A Stream Cipher Based on Fractional Pseudo Chaotic Random Number Generator

Chunxiao Yang, Ina Taralova, Jean-Jacques Loiseau, Safwan El-Assad

A stream cipher based on 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, Université de Nantes/Polytech Nantes
Nantes, France

Abstract—**In this paper, we focus on the design of fractional pseudo- chaotic random number generator (FPCRNG) based on the coupling of fractional chaotic systems. The proposed FPCRNG is composed of 3 fractional chaotic systems, including one fractional generalized double humped logistic system, two 3D fractional systems Chen's system and Lu's system, and one classical skew-tent map. A non-uniform gird calculation method is employed by introducing the skew-tent map into the numerical calculation of the states of the Chen's system and Lu's system to obtain greater chaoticity in terms of Lyaponov exponent. The XOR operations are applied to the fractional systems to obtain the final pseudo-random outputs. The security analysis and statistical experiment of a stream cipher implementing the FPCRNG prove that the proposed structure is effective and can be used into cryptosystem.**

Keywords: fractional chaotic systems; pseudo-chaotic random number generator; non-uniform gird calculation; stream cipher.

I. INTRODUCTION

While we are entering the information era, information security has become a very popular topic, especially for the multimedia data such as images, videos, etc. Both the transformation and the storage of these data containing confidential information are required to be processed securely. Thus, cryptosystems with novel techniques or structures are in greater demand to resist attacks and to ensure the security of the information.

Nonlinear systems with chaotic behavior have been vastly investigated and applied in the design of cryptosystem [1][2]. The pseudo-random generators are designed based on chaotic system due to its numerous merits such as random-like behavior and the sensitivity to the initial conditions and to parameters [3]. And the outputs of the system work as dynamic keys to the cryptosystem for the encryption process.

In the meantime, though long existing in the domain of mathematics, it is not until recent years that fractional calculus and fractional dynamic system have been introduced to the applications in science and engineering. In fact, due to their competence in describing the memory effect and hereditary properties [4], fractional dynamic systems described by fractional differential equations have been discussed and used to define and to model many real-life systems successfully in diverse disciplines like in physics, biology and economic etc [5][6].

In the meantime, the fractional chaotic system also attracts a lot of attentions. Compared to classical chaotic system, the fractional chaotic systems are much more complex and less discussed in the literature. The complexity lies in the fact that there exist different definitions for fractional calculus [7], and the chaotic behavior is dependent on the numerical method chosen to solve the fractional differential equations. However, from the aspect of cryptosystem, this complexity also brings great merits and possibilities. The fractional chaotic system possesses higher nonlinearity and degrees of freedom owning to the intricate geometric interpretation of fractional derivatives [8][9], the latter could be used to enlarge the secret key space and thus increase the complexity of the cryptosystem. The possibility of using fractional chaotic system to design random number generator has also been discussed in [10][11]. But the research remains straightforward and unsophisticated only applying one single fractional system in the generator structure. Further studies need to be done in order to make it 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 coupling several fractional chaotic systems. In addition, a non-uniform grid whose grid spaces are randomly altered by the states of a skew-tent map is employed to obtain the outputs of the fractional chaotic systems. Both the coupling of the systems and the use of non-uniform grid introduce extra chaoticity to the structure, along with the expansion of key space from the aspect of cryptosystem design. The tests results and the security analysis of a stream cipher based on proposed FPCRNG show that the generator passes the random requirements successfully, and it can be applied to encryption algorithm.

The paper is organized as follows: the proposed FPCRNG is described in Section 2. In Section 3, the performance of the FPCRNG is analyzed in terms of statistical analysis. Section 4 presents the cryptanalytic results of a stream cipher based on the proposed FPCRNG. Finally, the conclusion is drawn in Section 5.

II. PROPOSED FPCRNG DESIGN

In this section, the fractional systems used to design the proposed FPCRNG and their numerical calculation methods are discussed. Then the structure of the proposed FPCRNG is given.

A. Fractional systems used for the design of FPCRNG

Fractional systems are dynamic systems which can be modeled by differential equations with non-integer order derivatives[12]. To design the proposed FCPRNG, two 3D fractional systems, Chen's system [13] and Lu's system [14] respectively, and one 1D fractional generalized double humped logistic system (FGDHL) are used. The FGDHL is extended from classical integer order generalized double humped logistic map discussed in [15].The systems equations are given below,

Fractional Chen's system:

$$\begin{cases} D^{\beta_c} x_1(t) = a_c\left(x_2(t) - x_1(t)\right) \\ D^{\beta_c} x_2(t) = \left(c_c - a_c\right) x_1(t) - x_1(t) x_3(t) + c_c x_2(t) \\ D^{\beta_c} x_3(t) = x_1(t) x_2(t) - b_c x_3(t) \end{cases} \tag{1}$$

Fractional Lu's system:

$$\begin{cases} D^{\beta_l} x_1(t) = a_l\left(x_2(t) - x_1(t)\right) \\ D^{\beta_l} x_2(t) = -x_1(t) x_3(t) + c_l x_2(t) \\ D^{\beta_l} x_3(t) = x_1(t) x_2(t) - b_l x_3(t) \end{cases} \tag{2}$$

1D FGDHL system:

$$D^{\beta_g} x(t) = f\left(x(t)\right) = \rho\left(x(t) - c\right)^2 \left(c^2 - \left(x(t) - c\right)^2\right), \quad t > 0. \tag{3}$$

where β_c, β_l are the commensurate fractional derivative orders of Chen's system and Lu's system respectively; (a_c, b_c, c_c) and (a_l, b_l, c_l) denote the system parameters of fractional Chen's and Lu's systems; and β_g is the fractional order of FGDHL with c and ρ its system parameters.

B. Numerical solutions to the fractional Chen's and Lu's systems

To calculate numerically the states values of fractional Chen's and Lu's system, the fractional Corrector-predictor Adams Moulton Bashforth method [16] is applied. Different from the above classical corrector-predictor approach, a novel non-uniform grid is design and employed throughout the calculation for the first time.

Since the numerical solutions of both 3D systems are calculated in the same manner, only the equations for next state values of Chen's system Xc(n) are given below.

$$\begin{aligned} \mathrm{Xc}(n+1) &= \mathrm{Fc}\left[\mathrm{Xc}(n)\right] \\ &= \mathrm{Xc}(0) + \frac{h(n)^{\beta_c}}{\Gamma(\beta_c + 2)} f\left(\mathrm{Xc}^{\mathrm{Pr}}(n+1)\right) \qquad 0 < \beta_c < 1. \\ &\quad + \frac{h(n)^{\beta_c}}{\Gamma(\beta_c + 2)} \sum_{j=0}^{n} a_{j,n+1} f\left(\mathrm{Xc}(j)\right), \end{aligned} \tag{4}$$

$\Gamma(\bullet)$ in the equation represents the gamma function, $\mathrm{Xc}^{\mathrm{Pr}}(n+1)$ denotes the predicted value, defined by the following identity,

$$\mathrm{Xc}^{\mathrm{Pr}}(n+1) = \mathrm{Xc}(0) + \frac{1}{\Gamma(\beta_c)} \sum_{j=0}^{n} b_{j,n+1} f\left(\mathrm{X}(j)\right), \quad 0 < \beta_c < 1. \tag{5}$$

The coefficients $a_{j,i}$ and $b_{j,i}$ are written as,

$$a_{j,n+1} = \begin{cases} n^{\beta_c+1} - (n - \alpha_c)(n+1)^{\beta_c}, & \text{if } j = 0, \\ (n-j+2)^{\beta_c+1} + (n-j)^{\beta_c+1} - 2(n-j+1)^{\beta_c+1}, & \text{if } 1 \le j \le n \\ 1, & \text{if } j = n+1. \end{cases}, \tag{6}$$

$$b_{j,n+1} = \frac{h(n)^{\beta_c}}{\beta_c}\left(\left(n+1-j\right)^{\beta_c} - \left(n-j\right)^{\beta_c}\right).$$

For the classical uniform grid, the calculation space step is set to a fixed value, while *h(n)* in the above equations is an original non-uniform grid space which is obtained by under-sampling based on the chaotic outputs of the skew-tent map Xst(n) by the following method,

$$h(n) = h * (i+1) \quad \text{while } \mathrm{Xst}(n) \in \left[\mathrm{Ub}(i), \mathrm{Lb}(i)\right[, \quad i = 0,1,2,3,4. \tag{7}$$

where

$$\mathrm{Xst}(n) = \mathrm{F}\left[\mathrm{Xst}(n-1)\right] = \begin{cases} \dfrac{\mathrm{Xst}(n-1)}{p}, & 0 < \mathrm{Xst}(n) \le p \\ \dfrac{1 - \mathrm{Xst}(n-1)}{1-p}, & \mathrm{Xst}(n) > p \end{cases} \tag{8}$$

In the above equations, p is the parameter for the skew tent map; h is the computation step size close to 0.001, and Ub(i) and Lb(i) are the *ith* upper and lower bounds of Xst(n) value which work as a threshold to get the grid space *h(n)*. Therefore, *h(n)* values from 0.001 to 0.005 according to the interval Xst(n) is in. To be noticed that, Ub(i) and Lb(i) can be arranged randomly in the interval of [0 1] (the range of Xst(n)). And the choices of these bounds' values spread evenly over 0.001 to 0.005 with a gap of h according to the uniform distribution of skew tent map properties suggested in [17]. The bounds, together with computation step size h, can also be considered as secret keys which make the cryptosystem even more complex and difficult to predict.

The calculation results show that only the outputs of x_1 of the two 3D Chen's and Lu's systems exhibit chaotic behavior, so in the proposed FPCRNG, the x_1 of the 3D fractional chaotic systems are used. What's more, the LEs for the systems calculated as in [18] show that the non-uniform grid systems possess greater chaoticity compared to systems calculated on uniform grid. The LEs of x_1 for both uniform and non-uniform Chen's systems are shown in Fig.1 with their parameters (a_c, b_c, c_c) and initial value (x_1, x_2, x_3) set to [35 28 3.2] and [-9 -5 14], respectively.

C. Numerical solutions to the Fractional Generalized Double Humped Logistic system

The 1D FGDHL system used for the FPCRNG design is calculated by adapting the piecewise constant arguments method [19]. The calculation of next state value is given by the following equation, where r is the discretization step size. In the following work, r is set to 0.2.

$$\begin{aligned} \mathrm{Xg}(n+1) &= \mathrm{Fg}(n+1) \\ &= \mathrm{Xg}(n) + \frac{r^{\beta_g}}{\Gamma(1+\alpha)} \rho\left(\mathrm{Xg}(n) - c\right)^2 \left(c^2 - \left(\mathrm{Xg}(n) - c\right)^2\right) \end{aligned} \tag{9}$$

D. FPCRNG structure

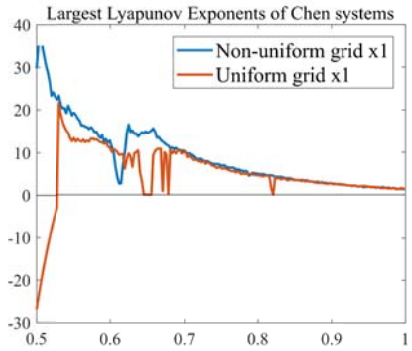


Figure. 1 LE results for Chen system with calculated with different grid choice

With all the systems states calculated, the FPCRNG output X(n) is obtained by the scheme in Fig. 2. The output of one integer order skew tent map Fst is first used to generate the non-uniform grid (as given in equation (7)-(8)) to calculate the outputs of fractional Chen's and Lu's systems (equation(4)-(6)); then, the XOR operations are performed to the x_1 output of fractional Chen's, fractional Lu's systems and the output of FGDHL map. To be mentioned that, in order to get greater uniformity for the output sequence distribution, the states of the two fractional 3D systems with decimal values are injected into the interval of [-10 10] by a folding mechanism similar to that introduced in [20], and the states of FGDHL is truncated with a window of [-0.15 0.7]. The FPCRNG output is obtained by performing XOR operations to the three fractional systems after converting the decimal values of the systems to 32 bits binary values using MATLAB dec2bin function.

III. PERFORMANCE ANALYSIS OF THE FPCRNG

In this section, the performances of the proposed FPCRNG are discussed. The statistical properties of the FPCRNG are analyzed by the histogram, Chi-analysis of the outputs. The NIST test is also performed to justify the randomness of the proposed FPCRNG.

A. Histogram and Chi-square test

To do the statistical analysis, 100 chaotic sequences with 31250 samples are generated by the proposed FPCRNG using 100 pairs of different secret keys. The histogram of these 3125000 samples whose values are in the interval of [0, 2^n-1] (n=32) is given in Fig.3 which shows that the outputs of the proposed FCPRNG are uniformly distributed in 1000 statistical classes. The parameters are set as following, $\beta_c \in [0.65, 0.9]$, $\beta_l \in [0.65, 0.9]$, $\beta_g = 0.85$; $p = 0.4$, $(a_c, b_c, c_c) = [35\ 28\ 3.2]$, $c = -0.85$, $\rho = -10.3$; $(a_l, b_l, c_l) = [36\ 3\ 20]$; Xst $\in$ [0, 1], Xc(0) = [-9 -5 14], Xl(0) = [0.2 0.5 0.3], Xg(0) = 0.7.

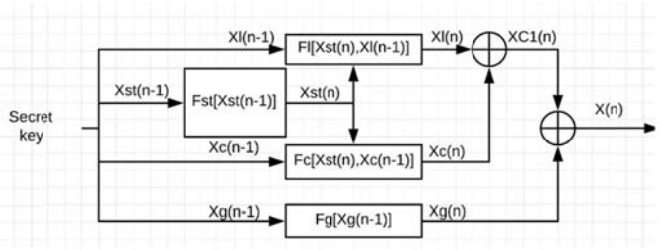


Figure. 2 FPCRNG structure

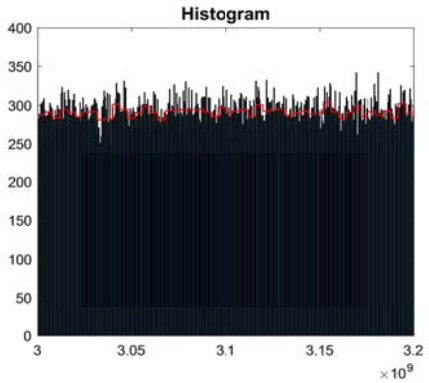


Figure. 4 Histogram of the partial FPCRNG and average value per interval (in red)

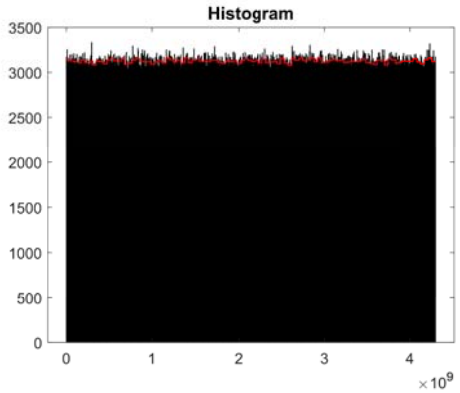


Figure. 3 Histogram of the FPCRNG sequence and average value per interval (in red)

To better observe the distribution, the histogram for the outputs ranging from [3×10^9, 3.2×10^9] is also given in Fig.4. 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.

Apart from the histogram result, the Chi-Square test [21] is also applied to further validate the hypotheses of the uniformity of the FPCRNG outputs. The experimental value of Chi-Square is calculated by the equation below,

$$\chi^2_{exp} = \sum_{i=0}^{N_c-1} \frac{(O_i - E_i)^2}{E_i} \tag{10}$$

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 which is expected for a uniform distribution. Knowing that the critical Chi-square value for 1000 classes (degree of freedom = 1000-1 = 999) equals to 1073.6427 when having a significant level of 0.05, with an experimental value χ^2_{exp} calculated equal to 1021.0521, the hypothesis is not rejected and the uniformity of the generated sequence is justified.

B. NIST test

The NIST (National Institute of Standard and Technology) test is a suite of test consisting of 15 different bitwise tests used to investigate and measure the randomness of a sequence [22]. A P-value greater than 0.01 indicates that the sequence tested is random with a confidence of 0.99(99%) [23]. The NIST test

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

result for 10^9 bits (100×31250×32) are shown in the TABLE I. It shows that the sequence generated by FPCRNG passes all the 15 tests successfully with P-values greater than 0.01.

IV. SECURITY ANALYSIS OF A STREAM CIPHER BASED ON PROPOSED FPCRNG

One 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. To analyze its security performance, the stream cipher is used to encrypt several colored and grey images.

A. Key space anaylsis

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 or greater than 2^{128} as stipulated in [24].

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 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 10^{266}, which is greater than 2^{128}. Hence, the stream cipher based on the proposed FPCRNG can resist the brute-force attack.

B. Histogram and Chi-square test

For the 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 and 6 the histograms of two different benchmark images 'Lenna' and 'Goldhill' are given. It can be seen from d) and h) that the ciphered image c) and g) have uniform distribution.

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). And the experimental Chi-square values calculated by equation (10) given in TABLE II confirm that the pixel values of ciphered images are uniformly distributed.

C. 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, the 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 value, should be equal or at least almost the same.

The information entropy of ciphered image is calculated as follows,

$$H(C)=\sum_{i=0}^{Q-1} Pro(c_i)\times log_2 \frac{1}{Pro(c_i)} \tag{11}$$

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 c_i 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 calculated as,

$$H(C)=\sum_{i=0}^{Q-1} 2^{-8}\times log_2 256 = 8 \tag{12}$$

The entropy test is performed to 7 different images. The entropy of each pain 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.

D. 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. And the Hamming distance between these two ciphered images is calculated as following,

$$HD(C_1,C_2)=\frac{1}{|lb|}\sum_{k=1}^{lb} C_1[k]\oplus C_2[k] \tag{13}$$

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 pairs of ciphered images, the probability of bit changes is close to the optimal value of 50%. This proves that the stream cypher is

TABLE II. RESULTS OF CHI-SQUARE, ENTROPY TEST AND MEAN HD

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

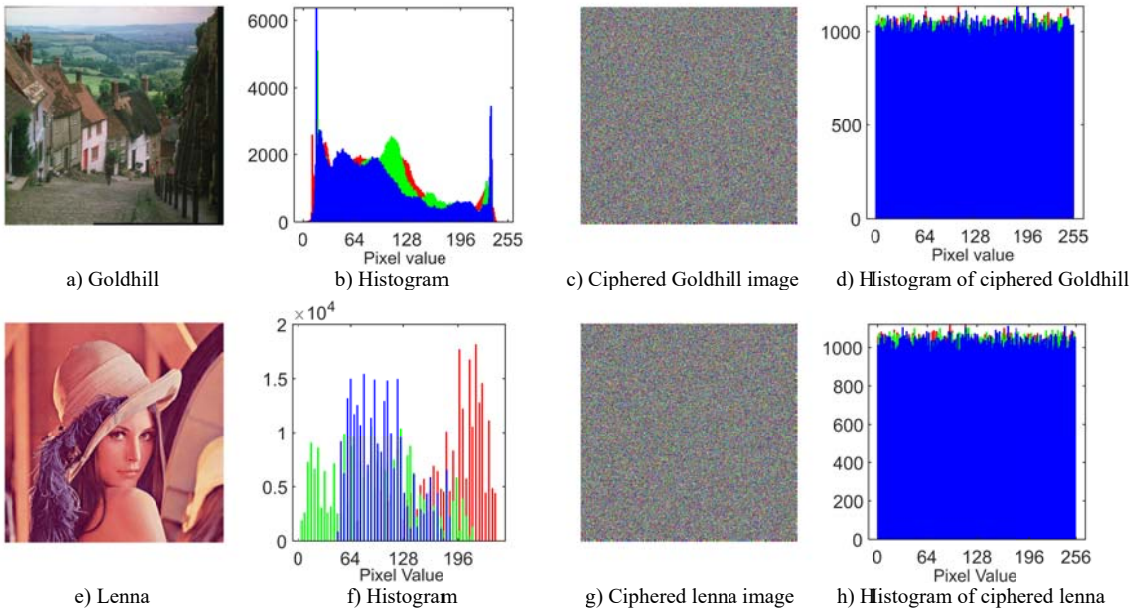
sensitive to the secret key.

E. Correlation analysis

The correlation between pixels is another feature tested to evaluate 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 the directions of horizontal, vertical and diagonal respectively to evaluate the correlation properties of the images. The correlation coefficient is calculated by the equation below.

$$\rho_{xy} = \frac{\sum_{i=1}^{N_p}\left[\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)\right]}{\sqrt{\sum_{i=1}^{N_p}\left(x_i-\bar{x}\right)^2}\sqrt{\sum_{i=1}^{N_p}\left(y_i-\bar{y}\right)^2}} \tag{16}$$

For each image, the plain image is encrypted by 50 different secret keys. And the correlation property of the ciphered image is obtained by averaging the correlation coefficients over these 50 different ciphered images. The correlation coefficients in horizontal, vertical and diagonal direction are given in TABLE IV. And the correlations of both plain and ciphered image "Baboon" are given in Fig. 6. Both the table and the figure reveal that after encryption, the high correlation in the plain image is broken.



a) Goldhill b) Histogram c) Ciphered Goldhill image d) Histogram of ciphered Goldhill

e) Lenna f) Histogram g) Ciphered lenna image h) Histogram of ciphered lenna

Figure. 5 Plain and Ciphered Image of two color images and their histograms

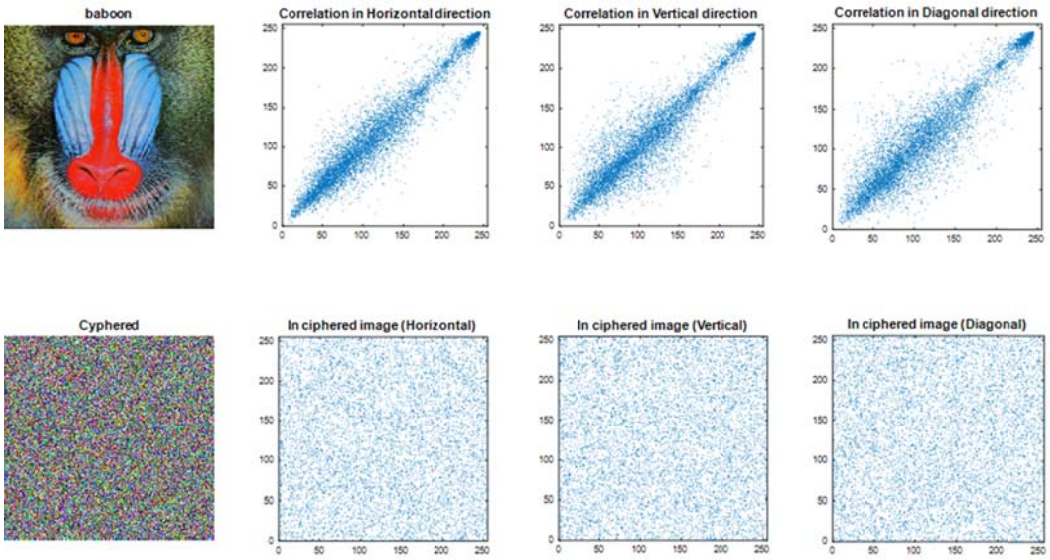


Figure. 6 Correlation in three directions of image "Baboon" and its Ciphered image

TABLE IV. CORRELATION RESULTS

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

V. CONCLUSION

In this paper, a FPCRNG consisting of 3 different fractional chaotic systems is discussed for the first time. The XOR operations are performed between the outputs of two 3D fractional systems extended from classical chaotic Chen's system and Lu's system, and a 1D FGDHL system. By numerically calculating the states of the 3D fractional systems on a non-uniform grid, the systems gained higher chaoticity which increases the unpredictability of the systems' outputs. And the use of FGDHL further increases the complexity of the structure which again enhances the pseudo-chaotic properties of the FPCRNG's final output, and therefore, the security of the encryption scheme. The experimental results show that the numbers generated from the proposed FPCRNG possess excellent characteristic in terms of randomness. And the image encryption application discussed demonstrates that the stream cipher applying the proposed FPCRNG possesses great cryptographic performance and properties.

REFERENCE

[1] S. El Assad, M. Farajallah and C. Vladeanu, "Chaos-based block ciphers: An overview", 2014 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,Vol. 11, pp. 1041-1048, 2020.

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

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

[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, vol. 338, pp. 466-486, 2018.

[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, vol. 14, no. 3, pp. 863–879, 2009.

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

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

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

[11] 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, Vol.1m Issue.1, pp.1-18, 2019.

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

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

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

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

[16] K. Diethelm, N. J. Ford, A. D. Freed, "A predictor-corrector approach for the numerical solution of fractional differential equations", Nonlinear Dynamics, vol. 29, issue. 8, pp. 3–22, 2002.

[17] M. Hasler and Y. L. Maistrenko, "An introduction to the synchronization of chaotic systems: coupled skew tent maps", in IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, no. 10, pp. 856-866, Oct. 1997.

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

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

[20] O. Garasym, R. Lozi, I. Taralova, "Exploring some topologies of coupled chaotic networks", NOMA'15, International Workshop on Nonlinear Maps and their Applications, Dublin, Ireland, pp.34-39, 2015.

[21] B. Nolan, Data analysis: an introduction, Polity Press ,UK, 1994.

[22] M. Hemattil, A. Ahmadi, S. V. Makkil, M. Ahmadi, "Hardware Design of Chaotic Pseudo-Random Number Generator Based on Nonlinear Feedback Shift Register", IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), Windsor, ON, Canada, pp. 980-983, 2018.

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

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