Encryption/decryption methods using chaotic systems: Analysis based on statistical methods and control system theory.
Octaviana Datcu

To cite this version:

HAL Id: tel-00802659
https://tel.archives-ouvertes.fr/tel-00802659
Submitted on 27 Nov 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
FONDUL SOCIAL EUROPEAN
Investește în oameni!
Programul Operațional Sectorial pentru Dezvoltarea Resurselor Umane 2007 –2013
Proiect POSDRU/88/1.5/S/61178 – Competitivitate și performanță în cercetare prin programe doctorale de calitate (ProDOC)

UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI
Facultatea de Electronică, Telecomunicații și Tehnologia Informației
Catedra de Electronică Aplicată și Ingineria Informației

UNIVERSITÉ DE CERGY-PONTOISE
Ecole Nationale Supérieure de l’Electronique et de ses Applications
Equipe Commande des Systemes

Nr. Decizie Senat din

TEZĂ DE DOCTORAT

Procedee de cifrare/descifrare folosind sisteme haotice.
Analiză bazată pe metode statistice și teoria controlului sistemelor.

Encryption/decryption methods using chaotic systems.
Analysis based on statistical methods and control system theory.

Autor: Ing. Octaviana DATCU

<table>
<thead>
<tr>
<th>Conducător de doctorat-1</th>
<th>Prof. Dr. ing. Adriana Vlad</th>
<th>de la</th>
<th>Universitatea Politehnica din București, România</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conducător de doctorat-2</td>
<td>Prof. Jean-Pierre Barbot</td>
<td>de la</td>
<td>Université de Cergy-Pontoise, France</td>
</tr>
<tr>
<td>Referent</td>
<td>Prof. Krishna Busawon</td>
<td>de la</td>
<td>Northumbria University, U.K.</td>
</tr>
<tr>
<td>Referent</td>
<td>Prof. Dr. ing. Alexandru Șerbănescu</td>
<td>de la</td>
<td>Acad. Tehnică Militară, București, România</td>
</tr>
<tr>
<td>Referent</td>
<td>Prof. Maï Nguyen-Verger</td>
<td>de la</td>
<td>Université de Cergy-Pontoise, France</td>
</tr>
<tr>
<td>Referent</td>
<td>Prof. Dr. ing. Radu Dogaru</td>
<td>de la</td>
<td>Universitatea Politehnica din București, România</td>
</tr>
<tr>
<td>Referent</td>
<td>Prof. Christian Faye</td>
<td>de la</td>
<td>Université de Cergy-Pontoise, France</td>
</tr>
</tbody>
</table>

București, 2012
First of all, I want to express my gratitude to my Thesis Directors, Professor Adriana Vlad and Professor Jean-Pierre Barbot. They knew when to be gentle and comprehensive, as well as exigent, imperatively demanding results from my research work. I am grateful for the human quality they have shown to me during my three years of PhD Study, as well as for my Diploma Project. Their continuous wondering of how a theoretical idea can be improved to open new possibilities to contribute to the rapidly developed and optimized technology is an example for me, in my future career as a researcher and as a professor. The collaboration between my Thesis Directors allowed me to grow as an engineer, to understand the link between sciences that explain the laws of the Nature, to transform in real-life concepts notions that previously were only theory, for me.

I am deeply grateful to Mr. Roger Tauleigne, Professor at the University from Cergy-Pontoise, for his active involvement in developing my thesis. The long discussions with him have added important steps in my understanding of the physics of the phenomenon named deterministic chaos and the etymology of the notion. Thanks to him, the fact that the machine computed values are not always in conformity with the theoretical expectations, due to truncation and rounding operation afferent to the computers, become a practical notion for me. A beautiful exemplification was done in the context of an analytically described (thus deterministic) very simple map engendering a very complex (chaotic) behavior. Also, the synchronization between the two Colpitts chaotic oscillators was, in great part, possible to his helping me with the analog implementation, particularly to understand the physics underlying the behavior of the circuit. A tough task for me was to make the connection between notions that are specific to the field of statistics and the one targeting the domain of automatics, geometrical and physical interpretations of phenomena. Thanks to my Professors, a bridge was created in order to render the new research field, achieved by combining the two disciplines, into a meaningful scientific area.

I would like to thank to my Referents, Professors Mai Nguyen, Christian Faye, Khrishna Busawon, Alexandru Şerbănescu and Radu Dogaru, for the fact that they have made me the honor of accepting to be part of my jury. I am grateful for the patience with which Mr. Professor Leonid Fridman (Universidad Nacional Autonoma de Mexico, Facultad de Ingeneria, Mexico City) explained to me the technique of high order sliding-mode observers.

Imane Dilaneh, Hassiba Tagueb, Tihab el Houda Thabet, Diana Papancea, Mrs. Veronique Grillo, Mrs. Nacira Rebiai, Fernando Salinas, Karim Kemih, Hamid Hamiche, Sid Ahmed Raka, François Caudron, Hamid Hamiche, Gang Zheng, Mădălin Frunzete, Adrian Luca, Valentin Ștefănescu, Essaid Edjekouane, Mr. Malek Ghanes (Maître de Conferences, E.C.S.-Lab, E.N.S.E.A.), Mr. Professor Achour Ouslimani, and the entire E.C.S.-Lab Team, from Ecole Nationale de l'Electronique et de Ses Applications, from Cergy-Pontoise, Ile-de-France, France. They all have left traces in my life.

I appreciate my parents, Adelina and Ioan, believing in me.

Last, but not the least, I am grateful to Mr. Prof. Dr. ing. Corneliu Burileanu and to Mr. Conf. Dr. ing. Mihai Stanciu for their advices regarding my incipient career as a Teaching Assistant, for encouraging me to improve as a professional, and to morally support me when the direction seemed not to be favorable.
Contents

1 Introduction ........................................... 13
  1.1 Motivation ........................................... 13
  1.2 Structure of the Thesis ......................... 17
  1.3 Theoretical Background ....................... 19

2 The Lyapunov exponents .......................... 22
  2.1 Introduction ........................................... 22
    1 Significance of the Lyapunov exponent .......... 22
    2 The algorithm of Wolf, Swinney and Vastano .... 23
    3 An iterated map: The Hénon map ................. 24
    4 A differential system: The Lorenz system ........ 24
  2.2 The generalized Hénon map ...................... 25
  2.3 The Hitzl-Zele map .................................... 26
  2.4 A continuous time system: The Colpitts oscillator... 28
    1 Theoretical analysis of the oscillator ........ 28
    2 The Lyapunov Exponents ........................... 33

3 Observability Indexes and Observability-Singularity Manifolds 37
  3.1 Introduction ........................................... 37
    1 Observability index .................................. 37
    2 Observability singularity manifolds ............. 38
  3.2 Case study. The generalized Hénon map ........ 39
    1 Observability indexes ................................ 39
    2 Observability singularity manifolds ............. 41
  3.3 Case study. The Hitzl-Zele map .................. 42
    1 Observability coefficients ....................... 42
    2 Observability singularity hyper-surfaces ....... 43
  3.4 Case study. The Colpitts chaotic oscillator .... 47
    1 Observability indexes ............................. 47
    2 Observability singularity manifolds ............. 48

4 The minimum sampling distance to achieve independent samples from chaotic signals 53
  4.1 Introduction ........................................... 53
  4.2 The Vlad-Badea statistical independence test .... 54
  4.3 The Smirnov test ..................................... 56
  4.4 Case study. The generalized Hénon map ........ 57
    1 Transient time measurements ....................... 58
    2 Ergodicity of the generalized Hénon map .......... 61
    3 Statistical independence of random variables extracted from the generalized Hénon map .......... 62
5 A spatial investigation of chaotic attractors. 
5.1 Introduction .................................................. 68
5.2 An example: the Colpitts chaotic oscillator. ................. 69

6 An enciphering-deciphering algorithm based on the discrete generalized Hénon map. 
6.1 Introduction .................................................. 80
6.2 The Proposed Enciphering Method .......................... 83
  1 Scheme of the proposed enciphering method ................. 83
  2 Deciphering .................................................. 85
6.3 Analyze of results of the proposed enciphering algorithm 85
  1 Results of encryption of natural language text ............... 85
  2 Results when enciphering images .......................... 86
  3 A concrete example. The enciphering and the deciphering of a character. 87
6.4 Conclusions .................................................. 88

7 Chaotic synchronization 
7.1 Reconstructing the dynamics of a delayed transmitter ........ 90
  1 A chaotic delayed transmitter ............................... 91
  2 A third order sliding mode observer as the receiver of the secret message ........................... 92
  3 Experimental results. ...................................... 94
7.2 Synchronization of analog circuits via sparse measurement. .... 98

8 Conclusions 

9 Annexes 
9.1 Baptista’s cryptography with chaos ......................... 117
9.2 Different behaviors of the studied chaotic systems. ........... 119
  1 The generalized Hénon map ................................ 119
  2 The generalized Hitzl-Zele map ............................ 122
  3 The Colpitts chaotic oscillator ............................. 123
9.3 Ergodicity hypothesis for the generalized Hénon map .......... 124
List of Figures

1.1 The bifurcation diagram of the logistic map. .......................... 14
1.2 The bifurcation diagram of the logistic map, for the bifurcation parameter $r \in [1, 4]$. ...................................................... 16
1.3 Illustration of stability islands (in blue) induced by the numerical calculus, for the control parameter $r \in [3, 4]$. ......................... 17
1.4 The logistic map sequence of values for the bifurcation parameter $r = 3.97$. .......................................................... 17

2.1 The generalized Hénon map. The bifurcation parameters are $a = 1.76$ and $b = 0.1$. The initial conditions are $x_1(0) = 0.8147, x_2(0) = 0.9057, x_3(0) = 0.1269$. The phase space (left) and the evolution of its first state, $x_1(k)$, $k \in \{0, N\}, N = 10000$ (right). ........................................ 26
2.2 Two trajectories for the generalized Hénon map with $a = 1.76$ and $b = 0.1$. With solid blue line, the sequence starting from $x_1(0), x_2(0), x_3(0)$. With dashed red line, the trajectory with initial conditions $x_1'(0) = x_1(0) + 0.01, x_2'(0) = x_2(0), x_3'(0) = x_3(0)$ ........................................ 26
2.3 The generalized Hénon map. The spectrum of the Lyapunov exponents when the parameter $a = 1.76$ is kept fixed (left) or the parameter $b = 0.1$ is kept fixed (right). The initial conditions are $x_1(0) = 1, x_2(0) = 0.2$ and $x_3(0) = 0$. ......................................................... 27
2.4 The three dimensional generalized Hénon map, for bifurcation parameters $a = 1.76$ and $b = 0.1$, initial conditions $x_1(0) = 0.8147, x_2(0) = 0.9057, x_3(0) = 0.1269$. The probability-density function of the states of the system (left) and the projection of the state space on the $(x_2, x_3)$ plane (right) ........ 27
2.5 The three dimensional generalized Hénon map, for bifurcation parameters $a = 1.76$ and $b = 0.1$, initial conditions $x_1(0) = 0.8147, x_2(0) = 0.9057, x_3(0) = 0.1269$. The projection of the state space on the $(x_1, x_3)$ plane (left) and the projection of the state space on the $(x_1, x_2)$ plane (right) .......... 28
2.6 The phase space of the Hitzl-Zele map, for $a = 0.25$, $b = 0.87$ and the initial conditions $x_1(0) = 0.8143, x_2(0) = 0.2435, x_3(0) = 0.9293$. $N = 10000$ iterations. .................................................. 28
2.7 The three dimensional Hitzl-Zele map, for $a = 0.25$ and $b = 0.87$ and the initial conditions $x_1(0) = 0.8143, x_2(0) = 0.2435, x_3(0) = 0.9293$. $N = 10000$ iterations. The evolution of its states $x_1(k), x_2(k), x_3(k)$, with $k \in \{0, ..., N\}$. .......................................................... 29
2.8 The three dimensional Hitzl-Zele map, for $a = 0.25$ and $b = 0.87$ and the initial conditions $x_1(0) = 0.8143, x_2(0) = 0.2435, x_3(0) = 0.9293$. $N = 10000$ iterations. Their probability density functions, $p_{X_1}(x_1), p_{X_2}(x_2), p_{X_3}(x_3)$. 30
2.9 The three dimensional Hitzl-Zele map, for $a = 0.25$ and $b = 0.87$ and the initial conditions $x_1(0) = 0.8143, x_2(0) = 0.2435, x_3(0) = 0.9293$. $N = 10000$ iterations. The projections of the phase space in the $(x_1, x_2), (x_1, x_3), (x_2, x_3)$ planes. .................................................. 31
2.10 The Hitzl-Zele map. The spectrum of the Lyapunov exponents when the parameter $a = 0.25$ is kept fixed (left) or the parameter $b = 0.87$ is kept fixed (right). The initial conditions are $x_1(0) = 0.8143$, $x_2(0) = 0.2435$ and $x_3(0) = 0.9293$.  

2.11 The Colpitts Oscillator-PSpice scheme.  

2.12 The phase space of the chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$.  

2.13 The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. Projections in the planes defined by its states.  

2.14 The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The temporal evolution of its states.  

2.15 The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The probability distribution functions of its states.  

2.16 The Lyapunov exponents for the Colpitts chaotic oscillator with parameters $g = 4.46$, $Q = 1.38$, $k = 0.5$, initial conditions $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$.  

3 The probability density functions for the determinant of the observability matrices determined by the three state variables of the Hitzl-Zele map. Parameters $a = 0.25$ and $b = 0.87$.  

3.1 The probability density functions for the determinant of the observability matrices determined by the three state variables of the Colpitts chaotic oscillator. Parameters $Q = 1.38$ and $g = 4.46$.  

4.1 Trajectories for the Hénon map, with different initial conditions.  

4.2 The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 5$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.  

4.3 The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 10$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.  

4.4 The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 20$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.  

4.5 The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 30$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.  

4.6 The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 40$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.  

4.7 The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 5$, and the temporal cumulative distribution function $F_{eY}$.  

6
4.8 The cumulative distribution functions $F_{E_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 10$, and the temporal cumulative distribution function $F_{E_Y}$. 

4.9 The cumulative distribution functions $F_{E_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 20$, and the temporal cumulative distribution function $F_{E_Y}$. 

4.10 The cumulative distribution functions $F_{E_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 30$, and the temporal cumulative distribution function $F_{E_Y}$. 

4.11 The cumulative distribution functions $F_{E_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 40$, and the temporal cumulative distribution function $F_{E_Y}$. 

4.12 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 0$. 

4.13 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 10$. 

4.14 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 20$. 

4.15 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 30$. 

4.16 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 40$. 

4.17 The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 50$. 

5.1 The attractor the intruder reconstructs from the measured variable (the Colpitts chaotic oscillator). 

5.2 The attractor the intruder reconstructs from the measured variable divided into $10^3$ smaller volumes. 

5.3 The volume of the attractor of the Colpitts chaotic oscillator divided in small volumes. The boxes which are intersected by the attractor of the chaotic system. 

5.4 The volume of the attractor of the Colpitts chaotic oscillator divided in small volumes, grouped in areas by colors. 

5.5 The evolution of the Euclidean distance between points starting their evolution from the box number 723. 

5.6 The evolution of the Euclidean distance between points starting their evolution from the box number 305. 

5.7 The evolution of the Euclidean distance between points starting their evolution from the box number 304. 

5.8 The evolution of the Euclidean distance between points starting their evolution from the box number 923. 

5.9 The evolution of the Euclidean distance between points starting their evolution from the box number 5. 

6.1 Sites of the generalized Hénon map, determined by the function $f = \sin(\frac{x_2 - x_3}{2})$. 

6.2 Sites of the generalized Hénon map, determined by the function $f = \sin(\frac{x_2 - x_3}{2})$. 

7
6.2 Histogram corresponding to the ten boxes, for bifurcation parameters
\[ a = 1.76 \text{ and } b = 0.1 \] on a trajectory of 50,000 iterations. The initial
conditions are \( x_1(0), x_2(0), x_3(0) = (0.8147, 0.9057, 0.1269) \). 82

6.3 Scheme of the proposed enciphering method 83

6.4 Frequency of occurrence of ASCII characters in a natural language text. 86

6.5 Frequency of occurrence of ASCII characters in ciphered version. 86

6.6 Original image (left) and enciphered image (right). 87

6.7 The error in estimating \( x \). 90

6.8 The noisy \( y \) in blue; noisy channel. 98

7.1 Chaos synchronization by means of high order sliding mode observers,
using the inclusion of the secret message in the dynamics of the chaotic
emitter. 91

7.2 The states \( x_1, x_1(\tau), x_2 \). The initial conditions are:
\( x_1(0) = 0, x_2(0) = 0.1 \) and \( x_2(t) \), \( \forall t \in [-\tau, 0) \). The message is \( u = 0 \) (left) and \( u = 0.5 \left[ 1 + (\frac{\eta}{2})^2 \right] \) (right). 92

7.3 The output of the transmitter with the message included in the evolution
of the delayed chaotic transmitter. The initial conditions are:
\( x_1(0) = 0, x_2(0) = 0.1 \) and \( x_2(t) \), \( \forall t \in [-\tau, 0) \). 92

7.4 The estimated \( \dot{u} \) in blue, and the transmitted message \( u \), in red. The
initial conditions are:
\( x_1(0) = 0, x_2(0) = 0.1 \) and \( x_2(t) \), \( \forall t \in [-\tau, 0) \). 95

7.5 The estimated \( \dot{x}_1 \) in red, and the state \( x_1 \) in blue. The initial conditions
are:
\( x_1(0) = 0, x_2(0) = 0.1 \) and \( x_2(t) \), \( \forall t \in [-\tau, 0) \). 95

7.6 The error in estimating \( x_1 \). 95

7.7 The estimated \( \dot{x}_2 \) in red, and the state \( x_2 \) in blue. The initial conditions
are:
\( x_1(0) = 0, x_2(0) = 0.1 \) and \( x_2(t) \), \( \forall t \in [-\tau, 0) \). 96

7.8 The error in estimating \( x_2 \). 96

7.9 The noisy \( y \) in blue, and \( y \) in red. 96

7.10 The estimated \( \dot{u} \) in red and the transmitted message \( u \) in blue; noisy
channel. 97

7.11 The estimated \( \dot{x}_1 \) in red, and the state \( x_1 \) in blue; noisy channel. 97

7.12 The estimated \( \dot{x}_2 \) in red, and the state \( x_2 \) in blue; noisy channel. 98

7.13 The synchronization between two chaotic Colpitts oscillators. Orcad
scheme. 99

7.14 Synchronization of two chaotic Colpitts oscillators. Continuous coupling
between the two circuits. 99

7.15 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 2\% \). 100

7.16 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 10\% \) (left) and \( \eta = 20\% \) (right). 100

7.17 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 50\% \) (left) and \( \eta = 70\% \) (right). 100

7.18 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 80\% \) (left) and \( \eta = 90\% \) (right). 101

7.19 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 98\% \). 101

7.20 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 2\% \) (left) and \( \eta = 5\% \) (right). Second buffer added. 101

7.21 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 10\% \) (left) and \( \eta = 20\% \) (right). Second buffer added. 102

7.22 Synchronization of two chaotic Colpitts oscillators. Transmission during
\( \eta = 50\% \) (left) and \( \eta = 70\% \) (right). Second buffer added. 102
7.23 Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 80\%$ (left) and $\eta = 90\%$ (right). Second buffer added. 

7.24 Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 98\%$. Second buffer added.

7.25 Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 98\%$. Second buffer and resistance added.

7.26 Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 80\%$ (left) and $\eta = 79\%$ (right). Second buffer and resistance added.

7.27 Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 70\%$ (left) and $\eta = 50\%$ (right). Second buffer and resistance added.

9.1 The subintervals corresponding to some of the ASCII characters, in Baptista’s enciphering method.

9.2 Enciphering the character ‘O’ as the first letter of a plain-text, with Baptista’s enciphering method.

9.3 Enciphering the character ‘c’ as the second letter of a plain-text, with Baptista’s enciphering method.

9.4 The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=0.04$ and $b=0.1\lambda_1,\lambda_2,\lambda_3, < 0$.

9.5 The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=0.4$ and $b=0.1\lambda_1,\lambda_2,\lambda_3, < 0$.

9.6 The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.25$ and $b=0.1 (\lambda_1, \lambda_2, \lambda_3, < 0)$.

9.7 The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.43$ and $b=0.3 (\lambda_1 > 0, \lambda_2 > 0, \lambda_3, < 0)$.

9.8 The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.6$ and $b=0.1 (\lambda_1 > 0, \lambda_2 > 0, \lambda_3, < 0)$.

9.9 The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.275$ and $b=0.87$.

9.10 The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.3$.

9.11 The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.5$.

9.12 The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.88$.

9.13 The evolution of the Colpitts chaotic oscillator over 400s, with $T_s = 0.001s$, with parameters $g=4.46$ and $Q=1 (\lambda_1 > 0, \lambda_2 < 0, \lambda_3, < 0)$.

9.14 The evolution of the Colpitts chaotic oscillator over 400s, with $T_s = 0.001s$, with parameters $g=1.01$ and $Q=1.38 (\lambda_1, \lambda_2, \lambda_3, < 0)$.

9.15 The cumulative distribution functions $F_X(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 15$, and the temporal cumulative distribution function $F_Y$.

9.16 The cumulative distribution functions $F_X(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 25$, and the temporal cumulative distribution function $F_Y$.

9.17 The cumulative distribution functions $F_X(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 35$, and the temporal cumulative distribution function $F_Y$. 

9
9.18 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 45 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 127

9.19 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 50 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 127

9.20 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 55 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 128

9.21 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 60 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 128

9.22 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 65 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 129

9.23 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 70 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 129

9.24 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 75 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 130

9.25 The cumulative distribution functions \( F_{e_X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 80 \), and the temporal cumulative distribution function \( F_{e_Y} \) ............................................... 130
List of Tables

4.1 Smirnov test values $\delta = |F_{e_X}(u) - F_{e_Y}(u)|$. Stationarity of the generalized Hénon map. .................................................. 61
4.2 Monte-Carlo type analysis for the Smirnov test attesting the stationarity region entry moment for the generalized Hénon map. .................. 61
4.3 Smirnov test values $\delta = |F_{e_X}(u) - F_{e_Y}(u)|$. Ergodicity of the generalized Hénon map. .................................................. 62
4.4 Monte-Carlo type analysis indicating the minimum independence sampling distance for the generalized Hénon map. .................. 64
5.1 The coordinates of the origin of the boxes in which the phase space of the Colpitts oscillator is split into. .................. 70
6.1 The ten subintervals of equal length. ........................................... 82
6.2 Key elements disposed in two matrices. ................................. 84
8.1 The Lyapunov exponents for the Hénon map. .................. 107
9.1 Smirnov test values $\delta = |F_{e_X}(u) - F_{e_Y}(u)|$. Ergodicity of the generalized Hénon map. .................................................. 124
Chapter 1

Introduction

1.1 Motivation

I have become interested by the domain of the cryptography when I first worked with Professor Adriana Vlad. It was my second year (2005-2006) as a student at The Faculty of Electronics, from the Politehnica University of Bucharest, Romania. Mrs. Professor Adriana Vlad offered me the possibility to develop my project for the annual practice under her scientific guidance. I became familiar with notions of strange attractor, bifurcations, phase space, etc. I also understood what stationarity and ergodicity are useful for in enciphering. I continued accumulating information and become more passionated by the ciphers with each passing year.

My fifth year as a student brought me joy. The first semester strengthened my knowledge in cryptography, due to Professor’s Vlad courses I attended during the academical year 2008-2009. The Erasmus-Socrates Project from 2008 and the collaboration Professor Adriana Vlad has with the E.N.S.E.A. Faculty from Cergy-Pontoise, opened me some new doors for professional development. I met Professor Jean-Pierre Barbot and his team. My diploma project was developed under the common guidance of Professor Adriana Vlad and Professor Jean-Pierre Barbot. I have learned to design a cipher, to look for its strength and for its weakness when exposed to cryptanalytic attacks.

The Doctoral Sectoral Operational Programme of Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/88/1.5/S/61178 gave me the opportunity to continue the collaboration with E.N.S.E.A. through my two, four months each, stages in France.

Many questions tried to find their answer through the present research work. Some of them did, some others did not. In the following lines and chapters I will describe my results and my scientific wondering.

How come deterministic chaos? Chaos is a state of disorder, it obeys no law in its evolution. Deterministic systems can be analytically described, their evolution follows rules. Long discussions have conduced me to understand from where the term deterministic chaos comes from, and how this apparently two antagonistic notions can intersect.

I found that the term chaos was used for the first time in thermodynamics, to designate molecular chaos. In this context, systems that manifest molecular chaotic behavior are dynamics with great number of degrees of freedom. Due to the huge number of particles involved in a thermodynamical study, Statistics is the only reasonable tool that can give answers to the analysis. Statistical analysis can be accurately done when a great quantity of observations is available. Which leads to the necessity of using computers to achieve the task. But machines have limited precision. Human beings do not have the ability of constructing a machine which disposes of infinite memory. Infinite
memory is equivalent to registers that contain infinite length binary words. This length would be necessary in order to obtain an infinite resolution. Consequently, all machines do truncation operations of the numbers they handle.

To illustrate our taking conscience of this limitations of what I call machine chaos we have considered the logistic map described by the recurrent equation (1.1). This simple one dimensional map engenders a behavior of great complexity (for which the recurrence is the cause). Depending on the value of the control parameter \( r \), the recurrence converges to an unique value, to two, to three, to four, eight values, etc. Or, most surprising, it does not converge to any value, but oscillates between multiple (theoretically, an infinity of) values.

\[
x(n + 1) = r \cdot x(n) \cdot (1 - x(n))
\]  

(1.1)

where \( x \in [0; 1] \) and \( r \in [0; 4] \).

The graph well-known as the bifurcation diagram of the logistic map, represented in Fig. 1.1 is only an indication of the complexity involved by the evolution of this equation. Works [12], [50], [3], [71], [37], are a few examples of the multitude of studies regarding the dynamical behavior of the logistic parabola.

![Figure 1.1: The bifurcation diagram of the logistic map.](image)

It is impossible to compute the long-time evolution of the logistic map (the affirmation is valid for any chaotic system) by hand. Thus, the numerical simulation becomes the only tool available to detect the truth. We do not have another tool that validates the accuracy of this computations. If the computations themselves are artifacts, our conclusions are not conform to the real situation we are analyzing. This is why, it is imperative to formally check that the obtained values respect the trend they should theoretically obey.

The aim of our work is to use the much studied behavior of the recurrence (1.1) to prove that the numerical calculus computers do, are not always totally reliable. To achieve this goal we consider the values of the bifurcation parameter \( r \) by intervals:

1. for \( r \in [0; 3] \) the recurrence converges to a unique value, the solution of the first return (also known as the fixed point of the logistic map):

\[
x(n + 1) = x(n)
\]  

(1.2)
The solution $x^{(2)}$ of the equation $rx(1 - x) = x$ is obtained:

$$x(rx + 1 - r) = 0 \Rightarrow x^{(2)} = 1 - \frac{1}{r} \quad (1.3)$$

It is obvious that the trivial solution of the first return, equation (1.2) is $x^{(1)} = 0$. The recurrence converges to 0, while $r \in (0; 1]$ and to $x^{(2)} = 1 - \frac{1}{r}$ while $r \in (1; 3]$. It is easy to prove this stability by the method of the perturbations. If the value $x_\infty$ is a stable solution, then the addition of a small perturbation would be reduced to zero while the recurrence evolves. While the solution is not stable, this perturbation, $\epsilon$, is amplified.

Let us note $x(n) = x_\infty + \epsilon$. The logistic recurrence becomes, for $x(n)$:

$$x(n+1) = r \cdot (x_\infty + \epsilon) \cdot (1 - (x_\infty + \epsilon)) \Rightarrow x(n+1) = -r \cdot \epsilon^2 + \epsilon \cdot (2 - r) + 1 - \frac{1}{r} \quad (1.4)$$

As $|\epsilon| << 1$, the second order term $\epsilon^2$ can be ignored. Thus, $x(n+1) = x_\infty + \epsilon \cdot (2 - r)$. As long as $|2 - r| < 1$, $x(n+1) < x_\infty$. The recurrence is, then, convergent and the solution of the first return is stable. The condition $-1 < 2 - r < 1$ results in stable solution $x_\infty$ for $r \in (1, 3)$ and unstable solution for $r \in [3, 4)$, when the small initial error becomes greater and greater with the evolution of the recurrence.

The second return satisfies the condition (1.5). It corresponds to a fourth order equation, (1.6). The equation (1.5) has the solutions $x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}$ from equation (1.7).

$$x(n + 2) = x(n) \quad (1.5)$$

$$r^2 \cdot (x_n - x_n^2) \cdot [1 - r \cdot (x_n - x_n^2)] - x_n = 0 \quad (1.6)$$

$$\begin{cases} x^{(1)} = 0 \\ x^{(2)} = 1 - \frac{1}{r} \\ x^{(3)} = \frac{r + 1 + \sqrt{r^2 - 2r - 3}}{2r} \\ x^{(4)} = \frac{r + 1 - \sqrt{r^2 - 2r - 3}}{2r} \end{cases} \quad (1.7)$$

When $x(0) = 1 - \frac{1}{r}$ is taken as initial condition of the logistic map and for the control parameter $r \in (3, 4)$, the unstable interval for the first return, a large number of numeric simulations do not diverge and remain on the initial value $1 - \frac{1}{r}$. The rest of the simulations leave these initial conditions and converge to usual solutions. The expected behavior being the latter.

This experimental behavior implies many questions. All the simulations have the same initial condition, a function of $r$. If the computations were of infinite resolution, these simulations would diverge, because they are initialized exactly in an unstable equilibrium point. In order to alter this equilibrium, a perturbation is needed. The necessary perturbation occurs always in the physical case of analog circuitry and only casual in simulations as the computational cases. The persistence of this unstable equilibrium is surprising for the one that knows the bifurcation diagram of this recurrence, because of its mathematical exactitude.
Figure 1.2: The bifurcation diagram of the logistic map, for the bifurcation parameter $r \in [1, 4]$. 

Unfortunately, we do not find such a nice situation for many of our simulations, however, despite them being performed under the same conditions. This convergence paradoxically proves that the numerical computation is not infinite, fact already known. But the great difficulty is that it is not possible to determine which are the simulations that will diverge and which others will remain in this infinitely precarious equilibrium. It seems that the congruence of these truncations themselves induce unexpected islands of stability. Truncation operation, because of finite representation, disregard (theoretically) the least significant part of the values of the numbers the computer handles.

Fig. 1.2 illustrates how cautious one should be when interpreting numerical (obtained from simulations) results. It is imperative to test their robustness in the automatics sense, before considering them as true (corresponding to the considered reality). We have detailed the interval $[3, 4]$ of the bifurcation diagram in Fig. 1.3. One can see, beside the well-known bifurcation diagram of the logistic map, the solutions of the first (green line) and the second (green, red, yellow) return maps. The trivial solution $0$ is not represented. The last 500 points among 10000 corresponding to each value of the bifurcation parameter $r$ are plotted, between $r = 1$ and $r = 4$, with a step of $\Delta = \frac{r_{\text{max}} - r_{\text{min}}}{1000} = 3 \cdot 10^{-3}$. Theoretically, in this interval, any of the 10000 values should not remain on the starting point $x_0 = 1 - \frac{1}{r}$. Contrary to this expectation, a percentage of approximately 30% of the 344 values for $3 \leq r \leq 4$ remain stable because of rounding and truncation operations. These situations are marked with a blue line at the corresponding $r$ values. It is true that we have chosen particular initial conditions, but the quantity of non-robust solutions, that appear as stable, is far from being rare.

To illustrate one of the cases in which the recurrence behaves in simulation as expected from theory, we choose $r = 3.97$, and plot the sequence of values obtained for the logistic map, in Fig. 1.4. One can notice as the entire co-domain of the logistic parable, the interval $[0, 1]$, is visited by its evolution.

We conclude that chaos can be assigned to the sensory limitation of human beings. Due to the high number of degrees of freedom the so-called chaotic systems have, the human mind can not conceptualize such complexity. This is why a deterministic mechanism seems to be without law, random. Similarly, the behavior of simple equations such as the logistic parable, produces values that seem unpredictable. We attribute to
these systems the term of deterministic chaos because the equations that produce these values are perfectly deterministic.

The next section briefly presents the research this work is based on.

### 1.2 Structure of the Thesis

Chapter I presents my motivation for choosing the area situated at the intersection of three sciences, statistics, cryptography, and control theory, to develop the research work whose details are given in the next chapters. The theoretical frame of this work is given, following. The notions and the algorithms specific to a certain chapter only, will be discussed in the respective chapter.

Chapter II is dedicated to the study of the Lyapunov exponents, the rate of divergence of initially neighboring trajectories of (chaotic) systems. Three chaotic systems
are considered for the study:

1. the generalized Hénon map, discrete, three-dimensional, hyper-chaotic.

2. the Hitzl-Zele map, discrete, three-dimensional, structurally more complex than the generalized Hénon map.

3. the chaotic Colpitts oscillator, continuous, three-dimensional, allowing the introduction of continuous delays, leading to an infinite dimension of the chaotic dynamics.

The investigation concerning the Lyapunov specter is performed in order to determine domains for the parameters which generate chaotic behavior of the systems. In the literature, there are only particular values given for these parameters.

The computation of the Lyapunov exponents spectra is the opportunity to briefly present the history of the systems mentioned above and some of their statistical properties.

Chapter III presents a study of some structural properties of the three systems from Chapter II. The investigation is focused on the determination of the observability singularity manifolds and the calculation of the observability indexes.

At the intersection of these hyper surfaces with the considered chaotic attractor, the left inversion problem is no longer reduced to an observer, but to an estimator challenge, which requires that the unknown input is constant during the intersection of the attractor with the singularity manifold.

Observability indexes give an indication of the quality of the states of the chaotic systems when they are considered as the output of the transmitter. They quantify how observable is the transmitter when its output is represented by one particular chosen variable among its states.

Chapter IV analyzes the statistical independence in the context of the considered chaotic systems: how large should be the sampling distance (how many iterations or, equivalently, time) to ensure statistical independence between random variables extracted from the chaotic systems. The Vlad-Badea test for statistical independence was used; the procedure is applicable to all kind of continuous random variables, even of unknown probability law as needed here.

Chapter V illustrates the physical point of view. The transient time corresponds to the time spent by the chaotic system in the basin of attraction before rejoining the strange attractor. Depending on the starting spatial region of the strange attractor corresponding to the investigated chaotic system, the points belonging to the respective area become, faster or slower, uncorrelated (weakly correlated). In terms of cryptology, this dependence of the chosen region on the strange attractor is of great importance, both for the cryptographer, and for the cryptanalyst. The first, wishing to achieve the best inclusion of the message in the chaotic dynamics, choosing the area where its evolution becomes uncorrelated at the smallest distance, the other to effectuate an attack on those portions on which the system folds (converges), it is slow in achieving non-correlation.

Chapter VI starts from the question How robust are discrete time polynomial chaotic systems as dynamics including a secret message? For the chaotic generalized Hénon map, when this dynamic includes a secret message encoded in ASCII, the knowledge of three characters composing the plain-message is sufficient in order to constitute a system of three algebraic equations, the unknown variables being the two bifurcation parameters of the system and the scaling factor of the ASCII representation necessary for the chaotic dynamics to remain unaltered. We propose a simple improvement of inclusions in this type of cryptosystems, where the parameters and the scaling factor can be part of the
(internal) secret key. The plain-text is encrypted by classical methods, with S-box and P-box type transformations, according to the amplitude in which the values of a trigonometric function of the states of the chaotic system (this function leads to a pseudo-uniform distribution of external secret keys for substitution and transposition) lays when the plain character is enciphered. The results of the proposed algorithm are evaluated on text and images. Showing a stronger correlation than the text, images reveal the weaknesses of the method of encryption. Redundancy between the color planes is diffused, but it does not reach its uniformity, just as it is expected from a good practical cipher, [70]. Ideas to improve the algorithm are multiple and suggested as future work.

Chapter VII rises some questions, and tries to find some answers to these questions, in the context of hybrid chaotic schemes. A first idea is to substitute the Colpitts oscillator with a continuous time delay (infinite dimensional dynamic, because it is necessary to characterize the whole phase space not only in the present moment, but also in the past, a continuum of moments between \( t_0 - \tau \) and \( t_0 \) being required). Is it possible to recover the secret message by using an observer, when the dynamic that includes it is time delayed? The answer is positive, and this is shown for a delay chaotic system inspired by Uçar [81], in the work [24], where a full transmission of the output of the system (the cryptogram) is considered. What if the transmission is done on only 10% of the time? How possible is the synchronization between continuous delayed dynamics when they communicate only a very short time? To begin this study, we implemented in analog circuitry the synchronization between two Colpitts oscillators (information is only transmitted from the transmitter to the receiver). First, the transmission was set to be continuous (the duty factor \( \eta = \frac{\tau}{T} = 100\% \)). When plotting the estimation of the output of the transmitter versus the original output, the first bisector was obtained. This proves the synchronization of the two considered systems. When decreasing the transmission duration to 80%, 50%, 30% and 10% the capability of synchronization of the two oscillators decreases. This is due to integrated circuits that simulate the transmission channel (the buffer for unidirectional transmission of the information, the switch used to allow only a fraction of the transmission period of the oscillator), and, especially, to the operation in low output impedance of the common base configuration of the bipolar junction transistor which is the active element of the Colpitts oscillator. An open challenge is to achieve synchronization of delayed analog chaotic systems. Or, at least, to get an answer whether it is possible or not to synchronize them.

Chapter VIII concludes the thesis and gives the perspectives of the research for future development.

Chapter IX presents some of the results that were not introduced in the previous chapters.

References are given as a theoretical support we used in order to establish the historical frame of statistics, cryptography and control theory, as well as to get a solid knowledge of the procedures and algorithms already existing in the chosen fields.

1.3 Theoretical Background

Our research work is an extension of the experiments and investigations developed by my colleagues: Adrian Luca with his thesis „Statistical analysis of chaotic systems from the perspective of the utility in cryptography”, Mădălin Frunzete having „Contributions in the field of cryptography based on chaotic systems using information theory and statistics”, Maryam l’Hernault-Zanganeh who proved, in theory and practice, the „Feasibility of an analog emission-receiving system for the secure communications using chaos” (Faisabilité d’un système d’émission-réception analogique pour les communications sécurisées.
par le chaos) and Hamid Hamiche analyzing the „Left inversion of the hybrid chaotic dynamical systems. Application to secured transmission of data” (Inversion à gauche des systèmes dynamiques hybrides chaotiques. Application à la transmission sécurisée des données.) Therefore, the definitions of the notions which are specific to the fields of statistics, cryptography, chaotic systems and control system theory, were already given in their doctoral works.

Nevertheless, we will introduce those definitions and algorithms involved by our approach in the chapters their application is required.

Still, we have to mention the fundamental works of Shannon ([69] and [70]), Ruelle and Eckmann ([32]) and Takens ([76]).
Chapter 2
The Lyapunov exponents

2.1 Introduction

From the literature we only know particular parameter pairs which induce chaos for the systems they describe. We want to enrich the domain of values for the parameters. Thus, this chapter is dedicated to the study of the Lyapunov exponents, which express the rate of divergence/convergence of initially neighboring trajectories of (chaotic) systems. Subsection 1 explains the physical meaning of this rate. Subsection 2 describes the steps of the most popular algorithm used to compute the Lyapunov exponents, the Wolf-Swinney-Vastano algorithm. Sections 8.1, 2.3, 2.4 apply the notions presented in the section 2.1 to calculate the spectrum of the Lyapunov exponents for:

1. the generalized Hénon map, discrete, three-dimensional, hyper-chaotic.
2. the Hitzl-Zele map, discrete, three-dimensional, structurally more complex than the generalized Hénon map.
3. the chaotic Colpitts oscillator, continuous, three-dimensional, allowing the introduction of continuous delays, leading to an infinite dimension of the chaotic dynamics.

The computation of the Lyapunov exponents spectra is the opportunity to briefly present the systems mentioned above and some of their statistical properties.

1 Signification of the Lyapunov exponent

For the ease of exemplification, let us consider the one-dimensional logistic map, \( x(n + 1) = f(x(n)) \), with \( f(x) = r \cdot x \cdot (1 - x) \). For values of the parameter of bifurcation \( r \) greater than 3.57, two trajectories (i.e. sequences \( \{x_i\} \), with \( i = 0, 1, 2, \ldots \)), initially situated in a small vicinity, diverge rapidly. This translates itself in chaotic behavior. The Lyapunov exponent \( \lambda(x_0) \) measures this divergence as follows:

Two infinitesimally different initial points, \( x_0 \) and \( x_0 + \epsilon \), are considered. After \( n \) iterations, the Lyapunov exponent \( \lambda(x_0) \) is defined by equation (2.1).

\[
\epsilon \cdot e^{n \cdot \lambda(x_0)} = |f^n(x_0 + \epsilon) - f^n(x_0)| \tag{2.1}
\]

Passing to the limit (when the difference between the two starting conditions is negligible and the number of iteration is infinitely large), the expression for \( \lambda \) becomes (2.2):
\[ \lambda(x_0) = \lim_{n \to \infty} \lim_{\epsilon \to 0} \frac{1}{n} \log \left| \frac{f^n(x_0 + \epsilon) - f^n(x_0)}{\epsilon} \right| \]

\[ = \lim_{n \to \infty} \frac{1}{n} \log \left| \frac{df^n(x_0)}{dx} \right| \quad (2.2) \]

Using the notation \( f^i(x_0) = x_i \), recall that \( f^n(x_0) = f(f^{n-1}(x_0)) \) and the derivative \( \frac{df^n(x_0)}{dx} \) can be written as in (2.3) (using the chain rule). Thus, the equation (2.2) can be expressed as in (2.4).

\[ \frac{df^n(x_0)}{dx} = f'(x_{n-1}) \cdot f'(x_{n-2}) \cdot \ldots \cdot f'(x_1) \cdot f'(x_0) \quad (2.3) \]

\[ \lambda(x_0) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \log |f'(x_i)| \quad (2.4) \]

2 The algorithm of Wolf, Swinney and Vastano

The algorithm used in this work in order to compute the Lyapunov spectra (the number of the Lyapunov exponents of a system is equal to the number of its directions of its states) is the one proposed in 1985 in the paper [87]. Its steps are described in the following lines:

At the initial iteration \( k = 0 \) of the application (2.5), let as consider in the phase space a \( n \)-sphere. With the evolution of the map, when \( k \to \infty \) the \( n \)-sphere transforms into a \( n \)-ellipsoid (whose main axes are assumed in descending order).

\[ x_{k+1} = f(x_k) \quad (2.5) \]

with \( k = 0, 1, 2, \ldots \) and \( x_k \in \mathbb{R}^n \to \mathbb{R}^n \).

The \( i \)-th Lyapunov exponent is defined based on the rate of increasing of the \( i \)-th main axis \( v_i \) through the equation (2.6).

\[ \lambda_i = \lim_{N \to \infty} \frac{1}{N} \log \left( \frac{||v_i(N)||}{||v_i(0)||} \cdot \frac{||v_i(1)||}{||v_i(1)||} \cdot \ldots \cdot \frac{||v_i(N)||}{||v_i(N-1)||} \right) \quad (2.6) \]

with \( i = 1, 2, \ldots, n \).

This formula implies that, when iterating the formula (2.5), the length of the first main axis increases by \( e^{\lambda_1 \cdot k} \), the area defined by the first two main axes increases by \( e^{(\lambda_1 + \lambda_2) \cdot k} \). The volume described by the first three main axes increases by \( e^{(\lambda_1 + \lambda_2 + \lambda_3) \cdot k} \) and so on.

When iterating, the main axes transform according to the formula (2.7).

\[ v_i(k + 1) = J(k) \cdot v_i(k) \quad (2.7) \]

where \( J(k) \) is the Jacobian of the application \( f \) computed at \( x_k \), and \( i = 1, 2, \ldots, n \).

The expression (2.6) can be reformulated as in (2.8).

\[ \lambda_i = \lim_{N \to \infty} \frac{1}{N} \log \left( \frac{||v_i(1)||}{||v_i(0)||} \cdot \frac{||v_i(2)||}{||v_i(1)||} \cdot \ldots \cdot \frac{||v_i(N)||}{||v_i(N-1)||} \right) \quad (2.8) \]
with \(i = 1, 2, ..., n\).

At \(k = 0\), the vectors \(v_i, i = 1, 2, ..., n\) are defined by:

\[
\begin{align*}
v_1 &= (1, 0, 0, 0, ..., 0) \\
v_2 &= (0, 1, 0, 0, ..., 0) \\
&\vdots \\
v_n &= (0, 0, 0, 0, ..., 1)
\end{align*}
\] (2.9)

In order to avoid divergence, at each iteration, the vectors \(v_1(k), v_2(k), ..., v_n(k)\) are orthonormalized using the Gram-Schmidt procedure as in (2.10):

\[
\begin{align*}
v'_1 &= \frac{v_1}{||v_1||} \\
v'_2 &= \frac{v_2 - \langle v_2, v'_1 \rangle \cdot v'_1}{||v_2 - \langle v_2, v'_1 \rangle \cdot v'_1||} \\
&\vdots \\
v'_n &= \frac{v_n - \langle v_n, v'_{n-1} \rangle \cdot v'_{n-1} - ... - \langle v_n, v'_1 \rangle \cdot v'_1}{||v_n - \langle v_n, v'_{n-1} \rangle \cdot v'_{n-1} - ... - \langle v_n, v'_1 \rangle \cdot v'_1||}
\end{align*}
\] (2.10)

3 An iterated map: The Hénon map.

The Hénon two dimensional discrete map, [41], is expressed by (2.11):

\[
\begin{align*}
x_1(k+1) &= 1 - a \cdot x_1^2(k) + x_2(k) \\
x_2(k+1) &= b \cdot x_1(k)
\end{align*}
\] (2.11)

Its Jacobian matrix \(J(k)\) can be written:

\[
J(k) = \begin{pmatrix} -2 \cdot a \cdot x_k & 1 \\ b & 0 \end{pmatrix}
\] (2.12)

Further explanations about Lyapunov exponents and more detailed notions specific to chaotic dynamic can be found in [21]. The results got in [21], for bifurcation parameters \(a = 1.4\) and \(b = 0.3\), are \(\lambda_1 = 0.604\) and \(\lambda_2 = -2.341\). The exponent \(\lambda_1 > 0\) expresses the chaotic behavior of the Hénon map.

4 A differential system: The Lorenz system.

The computation of Lyapunov exponents of a system of differential equations \(\frac{dx}{dt} = f(x), f: \mathbb{R}^n \rightarrow \mathbb{R}^n\) is similar. The equations (2.6) and (2.7) are replaced by (2.13) and (2.14).

\[
\lambda_i = \lim_{t \to \infty} \frac{1}{t} \log \frac{||v_i(t)||}{||v_i(0)||}
\] (2.13)

with \(i = 1, 2, ..., n\).

\[
\dot{v}_i(t) = J(x) \cdot v_i(t)
\] (2.14)
with \( i = 1, 2, \ldots, n \).

Thus, a \( n + n^2 \) equations system is obtained. At each iteration, the \( n \) vectors \( v_i, \quad i = 1, 2, \ldots, n \), defined at \( t = 0 \) by (2.9), are calculated with (2.14) and orthonormalized by the Gramm-Schmidt procedure.

In \([21]\) the three Lyapunov exponents for the Lorenz system (2.15), [60], are found to be \( \lambda_1 = 2.11, \quad \lambda_2 = 0.00, \quad \lambda_3 = -32.40 \).

\[
\begin{align*}
\dot{x}_1 &= \sigma \cdot (x_2 - x_1) \\
\dot{x}_2 &= x_1 \cdot (r - x_3) - x_2 \\
\dot{x}_3 &= x_1 \cdot x_2 - b \cdot x_3
\end{align*}
\]

(2.15)

with the bifurcation parameters \( \sigma = 16, \quad r = 45.92, \quad b = 4 \).

### 2.2 The generalized Hénon map

The Hénon generalized functions have the form in equation (2.16):

\[
\begin{pmatrix}
x_1(k+1) \\
x_2(k+1) \\
\vdots \\
x_n(k+1)
\end{pmatrix}
= f(x(k)) =
\begin{pmatrix}
a - x_{n-1}^2(k) - bx_n(k) \\
x_1(k) \\
\vdots \\
x_{n-1}(k)
\end{pmatrix}
\]

(2.16)

where the bifurcation parameters \( a > 0 \) and \( b > 0 \). The iterations \( x \in \mathbb{R}^n \), [15].

Due to their simplicity, the generalized Hénon functions are frequently used as exemplification in the analysis of chaotic discrete-time systems.

In the present work, the case \( n = 3 \) is illustrated aiming a simple approach. The particular choice gives the expression in (2.17).

\[
\begin{align*}
x_1(k+1) &= a - x_2^2(k) - bx_3(k) \\
x_2(k+1) &= x_1(k) \\
x_3(k+1) &= x_2(k)
\end{align*}
\]

(2.17)

where \( x_1, x_2, x_3 \in (-2; 2), a > 0, b > 0 \).

The phase space of the generalized Hénon map is illustrated in Fig. 2.1.

The system described by the equations (2.17) is very sensitive to initial conditions, as it might be seen in Fig. 2.2. The evolution of the first state of the system is also shown for iterations \( k = 0, \ldots, 30 \). As it can be observed from the equations (2.17), the states \( x_2 \) and \( x_3 \) are shifted (delayed) versions of the state \( x_1 \).

The rate of the divergence of the trajectories is calculated as explained in Section 2.1. We have adjusted, for the generalized Hénon map, the algorithm described in [21]. The simulation results can be seen in Fig. 2.3.

Having, for certain pairs \((a,b)\), more than one Lyapunov exponent superior to zero, the generalized Hénon map is said to be hyperchaotic. Its evolution diverges in two directions.

The probability density functions of the states of the system, \( p_{X_1}(x_1) \) and the projection of the phase space on the \((x_2,x_3)\) plane are given in Fig. 2.4. The projections on the \((x_1,x_3)\) and on the \((x_1,x_2)\) planes are given in Fig. 2.5.

To our knowledge, the commonly used values for the bifurcation parameters in the literature are \( a = 1.76, b = 0.1 \), as in [36] and \( a = 1.9, b = 0.03 \), in [58]. Observing the graphics in Fig. 2.3, one can determine a wider set of parameters for chaotic behavior \( (\lambda_1 > 0 \text{ or } \lambda_1, \lambda_2 > 0) \).
2.1. The generalized Hénon map

The bifurcation parameters are $a = 1.76$ and $b = 0.1$. The initial conditions are $x_1(0) = 0.8147$, $x_2(0) = 0.9057$, $x_3(0) = 0.1269$. The phase space (left) and the evolution of its first state, $x_1(k)$, $k \in \{0, N\}$, $N = 10000$ (right).

Figure 2.1: The generalized Hénon map. The bifurcation parameters are $a = 1.76$ and $b = 0.1$. The initial conditions are $x_1(0) = 0.8147$, $x_2(0) = 0.9057$, $x_3(0) = 0.1269$. The phase space (left) and the evolution of its first state, $x_1(k)$, $k \in \{0, N\}$, $N = 10000$ (right).

2.2. Two trajectories for the generalized Hénon map with $a = 1.76$ and $b = 0.1$. With solid blue line, the sequence starting from $x_1(0), x_2(0), x_3(0)$. With dashed red line, the trajectory with initial conditions $x'_1(0) = x_1(0) + 0.01, x'_2(0) = x_2(0), x'_3(0) = x_3(0)$.

Figure 2.2: Two trajectories for the generalized Hénon map with $a = 1.76$ and $b = 0.1$. With solid blue line, the sequence starting from $x_1(0), x_2(0), x_3(0)$. With dashed red line, the trajectory with initial conditions $x'_1(0) = x_1(0) + 0.01, x'_2(0) = x_2(0), x'_3(0) = x_3(0)$.

2.3. The Hitzl-Zele map

As we will demonstrate in Chapter 3, the Hitzl-Zele map shows more complex structural properties, when compared to the generalized Hénon map. Saha and Stratgatz show how the period-3 cycle is born from chaos in [68] and give reference of the work of Hitzl and Zele [45]. The Hitzl-Zele map is analytically determined by equations (2.18).

$$\begin{align*}
x_1(k + 1) &= 1 + x_2(k) - x_3(k) \cdot x_1^2(k) \\
x_2(k + 1) &= a \cdot x_1(k) \\
x_3(k + 1) &= b \cdot x_1^2(k) + x_3(k) - 0.5
\end{align*}$$ (2.18)

with the bifurcation parameters $a = 0.25$ and $b = 0.87$ for chaotic behavior.
Figure 2.3: The generalized Hénon map. The spectrum of the Lyapunov exponents when the parameter $a = 1.76$ is kept fixed (left) or the parameter $b = 0.1$ is kept fixed (right). The initial conditions are $x_1(0) = 1, x_2(0) = 0.2$ and $x_3(0) = 0$.

Figure 2.4: The three dimensional generalized Hénon map, for bifurcation parameters $a=1.76$ and $b=0.1$, initial conditions $x_1(0) = 0.8147, x_2(0) = 0.9057, x_3(0) = 0.1269$. The probability-density function of the states of the system (left) and the projection of the state space on the $(x_2, x_3)$ plane (right).

The phase space of the Hitzl-Zele map is represented in Fig. 2.6, the evolution of the states $x_1, x_2, x_3$ of the systems in Fig. 2.7 and the probability density functions, $p_{X_1}(x_1), p_{X_2}(x_2)$ and $p_{X_3}(x_3)$ in Fig. 2.8. The projections of the phase space in the planes $(x_1, x_2), (x_1, x_3)$ and $(x_2, x_3)$ are shown in Fig. 2.9.

By plotting the Lyapunov spectra for the Hitzl-Zele map, in Fig. 2.10, we confirm its great complexity, affirmed in the begging of the section, and determine more values convenient for the chaotic regime.
Figure 2.5: The three dimensional generalized Hénon map, for bifurcation parameters $a=1.76$ and $b=0.1$, initial conditions $x_1(0) = 0.8147$, $x_2(0) = 0.9057$, $x_3(0) = 0.1269$. The projection of the state space on the $(x_1, x_3)$ plane (left) and the projection of the state space on the $(x_1, x_2)$ plane (right).

Figure 2.6: The phase space of the Hitzl-Zele map, for $a = 0.25$, $b = 0.87$ and the initial conditions $x_1(0) = 0.8143$, $x_2(0) = 0.2435$, $x_3(0) = 0.9293$. $N = 10000$ iterations.

2.4 A continuous time system: The Colpitts oscillator.

1 Theoretical analysis of the oscillator.

The PSpice scheme of the Colpitts oscillator is given in Fig. 2.11. Notations and assumptions are done in its context, as follows:

The npn BJT transistor [52] is considered to be in the forward active region. This assumption, implies that the collector current $I_C$ is approximatively equal to the emitter current $I_E$, while the base current $I_B$ is much lower than the current through the collector.

The voltage difference between the base and the emitter $V_{BE}$ is much higher than the thermal voltage $V_T$, which, from the Ebers-Moll model (2.19), implies that the approximation (2.20) is valid.
Figure 2.7: The three dimensional Hitzl-Zele map, for $a=0.25$ and $b=0.87$ and the initial conditions $x_1(0) = 0.8143$, $x_2(0) = 0.2435$, $x_3(0) = 0.9293$. $N = 10000$ iterations. The evolution of its states $x_1(k), x_2(k), x_3(k)$, with $k \in \{0, \ldots, N\}$.

\[
I_E = I_s \cdot \left( e^{\frac{V_{BE}}{V_T}} - 1 \right) \\
I_C = \alpha_F \cdot I_E \\
I_B = (1 - \alpha_F) \cdot I_E
\]  

(2.19)

where $I_S$ is the saturation inverse current of the transistor. $V_T = \frac{k_B T}{q}$ is the thermal voltage, with $k_B$ the Boltzmann constant, relating energy at the individual particle level with temperature. It represents the ratio between the gas constant $R$ and the Avogadro constant $N_A$ ($k_B = 8.6173324(78) \cdot 10^{-5} \text{eV} \cdot K^{-1}$) [52]. $T$ is the absolute temperature in Kelvin. $q$ is the magnitude of the electrical charge on the electron ($q = 1.602176565(35) \cdot 10^{-19} \text{Coulomb}$). In semiconductors, the relationship between the flow of electrical current and the electrostatic potential across a $p-n$ junction depends on the thermal voltage. At room temperature ($T \approx 300K$), $V_T \approx 26mV$. The thermal voltage $V_T$ is a measure of how much the spatial distribution of electrons or ions is affected by a boundary held at a fixed voltage.

$\alpha_F$ is the common base forward short circuit current gain ($\alpha_F \approx 0.9$).

\[
I_E = I_s \cdot \left( e^{\frac{V_{BE}}{V_T}} \right)
\]  

(2.20)
Figure 2.8: The three dimensional Hitzl-Zele map, for $a=0.25$ and $b=0.87$ and the initial conditions $x_1(0) = 0.8143$, $x_2(0) = 0.2435$, $x_3(0) = 0.9293$. $N = 10000$ iterations. Their probability density functions, $p_{X_1}(x_1), p_{X_2}(x_2), p_{X_3}(x_3)$.

The Colpitts oscillator in Fig. 2.11 is in common-base configuration, with $LC$-tank circuit. In this subsection, the analysis of the circuit is done:

- From the Kirchhoff’s second (voltage) theorem, it results that:
  \[ V_{BE} + v_{C_2} = 0 \implies V_{BE} = -v_{C_2} \]  \hspace{1cm} (2.21)

- The current through the capacitor $C_1$ results from the Kirchhoff’s first theorem.
  \[ -i_{C_1} - I_C + i_L = 0 \implies i_{C_1} = i_L - I_C \]  \hspace{1cm} (2.22)

- Applying Kirchhoff’s first (current) theorem $I = I_C - I_0$, with $I_0 = \frac{V_2}{R_2}$ and $i_{C_2} = I + i_{C_1}$. The equation (2.23) expresses the current through the capacitor $C_2$.
  \[ i_{C_2} = i_L - I_0 \]  \hspace{1cm} (2.23)

- The Kirchhoff’s second theorem gives the expression in equation (2.24), for the voltage across the coil.
  \[ v_L = -(v_{C_1} + v_{C_2}) - i_L + V_1 \]  \hspace{1cm} (2.24)
Figure 2.9: The three dimensional Hitzl-Zele map, for $a=0.25$ and $b=0.87$ and the initial conditions $x_1(0) = 0.8143$, $x_2(0) = 0.2435$, $x_3(0) = 0.9293$. $N = 10000$ iterations. The projections of the phase space in the $(x_1,x_2), (x_1,x_3), (x_2,x_3)$ planes.

Figure 2.10: The Hitzl-Zele map. The spectrum of the Lyapunov exponents when the parameter $a = 0.25$ is kept fixed (left) or the parameter $b = 0.87$ is kept fixed (right). The initial conditions are $x_1(0) = 0.8143, x_2(0) = 0.2435$ and $x_3(0) = 0.9293$

It is known [51] that:

$$i_C(t) = i_C(0) + C \cdot \frac{dv_C(t)}{dt}$$
$$v_L(t) = v_L(0) + L \cdot \frac{di_L(t)}{dt}$$

Making the notation $v_C_1 = x_1$, $v_C_2 = x_2$, $i_L = x_3$, and using the known notation
\[ \frac{dx}{dt} = \dot{x}, \] the equations (2.22), (2.23) and (2.24) become:

\[
\begin{align*}
\dot{x}_1 &= -\frac{I_0}{C_2} \cdot e^{\frac{x_2}{VT}} + x_3 \\
\dot{x}_2 &= -\frac{I_0}{C_2} + \frac{1}{C_2} \cdot x_3 \\
\dot{x}_3 &= -\frac{1}{L} (x_1 + x_2) - \frac{R_1}{L} x_3 + V_1
\end{align*}
\] (2.26)

In the system (2.26) the term \( \frac{R_1}{L} \) corresponds to the quality \( Q \) factor of the tank \( RLC \)-circuit, \( Q = \frac{\omega_0}{R_1} \).

Although not specified, the states \( x_i \), with \( i \in \{1, 2, 3\} \) depend on time. The relation between the frequency \( f \) and the time \( t \) is \( f \cdot t = 1 \).

The oscillation frequency of the Colpitts oscillator is given by equation (2.27).

\[ f_0 = \frac{1}{2\pi \sqrt{L \frac{C_1 C_2}{C_1 + C_2}}} \] (2.27)

The loop gain of the oscillator when the phase condition of the Barkhausen criterion is satisfied, function of the circuit parameters, is given by equation (2.28). With \( k = \frac{C_2}{C_1 + C_2} \) is noted a scaling factor. For a detailed analysis see [61].

\[ g = \frac{I_0 L}{VT R_1 (C_1 + C_2)} \] (2.28)

The voltages, the currents and the time were normalized in [61]. Taking into account the physical signification of \( Q, g \) and \( k \), the state equations (2.26) became:

\[
\begin{align*}
\dot{x}_1 &= \frac{g}{Q(1-k)} (e^{-x_2} + 1 + x_3) \\
\dot{x}_2 &= \frac{g}{Q} \cdot x_3 \\
\dot{x}_3 &= -\frac{Qk(1-k)}{g} (x_1 + x_2) - \frac{1}{Q} x_3
\end{align*}
\] (2.29)

For an analog implementation of the chaotic common base Colpitts oscillator, we used the values \( R_1 = 10 \Omega, R_2 = 1.2k \Omega, C_1 = C_2 = 100nF, L = 2.2mH \).
$1.1 \text{mH}, Q_1 = 2N4401BJT$. The oscillation frequency of the Colpitts oscillator is, in this case, $f_0 \approx 21.46\text{kHz}$. Chaos was obtained for $V_1 = 9.7V$ and $V_2 = -6.1V$.

The Simulink normalized model was simulated and the phase portrait from Fig. 2.12 was obtained. Its projections in the coordinates $(x_1, x_2)$, $(x_1, x_3)$, $(x_2, x_3)$ are illustrated in Fig. 2.13. The temporal evolutions of the states of the system are presented in Fig. 2.14 and their probability density functions in Fig. 2.15.

![Figure 2.12: The phase space of the chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$.](image)

**2 The Lyapunov Exponents**

We modified the program written for the Lorenz chaotic system, so that it became suitable for the Colpitts chaotic oscillator with parameters $g = 4.46$, $Q = 1.38$, $k = 0.5$, initial conditions $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The result might be seen in Fig. 2.16.

The chaotic systems analyzed in this chapter from the point of view of the Lyapunov exponents, will serve as examples for the results of the research work we have developed, in the next chapters.
Figure 2.13: The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. Projections in the planes defined by its states.
Figure 2.14: The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The temporal evolution of its states.
Figure 2.15: The chaotic Colpitts oscillator for bifurcation parameters $g = 4.46$, $Q = 1.38$ and scaling factor $k = 0.5$. The initial conditions are $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The probability distribution functions of its states.

Figure 2.16: The Lyapunov exponents for the Colpitts chaotic oscillator with parameters $g = 4.46$, $Q = 1.38$, $k = 0.5$, initial conditions $x_1(0) = 0.6221$, $x_2(0) = 0.3510$ and $x_3(0) = 0.5132$. The Lyapunov exponents are shown for $\lambda^1 = -0.867$, $\lambda^2 = 0.009$, and $\lambda^3 = -0.320$, respectively.
Chapter 3

Observability Indexes and Observability-Singularity Manifolds.

3.1 Introduction

In the '80s Takens, in [76], formulated the conditions that ensure the capability to reconstruct the dynamics of a transmitter when an observer receives one scalar output of the transmitter.

In a number of practical situations, the reconstruction of the original system is strongly influenced by the choice of the observable (the output of the system). That influence is analyzed by Letellier et. al in [57].

In the following sections, we investigate the behavior of the systems presented in Chapter 2, under the different choices for the observable output of the considered system. The next two subsections present two algorithms used in order to investigate the structural properties of the studied chaotic systems.

1 Observability index

The algorithm used to calculate the observability indexes is described in [34]. The steps of this algorithm are given below. See Section 3.2 for the illustration in the case of the generalized Hénon map, Section 3.3 for the Hitzl-Zele map and Section 3.4 for the chaotic Colpitts oscillator.

1. Write the fluency matrix. In the Jacobian matrix corresponding to the studied system, replace each constant element by 1, each variable element (a nonlinear term in the vector field) by −1. If the element of the Jacobian is neither constant, nor variable, its corresponding value in the fluency matrix will be 0.

2. Define by $C_{1,i}$ the column vectors corresponding to each state of the studied system, $i$ corresponding to the measured state variable $x_1$, $x_2$ or $x_3$. A value of 1 indicates the state which was chosen to reconstruct the dynamics of the system (the state is the one the receiver measures).

Replace the diagonal element of the fluency matrix corresponding to each variable by a dot and multiply each row of it by the corresponding element in $C_{1,i}$. Matrices $H_{1,i}$ are obtained.

3. Count the number $p_{1,i}$ of linear elements and the number of $q_{s}^{1}$ of nonlinear elements in $H_{1,i}$
4. Replace the dot in $H_{1,i}$ by 0, 1 or $\bar{1}$ according to the fluency matrix, and transpose $H_{1,i}$.

5. Count the number of non-null elements of each row, defining the new column vectors $C_{2,i}$.

6. Obtain the matrices $H_{2,i}$ by replacing each non zero element of $H_{1,i}^T$ by a dot and the rest of the elements by their corresponding elements in the fluency matrix multiplied by the corresponding element of the column vector $C_{2,i}$.

7. Count the number $p_{2,i}$ of linear elements and the number of $q_{2,i}$ of nonlinear elements in $H_{2,i}$.

8. Compute the observability coefficients with formula (3.1):

$$\eta_i = \frac{1}{2} \left[ \frac{p_{1,i}}{p_{1,i} + q_{1,i}} + \frac{q_{1,i}}{(p_{1,i} + q_{1,i})^3} + \frac{p_{2,i}}{p_{2,i} + q_{2,i}} + \frac{q_{2,i}}{(p_{2,i} + q_{2,i})^2} \right]$$

(3.1)

where $p_{1,i} + q_{1,i} = 1 + q_{1,i}$, if $p_{1,i} = 0$ or $p_{2,i} + q_{2,i} = 1 + q_{2,i}$, if $p_{2,i} = 0$.

2 Observability singularity manifolds

A system is said to be observable when, by measuring the sequence of values of one of the system’s states, the entire phase space of the system can be reconstructed, under a suitable smooth transformation.

The study of the observability properties of a system is performed under the assumption that the parameters of the system are known.

The work of Hermann and Krener [42] deals with the concepts of controllability and observability in the context of nonlinear dynamical systems as a further step of the already well-known, in the '70s, properties of the linear dynamics. Diop and Fliess discuss the algebraic frame of these properties in [25].

The singularity observability manifold $S_O$ of a chaotic system is the mathematical space in which, seen from the measured variable, the system loses its observability property.

Some definitions are given in the case of the discrete-time hyper-chaotic Rössler map in [34]. Let us consider a nonlinear discrete system described in the three-dimensional space $\mathbb{R}^3$, with $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ the state vector evaluated at the $k$-th iteration. Let the evolution of the system at the next iteration $k + 1$ be $x^+ = x(k + 1)$. Using the sequence of values of the observable $\{x_i(k)\}$ and its subsequent iterations till the $n - 1$-th order it is possible to reconstruct the entire phase space of the system that produced the measured state. In the considered case, $n = 3$ denotes the dimension of the involved attractor. The coordinate change between the original three-dimensional real phase space $(x_1, x_2, x_3)$ and the iterative embedding $(X, Y, Z)^T \in \mathbb{R}^3$ is defined by equations (3.2).

$$\phi_i = \begin{cases} X = s = x_i \\ Y = s^+ = x_i^+ \\ Z = s^{++} = x_i^{++} \end{cases} \quad (3.2)$$

The observability matrix $O_i$ of a nonlinear system observed from the perspective of the $i$-th state variable of the system is the Jacobean of the application $\phi_i$, as defined in [63] and in [57] for continuous systems. The observation matrix $O_i$ is then expressed by equations (3.3).
\[ O_i = \begin{bmatrix}
\frac{\partial X}{\partial x_1} & \frac{\partial X}{\partial x_2} & \frac{\partial X}{\partial x_3} \\
\frac{\partial Y}{\partial x_1} & \frac{\partial Y}{\partial x_2} & \frac{\partial Y}{\partial x_3} \\
\frac{\partial Z}{\partial x_1} & \frac{\partial Z}{\partial x_2} & \frac{\partial Z}{\partial x_3}
\end{bmatrix} \quad (3.3) \]

When the map \( \phi_i \) defines a global diffeomorphism, being also injective, and its determinant is different from zero, the application is associated with a fully observable system. When the determinant \( \det(O_i) \) is always non-null, the function \( \phi_i \) can be inverted everywhere, a reiterative form for the original system can always be found, as shown by equations (3.4).

\[
\begin{align*}
X^+ &= Y \\
Y^+ &= Z \\
Z^+ &= F_i(X,Y,Z)
\end{align*} \quad (3.4)
\]

where the function of the model \( F_i(X,Y,Z) \) is non-singular and subscript \( i \) corresponds to the measured state variable.

The studied system is said to be non-fully observable when the determinant of the observability matrix is null over some subspace of the phase space. The states cannot be distinguished in those subspaces of the reconstructed phase space constructed from the chosen observable. The observability singularity manifold \( S_{\bar{O}} \) is the subspace where the map \( \phi_i \) cannot be inverted. The system cannot be, thus, rewritten as in (3.4). The mathematical expression of this hyper-surface is given in equation (3.5).

\[
S_{O,i} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | \det(O_i) = 0\} \quad (3.5)
\]

where \( i \) is the number of the state variable that is measured.

In conclusion, in order to choose the best state variable to be the output of the transmitter, one should investigate the structural properties this variable induces to the system. The quality of the chosen measured variable is a function of the existence of the singularities and their intersection with the attractor of the considered system.

### 3.2 Case study. The generalized Hénon map.

In this section the observability indexes are calculated for the chaotic system with the analytical form given by equations (2.17), namely

\[
\begin{align*}
x_1^+ &= a - x_2^2 - bx_3 \\
x_2^+ &= x_1 \\
x_3^+ &= x_2
\end{align*}
\]

Moreover, the singularity observability manifolds are determined, for each of the state variables considered as the output of the transmitter.

### 1 Observability indexes

The Jacobian matrix of the chaotic system (2.17) is given by the formula (3.6) and its corresponding fluency matrix is expressed by (3.7).
\[
J = \begin{bmatrix}
0 & -2x_2 & -b \\
1 & 0 & 0 \\
0 & 1 & 0 \\
\end{bmatrix}
\] (3.6)

\[
F_{ij} = \begin{bmatrix}
0 & 1 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0 \\
\end{bmatrix}
\] (3.7)

The column vectors \( C_{1,i} \) with \( i \in \{1, 2, 3\} \) are:

\[
C_{1,1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad C_{1,2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad C_{1,3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}
\] (3.8)

The matrices \( H_{1,i} \) with \( i \in \{1, 2, 3\} \) have the following expressions:

\[
H_{1,1} = \begin{bmatrix}
\bullet & 1 & 1 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad H_{1,2} = \begin{bmatrix}
0 & 0 & 0 \\
1 & \bullet & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad H_{1,3} = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & \bullet \\
\end{bmatrix}
\] (3.9)

The numbers \( p_{1,i} \) of linear elements and the numbers \( q_{1,i} \) of nonlinear elements are:

\[
p_{1,1} = 1, \quad p_{1,2} = 1, \quad p_{1,3} = 1 \\
q_{1,1} = 1, \quad q_{1,2} = 0, \quad q_{1,3} = 0
\] (3.10)

The \( H_{1,i}^T \) matrices are given by:

\[
H_{1,1}^T = \begin{bmatrix}
0 & 0 & 0 \\
1 & 0 & 0 \\
1 & 0 & 0 \\
\end{bmatrix}, \quad H_{1,2}^T = \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad H_{1,3}^T = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0 \\
\end{bmatrix}
\] (3.11)

The column vectors \( C_{2,i} \) with \( i \in \{1, 2, 3\} \) are:

\[
C_{2,1} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \quad C_{2,2} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad C_{2,3} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}
\] (3.12)

The matrices \( H_{1,i} \) with \( i \in \{1, 2, 3\} \) have the following expressions:

\[
H_{2,1} = \begin{bmatrix}
0 & 0 & 0 \\
\bullet & 0 & 0 \\
\bullet & 1 & 0 \\
\end{bmatrix}, \quad H_{2,2} = \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad H_{2,3} = \begin{bmatrix}
0 & 0 & 0 \\
1 & 0 & \bullet \\
0 & 0 & 0 \\
\end{bmatrix}
\] (3.13)

The number \( p_{2,i} \) of linear and the number \( q_{2,i} \) of nonlinear elements:

\[
p_{2,1} = 1, \quad p_{2,2} = 1, \quad p_{2,3} = 1 \\
q_{2,1} = 0, \quad q_{2,2} = 0, \quad q_{2,3} = 0
\] (3.14)
The observability indexes are computed with the formula (3.1):

\[
\eta_1 \approx 81.25\% \\
\eta_2 = 100\% \\
\eta_3 = 100\%
\]  

(3.15)

Given the result in (3.15), from the cryptographer’s point of view, the best choice in order to embed the secret message is either the second, or the third state variable of the generalized Hénon map. The cryptanalyst will be puzzled by the existence of the singularities in the observability. The next subsection is dedicated to the investigation in that direction. The parameters \(a\) and \(b\) are kept fixed at the values 1.76, respectively 0.1.

2 Observability singularity manifolds.

We consider the measured variable to be \(s_1 = x_1\). The coordinate transformation between the original phase space and the iterative embedding is given by the expression in (3.16). The corresponding observability matrix is then \(O_1\) described by equations (3.17). Consequently, the determinant of the observability matrix \(O_1\) has the value \(\Delta_{x_1} = b^2\), which is constant and is not null. This implies that, when seen from the perspective of its first state variable, \(x_1\), the generalized Hénon map has no observability singularity manifold.

\[
\phi_1 = \begin{cases} 
X = x_1 \\
Y = x_1^\ast = a - x_2^2 - b \cdot x_3 \\
Z = x_1^{++} = a - x_1^2 - b \cdot x_2 
\end{cases} 
\]  

(3.16)

\[
O_1 = \begin{bmatrix} 
1 & 0 & 0 \\
0 & -2 \cdot x_2 & -b \\
-2 \cdot x_1 & -b & 0 
\end{bmatrix} 
\]  

(3.17)

Following, we determine the observability singularity manifold corresponding to the second state variable \(x_2\) as the measured variable. The coordinate transformations are, thus, given by \(\phi_2\) with equations (3.18) and the assigned observability matrix \(O_2\) has the expression in (3.19). The determinant \(det(O_2) = \Delta_{x_2} = b\) is constant and it is not zero, implying no observability singularity.

\[
\phi_2 = \begin{cases} 
X = x_2 \\
Y = x_1 \\
Z = a - x_2^2 - b \cdot x_3 
\end{cases} 
\]  

(3.18)

\[
O_2 = \begin{bmatrix} 
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & -2 \cdot x_2 & -b 
\end{bmatrix} 
\]  

(3.19)

From the perspective of the third state variable \(x_3\), the coordinate transform is realized by the equations (3.20), with the observability matrix in (3.21). The matrix \(O_3\) has the determinant \(\Delta_{x_3} = -1\). Thus, there exists no observability singularity manifold.
\[ \phi_3 = \begin{cases} X = x_3 \\ Y = x_2 \\ Z = x_1 \end{cases} \tag{3.20} \]

\[ O_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \tag{3.21} \]

The generalized Hénon map has no singularity of observability, regardless the state variable chosen for the embedding of its dynamics. We conclude this map is suitable for a simple enciphering algorithm. We will give an example of such a cipher in Chapter 6.1.

### 3.3 Case study. The Hitzl-Zele map.

Let us consider the discrete-time three-dimensional chaotic system described by equations (2.18). The vector of the bifurcation parameters is given by \((a, b) = (0.25, 0.87)\), for the analysis of the observability singularity manifolds induced by each of the state variables of the system.

#### 1 Observability coefficients.

The Jacobian matrix assigned to the Hitzl-Zele map, equations (2.18), and the fluency matrix corresponding to the chaotic system are expressed by equations (3.22) and (3.23).

\[ F_{ij} = \begin{bmatrix} -2x_1x_3 & 1 & -x_1^2 \\ a & 0 & 0 \\ 2bx_1 & 0 & 1 \end{bmatrix} \tag{3.22} \]

\[ F_{ij} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \tag{3.23} \]

The column vectors \(C_{1,i}\) with \(i \in \{1, 2, 3\}\) are:

\[ C_{1,1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad C_{1,2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad C_{1,3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \tag{3.24} \]

The matrices \(H_{1,i}\) with \(i \in \{1, 2, 3\}\) have the following expressions:

\[ H_{1,1} = \begin{bmatrix} \bullet & 1 & \bar{1} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad H_{1,2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad H_{1,3} = \begin{bmatrix} 0 & 0 & 0 \\ \bar{1} & 0 & \bullet \end{bmatrix} \tag{3.25} \]

The number \(p_{1,i}\) of linear elements and the number \(q_{1,i}\) of nonlinear elements are:
The $H_{i,1}^T$ matrices are given by:

$$H_{i,1}^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$H_{i,2}^T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$H_{i,3}^T = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The column vectors $C_{2,i}$ with $i \in \{1, 2, 3\}$ are:

$$C_{2,1} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$C_{2,2} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$C_{2,3} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

The matrices $H_{i,1}$ with $i \in \{1, 2, 3\}$ have the following expressions:

$$H_{2,1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$H_{2,2} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$H_{2,3} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The number $p_{2,i}$ and the number $q_{2,i}$ of linear and nonlinear elements:

$$p_{2,1} = 2 \quad p_{2,2} = 0 \quad p_{2,3} = 1$$

$$q_{2,1} = 1 \quad q_{2,2} = 2 \quad q_{2,3} = 2$$

The observability indexes are computed with the formula (3.1):

$$\eta_1 \approx 70.14\%$$

$$\eta_2 \approx 61.11\%$$

$$\eta_3 \approx 34.03\%$$

Evaluating the result in (3.31), we can conclude that the first state variable of the Hitzl-Zele map, $x_1$, is the best choice for the embedding of the secret message, while $x_3$ is the weakest state variable, for the cryptographic use.

2 Observability singularity hyper-surfaces.

We consider the measured variable to be $s_1 = x_1$. The coordinate transformation between the original phase space and the iterative embedding is given by the expressions in (3.32). The corresponding observability matrix is then $O_1$ described by equations (3.33).

$$\phi_1 = \begin{cases} X = x_1 \\ Y = x_2 - x_3 \cdot x_1^2 + 1 \\ Z = x_2^+ - x_3^+ \cdot x_1^2 + 1 \end{cases}$$

$$\phi_1 = \begin{cases} X = x_1 \\ Y = x_2 - x_3 \cdot x_1^2 + 1 \\ Z = x_2^+ - x_3^+ \cdot x_1^2 + 1 \end{cases}$$

43
\[
O_1 = \begin{bmatrix}
1 & 0 & 0 \\
-2x_1x_3 & 1 & -x_1^2
\end{bmatrix}
\]  
(3.33)

where \(E_1, E_2, E_3\) are \(\frac{\partial Z}{\partial x_1}\), \(\frac{\partial Z}{\partial x_2}\) and \(\frac{\partial Z}{\partial x_3}\) respectively. Its determinant is \(\det(O_1) = \Delta x_1 = x_1^2 E_2 + E_3\).

In the expression \(Z = 1 + ax_1 - (bx_1^2 + x_3 - 0.5)(-x_1^2 x_3 + x_2 + 1)^2\), when differentiated to obtain \(E_2\) and \(E_3\), in order to obtain the determinant of the observability matrix \(O_1\) the term in \(x_1\) is negligible. Thus, \(E_2 = (1 + x_2)(2bx_1^2 - 2x_3 + 1) - x_3(-2bx_1^2 + x_1^2 + 2x_3)\) and \(E_3 = -(1 + x_2)(2bx_1^4 + x_1^2 + 4x_1^2 x_3 + x_2 + 1) + x_1^2 x_3(3x_3 + 2bx_1^2 + 1)\). Substituting \(E_2\) and \(E_3\) in the expression of the determinant of the matrix \(O_1\), the result in equation (3.34) is obtained for the observability singularity manifold computed from the observable \(s_1 = x_1\).

\[
S_{O,1} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid -(1 + x_2)(6x_1^2 x_3 + 2x_1^2 + x_2 + 2) + x_1^2 x_3(3x_1^2 - 2) = 0\}
\]  
(3.34)

Given the complexity of the expression corresponding to the observability singularity manifold \(S_{O,1}\), we have computed the values of the determinant \(\det(O_1)\) over \(N = 30000\) iterations. We obtained the probability density function of \(\det(O_1)\) by distributing these values in 100 classes and normalizing for the \(N\) iterations. In Fig. 3.1 one can observe that the computed determinant never becomes zero.

When the measured state variable is \(x_2\), the coordinate transformation between the original phase space and the iterative embedding is given by the expression in (3.35). The corresponding observability matrix is then \(O_1\) described by equations (3.36).

\[
\phi_2 = \begin{cases}
X = x_2 \\
Y = a \cdot x_1 \\
Z = a \cdot (1 + x_2 - x_3 \cdot x_1^2)
\end{cases}
\]  
(3.35)

\[
O_2 = \begin{bmatrix}
0 & 1 & 0 \\
a & 0 & 0 \\
-2x_1x_3 & a & -ax_1^2
\end{bmatrix}
\]  
(3.36)

The determinant observability singularity manifold is thus given by the equation (3.37).

\[
S_{\tilde{O},2} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid -a^2 \cdot x_1^2 = 0\}
\]  
(3.37)

When the measured state variable is \(x_3\), the coordinate transformation between the original phase space and the iterative embedding is given by the expression in (3.38). The corresponding observability matrix is then \(O_3\) described by equations (3.39).

\[
\phi_3 = \begin{cases}
X = x_3 \\
Y = b \cdot x_1^2 + x_3 - 0.5 \\
Z = b \cdot x_1^2 + x_3 + b \cdot (1 + x_2 - x_3 \cdot x_1^2)^2 - 1
\end{cases}
\]  
(3.38)
\[ O_3 = \begin{bmatrix} 0 & 0 & 1 \\ 2bx_1 & 0 & 1 \\ E_1 & E_2 & E_3 \end{bmatrix} \]  

(3.39)

where \( E_1 = \frac{\partial Z}{\partial x_1} \), \( E_2 = \frac{\partial Z}{\partial x_2} \) and \( E_3 = \frac{\partial Z}{\partial x_3} \).

The determinant of the observability matrix is \( \Delta_{x_3} = \det(O_3) = 2 \cdot b \cdot x_1 \cdot E_2 \). The expression of the derivative \( E_2 \) is \( 2 \cdot b \cdot ( -x_1^2 \cdot x_3 + x_2 + 1 ) \). Consequently, the observability singularity manifold is given by the equation (3.40).

\[ S_{O,3} = \{ (x_1, x_2, x_3) \in \mathbb{R}^3 | 4b^2 x_1 (-x_1^2 + x_2 + 1) = 0 \} \]  

(3.40)

By analyzing Fig. 3.1, we can decide that the first state variable of the system implies an observability singularity manifold with a complicated expression, but no intersection with the attractor (the determinant \( \Delta_{x_1} \) never becomes null). In order to determine which of the other two state variables implies a more convenient manifold for the observability singularity, we consider a small segment on which the determinants \( \Delta_{x_2} \) and \( \Delta_{x_3} \) tend to zero. When this segment is considered \([v_1, v_2] = [-6 \cdot 10^{-4}, 6 \cdot 10^{-4}]\), the probabilities are \( P(v_1 \leq \Delta_{x_2} \leq v_2) = 0.0054 \) and \( P(v_1 \leq \Delta_{x_3} \leq v_2) = 0.00084 \). These probabilities indicate \( x_2 \) as being the measured variable which generates more singularities.

We conclude that the best choice for the observable of the Hitzl-Zele map, from the cryptographic point of view is the state variable \( x_2 \), engendering the greatest intersection between the original strange attractor and the observability singularity manifold, and being 61.11% observable.
Figure 3.1: The probability density functions for the determinant of the observability matrices determined by the three state variables of the Hitzl-Zele map. Parameters $a = 0.25$ and $b = 0.87$. 
3.4 Case study. The Colpitts chaotic oscillator.

1 Observability indexes.

The Jacobian and the fluency matrices corresponding to the equations which describe the Colpitts oscillator, (2.29), are given by the equations (3.41) and (3.42), respectively.

\[
J = \begin{bmatrix}
0 & \dot{x}_2 \cdot e^{-x_2} & A \\
0 & 0 & A \\
-\frac{k}{A} & -\frac{k}{A} & -B
\end{bmatrix}
\]

(3.41)

with \( A = \frac{g}{Q(1-k)} = \frac{g}{k} \), for \( k = 0.5 \) and \( B = -\frac{4}{Q} \).

\[
F_{ij} = \begin{bmatrix}
0 & 1 & 1 \\
0 & 0 & 1 \\
1 & 1 & 1
\end{bmatrix}
\]

(3.42)

The Taylor series for the exponential function \( e^{x_2} \) at \( x_2 = 0 \) (3.43) was used to approximate the term \( e^{-x_2} \).

\[
e^{-x_2} = \sum_{n=0}^{\infty} \frac{(-x_2)^n}{n!}
\]

(3.43)

The column vectors \( C^1_s \), for \( s = x_1, x_2, x_3 \):

\[
C_{1,1} = \begin{bmatrix}
1 \\
0 \\
0
\end{bmatrix}, \quad C_{1,2} = \begin{bmatrix}
0 \\
1 \\
0
\end{bmatrix}, \quad C_{1,3} = \begin{bmatrix}
0 \\
0 \\
1
\end{bmatrix}
\]

and the matrices \( H_{1,i} \), with \( i \in \{1, 2, 3\} \):

\[
H_{1,1} = \begin{bmatrix}
\bullet & 1 & 1 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}, \quad H_{1,2} = \begin{bmatrix}
0 & 0 & 0 \\
0 & \bullet & 1 \\
0 & 0 & 0
\end{bmatrix}, \quad H_{1,3} = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
1 & 1 & \bullet
\end{bmatrix}
\]

Thus, the number \( p_{1,i} \) of the linear elements and the number \( q_{1,i} \) of the nonlinear elements in the \( H_{1,i} \) matrices are:

\[
p_{1,1} = 1, \quad p_{1,2} = 1, \quad p_{1,3} = 2 \\
q_{1,1} = 1, \quad q_{1,2} = 0, \quad q_{1,3} = 0
\]

The transposed \( H^T_{1,i} \) matrices are:

\[
H^T_{1,1} = \begin{bmatrix}
0 & 0 & 0 \\
1 & 0 & 0 \\
1 & 0 & 0
\end{bmatrix}, \quad H^T_{1,2} = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 1 & 0
\end{bmatrix}, \quad H^T_{1,3} = \begin{bmatrix}
0 & 0 & 1 \\
0 & 0 & 1 \\
0 & 0 & 1
\end{bmatrix}
\]

The column vectors \( C^2_s \), for \( s = x_1, x_2, x_3 \):

\[
C_{2,1} = \begin{bmatrix}
0 \\
1 \\
1
\end{bmatrix}, \quad C_{2,2} = \begin{bmatrix}
0 \\
0 \\
1
\end{bmatrix}, \quad C_{2,3} = \begin{bmatrix}
1 \\
1 \\
1
\end{bmatrix}
\]

(3.44)

The matrices \( H_{2,i} \) have the expressions:
For the chaotic system in (2.29), the bifurcation parameters are kept at fixed values

The observability coefficients are computed using the formula (3.1). The obtained values are \( \eta_1 = 0.7325, \eta_2 = 1, \eta_3 = 0.8888 \). Taking into account the significance from [34], where a value of 1 means a full observable state, and a 0 value is synonym with the absence of the observability in the considered coordinate, the values obtained for the observability coefficients indicate 73.25% observability for \( x_1 \), 100% observable for \( x_2 \) and 88.89% observable for \( x_3 \).

The conclusion is that the worse situation regarding the property of observability is the scenario in which \( x_1 \) is chosen as the output of the chaotic system (2.29).

In the subsection 2 we determine the singularity observability manifolds when \( x_1, x_2, \) or \( x_3 \) is taken as the output.

2 Observability singularity manifolds.

For the chaotic system in (2.29), the bifurcation parameters are kept at fixed values \( g = 4.46 \) and \( Q = 1.38 \).

In the context in which the observable is chosen to be \( s_1 = x_1 \), the transformation between the original phase space and the differential embedding is given by:

\[
\begin{align*}
X &= s_1 = x_1 \\
Y &= s_1 = \dot{x}_1 \\
Z &= \ddot{s}_1 = \ddot{x}_1
\end{align*}
\]

It results that \( Y = A[\dot{e}^{-x_2} + x_3 + 1] \) and \( Z = A[\dot{x}_2 e^{-x_2} + \dot{x}_3] = A^2 e^{-x_2} x_3 - k(x_1 + x_2) + ABx_3 \). The observability matrix \( O_1 \) is given in (3.47).

\[
O_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -E_1 & A \\ -k & E_2 & E_3 \end{bmatrix}
\]

To obtain the observability-singularity manifold \( S_{O,1} \) the determinant \( \Delta O_1 = E_1 \cdot E_3 - A \cdot E_2 \) should be null. Replacing the expressions for \( E_1 = \frac{\partial^2 Y}{\partial x_2^2}, E_2 = \frac{\partial Z}{\partial x_2}, E_3 = \frac{\partial Z}{\partial s_3} \), the determinant of the observability matrix \( O_1 \) is given by \( \Delta x_1 = A^4 x_3 (e^{-x_2})^2 + A^3 x_3 e^{-x_2} (B + A x_3) + Ak \). The analysis of the Fig. 3.2 (top) conduces at the conclusion that this determinant becomes null almost always in the evolution of the Colpitts chaotic oscillator for parameters \( Q = 1.38, g = 4.46 \) and a simulation for 400s, with a fundamental sampling time of \( T_s = 1 \text{ms} \).

\[
S_{O,1} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | A^3 x_3 e^{-x_2} (e^{-x_2} + A x_3 + B) + Ak = 0 \}
\]

If the output is considered to be the second state of the system (2.29), then:

\[
\begin{align*}
X &= x_2 \\
Y &= \dot{x}_2 = Ax_3 \\
Z &= \ddot{x}_2 = A \ddot{x}_3 = -k(x_1 + x_2) + ABx_3
\end{align*}
\]
which results in an observability matrix having the expression in (3.49):

\[
O_2 = \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & A \\
-k & -k & AB
\end{bmatrix}
\] (3.49)

To obtain the surfaces of observability-singularity, the determinant of the observability matrix \( \Delta x_2 = -kA \) should be null. This is obvious that the value of the determinant \( \Delta x_2 \) is a non-null constant. We can conclude the same observing the probability density function \( p(\Delta x_2) \) in Fig. 3.2.

\[
S_{O,2} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | -kA = 0\}
\] (3.50)

If the output is considered to be the third state of the system (2.29), then:

\[
\phi_3 : \begin{cases}
X = x_3 \\
Y = \dot{x}_3 = -\frac{k}{A}(x_1 + x_2) + Bx_3 \\
Z = \ddot{x}_3 = -\frac{k}{A}(\dot{x}_1 + \dot{x}_2) + B\dot{x}_3
\end{cases}
\]

which results in an observability matrix having the expression in (3.51):

\[
O_3 = \begin{bmatrix}
0 & 0 & 1 \\
-k & -\frac{k}{A} & B \\
E_1 & E_2 & E_3
\end{bmatrix}
\] (3.51)

The expression \( Z = -k(e^{-x_2} + 2x_3 + 1) - \frac{kB}{A}(x_1 + x_2) + B^2x_3 \), conduces to \( E_1 = \frac{\partial Z}{\partial x_1} = -\frac{kB}{A} \) and \( E_2 = \frac{\partial Z}{\partial x_2} = \frac{k}{A}(-\frac{kB}{A} + kAx_3e^{-x_2} + \frac{kB}{A}) = k^2x_3e^{-x_2} \). The determinant \( \Delta x_3 \) is, thus, equal to \( \frac{k}{A}(E_1 - E_2) \). The observability-singularity manifold is given by equation (3.52).

\[
S_{O,3} = \{(x_1, x_2, x_3) \in \mathbb{R}^3 | x_3e^{-x_2} = 0\}
\] (3.52)

We show, in Fig. 3.2 (bottom), that the determinant \( \Delta x_3 \) is null almost everywhere. Among the two state variables \( x_1 \) and \( x_3 \) that engender observability singularity manifolds that intersect the strange attractor of the chaotic system almost always, we choose \( x_1 \), due to the fact that its dispersion is smaller than for \( x_3 \).
Figure 3.2: The probability density functions for the determinant of the observability matrices determined by the three state variables of the Colpitts chaotic oscillator. Parameters $Q = 1.38$ and $g = 4.46$. 
Regarding the observability analysis of the two discrete time systems, we conclude that the Hitzl-Zele map with $x_2$ as output is the most interesting from a cryptography point of view. Moreover, the observability analysis of the Colpitts oscillator allows to highlight that the mathematical tools use in continuous-time and discrete-time case are quite similar.

We conclude this section by few comments with respect to the extra difficulty to obtain, in addition of the state, the unknown input (for example the message), this problem is known in the literature as the left invertible problem [44], [73], [64], [33], [82], [77], [78], [16]. This is in many cases an open problem and a complete study of the left invertibility for chaotic systems is out of the scope of this thesis. Nevertheless, we end this section by an academical example in order to show some left invertibilty drawbacks. Let us consider the following continuous time system for the sake of simplicity:

$$
\begin{align*}
\dot{z}_1 &= (1 + z_1)z_2 \\
\dot{z}_2 &= (1 - z_2^2)u \\
y &= z_1
\end{align*}
$$

where $z \in \mathbb{R}^2$ is the state, $y \in \mathbb{R}$ is the output and $u \in \mathbb{R}$ is the unknown input.

The observability singularity manifold for system (3.53) is:

$$S_\bar{O} = \{ z \in \mathbb{R}^2 | 1 + z_1 = 0 \} \quad (3.53)$$

At this observability singularity manifold a new difficulty occurs for obtaining the unknown input. In fact, the link between the derivative of $z_2$ and the unknown input may be broken on a set of manifolds (in reality the union of two parallel planes):

$$S_{ad} = \{ z \in \mathbb{R}^2 | 1 - z_2^2 = 0 \} \quad (3.54)$$

So, we can conclude that the set of singularity manifolds for the left invertibility problem $S_{lf}$ is given by (3.53) and (3.54) (i.e. $S_\bar{O} \cup S_{ad}$):

$$S_{lf} = \{ z \in \mathbb{R}^2 | (1 - z_2^2) \cdot (1 + z_1) = 0 \} \quad (3.55)$$

This extension of the singularity set is interesting in data secure transmission, see for example [39].
Chapter 4

The minimum sampling distance to achieve independent samples from chaotic signals.

4.1 Introduction

Shannon characterizes an ergodic process to be a process in which every sequence produced by it is the same in statistical properties, in his work [69]. He specifies also, that there exist a few number of particular sequences that do not obey this rule, but their number is negligible in an ergodic process.

For a chaotic system for which bifurcation parameters are kept fixed, a number of random processes can be obtained. In general, the number of these processes is equal with the number of states of the system. Nevertheless, there are cases (and we should see that the generalized Hénon map is such a case) in which the statistical description of all the random processes involved reduces to the description of only one random process.

When considering chaotic systems as embeddings for the transmission of secret messages, we need to count on the independence of the samples extracted from the chaotic system we use in our enciphering scheme. We cannot determine the necessary sampling distance in order to have independent and identically distributed (i.i.d.) samples, by analyzing only a particular observation (i.e., a particular trajectory) of the considered system. Thus, we generate a large number of trajectories, \( N \), and we perform our study by sampling, in pairs, at two different moments \( k_1 \) and \( k_2 = k_1 + \Delta \), the random processes assigned to the chaotic system we investigate, as in Fig. 4.1.

The Vlad-Badea test [14], transforms random variables following no matter what statistical distribution, even an unknown law, into random variables distributed conform to the Standard Normal law (Gaussian law having the mean \( \mu = 0 \) and the variance \( \sigma^2 = 1 \)), by means of random variable transforms. The test aims to benefit from the Pearson statistical independence test which is applicable only to random variables following the standard Gaussian law.

We apply the Vlad-Badea test in order to establish the minimum sampling distance that enables one to benefit of acquiring independently and identically distributed (i.i.d.) data from chaotic signals. The field of cryptography is susceptible to be one of the first domains in which independence between considered samples is essential. Chaotic dynamics used to embed the secret plain-message, must present stationarity. Ergodicity and the possibility of acquiring at least non-correlated data from their evolution, are mandatory in cryptography. As it is well-known, statistical independence implies non-correlation of the considered data. The reciprocal statement, that the non-correlation of two investigated data sets implies their independence, is true only in the case of data sets...
generated by Gaussian distributions. The two data sets come from normal distributions that are also jointly Gaussian.

The test is engendered over two identically distributed random variables constructed by sampling the random process assigned to the chaotic system in the stationarity region. The random process is designated by fixed bifurcation parameters. $N$ (sufficiently large from the statistical point of view) trajectories of the system starting from $N$ different initial condition vectors will be sampled at two moments (i.e. number of iterations) $k_1$ and $k_2 = k_1 + d$, where $d$ is the sampling distance, consequently obtaining two random variables.

The first concern is that the two random variables must be identically distributed. This requirement is fulfilled by taking care, when applying the independence test, to be situated in the stationarity region. The moment (time or number of iterations) from which the stationarity region can be considered must be determined prior to performing the Vlad-Badea test. $k_1$ is the moment starting with which the statistical repartition of the random process remain the same when sampled at a moment $k_2 > k_1$. This particular number of iterations (or, equivalently, time, $t_1 = T_S \cdot k_1$, where $T_S$ is the sampling period) is determined using a Smirnov goodness-of-fit test [20].

Once situated in the stationarity region, the random variables obtained at two different moments are tested for statistical independence, until the minimum sampling distance $d$, that guarantees (from the statistical point of view) the loss of link between them, is achieved.

Monte-Carlo analysis [6] are performed in order to validate the results, i.e. the experiments are repeated 500 times, and the percentage corresponding to the non-rejection of the null hypothesis is calculated. Statistical errors of Type I and Type II, [53], are taken into consideration. For more detailed informations, theorems and demonstrations with respect to the type I and type II errors, see [53].

### 4.2 The Vlad-Badea statistical independence test.

The Vlad-Badea statistical independence test [14], can be resumed as follows:

1. Choose the investigated state variables ($x_1$, $x_2$ or $x_3$).

2. Choose the sampling iteration for the $N$ trajectories, the number of the steps in the evolution of the trajectory, $k_1$.

3. Choose the distance between the sampling iterations, $\Delta$. The relation between the two moments at which the particular values for the investigated random variables are taken is given by equation (4.1).

$$k_2 = k_1 + \Delta$$

(4.1)

4. Obtain $N$ trajectories of the chaotic system having as initial conditions $N$ different vectors ($x_1(0), x_2(0), x_3(0)$) uniformly distributed in the interval $(0; 1)$. Consider $N = 10000$ sufficiently large.

The two random variables which are to be tested in order to establish their statistical independence are $X = [x_1, x_2, ..., x_N]$ and $Y = [y_1, y_2, ..., y_N]$, where $x_i, y_i \in \{x_1, x_2, x_3\}$. $X$ and $Y$ are constituted by independent pairs ($x_i, y_i$).

5. The random variables $X$ and $Y$ are sorted in ascending order. The index of each particular value is stored in $x_{i nd}$ and $y_{i nd}$, respectively. The experimental cumulative distribution functions $F_X(x)$ and $F_Y(y)$ are constructed. Each value $x_i$ ($y_i$) of these functions represents the probability $P(x_j < x_i)$ ($P(y_j < y_i)$). In
terms of classical probability the analytical expressions are given by the equations (4.2). As the considered signals are chaotic, all of their values are distinct, $x_i \neq x_j$, $\forall i \neq j$. Thus, the probability of each value $x_i$ ($y_i$) is $\frac{1}{N}$, and consequently, each value of the cumulative distributions $F_{eX}(x_i) = \frac{i}{N}$, respectively $F_{eY}(y_i) = \frac{i}{N}$.

$$F_{eX}(x_i) = \frac{\text{number}(x_j < x_i)}{|X|}$$
$$F_{eY}(y_i) = \frac{\text{number}(y_j < y_i)}{|Y|}$$ (4.2)

where $|X|$ ($|Y|$) is the cardinal (number of elements) of the data set. In the considered case, $|X| = |Y| = 10000$.

6. The repartition function $F_{eX}$ ($F_{eY}$) is applied to the set of values $x_i; i \in \{1, ..., N\}$ ($y_i; i \in \{1, ..., N\}$). It is well known, [26], that data values that are modeled as being random variables from any given continuous distribution can be converted to random variables having a uniform distribution (the probability integral transform). Two new data sets, $X'$ and $Y'$, described by equations (4.3) are obtained. The data sets $X'$ and $Y'$ are uniformly distributed in the interval $[0; 1]$.

$$x'_i = F_{eX}(x_i)$$
$$y'_i = F_{eY}(y_i)$$ (4.3)

7. The inverse function of the standard normal distribution function (the probit function, [72]) is applied to the $X'$ and $Y'$ data sets. Denote $G^{-1}$ the probit function. Then, the transforms that give two new Gaussian random variables, $U$ and $V$, are formulated in equations (4.4).

$$U(x_i) = G^{-1}(x_i)$$
$$V(y_i) = G^{-1}(y_i)$$ (4.4)

8. The correlation coefficient between the random variables $U$ and $V$ is computed using the formula in equation (4.5).

$$\rho = \frac{\sum_{i=1}^{N} (u_i - \bar{u}) \cdot (u_i - \bar{u})}{\sqrt{\sum_{i=1}^{N} (u_i - \bar{u}) \cdot \sum_{i=1}^{N} (u_i - \bar{u})}}$$ (4.5)

The test value given by the formula (4.6) is computed.

$$t = \rho \cdot \sqrt{\frac{N - 2}{(1 - \rho)^2}}$$ (4.6)

The null hypothesis of the test is $H_0$ and the alternative hypothesis is $H_1$. 

55
**4.3 The Smirnov test**

We briefly describe the algorithm for the Smirnov test:

1. Determine the cumulative distribution functions for the two investigated random variables $X$ and $Y$, $Fe_X(u)$ and $Fe_Y(u)$, respectively.
2. Calculate the test value:

\[ \delta = \max_u [F e_X(u) - F e_Y(u)] \] (4.9)

3. Choose the statistical threshold \( \alpha \).

4. Determine the maximum allowable distance for the test decision:

\[ \Delta_\alpha \approx \sqrt{\frac{N_1 + N_2}{N_1N_2}} \cdot \frac{1}{2} \cdot \ln \frac{2}{\alpha} \] (4.10)

where \( N_1 \) is the number of observations for the random variable \( X \) and \( N_2 \) is the number of observations for the random variable \( Y \).

5. Compare the test value \( \delta \) with the maximum allowable distance \( \Delta_\alpha \). If \( \delta \leq \Delta_\alpha \) we accept the null hypothesis, the random variables \( X \) and \( Y \) come from the same probability law. If \( \delta > \Delta_\alpha \) the random variables \( X \) and \( Y \) have different laws.

### 4.4 Case study. The generalized Hénon map.

We determine the transient time and the minimum sampling distance for the discrete-time chaotic generalized Hénon map, given in (2.17). We recall the equations:

\[
\begin{align*}
    x_1(k + 1) &= a - x_2^2(k) - b \cdot x_3(k) \\
    x_2(k + 1) &= x_1(k) \\
    x_3(k + 1) &= x_2(k)
\end{align*}
\] (4.11)

We have to decide the entry in the stationarity region and to determine the minimum distance that ensures statistical independence between two random variables obtained by sampling the random process assigned to the generalized Hénon map.

It can be observed from (4.11) that the state variables \( x_2 \) and \( x_3 \) are obtained by shifting the \( x_1 \) state variable, thus the description of the statistical behavior associated with the Hénon map can be reduced to the description of the random process assigned to the \( x_1 \) state variable. A random process corresponds to a fixed set of parameters \( a \) and \( b \) and is obtained starting from \( N \) randomly chosen initial conditions set \( (x_1(0), x_2(0), x_3(0)) \). An initial condition set defines a sample (a trajectory) of the random process. So, a trajectory of the process will represent the sequence of values obtained from the \( x_1 \) state variable by iterating the system (4.11) from the initial condition \( (x_1(0), x_2(0), x_3(0)) \).

The probability law of the random process will evolve from one iteration to another, starting from the uniform law (at iteration \( k = 0 \)) until the entrance in the stationarity region. The first concern of the study is to determine the entry point in the stationarity region of the random process.

To investigate stationarity and statistical independence, it is necessary to sample the random process assigned to the generalized Hénon Map at two distinct iterations, \( k_1 \) and \( k_2 \) (where \( k_2 = k_1 + \Delta \)), obtaining two random variables further noted with \( X \) and \( Y \). We plot in Fig. 4.1 the \( N \) trajectories of the generalized Hénon map, for \( a = 1.76 \) and \( b = 0.1 \).
1 Transient time measurements

At the moment \( k = 0 \), the states of the system are identical with the set of initial conditions. We determine the moment (number of iterations) \( k_1 \) from which the probability law of the random process remains unchanged. This moment corresponds to the entrance in the stationarity region of the random process. The transient time measurements follow the procedure described in [84]. So, we consider that the random variable, denoted \( Y \) in Fig. 4.1, is obtained by sampling the random process in the stationarity region (we assume that the iteration \( k_2 = 200 \) is large enough). The problem is to determine the iteration \( k_1 \) starting from which the random variable \( X \) (formed by sampling the random process at the moment \( k_1 \)) has the same probability law as the random variable \( Y \). For this, we use the Smirnov test. The null hypothesis of the Smirnov test is that the two continuous (in amplitude) random variables which are investigated have the same probability law. Our analysis is as follows:

- We consider \( N_1 = N_2 = 10000 \). We obtain, at the moment \( k_2 = 200 \) the random variable \( Y \), by sampling the random process assigned to the state variable \( x_1 \).
- We sample the random process at \( k_1 = 5 \) to \( k_1 = 195 \), with the fixed step equal to 5, obtaining the random variable \( X \).
- We plot the cumulative distribution functions \( F_{e_X}(u) \) and \( F_{e_Y}(u) \). We give some examples of the graphics we obtained in Fig.4.2-Fig. 4.6. More illustrations are done in Chapter 9.
Figure 4.2: The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 5$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.

Figure 4.3: The cumulative distribution functions $F_{eX}(u)$ and $F_{eY}(u)$, obtained at $k_1 = 10$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.
Figure 4.4: The cumulative distribution functions $F_{e_X}(u)$ and $F_{e_Y}(u)$, obtained at $k_1 = 20$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.

Figure 4.5: The cumulative distribution functions $F_{e_X}(u)$ and $F_{e_Y}(u)$, obtained at $k_1 = 30$ and $k_2 = 200$, sampling the random process assigned to the first state of the generalized Hénon map.

- We calculate the test value given by the formula (4.9) corresponding to each iteration number $k_1$, the results are given in Table 4.1.
- We choose the statistical threshold $\alpha = 0.05$. Following, we determine the maximum admissible distance for the test decision, $\Delta_\alpha$, with the formula (4.10). For $N = 10000$, $\Delta_\alpha = 0.0192$.

Comparing the distances $\delta$ with the maximum allowable distance $\Delta_\alpha = 0.0192$, we notice that from $k_1 = 30$ the random process is situated in the stationarity region.
Figure 4.6: The cumulative distribution functions \( F_{e_X}(u) \) and \( F_{e_Y}(u) \), obtained at \( k_1 = 40 \) and \( k_2 = 200 \), sampling the random process assigned to the first state of the generalized Hénon map.

Table 4.1: Smirnov test values \( \delta = |F_{e_X}(u) - F_{e_Y}(u)| \). Stationarity of the generalized Hénon map.

<table>
<thead>
<tr>
<th>( k )</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \delta )</td>
<td>0.32</td>
<td>0.09</td>
<td>0.02</td>
<td>0.04</td>
<td>0.02</td>
<td>0.01</td>
<td>0.01</td>
<td>0.008</td>
</tr>
</tbody>
</table>

We apply the Smirnov test 500 times, i.e. a Monte-Carlo type analysis. The results in Table 4.2 confirm that the moment \( k_1 = 30 \) is the stationarity entrance moment, for the parameters \( a = 1.76 \) and \( b = 0.1 \) of the generalized Hénon map.

Table 4.2: Monte-Carlo type analysis for the Smirnov test attesting the stationarity region entry moment for the generalized Hénon map.

<table>
<thead>
<tr>
<th>( \Delta = k_2 - k_1 ) [iterations]</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
<th>55</th>
<th>60</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H_0 ) acceptance [%]</td>
<td>17.5</td>
<td>89.2</td>
<td>93.2</td>
<td>93.4</td>
<td>94.2</td>
<td>93.8</td>
<td>95.6</td>
<td>94.8</td>
</tr>
</tbody>
</table>

2 Ergodicity of the generalized Hénon map.

We go one step further, and investigate the ergodicity of the generalized Hénon map. The ergodicity property of a process implies the fact that its statistical properties can be computed from a single, sufficiently long, observation (sample) of the process. In order to analyze the possibility that the temporal cumulative distribution and the statistical cumulative distributions have the same probability law we iterate the generalized Hénon map from a set of initial conditions \((x_1(0), x_2(0), x_3(0))\) (from the 10000 sets) for \( N=10000 \) discrete moments. We, then, apply a Smirnov test as in the Subsection 1. This time the reference cumulative distribution function is the \( cdf \) of the temporal process assigned to the generalized Hénon map. Observing the results presented in Table 9.3 and Fig. 4.7 - Fig. 4.11, we conclude that the iteration \( k_1 = 30 \) corresponds the mo-
Table 4.3: Smirnov test values $\delta = |Fe_X(u) - Fe_Y(u)|$. Ergodicity of the generalized Hénon map.

<table>
<thead>
<tr>
<th>$k_1$</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\delta$</td>
<td>0.35</td>
<td>0.10</td>
<td>0.02</td>
<td>0.03</td>
<td>0.013</td>
<td>0.019</td>
<td>0.005</td>
<td>0.006</td>
</tr>
</tbody>
</table>

...moment where we can start to speak about an ergodic and stationary process assigned to the generalized Hénon map. Nevertheless, a Monte-Carlo type analysis should validate this conclusion. More results, for different values for $k_1$ (the sampling moment for the statistical random variable obtained from the generalized Hénon map) are shown in the Chapter 9.

Figure 4.7: The cumulative distribution functions $Fe_X(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 5$, and the temporal cumulative distribution function $Fe_Y$.

3 Statistical independence of random variables extracted from the generalized Hénon map.

We apply the Vlad-Badea statistical independence test for the random variable $Y$ obtained by sampling the random process assigned to the generalized Hénon map at the iteration $k_2 = 200$ kept fixed and the random variable $X$, sampling at the variable iteration $k_1$. Some of the scatter diagrams for the transformed variables $U$ and $V$ are given in Fig. 4.12 - Fig. 4.17, for particular cases for the value of the $k_1$ iteration.
Figure 4.8: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 10$, and the temporal cumulative distribution function $F_{e_Y}$.

Figure 4.9: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 20$, and the temporal cumulative distribution function $F_{e_Y}$.

We compute the acceptance proportions of the statistical independence test, as consequence of a Monte-Carlo type analysis, repeating the experiment for 500 times. Results are shown in Table 4.4. In conclusion minimum sampling distance that ensures statistical independence for the generalized Hénon map is $\Delta > 30$.

Some results given in this Section can also be hound in [46].
Figure 4.10: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 30$, and the temporal cumulative distribution function $F_{e_Y}$.

Figure 4.11: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 40$, and the temporal cumulative distribution function $F_{e_Y}$.

Table 4.4: Monte-Carlo type analysis indicating the minimum independence sampling distance for the generalized Hénon map.

<table>
<thead>
<tr>
<th>$\Delta = k_2 - k_1$ [iterations]</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
<th>30</th>
<th>35</th>
<th>40</th>
<th>45</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H_0$ acceptance [%]</td>
<td>0</td>
<td>24</td>
<td>68.6</td>
<td>89.2</td>
<td>93.6</td>
<td>95.6</td>
<td>94.6</td>
<td>94.4</td>
<td>95.4</td>
<td>95.4</td>
</tr>
</tbody>
</table>
Figure 4.12: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 0$.

Figure 4.13: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 10$. 
Figure 4.14: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 20$.

Figure 4.15: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 30$. 
Figure 4.16: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 40$.

Figure 4.17: The scatter diagram of the transformed variables $U$ and $V$, for $\Delta = k_2 - k_1 = 50$. 
Chapter 5

A spatial investigation of chaotic attractors.

5.1 Introduction

When our senses through which we observe the physical phenomena can no more follow in detail all the movements. When our thought can no more simultaneously describe all the interactions, then we are constrained to limit our observations to the only accessible measures. The thermodynamics is, from this point of view, exemplar. Even prior to the discovery of atoms, the chemists clearly identified that the bodies are constituted by molecules, a huge number of indivisible particles. Despite this conclusion occurring in the precise moment of the rational mechanics reached its apogee, it was rapidly assimilated that the description, as the modeling through equations of the movements of each of the particles of a gas is impossible. The cause was not the nature of the trajectories, but the unimaginable number of existing particles, which impose a number of equations that is unaccessible to the human beings when writing and thinking. It is highly possible that it is the first scientific approach of a new infinity, the third one, the complexity.

Aiming the research not to be stopped by the wall of complexity, one uses the statistics, which logically leads to probabilities. In the XX-th century, the barrier of the infinitesimally small also led to a statistical approach, which confers to the quantum mechanics its probabilistic aspect.

Initiated by Pascal, prolonged by Gauss, Boltzmann, Maxwell and more recent by Borel, to cite only the most illustrious contributors, the statistics extracts from a long sequence of numbers invariants which are named mathematical expectation, variance, standard deviation, correlation, etc. This invariants are obviously properties of the sequence analyzed of number, but it is fundamental to conceive that the process which engenders this sequence is unknown, by its nature. That is from where the idea of a black box, concept used by Shannon in its theory of information, [69], to characterize the source of information. Our approach follows this line in the chapters of this thesis. It finds a second justification, in the point of view of the cryptanalyst who tries to decipher the transmitted message, when the exactly knowledge of the process that produced the information is not available.

The construction of a cryptosystem which is capable of hiding the message transmitted by a chaotic phenomenon opens an entirely different analysis. The designer must use the appearance of these phenomena at its maximum aiming to include the message in a data flow as uncorrelated as possible. In this case, the process is perfectly known and the use of statistical tools is meant to identify the maximum of non-correlation. The aim is no more to define the invariants which are susceptible to characterize the process
which engenders the long sequence of numbers, but to localize the region of the phase
space of the investigated system which disperses most the information, starting with the
deterministic equations describing the system. This dispersion is measured through the
correlation coefficient of the states of the studied chaotic dynamics. In the vicinity of a
null correlation, the difficulty to extract the transmitted message is maximum. This is
why we choose the statistical analysis of the strange attractor in the evaluation of the
chaos based cryptography.

5.2 An example: the Colpitts chaotic oscillator.

The aim of this chapter is to determine how much information an intruder can ob-
tain, once he can correctly intercept, on the communication channel, the output of the
transmitter of a secret message.

We will use, for exemplification, in our study the Colpitts chaotic oscillator described
by equations (2.29). Thus, let the attractor in Fig. 5.1 be the one the intruder obtains.
He does not know the initial condition set \((x_1(0), x_2(0), x_3(0))\), nor the parameters of
the system that has produced the dynamics he analyzes. To engender an easier attack he
tries to observe some patterns from the information which is available. We put ourselves
in the shoes of the intruder, and try to find this possible patterns in the structure of the
observed attractor.

The volume in which the attractor evolves is \(V_S = \Delta_X \cdot \Delta_Y \cdot \Delta_Z\), where \(\Delta_X = \max X - \min X, \Delta_Y = \max Y - \min Y, \Delta_Z = \max Z - \min Z\). From the Fig. 5.1, one
can determine \(\min X = -80, \min Y = -5, \min Z = -2\) and \(\max X = 10, \max Y = 45, \max Z = 4\). Therefore, \(V_S = 27 \cdot 10^3\). We divide our attractor into \(10^3\) volumes of
interest, \(V_B = \Delta_x \cdot \Delta_y \cdot \Delta_z = \frac{\Delta X}{10} \cdot \frac{\Delta Y}{10} \cdot \frac{\Delta Z}{10}\), as in Fig. 5.2.

Figure 5.1: The attractor the intruder reconstructs from the measured variable (the
Colpitts chaotic oscillator).

We know that the system which produced the investigated attractor is a continuous-
time dynamics. Each time that the evolution of the attractor intersects a certain box
(small volume), we store the position of this intersection. Once this index is recorded,
we ignore the rest of the points, until the attractor escapes from the box. We track
the evolution of the attractor until a new intersection is found, we store its position (in
number of samples) and disregard the rest of the points, and so on until the attractor
is investigated in its totality (number of total points of the evolution). The attractor
The attractor the intruder reconstructs from the measured variable divided into \(10^3\) smaller volumes.

never intersects 778 of the boxes from the total of 1000. This observation outlines only that the attractor does not occupy the entire phase space, which does not constitute an useful information for our study.

The coordinates of the origins of the small volumes are as in Table 5.1, and the dimensions of the boxes are given by \(\Delta_x = 9\), \(\Delta_y = 4.5\) and \(\Delta_z = 0.6\).

Table 5.1: The coordinates of the origin of the boxes in which the phase space of the Colpitts oscillator is split into.

<table>
<thead>
<tr>
<th>Box no.</th>
<th>(O_1)</th>
<th>(O_2)</th>
<th>(O_3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(\min X)</td>
<td>(\min Y)</td>
<td>(\min Z)</td>
</tr>
<tr>
<td>2</td>
<td>(\min X)</td>
<td>(\min Y)</td>
<td>(\min Z + \Delta_z)</td>
</tr>
<tr>
<td>3</td>
<td>(\min X)</td>
<td>(\min Y)</td>
<td>(\min Z + 2 \cdot \Delta_z)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10</td>
<td>(\min X)</td>
<td>(\min Y)</td>
<td>(\max Z - \Delta_z)</td>
</tr>
<tr>
<td>11</td>
<td>(\min X)</td>
<td>(\min Y + \Delta_y)</td>
<td>(\min Z)</td>
</tr>
<tr>
<td>12</td>
<td>(\min X)</td>
<td>(\min Y + \Delta_y)</td>
<td>(\min Z + \Delta_z)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>20</td>
<td>(\min X)</td>
<td>(\min Y + \Delta_y)</td>
<td>(\max Z - \Delta_z)</td>
</tr>
<tr>
<td>21</td>
<td>(\min X)</td>
<td>(\min Y + 2 \cdot \Delta_y)</td>
<td>(\min Z)</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>900</td>
<td>(\max X - 2 \cdot \Delta_x)</td>
<td>(\max Y - \Delta_y)</td>
<td>(\max Z - \Delta_z)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>999</td>
<td>(\max X - \Delta_x)</td>
<td>(\max Y - \Delta_y)</td>
<td>(\max Z - 2 \cdot \Delta_z)</td>
</tr>
<tr>
<td>1000</td>
<td>(\max X - \Delta_x)</td>
<td>(\max Y - \Delta_y)</td>
<td>(\min Z - \Delta_z)</td>
</tr>
</tbody>
</table>

We further pay attention to those boxes which are intersected by the attractor at least 4 times (194 small volumes that can be observed in Fig. 5.3). Our goal is to see how do different regions of the attractor behave in terms of parting: considering the points within a small box, we track them, in their evolution, to conclude upon their rate of divergence. We find an useful tool in the Euclidean distance between two three dimensional points (noted \(A(x_A, y_A, z_A)\) and \(B(x_B, y_B, z_B)\)), computed as in equation (5.1).
\[ d_{AB} = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2 + (z_B - z_A)^2} \] (5.1)

Figure 5.3: The volume of the attractor of the Colpitts chaotic oscillator divided in small volumes. The boxes which are intersected by the attractor of the chaotic system.

For each box which is intersected by the attractor at least 4 times, \( B_i \), with \( i = \{1, 2, ..., 194\} \), we compute the Euclidean distances between the first 4 points of intersection, \( P_{i1}, P_{i2}, P_{i3}, P_{i4} \). We obtain the \( C_4^2 = 6 \) distances \( d_{i1}, d_{i2}, d_{i3}, d_{i4}, d_{i23}, d_{i24} \), with a step of 10 iterations. At each moment (expressed in iteration number) we determine and we store the maximum value of these distances. It is intuitive that the maximum the Euclidean distance between the points, the less they are related. We present, in Table 5.2 to Table 5.2 the maximum Euclidean distance between the considered point for each box, the position (in number of iterations) at which the maximum value is obtained, and the coordinates corresponding to the small volume.

From the Tables 5.2 to 5.2 we delimit some volumes:
- The distance \( D \) is smaller than 1000. We represent this volume in cyan in Fig. 5.4.
- The distance \( D \in (1000, 12000) \). We represent this volume green in Fig. 5.4.
- The distance \( D \in (13000, 18000) \). We represent this volume in red in Fig. 5.4.
- The distance \( D \in (18000, 29000) \). We represent this volume in yellow in Fig. 5.4.
- The distance \( D \in (29000, 40000) \). We represent this volume in magenta in Fig. 5.4.
- The distance \( D \in (40000, 80000) \). We represent this volume in white in Fig. 5.4.
- The distance \( D \in (150000, 400000) \). We represent this volume with ‘flat’ (each face of the cube has a different color) in Fig. 5.4.

We give, in Fig. ?? to Fig. 5.9, for exemplification with respect to each area mentioned above, some graphics that illustrate the evolution of the Euclidean distance between points starting from a particular area of the chaotic attractor, once they are mapped by the chaotic dynamics.

In conclusion, the evolution of a chaotic attractor presents several types of manifolds (in our case, being three dimensional, the manifold reduces to a volume), regions that are favoring the parting of the points included initially within, and zones that are slower in spreading in the entire attractor. We can observe that the regions which are the fastest in becoming unlinked (positionally), disregarding the ones with \( D < 1000 \), in cyan (which necessitate a more detailed analysis), are the ones situated at the lowest
<table>
<thead>
<tr>
<th>Box. no.</th>
<th>$O_1$</th>
<th>$O_2$</th>
<th>$O_3$</th>
<th>$D$</th>
<th>index</th>
<th>sample number</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>-80</td>
<td>-5</td>
<td>0.4</td>
<td>77.0725</td>
<td></td>
<td>75481</td>
</tr>
<tr>
<td>6</td>
<td>-80</td>
<td>-5</td>
<td>1.0</td>
<td>80.1189</td>
<td></td>
<td>52281</td>
</tr>
<tr>
<td>7</td>
<td>-80</td>
<td>-5</td>
<td>1.6</td>
<td>79.9826</td>
<td></td>
<td>52181</td>
</tr>
<tr>
<td>17</td>
<td>-80</td>
<td>0</td>
<td>1.6</td>
<td>79.6735</td>
<td></td>
<td>35281</td>
</tr>
<tr>
<td>18</td>
<td>-80</td>
<td>0</td>
<td>2.2</td>
<td>77.0777</td>
<td></td>
<td>75221</td>
</tr>
<tr>
<td>19</td>
<td>-80</td>
<td>0</td>
<td>2.8</td>
<td>77.0791</td>
<td></td>
<td>75061</td>
</tr>
<tr>
<td>105</td>
<td>-71</td>
<td>-5</td>
<td>0.4</td>
<td>79.8489</td>
<td></td>
<td>32321</td>
</tr>
<tr>
<td>106</td>
<td>-71</td>
<td>-5</td>
<td>1.0</td>
<td>80.0177</td>
<td></td>
<td>32281</td>
</tr>
<tr>
<td>107</td>
<td>-71</td>
<td>-5</td>
<td>1.6</td>
<td>80.5124</td>
<td></td>
<td>32141</td>
</tr>
<tr>
<td>117</td>
<td>-71</td>
<td>0</td>
<td>1.6</td>
<td>80.0421</td>
<td></td>
<td>32041</td>
</tr>
<tr>
<td>118</td>
<td>-71</td>
<td>0</td>
<td>2.2</td>
<td>84.0020</td>
<td></td>
<td>241141</td>
</tr>
<tr>
<td>119</td>
<td>-71</td>
<td>0</td>
<td>2.8</td>
<td>79.7860</td>
<td></td>
<td>31781</td>
</tr>
<tr>
<td>129</td>
<td>-71</td>
<td>5</td>
<td>2.8</td>
<td>78.1895</td>
<td></td>
<td>51741</td>
</tr>
<tr>
<td>130</td>
<td>-71</td>
<td>5</td>
<td>3.4</td>
<td>77.0781</td>
<td></td>
<td>74841</td>
</tr>
<tr>
<td>140</td>
<td>-71</td>
<td>10</td>
<td>3.4</td>
<td>77.0698</td>
<td></td>
<td>74721</td>
</tr>
<tr>
<td>204</td>
<td>-62</td>
<td>-5</td>
<td>-0.2</td>
<td>78.1841</td>
<td></td>
<td>52441</td>
</tr>
<tr>
<td>205</td>
<td>-62</td>
<td>-5</td>
<td>0.4</td>
<td>59.1811</td>
<td></td>
<td>20381</td>
</tr>
<tr>
<td>206</td>
<td>-62</td>
<td>-5</td>
<td>1.0</td>
<td>39.1953</td>
<td></td>
<td>18161</td>
</tr>
<tr>
<td>207</td>
<td>-62</td>
<td>-5</td>
<td>1.6</td>
<td>34.1723</td>
<td></td>
<td>17921</td>
</tr>
<tr>
<td>217</td>
<td>-62</td>
<td>0</td>
<td>1.6</td>
<td>38.1270</td>
<td></td>
<td>17921</td>
</tr>
<tr>
<td>218</td>
<td>-62</td>
<td>0</td>
<td>2.2</td>
<td>39.8073</td>
<td></td>
<td>17801</td>
</tr>
<tr>
<td>228</td>
<td>-62</td>
<td>5</td>
<td>2.2</td>
<td>77.0805</td>
<td></td>
<td>55021</td>
</tr>
<tr>
<td>229</td>
<td>-62</td>
<td>5</td>
<td>2.8</td>
<td>80.4535</td>
<td></td>
<td>31741</td>
</tr>
<tr>
<td>230</td>
<td>-62</td>
<td>5</td>
<td>3.4</td>
<td>81.1977</td>
<td></td>
<td>90801</td>
</tr>
<tr>
<td>240</td>
<td>-62</td>
<td>10</td>
<td>3.4</td>
<td>78.2889</td>
<td></td>
<td>51441</td>
</tr>
<tr>
<td>250</td>
<td>-62</td>
<td>15</td>
<td>3.4</td>
<td>77.0781</td>
<td></td>
<td>74501</td>
</tr>
<tr>
<td>304</td>
<td>-53</td>
<td>-5</td>
<td>-0.2</td>
<td>59.0555</td>
<td></td>
<td>20481</td>
</tr>
<tr>
<td>305</td>
<td>-53</td>
<td>-5</td>
<td>0.4</td>
<td>74.0932</td>
<td></td>
<td>15481</td>
</tr>
<tr>
<td>306</td>
<td>-53</td>
<td>-5</td>
<td>1.0</td>
<td>81.2284</td>
<td></td>
<td>71961</td>
</tr>
<tr>
<td>307</td>
<td>-53</td>
<td>-5</td>
<td>1.6</td>
<td>78.6529</td>
<td></td>
<td>203041</td>
</tr>
<tr>
<td>316</td>
<td>-53</td>
<td>0</td>
<td>1.0</td>
<td>84.4280</td>
<td></td>
<td>160101</td>
</tr>
<tr>
<td>317</td>
<td>-53</td>
<td>0</td>
<td>1.6</td>
<td>81.2214</td>
<td></td>
<td>71741</td>
</tr>
<tr>
<td>318</td>
<td>-53</td>
<td>0</td>
<td>2.2</td>
<td>78.7029</td>
<td></td>
<td>15381</td>
</tr>
<tr>
<td>328</td>
<td>-53</td>
<td>5</td>
<td>2.2</td>
<td>73.9434</td>
<td></td>
<td>16041</td>
</tr>
<tr>
<td>329</td>
<td>-53</td>
<td>5</td>
<td>2.8</td>
<td>39.4741</td>
<td></td>
<td>17461</td>
</tr>
<tr>
<td>339</td>
<td>-53</td>
<td>10</td>
<td>2.8</td>
<td>36.8660</td>
<td></td>
<td>17641</td>
</tr>
<tr>
<td>340</td>
<td>-53</td>
<td>10</td>
<td>3.4</td>
<td>83.9785</td>
<td></td>
<td>240521</td>
</tr>
<tr>
<td>350</td>
<td>-53</td>
<td>15</td>
<td>3.4</td>
<td>79.8830</td>
<td></td>
<td>31261</td>
</tr>
<tr>
<td>360</td>
<td>-53</td>
<td>20</td>
<td>3.4</td>
<td>80.0822</td>
<td></td>
<td>51141</td>
</tr>
<tr>
<td>Box. no.</td>
<td>$O_1$</td>
<td>$O_2$</td>
<td>$O_3$</td>
<td>D</td>
<td>index</td>
<td>sample number</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>404</td>
<td>-44</td>
<td>-5</td>
<td>-0.2</td>
<td>58.5905</td>
<td>20541</td>
<td></td>
</tr>
<tr>
<td>405</td>
<td>-44</td>
<td>-5</td>
<td>0.4</td>
<td>16.0164</td>
<td>481</td>
<td></td>
</tr>
<tr>
<td>406</td>
<td>-44</td>
<td>-5</td>
<td>1.0</td>
<td>4.23424</td>
<td>241</td>
<td></td>
</tr>
<tr>
<td>416</td>
<td>-44</td>
<td>0</td>
<td>1.0</td>
<td>3.88399</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>417</td>
<td>-44</td>
<td>0</td>
<td>1.6</td>
<td>6.73219</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>418</td>
<td>-44</td>
<td>0</td>
<td>2.2</td>
<td>79.9027</td>
<td>69881</td>
<td></td>
</tr>
<tr>
<td>428</td>
<td>-44</td>
<td>5</td>
<td>2.2</td>
<td>81.2206</td>
<td>71381</td>
<td></td>
</tr>
<tr>
<td>438</td>
<td>-44</td>
<td>10</td>
<td>2.2</td>
<td>80.8304</td>
<td>51121</td>
<td></td>
</tr>
<tr>
<td>439</td>
<td>-44</td>
<td>10</td>
<td>2.8</td>
<td>36.0589</td>
<td>17261</td>
<td></td>
</tr>
<tr>
<td>449</td>
<td>-44</td>
<td>15</td>
<td>2.8</td>
<td>36.0403</td>
<td>17361</td>
<td></td>
</tr>
<tr>
<td>459</td>
<td>-44</td>
<td>20</td>
<td>2.8</td>
<td>80.6881</td>
<td>31041</td>
<td></td>
</tr>
<tr>
<td>460</td>
<td>-44</td>
<td>20</td>
<td>3.4</td>
<td>79.0016</td>
<td>34261</td>
<td></td>
</tr>
<tr>
<td>469</td>
<td>-44</td>
<td>25</td>
<td>2.8</td>
<td>78.9986</td>
<td>34081</td>
<td></td>
</tr>
<tr>
<td>470</td>
<td>-44</td>
<td>25</td>
<td>3.4</td>
<td>77.0771</td>
<td>74101</td>
<td></td>
</tr>
<tr>
<td>479</td>
<td>-44</td>
<td>30</td>
<td>2.8</td>
<td>77.0749</td>
<td>73881</td>
<td></td>
</tr>
<tr>
<td>503</td>
<td>-35</td>
<td>-5</td>
<td>-0.8</td>
<td>58.2170</td>
<td>20601</td>
<td></td>
</tr>
<tr>
<td>504</td>
<td>-35</td>
<td>-5</td>
<td>-0.2</td>
<td>47.0460</td>
<td>501</td>
<td></td>
</tr>
<tr>
<td>505</td>
<td>-35</td>
<td>-5</td>
<td>0.4</td>
<td>7.66324</td>
<td>321</td>
<td></td>
</tr>
<tr>
<td>506</td>
<td>-35</td>
<td>-5</td>
<td>1.0</td>
<td>33.7740</td>
<td>6101</td>
<td></td>
</tr>
<tr>
<td>516</td>
<td>-35</td>
<td>0</td>
<td>1.0</td>
<td>23.7608</td>
<td>6361</td>
<td></td>
</tr>
<tr>
<td>517</td>
<td>-35</td>
<td>0</td>
<td>1.6</td>
<td>8.26137</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>527</td>
<td>-35</td>
<td>5</td>
<td>1.6</td>
<td>4.07430</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>538</td>
<td>-35</td>
<td>10</td>
<td>2.2</td>
<td>81.2283</td>
<td>71041</td>
<td></td>
</tr>
<tr>
<td>548</td>
<td>-35</td>
<td>15</td>
<td>2.2</td>
<td>78.7569</td>
<td>14681</td>
<td></td>
</tr>
<tr>
<td>549</td>
<td>-35</td>
<td>15</td>
<td>2.8</td>
<td>30.7457</td>
<td>16841</td>
<td></td>
</tr>
<tr>
<td>558</td>
<td>-35</td>
<td>20</td>
<td>2.2</td>
<td>36.7108</td>
<td>16741</td>
<td></td>
</tr>
<tr>
<td>559</td>
<td>-35</td>
<td>20</td>
<td>2.8</td>
<td>71.0003</td>
<td>30161</td>
<td></td>
</tr>
<tr>
<td>568</td>
<td>-35</td>
<td>25</td>
<td>2.2</td>
<td>70.3636</td>
<td>30541</td>
<td></td>
</tr>
<tr>
<td>569</td>
<td>-35</td>
<td>25</td>
<td>2.8</td>
<td>83.9119</td>
<td>239941</td>
<td></td>
</tr>
<tr>
<td>578</td>
<td>-35</td>
<td>30</td>
<td>2.2</td>
<td>79.8887</td>
<td>30521</td>
<td></td>
</tr>
<tr>
<td>579</td>
<td>-35</td>
<td>30</td>
<td>2.8</td>
<td>78.2563</td>
<td>50561</td>
<td></td>
</tr>
<tr>
<td>588</td>
<td>-35</td>
<td>35</td>
<td>2.2</td>
<td>77.0771</td>
<td>73621</td>
<td></td>
</tr>
<tr>
<td>603</td>
<td>-26</td>
<td>-5</td>
<td>-0.8</td>
<td>57.7723</td>
<td>20661</td>
<td></td>
</tr>
<tr>
<td>604</td>
<td>-26</td>
<td>-5</td>
<td>-0.2</td>
<td>17.5738</td>
<td>701</td>
<td></td>
</tr>
<tr>
<td>605</td>
<td>-26</td>
<td>-5</td>
<td>0.4</td>
<td>36.9813</td>
<td>24381</td>
<td></td>
</tr>
<tr>
<td>615</td>
<td>-26</td>
<td>0</td>
<td>0.4</td>
<td>50.1378</td>
<td>5381</td>
<td></td>
</tr>
<tr>
<td>616</td>
<td>-26</td>
<td>0</td>
<td>1.0</td>
<td>62.2662</td>
<td>18941</td>
<td></td>
</tr>
<tr>
<td>617</td>
<td>-26</td>
<td>0</td>
<td>1.6</td>
<td>11.3343</td>
<td>5821</td>
<td></td>
</tr>
<tr>
<td>626</td>
<td>-26</td>
<td>5</td>
<td>1.0</td>
<td>37.8482</td>
<td>5161</td>
<td></td>
</tr>
<tr>
<td>627</td>
<td>-26</td>
<td>5</td>
<td>1.6</td>
<td>5.18720</td>
<td>981</td>
<td></td>
</tr>
<tr>
<td>Box. no.</td>
<td>$O_1$</td>
<td>$O_2$</td>
<td>$O_3$</td>
<td>D</td>
<td>index</td>
<td>sample number</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>---------------</td>
</tr>
<tr>
<td>633</td>
<td>-26</td>
<td>10</td>
<td>-0.8</td>
<td>78.3139</td>
<td>29221</td>
<td></td>
</tr>
<tr>
<td>636</td>
<td>-26</td>
<td>10</td>
<td>1.0</td>
<td>77.1106</td>
<td>35281</td>
<td></td>
</tr>
<tr>
<td>637</td>
<td>-26</td>
<td>10</td>
<td>1.6</td>
<td>7.06290</td>
<td>1161</td>
<td></td>
</tr>
<tr>
<td>642</td>
<td>-26</td>
<td>15</td>
<td>-1.4</td>
<td>78.8579</td>
<td>46381</td>
<td></td>
</tr>
<tr>
<td>643</td>
<td>-26</td>
<td>15</td>
<td>-0.8</td>
<td>78.2707</td>
<td>46181</td>
<td></td>
</tr>
<tr>
<td>647</td>
<td>-26</td>
<td>15</td>
<td>1.6</td>
<td>83.4110</td>
<td>70721</td>
<td></td>
</tr>
<tr>
<td>648</td>
<td>-26</td>
<td>15</td>
<td>2.2</td>
<td>80.8484</td>
<td>50581</td>
<td></td>
</tr>
<tr>
<td>651</td>
<td>-26</td>
<td>20</td>
<td>-2.0</td>
<td>79.4588</td>
<td>30461</td>
<td></td>
</tr>
<tr>
<td>652</td>
<td>-26</td>
<td>20</td>
<td>-1.4</td>
<td>78.3708</td>
<td>46941</td>
<td></td>
</tr>
<tr>
<td>657</td>
<td>-26</td>
<td>20</td>
<td>1.6</td>
<td>80.8322</td>
<td>50421</td>
<td></td>
</tr>
<tr>
<td>658</td>
<td>-26</td>
<td>20</td>
<td>2.2</td>
<td>77.1530</td>
<td>14841</td>
<td></td>
</tr>
<tr>
<td>661</td>
<td>-26</td>
<td>25</td>
<td>-2.0</td>
<td>77.0754</td>
<td>70781</td>
<td></td>
</tr>
<tr>
<td>666</td>
<td>-26</td>
<td>25</td>
<td>1.0</td>
<td>24.4274</td>
<td>15781</td>
<td></td>
</tr>
<tr>
<td>667</td>
<td>-26</td>
<td>25</td>
<td>1.6</td>
<td>73.7415</td>
<td>14761</td>
<td></td>
</tr>
<tr>
<td>668</td>
<td>-26</td>
<td>25</td>
<td>2.2</td>
<td>38.5589</td>
<td>16461</td>
<td></td>
</tr>
<tr>
<td>671</td>
<td>-26</td>
<td>30</td>
<td>-2.0</td>
<td>77.0592</td>
<td>70861</td>
<td></td>
</tr>
<tr>
<td>676</td>
<td>-26</td>
<td>30</td>
<td>1.0</td>
<td>26.3158</td>
<td>16261</td>
<td></td>
</tr>
<tr>
<td>677</td>
<td>-26</td>
<td>30</td>
<td>1.6</td>
<td>77.9619</td>
<td>30281</td>
<td></td>
</tr>
<tr>
<td>678</td>
<td>-26</td>
<td>30</td>
<td>2.2</td>
<td>83.8907</td>
<td>239581</td>
<td></td>
</tr>
<tr>
<td>686</td>
<td>-26</td>
<td>35</td>
<td>1.0</td>
<td>83.9385</td>
<td>239241</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Box. no.</th>
<th>$O_1$</th>
<th>$O_2$</th>
<th>$O_3$</th>
<th>D</th>
<th>index</th>
<th>sample number</th>
</tr>
</thead>
<tbody>
<tr>
<td>687</td>
<td>-26</td>
<td>35</td>
<td>1.6</td>
<td>79.4569</td>
<td>30121</td>
<td></td>
</tr>
<tr>
<td>688</td>
<td>-26</td>
<td>35</td>
<td>2.2</td>
<td>79.6207</td>
<td>50201</td>
<td></td>
</tr>
<tr>
<td>695</td>
<td>-26</td>
<td>40</td>
<td>0.4</td>
<td>77.0768</td>
<td>72941</td>
<td></td>
</tr>
<tr>
<td>696</td>
<td>-26</td>
<td>40</td>
<td>1.0</td>
<td>80.1373</td>
<td>49961</td>
<td></td>
</tr>
<tr>
<td>697</td>
<td>-26</td>
<td>40</td>
<td>1.6</td>
<td>77.0737</td>
<td>73301</td>
<td></td>
</tr>
<tr>
<td>703</td>
<td>-17</td>
<td>-5</td>
<td>-0.8</td>
<td>46.6196</td>
<td>601</td>
<td></td>
</tr>
<tr>
<td>704</td>
<td>-17</td>
<td>-5</td>
<td>-0.2</td>
<td>25.0366</td>
<td>541</td>
<td></td>
</tr>
<tr>
<td>705</td>
<td>-17</td>
<td>-5</td>
<td>0.4</td>
<td>77.0401</td>
<td>80701</td>
<td></td>
</tr>
<tr>
<td>715</td>
<td>-17</td>
<td>0</td>
<td>0.4</td>
<td>80.4314</td>
<td>66141</td>
<td></td>
</tr>
<tr>
<td>716</td>
<td>-17</td>
<td>0</td>
<td>1.0</td>
<td>80.2844</td>
<td>37341</td>
<td></td>
</tr>
<tr>
<td>723</td>
<td>-17</td>
<td>5</td>
<td>-0.8</td>
<td>73.3634</td>
<td>10781</td>
<td></td>
</tr>
<tr>
<td>724</td>
<td>-17</td>
<td>5</td>
<td>-0.2</td>
<td>77.0771</td>
<td>48201</td>
<td></td>
</tr>
<tr>
<td>725</td>
<td>-17</td>
<td>5</td>
<td>0.4</td>
<td>80.9769</td>
<td>191181</td>
<td></td>
</tr>
<tr>
<td>726</td>
<td>-17</td>
<td>5</td>
<td>1.0</td>
<td>56.6761</td>
<td>4901</td>
<td></td>
</tr>
<tr>
<td>732</td>
<td>-17</td>
<td>10</td>
<td>-1.4</td>
<td>73.9111</td>
<td>11641</td>
<td></td>
</tr>
<tr>
<td>733</td>
<td>-17</td>
<td>10</td>
<td>-0.8</td>
<td>72.2780</td>
<td>11621</td>
<td></td>
</tr>
<tr>
<td>734</td>
<td>-17</td>
<td>10</td>
<td>-0.2</td>
<td>79.7290</td>
<td>24981</td>
<td></td>
</tr>
<tr>
<td>736</td>
<td>-17</td>
<td>10</td>
<td>1.0</td>
<td>8.62767</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>737</td>
<td>-17</td>
<td>10</td>
<td>1.6</td>
<td>4.33842</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>741</td>
<td>-17</td>
<td>15</td>
<td>-2.0</td>
<td>32.4617</td>
<td>13421</td>
<td></td>
</tr>
<tr>
<td>Box. no.</td>
<td>$O_1$</td>
<td>$O_2$</td>
<td>$O_3$</td>
<td>D</td>
<td>index</td>
<td>[sample number]</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>------</td>
<td>-------</td>
<td>-----------------</td>
</tr>
<tr>
<td>742</td>
<td>-17</td>
<td>15</td>
<td>-1.4</td>
<td>31.7267</td>
<td></td>
<td>13441</td>
</tr>
<tr>
<td>745</td>
<td>-17</td>
<td>15</td>
<td>0.4</td>
<td>3.92091</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>746</td>
<td>-17</td>
<td>15</td>
<td>1.0</td>
<td>7.09087</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>747</td>
<td>-17</td>
<td>15</td>
<td>1.6</td>
<td>82.7718</td>
<td></td>
<td>70341</td>
</tr>
<tr>
<td>751</td>
<td>-17</td>
<td>20</td>
<td>-2.0</td>
<td>31.4633</td>
<td></td>
<td>7441</td>
</tr>
<tr>
<td>755</td>
<td>-17</td>
<td>20</td>
<td>0.4</td>
<td>82.9358</td>
<td></td>
<td>69881</td>
</tr>
<tr>
<td>756</td>
<td>-17</td>
<td>20</td>
<td>1.0</td>
<td>83.4660</td>
<td></td>
<td>70241</td>
</tr>
<tr>
<td>757</td>
<td>-17</td>
<td>20</td>
<td>1.6</td>
<td>81.1915</td>
<td></td>
<td>70321</td>
</tr>
<tr>
<td>761</td>
<td>-17</td>
<td>25</td>
<td>-2.0</td>
<td>37.0459</td>
<td></td>
<td>15521</td>
</tr>
<tr>
<td>765</td>
<td>-17</td>
<td>25</td>
<td>0.4</td>
<td>80.8413</td>
<td></td>
<td>49781</td>
</tr>
<tr>
<td>766</td>
<td>-17</td>
<td>25</td>
<td>1.0</td>
<td>80.7964</td>
<td></td>
<td>50081</td>
</tr>
<tr>
<td>771</td>
<td>-17</td>
<td>30</td>
<td>-2.0</td>
<td>80.9995</td>
<td></td>
<td>28501</td>
</tr>
<tr>
<td>772</td>
<td>-17</td>
<td>30</td>
<td>-1.4</td>
<td>77.1052</td>
<td></td>
<td>52221</td>
</tr>
<tr>
<td>773</td>
<td>-17</td>
<td>30</td>
<td>0.0</td>
<td>13.3293</td>
<td></td>
<td>15321</td>
</tr>
<tr>
<td>774</td>
<td>-17</td>
<td>30</td>
<td>0.2</td>
<td>25.3882</td>
<td></td>
<td>15401</td>
</tr>
<tr>
<td>775</td>
<td>-17</td>
<td>30</td>
<td>1.0</td>
<td>38.0386</td>
<td></td>
<td>15821</td>
</tr>
<tr>
<td>776</td>
<td>-17</td>
<td>30</td>
<td>1.0</td>
<td>37.4676</td>
<td></td>
<td>16021</td>
</tr>
<tr>
<td>781</td>
<td>-17</td>
<td>35</td>
<td>-2.0</td>
<td>78.4176</td>
<td></td>
<td>48381</td>
</tr>
<tr>
<td>782</td>
<td>-17</td>
<td>35</td>
<td>-1.4</td>
<td>80.4559</td>
<td></td>
<td>29001</td>
</tr>
<tr>
<td>783</td>
<td>-17</td>
<td>35</td>
<td>-0.8</td>
<td>73.7741</td>
<td></td>
<td>29221</td>
</tr>
<tr>
<td>784</td>
<td>-17</td>
<td>35</td>
<td>-0.2</td>
<td>77.0808</td>
<td></td>
<td>52941</td>
</tr>
<tr>
<td>785</td>
<td>-17</td>
<td>35</td>
<td>0.4</td>
<td>78.1863</td>
<td></td>
<td>29781</td>
</tr>
<tr>
<td>786</td>
<td>-17</td>
<td>35</td>
<td>1.0</td>
<td>83.8559</td>
<td></td>
<td>239101</td>
</tr>
<tr>
<td>791</td>
<td>-17</td>
<td>40</td>
<td>-2.0</td>
<td>77.0787</td>
<td></td>
<td>71761</td>
</tr>
<tr>
<td>792</td>
<td>-17</td>
<td>40</td>
<td>-1.4</td>
<td>79.9421</td>
<td></td>
<td>48981</td>
</tr>
<tr>
<td>793</td>
<td>-17</td>
<td>40</td>
<td>-0.8</td>
<td>78.6065</td>
<td></td>
<td>49021</td>
</tr>
<tr>
<td>794</td>
<td>-17</td>
<td>40</td>
<td>-0.2</td>
<td>79.1062</td>
<td></td>
<td>32801</td>
</tr>
<tr>
<td>795</td>
<td>-17</td>
<td>40</td>
<td>0.4</td>
<td>78.9994</td>
<td></td>
<td>33041</td>
</tr>
<tr>
<td>802</td>
<td>-8</td>
<td>-5</td>
<td>-1.4</td>
<td>80.9792</td>
<td></td>
<td>187461</td>
</tr>
<tr>
<td>803</td>
<td>-8</td>
<td>-5</td>
<td>-0.8</td>
<td>62.7318</td>
<td></td>
<td>681</td>
</tr>
<tr>
<td>804</td>
<td>-8</td>
<td>-5</td>
<td>-0.2</td>
<td>79.6479</td>
<td></td>
<td>61981</td>
</tr>
<tr>
<td>812</td>
<td>-8</td>
<td>0</td>
<td>-1.4</td>
<td>76.0286</td>
<td></td>
<td>7501</td>
</tr>
<tr>
<td>813</td>
<td>-8</td>
<td>0</td>
<td>-0.8</td>
<td>42.4465</td>
<td></td>
<td>1221</td>
</tr>
<tr>
<td>814</td>
<td>-8</td>
<td>0</td>
<td>-0.2</td>
<td>83.9234</td>
<td></td>
<td>213601</td>
</tr>
<tr>
<td>815</td>
<td>-8</td>
<td>0</td>
<td>0.4</td>
<td>84.7446</td>
<td></td>
<td>3221</td>
</tr>
<tr>
<td>822</td>
<td>-8</td>
<td>5</td>
<td>-1.4</td>
<td>83.2320</td>
<td></td>
<td>8221</td>
</tr>
<tr>
<td>823</td>
<td>-8</td>
<td>5</td>
<td>-0.8</td>
<td>69.4361</td>
<td></td>
<td>9901</td>
</tr>
<tr>
<td>824</td>
<td>-8</td>
<td>5</td>
<td>-0.2</td>
<td>78.1906</td>
<td></td>
<td>3541</td>
</tr>
<tr>
<td>825</td>
<td>-8</td>
<td>5</td>
<td>0.4</td>
<td>80.4123</td>
<td></td>
<td>36701</td>
</tr>
<tr>
<td>826</td>
<td>-8</td>
<td>5</td>
<td>1.0</td>
<td>77.0796</td>
<td></td>
<td>60061</td>
</tr>
<tr>
<td>832</td>
<td>-8</td>
<td>10</td>
<td>-1.4</td>
<td>83.2235</td>
<td></td>
<td>8841</td>
</tr>
<tr>
<td>Box. no.</td>
<td>$O_1$</td>
<td>$O_2$</td>
<td>$O_3$</td>
<td>D</td>
<td>index [sample number]</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>833</td>
<td>-8</td>
<td>10</td>
<td>-0.8</td>
<td>78.9717</td>
<td>43341</td>
<td></td>
</tr>
<tr>
<td>834</td>
<td>-8</td>
<td>10</td>
<td>-0.2</td>
<td>69.1127</td>
<td>24401</td>
<td></td>
</tr>
<tr>
<td>835</td>
<td>-8</td>
<td>10</td>
<td>0.4</td>
<td>62.2649</td>
<td>4161</td>
<td></td>
</tr>
<tr>
<td>836</td>
<td>-8</td>
<td>10</td>
<td>1.0</td>
<td>38.9301</td>
<td>4501</td>
<td></td>
</tr>
<tr>
<td>841</td>
<td>-8</td>
<td>15</td>
<td>-2</td>
<td>78.9466</td>
<td>198901</td>
<td></td>
</tr>
<tr>
<td>842</td>
<td>-8</td>
<td>15</td>
<td>-1.4</td>
<td>83.4536</td>
<td>9541</td>
<td></td>
</tr>
<tr>
<td>843</td>
<td>-8</td>
<td>15</td>
<td>-0.8</td>
<td>28.5299</td>
<td>3981</td>
<td></td>
</tr>
<tr>
<td>844</td>
<td>-8</td>
<td>15</td>
<td>-0.2</td>
<td>22.6308</td>
<td>4341</td>
<td></td>
</tr>
<tr>
<td>845</td>
<td>-8</td>
<td>15</td>
<td>0.4</td>
<td>5.10003</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>851</td>
<td>-8</td>
<td>20</td>
<td>-2.0</td>
<td>82.5911</td>
<td>87081</td>
<td></td>
</tr>
<tr>
<td>852</td>
<td>-8</td>
<td>20</td>
<td>-1.4</td>
<td>81.0907</td>
<td>68721</td>
<td></td>
</tr>
<tr>
<td>853</td>
<td>-8</td>
<td>20</td>
<td>-0.8</td>
<td>82.3409</td>
<td>68941</td>
<td></td>
</tr>
<tr>
<td>854</td>
<td>-8</td>
<td>20</td>
<td>-0.2</td>
<td>5.58819</td>
<td>401</td>
<td></td>
</tr>
<tr>
<td>855</td>
<td>-8</td>
<td>20</td>
<td>0.4</td>
<td>4.87832</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>861</td>
<td>-8</td>
<td>25</td>
<td>-2.0</td>
<td>27.8518</td>
<td>14121</td>
<td></td>
</tr>
<tr>
<td>862</td>
<td>-8</td>
<td>25</td>
<td>-1.4</td>
<td>76.3155</td>
<td>12101</td>
<td></td>
</tr>
<tr>
<td>863</td>
<td>-8</td>
<td>25</td>
<td>-0.8</td>
<td>81.2263</td>
<td>69181</td>
<td></td>
</tr>
<tr>
<td>864</td>
<td>-8</td>
<td>25</td>
<td>-0.2</td>
<td>81.2254</td>
<td>69541</td>
<td></td>
</tr>
<tr>
<td>865</td>
<td>-8</td>
<td>25</td>
<td>0.4</td>
<td>83.9672</td>
<td>399261</td>
<td></td>
</tr>
<tr>
<td>872</td>
<td>-8</td>
<td>30</td>
<td>-1.4</td>
<td>33.6623</td>
<td>14801</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Box. no.</th>
<th>$O_1$</th>
<th>$O_2$</th>
<th>$O_3$</th>
<th>D</th>
<th>index [sample number]</th>
</tr>
</thead>
<tbody>
<tr>
<td>873</td>
<td>-8</td>
<td>30</td>
<td>-0.8</td>
<td>25.1496</td>
<td>15101</td>
</tr>
<tr>
<td>902</td>
<td>1</td>
<td>-5</td>
<td>-1.4</td>
<td>48.4075</td>
<td>21061</td>
</tr>
<tr>
<td>903</td>
<td>1</td>
<td>-5</td>
<td>-0.8</td>
<td>63.2645</td>
<td>7141</td>
</tr>
<tr>
<td>912</td>
<td>1</td>
<td>0</td>
<td>-1.4</td>
<td>53.4174</td>
<td>1501</td>
</tr>
<tr>
<td>913</td>
<td>1</td>
<td>0</td>
<td>-0.8</td>
<td>66.7198</td>
<td>2001</td>
</tr>
<tr>
<td>914</td>
<td>1</td>
<td>0</td>
<td>-0.2</td>
<td>80.5441</td>
<td>79741</td>
</tr>
<tr>
<td>922</td>
<td>1</td>
<td>5</td>
<td>-1.4</td>
<td>36.6414</td>
<td>2441</td>
</tr>
<tr>
<td>923</td>
<td>1</td>
<td>5</td>
<td>-0.8</td>
<td>79.0892</td>
<td>34961</td>
</tr>
<tr>
<td>924</td>
<td>1</td>
<td>5</td>
<td>-0.2</td>
<td>77.0706</td>
<td>78741</td>
</tr>
<tr>
<td>932</td>
<td>1</td>
<td>10</td>
<td>-1.4</td>
<td>52.3469</td>
<td>2761</td>
</tr>
<tr>
<td>933</td>
<td>1</td>
<td>10</td>
<td>-0.8</td>
<td>32.5788</td>
<td>3221</td>
</tr>
<tr>
<td>934</td>
<td>1</td>
<td>10</td>
<td>-0.2</td>
<td>38.3271</td>
<td>22121</td>
</tr>
<tr>
<td>942</td>
<td>1</td>
<td>15</td>
<td>-1.4</td>
<td>69.5231</td>
<td>16481</td>
</tr>
<tr>
<td>943</td>
<td>1</td>
<td>15</td>
<td>-0.8</td>
<td>13.6065</td>
<td>4041</td>
</tr>
</tbody>
</table>
Figure 5.4: The volume of the attractor of the Colpitts chaotic oscillator divided in small volumes, grouped in areas by colors.

Figure 5.5: The evolution of the Euclidean distance between points starting their evolution from the box number 723.

coordinates on the attractor ($D < 12000$, green zone), while the slowest part of the attractor is represented by the white region, its extremities.
Figure 5.6: The evolution of the Euclidean distance between points starting their evolution from the box number 305.

Figure 5.7: The evolution of the Euclidean distance between points starting their evolution from the box number 304.
Figure 5.8: The evolution of the Euclidean distance between points starting their evolution from the box number 923.

Figure 5.9: The evolution of the Euclidean distance between points starting their evolution from the box number 5.
Chapter 6

An enciphering-deciphering algorithm based on the discrete generalized Hénon map.

Chapter 6 focuses on how robust are chaotic systems described by polynomial equations as dynamics including a secret message, when exposed to a known plain-message attack.

6.1 Introduction

Our investigation is developed in the context of the chaotic generalized Hénon map, described by equations (2.17). The inclusion method, presented in [27], is used to transmit a secret message (in ASCII format) embedded in the evolution of the Hénon three dimensional discrete-time map. The secret key is constituted by the two bifurcation parameters of the map, $a$ and $b$, the initial conditions $(x_1(0), x_2(0), x_3(0))$ and the scaling factor $\nu$. The latter is necessary to maintain unaltered the chaotic dynamics (i.e., not to diverge). For this type of cryptosystem, when a known-text attack is engendered, the knowledge of three characters in the plain-text is sufficient in order to constitute a system of three algebraic equations, the unknown variables being the parameters of the chaotic system and the scaling factor. Once the $a$, $b$ and $\nu$ parameters are found, the dimension of the space of the secret key is decreased. This is a severe lack of security for a cryptosystem.

Suppose that the plain message, $m = m(1)m(2)...m(L)$, is added by inclusion to the evolution of the map, to its first state, see equations (6.1).

$$\begin{align*}
x_1(k+1) &= a - x_2^2(k) - bx_3(k) + \frac{m(k)}{\nu} \\
x_2(k+1) &= x_1(k) \\
x_3(k+1) &= x_2(k)
\end{align*}$$ (6.1)

Knowing the values of the bifurcation parameters, the cryptanalyst could easily determine the plain text from the series $\{x_3(k)\}$, considered to be the output of the system. See equation (6.2) for the solution to the left invertibility problem.

$$\frac{m(k)}{\nu} = x_3(k+3) + x_3^2(k+1) + b \cdot x_3(k) - a$$ (6.2)

Assume the cryptanalyst knows three entities of the plain message, $m(i)$, $m(j)$ and $m(u)$, where $i \neq j \neq u, i, j, u \in \mathbb{N}$. The eavesdropper can get the values of the cryptogram $\{x_3(k)\}, k \in \{3, 4, ..., L + 3\}$ from the communication channel. Consequently, the attacker forms a three equations algebraic system with three unknown variables, $a$, $b$ and $\nu$, as expressed by equations (6.3).
When subtracting the second equation of the system (6.3) from the first one, the parameter \( b \) is determined with the formula (6.3).

\[
b = \frac{m(i) - m(j)}{\nu} - \frac{x_3(i + 3) + x_3(j + 3) - x_3^2(i + 1) - x_3^2(j + 1)}{x_3(i) + x_3(j)} \quad (6.3)
\]

Multiplying the first equation with \( x_3(j) \) and the second with \( x_3(i) \), and subtracting the second from the first, the equation (6.4) is obtained.

\[
a = \frac{m(i) - m(j)}{\nu} - \frac{x_3(i + 3) \cdot x_3(j) + x_3(j + 3) \cdot x_3(i) - x_3^2(i + 1) \cdot x_3(j) - x_3^2(j + 1) \cdot x_3(i)}{x_3(i) - x_3(j)} \quad (6.4)
\]

Substituting (6.3) and (6.4) in the third equation of (6.3), the scaling factor \( \nu \) is determined. Knowing its value implies knowing the values of the bifurcation parameters \( a \) and \( b \). For another approach for testing the parametric identifiability for the choice of the static key (i.e., fixed values of bifurcation parameters), see [8].

Hence, the necessity to include the message into the evolution of the system not in its original form, but already enciphered.

We propose a simple improvement of inclusions in this type of cryptosystems. The plain-message is ciphered using classical S-box and P-box (substitution and transposition) transformations, mixing functions as the ones proposed by Claude-Shannon [70] (founder of cryptography as a science), prior to its inclusion in the chaotic dynamics. The proposed enciphering scheme may be used as an inner element in a cipher, providing a good practical diffusion and confusion. One of our studies regarding the ergodicity and some of the statistical properties of the generalized Hénon map is presented in [46].

Baptista promotes chaotic systems as a possibility of enciphering and simultaneously embedding secret information [13]. He uses the ergodicity feature of the chaotic logistic map to inspect and to reveal diffusion and confusion of his enciphering method.

Firstly, we choose a chaotic system of a higher dimension than Baptista used, aiming to obtain a more complex system having a hyperchaotic behavior for a number of bifurcation parameters \( a \) and \( b \). See [36] for details.

The requirement that a good cipher has to provide the equiprobability of the elements of the key, highlighted in [70] and specified in [9] and [11], is taken into account. Thus, the distribution of the states of the generalized Hénon map from Fig. 2.4 is analyzed. Baptista’s idea of dividing the attractor of the chaotic system in subintervals is borrowed. The interval \((-2, 2)\) in which the iterations take values, is mapped in \((-1, 1)\) throughout the sine function. The domain \((-1, 1)\) is, then, divided as in Fig. 6.1. The 10 subintervals of equal length are explicitly given in Table 6.1. The quasi-uniform distribution of the function \( f = sin(\frac{x_3 - x_2}{2}) \) may be observed in Fig. 6.2. The 10 subintervals will be chosen by the evolution of the hyperchaotic map in a deterministic-random manner.
Figure 6.1: Sites of the generalized Hénon map, determined by the function \( f = \sin(\frac{2x_2 - x_3}{2}) \).

Table 6.1: The ten subintervals of equal length.

<table>
<thead>
<tr>
<th>Box no.</th>
<th>Box interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>[-1.0; -0.8)</td>
</tr>
<tr>
<td>2</td>
<td>[-0.8; -0.6)</td>
</tr>
<tr>
<td>3</td>
<td>[-0.6; -0.4)</td>
</tr>
<tr>
<td>4</td>
<td>[-0.4; -0.2)</td>
</tr>
<tr>
<td>5</td>
<td>[-0.2; 0.0)</td>
</tr>
<tr>
<td>6</td>
<td>[0.0; 0.2)</td>
</tr>
<tr>
<td>7</td>
<td>[0.2; 0.4)</td>
</tr>
<tr>
<td>8</td>
<td>[0.4; 0.6)</td>
</tr>
<tr>
<td>9</td>
<td>[0.6; 0.8)</td>
</tr>
<tr>
<td>10</td>
<td>[0.8; 1.0)</td>
</tr>
</tbody>
</table>

Figure 6.2: Histogram corresponding to the ten boxes, for bifurcation parameters \( a = 1.76 \) and \( b = 0.1 \) on a trajectory of 50,000 iterations. The initial conditions are \((x_1(0), x_2(0), x_3(0)) = (0.8147, 0.9057, 0.1269)\).

In our enciphering scheme, a random variable transform is applied on the state of the chaotic system at each iteration in order to obtain a new random variable of a quasi
uniform law. This new random variable is further transformed, through a series of other functions containing elements of the secret key, into a discrete random variable. The discrete values - which are ASCII numbers - are combined by a simple relation with the plain message, also in ASCII format. A first mask of the original message, involving the generalized Hénon map (GHM) is obtained. On this result (in its binary representation form) other simple transformations that depend on the state of the GHM are applied. That finally allows getting a transformed version of the message that can be included in one of the states of the GHM without disturbing its chaotic behavior. The results, including a perception of the diffusion and the confusion involved, are illustrated on natural text and jpeg images.

Remark: The experimenter may use the algorithm proposed in literature [87] to determine the pairs of bifurcation parameters that induce hyperchaotic behavior of the generalized Hénon map. The experimenter has also to pay attention to the fact that not all these parameters allow the distribution seen in Fig. 6.2. For the pairs of parameters \((a,b)\) which fulfill the requirement of hyperchaoticity, refer to Fig. 2.3.

The steps of the enciphering algorithm we propose are presented in the section 6.2. The presentation is also exposed in [22].

6.2 The Proposed Enciphering Method

1 Scheme of the proposed enciphering method

The scheme of the proposed enciphering method is illustrated in Fig. 6.3, where:

- \([XYZ]^T\) denotes the random vector of the states of the generalized Hénon map, \((x_1, x_2, x_3)\). For fixed \((a, b)\) and initial conditions \((x_1(0), x_2(0), x_3(0))^T\) randomly and uniformly chosen in the interval \([-1, 1]\), there are three (deterministic) random processes assigned to the three state variables of the chaotic dynamics. Thus, at each and every \(k\) iteration we can speak of a random vector \((x_1(k), x_2(k), x_3(k))^T\).

- \(f\) is a random variable transform that produces a discrete random variable \(\xi = f(\sin\frac{x_2-x_3}{2}).\) \(\xi \in 1, 2, ..., 10.\) The probabilities of occurrence of the values of \(\xi\) are almost equal, see Fig. 6.2. The \(\xi\) values are chosen by the states of the generalized Hénon map, assigned as in Table 6.1.

- \(g_1\) and \(g_2\) are two new random variable transforms applied to \(\xi\). They imply the external secret key. \(g_1\) is a transform that assigns to the random variable \(\xi\) a discrete random variable with 10 values, bytes, in \([0, 255]\), the ASCII interval, \(g_1(\xi) = \zeta\). We choose \(\zeta\) among the set of possibilities presented in Table 6.2. The total key space is \(K = \{a, b, x_1(0), x_2(0), x_3(0), K_{\zeta}, K_P\}.\) \(\alpha_{i,j} \in \{1, 2, ..., 255\}.\) Because 10 values are chosen among 255, \(|K_{\zeta}| = C_{255}^{10} = 2.679 \cdot 10^{17}.\) \(\beta_{i,j} \in P,\) with \(|P| = 8! = 40320.\) The \(K_{(a,b)}\) subspace is constituted by the pairs determined by computing the Lyapunov exponents of the generalized Hénon map and the distribution of the function \(f.\) The
initial conditions are taken uniformly in $[-1, 1]$ and the cardinal of the set is given by the huge number of the combinations between all the possible values $x_1, x_2, x_3$ can take. The number of the elements of $K_{(a,b)}$ and $K_{(x_1,x_2,x_3)}$ depends on the computing precision used in computation. The cardinal of the key space, $|K|$, is given by the number of possible combinations between the elements of the key subspaces $K_{(a,b)}, K_{(x_1,x_2,x_3)}, K_{\zeta}, K_P$.

Table 6.2: Key elements disposed in two matrices.

<table>
<thead>
<tr>
<th>$\xi$</th>
<th>$K_\zeta$</th>
<th>$K_P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\alpha_{1,1}$</td>
<td>$\beta_{1,1}$</td>
</tr>
<tr>
<td>2</td>
<td>$\alpha_{2,1}$</td>
<td>$\beta_{2,1}$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>10</td>
<td>$\alpha_{1,1}$</td>
<td>$\beta_{1,1}$</td>
</tr>
</tbody>
</table>

Applying $g_2$, a second set of 10 bytes is assigned to the variable $\xi$. They are 8 bits (1 byte) permutations, described in Table 6.2, in correspondence with the variable $\xi$, $g_2(\xi) = P$.

- $m$ is the sequence of 8-bit characters, being the ASCII values of the characters in the plain message.
- $R$ is the cryptogram obtained from the first enciphering step. It is a byte resulted as the addition modulo 2 without carry (bitxor) between the character that is enciphered and the byte $\zeta$. The value $\zeta$ is the one assigned to the interval selected by the function $\sin(x_2(k) - x_3(k))$ depending on the state of the generalized Hénon map at the moment of the enciphering of the $k$-th character.
- $m'$ is the byte obtained after the second enciphering step, meaning the permutation of the resulted byte $R$, involving the rule established by the state of the hyperchaotic system at the enciphering moment.
- Fixed reversible transformations are represented by a binary to decimal conversion and scaling by a factor. The scaling allows the inclusion of the masked character (after bitxor and permutation transformations) into the evolution of the chaotic map without disturbing its dynamics (i.e., it does not leave the bounded space).
- $\tilde{m}$ is the masked and scaled message, that is added to the evolution of the hyperchaotic system, in system (6.1) instead of $m$.
- In order to allow the recovery of the masked character from the series of the output $x_3$ of the generalized Hénon map, it is imperative to iterate the system three more times, after the last character of the message is enciphered, as it can be seen from the observer formula (6.2).

Remark: Depending of the application, the enciphering scheme from Fig. 6.3 enables two variants for the cryptograms:

1. The user may transmit on the communication channel only the series $\{x_3(3), x_3(4), ..., x_3(L+3)\}$ of the output of the system, where $L$ is the length of the message to be transmitted. Knowing the initial conditions $(x_3(2), x_3(1), x_3(0)) = (x_1(0), x_2(0), x_3(0))$ and the bifurcation parameters $(a, b)$, the receiver can easily synchronize the reception
system with the emission one, and recover the set of masked characters having also the value of the scaling factor. In this case, \( \hat{m}(0)\hat{m}(1)\ldots \hat{m}_L \) is considered the enciphered message.

2. On the channel the user may also transmit the document containing the masked message, \( m' \). So, \( m' \) will be the cryptogram. In this case, the only role of the generalized Hénon map is to embed the secret information and to provide the random non-preferential distribution of the bytes for the bitxor and the permutations which follow this operation.

Actual encoding of the message is delivered in two stages within the dotted lines in Fig.6.3. The two stages consist in multiple substitution and transposition, on 8-bit segments, following a random rule carried by the generalized Hénon map.

The security of the cipher can be increased by increasing the key dimension, selecting more than 10 bytes both for the bitxor operation and for the permutation as well. Another method is working on groups of two (digrams, 16b), three (trigrams, 24b) or four (tetragrams, 32b) characters. The transformations applied to the masked version may contain, for the same purpose, mixing transformations, as the ones suggested by Shannon, [70]. The proposed cipher is a closed secrecy system. Having finite key number, it will have unique solution. When the elements of the key involved in transformations and are not known, important delays in recovering the solution are caused, even knowing the masked version of the plain.

The key elements used in this cipher are presented in Table 6.2. They are disposed in two matrices. Matrix \( K_\zeta \) contains elements of the key which intervene in transformations of type \( \gamma \). So, on every column of the matrix \( K_\zeta \) there are 10 ASCII characters which are distinct each one from the others and randomly chosen, \( \alpha_{1,1} \neq \alpha_{1,2} \neq \alpha_{T,10} \). The illustration is done for a simple case, where the matrix was reduced to one column, but the procedure may be extended to multiple columns.

Similarly, the matrix \( K_P \) has columns formed with any 10 bytes randomly chosen, constraint to be distinct \( \beta_{1,1} \neq \beta_{1,2} \neq \beta_{T,10} \). They are the permutation \( P \) chosen by the transformation of type \( \gamma_2 \).

2 Deciphering

Once the receiver gets the set of masked characters \( m' \) either directly, or deduced from the series \( \{x_3\} \), knowing the 10 bytes for bitxor and the 10 bytes for the permutation, in dependence with the evolution of the generalized Hénon map, he is led directly to the message. The synchronization between emission and reception systems must be ensured. Thus, he benefits from the easily reversibility of the two enciphering transformations.

6.3 Analyze of results of the proposed enciphering algorithm

The results obtained using the simple case when the key has only \( 2 \cdot 10 \) bytes as key elements, a column in \( K_\zeta \) and a column in \( K_P \), Table 6.2.

1 Results of encryption of natural language text

Fig. 6.4 presents the frequency of occurrence of ASCII characters in natural language texts. It can be observed the preference for the interval corresponding to letters, numbers
and spacing characters. In Fig. 6.5, after encryption, one can observe the tendency of equalization of the frequencies of occurrence of ASCII characters.

Figure 6.4: Frequency of occurrence of ASCII characters in a natural language text.

Figure 6.5: Frequency of occurrence of ASCII characters in ciphered version.

2 Results when enciphering images

The proposed enciphering algorithm has quite good results on images also, when every pixel of the image, ASCII number, is analogously enciphered. In Fig. 6.6 it can be observed that pixels mix in non-recognizable manner.

Figure 6.6: Original image (left) and enciphered image (right).
3 A concrete example. The enciphering and the deciphering of a character.

Let us suppose that the character 'C' is enciphered. The function $f = \sin\left(\frac{x_1 - x_2}{2}\right) = -0.7665$ selects the first subinterval in Fig. 6.1. The binary number $\alpha_{1,1} = 222$ (11011110 in binary) and the permutation $P$ (see equation (6.5)) are assigned to the first box.

$$
P = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
5 & 3 & 8 & 6 & 4 & 2 & 7 & 1
\end{pmatrix}
$$

(6.5)

**Enciphering**

The character 'C' is encoded in ASCII format as the number 67. In binary representation this means 01000011.

'C' 0 1 0 0 0 0 1 1
ζ 1 1 0 1 1 1 0 0
R 1 0 0 1 1 1 0 1

The R byte is then permuted according to permutation $P$. The binary value of the result is $m' = 10011101$. To obtain the number that will be included in the evolution of the chaotic generalized Hénon map, at the next iteration, $m'$ is transformed into decimal and divided by $\nu = 10^5$. The value $\tilde{m} = 186 \cdot 10^{-5}$ is then summed up to the first equation of the system (2.17). The ASCII value $m' = 186$ is the encoding for the '∥' character.

**Deciphering**

At the reception, from the series of the $\{x_3\}$ values, the number of the box is retrieved. Knowing the values of the scaling factor $\nu = 10^5$ and the bifurcation parameters $a$ and $b$, the value for $\tilde{m}$ is determined with the formula (6.2) as being $\tilde{m} = 186$. The knowledge of the assigned inverse permutation $P^{-1}$ from equation (6.6) allows the computation of the $R$ value. Therefore, $R = 157$, binary represented as 10011101. As the operation modulo 2 without carry is invertible, knowing $\zeta_1 = 222$, allows the calculation of the plain character $m(k)$, where $k$ corresponds to the index of the character 'C' in the plain-text.

$$
P^{-1} = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
8 & 6 & 2 & 5 & 1 & 4 & 7 & 3
\end{pmatrix}
$$

(6.6)

R 1 0 0 1 1 1 0 1
ζ 1 1 0 1 1 1 1 0
'C' 0 1 0 0 0 0 1 1
6.4 Conclusions

We propose an algorithm that uses simple transformations, multiple substitutions and fixed transposition type. They are embedded by a hyperchaotic system having a simple form that allows easy synchronization between emission and reception, offering a random-deterministic rule to choose in a non-preferential way the enciphering key. The method has the advantage of multiple possibilities of improvement and extension.

Showing a stronger correlation than the text, images reveal the weaknesses of the method of encryption. Redundancy between the color planes is diffused, but it does not reach its uniformity, just as it is expected from a good practical cipher, [70].

Ideas to improve the algorithm are multiple and suggested by our research activity:

- a chaotic generator (the logistic map, for example) can be used to disperse the redundancy of the image (text) before its transformation by S-boxes and P-boxes. A hardware implementation of chaotic generators is performed for the logistic map-based generator in [47] and [66]. Better results are obtained for the tent map-based chaotic generator in [67].
- the external secret-key can be varying, and not be kept fixed. The paper [83] extends the running-key cipher for ergodic sources in order to provide good quality generators for chaotic cryptography.
- the samples of the generalized Hénon map can be taken in accordance with the independence distance determined using the Badea-Vlad test, and not at successive iterations.
- two or more simple systems as the generalized Hénon map, can alternatively be used, in order to increase the mixing of areas associated to the substitution and transposition boxes.
- enciphering can be done on $m$-grams (groups of $m$ bytes), not per pixel (ASCII character).

In its simplest form, the algorithm is presented in the paper [22]. The minimum distance for independence and transient for the generalized Hénon map are determined in [46]. The field of cryptography and the statistical study that extracts identically and independently distributed data from chaotic systems are put in relationship in [23].

The high degree of feasibility of analog systems (continuous also in time, not only in amplitude), and that of the observers allowing the recovery of the message included in their dynamics, l’Hernault demonstrated in [43], suggests a new idea to improve the proposed cipher, easily adaptable to the new considered system. A novel idea for chaos based cryptosystems is to mix discrete-time and continuous-time chaotic systems in order to enrich the embedding dynamics which includes the secret message. See [38].

To mix the two kinds of systems, a sampling is necessary for the continuous-time. We have done a step in this direction by implementing the above described generalized Hénon map based scheme, on an AVR microcontroller, in [74]. The gain in such of implementation is not at the level of the processor, but the possibility to use analog circuitry for the continuous dynamics, followed by an analog-to-digital conversion in order to include its samples in the discrete dynamics.

It remains, however, the problem of the identifiability of the bifurcation parameters of the system, when known plain-text attacks are effectuated.
A proposal that aims to robustify ciphers based on chaotic dynamics to known plaintext attacks is proposed by Hamiche in [38]. A hybrid dynamical system, constituted by the discrete generalized Hénon map and the continuous-time Colpitts oscillator, is used to transmit secret information. In this direction, we show an AVR-microcontroller implementation of the algorithm from [22], in the paper [74].

Chapter 7 raises some questions, and tries to find some of the answers, in the context of hybrid dynamical schemes.

A first idea is to substitute the Colpitts oscillator with a continuous time delay (infinite dimensional dynamic, because it is necessary to characterize the whole phase space not only in the present moment, but also in the past, a continuum of moments between $t_0 - \tau$ and $t_0$ being required).

Is it possible to recover the secret message by using an observer, when the dynamics that includes it is time delayed, [18], [19]? The answer is positive, at the simulation level. We illustrate this possibility, in the work [24] for a delay chaotic system inspired by Uçar [81], where a full transmission of the output of the system (the cryptogram) is considered. Section 7.1 presents this results.

What if the transmission is only done over a fraction of the time? Is the synchronization between continuous delayed dynamics when they communicate only a very short time, (see for another point of view [49], [65])?

To begin this study, we implemented in analog, unidirectional synchronization (information is only transmitted from the transmitter to the receiver) between two Colpitts oscillators. Results and comments are given in section 7.13.

### 7.1 Reconstructing the dynamics of a delayed transmitter

The aim of this section is not to deal with the secure data transmission by synchronization of chaotic delayed systems. Nevertheless, the thread of this work is secure data transmission.

Here, the main purpose is to show that it is possible to directly solve a left invertibility problem for chaotic delayed systems with Levant’s homogenous sliding mode differentiator [54].

For the ease of exemplification, a two dimensional, very simple delayed system is considered. A homogeneous third order sliding mode observer [54] is used, to recover the dynamics of the transmitter and the secret message.

The structure of the observer is slightly modified in order to resolve the left invertibility problem. To take into account the noisy output measurement, due to the noise in the public channel, some low pass filters are added.
To highlight the efficiency of high order sliding mode observers an academical secure data transmission scheme based on chaos synchronization is used. It corresponds to the so called inclusion method [27] and it is represented in Fig. 7.1. The robustness of the aforementioned example with respect to known plain text attacks is not the goal here. Though, it is important to underline that it is generally more difficult to identify continuous-time delayed chaotic systems than classical ones.

Figure 7.1: Chaos synchronization by means of high order sliding mode observers, using the inclusion of the secret message in the dynamics of the chaotic emitter.

The subsection 7.1.1 presents the proposed chaotic delayed system. In subsection 7.1.2 recalls on high order sliding mode are given. The proposed observer is introduced. Subsection 7.1.3 shows the simulation results and their analysis.

1 A chaotic delayed transmitter

For timed chaotic systems, three dimensions are required in order to fulfill the requirements of the complex behavior. One of the main advantages of delay systems is the possibility to generate a chaotic behavior with a state dimension smaller than three.

The following chaotic delayed system, strongly inspired by [81], is proposed as transmitter:

\[
\begin{align*}
\dot{x}_1 &= x_2 - x_1 \\
\dot{x}_2 &= x_2(\tau) - x_3^2(\tau) + 0.5 \left[ 1 + \left( \frac{x_2}{10} \right)^2 \right] u \\
y &= x_1 
\end{align*}
\]  

where \( x = (x_1, x_2)^T \) is the state, \( y \) is the output, and \( u \) is the message. Moreover, \( x_i \) denotes the \( i \)-th state of the system at time \( t \), \( x_i(\tau) \) denotes the state \( x_i \) at time \( t - \tau \), the initial conditions are \( x_1(0) \) and the function \( x_2(t) \), defined on \([-\tau, 0]\).

The behavior of system (7.1) for \( u \) equal to zero is chaotic as shown in Fig.7.2, where the three dimensional space behavior \((x_1, x_1(\tau), x_2)\) is given for \( \tau = 1.6s \). We have given the state portrait in three dimensions in order to highlight the key-role of the delay.

Setting, as academical example, a message of the form:

\[ u(t) = A \sin(\omega t) \]  

with \( A = 0.5V \) and \( \omega = 2\pi f \), where \( f = 1Hz \), the chaotic state space behavior of \((x_1, x_1(\tau), x_2)\) is preserved as shown in Fig. 7.2 (right).

Remark: The preservation of the chaotic behavior is the first restriction on the additional message; another restriction is that the message must not be detectable in

91
Figure 7.2: The states $x_1, x_1(\tau), x_2$. The initial conditions are: $x_1(0) = 0, x_2(0) = 0.1$ and $x_2(t) = 0, \forall t \in [-\tau, 0)$. The message is $u = 0$ (left) and $u = 0.5 \left[ 1 + \left( \frac{x_2}{10} \right)^2 \right]$ (right).

Figure 7.3: The output of the transmitter with the message included in the evolution of the delayed chaotic transmitter. The initial conditions are: $x_1(0) = 0, x_2(0) = 0.1$ and $x_2(t) = 0, \forall t \in [-\tau, 0)$.

the output by a simple frequency analysis. Other restrictions will be given in the next section. Obviously, it is also possible to send binary messages, if the amplitude of such messages is small enough to preserve the chaotic behavior.

The state $x_1$ of the transmitter (7.1) is presented with the message included in the evolution of the delayed chaotic system in Fig.7.3.

2 A third order sliding mode observer as the receiver of the secret message

At the reception, the ciphertext, $y$, is represented by the first state of the transmitter (7.1). A high-order sliding mode observer, (7.4), is used in order to recover the states $x_1$ and $x_2$ of the transmitter and the secret message $u$ included in its evolution, when knowing only its output $x_1$. The presented proposed observer is based on the so-called real-time exact robust HOSM differentiator [56]. Considering the output $y(t)$ at least $\mathcal{C}^k$ (at least $k$ times differentiable) the $k$-differentiator (i.e. recovering $\dot{y}, \ddot{y}, ..., y^{(k)}$, from the measurement of $y$) has the following form:
\[
\begin{align*}
\dot{z}_0 &= u_0 \\
\nu_0 &= z_1 - \lambda_k M \frac{1}{\nu_1} \vert z_0 - y \vert^{\frac{2}{3}} \text{sign}(z_0 - y) \\
\dot{z}_1 &= \nu_1 \\
\nu_1 &= z_2 - \lambda_{k-1} M \frac{1}{\nu_0} \vert z_1 - \nu_0 \vert^{\frac{1}{k-1}} \text{sign}(z_1 - \nu_0) \\
&\vdots \\
\dot{z}_{k-1} &= \nu_{k-1} \\
\nu_{k-1} &= z_k - \lambda_1 M \frac{1}{\nu_{k-2}} \vert z_{k-1} - \nu_{k-2} \vert^{\frac{1}{2}} \cdot \text{sign}(z_{k-1} - \nu_{k-2}) \\
\dot{z}_k &= -\lambda_0 M \text{sign}(z_k - \nu_{k-1})
\end{align*}
\]

(7.3)

In the present case, a third order HOSM differentiator is enough. This implies that \( y \) must be at least \( C^3 \). Moreover, as the observer must reconstruct the states and the secret message \( u \), using only the knowledge of \( y \), an extended state \( x_3 = 0.5[1+(\nu_1/10)^2]u \) is needed in order to obtain also the unknown input. Obviously, this dynamical extension implied some assumptions on the unknown input. Hereafter, all hypotheses on \( u \) are summarized:

**Hypothesis 1:**
- \( u \) must be sufficiently small in order to preserve the chaotic behavior of (7.1).
- \( u \) must be sufficiently small and within the frequency bandwidth of the transmitter in order to be undetectable by output frequency analysis.
- \( u \) must be at least \( C^1 \) and both \( u \) and its derivative must be bounded.

Finally, the proposed observer has a slightly different form from (7.3) in order to reduce the gain \( M \), and taking into account the structure of (7.1):

\[
\begin{align*}
\dot{\hat{x}}_1 &= \dot{x}_2 - y - 3M^{1/3} \vert \dot{x}_1 - y \vert^{2/3} \text{sign}(\dot{x}_1 - y) \\
\dot{\hat{x}}_2 &= \dot{x}_2(\tau) - \dot{x}_2(\tau) + \dot{x}_3 - 1.5M^{1/2} \cdot \vert \dot{x}_2 - \nu_0 \vert^{1/2} \text{sign}(\dot{x}_2 - \nu_0) \\
\dot{\hat{x}}_3 &= \frac{\dot{x}_2(\tau) - \dot{x}_2(\tau) + \dot{x}_3}{50} \cdot \frac{\dot{x}_3}{1 + (\frac{\dot{x}_2}{10})^2} \cdot (-1.1M) \text{sign}(\dot{x}_3 - \nu_1)
\end{align*}
\]

(7.4)

where

\[
\begin{align*}
\nu_0 &= \dot{x}_2 - 3M^{1/3} \vert \dot{x}_1 - y \vert^{2/3} \text{sign}(\dot{x}_1 - y) \\
\nu_1 &= \dot{x}_3 - 1.5M^{1/2} \vert \dot{x}_2 - \nu_0 \vert^{1/2} \text{sign}(\dot{x}_2 - \nu_0)
\end{align*}
\]

**Proposition:** If the initial conditions of system (7.1) are in the attraction basin of the strange attractor, and if all conditions in the hypothesis 1 are verified, then there exists \( M_0 > 0 \) such that \( \forall M \geq M_0 \), observer (7.4) resolves the left invertible problem for system (7.1) (i.e. the recovering of \( x_2 \) and \( u \)).

**Sketch of convergence proof:**
Denoting \( e := x - \dot{x} \), a sliding manifold one has is:

\[
\begin{align*}
e_2 - 3M^{1/3} \vert e_1 \vert^{2/3} \text{sign}(e_1) &= 0 \\
e_3 - 1.5M^{1/2} \vert e_2 \vert^{1/2} &= 0 \\
0.5 \left[ 1 + \left( \frac{\dot{e}_2}{10} \right)^2 \right] \dot{u} - 1.1M \text{sign}(\dot{x}_3 - \nu_1) &= 0
\end{align*}
\]
For convergence analysis with the homogeneity argument see [54], [55] and for noise robustness see [7]. From (7.5), one obtains

\[ x_2 = \hat{x}_2 - 3M^{1/3}|e_1|^{2/3}\text{sign}(e_1) = \nu_0 \]
\[ x_3 = \hat{x}_3 - 1.5M^{1/2}|e_2|^{1/2} = \nu_1 \]

So, when \( e_1 \) and \( e_2 \) have converged, \( \hat{x}_2 = x_2 = \nu_0 \) and \( \hat{x}_3 = x_3 = \nu_1 \). Consequently, from the definition of \( x_3 \), it can be concluded that:

\[ u = \frac{\hat{x}_3}{0.5 \left[ 1 + \left( \frac{\hat{x}_1}{10} \right)^2 \right]} \]

This ends the sketch of proof.

3 Experimental results.

In order to prove the performance of the proposed observer, simulations were done in Simulink and relevant results were obtained. The simulation was done over 400s, with a fixed sampling step of \( T_s = 5 \cdot 10^{-6} \) s, using the first order Euler’s method in order to solve the ordinary differential equations (ODE) describing the dynamics of the transmitter (chaotic delayed continuous system) and of the receiver (high-order sliding mode observer). On the public channel, the output \( y = x_1 \) of the transmitter reaches the receiver (7.4). The estimations of the states and of the unknown input are presented in two cases:

- **Noise-free channel.**
  After a transient time of 1.94 s, the estimated message \( \hat{u} \) converges to the secret message embedded in the evolution of the transmitter, \( u \), as shown in Fig. 7.4. A low pass Butterworth second order filter was used in order to obtain an accurate chattering-free waveform. The transfer function \( H(s) = \frac{1}{s^2 + \sqrt{2}s + 1} \) uses a cutoff frequency \( \omega_c = 30 \) rad/s. Due to filtering, a delay exists between the two signals. In [17] an analysis of the high-frequency self-sustained oscillations called chattering in continuous sliding-mode controllers is performed.

  The estimated state \( \hat{x}_1 \) converges to the state \( x_1 \) of the transmitter after a short time, approximatively 0.06 s. The evolution of the two signals is represented in Fig. 7.5 and the error \( e_1 = \hat{x}_1 - x_1 \) in Fig. 7.6. Similarly, the estimated state \( \hat{x}_2 \) converges to the state \( x_2 \) of the transmitter after a short time, approximately 1.65 s, the evolution of the two signals being represented in Fig. 7.7 and the error \( e_2 = \hat{x}_2 - x_2 \) in Fig. 7.8.

- **Channel affected by additive Gaussian band-limited white noise.**
  The considered Gaussian additive band-limited noise has a power of \( P_{\text{noise}} = 10^{-3} \) W, when compared to a signal power of \( P_{\text{signal}} = 1 \) W, which gives a signal-to-noise ratio of \( SNR = 30 \) dB. The measured noisy transmitted output is filtered, using the same filter as the one used for the estimation \( \hat{u} \), prior to its input to the sliding-mode observer. Fig. 7.9 illustrates the \( y \) signal at the output of the noisy channel. The estimated message \( \hat{u} \) converges to \( u \) in 2 s, as shown in Fig. 7.7. The convergence of \( \hat{x}_1 \) to the state \( x_1 \) is shown in Fig. 7.11, and the convergence of \( \hat{x}_2 \) to \( x_2 \), in Fig. 7.12.

  The experimental gain of the observer is \( M = 10^4 \), \( e_1 = \hat{x}_1 - x_1, \nu_0 \) and \( \nu_1 \) are amplified \( K = 10^5 \) times.

  The presented results stand as proof for the performance of the proposed observer in estimating the states of the transmitter and its unknown input, in the case of a chaotic continuous delayed system, considering the transmission through noise-free channel and through a channel affected by Gaussian additive noise, solving the left invertibility problem these dynamics impose.
Figure 7.4: The estimated $\hat{u}$, in blue, and the transmitted message $u$, in red. The initial conditions are: $x_1(0) = 0, x_2(0) = 0.1$ and $x_2(t) = 0, \forall t \in [-\tau, 0)$.

Figure 7.5: The estimated $\hat{x}_1$ in red, and the state $x_1$ in blue. The initial conditions are: $x_1(0) = 0, x_2(0) = 0.1$ and $x_2(t) = 0, \forall t \in [-\tau, 0)$.

Figure 7.6: The error in estimating $x_1$. 
Figure 7.7: The estimated $\hat{x}_2$ in red, and the state $x_2$ in blue. The initial conditions are: $x_1(0) = 0, x_2(0) = 0.1$ and $x_2(t) = 0, \forall t \in [-\tau, 0)$.

Figure 7.8: The error in estimating $x_2$.

Figure 7.9: The noisy $y$ in blue, and $y$ in red.
Figure 7.10: The estimated $\hat{u}$ in red and the transmitted message $u$ in blue; noisy channel.

Figure 7.11: The estimated $\hat{x}_1$ in red, and the state $x_1$ in blue; noisy channel.
A third-order sliding-mode observer was presented. Its efficiency on the estimation of the states and of the unknown input of a chaotic continuous delayed system was demonstrated. The main contribution is to propose an observer to solve the left invertible problem for a particular chaotic delayed system, with and without noisy output measurement. There are many extensions to this preliminary work: the faster and more complicated chaotic delayed transmitter in order to be closer to the secure transmission of real data, analysis of the robustness of such systems to a known plain text attack, conceiving an observer for a chaotic delayed hybrid dynamical system, using the same left invertible technique of high order sliding mode for identification or diagnosis purposes. In a more general context, it may be interesting to synthesize a generic high order sliding mode observer for delayed systems, and to determine under which conditions such an observer works.

7.2 Synchronization of analog circuits via sparse measurement.

We implemented the synchronization between two chaotic Colpitts oscillators in analog circuitry. The components and their assembly is done as in Fig.7.13. These two chaotic oscillators are intended to be used as the transmitter and the receiver of a secret digital ASCII-encoded message scaled so that the chaotic dynamics of the Colpitts oscillator is not altered. The supply voltages are $V^+ = 8.9V$ and $V^- = -4.19V$. We have examples of how chaotic synchronization can be achieved in [79] and [80]. The first article clarifies that the difference in structure of the two oscillators translates itself by a phase shift in the synchronization. The latter paper gives the reason why the synchronization is independent of the systems that synchronize being linear or not: the synchronization is imposed by a minimum of exchanged energy.

The two Colpitts oscillators synchronize unidirectionally (a buffer ensures the transmission only from the transmitter to the receiver), in the chaotic regime, communicating through a $R_{sync} = 0.47\Omega$, as it can be seen in Fig.7.14. The transmission of the output of the emitter is continuous. The resistance $R_{sync} = 0.47\Omega$ is a low value, which is explained by the coupling point of the Colpitts oscillators. The circuit in common-base configuration has a very low input impedance (through the emitter). Consequently, the coupling current must be significantly higher than the emitter current $I_E$. Thus, the
Figure 7.13: The synchronization between two chaotic Colpitts oscillators. Orcad scheme.

necessity for a low coupling resistance value. Experimentation shows that going above 10 – 20Ω results in very difficult synchronization.

Figure 7.14: Synchronization of two chaotic Colpitts oscillators. Continuous coupling between the two circuits.

The next step is to decrease the temporal coupling between the emitting and receiving circuits. The analog switch CD4066 is commanded with a pulse having amplitude from −4V to 8V, and at a frequency $f = 50kHz$. In this case, the Shannon-Nyquist sampling theorem is satisfied, $f > 2 \cdot f_0$. The oscillation frequency of the Colpitts oscillator used for those experiments is $f_0 \approx 22kHz$.

The weakest admissible coupling between the transmitter and the receiver is 2%. The results illustrated by Fig. 7.15 show that the two circuits are extremely weakly synchronized. Increasing the coupling to $\eta = 10\%$ and to $\eta = 20\%$, the synchronization is slightly ameliorated, see Fig. 7.16.

As the duration of the transmission is increased more, the graphic tends more and more to resemble the first bisector, which corresponds to the identity of the two signals. This tendency can be observed in Fig. 7.17 and Fig. 7.18.

When the coupling between the two circuits is set at $\eta = 98\%$, the synchronization should be perfect, as in Fig. 7.14. The graphic in Fig. 7.19 shows a deficient synchronization. Despite a long-time coupling, the imperfection of the synchronization can be explained by the input resistance of the switch $CD4066$, as it can be observed from
its data-sheet. Given the supply voltages of the switch, the integrated circuit has the
input resistance of $R_{ON}$ of about 100Ω, while a perfect synchronization was obtained
for 0.47Ω. This is slightly improved by using a second buffer (U1B in Fig. 7.13). The
duration of the connexion between the transmitter and the receiver is slightly increased,
thus explaining a very good synchronization (compare Fig. 7.14 and Fig. 7.25). The high
input impedance of this element induces an important time constant which alters the
speed of the closing of the switch and distorts the synchronization channel transmitted
to the receiver. We counterbalance this effect by diminishing the input resistance of the
In order to increase accuracy, a second buffer is added at the output of the switch, to compensate its high output impedance. Experiments are repeated in the new configuration and represented in Fig. 7.20.

An additional resistance $R_{\text{switch}} = 1.2k\Omega$ is added between the output of the switch and ground, in order to avoid the lagging of the signal. Results are illustrated in Fig. 7.24, Fig.7.25, Fig.7.26 and Fig. 7.27.
In conclusion, the synchronization is increasingly better with the duration of the coupling between the transmitter and the receiver.

First, the transmission was set to be continuous (the duty factor $\eta = \frac{T}{T} = 100\%$). When plotting the estimation of the output of the transmitter versus itself, the first bisector was obtained. This proves the synchronization of the two considered systems. When decreasing the transmission duration to $80\%, 50\%, 30\%$ and $10\%$ the capability of synchronization of the two oscillators decreases. This is due to integrated circuits that simulate the transmission channel (the buffer for unidirectional transmission of the
information, the switch used to allow only a fraction of the transmission period of the oscillator), and, especially, to the operation in low output impedance of the common base configuration of the bipolar junction transistor which is the active element of the Colpitts oscillator.

The experiments, despite its imperfections ($R_{ON}$ to large), show that diminishing the time during which the two circuits (transmitter and receiver) are coupled, results in the degradation of the synchronization. This result corresponds to the theoretical expectations. It is reasonable to deduce that using a switch with a low resistance $R_{ON}$
Figure 7.27: Synchronization of two chaotic Colpitts oscillators. Transmission during $\eta = 70\%$ (left) and $\eta = 50\%$ (right). Second buffer and resistance added.

will allow a good synchronization with a coupling of 50%.

An open challenge is to achieve synchronization via sparse measurements of the output of delayed analog chaotic systems. Or, at least, to determine whether such synchronization is possible or not.
Chapter 8

Conclusions

My research work is an extension of the experiments and investigations developed by my colleagues: Adrian Luca with his thesis „Statistical analysis of chaotic systems from the perspective of the utility in cryptography”, Mădălin Frunzete having „Contributions in the field of cryptography based on chaotic systems using information theory and statistics”, Maryam l’Hernault-Zanganeh who proved, in theory and practice, the „Feasibility of an analog emission-receiving system for the secure communications using chaos” (Faisabilité d’un système d’émission-réception analogique pour les communications sécurisées par le chaos) and Hamid Hamiche analyzing the „Left inversion of the hybrid chaotic dynamical systems. Application to secured transmission of data” (Inversion à gauche des systèmes dynamiques hybrides chaotiques. Application à la transmission sécurisé des données).

This Thesis deals with the domain of cryptography based on hybrid chaotic dynamics. In order to increase the robustness of the security in data transmission with respect to known text attacks, this work was particularly focused on two directions: the statistical approach and the control system theory. The main contributions of this work are organized in the mentioned two directions. Our approach is done in the context of hybrid (continuous and discrete time dynamics mixing) chaotic secured transmission of the data. The Chapters of the thesis answer to some questions raised by these communication schemes.

In Chapter 2 we take from the literature the algebraic equations which describe the systems we analyze. Usually, the description given in the literature lack in being accompanied by more than one parameters pair which engender chaos. To get an wider range for thevalues of the bifurcation parameters, we adapt existing algorithms in order to compute the Lyapunov exponents, known as detecting the chaotic behavior of a system, when the values of the parameters of the system are kept fixed. We remind that at least one positive Lyapunov exponent implies chaotic behavior, and the presence of at least two positive Lyapunov exponents is the mark of a hyper-chaotic behavior. The computation of the Lyapunov exponents spectra was the opportunity to briefly present the history of the systems mentioned above and some of their statistical properties. We analyze:

1. the generalized Hénon map (equations 2.17), discrete, three-dimensional, hyper-chaotic.
2. the Hitzl-Zele map (equations 2.18), discrete, three-dimensional, structurally more complex than the generalized Hénon map.
3. the chaotic Colpitts oscillator (equations 2.29), continuous, three-dimensional, allowing the introduction of continuous delays, leading to an infinite dimension of
the chaotic dynamics.

We made use of some pairs mentioned in the literature to determine the domain in which at least one Lyapunov exponent of the investigated systems is positive.

For the generalized Hénon map, when keeping the parameters $a = 1.76$ or $b = 0.1$ fixed, observing the results in Table 8.1, we conclude that, for the chaotic region, the domain for the parameter $b$, when $a$ is kept fixed at 1.76 is the interval $b \in (0.06, 0.078) \cup (0.080, 0.085) \cup (0.085, 0.100)$. For the chaotic behavior of the generalized Hénon map, when $b$ is kept fixed at $b = 0.1$, the parameter $a \in \{(1.4, 1.8)\}$.

Table 8.1: The Lyapunov exponents for the Hénon map.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.76</td>
<td>(0.06, 0.078)</td>
<td>$&gt; 0$</td>
<td>$= 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>1.76</td>
<td>(0.078, 0.080)</td>
<td>$= 0$</td>
<td>$= 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>1.76</td>
<td>(0.080, 0.085)</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>1.76</td>
<td>(0.085, 0.150)</td>
<td>$&gt; 0$</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0.8)</td>
<td>0.1</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(0.8, 1.1)</td>
<td>0.1</td>
<td>$= 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(1.1, 1.4)</td>
<td>0.1</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(1.4, 1.5)</td>
<td>0.1</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(1.5, 1.8)</td>
<td>0.1</td>
<td>$&gt; 0$</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
</tr>
</tbody>
</table>

The behavior of the generalized Hénon map for some of the $(a, b)$ pairs belonging to the intervals determined in Table 8.1 are illustrated in the Chapter 9.

Observing the evolution of the Lyapunov spectra for the Hitzl-Zele map, we can deduce that the intervals in which the parameters $a$ and $b$ are situated for chaotic behavior of the system are as following: $a \in (0.25, 0.3)$ for fixed $b = 0.87$ and $b \in \{(0.25, 0.35) \cup (0.81, 0.90)\}$ for fixed $a = 0.25$. The sign of the Lyapunov exponents for each interval of the $a, b$ parameters is summarized in Table 8.

The behavior of the generalized Hitzl-Zele map for some of the $(a, b)$ pairs belonging to the intervals determined in Table 8 are illustrated in the Chapter 9.

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-0.7,-0.4)</td>
<td>0.87</td>
<td>$= 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(-0.4,-0.25)</td>
<td>0.87</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>(0.25,0.3)</td>
<td>0.87</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>$\lambda_1$</th>
<th>$\lambda_2$</th>
<th>$\lambda_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.25</td>
<td>(0.25,0.35)</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>0.25</td>
<td>(0.35,0.81)</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
<tr>
<td>0.25</td>
<td>(0.81,0.90)</td>
<td>$&gt; 0$</td>
<td>$&lt; 0$</td>
<td>$&lt; 0$</td>
</tr>
</tbody>
</table>
Chapter III presents a study of some structural properties of the chaotic systems from Chapter II. The investigation is focused on the calculation of the observability indexes and the determination of the manifolds of observability singularity.

Chapter IV analyses the statistical independence in the context of the considered chaotic systems: how large should be the sampling distance (how many iterations or, equivalently, time) to ensure statical independence between variables extracted from the chaotic systems.

An original test for statistical independence (the Badea-Vlad test) was used: the procedure is applicable to all kind of continuous random variables, even of unknown probability law as needed here.

Chapter V illustrates the physical point of view. The transient time corresponds to the time spent by the chaotic system in the basin of attraction before rejoining the strange attractor. It is also important to know after how long the points localized in a certain region of the strange attractor become uncorrelated.

In Chapter VI, knowing the identifiability of the parameters of chaotic systems described by polynomial equations, an improvement of the inclusion of messages in this type of enciphering is proposed. The plain-message is enciphered using classical substitution and transposition boxes, prior to its inclusion in the chaotic transmitter. The results of the proposed algorithm are evaluated on text and image.

Chapter VII rises some questions, and tries to find some answers to these questions, in the context of hybrid dynamical schemes. As for example if it is possible to recover the secret message by using an observer, when the dynamics that includes it is time-delayed. The answer is positive and this is shown in the case of a full transmission of the output of the system.

It is important to mention that this work is multidisciplinary, starting from control theory and going to the statistical methods through the fields of electronics, mathematics and computing.
Bibliography

[1] N. Adila, and F. Senan, Department of Mechanical Engineering University of California at Berkeley, A brief introduction to using ode45 in MATLAB.


[75] Student [William Sealy Gosset], The probable error of a mean, Biometrika, 6 (1908), pp. 1–25, reprinted on pp. 11–34 in “Student’s” Collected Papers, Edited by E. S. Pearson and John Wishart with a Foreword by Launce McMullen, Cambridge University Press for the Biometrika Trustees, 1942, 1908.


[86] J. Widloski, R. Hovden, P. Mathew, Deterministic chaos lab, School of Physics, Georgia Institute of Technology, Atlanta, GA 30332.

Chapter 9

Annexes

9.1 Baptista’s cryptography with chaos

This thesis is based on a study which is situated at the intersection of the interests of two research groups: Professor’s Adriana Vlad research group, in Bucharest, Romania, and Professor’s Jean-Pierre Barbot team, from Cergy-Pontoise, France. Therefore, my work approaches the applicability of chaotic systems in cryptography and the afferent problematics from the statistical point of view, together with a perspective from the control system theory.

My first concrete application was to implement Baptista’s chaos-based cryptography method [13]. Baptista’s algorithm arouses curiosity in the research field. His method is applied on images ([48]), it is criticized and improved ([4], [59]). He emphasis the ergodic property of the logistic map and its usefulness in cryptography, giving the opportunity of new ideas in this direction: the work [35] uses the logistic map to disturb the correlation among pixels prior to a second encryption step based on a hyper-chaotic system generated from Chen’s chaotic system, and [62] employs an external of 80 bits and 2 chaotic logistic map to transmit secure data. Baptista’s paper led to new works, which made possible creating a frame for the evaluation of the chaos-based cryptosystems ([5] and [10]). Physical Resistance-Inductance-Diode (RLD) circuits, giving birth to signals similar to the logistic map, were implemented and evaluated based on the existing theory ([86], [2], [40]). Baptista’s method can be described in some phrases as follows: he limits the co-domain of the logistic map ([0,1]) to [0.2,0.8] and divides this interval into S (=256) subintervals corresponding to each ASCII character. Each subinterval has the length \( \epsilon = \frac{x_{max} - x_{min}}{S} \), where \( x_{min} = 0.2 \) and \( x_{max} = 0.8 \). In Fig. 9.1 we present the corresponding intervals for some characters. The logistic map is initialized in [0, 1] and, after a transient time of 250 iterations, among the values of the function, the first visit of the interval assigned to the plain-character to be enciphered is searched, as in Fig. 9.2. The number of the iteration corresponding to the first visit of the searched subinterval is stored as the cryptogram, and the logistic map is reinitialized with the precise value it has at that moment, and the next character is enciphered as in Fig. 9.3. The enciphering procedure is reiterated until the entire plain-text is enciphered.
Figure 9.1: The subintervals corresponding to some of the ASCII characters, in Baptista’s enciphering method.

Figure 9.2: Enciphering the character ‘O’ as the first letter of a plain-text, with Baptista’s enciphering method.
Figure 9.3: Enciphering the character 'c' as the second letter of a plain-text, with Baptista’s enciphering method.

9.2 Different behaviors of the studied chaotic systems.

1 The generalized Hénon map
Figure 9.4: The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=0.04$ and $b=0.1\lambda_1$, $\lambda_2$, $\lambda_3$, $<0$.

Figure 9.5: The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=0.4$ and $b=0.1\lambda_1$, $\lambda_2$, $\lambda_3$, $<0$.
Figure 9.6: The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.25$ and $b=0.1$ ($\lambda_1, \lambda_2, \lambda_3, < 0$).

Figure 9.7: The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.43$ and $b=0.3$ ($\lambda_1 > 0, \lambda_2 > 0, \lambda_3, < 0$).
Figure 9.8: The evolution of the generalized Hénon map over 10000 iterations, with parameters $a=1.6$ and $b=0.1$ ($\lambda_1 > 0$, $\lambda_2 > 0$, $\lambda_3 < 0$).

2 The generalized Hitzl-Zele map

Figure 9.9: The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.275$ and $b=0.87$. 

122
Figure 9.10: The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.3$.

Figure 9.11: The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.5$.

3 The Colpitts chaotic oscillator
Figure 9.12: The evolution of the Hitzl-Zele map over 10000 iterations, with parameters $a=0.25$ and $b=0.88$.

Figure 9.13: The evolution of the Colpitts chaotic oscillator over 400s, with $T_s = 0.001s$, with parameters $g=4.46$ and $Q=1$ ($\lambda_1 > 0$, $\lambda_2 < 0$, $\lambda_3 < 0$).

9.3 Ergodicity hypothesis for the generalized Hénon map

Table 9.1: Smirnov test values $\delta = |F_{e_X}(u) - F_{e_Y}(u)|$. Ergodicity of the generalized Hénon map.

<table>
<thead>
<tr>
<th>$k_i$</th>
<th>45</th>
<th>50</th>
<th>55</th>
<th>60</th>
<th>65</th>
<th>70</th>
<th>75</th>
<th>80</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\delta$</td>
<td>0.007</td>
<td>0.007</td>
<td>0.008</td>
<td>0.002</td>
<td>0.004</td>
<td>0.001</td>
<td>0.006</td>
<td>0.007</td>
</tr>
</tbody>
</table>
Figure 9.14: The evolution of the Colpitts chaotic oscillator over 400s, with $T_s = 0.001s$, with parameters $g=1.01$ and $Q=1.38$ ($\lambda_1, \lambda_2, \lambda_3, < 0$).

Figure 9.15: The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 15$, and the temporal cumulative distribution function $F_{eY}$. 
Figure 9.16: The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 25$, and the temporal cumulative distribution function $F_{eY}$.

Figure 9.17: The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 35$, and the temporal cumulative distribution function $F_{eY}$.
Figure 9.18: The cumulative distribution functions \( F_{\epsilon X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 45 \), and the temporal cumulative distribution function \( F_{\epsilon Y} \).

Figure 9.19: The cumulative distribution functions \( F_{\epsilon X}(u) \) of the random variable \( X \) obtained by sampling the random process assigned to the first state of the generalized Hénon map, at \( k_1 = 50 \), and the temporal cumulative distribution function \( F_{\epsilon Y} \).
Figure 9.20: The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 55$, and the temporal cumulative distribution function $F_{eY}$.

Figure 9.21: The cumulative distribution functions $F_{eX}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 60$, and the temporal cumulative distribution function $F_{eY}$.
Figure 9.22: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 65$, and the temporal cumulative distribution function $F_{e_Y}$.

Figure 9.23: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 70$, and the temporal cumulative distribution function $F_{e_Y}$. 
Figure 9.24: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 75$, and the temporal cumulative distribution function $F_{e_Y}$.

Figure 9.25: The cumulative distribution functions $F_{e_X}(u)$ of the random variable $X$ obtained by sampling the random process assigned to the first state of the generalized Hénon map, at $k_1 = 80$, and the temporal cumulative distribution function $F_{e_Y}$. 