2024 3rd International Conference for Innovation in Technology (INOCON)
Karnataka, India. Mar 1-3, 2024

Image Encryption Using Novel Chaotic System

Kriti Suneja, Bhushan Kumar, Kshitiz Jha, Lakshya Singh Chuphal
Department of Electronics and Communication
Delhi Technological University
New Delhi, Delhi
kritisuneja@dtu.ac.in, bhushankumar98178@gmail.com, jhak2001@gmail.com, lxyachuphal02@gmail.com

Abstract **– In the modern digital world, data security has become a major concern. All kinds of data are transmitted through various channels in different forms. For safeguarding this information and maintaining privacy, encryption techniques have proved very useful. In this paper, we have designed a new 3D chaotic system to be used in image encryption algorithms. The chaotic system's random and unpredictable nature make them highly suitable for encryption techniques. We have put forward a new 3D chaotic system, calculating its Lyapunov exponents, fractal dimension and performed its bifurcation analysis for successful analysis of the proposed system. A pixel-value diffusion-based encryption algorithm, using the novel chaotic system, has been performed.**

Keywords – Chaotic system, Lyapunov exponents, Image encryption, Pseudo Random Number Generator (PRNG), Pixel diffusion.

I. INTRODUCTION

Chaotic systems are a class of dynamic system which exhibit high sensitivity to initial conditions. Even a small change in the starting conditions can cause the system to diverge drastically, resulting in totally different outcomes. Chaotic systems are deterministic and can be modelled using a set of differential equations. However, they exhibit random nature because they get highly affected by small changes in input conditions. Chaos theory is a field in mathematics that showcases the pattern of nonlinear dynamic systems, showing their highly susceptible dependence on initial conditions. Some of the applications of chaos theory are random number generator [1], unmanned aerial systems [2], DC motor [3], cryptography [4], magnetic levitation oscillation [5], memristive devices [6] and many more.

To protect data from unauthorized access, the complex and unpredictable nature of the chaotic systems is used to perform encryption. In case of digital images, the pixel value or position are altered using the chaotic system due to which it appears random. Decryption of such image without the knowledge of exact chaotic parameters becomes difficult. The sensitive dependence of chaotic system makes sure that even a minute variation in chaotic parameters result in totally different decrypted image.

We have generated a new image encryption algorithm based on pixel value diffusion using the proposed new chaotic system. Pseudo random numbers are generated using the chaotic system.

There have been numerous works on using chaotic systems for image encryption. Xing-Yuan Wang et al. [7] proposed a new image encryption algorithm based on cycle shift and chaotic system. In this technique, we generate some integers which are of the same size as is the image and use these integers to scramble the plain-text image. Xiuli Chai et al. [8] proposed a chaos-based image encryption algorithm using DNA sequence operation. In this technique, a DNA matrix is used to encode the plain image. In the second step, a wave-based permutation scheme is performed on it. Hossein Movafegh Ghadirli et al. [9] discussed various encryption algorithms for color images. Li et al. [10] proposed a new algorithm for grayscale images which utilized the concepts of bit-level scrambling and multiplication diffusion for removing the correlation between pixels.

This paper is divided into five sections. The mathematical model of the new chaotic system and its dynamic properties are described in Section 2. Section 3 presents the results of simulation of chaotic system and its bifurcation analysis. Section 4 describes the applications of image encryption process using the new chaotic system. Section 5 provides the conclusion.

II. MATHEMATICAL MODEL OF THE NEW CHAOTIC SYSTEM

The newly designed 3D chaotic system is given by the following equations:

$$\dot{x} = z + a \tag{1}$$

$$\dot{y} = -x^2 - bz \tag{2}$$

$$\dot{z} = |y| + cxy \tag{3}$$

where x, y and z are the states and a, b and c are the chaotic parameters. As can be seen from the equation (1), (2) and (3), the proposed chaotic system consists of two quadratic nonlinearities and one modulus function nonlinear term.

For the system to exhibit chaotic nature, we have taken the value of chaotic parameters as:

$$(a, b, c) = (5, 2.9, 2.6) \tag{4}$$

and initial conditions as:

$$X(0) = (x(0), y(0), z(0)) = (0.2, 0.2, 0.2) \tag{5}$$

We calculated the Lyapunov exponents using the Wolf algorithm [11]. We used the conditions mentioned in (4) and (5) and run the simulation for T = seconds. The obtained Lyapunov exponents are:

$$(L1, L2, L3) = (0.0067, 0.0009, -0.0223) \tag{6}$$

From (6), we observe that of the three Lyapunov exponents two are positive which proves that the system is indeed chaotic.

979-8-3503-8193-1/24/$31.00 ©2024 IEEE

The sum of the Lyapunov exponents is

$$L1 + L2 + L3 = -0.0147 \ < 0 \qquad (7)$$

The sum is less than zero indicating that the system is dissipative in nature, which again, represents its unpredictable nature.

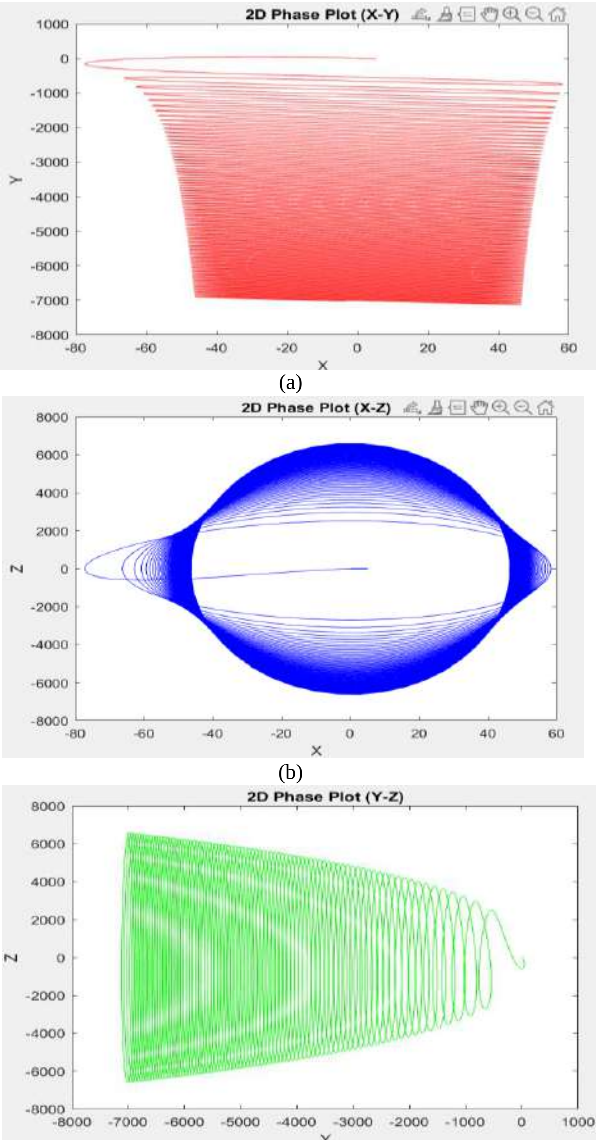
Chaotic systems exhibit fractal dimensions. The Kaplan – Yorke Fractal dimension [12] for a chaotic system is calculated as

$$D\text{xy} = 2 + \frac{L1+L2}{|L3|} \qquad (8)$$

The fractal dimension of the new chaotic system comes out to be 2.3408 indicating highly chaotic nature of the system.

III. SIMULATION

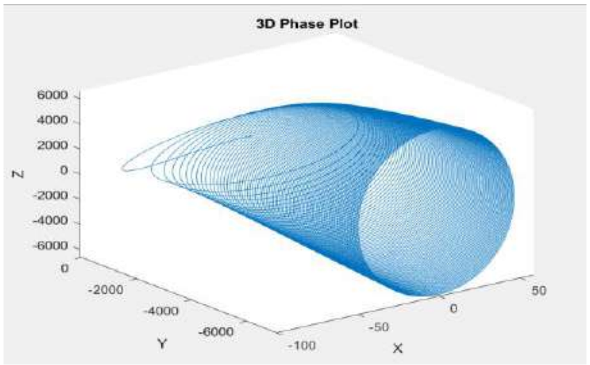
The plots obtained from the proposed chaotic system are as follows,



(a)

(b)

(c)



(d)

Fig. 1. (a) Phase Plot (X vs Y), (b) Phase Plot (X vs Z), (c) Phase Plot (Y vs Z), (d) Complete 3-D Phase Plot

The variation of Lyapunov exponents, can be seen in the following plot. After some initial fluctuations which was to be expected but eventually it settles down to the values mentioned previously.

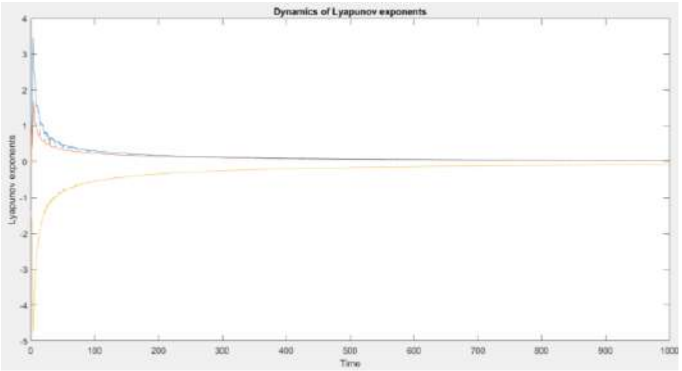
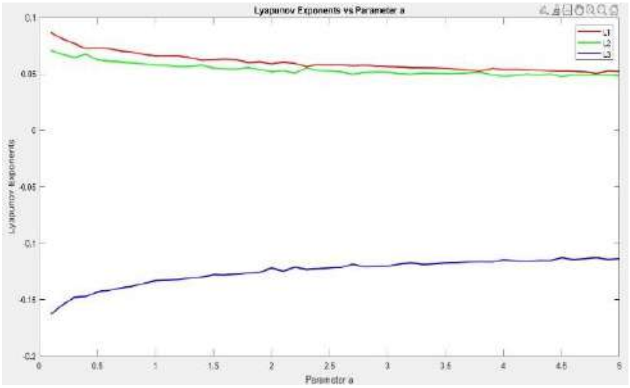
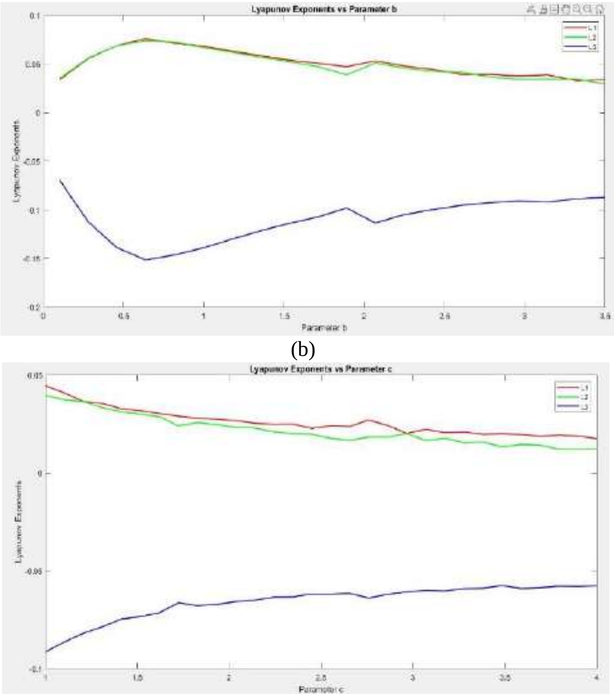


Fig. 2 Variation of Lyapunov Exponents L1, L2, L3 with time

Usually, rigid chaotic systems are not preferred. Therefore, we have used 'Bifurcation Analysis' on all the three parameters to determine the ranges in which the chaotic system preserves its chaotic and unpredictable nature.



(a)



(b)

(c)

Fig. 2. Bifurcation Analysis vs (a) Parameter ‘a’, (b) Parameter ‘b’, (c) Parameter ‘c’

Following this, is the image encryption done using the proposed novel chaotic system and its respective decryption.

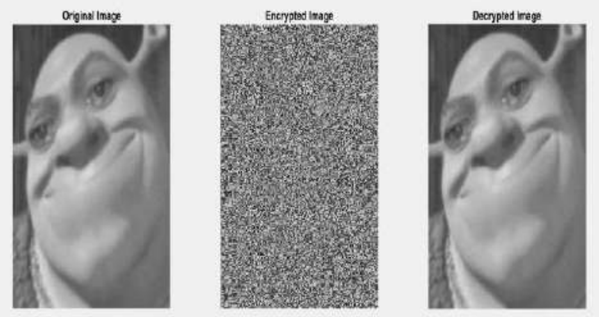


Fig. 3. Encrypted and Decrypted Image using proposed Novel Chaotic System

IV. APPLICATION

Encryption Process has been done using the Symmetric Key Block Ciphering Technique. Chaotic system’s independent variable is used to make the Key for encryption. The first step includes interpretation of the image to be transmitted in the form of pixels. Following which, the data is converted into a matrix of rows and columns. In a similar manner, the Encryption Key is also reshaped to be of a matrix with same number of rows and columns as the original image matrix, so that, smooth operation of EXOR can be executed. It is to be kept in mind that this Key matrix is generated with the use of the proposed chaotic system.

EXOR operation is performed between the first column of the original image matrix taken as blocks of data and the Key matrix to get the first column of the encrypted image matrix, which in succession is then XORed with the column obtained from the EXOR operation performed between the second column of original image matrix and the second column of the Key matrix. And so on and so forth until all the columns of the encrypted matrix has been obtained according to the following equations,

$$E_1 = P_1 \oplus K_1 \tag{9}$$

$$E_2 = (P_2 \oplus K_2) \oplus R_1 \tag{10}$$

$$E_n = (P_n \oplus K_n) \oplus R_{n-1} \tag{11}$$

Decryption process can also be performed in a similar fashion with a little tuning in the equations. The same Key matrix is required to successfully decrypt the image. To get the first column of the decrypted image data, first column of the encrypted image matrix is XORed with first column of the Key matrix. Subsequently, to get the second column of the decrypted image matrix, the second column of the encrypted image matrix is XORed with its previous column and then, with the corresponding column from the key matrix. Thus, after complete decryption the original image is successfully retrieved according to the following equations,

$$D_n = E_n \oplus K_n \oplus E_{n-1} \tag{12}$$

V. CONCLUSION

Encryption performed through the proposed chaotic system showed better efficiency against unauthorized external attacks. The Lyapunov exponents L1, L2 and L3 were plotted and obtained to be 0.0067, 0.0009 and -0.0223, respectively. Also, the Fractal Dimension was evaluated to be equal to 2.3408, which was found out to be more than those of some of the more popular chaotic systems like Lorentz and Rössler Chaotic Systems. Thus, providing further unpredictability and hence, better suited for encryption techniques as a PRNG (Key Matrix).

REFERENCES

[1] F. Pareschi, G. Setti, and R. Rovatti, “Implementation and testing of highspeed CMOS true random number generators based on chaotic systems,” *IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 12, pp. 3124_3137, Dec. 2010.*

[2] H. Bi, G. Qi, J. Hu, P. Faradja, and G. Chen, “Hidden and transient chaotic attractors in the attitude system of quadrotor unmanned aerial vehicle,” *Chaos, Solitons Fractals*, vol. 138, Sep. 2020, *Art. no. 109815.*

[3] Q. Wang, E. Dong, S. Du, J. Tong, H. Yu and F. Duan, "Mega-Stability and Transient Chaos Analysis of Brushless DC Motor with Winding Heat Loss," 2022 IEEE International Conference on Mechatronics and Automation (ICMA), Guilin, Guangxi, China, 2022, pp. 1801-1806, doi: 10.1109/ICMA54519.2022.9856249.

[4] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. A. El-Latif, O. Guille-Fernandez, Y. Hidayat, and G. Gundara, “A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption,” *IEEE Access, vol. 8, pp. 137116137132, 2020.*

[5] M. Gao, Y. Wang, Y. Wang, and P. Wang, “Experimental investigation of non-linear multi-stable electromagnetic-induction energy harvesting mechanism by magnetic levitation oscillation,” *Appl. Energy, vol. 220, pp. 856875, Jun. 2018.*

[6] C. Li, J. C. T. Wesley, H. C. I. Herbert, and T. Lu, “A memristive chaotic oscillator with increasing amplitude and frequency,” *IEEE Access, vol. 6, pp. 1294512950, 2018.*

[7] Xingyuan Wang, & Gu, Sheng-Xian. (2015), “Novel image encryption algorithm based on cycle shift and chaotic system,” *Optics and Lasers in Engineering. 68. 10.1016/j.optlaseng.2014.12.025.*

[8] X. Chai, Z. Gan, K. Yuan et al, “A novel image encryption scheme based on DNA sequence operations and chaotic systems,” *Neural Comput & Applic 31, 219–237 (2019).*

[9] Hossein Movafegh Ghadirli, Ali Nodehi, & Rasul Enayatifar, (2019), “An overview of encryption algorithms in color images,” *Signal Processing. 164. 163-185. 10.1016/j.sigpro.2019.06.010.*

[10] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, ``Image encryption scheme with bit-level scrambling and multiplication diffusion," Multime- dia Tools Appl., vol. 80, no. 12, pp. 1847918501, May 2021.

[11] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, “Determining Lyapunov exponents from a time series,” *Phys. D, Nonlinear Phenomena, vol. 16, no. 3, pp. 285317, 1985.*

[12] Z.-M. Chen, “A note on Kaplan-Yorke-type estimates on the fractal dimension of chaotic attractors”, *Chaos Solitons and Fractals, vol. 3, no. 5, pp. 575–582, 1993. doi:10.1016/0960-0779(93)90007-N.*