# Image Encryption Algorithm Using Natural Interval Extensions

Lucas Giovani Nardo
*Control and Modelling Group (GCOM)*
*Department of Electrical Engineering*
*Federal University of São João del-Rei*
São João del-Rei, Brazil
gnlucas@gmail.com

Arthur Mendes Lima
*Department of Electrical Engineering*
*University of Brasília*
Brasília, Brazil
arthurlima67@yahoo.com.br

Erivelton Geraldo Nepomuceno
*Control and Modelling Group (GCOM)*
*Department of Electrical Engineering*
*Federal University of São João del-Rei*
São João del-Rei, Brazil
nepomuceno@ufsj.edu.br

Janier Arias-Garcia
*Mechatronics, Control and Robotics (MACRO)*
*Department of Electronic Engineering*
*Federal University of Minas Gerais*
Belo Horizonte, Brazil
janier.arias@gmail.com

***Abstract*—It is known that chaotic systems have widely been used in cryptography. Generally, floating point simulations are used to generate pseudo-random sequence of numbers. Although, it is possible to find some works on the degradation of chaotic systems due to finite precision of digital computers, little attention has been paid to exploit this limitation to formulate efficient process for image encode. This article proposes a novel image encryption method using natural interval extensions. The sequence of arithmetic operations is different in each natural interval extension. This is what we need to produce two different sequences; the difference between these sequences is used to generate the lower bound error, which has been shown to present satisfactory pseudo-random properties. The approach has been successfully tested using the Chua's circuit as the chaotic system. The secret key has presented good properties for encrypting the Lena image.**

***Index Terms*—Image encryption, Natural interval extensions, Lower bound error, Chua's circuit.**

## I. Introduction

It has been an integral part of human nature to maintain control of the access to information. For this reason, encryption has received such attention over the past few years. For example, encryption takes place in bank and cryptocoins transactions [1]. Additionally, this area has such importance in image encryption [2]. In Computer Science and Electrical Engineering fields, more robust and effective encryption methods have emerged as demonstrated by the linear congruential method [3], by the use of irrational numbers [4] and also for chaotic systems [5].

Chaotic dynamical systems present interesting properties as its transitivity, the high density of the periodic points of the function $f$ in metric space and its sensitive to initial conditions [6], [7]. Therefore, these systems can generate pseudo-randomness sequences, which can be used in cryptography. In fact, Herring e Palmore [8] have already told that pseudo-random number generators are examples of deterministic chaotic dynamical systems.

This work was supported by the funding groups CNPq/INERGE, Fapemig and Capes.

In the information security area, chaotic systems have been vastly studied and several methods have been emerged. Fridrich [9] used only the chaotic properties of the baker map; Ismail et al. [10] added two parameters to the classical fractional logistic equation to improve its flexibility and control; and Zhang [11] used the hyper-chaotic Chen's system, diffusion and shuffling operations to encrypt images. One of the key problems faced by researchers in this area is the degradation of chaotic systems due to finite precision of digital computers, as reported by Li et al. [12]. The last few years many attempts have been investigated to overcome this problem, such as the use of high finite precision, cascading multiple chaos systems, switching multiple chaos systems, coupling different chaotic systems or pseudo randomly perturbing the chaotic system. The reader is invited to read the work by Cao et al. [5] for more information on these methods.

Although, many researchers have succeed to reduce the degradation of the chaotic properties of digital systems, little attention has been paid to exploit this limitation to formulate encryption algorithms. Instead of seeing the finite digital precision as a problem, this paper proposes a novel image encryption method using natural interval extensions. When solving a chaotic system by means of numerical computation, it is verified that, based on two natural interval extensions (for more details, see section II-C), starting from the same set of parameters and initial conditions, after a certain number of iterations, the results of each simulation of the system diverge. Such an event could not occur due to the exactly equal initial sets of parameters and conditions for each simulation. This happens because of the constructive limitations of computers and the IEEE 754-2008 floating point standard [13]. As observed in [14], [15], the sequence of arithmetic operations is different in each natural interval extension. This is what we need to produced two different sequences to generate the lower bound error, which has been shown to present satisfactory pseudo-random properties.

This paper is developed as follows: a brief introduction, followed by a bibliographic review was presented in this

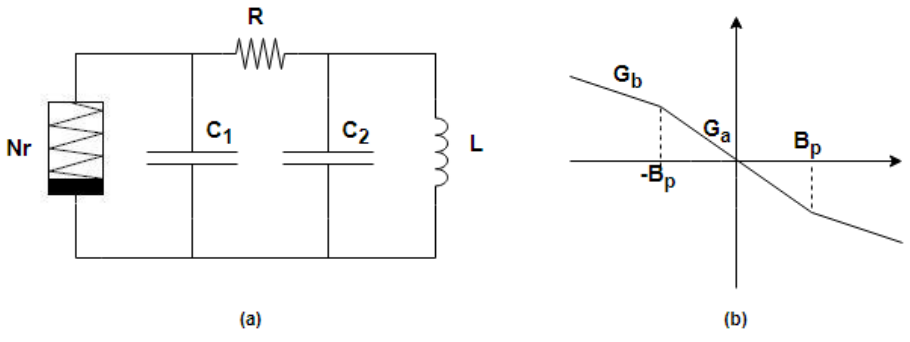


Fig. 1. (a) Chua's circuit. (b) Chua's diode curve. $G_a$, $G_b$ and $B_p$ are the slopes and the breaking points of the nonlinear element, respectively.

$$\begin{cases} C_1 \dfrac{dv_{c_1}}{dt} &= \dfrac{v_{c_2} - v_{c_1}}{R} - i_R(v_{c_1}) \\ C_2 \dfrac{dv_{c_2}}{dt} &= \dfrac{v_{c_1} - v_{c_2}}{R} + i_L \\ L \dfrac{di_L}{dt} &= -v_{c_2} \end{cases} \tag{1}$$

$$i_R(v_{C_1}) = \begin{cases} G_b v_{C_1} + B_p(G_b - G_a), & \text{if} \quad v_{C_1} < -B_p \\ G_a v_{C_1}, & \text{if} \quad |v_{C_1}| \leq B_p \\ G_b v_{C_1} + B_p(G_a - G_b), & \text{if} \quad v_{C_1}) > B_p \end{cases} \tag{2}$$

section. Section II points out important concepts for understanding the rest of the text. The methods used in this work, as well as the results, are shown in Sections III and IV, respectively. Finally, section V contains the conclusion of the paper.

## II. Preliminary Concepts

### A. Chua's circuit

The circuit developed by Chua et al. [16], exhibits nonlinear behaviour, such as a spiral attractor and double-scroll attractor. Since then, this circuit (Fig. 1) has been extensively studied and simulated computationally. The circuit is composed by linear passive elements: two capacitors, an inductor and a resistor, which are connected to an active, nonlinear element called the Chua's diode (Nr), as shown in Fig. 1a. Therefore, according to Kirchhoff's law, it is possible to obtain the differential equations which represents the circuit's dynamic, (1). The resistive effect of the inductor is considered as imperceptible. The current through the nonlinear element, $i_R(v_{C_1})$ is given by (2). Fig. 1b displays the nonlinear behaviour of the Chua's diode, given by the relation *voltage* x *current* of the component.

### B. Lyapunov Exponent

There are many definitions about chaos. However, the concepts of Lyapunov exponents are the most influential work present in literature. The Lyapunov Exponent (LE), is a method which quantifies the exponential divergence of initially close orbits. The presence of a positive LE indicates chaos. In literature, there are numerous methods to determine the LE, as the Kantz's method [17], for example. In Kantz's approach, he considers the following equation:

$$S(\Delta n) = \frac{1}{N-m} \sum_{n=m+1}^{N} \times ln \left( \frac{1}{|\eta_n|} \sum_{x_{n'} \epsilon \eta_n} |x_{n'+\Delta n} - x_{n+\Delta n}| \right) \tag{3}$$

where $\eta_n$ is the set of all others delay vectors in an $\epsilon$-neighborhood of the vector $x_n$ (data from trajectories of the system under investigation) and $|\eta_n|$ is the number of elements in $\eta_n$. The Lyapunov exponent can be estimated by searching for a linear scaling in plot $S(\Delta n)$ versus $\Delta n$ [18].

By the characteristics mentioned above, it is possible to relate the importance of this topic in cryptography. Since the system (Chua's circuit) used to encrypt the image is chaotic, the process of decryption, without knowing the seed and the secret key is computationally expensive, making it a difficult task.

### C. The lower bound error

The lower bound error is used to analyze the error propagation in numerical simulations [15]. For the understanding of this tool, orbits, pseudo-orbits and natural interval extensions are defined in this section.

**Definition 1**: an orbit is a sequence of values of a map or system, represented by $x_i = [x_0; x_1; x_2; x_3 ... x_i]$.

Results of numerical simulation, due to truncation and rounding errors, inherent of a computer, cannot fit into a true orbit, therefore they are called pseudo-orbits.

**Definition 2**: a pseudo-orbit is an approximation of the true orbit, represented by $\hat{x_i} = [\hat{x_0}, \hat{x_1}, \hat{x_2}, \hat{x_3} ... \hat{x_i}]$ which accepts the relation $|x_i - \hat{x}_i| \leq \delta$, where $\delta$ is the associated error.

As described by Nepomuceno and Martins [14], a natural interval extension is defined:

**Definition 3**: a natural interval extension of a function $f$ is an interval-valued function $F$ of an interval variable $X$, with the property $F(x) = f(x)$, where by an interval it is meant to be a closed set of real numbers $x \in \Re$ such that $X = [\underline{X}, \overline{X}] = x : \underline{X} \leq x \leq \overline{X}$.

Using the Chua's circuit equations, examples of natural interval extensions are shown by (4) and (5).

$$C_1 \frac{dv_{C_1}}{dt} = \frac{v_{C_2} - v_{C_1}}{R} - i_R(v_{c_1}) \tag{4}$$

$$C_1 \frac{dv_{C_1}}{dt} = \frac{v_{C_2}}{R} - \frac{v_{C_1}}{R} - i_R(v_{c_1}) \tag{5}$$

The lower bound error is established by the following definition:

**Definition 4**: given two pseudo-orbits $\hat{x}_{a,n}$ and $\hat{x}_{b,n}$, arising from two different natural interval extensions of the function $f(x)$, the lower bound error $\delta$ is given by:

$$\delta = \frac{|\hat{x}_{a,n} - \hat{x}_{b,n}|}{2}. \tag{6}$$

### *D. Cryptography*

Cryptography is the science which studies techniques to make data illegible. In this way, it is possible to transmit all information securely. To perform the decryption, one should be aware of cryptographic key [19].

The encryption and decryption can be done using the bit-wise XOR operation, because the probability of the XOR output being zero or one is $50\%$ and by the following propriety: $(A \oplus B) \oplus B = A \oplus 0 = A$. In other words, using the cryptographic key B twice in the document that you want to encrypt A, the result remains A. This property represents the entire cryptographic process.

To ensure that the encryption process is good enough to make the image illegible, there are several ways to testify this: the correlation coefficient of adjacent pixels randomness test, the Shannon entropy test and the distribution of pixel in an image plotting an histogram. In a histogram, when the encryption process is performed, the cipher image must be uniform, in other words, the frequencies of the pixels must be approximately equal to all color intensities. So doing, the cipher image does not bring any relevant information.

It is well known that in plain-images, the adjacent pixels are strongly correlated with each other. Therefore, in a cipher image, the correlation coefficient in horizontal, vertical and diagonal directions are expected to be close to zero. The correlation coefficient of adjacent pixels randomness test measures this correlation by (7) [20].

$$\rho(X, Y) = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \tag{7}$$

where $X$ represents the series of pixels at position, $Y$ represents the series of adjacent pixels, $\mu$ and $\sigma$ are the mean and the standard deviation values, respectively, and $E$ is the mathematical expectation.

The Shannon entropy is a tool to measure the randomness in a communication systems. It is defined by (8) [21]:

$$H(X) = \sum_{i=1}^{2^N - 1} P_i log_2 \frac{1}{P_i} \tag{8}$$

where $H(X)$ is the entropy (bits), $X$ is a symbol and $P_i$ is the probability value of symbol $X$.

In image encryption, there are 256 values that each pixel can be defined. Therefore, for a cipher image, the expected value is $H(X) = 8$ bits.

## III. Methodology

A fundamental part of the method is the cryptographic key, which is the pseudo-randomness sequence. The sequence is generated simulating the Chua's circuit using the fourth order Runge-Kutta method, an integration step equal to $10^{-6}$ and the most important, the two natural interval extensions presented by (4) and (5) (see section II-C). This system has been chosen to apply the method, because it is a benchmark in the study of dynamical systems and the most important, its chaotic properties. The following Chua's parameters was used to generate the two pseudo-orbits: $C_1 = 10nF$, $C_2 = 100nF$, $L = 19mH$, $R = 1.8k\Omega$, $G_a = -0.68mS$, $G_b = -0.37mS$, $Bp = 1.1V$, $V_{C1} = -0.5V$, $V_{C2} = -0.2V$, $I_L = 0A$. Afterwards, to encrypt an image, we have used the following steps, adapted from [5]:

- **Step 1**: For an image with $M \times N$ pixels, perform two simulations with different natural interval extensions of the Chua's circuit with $2000 + M \times N - 1$ iterations. The first 2000 points generated will be discarded. This is due to the fact that at the beginning of the simulation, the two pseudo-orbits are close to each other, making the generated sequence easy to identify. We have chosen 2000 points according to the critical time simulation described in [22].
- **Step 2**: After the two sequences $S_1$ and $S_2$ generated, the logarithm of the lower bound error is done, generating a single sequence S:

$$S = log_{10} \frac{|S_1 - S_2|}{2}. \tag{9}$$

- **Step 3**: The normalizing process of the sequence S is done as follows:

$$S_n = uint8(mod(S \times 10^{15}, 256)), \tag{10}$$

  which $S_n$ is the normalized sequence. Uint8 is an algorithm available on the latest release of the software *Matlab*, which converts the sequence into 8-bit positive integer and mod represents the modulo operation: the rest of the division $S \times 10^{15}$ by 256. This is necessary as tested images are 8-bit gray using a pixel matrix with number between 0 (black tone) and 255 (white tone).
- **Step 4**: With the key $S_n$ and the media to be encrypted in the same numeric format, the bit-wise XOR operation is performed.

The standard gray $256 \times 256$ Lena image was used to assess the algorithm performance. All data, routines and simulations used in this work were generated using the Matlab software and are available upon request.

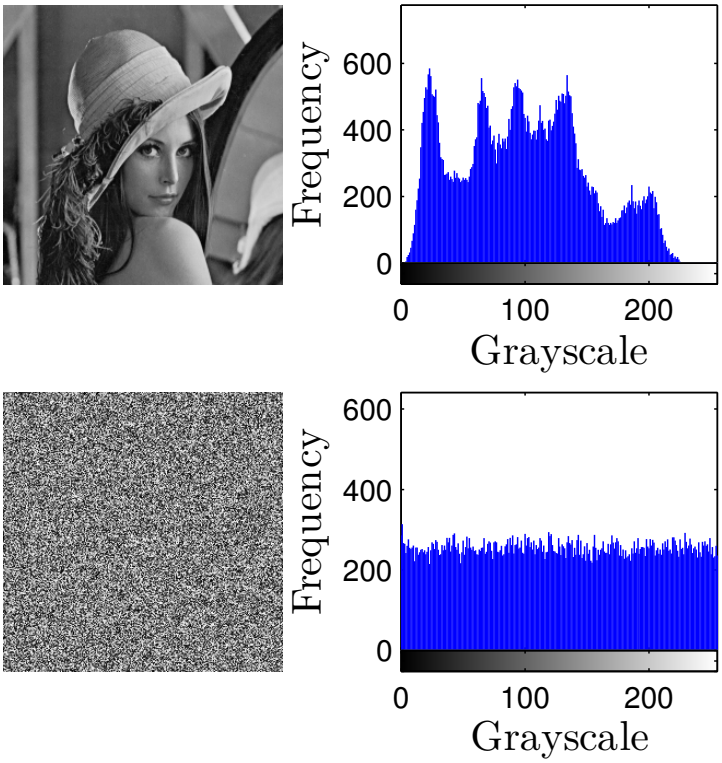


Fig. 2. The plain-image Lena as well as the cipher image herewith their histograms.

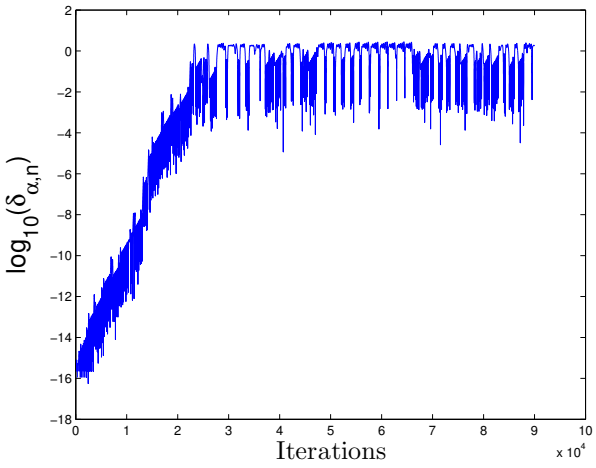


Fig. 3. The lower bound error obtained from two interval extensions.

## IV. Results and Discussion

The lower bound error, which is obtained from the parameters specified in the previous section, is shown in the Fig. 3. The two natural interval extensions used are $C_1\frac{dv_{C_1}}{dt} = \frac{v_{C_2} - v_{C_1}}{R} - i_R(v_{c_1})$ and $C_1\frac{dv_{C_1}}{dt} = \frac{v_{C_2}}{R} - \frac{v_{C_1}}{R} - i_R(v_{c_1})$. The LE ($\lambda$) was calculated by the Kantz's method, which resulted in a positive value equal to $\lambda = 0.199$, demonstrating its chaotic behavior and pseudo-randomness.

The Lena image was encrypted, after all the steps performed. Fig. 2 shows the plain-image and the cipher image along with their respective histograms. The original Lena image features a non-uniform distribution in the graphic. However, when it is encrypted, the histogram features a uniform distribution, which each color intensity level has the same frequency, approximately, becoming an illegible image. It is worth noting that with the decryption process, the image becomes legible again, as shown in Fig. 4.

The entropy test and correlation between two adjacent pixels was executed and the results were slightly close to the expected value (see Table 1).

TABLE I
Tests for the cipher image

| Correlation Coefficient | | | Entropy | References |
|---|---|---|---|---|
| Horizontal | Vertical | Diagonal | | |
| 0.0028 | 0.0059 | 0.0031 | 7.9969 | This work |
| 0.0016 | 0.0025 | 0.0003 | 7.9998 | C. Li et al. [23] |
| 0.00083 | 0.00223 | 0.00650 | 7.9826 | Y. Luo et. al [21] |

## V. Conclusion

In this paper, a novel image encryption method has been presented. This method is based on the concept of natural interval extension and the fact of limitation of numerical representation presented on computers. The proposed method was very efficient, producing a pseudo-random sequence with good cryptographic properties and encrypting the Lena image. The entropy measure and the correlation coefficients calculated using our approach has been shown to be as efficient as other works presented in literature. Furthermore, it is important to emphasise that the method evidence the random characteristic of the error.

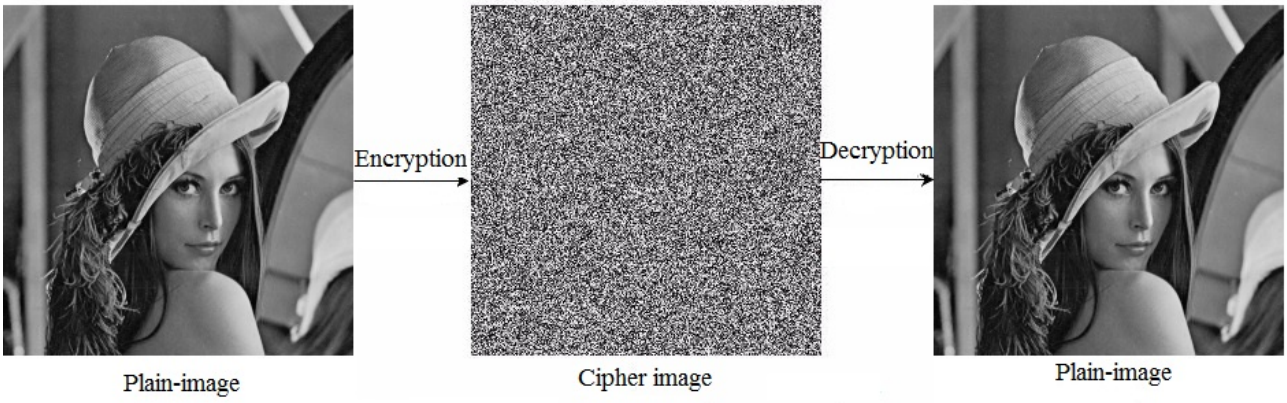


Fig. 4. By performing the bit-xor operation twice, the encryption and decryption process of an image is made, which represents the entire cryptographic process.

As a future work, the authors propose the study and the accomplishment of other tests, with the intention of analysing the computational performance and improving the proposed method, also constructing an embedded system for the use of cryptography in the most diverse fields.

## ACKNOWLEDGMENT

The authors thank the anonymous reviewers for their constructive comments which helped to improve the manuscript.

## REFERENCES

[1] R. F. Carrott, "Secure authorizations using independent communications and different one-time-use encryption keys for each party to a transaction," US Patent 9,569,776, Feb. 14, 2017

[2] X. Chai, "An image encryption algorithm based on bit level Brownian motion and new chaotic systems," Multimed. Tools Appl., vol. 76, no. 1, pp. 1159–1175, Jan. 2017.

[3] R. Jain, "The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling," John Wiley & Sons, 1990.

[4] X. Liu, P. Lu, J. Shao, H. Cao, and Z. Zhu, "Information hiding technology and application analysis based on decimal expansion of irrational numbers," AOPC 2017: Fiber Optic Sensing and Optical Communications, Oct. 2017.

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

[6] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, vol. 24, no. 3, pp. 759–765, May 2005.

[7] J. Banks, J. Brooks, G. Cairns, G. Davis and P. Stacey, " On Devaney's definition of chaos," The American Mathematical Monthly, vol. 99, no. 4, pp. 332–334, Apr. 1992.

[8] C. Herring and J. I. Palmore, "Random number generators are chaotic," ACM SIGPLAN Not., vol. 24, no. 11, pp. 76–79, Nov. 1989.

[9] J. Fridrich, "Image encryption based on chaotic maps," in 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, 1997, vol. 2, pp. 1105–1110.

[10] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, M. F. Abu-ElYazeed, and A. M. Soliman, "Generalized fractional logistic map suitable for data encryption," in 2015 International Conference on Science and Technology (TICST), 2015, pp. 336–341.

[11] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," IETE Tech. Rev., vol. 33, no. 3, pp. 310–322, May 2016.

[12] S. Li, G. Chen, and X. Mou, "On The Dynamical Degradation Of Digital Piecewise Linear Chaotic Maps," Int. J. Bifurc. Chaos, vol. 15, no. 10, pp. 3119–3151, Oct. 2005.

[13] IEEE Standard for Floating-Point Arithmetic," in IEEE Std 754-2008, pp.1-70, Aug. 29, 2008

[14] E. G. Nepomuceno and S. A. M. Martins, "A lower bound error for free-run simulation of the polynomial NARMAX," Syst. Sci. Control Eng., vol. 4, no. 1, pp. 50–58, Jan. 2016.

[15] E. G. Nepomuceno, S. A. M. Martins, G. F. V. Amaral, and R. Riveret, "On the lower bound error for discrete maps using associative property," Syst. Sci. Control Eng., vol. 5, no. 1, pp. 462–473, Jan. 2017.

[16] L. O. Chua, C. W. Wu, A. Huang, and G.-Q. Zhong, "A universal circuit for studying and generating chaos. I. Routes to chaos," IEEE Trans. Circuits Syst. I Fundam. Theory Appl., vol. 40, no. 10, pp. 732–744, Oct. 1993.

[17] H. Kantz, "A robust method to estimate the maximal Lyapunov exponent of a time series," Phys. Lett. A, vol. 185, no. 1, pp. 77–87, Jan. 1994.

[18] E. M. A. M. Mendes and E. G. Nepomuceno, "A Very Simple Method to Calculate the (Positive) Largest Lyapunov Exponent Using Interval Extensions," Int. J. Bifurc. Chaos, vol. 26, no. 13, p. 1650226, Dec. 2016.

[19] R. A. Molin, "An introduction to cryptography," CRC Press, 2000.

[20] A. V. Diaconu and A. C. Dascalescu, "Correlation distribution of adjacent pixels randomness test for image encryption," Proc. Rom. Acad. Ser. A, vol. 18, pp. 351–359, 2017.

[21] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," Commun. Nonlinear Sci. Numer. Simul., vol. 20, no. 2, pp. 447–460, Feb. 2015.

[22] E. G. Nepomuceno and E. M. A. M. Mendes, "On the analysis of pseudo-orbits of continuous chaotic nonlinear systems simulated using discretization schemes in a digital computer," Chaos, Solitons & Fractals, vol. 95, pp. 21–32, Feb. 2017.

[23] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," Nonlinear Dyn., vol. 87, no. 1, pp. 127–133, Jan. 2017.