symmetry

MDPI

Article

New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography

Marcin Lawnik [1,*] **and Marek Berezowski** [2]

[1] Department of Mathematics Applications and Methods for Artificial Intelligence, Faculty of Applied Mathematics, Silesian University of Technology, Kaszubska 23, 44-100 Gliwice, Poland

[2] Faculty of Chemical Engineering and Technology, Cracow University of Technology, ul. Warszawska 24, 30-155 Kraków, Poland; marek.berezowski@pk.edu.pl

* Correspondence: marcin.lawnik@polsl.pl

Abstract: One of the applications of dynamical systems with chaotic behavior is data encryption. Chaos-based cryptography uses chaotic dynamical systems as the basis for creating algorithms. The present article discusses a new dynamical system called M-map with its analysis: fixed points, bifurcation diagram, Lyapunov exponent, and invariant density. The obtained bifurcation diagram and the plot of the Lyapunov exponent (with a minimum value of $\ln 2$ and a maximum value of $\ln 4$) suggest that the so-called robust chaos characterizes this map. Moreover, the obtained results are compared with other dynamical systems used in cryptography. Additionally, the article proposes a new image encryption algorithm. It uses, among others, cyclically shifted S-box or saving encrypted pixels on the first or last free space in the cipher-image. The conducted analysis shows that the cipher-images are characterized by an entropy value close to 8, a correlation of adjacent pixels value close to 0, or values of Number of Pixel of Change Rate ($NPCR$) and Unified Average Changing Intensity ($UACI$) measures close to 100% and 33%, respectively.

Keywords: discrete dynamical system; logistic map; tent map; sine map; chaos; Lyapunov exponent; image encryption

check for updates

Citation: Lawnik, M.; Berezowski, M. New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography. *Symmetry* **2022**, *14*, 895. https://doi.org/10.3390/sym14050895

Academic Editors: Alexander Zaslavski and Christos Volos

Received: 26 March 2022
Accepted: 25 April 2022
Published: 27 April 2022

1. Introduction

Dynamical systems with chaotic behavior describe many physical phenomena. Their particular application is cryptography based on the chaos theory, which uses these types of recurrences to keep data secure [1–3]. This is possible due to the properties of chaotic maps, such as random-like behavior and sensitivity to changing initial conditions and, at the same time, the deterministic method of obtaining successive states. In chaotic cryptography, the values of the initial conditions and parameters are treated as secret keys.

The vast majority of scientific publications in the area of using chaos in cryptography focus on defining new algorithms that will be used to keep data secure based on the selected chaotic system. Many of these algorithms turn out to be ineffective or even dangerous [4–9]. On the other hand, sparse works have focused on dynamical systems, which are a significant part of the encryption process. Of course, new systems appear in the works mentioned above; however, they are often treated as additions to the algorithms.

Chaotic cryptography requires a dynamical system that is appropriate from its point of view. Such a system should be characterized, among others, by a large range of values of initial conditions and parameters for which chaos can be observed. In addition, the distribution of the iterated variable of such systems should be flat to make it impossible to perform statistical analysis.

In the professional literature, multi-dimensional chaotic dynamical systems, such as the Lorentz system [10,11], Henon map [12], discrete memristor hyperchaotic maps [13], two-dimensional sine logistic modulation map [14], or memristive Rulkov neuron model [15], have been used in chaotic cryptography. The use of such mappings increases the number of calculations to obtain the next state of the system, which results directly from their complicated structure [16]. For this reason, one-dimensional mappings of the following form are often used for encryption:

$$x_{k+1} = f(x_k), \tag{1}$$

where $f : [0,1] \rightarrow [0,1]$ is a given function.

Chaotic cryptography uses only chaotic systems. Therefore, it is necessary to determine whether the given system meets this condition. One of the measures determining whether the mapping of the form (1) generates chaotic orbits is the Lyapunov exponent defined by the formula

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln|f'(x_i)|. \tag{2}$$

The value of the Lyapunov exponent determines whether the obtained orbit is stable ($\lambda \leq 0$) or whether the trajectories starting from close initial conditions diverge after some time ($\lambda > 0$). It should be emphasized that condition $\lambda > 0$ is only a necessary condition for chaos to occur. Another valuable feature of dynamical systems is the so-called invariant density, which from a practical point of view is the distribution of the iterated variable, which can be obtained by solving the Frobenius–Perron [17,18] equation. Both the Lyapunov exponent value and the invariant density are normally obtained numerically.

Examples of systems (1) that are commonly used in recent years in chaotic cryptography are the logistic map [1,19–29], (skew or asymmetric) tent map [19,21,25,27,30–32], or sinus map [19,25,28,33]. However, from a cryptographic point of view, the mentioned mappings have properties not entirely suitable for use in such applications [34]. This is evidenced by, for example, the logistic map, which is the most frequently used dynamic system in the professional literature. For this reason, this article presents a new dynamical system characterized by chaotic behavior. Its properties are much better than in the case of the mappings mentioned above. In addition, this article analyzes, among other things, the Lyapunov exponent and the potential applications for data encryption of the presented system.

The main contributions and novelty of this article are (i) the development of a new dynamic system that can be used in chaotic cryptography, (ii) the presentation of a new image encryption algorithm, and (iii) the development of a simple S-box algorithm which is part of the encryption process.

This article is structured in the following order—the first part, the Introduction, outlines the topics. In Section 2, some mappings often used in cryptography are shown. Section 3, which is the Model section, shows the M-map equation. Section 4 presents the analysis, which shows inter alia, fixed points, bifurcations, Lyapunov exponent, and the invariant density. Then, in Section 5, a new image encryption algorithm with its analysis is shown. The last sections include the Conclusion and References.

2. One-Dimensional Mapping Used in Cryptography

In chaotic cryptography, one-dimensional mappings are particularly popular. The most frequently used dynamic systems of this type are presented below.

The logistic map is given by the following formula [1,19–29]:

$$x_{k+1} = ax_k(1 - x_k), \tag{3}$$

where $a \in [0,4]$. It is characterized, among others, by chaotic behavior for the value of the parameter $a \in [3.57,4]$ except for the so-called periodic windows. More about its analysis and possible modifications can be found, among others, in [35,36].

Equally often, in scientific publications on chaotic cryptography, the asymmetric tent map is used, which is given by the following formula [19,21,25,27,30–32]:

$$x_{k+1} = \begin{cases} \frac{x_k}{p} & 0 < x_k < p \\ \frac{1-x_k}{1-p} & p \leq x_k < 1 \end{cases}, \tag{4}$$

where $p \in (0, 1)$. This mapping for each value of the p parameter has a chaotic solution with a positive Lyapunov exponent.

Another mapping that is used in chaotic cryptography is the sine map, which can be defined by the following equation [19,25,28,33]:

$$x_{k+1} = a \sin(\pi x_i), \tag{5}$$

where $a \in [0, 1]$. This system has very similar features to the logistic map.

The above list can be enriched with other one-dimensional dynamical systems, such as a Gauss map [37,38]. However, their values are not specified in the $[0, 1]$ interval; therefore, they are not taken into account in the comparative analysis in this article.

3. The M-Map

This article introduces a new model of a one-dimensional chaotic map, which has been named M-map. The recursive equation of the M-map is determined by the following formula:

$$x_{k+1} = f(x_k, p) = \begin{cases} \frac{x_k}{p}\left(2 - \frac{x_k}{p}\right), & 0 \leqslant x \leqslant 0.5 \\ \frac{1-x_k}{p}\left(2 - \frac{1-x_k}{p}\right), & 0.5 < x \leqslant 1 \end{cases}, \tag{6}$$

where $p \in [0.25, 0.5]$.

Figure 1 shows the M-map graphically. This figure shows that this system looks like the letter "M" and, hence, the name of this map: M-map. Moreover, it can be observed that when the p parameter changes from the value of $p = 0.25$ to $p = 0.5$, the form of the map changes from two parabolas to the letter "M" to switch finally to the logistic map for $p = 0.5$. It can also be easily seen that this map is symmetric about the line $x = \frac{1}{2}$.

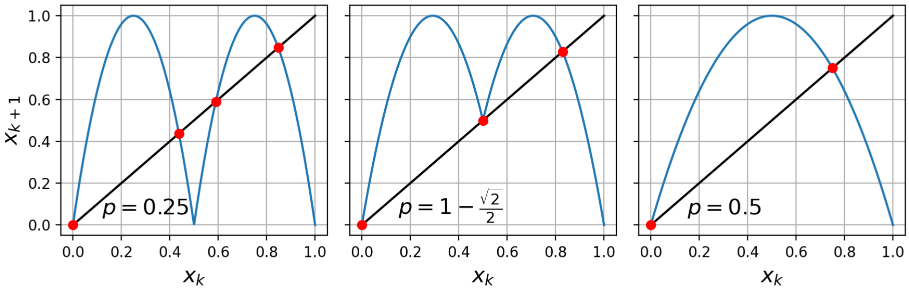


Figure 1. M-map (6) for different p parameter values. Additionally, fixed points are marked in red.

4. Analysis

The analysis of the dynamical system (6) was divided into several subsections. It deals with fixed points, bifurcation diagram, Lyapunov exponent, and invariant density.

4.1. Fixed Points

One of the elements of the analysis of dynamical systems is the determination of their fixed points, i.e., such values x^* for which the following equation holds

$$x^* = f(x^*). \tag{7}$$

In the case of M-map, we distinguish the following cases:

- For $p \in \left[\frac{1}{4}, 1 - \frac{\sqrt{2}}{2}\right)$:
  $x^* \in \left\{0, -p^2 + p, \frac{-p^2-2p+2-\sqrt[3]{p^3(p+4)}}{2}, \frac{-p^2-2p+2+\sqrt[3]{p^3(p+4)}}{2}\right\}$
- For $p = 1 - \frac{\sqrt{2}}{2}$:
  $x^* \in \left\{0, -p^2 + p, \frac{-p^2-2p+2+\sqrt[3]{p^3(p+4)}}{2}\right\}$
- For $p \in \left(1 - \frac{\sqrt{2}}{2}, \frac{1}{2}\right]$:
  $x^* \in \left\{0, \frac{-p^2-2p+2+\sqrt[3]{p^3(p+4)}}{2}\right\}$
  The calculated fixed points are shown in Figure 1.

4.2. Bifurcation Analysis

The bifurcation diagram shows the solutions of the system depending on the value of its parameter. For M-map, the bifurcation diagram of the mapping is shown in Figure 2. It can be read that the M-map has no visible periodic windows, which makes the behavior of the dynamical system in this area chaotic. Moreover, the iteration variable density for the given p parameters is noticeable. The darker area around the values of 0 and 1 means that there is a greater accumulation of the mapping values. Thus, the density of the M-map will have a U-like shape similar to the logistic map density. This observation was confirmed in the analysis of the invariant density in Section 4.4.

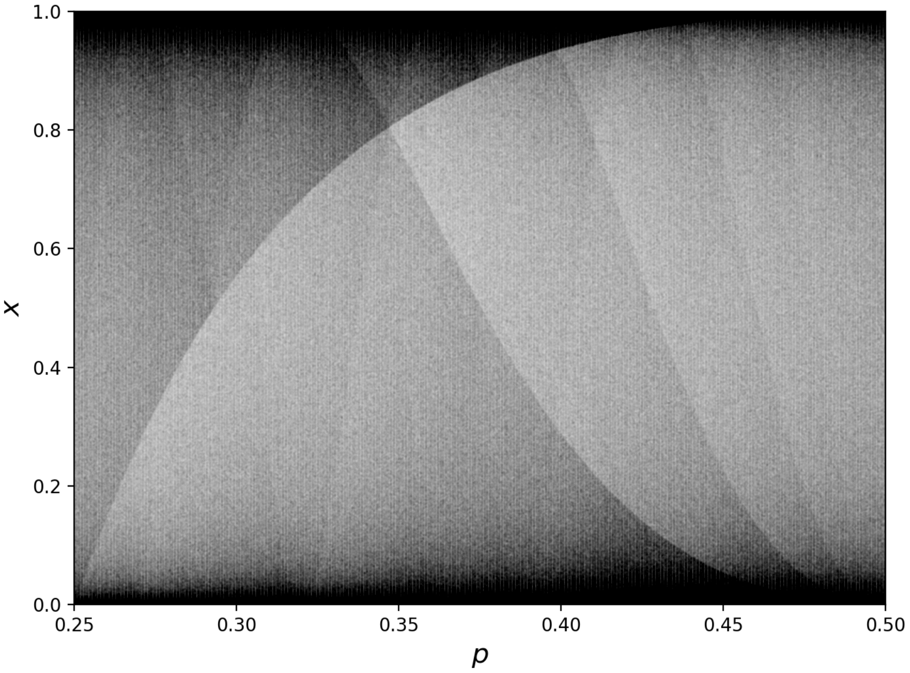


Figure 2. Bifurcation diagram of (6) mapping for different values of p parameter ($\Delta p = 0.000125$).

4.3. Lyapunov Exponent

The Lyapunov exponent is a measure of the chaotic nature of a dynamical system and can be determined using Formula (2). Its positive value is necessary for a dynamic system to behave in a chaotic manner.

For the M-map, its graph is shown in Figure 3. This plot confirms that this mapping does not have the so-called periodic windows. Moreover, the shape of the Lyapunov exponent curve is interesting—it is not fractal. In this case, as in the case of Weierstrass recurrence [39,40], its shape is smooth. This phenomenon occurs in so-called robust chaos [41].

The value of the Lyapunov exponent directly translates into the sensitivity of the dynamical system to changes in the initial condition. The greater the value of the Lyapunov exponent, the faster the trajectories starting from very close initial conditions diverge. This process can be seen in Figure 4.

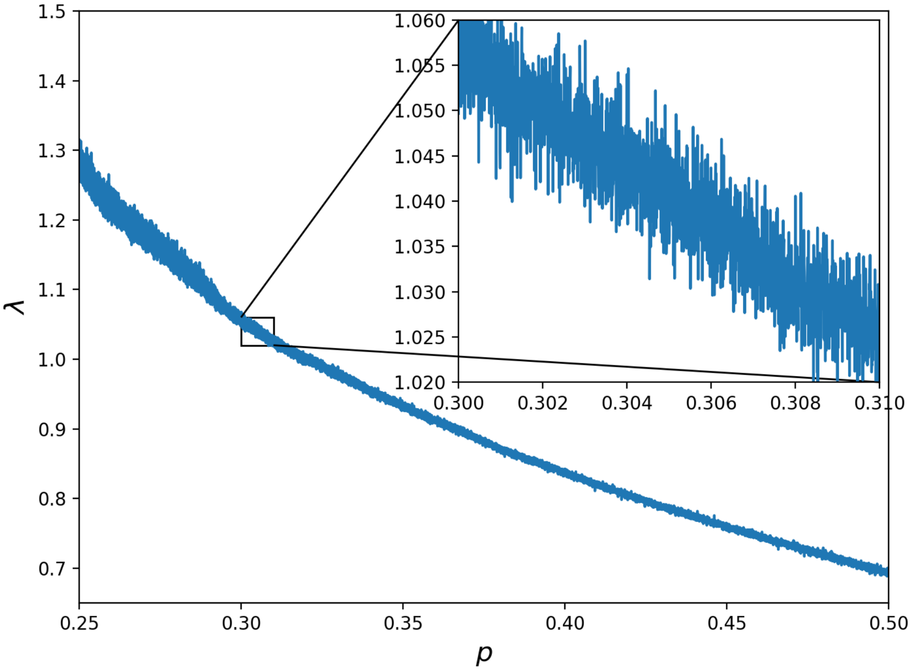


Figure 3. The Lyapunov exponent of (6) for different values of the p parameter ($\Delta p = 0.000005$).

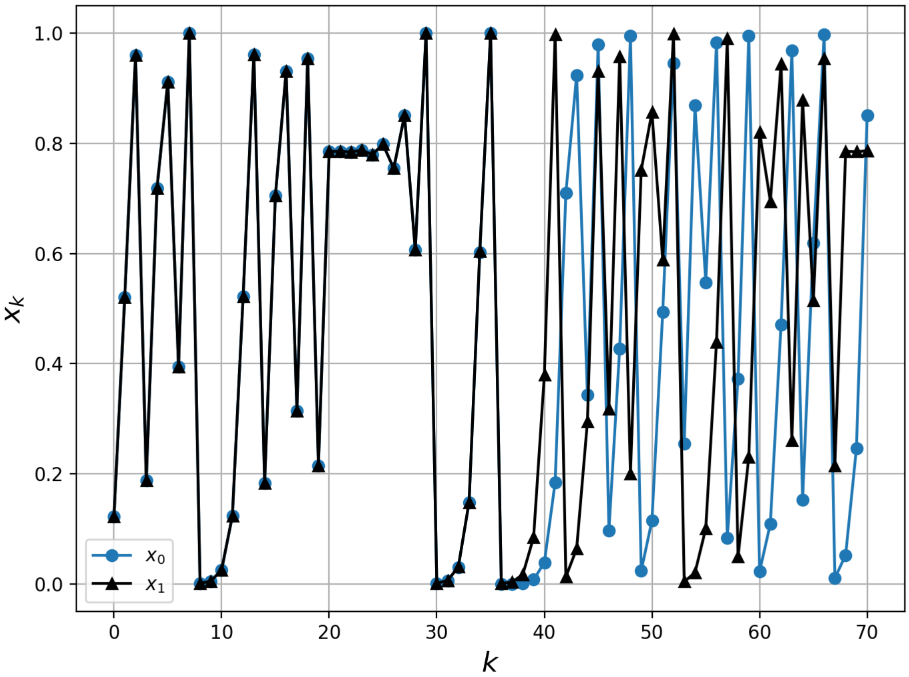


Figure 4. Sensitivity to the change of initial conditions of (6) with $x_0 = 0.123$ and $x_1 = 0.123 + 10^{-15}$.

4.4. Density of the Iterated Variable

Invariant density allows determining the probability distribution of the iterated variable. It can be determined from the Frobenius–Perron [17,18] formula. However, as a rule, determining it in an analytical manner is difficult or even impossible. For this reason, it is approximated numerically using histograms.

Graphs of the numerically obtained densities for the selected p parameter values are shown in Figure 5. The lower right graph shows the invariant density of the logistic mapping for the value of the parameter $a = 4$, which can be determined by the following formula

$$\rho(x) = \frac{1}{\pi\sqrt{x(1-x)}}. \tag{8}$$

The densities for the remaining cases still resemble the "U" shape. However, their shape is not perfectly equal to (8).

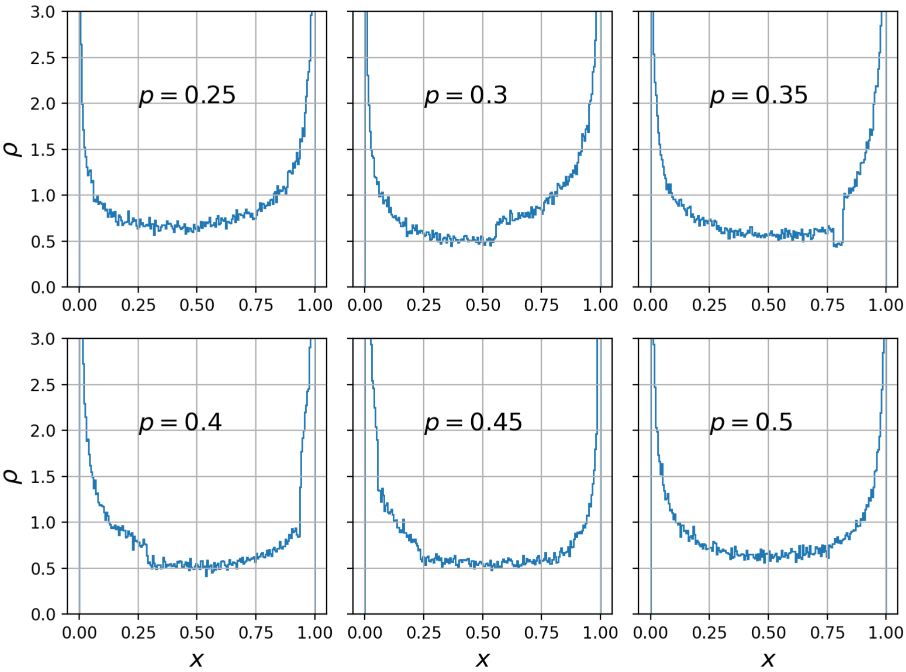


Figure 5. Density of the iterated variable of the M-map for different values of p parameter.

4.5. Comparative Analysis

The dynamic systems used in the construction of cryptographic algorithms must have appropriate properties. These properties include, among others, the largest possible range of parameter values and initial conditions for which chaos occurs. Looking at the graphs of both the bifurcation diagram in Figure 2 or the Lyapunov exponent in Figure 3, it can be seen that the interval in which chaos occurs is within the value of the parameter $p \in [0.25, 0.5]$. At the same time, it is worth emphasizing that there are no periodic windows, which appear in many dynamic systems with chaotic behavior. The analysis also shows that the Lyapunov exponent has a stable value, i.e., its value does not change significantly for values close to the parameter value. Such a situation is also very desirable from the point of view of chaotic cryptography. Moreover, the density of the iterated variable resembles the letter "U" similarly to the logistic mapping (Figure 5). This means that the density of this mapping is flat in the middle and relatively symmetrical and, thus, can be used to generate pseudo-random values.

Table 1 compares the proposed M-map mapping with logistic, skew tent, and sine map. A similar juxtaposition is shown in Figure 6. As criteria, aspects important in chaotic cryptography were selected, i.e., the range of parameter values for chaos, the value of the Lyapunov exponent, and the map density.

Table 1. Comparison of different dynamical systems.

	M-Map	**Logistic Map**	**Tent Map**	**Sine Map**
Chaos	$p \in [0.25, 0.5]$	$a \in [3.57; 4]$	$p \in (0, 1)$	$a \in [0.87, 1]$
Lyapunov exponent	always positive	unstable	always positive	unstable
Density	stable	unstable	uniform	unstable

The range of M-map values for which there is chaos is comparable to the other mappings. However, in the case of the logistic map and sine map in the given ranges, there are the so-called periodic windows. This means that by selecting the parameter value, there is a risk of hitting the periodic window and thus obtaining a periodic solution. This situation is, of course, very undesirable from a cryptographic point of view.

The value of the Lyapunov exponent confirms the range of parameters for which there is chaos. Only M-map and tent map are consistently positive of the four compared mappings. In the case of the tent map, its value can be determined using the following formula

$$\lambda = -p \ln p - (1-p) \ln(1-p). \tag{9}$$

Despite the fact that its value is constantly greater than zero, for values of p close to 0 and 1, its value is close to zero. In such cases, numerically obtained trajectories of the tent map (4) lose their properties (e.g., uniform density) [42]. On the other hand, the Lyapunov exponent for M-maps proceeds from $\ln 2$ for $p = 0.5$ to $\ln 4$ at $p = 0.25$. Additionally, for all mappings that consist of only two arms, the maximum value of the Lyapunov exponent is $\ln 2$. In this respect, the M-map representation has by far the best features.

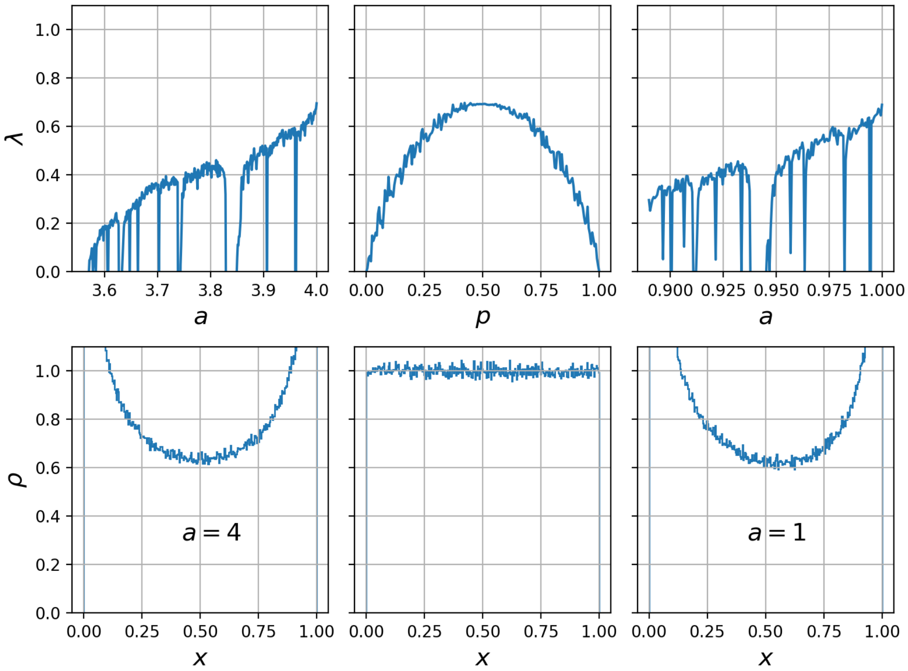


Figure 6. Value of the Lyapunov exponent (**first row**) and density (**second row**) for the logistic, tent, and sine map.

On the other hand, in the case of invariant density, the best mapping for chaotic cryptography is the tent map. The distribution of this mapping is uniform over the entire range of p parameter values. On the other hand, the M-map has a "U" -like density. A similar shape of the density function also has the logistic map but only for the value of the a parameter close to 4, which is given by the Formula (8).

Moreover, it is possible to improve the density of the proposed mapping in such a way that its shape resembles the density with the given Relation (8). This procedure may consist in changing the mapping parameter according to the adopted scheme. It is possible to use, e.g., the following scheme.

$$p_{i+1} = 0.25 + ((p_i + x_i) \mod 0.25) \tag{10}$$

$$x_{i+1} = f(x_i, p_i) \tag{11}$$

The distribution of the mapping obtained as a result of the operation of the above procedure is presented in Figure 7. In this graph, it can be seen that the map density approximates the density (8) better than it does for single parameter values (see Figure 5).

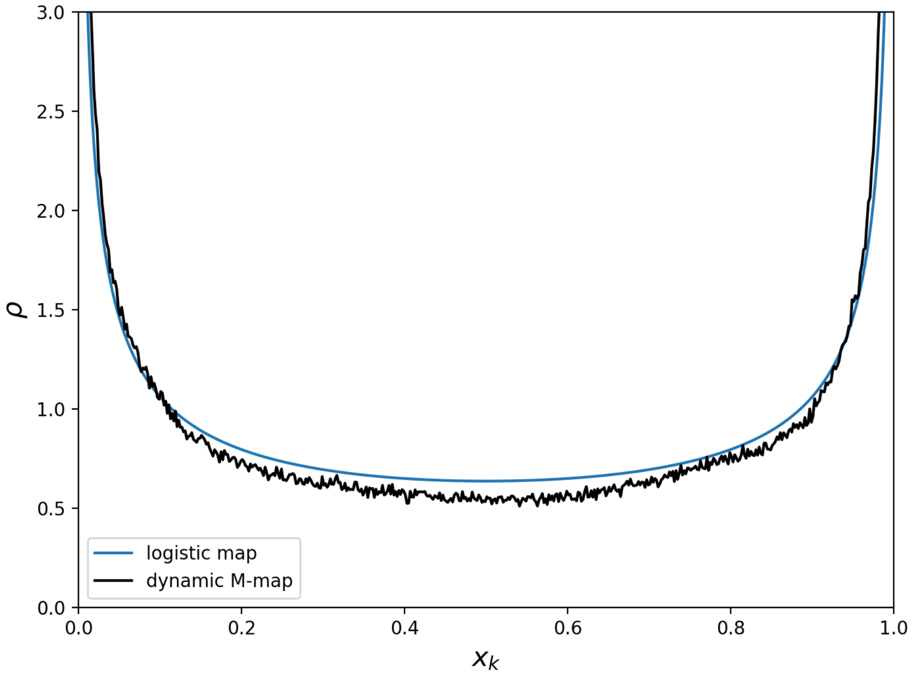


Figure 7. Distribution of an exemplary orbit when changing the value of the p parameter.

The above comparison shows that the M-map can replace the logistic map and other one-dimensional chaotic maps in cryptography applications.

5. Application in Chaos-Based Cryptography

5.1. Simple Image Encryption Algorithm

A simple encryption algorithm was developed to demonstrate the use of the M-map that depicts the image's encryption. This encryption procedure is based on using a dynamic S-box and saving the encrypted pixels in the appropriate place in the cipher-image. The S-box dynamics consist of its dynamic shift for each encrypted pixel. Moreover, successive pixels are stored in the first free position from the beginning or end of the cipher-image. The value of the M-map determines which variant is selected.

5.1.1. Image Encryption Algorithm

The proposed image encryption algorithm operates on pixels in RGB encoding. Hence, it is required that the images be in this format. The next steps are Algorithm 1.

The general scheme of the encryption algorithm is shown in Figure 8.

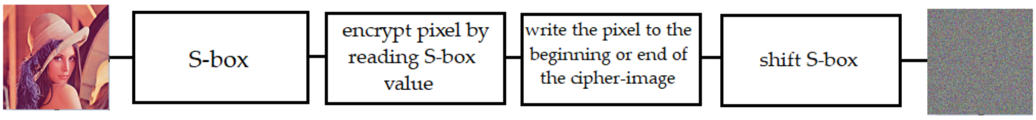

S-box
encrypt pixel by reading S-box value
write the pixel to the beginning or end of the cipher-image
shift S-box

Figure 8. Encryption scheme.

Algorithm 1 Image Encryption Algorithm

```
1. Set the keys: $x$ and $p$;
2. From the set $\{0, 1, \cdots, 255\}$, generate an $S - box$;
3. For every pixel value $px(i, j)$:
   (a) Calculate $x$ from (6) ($x = f(x, p)$);
   (b) Calculate $shift = floor(256 \cdot x)$ and shift the S-box in a cyclic way by the value $shift$;
   (c) Read the $S - box$ value for the pixels RGB components ($S - box(px(i, j))$);
   (d) If $x \leq 0.5$ :
           write value $S - box(px(i, j))$ in the first free place in the cipher-image;
   (e) If $x > 0.5$ :
           write value $S - box(px(i, j))$ in the last free place in the cipher-image.
```

In step 3b of the encryption algorithm, the *shift* value for the S-box shifting is calculated. Examples of such an S-box and its shifted version are shown in Table 2.

Table 2. S-box and shifted S-box by the value of n.

S-Box	Value
original	$100, \cdots, 47, \underbrace{113, \cdots, 7}_{n}$
shifted	$113, \cdots, 7, 100, \cdots, 47$

5.1.2. Decryption Algorithm

Decryption algorithm is shown in Algorithm 2

Algorithm 2 Decryption Algorithm

```
1. Set the keys: $x$ and $p$;
2. From the set $\{0, 1, \cdots, 255\}$ generate an $S - box$;
3. When not all pixels are read:
   (a) Calculate $x$ from (6) ($x = f(x, p)$);
       i.  If $x \leq 0.5$ :
               read the first free pixel $px$;
       ii. If $x > 0.5$ :
               Read the last free pixel $px$;
   (b) Find the $S - box$ indexes for the RGB components of the pixel $px$
   (c) Calculate $shift = floor(256 \cdot x)$ and shift the S-box in a cyclic manner by the value $shift$;
   (d) Write the read indexes in the first free place in the plain-image.
```

The general scheme of the decryption algorithm is shown in Figure 9.

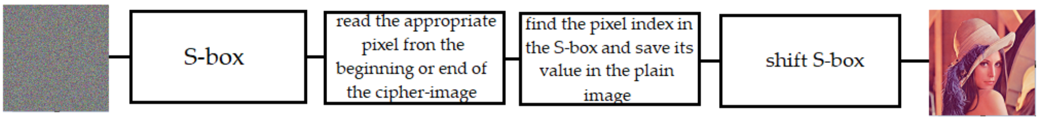

S-box
read the appropriate pixel fron the beginning or end of the cipher-image
find the pixel index in the S-box and save its value in the plain image
shift S-box

Figure 9. Decryption scheme.

5.1.3. S-Box Generation

The S-box should be generated in the second step of the proposed encryption algorithm. For this purpose, known from the literature, methods of generating permutations with, for example, chaotic mappings can be used. This article proposes a procedure that is based on generating permutations using the Fisher–Yates algorithm. More about the Fisher–Yates method itself, as well as its variants concerning the use of chaotic mappings, can be found in [43,44].

The proposed algorithm uses the tent map (4) due to uniform distribution. However, the M-map can also be used for this purpose even despite a non-uniform distribution (see Figure 7). A flat distribution from such values can be obtained by using, e.g., the procedure described in [45].

Preliminary assumptions: Let Sn be a list consisting of $[0, 1, \ldots, 255]$, $length_{Sn}$ represents its length, Sb is an empty list, N and M are the image dimensions:

1. Calculate the value of S_{px}, which is the sum of all pixels of the plain-image. S_{px} is the private key of the S-box;
2. Starting from initial value $((x + \frac{S_{px}}{3 \cdot 255 \cdot N \cdot M}) \mod 1)$ and parameter p, drop the first 10^3 recurrence (4) values;
3. From set $\{0, 1, \ldots, 255\}$, generate the following permutation:

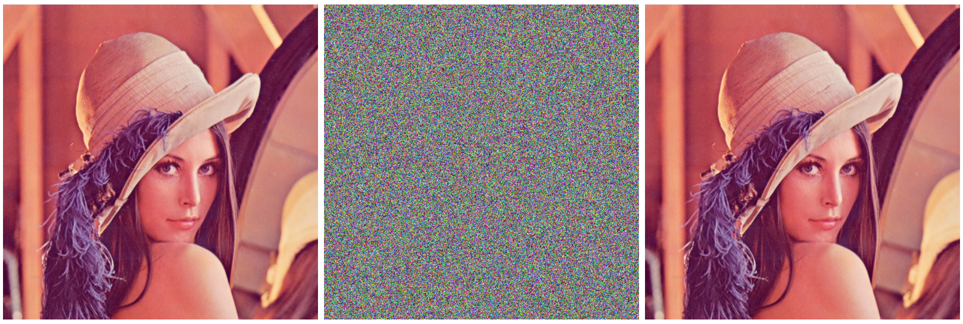
    While $length_{Sn} > 0$:

    i. Calculate x from recurrence (4);
    ii. Calculate $index = floor(x \cdot length_{Sn})$;
    iii. Add $Sn[index]$ to Sb;
    iv. Remove from Sn element $Sn[index]$;
    v. Decrease $length_{Sn}$ by 1.

The S-box generation algorithm depends on the value of S_{px}. This means that this value must be passed as a secret or public key. An incorrect value of S_{px} entered for decryption will result in receiving another S-box; thus, the cipher-image will not be decrypted correctly. If the value of S_{px} is treated as a secret key, then the number of all such keys is equal to $3 \cdot 255 \cdot N \cdot M$. For an image with dimensions of 512 × 512, the number of all possible keys is 200540160.

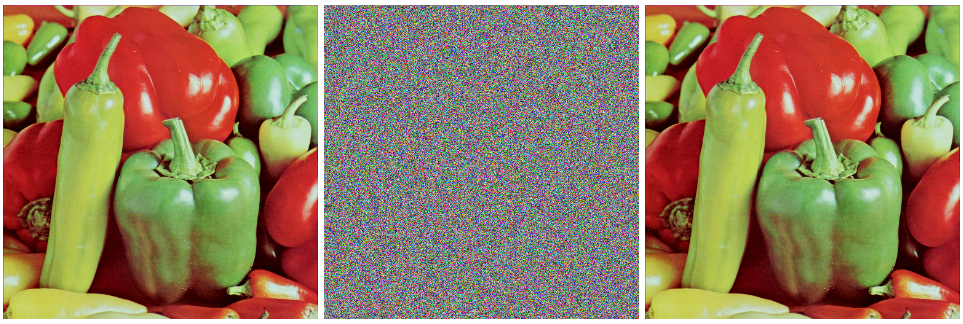
5.2. Cipher-Images of Selected Benchmark Images

Standard images of Lena, Pepper, and Baboon, shown in Figures 10a–12a, were selected to analyze the proposed encryption algorithm. The cipher-images obtained for the initial condition value of $x = 0.789$ and the parameter value of $p = 0.352$ are shown in Figures 10b–12b. On the other hand, Figures 10c–12c show images after decryption.



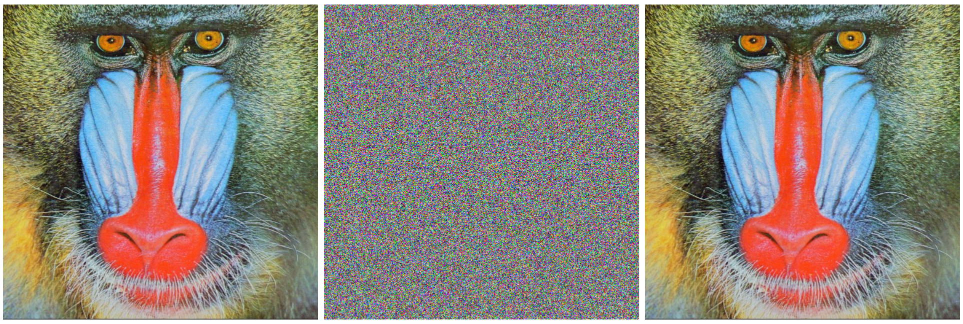
(**a**) (**b**) (**c**)

Figure 10. Image of Lena, its cipher-image and decrypted image. (**a**) Image of Lena; (**b**) cipher-image of Lena; (**c**) decrypted image of Lena.



(**a**) (**b**) (**c**)

Figure 11. Image of Peppers, its cipher-image, and decrypted image. (**a**) Image of Peppers; (**b**) cipher-image of Peppers; (**c**) decrypted Peppers image.



(**a**) (**b**) (**c**)

Figure 12. Image of Baboon, its cipher-image, and decrypted image. (**a**) Image of Baboon; (**b**) cipher-image of Baboon; (**c**) decrypted Baboon image.

For the selected test images and their cipher-images, an analysis was carried out in the next subsections. The diagram of this analysis is shown in Figure 13.

Research methodology:

- Key sensitivity analysis
- Histograms analysis
- Differential attack analysis
- Entropy analysis
- Correlation analysis for the adjacent pixels
- Comparative analysis

Figure 13. Research methodology for cipher-images analysis.

5.3. Key Sensitivity Analysis

A secure cipher should be sensitive to changes of the key values. To encrypt the image of Lena (Figure 10a), parameter $p = 0.352$ values was chosen, while the initial condition is set to $x_0 = 0.789$. The key resulting from the S-box generation algorithm is equal to 100842898. The images obtained with a tiny change of one of the keys are visible in Figure 14. Figure 14a is obtained for initial condition $x_0 = 0.789 + 10^{-16}$. In turn, Figure 14b is obtained for the map parameter equal to $p = 0.352 + 10^{-16}$. Finally, Figure 14c is obtained for the key obtained from the S-box equal to 100842897. In each of the above cases, the keys used differ from the correct ones by a tiny value. However, the recovered images are completely different from Lena's image from Figure 10a.

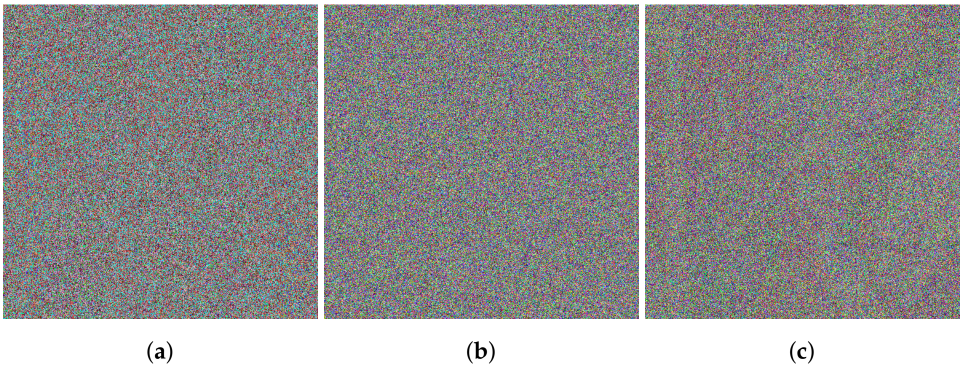


Figure 14. Images recovered with invalid values of keys. (**a**) Initial condition value changed by 10^{-16}; (**b**) parameter value changed by 10^{-16}; (**c**) the key from the S-box changed by 1.

5.4. Histograms

The simplest analysis of an encryption algorithm is to analyze the cipher-image histogram. The histogram of the cipher-image should be perfectly flat to make any statistical analysis impossible. In the case of a color image, such an analysis applies to each of the channels, i.e., it is performed separately for the pixels representing the red channel, separately for the green channel, and finally for the blue channel. The results obtained from this analysis for the original images and cipher-images are presented in Figures 15–17. From these figures, it can be seen that the histograms of the encrypted images for each channel are flat. From a cryptographic point of view, this is the most appropriate situation.

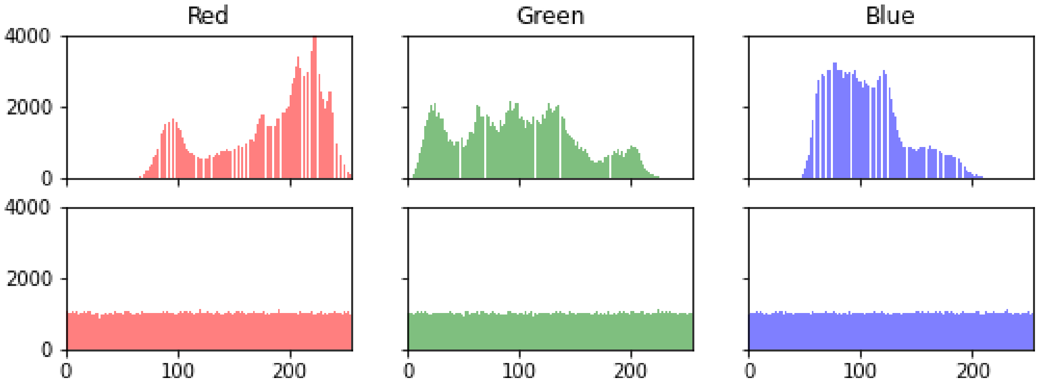


Figure 15. Histograms of Lena (Figure 10a (**top row**)) and its cipher-image (Figure 10b (**bottom row**)).

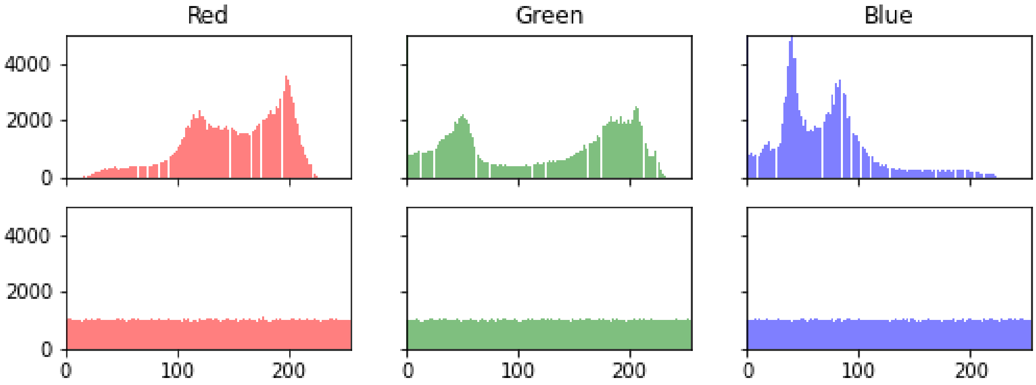


Figure 16. Histograms of Pepper (Figure 11a (**top row**)) and its cipher-image (Figure 11b (**bottom row**)).

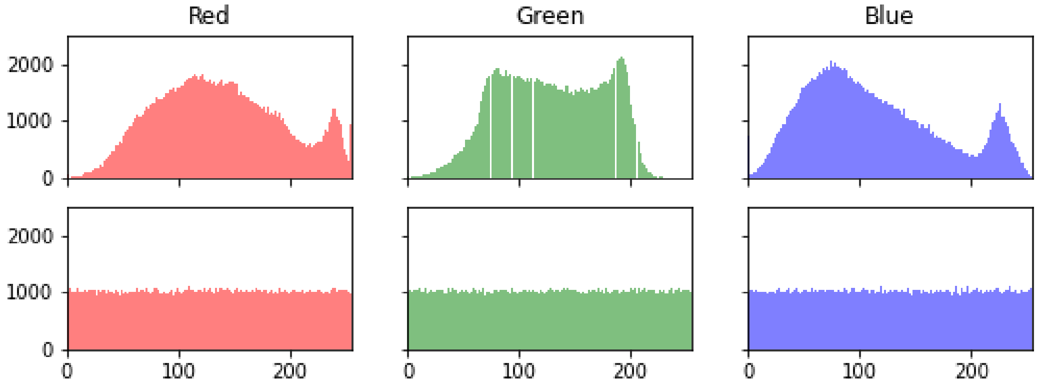


Figure 17. Histograms of Baboon (Figure 12a (**top row**)) and its cipher-image (Figure 12b (**bottom row**)).

5.5. *Differential Attack Analysis*

$NPCR$ (Number of Pixel of Change Rate) and $UACI$ (Unified Average Changing Intensity) are two crucial measures of the algorithm's resistance to differential attacks. To determine them, we need two encrypted images E_1 and E_2, for which its plain-images P_1 and P_2 differ from each other for only one randomly selected pixel. Furthermore, E_1 and E_2 are received using the same values of keys.

5.5.1. $NPCR$ Analysis

The $NPCR$ value is calculated from the following formula:

$$NPCR = \frac{1}{N \times M} \sum_{i,j} D(i,j) \times 100\%, \tag{12}$$

where the following is the case:

$$D(i,j) = \begin{cases} 0 & \text{if } E_{1(i,j)} = E_{2(i,j)} \\ 1 & \text{if } E_{1(i,j)} \neq E_{2(i,j)} \end{cases}, \tag{13}$$

and $N \times M$ denotes the image dimensions, and $E_{*(i,j)}$ is the pixel in the (i,j) coordinates of the E_* image. The ideal value for $NPCR$ is 100%. In practice, $NPCR$ close to 100% means that the encryption algorithm is resistant to differential attacks. The results for the cipher-images are presented in Table 3. The numerical values in this table are close to the ideal value, which concludes that the proposed algorithm is resistant to differential attacks.

Table 3. $NPCR$ values for test cipher images. The first column is the image, and the next one is the $NPCR$ value for the Red, Green, and Blue channels.

Image	Red	Green	Blue
Lena	99.19	99.23	99.21
Pepper	99.24	99.24	99.25
Baboon	100	100	100

5.5.2. $UACI$ Analysis

The $UACI$ value is calculated from the following formula:

$$UACI = \frac{1}{N \times M} \left[\sum_{i,j} \frac{|E_{1(i,j)} - E_{2(i,j)}|}{255} \right] \times 100\%, \tag{14}$$

and $N \times M$ denotes the image dimensions, and $E_{*(i,j)}$ is the pixel in the (i,j) coordinates of the E_* image. The desired value for $UACI$ is 33%. The results for the cipher-images are presented in Table 4. The numerical values in this table are close to the ideal value, which concludes that the proposed algorithm is resistant to differential attacks.

Table 4. $UACI$ values for test cipher images. The first column is the image, and the next one is the $UACI$ value for the Red, Green, and Blue channels.

Image	Red	Green	Blue
Lena	32.62	32.60	32.64
Pepper	32.78	32.85	32.78
Baboon	34.74	34.80	34.75

5.6. Entropy

Entropy measures the amount of information in the source. The greater its value, the more information this source carries with it. It can be calculated with the formula:

$$H(m) = \sum_{i=0}^{255} -p(m_i) \log_2 p(m_i), \tag{15}$$

where $p(m_i)$ is the probability of element m_i in message m. In the case of images, m_i is understood as the pixel value for a specific channel, i.e., it takes the value from the set $\{0, 1, \cdots, 255\}$, while $p(m_i)$ is the probability of m_i in a given channel, in all pixels of the image. For m defined as above, the entropy has a maximum value of 8. This case means that all probabilities of $p(m_i)$ are equal to $\frac{1}{256}$. The entropy results for the test images are presented in Table 5. The obtained results show that the entropy for the cipher-images is close to 8.

Table 5. Entropy value for test cipher images. The first column is the image, and the next one is the entropy value for the Red, Green, and Blue channels.

Image	Red	Green	Blue
Lena	7.9992	7.9992	7.9993
Pepper	7.9992	7.9992	7.9993
Baboon	7.9993	7.9993	7.9993

5.7. Correlation Analysis for the Adjacent Pixels

Pearson's correlation coefficient r can be used to determine the correlation between pixels. It is is given by the following formula:

$$r = \frac{\mathrm{Cov}(x, y)}{\sigma_x \cdot \sigma_y}, \tag{16}$$

where the following is the case:

$$\sigma_x = \sqrt{\mathrm{Var}(x)} = \sqrt{\frac{1}{N} \sum_{i=i}^{N} \left(x_i - \frac{1}{N} \sum_{i=1}^{N} x_i \right)^2}, \tag{17}$$

$$\sigma_y = \sqrt{\mathrm{Var}(y)} = \sqrt{\frac{1}{N} \sum_{i=i}^{N} \left(y_i - \frac{1}{N} \sum_{i=1}^{N} y_i \right)^2}, \tag{18}$$

$$\mathrm{Cov}(x, y) = \frac{1}{N} \sum_{i=i}^{N} \left(x_i - \frac{1}{N} \sum_{i=1}^{N} x_i \right) \left(y_i - \frac{1}{N} \sum_{i=1}^{N} y_i \right). \tag{19}$$

x and y are consecutive image pixels with dimensions $N \times M$. The results of the r correlation coefficient for the cipher-images are presented in Table 6. The obtained values of the r coefficient are close to zero, which means that the cipher-image pixels are not correlated. The lack of correlation applies to adjacent pixels in the horizontal, vertical, and diagonal arrangements.

Table 6. Correlation coefficient values (r) for test cipher images. The first column is the image, and the next one is the correlation coefficient value for the RGB channels of the horizontal, vertical, and diagonal adjacent pixels.

Image		Horizontal			Vertical			Diagonal	
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	0.0022	0.0002	0.0030	0.0008	0.0007	−0.0001	−0.0011	0.0016	0.0007
Pepper	0.0027	−0.0024	0.0013	0.0013	−0.0004	−0.0001	−0.0004	0.0019	−0.0006
Baboon	0.0048	0.0035	0.0009	−0.0050	0.0006	−0.0013	−0.0002	−0.0007	−0.0003

5.8. Comparative Analysis

To illustrate the proposed algorithm against the background of encryption procedures, Lena's image and measures for its cipher-image from the publication [46–48] were selected. And so, the Table 7 shows the values for $NPCR$, Table 8 shows the comparison for the $UACI$ measure, Table 9 shows the entropy, while the Table 10 shows the correlation coefficient for adjacent pixels. These Tables show that the values obtained for Lena's image from the proposed algorithm and those cited in the literature are similar. And so, looking at the $NPCR$ value in the Table 7 in the case of [47,48] publications, the obtained values are very similar. In the case of the $UACI$ measure, the result from work [47] is very similar again, but those from work [48] are already much worse (close to 49%) than the proposed algorithm. In the case of the entropy values presented in Table 9, all compared values are similar, although the closest values to the optimal value 8 are those from the proposed algorithm. Table 10 shows the correlation values for adjacent pixels for the compared works. Both the proposed algorithm and those from [47,48] have values very similar, close to the optimal value of 0.

Table 7. Comparison of the $NPCR$ values for cipher-images components of Lena from different publications. The first column is the image, and the next one is the $NPCR$ value for the Red, Green, and Blue channels.

Image	Red	Green	Blue
Proposed	99.19	99.23	99.21
[47]	99.58	99.56	99.64
[48]	99.7909	99.7925	99.7910

Table 8. Comparison of the $UACI$ values for cipher-images components of Lena from different publications. The first column is the image, and the next one is the $UACI$ value for Red, Green, and Blue channels.

Image	Red	Green	Blue
Proposed	32.62	32.60	32.64
[47]	33.27	33.36	33.50
[48]	49.1964	49.2234	49.2374

Table 9. Comparison of the entropy values for cipher-images components of Lena from different publications. The first column is the image, and the next one is the entropy value for Red, Green, and Blue channels.

Image	Red	Green	Blue
Proposed	7.9992	7.9992	7.9993
[46]	7.7771	7.6251	7.7150
[47]	7.9973	7.9972	7.9975
[48]	7.9893	7.9898	7.9894

Table 10. Comparison of correlation coefficient values (r) for cipher-images components of Lena from different publication. The first column is the image, and the next one is the correlation coefficient value for the RGB channels of the horizontal, vertical, and diagonal adjacent pixels.

Image		Horizontal			Vertical			Diagonal	
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Proposed	0.0022	0.0002	0.0030	0.0008	0.0007	−0.0001	−0.0011	0.0016	0.0007
[47]	0.0017	0.0011	−0.0030	−0.0004	0.0076	0.0050	0.0049	−0.0002	0.0049
[48]	0.0024	−0.0056	−0.0078	0.0010	−0.0037	0.0031	−0.0148	−0.0295	−0.0247

6. Conclusions

The article proposes a new dynamical system for cryptography applications based on the chaos theory. To confirm its usefulness, the analysis of fixed points, bifurcation, Lyapunov exponent, and invariant density was performed. The analysis shows that the so-called robust chaos characterizes the proposed dynamic system, i.e., there are no periodic windows. Moreover, both the Lyapunov exponent's stable value and the iterated variable's density suggest that this mapping can be used in chaotic cryptography applications. Additionally, the proposed mapping was compared with logistic, tent, and sine maps. The obtained results show its better features concerning other compared dynamical systems.

The article also introduces a new image encryption algorithm. It uses, among others, S-box, which is cyclically shifted and saves encrypted pixels in the cipher-image in the first free place from its beginning or end. However, it is required that the images be saved in RGB color format. The algorithm was tested on the images of Lena, Baboon, and Pepper, for which color histograms, $NPCR$ and $UACI$ measures, entropy, and correlation analysis for the adjacent pixels are presented. These values are successively almost equal to the following: 8 for the entropy, 0 for the correlation of adjacent pixels, 100% for the $NPCR$, and 33% for the $UACI$. The obtained values show that this simple algorithm can be used in practice to encrypt images.

Author Contributions: Conceptualization, M.L.; methodology, M.L. and M.B.; formal analysis, M.L. and M.B.; writing—original draft preparation, M.L. and M.B.; writing—review and editing, M.L. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Baptista, M. Cryptography with Chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
2. Yavuz, E.; Yazıcı, R.; Kasapbaşı, M.C.; Yamaç, E. A Chaos-Based Image Encryption Algorithm with Simple Logical Functions. *Comput. Electr. Eng.* **2016**, *54*, 471–483. [CrossRef]

3. Safi, H.W.; Maghari, A.Y. Image Encryption Using Double Chaotic Logistic Map. In Proceedings of the 2017 International Conference on Promising Electronic Technologies (ICPET), Deir El-Balah, Palestine, 16–17 October 2017; pp. 66–70. [CrossRef]
4. Fan, H.; Li, M. Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation. *Math. Probl. Eng.* **2017**, *2017*, 8124912. [CrossRef]
5. Özkaynak, F.; Özer, A.B. Cryptanalysis of a New Image Encryption Algorithm Based on Chaos. *Optik* **2016**, *127*, 5190–5192. [CrossRef]
6. Su, X.; Li, W.; Hu, H. Cryptanalysis of a Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy. *Multimed. Tools Appl.* **2017**, *76*, 14021–14033. [CrossRef]
7. Hu, Y.; Yu, S.; Zhang, Z. On the Cryptanalysis of a Bit-Level Image Chaotic Encryption Algorithm. *Math. Probl. Eng.* **2020**, *2020*, 5747082. [CrossRef]
8. Huang, R.; Liao, X.; Dong, A.; Sun, S. Cryptanalysis and Security Enhancement for a Chaos-Based Color Image Encryption Algorithm. *Multimed. Tools Appl.* **2020**, *79*, 27483–27509. [CrossRef]
9. Mastan, J.M.K.; Pandian, R. Cryptanalysis of Two Similar Chaos-Based Image Encryption Schemes. *Cryptologia* **2020**, *45*, 541–552. [CrossRef]
10. Masood, F.; Ahmad, J.; Shah, S.A.; Jamal, S.S.; Hussain, I. A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map. *Entropy* **2020**, *22*, 274. [CrossRef]
11. Al-Maadeed, T.A.; Hussain, I.; Anees, A.; Mustafa, M.T. A Image Encryption Algorithm Based on Chaotic Lorenz System and Novel Primitive Polynomial S-Boxes. *Multimed. Tools Appl.* **2021**, *80*, 24801–24822. [CrossRef]
12. Shahna, K.U.; Mohamed, A. An Image Encryption Method Using Henon Map and Josephus Traversal. In *Innovations in Bio-Inspired Computing and Applications*; Abraham, A., Gandhi, N., Pant, M., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 375–385.
13. Bao, H.; Hua, Z.; Li, H.; Chen, M.; Bao, B. Discrete Memristor Hyperchaotic Maps. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 4534–4544. [CrossRef]
14. Hua, Z.; Zhou, Y.; Pun, C.M.; Chen, C.P. 2D Sine Logistic Modulation Map for Image Encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
15. Li, K.; Bao, H.; Li, H.; Ma, J.; Hua, Z.; Bao, B. Memristive Rulkov Neuron Model with Magnetic Induction Effects. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1726–1736. [CrossRef]
16. Khairullah, M.; Alkahtani, A.; Bin Baharuddin, M.; Al-Jubari, A. Designing 1D Chaotic Maps for Fast Chaotic Image Encryption. *Electronics* **2021**, *10*, 2116. [CrossRef]
17. Lasota, A.; Mackey, M.C. *Chaos, Fractals, and Noise*; Springer: New York, NY, USA, 1994; pp. 41–47.
18. Ott, E. *Chaos in Dynamical Systems*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2002; pp. 51–56. [CrossRef]
19. Parvaz, R.; Zarebnia, M. A Combination Chaotic System and Application in Color Image Encryption. *Opt. Laser Technol.* **2018**, *101*, 30–41. [CrossRef]
20. Shahna, K.; Mohamed, A. An Image Encryption Technique Using Logistic Map and Z-Order Curve. In Proceedings of the 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR), Ernakulam, India, 11–13 July 2018; pp. 1–6. [CrossRef]
21. Boumaraf, M.; Merazka, F. Partial and full speech encryption schemes based on 1D chaotic maps for AMR-WB codec. In Proceedings of the 2018 2nd International Conference on Natural Language and Speech Processing (ICNLSP), Algiers, Algeria, 25–26 April 2018; pp. 1–5. [CrossRef]
22. Prasad, N.; Ravi, V.M.; Chandrasekhar, L. Image Encryption with an Encrypted QR, Random Phase Encoding, and Logistic Map. In Proceedings of the 2018 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 4–6 January 2018; pp. 1–4. [CrossRef]
23. Jonathan Satish, T.; Naga Sai Theja, M.; Girish Kumar, G.; Thanikaiselvan, V. Image Encryption Using Integer Wavelet Transform, Logistic Map and XOR Encryption. In Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018; pp. 704–709. [CrossRef]
24. Singh, D.k.; Tomar, K. A Robust Color Image Encryption Algorithm in Dual Domain Using Chaotic Map. In Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 20–21 April 2018; pp. 931–935. [CrossRef]
25. Draksharam, S.; Katravulapalli, D.; Rohith Krishna, K.; Thanikaiselvan, V. Analysis of Hybrid Chaotic Image Encryption. In Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29–31 March 2018; pp. 697–703. [CrossRef]
26. Liansheng, S.; Cong, D.; Xiao, Z.; Ailing, T.; Anand, A. Double-Image Encryption Based on Interference and Logistic Map under the Framework of Double Random Phase Encoding. *Opt. Lasers Eng.* **2019**, *122*, 113–122. [CrossRef]
27. Macovei, C.; Răducanu, M.; Datcu, O. Image Encryption Algorithm Using Wavelet Packets and Multiple Chaotic Maps. In Proceedings of the 2020 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 5–6 November 2020; pp. 1–4. [CrossRef]
28. Rehman, M.U.; Shafique, A.; Khalid, S.; Hussain, I. Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps. *IEEE Access* **2021**, *9*, 52277–52291. [CrossRef]

29. Rama Devi, K.; Janaki, V.; VijayaLaxmi, G. Encryption Methodology on Crypto Keys from Image Using Chaos Logistic Maps. *Mater. Today Proc.* **2021**. [CrossRef]
30. Mondal, B.; Singh, S.; Kumar, P. A Secure Image Encryption Scheme Based on Cellular Automata and Chaotic Skew Tent Map. *J. Inf. Secur. Appl.* **2019**, *45*, 117–130. [CrossRef]
31. Yoosefian Dezfuli Nezhad, S.; Safdarian, N.; Hoseini Zadeh, S.A. New Method for Fingerprint Images Encryption Using DNA Sequence and Chaotic Tent Map. *Optik* **2020**, *224*, 165661. [CrossRef]
32. Khan, J.S.; Kayhan, S.K. Chaos and Compressive Sensing Based Novel Image Encryption Scheme. *J. Inf. Secur. Appl.* **2021**, *58*, 102711. [CrossRef]
33. Sangavi, V.; Thangavel, P. An Exotic Multi-Dimensional Conceptualization for Medical Image Encryption Exerting Rossler System and Sine Map. *J. Inf. Secur. Appl.* **2020**, *55*, 102626. [CrossRef]
34. Arroyo, D.; Amigó Garcia, J.M.; Li, S.; Alvarez, G. On the Inadequacy of Unimodal Maps for Cryptographic Applications. In Proceedings of the RECSI 2010: IX [i.e., XI] Reunión Española sobre Criptología y Seguridad de la Información, Tarragona, Spain, 7–10 September 2010; Ferrer, J.D., Ed.; Publicacions URV: Tarragona, Spain, 2010; pp. 37–42.
35. Lawnik, M. Combined Logistic and Tent Map. *J. Phys. Conf. Ser.* **2018**, *1141*, 012132. [CrossRef]
36. Lawnik, M. Logistic Map as a Fourier's Series Expansion: Numerical Analysis. *J. Phys. Conf. Ser.* **2019**, *1391*, 012078. [CrossRef]
37. Sahay, A.; Pradhan, C. Gauss Iterated Map Based RGB Image Encryption Approach. In Proceedings of the 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 6–8 April 2017; pp. 0015–0018. [CrossRef]
38. Rahmawati, W.M.; Liantoni, F. Image Compression and Encryption Using DCT and Gaussian Map. *IOP Conf. Ser. Mater. Sci. Eng.* **2019**, *462*, 012035. [CrossRef]
39. Berezowski, M.; Lawnik, M. Identification of Fast-changing Signals by Means of Adaptive Chaotic Transformations. *Nonlinear Anal. Model. Control* **2014**, *19*, 172–177. [CrossRef]
40. Lawnik, M. The Approximation of the Normal Distribution by Means of Chaotic Expression. *J. Phys. Conf. Ser.* **2014**, *490*, 012072. [CrossRef]
41. Banerjee, S.; Yorke, J.A.; Grebogi, C. Robust Chaos. *Phys. Rev. Lett.* **1998**, *80*, 3049–3052. [CrossRef]
42. Lawnik, M. Analysis of the Chaotic Maps Generating Different Statistical Distributions. *J. Phys. Conf. Ser.* **2015**, *633*, 012086. [CrossRef]
43. Fisher, R.A.; Yates, F. *Statistical Tables for Biological, Agricultural and Medical Research*, 3rd ed.; Oliver & Boyd: London, UK, 1948; pp. 26–27.
44. Lawnik, M.; Banasik, A. Generating and Numbering Permutations with the Use of Chaotic Maps. In Proceedings of the 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Cracow, Poland, 22–25 September 2021; Volume 1, pp. 387–390. [CrossRef]
45. Lawnik, M. Generation of Numbers with the Distribution Close to Uniform with the Use of Chaotic Maps. In Proceedings of the 4th International Conference on Simulation and Modeling Methodologies, Technologies and Applications—SIMULTECH, Vienna, Austria, 28–30 August 2014; INSTICC, SciTePress: Setúbal, Portugal, 2014; pp. 451–455. [CrossRef]
46. Faragallah, O.S.; Alzain, M.A.; El-Sayed, H.S.; Al-Amri, J.F.; El-Shafai, W.; Afifi, A.; Naeem, E.A.; Soh, B. Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding. *IEEE Access* **2019**, *7*, 4184–4194. [CrossRef]
47. Khan, M.; Masood, F. A Novel Chaotic Image Encryption Technique Based on Multiple Discrete Dynamical Maps. *Multimed. Tools Appl.* **2019**, *78*, 26203–26222. [CrossRef]
48. Wu, X.; Li, Y.; Kurths, J. A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System. *PLoS ONE* **2015**, *10*, e0119660. [CrossRef]