RECENT ADVANCES IN THE TRANSMISSION OF INFORMATION USING A CHAOTIC SIGNAL

Martin Hasler
Department of Electrical Engineering
Swiss Federal Institute of Technology
1015 Lausanne, Switzerland

Abstract

The current techniques of communications using a chaotic carrier signal are presented. The different ways to achieve synchronization of chaotic systems are listed and some of the complex phenomena that arise in this context are mentioned. The role of synchronization of chaotic systems in digital communications is reviewed shortly. The point is made that progress in communications with chaos depends on developing synchronization methods that are robust against channel noise.

1. Introduction

When it was realized that chaotic systems could synchronize [1-4], it became clear that chaotic signals could be used as carrier signals for the transmission of information. In the beginning, the main motivation was to hide the information in chaos. At this point, however, it is felt that from a cryptoghraphic point of view the current methods of chaos communications are not so strong. On the other hand, using chaos for communcations resembles closely spread spectrum communications, a techniques that has its roots in the military sector, but has become very popular in the civil sector in recent years. With the rapid development of mobile communications, chaos communciations will find its way to commercial applications, if its advantage can be proved under suitable conditions.

It is therefore important to compare the performance of chaos communication systems to conventional communication systems in order to find out what the real advantages are. At present, it seems that chaos communication systems require a less complicated circuitry as compared to conventional spread spectrum communication systems. However, their performance in presence of noise is not competitive yet, and a major research effort has to be made in this direction.

In this paper, we give our view of the state of the art of chaotic communications, of how it compares with conventional spread spectrum communications and of what the main problems are that research should address.

2. The principles of chaotic communications

A system of information transmission can be decomposed according to Fig.1. An information signal s(t) is injected into a chaotic dynamical system, which produces a chaotic output signal y(t). The transmission of y(t) through some medium, called the channel, degrades it, so that some modified, chaos-like signal z(t) enters the receiver. The receiver extracts by a

suitable procedure the information from z(t). This produces a signal $\hat{s}(t)$ which should be a copy of the original information signal s(t).

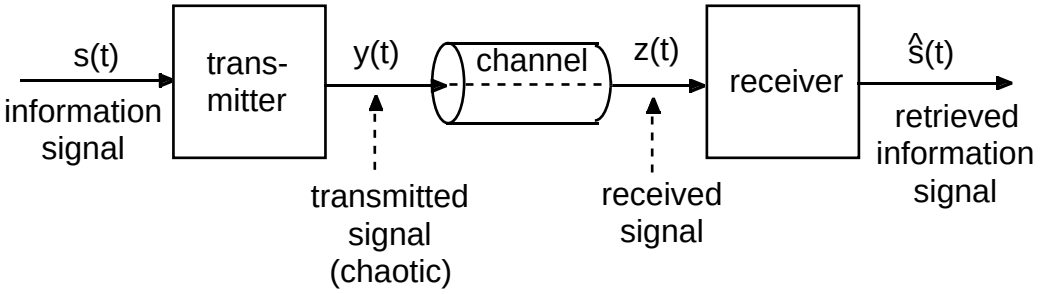

Fig.1. Transmission system

We distinguish *non coherent receivers and coherent receivers*. The non coherent receivers use the statistical properties of the incoming signal z(t) to extract the information. Only the chaos modulation method of the transmitter has to be known, but not its preceise parameters. Therefore, this method does not provide any intrinsic privacy for the transmitted message. On the other hand, much of the knowledge developed for conventional systems can be used and reasonable robustness against noise can be achieved.

The coherent receivers usually are dynamical systems that resemble the chaos producing transmitters. They achieve synchronization with the transmitter and thanks to synchronization are able to extract the information signal from the received chaotic signal. In order to achieve synchronization, the parameters of the transmitter have to be known. They can be considered as the encryption key of the message and thus, coherent receptions allows for some privacy of the information transmission. At present, however, synchronization of chaotic systems is very sensitive to channel noise. This is a crucial point that should be addressed by further research.

3. The notion of synchronization

We consider synchronization in the framework of Fig.2.

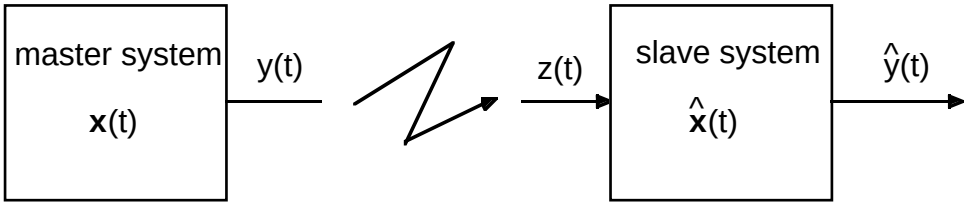

Fig.2. Master-slave system with perturbed interaction, for the study of synchronization

We suppose that the state at time 0, $\mathbf{x}(0)$, resp. $\hat{\mathbf{x}}(0)$, determines the time evolution $\mathbf{x}(t)$ resp $\hat{\mathbf{x}}(t)$, and of the output signal y(t), resp. $\hat{y}(t)$. If the channel disturbances are absent, i.e. z = y, and if the master and the slave systems have ideal parameter values, we use the following definition for synchronization that can be applied to arbitrary systems.

Definition 1.
The *slave system synchronizes with the master system* if

$$\left|\hat{y}(t) - y(t)\right| \xrightarrow[t \to +\infty]{} 0 \qquad (1)$$

for arbitrary initial conditions $\mathbf{x}(0)$ and $\hat{\mathbf{x}}(0)$.

If the channel disturbances are present and/or the two systems have inaccurate parameters, we cannot achieve (1) and a more realistic synchronization condition would be that for all or almost all pairs of initial conditions $\mathbf{x}(0)$ and $\hat{\mathbf{x}}(0)$ there exists a time T such that

$$\frac{\left|\hat{y}(t) - y(t)\right|}{\sqrt{< y(\cdot)^2 >}} < \eta \quad \text{for } t > T \qquad (2)$$

where η is a suitably chosen synchronization threshold, e.g. 0.2, and $< f >$ denotes the mean value of f along the trajectory. If the channel degrades the signal with noise of unbounded amplitude, such as gaussian noise, relation (2) cannot be required for every $t > T$, but with high probability for any $t > T$.

Let us leave the channel disturbances and the parameter mismatch temporarily aside. How does definition 1 compare with conventional synchronization definitions?

Usually the notion of synchronization is used for periodic signals. Suppose that the master system produces a periodic signal y(t). Conventionally, one says that the slave system synchronizes with the master system if its output signal $\hat{y}(t)$ asymptotically, as $t \to \infty$, has the same period as y(t) or, equivalently, if their phases are locked, i.e. if asymptotically their phases have a fixed difference. This notion of synchronization cannot be applied in an evident manner to systems with non-periodic behavior. Some recent publications use a notion of phase for nonperiodic signals and therefore are able to generalize accordingly the conventional notion of synchronization [5]. Compared to (1) this is a less stringent condition since only the phases have to be locked whereas in (1) the whole waveforms have to be identical, asymptotically. Indeed, in [5] an example of two coupled analog systems are given where phase synchronization takes place, but the amplitudes of the two systems remain uncorrelated. Perhaps this approach can lead to more robust chaos communication systems. At present, however, all proposed chaos communication systems with coherent receivers work on the basis of definition 1 for synchronization, and we will limit in the sequel our discussion to this notion.

3. Master-slave couplings

We suppose that the master and the slave system are similar nonlinear analog or discrete dynamical systems, described by state equations. We give here the form for analog systems. Discrete time systems are described similarly.

$$\begin{aligned} \frac{d\mathbf{x}}{dt} &= \mathbf{F}(\mathbf{x}) & \frac{d\hat{\mathbf{x}}}{dt} &= \hat{F}(\hat{\mathbf{x}}, z) \\ y &= g(\mathbf{x}) & \hat{y} &= \hat{g}(\hat{\mathbf{x}}, z) \end{aligned} \qquad (3)$$

where $\mathbf{F} : \Re^N \to \Re^N$, $\hat{\mathbf{F}} : \Re^{N+1} \to \Re^N$ and $g : \Re^N \to \Re$, $\hat{g} : \Re^{N+1} \to \Re$

We suppose that the master and the slave system can have identical solutions $\mathbf{x}(t) \equiv \hat{\mathbf{x}}(t)$ under ideal condition, i.e.when the channel disturbances are absent ($z(t) \equiv y(t)$), and when the master and the slave systems match perfectly. This amounts to requiring that for all $\mathbf{x}$

$$\hat{\mathbf{F}}(\mathbf{x}, g(\mathbf{x})) = \mathbf{F}(\mathbf{x}) \quad \text{and} \quad \hat{g}(\mathbf{x}, g(\mathbf{x})) = g(\mathbf{x}) \qquad (4)$$

Typical master-slave couplings are

a) Imposing a state:

$$\begin{aligned} g(\mathbf{x}) &= \hat{g}(\mathbf{x}, z) = x_1 \\ \hat{\mathbf{F}}(x_1, ..., x_N, z) &= \mathbf{F}(z, x_2, ..., x_N) \end{aligned} \qquad (5)$$

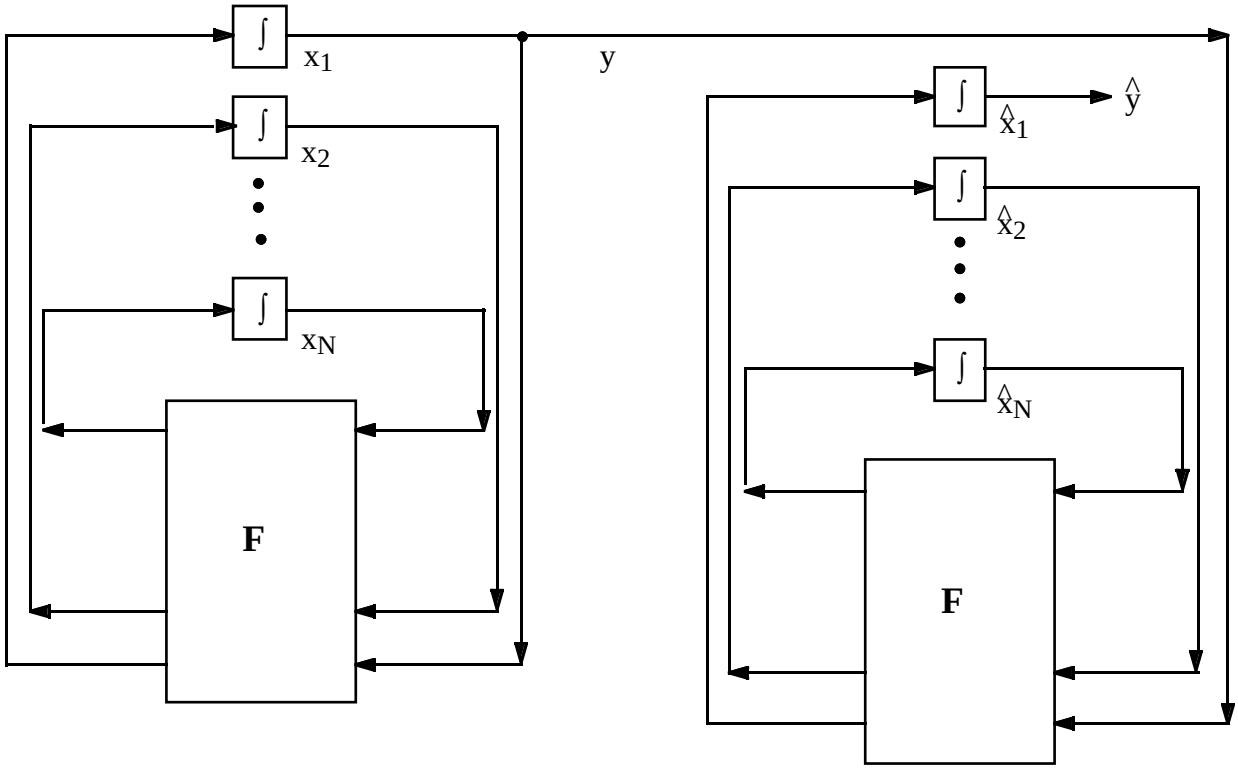

Fig.3. Master-slave coupling by transmission of a state.

Strictly speaking, in this case synchronization cannot be achieved, because changing the initial condition of $\hat{x}_1$ by an amount causes a constant change of $\hat{y}(t)$ by the same amount. However, for practical purposes this is not very important.

b) Drive-response coupling

This case has been introduced by Peccora and Carrol [4]. It is based on the decomposition of the system into two subsystems that interact through two signals.

$$\mathbf{F}(\mathbf{x}) = \begin{pmatrix} \mathbf{F}^{(1)}(x_1, ..., x_M, x_N) \\ \mathbf{F}^{(2)}(x_1, x_{M+1}, ..., x_N) \end{pmatrix}$$

$$g(\mathbf{x}) = \hat{g}(\mathbf{x}, z) = z \qquad (6)$$

$$\hat{\mathbf{F}}(\mathbf{x}, z) = \begin{pmatrix} \mathbf{F}^{(1)}(x_1, ..., x_M, x_N) \\ \mathbf{F}^{(2)}(z, x_{M+1}, ..., x_N) \end{pmatrix}$$

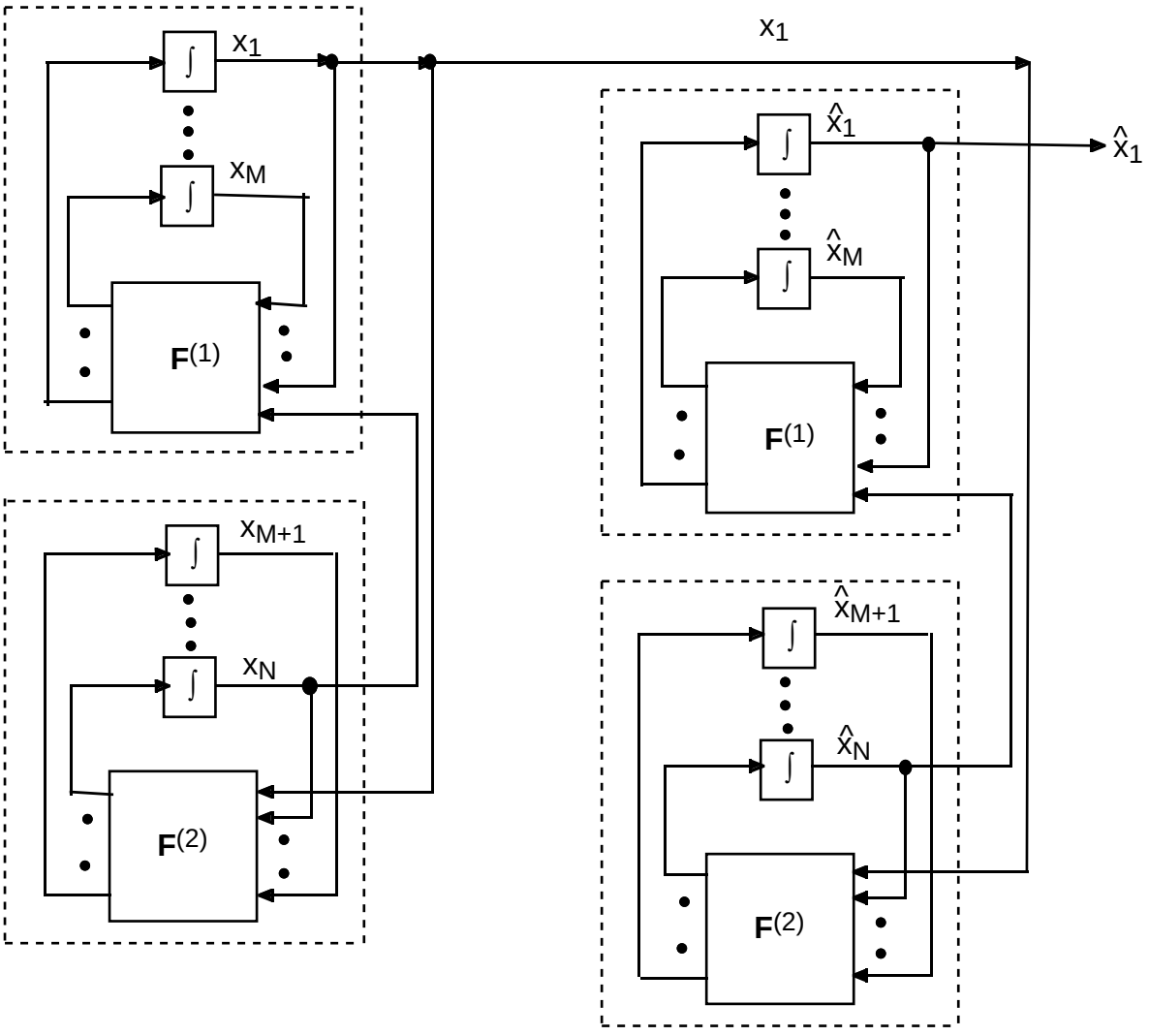

Fig.3. Drive-response coupling

c) Partially imposing a state

This is a generalization of both a) and b). As in a) x_1 is transmitted and imposed on the slave system, but only part of the occurrences of $\hat{x}_1$ in the state equations of the slave system are replaced by x_1. This is also done in b) where the occurrences of $\hat{x}_1$ in the lower subsystem of the slave system in Fig.3 are replaced by x_1, whereas in the upper subsystem $\hat{x}_1$ is not replaced. Here, we impose no restriction on which occurrences of $\hat{x}_1$ should be replaced by x_1, nor do we suppose that the system should be decomposable into two parts as in Fig.3.

d) Coupling by linear error feedback

This coupling is inspired by control theory.

$$\begin{aligned} g(\mathbf{x}) &= \hat{g}(\mathbf{x}, z) = x_1 \\ \hat{\mathbf{F}}(\mathbf{x}, z) &= \mathbf{F}(\mathbf{x}) + \mathbf{k}(z - x_1) \end{aligned} \tag{7}$$

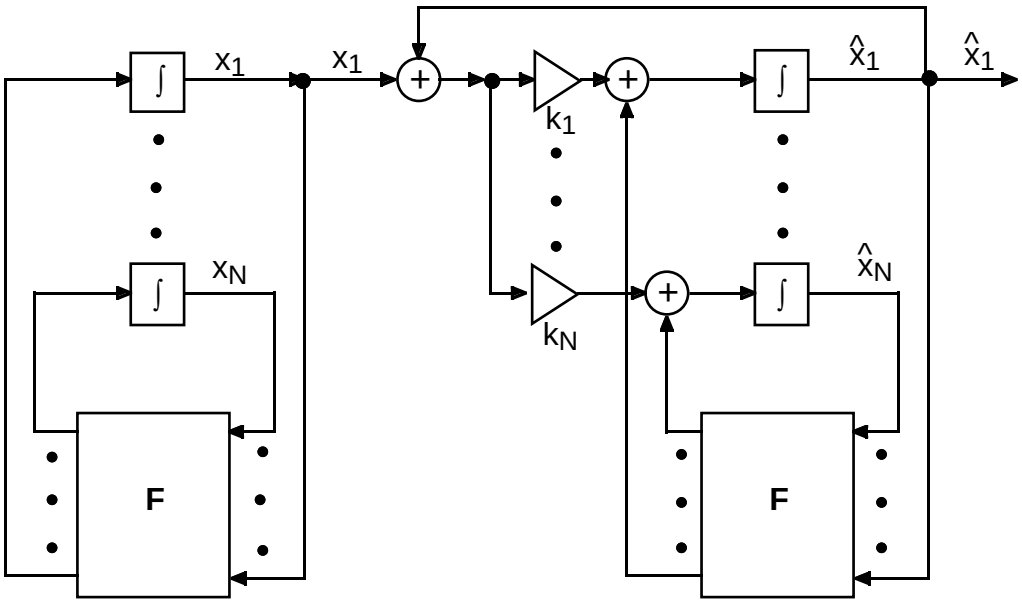

Fig.4. Coupling by linear error feedback

All these couplings satisfy condition (4) and therefore they are good candidates for synchronizing master-slave systems. However, condition (4) by no means implies synchronization.

4.Synchronizing master-slave systems

Depending on the example, synchronization is easy or difficult, if not impossible, to prove. A typical example where the proof is easy is the following coupling of two Lure's systems (Fig.5), which belongs to the category c) of section 3.

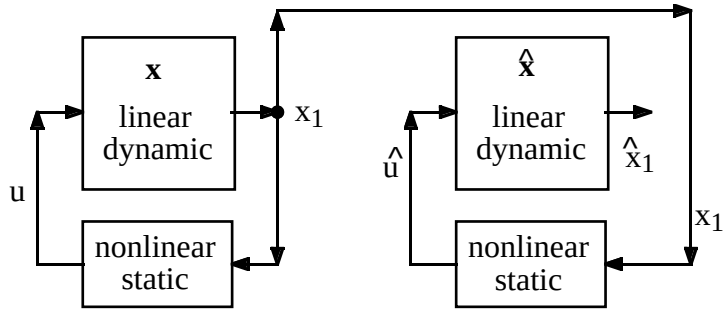

Fig.5 Coupled Lure's systems

They are described by

$$\frac{d\mathbf{x}}{dt} = \mathbf{A}\mathbf{x} + \mathbf{b}u \qquad \frac{d\hat{\mathbf{x}}}{dt} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{b}v$$
$$u = f(x_1) \qquad v = f(x_1) \tag{8}$$

Clearly, u = v and the state synchronization error $\mathbf{x} - \hat{\mathbf{x}}$ satisfies the linear equation

$$\frac{d(\mathbf{x} - \hat{\mathbf{x}})}{dt} = \mathbf{A}(\mathbf{x} - \hat{\mathbf{x}}) \tag{9}$$

Thus, if all eigenvalues of **A** have negative real parts, the slave system synchronizes with the master system. Note that if synchronization takes place, (1) not only holds for $y = x_1$, but for all states. This usually is the case.

A circuit realization of this coupling of Lure's systems is given in Fig.6, using Chua's circuit [6].

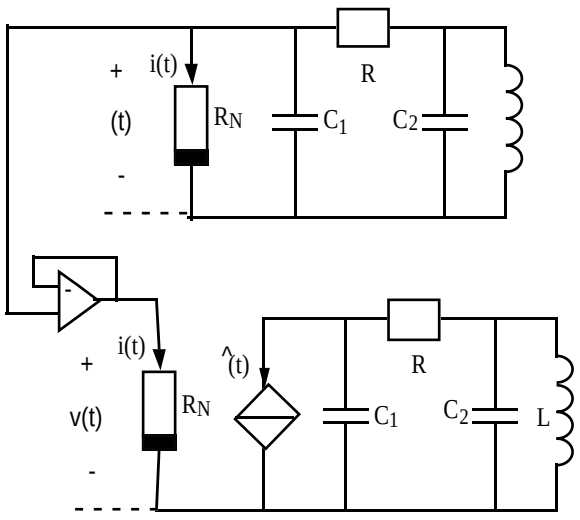

Fig.6. Two coupled Chua's circuits that always synchronize

In many other master-slave systems, no proof has been found for synchronization, even though numerical simulations appear to confirm synchronization. In some of them, it can be seen that the conditions of definition 1 do not hold. In [7] two uniform piecewise linear Markov maps are coupled by imposing a state. In this case, not for all initial conditions $\mathbf{x}(0)$ and $\hat{\mathbf{x}}(0)$ condition (1) for synchronization is satisfied, but only for **almost all**. From a practical point of view it may seem that this is of no importance, because exceptional initial conditions with no synchronization will never be realized. However, it happens that close to exceptional initial conditions synchronization will be slow, which is a drawback for practical applications.

Recently, it has been realized that synchronization of chaotic systems is a rather complex phenomenon and that strong and weak forms of synchronization exist. We give here some very quick introduction to these phenomena. For a more extensive introduction along the same lines we refer to [8] and for deeper analysis we refer to the pertinent mathematics and physics literature [9-15].

To illustrate the phenomena, we consider, as in [8], the iterations of two skew tent maps

$$f(x) = \begin{cases} \dfrac{x}{a} & \text{if} \quad x \le a \\ \dfrac{1-x}{1-a} & \text{if} \quad a < x \end{cases} \tag{10}$$

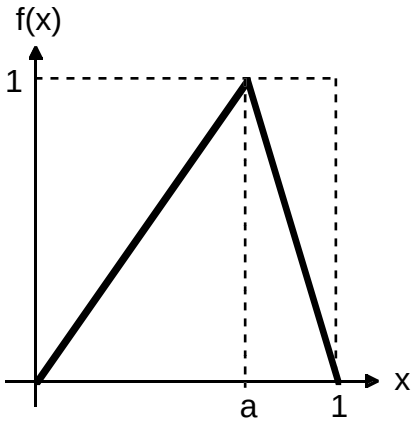

Fig.7. Skew tent map

with $0.5 < a < 1$ that are coupled either according to **version 1**

$$\begin{aligned} x(k+1) &= f\left[x(k)\right] \\ \hat{x}(k+1) &= f\left[\hat{x}(k)\right] + \varepsilon\left(x(k) - \hat{x}(k)\right) \end{aligned} \tag{11}$$

or according to **version 2**

$$\begin{aligned} x(k+1) &= f\left[x(k)\right] \\ \hat{x}(k+1) &= f\left[\hat{x}(k) + \varepsilon\left(x(k) - \hat{x}(k)\right)\right] \end{aligned} \tag{12}$$

In the terminology of section 3, $F(x) = f(x)$, $g(x) = x$, $\hat{F}(x,z) = f(x) + \varepsilon(z - x)$, $\hat{g}(x,z) = x$, and thus version 1 is linear feedback coupling, whereas version 2 is a nonlinear feedback not mentioned in section 3.

We consider (11) and (12) as the iteration of a map in the plane. Since (4) is satisfied, the diagonal $x = \hat{x}$ is invariant and thus synchronization is possible. Synchronization means that all solutions $\left(x(k), \hat{x}(k)\right)$ converge to the diagonal. However, many solutions tend to (-∞, -∞) whereas we are only interested in the convergence to the invariant part $S = \left\{(x,\hat{x}) \middle| 0 \le x = \hat{x} \le 1\right\}$. Actually, for version 2 coupling and $\varepsilon > 0$ the square $[0,1]^2$ is invariant, whereas in the other cases some region of the plane containing S is invariant. We suppose that we limit our initial ocnditions $\left(x(0), \hat{x}(0)\right)$ to this region and thus synchronization means convergence to S.

The most obvious way to prove synchronization is to find a Lyapunov function in the differences of the states of the master and the slave system. In our simple case, we have to find a Lyapunov function in $\Delta x = x - \hat{x}$, e.g. $W(\Delta x) = (\Delta x)^2$. For version 2 coupling we find

$$\begin{aligned} W(\Delta x(k+1)) &= \left(f(x(k)) - f\left(\hat{x}(k) + \varepsilon \Delta x(k)\right)\right)^2 \\ &\le \left(\max\left(\frac{1}{a}, \frac{1}{1-a}\right) \cdot \Delta x(k) \cdot (1-\varepsilon)\right)^2 \\ &= \left(\frac{1}{1-a}\right)^2 (1-\varepsilon)^2 W(\Delta x(k)) \end{aligned} \qquad (13)$$

Thus, for $|1-\varepsilon| < |1-a|$ or, equivalently, for $a < \varepsilon < 2-a$, W is indeed a Lyapunov function and synchronization according to definition 1 takes place.

If for version 2 coupling $a < \varepsilon < 2-a$ is not satisfied or for version 1 coupling irrespective of the values of a and ε, no Lyapunov function in Δx can be found. In this case, one can try to establish the local stability of the synchronization subspace S. Local stability properties of a solution is often investigated using Lyapunov exponents.

Definition 2:

The *Lyapunov exponents* of a trajectory **x**(k) obtained by iteration of a map **F**: $R^N \to R^N$ are defined to be the eigenvalues of the matrix

$$\Lambda = \lim_{k\to\infty} \frac{1}{2k} \ln\left[\mathbf{D}_k^T \mathbf{D}_k\right] \qquad (14)$$

whenever $\mathbf{D}_k$ is well-defined and the limit exists. Here $\mathbf{D}^T$ denotes the transpose of **D** and

$$\mathbf{D}_k = \frac{\partial \mathbf{F}}{\partial \mathbf{x}}(\mathbf{x}(k-1)) \frac{\partial \mathbf{F}}{\partial \mathbf{x}}(\mathbf{x}(k-2)) \ldots \frac{\partial \mathbf{F}}{\partial \mathbf{x}}(\mathbf{x}(0)) \qquad (15)$$

where $\frac{\partial \mathbf{F}}{\partial \mathbf{x}}(\mathbf{x}(j))$ is the Jacobian matrix of **F** at the point **x**(j).

In our case N = 2 and we are only considering the synchronized trajectories, i.e. the trajectories with $0 \leq x(k) = \hat{x}(k) \leq 1$. It can be seen [8] that for almost all such trajectories (14) exists and the Lyapunov exponents are

$$\lambda_{\|} = -a\ln(a) - (1-a)\ln(1-a) \tag{16}$$

and

$$\begin{aligned} \lambda_{\perp} &= a\ln\left|\frac{1}{a}-\varepsilon\right| + (1-a)\ln\left|\frac{1}{1-a}+\varepsilon\right| \quad \text{(version 1)} \\ \lambda_{\perp} &= -a\ln(a) - (1-a)\ln(1-a) + \ln|1-\varepsilon| \quad \text{(version 2)} \end{aligned} \tag{17}$$

The *parallel Lyapunov exponent* $\lambda_{\|}$ concerns the stability of the solution with respect to perturbations within S. It is always positive which means instability and expresses the chaotic nature of the dynamics confined to S. The *transversal Lyapunov exponent* $\lambda_{\perp}$ concerns the stability of the solution with respect to perturbations that lead away from S. For version 1 coupling there are two intervals on the ε-axis where $\lambda_{\perp}$ is negative and for version 2 coupling there is one such interval, which, of course, contains the interval where we have found a Lyapunov function, but which is larger than this interval.

One is tempted to conclude that whenever the transversal Lyapunov exponent is negative synchronization synchronization is achieved, i.e. $|x(k) - \hat{x}(k)| \to 0$ as k -> ∞. This conclusion is not correct. In our example, however, numerical simulations seem to confirm synchronization for negative transversal Lyapunov exponents, even though convergence to S is not monotone, but proceeds for most initial conditions through a series of desynchronization bursts of gradually diminishing amplitude.

From a practical point of view, however, more important than exact synchronization under ideal conditions is approximate synchronization (cf. inequality (2)) for noisy channels and master-slave pairs whose parameters a are not exactly equal. Here, the difference between **strong synchronization**, when definition 1 holds, and **weak synchronization**, when only for almost all synchronized trajectories the transversal Lyapunov exponents are negative, becomes apparent. Using the Lyapunov function introduced above, one can show [8] that for sufficiently small channel noise and sufficiently small parameter mismatch, approximate synchronization holds for strong synchronization, and it is even possible to relate η in (2) to the channel noise variance and to the parameter mismatch. In Fig. 8 the synchronization error Δx(k) is shown in the case when there is strong synchronization and when z(k) = y(k) + n(k), where the channel noise is gaussian with mean 0 and standard deviation 0.001. As could be expected from good synchronization behavior, the deviation of the solution from S, after some initial transient behavior, is of the same order of magnitude as the standard deviation of the noise.

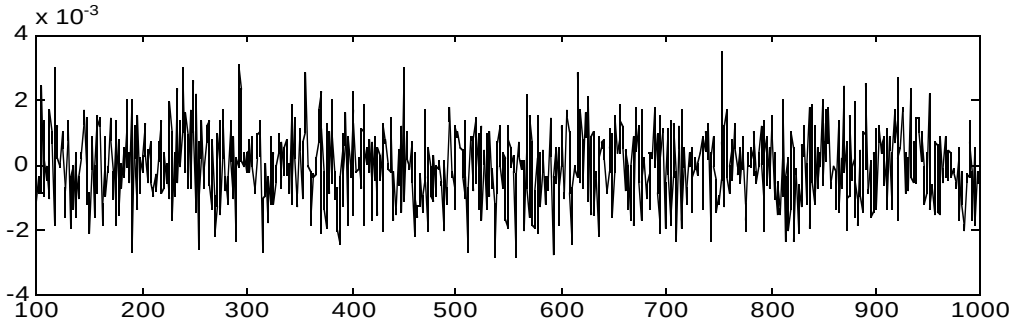

Fig.15. Synchronization error of a trajectory of two version 2 master-slave coupled tent maps with parameter a = 0.63 and coupling constant ε = 0.88 (transversal Lyapunov exponent -1.4613..) with additive gaussion noise of standard deviation 0.001.

However, when the same channel noise is applied to version 1 coupled systems with the same parameters a and a coupling coefficient such that the transversal Lyapunov exponent has almost the same negative value, the behavior of a typical solution (Fig.9) is quite different. In this case periods with small synchronization errors alternate with large desynchronization bursts. Such a behavior cannot be used for chaos communications.

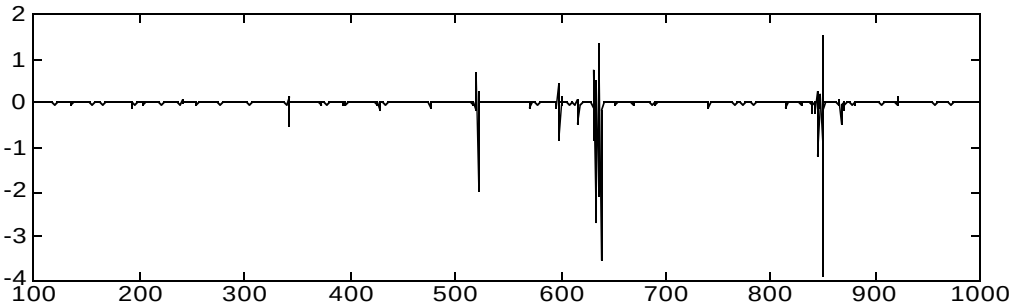

Fig.9. Synchronization error of a trajectory of two version 1 master-slave coupled tent maps with parameter a = 0.63 and coupling constant ε = 1.545 (transversal Lyapunov exponent -1.4575..) with additive gaussion noise of standard deviation 0.001.

5. Transmitting information on chaos using coherent reception

Many ways have been proposed in the literature to transmit information on a chaotic carrier signal. They can be classified into the following categories.

a) Chaotic masking

In this method [16,17] an analog information carrying signal s(t) is added to the output y(t) of the chaotic system in the transmitter. On the receiver side an identical chaotic system tries to synchronize with y(t). From this point of view, the information signal s(t) is a perturbation and

synchronization will take place only approximately. However, if the synchronization error is small with respect to s(t), the latter can be approximately retrieved by subtraction (Fig.10). The disadvantage of this method is that the information signal cannot be distinguished from channel noise.

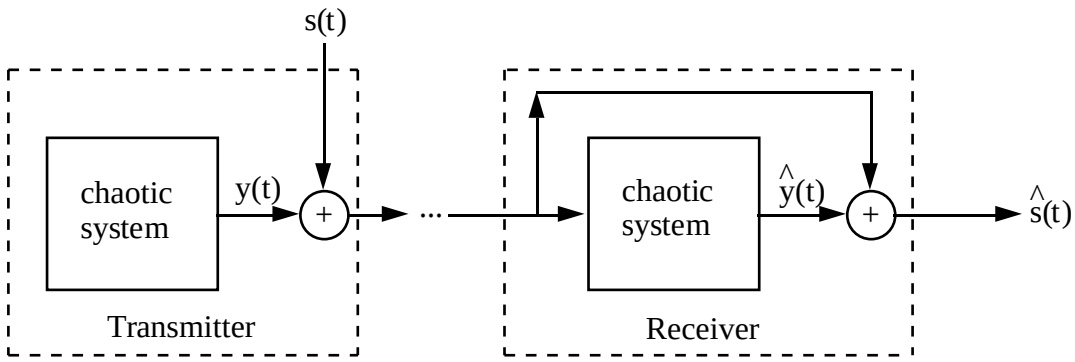

Fig.10. Transmission using chaotic masking

b) Chaotic switching or chaotic shift keying (CSK)

In this method [18,19,20] the information signal s(t) is supposed to be binary. It controls a switch whose action changes the parameter values of the chaotic system. Thus, according to the value of s(t) at any given instant t, the chaotic system has either the parameter vector **p** or the parameter vector **p'**. The output y(t) of the chaotic system is transmitted to two copies of the chaotic system, one with the parameter vector **p** and the other with the parameter vector **p'** (Fig.15).

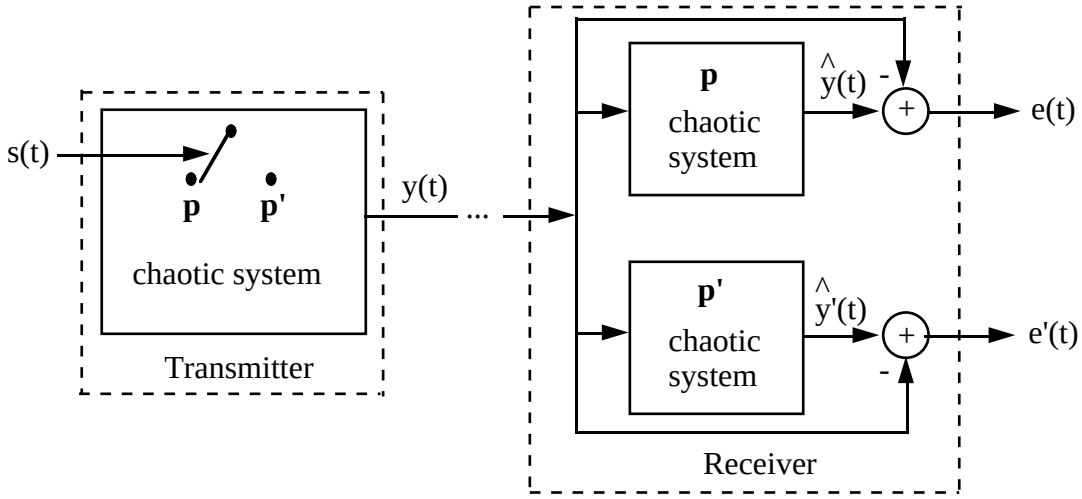

Fig. 15. Transmission using chaotic switching

If the momentary position of the switch in the transmitter is on position **p**, then the system with parameter vector **p** in the receiver will synchronize, whereas the system with parameter vector **p'** will desynchronize. Thus the error signal e(t) will converge to zero, whereas e'(t) will have an irregular wave form with a distinctly non zero amplitude. If the switch in the transmitter is on position **p'**, then we have the opposite situation, e'(t) will converge to zero and e(t) will be of non zero amplitude. Consequently, the signal s(t) can be retrieved from the error signals

e(t) and e'(t). Clearly, one has to leave the switch in the transmitter a certain time in the same position in order to be able to observe the convergence of the corresponding error signal to zero. Thus, this method is relatively slow.

c) Direct chaotic modulation using the inverse system

Consider the master-slave system of Fig.16 The slave system is an *inverse system* of the transmitter system in the sense that for suitable initial conditions, the signal $\hat{s}(t)$ retrieved from the receiver is identical to the signal s(t) injected into the transmitter [21]. If we start from a different initial condition, we hope that

$$|\hat{s}(t) - s(t)| \xrightarrow[t\to\infty]{} 0 \qquad (13)$$

If this is the case, we say that the *inverse system synchronizes* with the original system.

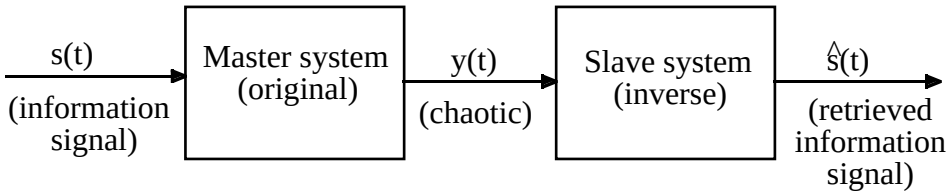

Fig.16. Original and inverse system

In principle, this is a very different structure as compared with Fig.2, but in practice again the master and slave systems have similar structure and usually the states of the two systems can be identified. When the inverse system synchronizes with the original system, then the corresponding states will also synchronize. A simple circuit realization of an original-inverse system pair is shown in Fig.17. The current i(t) plays the role of the input signal s(t) and the voltage v(t) the role of the transmitted signal y(t). The retrieved signal is the current $\hat{i}(t)$ through the voltage controlled voltage source.

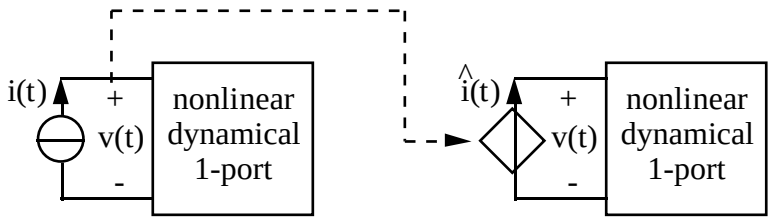

Fig. 17. Realization of the inverse system by circuits

Information is transmitted using the inverse sytem in a straightforward way [22-24]. The signal s(t) is the information carrying signal and y(t) is the transmitted signal. Thus, no additional circuitry has to be used, the chaotic system is the transmitter and the inverse system is the receiver. This methods allows to transmit information faster than using chaotic switching. In some realizations, it appears to be more sensitive to channel disturbances.

d) Predictive control

This method uses the ideas from symbolic analysis for the coding of binary information [25,26].Since it is less developed, we shall not explain it here.

6. Transmission of information on chaos using non coherent reception

The following method has been proposed in [27] under the name of **Differential chaos shift keying.** The information is transmitted in binary form. For each bit a piece of a chaotic waveform is transmitted and repeated once. If the bit is a "0", the repeated waveform is changed in sign, if the bit is a "1", it is simply repeated. Thus, apart from clock recovery, which is task for any digital receiver, the receiver simply has to compare the two successive waveforms and in the presence of noise decide whether they are the sme or whether they have opposite sign.

Actually, the chaos shift keying method introduced in section 5c) also can be designed to work with a non coherent receiver. In this case, the statistical properties of the solutions of the chaotic systems with different parameters are chosen to be very distinct so that the receiver can distinguish the bits on the basis of these properties alone. This is to some extent the opposite strategy compared with coherent reception. In the latter, the statistical properties of the solutions should be as close as possible when the parameter is changed in order to guarantee a certain privacy of the message.

7. The role of synchronization from the point of view of digital communiations

All methods of transmission on chaos admit the transmission of digital information. Even if the method is inherently analog, such as chaotic masking and direct chaotic modulation, digital information can be transmitted using some preliminary modulation scheme such as binary phase shift keying.

In digital communications a digital information signal has to be transmitted through an analog channel. To simplify, we limit ourselves here to binary information signals. To both values 0 and 1 of the m-th bit of the information signal, there corresponds a finite segment of an analog signal, $y^{(0)}(t)$ and $y^{(1)}(t)$, $mT \le t \le (m+1)T$, that is sent through the channel. At a given instant t, the transmitted signal y(t) is either $y^{(0)}(t)$ or $y^{(1)}(t)$, depending on whether a "0" or a "1" is being transmitted.

In the case of conventional phase shift keying, $y^{(0)}(t) = a.\cos\omega t$ and $y^{(1)}(t) = -a.\cos\omega t$. The length T of the segment is chosen to be a multiple of the period $2\pi/\omega$. Thus the transmitted segments corresponding to "0" as well aas those corresponding to "1" are always the same. When information is transmitted on chaos, $y^{(0)}(t)$ and $y^{(1)}(t)$ are chaotic waveforms and therefore, consecutive segments are different.

The segment that is sent, $y^{(0)}(t)$ or $y^{(1)}(t)$, $mT \le t$ $(m+1)T$ arrives at the receiver as the signal $z^{(0)}(t)$ or $z^{(1)}(t)$, $mT \le t \le (m+1)T$, corrupted with noise and distorted. In principal, it should be compared with the "clean" segments of $y^{0)}(t)$ and $y^{(1)}(t)$, $mT \le t \le (m+1)T$, and then it must be decided which of the two was sent by the transmitter. This last step is usually performed by correlation of y(t) with $y^{(0)}(t)$ and $y^{(1)}(t)$ for $mT \le t \le (m+1)T$ and by setting a decision threshold.

Therefore, it is necessary to produce in the receiver the "clean" segments of $y^{(0)}(t)$ and $y^{(1)}(t)$ and the correct timing to delimit the segments. While the timing, or *clock recovery*, is similar problem for conventional and chaos communications, the generation of $y^{(0)}(t)$ and $y^{(1)}(t)$ at the receiver appears to be more difficult for choatic signals. When sinusoidal signals are transmitted, a phase-locked loop can produce the correct sinusoid in the receiver.

In the differential phase shift keying method, $z(t)$ for $mT \le t \le (m+1/2)T$ is taken as the reference signal, even though it is not "clean" and it is compared with $z(t)$ for $(m+1/2) \le t \le mT$. The idea is that the distortion should be similar for the two half-segments and whereas the noise should be uncorrelated.

In the case of coherent receivers, it is the role of synchronization to produce "clean" segments $y^{(0)}(t)$ and $y^{(1)}(t)$, $mT \le t \le (m+1)T$ [. This is quite obvious in the case of chaotic masking and chaos shift keying. When chaotic masking is used, the receiver has to produce by synchronization a signal that is as close as possible to the chaotic signal generated by the transmitter, before the information signal is added. Then the information signal can be retrieved by subtraction. When chaos shift keying is used, the receiver subsystem that corresponds to the bit sent should reproduce by synchronization a signal as close as possible to $y(t)$ whereas the subsystem that corresponds to the wrong bit value should produce by desynchronization a signal that is as uncorrelated as possible with $y(t)$. When direct chaotic modulation with the inverse system is used, the role of synchronization cannot be related in such an obvious way to the recovery of $y(t)$. It is possible that the inverse system produces by synchronization $y(t)$ internally and then recovers the information signal. Thus, the two tasks to be performed in the receiver are intrinsically mixed.

Finally, let us point out one possible advantage of the use of chaos. When sinusoids are used, the segments of $y(t)$ that are sent over the channel for subsequent bits are highly correlated. This remains true even in conventional spread spectrum communications where the spreading sequences are repeated from transmitted bit to bit. Therefore, if the received signal $z(t)$ is composed of different delayed versions of $y(t)$, as is the case for mobile communications, and if the delays are comparable to the bit duration, the receiver will have problems to extract the correct information. In contrast to this, subsequent segments of chaotic waveforms have very low correlation and thus they potentially perform better in the presence of delays.

8. Conclusions

Research in communications on chaos has reached a state, where the communication theoretical aspects have to be addressed properly. The main problem today is the insufficient robustness against channel noise and other degradation of the transmitted signal. Non coherent receivers achieve, imitating traditional methods, performance that are comparable to conventional methods, whereas coherent receivers suffer from the insufficient robustness of chaos synchronization with respect to additive noise. We believe that here much better results could be obtained and this is one of the areas where research should be directed to. Non coherent receivers do not use any specific knowledge of the system that produces the chaotic signal, whereas coherent receivers use a modified copy of the transmitter to achieve synchronization. It should be possible to take advantage of the additional information to achieve better performance.

To make synchronization of chaotic systems more robust against noise will also help to develop efficient systems where more than one chaos communication is using the same channel, as is the case for conventional CDMA (Code Division Multiple Access) systems. Indeed, the other communications can be regarded as noise.

It is hoped that research in the indicated direction will enable to chaos communcations to find their way into applications where its intrinsic advantages, such as the performance in the presence of a superposition of delayed versions of the transmitted signal that is typical for mobile or indoor communications.

9. Acknowledgements

Thanks are due to Y.Maistrenko and A.Dmitriev for many enlightning discussions about synchronization and to M.P.Kennedy presenting the explanation, developed together with G.Kolumbán, of the role of synchronization from a digital communications point of view. This work has been supported by the Swiss National Science Foundation, grant nr. 2000-047172.96

References

[1] H.Fujisaka, T.Yamada, "Stability theory of synchronized motion in coupled oscillator systems", *Progr. Theor. Phys*., vol. 69, p.32, 1983

[2] A.S.Pikovsky, "On the interaction of strange attractors", *Z.Physik*, vol. B55, p.149, 1984

[3] V.Afraimovich, N.Veritchev, M.Rabinovich, "Stochastically synchronized oscillators in dissipative systems", *Radiophysics and Quantum Electronics*, vol.29, p.795, 1986 (in russian)

[4] L.M.Pecora, T.L.Carroll, "Synchronization in Chaotic Systems", *Phys. Rev. Lett.*, vol.64, pp.821-824, 1990.

[5] J.Kurths, A.Pikovsky, M.Rosenblum, "Phase synchronization of chaotic self-oscillatory systems", *ICND-96 Proceedings*, Saratov, Russia, 1996.

[6] R.N.Madan, Ed., *Chua's circuit, a paradigm for chaos*, World Scientific, Singapore, 1993.

[7] M.Hasler, M.Delgado-Restituto, A.Rodríguez-Vázquez, “Markov maps for communications with chaos”, *Proc. NDES’96*, pp.161-166, Sevilla, June 1996.

[8] M.Hasler, Y.Maistrenko, "An introduction to the synchronization of chaotic systems", to appear in IEEE Trans.Circ.Syst., part I, 1997.

[9] J.C.Alexander, J.A.Yorke, Z.You, "Riddled basins", *Int. J. of Bif. and Chaos*, vol. 2, pp.795-813, 1992.

[10] P.Ashwin, J.Buescu, I.Stewart, "Bubbling of attractors and synchronization of chaotic oscillators", *Phys. Lett. A*, vol. 193, pp.126-139, 1994.

[11] E.Ott, J.C.Sommerer, "Blowout bifurcations: the occurrence of riddled basins", *Phys. Lett.A*, vol. 188, pp.39-47, 1994.

[12] Y-C.Lai, C.Grebogi, J.A.Yorke, "Riddling bifurcation in chaotic dynamical systems", *Phys. Rev. Lett*, vol. 77, 1996, pp.55-58, 1996.

[13] P.Ashwin, J.Buescu, I.Stewart, "From attractor to chaotic saddle: a tale of transverse instability", *Nonlinearity*, vol.9, pp.703-737, 1996.

[14] Y.Maistrenko, T.Kapitaniak, "Different types of chaos synchronization in two coupled piecewise linear maps", *Phys. Rev.E.*, vol.54, pp.3285-3292, 1996.

[15] J.F.Haegy, T.L.Carroll, L.Peccora, "Experimental and numerical evidence for riddled basins in coupled chaotic systems", *Phys. Rev. Lett.*, vol. 73, pp.3528-3531, 1994.

[16] Oppenheim A.V., Wornell G.W., Isabelle S.H. and Cuomo K.M., "Signal Processing in the Context of Chaotic Signals", *Proc. IEEE ICCASP'92*, pp.IV-117 - IV-120, 1992.

[17] Kocarev Lj., Halle K. S. , Eckert K., Chua L. O. and Parlitz U. "Experimental Demonstration of Secure Communications via Chaotic Synchronization", *International Journal of Bifurcation and Chaos* , vol.2, pp. 709-713, 1992.

[18] H.Dedieu, M.P.Kennedy, M.Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits", *IEEE Trans. Circ. Syst., Part II* **40**, pp.634-642, 1993.

[19] Yu.L.Bel'skii, A.S.Dmitriev, "Information transmission using deterministic chaos" (in Russian). *Radiotechnika i Elektronika* **38**, Russian Academy of Sciences, pp.1310 - 1315, 1993.

[20] U.Parlitz, L.O:Chua, Lj.Kocarev, K.S.Halle, A.Shang, "Transmission of digital signals by chaotic synchronization", *International Journal of Bifurcation and Chaos* **2**, pp.973-977, 1993.

[21] U.Feldmann, M.Hasler, W.Schwarz, "Communication by chaotic signals: the inverse system approach", *International Journal on Circuit Theory and Applications*, vol.24, pp.551-579, Sept.-Oct. 1996.

[22] Boehme F., Feldmann U., Schwarz W., Bauer A., "Information transmission by chaotizing", *Proc. NDES'94, Crakow, Poland*, pp.163-168, 1994.

[23] Halle K.S, Wu Chai Wah, Itoh M. and Chua L. O. "Spread Spectrum Communication Through Modulation of Chaos", *Int. Journal of Bifurcation and Chao* **3**, pp.469-477,1993

[24] Hasler M., Dedieu H., Kennedy M.P., Schweizer J., "Secure Communication via Chua's Circuit", *Proc. NOLTA'93 workshops Hawaii*, pp.87-92, 1993.

[25] S.Hayes, C.Grebogi, E.Ott, "Communicating with chaos", *Phys. Rev. Lett.*, vol.70(20), pp.3031-3034, 1993.

[26] J.Schweizer, M.P.Kennedy, "Predictive Poincaré control: a control theory for chaotic systems", Phys.Rev.Letters, 1995.

[27] G.Kolumbán, B.Vizvári, W.Schwarz, A.Abel, "Differential chaos shift keying: a robust coding for chaotic communications", *Proc. NDES'96*, pp.87-92, Sevilla, Spain, 1996.

[28] G.Kolumbán, M.P.Kennedy, L.O.Chua, "The role of synchronization in digital communication using chaos", to appear in IEEE Trans.Circ.Syst.