A NOVEL CHANNEL CODING SCHEME BASED ON CONTINUOUS-TIME CHAOTIC DYNAMICS

Inés P. Mariño[1], *Luis López*[1], *Joaquín Míguez*[2], *Miguel A. F. Sanjuán*[1]

[1]Nonlinear Dynamics and Chaos Group, Universidad Rey Juan Carlos
Escuela Superior de Ciencias y Tecnología, c/ Tulipán s/n, 28933 Móstoles, Madrid (SPAIN)
e-mail: iperez@escet.urjc.es, llopez@escet.urjc.es, msanjuan@escet.urjc.es
[2]Departamento de Electrónica e Sistemas, Universidade da Coruña, Facultade de Informática
Campus de Elviña s/n, 15071 A Coruña (SPAIN), *e-mail:* jmiguez@udc.es

ABSTRACT

One of the most outstanding properties of chaotic dynamical systems is their extreme sensitivity to small perturbations. Far from being a disadvantage, this feature can be exploited to devise a simple technique that allows to control the symbolic dynamics of a chaotic system by applying small perturbations to the system trajectory. In this paper, we show how this procedure can be employed to differentially encode an arbitrary binary message within a continuous-time chaotic waveform generated by a chaotic system. This chaotic waveform is an information-bearing signal that naturally presents a high degree of redundancy. By exploiting this property, we introduce a novel chaotic channel code with error-correcting capabilities.

1. INTRODUCTION

Recent developments in communication with chaos have provided a great variety of potential practical applications, which include transmitter-receiver synchronization [1], signal masking and recovery [2], reconstruction of information signals [3, 4] and encoding/decoding algorithms that allow to embed an arbitrary digital message into the symbolic dynamics of a chaotic system [3, 4, 5, 6]. The latter contributions show that it is possible to guide the evolution of a chaotic signal by applying small perturbations on the system variables. This feature allows to generate controlled chaotic waveforms whose symbolic representation corresponds to a desired message. Thus, these techniques are specially appealing because they take advantage of the most outstanding property of chaotic systems, their extreme sensitivity to the initial conditions, which had been previously seen as an obstacle for practical applications.

In this manuscript, we elaborate on the control technique reported in Ref. [3] and make a first effort to investigate its potential application to the important task of channel coding [7], since little attention has been devoted to this topic from the point of view of chaotic dynamics [8, 9]. We focus our attention in exploiting the natural redundancy of a continuous-time chaotic signal that bears a desired message within its symbolic dynamics. As a result, a novel error-correcting code is proposed, whose performance is illustrated through computer simulations.

The remaining of the paper is organized as follows. In Section 2 we review the control technique of [3] and discuss some details relevant to the error-correcting code proposed in Section 3. Finally, Section 4 is devoted to the conclusions.

2. CONTROLLING THE SYMBOLIC DYNAMICS OF A CHAOTIC SYSTEM

As shown in [3, 5, 6], small perturbations applied to the system trajectory of a chaotic attractor can be used to make the output waveform carry a desired symbol sequence representing a message. The chaotic Lorenz system,

$$\begin{aligned} dx/dt &= -\sigma(x-y), \\ dy/dt &= Rx - y - xz, \\ dz/dt &= bz + xy, \end{aligned} \qquad (1)$$

provides a good framework for investigating the idea of controlling the chaotic dynamics in this way. Recall that, for the standard parameter values, $\sigma = 10$, $R = 28$, and $b = 8/3$, the state coordinate $(x(t), y(t), z(t))$ moves on a chaotic attractor in a three-dimensional state space forming two lobes. The standard parameters will be used all throughout the paper. In order to control the system, let us also consider the two Poincaré surfaces of section given by the half-planes $y = \pm\sqrt{b(R-1)}$ and $|x| \geq \sqrt{b(R-1)}$, each one defined on a different lobe (see Fig. 1). When the system crosses the surface with $y = -\sqrt{b(R-1)}$ in a previously fixed direction it is said to generate a symbol "A" and when the system crosses the surface with $y = +\sqrt{b(R-1)}$ it is said to generate a symbol "B". Thus, a direct relationship exists between the system time evolution and the symbol string resulting from the successive crossings, which is referred to as the *symbolic dynamics* of the system.

Since the system is deterministic, there is a one-to-one correspondence between the point where the three-dimensional state coordinate crosses one of these surfaces

This work has been supported by the Ministry of Science and Technology of Spain, under project BFM2000-0967

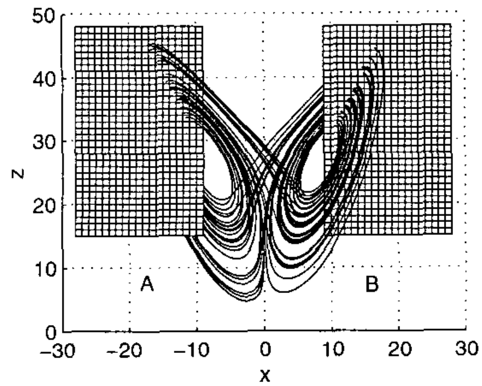

Fig. 1. Projection onto the x-z plane of the chaotic Lorenz attractor crossed by the Poincaré surfaces defined by $y = +\sqrt{b(R-1)}$ and $|x| \geq \sqrt{b(R-1)}$ and by $y = -\sqrt{b(R-1)}$ and $|x| \geq \sqrt{b(R-1)}$.

of section and the future n-symbol sequence, $s_1 \dots s_n$, generated after the crossing. The first symbol, s_1, indicates the present crossing and s_n represents the surface that is being crossed $n-1$ oscillations later. When the system runs free, the long-term temporal evolution of the state coordinate yields a random-like symbol string. This is easily observed in the scalar continuous-time signal $x(t)$ shown in Fig. 2, where the symbols "A" and "B" appear as a random-like sequence of positive and negative peaks.

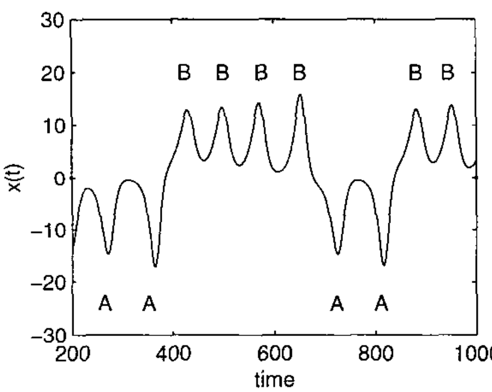

Fig. 2. Temporal evolution of variable $x(t)$ in the Lorenz system.

In [3], a control technique was first introduced that allows to determine the symbol string generated by the chaotic system after crossing a Poincaré surface of section. Control is exercised by applying small perturbations to one single system variable, $z(t)$. In order to correctly determine the perturbation signal a learning process is needed. Let us assume that we want to control the n-symbol string

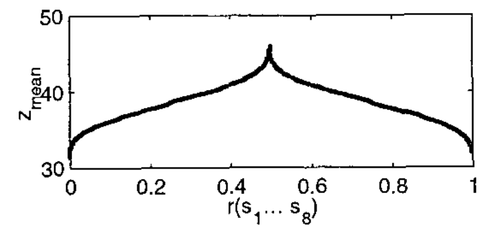

Fig. 3. Values of z_{mean} associated to each 8-symbol sequence, represented by $r(s_1 \dots s_8)$.

$s_1 \dots s_n$ generated after a crossing. The learning process is characterized by the value of n and works as follows: We let the system run freely for a long enough period of time and observe both the values that variable $z(t)$ takes at the crossings with the surfaces of section and the subsequent n-symbol strings generated by the system. In that way, we can associate a range of values of z, hereinafter referred to as a *bin*, to each one of the 2^n different possible n-symbol sequences. Once the bins are identified, an average of all z in the same bin, referred to as z_{mean}, can be calculated (notice that all z in the same bin have been observed to generate the same n-symbol sequence). The value of z_{mean} associated to each bin completely determines the future n-symbol sequence, represented by the real magnitude $r(s_1 \dots s_n) = \sum_{i=1}^{n} f(s_i) 2^{-i} < 1$, where $f(A) = 0$ and $f(B) = 1$. When this association is done for all bins, the learning process is complete. As an example, the dependence between z_{mean} and $r(s_1 \dots s_n)$ for $n = 8$ is plotted in Fig. 3.

The procedure to control the symbolic dynamics is examined next. Let us suppose that we want the chaotic waveform $x(t)$ to represent some binary message, as, for example, $m = 00111010110100 \dots$. We can associate the bit "0" with a change of symbol in two consecutive crossings with the Poincaré surfaces of section (i.e., AB or BA) and the bit "1" with the repetition of the same symbol (i.e., AA or BB). In this way, the same message can be represented either by the symbol sequence $ABAAAABBAAABBAB\dots$, begining with symbol "A", or by the complementary string $BABBBBAABBBAABA\dots$, begining with "B". This is useful in order to avoid problems related to the symmetry of function $z_{mean}(r)$ (see Fig. 3: every value of $z_{mean}(r)$ is associated with two complementary binary sequences) and is usually referred to as a differential bit encoding in the context of digital communications [7].

The aim of the symbol encoder is to introduce small perturbations in the variable $z(t)$ at each crossing with the surfaces of section in order to generate the desired n-symbol sequence. This desired sequence, $s_1 \dots s_n$, consists of $n-1$ symbols which are predetermined plus one new information symbol, i.e., s_1 is given by the current crossing and $s_2 \dots s_{n-1}$ must be the same symbols that would be generated by the system if we did not apply any perturbation at all. Therefore, the perturbation we apply in the k-th crossing sets the value of the $(k+n)$-th symbol generated by the system, the perturbation in the $(k+1)$-th crossing sets the $(k+n+1)$-th symbol and so on. From a practical point of view, each perturbation consists of moving the z coordinate to the central point in the bin corresponding to the desired n-bit sequence, i.e., the z_{mean} value of the bin.

3. CHANNEL CODING SCHEME

Once a desired message is encoded into the chaotic waveform $x(t)$ the most straightforward design of a communication system consists of transmitting this chaotic signal $x(t)$ through a communication channel. At the receiver, the message could be recovered just by observing the sequence of positive and negative peaks of the variable $x(t)$, possibly corrupted by thermal noise and other sources of distortion. This approach has already been described in the literature [3, 4], where signal reconstruction methods are proposed to account for the existence of impulsive noise in the channel by exploiting the properties of the encoding method and the chaotic signal. Here, we explore a different approach where the signal $x(t)$ is not transmitted itself. Instead, the transmission part of the communication system is implemented by conventional engineering methods, while the controlled Lorenz system is used to construct a novel *channel code* [7], i.e., a redundant representation of the message to be transmitted, that enables the receiver to partially detect and correct the transmission errors caused by channel noise and other sources of distortion.

Due to the control procedure that has been described to encode the desired message into the chaotic waveform $x(t)$, it is apparent that knowing the initial conditions for the Lorenz system, $x(0), y(0), z(0)$, with a sufficient degree of accuracy, all the relevant information of the signal $x(t)$ (and, therefore, the message) is contained in the value of the perturbations applied to the variable $z(t)$ at each crossing with a Poincaré surface. Hence, we propose the communication scheme where only the values of the succesive spots $z_{mean}(k), (k = 0, 1, ...)$, that indicate where the variable $z(t)$ must be placed by the control algorithm, are transmitted. Notice that index $k = 0, 1, ...$ represents the crossing or symbol number.

The communication system takes the following successive steps:

- The information bits (i.e., the message), $b_1 b_2 ... b_k ...$, are converted into a sequence of real values $z_{mean}(0) z_{mean}(1) ... z_{mean}(k) ...$ using the learned relationship between variable z and the symbolic dynamics of the system.

- A conventional analog-to-digital converter (A/D) transforms this sequence of real values into digital *words*, $w_1 w_2 ... w_k ...$. Each of these words is a signal in digital format that may be easily transmitted through the communication channel. This is a classical problem that can be solved in several different ways using well-tested engineering methods.

- A conventional digital receiver detects the digital words. Let us refer to the *detected* words as $\hat{w}_1 \hat{w}_2 ... \hat{w}_k ...$. The reason to use a different notation is that digital detection is subject to errors due to channel noise and distortion, hence, the detected word, $\hat{w}_k$, may be different from the transmitted one, w_k.

- A conventional digital-to-analog (D/A) converter transforms the detected words into a real sequence $\hat{z}_{mean}(0) \hat{z}_{mean}(1) ... \hat{z}_{mean}(k) ...$, where $\hat{z}_{mean}(k) = z_{mean}(k)$ if, and only if, $\hat{w}_k = w_k$.

- The real sequence $\hat{z}_{mean}(0) \hat{z}_{mean}(1) ... \hat{z}_{mean}(k) ...$ is used to reconstruct the temporal evolution of the variable $x(t)$ from a perturbed Lorenz system using the control algorithm described in Section 2. If no errors occurred during the transmission of the digital words, the recovered message, $\hat{b}_1 \hat{b}_2 ... \hat{b}_k ...$ will coincide with the original one, $b_1 b_2 ... b_k ...$. Notice that the recovered message is observed in the peaks of the variable $x(t)$ of the reconstructed perturbed system.

Overall, the proposed communication scheme can be seen as splitting the control algorithm into two parts: at the transmitter, we take the message and compute the perturbations (actually, the $z_{mean}(k)$ values) to be applied on the Lorenz system. This information regarding the perturbations is *passed* to the receiver conventionally, meaning that we use standard digital communication techniques. At the receiver, we apply the perturbations to the Lorenz system and observe the time evolution of the variable $x(t)$ in order to recover the message.

Since the perfect recovery of the message at the receiver using the scheme described above depends on wether there are errors or not in the conventional digital transmission step, the obvious question is: why is this scheme better than simply transmitting the information bits $b_1 b_2 ... b_k ...$ conventionally? The answer is that the proposed form of transmission turns out to provide protection against transmission errors because the $z_{mean}(k)$ values are highly redundant. Indeed, if the perturbations are small enough, the deterministic behavior of the system allows to predict, from the value of the variable $z(t)$ at any crossing with the Poincaré surfaces of section, which symbols will be generated in the $n-1$ subsequent crossings. This is the basis of the symbol encoding method. As explained in the previous section, the perturbation applied in the k-th crossing with a Poincaré surface modifies the symbol $s(k+n-1)$ produced by the system, but symbols $s(k) \ldots s(k+n-2)$ are the same as if the perturbation had not been applied.

What is the effect of this property on the receiver? Recall that $z_{mean}(k)$ is the central value of the bin associated with the n-symbol string generated after the k-th crossing with a surface of section. Therefore, even if there are some mismatch, i.e., if $\hat{z}_{mean}(k) \neq z_{mean}(k)$ due to transmission errors, $\hat{z}_{mean}(k)$ may still be within the bin associated with the same n-symbol string as $z_{mean}(k)$ and we will still recover the same information without error. But more importantly, even if $\hat{z}_{mean}(k)$ does not belong to the same bin as $z_{mean}(k)$, it is likely to belong to a neighbouring bin which, by construction, is associated to a symbol sequence that only differs in the last symbols. Hence, errors can still be avoided.

In order to clarify how the receiver can work we show the following example for 3-symbol control. At the transmitter, there is a local Lorenz oscillator with standard parameters that is controlled using the procedure in Section 2 to differentially encode a desired binary message. After the k-th crossing (with $k = 0, 1, 2, ...$), the resulting value of $z_{mean}(k)$ is converted into a binary word, w_k, which is digitally transmitted. Just to illustrate the method (a more sophisticated algorithm should be used in practice) we add a single parity bit to w_k (this yields w_k, p_k as the new word to be transmitted). This parity bit allows to easily detect transmission errors of exactly one bit. When no error is detected, the received word is converted back into a real form to yield the corresponding $z_{mean}(k)$ value, which is used to control the local Lorenz system. When an error is detected, no perturbation is applied at the k-th crossing of the oscillator and we let the redundancy of the system to account for this absence. Notice that the previous perturbation already fixed the next two symbols, so we are not actually losing information unless two perturbations in a row are absent. Clearly, this is a very simple way of implementing the proposed channel coding method, but it serves to the purpose of illustrating its error-correcting capability.

The performance of a system using the described channel code is shown in Fig. 4. We plot the coded Bit Error Rate (BER), which is the BER attained by the system when the proposed channel code with $n = 3$ is applied versus the uncoded BER of the digital channel, i.e., the BER of the binary transmission system when no channel code is used either to detect or to correct errors. In the plot, the diagonal line represents the performance of the uncoded system. After decoding, points over the diagonal indicate a performance loss, meaning that the BER has worsened, and values below the diagonal indicate a performance improvement, i.e., a reduction in BER after channel decoding. We observe that a gain of up to three orders of magnitude is achieved when the uncoded BER is 10^{-4}. We would like to remark that the coded BER is always equal to or better than the uncoded BER. This is not the case with many conventional channel coding techniques, that lead to a noticeable performance degradation when the uncoded BER is low [7].

4. CONCLUSIONS

We have introduced a novel channel code with error-correcting capabilities based on the dynamics of a continuous-time chaotic system. This channel code takes advantage of the natural redundancy contained in the perturbations applied to the system in order to encode a desired message in the symbolic dynamics of the chaotic waveform. The performance of this chaotic channel code has been illustrated through computer simulations for the case of the Lorenz system.

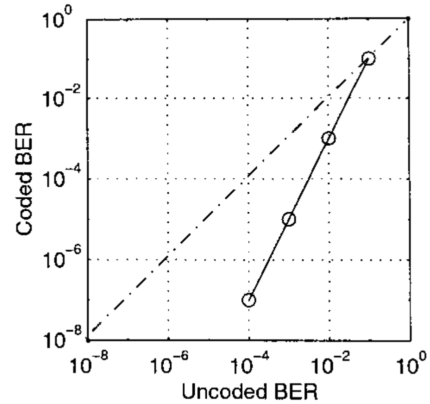

Fig. 4. Coded BER as a function of the uncoded BER when 3-symbol control is used.

5. REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[2] K. M. Short, "Signal extraction from chaotic communications," *Int. J. Bifurcation and Chaos*, vol. 7, pp. 1579–1597, 1997.

[3] I.P. Mariño, E. Rosa Jr., and C. Grebogi, "Exploiting the natural redundancy of chaotic signals in communication systems," *Phys. Rev. Lett.*, vol. 85, pp. 2629–2632, 2000.

[4] I.P. Mariño, C. Grebogi, and E. Rosa Jr., "Reconstruction of information-bearing chaotic signals in additive white gaussian noise: performance analysis and evaluation," *Int. J. Bifurcation and Chaos*, vol. 11, pp. 2631–2636, 2001.

[5] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, pp. 3030–3033, 1993.

[6] S. Hayes, C. Grebogi, E. Ott, and A. Mark, "Experimental control of chaos for communication," *Phys. Rev. Lett.*, vol. 73, pp. 1781–1784, 1994.

[7] J. G. Proakis, *Digital Communications*, McGraw-Hill, Singapore, 1995.

[8] M.S. Baptista, E.E. Macau, C. Grebogi, Y.-C. Lai, and E. Rosa Jr., "Integrated chaotic communication scheme," *Phys. Rev. E*, vol. 62, pp. 4835–4845, 2000.

[9] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," *IEEE Trans. Commun.*, vol. 46, pp. 881–890, 1998.