Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 8148831, 18 pages
https://doi.org/10.1155/2022/8148831

Research Article

On Discrete Fractional Complex Gaussian Map: Fractal Analysis, Julia Sets Control, and Encryption Application

Amr Elsonbaty[1,2] **A. Elsadany,**[1,3] **and Fatma Kamal**[2]

[1]*Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia*
[2]*Mathematics and Engineering Physics Department, Faculty of Engineering, Mansoura University, P.O. 35516, Mansoura, Egypt*
[3]*Department of Basic Science, Faculty of Computers and Informatics, Suez Canal University, Ismailia, Egypt*

Correspondence should be addressed to Amr Elsonbaty; sonbaty2010@gmail.com

Received 16 December 2021; Revised 17 February 2022; Accepted 7 March 2022; Published 19 April 2022

Academic Editor: Amin Jajarmi

This work is devoted to present a generalized complex discrete fractional Gaussian map. Analytical and numerical analyses of the proposed map are conducted. The dynamical behaviors and stability of fixed points of the map are explored. The existence of fractal Mandelbrot and Julia sets is examined along with the corresponding fractal characteristics. The influences of the key parameters of the map and fractional order are examined. Moreover, nonlinear controllers are designed in the complex domain to control Julia sets generated by the map or to achieve synchronization between two Julia sets in master/slave configuration. Numerical simulations are provided to attain a deep understanding of nonlinear behaviors of the proposed map. Then, a suggested efficient chaos-based encryption technique is introduced by integrating the complicated dynamical behavior and fractal sets of the proposed map with the pseudo-chaos generated from the modified lemniscate hyperchaotic map.

1. Introduction

Mathematical models are used to describe and understand the interesting behaviors of nonlinear systems, which arise in different disciplines of science. There are a plethora of mathematical tools, which have proved their efficacy in mathematical modeling of biological, physical, engineering, economic, and natural systems. Among these tools, the differential equations, difference equations, and statistical methods have attracted a considerable interest [1–5].

However, when dealing with systems with memory, that is, the associated rate of changes depends on the past values of state variables in addition to the present values, the conventional continuous-time differential equation and discrete-time maps cannot describe these systems properly. To address this issue, mathematicians and engineers employ fractional calculus to formulate nonlocal differential operators, which are necessary to study systems with memory. Firstly, they focused on the fractional-order differential equations (FDEs) for the past two decades. The electric circuits, fluid mechanics, electromagnetics, immune systems, nanofluids, epidemics, and biological and financial systems are only examples of the fields, where FDEs are of great importance [6–13]. There are a few definitions for fractional-order derivatives and integrals, which have been developed so far such as Riemann–Lioville, Caputo Grunwald–Letinkov, and Wyl–Riesez fractional operators. More details are provided in references [14–18]. In reference [19], a fractional-order model based on Atangana–Baleanu–Caputo fractional derivative was proposed to understand the dynamics of differentiation of stem cells. The state-of-the-art developments in special functions and mathematical analysis tools associated with fractional-order differential equations are provided in reference [20].

The numerical solutions of FDEs are usually carried out with high computational cost and induce several types of numerical errors.

Therefore, while searching for an efficient and reasonable alternative, it is recognized that the fractional difference operators can be applied in a straightforward way to the mathematical modeling of different nonlinear systems. More recently, attention has been turned to the discrete fractional difference equations [21–25], where they have been successfully applied in different fields.

On the other side, complex maps are found to exhibit very interesting and fascinating geometrical structures known as Julia and Mandelbrot fractal sets [26–28]. These sets are known to have fractal dimensions and have many interesting applications. The nonlinear dynamics and chaotic behavior of discrete fractional Gauss maps are investigated in the literature. It has been observed that the fractional Gauss map is more stable compared with the associated integer map. The width of period-3 windows is found to increase with the decrement in the value of fractional order [29]. Also, the synchronization for standard integer-order Gauss maps and discrete fractional Gauss maps has been studied using a parameter estimation scheme [30]. The emerging nonlinear dynamics and synchronization in coupled integer-order and fractional-order Gauss maps with different topologies have been explored in reference [31, 32]. The motivation of this study is based on the observation that the nonlinear characteristics and dynamics of the fractional complex maps are still almost an unexplored point in literature. Indeed, there are very few works that begin to investigate only the case of fractional-order complex differential equations [33, 34]. The present work extends the aforementioned works to the more general and unexplored case, where the state variable of the map has complex values, and it also investigates the emerging Julia and Mandelbrot fractal sets along with synchronization methodology of discrete fractional Gaussian map in complex domain for the first time, to the best of authors' knowledge. Moreover, the present work combines the induced fractal sets into a proposed efficient chaos-based encryption technique.

The very complicated behaviors of chaotic systems along with noise-like dynamics, very broadband spectrum, and ability to attain synchronization between distant systems have been utilized efficiently in a plethora of schemes for chaos-based communications [35–52]. In the last two decades, the chaos-based cryptography has become a focus research point of great interest. The critical evaluation of chaos-based encryption systems reveals that it is essential to keep high complexity and dimensionality of chaotic dynamics in encryption schemes along with effectively preventing any information leakage by possible eavesdroppers attacks [40–42]. The chaotic maps, in particular, are easily implementable on digital hardware, which can be straightforwardly integrated with modern communication systems. However, several works have highlighted the problem of degradation and suppression of chaotic behavior in simple structure and low-dimensional chaotic maps. These problems result from hardware finite precision of floating numbers [43–45]. Also, the small key space in these chaotic maps is another drawback. The employment of multiple chaos systems and switching between their outputs is offered along with sufficient long finite precision computations to improve the performance of chaotic maps [46]. The pseudo-chaotic orbits can be employed as another solution to the aforementioned chaos degradation issue [47, 48]. More specifically, pseudo-chaotic time series can be attained by subtracting the output sequences of two mathematically equivalent chaotic maps, which are nonequivalent in computations when machine finite precision is considered [47, 48]. The application of discrete fractional complex maps in the field of chaos-based encryption systems is also an unexplored research point, to the best of our knowledge. So, this article aims also at investigating this challenging task and providing a reliable encryption machine based on the complicated dynamics of a proposed fractional complex map.

This study is organized as follows: the mathematical model of the proposed discrete fractional complex Gaussian map is presented in Section 2. The control and synchronization of Julia sets generated by the proposed map are examined in Section 3. The proposed hybrid chaos-fractal encryption scheme is presented in Section 4, while the associated security analysis is addressed in Section 5. Section 6 contains conclusion and final discussion.

2. Discrete Fractional Complex Gaussian Map

The discrete fractional complex Gaussian map is proposed in the following form:

$$ {}^{C}\Delta_0^{\alpha} z(t) = e^{-az^2(t+\alpha-1)} + b, \tag{1}$$

where z, $a \neq 0$, and $b \neq 0$ take complex values, whereas the fractional order $\alpha \in (0,1]$. The complex discrete fractional map (1) has infinite number of fixed points, which can be evaluated from the following equation:

$$ e^{-az^{*2}} = -b, \tag{2}$$

or

$$ z^* = \left[\frac{\ln|b| + i\{\theta_0 + (2k+1)\pi\}}{a}\right]^{1/2}, \quad k = 0, \pm 1, \pm 2, \ldots, \tag{3}$$

where θ_0 denotes the principal argument of complex-valued constant b. This means that the equilibrium points of the proposed map are determined according to the assigned values for a, b, and k.

The asymptotic stability analysis of fixed points in the complex fractional Gaussian map (1) is conducted in the following subsection:

2.1. Stability Analysis of Fixed Points

Theorem 1. *The fixed point z^* of the fractional complex Gaussian map (1) is locally asymptotically stable if*

$$\left|-2az^* e^{-az^{*2}}\right| < \left(2\cos\frac{Arg\left(-2az^* e^{-az^{*2}}\right) - \pi}{2-\alpha}\right)^{\alpha},$$
$$\left|Arg\left(-2az^* e^{-az^{*2}}\right)\right| > \frac{\alpha\pi}{2}. \tag{4}$$

Proof. Assume that $\varepsilon(t) = z(t) - z^*$, then the next linearized map is derived from equation (1):

$$\begin{aligned} {}^{C}\Delta_0^{\alpha}\varepsilon(t) &= -2az^* e^{-az^{*2}}\varepsilon(t+\alpha-1) \\ &= \gamma\varepsilon(t+\alpha-1). \end{aligned} \tag{5}$$

Expressing the above equation in terms of its real and imaginary parts, it follows that

$$\begin{aligned} \Delta_0^{\alpha}\varepsilon_r(t) + i^{C}\Delta_a^{\alpha}\varepsilon_i(t) &= (\gamma_r + i\gamma_i) \\ &\quad\cdot\left(\varepsilon_r(t+\alpha-1) + i\varepsilon_i(t+\alpha-1)\right), \end{aligned} \tag{6}$$

and therefore the next equivalent 2D discrete fractional system is attained:

$$\begin{aligned} \Delta_0^{\alpha}\varepsilon_r(t) &= \gamma_r\varepsilon_r(t+\alpha-1) - \gamma_i\varepsilon_i(t+\alpha-1), \\ \Delta_0^{\alpha}\varepsilon_i(t) &= \gamma_i\varepsilon_r(t+\alpha-1) + \gamma_r\varepsilon_i(t+\alpha-1). \end{aligned} \tag{7}$$

Now, the above two equations can be expressed as follows:

$$\begin{pmatrix} \Delta_0^{\alpha}\varepsilon_r(t) \\ \Delta_0^{\alpha}\varepsilon_i(t) \end{pmatrix} = \begin{pmatrix} \gamma_r & -\gamma_i \\ \gamma_i & \gamma_r \end{pmatrix}\begin{pmatrix} \varepsilon_r(t+\alpha-1) \\ \varepsilon_i(t+\alpha-1) \end{pmatrix}, \tag{8}$$

where it can be verified that the eigenvalues of the matrix of coefficients are given by $\gamma_r \pm i\gamma_i$.

Define Λ by

$$\Lambda = \begin{pmatrix} \gamma_r & -\gamma_i \\ \gamma_i & \gamma_r \end{pmatrix}, \tag{9}$$

such that $tr(\Lambda) = 2\gamma_r$. and $\det(\Lambda) = \gamma_r^2 + \gamma_i^2 > 0$. The zero equilibrium point of equation (8) is asymptotically stable if its associated eigenvalues satisfy

$$\sqrt{\gamma_r^2 + \gamma_i^2} < \left(2\cos\frac{\left|\tan^{-1}(\gamma_i/\gamma_r)\right| - \pi}{2-\alpha}\right)^{\alpha}, \left|\tan^{-1}\left(\frac{\gamma_i}{\gamma_r}\right)\right| > \frac{\alpha\pi}{2}. \tag{10}$$

For $z^* = [\ln|b| + i\{\theta_0 + (2k+1)\pi\}/a]^{1/2}$, $k = 0, \pm 1, \pm 2, \ldots$, the stability conditions reduce to

$$\begin{aligned} &\left|-2az^* e^{-az^{*2}}\right| < \left(2\cos\frac{\left|Arg\left(-2az^* e^{-az^{*2}}\right)\right| - \pi}{2-\alpha}\right)^{\alpha} \\ &\quad\cdot\left|Arg\left(-2az^* e^{-az^{*2}}\right)\right| > \frac{\alpha\pi}{2}. \end{aligned} \tag{11}$$

In this case, the trajectories which start from small initial perturbations $\varepsilon_r(0)$. and $\varepsilon_i(0)$. around the origin will algebraically decay to the equilibrium point such that$\|\varepsilon(n)\| = O(n^{-\alpha})$. as $n \longrightarrow \infty$.

For the special case, where principal argument of b is considered, that is, $k = 0$, we get

$$\begin{aligned} z_{1,2}^* &= \left[\frac{1/2\ln\left(b_r^2 + b_i^2\right) + i\left(\theta_0 + \pi\right)}{a_r + ia_i}\right]^{1/2} \\ &= \left[\frac{\left(1/2a_r\ln\left(b_r^2 + b_i^2\right) - a_i\left(\theta_0 + \pi\right)\right) + i\left(a_r\left(\theta_0 + \pi\right) + 1/2a_i\ln\left(b_r^2 + b_i^2\right)\right)}{a_r^2 + a_i^2}\right]^{1/2} \\ &= \frac{1}{\sqrt{a_r^2 + a_i^2}} r^{*^{1/2}}\left[\cos\left(\frac{\phi_0}{2}\right) + i\sin\left(\frac{\phi_0}{2}\right)\right], \frac{1}{\sqrt{a_r^2 + a_i^2}} r^{*^{1/2}}\left[\cos\left(\frac{\phi_0 + \pi}{2}\right) + i\sin\left(\frac{\phi_0 + \pi}{2}\right)\right], \end{aligned} \tag{12}$$

where $a = a_r + ia_i$ and $b = b_r + ib_i$,

$$\begin{aligned} r^* &= \sqrt{\left(\frac{1}{2}a_r\ln\left(b_r^2 + b_i^2\right) - a_i\left(\theta_0 + \pi\right)\right)^2 + \left(a_r\left(\theta_0 + \pi\right) + \frac{1}{2}a_i\ln\left(b_r^2 + b_i^2\right)\right)^2}, \\ \phi_0 &= \tan^{-1}\left(\frac{a_r\left(\theta_0 + \pi\right) + 1/2a_i\ln\left(b_r^2 + b_i^2\right)}{1/2a_r\ln\left(b_r^2 + b_i^2\right) - a_i\left(\theta_0 + \pi\right)}\right). \end{aligned} \tag{13}$$

The specific forms of $z_{1,2}^*$ can be substituted in above-mentioned stability conditions to investigate their stability.

By the aid of numerical simulations, previous results regarding stability conditions of fixed points are validated for different values of α, k, a, and b (Figure 1). The obtained solution orbits indicate that the stability conditions are satisfied for selected parameter sets employed in Figure 1.

2.2. Fractal Sets Induced by Discrete Fractional Complex Gaussian Map. The notions of Julia fractal set and Mandelbrot fractal set in integer-order complex-valued maps can be extended to the general case of discrete fractional-order complex maps. Given the next discrete fractional map of order α

$$\Delta_0^\alpha z(t) = \Psi(z(t+\alpha-1), \mu), \tag{14}$$

where $\Psi: \mathbb{C} \longrightarrow \mathbb{C}$ and $\mu \in \mathbb{C}$. The Julia set generated by map (5) is described in the following definition [26–28, 33, 34]:

Definition 2. The filled-in Julia set of complex-valued discrete fractional map (5) is defined as the set Ω of initial points $z \in \mathbb{C}$, whose solution orbits are bounded. The boundary of Ω set is referred to as $\partial\Omega$ and it is known as the Julia set Υ_Ψ^α of the map (5).

The main characteristics of Julia set Υ_Ψ^α are summarized as follows [27, 28, 33, 34]:

(1) $\Upsilon_\Psi^\alpha \neq \phi$ (Julia set is nonempty).

(2) Υ_Ψ^α is invariant with respect to associated map (5) in the forward and backward directions of time.

(3) Assuming that an attractive fixed point $\widehat{z}$ of the discrete fractional map (5) has period p and exists at $\overline{\alpha}$, then $\Upsilon_\Psi^{\overline{\alpha}}$ includes the basin of attraction of $\widehat{z}$.

The well-known Mandelbrot set has been investigated by Benoit Mandelbrot in 1979 [27, 28]. Its concept can also be generalized to the discrete fractional case. More specifically, fixing the value of fractional order α, the Mandelbrot set χ_Ψ^α consists of the set of values of parameter $\mu \in \mathbb{C}$ at which the values of $|z(t)|$, $t > 0$ are bounded for $z(0) = 0$.

The space-filling dimension can be employed to quantify the fractal properties of Julia and Mandelbrot sets. In particular, the box-counting measure for dimension is one of the most accessible measures in fractal analysis and it is defined as follows:

Definition 3. Consider the nonempty bounded subset Ξ of $\mathbb{R}^n$ and suppose that there are N_ρ boxes with side length ρ, which are required to cover the set Ξ. Then, the box-counting dimension (Minkowski–Bouligand dimension) is determined by the following equation:

$$\dim_\Xi = \lim_{\rho\longrightarrow 0} \frac{\log(N_\rho)}{\log(1/\rho)}, \tag{15}$$

where N_ρ is the number of boxes to cover Ξ. In addition, the upper box dimension (entropy dimension) and the lower box dimension (lower Minkowski dimension) of Ξ are also defined, respectively, by the following equations:

$$\begin{aligned} \overline{\dim}_\Xi &= \overline{\lim_{\rho\longrightarrow 0}} \frac{\log(N_\rho)}{\log(1/\rho)}, \\ \underline{\dim}_\Xi &= \underline{\lim_{\rho\longrightarrow 0}} \frac{\log(N_\rho)}{\log(1/\rho)}. \end{aligned} \tag{16}$$

The generation of Mandelbrot and Julia sets is explored through numerical simulations at different values of parameters. The following table summarizes the obtained results at different values of fractional order α, constant q, and exponent p. In addition, the box-counting dimensions for the different cases considered in simulations are also presented in Table 1 The corresponding Mandelbrot and Julia sets are depicted in Figures 2 to 4.

3. Control and Synchronization of Julia Sets

The problem of achieving control and synchronization of Julia sets generated by the discrete fractional complex Gaussian map is discussed in this section.

For two discrete fractional-order complex Gaussian maps, the first map is known as the master map and it produces the output $z_1(t)$, while the second map, with the output $z_2(t)$, will be referred to as the slave one.

Definition 4. The synchronization between the master and slave maps is achieved, if $z_2(t) \longrightarrow z_1(t)$ as $t \longrightarrow \infty$. In other words, it can be expressed as follows [33, 34]:

$$\lim_{t\longrightarrow\infty} |z_2(t) - z_1(t)| = 0. \tag{17}$$

When the synchronization is attained between two trajectories, it implies that the corresponding characteristics of convergence and divergence are identical. Assume that Υ_1^α and Υ_2^α denote the Julia sets induced by fractional-order master and fractional-order slave Gaussian maps, respectively, at fractional order α. Therefore, the synchronization between the mentioned two Julia sets can be defined as follows [29,30]:

Definition 5. The asymptotic synchronization of the two Julia sets Υ_1^α and Υ_2^α is satisfied if

$$\lim_{t\longrightarrow\infty} (\Upsilon_1^\alpha \cup \Upsilon_2^\alpha - \Upsilon_1^\alpha \cap \Upsilon_2^\alpha) = \varnothing. \tag{18}$$

3.1. Control of Julia Sets of Discrete Fractional Complex Gaussian Map. In this section, the appropriate controller is designed in order to change the characteristics and geometry of Julia sets generated by the proposed fractional map via varying the type of stability of one of the fixed points of the present map. More specifically, we consider the feedback controller in the following form:

$$\varrho(t) = -\varsigma(z(t) - \widetilde{z}) - e^{-az^2(t)} - b, \tag{19}$$

where $\widetilde{z}$ is the selected unstable fixed point intended to be stabilized under the influence of controller and $\varsigma = \varsigma_r + i\varsigma_i$

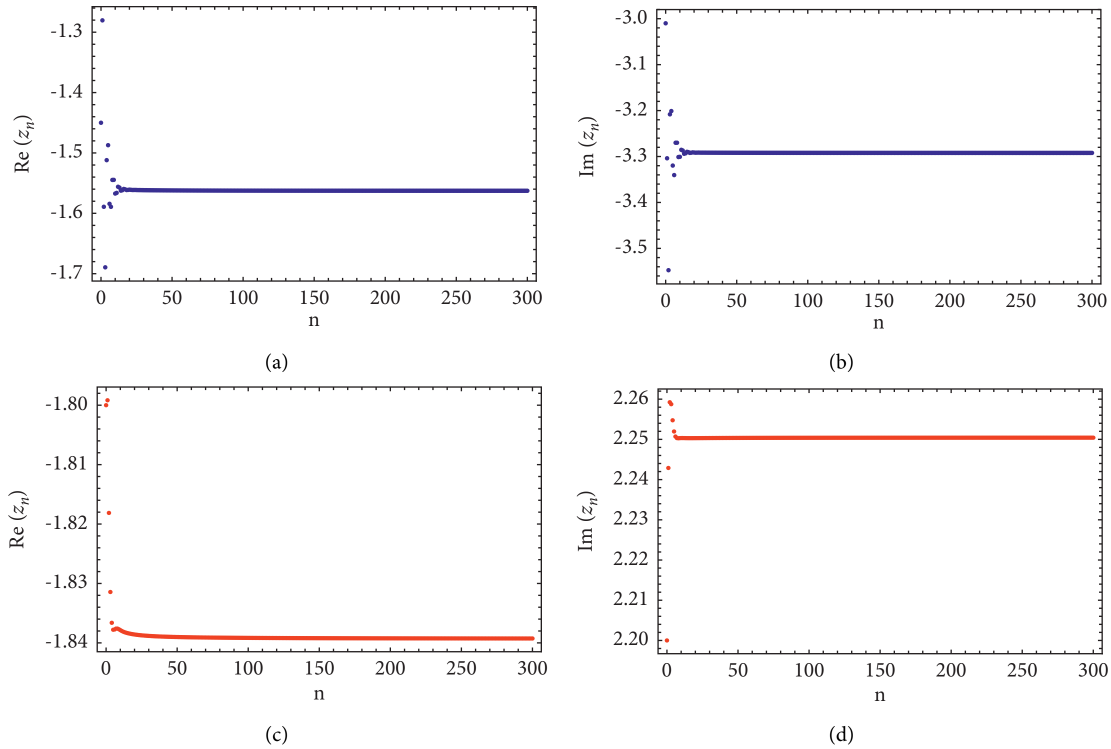


FIGURE 1: Time series solution of fractional Gaussian map depicting stable fixed points at (a, b) $a = 0.15 - 0.15i$, $\alpha = 0.9$, $b = 0.71 + 0.25i$ and (c, d) $a = 0.3 + 0.2i$, $\alpha = 0.85$, $b = 0.3 - 0.1i$.

TABLE 1: Summary of fractal sets generated from complex fractional Gaussian map and their fractal dimensions.

Graph	Fractal set	Parameters	Dimension
Figure 2(a)	Mandelbrot set	$\alpha = 1$, $a = 0.5 + 0.3i$	1.544
Figure 2(b)	Julia set	$\alpha = 1$, $a = 0.5 + 0.3i$, $b = 0.3 + 0.3i$	1.838
Figure 2(c)	Julia set	$\alpha = 1$, $a = 0.5 + 0.3i$, $b = -0.15 - 0.4i$	1.6438
Figure 2(d)	Mandelbrot set	$\alpha = 1$, $a = 0.19 - 0.5i$	1.429
Figure 2(e)	Julia set	$\alpha = 1, a = 0.19 - 0.5i$, $b = 0.5 - 0.5i$	1.8321
Figure 3(a)	Mandelbrot set	$\alpha = 0.8, a = 0.19 - 0.5i$	1.753
Figure 3(b)	Mandelbrot set	$\alpha = 0.5, a = 0.19 - 0.5i$	1.4775
Figure 3(c)	Mandelbrot set	$\alpha = 0.3, a = 0.19 - 0.5i$	1.512
Figure 3(d)	Julia set	$\alpha = 0.8, a = 0.19 - 0.5i$, $b = 0.5 - 0.5i$	1.781
Figure 3(e)	Julia set	$\alpha = 0.5, a = 0.19 - 0.5i$, $b = 0.5 - 0.5i$	1.6574
Figure 3(f)	Julia set	$\alpha = 0.3, a = 0.19 - 0.5i$, $b = 0.5 - 0.5i$	1.932
Figure 4(a)	Mandelbrot set	$\alpha = 0.9, a = -0.59 + 0.93i$	1.5016
Figure 4(b)	Julia set	$\alpha = 0.9, a = -0.59 + 0.93i$, $b = -0.75 - 0.05i$	1.753
Figure 4(c)	Mandelbrot set	$\alpha = 0.5, a = 1.15 - 0.7i$	1.483
Figure 4(d)	Julia set	$\alpha = 0.5, a = 1.15 - 0.7i$, $b = 0.5 - 0.5i$	1.4485

represents the complex-valued gain of the controller, which can be evaluated as follows:

Theorem 6. *Assume that the gain ς of controller $\varrho(t)$ of the controlled fractional-order complex Gaussian map*

$$\Delta_0^\alpha z(t) = e^{-az^2(t+\alpha-1)} + b + \varrho(t+\alpha-1), \tag{20}$$

fulfills the two inequalities

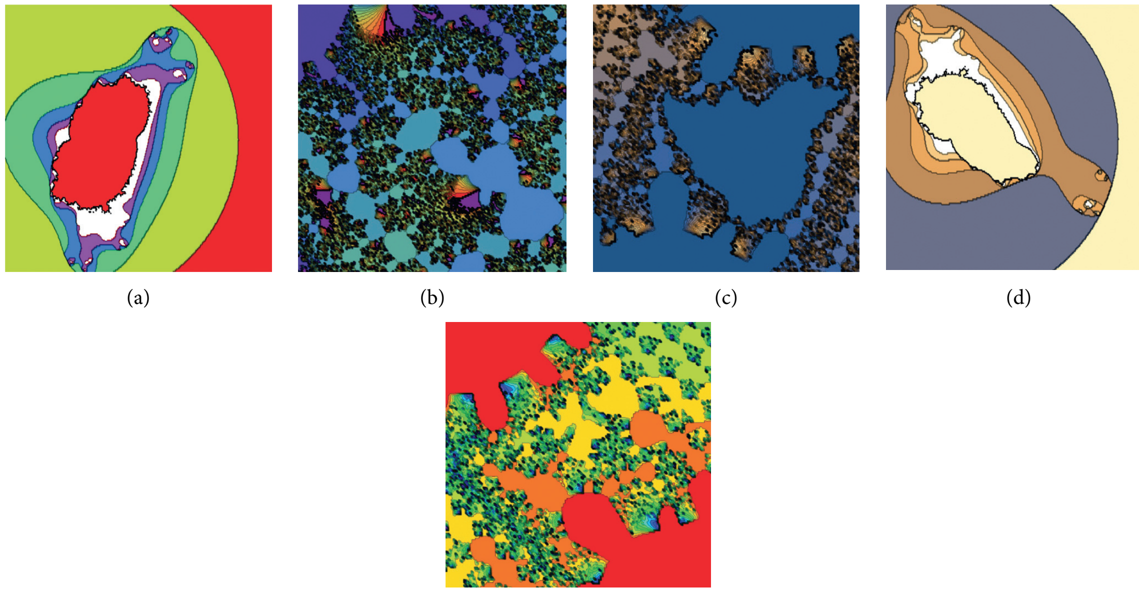
$$\varsigma_r > 0, \ \sqrt{\varsigma_r^2 + \varsigma_i^2} < 2^\alpha, \tag{21}$$

then the fixed point $\tilde{z}$ become stable, such that the associated Julia set in its neighborhood is changed.

Proof. By applying the control signal (6), we get the following controlled fractional-order complex map:

$$\Delta_0^\alpha z(t) = -\varsigma(z(t+\alpha-1) - \tilde{z}). \tag{22}$$

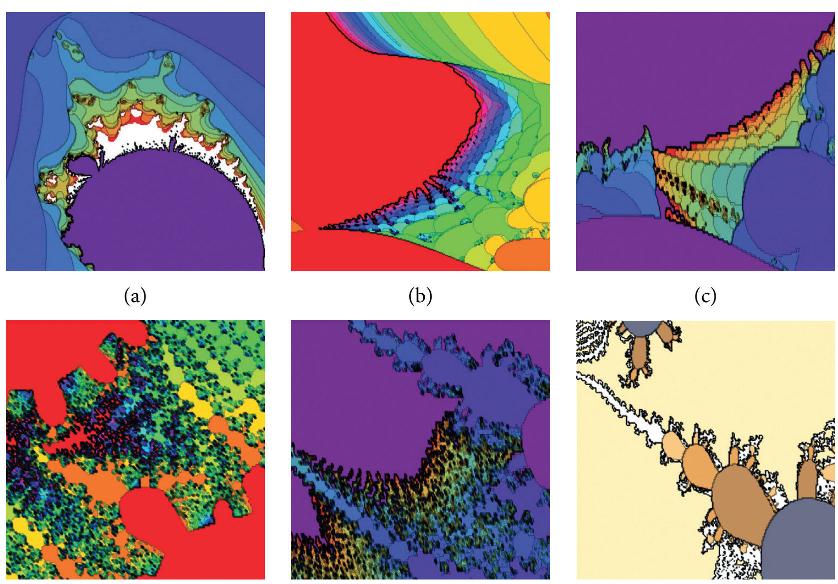
Defining $\delta(t) = z(t) - \tilde{z} \in \mathbb{C}$, equation (22) takes the following form:



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

(e)

Figure 2: The Mandelbrot and Julia sets of generalized fractional Gaussian map obtained at specified values in Table 1.



(a) (b) (c)

(d) (e) (f)

Figure 3: The Mandelbrot and Julia sets of generalized fractional Gaussian map obtained at specified values in Table 1.

$$\Delta_0^\alpha \delta(t) = -\varsigma\delta(t+\alpha-1). \tag{23}$$

The corresponding two-dimensional real-valued fractional map can be expressed as follows:

$$\begin{aligned}\Delta_0^\alpha \delta_r(t) &= -\varsigma_r\delta_r(t+\alpha-1) + \varsigma_i\delta_i(t+\alpha-1),\\ \Delta_0^\alpha \delta_i(t) &= -\varsigma_i\delta_r(t+\alpha-1) - \varsigma_r\delta_i(t+\alpha-1).\end{aligned} \tag{24}$$

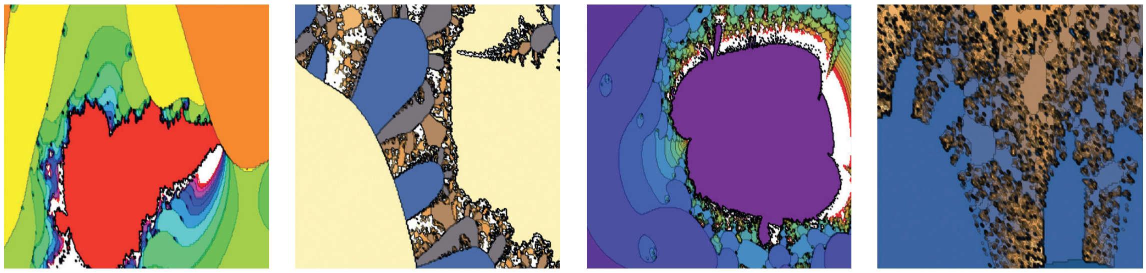
Then, the coefficients of the above system can be put in the following matrix:

$$\Lambda = \begin{pmatrix} -\varsigma_r & \varsigma_i \\ -\varsigma_i & -\varsigma_r \end{pmatrix}, \tag{25}$$

and the associated eigenvalues are computed as $-\varsigma_r \pm i\varsigma_i$. Hence, the sufficient conditions required for local asymptotic stability of $\tilde{z}$ can be formulated as $\varsigma_r > 0$ and $\sqrt{\varsigma_r^2 + \varsigma_i^2} < 2^\alpha$. □

3.2. Synchronization of Julia Sets. The discrete fractional master system is defined in the following form:

$$\Delta_0^\alpha z_1(t) = e^{-az_1^2(t+\alpha-1)} + b, \tag{26}$$



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

FIGURE 4: The Mandelbrot and Julia sets of generalized fractional Gaussian map obtained at specified values in Table 1.

whereas the corresponding slave system is formulated as follows:

$$\Delta_0^\alpha z_2(t) = e^{-az_2^2(t+\alpha-1)} + b + \phi(z_1, z_2, t+\alpha-1), \tag{27}$$

where $\phi(z_1, z_2, t+\alpha-1)$ is the adequate controller to be designed. Note that the initial values of two systems are assumed to be different and since the present map has infinite number of fixed points, the solutions z_1 and z_2 may converge to different fixed points in the way that they induce distinct filled Julia sets. When the synchronization is achieved between the two maps, it is achieved for the associated Julia sets.

Theorem 7. *The two fractional maps (8) and (9) are synchronized under the influence of the following controller:*

$$\begin{aligned}\phi(z_1, z_2, t+\alpha-1) = {} & e^{-az_1^2(t+\alpha-1)} - e^{-az_2^2(t+\alpha-1)} \\ & - \kappa(z_2(t+\alpha-1) - z_1(t+\alpha-1)),\end{aligned} \tag{28}$$

where the gain $\kappa = \kappa_r + i\kappa_i$, satisfying $|\kappa| < 2^\alpha$ and $\kappa_r > 0$.

Proof. The discrete fractional error map is obtained by subtracting equation (8) from equation (9) as follows:

$$\begin{aligned}\Delta_0^\alpha e(t) &= e^{-az_2^2(t+\alpha-1)} - e^{-az_1^2(t+\alpha-1)} + \phi(z_1, z_2, t+\alpha-1), \\ e(t) &= z_2(t) - z_1(t).\end{aligned} \tag{29}$$

Using the proposed controller (10) into the above fractional error system, it results in

$$\Delta_0^\alpha e(t) = -\kappa e(t+\alpha-1), \tag{30}$$

or

$$\begin{aligned}\Delta_0^\alpha (e_r(t) + ie_i(t)) = {} & (-\kappa_r - i\kappa_i) \\ & \cdot (e_r(t+\alpha-1) + ie_i(t+\alpha-1)),\end{aligned} \tag{31}$$

which can be expressed in the following two dimensional system:

$$\begin{aligned}\Delta_0^\alpha e_r(t) &= -\kappa_r e_r(t+\alpha-1) + \kappa_i e_i(t+\alpha-1), \\ {}^C\Delta e_i(t) &= -\kappa_i e_r(t+\alpha-1) - \kappa_r e_i(t+\alpha-1).\end{aligned} \tag{32}$$

It is obvious that the eigenvalues of error system are $-\kappa_r \pm i\kappa_i$, so that the asymptotic stability to zero fixed point of error system is attained provided that $|\kappa| < 2^\alpha$ and $\kappa_r > 0$.

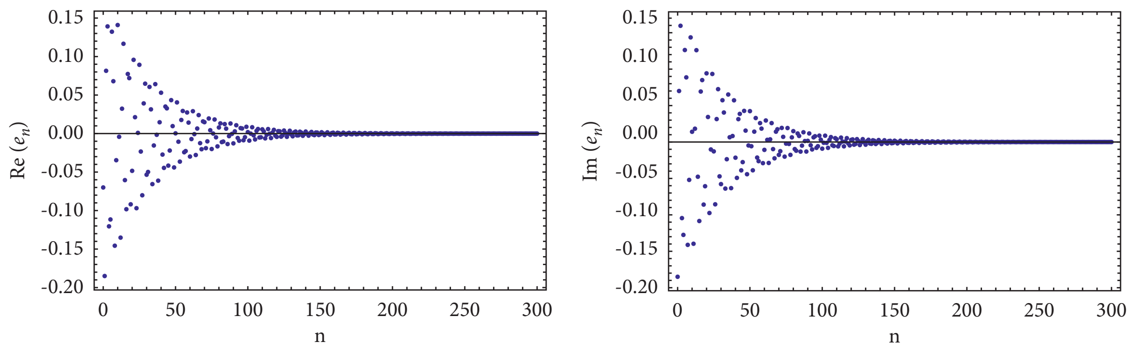
Numerical simulations are now employed to validate the theoretical results acquired in this section. The synchronization between orbits of two fractional-order complex Gaussian maps initiated from different initial conditions is shown in Figure 5. □

4. Proposed Encryption Algorithm

The objective of this section is to introduce an efficient chaos-based encryption technique, which utilizes the idea of pseudo-chaotic dynamics along with complicated fractal patterns to boost its security performance.

Consider the following two modified chaotic lemniscate maps [47]:

$$\begin{aligned}x_1(n+1) &= \frac{\cos\left[2^{3/2+r}\ \cos[2^r x_1(n)]\sin[2^r x_1(n)]/1+\ \sin^2[2^r x_1(n)]\right]}{1+\ \sin^2\left[2^{3/2+r}\cos[2^r x_1(n)]\sin[2^r x_1(n)]/1+\ \sin^2[2^r x_1(n)]\right]}, \\ y_1(n+1) &= \frac{2\sqrt{2}\cos\left[2^r\cos[2^r y_1(n)]/1+\ \sin^2[2^r y_1(n)]\right]\sin\left[2^r\cos[2^r y_1(n)]/1+\ \sin^2[2^r y_1(n)]\right]}{1+\ \sin^2\left[2^r\cos[2^r y_1(n)]/1+\ \sin^2[2^r y_1(n)]\right]},\end{aligned} \tag{33}$$



(a) (b)

Figure 5: Synchronization errors between master and slave systems at $a = 0.15 - 0.15i$, $\alpha = 0.9$, $b = 0.71 + 0.25i$, where initial value for master system is $(-1.43 - 3i)$ and that for slave system is $(-1.4 - 2.8i)$, whereas $\kappa = 1 + i$.

$$x_2(n) = \frac{\cos\left[2^{3/2}\cos\left(2^r x_2(n)\right)/\sqrt{1+\sin^2\left(2^r x_2(n)\right)} \times 2^r \sin\left(2^r x_2(n)\right)/\sqrt{1+\sin^2\left(2^r x_2(n)\right)}\right]}{1+\sin^2\left[2^{3/2}\cos\left(2^r x_2(n)\right)/\sqrt{1+\sin^2\left(2^r x_2(n)\right)} \times 2^r \sin\left(2^r x_2(n)\right)/\sqrt{1+\sin^2\left(2^r x_2(n)\right)}\right]},$$

$$y_2(n) = \frac{2\cos\left[2^r/\sqrt{1+\sin^2\left(2^r y_2(n)\right)} \times \cos\left(2^r y_2(n)\right)/\sqrt{1+\sin^2\left(2^r y_2(n)\right)}\right]}{1+\sin^2\left[2^r\cos\left(2^r y_2(n)\right)/1+\sin^2\left(2^r y_2(n)\right)\right]} \times \frac{\sin\left[2^r \sin\left(2^r x_2(n)\right)/1+\sin^2\left(2^r x_2(n)\right)\right]}{1/\sqrt{2}}. \tag{34}$$

It is obvious that these two maps are mathematically equivalent, yet the finite floating-point representation renders the corresponding orbits diverge exponentially from each other even in the case where identical initial conditions are used. Now, a set of q random perturbation values, $\{b_1, b_2, \ldots, p_q\}$, is chosen and used to update the generated sequences from the above two systems as follows:

For $n = 1{:}\ 1000$

$$\begin{aligned} X_i(n) &= x_i(n) + b_1, \\ Y_i(n) &= y_i(n) + b_1, \\ &\quad \mathrm{i} = 1, 2. \end{aligned} \tag{35}$$

For $n = 1001{:}\ 2000$

$$\begin{aligned} X_i(n) &= x_i(n) + b_2, \\ Y_i(n) &= y_i(n) + b_2, \\ &\quad \mathrm{i} = 1, 2. \end{aligned} \tag{36}$$

. . ..

For $n = (q-1)(1000) + 1{:}\ q \times 1000$,

$$\begin{aligned} X_i(n) &= x_i(n) + b_q, \\ Y_i(n) &= y_i(n) + b_q, \\ &\quad \mathrm{i} = 1, 2. \end{aligned} \tag{37}$$

The modular one operations are employed to get

$$\begin{aligned} \widehat{X}_i(n) &= \mod\left(X_i(n), 1\right), \\ \widetilde{Y}_i(n) &= \mod\left(Y_i(n), 1\right), \end{aligned} \tag{38}$$

and hence, the associated lower bound errors can be obtained by setting

$$\begin{aligned} e_X(n) &= \frac{\widehat{X}_1(n) - \widehat{X}_2(n)}{2}, \\ e_X(n) &= \frac{\widehat{Y}_1(n) - \widehat{Y}_2(n)}{2}. \end{aligned} \tag{39}$$

Fractal images are used in the proposed encryption technique to boost the security performance of the technique via incorporating additional layers of encryption. More specifically, the color components of each pixel in randomly selected two fractal images are used to confuse the values of each color component in the way that the first fractal image is used with the plain image and the second one is concerned with the shuffled plain image. In order to control and reduce the computation cost, a catalog of secretly pregenerated fractal images can be saved and then employed as one of the secret keys in the scheme. The advantages of using discrete fractional complex maps in the generation of fractal images are that they significantly increase key space. In particular, the two complex-valued parameters a and b in addition to the real-valued parameters α, r, $x(0)$, and $y(0)$ are the key parameters in the system in addition to the random perturbing values for pseudo-chaotic signals. This implies that using IEEE 754 double-precision floating-point format, the established key space is approximately 2^{3922} for 256×256 plain images and increases considerably for larger plain images. The pseudo-chaotic time series represented by the obtained lower bound errors are utilized in the encryption process as illustrated in the next section.

4.1. Steps of the Proposed Algorithm

Step 1. The original color image is separated into R-channel P_r, G-channel P_g, and B-channel P_b, which are arranged into three matrices of size $M \times N$.

Step 2. Establish three time-varying and plain-image dependent perturbation values $\xi_{r,g,b}$ by evaluating

$$\xi_{r,g,b} = \nu\tau(t) + \frac{1}{3(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} P_{r,g,b}(i, j), \quad (40)$$

where the value of $\tau(t)$ refers to a scaled value of time difference between the moment when the plain image was supplied to encryption machine and another secretly specified moment in the past, for example, 10 : 45 : 12 : 73 Jan 1, 2000. The difference can be taken in units of milliseconds. Also, the scaling factor ν is used to render $\nu\tau(t)$spans the required range of time range. Moreover, i and j are pixel positions of the R-channel, G-channel, and B-channel matrices of plain images, that is, P_r, P_g, P_b, respectively. We use $\xi_{r,g,b}$. as perturbation values for chaotic map parameter r, such that

$$r_{1,2,3} = r_0 + \xi_{r,g,b}, \quad (41)$$

where r_0 is a base-value for r. Therefore, three pseudo-chaotic sequences are generated and utilized in permutation and diffusion processes of the aforementioned three plain image channels.

Step 3. The chaotic lemniscate map is used to generate two pseudo-chaotic sequences $e_x(i), e_y(i)$ and used in creating the following sequences:

$$\begin{aligned} rowCol_i &= \operatorname{mod}\left(floor\left(e_x(i) \times 10^{15}\right), 450\right) + 1, \\ ks_i &= \operatorname{mod}\left(floor\left(e_y(i) \times 10^{15}\right), 256\right). \end{aligned} \quad (42)$$

We use mod operation between variables x_i and $M = N$ to get a sequence to build a new position for pixels value image matrices IR, IG, IB as shuffling process. Also, we use mod operation between the variable y_i and 256 to get a random sequence that we used it in encryption process as a secret key.

Step 4. We get $row(j)$ and $column(j)$ as a new position of image pixels, where $j = 1, 2, \ldots, M$, from $rowCol_i$ sequence.

Step 5. Rearrange the pixel position as shuffle process as follows:

$$\begin{aligned} IR_{sh}(i, j) &= IR(row(i), column(j)), \\ IG_{sh}(i, j) &= IG(row(i), column(j)), \\ IB_{sh}(i, j) &= IB(row(i), column(j)), \end{aligned} \quad (43)$$

where IR_{sh} and IR are the matrix for shuffled and plain images, respectively, where $i = 1, 2, \ldots, M$ and $j = 1, 2, \ldots, N$ are the image matrix dimensions.

Step 6. We use two randomly selected fractal images from previously constructed catalog, for example, Figures 6(a) and 6(b), as secret keys Key_{f1} and Key_{f2} for each red, green, and blue color images by separating each color image from each fractal image and using it as secret keys with corresponding color in the plain image. Therefore, we have six secret keys based on the two fractal images.

In addition, to enhance the confusion of the secret key, we do a shuffle process as in step 4 to R-channel, G-channel, and B-channel of fractal image (Figure 6(a)) before using them as a secret key.

Step 7. We divide the sequence ks to three sequences ksr, ksg, ksb for each color in the plain image. To set the secret keys in matrix form, the $reshape$ function is used as follows:

$$\begin{aligned} ksR &= reshape(ksr, M, N), \\ ksG &= reshape(ksg, M, N), \\ ksB &= reshape(ksb, M, N), \end{aligned} \quad (44)$$

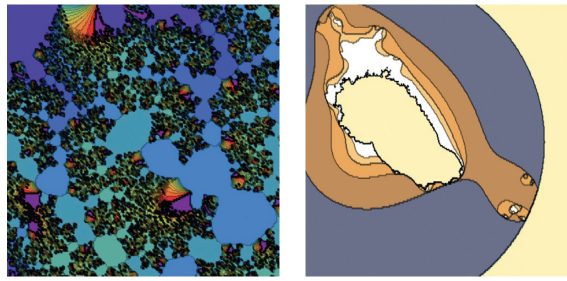
to be used as secret keys ksR, ksG, ksB for red, green, and blue channels in the plain images, respectively.

Step 8. Apply two bitwise XOR operation between Key_f, ks, I_{sh} to establish the encrypted image I_{en} as follows:

$$\begin{aligned} IR_{en}(i, j) &= \left(\left(IR_{sh}(i, j) \oplus Key_{fR1}(i, j)\right) \oplus Key_{fR2}(i, j)\right) \oplus ksR(i, j), \\ IG_{en}(i, j) &= \left(\left(IG_{sh}(i, j) \oplus Key_{fG1}(i, j)\right) \oplus Key_{fG2}(i, j)\right) \oplus ksG(i, j), \\ IB_{en}(i, j) &= \left(\left(IB_{sh}(i, j) \oplus Key_{fB1}(i, j)\right) \oplus Key_{fB2}(i, j)\right) \oplus ksB(i, j), \end{aligned} \quad (45)$$

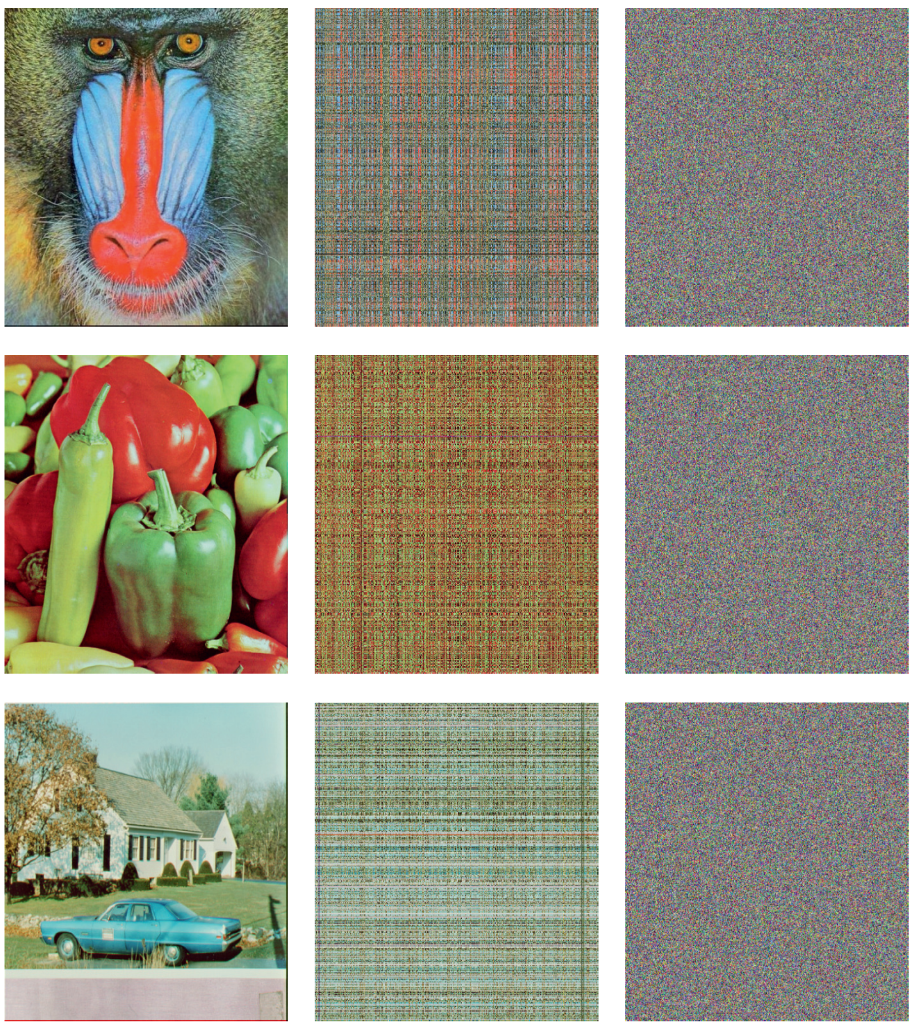
where IR_{en}, IG_{en}, and IB_{en} are the encrypted images for each color component in plain image.

The process of decryption is carried out using the reverse approach. The proposed encryption scheme is applied to three colored images. The three perturbation constants that are used in the proposed scheme are 3.9724×10^{-4}, 3.7782×10^{-4}, and 4.0288×10^{-4} for baboon, pepper, and house images, respectively. The values of $r_0, x(0), y(0)$ are taken as $35, 0.5, 0.5$, respectively. Figure 7 depicts the original, shuffled, and encrypted images for the three images with size $M = N = 450$ after applying the presented algorithm.



(a) (b)

Figure 6: Example of fractal images that are generated by the proposed fractional complex map (1).



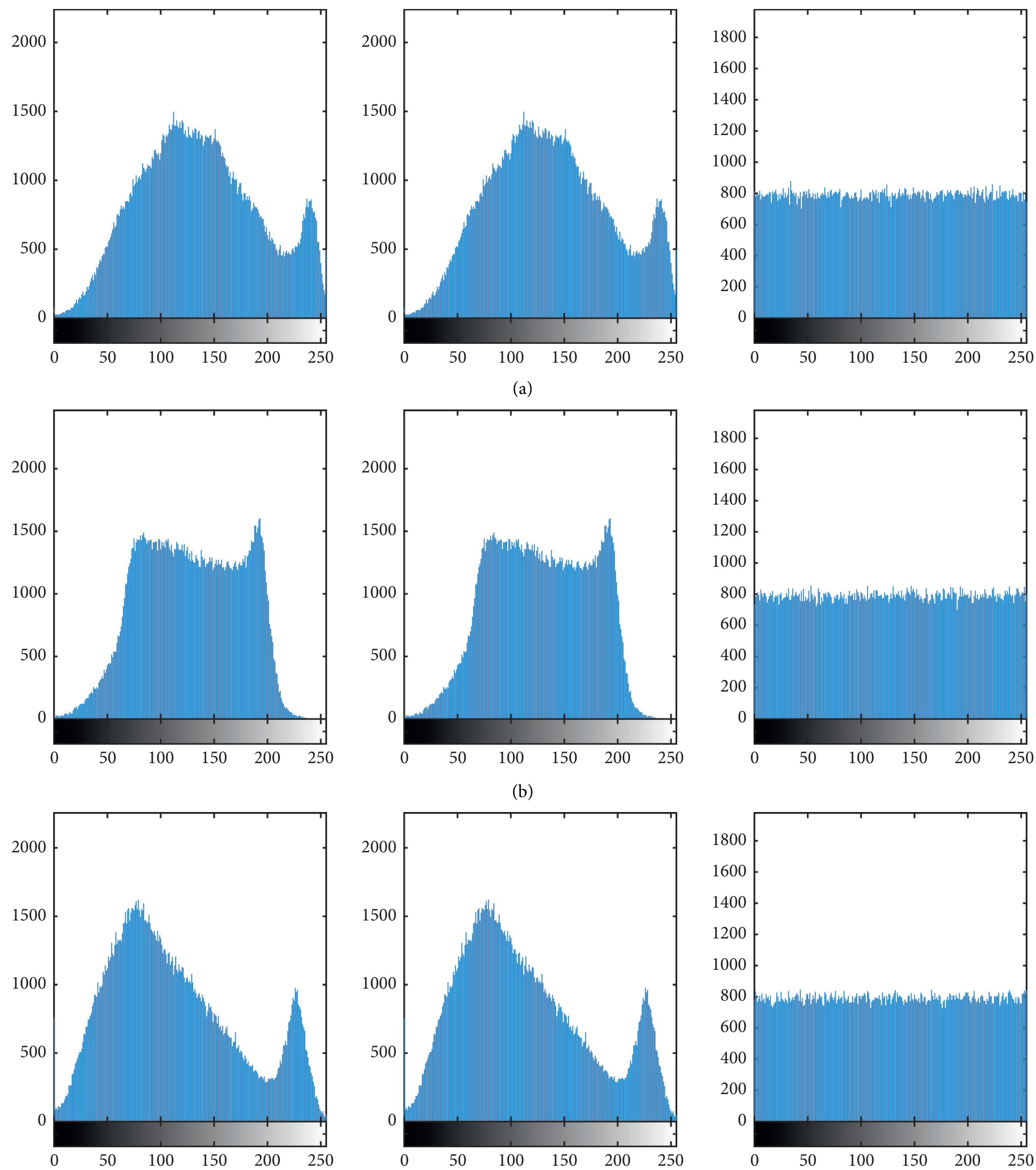
(a) (b) (c)

Figure 7: The plain, shuffled, and encrypted images in (a), (b), and (c), respectively, for baboon, pepper, and house images.

5. Security Analysis

The proper encryption scheme must be evaluated to investigate his efficacy in resisting several types of attacks. These involve brute force, statistical, differential, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks. In this section, a thorough security analysis is carried out considering these types of attacks.

5.1. Histogram. The histogram analysis is used to visualize the distribution of pixels in an image before and after the encryption process. Uniformity of pixels distribution in encrypted data implies that statistical features of input data are efficiently hidden by encryption operation. Histograms for red, green, and blue plain, shuffled, and encrypted images for baboon image are shown in Figure 8 whereas histograms for red, green, and blue plain, shuffled, and encrypted images



(a)

(b)

(c)

Figure 8: Histograms for (a) red, (b) green, and (c) blue baboon image for plain, shuffled, and encrypted image, respectively.

for pepper image are shown in Figure 9. Finally, histograms for red, green, and blue plain, shuffled, and encrypted images for house image are shown in Figure 10.

In order to quantify the uniformity of histograms, the variance of histogram is utilized as a useful measure. The variance of histogram is calculated as follows [51]:

$$\mathrm{Var}(h) = \frac{1}{256^2} \sum_{i=1}^{256} \sum_{j=1}^{256} \frac{1}{2} \left(h_i - h_j\right)^2, \quad (46)$$

where h represents the histogram values arranged in vector form and h_i and h_j denote the numbers of pixels having values of i and j, respectively. The variance of histogram for original and ciphered images is depicted in Table 2 with the percentage of reduction between the plain and encrypted images. Noting that the percentage of reduction is greater than 99.6% in the red, green, blue baboon images and greater than 99.8% in three separated colors for pepper and house images. These results confirm the efficiency of the proposed technique.

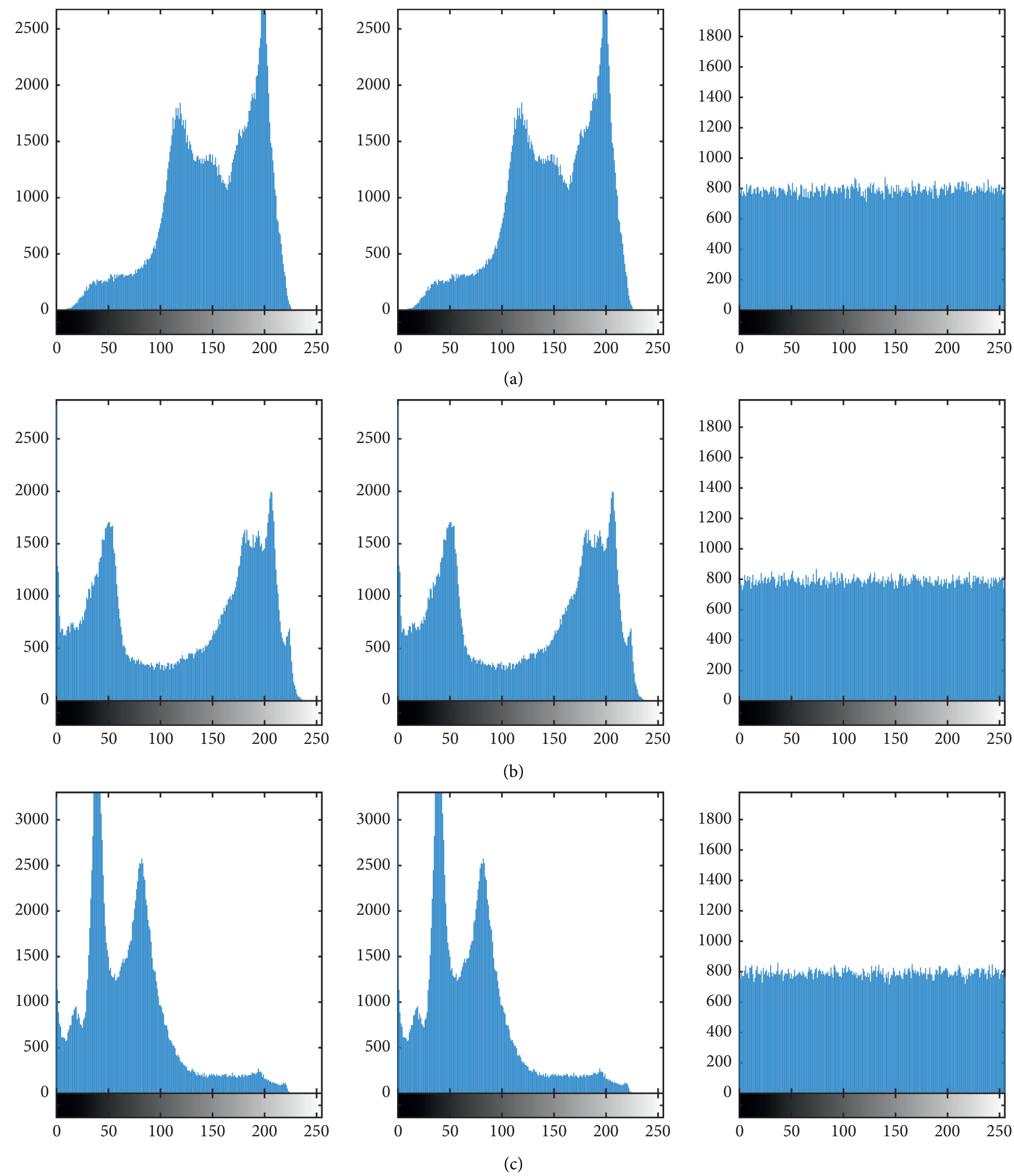


Figure 9: Histograms for (a) red, (b) green, and (c) blue pepper image for plain, shuffled, and encrypted image, respectively.

5.2. Key Space Analysis. Evaluating the size of secret key space in a specific encryption technique is a crucial step to evaluate its performance against brute force attacks. When the capabilities and characteristics of the state-of-the-art computer are taken into account, it is found that a threshold value for a minimum sufficient key space is a size of 2^{100} to ensure that the brute-force attacks are unfeasible [47, 51]. In our suggested scheme, the two complex-valued parameters a and b in addition to the real-valued parameters α, r, $x(0)$, and $y(0)$ are the key parameters in the system in addition to the random perturbing values for pseudo-chaotic signals. This implies that using IEEE 754 double-precision floating-point format, the attained key space is approximately 2^{3922} for 256×256 plain images and increases considerably for larger plain images. Accordingly, the presented scheme has key space that is much greater than the minimum value of 2^{100}.

5.3. Correlation Analysis. The correlation analysis utilized to measure and quantify the similarity among adjacent pixels throughout the image under consideration, which can be the

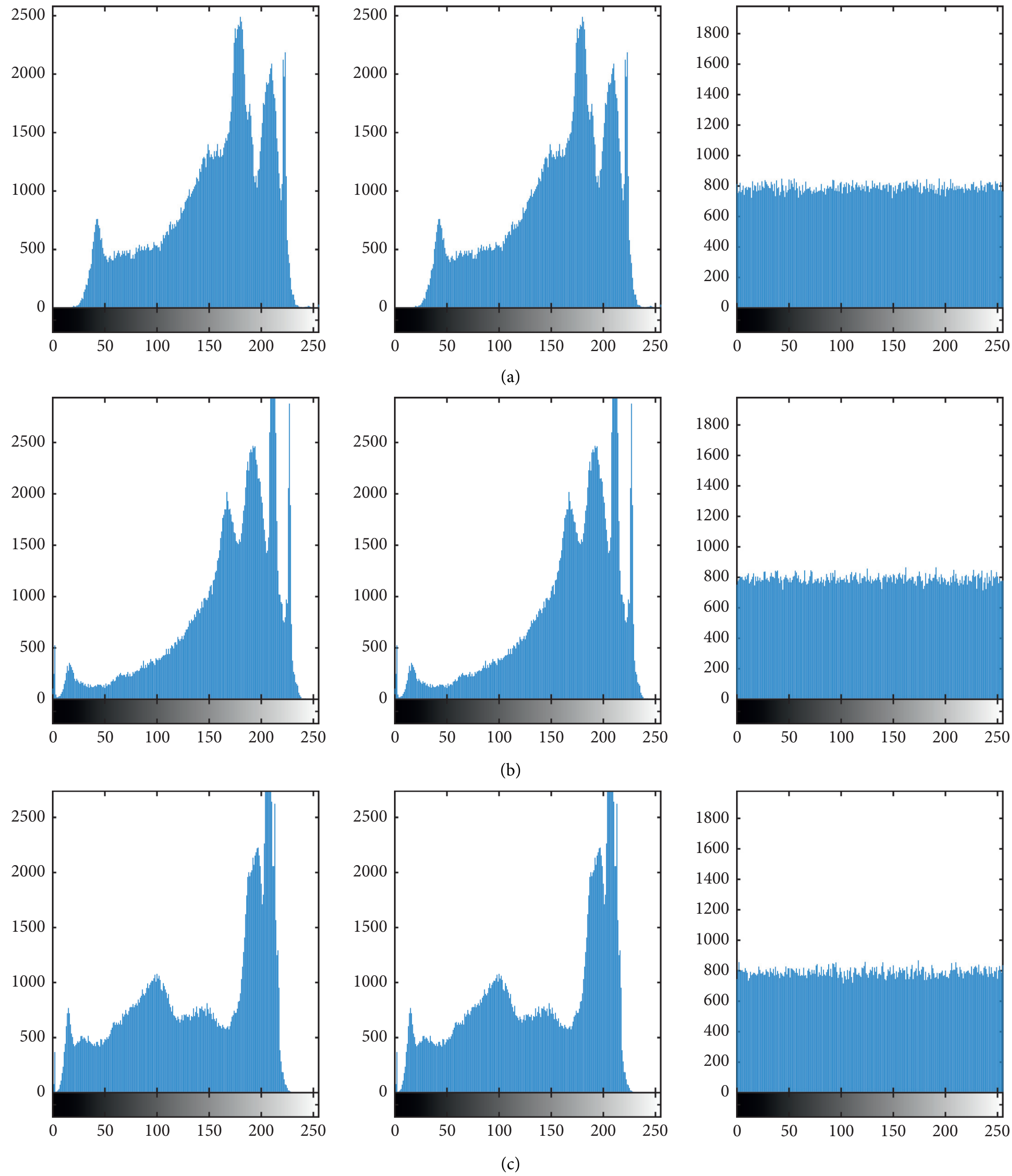


FIGURE 10: Histograms for (a) red, (b) green, and (c) blue house image for plain, shuffled, and encrypted image, respectively.

plain image or the encrypted image. The efficient encryption scheme should make the correlation coefficient as small as possible to boost the security against conventional statistical attacks. The correlation coefficient can be defined as follows:

$$r = \frac{\operatorname{cov}(x, y)}{\sigma_x \sigma_y}, \tag{47}$$

where $\sigma_\phi = \sqrt{var(\phi)}, \sigma_\psi = \sqrt{var(\psi)}$.

$$\begin{aligned} var(\phi) &= \frac{1}{N} \sum_{i=1}^{N} (\phi_i - E(\phi))^2, \\ cov(\phi, \psi) &= \frac{1}{N} \sum_{i=1}^{N} (\phi_i - E(\phi))((\psi_i) - E(\psi)), \end{aligned} \tag{48}$$

where the values of pixels of plain and encrypted images are denoted by ϕ and ψ, respectively. The correlation values between adjacent pixels in horizontal, vertical, and diagonal

Table 2: The histogram variance and its reduction for the original and cipher images for baboon, pepper, and house images.

	Variance			
	Plain		Encrypted	Reduction (%)
Baboon	Red	176920	701.4429	99.6035
	Green	348200	755.0115	99.7832
	Blue	188610	650.039	99.6553
Pepper	Red	520530	818.9017	99.8427
	Green	695920	672.1017	99.9034
	Blue	1122000	694.6978	99.9381
House	Red	440620	710.8939	99.8387
	Green	756780	764.3449	99.899
	Blue	577050	800.1174	99.8613

directions are acquired for baboon, pepper, and house images and listed in Table 3. It is obvious that the proposed algorithm is immune to statistical attacks because it is successfully minimized the values of correlation coefficients in the encrypted images to about zero.

5.4. Information Entropy. The information entropy is another powerful analysis tool used to find the unpredictability and randomness in the proposed scheme. It is reported that the optimum value is 8. The information entropy of a given image is outlined as follows:

$$H(m) = \sum_{i=1}^{2^N-1} p_i \log_2 \frac{1}{p_i}, \tag{49}$$

where $H(m)$ denotes the entropy in bits, m is an input parameter, and finally the value of probability for parameter m is referred to as p_i.

The entropy values for red, green, and blue images have been evaluated for baboon, pepper, and house encrypted images and summarized in Table 4. It is cleared that the entropy values for the three images are very close to 8; therefore, the proposed scheme is less feasible to expose information of the plain image.

5.5. Differential Attack Analysis. To evaluate the immunity of the proposed cryptosystem against the powerful differential, two useful quantities reevaluated, namely, the number of pixels changing rate (NPCR) and unified average changing intensity (UACI). These measures identify the sensitivity of the encryption scheme to change a single-pixel value of supplied plain image or sensitivity to small changes in the secret key. The equations to evaluate NPCR and UACI are expressed as follows [47]:

$$\begin{aligned} \text{NPCR}(\%) &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| \operatorname{sign}\left(C_1(i,j) - C_2(i,j)\right) \right| \times 100, \\ \text{UACI}(\%) &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left| C_1(i,j) - C_2(i,j) \right|}{255} \times 100, \end{aligned} \tag{50}$$

Table 3: The correlation values between adjacent pixels, in all directions, were obtained for red, green, and blue color components in baboon, pepper, and house images, respectively.

			Correlation coefficients		
			Horizontal	Vertical	Diagonal
Baboon	Red	Plain	0.9193	0.864	0.8403
		Cipher	−0.0005	−0.0039	0.001
	Green	Plain	0.8795	0.7997	0.7628
		Cipher	0.0032	−0.001	−0.0028
	Blue	Plain	0.9285	0.8827	0.8597
		Cipher	−0.0021	−0.0013	0.0027
Pepper	Red	Plain	0.9681	0.9703	0.9519
		Cipher	0.0001	−0.0000	−0.0007
	Green	Plain	0.9786	0.979	0.9616
		Cipher	0.0000	−0.0036	−0.0003
	Blue	Plain	0.9654	0.9643	0.9414
		Cipher	−0.0048	−0.0044	−0.0029
House	Red	Plain	0.9484	0.9467	0.9087
		Cipher	−0.0001	0.0024	0.0005
	Green	Plain	0.9286	0.9481	0.8893
		Cipher	−0.0005	−0.0003	−0.0004
	Blue	Plain	0.9704	0.9718	0.9472
		Cipher	−0.0005	0.0013	−0.0008

Table 4: The entropy for encrypted image for red, green, and blue images for baboon, pepper, and house image, respectively.

Plain	Red (%)	Green (%)	Blue (%)
Baboon	7.9992	7.9991	7.9993
Pepper	7.9991	7.9992	7.9992
House	7.9992	7.9991	7.9991

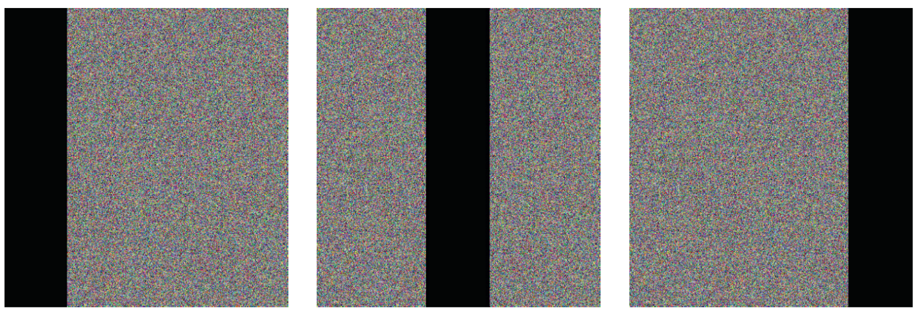
where the well-known sign function is referred to as sign(), while C_is refer to the cipher image. In Table 5, the evaluated values of UACI and NPCR are given for the three submitted plain images. It is observed that the values of NPCR are generally greater than 99.5, while those of UACI are greater than 33.4, which indicates the sensitivity to a pixel change in the proposed encryption algorithm.

5.6. Cropping Attack. In order to detect the robustness of the proposed technique, some blocks of size 450×100 of a cipher house image are converted into black. The restored image after is depicted in Figure 11. Although there is a loss of significant information, the encrypted image after the decryption process is still recognizable.

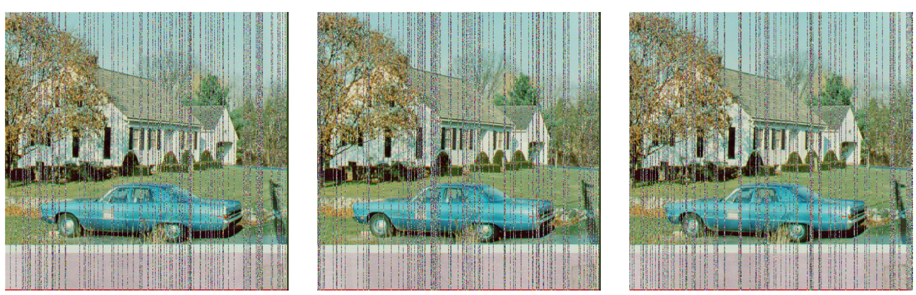
Finally, the aforementioned results are summarized. The proposed encryption technique combines the pseudo-chaos of modified chaotic lemniscate map [47], which has a distinct complicated dynamics and large value of positive Lyapunov exponent with the fractal images generated by complex discrete fractional Gauss map. When compared with different state-of-the-art chaos-based encryption techniques, the main advantages of the present encryption technique are as follows: (a) it deploys superior positive values of maximum Lyapunov exponents. For example, the maximum value of Lyapunov exponent of chaos employed in the image encryption system [48] and bit-level

Table 5: NPCR and UACI results for red, green, and blue images for baboon, pepper, and house images, respectively.

Image		NPCR (%)	UACI (%)
Baboon	Red	99.601	33.559
	Green	99.6015	33.4034
	Blue	99.6133	33.534
Pepper	Red	99.6281	33.5021
	Green	99.597	33.4069
	Blue	99.5901	33.5242
House	Red	99.598	33.4591
	Green	99.5817	33.4822
	Blue	99.5936	33.542



(a)



(b)

Figure 11: The encrypted house image after converting the left, middle, and right blocks, respectively, of the house image into black color (a) and the corresponding recognizable decrypted images (b).

permutation spatial system [48] is less than three, while it is greater than 30 in the present scheme. (b) The pseudo-chaotic time series tame the possible degradation of statistical features of chaos signals in the cases, where they are applied immediately [46]. (c) The assigned keys for the suggested encryption technique are set in a way that renders them controlled by plain data features as well as the time moment of their processing. This means that if identical plain images are encrypted at different instants, different secret keys will be used for the encryption process inducing different cipher images. Moreover, the pseudo-chaos or lower bound errors between the outputs of two interval extensions are employed in the presented scheme instead of applying chaotic signals directly in permutation and diffusion stages. This adds another layer of security and hides the internal characteristics of chaos generators maps. More details about the lower bound errors and analysis of interval extensions can be found in references [49, 50]. Now, the critical scenario of known-plaintext attack (KPA) is considered, where the opponent successfully attains the specific plain image and corresponding cipher image, and then he cannot proceed further to obtain any extra useful information about secret keys' values, which will be used for upcoming plain images as the scheme utilizes time-varying secret keys. The proposed encryption technique can resist KPA even in special cases when uniform plain images with zero values of pixels are deployed, which may lead to a degenerate performance in other encryption techniques [52–54]. The adoption of fractal images in the scheme boosts complexity, key space range, and security performance. Moreover, if the opponent employs chosen-ciphertext attack (CCA) to supply some specially selected cipher images to decryption part of the scheme, he would not fulfill his target too.

The running time of the proposed encryption scheme on personal computer with 16 GB RAM and Intel Core i7-8550U CPU 1.8 GHz is approximately 0.582 s for 450×450 colored images. The comparison aspects with some recent chaos-based encryption techniques are summarized in Table 6. The MCC and AVR abbreviations are used to denote

Table 6: Some comparisons with recent chaos-based encryption techniques.

Work	UACI	NPCR	MLE	Entropy	Key space	MCC	AVR (sec)
Proposed work	33.532	99.814	Up to 60	7.999	2^{3922}	0.0031	0.582
Reference [55] (2 rounds)	33.484	99.809	2	7.903	2^{318}	0.0191	0.385
Reference [56]	33.421	99.611	2	7.997	2^{312}	0.0131	1.860
Reference [57]	33.452	99.607	0.82	7.991	2^{187}	0.0082	0.478
Reference [58]	33.411	99.610	6.756	7.998	2^{399}	0.0143	0.8342

the maximum correlation coefficients attained in all directions of encrypted color baboon/pepper images and average running time, respectively.

6. Conclusion

This study establishes a framework to study dynamical and fractal characteristics, in addition to potential applications, of generalized complex-valued discrete fractional Gaussian map. The occurrence of Mandelbrot and Julia sets of the proposed map is scrutinized at different scenarios for values of parameters. The control and synchronization problems of Julia sets in the complex domain are addressed. A combined pseudo-chaos-fractal image encryption technique is introduced as an efficient tool to resist several kinds of attacks. A thorough security analysis is carried out to validate its robustness and efficiency against statistical, differential, and cropping attacks. Indeed, there is a trade-off between increasing chaoticity and security strength from one side and computational speed from the other side. The present application in this work is the first step and subsequent work will focus on realization aspects on a suitable digital hardware platform, that is, DSP or FPGA, further reduce its running time, and discuss all possible issues that need separate work and cannot be treated here. Future work can also involve extending this study to the case of higher dimensional complex fractional maps [31, 32].

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research work was funded through the project number (IF-PSAU-2021/01/17817) by the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia. The authors extend their appreciation to the Deputyship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (IF-PSAU-2021/01/17817).

References

[1] S. H. Strogatz, *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*, CRC Press, Boca Raton, Florida, 2018.

[2] Y. A. Kuznetsov, *Elements of Applied Bifurcation Theory*, Springer Science & Business Media, Berlin/Heidelberg, Germany, 2013.

[3] J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector fields*, Springer Science & Business Media, Berlin/Heidelberg, Germany, 2013.

[4] E. M. Izhikevich, *Dynamical Systems in Neuroscience: The Geometry of Excitability and Bursting*, Mit Press, Cambridge, MA, 2007.

[5] P. N. V. Tu, *Dynamical Systems- an Introduction with Applications in Economics and Biology*, Springer-Verlag, Berlin/Heidelberg, Germany, 1995.

[6] D. Baleanu and A. M. Lopes, *Applications in engineering, life and social sciences, part b, in Handbook of Fractional Calculus with Applications*, De Gruyter, Germany, 2019.

[7] Y. Sun and W. Sumelka, "Fractional viscoplastic model for soils under compression," *Acta Mechanica*, vol. 230, no. 9, pp. 3365–3377, 2019.

[8] M. A. Matlob and Y. Jamali, "The concepts and applications of fractional order differential calculus in modeling of viscoelastic systems: a Primer," *Critical Reviews in Biomedical Engineering*, vol. 47, no. 4, pp. 249–276, 2019.

[9] S. Aman, I. Khan, Z. Ismail, and M. Zuki Salleh, "Applications of fractional derivatives to nanouids: exact and numerical solutions," *Mathematical Modelling of Natural Phenomena*, vol. 13, pp. 1–12, 2018.

[10] Y. Zhang, H. Sun, H. H. Stowell, M. Zayernouri, and S. E. Hansen, "A review of applications of fractional calculus in Earth system dynamics," *Chaos, Solitons & Fractals*, vol. 102, pp. 29–46, 2017.

[11] A. M. A. El-Sayed, H. M. Nour, A. Elsaid, A. E. Matouk, and A. Elsonbaty, "Dynamical behaviors, circuit realization, chaos control, and synchronization of a new fractional order hyperchaotic system," *Applied Mathematical Modelling*, vol. 40, no. 5–6, pp. 3516–3534, 2016.

[12] R. Hilfer, *Applications of Fractional Calculus in Physics*, World Scientific, New Jersey, 2000.

[13] N. Engheia, "On the role of fractional calculus in electromagnetic theory," *IEEE Antennas and Propagation Magazine*, vol. 39, no. 4, pp. 35–46, 1997.

[14] F. Jarad, E. Uurlu, T. Abdeljawad, and D. Baleanu, "On a new class of fractional operators," *Advances in Difference Equations*, vol. 2017, pp. 1–16, 2017.

[15] F. Jarad, T. Abdeljawad, and D. Baleanu, "Caputo type modification of the Hadamard fractional derivatives," *Advances in Difference Equations*, vol. 2012, pp. 1–8, 2012.

[16] T. Abdeljawad, "On Riemann and Caputo fractional differences," *Computers & Mathematics with Applications*, vol. 62, no. 3, pp. 1602–1611, 2011.

[17] S. Momani and R. W. Ibrahim, "On a fractional integral equation of periodic functions involving Weyl-Riesz operator in Banach algebras," *Journal of Mathematical Analysis and Applications*, vol. 339, no. 2, pp. 1210–1219, 2008.

[18] K. Diethelm and N. J. Ford, "Analysis of fractional differential equations," *Journal of Mathematical Analysis and Applications*, vol. 265, no. 2, pp. 229–248, 2002.

[19] R. Singh, A. U. Rehman, A. U. Rehman et al., "Fractional order modeling and analysis of dynamics of stem cell differentiation in complex network," *AIMS Mathematics*, vol. 7, no. 4, pp. 5175–5198, 2022.

[20] P. Agarwal, R. P. Agarwal, and M. Ruzhansky, *Special Functions and Analysis of Differential Equations*, CRC Press, Boca Raton, Florida, 2020.

[21] L.-L. Huang, G.-C. Wu, D. Baleanu, and H. Y. Wang, "Discrete fractional calculus for interval-valued systems," *Fuzzy Sets and Systems*, vol. 404, pp. 141–158, 2021.

[22] A. Elsonbaty and A. A. Elsadany, "On discrete fractional-order Lotka-Volterra model based on the Caputo difference discrete operator," *Mathematical Sciences*, pp. 1–13, 2021.

[23] G. C. Wu, M. Luo, L. L. Huang, and S. Banerjee, "Short memory fractional differential equations for new memristor and neural network design," *Nonlinear Dynamics*, vol. 100, no. 4, pp. 3611–3623, 2020.

[24] Y. Wang, S. Liu, and H. Li, "On fractional difference logistic maps: dynamic analysis and synchronous control," *Nonlinear Dynamics*, vol. 102, no. 1, pp. 579–588, 2020.

[25] C. Goodrich and A. C. Peterson, *Discrete Fractional Calculus*, Springer International Publishing, Germany, 2015.

[26] K. Falconer, *Fractal Geometry: Mathematical Foundations and Applications*, John Wiley & Sons, Chichester, 2014.

[27] B. B. Mandelbrot, C. J. Evertsz, and M. C. Gutzwiller, *Fractals and Chaos: The Mandelbrot Set and beyond*, Springer, Salmon Tower Building New York City, 2004.

[28] H. Peitgen, H. Jurgens, and D. Saupe, *Chaos and Fractals: New Frontiers in Science*, Springer-Verlag, Berlin/Heidelberg, Germany, 1992.

[29] A. Deshpande and V. D. Gejji, "Chaos in discrete fractional difference equations," *Pramana - Journal of Physics*, vol. 87, no. 4, pp. 1–10, 2016.

[30] Y. Peng, K. Sun, and S. He, "Synchronization for the integer-order and fractional-order chaotic maps based on parameter estimation with JAYA-IPSO algorithm," *The European Physical Journal Plus*, vol. 135, no. 3, pp. 1–12, 2020.

[31] S. S. Pakhare, S. Bhalekar, and P. M. Gade, "Synchronization in coupled integer and fractional-order maps," *Chaos, Solitons & Fractals*, vol. 156, Article ID 111795, 2022.

[32] S. S. Pakhare, V. D. Gejji, D. S. Badwaik, A. Deshpande, and P. M. Gade, "Emergence of order in dynamical phases in coupled fractional gauss map," *Chaos, Solitons & Fractals*, vol. 135, Article ID 109770, 2020.

[33] Y. WangE, S. Liu, and H. Li, "Adaptive synchronization of Julia sets generated by Mittag-Leffler function," *Communications in Nonlinear Science and Numerical Simulation*, vol. 83, Article ID 105115, 2020.

[34] Y. Wang, S. Liu, and W. Wang, "Fractal dimension analysis and control of Julia set generated by fractional Lotka-Volterra models," *Communications in Nonlinear Science and Numerical Simulation*, vol. 72, pp. 417–431, 2019.

[35] S. Askar, A. Al-Khedhairi, A. Elsonbaty, and A. Elsadany, "Chaotic discrete fractional-order food chain model and hybrid image encryption scheme Application," *Symmetry Plus*, vol. 13, no. 2, p. 161, 2021.

[36] A. E. Elfiqi, H. S. Khallaf, S. F. Hegazy, A. Elsonbaty, H. M. H. Shalaby, and s. S. A. Obayya, "Chaotic polarization-assisted ${L}$ DPSK-MPPM modulation for free-space optical communications," *IEEE Transactions on Wireless Communications*, vol. 18, no. 9, pp. 4225–4237, 2019.

[37] L. Kocarev and S. Lian, *Chaos-Based Cryptography*, Springer, Salmon Tower Building New York City, 2011.

[38] P. Stavroulakis, *Chaos Applications in Telecommunications*, CRC Press, Boca RatonFlorida, 2006.

[39] G. Chen and X. Yu, *Chaos Control- Theory and Applications*, Springer, Salmon Tower Building New York City, 2003.

[40] Z. Lin, G. Wang, X. Wang, S. Yu, and J. Lü, "Security performance analysis of a chaotic stream cipher," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1003–1017, 2018.

[41] A. Sonbaty, S. F. Hegazy, and S. S. Obayya, "Simultaneous concealment of time delay signature in chaotic nanolaser with hybrid feedback," *Optics and Lasers in Engineering*, vol. 107, pp. 342–351, 2018.

[42] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[43] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[44] L.-C. Cao, Y.-L. Luo, S.-H. Qiu, and J.-X. Liu, "A perturbation method to the tent map based on Lyapunov exponent and its application," *Chinese Physics B*, vol. 24, no. 10, p. 100501, 2015.

[45] C. Li, T. Xie, Q. Liu, and G. Cheng, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1545–1551, 2014.

[46] E. G. Nepomuceno, L. G. Nardo, J. Arias-Garcia, D. N. Butusov, and A. Tutueva, "Image encryption based on the pseudo-orbits from 1D chaotic map," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29, no. 6, Article ID 061101, 2019.

[47] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany, and E. A. A. Hagras, "Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves," *IEEE Access*, vol. 8, pp. 57733–57748, 2020.

[48] L. Hongjuna and W. Xingyuan, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, pp. 3320–3327, 2010.

[49] E. G. Nepomuceno, S. A. M. Martins, G. F. V. Amaral, and R. Riveret, "On the lower bound error for discrete maps using associative property," *Systems Science & Control Engineering*, vol. 5, no. 1, pp. 462–473, 2017.

[50] R. E. Moore and R. B. Kearfott, *Introduction to Interval Analysis*, SIAM, Thailand, 2009.

[51] Z. Y. Qian, W. X. Yuan, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Information Scientist*, vol. 273, pp. 329–351, 2014.

[52] Z. Lin, S. Yu, X. Feng, and J. Lü, "Cryptanalysis of a chaotic stream cipher and its improved scheme," *International Journal of Bifurcation and Chaos*, vol. 28, no. 7, pp. 1850086–1850112, 2018.

[53] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[54] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[55] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Processing*, vol. 164, pp. 249–266, 2019.

[56] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[57] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Optics and Lasers in Engineering*, vol. 128, Article ID 106040, 2020.

[58] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.