

## Article

# A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications

Adina Elena Lupu (Blaj)<sup>1,\*</sup> and Adriana Vlad<sup>1,2,\*</sup><sup>1</sup> Faculty of Electronics, Telecommunications and Information Technology, National University of Science and Technology Politehnica of Bucharest, 061071 Bucharest, Romania<sup>2</sup> Research Institute for Artificial Intelligence, Romanian Academy Bucharest, 050711 Bucharest, Romania

\* Correspondence: adina\_elena.lupu@stud.etti.upb.ro (A.E.L.); avlad@racai.ro (A.V.)

**Abstract:** One technique, especially in chaos-based cryptographic applications, is to include the message in the evolution of the dynamical system. This paper aims to find out if and to what extent the statistical behavior of the chaotic system is affected by the message inclusion in its dynamic evolution. The study is illustrated by the dynamical system described by the logistic map in cryptographic applications based on images. The evaluation of the statistical behavior was performed on an original scheme proposed. The Monte Carlo analysis of the applied Kolmogorov–Smirnov statistical test revealed that the dynamical system in the processing scheme with message inclusion does not modify its proper statistical behavior (revealed by definition relation). This was possible due to the proposed scheme designed. Namely, this scheme contains a decision switch which, supported by an appropriate choice of the magnitude of the scaling factor, ensures that the values of the dynamical system are maintained in the definition domain. The proposed framework for analyzing the statistical properties and for preserving the dynamical system behavior is one main contribution of this research. The message inclusion scheme also provides an enhancement with cryptographic mixing functions applied internally; the statistical behavior of the dynamical system is also analyzed in this case. Thus, the paper contributes to the theoretical complex characterization of the dynamical system considering also the message inclusion case.



**Citation:** Lupu, A.E.; Vlad, A. A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications. *Electronics* **2024**, *13*, 2270. <https://doi.org/10.3390/electronics13122270>

Academic Editor: Hung-Yu Chien

Received: 15 April 2024

Revised: 25 May 2024

Accepted: 4 June 2024

Published: 10 June 2024



**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** chaotic system with message inclusion; logistic map; Kolmogorov–Smirnov test; Monte Carlo analysis; image encryption

## 1. Introduction

The encryption technique of including the message in the chaotic system is realized by introducing the characters of the message directly into the evolution of the dynamical system [1–3]. A detailed theoretical description of this method is presented in [4]. Examples of schemes in which the dynamical system functions with the inclusion of the message are illustrated in various articles in the literature; see for example [5–8]. An advantage of using this technique is the fact that the encrypted message at the current iteration does not only depend on the original message from that iteration, but also on its values from previous iterations, contributing to diffusion [9].

It is known that statistical properties of chaotic systems such as ergodicity and pseudo-randomness are favorable for use in cryptographic applications [10]. The extent to which the behavior of the dynamical system is affected by the inclusion is of real interest for the development of cryptographic applications and in the larger domain of communications. Keeping the properties of the chaotic system is essential throughout the encryption process [11].

To the best of our knowledge, such a study that closely follows the statistical behavior of the chaotic system with inclusion is lacking in the literature. In this regard, the main objective of the present work is to clarify the impact of inclusion on the statistical behavior of the chaotic signal.

We started from a preliminary research performed in [7], where the main goal was to determine the contribution of the dynamical system to message encryption using the inclusion technique. Here, the main objective is to analyze to what extent the chaotic system completed by message inclusion preserves its statistical properties. All detailed analysis is performed using an original proposed encryption scheme. In order to keep the values of the chaotic system in the definition domain, we propose to use in the scheme a decision switch which controls message inclusion. A study is also carried out for the appropriate choice of the magnitude of the scaling factor, in order to include the message in the evolution of the dynamical system, without altering its chaotic behavior.

In the proposed scheme, the dynamical system chosen is the logistic map, because it allows a clear illustration of the impact of inclusion by referring to the known probability law for  $R = 4$  control parameter value (for  $R = 4$ , the probability density function and the distribution function are known). It is known that the random process associated to the logistic map is ergodic; see for example [12,13]. To verify whether or not the statistical properties of the system are affected by inclusion, a Monte Carlo analysis on the Kolmogorov–Smirnov statistical test is performed. A detailed description of the steps of the Kolmogorov–Smirnov test is presented in [14].

One main contribution of this paper is the manner of statistically evaluating the processing schemes containing dynamical systems with message inclusion and the proposed framework to keep the statistical behavior of the chaotic random signal, as revealed by its definition relation. The analysis is performed using the logistic map, but the procedure can be extended in a similar way for other dynamical systems.

The logistic map is defined as follows [15]:

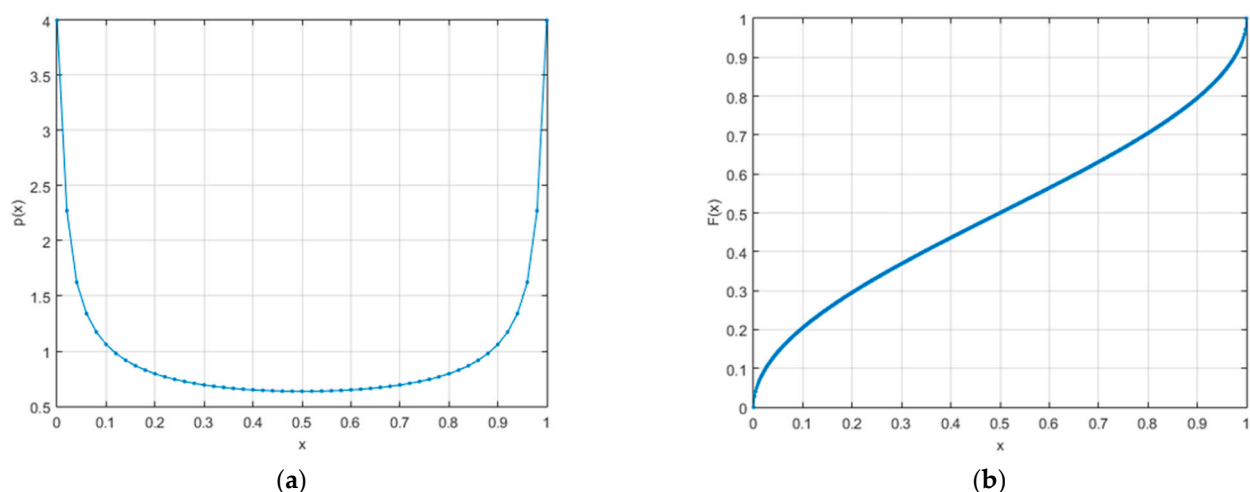
$$x_{k+1} = Rx_k(1 - x_k) \quad (1)$$

where  $R$  is the control parameter, with values in  $[0, 4]$  and the  $x_k$  generated values belong to  $[0, 1]$ ;  $k$  denotes the iteration (discrete time).

The first order probability density function of the random process associated to the logistic map for  $R = 4$  is the following:

$$p_X(x) = \frac{1}{\pi\sqrt{x(1-x)}} \quad (2)$$

and the graphical representation is in Figure 1a.



**Figure 1.** (a) 1st order probability density function associated to the logistic map for  $R = 4$ ; (b) 1st order distribution function associated to the logistic map for  $R = 4$ .

The distribution function corresponding to the logistic map for  $R = 4$  is given by the following relation:

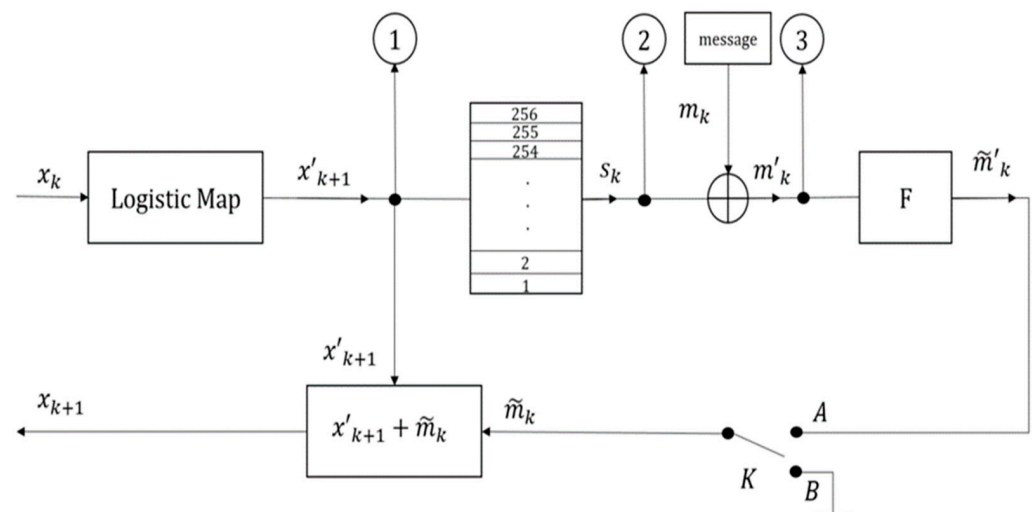
$$F_X(x) = \int_{-\infty}^x \frac{1}{\pi \sqrt{u(1-u)}} du \quad (3)$$

and the graph is represented in Figure 1b.

The paper is structured as follows. In Section 2, the proposed scheme is described and the role of the decision switch regarding the message inclusion is explained. In Section 3, the statistical behavior of the logistic map is evaluated and a study is carried out on the sizing of the scaling factor involved in the message inclusion technique. Section 4 completes the scheme by introducing the cryptographic mixing function, which operates on the message included in the evolution of the dynamical system. The analysis of the statistical behavior of the dynamical system is resumed in this situation as well. The Section 5 presents the final conclusions, summarizing the main contributions made in the paper.

## 2. Functional Description of the Scheme Based on the Decision Switch

In this section, an encryption scheme illustrated using the logistic map is proposed (Figure 2). An explanation of how the scheme operates is given and the contribution of a switch with a role in the message inclusion decision is detailed.



**Figure 2.** Message inclusion scheme.

### 2.1. Functional Description of the Scheme

Starting from the initial condition  $x_0$ , the logistic map is iterated according to the relation:

$$x'_{k+1} = Rx_k(1 - x_k) \quad (4)$$

*Note:* The notation  $x'_{k+1}$  in relation (4) differs from  $x_{k+1}$  in relation (1), due to the fact that the scheme functions by inclusion, which causes the dynamical system input to be affected at each iteration by an additional value. Thus, the value denoted by  $x_{k+1}$  in (1) is changed to  $x'_{k+1}$  according to the following details.

In Figure 2, at each iteration, a byte  $s_k$  is associated with the  $x'_{k+1}$  output of the chaotic system. This association is made by dividing the  $[0, 1]$  interval of the value space of the logistic map into 256 subintervals of equal length. To each subinterval is assigned an integer from the range  $[0, 255]$ . Thus, the subinterval to which  $x'_{k+1}$  belongs is determined and the integer associated with that subinterval is converted to byte  $s_k$ .

A bitwise XOR is performed between  $s_k$  and a byte  $m_k$  of the input message,  $k$  representing the iteration. The  $m'_k$  byte is obtained, representing the output of the processing scheme, control point (visualization point) 3 in Figure 2.

$$m'_k = s_k \oplus m_k \quad (5)$$

The  $m'_k$  byte is converted back to integer and scaled by the factor  $F$ , in order to be reintroduced in the evolution of the dynamical system. The obtained value is denoted by  $\tilde{m}'_k$ .

$$\tilde{m}'_k = m'_k \cdot F \quad (6)$$

The next step is to make the decision to include or not the processed and scaled message  $\tilde{m}'_k$  in the evolution of the chaotic system. The decision depends on the  $x'_{k+1}$  value.

$$\tilde{m}_k = \begin{cases} \tilde{m}'_k, & \text{if } x'_{k+1} \in [0; D), \\ 0, & \text{if } x'_{k+1} \in [D; 1) \end{cases}, \text{ where } D = 1 - 255 \cdot F; \quad (7)$$

Next,  $\tilde{m}_k$  is added in the evolution of the system:

$$x_{k+1} = Rx_k(1 - x_k) + \tilde{m}_k. \quad (8)$$

As an example, we follow the input values of the chaotic system for several iterations:

$$\begin{aligned} x_0 &\rightarrow x'_1 = Rx_0(1 - x_0) \\ x_1 &= x'_1 + \tilde{m}_0 = Rx_0(1 - x_0) + \tilde{m}_0 \\ x_1 &\rightarrow x'_2 = Rx_1(1 - x_1) \\ x_2 &= x'_2 + \tilde{m}_1 = Rx_1(1 - x_1) + \tilde{m}_1 \\ x_2 &\rightarrow x'_3 = Rx_2(1 - x_2) \\ x_3 &= x'_3 + \tilde{m}_2 = Rx_2(1 - x_2) + \tilde{m}_2 \end{aligned}$$

Therefore, a new system is obtained, where  $x_0, x_1, x_2, \dots, x_k$  represent the input values, and  $x'_1, x'_2, x'_3, \dots, x'_{k+1}$  are its intermediate output values. Note that  $x_1, x_2, x_3, \dots, x_{k+1}$  are the new state values of the dynamical system altered with the inclusion of  $\tilde{m}_k$ .

Decryption is performed by applying operations in reverse order. The output of the encryption scheme is the  $m'_k$  cryptogram (visualization point 3) in Figure 2. The secret key elements are the  $R$  control parameter, the  $x_0$  initial condition and the  $F$  scaling factor. Knowing the key and the  $m'_k$  cryptogram, the states of the chaotic system can be recreated at the receiver, determining the  $s_k$  byte. A bitwise XOR is performed between  $m'_k$  and  $s_k$ , obtaining the  $m_k$  byte of the input message. *Important note:* similar to the encryption process, each  $m'_k$  byte is converted to integer and scaled by the factor  $F$ ; then follows the decision to include it or not in the evolution of the dynamical system, taking into account the decision switch.

## 2.2. The Role of the Decision Switch in the Processing Scheme

To ensure that the dynamical system maintains its chaotic behavior after the inclusion of the processed and scaled message, it is necessary that the values  $x_1, x_2, x_3, \dots, x_{k+1}$  remain in the definition domain  $[0, 1]$  of the logistic map. When  $x'_{k+1}$  value is very close to 1, by adding  $\tilde{m}_k$  there is a possibility that  $x_{k+1}$  becomes greater than 1 and, in this case, the system no longer maintains its trajectory in the  $[0, 1]$  domain of definition and loses its chaotic behavior. It can be observed that, after the dynamical system has reached a value outside the range  $[0, 1]$ , the proposed scheme no longer functions, an interval for discretization cannot be selected.

As an example, we iterated the logistic map (in the diagram in Figure 2) for the control parameter  $R = 4$ , initial condition  $x_0 = 0.2$  and scaling factor  $F = 10^{-9}$ . In this example, we considered the external message equal to zero and assumed the switch  $K$

is always in position A (at each iteration the  $\tilde{m}'_k$  value is reintroduced). It is observed that after the dynamical system has reached a value outside the range  $[0, 1]$ —namely  $x_k = 1.000000124519015$  at iteration  $k = 602$ —the proposed scheme no longer functions, an interval for discretization cannot be selected.

To eliminate this undesirable behavior, a decision threshold  $D$ , that controls inclusion and determines the  $\tilde{m}_k$  values, has been introduced into the processing scheme. Therefore:

- If  $x'_{k+1} \in [D, 1)$ , then  $\tilde{m}_k = 0$ , no inclusion is considered; switch  $K$  is in position B;
- If  $x'_{k+1} \in (0, D)$ , then  $\tilde{m}_k = \tilde{m}'_k = m'_k \cdot F$ , inclusion is considered; switch  $K$  is in position A.

Thus, the value of the decision threshold  $D$  is equal to the maximum admissible  $x'_{k+1}$  value, for which adding the maximum value of  $\tilde{m}_k$ ,  $x_{k+1}$  does not exceed 1.

$$\begin{aligned} x_{k+1} < 1 &\rightarrow x'_{k+1} + \tilde{m}_k < 1 \\ x'_{k+1} < 1 - \max(\tilde{m}_k) &\rightarrow x'_{k+1} < 1 - \max(\tilde{m}'_k) \rightarrow x'_{k+1} < 1 - \max(m'_k) \cdot F \quad (9) \\ x'_{k+1} < 1 - 255 \cdot F &\rightarrow D = 1 - 255 \cdot F \end{aligned}$$

In conclusion, the operating scheme represents a new system that differs from the logistic map by including the message in its evolution. This processing scheme is controlled by a decision switch with the role of maintaining the evolution of the new system in the definition range  $[0, 1]$ .

It will be further examined to what extent the chaotic system, completed by message inclusion, preserves its initial statistical behavior corresponding to relation (1).

### 3. Message Inclusion Impact on the Statistical Chaotic Behavior: An Evaluation

#### 3.1. Study Scenario Description

At first, we will consider that the value of the external message is zero and the inclusion loop is not taken into account (in Figure 2, switch  $K$  is in position B). This is denoted as the *reference scenario* because in this case the scheme represents the dynamical system described by the logistic map without any other intervention. The results of this scenario (outputs/visualization points marked on the scheme with 1 and 2) will be used for comparison in a *study scenario*, that will consider the dynamical system affected by inclusion.

For the *study scenario* we consider the external message as a byte session (image or text) and the inclusion loop is taken into account (i.e., the switch works in positions A or B). Thus, the inclusion signal will be formed by summing the discretized chaotic signal with the external message. These resulting values will be included in the dynamical system evolution after scaling them by a given  $F$  factor.

We will compare the results of this *study scenario* with the previous scenario, the reference one, in the visualization points (1,2,3) marked on the diagram in Figure 2.

#### 3.2. Study Method

In visualization point 1, the random process associated with the logistic map can be followed; specifically, we follow the trajectories (the particular realizations of the random process). Each trajectory is determined by the initial condition and the  $R$  control parameter value. It is known that this random process is ergodic [12,13]. In our study, we consider  $R = 4$ ; in this case, the first-order probability law of the random process is described by the probability density function in Figure 1a. The probability law in Figure 1a is considered in the stationarity region of the random process (after the transient time has elapsed) [14]. We follow whether the first-order probability law of the chaotic system is affected by inclusion. Therefore, we analyze the random process at observation point 1 of the scheme in the scenario with inclusion and will refer to the *reference scenario*. For this we apply the Kolmogorov–Smirnov test.

The Kolmogorov–Smirnov statistical test verifies the concordance between an experimental distribution law and a theoretical one. A detailed description of the steps of the Kolmogorov–Smirnov test is presented in [14]. The experimental data set used for the Kolmogorov–Smirnov test consists of the values  $(x'_{k1}, x'_{k2}, x'_{k3}, \dots, x'_{kN})$  obtained by sampling  $N$  trajectories of the random process of the new system (with message inclusion) at iteration  $k$ . To obtain the trajectories, we considered  $N$  initial conditions  $x_{01}, x_{02}, x_{03}, \dots, x_{0N}$ ; randomly generated according to the uniform distribution law in  $[0, 1]$  and  $R = 4$ , iterating the dynamical system until the chosen  $k$  iteration. In this paper, we used  $N = 10,000$  trajectories,  $k = 150$ , and the statistical significance level of the test,  $\alpha = 0.05$ . To choose the  $k$  value, we considered an iteration in the stationary region of the logistic map [14]. Using the experimental data set sampled from the random process at  $k$  iteration, we check whether the experimental probability law verifies the theoretical law.

The two hypotheses of the Kolmogorov–Smirnov statistical test are:

$H_0$ : the experimental data set comes from the same theoretical distribution as in (3), the inclusion does not modify the probability law.

$H_1$ : the experimental data set does not come from the same theoretical distribution as in (3), the inclusion affects the probability law.

The maximum absolute deviation between the two distribution functions, theoretical  $F(x)$  and experimental  $F_e(x)$ , is calculated. This becomes the  $\delta$  test value.

$$\delta = \max_x \{|F_e(x) - F(x)|\} \quad (10)$$

The  $\delta$  test value is compared to the  $\Delta_\alpha$  threshold value, according to the chosen  $\alpha$  value:

$$\Delta_\alpha = \sqrt{\frac{1}{2N} \ln \frac{2}{\alpha}}, \quad (11)$$

where  $N$  = data volume (number of trajectories considered) and  $\alpha$  = significance level of the test.

If  $\delta \leq \Delta_\alpha$ ,  $H_0$  hypothesis is accepted.

According to the estimation theory [16], for  $\alpha = 0.05$  and using Monte Carlo analysis by resuming the statistical test for  $L = 500$  times, the range of accepted proportions is  $[0.93, 0.97]$ .

*Note:* To determine the range of accepted proportions, we use the confidence interval defined as  $\hat{p} \pm z_{\alpha/2} \sqrt{\hat{p}(1 - \hat{p})/L}$ , where  $\hat{p} = 1 - \alpha = 1 - 0.05 = 0.95$ ;  $L = 500$ ;  $z_{\alpha/2}$  is  $\alpha/2$  point value of the standard gaussian law. In our case  $z_{\alpha/2} = 1.96$  for  $\alpha = 0.05$ . Thus, the accepted region will be  $0.95 \pm 1.96 \sqrt{0.95(1 - 0.95)/500}$ ; namely  $[0.93, 0.97]$ .

In observation point 2, we acquire the data representing the trajectory of the chaotic system after discretization. This trajectory appears as a sequence of bytes, and we represent it as an image. We also display the corresponding histogram.

In observation point 3, the output image of the encryption scheme and its histogram are visually inspected. For illustration, we used black and white images of size  $256 \times 256$  pixels, each pixel being represented by 8 bits. Thus, the corresponding histograms are made in 256 values.

The processing scheme and simulations were implemented using the Matlab R2017b development environment.

### 3.3. Experimental Results

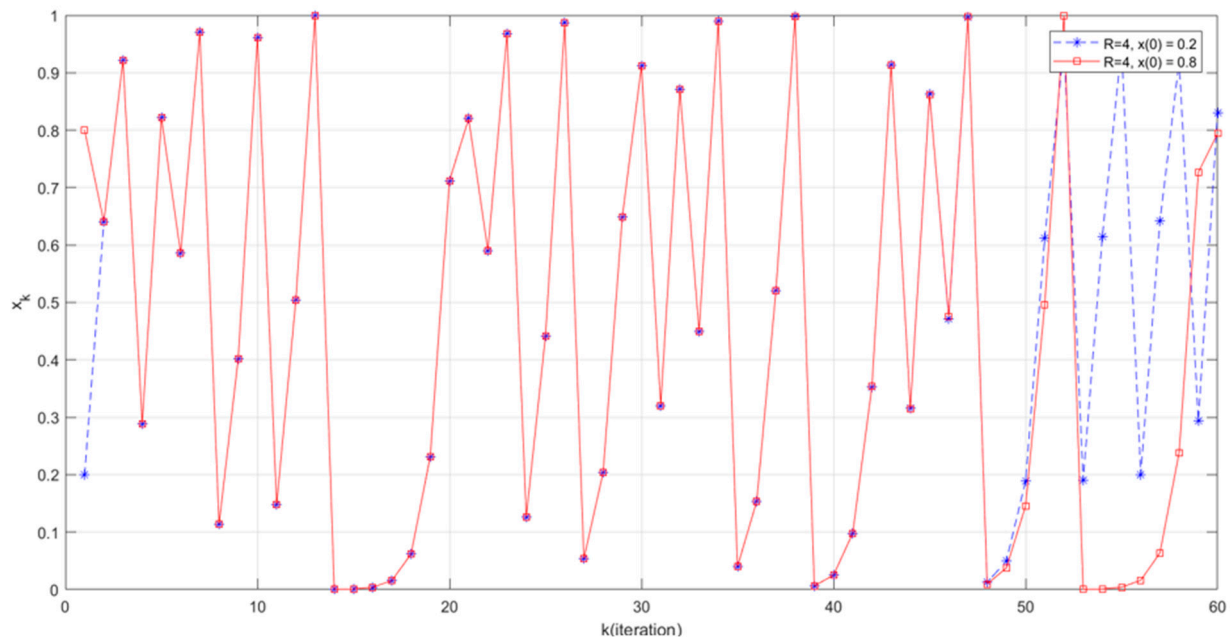
In order to perform the simulations corresponding to the two scenarios (*reference* and *study scenario*) we considered for the logistic map the control parameter  $R = 4$  and the initial condition  $x_0 = 0.2$ . For the scaling factor  $F$  in the scheme in Figure 2 we have chosen the value  $F = 10^{-12}$  based on the study made in Section 3.4.

In the *reference scenario*, the scheme in Figure 2 is in fact the dynamical system logistic map working according to relation (1) (unaffected by inclusion). Thus, the inclusion loop is not taken into account, the decision switch  $K$  is always in position B (open). We illustrate



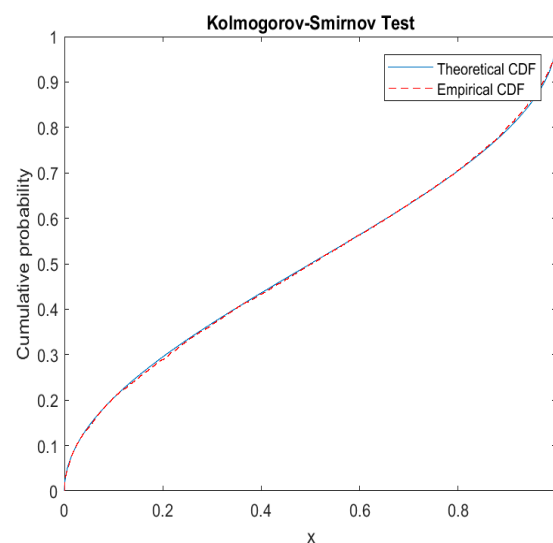
graphically some elements that will matter in discussing the effect of inclusion in the study scenario.

By plotting the trajectory of the dynamical system at observation point 1 in Figure 2, for two different initial conditions and  $R = 4$ , we obtain two distinct trajectories; illustrated in Figure 3.



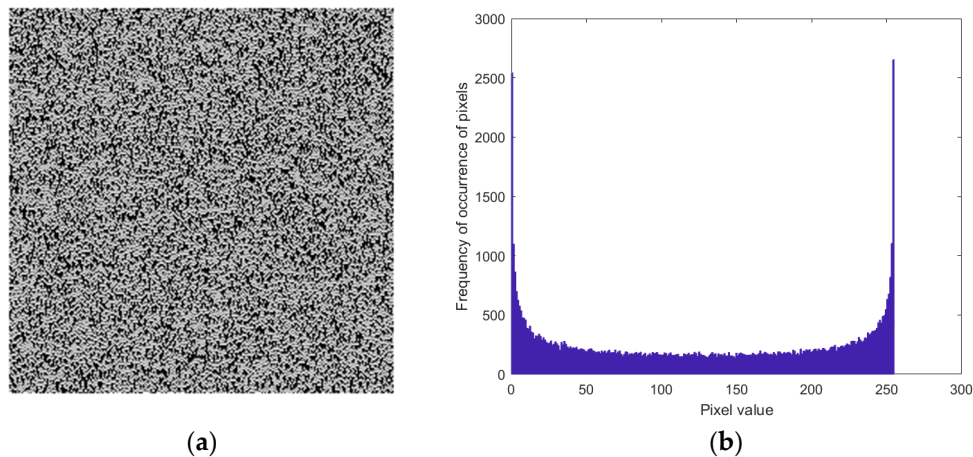
**Figure 3.** Trajectories of the logistic map for two different initial conditions (*reference scenario*).

Figure 4 shows the theoretical first order distribution function and the experimental distribution function of the random variable sampled at iteration  $k = 150$ , obtained using the method described in Section 3.2. A Monte Carlo analysis was performed, the Kolmogorov–Smirnov test being repeated 500 times. The obtained percentage of  $H_0$  hypothesis acceptance was 94.8%, which is in the estimation range  $[0.93, 0.97]$ . Therefore, we can state with 95% statistical confidence that the experimental data come from the theoretical probability law of the logistic map for  $R = 4$ .



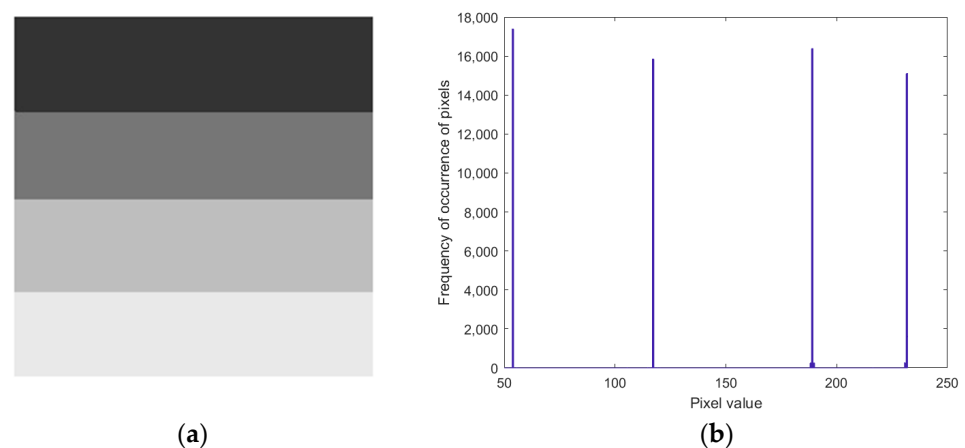
**Figure 4.** Theoretical and experimental cumulative distribution function (CDF) at iteration  $k = 150$ —*reference scenario*.

Figure 5 shows the image after discretizing the dynamical system values and its corresponding histogram, obtained at the observation point 2. Analyzing the obtained histogram, it can be noticed that it corresponds to the histogram of the probability density of the logistic function from Figure 1a. This is a result of the ergodicity of the random process because the image is obtained from a temporal analysis of the measurements at visualization point 2, tracked over time, over a large number of iterations, on a random chosen trajectory.



**Figure 5.** (a) Image at observation point 2 and (b) corresponding histogram—*reference scenario*.

Next, we analyze the behavior of the dynamical system in the *study scenario* by comparison with the *reference scenario*. To illustrate the *study scenario*, we consider the external message to be an image of size  $256 \times 256$  pixels, with low entropy; this is illustrated in Figure 6.



**Figure 6.** (a) Input image in the *study scenario* and (b) its corresponding histogram.

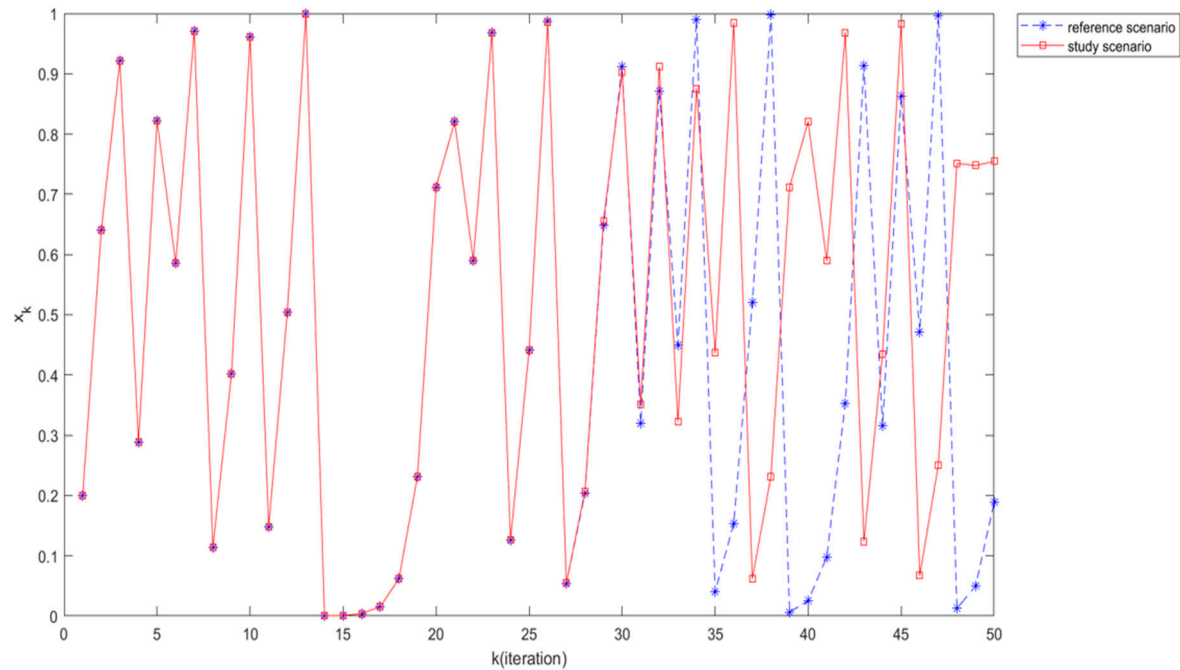
The first analysis step is the comparison of the evolution of the dynamical system trajectories in the *study scenario* with the *reference scenario* at observation point 1, as shown in Figure 7. The trajectories were obtained using  $x_0 = 0.2$ ,  $R = 4$  and  $F = 10^{-12}$ .

It can be observed that the trajectories are different. This shows that inclusion leads to a new system with modified dynamics. Further, we check whether the properties of the new system follow the statistical behavior of the reference system described by the logistic map.

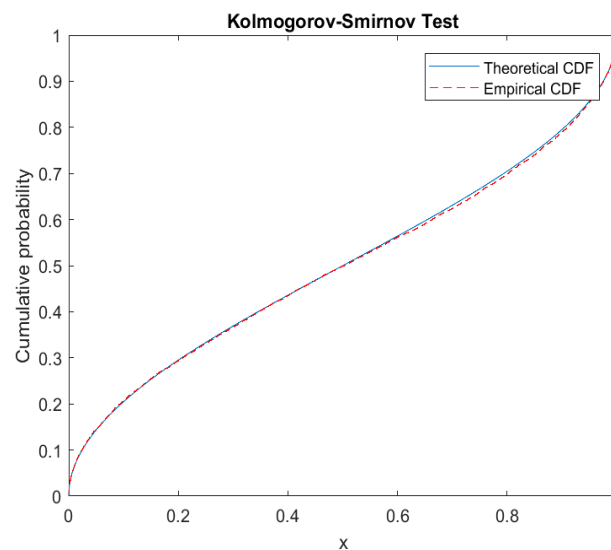
A first step in verifying that the properties are preserved is to perform the Kolmogorov–Smirnov test in the *study scenario* for the data sets obtained at observation point 1, using the method described in Section 3.2. As can be seen in Figure 8, the experimental distribution function of the new dynamical system corresponds to the theoretical one. A Monte Carlo



analysis was performed, the Kolmogorov–Smirnov test was repeated 500 times. The obtained percentage of acceptance of hypothesis  $H_0$  was 95.4%.



**Figure 7.** Comparison of dynamical system trajectories in the *study scenario* with the *reference scenario*.

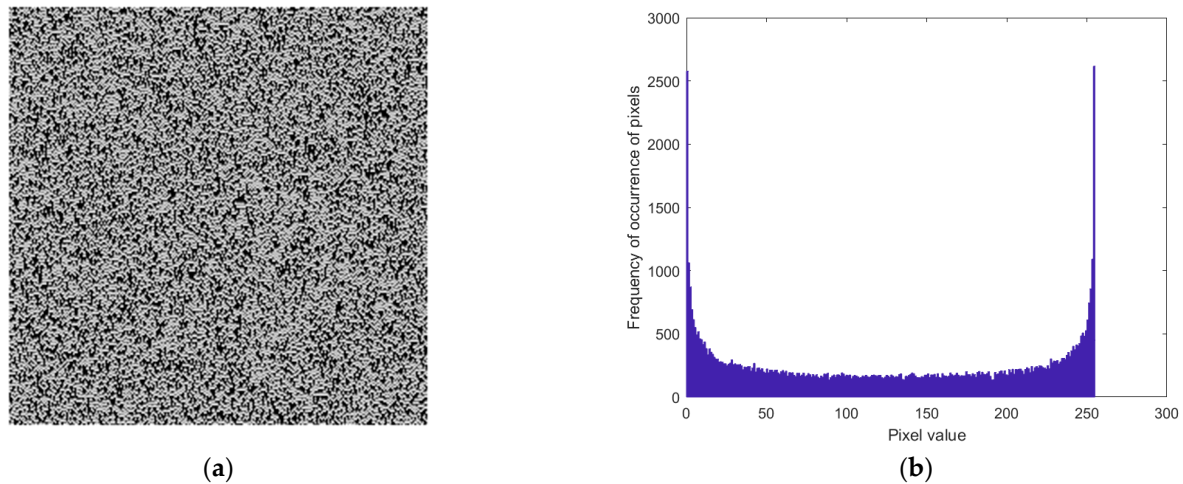


**Figure 8.** Theoretical and experimental cumulative distribution function (CDF) at iteration  $k = 150$ —*study scenario*.

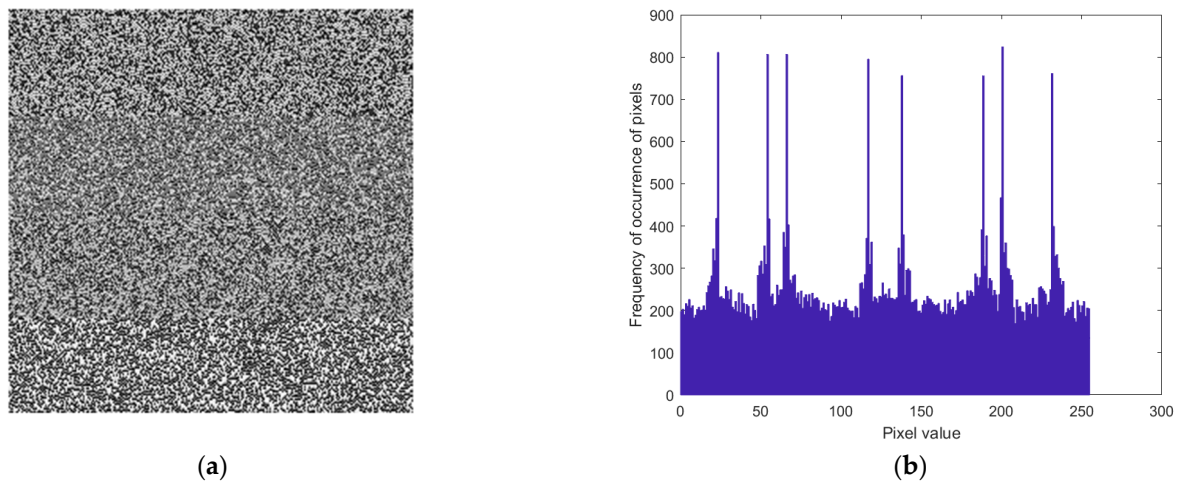
Next, we verify in observation point 2 the image obtained after discretizing the values of the new dynamical system and the corresponding histogram, illustrated in Figure 9. Analyzing the histogram in Figure 9 by comparison with the histogram obtained for the *reference scenario* in Figure 5, it can be stated that the experimental probability density of the new dynamical system is also similar to the theoretical probability density of the logistic map.

Adding now observation point 3, for the *study scenario* we can illustrate the use of the dynamical system for encryption when the input message is introduced in its dynamics (encryption by inclusion). The result is illustrated in Figure 10 and shows that a visual transformation of the input image is achieved, but with low diffusion. A similar processing

was performed in [7], the difference in the operation of the encryption scheme in the current paper being the introduction of the decision switch. Hence, the addition of this switch does not influence the performance of the encryption, but is intended to ensure the possibility of inclusion and avoid situations where the system exceeds the range of values of the logistic function  $[0, 1]$ . In Section 4, a cryptographic improvement will be made by adding mixing functions [7] to the processing scheme in Figure 2.



**Figure 9.** (a) The image at observation point 2 and (b) the corresponding histogram for the *study scenario*.



**Figure 10.** (a) The image at observation point 3 and (b) the corresponding histogram for the *study scenario*.

In conclusion, the statistical behavior of the new system obtained by message inclusion respects the 1st order probability law of the random process associated to the logistic map. Both the addition of the decision switch in the processing scheme and a good choice of the scaling factor contribute to this fact. In order to determine the impact of the scaling factor on the statistical behavior of the new dynamical system, a study is performed in the next section.

### 3.4. Determining the Upper Limit of the Magnitude of the Scaling Factor

To include the message in the evolution of the dynamical system without affecting its behavior, message scaling is required. In previous studies [5,6] the choice of scaling factor was done empirically, and no upper limit was given for it. We propose to determine the limits of the magnitude of the scaling factor. We expect the magnitude of the scaling factor to be small enough to allow the scheme to operate within the range of definition of the logistic function and not to change its statistical properties. No minimum value is given for

the lower limit. As the value of the scaling factor tends to 0, the inclusion of the message no longer influences the evolution of the dynamical system.

For this purpose, we applied the Kolmogorov–Smirnov statistical test using the experimental data from observation point 1 for a set of  $F$  values in the *study scenario* where we do not have external message. The experimental data set was obtained under the same conditions described in the presentation of the Kolmogorov–Smirnov test in Section 3.2. To decide on the results, we performed a Monte Carlo analysis by repeating the Kolmogorov–Smirnov test 500 times for each value of  $F$ . Considering the significance level of the test  $\alpha = 0.05$ , the acceptance rate of the test is  $[0.93, 0.97]$ .

Analyzing the results obtained in Table 1, it can be stated that the experimentally determined upper limit of the scaling factor is  $10^{-8}$ , since for values less than or equal to this value, the Kolmogorov–Smirnov test had an acceptance proportion of the  $H_0$  hypothesis in the range  $[0.93, 0.97]$ .

**Table 1.** Monte Carlo analysis of Kolmogorov–Smirnov (K–S) test results for a set of  $F$  values.

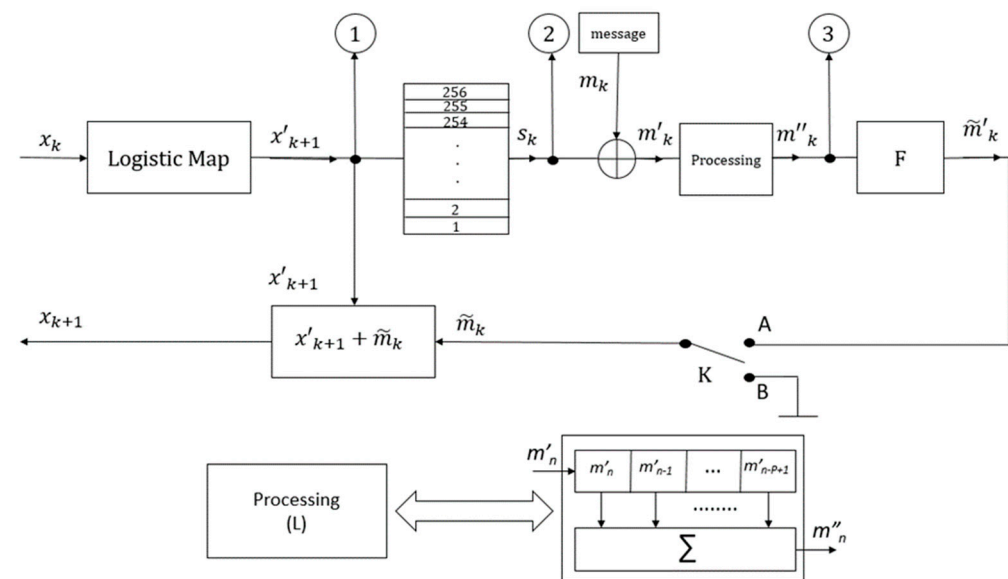
F	$10^{-5}$	$10^{-6}$	$10^{-7}$	$10^{-8}$	$10^{-9}$	$10^{-10}$	$10^{-11}$	$10^{-12}$	$10^{-13}$
K–S	0%	26.4%	91.2%	94.6%	95.2%	96.4%	94.6%	94.8%	95.8%

Therefore, considering that the acceptance proportion of the  $H_0$  hypothesis is in the range  $[0.93, 0.97]$  for values of  $F \leq 10^{-8}$ , it can be concluded that simply using the decision switch alone—without a proper choice of the magnitude of the scaling factor—is not sufficient to not disturb the statistical behavior of the dynamical system.

Thus, this study contributes to a correct choice of the scaling factor that, together with the use of the decision switch, contributes to the proper functionality of the encryption scheme based on the logistic map for  $R = 4$ .

#### 4. An Analysis of the Statistical Behavior of the Dynamical System for Cryptographic Applications

Message inclusion is a technique used for cryptographic applications [5,6]. To improve encryption performance, internally applied mixing functions have been introduced into the scheme in Figure 2, resulting in a new encryption scheme illustrated in Figure 11.



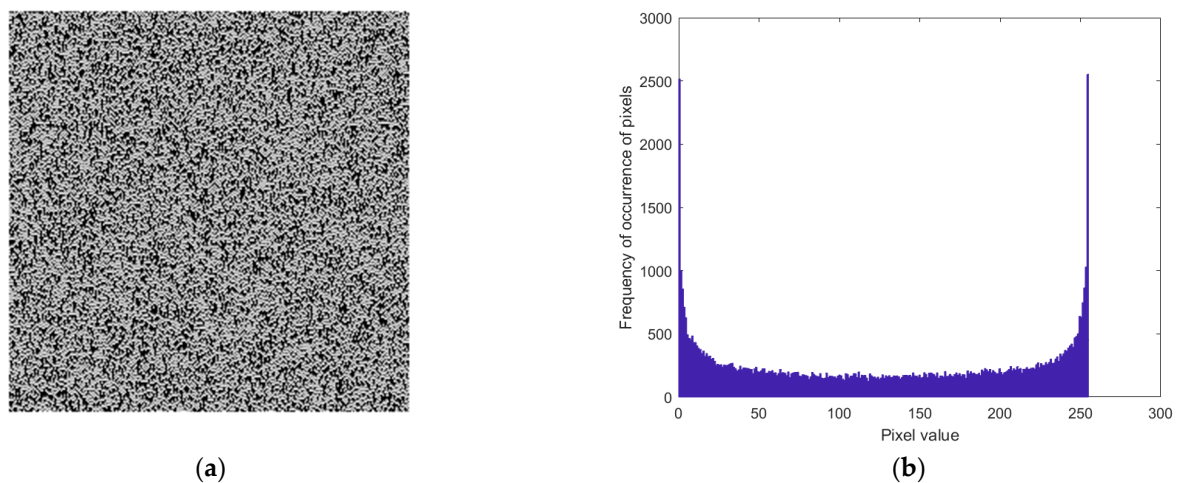
**Figure 11.** Enhanced encryption scheme.

The introduction of the internally applied mixing function was proposed in [7] and led to improved encryption performance. The use of the mixing function in this configura-

tion results in an emphasis on diffusion and confusion properties by using only a linear averaging operation [7].

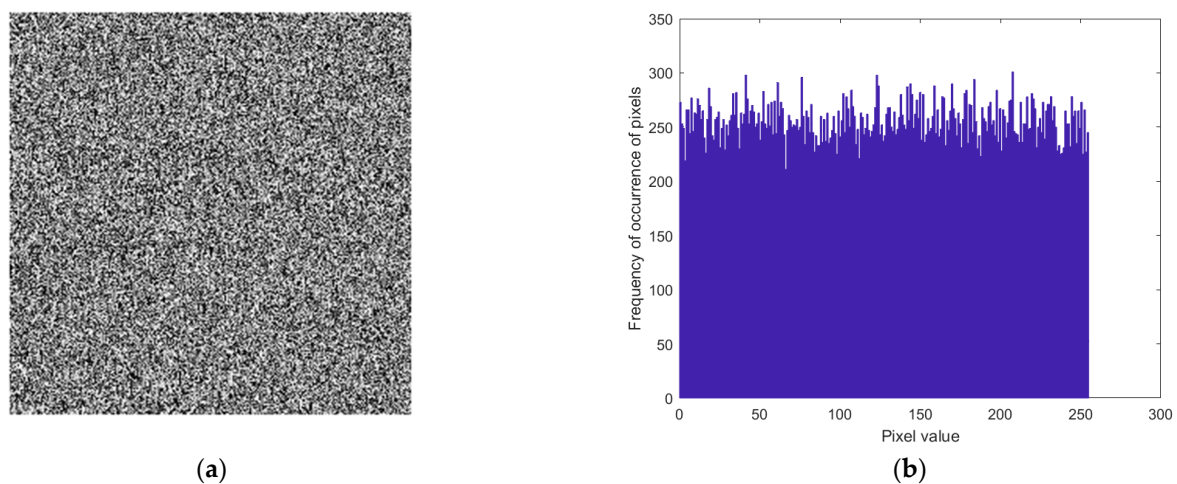
The decision switch, introduced in the current paper, is intended to ensure the correct operation of the scheme by keeping the values of the chaotic system in the reference interval (the definition interval of the dynamical system operation). Furthermore, through the study presented in Section 3.4, the encryption scheme is completed by giving the user the possibility to select a scaling factor from a predefined range, which allows the proper functioning of the scheme.

This scheme was evaluated using the same method as presented in Section 3.2. Thus, in observation point 1, we follow whether the probability law of the new system is affected by inclusion. A Monte Carlo analysis was performed, the Kolmogorov–Smirnov test was repeated 500 times. The obtained percentage of acceptance of the  $H_0$  hypothesis (i.e., the experimental data have the same distribution as in relation (3), the inclusion does not change the distribution law) was 95.6%. This result is also emphasized by the visualization at observation point 2. It can be noticed that the histogram of the image corresponding to the trajectory of the modified chaotic system follows the first-order probability law of the random process associated to the logistic map; a result illustrated in Figure 12.



**Figure 12.** (a) Image at observation point 2 and (b) corresponding histogram—enhanced scheme.

Figure 13 shows the encrypted image and its corresponding histogram at observation point 3. A visual inspection shows that the performance of the new system with mixing functions is clearly improved compared to the system in Figure 2.



**Figure 13.** (a) Image at observation point 3 and (b) corresponding histogram—enhanced scheme.



Therefore, by including the mixing functions and adding the decision switch, the encryption scheme proposed and analyzed in this paper is a complete one, providing optimal results from a cryptographic point of view while preserving the statistical properties of the dynamical system.

## 5. Conclusions: Main Novelties Introduced

The main novelty elements introduced are resumed:

(1) The main objective was to find out whether the dynamical system preserves the same statistical description after the inclusion of an external message. For this, an original processing scheme has been conceived, highlighting the whole information path and the main control/visualization points.

(2) The inclusion of an external message always requires a scaling factor for the dynamical system to function with this external disturbance. An interval was determined for the appropriate choice of the scaling factor so that the statistical behavior of the dynamical system does not change.

(3) The scheme contains a decision switch that controls the inclusion so as to preserve the definition domain of the dynamical system.

(4) Kolmogorov–Smirnov tests with Monte Carlo analysis were performed, demonstrating that the statistical properties of the dynamical system remain unchanged after inclusion.

(5) The analysis has also been pursued in the case when additional processing is performed, applying cryptographic mixing transformations upon the included message. In this case also, the statistical properties of the dynamical system remain unchanged; in addition, the utility for cryptography is highlighted.

The entire analysis was performed on the logistic map, but it can be extended in the same manner for other dynamical systems.

**Author Contributions:** Conceptualization, A.V.; methodology, A.V. and A.E.L.; software, A.E.L.; validation, A.E.L. and A.V.; writing—original draft preparation, A.E.L. and A.V.; writing—review and editing, A.E.L. and A.V. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Data sharing is not applicable (the article describes entirely theoretical research).

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

## References

1. Djemai, M.; Barbot, J.P.; Boutat, D. New type of data transmission using a synchronization of chaotic systems. *Int. J. Bifurc. Chaos* **2005**, *15*, 207–223. [\[CrossRef\]](#)
2. L'Hernault, M.; Barbot, J.P.; Ouslimani, A. Sliding mode observer for a chaotic communication system: Experimental results. *IFAC Proc. Vol.* **2006**, *39*, 401–406. [\[CrossRef\]](#)
3. Alvarez, G.; Amigo, J.M.; Arroyo, D.; Li, S. Lessons learnt from the cryptanalysis of chaos-based ciphers. In *Chaos-Based Cryptography: Theory, Algorithms and Applications*; Kocarev, L., Lian, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 354, pp. 257–295.
4. Millérioux, G.; Amigo, J.M.; Daafouz, J. A connection between chaotic and conventional cryptography. *IEEE Trans. Circuits Syst. Part 1 Fundam. Theory Appl.* **2008**, *55*, 1695–1703. [\[CrossRef\]](#)
5. Datcu, O.; Barbot, J.-P.; Vlad, A. New enciphering algorithm based on chaotic generalized Hénon map. In *Chaos Theory: Modeling, Simulation and Applications, Selected Papers from the 3rd Chaotic Modeling and Simulation International Conference (CHAOS2010)*, Chania, Crete, Greece, 1–4 June 2010; Skiadas, C.H., Dimotikalis, I., Skiadas, C., Eds.; World Scientific Publishing Co. Pte. Ltd.: Singapore, 2011; pp. 143–150.
6. Macovei, C.; Lupu (Blaj), A.E.; Răducanu, M. Enhanced cryptographic algorithm based on chaotic map and wavelet packets. *UPB Sci. Bull. Series C* **2020**, *82*, 119–130.
7. Lupu (Blaj), A.E.; Blaj, T.; Vlad, A. Cryptographic mixing transformations and message embedding in chaotic systems. In *Proceedings of the 2022 14th International Conference on Communications (COMM)*, Bucharest, Romania, 16–18 June 2022.
8. Chan, J.C.L.; Lee, T.H.; Tan, C.P. Secure Communication Through a Chaotic System and a Sliding-Mode Observer. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 1869–1881. [\[CrossRef\]](#)

9. Millérioux, G.; Hernandez, A.; Amigo, J.M. Conventional cryptography and message-embedding. In Proceedings of the 2005 International Symposium on Nonlinear Theory and its Applications, NOLTA 2005, Bruges, Belgium, 18–21 October 2005.
10. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. *Mathematics* **2023**, *11*, 2585. [[CrossRef](#)]
11. Zhu, F.; Wang, F.; Ye, L. Artificial switched chaotic system used as transmitter in chaos-based secure communication. *J. Frankl. Inst.* **2020**, *357*, 10997–11020. [[CrossRef](#)]
12. Baptista, M.S. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [[CrossRef](#)]
13. Vlad, A.; Ilyas, A.; Luca, A. Unifying running-key approach and logistic map to generate enciphering sequences. *Ann. Telecommun.* **2013**, *68*, 179–186. [[CrossRef](#)]
14. Vlad, A.; Luca, A.; Frunzete, M. Computational Measurements of the Transient Time and of the Sampling Distance That Enables Statistical Independence in the Logistic Map. In *Lecture Notes in Computer Science*; Gervasi, O., Taniar, D., Murgante, B., Laganà, A., Mun, Y., Gavrilova, M.L., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5593, pp. 703–718.
15. Strogatz, S.H. *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*, 2nd ed.; CRC Press: Boca Raton, FL, USA, 2018; pp. 360–364.
16. Walpole, R.E.; Myers, R.H.; Myers, S.L.; Ye, K. *Probability & Statistics for Engineers & Scientists, Global Edition*, 9th ed.; Pearson Education Limited: Essex, UK, 2016; pp. 316–319.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.