Design of a Fractional Pseudo-Chaotic Random Number Generator

Chunxiao Yang, Ina Taralova, J.-J. Loiseau, Safwan El-Assad

Design of a Fractional Pseudo-Chaotic Random Number Generator

Chunxiao Yang, Ina Taralova,
Jean-Jacques Loiseau
Laboratoire des Sciences du Numérique de Nantes
LS2N, UMR CNRS 6004
Ecole Centrale de Nantes
Nantes, France

Safwan El Assad
Institut d'Electronique et des Technologies du Numérique
IETR, UNR CNRS 6164
Université de Nantes/Polytech Nantes
Nantes, France

Abstract

In this paper, we design a pseudo-chaotic random number generator using fractional chaotic systems. A non-uniform grid calculation method is proposed and employed to numerically solve the fractional systems by introducing a skew-tent map to vary the step size of the grid. Greater chaoticity in terms of Lyapunov exponent has been achieved by applying the proposed approach to the solution calculation of the fractional chaotic Chen's and Lu's systems. By adopting the piecewise constant argument method, one 1D fractional generalized double-humped logistic system (FGDHL) is discretized. A fractional pseudo-chaotic random number generator (FPCRNG) has been proposed by performing XOR (exclusive-or) operations to the states of the fractional Chen's system, fractional Lu's system, and the FGDHL systems. The security analysis of the generator and the statistical experiment of a stream cipher implementing the proposed FPCRNG prove that the proposed structure is efficient and can be used in the cryptosystem design.

1. Introduction

With the development of information technology, people now are plunging into an Information Explosion Era in an inevitable and irreversible way. While being free to access excessive information with a simple click of the mouth or on the cellphone, one also exposes themselves to the danger of personal information leakage. Therefore, information security, especially for multimedia data such as images, videos, etc., has become a prevalent topic which not only attracts researchers' attention but also affects the everyday life of everyone. The demand for the secure processing of data containing confidential information is witnessing constant growth. Cryptosystems with novel techniques or structures are called upon for both the transmission and the storage of the data.

To meet the demand of novel secure cryptosystems, many researchers have oriented their investigation to the use of nonlinear systems with chaotic behavior [1][2]. The pseudo-random generators have been designed based on chaotic systems due to their numerous merits, such as random-like behavior and the sensitivity to the initial conditions and parameters [3]. The outputs of the generator work as dynamic keys to the cryptosystem for the encryption process.

On the other hand, fractional calculus has existed for a long time in the field of mathematic. The use of it in science and engineering applications has started to be explored in recent decades. Fractional dynamic systems described by fractional differential equations have been considered suitable for modelling many real-life systems due to the memory effect and hereditary properties[4]. They have been applied successfully in diverse disciplines like physics, biology, economics, etc.[5][6].

The fractional systems with chaotic behavior have also attracted a lot of attention. Compared to the classical integer chaotic system, the fractional chaotic systems are much more complex and less studied in the literature. One reason for this is because there are different definitions for fractional calculus [7], and the fact that the systems' chaotic behavior differs with different numerical methods chosen to solve the fractional differential equations, also adds to its intricacy. However, from the aspect of the cryptosystem, this complexity also bears great merits and possibilities. Due to the intricate geometric interpretation of the fractional derivatives, the fractional chaotic system possesses higher nonlinearity and degrees of

freedom [8]. The latter could be used to enlarge the secret key space, which in turn, increases the complexity of the cryptosystem.

In [9][10], the authors discussed the possibility of using the fractional chaotic system to design random number generators. However, by applying only one fractional system in the generator structure, their research remains straightforward and unsophisticated. Further studies are needed to make their discussed work suitable for applications in secure information transmission. In this work, we take a step forward in fractional chaotic pseudo-random number generator (FPCRNG) design by combining 3 different fractional chaotic systems. In addition, a non-uniform grid for the numerical calculation of the fractional chaotic systems' solutions is proposed by employing a skew-tent map to vary the grid spaces. Both the coupling of the systems and the use of the non-uniform grid introduce extra chaoticity to the structure, along with the expansion of key space from the aspect of cryptosystem design.

The paper is organized as follows: In section 2, some fundamental knowledge on fractional calculus and fractional systems is illustrated. A non-uniform grid calculation approach is proposed in section 3 where the skew-tent map is also discussed to form the grid. In section 4, the systems adopted to design the FPCRNG and their chaotic behaviors are discussed. In section 5, the FPCRNG structure is illustrated and its performance is analyzed. The security analysis of a stream cipher using the proposed generator is given in section 6. Finally, the conclusion is drawn in the last section.

2. Preliminaries

In this section, some basic knowledge of the fractional calculus and the fractional system is reviewed.

2.1. Fractional calculus

Fractional calculus discusses the integrals and derivatives of non-integer order. It is a generalization of integration and differentiation to non-integer order fundamental operator ${}_aD_t^{\alpha}$, and the term fractional is kept only for historical reason.

There are different definitions for fractional calculus, here, we list out two frequently discussed definitions, Riemann-Liouville (RL) definition, and Caputo definition. Some properties are also recalled. For a more comprehensive introduction of fractional calculus, one can refer to [11] and other textbooks.

The fractional integral of fractional order α ($\alpha > 0$) under RL definition is described as follows,

$$ {}_aI_t^{\alpha} f(t) = \frac{1}{\Gamma(\alpha)} \int_a^t (t-\tau)^{\alpha-1} f(\tau)\, d\tau \tag{1} $$

for $a \in \mathrm{R}$ and $\alpha < 0$. The formula is a generalization of the standard integral, which is the particular case of RL integral when $\alpha = 1$.

$\Gamma(.)$ in the formula represents the Euler Gamma function and holds the form as below,

$$ \Gamma(\alpha) = \int_0^{\infty} \frac{t^{\alpha-1}}{e^t} dt. \tag{2} $$

The RL definition for the fractional derivative is the left inverse of ${}_aI_t^{\alpha}$ and is described as the formula below,

$$ {}_aD_t^{\alpha} f(t) = D^n\, {}_aI_t^{\alpha} f(t) = \frac{1}{\Gamma(n-\alpha)} \frac{d^n}{dt^n} \int_a^t \frac{f(\tau)}{(t-\tau)^{\alpha-n+1}}\, d\tau \tag{3} $$

where $n = \lceil \alpha \rceil$ is the smallest integer greater or equal to α. D^n denotes the standard integer-order derivative. a and t are the limits of operation ${}_aD_t^{\alpha}$.

It is to be remarked that for a causal function $f(t)$, when $t < 0$, $f(t) = 0$, and we have $a = 0$. Therefore, a fractional derivative in the Caputo sense with $f(t)$ being causal can be defined as follows

$$ D_*^{\alpha} f(t) = I^{n-\alpha} D^n f(t) = \frac{1}{\Gamma(n-\alpha)} \int_0^t (t-\tau)^{n-\alpha-1} f^{(n)}(\tau)\, d\tau \tag{4} $$

where $n - 1 < \alpha \le n$, $t > 0$. The following properties apply,

$$ \begin{aligned} D_*^{\alpha} I^{\alpha} f(t) &= f(t), \\ I^{\alpha} D_*^{\alpha} f(t) &= f(t) - \sum_{k=0}^{n-1} f^{(k)}(0^+) \frac{t^k}{k!}, \quad t > 0 \end{aligned} \tag{5} $$

The Caputo definition is widely applied in engineering applications due to the fact that the fractional differential equations of the Caputo type are competent in providing the applied problems with clearly interpretable initial conditions.

2.2. Fractional systems

The fractional system, if explained briefly, is the dynamic system that can be modeled by differential equations with non-integer order derivatives [12].

As mentioned before, the differential equations in the Caputo sense are chosen in most cases to depict and solve applied problems. So, here the fractional differential equation of the Caputo type is illustrated as in the following form,

$$ D_*^{\alpha} x(t) = f(t, x(t)) \tag{6} $$

the initial conditions are of the form

$$ x^{(k)}(0) = x_0^k, k = 0, 1, 2, \ldots, n-1. \tag{7} $$

where $n := \lceil \alpha \rceil$ denotes the fractional order celling.

The system equation which described the fractional system consists of a series of fractional differential equations. It is to be remarked that, if the fractional derivatives in the fractional differential equations take

different values, the system is incommensurate. Otherwise, the system is commensurate.

In our following work, the systems discussed have a commensurate order between 0 and 1 for all their fractional derivatives. Hence, their system equations can be expressed as,

$$\begin{aligned} D_i^{\alpha} x_i(t) &= f_i\left(x_1(t), x_2(t), ..., x_n(t), t\right) \\ x_i(0) &= c_i, i = 1, 2, ..., n. \end{aligned} \tag{8}$$

where c_i denote the initial conditions, and α is the commensurate fractional order.

3. Non-uniform grid calculation method for the fractional systems

In this section, we propose a non-uniform grid calculation method for the fractional system solutions based on the classical fractional Corrector-predictor Adams-Bashforth-Moulton method (ABM).

The characteristics and properties of the chaotic skew-tent map are firstly reviewed and discussed. The calculation method whose step size is determined by the skew-tent map's outputs is then illustrated explicitly.

3.1. Characteristics of the skew-tent map

The skew tent map used in our paper is formulated as given in equation (9),

$$\mathrm{Xst}(n) = \begin{cases} \dfrac{\mathrm{Xst}(n-1)}{p}, & 0 < \mathrm{Xst}(n-1) \le p \\ \dfrac{1-\mathrm{Xst}(n-1)}{1-p}, & p < \mathrm{Xst}(n-1) \le 1 \end{cases}, \tag{9}$$

where $\{\mathrm{Xst}(n), n = 0,1,2,3,...\}$ represents the iterated states and p is the control parameter.

Similar to the tent map, the graphical expression of the skew-tent map takes the form of a triangle with its right-side slope equal to the value of parameter p, left-slope equal to 1-p, and its summit at (p,1). The phase plans for three different p values 0.25, 0.5, and 0.9 are given in Fig. 1(a). The initial value Xst(0) is 0.3.

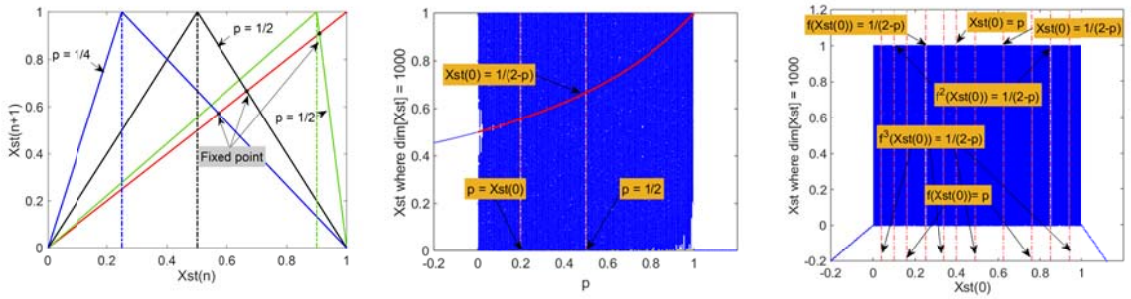
The intersections of the phase plan and the bisector Xst(n+1)) = x(n) (in red) denote the fixed points of the map. It is easy to see that the map has two fixed points, 0 and 1/(2-p).

It is to be remembered that the fixed points should be excluded when one aims to design maps with chaotic behavior. One should also avoid the initial values that are the pre-images of the fixed points because they also lead to the fixed points after iterating forward.

The bifurcation diagram is a graph that gives a visual illustration of the system states' values versus the evolution of the parameters. It shows the changes in the dynamic behavior of the chaotic map with the variation of the parameter values.

From the bifurcation diagrams of the skew-tent map over different p values with Xst(0) = 0.2 given in Fig.1(b). It can be seen that from p equals -0.2 to 1 and 1 to 1.2, the values of the skew-tent map's states, Xst(n), remain unchanged for every p. However, after the transient period, with p varying from 0 to 1, the outputs scattered between (0,1). This verifies that the map is chaotic with its control parameter p chosen in the interval of]0,1[. It can be observed that there are two white lines in Fig. 1(b) at p equal to 1/2 and the initial value Xst(0). When p = Xst(0), the map maps to the fixed point 0 after 2 iterations, so, no chaotic behavior is displayed. When p = 1/2, it is easy to calculate that after several iterations, the map exhibits a periodic behavior with period 2 where the states take one of two values.

Fig. 1(c) shows the impact of the different initial values on the chaotic behavior of the skew-tent map. The control parameter p is set to 0.4. One can observe that when Xst(0) is in the range of [0, 1], the image of the map through iterations also lies in the same range and exhibits chaotic behavior throughout the interval except for a finite set of points. These specific values (where the white lines appear) are the fixed points of the map and their pre-images as mentioned previously.



(a)Skew-tent map graph (b)Bifurcation diagram, Xst(0) = 0.2 (c) Impact of the initial value, p = 0.4

Figure 1. Skew-tennt map

For example, within 3 iterations, the skew-tent map with control parameter p = 0.4, initial value Xst(0) = 0.04 produces the state values Xst(1) = 0.04/0.4 = 0.1, Xst(2) = 0.1/0.4 = 0.25 and Xst(3) = 0.25/0.4 = 0.625, which attains the non-trivial fixed point 1/(2-p).

3.2. Non-uniform grid calculation method for the fractional systems

There are various approaches to numerically calculate the solutions of fractional differential equations. Among all of them, one popular and widely used approach is the fractional Corrector predictor ABM method introduced in[13].

For the classical corrector predictor ABM method, the solutions of the system are calculated on a uniform grid with grid space h setting to a fixed value. The response of the fractional system is numerically calculated by the following equations,

$$\begin{aligned} x_h(t_{n+1}) = &\sum_{k=0}^{\lceil\alpha\rceil-1} \frac{t_{n+1}^k}{k!} x_0^{(k)} + \frac{h^\alpha}{\Gamma(\alpha+2)} f\left(t_{n+1}, x_h^P(t_{n+1})\right) \\ &+ \frac{h^\alpha}{\Gamma(\alpha+2)} \sum_{j=0}^{n} a_{j,n+1} f\left(t_j, x_h(t_j)\right), \end{aligned} \tag{10}$$

where $x_h^P(t_{n+1})$ denotes the predicted value and is expressed as,

$$x_h^P(t_{n+1}) = \sum_{k=0}^{\lceil\alpha\rceil-1} \frac{t_{n+1}^k}{k!} x_0^{(k)} + \frac{1}{\Gamma(\alpha)} \sum_{j=0}^{n} b_{j,n+1} f\left(t_j, x_h(t_j)\right). \tag{11}$$

a and b in the above equations take the form below,

$$a_{j,n+1} = \begin{cases} n^{\alpha+1} - (n-\alpha)(n+1)^\alpha, & \text{if } j = 0, \\ (n-j+2)^{\alpha+1} + (n-j)^{\alpha+1} - 2(n-j+1)^{\alpha+1}, & \text{if } 1 \le j \le n, \\ 1, & \text{if } j = n+1. \end{cases}$$

$$b_{j,n+1} = \frac{h^\alpha}{\alpha}\left((n+1-j)^\alpha \alpha - (n-j)^\alpha\right) \tag{12}$$

According to [14], to avoid the computational error of size 10^{-6}, the grid space h should be set close to 10^{-3} (0.001).

For our work, based on the classical fractional Corrector and predictor ABM method, we proposed a new version of the algorithm with the introduction of a variable discretization step which gives rise to a non-uniform grid for the calculation.

This variable sampling step is determined by the outputs of the skew-tent map discussed previously. The grid space $h(n)$ is obtained by multiplying a fixed value h by i+1 as shown in the following formula,

$$h(n) = h \times (i+1) \text{ if } \mathrm{Xst}(n) \in \left[0.2 \times i,\ 0.2 \times (i+1)\right[, \tag{13}$$

where $i = 0,1,2,3,4,$ and Xst(n) denotes the state of the skew-tent map.

To be more specific, if we set h = 0.001, then the variable sampling step $h(n)$ is given by

$$h(n) = \begin{cases} 0.001, & 0 < \mathrm{Xst}(n) \le 0.2 \\ 0.002, & 0.2 < \mathrm{Xst}(n) \le 0.4 \\ 0.003, & 0.4 < \mathrm{Xst}(n) \le 0.6 \\ 0.004, & 0.6 < \mathrm{Xst}(n) \le 0.8 \\ 0.005, & 0.8 < \mathrm{Xst}(n) \le 1 \end{cases} \tag{14}$$

It is to be noticed that, here we choose 5 sequentially sorted intervals in which lies the Xst(n) to determine the corresponding value of $h(n)$. However, we can also adopt different sorting orders for the intervals. With the change of the sorting intervals, different sampling steps will be provided, leading to distinguished states' values, which might increase the unpredictability of the system output.

By substituting the fixed grid space h by this variable sampling step $h(n)$, the numerical solution of the fractional systems can then be rewritten as the following equations,

$$\begin{aligned} \mathrm{X}(n+1) = &\mathrm{X}(0) + \frac{h(n)^\alpha}{\Gamma(\alpha+2)} f\left(\mathrm{X}^{\mathrm{Pr}}(n+1)\right) \\ &+ \frac{h(n)^\alpha}{\Gamma(\alpha+2)} \sum_{j=0}^{n} a_{j,n+1} f\left(\mathrm{X}(j)\right), \end{aligned} \tag{15}$$

with fractional order $0 < \alpha < 1$, where a remains the same as given in equation (12) and the predictor and b are given by

$$\begin{aligned} \mathrm{X}^{\mathrm{Pr}}(n+1) &= \mathrm{X}(0) + \frac{1}{\Gamma(\alpha)} \sum_{j=0}^{n} b_{j,n+1} f\left(\mathrm{X}(j)\right), \\ b_{j,n+1} &= \frac{h(n)^\alpha}{\alpha}\left((n+1-j)^\alpha - (n-j)^\alpha\right). \end{aligned} \tag{16}$$

By employing this non-uniform grid calculation approach, we achieve get greater chaoticity in terms of Lyapunov Exponent (LE), which in turn, ameliorates the chaotic features of the response. This is to be illustrated in the following section.

4. Fractional chaotic systems used for FPCRNG design

In this section, the fractional chaotic systems used for our FPCRNG design are discussed, namely, the 3D fractional chaotic Chen's and Lu's system, and the fractional generalized double-humped logistic system (FGDHL). The non-uniform grid calculation method proposed in the previous section is adopted to calculate the numerical solutions (the next state value) of the 3D fractional chaotic systems and we explain in detail the FGDHL system and its discretization process. The characteristics and chaotic behaviors of the systems are also discussed.

4.1. Fractional chaotic Chen's and Lu's systems

We employ two 3D fractional systems, Chen's and Lu's systems for our generator design. These fractional systems have been extended directly from the classical Chen's and Lu's systems. Their chaotic behavior has been discussed in papers [15] and [16] respectively.

The system equation for the fractional chaotic Chen's system that we adopt can be expressed as follows,

$$\begin{cases} D^{\beta_c} x_1(t) = a_c\left(x_2(t) - x_1(t)\right) \\ D^{\beta_c} x_2(t) = \left(c_c - a_c\right)x_1(t) - x_1(t)x_3(t) + c_c x_2(t) \\ D^{\beta_c} x_3(t) = x_1(t)x_2(t) - b_c x_3(t) \end{cases} \quad (17)$$

where β_c stands for the identical commensurate fractional derivative order for x_1, x_2, and x_3. (a_c, b_c, c_c) denotes the system parameters.

In Fig. 2(a)-(d), we depict the phase portrait of the fractional Chen's system in different planes. The parameters (a_c, b_c, c_c) is set to (35, 28, 3.2), and the initial condition is (-9, -5, 14).

To evaluate the chaoticity of the system calculated by the non-uniform grid, the Lyapunov exponent (LE) and Maximum Lyapunov exponent (MLE) are used. The LE of a dynamic system characterizes the rate of separation of infinitesimally closely initialized trajectories. And MLE corresponds to the largest LE value among different orientations of the system. An MLE greater than 0 normally indicates the chaotic characteristics of the system.

The MLEs over different fractional orders for Chen's system are given in Fig. 2(e) to compare the impact of the proposed non-uniform grid calculation method and the classical uniform method on the system's chaoticity. The system parameters and initial conditions are the same as for the graphs of the phase portraits in Fig. 2(a)-(d).

It can be observed that for most of the derivative orders in the range of 0.4 to 1, the MLE values (LE for x1) under both calculation methods are greater than 0 from a certain value between 0.45 to 0.55. This confirms that the fractional system is chaotic. What's more, it can be seen that the MLE of the non-uniform grid outputs is greater than that of the classical one, which shows that our proposed calculation method provides the system's outputs with greater chaoticity.

For the fractional chaotic Lu's system, it holds a similar form to the fractional Chen's system and is given in equation (18) below,

$$\begin{cases} D^{\beta_l} x_1(t) = a_l\left(x_2(t) - x_1(t)\right) \\ D^{\beta_l} x_2(t) = -x_1(t)x_3(t) + c_l x_2(t) \\ D^{\beta_l} x_3(t) = x_1(t)x_2(t) - b_l x_3(t) \end{cases} \quad (18)$$

where β_l is the commensurate fractional order, with a_l, b_l, and c_l denoting the system parameters.

The phase portraits of the fractional Lu's system are given in Fig. 2(g)-(j). The parameters are (36, 3, 20) and initial conditions are set to (0.2, 0.5, 0.3). In Fig. 2(k), we also compare the MLE of the proposed calculation method and that of the classical ABM method. It is observable that from a certain value in the interval of [0.5 0.6], the chaotic behavior is exhibited under both calculation methods. In the meantime, with LE non-uniform grid variation exceeding the Le uniform grid variation (the blue curve above the orange curve), the enhancement of chaotic features in terms of Lyapunov Exponent for our proposed non-uniform grid calculation method is confirmed.

The histogram diagrams of the systems' states are employed to have a general idea for the distribution of the fractional systems' outputs and the following study of the PCRNG.

In total, 1000 classes have been adopted to plot the histogram of 31250 states of the fractional systems discussed above. As shown in Fig. 2(f), one can observe that for fractional chaotic Chen's system, the values of the states lie in the interval of [-20 20]. Two peaks close to -10 and 10 in the histogram indicate that there are relatively more states that fall into the classes around these values.

The distribution of the fractional chaotic Lu's system is also given in Fig. 2(l). The graph shows that the lower and upper bound of the states' values are around -20 and 20, respectively, and the values are relatively less attained for each end.

4.2. Fractional generalized double-humped logistic system

The fractional generalized double-humped logistic system (FGDHL), as its name reveals, is the fractional order version of the generalization of the double-humped logistic map.

The original one-dimensional generalized double-humped logistic map can be written as

$$x_{n+1} = \rho\left(x_n - 1\right)^2\left(1^2 - \left(x_n - 1\right)^2\right) \quad (19)$$

where ρ is the growth rate and also the sole parameter in the system. It is called double-humped because it exhibits a double hump in its first iteration.

The one-dimensional generalized double-humped logistic map is discussed in[17] and is described by the equation below,

$$x_{n+1} = \rho\left(x_n - c\right)^2\left(c^2 - \left(x_n - c\right)^2\right) \quad (20)$$

where ρ and c are the control parameters.

The FGDHL used in our work is inspired and extended from this integer order generalized double-

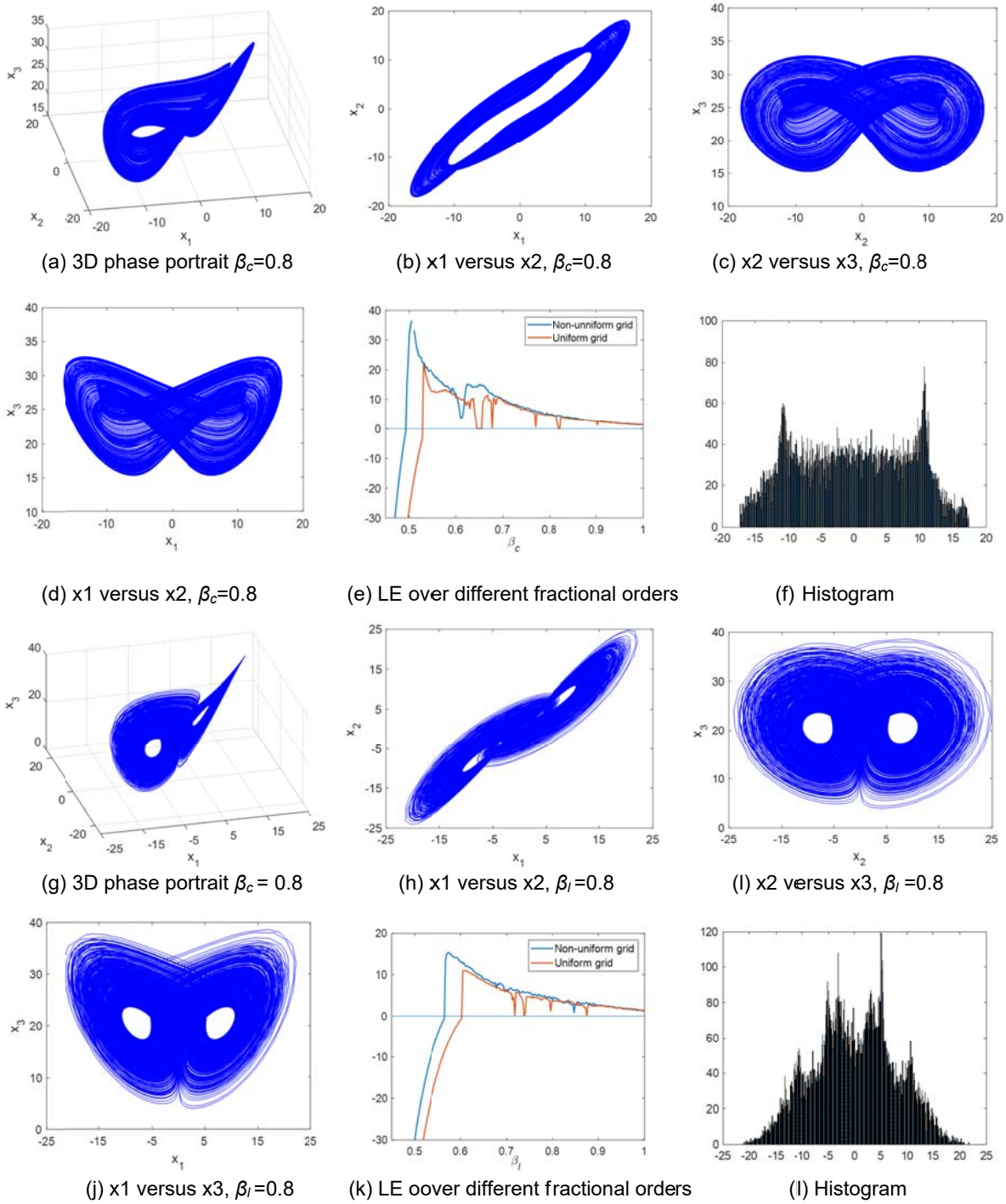
humped logistic map. The differential equation for the considered FGDHL is described as follows,

$$D^{\alpha_g} x_g(t) = \rho\left((x_g(t)-c)^2\left(c^2-\left(x_g(t)-c\right)^2\right)\right), \quad t>0 \quad (21)$$

where $x_g(0)$ is the initial condition, ρ and c are the parameters, and α_g represents the fractional derivative order.

With the introduction of piecewise constant arguments, the corresponding FGDHL system equation can be rewritten as,

$$D^{\alpha_g} x_g(t) = \rho\left(x_g\left(\left[\left[\frac{t}{r}\right]r\right)-c\right)^2\left(c^2-\left(x_g\left(\left[\left[\frac{t}{r}\right]r\right)-c\right)^2\right)\right) \quad (22)$$



(a) 3D phase portrait β_c=0.8 (b) x1 versus x2, β_c=0.8 (c) x2 versus x3, β_c=0.8

(d) x1 versus x2, β_c=0.8 (e) LE over different fractional orders (f) Histogram

(g) 3D phase portrait β_c = 0.8 (h) x1 versus x2, β_l =0.8 (I) x2 versus x3, β_l =0.8

(j) x1 versus x3, β_l =0.8 (k) LE oover different fractional orders (l) Histogram

Figure 2. Chaotic behavior of fractional chaotic Chem's and Lu's system

The discretization process is performed to the above equation using the method described in [18]. And the formula below for the state of the FGDHL is derived,

$$x_g(n+1) = x_g(n) + \frac{r^{\alpha_g}}{\Gamma(1+\alpha_g)} \rho \left(x_g(n)-c\right)^2 \left(c^2 - \left(x_g(n)-c\right)^2\right) \quad (23)$$

We notice that, with different r values, the solutions of the system can be very different. So, for the sake of simplification and consistency, in the following discussion, we set r =0.2.

To briefly discuss the chaotic property of the proposed FGDHL system, the bifurcation diagrams, Lyapunov exponent results, and histogram of the states of the system are given and analyzed from the experimental simulation point of view.

The effect of the control parameter c through bifurcation diagram for different fractional orders α_g from 0.25 to 0.95, while ρ = -4.3 is shown in Fig. 3(a) and 3(b). It can be seen from the figure that with higher fractional order ($0 < \alpha_g < 1$), a greater c value is needed for the system to exhibit chaotic behavior. Besides, the vertical scale of $x_g(n)$ is proportional to the c. That is to say, with the increase of c, the system states fall into a wider range of values.

The bifurcation diagrams for the parameter ρ over different fractional orders are given in Fig. 3(d) and (e). The parameter c is set to 0.9. It is observable that the range for the system state remains approximately the same. In terms of the chaotic behavior, for fractional orders from 0.25 to 0.95, the bifurcation point for the parameter ρ shifted leftwards with the increase of the fractional order value. That is to say that for the system to exhibit chaotic behavior, a smaller ρ value is required with the increase of the non-integer order.

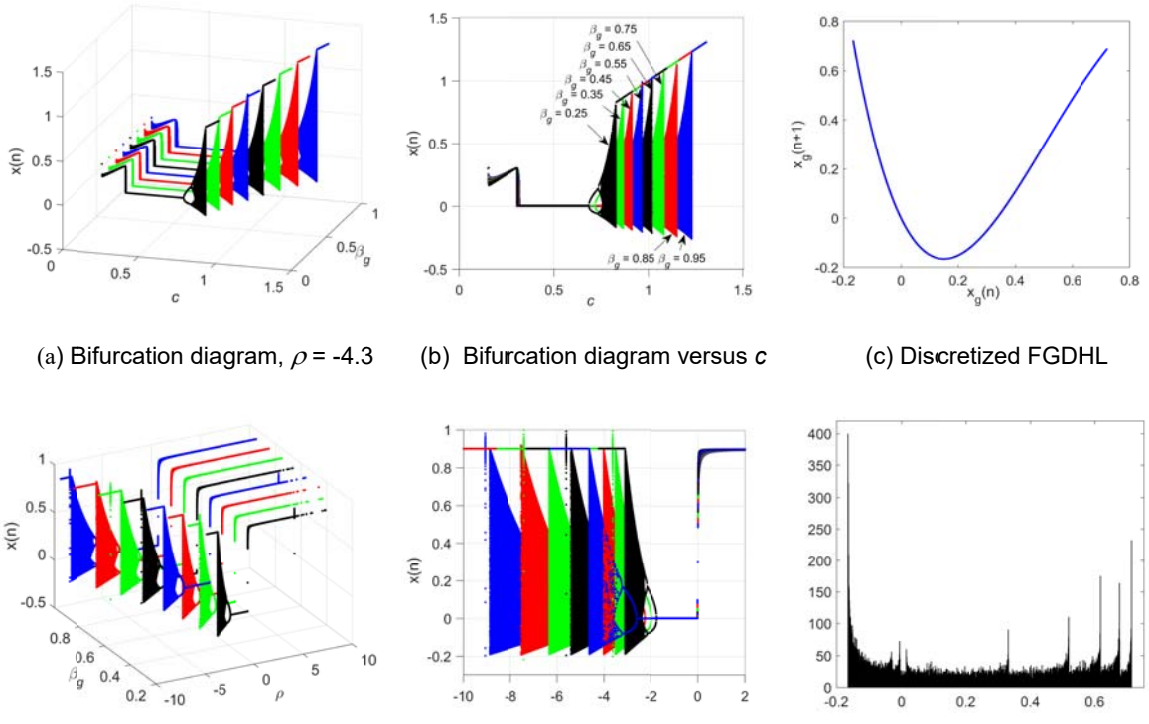
By setting the initial condition $x_g(0)$ to 0.7, the fractional order α_g, control parameter c and ρ as 0.85, 0.85 and -10.3. The phase delay and histogram of 31250 states are obtained and shown in Fig. 3(c) and 3(f), respectively.

5. Proposed fractional pseudo-chaotic random number generator

In this section, the designed fractional pseudo-chaotic random number generator (FPCRNG) is illustrated and discussed. The performance of the proposed generator is also evaluated through statistical tests and NIST test suite.

5.1. Proposed FPCRNG

We give the structure of the proposed FPCRNG in Fig. 4(a). In the figure, Fst[Xst(n-1)] denotes the classical skew-tent map, Fl [Xst(n), Xl(n-1)] and Fc



(a) Bifurcation diagram, ρ = -4.3 (b) Bifurcation diagram versus c (c) Discretized FGDHL

(d) Bifurcation diagram, c = 0.9 (e) Bifrucation diagram versus ρ (f) Histogram of 31250 states

Figure 3. Chaotic behavior of FGDHL system

[Xst(n), Xc(n-1)] represent the fractional Lu's and Chen's system calculated on the non-uniform grid whose grid space is determined by the outputs of the skew-tent map. Fg [Xg(n-1)] stands for the fractional double-humped logistic system. The generator's final output X(n) is obtained by performing XOR operations among the x1 outputs of fractional Chen's, fractional Lu's systems, and the outputs of the FGDHL system.

As shown in the previous sections, the states of the fractional systems discussed in the paper are not uniformly distributed. Therefore, to acquire the final output that satisfies the distribution requirement for the pseudo-random generator (uniformly distributed), we applied some adjustments to the outputs of the fractional systems.

The states of the Chen's and Lu's 3D systems, Xc(n) and Xl(n) with decimal values are injected into the interval of [-10 10] by a folding mechanism as given below,

$$\mathrm{Xc}(n)=\begin{cases}10-\left(\mathrm{Xc}(n)-10\right), & \text{if } \mathrm{Xc}(n)\geq 10\\ -10-\left(\mathrm{Xc}(n)-(-10)\right), & \text{if } \mathrm{Xc}(n)\leq -10,\\ \mathrm{Xc}(n), & \text{else}\end{cases} \quad (24)$$

$$\mathrm{Xl}(n)=\begin{cases}10-\left(\mathrm{Xl}(n)-10\right), & \text{if } \mathrm{Xl}(n)\geq 10\\ -10-\left(\mathrm{Xl}(n)-(-10)\right), & \text{if } \mathrm{Xl}(n)\leq -10,\\ \mathrm{Xl}(n), & \text{else}\end{cases} \quad (25)$$

The states of FGDHL Xg(n) are truncated with a window of [-0.15 0.7] as described in the following formula,

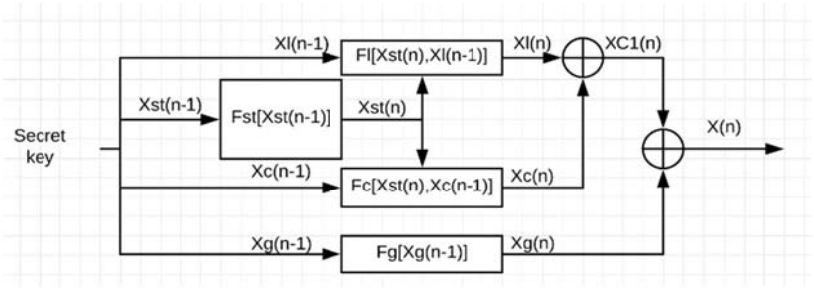
$$\mathrm{Xg}(n)=\begin{cases}\mathrm{Xg}(n), & \text{if } -0.15\leq \mathrm{Xg}(n)\leq 0.7\\ \mathrm{Xg}(n+1), & \text{else}\end{cases}. \quad (26)$$

To evaluate the performance of the proposed generator and to use it in the following stream cipher, each decimal value of the systems states is converted into 32 bits binary values using MATLAB dec2bin function.

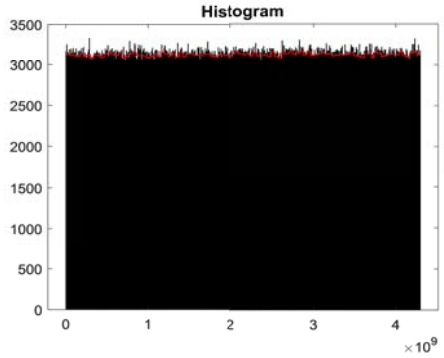
5.2. Performance analysis of the FPCRNG

To do the statistical analysis and NIST test, 100 chaotic sequences with 31250 samples are generated by the proposed FPCRNG using 100 pairs of different secret keys. The parameters and fractional orders of the systems are chosen using the MATLAB random generation function rand. The ranges for fractional orders of the fractional chaotic Chen's and Lu's systems are $\beta_c \in [0.65, 0.9]$ and $\beta_l \in [0.65, 0.9]$, respectively; the order for fractional FGDHL is set to $\beta_g = 0.85$. The parameters for the systems are given as follows: $p = 0.4$, $c = -0.85$, $\rho = -10.3$; $(a_c, b_c, c_c) = (35, 28, 3.2)$, $(a_l, b_l, c_l) = (36, 3, 20)$. The initial conditions are Xst(0) $\in$[0, 1], Xc(0) = (-9, -5, 14), Xl(0) = (0.2, 0.5, 0.3), Xg(0) = 0.7.

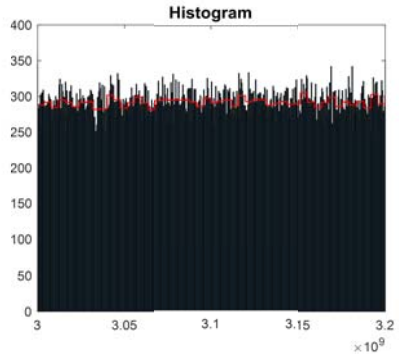
5.2.1. Histogram. The histogram of these 3125000 samples whose values are in the interval of [0, 2^n-1] (n = 32) is given in Fig. 4(b) In total 1000 statistical classes are chosen. The graph shows that the outputs of the proposed FCPRNG are uniformly distributed. To



(a) Structure of the FPCRNG



(b) Histogram of 3125000 samples



(c) Partialhistoogram of the samples

Figure 4. Proposed FPCRNG

better observe the distribution, the histogram for the outputs ranging from [3×10^9, 3.2×10^9] is also given in Fig. 4(c). It can be seen that this zoomed-in partial histogram holds a form that is qualitatively similar to its preceding histogram depicting the distribution of all the samples.

5.2.2. Chi-square test. The Chi-Square test is also applied to further validate the hypotheses of the uniformity of the FPCRNG outputs. We assume that hypothesis H_0 is that the outputs of the generator are uniformly distributed. The experimental value of Chi-Square is calculated by equation (27),

$$V = \sum_{i=0}^{N_c-1} \frac{(O_i - E_i)^2}{E_i} \tag{27}$$

where N_c is the number of classes chosen, O_i is the number of samples in the *i-th* class that are observed and E_i represents the number of samples that are expected for a uniform distribution. Knowing that for a significant level of 0.05, the critical Chi-square value for 1000 classes (degree of freedom = 1000-1 = 999) equals 1073.6427. Then, with an experimental value V equal to 1021.0521, the H_0 is not rejected and the uniformity of the generated sequence is validated.

5.2.3. NIST test. The NIST (National Institute of Standard and Technology) test is a suite of 15 different bitwise tests used to investigate and measure the randomness of a sequence[19]. A P-value greater than 0.01 indicates that the sequence tested is random with a confidence of 0.99(99%). The NIST test result for 10^9 bits (100×31250×32) is shown in TABLE I. It shows that the sequence generated by FPCRNG passes all 15 tests successfully with P-values greater than 0.01.

Table I. Nist Test Results

Test	P-value	Proportion
Frequency test	0.122	99.000
Cumulative-sum test	0.117	99.000
Longest-run test	0.019	99.000
FFT test	0.172	97.000
Overlapping-templates	0.760	99.000
Approximty entropy	0.679	98.000
Random-excursions-variant	0.334	99.171
Serial test	0.403	99.500
Runs test:	0.868	100.000
Rank test	0.419	99.000
Nonperiodic-templates	0.518	99.041
Universal	0.145	100.000
Random-excursions	0.464	99.440
Linear-complexity	0.740	98.000
Block-frequency test	0.679	99.000

6. Security analysis of a stream cipher based on the proposed FPCRNG

A stream cipher based on the proposed FPCRNG is discussed in this section. The stream cipher is achieved by performing XOR operations between the plaintext and the key stream generated by the FPCRNG bit by bit. Several colored and grey images were encrypted by the stream cipher. We analyze in the following the performance of this stream cipher, applying tests that are currently used for quality evaluation of image encryption.

6.3.1. Key space analysis. To be able to resist brute-force attacks, the key space for an encryption scheme must be large enough. A secure cryptosystem should have a key space equal to or greater than 2^{128} as stipulated in [20].

For the stream cipher based on the proposed FPCRNG, the secret key includes the input of the initial conditions for the systems and the fractional orders of the three fractional chaotic systems. Thus, the key space is composed by the parameters (a_c, b_c, c_c, a_l, b_l, c_l, ρ, β_c, β_l, β_g, p), and the initial conditions $Xc_i(0)$, $Xl_i(0)$ (i=1,2,3), Xg(0), Xst(0). With a computation precision of 10^{-14}, the key space is greater than 2^{128}. Hence, the stream cipher based on the proposed FPCRNG can resist the brute-force attack.

6.3.2. Histogram and Chi-square test. For image encryption, the pixel values of the ciphered image should follow a uniform distribution to resist the statistical attack. Thus, to evaluate the performance of the stream cipher in terms of the pixel value distribution after the encryption, the histogram and Chi-square test are employed.

In Fig. 5(a)-(h), the histograms of two different benchmark color images 'Lenna' and 'Goldhill' are given. It can be seen from (d) and (h) that the ciphered images (c) and (g) have a uniform distribution in every color layer. Fig. 5(j)-(p) illustrate the encryption results for the grey images, "boat" and all-white image. The histogram results also confirm the uniform distribution of pixel values after encryption.

By adopting different parameters N_c =256 (pixel value levels), E_i = ImageSize/N_c, the critical Chi-square value is equal to 293.2478 (degree of freedom=256-1=255). The experimental Chi-square values calculated by equation (10) given in Table II confirm that the pixel values of the ciphered images are uniformly distributed.

6.3.3. Entropy test. In information theory, the entropy of a variable represents the average level of uncertainty inherent in the variable's possible outcome. From the aspect of image encryption, entropy can be used to evaluate the randomness of the image pixel value and works as an indicator to estimate whether the cipher algorithm is robust or not. If taking the pixel value as the variable, for the cipher algorithm to be robust, the occurrence probability, hence, the entropy, of different pixel values, should be equal or at least almost the same.

The information entropy of the ciphered image is calculated by the following equation,

$$H(C)=\sum_{i=0}^{Q-1} Pro(c_i)\times log_2\frac{1}{Pro(c_i)} \quad (28)$$

where H(C) stands for the entropy of the cipher image; Q represents the number of levels for pixel value (Q = 256 =2^8); and $Pro(c_i)$ is the occurrences of ci in each level (i=1,2,…,256). In the ideal case, for a well-ciphered image, each pixel value level of the image possesses equal occurrence probability $Pro(c_i)$, which is equal to 1/Q=2^{-8}. Thus, the information entropy is given as follows,

$$H(C)=\sum_{i=0}^{Q-1} 2^{-8}\times log_2 256=8 \quad (29)$$

The entropy test is performed on 7 different images. The entropy of each plain image (H(P)) and its cipher image (H(C)) are obtained by evaluating the average entropy over 50 different secret keys. The results are given in Table II. It can be seen that the average information entropy of the ciphered image for all 7 tested images is close to the ideal value 8.

6.3.4. Key sensitivity test. For a cipher stream to be robust, it must hold high sensitivity to the secret key. This can be evaluated through the calculation of Hamming distance (HD) between two ciphered images which are obtained from one same plain image by changing the secret key of the stream cipher. The Hamming distance between these two ciphered images is calculated as follows,

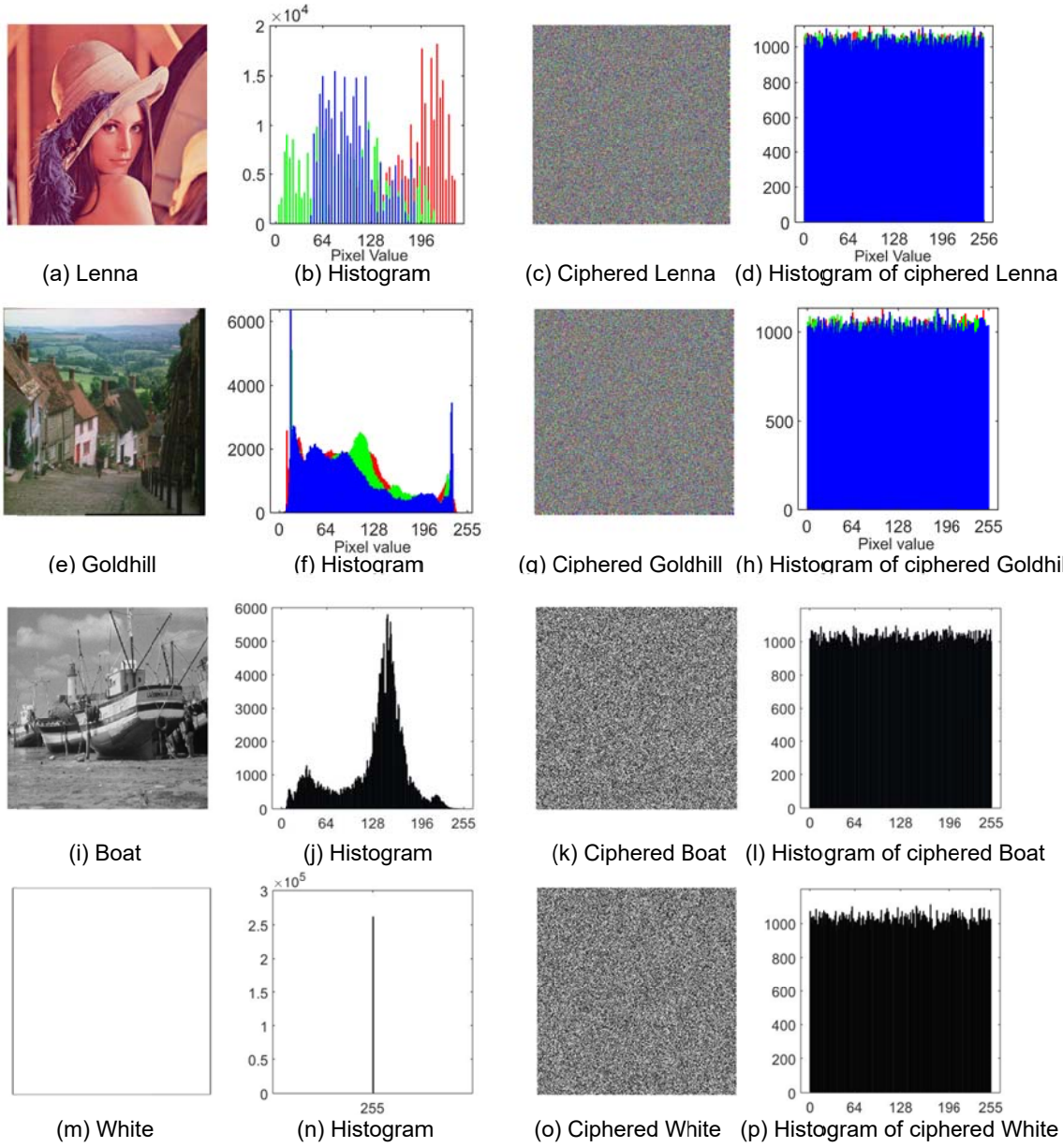


Figure 5. Plain and cipher images and their histograms

Table II. Results of Chi-square and entropy test

Image	Chi-square	Entropy (H(P))	Entropy (H(C))	Mean HD
Lenna Grey	248.5039	7.4116	7.9973	50.0118
Lenna rgb	257.1031	5.6822	7.9998	49.9993
Baboon	254.2773	7.7073	7.9991	49.9861
Black	255.0596	0	7.9993	50.0010
White	262.4511	0	7.9993	50.0014
Goldhill	258.0690	7.6220	7.9998	50.0023
Boat	257.1068	7.1914	7.9993	49.9944

$$HD(C_1,C_2)=\frac{1}{lb}\sum_{k=1}^{lb}C_1[k]\oplus C_2[k] \tag{30}$$

where *lb* is the bit length of the image.

50 different secret keys are used for this experiment, and the average HDs given in Table II show that for each pair of cipher images, the probability of bit changes is close to the optimal value of 50%. This proves that the stream cipher is sensitive to the secret key.

6.3.5. Correlation analysis. The correlation between pixels is another feature tested to evaluate the security of the cryptosystem. A secure cryptosystem should break the high correlation between the pixels of the plain image. For the plain image and its corresponding ciphered image, 8000 different pairs of adjacent pixels are selected in horizontal, vertical, and diagonal directions, respectively to evaluate the correlation properties of the images. The correlation coefficient is calculated by the equation below.

$$\rho_{xy}=\frac{\sum_{i=1}^{N_p}\left[\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)\right]}{\sqrt{\sum_{i=1}^{N_p}\left(x_i-\bar{x}\right)^2}\sqrt{\sum_{i=1}^{N_p}\left(y_i-\bar{y}\right)^2}} \tag{31}$$

For each image, the plain image is encrypted by 50 different secret keys. The correlation property of the ciphered image is obtained by averaging the correlation coefficients over these 50 different ciphered images. Table III shows the correlation coefficients for 5 different images in horizontal, vertical, and diagonal directions. From the table, it can be observed that the correlation coefficients of the cipher images in all directions are around 0. This means that there is almost no correlation between pixels in the cipher images. The correlation results of the benchmark image "Baboon" and the grey image "airfield" given in Fig. 6(a) and (b) also visually confirm that the correlation between pixels in plain images is broken after encryption.

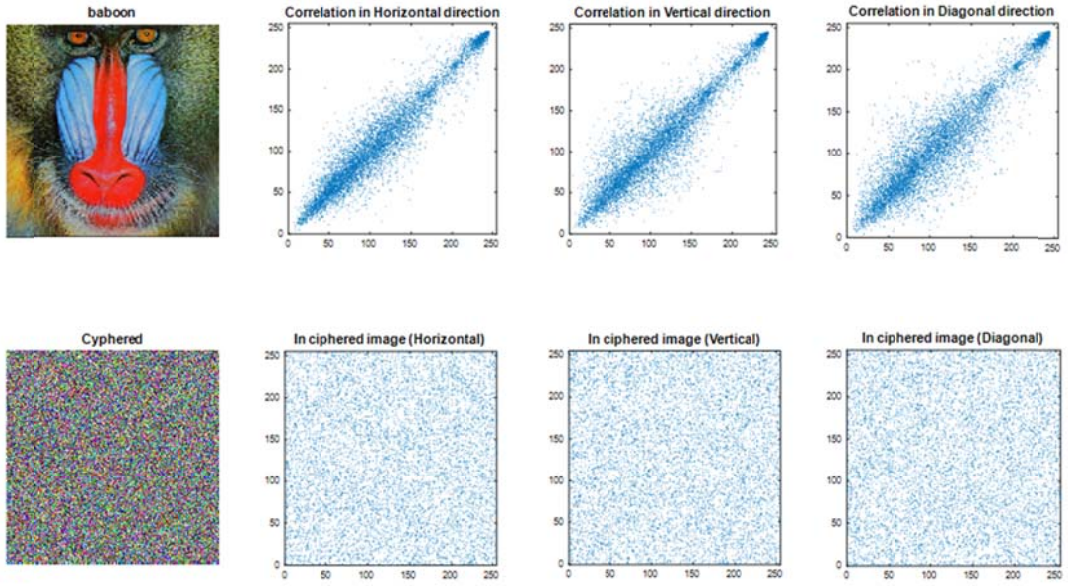
7. Conclusion

In this paper, an innovative fractional pseudo-random number generator is designed by employing three different fractional chaotic systems. To numerically solve the 3D fractional system, a non-uniform grid calculation method based on the fractional Corrector-Predictor Adams-Bashforth-Moulton calculation method is proposed. The method has proved to provide the fractional system with higher chaoticity in terms of Lyapunov exponent which in turn, increases the capriciousness of the systems' outputs. The use of the FGDHL discretized through piecewise constant arguments method further increases the complexity of the structure which enhances the pseudo-chaotic properties of the FPCRNG's final output. The statistical analysis and the NIST test results of the proposed generator show that it possesses excellent characteristics in terms of pseudo-randomness. The experimental results of the stream cipher and the image encryption analysis also confirm that the proposed FPCRNG possesses excellent cryptographic performances.

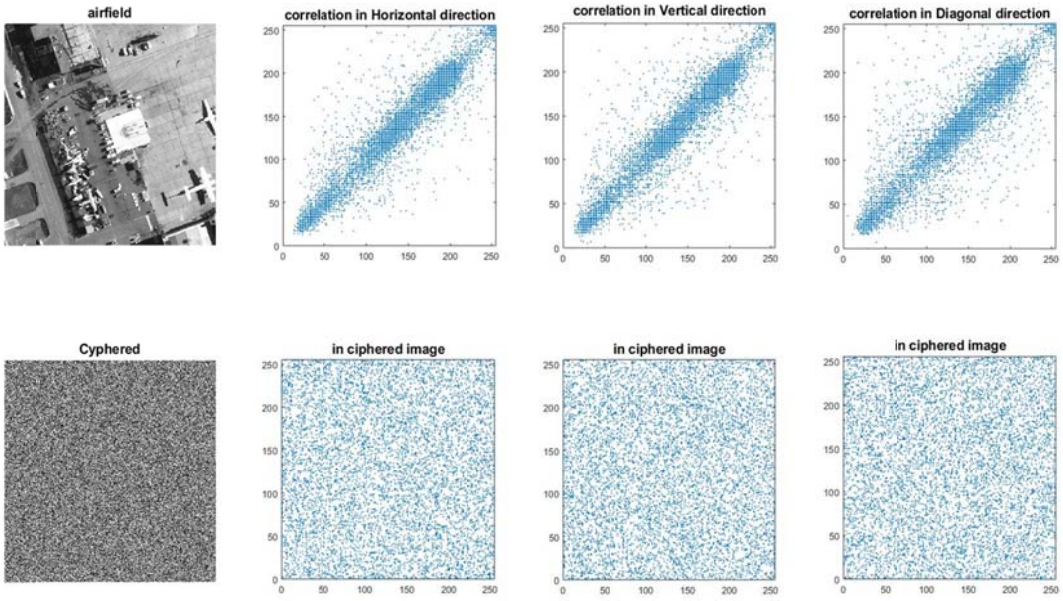
For future work, one possible direction is to investigate the use of the incommensurate fractional chaotic systems in the design of FPCRNG. In the meantime, due to the memory effect of the fractional systems, the computation time is relatively long for the currently proposed generator which leads to a time-consuming encryption algorithm. This makes the proposed scheme more suitable for secure information storage (biomedical data, pictures, confidential files, etc.) So, in the future, how to design a cryptosystem with enhanced computational efficiency is another perspective research direction.

Table III. Correlation results for different images

Image	Plain image			Ciphered image		
	Hor-D	Ver-D	Dia-D	Hor-D	Ver-D	Dia-D
Lenna Grey	0.9458	0.9727	0.9217	-0.0035	-0.0030	-0.0056
Lenna rgb	0.9750	0.9852	0.9652	-0.0011	-0.0012	-0.0029
Baboon	0.9538	0.9384	0.9175	-0.0005	-0.0025	0.0004
Goldhill	0.9775	0.9762	0.9601	0.0014	0.0039	0.0016
Boat	0.9385	0.9718	0.9227	0.0014	-0.00004	0.0001



(a) Correlation in horizontal, vertical, and diagonal direction of plain and ciphered Baboon image



(b) Correlation in horizontal, vertical, and diagonal direction of plain and ciphered airfield image

Figure 6. Correlation results for different directions

7. Reference

[1] S. El Assad, M. Farajallah and C. Vladeanu, "Chaos-based block ciphers: An overview", *10th International Conference on Communications (COMM)*, Bucharest, 2014, pp. 1-4.

[2] Z. Qiao, I. Taralova, S. El Assad, "Efficient Pseudo-chaotic Number Generator for Cryptographic Applications", *International Journal of Intelligent Computing Research*, 2020, vol. 11, pp. 1041-1048.

[3] G. Alvarez, S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", *International Journal of Bifurcation and Chaos*, 2006, vol. 16, no. 8, pp. 2129–2151.

[4] Z. Odiba, N. Corson, C. Bertelle, "Synchronization of chaotic fractional-order systems via linear control", *International Journal of Bifurcation and Chaos*, 2010, vol. 20, no.01, pp.81-97.

[5] F. Mainardi, *Fractional Calculus and Waves Linear Viscoelasticity: An Introduction to Mathematical Models*, Imperial College Press, London, UK, 2010.

[6] V.E. Tarasov, V.V. Tarasova, "Macroeconomic models with long dynamic memory: Fractional calculus approach", *Applied Mathematics and Computation*, 2018, vol. 338, pp. 466-486.

[7] A. Kiani-B, K. Fallahi, N. Pariz, H. Leung, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter",

Communications in Nonlinear Science and Numerical Simulation, 2009, vol. 14, no. 3, pp. 863–879.

[8] T. Li, M. Yang, J. Wu, X. Jing, "A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing", *Complexity*, 2017, vol. 2017, Special issue.

[9] F. Ozkaynak, "A Novel Random Number Generator Based on Fractional Order Chaotic Chua System", *ELEKTRON ELEKTROTECH*, 2020, vol. 26, no. 1, pp. 52-57.

[10] A. Akgul, C. Arslan, B. Aricioglu, "Design of an Interface for Random Number Generators based on Integer and Fractional Order Chaotic Systems", *Chaos Theory and Applications*, 2019, vol.1m Issue.1, pp.1-18.

[11] I. Petráš, *Fractional-Order Nonlinear Systems: Modeling, Analysis and Simulation*, Springer, Berlin, Heidelberg, 2011.

[12] B. J.West, M. Bologna, P. Grigolini, "Physics of fractal operators", Springer, New York, pp. 235-270, 2003.

[13] Diethelm. K, Ford. N. (2002) "A Predictor-Corrector Approach for the Numerical Solution of Fractional Differential Equations", *Nonlinear Dynamics*, July 2002, 29(1):3–22.

[14] M.F Danca, N. Kuznetsov, "Matlab Code for Lyapunov Exponents of Fractional-Order Systems", *International Journal of Bifurcation and Chaos*, 2018, vol. 28, Issue. 5, 1850067.

[15] J. Lu, G. Chen, "A note on the fractional-order Chen system", *Chaos, Solitons & Fractals*, Elsevier, 2006, vol. 27(3), pp. 685-688.

[16] W.H. Deng, C.P. Li, "Chaos synchronization of the fractional Lü system", *Physica A: Statistical Mechanics and its Applications*, 2005, vol. 353, pp. 61-72.

[17] Samar M. Ismail, Lobna A. Said, Ahmed G. Radwan, Ahmed H. Madian, Mohamed F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption", *Journal of Advanced Research*, 2018, vol. 10, pp.85-98.

[18] Z. F. El Raheem, S.M. Salman, "On a discretization process of fractional order logistic differential equation", *Journal of the Egyptian Mathematical Society*, 2014, vol. 22, pp. 407–412.

[19] A. Rukhin, J. Soto, J. Nechvatal, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST Spec. Publi, no. April, 2010, vol. 22, pp1/1—G/1,.

[20] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, 2018, vol. 92, no.2, pp. 305-313.

