from the figure that the pixels have been dispersed correctly and seem to be an entirely different image from the one they were originally from.

Figure 14(a–c) shows the histogram of the original Lena image, an encrypted version of the original Lena, and the decrypted version of the original Lena, respectively. The histogram of the encrypted image reveals that the pixel values of each are scattered evenly throughout the board, which means that it does not contain any information that may be used by the intruder [16].



(a) **(b)**

(c)

Figure 13. Lena.

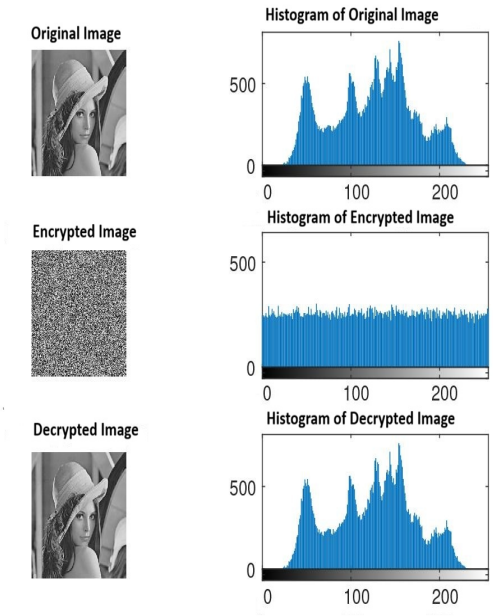


Figure 14. Histograms of Lena.

6.3. Statistical analysis and differential attacks

To assess the security and performance of the proposed 3D chaos-based image encryption scheme, several statistical and differential attack analyses were performed. These metrics evaluate the scheme's ability to obscure image features, resist cryptanalysis, and maintain robustness against slight variations in input. These include:

6.3.1. Mean square error

Mean square error (MSE) is a standard value for evaluating the quality of image encryption and decryption processes [28]. It calculates the ordinary squared difference between the original and decrypted image pixel values. A low MSE value is desired for excellent encryption and decryption. A low MSE means that the decrypted image closely matches the original image with little distortion or information loss. Mathematically, it can be written as:

$$MSE(I_1, I_2) = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I_1(i, j) - I_2(i, j))^2. \quad (13)$$

Mean square error between decrypted and the original Lena image is 0, which shows that the decrypted image is the same as the original Lena image.

6.3.2. Peak signal-to-noise ratio (PSNR)

A high peak signal-to-noise ratio (PSNR) is often needed for excellent encryption and decryption. The PSNR is a popular statistic for evaluating the quality of image encryption and decryption processes. A high PSNR value implies that the decrypted image is almost identical to the original image, with little distortion or loss of information. It demonstrates a high degree of resemblance between the two images and indicates that the encryption and decryption methods successfully retained the image's fidelity and integrity throughout the process.

$$PSNR = 10\log_{10}\left(\frac{(2^N-1)^2}{MSE}\right). \tag{14}$$

The calculated PSNR value is infinity, which shows that the decrypted image is the same as the original Lena image.

6.3.3. Entropy

Entropy is a property that measures the continuous dispersal of the grey pixel level in an image. It is also responsible for defining the degree of uncertainty and unpredictability that exists within the data. The mathematical definition of it is as follows:

$$H(S) = -\sum_{i=0}^{2^n-1} P(S_i)\log\left(\frac{1}{P(S_i)}\right). \tag{15}$$

The calculated entropy values of the images are shown in Table 5. We can see that the entropy of the encrypted image is close to the ideal value of 8, which shows that the encryption is strong.

Table 5. Correlation coefficient and entropy analysis of the Lena image.

Position	Correlation Coefficient		Entropy	
	Original	Encrypted	Original	Encrypted
Horizontal	0.9717	-0.0080	7.4612	7.9562
Vertical	0.9076	-0.0034		

6.3.4. Correlation

To estimate the encryption worth of the planned technique, we employ the following equation to calculate correlation coefficients between vertically and horizontally adjacent pixels in the encrypted image. This allows us to analyze the relationships between neighboring pixels and assess the effectiveness of the encryption process.

$$C_r = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{N}(y_i-\bar{y})^2}}. \tag{16}$$

The outcomes are shown in Table 5, and they indicate that the suggested approach did a very excellent job of randomizing the pixels. The correlation for a 256 × 256 Lena image is shown in Figure 15(a–d). Figure 15(a) is the vertical correlation and Figure 15(b) is the horizontal correlation of the original Lena image. Figure 15(c) is the vertical correlation and Figure 15(d) is the horizontal correlation of the encrypted Lena image. Figure 15(a–d) demonstrates that following encryption, pixel values have been evenly dispersed, which has the influence of lowering the correlation value. This occurs despite the fact that the values of pixels in the original image are strongly correlated to those of neighboring pixels and are concentrated toward the image's center.

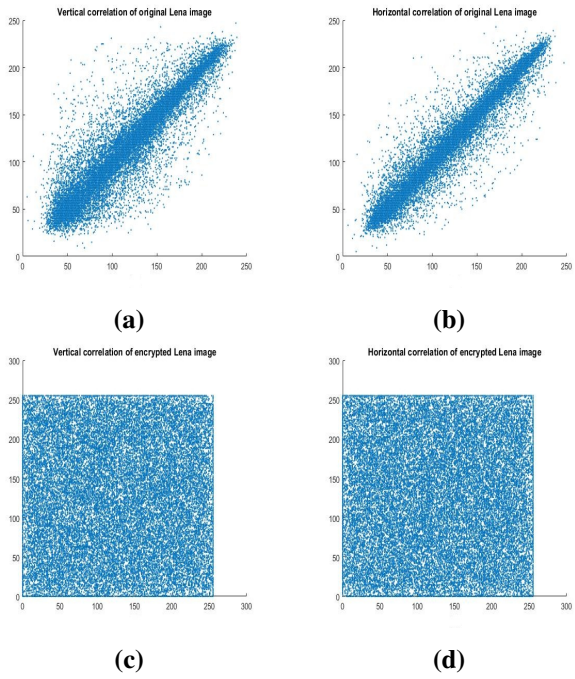


Figure 15. Correlation of Lena images.

6.3.5. Distance analysis

Through image distance evaluations, we aimed to assess the security of our encryption technique. By observing an increase in the squared Euclidean distance values between the original and encrypted images, we found evidence of significant distinctions. These analyses provide compelling evidence that the encrypted images are entirely dissimilar from their corresponding original image. The evaluated image's distance is 3397.8.

6.3.6. Chi-square test

To evaluate the uniformity of the encrypted image histogram, a Chi-square goodness-of-fit test was applied. This statistical test determines whether the distribution of pixel intensities in the encrypted image deviates significantly from a uniform distribution. A uniform histogram is a key indicator of strong encryption, as it suggests high randomness and resistance to statistical attacks. In our analysis, the Chi-square statistic was calculated to be 241.66, with an associated p-value of 0.7163. Since the p-value is significantly greater than common significance levels (e.g., 0.05), we fail to reject the null hypothesis. This indicates that there is no statistically significant difference between the observed and expected pixel distributions. Therefore, we conclude that the histogram of the encrypted image is uniform, which confirms the effectiveness of the encryption scheme in terms of statistical uniformity.

6.3.7. Number of pixel change rate (NPCR)

The number of pixel change rate (NPCR) measures the percentage of different pixel values between two encrypted images that differ by only a single pixel in the original image. It is defined as:

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \tag{17}$$

where:

$$D(i, j) = \begin{cases} 1, & \text{if } C_1(i, j) \neq C_2(i, j), \\ 0, & \text{otherwise.} \end{cases}$$

Here, $C_1(i, j)$ and $C_2(i, j)$ represent the pixel values at position (i, j) in the two encrypted images, and $M \times N$ is the total number of pixels. The calculated value of the NPCR is 99.6414, indicating that the proposed encryption algorithm has excellent sensitivity to small changes in the plaintext image, demonstrating strong resistance to differential attacks.

6.3.8. Unified average changing intensity (UACI)

The unified average changing intensity (UACI) measures the average intensity difference between two encrypted images generated from slightly different plaintext images. It is calculated as:

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%, \tag{18}$$

where $C_1(i, j)$ and $C_2(i, j)$ are the pixel values of the two encrypted images at position (i, j), and 255 is the maximum gray level value for an 8-bit image. The calculated UACI value is 33.4719, which is very good and falls within the ideal range for image encryption.

7. Conclusions

A unique, three-dimensional, non-equilibrium-point, multidirectional chaotic system has been studied in this article under the ABC fractional operator. We simulated fractional-order numerical solutions to study the multidirectional chaotic dynamical system's more sophisticated behavior. A single exceptional characteristic is that the machine has a modest algebraic structure, comprising the grading terms of a continuous and signum function, but without the square and complex non-linearity. This is the simplest in comparison to other chaotic, non-equilibrium systems. At the moment, it is possible that this system has three variable factors, and by presenting three additional managed constants, the chaotic attractor has already been identified in the x-axis, y-axis, z-axis, $(x(t), y(t))-$plane, $(x(t), z(t))-$plane, $(y(t), z(t))-$plane, and $(x(t), y(t), z(t))$ transmitted main grid. A basic analog circuit with fewer electronic components was also built to evaluate the circuit capability of the contemplated system. Analog circuit testing substantiates the numerical results, making the system more usable. To conclude, the recording properties of the chaotic series produced by the analog

circuit are also verified using the NIST test package. The NIST standards have been met by the randomness that has been tested. As a result, it may be considered an appropriate viewpoint for a number of chaos-based executive applications. We employed a straightforward encryption technique for images, utilizing 3D chaos and combining position transformation and value transformation methods. This approach provides a robust encryption scheme by shuffling pixel positions and modifying pixel values using the chaotic behavior of the system. To evaluate resistance against differential attacks, the scheme was tested using standard NPCR and UACI metrics. The results, NPCR 99.6414 and UACI 33.4719, demonstrate excellent sensitivity to small changes in the input image, confirming the robustness of the encryption method.

Use of Generative-AI tools declaration

The authors declare they have not used artificial intelligence (AI) tools in this study.

Conflict of interest

The authors declare that there are no conflicts of interest in this paper.

References

1. B. Wang, J. Liu, Y. Deng, M. O. Alassafi, F. E. Alsaadi, H. Jahanshahi, et al., Intelligent parameter identification and prediction of variable time fractional derivative and application in a symmetric chaotic financial system, *Chaos Soliton. Fract.*, **154** (2022), 111590. https://doi.org/10.1016/j.chaos.2021.111590
2. N. A. Khan, T. Hameed, M. A. Qureshi, S. Akbar, A. K. Alzahrani, Emulate the chaotic flows of fractional jerk system to scramble the sound and image memo with circuit execution, *Phys. Scr.*, **95** (2020), 065217. https://doi.org/10.1088/1402-4896/ab8581
3. I. Podlubny, A. Chechkin, T. Skovranek, Y. Chen, B. M. Vinagre Jara, Matrix approach to discrete fractional calculus II: partial fractional differential equations, *J. Comput. Phys.*, **228** (2009), 3137–3153. https://doi.org/10.1016/j.jcp.2009.01.014
4. X. Li, Y. L. Wang, Numerical simulation of the fractional-order Rössler chaotic systems with Grünwald-Letnikov fractional derivative, *Fractals*, **30** (2022), 2240229. https://doi.org/10.1142/s0218348x22402290
5. R. S. E. Alatwi, A. F. Aljohani, A. Ebaid, H. K. Al-Jeaid, Two analytical techniques for fractional differential equations with harmonic terms via the Riemann-Liouville definition, *Mathematics*, **10** (2022), 4564. https://doi.org/10.3390/math10234564
6. S. Deepika, P. Veeresha, Dynamics of chaotic waterwheel model with the asymmetric flow within the frame of Caputo fractional operator, *Chaos Soliton. Fract.*, **169** (2023), 113298. https://doi.org/10.1016/j.chaos.2023.113298
7. M. Toufik, A. Atangana, New numerical approximation of fractional derivative with non-local and non-singular kernel: application to chaotic models, *Eur. Phys. J. Plus*, **132** (2017), 1–16. https://doi.org/10.1140/epjp/i2017-11717-0
8. X. Lin, Y. Wang, J. Wang, W. Zeng, Dynamic analysis and adaptive modified projective synchronization for systems with Atangana-Baleanu-Caputo derivative: a financial model with nonconstant demand elasticity, *Chaos Soliton. Fract.*, **160** (2022), 112269. https://doi.org/10.1016/j.chaos.2022.112269
9. S. Bhalekar, *Current developments in mathematical sciences: frontiers in fractional calculus*, Bentham Science Publishers, 2018. https://doi.org/10.2174/9781681085999180101
10. J. Hristov, On the Atangana-Baleanu derivative and its relation to the fading memory concept: the diffusion equation formulation, In: *Fractional derivatives with Mittag-Leffler kernel: trends and applications in science and engineering*, 2019, 175–193. https://doi.org/10.1007/978-3-030-11662-0_11
11. J. Čermák, L. Nechvátal, Local bifurcations and chaos in the fractional Rössler system, *Int. J. Bifurcat. Chaos*, **28** (2018), 1850098. https://doi.org/10.1142/S0218127418500980
12. S. S. Hassan, M. P. Reddy, R. K. Rout, Dynamics of the modified n-degree Lorenz system, *Appl. Math. Nonlinear Sci.*, **4** (2019), 315–330. https://doi.org/10.2478/AMNS.2019.2.00028

13. B. Chen, Y. Liu, Z. Wei, C. Feng, New insights into a chaotic system with only a Lyapunov stable equilibrium, *Math. Methods Appl. Sci.*, **43** (2020), 9262–9279. https://doi.org/10.1002/mma.6619
14. B. Zhang, X. Shu, *Fractional-order electrical circuit Theory*, Singapore: Springer, 2022. https://doi.org/10.1007/978-981-16-2822-1
15. M. B. Hossain, M. T. Rahman, A. S. Rahman, S. Islam, A new approach of image encryption using 3D chaotic map to enhance security of multimedia component, *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, IEEE, 2014. https://doi.org/10.1109/ICIEV.2014.6850856
16. S. Xu, X. Wang, X. Ye, A new fractional-order chaos system of Hopfield neural network and its application in image encryption, *Chaos Soliton. Fract.*, **157** (2022), 111889. https://doi.org/10.1016/j.chaos.2022.111889
17. P. V. Deshmukh, A. S. Kapse, V. M. Thakare, A. S. Kapse, An effective high-level capacity reversible data hiding in encrypted images, *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, IEEE, 2022. https://doi.org/10.1109/ICAIS53314.2022.9742887
18. M. Shahzad, V. T. Pham, M. A. Ahmad, S. Jafari, F. Hadaeghi, Synchronization and circuit design of a chaotic system with coexisting hidden attractors, *Eur. Phys. J. Spec. Top.*, **224** (2015), 1637–1652. https://doi.org/10.1140/epjst/e2015-02485-8
19. V. T. Pham, C. Volos, S. Jafari, T. Kapitaniak, Coexistence of hidden chaotic attractors in a novel no-equilibrium system, *Nonlinear Dyn.*, **87** (2017), 2001–2010. https://doi.org/10.1007/s11071-016-3170-x
20. Z. Wang, A. Akgul, V. T. Pham, S. Jafari, Chaos-based application of a novel no-equilibrium chaotic system with coexisting attractors, *Nonlinear Dyn.*, **89** (2017), 1877–1887. https://doi.org/10.1007/s11071-017-3558-2
21. S. Zhang, Y. Zeng, A simple Jerk-like system without equilibrium: asymmetric coexisting hidden attractors, bursting oscillation and double full Feigenbaum remerging trees, *Chaos Soliton. Fract.*, **120** (2019), 25–40. https://doi.org/10.1016/j.chaos.2018.12.036
22. S. Ullah, X. Liu, A. Waheed, S. Zhang, An efficient construction of S-box based on the fractional-order Rabinovich–Fabrikant chaotic system, *Integration*, **94** (2024), 102099. https://doi.org/10.1016/j.vlsi.2023.102099
23. S. Ullah, X. Liu, A. Waheed, S. Zhang, S-box using fractional-order 4D hyperchaotic system and its application to RSA cryptosystem-based color image encryption, *Comput. Stand. Inter.*, **103980** (2025). https://doi.org/10.1016/j.csi.2025.103980
24. S. Ullah, X. Liu, A. Waheed, S. Zhang, S-boxes on the combined dynamics of fractional order chaotic systems and their application to provably secure image encryption, *Multimed. Tools Appl.*, **84** (2025), 44145–44181. https://doi.org/10.1007/s11042-025-20882-3
25. S. Zhang, X. Wang, Z. Zeng, A simple no-equilibrium chaotic system with only one signum function for generating multidirectional variable hidden attractors and its hardware implementation, *Chaos*, **30** (2020), 053129. https://doi.org/10.1063/5.0008875
26. N. A. Khan, S. Akbar, T. Hameed, M. A. Qureshi, Stumped nature hyperjerk system with fractional order and exponential nonlinearity: analog simulation, bifurcation analysis and cryptographic applications, *Integration*, **79** (2021), 73–93. https://doi.org/10.1016/j.vlsi.2021.03.006
27. I. Petráš, Control of fractional-order chaotic systems, In: *Fractional-order nonlinear systems*, Springer, 2011. https://doi.org/10.1007/978-3-642-18101-6_6
28. P. V. Deshmukh, A. S. Kapse, V. Thakare, A. S. Kapse, An effective high-level capacity reversible data hiding in encrypted images, *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, IEEE, 2022. https://doi.org/10.1109/ICAIS53314.2022.9742887

AIMS Press