Chaos, Solitons and Fractals 123 (2019) 69–78

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

Frontiers

# Image encryption using finite-precision error

Lucas G. Nardo[a], Erivelton G. Nepomuceno[a,*], Janier Arias-Garcia[b], Denis N. Butusov[c]

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

ARTICLE INFO

*Article history:*
Received 28 January 2019
Revised 26 March 2019
Accepted 27 March 2019
Available online 3 April 2019

*Keywords:*
Image encryption
Finite-precision error
Natural interval extension
Lower bound error
Computer arithmetic
NIST tests

ABSTRACT

Chaotic systems are broadly adopted to generate pseudo-random numbers used in encryption schemes. However, when implemented on a finite precision computer, chaotic systems end up in dynamical degradation of chaotic properties. Many works have been proposed to address this issue. Nevertheless, little attention has been paid to exploit the finite precision as a source of randomness rather a feature that should be mitigated. This paper proposes a novel plain-image encryption using finite-precision error. The error is obtained by means of the implementation of a chaotic system using two natural different interval extensions. The generated sequence has passed all NIST test, which means it has sufficient randomness to be used in encryption. Several benchmark images have been effectively encrypted using the proposed approach.



## 1. Introduction

Chaotic systems have been considered as an important nonlinear source in designing encryption schemes [1–3]. Encryption has received great attention over the last few decades due to an exponential increase in the amount of data traffic [4]. Among the many applications of encryption, image security attracts huge concerns from academic and industry actors. According to Wu [5], the unplanned exposure of particular and governmental photos accentuates the importance of image security. These images can be related to objects, persons, technical specifications of projects, among others [6].

One of the main reasons to exploit chaotic systems in encryption schemes is related to the statement made by Herring and Palmore [7], who have established an intrinsic relationship between pseudo-random number generators and chaotic systems. Matthews [8] has been considered as pioneer to propose an encryption scheme based on chaos. After that, many works with different chaotic systems have been employed to propose cryptographic methods [9–18]. Here are some examples: Li et al. [18] have proposed an image encryption algorithm using the tent map. In the same way, Wang et al. [10] have developed a new scheme using the logistic map, as the chaotic system and several other operations, such as the applications of disturbance, the pixels shuffling and pixels substitution to ensure the encryption performance. There are also combinations of chaotic systems, such as logistic-tent system proposed by Chai [9] or continuous three-dimensional chaotic, as the Lorenz system used in [19] and Van der Pol-Duffing oscillator in [20].

Whereas most of chaos-based encryption schemes have been shown successful in literature, some studies have questioned the effectiveness of such methods. Recently, Özkaynak [21] has done several case studies indicating that some methodologies are easy to break and also showed a series of steps that cryptographic methods must follow to be considered safe. Wu et al. [22] have reported that a number of papers, well accepted in the academic community, do not pass the statistical tests NPCR and UACI when rigorous expected values are applied, therefore such methods are vulnerable to differential attacks. Apart from that, a major challenge to be faced in the application of chaotic systems is that certain systems show degradation of their chaotic properties due to the use of finite precision in digital computers, as reported by Li et al. [23]. Over the past few years, many researchers have been successful in reducing the degradation of the chaotic properties of digital systems, as shown in [24]. The reader is referred to [25–43] for an extensive bibliography on this topic. Nevertheless, little attention has been paid to exploit the finite precision as a source of randomness rather a feature that should be mitigated. The authors in [44] have considered the finite-precision, but their work deals with the short-period phenomena in chaotic system using binary approach and it can be seen as a standard technique to deal with chaos degradation. In general, finite-precision error is something to be minimized [45,46].

* Corresponding author.
*E-mail addresses:* nepomuceno@ufsj.edu.br (E.G. Nepomuceno), janier-arias@ufmg.br (J. Arias-Garcia), dnbutusov@etu.ru (D.N. Butusov).

https://doi.org/10.1016/j.chaos.2019.03.026

This paper proposes a novel image encryption using finite-precision error. The error is obtained by means of the implementation of a chaotic system using two natural different interval extensions. With these two extensions, we calculate the lower bound error [47,48]. This measure has been used successfully to compute the largest Lyapunov exponent, in a sense that the calculated pseudo-orbit diverges exponentially from the precise orbits. More details on the lower bound error and its application can be seen in [49–53]. Chua's circuit has been employed as chaotic system [54–56]. An important feature of the proposed method is that the keystreams not only depend on the cipher keys, but also to the original plain-images. In this work, we have shown that the lower bound error presents suitable pseudo-random properties for our proposed encryption scheme. Indeed, the generated sequence by the lower bound error has passed all NIST test [24,57], which means it has sufficient randomness to be used in encryption [3,58]. To show the effectiveness of our proposal, several performance analysis have been performed in five images. Experiments show that the proposed scheme has a good performance upon the following performance criteria: key space, key sensitive, correlation of adjacent pixels, information entropy, histogram, differential, time and algorithm complexity analysis, resistance to known and chosen-plaintext attacks, noise attack and information loss.

The remainder of the article is presented as follows. In Section 2, an overview of preliminary concepts for understanding the rest of the work is presented. The methodology as well as the proposed algorithms of encryption and decryption are explained in Section 3. In Section 4, it is shown the performance analysis of the algorithm under a series of tests and compared with the results found in the literature. Finally, Section 5 contains the conclusion of the paper.

## 2. Preliminary concepts

### 2.1. Chua's circuit

The autonomous Chua's circuit [54] is formed by linear components: a resistor, an inductor and two capacitors, combined with to an active, piecewise linear component, well-known as the Chua's diode. This system is represented by Eq. (1). Moreover, Eq. (2) represents the current of the Chua's diode ($i_R(v_{c_1})$), which $G_a$, $G_b$ and $B_p$ are the slopes and the breaking points of the nonlinear component.

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

$$i_R(v_{c_1}) = \begin{cases} G_b v_{c_1} + B_p(G_b - G_a), & \text{if} \quad v_{c_1} < -B_p \\ G_a v_{c_1}, & \text{if} \quad |v_{c_1}| \le B_p \\ G_b v_{c_1} + B_p(G_a - G_b), & \text{if} \quad v_{c_1} > B_p \end{cases} \tag{2}$$

This circuit is one of the most used benchmarks in the research of dynamical systems and it has already been applied in encryption schemes as described in [59,60].

### 2.2. The lower bound error

Nepomuceno and Martins [47] have developed a technique to estimate an error bound propagation in numerical simulations. In order to understand the mechanisms of this technique, some definitions are given as follows.

**Definition 2.1.** A map or a system originate a sequence of values which configure an orbit, represented by $x_i = [x_0, x_1, x_2, x_3, \ldots, x_i]$.

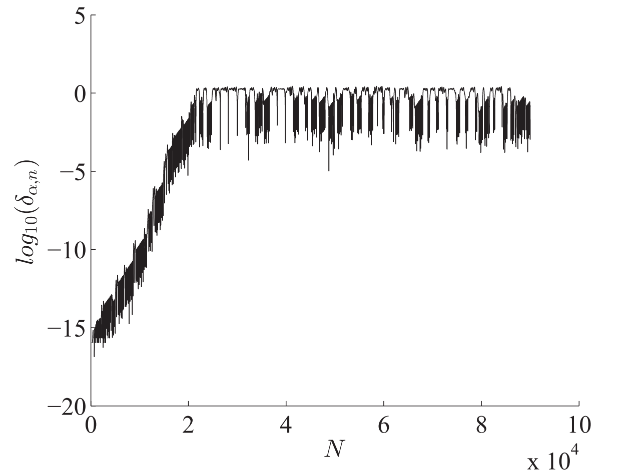


**Fig. 1.** The lower bound error from two pseudo-orbits. The logarithmic scale exhibits the loss of decimal places in the simulation and it is close related to error propagation of the simulation [63]. The x-axis is the number of iterates used by the discretization scheme as explained in Step 2 of Section 3. We have exploited the randomness properties of this sequence to generate the keystream for our proposed image encryption scheme.

**Definition 2.2.** A pseudo-orbit approximates a true orbit, represented by $\{\hat{x}_{i,n}\} = [\hat{x}_{i,0}, \hat{x}_{i,1}, \ldots, \hat{x}_{i,n}]$. A pseudo-orbit is originated due to computer finite-precision [47].

Interval and natural interval extension have been defined by Moore et al. [61] as:

**Definition 2.3.** An interval is a closed set of real numbers $x \in \mathbb{R}$ such that $X = [\underline{X}, \overline{X}] = x : \underline{X} \le x \le \overline{X}$.

**Definition 2.4.** A natural interval extension of a function $f$ is an interval-valued function $F$ of an interval variable $X$, with the property $F(x) = f(x)$ [47,62].

Here we present an example of such interval extension given by Eqs. (3) and (4)

$$c_1\frac{dv_{c_1}}{dt} = \frac{v_{C_2}-v_{c_1}}{R} - i_R(v_{c_1}) \tag{3}$$

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

Finally, the lower bound error can be established as follows.

**Definition 2.5.** Let be 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 [48]:

$$\delta = \frac{|\hat{x}_{a,n} - \hat{x}_{b,n}|}{2}. \tag{5}$$

Where $\delta$ has the same unit of measurement of the pseudo-orbits $\hat{x}_{a,n}$ and $\hat{x}_{b,n}$. Fig. 1 shows the divergence of the pseudo-orbits and the gradual increase of the error.

## 3. Proposed algorithm

The keystream of the proposed algorithm is obtained by the pseudo-random sequence of the lower bound error. We have used standard Matlab routines to describe the main steps of the encryption scheme [24].

**Step 1**: As a way to obtain a different keystream for different images, ensuring the diffusion and confusion properties, a factor for each original image is added to the initial condition ($V_{C1}$) according to Eq. (6).

$$V'_{C1} = V_{C1} + F_o, \tag{6}$$

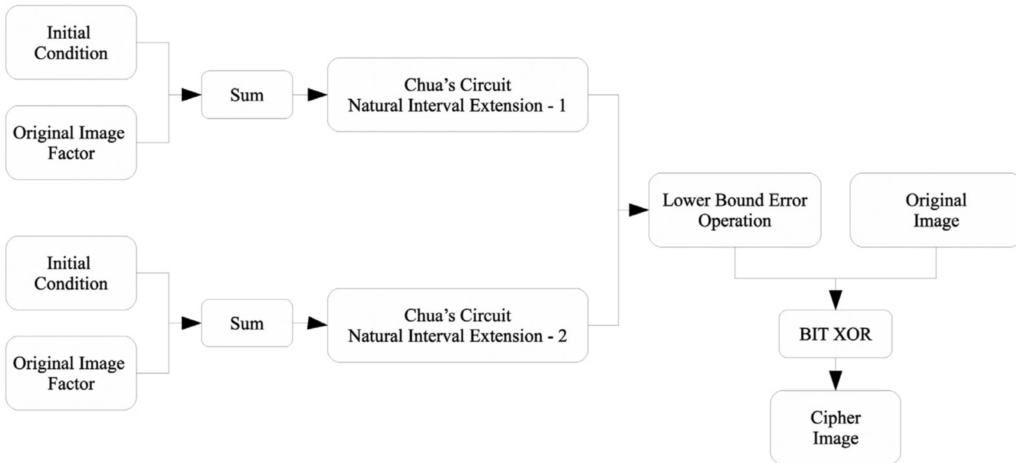


**Fig. 2.** Encryption process. The scheme shows the main steps of the proposed technique. The novelty propose here is based on the lower bound error [47,48].

where $F_o$ is dependent of the original plain-image. We call $F_0$ as original image factor and it is given by

$$F_o = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} P_a(i, j) \times 10^{-5}. \tag{7}$$

In Eq. (7), $P_a$ is an image of dimensions $M \times N$; $i$ and $j$ are the respective coordinate values. Note that the original image factor is given by the simple average of the pixel values multiplied by an element equal to $10^{-5}$.

**Step 2**: Chua's circuit is simulated using the 4th order Runge–Kutta method with an integration step of $10^{-6}$. The same initial condition is used for each natural interval extension. The number of iterates is given by $tr + M \times N - 1$, where $tr$ is the discarded transient time, and $M$ and $N$ are the dimension of the image to be encrypted. The $tr$ points can be estimated according the critical time suggested in [47].

**Step 3**: Two sequences $S_1$ and $S_2$ are generated by each natural interval extension. The logarithm of the lower bound error is performed to obtain single sequence $S \in \mathbb{R}^{M \times N - 1}$ given by (8):

$$S = log_{10} \frac{|S_1 - S_2|}{2}. \tag{8}$$

**Step 4**: Images are 8-bit grey using a pixel matrix with numbers between 0 (black tone) and 255 (white tone). The normalized sequence $S$ is given by:

$$S_n = uint8(mod(S \times 10^{15}, 256)), \tag{9}$$

where $uint8$ is Matlab routine to convert the sequence into 8-bit positive integer and $mod$ represents the modulo operator.

**Step 5**: In order to transform the sequence $S_n$ in an array with equivalent format of the original image, the following process is done:

$$S_n = vec2mat(S_n, N), \tag{10}$$

where $vec2mat$ is the process of converting vector to matrix and N is the width of the image.

**Step 6**: To encrypt the plain image ($P_a$) in a cipher image ($C_i$), the bit-wise XOR operation is executed with the normalized sequence and the image, such as

$$C_i(i, j) = S_n(i, j) \oplus P_a(i, j).$$

These steps are illustrated by the image cryptosystem shown in Fig. 2. It is worth to say this encryption system respect the Kerckhoffs's principle [64], in other words, the only secret parameter is just the key. Once the image is encrypted, the process of converting the noise-like image to the original image is basically the reverse encryption process.

## 4. Performance analysis

A series of numerical experiments has been conducted to demonstrate the efficiency and security of the proposed approach. We have used the following benchmark $256 \times 256$ pixels images: Lena, boat, house, pepper and cameraman.

The experiments and validations are presented in Sections 4.1–4.11. Eleven criteria have adopted: NIST SP 800-22 test, key space, key sensitive, correlation of adjacent pixels, information entropy, histogram, differential, resistance to known and chosen plaintext attacks, noise attack, information loss and time and algorithm complexity analysis. Moreover, we have compared our results with other papers found in literature such as [13,18,19,65].

The following parameters have been used to generate the secret key, based on the circuit described in Aguirre [55]: $C_1 = 10nF$, $C_2 = 100nF$, $L = 19mH$, $R = 1.8k\Omega$, $G_a = -0.68mS$, $G_b = -0.37mS$, $Bp = 1.1V$. While the initial conditions are given by $V_{c_1} = 0.5V$, $V_{c_2} = -0.2V$, $I_L = 0A$. The natural interval extensions are presented in Eqs. (3) and (4). The original image factors added to the initial condition ($V_{c_1}$) are showed in Table 1. Fig. 3 shows the encryption and decryption results using the parameters and methodology.

### 4.1. NIST SP 800-22 test

The NIST SP 800-22 is a statistical test suite for RNGs (random number generators) and PRNGs (pseudo-random number generators) composed by 15 statistical tests. From each P-value, which is produced by the end of each test, it is possible to determine if the sequence can be or cannot be accepted as a random sequence. The significance level $\alpha$ helps in this decision, if $P - value \geq \alpha$, then the sequence passes the proposed test [24,57].

In order to generate the sequence according to NIST framework, we have adopted Eq. (9) as $S_n = uint32(mod(S \times 10^{15}, 2^{32}))$, since a

**Table 1**
The original image factor for the benchmark images. This factor has been calculated according to Eq. (7). This factor aims at increasing diffusion and confusion properties of the proposed encryption scheme. In order to guarantee the reproducibility of our results, the hexadecimal representation of the original image factor have been presented in the third column.

| Image | Factor | Hexadecimal representation |
|---|---|---|
| Lena | $9.867648315429686 \times 10^{-4}$ | 3f502acaab8a5ce5 |
| Boat | $1.360362091064453 \times 10^{-3}$ | 3f5649c5ac471b47 |
| House | $1.379846038818359 \times 10^{-3}$ | 3f569b7e670e2c12 |
| Pepper | $1.231443634033203 \times 10^{-3}$ | 3f542d0c88a47ecf |
| Cameraman | $1.187226562500000 \times 10^{-3}$ | 3f537396d0917d6b |

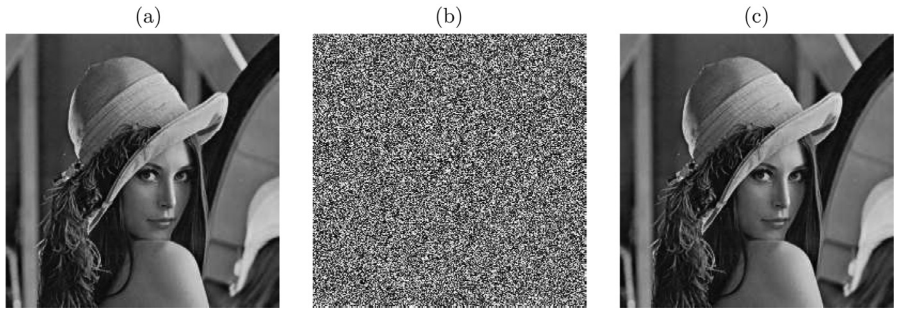


**Fig. 3.** Representation of cryptography by XOR operation. (a) and (c): Plain image. (b): Cipher image. The encryption occurs from image (a) to (b). The decryption is performed from image (b) to (c). The performance of bit-XOR operation twice represents the entire cryptographic process of encryption and decryption.

**Table 2**
P-value results for fifteen tests. The feasibility of the cryptosystem is proved, as the $P-value \geq \alpha = 0.01$ for all tests. Similar test has been performed by Cao et al. [24].

| Statistical Test | P-value | Result |
|---|---|---|
| Frequency | 0.883171 | **Passed** |
| Block Frequency ($m = 128$) | 0.236810 | **Passed** |
| Cusum-Forward | 0.437274 | **Passed** |
| Cusum-Reverse | 0.437274 | **Passed** |
| Runs | 0.759756 | **Passed** |
| Long Runs of Ones | 0.759756 | **Passed** |
| Rank | 0.145326 | **Passed** |
| Spectral DFT | 0.719747 | **Passed** |
| NonOverlapping Templates ($m = 9$, $B = 000000001$) | 0.554420 | **Passed** |
| Overlapping Templates ($m = 9$) | 0.595549 | **Passed** |
| Universal | 0.304126 | **Passed** |
| Approximate Entropy ($m = 10$) | 0.867692 | **Passed** |
| Random Excursions ($x = +1$) | 0.494392 | **Passed** |
| Random Excursions Variant ($x = -1$) | 0.236810 | **Passed** |
| Linear Complexity ($M = 500$) | 0.534146 | **Passed** |
| Serial ($m = 16$) | 0.554420 | **Passed** |

long sequence length is required. Starting from a bit stream length equal to 1000000 and $\alpha = 0.01$, the P-value for each test is exhibited in Table 2. As indicated by test outcomes, it is clear that the series generated proved successful at NIST tests. Thus, the designed system is suitable for use in encryption algorithm to generate random number [3,58].

### 4.2. Key space

In the proposed scheme, four secret parameters have been used to compose the key, namely: three initial conditions of Chua's circuit and the original image factor according to Eq. (7), which has been shown in Table 1. The three initial conditions are represented using floating-point [66] with precision of $p = 53$ bits, which yields $2^{53^3}$. The image factor gives a space of $256 \times 256 = 2^{16}$. Thus, the key space is approximately $2^{53^3} \times 2^{16} = 2^{175}$, which is larger than the minimum of $2^{100}$ suggested in the literature, which has been employed by Norouzi and Mirzakuchaki [12] and Hu et al. [19] to ensure robustness against brute-force attack.

### 4.3. Key sensitivity analysis

An encryption scheme must have high sensitivity to secret key changes. We have analysed this feature according to Zhang [16] as follows. Each of initial conditions $V'_{C1}$, $V_{C2}$ and $I_L$ have been perturbed separately by $10^{-14}$. The difference in the cipher image due to this perturbation has been quantified by [16]:

$$\mathrm{Diff}_1(\%) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |sign(C_1(i,j) - C_2(i,j))| \times 100, \qquad (11)$$

**Table 3**
Results of key sensitivity tests in the encryption and decryption processes applied to Lena. The Lena image has $(256 \times 256)$ pixels. A very small value is added to initial condition of each of the states of Chua's Circuit. The third and fourth columns present the values calculated according to Eq. (11) (encryption) and (12) (decryption) [16]. Values close to 100% indicate a completely different image.

| Secret Key | $\mathrm{Diff}_1(\%)$ | $\mathrm{Diff}_2(\%)$ |
|---|---|---|
| $V'_{C_1} + 10^{-14}$ | 99.64 | 99.64 |
| $V_{C_2} + 10^{-14}$ | 99.62 | 99.62 |
| $I_L + 10^{-14}$ | 99.59 | 99.59 |

where $M$ and $N$ are the length and width, respectively, of the cipher images $C_1$ (without perturbation) and $C_2$ (with perturbation); $sign()$ is the sign function.

The decryption process has been analysed in a similar way. The quantitative difference between two decrypted images $P_1$ (without perturbation) and $P_2$ (with perturbation) has been determined by [16]:

$$\mathrm{Diff}_2(\%) = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |sign(P_1(i,j) - P_2(i,j))| \times 100. \qquad (12)$$

Table 3 shows the results of key sensitive in the encryption and decryption process. The process is highly sensitive to changes in the secret key, as the difference in both cases are close to 100%.

### 4.4. Correlation analysis of adjacent pixels

Hackers often attempt to break cryptosystems by analysing the correlation information [19,67]. In a cipher image, the correlation coefficient is expected to be close to zero in the horizontal, vertical and diagonal directions to avoid such attacks. The correlation coefficient of adjacent pixels randomness test measures this correlation by Eq. (13) [67].

$$\rho(X,Y) = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y}, \qquad (13)$$

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 expectation value.

Table 4 shows the correlation coefficients for different images. Note that the original images have a high coefficient, indicating that the pixels are strongly correlated, while the encrypted images do not. Results shown in Table 5 are evidenced through Fig. 4. Table 5 compares the coefficients of the Lena image with different works in literature. In spite of the correlation coefficients of our proposed scheme are not the lowest, the calculated values are close to zero.

**Table 4**
Correlation coefficients test for the five benchmark images. We have shown the correlation for each original and encrypted image. The encrypted images exhibit values very close to zero, which is expected for robust encryption schemes.

| Image | | Correlation Coefficient | | |
|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal |
| Lena | Original | 0.93998 | 0.96934 | 0.91793 |
| | Cipher | 0.00405 | 0.00302 | 0.00113 |
| Boat | Original | 0.92066 | 0.93714 | 0.88052 |
| | Cipher | 0.00842 | 0.00187 | 0.00136 |
| House | Original | 0.97807 | 0.96528 | 0.94835 |
| | Cipher | −0.00426 | 0.00561 | −0.00259 |
| Pepper | Original | 0.95223 | 0.95303 | 0.90949 |
| | Cipher | 0.00130 | −0.00159 | 0.00354 |
| Cameraman | Original | 0.93321 | 0.95928 | 0.90764 |
| | Cipher | −0.00089 | −0.00096 | −0.00084 |

**Table 5**
Comparison of correlation coefficients of cipher Lena image. In spite of the correlation coefficients of our proposed scheme are not the lowest, the calculated values are close to 0.

| Correlation coefficient | | | Lena |
|---|---|---|---|
| Horizontal | Vertical | Diagonal | |
| 0.00405 | 0.00302 | 0.00113 | Ours |
| 0.00083 | 0.00223 | 0.00650 | [13] |
| 0.00352 | 0.00649 | 0.00356 | [65] |
| 0.00160 | 0.00250 | 0.00030 | [18] |
| −0.00170 | 0.00130 | −0.00050 | [19] |
| 0.93998 | 0.96934 | 0.91793 | Original |

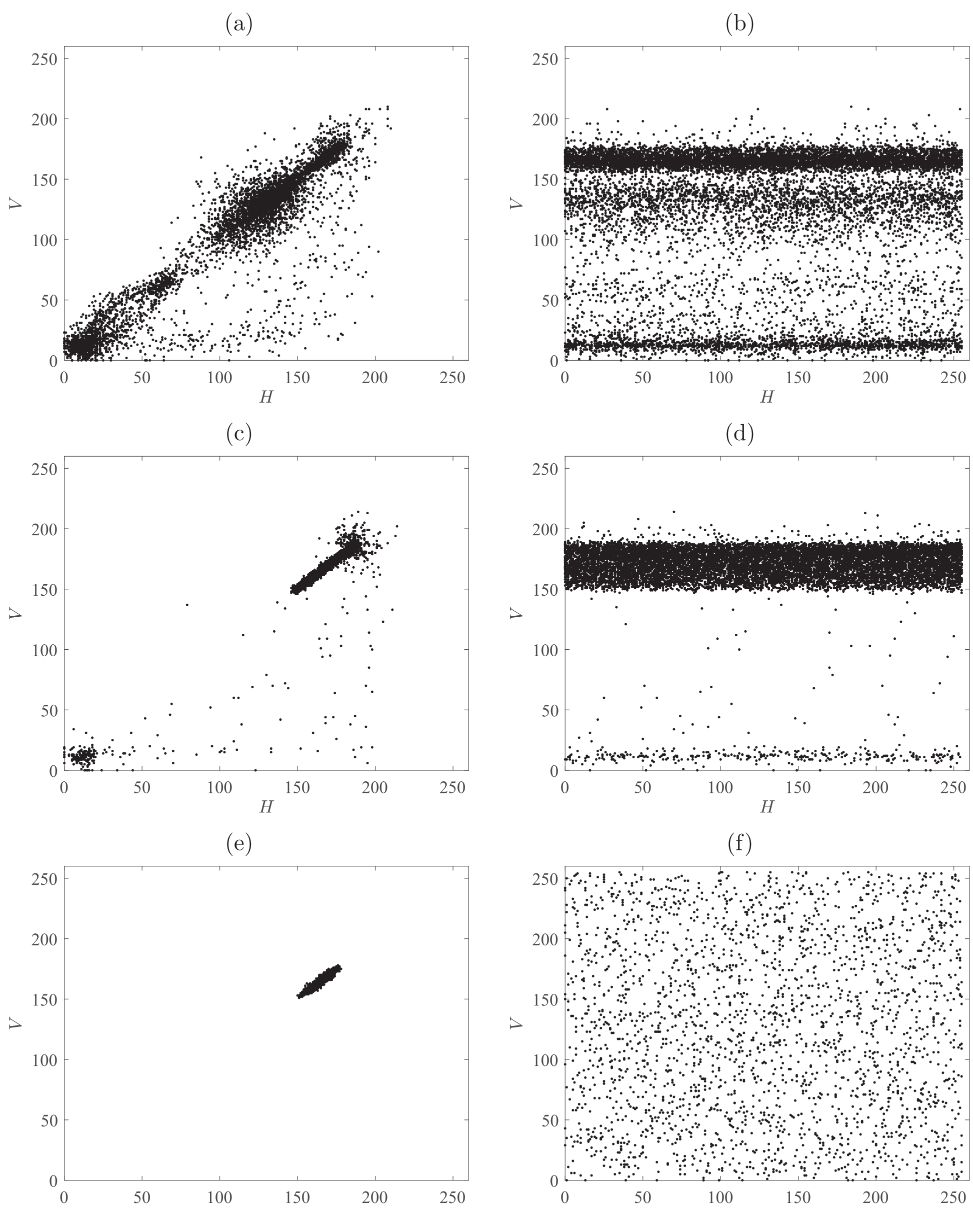


**Fig. 4.** Correlation distribution of two adjacent pixels. The first column is for the plain image, while the second column is for the cipher image. We have shown only an area of $50 \times 50$ pixels. Three types of correlations have been performed: i) (a)-(b): horizontally adjacent pixels with $H = (1:50, 1:49)$ and $V = (1:50, 2:50)$. ii) (c)-(d) vertically adjacent pixels with $H = (1:49, 1:50)$ and $V = (2:50, 1:50)$. iii) (e)-(f) diagonal adjacent pixels with $H = (1:49, 1:49)$ and $V = (2:50, 2:50)$. The axis represents the pixel gray value location. As it is possible to see, the distribution of pixel for the cipher image is well distributed over all range of gray scale. The correlation of the adjacent pixels is very high in plain image. The cipher algorithm decreases the correlation of between adjacent pixels. See more details in [68].

**Table 6**
Information entropy of the Lena's encrypted image for different approaches. The ideal information entropy is 8. The values of entropy for the images boat, house, pepper and cameraman have been calculated as 7.9971, 7.9969, 7.9975 and 7.9969, respectively.

| Entropy | References |
|---|---|
| 7.9968 | Ours |
| 7.9826 | [13] |
| 7.9980 | [65] |
| 7.9998 | [18] |
| 7.9975 | [19] |

**Table 7**
Variances of the histograms in the respective images. The third column shows the percentage of reduction in variance of cipher image compared to the plain image. As a matter of comparison, Namasudra and Deka [72] have reduced the variance of Lena histogram in 99.089%.

| Images | Variance | | |
|---|---|---|---|
| | Plain | Cipher | Reduction (%) |
| Lena | 30697.616 | 290.157 | 99.055 |
| Boat | 99221.152 | 262.596 | 99.735 |
| House | 300964.870 | 276.760 | 99.908 |
| Pepper | 37241.419 | 227.012 | 99.390 |
| Cameraman | 99630.761 | 283.522 | 99.715 |

### 4.5. Information entropy analysis

Shannon's entropy [69] is an approach for measuring randomness in a communication system, defined by Eq. (14) [13],

$$H(X) = \sum_{i=1}^{2^N-1} P_i log_2 \frac{1}{P_i}, \tag{14}$$

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

The theoretical value for entropy measure is $H = log_2(256) = 8$ [70]. As the cipher images originated by PRNG (pseudo-random number generator) are not truly random images, the expected entropy value for the system to be considered secure is $H(X) \approx 8$. The values of entropy for the boat, house, pepper and cameraman images have been calculated as 7.9971, 7.9969, 7.9975 and 7.9969, respectively. These values indicate good randomness properties. Moreover, Table 6 compares the entropy obtained by the encryption of Lena image. Our method presents value very close to 8 and it is very similar to other works in literature. Li et al. [18] present the most approximate value of entropy for Lena cipher image, although the difference is only in the third decimal place. A metadata analysis in three papers [12,19,71] has been performed, and we have collected 50 calculated entropy values. The calculate mean of such sample is 7.992994 and the standard deviation is 0.009166. Therefore, we can be 95% confident that the population mean falls between 7.9905 and 7.9955. It means that our result of 7.9968 is higher than the expected mean entropy calculated in the literature upon this metadata analysis.

### 4.6. Histogram analysis

The histogram of cipher image should be random and uniform. A quantitatively histogram analysis can be performed by Eq. (15) [6,16]:

$$Var(h) = \frac{1}{G_L^2} \sum_{i=0}^{G_L-1} \sum_{j=0}^{G_L-1} \frac{1}{2}(h_i - h_j)^2, \tag{15}$$

where $G_L = 256$ is the gray level and $h$ is the vector of the histogram values. Fig. 5 shows the plain images and the cipher images along with their respective histograms. It is clear that the encryption scheme produces uniform histograms. Table 7 exhibits a significant decrease in the cipher images. In all images, our encryption scheme has reduced the variance of the plain image histograms in more than 99%. As a matter of comparison, Namasudra and Deka [72] have reduced the variance of Lena histogram in 99.089%, while our proposed scheme has obtained a very close value of 99.055%.

### 4.7. Differential analysis

Attackers often try to find common statistical patterns in encrypted images to break the algorithm and identify the original picture [6,12,19]. The number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) are the two most used metrics to evaluate the resistance against these differential attacks [11,15]. The NPCR and UACI scores can be obtained by the following equations Eqs. (16) and (17) [16]:

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

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

where $M$ and $N$ are the length and width, respectively, of the cipher image $C_i$ and $sign()$ is the sign function.

Wu et al.[22] have established scores as random variables and derive their expectations and variances, providing the NPCR critical value and the accepted UACI interval values, for a variety of image sizes. In order to perform the test [6,12,14], the authors firstly encrypted the original plain image. Secondly, one pixel in the original plain image was randomly chosen and its value was modified. With the modified plain image, another cipher image is achieved by encrypting it. Lastly the NPCR and UACI scores can be computed by Eqs. (16) and (17). The results obtained are shown in Table 8. It can be observed that values respect the limits described by Wu et al. [22]. Hence, the algorithm can resist to differential attack. Table 9 compares the NPCR and UACI scores with the values found in other literature.

**Table 8**
Results of NPCR and UACI scores for the proposed cryptosystem. We have considered the following NPCR critical scores: $\mathcal{N}^*_{0.05} = 99.57\%$, $\mathcal{N}^*_{0.01} = 99.55\%$ and $\mathcal{N}^*_{0.001} = 99.53\%$. The UACI critical scores are as follows: $\mathcal{U}^{*-}_{0.05} = 33.28\%$, $\mathcal{U}^{*-}_{0.01} = 33.23\%$, $\mathcal{U}^{*-}_{0.001} = 33.16\%$, $\mathcal{U}^{*+}_{0.05} = 33.64\%$, $\mathcal{U}^{*+}_{0.01} = 33.70\%$ and $\mathcal{U}^{*+}_{0.001} = 33.77\%$. All images are $256 \times 256$ pixels.

| Image | NPCR score (%) | NPCR critical scores (%) | | |
|---|---|---|---|---|
| | | $\mathcal{N}^*_{0.05}$ | $\mathcal{N}^*_{0.01}$ | $\mathcal{N}^*_{0.001}$ |
| Lena | 99.57% | Pass | Pass | Pass |
| Boat | 99.59% | Pass | Pass | Pass |
| House | 99.57% | Pass | Pass | Pass |
| Pepper | 99.60% | Pass | Pass | Pass |
| Cameraman | 99.58% | Pass | Pass | Pass |
| | UACI score (%) | UACI critical scores | | |
| | | $\mathcal{U}^{*-}_{0.05}$ $\mathcal{U}^{*+}_{0.05}$ | $\mathcal{U}^{*-}_{0.01}$ $\mathcal{U}^{*+}_{0.01}$ | $\mathcal{U}^{*-}_{0.001}$ $\mathcal{U}^{*+}_{0.001}$ |
| Lena | 33.41% | Pass | Pass | Pass |
| Boat | 33.44% | Pass | Pass | Pass |
| House | 33.55% | Pass | Pass | Pass |
| Pepper | 33.40% | Pass | Pass | Pass |
| Cameraman | 33.30% | Pass | Pass | Pass |

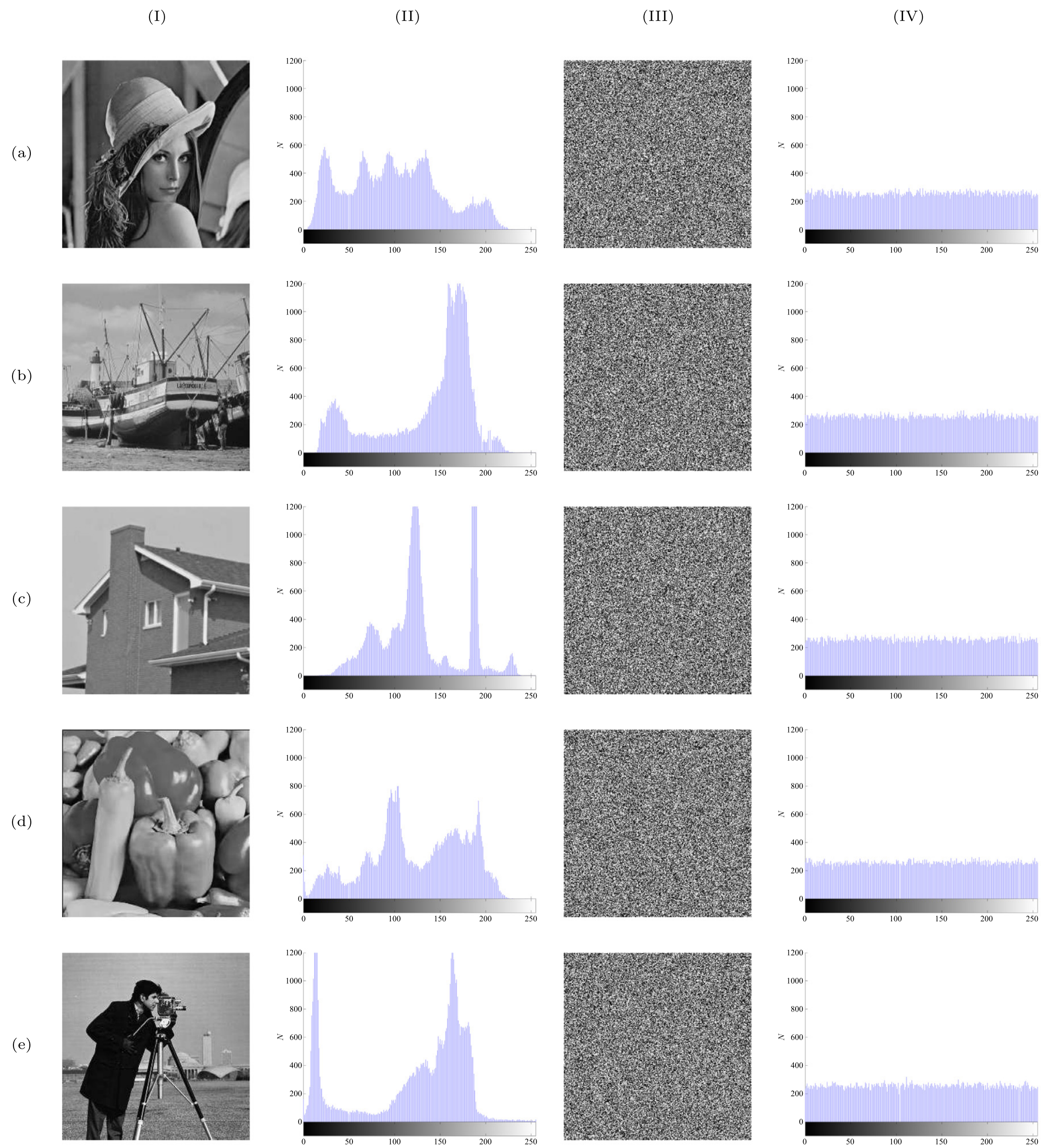


**Fig. 5.** This set of figures show histogram for five different images before and after application of our encryption scheme. The columns are following described: (I) plain image; (II) histogram of the plain images; (III) cipher image; (IV) histogram of the cipher image. Each line represents a different image as follows: (a) Lena; (b); boat; (c) house; (d) pepper; (e) cameraman. All images are given in grayscale with size 256 × 256. Although the plain image exhibits a high presence of particular shading gray values, the proposed scheme converts the plain image to a noise-like image, with uniform distribution of pixel.

**Table 9**
NPCR and UACI values for the Lena's image. The results are very similar with those found by Diaconu [65] and Hu et al. [19].

| NPCR score | UACI score | References |
|---|---|---|
| 99.57% | 33.41% | Ours |
| 99.57% | 33.48% | [65] |
| 99.61% | 33.46% | [19] |

### 4.8. Resistance to known and chosen-plaintext attacks

Known and chosen-plaintext attacks are very often attacks to cryptosystems [14]. In the known-plaintext attacks, a hacker knows a string of both cipher and plain images [13]. On the other hand, in the chosen-plaintext attacks, the hacker encrypts a chosen plaintext seeking for further information that compromises the cryptosystem. In our proposed encryption scheme, one of the keys is obtained from the plain image (see Eq. (7)), which is an additional protection against attacks. Furthermore, commonly used black and white images [6,11] have been encrypted and no useful information in the cipher images has appeared. This fact has been confirmed by the indexes shown in Table 10.

### 4.9. Noise attack

The cryptographic method must be robust to noise disturbance [2,6,14]. We have performed such attack as follows [6]. A white


**Fig. 6.** Noised encrypted images and decrypted images. In the first row, five cipher images have been perturbed with white Gaussian noise. In all cases the mean is zero. The variance has been different in each case with the values 0.00001 (A), 0.0001 (B), 0.001 (C), 0.01 (D) and 0.1 (E). The second row (F-J) shows the decrypted images, respectively. Most of information has been properly restored.

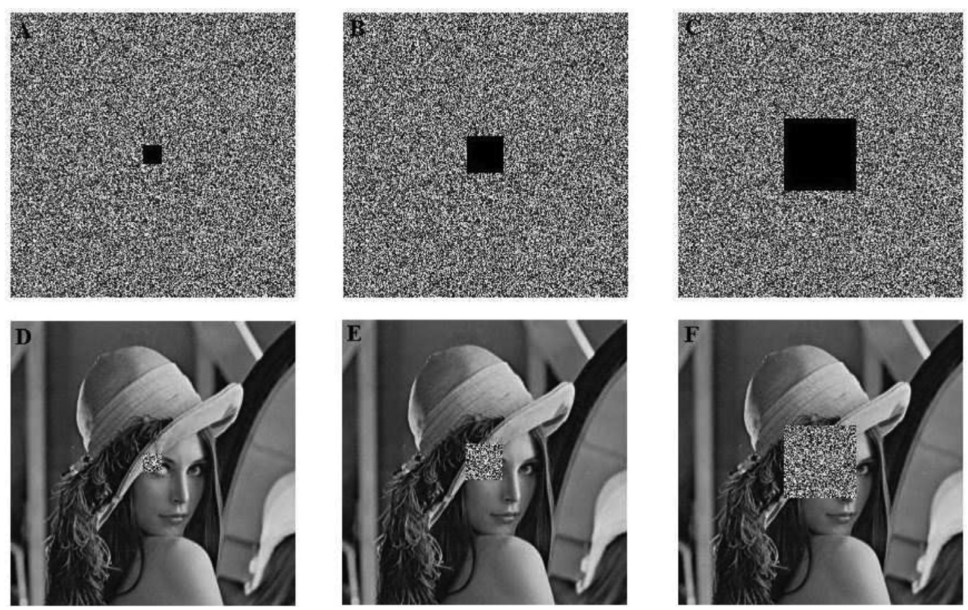


**Fig. 7.** Cropping attack in the cipher images A-C. The decrypted images D-F show that the approach is resistance to information loss.

**Table 10**
Results of four tests applied on totally white and black images. These results indicate that the method is resistant to chosen-plaintext attacks as suggested by Wu et al. [14].

| Test | | Images ($512 \times 512$) | |
|---|---|---|---|
| | | White | Black |
| Entropy | | 7.9977 | 7.9975 |
| Corr. coef. | Horizontal | −0.00161 | −0.00091 |
| | Diagonal | −0.00066 | −0.00043 |
| | Vertical | 0.00040 | −0.00177 |
| Histogram | Variance - Plain | $2.68 \times 10^8$ | $2.64 \times 10^8$ |
| | Variance - Cipher | $3.24 \times 10^3$ | $3.56 \times 10^3$ |
| Diff. anal. | NPCR score | 99.62% | 99.59% |
| | UACI score | 33.44% | 33.52% |

Gaussian noise with mean equal to zero and variance within 0.00001 to 0.1, has been introduced to the image. Fig. 6(A)–(E) show the noised encrypted images and Fig. 6(F)–(J) show decrypted images, respectively. It can be concluded that most of the information in the original image can be restored and the encryption scheme is resistant to noise disturbance. As a matter of comparison, the authors in [6,73] have used noise with variance equal to 0.0001 and 0.0025, respectively. While our results have shown good quality visual decrypted images with a significant higher variance equal to 0.1.

### *4.10. Information loss*

An effective cryptosystem must consider information loss [2,6]. Fig. 7 shows block removal in cipher images with pixel-size of $16 \times 16$, $32 \times 32$ and $64 \times 64$. The decrypted plain images continue to be meaningful. Hence, our method is robust against to this kind of attack.

### *4.11. Time and algorithm complexity analysis*

In addition to being resistant to various attacks, the algorithm must encrypt and decrypt an image efficiently [12]. In order to analyse the computational complexity of the cryptosystem, the authors counted the mathematical operations in the encryption scheme, as done in [12] and [19]. Table 11 shows the summary of the basic operations used throughout the encryption scheme. For an image of size $n \times n$, the total number of operations is $78n^2 + 75tr + 32$, which furnishes a computational complexity of $O(n^2)$, the same as obtained by Norouzi and Mirzakuchaki [12].

**Table 11**
Summary of computational complexity. We have analysed the basic operations used throughout the encryption scheme. $n$ stands for the dimension of the image and $tr$ is the transient time for the chaotic system. Our proposed method has the computational complexity of $O(n^2)$, which is the same in [12].

| Operations | Encryption process |
|---|---|
| Sum/Subtraction | $32n^2+30tr+3$ |
| Multiplication/Division | $37n^2+37tr+14$ |
| Power | 15 |
| Absolute | $5n^2+5tr$ |
| Logarithm | $n^2+tr$ |
| Module | $n^2+tr$ |
| Uint8 | $n^2+tr$ |
| bit-wise XOR | $n^2$ |
| Summation of operators | $78n^2+75tr+32$ |

## 5. Conclusion

We have designed a novel image encryption scheme using finite-precision error. This design makes contact with earlier works obtained by us [47–51]. Instead of attempting to mitigate the degradation effects of finite precision in chaotic digital systems, we have used natural interval extensions to exploit computer error as a source of randomness. Initial conditions of the Chua's circuit and a factor based on the image to be ciphered have been employed to generate the keystream. The generated sequence successfully passed the NIST test suite SP800-22 and we concluded that our pseudo-random sequence has sufficient randomness to be used in encryption. The bit XOR operation along with the keystream have been used to encrypt the image.

The proposed approach proved to be efficient, producing a pseudo-random sequence with overwhelming cryptographic properties and encrypting the test picture set pictures. Additionally, the simulation results have shown the algorithm to be at least as efficient as other methods presented in literature. We illustrated the resistant of proposed technique to a set of well-known cyberattacks.

This investigation therefore indicates a cost-effective source of randomness to increase the use of chaotic systems in encryption schemes. Most notably, this is the first study to our knowledge to investigate the computer error in encryption schemes. Our results provide convincing evidence of such endeavour. However, the complexity analysis has shown our proposed scheme with no lower time consumption than other similar works. In a high demanding real-time application, future work should devote some effort to apply more efficient chaotic system. Such effort may be avoid the degradation of chaos in computers, such as the case shown by Cao et al. [24], and improve of the method's performance through the reduction of encryption time. We also plan to develop an embedded system based on our technique. Recent work on a minimal digital chaotic system [74] has certainly established a way to turn the method proposed here even more efficient.

## Acknowledgements

Erivelton. G. Nepomuceno was supported by Brazilian Research Agencies: CNPq/INERGE, CNPq (grant no. 425509/2018-4), FAPEMIG (grant no. APQ-00870-17). The authors would like to give a special thanks to Arthur Mendes Lima.

## References

[1] Liu L, Lin J, Miao S, Liu B. A double perturbation method for reducing dynamical degradation of the digital baker map. Int J Bifurcation Chaos 2017;27(07):1750103.
[2] Ullah A, Jamal SS, Shah T. A novel scheme for image encryption using substitution box and chaotic system. Nonlinear Dyn 2018;91(1):359–70.
[3] Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based s-box. Chaos Solitons Fractals 2017;95:92–101.
[4] Terzi DS, Terzi R, Sagiroglu S. A survey on security and privacy issues in big data. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE; 2015. p. 202–7.
[5] Wu Y. Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 2012;21(1):013014.
[6] Gan Z-H, Chai X-L, Han D-J, Chen Y-R. A chaotic image encryption algorithm based on 3-D bit-plane permutation. Neural Comput Appl 2018;28(01):1850010.
[7] Herring C, Palmore JI. Random number generators are chaotic. ACM SIGPLAN Notices 1989;24(11):76–9.
[8] Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia 1989;13(1):29–42.
[9] Chai X. An image encryption algorithm based on bit level brownian motion and new chaotic systems. Multimed Tools Appl 2017;76(1):1159–75.
[10] Wang X, Zhao J, Liu H. A new image encryption algorithm based on chaos. Opt Commun 2012;285(5):562–6.
[11] Zhu H, Zhang X, Yu H, Zhao C, Zhu Z, Zhu H, et al. An image encryption algorithm based on compound homogeneous hyper-chaotic system. Nonlinear Dyn 2017;89:61–79.
[12] Norouzi B, Mirzakuchaki S. A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dyn 2014;78(2):995–1015.
[13] Luo Y, Du M, Liu J. A symmetrical image encryption scheme in wavelet and time domain. Commun Nonlinear Sci Numer Simul 2015;20(2):447–60.
[14] Wu X, Wang K, Wang X, Kan H. Lossless chaotic color image cryptosystem based on dna encryption and entropy. Nonlinear Dyn 2017;90(2):855–75.
[15] Xing-Yuan W, Qian W. A fast image encryption algorithm based on only blocks in cipher text. Chin Phys B 2014;23(3):030503.
[16] Zhang Y. The Image Encryption Algorithm with Plaintext-related Shuffling. In: IETE Technical Review, 33. India: Institution of Electronics and Telecommunication Engineers; 2016. p. 310–22.
[17] Su Z, Zhang G, Jiang J. Multimedia security: a survey of chaos-based encryption technology. In: Multimedia-A Multidisciplinary Approach to Complex Issues. InTech; 2012. p. 99–124.
[18] Li C, Luo G, Qin K, Li C. An image encryption scheme based on chaotic tent map. Nonlinear Dyn 2017;87:127–33.
[19] Hu T, Liu Y, Gong L-H, Ouyang C-J, Hu T, Liu Y, et al. An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dyn 2017;87:51–66.
[20] Kuiate GF, Rajagopal K, Kingni ST, Tamba VK, Jafari S. Autonomous van der pol–duffing snap oscillator: analysis, synchronization and applications to real-time image encryption. Int J Dyn Control 2017;6(3):1008–22.
[21] Özkaynak F. Brief review on application of nonlinear dynamics in image encryption. Nonlinear Dyn 2018;92(2):305–13.
[22] Wu Y, Member S, Noonan JP, Member L. NPCR And UACI randomness tests for image encryption. Cyber J: Multidiscip J Sci Technol, J Sel Areas Telecommun (JSAT) 2011;2011:31–8.
[23] Li S, Chen G, Mou X. On the dynamical degradation of digital piecewise linear chaotic maps. Int J Bifurcation Chaos 2005;15(10):3119–51.
[24] Cao L, Luo Y, Qiu S, Liu J. A perturbation method to the tent map based on lyapunov exponent and its application. Chin Phys B 2015;24(10):1–8.
[25] Li S, Chen G, Mou X. On the dynamical degradation of digital piecewise linear chaotic maps. Int J Bifurcation Chaos 2005;15(10):3119–51.
[26] Amigó JM, Kocarev L, Szczepanski J. Discrete lyapunov exponent and resistance to differential cryptanalysis. IEEE Trans Circuits Syst II 2007;54(10):882–6.
[27] Li C-Y, Chen Y-H, Chang T-Y, Deng L-Y, To K. Period extension and randomness enhancement using high-Throughput reseeding-Mixing PRNG. IEEE Trans VLSI Syst 2012;20(2):385–9.
[28] Li C, Liu Y, Zhang LY, Chen MZQ. Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation. Int J Bifurcation Chaos 2013;23(04):1350075.
[29] Azzaz MS, Tanougast C, Sadoudi S, Fellah R, Dandache A. A new auto-switched chaotic system and its FPGA implementation. Commun Nonlinear Sci Numer Simul 2013;18(7):1792–804.
[30] Liu L, Hu H, Deng Y. An analoguedigital mixed method for solving the dynamical degradation of digital chaotic systems. IMA J Math Control Inf 2014;32(4):dnu015.
[31] Bakhache B, Ghazal JM, Assad SE. Improvement of the security of zigbee by a new chaotic algorithm. IEEE Syst J 2014;8(4):1024–33.
[32] Hu H, Deng Y, Liu L. Counteracting the dynamical degradation of digital chaos via hybrid control. Commun Nonlinear Sci Numer Simul 2014;19(6):1970–84.
[33] Liu J, Zhang H, Song D. The property of chaotic orbits with lower positions of numerical solutions in the logistic map. Entropy 2014;16(11):5618–32.
[34] Öztürk I, Kiliç R. Cycle lengths and correlation properties of finite precision chaotic maps. Int J Bifurcation Chaos 2014;24(09):1450107.
[35] Li C, Xie T, Liu Q, Cheng G. Cryptanalyzing image encryption using chaotic logistic map. Nonlinear Dyn 2014;78(2):1545–51.
[36] Min L, Yang X, Chen G, Wang D. Some polynomial chaotic maps without equilibria and an application to image encryption with avalanche effects. Int J Bifurcation Chaos 2015;25(9):1–18.
[37] Deng Y, Hu H, Xiong W, Xiong NN, Liu L. Analysis and design of digital chaotic systems with desirable performance via feedback control. IEEE Trans Syst Man Cybern Syst 2015;45(8):1187–200.

[38] Öztürk I, Klç R. A novel method for producing pseudo random numbers from differential equation-based chaotic systems. Nonlinear Dyn 2015;80(3):1147–57.
[39] Wang Q-X, Yu S-M, Guyeux C, Bahi J, Fang X-L. Study on a new chaotic bitwise dynamical system and its FPGA implementation. Chin Phys B 2015;24(6):060503.
[40] Deng Y, Hu H, Liu L. Feedback control of digital chaotic systems with application to pseudorandom number generator. Int J Modern Phys C 2015;26(02):1550022.
[41] Deng Y, Hu H, Xiong N, Xiong W, Liu L. A general hybrid model for chaos robust synchronization and degradation reduction. Inf Sci 2015;305:146–64.
[42] Sayed WS, Radwan AG, Rezk AA, Fahmy HAH. Finite precision logistic map between computational efficiency and accuracy with encryption applications. Complexity 2017;2017:1–21.
[43] Liu L, Miao S. Delay-introducing method to improve the dynamical degradation of a digital chaotic map. Inf Sci 2017;396:1–13.
[44] Yan-Bin Z, Qun D. A New Digital Chaotic Sequence Generator Based on Logistic Map. In: 2011 Second International Conference on Innovations in Bio-inspired Computing and Applications. IEEE; 2011. p. 175–8.
[45] Lozi R. Can we trust in numerical computations of chaotic solutions of dynamical systems? Topol Dyn Chaos 2013:63–98.
[46] Galias Z. The dangers of rounding errors for simulations and analysis of nonlinear circuits and systems - and how to avoid them. IEEE Circuits Syst Mag 2013;13(3):35–52.
[47] Nepomuceno EG, Martins SAM. A lower bound error for free-run simulation of the polynomial NARMAX. Syst Sci Contr Eng 2016;4(1):50–8.
[48] Nepomuceno EG, Martins SAM, Amaral GFV, Riveret R. On the lower bound error for discrete maps using associative property. Syst Sci Contr Eng 2017;5(1):462–73.
[49] Mendes EMAM, Nepomuceno EG. A very simple method to calculate the (positive) largest Lyapunov exponent using interval extensions. Int J Bifurcation Chaos Appl Sci Eng 2016;26(13):1650226.
[50] Nepomuceno EG, Mendes EM. On the analysis of pseudo-orbits of continuous chaotic nonlinear systems simulated using discretization schemes in a digital computer. Chaos Solitons Fractals 2017;95:21–32.
[51] Nepomuceno EG, Martins SAM, Lacerda MJ, Mendes EMAM. On the use of interval extensions to estimate the largest lyapunov exponent from chaotic data. Math Probl Eng 2018;2018:1–8.
[52] Peixoto ML, Nepomuceno EG, Martins SA, Lacerda MJ. Computation of the largest positive lyapunov exponent using rounding mode and recursive least square algorithm. Chaos Solitons Fractals 2018;112:36–43.
[53] Zhou S, Wang X, Wang Z, Zhang C. A novel method based on the pseudo-orbits to calculate the largest lyapunov exponent from chaotic equations. Chaos Interdiscip J Nonlinear Sci 2019;29(3):033125.
[54] Chua LO, Wu CW, Huang A, Zhong G-Q. A universal circuit for studying and generating chaos. i. routes to chaos. IEEE Trans Circuits Syst I 1993;40(10):732–44.
[55] Aguirre LA. Introdução à identificação de sistemas -Técnicas lineares e não lineares aplicadas a sistemas: Teoria e Aplicação. UFMG; 2015. ISBN 9788542300796. In Portuguese.
[56] Kapitaniak T. Chaos for Engineers. Berlin, Heidelberg: Springer Berlin Heidelberg; 2000.
[57] Bassham LE, Rukhin AL, Soto J, Nechvatal JR, Smid ME, Barker EB, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications Tech. Rep. National Institute of Standards and Technology; 2010. doi:10.6028/nist.sp.800-22r1a.
[58] Elmanfaloty RA, Abou-Bakr E. Random property enhancement of a 1D chaotic PRNG with finite precision implementation. Chaos Solitons Fractals 2019;118:134–44.
[59] Gong-bin Q, Qing-feng J, Shui-sheng Q. A new image encryption scheme based on des algorithm and Chua's circuit. In: Imaging Systems and Techniques, 2009. IST'09. IEEE International Workshop on. IEEE; 2009. p. 168–72.
[60] Peng G, Min F. Multistability analysis, circuit implementations and application in image encryption of a novel memristive chaotic circuit. Nonlinear Dyn 2017;90(3):1607–25.
[61] Moore RE, Kearfott RB, Cloud MJ. Introduction to Interval Analysis, 110. Siam; 2009.
[62] Moore RE. Methods and Applications of Interval Analysis, 2. Siam; 1979.
[63] Nepomuceno EG, Martins SA, Silva BC, Amaral GF, Perc M. Detecting unreliable computer simulations of recursive functions with interval extensions. Appl Math Comput 2018;329:408–19.
[64] Fung WW, Golin MJ, Gray JW. Protection of keys against modification attack. In: Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on. IEEE; 2001. p. 26–36.
[65] Diaconu AV. Circular inter-intra pixels bit-level permutation and chaos-based image encryption. Inf Sci 2016;355–356:314–27.
[66] Institute of Electrical and Electronics Engineers (IEEE). 754-2008 – IEEE standard for floating-point arithmetic. IEEE; 2008. P. 1–58
[67] Dianocu A-V, Dascalescu AC. Correlation distribution of adjacent pixels randomness test for image encryption. Proc Romanian Acad, Series A 2017;18:351–60.
[68] Jangid RK, Mohmmad N, Didel A, Taterh S. Hybrid approach of image encryption using DNA cryptography and TF Hill Cipher Algorithm. In: 2014 International Conference on Communication and Signal Processing. IEEE; 2014. p. 934–8.
[69] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949;28(4):656–715.
[70] Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan JP, Natarajan P. Local shannon entropy measure with statistical tests for image randomness. Inf Sci 2013;222:323–42.
[71] Zhou Y, Bao L, Chen CP. A new 1D chaotic system for image encryption. Signal Process 2014;97:172–82.
[72] Namasudra S, Deka G. Advances of DNA Computing in Cryptography. CRC Press; 2018.
[73] Li H, Wang Y. Double-image encryption based on iterative gyrator transform. Opt Commun 2008;281(23):5745–9.
[74] Nepomuceno EG, Lima AM, Arias-García J, Perc M, Repnik R. Minimal digital chaotic system. Chaos Solitons Fractals 2019;120:62–6.