Chaos
An Interdisciplinary Journal
of Nonlinear Science

Image encryption based on the pseudo-orbits from 1D chaotic map

Cite as: Chaos **29**, 061101 (2019); https://doi.org/10.1063/1.5099261
Submitted: 08 April 2019 • Accepted: 15 May 2019 • Published Online: 12 June 2019

Erivelton G. Nepomuceno, Lucas G. Nardo, Janier Arias-Garcia, et al.

AIP Publishing

Image encryption based on the pseudo-orbits from 1D chaotic map

Cite as: Chaos **29**, 061101 (2019); doi: 10.1063/1.5099261
Submitted: 8 April 2019 · Accepted: 15 May 2019 ·
Published Online: 12 June 2019

View Online Export Citation CrossMark

Erivelton G. Nepomuceno,[1,a] Lucas G. Nardo,[1,b] Janier Arias-Garcia,[2,c] Denis N. Butusov,[3,d] and Aleksandra Tutueva[4,e]

AFFILIATIONS

[1] Control and Modelling Group (GCOM), Department of Electrical Engineering, Federal University of São João del-Rei, São João del-Rei, MG 36307-352, Brazil
[2] Department of Electronic Engineering, Federal University of Minas Gerais, Belo Horizonte, MG 31270-901, Brazil
[3] Youth Research Institute, Saint Petersburg Electrotechnical University "LETI," 5, Professora Popova st., 197376 Saint Petersburg, Russia
[4] Department of Computer-Aided Design, Saint Petersburg Electrotechnical University "LETI," 5, Professora Popova st., 197376 Saint Petersburg, Russia

[a] nepomuceno@ufsj.edu.br
[b] gnlucas@gmail.com
[c] janier-arias@ufmg.br
[d] dnbutusov@etu.ru
[e] avtutueva@etu.ru

ABSTRACT

Chaotic systems have been extensively applied in image encryption as a source of randomness. However, dynamical degradation has been pointed out as an important limitation of this procedure. To overcome this limitation, this paper presents a novel image encryption scheme based on the pseudo-orbits of 1D chaotic maps. We use the difference of two pseudo-orbits to generate a random sequence. The generated sequence has been successful in all NIST tests, which implies it has adequate randomness to be employed in encryption process. Confusion and diffusion requirements are also effectively implemented. The usual low key space of 1D maps has been improved by a novelty procedure based on multiple perturbations in the transient time. A factor using the plain image is one of the perturbation conditions, which ensures a new and distinct secret key for each image to be encrypted. The proposed encryption scheme has been efficaciously verified using the Lena, Baboon, and Barbara test images.

Chaotic systems have been widely applied to cryptosystems. However, the use of chaotic maps has been questioned by the dynamical degradation due to finite precision in computers. As a consequence, there is a significant concern on the robustness of chaos-based encryption schemes. In this paper, we apply the concept of pseudo-orbit to the generation of random sequence. Instead of using the chaotic systems directly, we have employed the error appearing due to the computer finite precision, which can be estimated as the difference of two pseudo-orbits. Another important feature of our proposal is related to the key space. Using a novelty procedure based on multiple perturbations during the transient time, we have been able to increase the usually low key space of 1D maps. As 1D maps are very simple to implement, the proposed scheme is compelling. The generated sequence has been successful in all NIST tests, which implies it has adequate randomness to be utilized in encryption process. The proposed technique has been successfully tested for different images and compared with other methods presented in the literature.

I. INTRODUCTION

Over the recent years, chaotic systems have been explored in many diverse fields, such as sensors design, location systems, and information security.[1–3] Encryption algorithms have received great attention over the last few decades due to an exponential increase in the data traffic.[4] There are many works with different approaches investigating the chaos applications in cryptography. For instance, Wu *et al.*[5] have elaborated a cryptosystem using the operations of DNA confusion and diffusion, with the joint of two chaotic systems. Gao and Che[6] have used logistic map and hyperchaotic Chen's system to encrypt images. Lastly, Rostami *et al.*[7] applied the logistic map creating a fast encryption scheme suitable for parallel processing.

Alongside the cryptographic studies, many works have reported dynamical degradation of chaotic properties due to the finite precision effects.[8–10] Notably, Cao *et al.*[9] have exhibited a case of chaos suppression in the logistic map for a specific set of parameters. A great effort has been undertaken to mitigate such problems and many strategies have been reported. These approaches can be categorized into four general types: (a) using high finite precision calculations,[11] (b) coupling or cascading chaotic systems,[12,13] (c) switching between multiple chaotic systems,[14] and (d) perturbation chaotic systems by means of a pseudorandom process.[15] Although these strategies have shown some advances, chaotic-based encryption has still been reported to be vulnerable to known/chosen plaintext attacks.[10,16] All these factors determine the difficulties to efficiently use simple 1D chaotic maps, such as logistic map or tent map,[17] in encryption algorithms. In addition, these 1D maps present only one initial condition, which results in a poor key space. Nevertheless, 1D maps are still appealing as they have a simple structure and are easy to implement in hardware.[18]

Therefore, a chaos-based encryption scheme, which could reduce the digital degradation of 1D chaos systems with a large key space and good security properties, should be a desired solution. The novelty of this paper and its contribution are as follows. We present a method to mitigate the chaos degradation using two pseudo-orbits derived from two natural interval extensions. The initial condition is perturbed by a set of values. The perturbation conditions are chosen to appear after a few iterations that guarantee the loss of all significant digits according to critical time simulation.[19] The logistic map is chosen as a simple discrete chaotic system. In order to generate a single pseudorandom sequence, we have used the lower bound error operation.[20,21] Very recently, the concept of pseudo-orbit and interval extensions has successfully been applied to compute the Lyapunov exponent.[22] The efficiency of our proposal is shown through the performance analysis while encrypting three images. Experiments show that the proposed scheme has a good performance upon the following criteria: NIST SP 800-22, key space, key sensitive, correlation of adjacent pixels, information entropy, histogram, differential attacks, and information loss.

The remainder of this paper is organized as follows. Section II presents an overview of preliminary concepts used to define the designed scheme in Sec. III. Results as well as the discussion are shown in Sec. IV. Finally, Sec. V presents concluding remarks and further work analysis.

II. THE LOWER BOUND ERROR

Moore *et al.*[23] have described interval extensions, which are the basis for the lower bound error theorem. They defined an interval X as $[\underline{X}, \overline{X}] = x : \underline{X} \leq x \leq \overline{X}$. When considering the logistic map,[24] two examples of interval extensions are

$$F(X_n) = rX_n(1 - X_n), \tag{1}$$

$$G(Y_n) = rY_n - rY_nY_n. \tag{2}$$

Equations (1) and (2) are mathematically equivalent. However, due to the limitation of the numerical representation,[25,26] the two pseudo-orbits diverge exponentially. A simple procedure to estimate the simulation error is the lower bound error.[20,21]

Definition II.1. *Simulating two different natural interval extensions and giving the corresponding pseudo-orbits $\hat{x}_{a,n}$ and $\hat{x}_{b,n}$, the lower bound error δ is given by Ref. 20: $\delta = |\hat{x}_{a,n} - \hat{x}_{b,n}|/2$.*

III. THE 1D CHAOS-BASED SCHEME

The proposed scheme can be summarized in the following steps:[9,27]

Step 1: Choose the initial condition and perturbation values

$$M = [m_1 \quad m_2 \quad m_3 \quad m_4 \quad m_5 \quad c_i], \tag{3}$$

where $m_1 \in [0; 1]$ is the initial condition of the chaotic system. The parameters $m_i \in (0; 1), i = 2, \ldots, 5$, are the perturbation values. Here, we have chosen four perturbation values, but their numbers can be easily increased, which will lead to a corresponding increase in the parameter space. c_i is also a perturbation value, but it depends only on the image to be ciphered, and it is defined by

$$c_i = \frac{1}{(L \times W)^2} \sum_{i=1}^{L} \sum_{j=1}^{W} I_p(i, j), \tag{4}$$

where L and W are the length and width, respectively, and i and j are the coordinates of the plain image I_p. Moreover, each pixel of the matrix I_p can range from 0 to 255, for a grayscale image.

Step 2: Update the first initial condition $[X_0 = Y_0 = M(1, 1)]$ and the parameter r of the logistic map.

Step 3: From two natural interval extensions, simulate the 1D map twice $tr + L \times W - 1$ times. The tr points are discarded transient response. After $k \times 100$ iterations, $k = 1, 2 \ldots, 6$, the two interval extensions are perturbed with the vector M,

$$X_{n+1} = \mod (X_{n+1} + M(k, 1), 1), \tag{5}$$

$$Y_{n+1} = \mod (Y_{n+1} + M(k, 1), 1), \tag{6}$$

where mod is the module operation. One hundred iterations are sufficient to guarantee the loss of all significant digits in a double-precision floating-point format.[19,28]

Step 4: Calculate the lower bound error K given by

$$K = \frac{|X - Y|}{2}. \tag{7}$$

Step 5: The standardization process is as follows:

$$K_s = \text{uint8}(\text{mod}(K/\min(K)) \times 256, 256), \tag{8}$$

where uint8 is an algorithm to convert double-precision numbers in unsigned integer 8-bit numbers.

Step 6: Transform the vector key K into a matrix, using the reshape algorithm,

$$K_s = \text{reshape}(K_s, [L, W]). \tag{9}$$

Step 7: Obtain the cipher image I_c applying the bit-wise XOR operation between I_p and K_s,

$$I_c(i, j) = I_p(i, j) \oplus K_s(i, j). \tag{10}$$

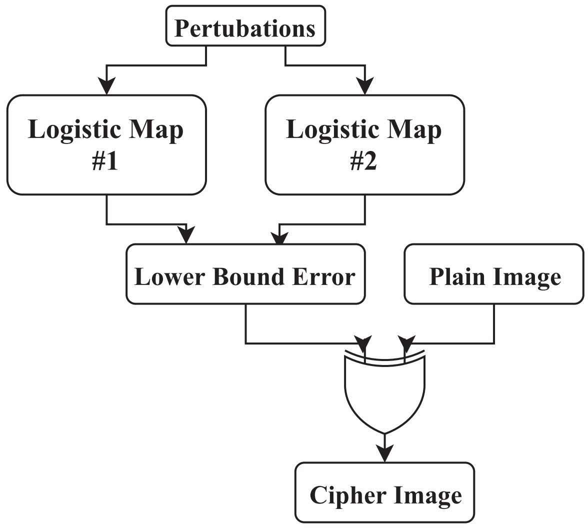

FIG. 1. Outline of the main novelty steps of the proposed encryption scheme based in the lower bound error.[20,21]

Figure 1 outlines the encryption scheme. The use of 1D map with multiple perturbation values and the lower bound error are the novel features of the proposed algorithm. It is important to notice that the scheme proposed here can be easily adapted to colored image. For instance, the generation of key stream can be done following the method designed in Ref. 29.

IV. RESULTS AND DISCUSSION

To validate the proposed encryption scheme, the following tests were performed: NIST SP 800-22 test, key space analysis, the correlation of adjacent pixels, information entropy, histogram, key sensitivity, differential analysis, and cropping attack.

The following parameters have been used to generate the key stream: $r = 3.99$, $M = [0.10.20.30.40.5c_i]$, $tr = 700$. We used two natural interval extensions given by Eqs. (1) and (2). The parameters c_i for Lena, Baboon, and Barbara are $4.731\,966\,182\,589\,531 \times 10^{-4}$, $4.997\,396\,608\,814\,597 \times 10^{-4}$, and $4.478\,178\,161\,662\,072 \times 10^{-4}$, respectively.

A. NIST SP 800-22 test

NIST SP 800-22 consists of 15 tests and has been extensively used to verify the pseudorandom features of a sequence.[9,30–32] The test provides a P-value at a level of significance α. If P-value $\geq \alpha$, then the sequence passes the test, and it can be considered as random.[9,30] Table I shows the P-value for 15 tests. The sequence tested had a bit stream length equal to 1 000 000, $\alpha = 0.01$, and it was obtained from an adjustment of Eq. 8 ($K_s = \text{uint16}(\text{mod}(K/\min(K)) \times 2^{16}, 2^{16})$, in order to obtain a long sequence. All the tests have been successful as the P-value ≥ 0.01.

TABLE I. Results of the NIST test for the proposed cryptosystem. All the tests have been successful as the P-value ≥ 0.01.

Statistical test	P-value	Result
Frequency	0.935 716	Passed
Block frequency ($m = 128$)	0.798 139	Passed
Cusum-forward	0.122 325	Passed
Cusum-reverse	0.554 420	Passed
Runs	0.181 557	Passed
Long runs of ones	0.171 867	Passed
Rank	0.816 537	Passed
Spectral Discrete Fourier Transform (DFT)	0.075 719	Passed
Nonoverlapping templates ($m = 9$)	0.262 249	Passed
Overlapping templates ($m = 9$)	0.383 827	Passed
Universal	0.080 519	Passed
Approximate entropy ($m = 10$)	0.964 295	Passed
Passed excursions ($x = +1$)	0.155 209	Passed
Passed excursions variant ($x = -1$)	0.970 538	Passed
Linear complexity ($M = 500$)	0.262 249	Passed
Serial ($m = 16$, $\nabla\Psi^2_m$)	0.616 305	Passed

B. Key space

A secure cryptosystem must have a key space larger than 2^{100} to be robust against brute-force attacks.[3,33,34] Our algorithm contains one initial condition and four perturbation values with the approximate key space of 2^{53^5}. We consider a factor that is the average of the image pixel values, which represents a key space $512 \times 512 = 2^{18}$. Hence, the overall scheme key space is 2^{283}, which is larger than the required minimum.

C. Correlation analysis of adjacent pixels

In a plain image, the correlation coefficient is close to one, indicating high correlation among pixels. On the other hand, encrypted images display correlation coefficients close to zero.[34] The correlation coefficients are given by[35]

$$\rho(X, Y) = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}, \tag{11}$$

TABLE II. The correlation coefficients for the test images. The correlation for each original and encrypted image is given. Encrypted images display values near to zero, which are expected for strong encryption schemes. (O) stands for original and (C) for ciphered image.

	Correlation coefficient		
Image	Horizontal	Vertical	Diagonal
Lena (O)	0.973 23	0.986 48	0.960 31
Lena (C)	−0.002 51	−0.002 92	−0.001 56
Baboon (O)	0.869 98	0.829 20	0.800 18
Baboon (C)	−0.001 80	0.000 66	−0.001 28
Barbara (O)	0.895 39	0.958 87	0.883 04
Barbara (C)	0.000 11	0.003 46	0.001 84

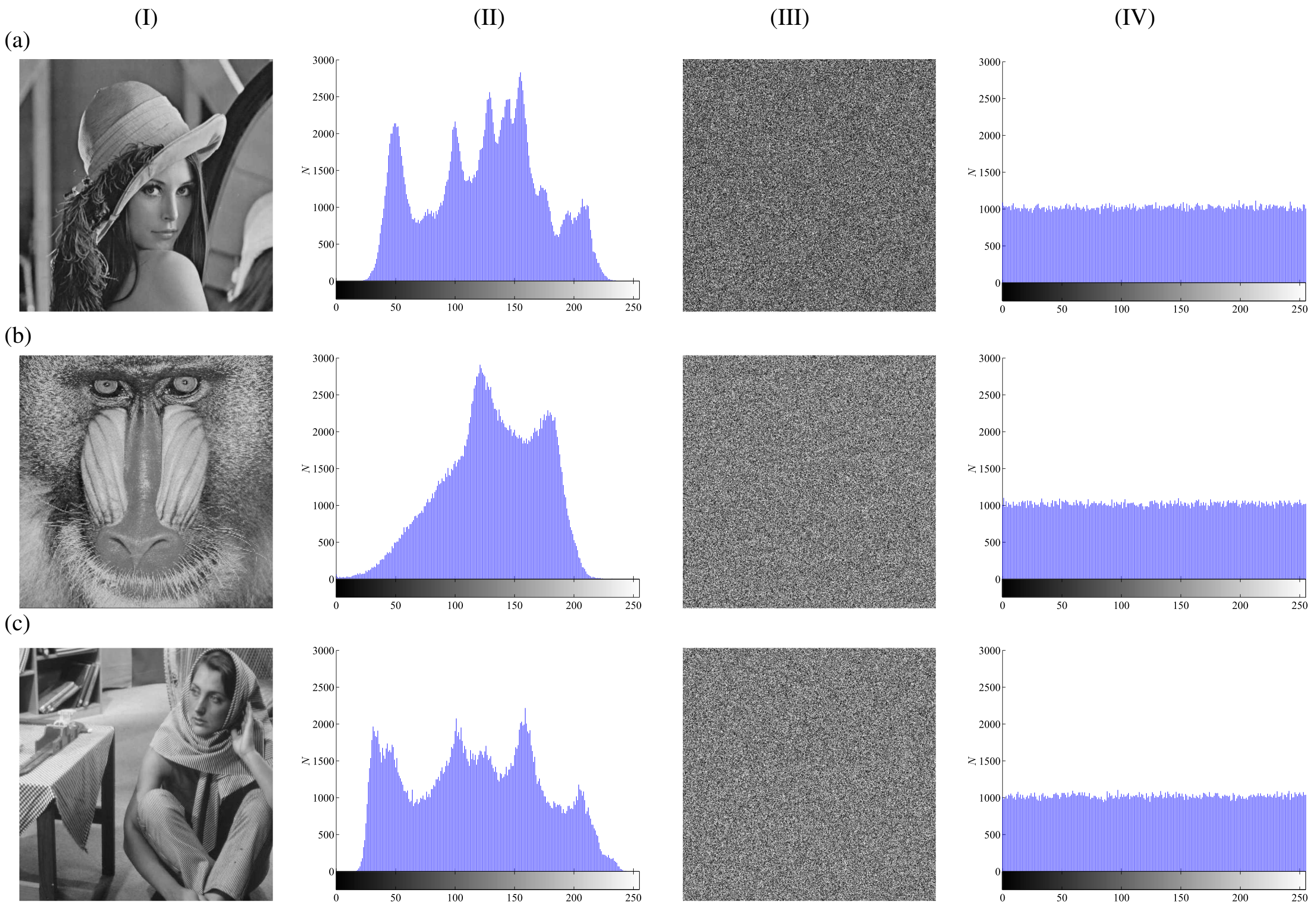

FIG. 2. Histograms for plain and ciphered images. The second and fourth columns exhibit the histograms for the plain and encrypted images, respectively. Although the plain image displays a significant presence of particular gray value, our encryption algorithm converts the plain image to a noiselike image with uniform distribution of pixels. Table III evidences the significant reduction of variance.

where μ, σ, and E are the mean, the standard deviation, and expectation values for the variables X and Y, respectively. Table II shows that correlation coefficients for the encrypted images are very close to zero, which confirms the applicability of the proposed algorithm.

D. Entropy analysis

An estimation of randomness using entropy is given by[36]

$$H(X) = \sum_{i=1}^{2^N-1} P_i \log_2 \frac{1}{P_i}, \tag{12}$$

where $H(X)$ is the entropy in bits, X is an input variable, and P_i is the likelihood estimation of variable X. For a ciphered image, $H(X) \approx 8$. The entropy value for Lena, Baboon, and Barbara is 7.999 3. The information entropy of the ciphered image should be close to 8 after encryption. The closer it gets to 8, the less feasible for the cryptosystem to unveil information.[29] Therefore, as the calculated entropy is very close to 8 for the three images, the probability of information leakage is very little.

E. Histogram analysis

It is expected to obtain uniform histograms for the encrypted images.[33,37] Figure 2 displays the results of histogram analysis for test images. Note the reduction of pixel variance between the plain and encrypted images. Table III shows the respective variances, according to Eq. (13),[37,38] as

$$\mathrm{Var}(h) = \frac{1}{G_L^2} \sum_{i=0}^{G_L-1} \sum_{j=0}^{G_L-1} \frac{1}{2}(h_i - h_j)^2, \tag{13}$$

where $G_L = 256$ is the gray level and h is the vector of the histogram values. The variances were significantly reduced. The percentage reduction between the cipher and plain images is greater than 99.7% in all cases, which is a superior level comparing to 99.1% obtained in Ref. 39.

TABLE III. Histogram variances for the test images. The third column demonstrates that the level of decrease in variance of the cipher image is in contrast to the plain image.

Image	Variance		
	Plain	Ciphered	Reduction (%)
Lena	643 270.56	1000.18	99.84
Baboon	847 461.35	990.11	99.88
Barbara	383 694.31	963.07	99.75

F. Key sensitivity analysis

Based on the methodology described by Zhang,[38] we analyze how the key stream changes when minor disturbances are introduced. The values of vector M, one at a time, are perturbed by a factor equal to 10^{-14}, and the encryption process is performed, getting C_2. The difference between the ciphered images is quantified by[38]

$$\text{Diff}_1(\%) = \frac{100}{L \times W} \sum_{i=1}^{L} \sum_{j=1}^{W} |\text{sign}(C_1(i,j) - C_2(i,j))|, \tag{14}$$

where L and W are the length and width of the cipher images C_1 (with no perturbed values) and C_2. From the key stream obtained via perturbations as vector M, we perform the decryption process using C_1, getting P_2. Equation (15) quantifies the difference between the plain images P_1 and P_2,

$$\text{Diff}_2(\%) = \frac{100}{L \times W} \sum_{i=1}^{L} \sum_{j=1}^{W} |\text{sign}(P_1(i,j) - P_2(i,j))|. \tag{15}$$

Table IV displays the differences using Eqs. (14) and (15) in the Lena image test. As it has been expected, the outcome is completely different.

G. Differential analysis

The number of changing pixel rate (NPCR) is described by Eq. (16), while the unified average changed intensity (UACI) is described by Eq. (17). These two indexes allow measuring the vulnerability to differential attacks.[38] To perform this test, two plain images are encrypted, with the particular attention that one of the plain images has a randomly chosen pixel with a modified value,

$$\text{NPCR}\ (\%) = \frac{100}{L \times W} \sum_{i=1}^{L} \sum_{j=1}^{W} |\text{sign}(C_1(i,j) - C_2(i,j))|, \tag{16}$$

$$\text{UACI}\ (\%) = \frac{100}{L \times W} \sum_{i=1}^{L} \sum_{j=1}^{W} \frac{|C_1(i,j) - C_2(i,j)|}{255}, \tag{17}$$

where L and W are the length and width of the ciphered image C_i. Table V displays the NPCR and UACI scores from distinct images. The proposed scheme has been successfully tested considering the critical values provided by Wu *et al.*[40]

TABLE IV. Results of key sensitivity analysis for the Lena image. Levels near to 100% suggest completely different images.

Secret key	Diff_1 (%)	Diff_2 (%)
$0.1 + 10^{-14}$	99.59	99.59
$0.2 + 10^{-14}$	99.62	99.62
$0.3 + 10^{-14}$	99.62	99.62
$0.4 + 10^{-14}$	99.61	99.61
$0.5 + 10^{-14}$	99.59	99.59
$b + 10^{-14}$	99.61	99.61

TABLE V. NPCR and UACI results. The encryption is successful according to the criteria established in Ref. 40.

Image	NPCR (%)	UACI (%)	Decision
Lena	99.61	33.46	Passed
Baboon	99.61	33.48	Passed
Barbara	99.60	33.43	Passed

H. Cropping attack

To analyze the robustness against cropping attack, we converted some 512 × 256 blocks of a ciphered image into black.[37,41] Figure 3 displays the ciphered images with blackened blocks and the decrypted images. Even with significant information loss, the decrypted Lena image is still recognizable. To achieve this result, a step has been added in the main algorithm.

Step A: The vector K in Eq. (7) is sorted in the ascending order using the MATLAB function [a, b]=sort(K). Before the XOR operation, the position of pixels is scrambled using the index b obtained from the sort function.

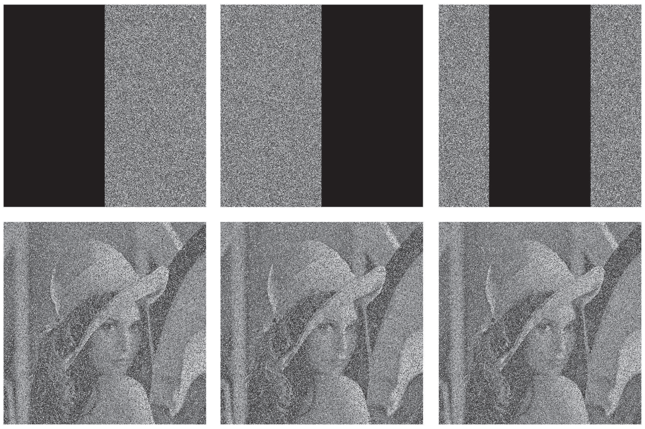

FIG. 3. Results of cropping attack. The first line displays the ciphered images, while the second line shows the respective decrypted images. Even in hard situation of 50% data-loss, our encryption scheme has been able to recover an original image.

TABLE VI. Performance comparison using the Lena image (512 × 512). With a very simple 1D chaotic system, our encryption algorithm possesses similar or better performance than the other methods described in the literature.[42–45]

Criteria	Ours	Ref. 42	Ref. 43	Ref. 44	Ref. 45
Key space	2^{283}	2^{128}	$\approx 2^{219}$	$\approx 2^{268}$	2^{280}
Entropy	7.999 3	…	7.998 3	7.999 3	7.999 3
CC—H	−0.002 1	−0.002 1	0.032 1	−0.004 5	0.001 7
CC—V	−0.002 9	−0.016 2	0.0272	−0.000 2	−0.002 2
CC—D	−0.001 6	0.017 8	0.038 4	0.005 3	−0.000 9
NPCR (%)	99.61	99.62	99.62	99.59	99.61
UACI (%)	33.46	33.48	33.49	33.41	33.46

Our results are in good agreement with other works.[42–45] In spite of being based on a very simple 1D chaotic system, our encryption scheme is superior in some cases, as it can be seen in Table VI.

V. CONCLUSION

In this paper, we reported a novel 1D chaos-based image encryption scheme. We have shown a way to undertake a simple and easy-to-implement 1D chaotic system for encryption of a plain image. Natural interval extensions and the lower bound error have been used to generate a random sequence based on the pseudo-orbits of the 1D logistic map, which has passed the NIST test. Using multiple perturbations during the transient time, the proposed technique possess a large key space, which can be easily increased. The experimental study shows that the proposed algorithm is effective, and the results can be further applied to other studies aimed at efficient chaos-based cryptography.[9,46] A natural continuation of this work will be the use of a similar scheme in embedded encryption systems using hardware description language and the formulation described in Ref. 47.

ACKNOWLEDGMENTS

Erivelton G. Nepomuceno was supported by Brazilian Research Agencies: Conselho Nacional de Desenvolvimento Cientíco e Tecnológico, Grant Nos. 465704/2014-0 and 425509/2018-4, and Fundação de Amparo à Pesquisa do Estado de Minas Gerais, Grant No. APQ-00870-17.

REFERENCES

[1] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," Chaos **16**, 033118 (2006).

[2] J. Machicao and O. M. Bruno, "Improving the pseudo-randomness properties of chaotic maps using deep-zoom," Chaos **27**, 053116 (2017).

[3] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," IEEE Access **6**, 75834–75842 (2018).

[4] D. S. Terzi, R. Terzi, and S. Sagiroglu, "A survey on security and privacy issues in big data," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (IEEE, 2015), pp. 202–207.

[5] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic color image cryptosystem based on DNA encryption and entropy," Nonlinear Dyn. **90**, 855–875 (2017).

[6] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," Phys. Lett. A **372**, 394–400 (2008).

[7] M. J. Rostami, A. Shahba, S. Saryazdi, and H. Nezamabadi-pour, "A novel parallel image encryption with chaotic windows based on logistic map," Comput. Electr. Eng. **62**, 384–400 (2017).

[8] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," Int. J. Bifurcat. Chaos **15**, 3119–3151 (2005).

[9] L. Cao, Y. Luo, S. Qiu, and J. Liu, "A perturbation method to the tent map based on Lyapunov exponent and its application," Chin. Phys. B **24**, 100501 (2015).

[10] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," IEEE Multimed. **25**, 46–56 (2018).

[11] S. Wang, W. Liu, H. Lu, J. Kuang, and G. Hu, "Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications," Int. J. Mod. Phys. B **18**, 2617–2622 (2004).

[12] G. Heidari-Bateni and C. McGillem, "A chaotic direct-sequence spread-spectrum communication system," IEEE Trans. Commun. **42**, 1524–1527 (1994).

[13] H. Hu, Y. Deng, and L. Liu, "Counteracting the dynamical degradation of digital chaos via hybrid control," Commun. Nonlinear Sci. Numer. Simul. **19**, 1970–1984 (2014).

[14] X.-J. Tong, "Design of an image encryption scheme based on a multiple chaotic map," Commun. Nonlinear Sci. Numer. Simul. **18**, 1725–1733 (2013).

[15] K. Persohn and R. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," Chaos Solitons Fractals **45**, 238–245 (2012).

[16] E. Y. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," Signal Process. **132**, 150–154 (2017).

[17] C. Li, T. Xie, Q. Liu, and G. Cheng, "Cryptanalyzing image encryption using chaotic logistic map," Nonlinear Dyn. **78**, 1545–1551 (2014).

[18] Y. Zhou, L. Bao, and C. P. Chen, "A new 1d chaotic system for image encryption," Signal Process. **97**, 172–182 (2014).

[19] E. G. Nepomuceno, S. A. Martins, B. C. Silva, G. F. Amaral, and M. Perc, "Detecting unreliable computer simulations of recursive functions with interval extensions," Appl. Math. Comput. **329**, 408–419 (2018).

[20] E. G. Nepomuceno and S. A. M. Martins, "A lower bound error for free-run simulation of the polynomial NARMAX," Syst. Sci. Control Eng. **4**, 50–58 (2016).

[21] E. Nepomuceno, S. Martins, G. Amaral, and R. Riveret, "On the lower bound error for discrete maps using associative property," Syst. Sci. Control Eng. **5**, 462–473 (2017).

[22] S. Zhou, X. Wang, Z. Wang, and C. Zhang, "A novel method based on the pseudo-orbits to calculate the largest Lyapunov exponent from chaotic equations," Chaos **29**, 033125 (2019).

[23] R. E. Moore, R. B. Kearfott, and M. J. Cloud, *Introduction to Interval Analysis* (SIAM, 2009), Vol. 110.

[24] R. M. May, "Simple mathematical models with very complicated dynamics," Nature **261**, 459–467 (1976).

[25] Institute of Electrical and Electronics Engineers (IEEE), *754-2008—IEEE Standard for Floating-Point Arithmetic* (IEEE, 2008), pp. 1–58.

[26] M. L. Overton, *Numerical Computing with IEEE Floating Point Arithmetic* (Society for Industrial and Applied Mathematics, 2001), p. 106.

[27] L. G. Nardo, A. M. Lima, E. G. Nepomuceno, and J. Arias-Garcia, "Image encryption algorithm using natural interval extensions," in *BTSym'18—Brazilian Techonology Symposium, 2018* (Unicamp ISSN: 2447-8326, 2018), pp. 1–5.

[28] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," IEEE Trans. Circuits Syst. I Regul. Pap. **66**, 2322–2335 (2019).

[29] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," Comput. Math. Appl. **59**, 3320–3327 (2010).

[30] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Technical Report, National Institute of Standards and Technology, April 2010.

[31] A. V. Tutueva, D. N. Butusov, D. O. Pesterev, D. A. Belkin, and N. G. Ryzhov, "Novel normalization technique for chaotic pseudo-random number generators based on semi-implicit ODE solvers," in *2017 International Conference on*

Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS) (IEEE, 2017), Vol. 2, pp. 292–295.

[32] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," Chaos Solitons Fractals **118**, 134–144 (2019).

[33] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," Nonlinear Dyn. **78**, 995–1015 (2014).

[34] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," Nonlinear Dyn. **87**, 51–66 (2017).

[35] A.-V. Dianocu and A. C. Dascalescu, "Correlation distribution of adjacent pixels randomness test for image encryption," Proc. Rom. Acad. Ser. A **18**, 351–360 (2017).

[36] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," Commun. Nonlinear Sci. Numer. Simul. **20**, 447–460 (2015).

[37] Z.-h. Gan, X.-l. Chai, D.-j. Han, and Y.-r. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," Neural Comput. Appl. **28**, 1–20 (2018).

[38] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," IETE Tech. Rev. **33**, 310–322 (2016).

[39] S. Namasudra and G. Deka, *Advances of DNA Computing in Cryptography* (CRC Press, 2018).

[40] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," Cyber J. Multidisciplinary J. Sci. Technol. (JSAT) **1**, 31–38 (2011).

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

[42] H. Yang, K. W. Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," Commun. Nonlinear Sci. Numer. Simul. **15**, 3507–3517 (2010).

[43] X. Wang and C. Jin, "Image encryption using game of life permutation and PWLCM chaotic system," Opt. Commun. **285**, 412–417 (2012).

[44] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Opt. Lasers Eng. **88**, 197–213 (2017).

[45] X. Zhang, Z. Zhao, and J. Wang, "Chaotic image encryption based on circular substitution box and key stream buffer," Signal Process. Image Commun. **29**, 902–913 (2014).

[46] 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)* (IEEE, 2015), pp. 336–341.

[47] E. G. Nepomuceno, A. M. Lima, J. Arias-García, M. Perc, and R. Repnik, "Minimal digital chaotic system," Chaos Solitons Fractals **120**, 62–66 (2019).