Information diffusion in images through encryption with Jerk chaotic systems

Alejandro Bucio-Gutiérrez[*], Eduardo S. Tututi and Ulises Uriostegui Legorreta

Facultad de Ciencias Físico-Matemáticas, Universidad Michoacana de San Nicolás de Hidalgo, Morelia, Mich., México.

Abstract

In the ongoing work a Jerk-type Duffing system with a sixth-order damped potential is applied into an image encryption algorithm, due to the sensitivity and non-periodicity of the response of system under different initial conditions. In most cases, image encryption generally consists of three main stages. First, the pseudorandom generation of the encryption key. Second, the shuffling of the image pixels. Third, the intensity of the pixel values is changed in a pseudorandom manner (diffusion). The proposed encryption algorithm based on diffusion, relies on a deterministic and chaotic Jerk-type dynamical system, whose purpose is to generate pseudo-random data used to modify the pixel intensity values. The image is encrypted only through the diffusion process, considering a known key generated by the user. To verify the reliability of the encryption process, the statistical properties of the plain image are compared with the encrypted image, taking as reference the statistical properties corresponding to an image with uniform distribution. The comparison is made by evaluating the correlation between adjacent pixels of each of the images and the Shannon information entropy, which quantifies information content or randomness in the image by measuring the uncertainty in pixel values, a high entropy indicates a complex image with diverse pixel values and low entropy indicates a uniform, simple image. It is found that the Jerk chaotic system optimally hides the image information by obtaining a high information entropy.

Keywords— Jerk system, Image encryption, Shannon information entropy, Correlation

1 Introduction

Chaos theory has been a topic of great interest in recent years due to complex behavior. Characterized by sensitivity to initial conditions, unpredictability, and deterministic evolution, chaotic dynamics has been extensively investigated and applied in diverse fields such as control and synchronization [1, 2], or, in our particular interest, secure communications [3]. In cryptography, these properties are particularly valuable, as chaotic systems can be employed to generate pseudorandom sequences and to design secure algorithms for image encryption and data protection.

Visual data, such as videos and digital images, are the most popular communication methods for transmitting information, giving rise to the need of encrypting this content to ensure information. Visual data, specifically digital images, are mainly characterized by a strong correlation among adjacent pixels; hence special attention is required when encrypting such data.

Recently, chaos has been applied to encryption schemes which consist of three processes: *i*) Selecting the encryption key that provides the values necessary for the encryption scheme. *ii*) Applying a confusion process (pixel shuffling) to conceal image patterns, and *iii*) applying diffusion over the pixels, which reduces image redundancy by spreading it throughout the entire encrypted image [4, 5, 6].

On the other hand, statistical properties of encrypted images reveal the viability of encryption schemes based on the histograms of images. It is possible to obtain statistical values of the distribution function of the pixels, such as the expected value, variance, or correlation [7].

Shannon information entropy is one of the most important functions in information theory, especially relevant for image encryption. It measures the average amount of information contained in the image or, equivalently, the amount of uncertainty removed upon revealing the contents of the image [8].

A basic method for image encryption via diffusion of intensity of the pixels with a Jerk system is presented in this work. This method could complement and give robustness the existing encryption methods. The encryption key for the diffusion process is provided by the user. More important, a logarithm function is applied to the key for obtaining initial conditions for the Jerk dynamical system, whose numerical solution is used for the diffusion of the

[*] Corresponding author: alejandro.bucio@umich.mx

Received: September 24, 2025, **Published:** December 29, 2025

pixels of the plain image. As a result, the encryption scheme proposed is expected to supply a secure algorithm for encryption of images.

The remainder of this paper is organized as follows. In Section 2, the proposed image encryption algorithm is described, as well as statistical theory used. Section 3 details the results of simulations and statistical analyses. Some remarks are drawn in Section 4 to conclude this paper.

2 Methodology

This section contains the proposed diffusion algorithm to encrypt an image and the statistical theory used to the interpretation of the numeric results. The suggested encryption algorithm via diffusion process consists of two simple steps:

1. In the first step, a password given by the user is operated to generate initial conditions to the Jerk System which is solved for a certain time. The use of a user key as input into the chaotic Jerk system increases the unpredictability of the encryption process, as the key directly influences the initial conditions to which the chaotic system is highly sensitive; a small change leads to significantly different trajectories.
2. In this step, the solution of the Jerk system is modulated in the same interval as the color space. Making XOR operation, bit to bit, in the pixels of the plain image and modulated by a pseudorandom sequence obtained from Jerk system. This process results in a cipher image where the statistical distribution of pixel values is significantly modified, thus enhancing security by ensuring diffusion and sensitivity to initial conditions.

The decryption process follows the same above methodology by using the same password (key) and the encrypted image instead the original plain image.

2.1 Algorithm

Certain types of deterministic dynamical systems exhibit behaviors that are highly sensitive to initial conditions and are characterized by the presence of strange attractors. In particular, nonlinear Jerk type systems, which in general can be expressed in the form $\dddot{x} = f\left(x, \dot{x}, \ddot{x}\right)$, with f a non-linear function, which has this property. The combination of strong sensitivity, determinism under precisely defined initial conditions and a non periodic solution, makes these systems suitable for the generation of pseudorandom numbers, which can be employed for the diffusion of pixel intensities in an image.

A Jerk equation, previously studied for its non-periodic and chaotic properties, is used to encrypt images [9]

$$\dddot{x} = c_1\ddot{x} + c_5 c_2\dot{x} - c_5 e^{-ax^2}\frac{d}{dx}\phi(x), \tag{1}$$

which can be transformed into the Jerk system

$$\begin{aligned} \dot{x} &= y, && (2)\\ \dot{y} &= c_5 z, && (3)\\ \dot{z} &= c_1 z + c_2 y + e^{-ax^2}\frac{d}{dx}\phi(x), && (4) \end{aligned}$$

where $\phi(x)$ is a triple well Duffing potential giving by

$$\phi(x) = \frac{x^2}{2} + c_3\frac{x^4}{4} + c_4\frac{x^6}{6}. \tag{5}$$

We choose the parameters as: $c_1 = -0.67$, $c_2 = -0.7$, $c_3 = -0.6$, $c_4 = 0.06$, $c_5 = 3.55$ and $\alpha = 0.01$, to generate chaotic dynamics with a strange attractor in the phase space.

An image encryption algorithm consists of three steps, namely: the generation of the encryption key, pixel shuffling, and changing intensity of the pixel values (diffusion). In this work, the first step involves an encryption key C giving by the user, which is nine characters long (consisting of numbers, uppercase and lowercase letters). The encryption key is splitted into three parts and operated as

$$x_i(0) = \frac{1}{\log\left((122)^3)\right)}\log\left(\prod_{j=3(i-1)+1}^{3i} c_j\right), \quad i = 1,2,3, \tag{6}$$

where $x_1(0) \equiv x(0)$, $x_2(0) \equiv y(0)$, $x_3(0) \equiv z(0)$ are the initial conditions at $t = 0$, of the system (i is also used as a label for the RGB colors), c_j ($j = 1, 2, \ldots, 9$) is the j-th alphanumeric character of the encryption key in ASCII decimal form and the term 122^3 results from dividing the key into three segments, where 122 denotes the highest alphanumeric ASCII value. This ensures that the initial conditions of the Jerk system are sufficiently different between keys of the same length, generating different responses from the dynamic system. For initialize diffusion process, the Jerk system is evolved via Runge-Kutta method until a value $t = M + N$ with time interval step

$$\Delta t = \frac{M+N}{100 + M \times N}, \tag{7}$$

being M and N integers. This guarantees a chaotic signal from the dynamic system of the same size as the number of pixels in the image.

We consider a plain image with $M \times N$ pixels in the RGB space color where $I^i(m,n)$ is the value of the intensity for the pixel at the position (m,n), with $m = 1,\ 2,\ \cdots,\ M$ and $n = 1,\ 2,\ \cdots,\ N$ in the color channel $i = 1 \equiv$ Red, $i = 2 \equiv$ Green, and $i = 3 \equiv$ Blue, that can be expressed by an index $k = (n-1)M + m$ where $k = 1, 2, ...M \times N$, that is $I^i(k) \in \left[0, 2^8 - 1\right]$ is the intensity for the k-th pixel. Thus, the value of $I^i(k)$ is operated according to the evolution of Equation (4) by considering the function for each color that will be used for the encryption process:

$$\xi^i(k) = \text{mod}\left(\left\lfloor \text{mod}\left(\left\lfloor 10^{15} \cdot \text{abs}(x_i(t = (100+k)\Delta t))\right\rfloor, 10^8\right)\right\rfloor, 2^8\right), \tag{8}$$

where $\lfloor \cdot \rfloor$ denotes the floor operation, which gives the value rounded to the immediately lowest integer, mod the modular operation and $k = 1,\ 2,\ \cdots,\ M \times N$.

In this way, the Equation (8) represents a pseudorandom sequence of numbers, each one by taking enough significant digits of $x_i(t = (100+k)\Delta t)$ and constraining the result to a possible color scale value from 0 to 255. Notice that $\xi^i(k)$ is analogous to the function σ^b of the Equation (10) in Reference [10] used for obtaining the encryption key at time $t = 0$, except that in our case the initial time begins at $t = 100\Delta t$, which avoids nearly equal solutions for times short enough.

Finally, the operation XOR bit to bit

$$E^i(k) = \text{bitXOR}(\xi^i(k), I^i(k)), \tag{9}$$

is performed to obtain obtaining the encrypted image with pixel intensity values $E^i(k)$ by combining the pseudorandom signal produced by the Jerk system with the image data modifying significantly statistical distribution of pixel values.

The decryption process uses the inverse operation to recover the original image

$$I^i(k) = \text{bitXOR}(\xi^i(k), E^i(k)). \tag{10}$$

2.2 Statistical Analysis

The statistical features of the image are usually used to verify the robustness of an image encryption scheme due to the fact that an image with some specific statistical values reveals its similarity with the case of an image with a uniform distribution in the color intensity of their pixels. This is because an image can be characterized by the distribution of its pixel intensities. The statistical analysis of this distribution allows us to compare the pixel intensity distribution of the image encrypted by the proposed algorithm with that of an image with a completely uniform pixel distribution, which exhibits characteristic statistical values for highly disordered images, as discussed later in this section.

The statistical analysis is carried out using the expected value μ, the standard deviation of the distribution of intensities, σ, and Shannon information entropy, H, given by

$$\begin{aligned} \mu(I^i) &= \sum_{j=0}^{2^8-1} I^i_j p_j, && (11) \\ \sigma\left(I^i\right) &= +\sqrt{\sum_{j=0}^{2^8-1} \left(I^i_j - \mu(I^i)\right)^2 p_j}, && (12) \\ H(I^i) &= -\sum_{j=0}^{2^8-1} p_j \log_2\left(p_j\right) \text{ (bits)}, && (13) \end{aligned}$$

respectively, where I^i is the event refer to intensity of the pixels in one of the RGB channels of the image, with possible values $I^i_j = 0, 1, \cdots, 255$, $p_j \equiv p\left(I^i_j\right)$ is the probability of I^i_j for the j-th possible value of the intensity of the pixels in the image in terms of the number of pixels with the same intensity value which are obtaining with the histogram of the image. Shannon information reflects the randomness and uncertainty of the image information. The encrypted image for a good encryption technique must have high randomness and the ideal value of entropy information is 8 on each channel.

Another statistical property of interest is the covariance between certain set of pairs of intensities of pixels. Usually these pairs of intensities are selected randomly [11, 12]. For the purpose of comparing the relationship between pixels and their neighborhoods before and after the encryption process, we take a set of intensities I^i for the pixels with index $k = (n-1)M + m$ with $m = 2, 3, \cdots, M-1$ and $n = 2, 3, \cdots, N-1$, and a set of intensities for its corresponding adjacent pixel I^i_{adj} which can be the set of the intensities for the vertical pixel with index $k = (n-1)M + m + 1$ or the set of intensities for the horizontal pixel $k = n \times M + m$ or the intensities for the diagonal pixel with index $k = n \times M + m + 1$. For any adjacent set selected the covariance is

$$\operatorname{cov}\left(I^i, I^i_{\text{adj}}\right) = \sum_{j=0}^{2^8-1}\sum_{l=0}^{2^8-1}\left(I^i_j - \mu(I^i)\right)\left(I^i_{\text{adj},l} - \mu(I^i_{\text{adj}})\right) p_{jl}, \tag{14}$$

being $p_{jl} \equiv p\left(I^i_j, I^i_{\text{adj},l}\right)$ the joint probability, i.e. , the probability that $I^i_j = j \in [0, 1, .., 255]$, and $I^i_{\text{adj},l} \ = l \in \ [0, 1, .., 255]$ occurs. Let us now introduce the covariance normalization

$$\gamma\left(I^i, I^i_{\text{adj}}\right) = \frac{\operatorname{cov}\left(I^i, I^i_{\text{adj}}\right)}{\sigma\left(I^i\right)\sigma\left(I^i_{\text{adj}}\right)}, \tag{15}$$

or simply correlation which is defined in the interval $-1 \leq \gamma\left(I^i, I^i_{\text{adj}}\right) \leq 1$. In the plain image, the correlation between adjacent pixels is high, so the encrypted images should have a correlation close to zero, that is an indication of randomness.

For example, in the case of a gray image, a pixel can take 256 different possible values. The Shannon information entropy for an image with a uniform intensity distribution for pixels takes a value of $H = log_2(256) = 8$. For the case of a bitorial image (with 2 tones), the Shannon information entropy is $H = 1$ [3]. In general, an image with uniform pixel distribution where each pixel can take 256 different possible values has statistical values shown in Table **??**. Images with similar statistical properties also exhibit a comparable intensity distribution. In this context, if the results obtained from encrypting an image approximate the values in Table 1, is indicative of a uniform intensity distribution. Furthermore, if the correlation between pairs of adjacent pixels is null, the analyzed images will exhibit a disordered position distribution of pixels with random intensities.

Table 1: Statistical values for an image with uniform intensity distribution.

Statist	value
H	8
μ	127.5
σ^2	5461.25
σ	73.9003

3 Results

An encryption algorithm should transform an image into another with uniform distribution pixel via an encryption key. The decryption process must recover all the original information of the original image if the correct key is given. To show the viability of the proposed algorithm we consider the image Mandrill.tiff (see Figure 1 (a)) as plain image with size 512 × 512 (262144 pixels) which is taken from the USC-SIPI[1] image database. First, we obtain the histogram of the image which reveals its statistical properties. These statistical values are obtaining using Equations (11)-(13). Firstly, the statistical values of the Mandrill image are obtained and displayed in Table 2 and Figures 1 (a)-(e).

[1] https://sipi.usc.edu/database/

Table 2: Statistical values for the original Mandrill image.

Statistical value	Channel R	Channel G	Channel B
H	7.7067	7.4744	7.7522
μ	137.3913	128.8588	113.1171
σ^2	3080.178	2282.0289	3806.7598
σ	55.4994	47.7706	61.6989
γ_v	0.86635	0.76554	0.88105
γ_h	0.92278	0.86453	0.90717
γ_d	0.85475	0.73532	0.84019

In Figure 1 (b) shows the distribution of the intensity of the pixels of the plain image. The various statistical values are calculated by using the intensity distribution for each color channel of the plain image with a entropy value per channel close to 7.6444, while the results obtained from the proposed algorithm, shown in Figures 1 (f)–(j), yield entropy values of approximately 7.9993 per channel. This demonstrates the high degree of complexity of the encrypted image and its similarity to the statistical properties of an image with a uniform distribution of pixel intensities. This comparison will be discussed below. Notice that Figures 1 (c)-(e) illustrate the approximate linear dispersion between adjacent pixels. Losing this linear behavior implies that the pixels do not form contours, such as those required to distinguish the Mandrill in the plain image. This is precisely the case in the encrypted image shown in Figure 1 (g), where no contours are visible, thus safeguarding the information of the composition of Mandrill.

To test the correlations of the adjacent pixels in the encrypted images by the proposed algorithm, we take 99.2203% of the pixels and its adjacent pixels (260100 pairs of pixels) along the horizontal direction γ_h , vertical direction γ_v and diagonal direction γ_d in both the plain image and its encrypted image, their correlation can be calculated using the Equation (15).

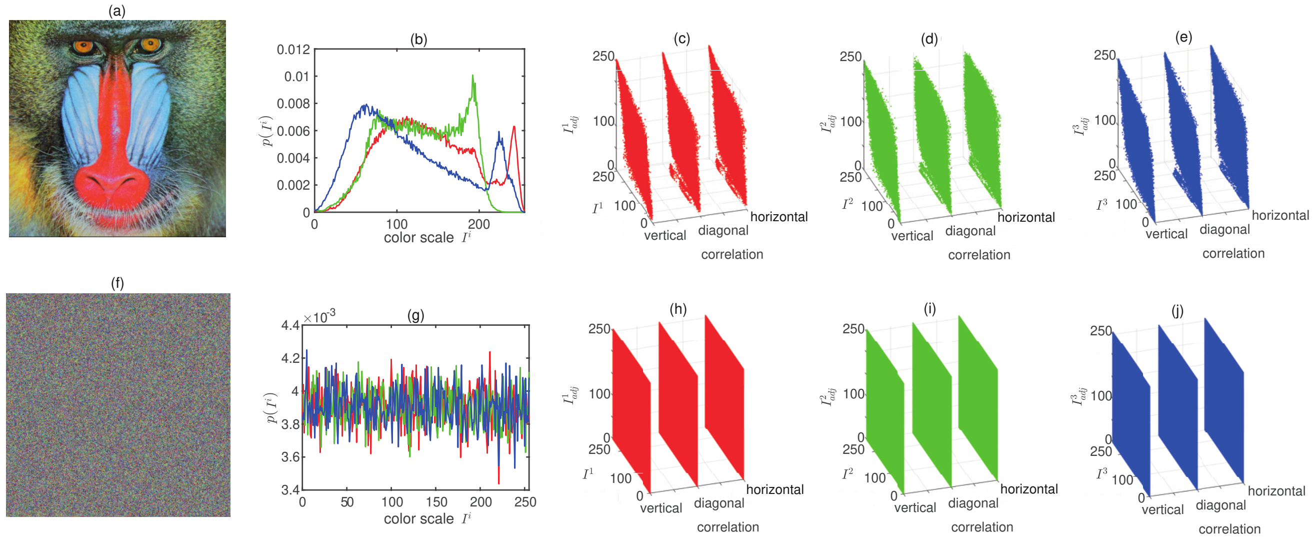

Figure 1: Plain image (up) and encrypted image (down). Pixel distribution of the images (second column). Correlations of two adjacent pixels vertical, horizontal and diagonal for red channel, green channel and blue channel, respectively.

Since the choice of the key provided by user, significantly changes the signal generated by the Jerk system, we consider a set of different keys with small variations. In first instance, applying the proposed encryption algorithm, a simply given password $C = 000000000$ generates a signal via Jerk system which gives the image shown in Figure 1 (f). The resulting distributions of intensities are uniform as it is shown in Figure 1 (g).

Comparing Figures 1 (c)-(e) with the corresponding Figures 1 (h)-(j), a decrease of the correlation can be appreciated, becoming the former figures uncorrelated between pairs of pixels. The statistical values of the encrypted image are shown in Table 3 which reveals its similarity with the statistical values of an image with a uniform intensity distribution. Nevertheless, that is one possible password. The Equation (6) of our encryption method can generate $c = (230764)^3$ different initial conditions for the Jerk system, which is still significantly lower than the minimum value required to withstand brute-force statistical attacks of 2^{100} [13]. However, it allows users to choose their own password. We take a small set of passwords and examine their implication in the encrypted images. The set is composed by 13843 different passwords that are used to encrypt the Mandrill image. Each password is identified by a label identification (ID) integer number from 1 to 13843, being some of them 000000000, 000000001,..., 0000001*nd*, etc.

Table 3: Statistical values for the Mandrill encrypted image.

Statistical value	Channel R	Channel G	Channel B
H	7.9993	7.9994	7.9993
μ	127.3313	127.2	127.3495
σ^2	5454.9853	5455.2485	5458.7516
σ	73.8579	73.8597	73.8834
γ_v	-0.00033335	-0.0026641	0.0012049
γ_h	0.0014461	-0.0015142	0.0026526
γ_d	0.0011214	-0.0018175	-0.00087718

For a more detailed statistical analysis, Figure 2 shows the statistical values of each encrypted image for every password in its 3 color channels: red, green, and blue. These results can be compared with the statistical values of an image with uniform pixel distribution shown in Table 1. Particularly, for sets of different initial conditions given by a set of passwords, Figure 2 (a), the Shannon information entropy of the encrypted image is shown in Figure 2 (b), obtaining values closer to 8, which means the similarity with a uniform distribution. Additionally, Figure 2 (f) to (h) show the correlation between vertical, horizontal and diagonal adjacent pixels for the pixels taken with values closer to 0, which means that they are uncorrelated.

Additionally, Table 4 lists the Shannon information entropy values of the encrypted Mandrill image compared to other encryption algorithms [14, 15]. The results in Table 4 show that the entropy value of our proposed algorithm falls within a range with an average fluctuation close to 8. Compared to other encryption schemes, our algorithm achieves results that the Shannon information entropy in a considerable number of cases are closer to 8. This, combined with the low correlation obtained between pairs of adjacent pixels under different keys, results in the encrypted image resembling one with randomly distributed pixels. Consequently,the encrypted pixels do not reveal any information about the original image, where some passwords have better encryption, due to the similarity of its statistical properties to those of a completely random image, as shown in Figure 2.

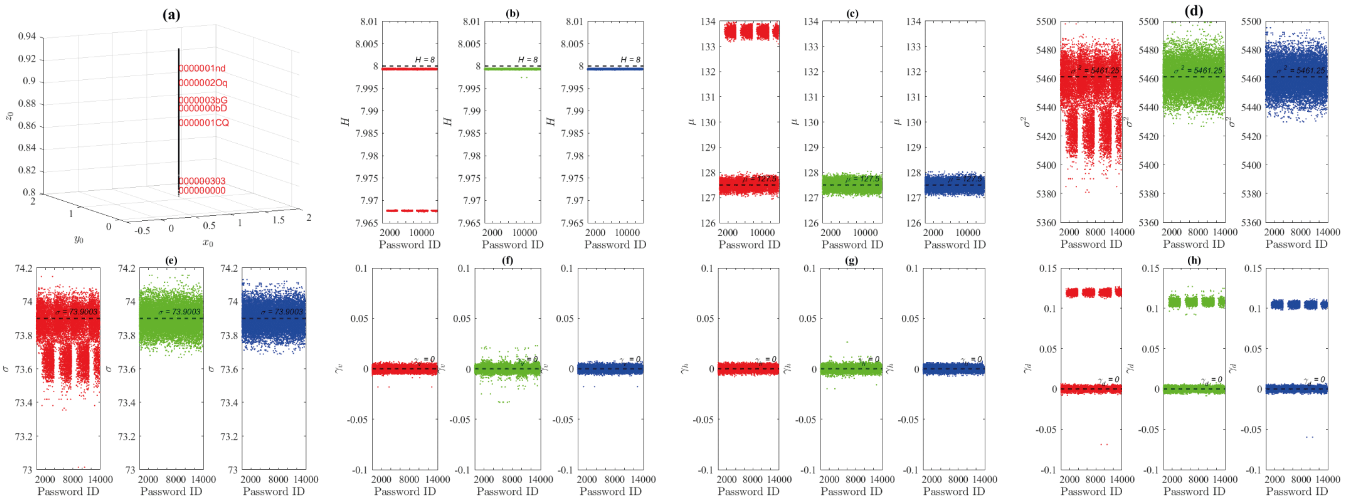

Figure 2: Statistical values for a set of different passwords used to image encryption. Initial conditions used in the Jerk system (a). Shannon information entropy (b), expected value (c), variance (d), standard deviation (e), vertical correlation (f), horizontal correlation (g) and diagonal correlation (h) for the Password ID.

Table 4: Shannon information entropy comparison different algorithms.

	Shannon information entropy		
Image	Channel R	Channel G	Channel B
Original Mandrill image	7.7066718	7.4744316	7.7522172
Ours encrypted image	$[7.9673910, 7.9994935]$	$[7.9974087, 7.9995007]$	$[7.9576495, 7.999529]$
Reference [14]	7.9993	7.9992	7.9994
Reference [15]	7.9992557	7.9993472	7.9993356

4 Discussion

In this work the Duffing type Jerk system with exponential damping was used to generate a signal with pseudorandom values whose initial condition depends on a password given by the user. This signal is used in an encryption algorithm without shuffle process. Applying the encryption algorithm for the collected key, the encrypted image is obtained. An analysis of the statistical properties is performed for different keys, in particular 000000000, and then another 13843 different passwords. It was found that passwords generate distinct signals in the dynamical system, resulting in different encrypted images whose statistical properties, such as Shannon information entropy H, exhibit behavior similar to that of an image with a uniform pixel distribution. This leads, in particular, to a Shannon information entropy value closer to 8 in each RGB color channel compared to other algorithms. We can state that the encryption algorithm generates an image that hides the original information via the Jerk system, which can be completely recovered.

Acknowledgments

This work was supported by Universidad Michoacana de San Nicolás de Hidalgo (UMSNH), Coordinación de la Investigación Científica (CIC-UMSNH) and Consejo Nacional de Humanidades Ciencias y Tecnologías (CONAHCYT).

Statements and Declarations

The authors declare that there is no conflict of interest regarding the publication of this paper and that they have no relevant financial or non-financial interests to disclose.

References

[1] U. Uriostegui-Legorreta and E.S. Tututi-Hernández. “Master-slave synchronization in the Rayleigh and Duffing oscillators via elastic and dissipative couplings”. In: *Revista de ciencias tecnológicas* 5.1 (2022), e214.

[2] U. Uriostegui-Legorreta and E.S. Tututi-Hernández. “Master-slave synchronization in the van der Pol and Duffing systems via elastic, dissipative and a combination of both couplings”. In: *Journal of Applied Research and Technology* 21.2 (2023), pp. 227–240.

[3] L. Moysis et al. “A Chaos Based Pseudo-Random Bit Generator Using Multiple Digits Comparison”. In: *Chaos Theory and Applications* 2.2 (2020), pp. 58–68.

[4] Z. T. Njitacke et al. “Circuit and microcontroller validation of the extreme multistable dynamics of a memristive Jerk system: application to image encryption”. In: *The European Physical Journal Plus* 137.5 (2022), p. 619.

[5] D. S. Laiphrakpam et al. “Encrypting Multiple Images With an Enhanced Chaotic Map”. In: *IEEE Access* 10 (2022), pp. 87844–87859.

[6] M. Yan, J. Jie, and P. Zhang. “Chaotic systems with variable indexs for image encryption application”. In: *Scientific Reports* 12.1 (2022), p. 19585.

[7] R.C. Gonzalez, R.E. Woods, and S.L. Eddins. *Digital Image Processing Using MATLAB*. Pearson Education, 2004.

[8] R.W. Yeung. *A First Course in Information Theory*. Information Technology: Transmission, Processing and Storage. Springer New York, NY, 2002.

[9] A. Bucio-Gutiérrez, E.S. Tututi-Hernández, and U. Uriostegui-Legorreta. "Analysis of the Dynamics of a ϕ^6 Duffing Type Jerk System". In: *Chaos Theory and Applications* 6.2 (2024), pp. 83–89.

[10] V.R. Folifack Signing et al. "Chaotic Jerk System with Hump Structure for Text and Image Encryption Using DNA Coding". In: *Circuits, Systems, and Signal Processing* 40.9 (2021), pp. 4370–4406.

[11] L. Moysis et al. "Application of a Hyperbolic Tangent Chaotic Map to Random Bit Generation and Image Encryption". In: *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*. 2021, pp. 559–565.

[12] M. Farajallah, S. El Assad, and O. Deforges. "Fast and Secure Chaos-Based Cryptosystem for Images". In: *International Journal of Bifurcation and Chaos* 26.02 (2016), p. 1650021.

[13] G. Alvarez and S. Li. "Some basic cryptographic requeriments for chaos-based cryptosystems". In: *International Journal of Bifurcation and Chaos* 16.08 (2006), pp. 2129–2151.

[14] G. Cheng, C. Wang, and H. Chen. "A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture". In: *International Journal of Bifurcation and Chaos* 29.09 (2019), p. 1950115.

[15] Y. He et al. "A new image encryption algorithm based on the OF-LSTMS and chaotic sequences". In: *Scientific Reports* 11.1 (2021), p. 6398.