ELSEVIER

13 October 1997

PHYSICS LETTERS A

Physics Letters A 234 (1997) 429–435

Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos

Chang-song Zhou [a], Tian-lun Chen [b,c,a]

[a] *Department of physics, Nankai University, Tianjin 300071, China*
[b] *CCAST (World Laboratory), Beijing 100080, China*
[c] *Institute of Theoretical Physics, Academia Sinica, P.O. Box 2735, Beijing 100080, China*

Received 19 June 1996; revised manuscript received 2 April 1997; accepted for publication 30 June 1997
Communicated by A.P. Fordy

Abstract

We show that the binary information masked by low dimensional chaos with the encoding method proposed by Parlitz and Ergezinger [Phys. Lett. A 188 (1994) 146] can be extracted with very simple methods, even though the channel noise level is rather high. The security of communication approaches using chaotic dynamics is generally discussed. © 1997 Published by Elsevier Science B.V.

PACS: 05.45.+b; 43.72.+q
Keywords: Communication; Chaos; Masking; Robustness; Security

1. Introduction

Chaotic dynamics with noise-like broadband power spectra is an interesting candidate for encoding and masking information signals in secure communication. Different approaches to realize this basic idea of using a chaotic signal as broadband carrier have been proposed. Most of them are based on synchronization of chaotic systems to recover the information signals [1–5]. Other methods include controlling chaotic systems to follow a desired wave form in which a message is encoded [6], and making use of the quick decay of the correlation function for chaotic signals [7].

Masking information with chaos is done to improve the security of communication. However, chaotic dynamical systems exhibit regular geometric structures which are often far from random when viewed in some suitable phase space. So it is possible to reveal the hidden information by recreating the geometric structure with some prediction based methods [8], particularly when the hidden signals are added to the chaotic carrier at very low power, which is demanded for sufficient masking and for the receiver to synchronize with the transmitter [1,8]. Also it is possible to find some suitable return maps which allow the information to be extracted [9]. These works indicate that using chaos as spread-spectrum carrier may be secure for casual but not motivated observers. Moreover, the sensitiv-

0375-9601/97/$17.00 © 1997 Published by Elsevier Science B.V. All rights reserved.
PII S0375-9601(97)00551-3

ity of chaotic synchronization to external noise may beget difficulties for the receiver as well as any party intending to intercept the information to recover the information accurately.

Focusing on the robustness of chaotic communication to external noise, Parlitz and Ergezinger proposed a method for encoding and transmitting binary data using chaotic systems [7]. In this Letter we will show that the information encoded with this method can be easily extracted with very simple methods if chaotic dynamics generated by low dimensional chaotic systems like the logistic map (used in Ref. [7]) are used to mask the information. Particularly, the information can be extracted with a very small error probability, even though the transmitted signals are contaminated with noise.

To begin with, let us give a brief description of the method presented by Parlitz and Ergezinger, The transmitter and receiver are supposed to generate the same chaotic sequence $\{x(n)\}$ according to a chaotic map $x(n+1) = f(x(n))$. Each binary information symbol $b^k \in \{-1, 1\}$ is associated to a string of N elements $x(n)$ $(n = 1 + (k-1)N, \ldots, kN)$, and b^k is encoded as the string

$$s(n) = b^k x(n). \tag{1}$$

The transmitted signal $s(n)$ is distorted by some external interferences $e(n)$ during the transmission and is received as $r(n) = s(n) + e(n)$. By computing the correlation function

$$C^{kN} = \sum_{n=1+(k-1)N}^{kN} r(n)x(n), \tag{2}$$

the information signal is recovered as

$$\begin{aligned} b_R^k &= -1, \quad C^{kN} < 0, \\ &= 1, \quad C^{kN} > 0. \end{aligned} \tag{3}$$

The authors studied the robustness of the method by estimating the error probability

$$P_e = P(b_R^k \neq b^k) \tag{4}$$

versus the noise level, showing that this method is robust to external interferences because of the quick decay of the correlation function of the chaotic signals. However, the information can only be recovered correctly in the case that the two chaotic systems of the transmitter and the receiver have exactly the same initial condition. Otherwise, any difference between the initial conditions will finally lead to much different chaotic signals due to the positive Lyapunov exponent of the systems, and the information bits cannot be recovered even though there is no external noise. To examine this effect, we consider the logistic map $x(n+1) = 1 - 2x^2(n)$ as in Ref. [7]. The transmitter is initiated with $x(1) = 0.2$ while the receiver has $x'(1) = 0.2 + 0.0001$. With a random information sequence of 2.5×10^5 bits and $N = 127$ (the same as in Ref. [7]), the error probability in the noise-free case is estimated as $P_e = 0.212$. So it seems very difficult for an eavesdropper to extract the information.

In the following, we present two simple methods to extract the information masked by chaos generated by the logistic map and distorted by external noise.

2. Extracting with return map: method I

For the method in Ref. [7] to work, the chaotic sequence $\{x(n)\}$ should have such symmetry that the switching from $s(n) = x(n)$ to $s(n) = -x(n)$ cannot be detected by visual inspection of the transmitted sequence $\{s(n)\}$, and the receiver must have exactly the same initial condition of the transmitter. It is possible that a motivated eavesdropper intending to intercept the information has knowledge of f and N (the logistic map $f(x) = 1 - 2x^2$ and $N = 127$ is used in this Letter, as in Ref. [7]), but not of the initial condition on which the decoding of the method depends. To explain the extracting method, we begin with the noise-free case, i.e. $r(n) = s(n)$. When an even symmetric chaotic system $f(-x) = f(x)$ like the logistic map is used in the communication, we have

$$\begin{aligned} r(n+1) = g(r(n)) = f(r(n)), \quad & b^k = 1, \\ = -f(r(n)), \quad & b^k = -1. \end{aligned} \tag{5}$$

So the return map g constructed from $r(n)$ has two branches, labelled with $+1$ and -1 respectively, as illustrated in Fig. 1a. The two branches intersect at points P_- $((-\frac{1}{2}\sqrt{2}, 0))$ and P_+ $((\frac{1}{2}\sqrt{2}, 0))$. To extract the information, we follow the received signal from its beginning and examine which branch the point

$(r(n), r(n+1))$ falls in, similar to the method in Ref. [9]. For $b^k = 1$, all the N points $(r(n), r(n+1))$ $(n = (k-1)N, kN-1)$ are on branch $+1$, while all are on branch -1 that have $b^k = -1$. The information can be extracted correctly.

In practice, the transmitted signals are contaminated with external noise. $e(n)$, a random number in $[-d, d]$, is added to the transmitted signal as the external noise. The additive noise results in a smeared map, as shown by crosses in Fig. 1b with $d = 0.2$. The clear map (Fig. 1a) is superimposed to Fig. 1b for the sake of comparison. Three dashed lines through points P_- and P_+ divide the phase space into six sections, each labelled with $+1$ or -1, as shown in Fig. 1b. To recover the information, what we do is to examine which section the point $(r(n), r(n+1))$ falls in, and give the variable $c^k(n+1)$ the corresponding label value, $+1$ or -1. The noise may make a point $(s(n), s(n+1))$ on the clear map in a certain section with label $+1$ (-1) fall into another section with the inverse label -1 $(+1)$, resulting in an erroneous $c^{k(n+1)}$. Such noise-induced errors may occur only in the regions near points P_- and P_+, specifically, $[-\frac{1}{2}\sqrt{2} - d, -\frac{1}{2}\sqrt{2} + d]$ and $[\frac{1}{2}\sqrt{2} - d, \frac{1}{2}\sqrt{2} + d]$. So the majority of $c^k(n)$ have the same value as b^k when d is not too large. Letting

$$A^k = \sum_{n=1+(k-1)N}^{kN} c^k(n), \tag{6}$$

the information is recovered as

$$\begin{aligned} b_R^k &= 1, \quad A^k > 0, \\ &= -1, \quad A^k < 0. \end{aligned} \tag{7}$$

An example of this extracting procedure with $d = 0.6$ is illustrated in Fig. 2. Fig. 2a is the return map constructed from the received signal, which no longer shows the appearance of the clear map. After examining the points, we plot A^k in Fig. 2b. Finally, the information is recovered correctly in Fig. 2c.

When an antisymmetric map $f(-x) = -f(x)$ is used in the communication, we have

$$r(n+1) = f(r(n)) \tag{8}$$

for both $b^k = 1$ and $b^k = -1$ and $n \neq kN$ in the noise-free case. However, at the points $(r(kN), r(kN+1))$, we have $r(kN+1) = -f(r(kN))$ if the bit is switching from -1 to $+1$ or $+1$ to -1. So by examining the events of $r(kN+1) = -f(r(kN))$ successively, the information can also be extracted. A similar division of the phase space makes it possible to recover the information in the presence of the external noise. The robustness of the extracting may be degraded compared with that of the even symmetric map because there is not a similar scheme for correcting the noise-induced errors, as in Eqs. (6), (7).

The application of this extracting method is straightforward if other low dimensional chaos with a simple return map is used in communication. When the return map is more complex, the $+1$ branch and the -1 branch may have more cross points, and the division of the phase space may become more sophisticated. So the more complicated the return map of the transmitted signal is, the more difficult it is to reveal the information in the presence of noise. If the chaotic carrier is so complex that no distinguishable branches can be constructed and the extracting method can no longer be applicable, the communication can be regarded secure till other extracting methods have been developed.

3. Extracting with correlation function: method II

When one-dimensional even symmetric chaotic systems like the logistic map are used in the communication, we can also use another method to extract the information. Instead of generating the same chaotic sequence $x(n)$ demanded for recovering the information in the receiver, we generate a chaotic sequence $y(n)$ from the received signal according to the following scheme,

$$y(n+1) = f(r(n)) = 1 - 2r^2(n). \tag{9}$$

The correlation function now is

$$C^{kN} = \sum_{n=1+(k-1)N}^{kN} r(n)y(n), \tag{10}$$

where $y(1)$ is a random number. When there is no noise, $y(n) = x(n)$ for $n > 1$, and the difference between $x(1)$ and $y(1)$ has only very little effect on C^{1N} when N is relatively large. The information can be recovered according to Eq. (3) without error.

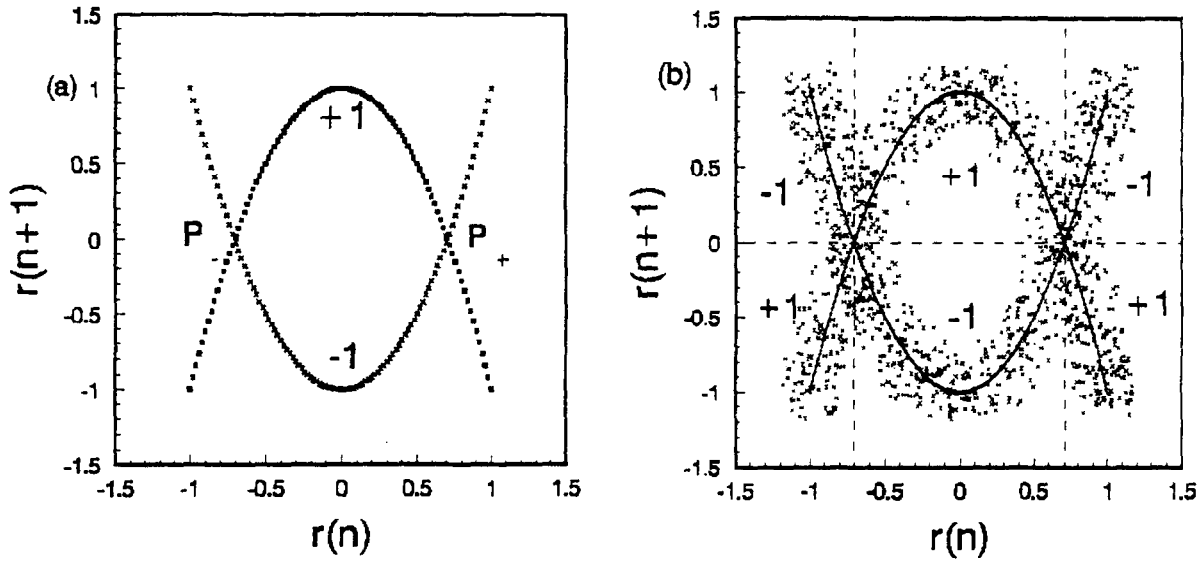

Fig. 1. (a) Return map $r(n) \sim r(n+1)$ without external noise. It consists of two branches with label $+1$ (dots) and -1 (crosses) respectively. P_- and P_+ are the intersect points of the two branches. (b) Return map $r(n) \sim r(n+1)$ (crosses) with external noise $e \in [-0.2, 0.2]$. The solid line is the clear map as in (a). The phase space is divided into six sections by three dashed lines, each having a corresponding label $+1$ or -1.

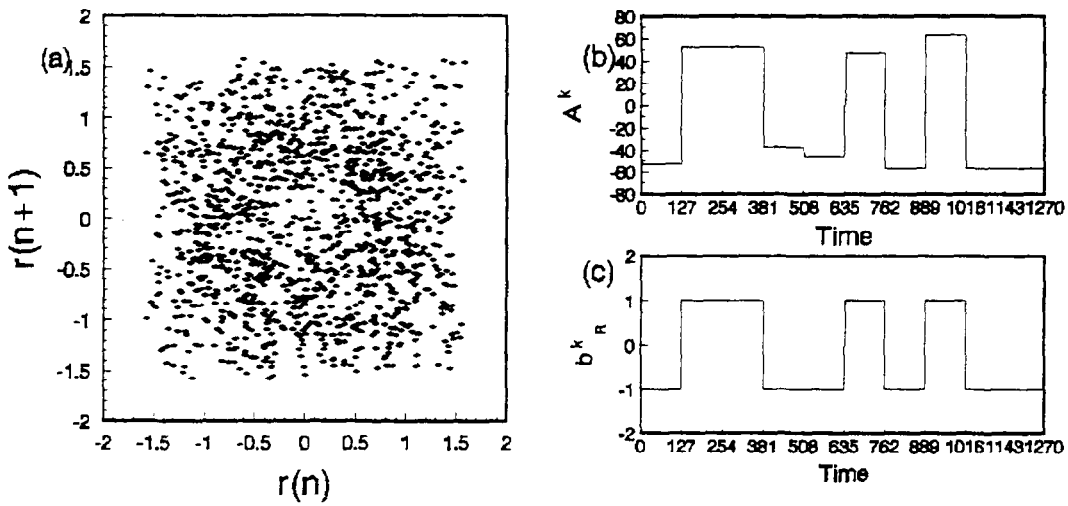

Fig. 2. Illustration of extracting procedure of method I. (a) Return map $r(n) \sim r(n+1)$, which contains noise $e \in [-0.6, 0.6]$. The points are no longer confined to the vicinity of the clear map as in Fig. 1b, because d is larger. (b) The value of A^k. (c) Correctly extracted bits b_R^k.

Now we study the performance of this method in the presence of noise. We denote $y(n) = x(n) + e'(n)$, where $e'(n) = -2e^2(n-1) - 4b^k x(n-1)e(n-1)$. Considering $\{x(n)\}_{n=1+(k-1)N}^{kN}$, $\{e(n)\}_{n=1+(k-1)N}^{kN}$, $\{e'(n)\}_{n=1+(k-1)N}^{kN}$ as N-dimensional vectors $\boldsymbol{x}^k$, $\boldsymbol{e}^k$ and $\boldsymbol{e}'^k$ respectively, we have

$$C^{kN} = \sum_{n=1+(k-1)N}^{kN} r(n)y(n)$$
$$= b^k\langle \boldsymbol{x}^k, \boldsymbol{x}^k\rangle + \langle \boldsymbol{x}^k, \boldsymbol{e}^k\rangle + b^k\langle \boldsymbol{x}^k, \boldsymbol{e}'^k\rangle + \langle \boldsymbol{e}^k, \boldsymbol{e}'^k\rangle, \quad (11)$$

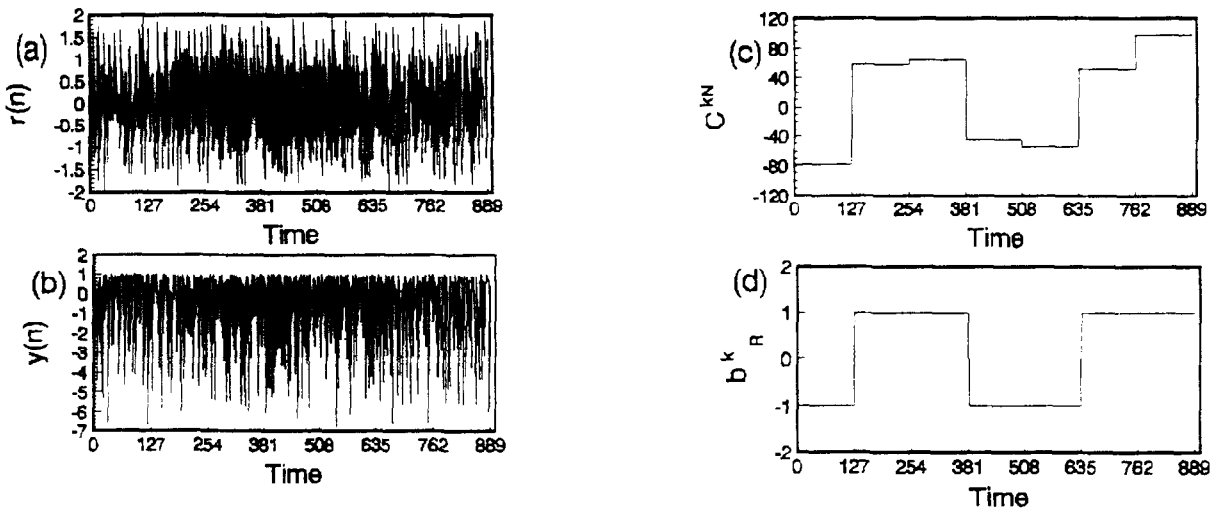

Fig. 3. Illustration of extracting procedure of method II. (a) Received signal $r(n)$ which contains noise $e(n) \in [-1, 1]$. (b) $y(n)$ generated with the received signals. (c) The correction function C^{kN}. (d) Correctly extracted bits b_R^k.

where $\langle\ ,\ \rangle$ means the scalar product of two vectors. The information can be recovered reliably if $|\langle \boldsymbol{x}^k, \boldsymbol{x}^k\rangle| > |\langle \boldsymbol{x}^k, \boldsymbol{e}^k\rangle + b^k\langle \boldsymbol{x}^k, \boldsymbol{e}'^k\rangle + \langle \boldsymbol{e}^k, \boldsymbol{e}'^k\rangle|$. Since $e(n)$ is independent of $x(n)$ and $e(n-1)$, the last three terms in Eq. (11) are very small provided that N is very large, as can be provided by the simulations. In the case of small N, for instance, $N = 127$ in this Letter, all the three terms in Eq. (10) may have considerable contributions to C^{kN}, and a recovery error may occur.

This extracting procedure with $N = 127$ is illustrated in Fig. 1. In this example, the transmitted signals are distorted by noise in $[-1, 1]$. The resulting received signal is shown in Fig. 3a. Fig. 3b is $y(n)$ generated according to Eq. (9). The values of the correlation functions C^{kN} are shown in Fig. 3c, and the information is recovered in Fig. 3d.

The above simple extracting method takes advantage of the even symmetry of the map f. If an antisymmetric map $f(-x) = -f(x)$ is used in the communication, it is obvious that this method will fail because in the noise-free case,

$$y(n+1) = f(r(n)) = x(n+1), \quad b^k = 1, \qquad = -x(n+1), \quad b^k = -1, \tag{12}$$

so that $C^{kN} > 0$ for all k and $b^k = -1$ is always recovered as $b_R^k = 1$.

4. Dependence of the methods on the noise level

To examine the performance of the simple extracting methods in the presence of external noise $e(n) \in [-d, d]$, we estimate the error probability P_e for different noise levels with random information sequences up to $K = 2.5 \times 10^5$ bits. For the sake of comparison, the original method in Ref. [7] is also studied.

With the above finite information bits, no error occurs ($P_e = 0$) when $d \leqslant 0.65$ for method I, $d \leqslant 0.85$ for method II and $d \leqslant 3.0$ for the method in Ref. [7]. As shown in Fig. 4, for all the three methods, P_e follows asymptotically an exponential law

$$P_e(R) = \alpha \exp(-\beta R), \tag{13}$$

with

$$R = \frac{\sum_n^{KN}[s(n) - \bar{s}]^2}{\sum_n^{KN}[e(n) - \bar{e}]^2}. \tag{14}$$

The constants α and β are estimated, giving $\alpha = 38.51$, $\beta = 5.22$ (plot 1 in Fig. 4) for method I, $\alpha = 3.73$, $\beta = 6.16$ (plot 2 in Fig. 4) for method II, and $\alpha = 0.234$, $\beta = 73.90$ (plot 3 in Fig. 4) for the method in Ref. [7].

The results show that the extracting methods presented in this Letter can be used to extract the information with very low error probability P_e, even though the external noise has a rather large amplitude, meaning that the method in Ref. [7] is not secure.

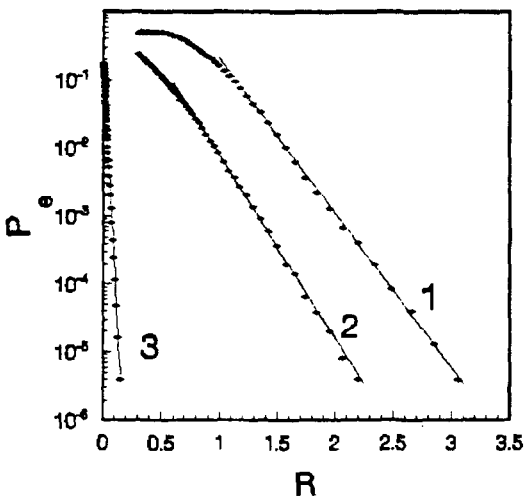

Fig. 4. The error probability P_e as a function of $R = \sum_n^{KN}[s(n) - \bar{s}]^2 / \sum_n^{KN}[e(n) - \bar{e}]^2$. (1) Method I, (2) method II, (3) method in Ref. [7].

5. Discussion

The security of communication approaches needs to be discussed generally. In a type of spread-spectrum signalling systems, the information is added to the chaotic carrier at very low power [1,8] for sufficient masking and for reducing the recovery errors resulting because the added message destroys the exact synchronization between the receiver and the transmitter [4]. Paradoxically, the fact of the message having low power makes it easier to reveal the hidden information by some forecasting approaches which predict the carrier dynamics based on a reconstruction of the geometric structure of the chaotic dynamics [8]. After examination of the security, Ref. [8] suggests that using multiple chaotic sources may provide added security. Another approach of extracting massages from a chaotic carrier does not reconstruct the full dynamics, but uses some suitable return maps [9]. This approach indicates that the security may be improved to transmit in the high frequency bands. However, the power spectra of the chaotic carrier (Lorentz system) in high frequency bands are quite low, and may not be sufficient to mask the message. Moreover, in this type of spread-spectrum signalling systems, external noise may make it both for the receiver and for any party intending to intercept the information difficult to recover the information accurately.

Some approaches for the transmission of digital signals have different recovery schemes; however, the main idea of encoding the signals is essentially the same, the two symbols corresponding to two chaotic attractors $\mathcal{A}$ and $\mathcal{B}$ of the system [1–3,5,7]. In Refs. [1–3], $\mathcal{A}$ and $\mathcal{B}$ are attractors of the same chaotic system with two different sets of parameters of the system (Chua's circuit). In Refs. [5,7], $\mathcal{B} = -\mathcal{A} = \{-x | x \in \mathcal{A}\}$. Since $\mathcal{A} \neq \mathcal{B}$, it is possible to construct some suitable return maps which can distinguish the differences between these two attractors, thus reading out the message, just as shown in Ref. [9] and this Letter.

Based on the above discussion, a possible way to improve the level of security of transmitting digital signals with the approaches of Refs. [1–3,5,7] is to employ very complex chaotic attractors of (very) high dimensional systems or hyperchaos [4,10,11], so that it may be much more difficult to reconstruct the full dynamics in an even higher dimensional embedded space, or to find some proper and distinguishable low dimensional return maps. However, high dimensional systems may cause new difficulties, for example, it may be difficult to achieve synchronization with one or very few driving signals; to initialize two high dimensional chaotic systems exactly, which is the prerequisite for the robust method in Ref. [7] to work, may be more difficult than to initialize two low dimensional chaotic systems; high dimensional systems may be much more difficult to implement than low dimensional systems.

Acknowledgement

The project is supported by the National Basic Research Project "Nonlinear Science" and the National Nature Science Foundation of China.

References

[1] K.M. Cuomo and A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[2] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, Int. J. Bifurcation Chaos 2 (1992) 973.
[3] H. Dedieu, M.P. Kennedy and M. Hasler, IEEE Trans. Circuits Syst. 40 (1993) 634.
[4] L. Kocarev and U. Parlitz, Phys. Rev. Lett. 74 (1995) 5028.
[5] C.S. Zhou and T.L. Chen, Phys. Lett. A 225 (1996) 60.

6] S. Hayes, C. Grebogi and E. Ott, Phys. Rev. Lett. 70 (1993) 3031.
7] U. Parlitz and S. Ergezinger, Phys. Lett. A 188 (1994) 146.
8] K.M. Short, Int. J. Bifurcation Chaos 4 (1994) 959.
9] G. Pérez and H.A. Cerdeira, Phys. Rev. Lett. 74 (1995) 1970.
[10] J.H. Peng, E.J. Ding, M. Ding and W. Yang, Phys. Rev. Lett. 76 (1996) 904.
[11] L. Kocarev, U. Parlitz and T. Stojanovski, Phys. Lett. 217 (1996) 280.