



**NATIONAL UNIVERSITY OF SCIENCE  
AND TECHNOLOGY POLITEHNICA OF  
BUCHAREST**



**Doctoral School of Electronics, Telecommunications  
and Information Technology**

**Decision No. 160 from 21-10-2025**

## **Ph.D. THESIS SUMMARY**

**Eng. Adina Elena LUPU (BLAJ)**

---

**CONTRIBUTIONS ON ENCRYPTED DATA TRANSMISSION WITH  
EMPHASIS ON THE USE OF CHAOS THEORY IN  
CRYPTOGRAPHY**

**CONTRIBUȚII PRIVIND TRANSMISIA CRIPTATĂ DE DATE CU  
ACCENT PE FOLOSIREA TEORIEI HAOSULUI ÎN CRIPTOGRAFIE**

---

### **THESIS COMMITTEE**

**Prof.dr.ing. Gheorghe BREZEANU**

National University of Science and  
Technology Politehnica of Bucharest

President

**Prof. Dr. Ing. Adriana VLAD**

National University of Science and  
Technology Politehnica of Bucharest

PhD Supervisor

**Prof.dr.ing. Victor Adrian**

**GRIGORAȘ**

Gheorghe Asachi Technical University  
of Iași

Referee

**Professeur Mihai MITREA**

Institut Polytechnique de Paris

Referee

**Conf.dr.ing. Șerban Georgică  
OBREJA**

National University of Science and  
Technology Politehnica of Bucharest

Referee

**BUCHAREST 2025**

---

# Table of contents

|   |           |
|---|-----------|
| <b>1. Introduction.....</b>   | <b>1</b>  |
| <b>2. The influence of dynamic systems in encryption schemes based on message inclusion and mixing functions .....</b>                    | <b>3</b>  |
| 2.1 Mixing transformations and message inclusion in chaotic systems .....   | 3         |
| 2.1.1 Introduction .....  | 3         |
| 2.1.2 A comparative look at dynamical systems based on the proposed scheme .....  | 4         |
| 2.1.3 Externally applied mixing transformations followed by message inclusion.....  | 6         |
| 2.1.4 Mixing transformations by including the message .....   | 7         |
| 2.1.5 Conclusions .....   | 8         |
| 2.2 Study on the influence of control parameters in the construction of mixing transformations.....                                       | 9         |
| 2.2.1 Introduction .....  | 9         |
| 2.2.2 Experimental study on the influence of control parameters.....  | 9         |
| 2.2.3 Expanding the mixing function.....  | 10        |
| 2.2.4 Conclusions .....   | 11        |
| <b>3. Analysis of the statistical behavior of a chaotic system in the case of message inclusion for applications in cryptography.....</b> | <b>12</b> |
| 3.1 Introduction .....  | 12        |
| 3.2 Description of the decision switch based scheme.....  | 13        |
| 3.2.1 Functional description of the scheme.....   | 13        |
| 3.2.2 Role of the decision switch in the processing scheme .....  | 13        |
| 3.3 Evaluating the impact of inclusion on the statistical behavior of the chaotic system  | 14        |
| 3.3.1 Description of the method of working .....  | 14        |
| 3.3.2 Experimental results.....   | 14        |
| 3.3.3 Determination of the upper limit of the scaling factor magnitude .....  | 15        |
| 3.4 Analysis of the statistical behavior of the dynamic system with a view to cryptographic applications. ....                            | 16        |
| 3.5 Conclusions .....   | 17        |
| <b>4. Comparative study upon encryption by message inclusion in chaotic systems preceded by external transformations .....</b>            | <b>18</b> |
| 4.1 Introduction .....  | 18        |
| 4.2 Operational description of the encryption scheme with external transformations .  | 18        |
| 4.3 Comparative study on encryption methods .....   | 20        |

|  |           |
|--|-----------|
| 4.3.1 Method of working.....   | 20        |
| 4.3.2 Evaluation of the encryption scheme using Hénon map .....  | 20        |
| 4.3.3 Evaluation of the encryption scheme using tent map.....  | 21        |
| 4.4 Conclusions .....  | 21        |
| <b>5. Evaluation of pRNGs based on chaotic systems using NIST tests, Lyapunov exponents, and bifurcation diagrams.....</b> | <b>22</b> |
| 5.1 Introduction .....   | 22        |
| 5.2 Further study of the pRNG based on the generalized Hénon system .....  | 23        |
| 5.3 Extension of the study to other chaos-based pRNGs from the literature.....   | 24        |
| 5.4 Conclusions .....  | 24        |
| <b>6. Conclusions.....</b>   | <b>25</b> |
| 6.1 Conclusions and original contributions .....   | 25        |
| 6.2 List of publications .....   | 27        |
| <b>Bibliography .....</b>  | <b>28</b> |



# Chapter 1

## Introduction

The main topic of the thesis entitled "Contributions on encrypted data transmission with emphasis on the use of chaos theory in cryptography" is to make new contributions in the field of chaos based cryptography, with the aim of increasing the robustness and reliability of chaos-based encryption schemes.

The influence and analysis of the behavior of chaotic systems in cryptographic applications constitutes the main research topic of this thesis. Cryptographic applications of chaotic systems are a widespread research topic in the specialized literature [1]-[3]. The most common applications of chaotic systems in cryptography are the construction of pseudo-random number generators (pRNG), for example [4]-[7] and image encryption, for example [8]-[11].

In Chapter 2, in Section 2.1 we investigate the contribution of dynamic systems in encryption schemes based on message inclusion [15], [16]. The following two issues are addressed: 1) What is the individual contribution of the dynamic system in the encryption scheme with message inclusion? and 2) How can good encryption be achieved in a framework with mixing functions and message inclusion, and given this, what is the contribution of message inclusion? For illustration, three chaotic systems commonly found in the literature were chosen: the Hénon map, the logistic map, the tent map, and the mixing functions suggested by Shannon [17] were used to perform additional processing of the message. In Section 2.2, the construction of mixing functions with chaotic systems is pursued, by taking into account the influence of control parameters on encryption performance. The chaotic systems chosen for the construction of the mixing function are the logistic map and the Hénon map, but other dynamical systems can also be used. The choice of the control parameters is of interest and was followed in this study, since in chaos-based cryptography, control parameters can be components of the secret key [18]. Increasing the security of encryption schemes based on mixing transformations with dynamic systems by expanding the key space is the main contribution of this research.

Chapter 3 statistically analyzes the properties of a chaotic system in the case of message inclusion for applications in cryptography. Preserving the properties of the chaotic system is essential throughout all the encryption process [19]. An important contribution of this chapter is the illustration of a way to statistically evaluate dynamic systems processing schemes based on message inclusion and the proposal of a framework for preserving the dynamic behavior of the system. The illustration is performed on the dynamic system described by the logistic map in image-based cryptographic applications. To verify whether or not the statistical properties of the new system obtained are affected by the inclusion, Monte Carlo analysis of the Kolmogorov-Smirnov statistical test is performed. Also, the upper limit of the magnitude of the scaling factor, for which the statistical properties of the system do not change by inclusion, is determined. The statistical analysis is also applied when cryptographic mixing functions applied internally are added to the scheme for the purpose of using this scheme in cryptographic applications. Thus, by using mixing functions and adding a decision switch, the encryption scheme proposed and analyzed in this chapter is a complete one, offering optimal results from a cryptographic point of view and, at the same time, preserving the statistical properties of the dynamic system [29].

In Chapter 4 of the thesis, a comparative study on image encryption through message inclusion in chaotic systems preceded by external processing is presented. A generic encryption scheme is proposed that includes a pre-processing block of the original message, a discretization block of the chaotic system and finally the process of message inclusion. The aim of this study is to evaluate which are the appropriate configurations of this scheme (in terms of the choice of the chaotic system used and the pre-processing method) to achieve secure and efficient image encryption. The Hénon 3D system and the tent map are proposed for analysis, and for the external pre-processing block, mixing functions and wavelet transforms. To evaluate and compare the results of the encrypted images, analysis metrics such as: histogram, correlation of adjacent pixels, and entropy are used.

Chapter 5 addresses the topic of chaos-based pseudo-random number generators in the context of their use in cryptographic applications. Starting from an existing study [14], we aim to validate the correlation between the results of the NIST tests and chaos theory metrics such as the bifurcation diagram [12] and Lyapunov exponents [13]. In Section 5.2 an analysis of the seed space (initial conditions and control parameters) for the Hénon map-based pRNG from [14] is extended by determining the Lyapunov exponents for other ranges of the control parameters and reducing the computational step. For the generated sequences, NIST tests are applied and the correspondence between the test suite results and the value of the largest Lyapunov exponent is evaluated. Section 5.3 follows the application of this method to three other chaos-based pRNGs from the literature. The correlation between chaos-specific metrics and NIST test results is being followed. Also, these pRNGs are evaluated in cryptographic applications using one-time-pad schemes, illustrated on images. The study in this chapter is useful to users of chaos-based pRNGs for establishing an extensive and correct seed selection space.

Chapter 6 presents the main conclusions, personal contributions and the list of published works.

# **Chapter 2**

## **The influence of dynamic systems in encryption schemes based on message inclusion and mixing functions**

This chapter analyzes the influence of dynamical systems in encryption schemes based on message inclusion and mixing functions. The research results were published in two conference papers [25], [26].

### **2.1 Mixing transformations and message inclusion in chaotic systems**

#### **2.1.1 Introduction**

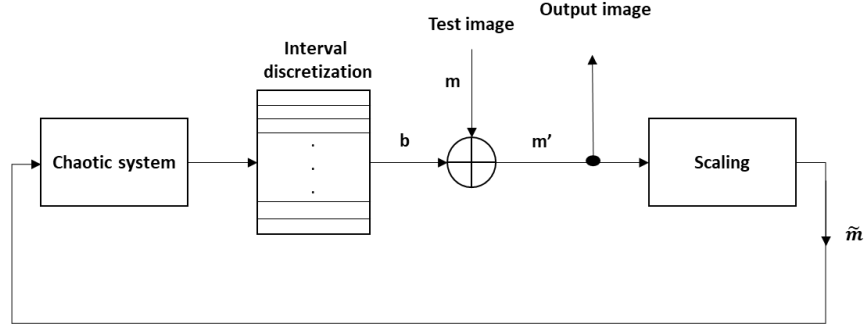
This study investigates the use of mixing functions in cryptography, also benefiting from the inclusion of the message in a dynamic system. The study addresses the following main issues: 1) what is the individual contribution of the dynamic system in the encryption scheme with message inclusion? and 2) how can good encryption be achieved in a framework with mixing functions and message inclusion and under these conditions, what is the contribution of message inclusion?

The results of this research can be used in chaos-based cryptographic applications [27], or for building mixing functions. The study is exemplified on images, but can also be applied to other multimedia content. The three chaotic

systems selected for the study are: the Hénon map [31], logistic map [12] and tent map [32].

### 2.1.2 A comparative look at dynamical systems based on the proposed scheme

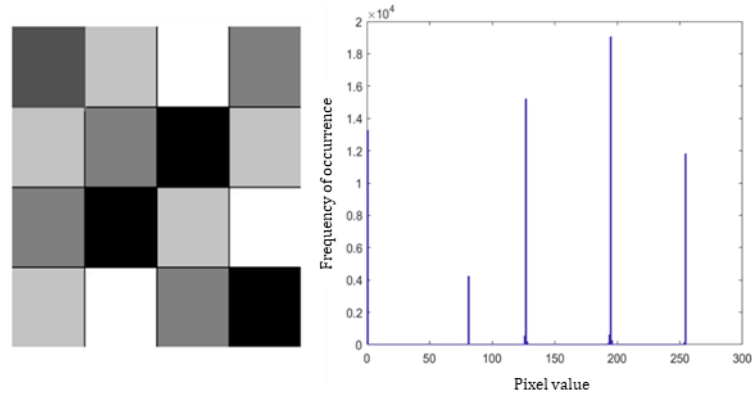
Next, the independent performance of the three previously described chaotic systems in image processing is evaluated and compared. For this study, the following scheme illustrated in Figure 2.1 was proposed.



**Figure 2.1** Proposed processing scheme (with message inclusion)

The operation of the processing scheme is described by the following steps. Starting from a set of initial conditions, the chaotic system is iterated. At each iteration, the output value of the chaotic system is transformed into a byte,  $b$ . A bitwise XOR operation is performed between the byte  $b$  and the 8-bit representation of a pixel in the message,  $m$ . The result of the XOR operation, denoted by  $m'$ , is considered the output of the processing scheme. The result  $m'$  is scaled by a factor  $v$ . The processed and scaled message is included in the evolution of the chaotic system and the iteration of the system continues.

For illustration, a test image with low entropy was chosen, illustrated in Figure 2.2.

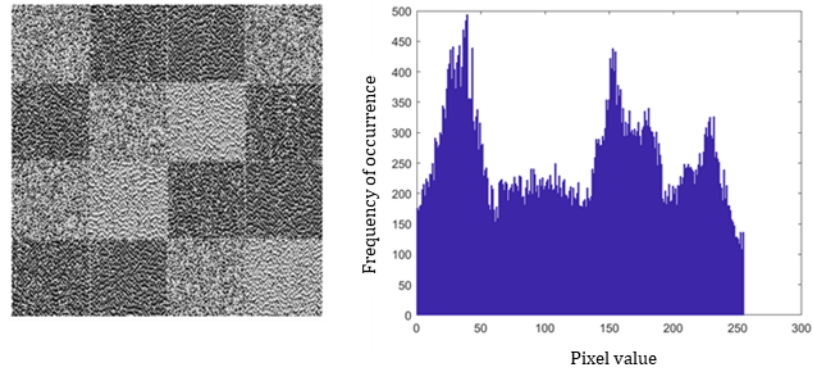


**Figure 2.2** The test image and its corresponding histogram

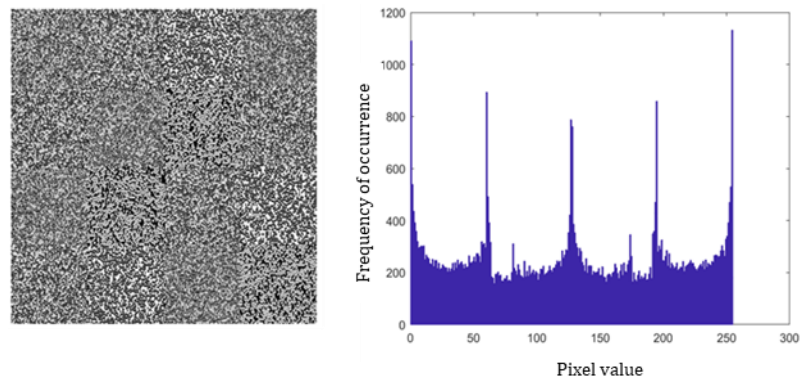
The results of image processing using each of the three chaotic systems are shown in Figure 2.3, Figure 2.4 and Figure 2.5. This processing step is illustrated only to highlight the contribution of the dynamic system by including the message. A



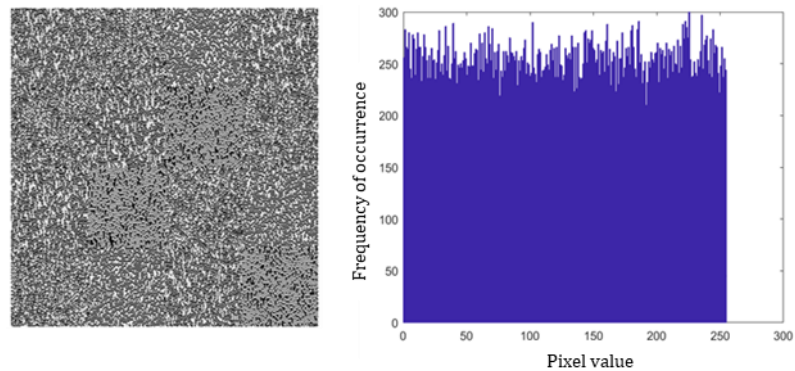
visual transformation can be observed as a result, more pronounced for the logistic map and the tent map and less pronounced for the Hénon map.



**Figure 2.3** The encrypted (processed) image using the Hénon map and the corresponding histogram



**Figure 2.4** The encrypted (processed) image using the logistic map and the corresponding histogram



**Figure 2.5** The encrypted (processed) image using the tent map and the corresponding histogram

### 2.1.3 Externally applied mixing transformations followed by message inclusion

The problem of lack of diffusion, observed previously, is addressed by adding a preprocessing block based on Shannon's suggestions, using mixing transformations [17]. The test image in Figure 2.2 is processed using the following chain of transformations:

$$T_k F S_j \quad (2.1)$$

where  $T_k$  and  $S_j$  can be simple transposition or substitution ciphers, followed by the mixing function  $F$ , which ensures diffusion and confusion. The inclusion process can be considered as the final point of the encryption chain, in which the dynamic system acts as a substitution method. For the mixing function  $F$ , we first consider a simplified formula:

$$F = SLT \quad (2.2)$$

and then we extend it according to C.E. Shannon's suggestions [17]:

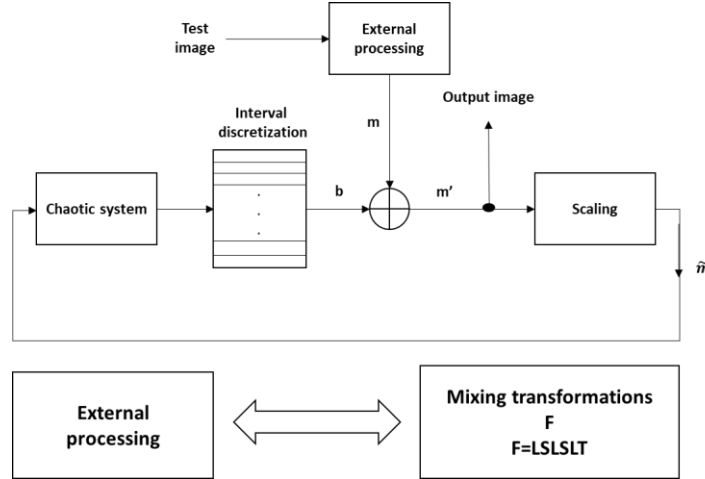
$$F = LSLSLT \quad (2.3)$$

where  $T$  and  $S$  represent here very simple transposition and substitution techniques, and  $L$  is a linear averaging operator, built based on Shannon's suggestions and applied in the form described in [28]:

$$y(j) = \sum_{i=0}^{P-1} x_{j+i} \bmod q; j=1, \dots, N-P \quad (2.4)$$

and for the last  $P$  characters (pixels),  $y(j) = x(j)$ ,  $j=N-P+1, \dots, N$ .

The encryption scheme with externally applied mixing transformations and message inclusion is exemplified in Figure 2.6.



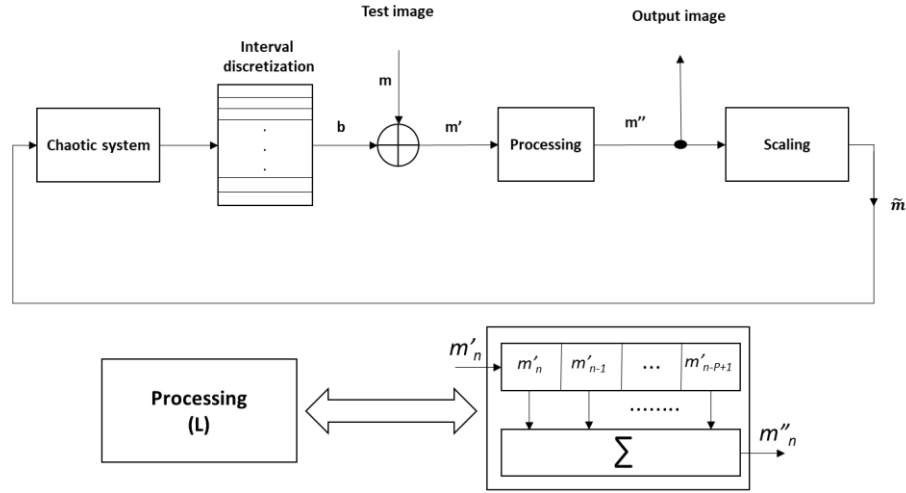
**Figure 2.6** Processing scheme with externally applied mixing transformations followed by message inclusion

The experimental study showed that the encryption performance improved significantly when using extended mixing functions (2.3), the resulting histograms are uniform regardless of the chaotic system used. At this stage, the role of the dynamic

system is that of a block cipher in the extension of mixing transformations, in which the initial conditions and control parameters are part of the secret key.

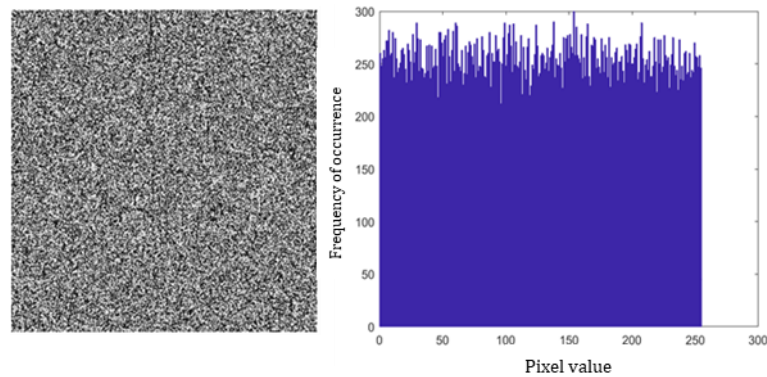
### 2.1.4 Mixing transformations by including the message

In this section the mixing function is implemented internally. Only the linear averaging operator  $L$  is used, the rest of the transformations being provided by the dynamic system which functions as a multiple substitution. This processing scheme is illustrated in Figure 2.7.

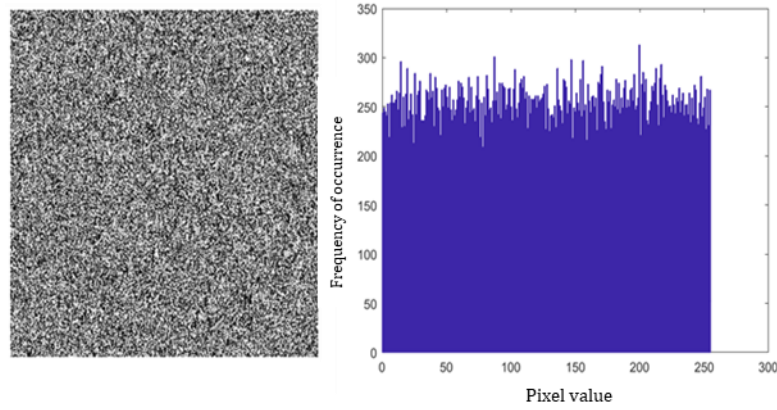


**Figure 2.7** Processing scheme with internally applied mixing transformations

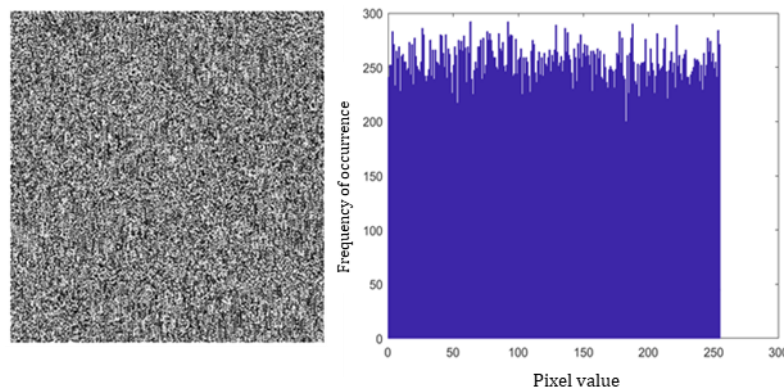
The results are shown in Figure 2.8, Figure 2.9 and Figure 2.10. The scheme with internally applied mixing transformations provides enhanced diffusion and confusion, regardless of the chaotic system used. This scheme is more efficient than the one in Section 2.1.3, because the mixing function consists of a single linear averaging operation.



**Figure 2.8** The encrypted image with internally applied mixing functions for the Hénon map and corresponding histogram



**Figure 2.9** The encrypted image with internally applied mixing functions for the logistic map and corresponding histogram



**Figure 2.10** Encrypted image with internally applied mixing functions for the tent map and corresponding histogram

### 2.1.5 Conclusions

The study showed that there are some differences between the dynamic systems in which the message inclusion is performed. These differences are attenuated as cryptographic mixing functions that increase confusion and diffusion are added to the processing scheme. A different construction of the mixing functions is proposed, keeping only the linear averaging operator,  $L$ , from Shannon's suggestions, the rest of the transformations being ensured by the contribution of the dynamic system. Thus, a result was obtained that may be interesting from the perspective of obtaining efficient mixing functions using the direct participation of the dynamic system in the architecture of these functions.

## 2.2 Study on the influence of control parameters in the construction of mixing transformations

### 2.2.1 Introduction

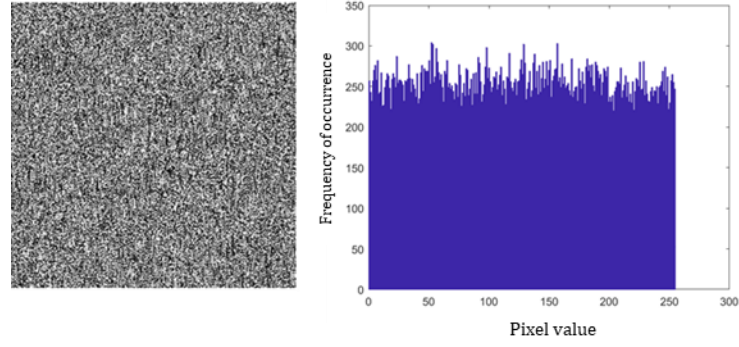
The contribution of this study is to experimentally evaluate the behavior of the encryption schemes described in 2.1.2 and 2.1.4 for different values of the control parameters, thus increasing the secret key space. It is also proposed to build an extended mixing function to improve the security of the encryption scheme. The chaotic systems analyzed are the logistic map and the Hénon map. Other values of the control parameters were chosen than the usual ones in the literature, for which the dynamic system has chaotic behavior: for the logistic map  $R \in \{3.7, 3.8, 3.9\}$ , and for the Hénon map, the control parameter pairs  $(a, b) \in \{(1.5, 0.1); (1.6, 0.1); (1.7, 0.1)\}$ .

### 2.2.2 Experimental study on the influence of control parameters

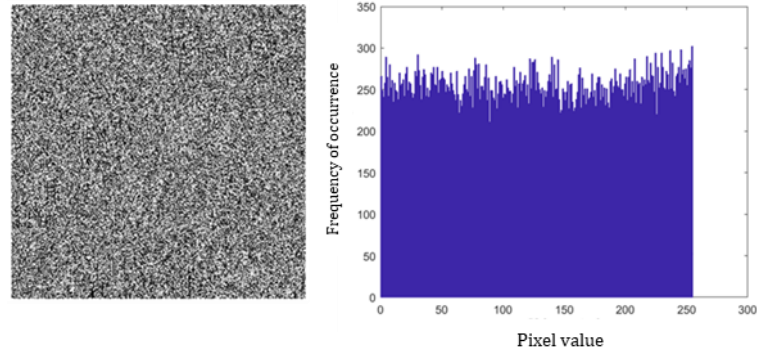
The study is analyzed progressively in two scenarios. In the first scenario, the individual contribution of the dynamic system to the encryption process is evaluated. In the second scenario, the dynamic system works as part of the mixing function. In both cases, the processing schemes used are those in [25], described in the sections 2.1.2 and 2.1.4.

For the first scenario, it was observed that for both Hénon map and logistic map, the role of the dynamical system is not significant for the selected control parameter values. Diffusion and confusion of the encrypted image are absent. The individual contribution of the dynamic system in image encryption is low even if the system operates in the chaotic regime.

In the second scenario, a linear averaging operation  $L$  is introduced which together with the chaotic system forms a new mixing function  $F = SL$  where the substitution is ensured by the XOR operation which is influenced by the values of the dynamic system. The experimental results obtained for the logistic function are illustrated in Figure 2.11, and those for the Hénon function in Figure 2.12. We can observe that the pixel distribution is uniform for the logistic map  $R = 3.9$  and for the Hénon map for the pair  $(a, b) = (1.7; 0.1)$ . For the other values of the control parameters considered in the study, the histogram of encrypted images does not show a uniform distribution.



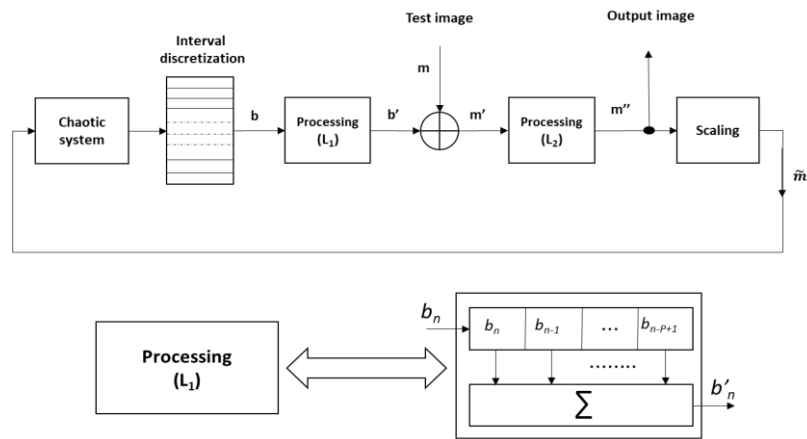
**Figure 2.11** Scenario 2 results for the logistic map:  $R=3.9$



**Figure 2.12** Scenario 2 results for the Hénon function:  $a=1.7$

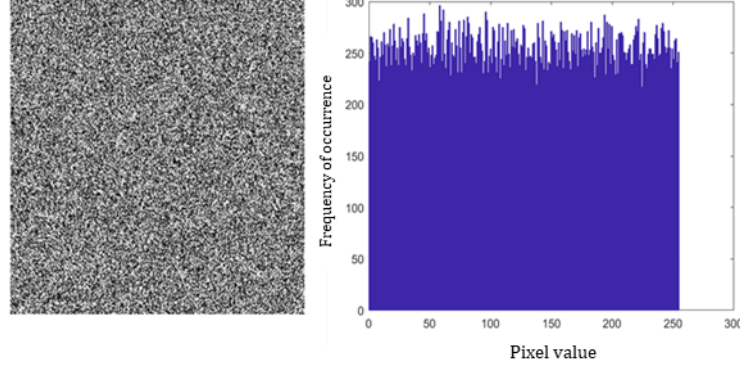
### 2.2.3 Expanding the mixing function

To obtain a good encryption for all values of the evaluated control parameters, a new linear averaging operation  $L$  is introduced into the processing scheme, obtaining the scheme in Figure 2.13. This operation is introduced before the substitution operation. Thus, a new mixing function defined as  $F = LSL$  is obtained.

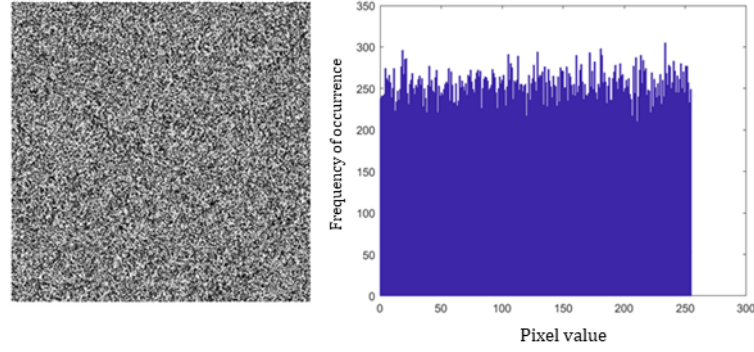


**Figure 2.13** Processing scheme with extended mixing function

The results of encrypting the input image are shown in Figure 2.14 for the logistic map for  $R = 3.7$  and in Figure 2.15 for the Hénon map for the pair  $(a, b) = (1.5, 0.1)$ . By extending the mixing function with one more  $L_I$  linear averaging operation, the encryption results are good for the entire set of considered control parameters.



**Figure 2.14** Extended function results for the logistic map:  $R=3.7$



**Figure 2.15** Extended function results for the Hénon map:  $a=1.5$

## 2.2.4 Conclusions

When the processing is ensured only by the chaotic system, it can be observed that the encryption results are different depending on the choice of the control parameter, and the image encryption is weak even if the system operates in the chaotic regime. By adding a linear averaging operation  $L$  in the processing scheme, the experimental results show that the choice of control parameters no longer influences the encryption results to the same extent, but the results can be improved. Finally, the processing scheme is improved by using two linear averaging operations and a substitution, thus obtaining an extended mixing function  $F = LSL$  that gives good performance for different values of the control parameters. The security of the encryption scheme is thus increased by increasing the key space. These results encourage the use of other chaotic systems in the construction of mixing functions.



## **Chapter 3**

# **Analysis of the statistical behavior of a chaotic system in the case of message inclusion for applications in cryptography**

In this chapter, a statistical analysis of the behavior of a dynamic system in the case of message inclusion is performed. The research results were published in a journal article [29].

### **3.1 Introduction**

Preserving the properties of the chaotic system is essential throughout the encryption process [19]. The extent to which the behavior of the dynamical system is affected by inclusion is important. Thus, the main objective of the research presented in this chapter is to clarify the impact of inclusion on the statistical behavior of the chaotic signal. All detailed analysis is performed on an original encryption scheme. In the proposed scheme, the dynamic system chosen is the logistic function, because it is illustrative for statistical analysis by referring to the knowledge of the probability law for  $R = 4$  (probability density and distribution function are known).



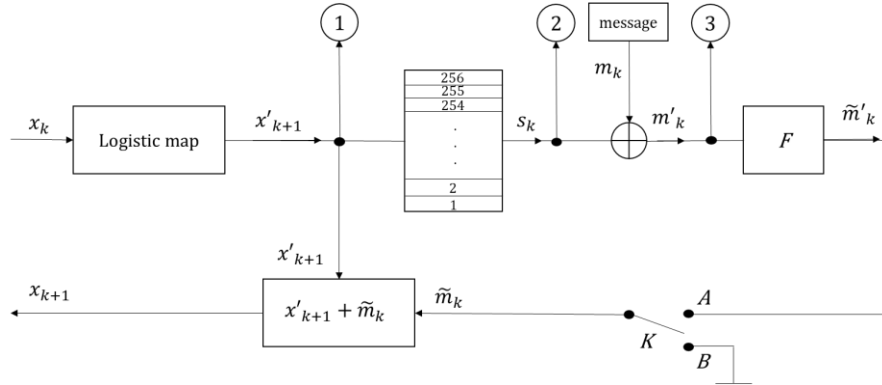
## 3.2 Description of the decision switch based scheme

### 3.2.1 Functional description of the scheme

In Figure 3.1, at each iteration, a byte  $s_k$  is associated with the output  $x'_{k+1}$  of the chaotic system. A bitwise XOR operation is performed between  $s_k$  and the  $m_k$  byte of the input message. The byte  $m'_k$  is obtained, representing the output of the processing scheme. The byte  $m'_k$  is converted to an integer and scaled by the factor  $F$ , so that it can be reintroduced into the evolution of the dynamical system. The value obtained is denoted by  $\tilde{m}'_k$ . The next step is to make the decision to include the processed and scaled message  $\tilde{m}'_k$ . The decision depends on the value of  $x'_{k+1}$ .

$$\tilde{m}_k = \begin{cases} \tilde{m}'_k, & \text{if } x'_{k+1} \in [0, D) \\ 0, & \text{if } x'_{k+1} \in [D, 1) \end{cases}, \quad \text{where } D = 1 - 255 \cdot F \quad (3.1)$$

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



**Figure 3.1** Message inclusion scheme

### 3.2.2 Role of the decision switch in the processing scheme

To ensure that the dynamic 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 within the domain of definition  $[0, 1]$  of the logistic function. For this reason, a decision switch  $K$  was introduced into the processing scheme which is activated by the decision threshold  $D$ . This switch controls the inclusion and determines the values of  $\tilde{m}_k$ . Thus:

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

- If  $x'_{k+1} \in (0, D)$ , then  $\tilde{m}_k = \widetilde{m}'_k = m'_k \cdot F$  inclusion is made; switch  $K$  is in position  $A$

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

### 3.3 Evaluating the impact of inclusion on the statistical behavior of the chaotic system

#### 3.3.1 Description of the method of working

We will first consider that the external message value is 0 and the inclusion loop is not taken into account (switch  $K$  in Figure 3.1 is in position  $B$ ). This scenario represents the *reference scenario*, because in this case the scheme represents the dynamic system described by the logistic map without any other intervention. The results of this scenario (the observation points marked on the scheme with **1** and **2**) will be used for comparison in the study scenario that will consider the impact of the dynamic system by inclusion.

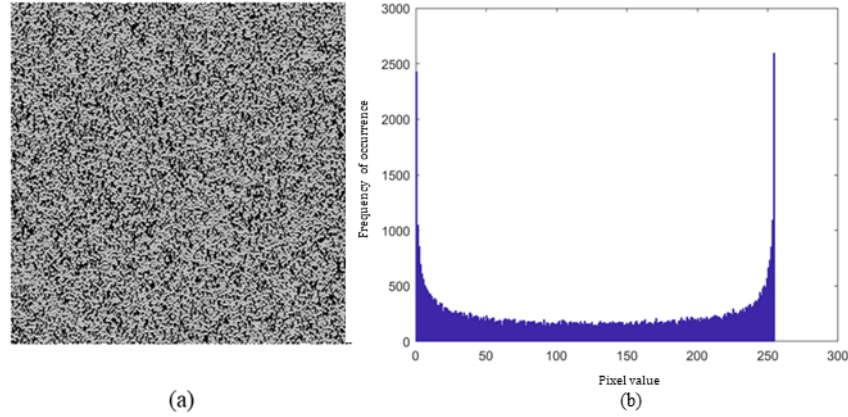
At observation point **1**, we can follow the random process associated with the logistic function, more precisely, we follow the trajectories (particular realizations of the random process). The analysis follows whether the inclusion affects the probability law of the chaotic system by performing a Monte Carlo analysis of the Kolmogorov-Smirnov test. In this study, we chose  $N = 10000$  trajectories,  $k = 150$  and the statistical significance threshold of the Kolmogorov-Smirnov test,  $\alpha = 0.05$ . According to the estimation theory [30], for  $\alpha = 0.05$  and using the Monte Carlo analysis by repeating the statistical test for  $L = 500$  times, the interval of accepted proportions is  $[0.93; 0.97]$ .

At 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 and analyze the corresponding histogram. At observation point **3** we visually inspect the output image of the encryption scheme and its histogram.

#### 3.3.2 Experimental results

For the *reference scenario*, the percentage of acceptance of the hypothesis  $H_0$  obtained was 94.8%. This is within the estimation interval  $[0.93; 0.97]$ . Therefore, we can state with a statistical confidence of 95% that the experimental data come from the theoretical probability law of the logistic function for  $R = 4$ .

For the *study scenario*, we consider the external message to be an image of size 256 x 256 pixels. For the study scenario, the percentage of acceptance of the hypothesis  $H_0$  obtained was 95.8%. Analyzing Figure 3.2, it can be stated that the experimental probability density of the new dynamic system is similar to the theoretical probability density of the logistic map.



**Figure 3.2** (a) Image at observation point 2 and (b) corresponding histogram – study scenario

In conclusion, the statistical behavior of the new system obtained by message inclusion respects the first-order probability law of the random process associated with the logistic map. The addition of the decision switch in the processing scheme, as well as a good choice of the scaling factor contributes to this fact.

### 3.3.3 Determination of the upper limit of the scaling factor magnitude

We seek to determine the limits of the magnitude of the scaling factor,  $F$ , so that it allows the scheme to operate within the definition range of the logistic function and does not change its statistical properties. For a set of values of  $F$ , we applied a Monte Carlo analysis by repeating the Kolmogorov-Smirnov test 500 times for each value of  $F$ .

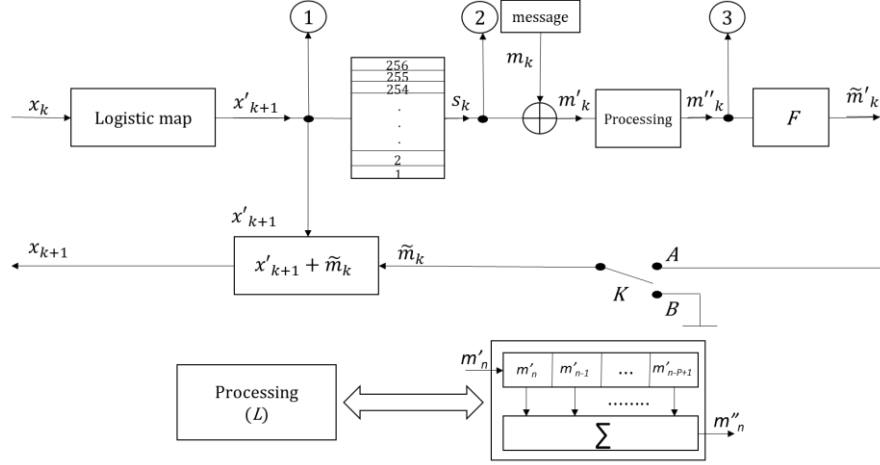
**Table 3.1** Monte Carlo analysis of Kolmogorov-Smirnov (K-S) test results for different scaling factor sizes

| 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%      |

Analyzing the results obtained in Table 3.1, it can be stated that the upper limit of the scaling factor determined experimentally is  $10^{-8}$ .

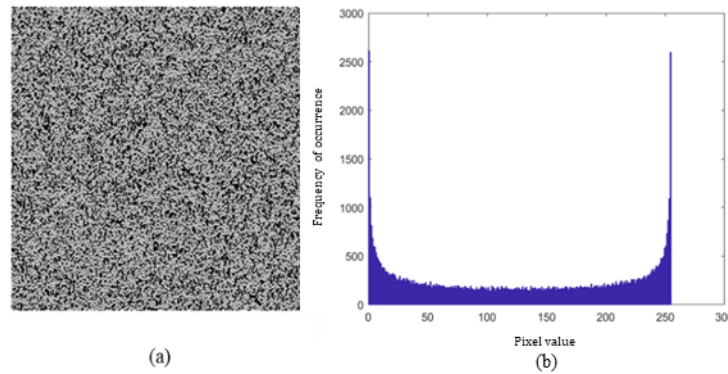
### 3.4 Analysis of the statistical behavior of the dynamic system with a view to cryptographic applications.

Internally applied mixing functions were introduced into the scheme in Figure 3.1 to improve encryption performance, resulting in a new encryption scheme illustrated in Figure 3.3.

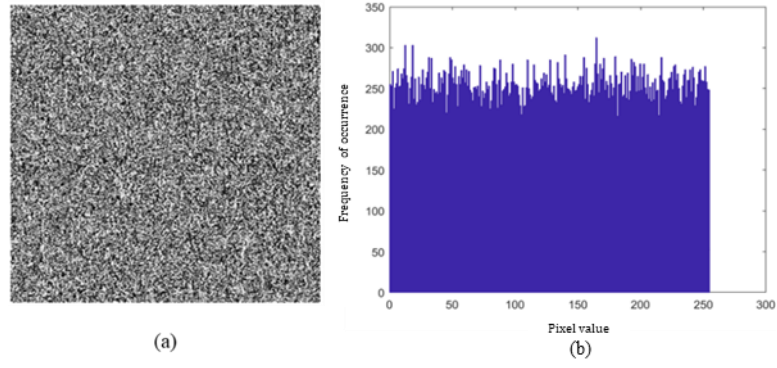


**Figure 3.3** Processing scheme with internally applied mixing transformations

Using the mixing function in this configuration results in an enhancement of the diffusion and confusion properties by using only a single linear averaging operation [25]. The percentage of acceptance of the  $H_0$  hypothesis obtained was 95.2%. In Figure 3.4 it is observed that the histogram of the image from observation point 2 follows the first order probability law of the logistic function. By visually inspecting Figure 3.5 it can be stated that the performances of the encryption scheme that includes mixing functions are visibly improved compared to those of the encryption scheme illustrated in Figure 3.1.



**Figure 3.4** (a) Image at observation point 2 and (b) corresponding histogram for the improved scheme



**Figure 3.5** (a) Image at observation point 3 and (b) corresponding histogram for the improved scheme

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

### 3.5 Conclusions

In conclusion, the main contribution of this study is to propose a functional and analytical framework for the proper operation of chaos-based encryption schemes using the message inclusion technique. The applicability in cryptography of the proposed processing scheme is also emphasized.

# **Chapter 4**

## **Comparative study upon encryption by message inclusion in chaotic systems preceded by external transformations**

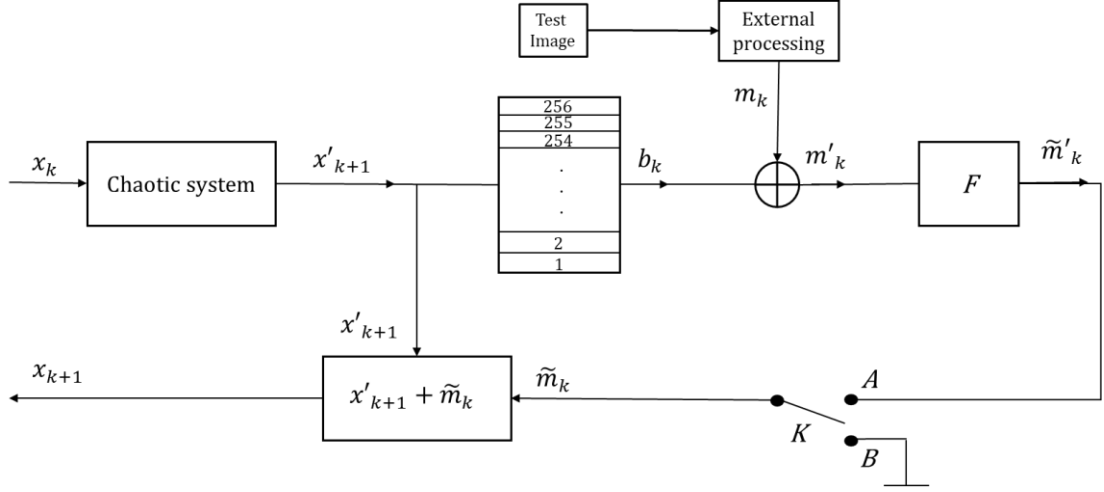
### **4.1 Introduction**

This chapter of the thesis presents a comparative study on image encryption using message inclusion in chaotic systems preceded by external transformations. The two external transformation methods analyzed are based on the wavelet transform and mixing transformations using linear averaging operations. The chaotic systems used are the Hénon map and the tent map, also presented in Chapter 2.

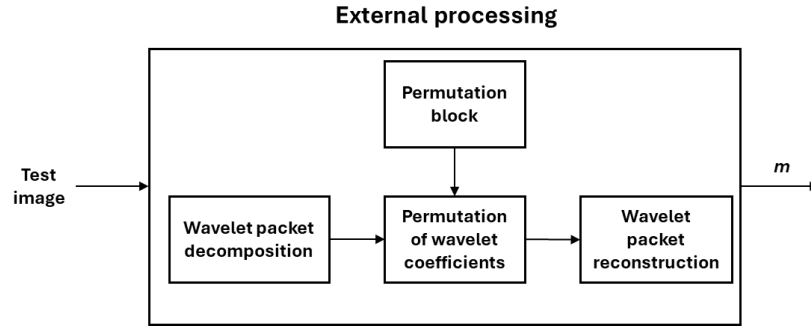
### **4.2 Operational description of the encryption scheme with external transformations**

The generic encryption scheme is shown in Figure 4.1. Initially, the input image is introduced into a pre-processing block which results in a new image, hereafter called the pre-encrypted image. The chaotic systems used are the Hénon map and the tent map. The details of the scheme are described in Section 3.2. The two pre-encryption methods are detailed further. Figure 4.2 illustrates the pre-processing method using the wavelet transform. The first step in external pre-processing using the wavelet transform is test image decomposition into 7-level using the Haar wavelet function. The coefficients of the wavelet packets are permuted using a randomly generated

permutation using the logistic function. The pre-encrypted image is obtained following reconstruction using permuted wavelet packets.

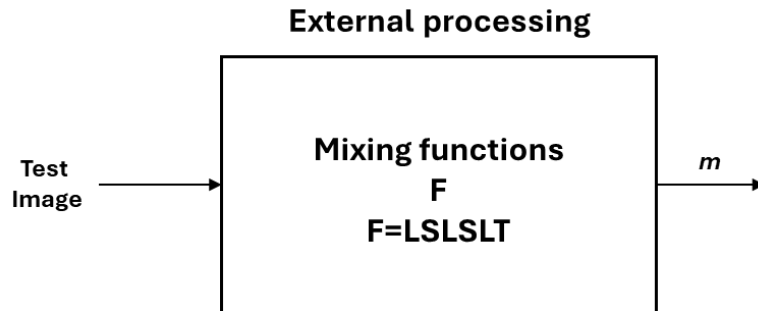


**Figure 4.1** Generic encryption scheme



**Figure 4.2** External processing using the wavelet transform

The second pre-processing method using mixing transformations is illustrated in Figure 4.3. The test image is pre-encrypted using the mixing function proposed by Shannon [17]. The functional description of the mixing transformations is given in Section 2.1.3.



**Figure 4.3** External processing using mixing transformations

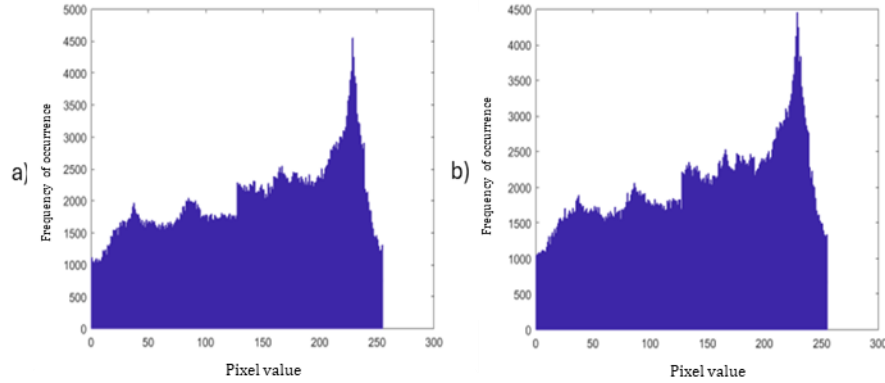
## 4.3 Comparative study on encryption methods

### 4.3.1 Method of working

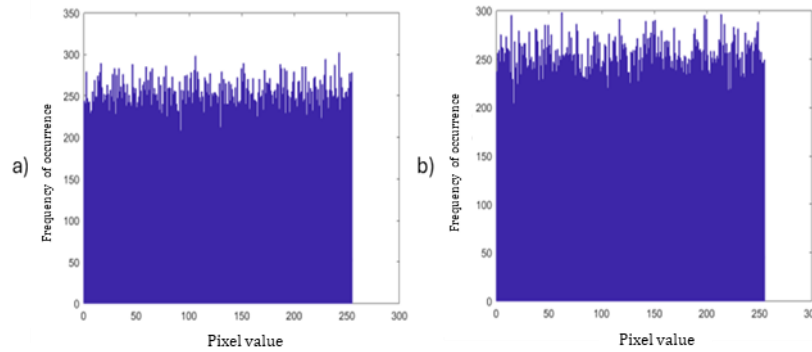
The encryption results are evaluated using different configurations of the generic scheme. Two different images of size 256x256 pixels, with low entropy and high entropy, were used as test images. For the logistic function used to permute the wavelet coefficients, we considered the control parameter  $R = 4$ .

### 4.3.2 Evaluation of the encryption scheme using Hénon map

The histograms of the encrypted images using the Hénon map and the two external transformation methods are shown in Figure 4.4 and 4.5. It can be noticed that the histograms corresponding to the configuration with the wavelet transform are not uniform, however when the mixing transformations were used, the pixel distribution is uniform, indicating a better encryption performance for this configuration.



**Figure 4.4** The corresponding histograms for the scheme using the wavelet transform and Hénon map: a) low entropy image; b) high entropy image

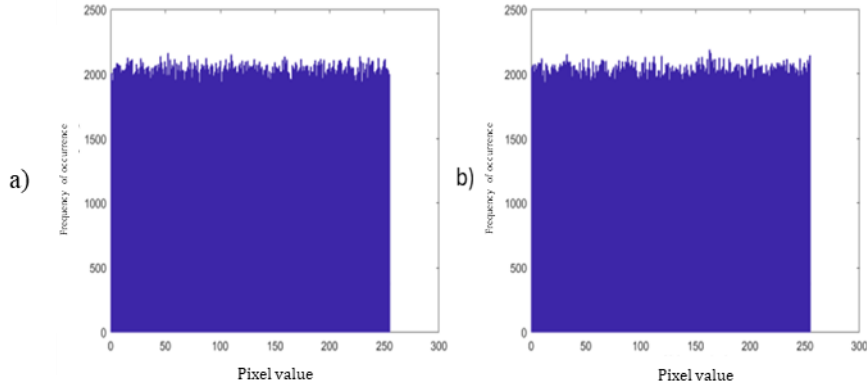


**Figure 4.5** The corresponding histograms for the scheme using mixing transformations and Hénon map: a) low entropy image; b) high entropy image

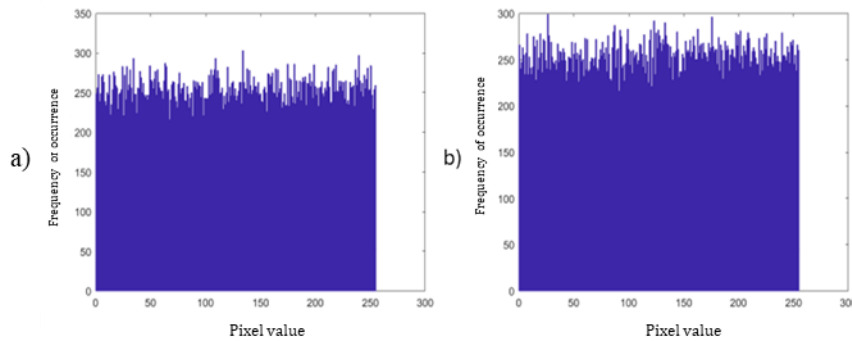


### 4.3.3 Evaluation of the encryption scheme using tent map

The performance for the scheme configuration with the tent function is evaluated. In Figure 4.6 and 4.7, the histograms for the encryption scheme with the wavelet transform configuration and respectively with the mixing transformation configuration are shown. It can be stated that in both configurations, the pixel distribution of the encrypted images is uniform.



**Figure 4.6** The corresponding histograms for the scheme using the wavelet transform and tent map: a) low entropy image; b) high entropy image



**Figure 4.7** The corresponding histograms for the scheme using mixing transformations and tent map: a) low entropy image; b) high entropy image

## 4.4 Conclusions

Encryption is performed in two stages, thus ensuring resistance to cryptographic attacks. Using the wavelet transform scheme configuration, good encryption results were obtained only for the tent map. For the configuration with mixing transformations, good results were obtained for both dynamic systems considered for inclusion. Therefore, the performance of the encryption scheme in this configuration does not depend on the image content nor on the choice of the chaotic system.

# **Chapter 5**

## **Evaluation of pRNGs based on chaotic systems using NIST tests, Lyapunov exponents, and bifurcation diagrams**

This chapter presents ways to evaluate pRNGs based on chaotic systems using various tools such as: NIST tests, Lyapunov exponents, and bifurcation diagrams. The results were presented at the "Romanian Cryptology Days Conference RCD-2019: Cryptography and Beyond, in a Connected World" and later published in a journal article in "Proceedings of the Romanian Academy", Series A [20].

### **5.1 Introduction**

The research started from the study in [14], where the authors evaluated the randomness of a chaos-based pRNG and observed a correlation between the results of NIST tests and metrics specific to chaos theory: Lyapunov exponents and the bifurcation diagram. Thus, using chaos-specific metrics could represent an easy method for evaluating chaos-based pRNGs and identifying valid work spaces (seeds). Evaluating the practical usability of this method is the main focus of this chapter. For this, the study in [14] is deepened and extended for other chaos-based pRNGs in the literature.

## 5.2 Further study of the pRNG based on the generalized Hénon system

In this chapter, we extend the range of investigation from [14]. The control parameter  $b$  of the 3D Hénon system is fixed  $b = 0.1$ , the initial conditions are  $x_0 = y_0 = z_0 = 0$  and the control parameter  $a$  varied throughout the domain of definition  $(0, 2)$ , with a step of  $10^{-3}$ .

The results showed that for the subinterval  $[0.786, 1.081]$ , the largest Lyapunov exponent ( $\lambda_l$ ) is approximately 0 which implies a stable behavior of the dynamic system. For the subinterval  $[1.4, 1.76]$ , three of the values of the largest Lyapunov exponent ( $\lambda_l$ ) are negative, therefore these values of parameter  $a$  do not form a valid pair with  $b = 0.1$ . As we decrease the variation step of the parameter  $a$ , at  $10^{-4}$ , a number of 14 values of the parameter  $a$  are observed which, together with  $b = 0.1$ , determine a periodic behavior of the system ( $\lambda_l < 0$ ). When the variation step is decreased further, at  $10^{-5}$ , the number of pairs that do not generate chaos is greater than one hundred.

The NIST test suite is run for  $b = 0.1$ ,  $x_0 = y_0 = z_0 = 0$  and  $a$  varied in  $[1.4, 1.76]$  with a step of  $10^{-3}$ . The results are summarized in Table 5.1. The number in parentheses indicates the number of failed tests for that particular test category.

**Table 5.1** NIST tests failed for  $b = 0.1$  and variable  $a$

| Failed NIST tests                  | $a \in [1.4, 1.76)$   |
|------------------------------------|---|
| Frequency                          | 1.404   |
| Block Frequency                    | 1.404, 1.427, 1.627, 1.655, 1.682   |
| CumulativeSums (2 tests)           | 1.404 ( <b>2</b> ); 1.600, 1.655, 1.682 ( <b>1</b> )  |
| Runs, LongestRun, Rank,            | 1.404, 1.655, 1.682   |
| OverlappingTemplate                | 1.481, 1.655, 1.68, 1.726   |
| Universal                          | 1.404, 1.655, 1.682   |
| FFT                                | 1.404, 1.425, 1.505, 1.655, 1.682   |
| NonOverlappingTemplate (148 tests) | 1.408, 1.411, 1.413, 1.418, 1.421, 1.423, 1.435, 1.447, 1.448, 1.451, 1.458, 1.461, 1.462, 1.486, 1.487, 1.493, 1.498, 1.502, 1.506, 1.511, 1.512, 1.514, 1.520, 1.529, 1.539, 1.544, 1.558, 1.584, 1.585, 1.594, 1.596, 1.597, 1.607, 1.623, 1.628, 1.630, 1.638, 1.641, 1.650, 1.470, 1.465, 1.658, 1.668, 1.672, 1.673, 1.679, 1.687, 1.691, 1.702, 1.727, 1.728, 1.733, 1.748, 1.753, 1.759, 1.481, 1.726 ( <b>1</b> ); 1.428, 1.523, 1.560, 1.632, 1.655, 1.682, 1.708, 1.723, 1.731, 1.537 ( <b>3</b> ); 1.404 ( <b>118</b> ) |
| ApproximateEntropy                 | 1.404, 1.578, 1.655, 1.682  |
| Serial (2 tests)                   | 1.483, 1.701 ( <b>1</b> ); 1.404, 1.655, 1.682 ( <b>2</b> )   |
| LinearComplexity                   | 1.404, 1.655, 1.682   |
| Random Excursions                  |   |

### 5.3 Extension of the study to other chaos-based pRNGs from the literature

In this section the analysis is extended to three other chaos-based pRNGs from the literature [21], [22], [23] in order to verify the assumption made in [14]. Control parameters that determine chaotic or periodic behavior were selected and NIST tests were performed on the sequences generated with these seeds. The pRNGs used are hereafter referred to as GENERATOR  $k$ ,  $k = \{1, 2, 3\}$ .

The experimental results are shown in Table 5.2. It can be seen that for GENERATORS 1 and 2 there are a number of failed tests even though the dynamic system behavior was chaotic. However, for GENERATOR 3 all NIST tests passed when the control parameter determines chaotic behavior. This result shows that the proper functioning of chaos-based pRNGs is not only influenced by the dynamic system, but also by the generator architecture and the processing performed.

**Table 5.2** Correspondence between NIST test results and pRNG control parameters for chaotic and periodic behavior

| pRNG        | Parameters           | Behavior | No. of failed NIST tests |
|-------------|----------------------|----------|--------------------------|
| GENERATOR 1 | $R = 3.9999$         | chaotic  | 31                       |
|             | $R = 3.961$          | periodic | 157                      |
| GENERATOR 2 | $R \in (3.6, 4)$     | chaotic  | 5                        |
|             | $R \in (3.3, 3.7)$   | periodic | 158                      |
| GENERATOR 3 | $a = 1.656, b = 0.1$ | chaotic  | 0                        |
|             | $a = 1.404, b = 0.1$ | periodic | 121                      |

We evaluate the performance of GENERATORS 1-3 in cryptographic applications using a one-time pad (OTP) [24] encryption scheme illustrated on images. For the values of the control parameters that determine chaotic behavior, good encryption of the images was obtained, which indicates a pseudo-random behavior of the generators. On the other hand, when we use values of the control parameters that generate periodic behavior, it is observed that the encryption results are poor. This fact shows the lack of random behavior of the pRNGs.

### 5.4 Conclusions

In conclusion, even though chaos metrics are easy to implement and provide an initial indication of the quality of the selected parameters, they do not replace analysis through NIST tests of the pRNG. However, the results obtained showed that this approach is promising and can provide a facile framework for expanding the seed value space.

# Chapter 6

## Conclusions

### 6.1 Conclusions and original contributions

The first chapter of the thesis includes the motivation and the positioning of the theme in the research field of chaos-based cryptography. The main characteristics of chaos theory are presented, highlighting its applicability in cryptography, in the construction of pRNGs and image encryption. The structure of the thesis and the content of the chapters are illustrated.

The following chapters of the thesis, 2, 3 and 4 addressed the applications of chaotic systems in image encryption by message embedding. Chapter 2 evaluated the contribution of dynamic systems in message-embedding encryption schemes. This contribution has been emphasized in two steps: initially, the message is just included in the system dynamics and later, the message is also processed with cryptographic mixing functions. When analyzing only the individual contribution of the dynamic system, the study showed that a visual image transformation is obtained and that there are differences between the chaotic systems used.

In the case of message processing with externally applied mixing functions, good encryption results were obtained for all three systems considered when an extended mixing function was used. In the case of applying the internal mixing function, the encryption scheme is more efficient, as good encryption results were observed for all chosen systems using a mixing function with a single linear averaging operation. Thus, a result was obtained that may be interesting from the perspective of obtaining efficient mixing functions using the direct participation of the dynamic system in the architecture of these functions.

The study of mixing transformations with chaotic systems is completed by evaluating the image encryption for different values of the control parameters for the logistic function and the Hénon map. By including a new linear averaging operation in the processing scheme, before the substitution operation, an extended mixing

function  $F = LSL$  was obtained, which provides good performance for different values of the control parameters. Thus, the security of the encryption scheme is enhanced by increasing the key space.

In chapter 3, the main objective pursued was to determine whether the inclusion of an external message in the evolution of the dynamical system affects its statistical properties. The research contributes theoretically to the complex characterization of the statistical behavior of the dynamic system by considering situations with message inclusion. To maintain the system output values within the definition range, the use of a decision switch in the processing scheme was proposed and an interval for the appropriate choice of the scaling factor was determined. To evaluate the impact of message inclusion on the statistical properties of the system, a Monte Carlo analysis of the Kolmogorov-Smirnov test was performed, which showed that the statistical properties of the dynamic system remain unchanged after inclusion. It has been shown that the statistical properties are preserved also when additional processing is performed by introducing a cryptographic mixing function upon the included message. Therefore, the main contribution of this study is to propose a framework and statistical analysis to ensure the correct functioning of dynamic systems in the encryption scheme based on message inclusion for image encryption.

In Chapter 4, the concepts proposed in the previous Chapters 2 and 3 were applied to construct an efficient and secure chaos-based encryption scheme applied on images. A comparative study was conducted between two external pre-processing methods and two different dynamic systems in order to choose an optimal configuration for image encryption. The applied external pre-processing methods were based on the wavelet transform and mixing transforms, respectively. The dynamic systems used were Hénon map and tent map. Encryption is performed in two stages, thus ensuring resistance to cryptographic attacks. The results showed that for the scheme with wavelet transform, good encryption results were obtained only for the tent function. However, in the case of configurations with mixing transformations, good results were obtained for both dynamic systems considered. Thus, the use of mixing functions allows for the construction of a scheme with good performance for various types of images and different dynamic systems.

In Chapter 5, there were presented possibilities of evaluating pRNGs based on chaotic systems using various tools such as NIST tests, Lyapunov exponents and bifurcation diagrams. An earlier study of the research team for a pRNG based on the Hénon map was extended. Correspondence evaluation between the NIST tests, Lyapunov exponents and bifurcation diagrams has also been performed for other chaos-based pRNGs in the literature. The study showed that chaos-specific metrics are useful tools for assessing the randomness of chaos-based pRNGs and easy to implement, but they cannot replace the statistical analysis of pRNGs. However, this approach can provide an easy framework for expanding the seed value space for a pRNG.

## 6.2 List of publications

### Journal articles:

- O. Datcu, A.E. Lupu (Blaj), T. Blaj, R. Hobincu, *NIST tests, Lyapunov exponents and bifurcation diagrams when evaluating chaos based PRNGS*, Special Issue of Proceedings of the Romanian Academy, Series A, The Publishing House Of The Romanian Academy, Vol 21, Issue 1, pp. 29-36, March 2020, **WOS: 000519765700004**
- C. Macovei, A.E. Lupu (Blaj), M. Răducanu, *Enhanced cryptographic algorithm based on chaotic map and wavelet packets*, U.P.B. Sci. Bull., Series C Vol. 82, Iss. 4, 2020, ISSN 2286-3540, **WOS: 000596151000010**
- A.E. Lupu (Blaj), A. Vlad, *A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications*, *Electronics*. 2024; 13(12):2270. <https://doi.org/10.3390/electronics13122270>, **WOS:001255765900001**

### Conference articles:

- A.E. Lupu (Blaj), T. Blaj, A. Vlad, *Cryptographic mixing transformations and message embedding in chaotic systems*, 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-5, doi: 10.1109/COMM54429.2022.9817169.
- A.E. Lupu (Blaj), *Revisiting Mixing Transformations and Chaotic Systems with a View to Cryptographic Applications*, 2024 International Symposium on Electronics and Telecommunications (ISETC), Timișoara, România, 2024, pp. 1-4, doi: 10.1109/ISETC63109.2024.10797432.

# Bibliography

- [1] L. Kocarev, *Chaos-based cryptography: a brief overview*, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001, doi: 10.1109/7384.963463
- [2] M.S. Baptista, *Cryptography with chaos*, Physics Letters A, Volume 240, Issues 1–2, 1998, Pages 50-54, ISSN 0375-9601, [https://doi.org/10.1016/S0375-9601\(98\)00086-3](https://doi.org/10.1016/S0375-9601(98)00086-3).
- [3] Lawnik, M., Moysis, L., & Volos, C. (2022). *Chaos-Based Cryptography: Text Encryption Using Image Algorithms*. Electronics, 11(19), 3156. <https://doi.org/10.3390/electronics11193156>
- [4] Hu, H., Liu, L., & Ding, N. (2013). *Pseudorandom sequence generator based on the Chen chaotic system*. in Computer Physics Communications, 184(3), 765-768.
- [5] Mohammed M. Al-Mhadawi, Ekhlas Abbas Albahrani, Sadeq H. Lafta, *Efficient and secure chaotic PRNG for color image encryption*, Microprocessors and Microsystems, Volume 101, 2023, 104911, ISSN 0141-9331, <https://doi.org/10.1016/j.micpro.2023.104911>.
- [6] O. Datcu, C. Macovei, R. Hobincu, *Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change*. Applied Sciences. 2020; 10(2):451. <https://doi.org/10.3390/app10020451>
- [7] C. Zhu, S. Li, Q. Lu, *Pseudo-random Number Sequence Generator Based on Chaotic Logistic-Tent System*, 2019 IEEE 2nd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 2019, pp. 547-551, doi: 10.1109/AUTEEE48671.2019.9033389
- [8] B. Zhang, L. Liu, *Chaos-Based Image Encryption: Review, Application, and Challenges*, Mathematics. 2023; 11(11):2585. <https://doi.org/10.3390/math11112585>
- [9] Safwan El Assad, Mousa Farajallah, *A new chaos-based image encryption system*, Signal Processing: Image Communication 41 (2016): 144-157. <https://doi.org/10.1016/j.image.2015.10.004>
- [10] Y. Pourasad, R. Ranjbarzadeh, A. Mardani, *A New Algorithm for Digital Image Encryption Based on Chaos Theory*, Entropy. 2021; 23(3):341. <https://doi.org/10.3390/e23030341>
- [11] Liu, Wenhao; Sun, Kehui; Zhu, Congxu. *A fast image encryption algorithm based on chaotic map*. Optics and Lasers in Engineering, 2016, 84: 26-36.
- [12] Steven H. Strogatz, *Nonlinear Dynamics and Chaos*, Publisher: Addison-Wesley 1994
- [13] Alan Wolf, Jack B. Swift, Harry L. Swinney, John A. Vastano, *Determining Lyapunov exponents from a time series*, Physica D: Nonlinear Phenomena, Volume 16, Issue 3, 1985, Pages 285-317, ISSN 0167-2789, [https://doi.org/10.1016/0167-2789\(85\)90011-9](https://doi.org/10.1016/0167-2789(85)90011-9).



- [14] O. Datcu, R. Hobincu, *NIST tests versus bifurcation diagrams and Lyapunov exponents when evaluating chaos-based PRNGs*, Proceedings of ITISE 2018, Granada, Spain, pp. 1640-1649
- [15] O. Datcu, J.P. Barbot, A. Vlad, *New enciphering algorithm based on chaotic Generalized Hénon map*, CHAOS THEORY, Modeling, Simulation and Applications, 2011, 143-150
- [16] Corina Macovei, Adina-Elena Lupu (Blaj), Mircea Răducanu, *Enhanced cryptographic algorithm based on chaotic map and wavelet packets*, U.P.B. Sci. Bull., Series C Vol. 82, Iss. 4, 2020, ISSN 2286-3540
- [17] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, 1949
- [18] 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.
- [19] 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
- [20] O. Datcu, A.E. Lupu (Blaj), T. Blaj, R. Hobincu, *NIST tests, Lyapunov exponents and bifurcation diagrams when evaluating chaos based PRNGs*, Special Issue of Proceedings of the Romanian Academy, Series A, The Publishing House Of The Romanian Academy, Vol 21, Issue 1, pp. 29-36, March 2020.
- [21] Patidar, Vinod & Sud, K.K. & Pareek, Narendra. (2009). *A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing*. Informatica. 33. 441-452.
- [22] Hamdi, M., Rhouma, R., & Belghith, S. (2015). *A Very Efficient Pseudo-Random Number Generator Based On Chaotic Maps and S-Box Tables*. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9, 481-485.
- [23] D. Sava, A. Vlad and R. Tataru, *A new type of keystream generator based on chaotic maps: Illustration on a Hénon generalized map*, 2014 10th International Conference on Communications (COMM), Bucharest, Romania, 2014, pp. 1-6, doi: 10.1109/ICComm.2014.6866726.
- [24] Lugrin, T. (2023). *One-Time Pad*. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. [https://doi.org/10.1007/978-3-031-33386-6\\_1](https://doi.org/10.1007/978-3-031-33386-6_1)
- [25] A. E. Lupu (Blaj), T. Blaj, A. Vlad, *Cryptographic mixing transformations and message embedding in chaotic systems*, 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-5, doi: 10.1109/COMM54429.2022.9817169.
- [26] A. E. Lupu (Blaj), *Revisiting Mixing Transformations and Chaotic Systems with a View to Cryptographic Applications*, 2024 International Symposium on

- Electronics and Telecommunications (ISETC), Timisoara, Romania, 2024, pp. 1-4, doi: 10.1109/ISETC63109.2024.10797432.
- [27] L. Kocarev, *Chaos-based cryptography: a brief overview*, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001, doi: 10.1109/7384.963463
  - [28] Adriana Vlad, Mihai Mitrea, *Cryptographic mixing transformations for image applications*, Proc. SPIE 3405, ROMOPTO '97: Fith Conference on optics, (2 July 1998)
  - [29] A.E. Lupu (Blaj), A.Vlad, *A Closer Look at the Statistical Behavior of a Chaotic System with Message Inclusion for Cryptographic Applications*, Electronics. 2024; 13(12):2270. <https://doi.org/10.3390/electronics13122270>
  - [30] 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.
  - [31] D. A. Miller, G. Grassi, *A discrete generalized hyperchaotic Henon map circuit*, Proceedings of the 44th IEEE 2001 Midwest Symposium on Circuits and Systems. MWSCAS 2001 (Cat. No.01CH37257), 2001, pp. 328-331 vol.1, doi: 10.1109/MWSCAS.2001.986179.
  - [32] A. Luca, A. Ilyas, A. Vlad, *Generating random binary sequences using tent map*, ISSCS 2011 - International Symposium on Signals, Circuits and Systems, 2011, pp. 1-4, doi: 10.1109/ISSCS.2011.5978664