Discrete-Time Synchronization of Chaotic Systems for Secure Communication

I. Belmouhoub[1], M. Djemai[2], J-P. Barbot[2] and K. Busawon[3]

[1]Equipe Commande des Systèmes (ECS), ENSEA,
6 Av. du Ponceau, 95014 Cergy-Pontoise Cedex.
[2]Univ Lille Nord de France, F-59000 Lille, France
UVHC, LAMIH, F-59313 Valenciennes, France
CNRS, UMR 8530, F-59313 Valenciennes, France
[3]Northumbria Univiversity
School of Computing, Engineering & Information Science
Newcastle upon Tyne, UK
mohamed.djemai@univ-valenciennes.fr ,
krishna.busawon@unn.ac.uk , barbot@ensea.fr

***Abstract*—This paper deals with the problem of designing an exact nonlinear reconstructor for discrete-time chaotic encrypted messages. More precisely, we investigate the problem of designing a discrete-time dead-beat observer for nonlinear systems with unknown inputs. The application of the proposed observer in the context of secure communication and data transmission is also investigated.**

I. Introduction

Since the past two decades, there has been an increasing interest in the problem of synchronization of chaotic systems due to their potential application in secure communication. In effect, in [11], Pecora and Carroll showed that when state variable from a chaotically evolving system is transmitted as an input to a copy of the original system, the replica subsystem (receiver) can synchronize to the original system (transmitter). In [10] they presented the synchronization of two Lorenz systems with different initial conditions.

Following these two works, a huge attention to the synchronization of chaotic systems was then paid due to their potential applications in secure data transmission ([9], [7], [12], [11], [7], [14], [5]...). For this, the idea of masking the messages by the chaotic signal generated by the transmitter and then transmitting the information to the receiver under the form of a combined signal - consisting of the addition of the message and the chaotic signal - was proposed. The message was then recovered by synchronizing the receiver with the scalar signal transmitted by the transmitter.

This synchronization may be viewed as an observer design problem (see for example the work of H.Nijmeijer and I. Mareels in [9]). Moreover, in [5] the authors have proved that the design of observer for system with unknown input may be used in the context of secure communication.

This paper proposes a new encryption algorithm based on chaotic models and a nonlinear discrete time observer. The main motivation in considering discrete time models id due to the fact that, the information such as it employed nowadays is in most cases digitalized and processed by computers. Thus it becomes primordial to study systems at discrete time.

Additionally, the increasing development of broadband networks and services, alongside the recent demand for privacy and paid services, has led to the need for systems and algorithms to encrypt information [15]. The most important applications include the encryption of video messages for pay-TV services, voice over IP (Internet Protocol), and data messages transmitted over telemetric networks (electronic signatures, electronic banking and commerce, etc.).

As already mentioned above, chaotic signals and systems for private or secured communications have been investigated with increasing interest in the last few years (see references of authors [1], [2], [3], [4]). The advantage of using methods based on chaos theory lies in the high level of security chaotic systems offer as compared with traditional encryption techniques. At the same time they are very competitive due to the fact that they are inexpensive to implement.

The application scenario of chaotic encryption mainly considered in literature is a traditional analog or digital communication system in which the transmitter and receiver must be synchronized in order to have a correct decoding phase [20], [21].

In particular in this paper, we describe the potential of a new chaotic ciphering process applied to secured communications based on the inclusion of the message in the structure of the transmitter.

II. Problem statement

The aim of our work consist in the design and the validation of digital schemes for secure communications based on chaotic maps. Past results have led to a prototypal realization of schemes based on synchronization. The actual objective is to optimize the choice of the chaotic system and its parameters, investigating its behavior in a real application context and its robustness against unauthorized receiver attacks. To realize this objective, we adopt a technique based on inclusion of the message in the system structure (see figure 1).

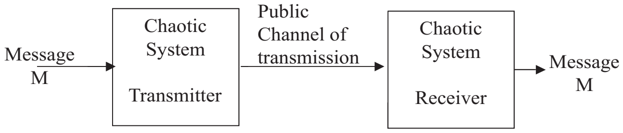

Fig. 1: Inclusion Method

In order to illustrate the last method let us consider the following discrete time system

$$x^{+} = f(x, u, p) \tag{1}$$

With x^{+} used instead of $x(k+1)$ and the state vector $x \in \Re^{n}$ instead of $x(k)$, $u \in \Re$ is the control variable, $p \in \Re^{m}$ is the parameters vector of the system, and the vector field $f : \Re^{n+m} \times \Re \longrightarrow \Re^{n}$. So, we can choose, without loss of generality the output as any component of the state variables.

The idea consist in using the parameter p as carrier of the message m, that is for example

$$u' = u + M \tag{2}$$

We replace u by u' in the equation of the transmitter which gives

$$x^{+} = f(x, u', p) \tag{3}$$

where, each iteration of the state convey to the $k-th$ byte of the message (text file, sound or image ...). In the public channel, only the output y will be sent to the receiver. To obtain the message, we have to synchronize both transmitter and receiver. This last one is the copy of the original system (1) of the form

$$\hat{x}^{+} = f(\hat{x}, u, p) \tag{4}$$

the error between the transmitter and the receiver
$e = x - \hat{x}$ is

$$e^{+} = f(x, u', p) - f(\hat{x}, u, p) \tag{5}$$

the method consist in trying to extract M from the equation of the error (5).

Remark 1: The inclusion method may be seen as an observer design with unknown input (M in the equation 3).

III. Main contribution

Recall that chaos is a deterministic, random-like process found in non-linear dynamical system, which is non-periodic and bounded. Moreover, it has a very sensitive dependence on its parameters and initial conditions generating it. A chaotic *Mandelbrot* map is a discrete-time dynamical system running in chaotic state and of the form:

$$\begin{matrix} x^{+} = f(x, u, p) \\ y = h(x) \end{matrix} \tag{6}$$

with:

$$f(x, u, p) = \left(\begin{array}{l} b + (a+b)x_1 + x_3 + x_1^2 - x_2^2 \\ b + c + 2x_1 x_2 \\ u \end{array} \right)$$

where $p = (a, b, c)^{T}$ is the parameters vector, u is the control that we apply to the system in order to preserve the chaotic behavior (for the simulations we will set $u = 0.09$). The constants b and c consist of the key shared between the sender and the receiver. The initial conditions are also a part of the key, but they are known to the transmitter. This system formed by basic function $f : \Re^{6} \times \Re \longrightarrow \Re^{3}$ is a chaotic generator and has the following properties:

- f has sensitive dependence on initial conditions;
- f is topologically transitive; i.e. if, given any two intervals U and V, there is some positive integer k such that $f^{k}(U) \cap V \neq \emptyset$. Vaguely, this means that neighborhoods of points eventually get flung out to "big" sets so that they don't necessarily stick together in one localized clump.

Intuitively, a map possesses sensitive dependence on initial conditions if there exist points arbitrarily closed to x which eventually separated from x by at least $\delta > 0$ under some iterations of f. On the other hand, a topologically transitive map has points which eventually move under iterations from one arbitrarily small neighborhood to any other. Thus a chaotic system is unpredictable because of the sensitivity on initial conditions perturbations.

Any chaotic system should be mixing, i.e. the phase space $\Re^{n}$ should be randomly mixed by repeated action of f. Further, most chaotic systems depend on some control parameters and exhibit sensitivity with respect to those parameters.

An ideal chaotic signal presents the main properties of a secure cryptographic system: it is unpredictable and it cannot be reliably reproduced. Starting from different parameters, in fact, it is impossible to obtain two identical series, even though the difference between the parameters is a very slight one. This is an essential feature of chaotic systems. Roughly speaking, encryption and chaos exhibit remarkably similar features. The parameters and the initial conditions can be used as the encoding key. Furthermore, some variations of parameters can be used as support of the *message* to amount; it is the idea of the method by inclusion (see figure 1).

Chaotic sequences are uncorrelated when their initial values are different. In addition, it is possible to synchronize two copies of a discrete-time chaotic system, in the sense that their state trajectories tend asymptotically to be identical when one system is suitably driven by the other. If the driving signal is selected appropriately, the discrete-time synchronization will be immediate.

To achieve the transmitter-receiver synchronization immediately, we try to apply the discrete-time synchronization to chaotic spread-spectrum communication systems by proposing a novel communication scheme.

In this work, we consider the nonlinear discrete time map given in (6). It is assumed that the output y is measured at discrete instances. We will consider conditions which guarantee that these measurements determine x exactly. Consequently, we describe how x can be computed by an observer with features similar to a dead-beat observer. This map exhibits a chaotic behavior in a large neighborhood of the parameter values.

The encryption algorithm proposed in our application, is based on the synchronization of both transmitter and receiver, which are represented by the same chaotic model and the message is hidden in the chaotic structure of the transmitter, for more security. Where the synchronization problem has been resolved quite simply by exploiting the intrinsic synchronization offered by the use of a dead-beat observer.

To study the problem of synchronization in discrete-time context, we assume the following system :

$$\begin{aligned} x_1^+ &= f_1(x_1, x_2, u', p) \\ x_2^+ &= f_2(x_1, x_2, u', p) \end{aligned}$$

Such that $x = (x_1, x_2)^T$, where $x_1 \in \Re^{n-1}$, $x_2 \in \Re$, and u' (defined in (2)) is the unknown control applied to the system. Let us choose $y = x_2$ as output.

Then the observer equations are:

$$\hat{x}_1^+ = \hat{f}_1(\hat{x}_1, x_2, u, p, y, ..., y^{N-}) \tag{7}$$

where $y^{i-} = y(k-i) \quad \forall\ i = 0, .., N$, and the observation errors are:

$$\begin{aligned} e_1^+ &= x_1^+ - \hat{x}_1^+ \\ &= f_1(x_1, x_2, u', p) - \hat{f}_1(\hat{x}_1, x_2, u, p,_k\ , ..., y_{k-N}) \end{aligned} \tag{8}$$

Synchronization of both systems now corresponds to required condition, that is:

$$\lim_{k \longrightarrow \infty} \|x - \hat{x}\| \longrightarrow 0 \tag{9}$$

This condition of asymptotic synchronization, will not be satisfied in general and, in fact, assumptions on f_1 and f_2 that guarantee this condition are only partially known. The technique which we propose in this paper, ensures a faster convergence, independently of the chaotic structures of f_1 and f_2. Indeed, our secure transmission scheme enable, a finished-time synchronization of the original system and the observer . i.e.

$$\forall\ k \succ k_0,\ \|x - \hat{x}\| = 0,\ \text{where } k_0 \text{ a small integer} \tag{10}$$

Remark 2: It is important to note that in our technique, the system may have some singularities bifurcations. However, it is impossible to use the implicit function theorem and in the same time the methods developed in [7] and [14] in order to reconstruct the state vector of the transmitter. In our case, we will use the information of delayed outputs values $y_k, ..., y_{k-N}$ and the observation error to reconstruct the transmitted message.

So we can see that the observation errors will reach exactly zero in three steps regardless of their initial values. This, means that chaotic systems achieve synchronization after three steps. Due to the deterministic nature of chaotic motions, once synchronization has been achieved, both systems remain synchronized.

Now let us consider the Mandelbrot system, and let us note that M represent the message and only the information $y = x_2$, the chaotic output, is transmitted to the receiver via a public channel. Then, the transmitter will have the following form

$$\begin{aligned} x_1^+ &= b + (a+b)x_1 + x_3 + x_1^2 - y^2 \\ x_2^+ &= b + c + 2\, x_1 y \\ x_3^+ &= u + M \end{aligned} \tag{11}$$

While the receiver will have the following form

$$\begin{aligned} \hat{x}_1^+ &= b + (a+b)\hat{x}_1 + \hat{x}_3 + \hat{x}_1^2 - y^2 \\ \hat{x}_2^+ &= b + c + 2\, \hat{x}_1 y \\ \hat{x}_3^+ &= u \end{aligned} \tag{12}$$

The dynamic error is given by

$$\begin{aligned} e_1^+ &= x_1^+ - \hat{x}_1^+ \\ &= (a+b)e_1 + e_3 + x_1^2 - \hat{x}_1^2 \\ e_2^+ &= x_2^+ - \hat{x}_2^+ = 2\, \hat{x}_1 y \\ e_3^+ &= M \end{aligned} \tag{13}$$

We can see from these equations that we have to compute e_3 to find the message. Before that, we must prove the synchronization of both systems (transmitter and receiver). For this, it is enough to show that $e_1 \longrightarrow 0$.

So the second equation gives $e_1 = \dfrac{e_2^+}{2y}$, which tends to zero for $y \neq 0$ (because $e_2 \longrightarrow 0$). Consequently, when $y = 0$ this leads to a singularity. However, to overcome this problem we will adopt the following definition of e_1 as:

$$e_1 = \frac{e_2^+ y}{2y^2 + \varepsilon}$$

Where $\varepsilon > 0$ is a small parameter. Under this consideration e_1 still converges to zero $\forall\ y \in \Re$.

So, to compute the error e_1^+ we need y^{++} which is not available at time $(k+1)$, to bypass this problem, we have to compute $\tilde{x}_1$ the reconstructed state of the transmitter $x_1$as:

$$\tilde{x}_1 = e_1 + \hat{x}_1$$

then, we obtain:

$$\tilde{x}_1 = \begin{cases} \hat{x}_1 + \dfrac{e_2^+ y}{2y^2 + \varepsilon} & \text{if} \quad |y| \gg \varepsilon \\ \hat{x}_1 & \text{if} \quad |y| \leq \varepsilon \end{cases}$$

And this will allows us to implement calculate $\tilde{x}_1$ in the first equation of the deed-beat observer

$$\begin{aligned} \hat{x}_1^+ &= b + (a+b)\tilde{x}_1 + \hat{x}_3 + \tilde{x}_1^2 - y^2 \\ \hat{x}_2^+ &= b + c + 2\, \hat{x}_1 y \\ \hat{x}_3^+ &= u \end{aligned} \tag{14}$$

It is now possible to compute e_1^+ as:

$$\begin{aligned} e_1^+ &= x_1^+ - \hat{x}_1^+ \\ &= (a+b)e_1 + e_3 + (\hat{x}_1 + e_1)^2 - \hat{x}_1^2 \\ &= (a + b + 2\hat{x}_1)e_1 + e_1^2 + e_3 \end{aligned}$$

from which we extract the observation error e_3

$$e_3 = -(a + b + 2\hat{x}_1)e_1 - e_1^2 + e_1^+$$

then, we obtain

$$\begin{aligned} e_3^{--} &= -(a+b+2\hat{x}_1^{--})e_1^{--} - \left(e_1^{--}\right)^2 + e_1^{-} \\ &= -(a+b+2\hat{x}_1^{--}) \left(\frac{e_2^{-} y^{--}}{2(y^{--2})+\varepsilon}\right) \\ &\quad - \left(\frac{e_2^{-} y^{--}}{2(y^{--2})+\varepsilon}\right)^2 + \left(\frac{e_2 y^{-}}{2(y^{-2})+\varepsilon}\right) \end{aligned}$$

Now, from the equation $e_3^{+} = M$, to find the message we delay e_3 two times for seek of causality:

$$e_3^{--} = x_3^{--} - \hat{x}_3^{--} = M^{---}$$

which means that $e_3(k-2) = M(k-3)$. So we have to wait three steps before starting to receive the message (i.e. recover M).

The delays applied to the reconstructed message depends strongly on the length of the chaotic system and on the position of the implemented message. In this example, the system is three dimensional and the message intervenes in the third equation, which explains the delay of three steps to recover the message.

Remark 3: In order to avoid the loss of information, we can add to the beginning of our confidential message, another message without particular meaning. This message should not be long, only three words (some bits are enough, the time that the transmitter and the receiver synchronize).

IV. SIMULATIONS RESULTS

To illustrate the efficiency of the proposed technique of ciphering, we consider the Mandelbrot system (11) as a transmitter and (12) as a receiver with the following initials conditions and parameters values: $a = 0.8$, the keys: $b = 0.2$ and $c = -0.7$. Finally, the initial condition: $x_1(0) = -0.2744$, $x_2(0) = -0.452$, $x_3(0) = 0.091$.

We carried out a computer-based experiments which allow us to encrypt and decrypt given files as well text as image or sound. The encryption and decryption programs were written with the Visual C++ version 6.0. The Following experiment results show that the synchronization of both systems (transmitter and receiver) is immediate and the communication result is correct and reliable.

It is necessary in this technique that the parameters of the system stay in a certain domain, appointed by a "Arnold tongues" [22] because if they exceed it, the system diverges from the chaotic trajectory and "blow up" completely. This occurs also for a bad choice of the initial conditions.

We can exploit this other characteristic of the chaos, in order to tighten up the transmissions security; by implementing high-dimensional chaotic systems, having a significant number of parameters, these possessing a rather wide "Arnold tongues ". Because, more this strip is wide, more the probability to success an "exhaustive attack" (for example) against the system, is weak.

We noticed that the second state of the system contains an important singularity, that we can isolate in the form of hyperplane. We can exploit this singularity to increase the security of our technique and this by introducing a function θ which will prolongs the singularity the necessary time to disorientate the possible "pirate" when he will try to intercept the chaotic signal, by making diverge its process of deciphering. This function is defined as follows

$$\theta(x_2) = \begin{cases} 0 & \text{if } |x_2| \leq \text{“}threshold\text{”} \\ x_2 & \text{else} \end{cases}$$

The "threshold" is chosen so as to respect the chaotic behavior of the used generator (10^{-4} in this example). This modification applied, as well to the transmitter as to the receiver, may perturb the trajectory of the chaotic signal and imply afterward a loss of punctual information. However, we do not have to choose between the quality of the reception and the security, if we use a good filter, allowing us to offset this loss of information.

The algorithm has been successfully applied to sound, pictures (see Figure 2 and Figure 3), texts and tested on the Visual C++ version 6.0.

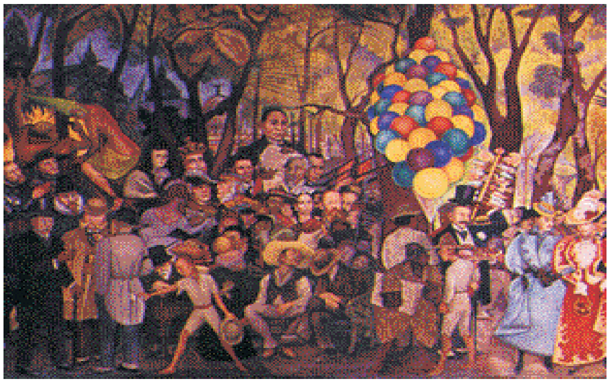

Fig. 2: Original picture

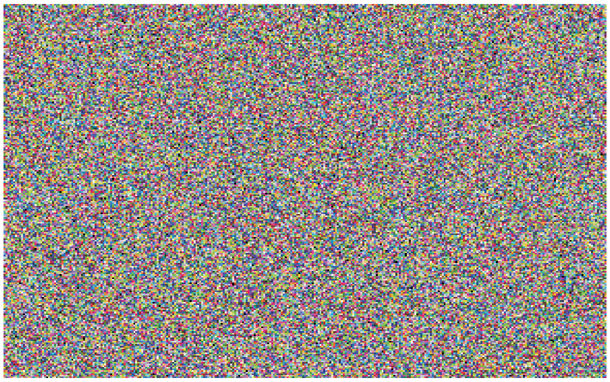

Fig. 3: Encrypted picture

It is important to note that in our case, this output is not used as a carrier signal for the message. It is included in the structure of the chaotic system (transmitter). The correct transmitter/receiver synchronization has been verified using several testing examples, but only the *Mandelbrot* model is presented in the paper. These test shows that the decryption algorithm does not depend on the type of information transmitted (audio, video, data) or the processing (if any) that the messages undergoes (compression, etc.).

V. Conlusion

In this paper, we have designed an exact nonlinear reconstructor for discrete-time chaotic encrypted messages. The application of the proposed observer for secure communication and data transmission was studied. In order to optimize the transmission time, it was shown that it is better to minimize the ratio between the clear message and the encrypted one. For this, one can for example, transmit, at the same time, three characters instead of one. Hence, for three characters input, we obtain four characters output, which reduce significantly the encrypted text size on the transmission line. However, to realize this type of encoding, one must be very careful as for pre-established boundaries of the given chaotic system and envisage a reducing factor of the digitized value of the message (ASCII code for text). This, in order to do not overflow variation field, this, necessary, leads the chaos to diverge from its trajectory. This last remark holds, for a signal transmission, whose amplitude should be known beforehand to calculate the suitable reduction to insert in the chaotic structure.

References

[1] I. Belmouhoub, M. Djemaï , J-P. Barbot, "*Observability quadratic normal forms for discrete-time systems*", IEEE Trans. On Automatic Control, Vol. 50, No. 7, pp. 1031-1038, July, 2005.

[2] M. Djemaï, J.P. Barbot and D. Boutat, "*New type of data transmission using a synchronization of chaotics systems*" International Journal of Bifurcations and Chaos, Vol 15, No 1, 1-17, 2005.

[3] M. Djemaï, J.P. Barbot and I. Belmouhoub,*Discrete time normal form for left invertibility problem*, in European Journal of Control, EJC Issue, in European Journal of Control, N2, Vol-15, pp 194-204, 2009.

[4] L. Boutat-Baddas, J-P. Barbot, D. Boutat and R. Tauleigne, "*Observability bifurcation versus observing bifurcations*". In Proc. Ifac World Congress, 2002.

[5] H.J.C. Huijberts, T. Lilge, H. Nijmeijer,"*Nonlinear Discrete-Time Synchronization Via Extended Observers*",International Journal of Bifurcation and Chaos, Vol 11, No 7, pp 1997-2006. 2001.

[6] U. Kotta,"*Inversion method in the discrete-time Nonlinear control systems synthesis problems, lecture notes in control and information sciences*", Vol 205. Springer-Verlay. 1995.

[7] T. Lilge, " *Nonlinear Discrete-Time observers for synchronization problems*", LNCIS 244, New Direction in nonlinear Observer Design, pp 491-510. 1999.

[8] S. Monaco and D. Normand-Cyrot, "*Functional expansions for nonlinear discrete-time systems*", Math.systems.theory,Vol 21, pp 235-254. 1989.

[9] H. Nijmeijer and I.M.Y. Mareels, "*An observer looks at synchronization*", IEEE Trans. on Circuits and Systems-1: Fundamental Theory and Applications, Vol 44, No 10, pp 882-891. 1997.

[10] L.M. Pecora and T.L. Carroll, "*Synchronizing in chaotic systems*". Phy. Rev. Let. 64, pp 821-823. 1990.

[11] L.M. Pecora and T.L. Carroll, "*Synchronizing chaotic circuits*". IEEE Trans. Circuits Systems 38, pp 453-456. 1991.

[12] U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle and A. Shang, Transmission of digital signals by chaotic synchronization, *Inter. Journal of Bifurcation and Chaos,* Vol 2, No 4, pp 973-997. 1992.

[13] A. Rapaport and A. Maloum,"*Embedding For Exponential Observers Of Nonlinear Systems*", In 39th CDC Conference.CDROM. 2000.

[14] H. Sira-Ramirez, C. Aguilar Ibanez and M. Suiarez-Castanon, " *Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems*". Personal communication. Internal report (CINVESTAV-IPN). 2001.

[15] W. Stallings, "*Cryptography and Network Security: principles and practice*", Prentice Hall, New Jersey. 1998.

[16] D. R. Frey, "*Chaotic Digital Encoding: An Approach to Secure Communication*", IEEE Trans. on Circuits System, Part II, Vol 40, No 10, pp 660-666. 1993.

[17] M. Gotz, K. Kelber and W. Schwarz, "*Discrete-Time Chaotic Encryption Systems - Part I: Statistical Design Approach*", IEEE Trans. on Circuits and System, Vol. 44, No 10, pp 963-970, Oct. 1997.

[18] T. Stojanovski, L. Kocarev and U. Parlitz, "*Digital Coding via Chaotic System*", IEEE Trans. on Circuits and System, Vol. 44, No 6, pp 562-565, 1997.

[19] F. Dachselt, K. Kelber and W. Schwarz,"*Chaotic Coding and Cryptoanalysis*", Proceedings of ISCAS'97, pp 1061-1064. 1997.

[20] G. Kolumban, M. P. Kennedy and L. O. Chua, "*The Role of Synchronization in Digital Communications Using Chaos-Part I: Fundamentals of Digital Communications*" IEEE Trans. on Circuits and Systems, Vol 44, No 10, pp 927-936, Oct. 1997.

[21] A. De Angeli, R. Genesio, and A. Tesi, "*Dead-Beat Chaos Synchronization in Discrete-Time System*", IEEE Trans Circuits Syst.-Part I, Vol 42, No 1, pp 54-56. 1995.

[22] S. Wiggins, "*Introdusction to applied Nonlinear Dynamical Systems and Chaos*", Springer-Verlag. 1990.