Ghost attractor in fractional order blinking system and its application

F. M. Kamal1*, A. Elsaid1,2, A. Elsonbaty1,3
1. Department of Engineering Mathematics and Physics, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt
2. Department of Mathematics, Basic and Applied Sciences School, Egypt-Japan University of Science and Technology, New Borg El-Arab City, Alexandria, 21934, Egypt.
3. Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia.

October 20, 2021

Abstract

In this paper, the occurrence of ghost attractor is verified in three cases of a proposed fractional order Rössler blinking system. Firstly, the dynamical behaviors of the short memory fractional order prototype-4 Rössler system with Chua’s diode are explored via bifurcation diagrams and Lyapunov exponents. It is depicted that this system exhibits a variety of dynamics including limit cycles, period doubling and chaos. Then, a proposed non-autonomous fractional order Rössler blinking system is introduced. Numerical simulations are employed to confirm the existence of ghost attractors at specific cases which involve very fast switching time between two composing autonomous fractional subsystems. It is found that the presented fractional order blinking system is very sensitive to system parameters, initial conditions and stochastic process parameters. Thus, the induced chaotic ghost attractor is utilized in a suggested ghost attractor-based chaotic image encryption scheme for first time. Finally, a detailed security analysis is carried out and reveals that the proposed image cryptosystem is immune against different types of attacks such as differential attacks, brute force attacks, cropping and statistical attacks.

1 Introduction

In recent decades, the applications of fractional calculus in the area of dynamical systems have attracted great interest. Indeed, many theoretical and experimental studies indicated that fractional order derivatives have many advantages in modeling intricate systems in contrast to conventional treatment using integer order calculus [1]. The essential reason is that fractional derivative possesses hereditary properties and can mimic memory effects in some nonlinear systems [2]. So, fractional order differential equations have successfully modeled many real applications, such as neural networks [3, 4], biological systems [5, 6], financial systems [7, 8], secure communications [9], electronic circuit models [10, 11, 12], nonlinear mechanical problems [13, 14] and many more. Fractional order switched system which includes switching parameter based on logical rule has recently drawn the attention of several researchers [15, 16].

Switched system is a hybrid dynamical system that is composed of a number of dynamical subsystems and has a specific rule to control the switching between its subsystems with time [17, 18]. Stochastic processes are usually employed to externally drive these blinking non-autonomous systems at the specified values of switching time scales. More specifically, there is a predetermined fixed period of time $\tau$ through which the dynamics of blinking system is determined by one of its composing subsystems then a random switching to another subsystem is done for the same time interval $\tau$ and the process continues in this way as long as the blinking system is running. The blinking systems have appeared in many realistic models in biology, the internet networks, and circuits like power converters where the connections are randomly switched on and off in time. Assuming that the blinking system has $n$ subsystems, the coupling between subsystems in each time interval of duration $\tau$ is done stochastically with probability $p_i$, $i = 1, 2, ..., n$.

In blinking systems, there are two time-scales belonging to the stochastic process and the blinking system itself. In fast-switching blinking systems, the time scale of stochastic process is much faster than intrinsic time scale of the dynamical subsystems of the blinking system. This means that the switching is considered to be fast according to its value in comparison with intrinsic time scale of the blinking system [19]. The switching occurs randomly and independently for different time intervals and connections in the system. It is found that the blinking systems can exhibit non-trivial and unexpected nonlinear behaviors which surprisingly do not exist in each of the composing subsystems [20]. The averaged systems...
associated to the blinking systems which are given by the expectation of stochastic variables have attractors called ghost attractors of the blinking systems if they are different from the set of attractors in the composing subsystems \[21\].

Up to now, the study and investigation of blinking systems have been reported in few works. For example, Belykh et al. \[22\] showed an example of a blinking system and the corresponding synchronization in small-world networks. Hasler et al. \[23\, 24\] investigated the dynamics, finite time properties and asymptotic properties of a stochastically blinking system. Barabash and Belykh \[20\] proved the existence of ghost attractors for certain parameter ranges in the blinking piecewise-linear Lorenz-type system being unexpectedly different with respect to the attractors of composing systems. Levanova et al. \[21\] obtained a ghost attractor in blinking Lorenz and Hindmarsh–Rose systems in spite of the trivial dynamics of the associated subsystems at selected values of parameters which is defined by stable equilibrium points.

In recent years, because of the rapid development of multimedia technologies and the increased exchange of multimedia data over the internet, the need to devise effective tools to make the transmitted multimedia secured and well preserved is becoming increasingly important \[25\]. Images have main features such as redundancy, a strong correlation between adjacent pixels, and a large amount of data. According to these features, the need to encryption schemes suitable for image encryption rather than traditional encryption algorithms such as DES, AES and RSA \[26\] for text encryption is required. In the last decades, researchers have developed algorithms based on chaos theory that are suitable for images encryption \[27\, 28\]. Chaotic systems are extremely sensitive to control parameters and initial values. In additions, inherent characteristics such as unpredictability, pseudorandomness and ergodicity are employed for keystream generation \[29\, 30\]. The required cryptographic characteristics through image diffusion and confusion can be achieved through the fascinating features of the image encryption techniques relying on chaotic systems \[31\]. The applicability of the fractional order chaotic systems and fractional order chaotic maps to image encryption are investigated to further enhance the security of the cryptosystem and increase key-space in several articles \[32\, 33\, 34\, 35\].

It is worth mentioning that all the aforementioned works are only concerned with blinking systems in integer order forms. Inspired by the above discussion, the main contributions of this paper is to study fractional order blinking system composed of two fractional order Rössler prototype-4 autonomous continuous time subsystems based on Chua’s diode nonlinearity. Random switching between internal parameters of the proposed system occurs stochastically and evolves over time. To the best of authors knowledge, this first time to explore of the ghost attractor in fractional order blinking systems. This work is organized such that firstly, the short memory fractional order Rössler system is studied using Lyapunov spectrum, bifurcation diagrams. Secondly, a fractional order blinking system is presented in three cases involving different values of intrinsic parameters of the fractional order Rössler system. The randomly and rapidly switching time between two values of fractional blinking system parameter is verified to yield a chaotic attractor which goes near the chaotic ghost attractor of the associated fractional order averaged system. Detailed numerical simulations are utilized to explore chaotic ghost attractors. Thirdly, fractional order blinking system is considered for the first time to present an image encryption scheme to improve cryptosystem security and further increase the secret key space. Finally, the proposed scheme is analyzed by several security tests to show the immunity against different attacks.

The layout of this paper is structure as follows: The mathematical preliminaries and definitions are summarized in Section 2. The fractional order blinking Rössler system is introduced in Section 3 along with its detailed numerical investigation. In Section 4, the chaotic image encryption scheme based on fractional order blinking system is proposed and the security analysis is conducted. The discussion and future work is concluded in Section 5.

## 2 Mathematical preliminaries

This section addresses the definition of fractional order Caputo derivative, the definition of short memory fractional differential equation, the definition of fractional blinking system and the associate fractional order averaged system.

Recently, many definitions for fractional order derivatives have been well-established. We focus on the Caputo fractional derivative \[1\]. The Caputo fractional derivative of order \( \alpha \) of function \( f(t) \) is defined as follows

\[
C_{t_0}^D_t \alpha f(t) = \frac{1}{\Gamma(1-\alpha)} \int_{t_0}^t \frac{f(s)}{(t-s)^\alpha} ds, \quad 0 < \alpha < 1,
\]

where \( \Gamma(\cdot) \) is the Gamma function. The standard fractional order system in Caputo sense is defined as follows \[36\]

\[
C_{t_0}^D_t \alpha x(t) = f(t,x(t)), \quad x(t_0) = x_0,
\]

where \( t_0 \) is a fixed starting point of the fractional derivative.

### Definition of short memory fractional order system

The standard fractional order system \[2\] holds the memory from \( t = t_0 \). The weight coefficients of \( x(t_0) \) be-
come smaller as the time $t$ increases. The meaning of short memory is summarized in Fig. 1. Let the

$$\mathcal{D}_t^\alpha x = f(t,x), \quad \mathcal{D}_t^\alpha x = f(t,x), \quad \mathcal{D}_t^\alpha x = f(t,x)$$

Figure 1: Short memory fractional order system.

interval $[t_0, T]$ is divided into $m$ subintervals with length $nh$ and $n$ is an integer number such that $[T - t_0] = [t_0, t_1] \cup [t_1, t_2] \cup \ldots \cup [t_{(m-1)}, t_m], h = (T - t_0)/N$. In the first subinterval $t \in [t_0, t_1]$, the fractional order system is described as $C^\alpha_{t^*} D_t^\alpha x(t) = f(t,x)$, then in the second subinterval $t \in [t_1, t_2]$, the fractional order system is described as $C^\alpha_{t^*} D_t^\alpha x(t) = f(t,x)$ so, the initial point is updated to $t_1$ and so on until the last subinterval.

Subsequently, the short memory fractional order system which holds short memory effect is defined as follows

$$C^\alpha_{t^*} D_t^\alpha x(t) = f(t,x), \quad x(t_0) = x_0, \quad t_\ast = t_k, \quad t \in [t_k, t_{k+1}], \quad k = 0, \ldots, m - 1. \quad (3)$$

The equation (3) has different initial points $t_\ast$ in the Caputo fractional derivative $[1]$. This provides more freedom degrees in real-world applications.

Definition of the fractional order blinking system

The blinking system is presented in [23] and it is defined in the form of time dependent ordinary differential equations. Here, we generalize the concept to the fractional order blinking system by defining it as

$$C^\alpha_{t^*} D_t^\alpha x(t) = f(t,x), \quad x(t_0) = x_0, \quad f : R^N \to R^N, \quad s(t) \in \{0, 1\}^M, \quad (4)$$

where $C^\alpha_{t^*} D_t^\alpha$ is a short memory derivative and the function $s(t)$ is a binary random constant discrete scalar value such that $s^i = (s^i_1, \ldots, s^i_M)$ with the probability $p_i$ at each $i$th time piecewise constant in the time interval $[i\tau, (i + 1)\tau]$ and $\tau$ is a constant switching period. All variables $s^i$ are random variables and independent and they take the value 1 with probability $p$ and the value 0 with probability $1 - p$. So, the switching sequence of the stochastic process is determined according to $s(t)$. Hence, this system is considered as a special case of random dynamical systems and its solution also is a stochastic process. The signal $s_i$ can be viewed as a closing and opening eye lid therefore, the system Eq. (4) is called a blinking system. The trajectories of $M$ autonomous systems are blinded together at $t = i\tau$ to consist the trajectories of system Eq. (4). In this type of system, there are two-time scales which are the one associated with the dynamical system itself and the other of the switching process. In this work, the switching process is considered to be much faster than the dynamical subsystems.

Definition of the fractional order averaged system

The fractional order averaged system associated with the fractional order blinking system Eq. (4) reads as

$$C^\alpha_{t^*} D_t^\alpha x(t) = \Phi(x(t)), \quad (5)$$

where

$$\Phi(x) = E(f(x,s)) = \sum_{s \in \{0, 1\}^M} f(x,s)p_s, \quad (6)$$

and $E(f(x,s))$ denotes the average or expected value of $f(x,s)$.

3 Proposed fractional order blinking systems

3.1 Fractional order prototype-4 Rössler system with short memory

We propose the following fractional order version of the prototype-4 Rössler system with short memory [38] as follows

$$C^\alpha_{t^*} D_t^\alpha x = y + qz, \quad C^\alpha_{t^*} D_t^\alpha y = -\beta x, \quad (7)$$

$$C^\alpha_{t^*} D_t^\alpha z = g(y) - \gamma z.$$

where $q, \beta$ and $\gamma$ have positive values and $g(y)$ is a piecewise-linear function with definition as

$$g(y) = m_1y + \frac{1}{2}(m_0 - m_1)(|y + 1| - |y - 1|), \quad (8)$$

where $m_0$ and $m_1$ are constants. Nonlinearity in Eq. (7) is known as a nonlinear component which called the Chua’s diode [39]. We call (7) a short memory fractional differential equation since the fractional derivative is defined from $t_\ast$ not from the fixed $t_0$ or 0. To solve (7) numerically, starting from initial conditions at $t = 0$ and updating initial conditions at each stage. We can get each subsystem as follows. For $t \in (0, t_1)$ and the initial conditions ($x_0, y_0, z_0$) are known, we solve the following subsystem

$$C^\alpha_0 D_t^\alpha x = y + qz, \quad C^\alpha_0 D_t^\alpha y = -\beta x, \quad C^\alpha_0 D_t^\alpha z = g(y) - \gamma z. \quad (9)$$
Then, for $t \in [t_k, t_{k+1}]$ with $(x_k, y_k, z_k)$ is known from the system on $[t_{k-1}, t_k]$ and we get the subsystem

\begin{align}
C_t \tau_m y &= y + qz, \\
C_t \tau_m \beta y &= -z, \\
C_t \tau_m \gamma z &= g(y) - \gamma z.
\end{align}

In spite of the simplicity of system Eq. (2), the dynamical behaviors of this system are complex depending on the value of the bifurcation parameters. Firstly, unlike the case of limit cycle presence in integer order systems, the limit set of a solution trajectory of fractional order system cannot be a constant periodic solution of the system. In additions, the nonexistence of periodic solutions was proved in time-invariant fractional order systems in [40]. However, some examples were given where the solutions of the fractional order system are not periodic, but they asymptotically converge to periodic signals [11].

Summarizing these results, the limit cycle that appears in phase portrait of the fractional order system is not a solution of the system, but it attracts nearby solutions. Secondly, some aspects of nonlinear dynamics of the model will be investigated in the following subsection.

### 3.1.1 Influence of system parameters

The bifurcation strategies have been successfully deployed to handle nonlinear properties of complex systems. Different bifurcation parameters have been explored in this section to investigate the dynamical behaviors of the system Eq. (2). Firstly, all the system parameters are fixed at values $\alpha = 0.98$, $\gamma = 1$, $m_0 = -1.5$, $m_1 = 0.3$, $q = 3$ and we start analyzing the sensitivity of system by varying each parameter individually. Fig. (2a) and Fig. (2b) show the bifurcation diagram and Lyapunov exponents spectrum, respectively, for bifurcation parameter $\beta$ in the range $[0.2, 3]$. For $0.4 \leq \beta \leq 0.85$ there is 6-period doubling and 0.85 $\leq \beta \leq 3$ the system goes to chaos. By fixing $\beta = 1$ and varying parameter $\gamma$ in range $[0.6, 3.6]$, the bifurcation diagram and Lyapunov exponents plots are illustrated in Fig. (2c) and Fig. (2d), respectively. In range $[0.6, 1.3]$ the system exhibits chaotic behavior and goes to 4-period doubling then 2-period doubling in the range $[1.3, 3.6]$. Then, we fix $\gamma = 1$ and explore the parameter $m_0$ within range $-2 \leq m_0 \leq -0.5$. It is noticed that from $m_0 = -2$ to $m_0 = -1.8$ and from $m_0 = -1.6$ to $m_0 = -0.75$ the system has chaotic behavior soon after that it tends to period doubling in two ranges $[-1.8, -1.6]$ and $[-0.75, -0.5]$ as displayed in Fig. (3a) and Fig. (3b). In addition, the value of parameter $m_0 = -1.5$ is fixed to analyze the effect of changing the value of parameter $m_1$ in range $0 \leq m_1 \leq 0.36$. It can be seen from Fig. (3c) and Fig. (3d) that the system is stable in the interval $[0, 0.01]$ then it undergoes period doubling within the interval $[0.01, 0.07]$ until it reaches the chaos behavior in the interval $m_1 \in [0.07, 0.36]$. We study the effect of varying parameter $q$ in the interval $[0, 4.5]$ as displayed in Fig. (4a) and Fig. (4b). The system is stable in the interval $[0, 0.7]$ then goes to 2-period doubling and 4-period doubling in the range $[0.7, 1.9]$ after that the system exhibits chaotic behavior.

The fractional order $\alpha$ is now considered as the bifurcation parameter to show its effects on the dynamics of the proposed system (7). The dynamics of the system with varying fractional order $\alpha$ in the range 0.5 to 1. We fix $q = 3$ and varying fractional order $\alpha$, the bifurcation diagram and Lyapunov exponents plots are obtained in Fig. (5a) and Fig. (5b), respectively. It is shown that from $\alpha = 0.5$ to $\alpha = 0.68$ it is a stable region. A cascade of period doublings in ranges $[0.68, 0.78]$ and $[0.875, 0.91]$ are observed. Then the system (7) shows chaotic dynamics over the ranges of $0.78 \leq \alpha \leq 0.875$ and $0.91 \leq \alpha \leq 1$.

![Figure 2](image-url)

**Figure 2:** (a) and (b) bifurcation diagram of the proposed fractional-order system and Lyapunov exponents, respectively, versus $\beta$ for $\beta \in [0.2, 3]$. (c) and (d) bifurcation diagram of the proposed fractional-order system and Lyapunov exponents, respectively, versus $\gamma$ for $\gamma \in [0.6, 3.6]$.

### 3.2 Fractional order blinking system

We propose fractional order blinking Rössler system $R(q)$ with Chua’s diode non-linearity as follows

\begin{align}
C_t \tau_m \alpha x &= y + q(t)z, \\
C_t \tau_m \beta y &= -\beta x, \\
C_t \tau_m \gamma z &= g(y) - \gamma z,
\end{align}

with time-varying parameter $q(t) = (q_1 - q_2)s(t) + q_2$. Based on random sequence, the parameter $s(t)$ switches in the non-autonomous system Eq. (11) between two
The emerging attractor of fractional order averaged system is referred to as ghost attractor if it is different from the set of attractors in the subsystems of corresponding integer order systems studied previously in literature. In first case, the solution trajectory of the system (11) is attracted to periodic orbit in phase space at $q = 0.75$ as shown in Fig. (6) and at $q = 3.83$ as shown in Fig. (7) with other parameters values $\beta = 1, \gamma = 1, m_0 = -1.5, m_1 = 0.3, \alpha = 0.98$ and $T = 500$, using a unit step $h = 0.005$. Accordingly, the blinking system Eq. (11) switches in random between first subsystem $R_1(q_1 = 0.75)$ with probability $p_1 = \frac{22}{100}$ and second subsystem $R_2(q_2 = 3.83)$ with probability $p_2 = \frac{78}{100}$. The fractional order averaged autonomous system associated with the fractional order blinking system (11) where $E(R(q, s(t)))$ is the expected value of $R(q, s(t))$ is $R_{\text{avg}}(q_{\text{avg}} = 3.1524)$ where $q_{\text{avg}} = p_1 \ast q_1 + p_2 \ast q_2$. The induced interesting ghost attractor is shown in Fig. (8). It is noticed that the trajectory of blinking system moves around the ghost attractor and after sufficient time remains close to the ghost attractor which means that it reaches a small neighborhood of the ghost attractor with appropriate fast switching. Indeed, the chaotic attractor of the fractional order averaged system represents the ghost attractor for the fractional order blinking system as shown in Fig. (9). Time series from the systems for first subsystem, second subsystem, averaged system and switching system are all depicted in Fig. (10).

3.3.1 Case 1

In second case, the system (7) has like a periodic behavior at $q = 1.8$ as shown in Fig. (11) and at $q = 3.34$ as shown in Fig. (12) with other parameters values as in Case 1 except $m_1 = 0.35$. Thus, the blinking system (11) randomly switches between first subsystem $R_1(q_1 = 1.8)$ with probability $p_1 = \frac{30}{100}$ and second subsystem $R_2(q_2 = 3.34)$ with probability $p_2 = \frac{70}{100}$.
system $R_2(q_2 = 3.34)$ with probability $p_2 = \frac{70}{100}$. The fractional order averaged system associated with the fractional order blinking system Eq. (11) where $E(R(q, s(t)))$ is the expected value of $R(q, s(t))$ as $R_q(q_{avg} = 2.878)$ where $q_{avg} = q_1 + q_2$. The ghost attractor of fractional order averaged system is shown in Fig. (13). For fast switching time, Fig. (14) displays the trajectory of fractional order blinking system reaches a small neighborhood of the ghost attractor and remains there. Time series of the solutions of first subsystem, second subsystem, averaged system and blinking system are depicted in Fig. (15).

3.3.3 Case 3

In third case, the system (11) has a stable equilibrium point at $q = 0.8, \gamma_1 = 2.4$ as shown in Fig. (16) and the solution trajectory of the system is attracted to periodic orbit in phase space at $q = 2.58, \gamma_2 = 0.8$ as shown in Fig. (17) with other parameters values $\beta = 1, \gamma = 1, m_0 = -1.5, m_1 = 0.3, \alpha = 0.98$ and $T = 700$, using a unit step $h = 0.005$. Thus, the blinking system (11) randomly switches between first subsystem $R_1(q_1 = 0.8, \gamma_1 = 2.4)$ with probability $p_1 = \frac{90}{100}$ and second subsystem $R_2(q_2 = 2.58, \gamma_2 = 0.8)$ with probability $p_2 = \frac{93.5}{100}$. The fractional order averaged autonomous system associated with the fractional order blinking system Eq. (11) where $E(R(q, s(t)))$ is the expected value of $R(q, s(t))$ as $R_a(q_{avg} = 2.4643, \gamma_{avg} = 0.904)$ where $q_{avg} = q_1 + q_2 + q_{avg} = q_1 + q_2$. The behavior of the averaged system is shown in Fig. (18). The trajectory of blinking system remains in a small neighborhood of the ghost attractor as shown in Fig. (19). Time series solutions of the first subsystem, second subsystem, averaged system and switching system are depicted in Fig. (20).

3.3.4 Euclidean distance

In this part, we calculate the Euclidean distance between the attractor of the blinking system and the ghost attractor. The Euclidean distance is an approximation of the
distance between invariant measures of the blinking system attractor and the ghost attractor. It is defined as [21]

\[ \delta(\tau) = \frac{1}{N} \left( \sum_{j=1}^{N} (h^T_j - h^q_j)^2 \right)^{1/2}, \]  

(12)

where \( h^T_j = \frac{h^T_1}{T_s}, \frac{h^T_2}{T_s}, ..., \frac{h^T_N}{T_s} \) represents a distribution of \( T_s \) calculated phase points which is taken from the attractor of blinking system after neglecting the sufficient transient interval at chosen value of switching period \( \tau \).

Similarly, \( h^q_j = \frac{h^q_1}{T_s}, \frac{h^q_2}{T_s}, ..., \frac{h^q_N}{T_s} \) is a distribution which is taken from the ghost attractor of fractional averaged system from these \( T_s \) points to the box \( D_j \), \( j = 1, ..., N \). These calculations are considered in the selected domain defined as \( D : x_i^- < x_i < x_i^+ \), \( i = 1, 2, 3 \) which contains both two attractors of the blinking system and the averaged system. The two boundaries in each \( i^{th} \) direction of domain \( D \) are denoted by \( x_i^- \) and \( x_i^+ \). The \( D \) region is divided into \( N = \prod_i N_i \) small boxes. The value of \( h_j \) represents the number of times that the solution trajectory hits the boundaries of box \( j \) after the initial transient time is ignored.

The Euclidean distance \( \delta(\tau) \) has been used to quantify the closeness of the attractors of blinking system with those of the averaged system when the value of switching time is varied. In numerical simulations, the Euclidean distance is evaluated in the domain \( D : x \in [-11, 13], y \in [-13, 13], z \in [-5.5, 5.5] \) and divide it into \( N = N_x \times N_y \times N_z \). For simplicity, we take \( N_x = N_y = N_z \) i.e. equal number of boxes in each direction such that \( N = 10^6 \). We select interval length \( T = 500 \) and \( T = 700 \) as it is used in the previous numerical simulation with the integration step 0.005 after neglecting \( 2 \times 10^4 \) iterations of the transition interval. For the switching period \( \tau \in [0.005, 1] \), the Euclidean distance \( \delta(\tau) \) is evaluated and displayed in Fig. [21]. It is noticed that the distance \( \delta(\tau) \) rapidly increases for very small values of \( \tau \) then undergoes slight changes for further values till \( \tau = 0.1 \).
This means that the attractor of system Eq. (11) changes under fast switching time $\tau < 1$ in a slight way. The attractors of the fractional blinking system Eq. (11) for the three presented cases are shown in Fig. 9, Fig. 14 and Fig. 19. Accordingly, it is highly probable that the ghost attractor and the attractor of fractional order blinking system sufficiently remain close to each other with the advance of time.

4 Image encryption algorithm

In this section, we are motivated by the characteristics of the proposed system Eq. (11) as its high sensitivity to initial conditions, parameter values of chaotic system and the stochastic process to propose an image encryption scheme that utilizes this system.
4.1 Algorithm steps

The algorithm is mainly composed of two parts: plain image pixel shuffling without changing the pixels values and image diffusion. The steps of the encryption strategy are illustrated below.

**Step 1.** Read the plain image $I_{M \times N}$ as a matrix with dimensions $M \times N$, where $M$ is the length and $M$ is the width.

**Step 2.** Evaluate a constant $img_c$ as a perturbation value which depends only on the image to be ciphered, and it is defined as

$$img_c = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} I(i, j), \quad (13)$$

where $i$ and $j$ are the pixel positions of original image $I$.

The image constant $img_c$ is added to one of the system parameters as a perturbation value to make the original image contributes in evaluating the secret key. We choose to add $img_c$ to the fractional derivative $\alpha$ in the three examples that are used in our procedure.

**Step 3.** To get the chaotic time series as $x(i), y(i), z(i)$, $i = 1, 2, ..., n, n = M \times N$, we first eliminate the transient values, then we take the time series with the required size where $x, y, z$ are the solutions of fractional order blinking system.

**Step 4.** Standardize the values of the state variables as follows

$$key_i = \text{mod}(\text{floor}(x_i \times 10^{15}), 256),$$

$$row_i = \text{mod}(\text{floor}(y_i \times 10^{15}), 512) + 1,$$

$$col_i = \text{mod}(\text{floor}(z_i \times 10^{15}), 512) + 1. \quad (14)$$

We get $x_i, y_i, z_i$ from solving fractional order blinking system Eq. (7) as the state variables. To obtain the value of the secret key $key_i$ value within range [0, 256] as image pixels value, we use mod operation among the state variable $x, y, z$ and 256. Also, we use mod operation between the state variables $y_i, z_i$ and 512 to get a new position for pixels value image matrix $I$ as shuffling process.

**Step 5.** We set a simple scheme from three steps to get $RW(j)$ and $CL(j)$ as a new position of image pixels where $j = 1, 2, ..., 512$.

**S1.** We used the generated values row and col to select from them first 512 different values.

**S2.** Use the first value $RW(1)$ in $RW(j)$ in ascending order with all values in $CL(j)$.

**S3.** To fit all the position of matrix $I$, repeat the second step 511 times where the pixels value remains unchanged.

**Step 6.** To set the secret key in matrix form the reshape function is used as follows

$$Key_s = \text{reshape}(key, M, N). \quad (15)$$

**Step 7.** Rearrange the pixels position as shuffle process.
as follows

\[ I_{sh}(i,j) = I(RW(i), CL(j)), \quad (16) \]

where \( I_{sh} \) and \( I \) are the matrix for shuffle and plain images, respectively, where \( i = 1, 2, \ldots, M \) and \( j = 1, 2, \ldots, N \) are the image matrix dimensions.

**Step 8.** Apply bitwise XOR operation between \( Key_s \) and \( I_{sh} \) to establish the encrypted image \( I_{en} \) as follows

\[ I_{en}(i,j) = I_{sh}(i,j) \oplus Key_s(i,j). \quad (17) \]

To reconstruct the original image, the encryption steps are reversed. So, the decryption procedure is presented as

**Step 1.** Apply the bitwise XOR operation between \( I_{en} \) and \( Key_s \) to attain decrypted image \( I_{de} \) as follows

\[ I_{de}(i,j) = I_{en}(i,j) \oplus Key_s(i,j). \quad (18) \]

**Step 2.** The image pixel positions are reversed to obtain the original image \( I_{dsh} \) as

\[ I_{dsh}(RW(i), CL(j)) = I_{de}(i,j). \quad (19) \]

The proposed encryption scheme is applied on three different images as shown in Fig. [22] which depicts the original, shuffled, encrypted and decrypted images for the presented algorithm.

4.2 Security analysis

A good encryption scheme should defend against all sorts of known and common attacks such as differential attack, the brute force attacks and statistical attacks. Various security tests have been used on encrypted images to assess the proposed image cryptosystem. These tests include histogram, information entropy, pixel correlation, differential attack, key space and cropping attack. We have chosen three images: Pepper, Man and Baboon image of size 512 \( \times \) 512 to explore the security of the proposed encryption scheme. The chaotic time series from the third case of fractional order blinking system has been used to generate new row, column image pixel positions and the secret key. In addition, the perturbation values \( img_c \) for Pepper, Man and Baboon are \( 4.5710 \times 10^{-4}, 2.9686 \times 10^{-4} \) and \( 4.9284 \times 10^{-4} \), respectively are used to make the system solutions depend on the plain image and increase the robust the encryption scheme.

4.2.1 Histogram analysis

Image histogram is an important criterion to measure the performance of encryption algorithm. It can describe the intensity distribution of image gray-scale level. In order to protect the information of the plain image to stand up against the statistical attacks, the statistical characteristics of pixel values in plain image should be eliminated to bear no statistical similarity to the original image. The good image encryption algorithm will lead to a flat or uniform histogram of encrypted image. Fig. [23] depicts the results of histogram analysis which is evaluated to Pepper, Man and Baboon images. It is shown that the encrypted image histogram is uniform and is different from the original image so, it is effectively resisting the statistical attacks.

The variance related to histograms is evaluated using

\[ Var(h) = \frac{1}{G^L_L} \sum_{i=0}^{G^L-1} \sum_{j=0}^{G^L-1} \frac{1}{2} (h_i - h_j), \quad (20) \]

where \( G^L_L = 256 \) is the grey level and \( h = [h_1, h_2, \ldots, h_{256}] \) where \( h_i \) and \( h_j \) are the numbers of pixels. The histogram variances for original and ciphered images are depicted in Table [1]. The reduction for Pepper, Man and Baboon images, respectively is verified with values approximate 99.8%.

4.2.2 Information entropy

In this subsubsection, we explore one of main features of randomness which is the information entropy. The greater information entropy means image pixels are less
4.2.3 Correlation analysis

The characteristic of image data is inherited by high correlation of adjacent pixels. Therefore, the correlation of adjacent pixels in the encrypted images should be as small as possible. To test the correlation coefficient \( r_{uv} \) between \( u, v \) as the gray-scale values of two adjacent pixels, the \( r_{uv} \) formula is defined as

\[
r_{uv} = \frac{\text{cov}(u, v)}{\sigma_u \sigma_v},
\]

where \( \text{cov}(u, v) \) is the covariance function, \( E(u) = \frac{1}{N} \sum_{i=1}^{N} u_i \) and \( \sigma_u = \frac{1}{N} \sum_{i=1}^{N} (u_i - E(u))^2 \). In vertical, horizontal and diagonal directions of the plain image and ciphered image, the value of correlation between two adjacent pixels are calculated for Pepper, Man and Baboon images and are shown in Table 2. Through the obtained results, we noticed that the correlations in the plain image are strong since the correlation coefficients are all around 0.8 and 0.97. And the correlation coefficients of the ciphered image are smaller and all around zero in the presented scheme, which demonstrates the insignificant correlation between adjacent pixels.

Table 2: In vertical, horizontal and diagonal directions of the plain image and ciphered image, the correlation values between two adjacent pixels are presented for Pepper, Man and Baboon images, respectively.

|                  | Horizontal | Vertical | Diagonal |
|------------------|------------|----------|----------|
| Pepper           | 0.9765     | 0.9788   | 0.9636   |
| Cipher           | -0.0009    | 0.004    | -0.0010  |
| Man              | 0.9572     | 0.9699   | 0.9433   |
| Cipher           | -0.0013    | -0.0001  | 0.0035   |
| Baboon           | 0.8749     | 0.7779   | 0.7404   |
| Cipher           | -0.0018    | -0.0020  | 0.0007   |

4.2.4 Differential attack

The cryptosystem should be kept safe from the different types of attacks. For a robust cryptosystem, an essential feature as differential attack is needed to analyze. To reflect the differences in the ciphers due to the changes in the encrypting keys which means that a slight change of secret key will cause an obvious distinction in the cipher-image. In order to test this feature, there are two benchmark values \( (NPCR) \) and \( (UACI) \) as in [43]. These evaluate the difference among the encrypted images obtained from an original image and its slightly modified copy. \( NPCR \) is used to calculate the total number of different pixels in the original cipher and modified ciphers. It is defined as

\[
\text{NPCR} = \frac{\sum_{i,j} \delta_{ij}}{M \times N} \times 100\%
\]

\[
\text{UACI} = \frac{1}{MN} \sum_{i,j} \frac{|C_{ij} - P_{ij}|}{\max(255,1) - \min(0,1)} \times 100\%
\]

where \( \delta_{ij} \) is defined as

\[
\delta_{ij} = \begin{cases} 
1 & \text{if } C_{ij} \neq P_{ij} \\
0 & \text{otherwise}
\end{cases}
\]

and \( M \), \( N \) are the number of rows and columns of the image.

Table 1: The variances for original, encrypted images for Pepper, Man and Baboon, respectively and their reduction.

|                  | Variance |
|------------------|----------|
|                  | Plain    | Encrypted | Reduction(%) |
| Pepper           | 481160   | 1012.6    | 99.7896      |
| Man              | 1163300  | 1024      | 99.9120      |
| Baboon           | 761390   | 1008.9    | 99.8675      |

feasible to show information for the encryption scheme.

The information entropy calculated by the following formula

\[
H(X) = \sum_{i=1}^{2^N-1} p_i \log_2 \frac{1}{p_i},
\]

where \( X \) is an input symbol, \( p_i \) is probability value of symbol \( X \) and \( H(X) \) is the entropy in bits. Image pixels are more invisible when \( H(X) \approx 8 \) for a encrypted image. The entropy values for Pepper, Man and Baboon images have been calculated as 7.9993, 7.9993, 7.9993, respectively. Consequently, the calculated entropy is approximately 8 therefore, the proposed scheme has a good property of information entropy and decoding encrypted image is less possible from attackers.
Table 3: The results of NPCR and UACI tests for Pepper, Man and Baboon, respectively.

|       | NPCR(%) | UACI(%) |
|-------|---------|---------|
| Pepper| 99.6204 | 33.4059 |
| Man   | 99.6254 | 33.4929 |
| Baboon| 99.6124 | 33.3543 |

\[
NPCR(\%) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |\text{sign}(C_1(i,j) - C_2(i,j))|}{MN} \times 100,
\]

where \(C_i\) is the ciphered image and \(\text{sign}()\) is the sign function. The UACI is used to obtain average difference in the pixel intensity in the original cipher \(C_1\) and the modified cipher \(C_2\). It is calculated by

\[
UACI(\%) = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100.
\]

The ideal results to NPCR and UACI tests for encryption schemes should be near to 100% and 33.33%, respectively as ideal results. Results of these two tests are introduced in Table 3. It is obvious that the calculated NPCR and UACI for the proposed encryption algorithm are very close to the ideal value and is highly sensitive to image pixel change and mismatched keys.

4.2.5 Key space

The robust image encryption algorithm should have key space with value greater than \(2^{100}\) at least \([43]\) to withstand brute-force attacks. In the presented scheme, the secret key is composed of the double precision based on the parameters of the chaotic systems, \(q_1, q_2, \gamma_1, \gamma_2, p_1, p_2, m_0, m_1, \alpha, (x_0, y_0, z_0), \text{img}_c\). The digits number are to be at least \(10^{-15}\) in each parameter. The key space of the presented scheme is \(10^{195}\) and it is effectively enough to stand up against violent attack.

4.2.6 Cropping attack

The cropping attacks are used to examine the immunity of encryption scheme to information loss. To study the robustness in defend the cropping attack \([45]\), we replaced an internal block of the ciphered image with size \(512 \times 100\) into black with left, middle and right positions. The black blocks inside the ciphered image and the decrypted images are displayed in Fig. 24. It is noticed that recovered images are all recognizable in spite of the significant information loss.

5 Conclusion

Over the past twenty years, the study of integer order blinking systems has been considered in few works. In this work, we have presented a blinking system in fractional order model for first time. We have shown through thorough numerical simulation that the attractor of fractional order blinking system follows the ghost attractor of the corresponding fractional order averaged system when the switching time is sufficiently fast. We utilized the chaotic time series of resulting ghost attractor in a novel encryption scheme. The presented image encryption scheme successfully stands against different types of attacks with a high level of security. In addition, we can also deal with other fractional order blinking systems rather than Rössler prototype-4 system and using them in color image cryptosystem in future work.

Data availability All data generated or analysed during this study are included in this article.

Funding: No funds.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

[1] J. T. A. Kilbas, H. Srivastava, Theory and application of fractional differential equations, Elsevier, New York, 2006.

[2] A. Elsadany, A. Matouk, Dynamical behaviors of fractional-order lotka-volterra predator–prey model and its discretization, J. Appl. Math. Comput. 49 (2015) 269–283.

[3] P. Xiong, H. Jahanshahi, R. Alcaraz, Y. Chu, J. Gómez-Aguilar, F. Alsaadi, Spectral entropy
analysis and synchronization of a multi-stable fractional-order chaotic system using a novel neural network-based chattering-free sliding mode technique, Chaos, Solitons and Fractals 144 (2021) 110576.

[4] C. Xu, M. Liao, P. Li, S. Yuan, Impact of leakage delay on bifurcation in fractional-order complex-valued neural networks, Chaos, Solitons and Fractals 142 (2021) 110535.

[5] J. Yuana, L. Zhao, C. Huangb, M. Xiaob, Stability and bifurcation analysis of a fractional predator–prey model involving two nonidentical delays, Mathematics and Computers in Simulation 181 (2021) 562–580.

[6] P. Trikha, E. Mahmoud, L. Jahanzaib, R. Matouog, M. Abdel-Aty, Fractional order biological snap oscillator: Analysis and control, Chaos, Solitons and Fractals 145 (2021) 110763.

[7] B. Xin, J. Zhang, Finite-time stabilizing a fractional-order chaotic financial system with market confidence, Nonlinear Dyn 79(2) (2015) 1399–1409.

[8] Y. Li, C. Sun, H. Ling, A. Lu, Y. Liu, Oligopolies price game in fractional order system, Chaos, Solitons and Fractals 132 (2020) 109583.

[9] Y. Yang, B. Guan, J. Li, D. L. and Y. Zhou, W. Shi, Image compression-encryption scheme based on fractional order hyperchaotic systems combined with 2d compressed sensing and dna encoding, Optics and Laser Technology 119 (2019) 105661.

[10] A. El-Sayed, H. Nour, A. Elsaïd, A. Matouk, A. Elsonbaty, Dynamical behaviors, circuit realization, chaos control, and synchronization of a new fractional order hyperchaotic system, Applied Mathematical Modelling 40 (2016) 3516–3534.

[11] A. El-Sayed, A. Elsonbaty, A. Eld sadany, A. Matouk, Dynamical analysis and circuit simulation of a new fractional-order hyperchaotic system and its discretization, International Journal of Bifurcation and Chaos 26 (2016) 1650222.

[12] R. Bansal, Stochastic filtering in fractional-order circuits, Nonlinear Dyn (2020).

[13] Y. Sun, Y. Gao, S. Song, Effect of integrating memory on the performance of the fractional plasticity model for geomaterials, Acta Mech. Sinica 34 (2018) 896–901.

[14] R. Liu, J. Niu, Y. Shen, S. Yang, Stability and bifurcation analysis of two-degree-of-freedom vibro-impact system with fractional-order derivative, International Journal of Non-Linear Mechanics 126 (2020) 103570.

[15] T. Kaczorek, Stability of positive fractional switched continuous-time linear systems, Technical Sciences 61 (013) 0033.

[16] T. Feng, L. Guo, B. Wu, Y. Chen, Stability analysis of switched fractional-order continuous-time systems, Nonlinear Dyn 102 (2020) 2467–2478.

[17] A. Lin, P. Antsaklis, Stability and stabilizability of switched linear systems: A survey of recent results, IEEE Transactions on Automatic Control 54 (2009).

[18] Q. Yu, X. Zhao, Stability analysis of discrete-time switched linear systems with unstable subsystems, Applied Mathematics and Computation 273 (2016) 718–725.

[19] I. Belykh, V. Belykh, R. Jeter, M. Hasler, Multistable randomly switching oscillators: The odds of meeting a ghost, Eur. Phys. J. Special Topics 222 (2013) 2497–2507.

[20] N. Barabash, V. Belykh, Non-stationary attractors in the blinking systems: Ghost attractor of lorenz type, Cybernetics and Physics 8 (2016) 209–214.

[21] N. Barabash, T. Levanova, V. Belykh, Ghost attractors in blinking lorenz and hindmarsh–rose systems, Chaos 30 (2020) 081105.

[22] I. Belykh, V. Belykh, M. Hasler, Blinking model and synchronization in small-world networks with a time-varying coupling, Physica D 195 (2004) 188–206.

[23] M. Hasler, V. Belykh, I. Belykh, Dynamics of stochastically blinking systems. part i: Finite time properties, SIAM J. Applied Dynamical Systems 12 (2013) 1031–1084.

[24] M. Hasler, V. Belykh, I. Belykh, Dynamics of stochastically blinking systems. part ii: Asymptotic properties, SIAM J. Applied Dynamical Systems 12 (2013) 1031–1084.

[25] C. Li, Z. Li, Y. T. W. Feng, J. Du, D. Wei, Dynamical behavior and image encryption application of a memristor-based circuit system, Int. J. Electron. Commun. (AEÜ) 110 (2019) 152861.

[26] A. Belazi, A.EL-Latif, R. Rhouma, S. Belghith, Selective image encryption scheme based on dwt, aes s-box and chaotic permutation, International wireless communications and mobile computing conference (IWCMC), IEEE (2015) 606–610.

[27] X. Wang, Y. Li, J. Jin, A new one-dimensional chaotic system with applications in image encryption, Chaos, Solitons and Fractals 139 (2020) 110102.
[28] G. Kaur, R. Agarwal, V. Patidar, Chaos based multiple order optical transform for 2d image encryption, Engineering Science and Technology 23 (2020) 998–1014.

[29] S. K. F. Musanna, A novel image encryption algorithm using chaotic compressive sensing and nonlinear exponential function, Journal of Information Security and Applications 54 (2020) 102560.

[30] S. Askar, A. Al-khedhairi, A. Elsonbaty, A. Elsadany, Chaotic discrete fractional-frder food chain model and hybrid image encryption scheme application, symmetry 13 (2021) 161.

[31] M. Zhou, C. Wang, A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks, Signal Processing 171 (2020) 107484.

[32] F. Yang, J. Mou, C. Ma, Y. Cao, Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application, Optics and Lasers in Engineering 129 (2020) 106031.

[33] Y. Sun, H. Zhang, X. yuan Wang, X. qing Wang, P. Yan, 2d non-adjacent coupled map lattice with q and its applications in image encryption, Applied Mathematics and Computation 373 (2020) 125039.

[34] M. Talhaoui, X. Wang, A new fractional one dimensional chaotic map and its application in high-speed image encryption, Information Sciences.

[35] S. Ismail, L. Said, A. Radwan, A. Madian, M. Abu-ElYazeed, A novel image encryption system merging fractional-order edge detection and generalized chaotic maps, Signal Processing.

[36] Y. Lia, Y. Chen, I. Podlubny, Stability of fractional-order nonlinear dynamic systems: Lyapunov direct method and generalized Mittag–Leffler stability, Comput. Math. Appl. 59 (2010) 1810–1821.

[37] G. Wu, Z. Deng, D. Baleanu, D. Zeng, New variable-order fractional chaotic systems for fast image encryption, Chaos 29 (2019) 083103.

[38] P. Kuate, A. Tchendjeu, H. Fotsin, A modified rossler prototype-4 system based on chua’s diode nonlinearity : Dynamics, multistability, multiscroll generation and fpga implementation, Chaos, Solitons and Fractals 140 (2020) 110213.

[39] L. Chua, M. Komuro, T. Matsumoto, The double scroll family, parts i and ii, IEEE Trans. Circuits. Syst. 33 (1986) 1073–1118.

[40] M. Tavazoei, M. Haeri, A proof for non existence of periodic solutions in time invariant fractional order systems, Automatica 45 (2009) 1886–1890.

[41] M. Tavazoei, A note on fractional-order derivatives of periodic functions, Automatica 46 (2010) 945–948.

[42] M. Lahdir, H. Hamiche, S. Kassim, M. Tahanout, K. Kemih, S. Addouche, A novel robust compression-encryption of images based on split coding and fractional-order discrete-time chaotic system, Optics and Laser Technology 109 (2019) 534–546.

[43] Y. Wu, J. Noonan, S. Agaian, Npcr and uaci randomness tests for image encryption, Cyber J. Multidisciplinary J. Sci. Technol. (2011) 31–38.

[44] E. Barker, A. Roginsky, Transitions, recommendation for transitioning the use of cryptographic algorithms and key lengths[j], NIST Special Publication 131A (2011) 800.

[45] A. Ullah, S. Jamal, T. Shah, A novel scheme for image encryption using substitution box and chaotic system, Nonlinear Dyn. 91 (2018) 359–370.