Secure transmission of information by digital chaotic signals

A. Gonzalez-Marcos*, J.A. Martín-Pereda[1]
E.T.S. Ingenieros de Telecomunicación. Universidad Politécnica de Madrid
Ciudad Universitaria. 28040 Madrid. Spain

ABSTRACT

Protecting signals is one of the main tasks in information transmission. A large number of different methods have been employed since many centuries ago. Most of them have been based on the use of certain signal added to the original one. When the composed signal is received, if the added signal is known, the initial information may be obtained. The main problem is the type of masking signal employed. One possibility is the use of chaotic signals, but they have a first strong limitation: the need to synchronize emitter and receiver. Optical communications systems, based on chaotic signals, have been proposed in a large number of papers. Moreover, because most of the communication systems are digital and conventional chaos generators are analogue, a conversion analogue-digital is needed. In this paper we will report a new system where the digital chaos is obtained from an optically programmable logic structure. This structure has been employed by the authors in optical computing and some previous results in chaotic signals have been reported. The main advantage of this new system is that an analogue-digital conversion is not needed. Previous works by the authors employed Self-Electrooptical Effect Devices but in this case more conventional structures, as semiconductor laser amplifiers, have been employed. The way to analyze the characteristics of digital chaotic signals will be reported as well as the method to synchronize the chaos generators located in the emitter and in the receiver.

Keywords: chaos synchronization, secure communications, digital chaos.

1. INTRODUCTION

It is known that chaos is one of the possible tools to obtain secure communications. It has been a long time since the first proposal to apply a certain type of chaos to communications was reported [1]. Since then, many different techniques and methods have been implemented in order to get systems with behaviour compatible with everyone of the current employed communication systems.

There are two main problems to be solved before any chaotic communication system gets the point to be a real system. The first one is related with the way to obtain chaotic signals and to control them. The second one has to do with the method employed in order to achieve that the chaotic signals generated by emitter and receiver have exactly the same properties. These characteristics have to be identical in any of the relevant aspects, in time and in analytical characteristics. This last problem is connected with chaos synchronization.

Several attempts have been made in this direction. The idea that chaotic systems could synchronize was first put forth in a paper almost ten years ago [1]. Several authors have followed the lines indicated in that paper. Pecora and Carroll demonstrated the possibility of synchronizing chaotic subsystems with a common driving signal. Their idea was to decompose the chaotic dynamical system in two subsystems, "driving" and response". The driving subsystem is composed by two state variable components whereas the second one just has one and uses as input signal one of the state components of the first subsystem [2-4]. Several authors have followed this idea and schemes using Chua's circuits are reported in the literature [5].

Several other methods have been proposed in the last years. Oppenheim and Kocarev [6-8] proposed a method with an analogic signal directly added to the chaotic signal. The receiver just subtracts to an internally generated chaos the received signal. This method is analogic and uses the chaotic signal from a Lorentz system as the basis for obtaining chaos. Other methods as Chaos Shift Keying (CSK) and a type of CDMA, as well as Time Division Chaotic Multiplexing (TDCM), Amplitude Division Chaotic Multiplexing (ADCM) and Frequency Division Chaotic

* Correspondence: Email agonmar@tfo.upm.es; E.T.S. Ingenieros de Telecomunicación. Universidad Politécnica de Madrid, Ciudad Universitaria. 28040 Madrid. Spain
[1] jamp@tfo.upm.es

Advanced Free-Space Optical Communications Techniques and Technologies,
edited by Monte Ross, Andrew M. Scott, Proceedings of SPIE Vol. 5614
(SPIE, Bellingham, WA, 2004) · 0277-786X/04/$15 · doi: 10.1117/12.578294

Multiplexing (FDCM) have been proposed too. A common characteristic of these systems is the use of analogic chaos. No digital chaos has been employed.

There are many advantages to use digital signals from the very beginning of the transmission systems. In some cases, chaos was first obtained with analogic methods and converted to digital after it was mixed with the signal to be transmitted. This method has the advantage of being easier to control and to take into account the huge quantity of work existing at the literature. But, to our opinion, should be much better to have a system able to generate digital chaotic signals from the very beginning. Moreover, there is another advantage that is even much more important. The bandwidth of the system needs to be much larger when one is dealing with analog chaotic signals due to the chaos characteristics. The system bandwidth has to be larger than when is transmitting the information signal alone. On the contrary, if the chaotic signal has the same characteristics than the original one, the bandwidth will be the same. Hence, the system characteristics could remain as before. This is, to our opinion, a very important property of the possible digital chaotic systems.

Among the many problems one has to handle only digital signals, the first one is the way how information and chaotic signals are put together in the transmission. The second one is, after transmission, how the information is recovered at the receiver. This situation needs to operate with a certain type of Boolean function, both at sender and receiver. The method to be reported in this paper follows the lines initiated by the authors previously [9-10].

2. DIGITAL CHAOS GENERATOR

The main block of our chaos generator is an Optically Programmable Logic Cell employed previously by us as a part of a possible optical computer. Although this structure has been reported in several places, some of its principal characteristics will be here presented again. Its main characteristic is the logic processing of two input binary signals, governed by two control signals. Two outputs give logical functions of these inputs. The type of processing is related to the eight main Boolean Functions, namely, AND, OR, XOR, NAND, NOR, XNOR, ON and OFF. The programmable ability of the two outputs, as it has been described, allows the generation of several data coding for optical transmission. Moreover, as it was shown, this circuit has the possibility to the generation of periodic and even chaotic solutions. A precise analysis of the output characteristic versus the main variable parameters, as control signal level and data signal level, has been reported [11].

With this configuration, the above mentioned digital character of the signal is directly obtained. Its main blocks are shown in Fig. 1. Two devices with a non-linear behaviour, P and Q, compose the circuit. The outputs of each one of them

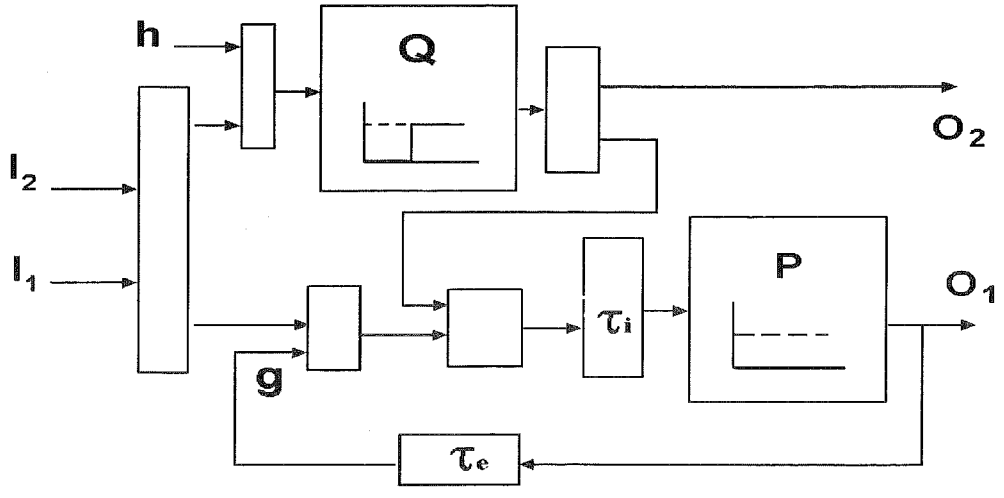


Figure 1.- Optical Programmable Logic Cell. Characteristics of the non-linear devices are shown at the insets. Feedback is allowed when the cell is intended to give a chaotic output.

correspond to the two final outputs, O_1 and O_2, of the cell. Four are the possible inputs to the circuit. Two of them are for input data, $\mathbf{I}_1$ e $\mathbf{I}_2$, and the other two, g and h, for control signals. The way these four inputs are arranged inside the circuit is also represented in Figure 1. A practical implementation we have carried out of the processing element has been based on an optoelectronical configuration. Lines in Fig. 1 represent optical multimode fibers. The indicated blocks, placed in order to combine the corresponding signals, are conventional optical couplers. In this way, optical inputs arriving to the individual devices are multilevel signals. The characteristics of the non-linear devices are also shown in Fig. 1. Device Q, corresponds to a thresholding or switching device, and device P is a multistate device, being the response of this non-linear optical device the one represented in Fig. 1. This response is similar to the behaviour of a SEED device.

2.1. Chaos generation from an OPLC

A non-linear behaviour is expected if some kind of feedback is applied to this cell. The feedback we have applied to the system, among the different possibilities, is the one going from the output O_1 of Q-device (see Fig. 1) to the control input, g, of P-device. No other additional control signal has been used. A chaotic output is obtained when the internal response time is made equal to zero or is much smaller than the external one. Some results have been reported by us [9-11].

In order to characterize the obtained chaotic signal, conventional methods are difficult to be applied here. The above results constitute a Time Series from where a chaos measure should be obtained. But the correct phase-space representation is not possible to be grasped from these results in a straightforward way. We do not even know what the adequate phase-space variables are and it is not even known how many variables are needed to fully describe the dynamics of this particular system. There is fortunately a partial answer to this problem that has been applied successfully in a large number of experimental investigations. The basic idea is that if the fundamental phase-space variables are **x** and **x'**, to study the evolution of the system numerically, x and x' have to be follow as functions of t. But since $x' = [x(t+\Delta t)-x(t)]/\Delta t$ in the limit as $\Delta t \to 0$, a knowledge of $x(t+\Delta t)$ is equivalent to a knowledge of x'. In other words, a knowledge of a trajectory of points $[x(t),x(t+\Delta t)]$ is equivalent to a knowledge of the trajectory of points $[x(t),x'(t)]$. As a consequence, a phase-space trajectory

$$x(t) = [x_1(t), x_2(t), ..., x_n(t)]$$

is replaced by a trajectory in an artificial phase space with points given by

$$y(t) = [y(t), y(t+\Delta), ..., y(t+m\Delta t)]$$

where y(t) is any one of the phase-space variables $x_i(t)$. Thus from a set of measurements of a single quantity y(t) we can construct a sequence of points in an artificial phase space

$$x(t) = [y(t), y(t+\Delta t), ..., y(t+m\Delta t]$$
$$x(t+\Delta t) = [y(t+\Delta t), ..., y(t+(m+1)\Delta t]$$

With the data we have, the first problem to solve is how to operate with our digital signal where just two values, "0" and "1", are present. If we adopt just this output as possible values for y, the resulting plot at the phase space should be concentrated on just four points, namely, (0,0), (0,1), (1,0) and (1,1). Almost no information could be obtained from it. Hence a new technique has to be implemented.

The method we have adopted is to group sets of four consecutive bits and to convert them to their corresponding hexadecimal values. Hence, a sequence of zeroes and ones is converted to a new string of hexadecimal values, namely, 0, 1, 2, ..., 15. For example, "0010" would be a "2", "1001" a "9" and "1110" a "14". Four divides the total number of data, but much more information can be obtained from them than with simple binary signals. A diagram, similar to the t_{i+1} versus t_i in analogue signals, can be drawn in this way. In the case of periodic signals, a closed configuration is obtained. But in the case of chaotic signals, no definite pattern would be obtained.

A further point needs to be considered. It is the one concerning the justification that the preceding quantity, namely the hexadecimal sequence, represents the same behaviour of the system than the previously obtained binary one. But this situation is equivalent to the reverse one: to convert a chaotic analog signal into a digital one. As it is well known from digital communications, any analog signal can be quantized and from this quantization to obtain a digital signal with the same main properties than the initial analog one. In our present case, we have accomplished the opposite operation, namely, to convert a digital signal into an analog quantized one with sixteen possible levels. And, according to digital communication signal processing theory, both representations are equivalent.

3. SYNCHRONIZATION OF CHAOTIC OPLCS

If two identical cells with feedback, as the above mentioned, are parallel connected (Fig. 2) and the same signal arrives to their inputs, an identical chaos is obtained at their outputs. This situation corresponds to two identical and ideal configurations working under identical conditions.

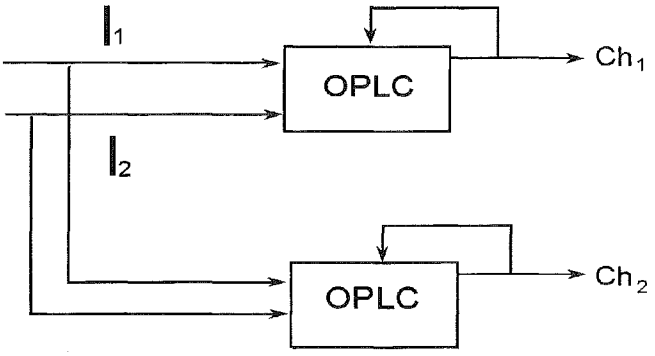


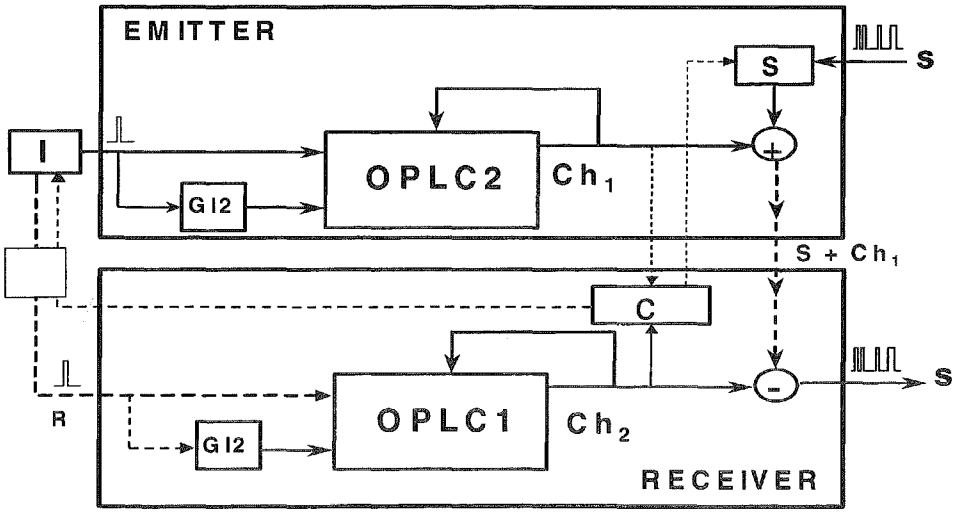
Figure 2.- Main blocks of the system when chaos synchronization is intended between emitter and receiver.

The behaviour becomes critical when the simulation tries to be close to a real situation. In this case, if both systems are not feed by exactly the same signal, the obtained outputs, although chaotic, are different. Hence, no possible relation between then should be feasible.

In a general situation, both systems, emitter and receiver, are located at different places. As a consequence, there is no possibility to introduce exactly the same input signals to their corresponding input ports. This is because although a common signal generator could send the same train of pulses to both cells, the arriving times to them can be different. The time need to get the first cell is known if this generator is at the receiver place. But the time when the signal arrives to the second cell may not be known. This is the most general case. Several solutions could be implemented to overcome this fact. The solution we have adopted is presented in Fig. 3.

The same driving signal is sent to both cells. A delay time, τ, is added before this signal gets into the emitter cell. This time has to be equal to the fly time from emitter to receiver. But this time is not known. Hence has to be changed until both times are the same. The way to change is imposed by the signal given by comparator C. There, the chaos signal coming from OPLC2 is compared with the chaotic signal obtained from OPLC1 and depending on the difference between these two signals, the order is given. As before, a delay time τ is added to the output from the OPLC1.

Figure 3.- Basic configuration of the reported system. OPLCs are the Optical Programmable Logic Cells of Fig. 1. τ is a time delay. It is the common signal to synchronize chaos. C is the control system. GI2 corresponds to some code added to the system to improve the security.



Two methods have been implemented in order to know the time delay magnitude to be added at the receiver. The first one is shown in Fig. 4. Chaos signal from OPLC1 is represented at the x-axis and the one from OPLC2 at the y-axis. A hexadecimal representation, as before, was taken. The represented case corresponds with the case when there is not synchronization between emitter and receiver. As it is obvious, when synchronization is obtained, an straight line is the result.

The second method is just to represent the difference "Chaos from OPLC1 – Chaos from OPLC2)" versus time. In this case, a particular example is given in Fig. 5. It corresponds to a situation where neither there is nor synchronisation at the beginning and after certain changes in delay times, synchronization is obtained.

The blocks diagrams corresponding to our computer simulation appears in Fig. 6.

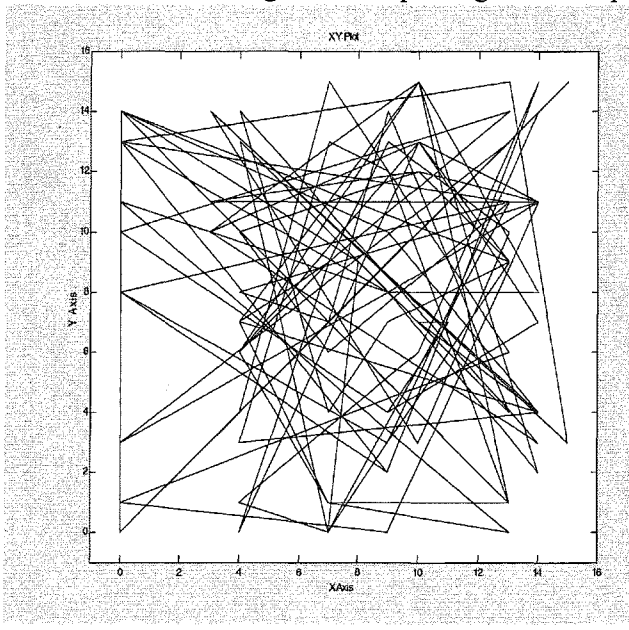


Figure 4.- Comparison of signals from channel 1 (x-axis) and channel 2 (y-axis) in Fig. 3 when no synchronization is present.

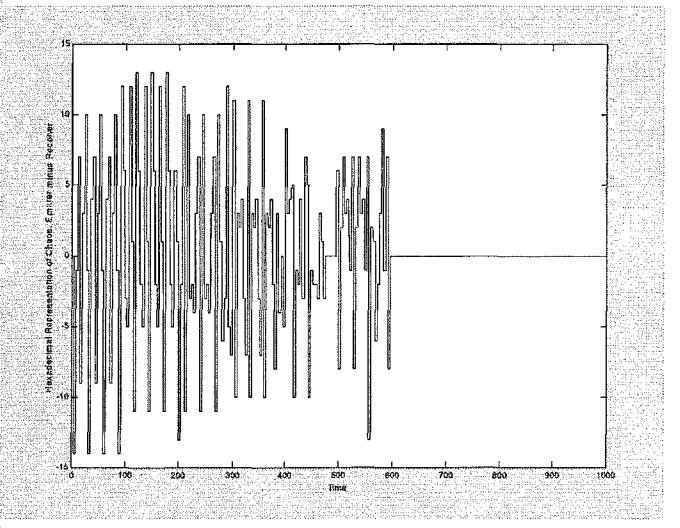


Figure 5.- Comparison of chaotic signals from channel 1and channel 2. (y-axis corresponds to (Channel 1 minus Channel 2)) in Fig. 3, versus time. No synchronization is present at the beginning. Time adjusting of time delay moves the system to synchronization.

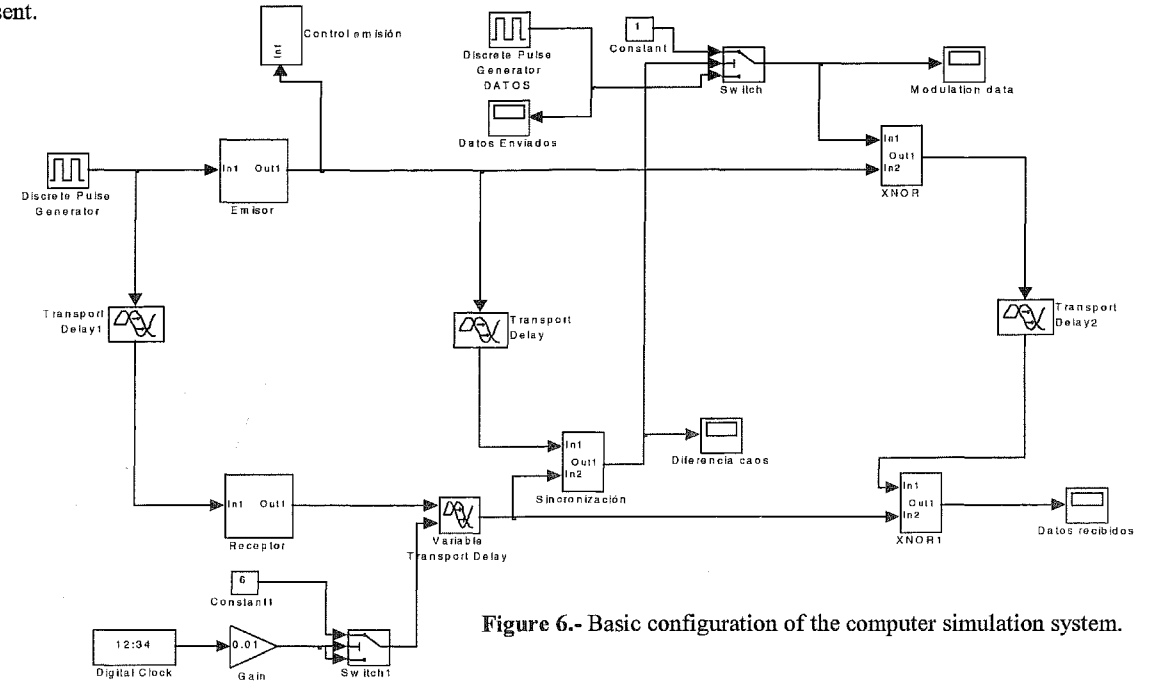


Figure 6.- Basic configuration of the computer simulation system.

4. DIGITAL MODULATION AND DEMODULATION OF CHAOTIC DIGITAL PORTRAIT

The main objective of this paper is to show the possibilities to send and receive digital information from this system. As it was pointed out before, the main problem concerns the way information data are added to the chaotic signal and how the result is sent to the receiver. A direct sum of the signals, as it is usual when one is dealing with analogic signals is not possible now. This is because our data are binary signals, namely "0"s and "1"s and signals with different levels are not allow.

The solution we have adopted is to perform a XNOR function at the emitter, from the chaos and information data. The result is the transmitted signal. At the receiver, this signal is again added, with another XNOR function, with the chaos generated there. The result is the original information signal imposed at the emitter. Results corresponding to a simple case, where the information signal is just an string of alternate "0"s and "1", appears at Fig. 7. As it can be seen, the recovered signals correspond with the original one.

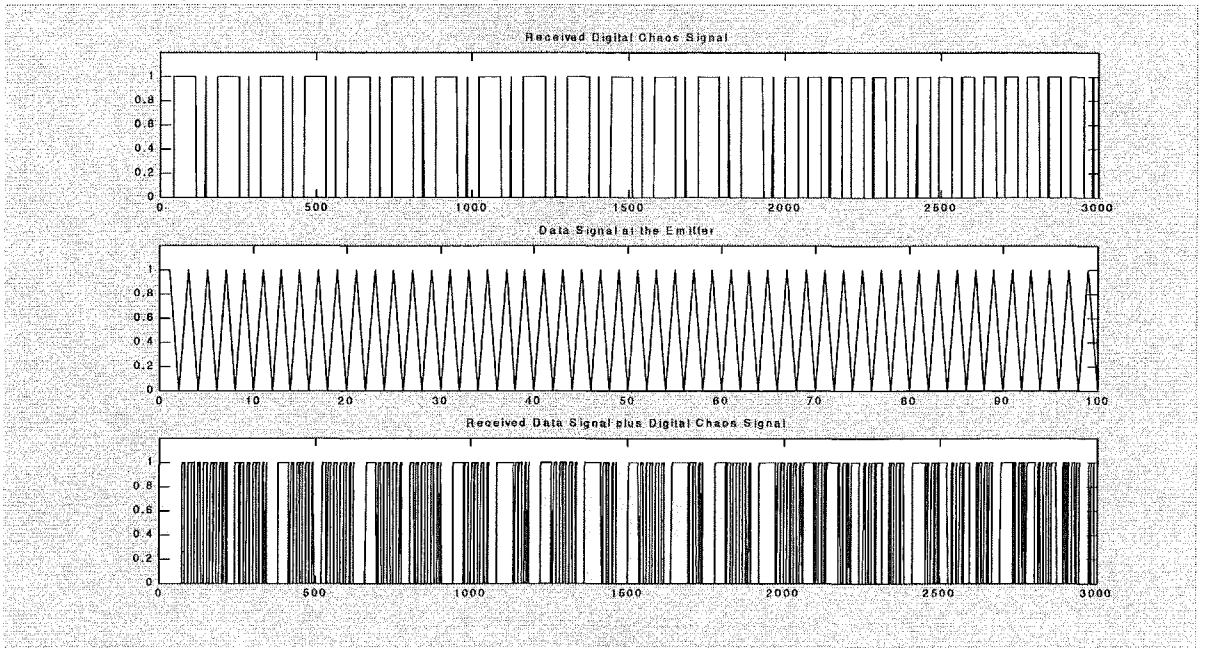


Figure 7.- Signals at the receiver. (a) chaotic signal, (b) data and (c) information signal plus chaos. Time scales are different at each figure.

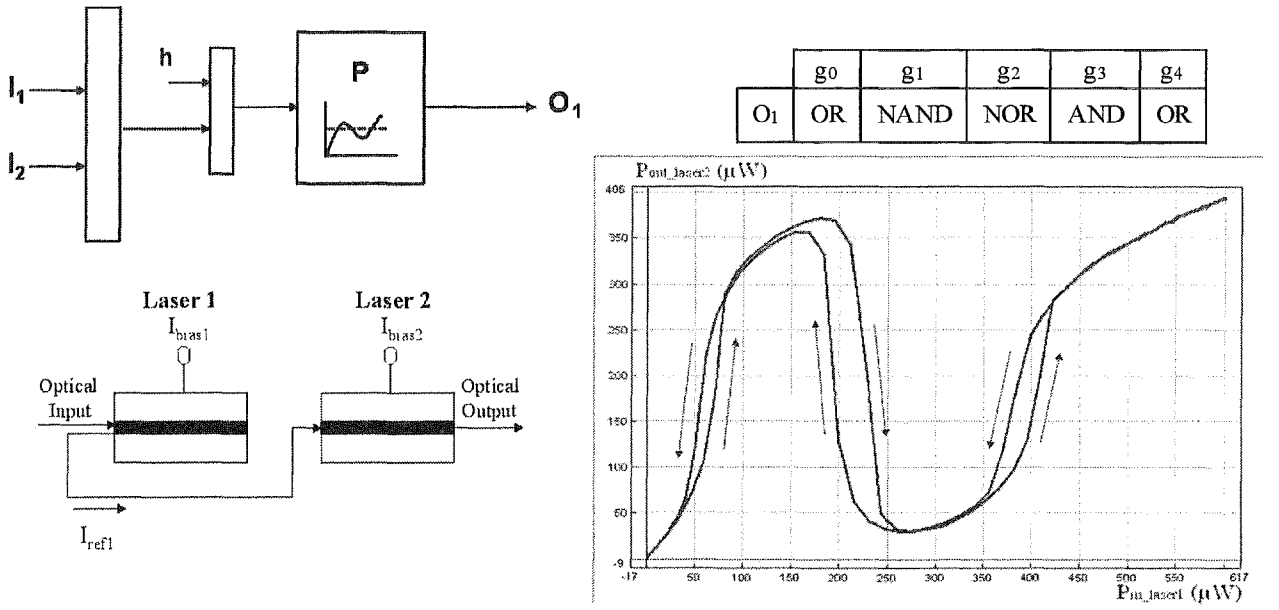
Although the reported case is a very straightforward one, it allows us to prove the possibility to send and receive information signals encoded with chaotic signals. Moreover allows its implementation by different methods in order to analyze results from different points of view.

5. IMPLEMENTATION OF SECURE TRANSMISSION SYSTEM

In previous section we have described how a digital chaos generator has bee studied and analyzed. Also it has been report the technique used to apply a digital chaos signal as a mask to encrypt data in a transmission system to ensure the security on it. Aspects of digital transmission are not covered.

5.1. OPLC with laser diodes

As it has been shown, similar results to the obtained with SEEDs are possible to achieve with Laser Diodes arranged in a particular configuration. The structure we have adopted appears in Fig. 8. As it is shown, the light going into the second laser is the one reflected from the first one. Both lasers are working with intensities under their threshold current.



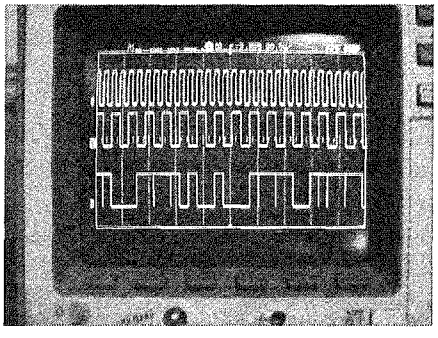
	g0	g1	g2	g3	g4
O1	OR	NAND	NOR	AND	OR

Figure 8.- Block Diagram of P-Device. Logic Table of OLG (Optical Logic Cell). Laser diode configuration and optical output power Pout characteristic in function of optical input power Pin for such LD configuration.

The relation between optical frequencies of light impinging onto the first laser and proper resonance frequency of the two lasers, as well as intensities of light and current, allow a wide range of working conditions being one of them the represented in Fig. 8. It is possible to see there that the response of the whole structure is similar to the SEED response and as a consequence, it is possible to employ it as main element for the previous structure. A simpler structure corresponds to the "on-off" device. Some more details are given in [12-13]. This possibility allows working with device with a very important property: they are possible to obtain them from any industry. SEEDs, on the contrary, are more specialized devices and they are more difficult to obtain.

5.2. OPLC with FPGA (Field Programmable Gate Array)

The OPLC-Optical Programmable Logic Cell was first made with an optoelectronic approximation of the internal devices. In this way, at the time this was designed, it was taken in advanced the optics aspect of an easier way of adding signals and the signal process was made electronically. The multilevel optical signal is detected and process with an analogue circuit; the output is then converted to an optical signal again that can be used to feedback. Smart pixels tech nology can be a good approach for it. This is an easier approach. But in order to take advantage of a more standard electronic design we are working on the implementation of what it is call the EPLC – Electrical Programmable Logic Cell – it is based on the design on the logic tables that offer the OPLC. The most complicated aspect it is how to emulate the control signals. This has to be able to have at least five different values, which means it needs at least 3 bits to



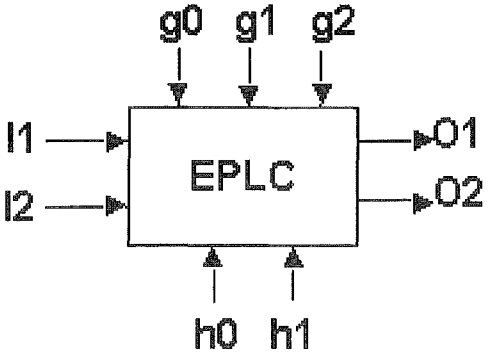


Figure 9.- EPLC (Electrical Programmable Logic Cell) Block Diagram. Compared with the OPLC, inputs (I1, I2) and outputs (O1,O2) are the same. Control signal needs more than one input (g0, g1, g2, h0, h1). Oscilloscope screen show two periodic input signals and the corresponding output in O1, apparently it is random or chaotic and an spread spectrum it its present.

codify in binary the five levels. In Fig. 9 it is show the block diagram of the EPLC. The digital design has been done with a FPGA-Field Programmable Gate Array. The main objective, on this design, it is to find an easy way to work with several PLC-Programmable logic cells. This type of logic cell allows an external and dynamically configuration of the function execute, being modified at the time desired. In this way with feedback apply to the control signal it is expected to obtain the digital chaos generator from periodic data, see fig.9.

5.3. Computer simulation by C language.

In order to prove the robustness of the system, a computer simulation in C has been obtained too. Two has been the objectives of this simulation. The first one is to operate with a language where all the details are known to the programmer and no internal and unknown routines, introduced by the owner of the commercial programmes, are present. The second one is the possibility to operate with higher capacity computer systems.

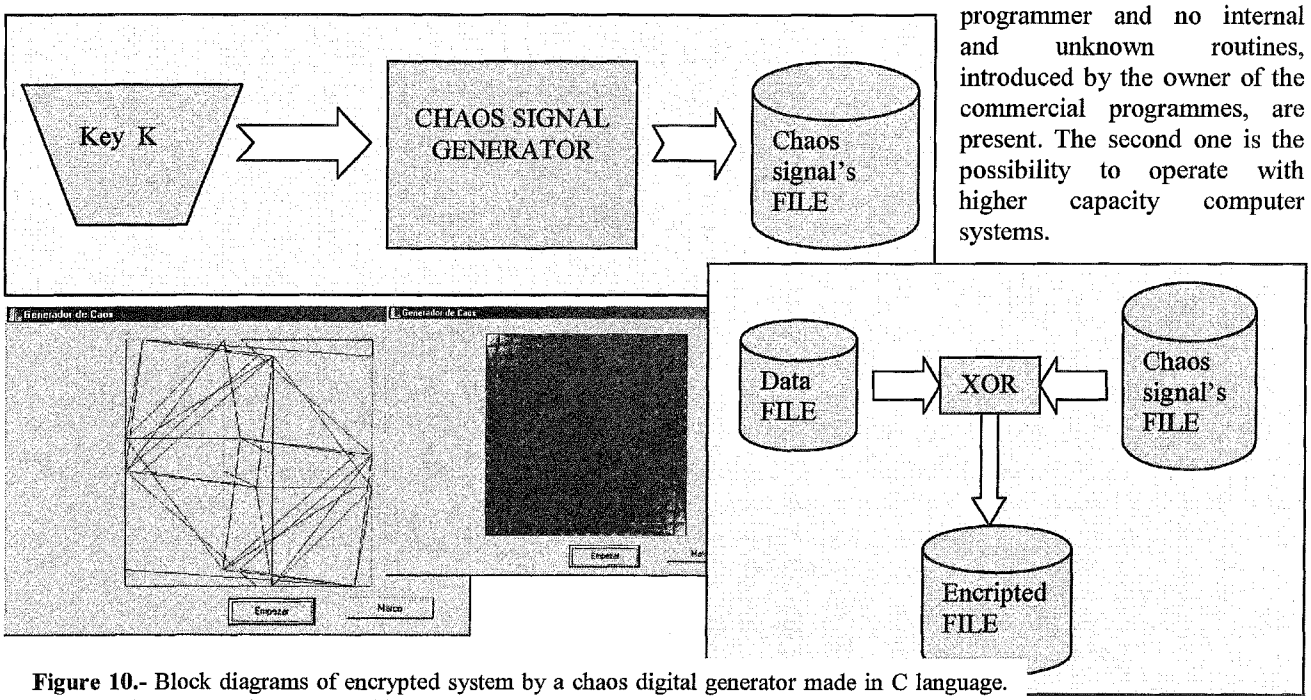


Figure 10.- Block diagrams of encrypted system by a chaos digital generator made in C language. The model has more than 10 variables for key k. Not all the values produce a chaos signal. With a phase space representation as the explained previously it is analysis the chaos quality of the signal generate. One screen shows a periodic signal and the other seems to be chaotic.

5.4. Techniques to analyze digital chaos to ensure secure transmission

As it can be seen from the previous sections the most important fact it is how to be sure that a digital time series is chaotic or it is just a random signal, or it is a periodic signal with a very long period. We have described the space – phase representation with an hexadecimal representation, but even in this approximation, that when almost all the possibilities in the space-phase it is cover, we are not sure if the signal it is periodic or not. We have development our on tools to analyzed and characterize a digital time series.

As an example, on Fig. 11 it is presented some results of the study done over a time digital series generated by the C program. First, it has been used the conversion of 16 bits on its decimal value, 2^n where n=16, which means we have 256 different levels. The statistics analysis of the time series gives the plot on fig. 11.(a). On reference [14, 15], it can be found some other approach done to study the statistical and complexity of a digital encoding. The information gives by this analysis must have a better understanding. Second, if we consider that the parameter of the systems remain constant and that the phenomenon is sufficiently sampled we can study linear correlation; on fig. 11.(b) Fourier coefficients are represented for the same signal. The plot gives some information but as the time series is not stationary it is necessary to apply nonlinear techniques; Fourier coefficients depends on the time period analyze. Finally, on fig.11(c) it is plot the estimation of the maximal Lyapunov exponent, a nonlinear technique to study a time series. This exponent is a strong signature of chaos. As it can be seen the slope represents a positive exponent and is based on the algorithm reported on reference [16]. Further studies must be done to obtain a complete characterization of our time series.

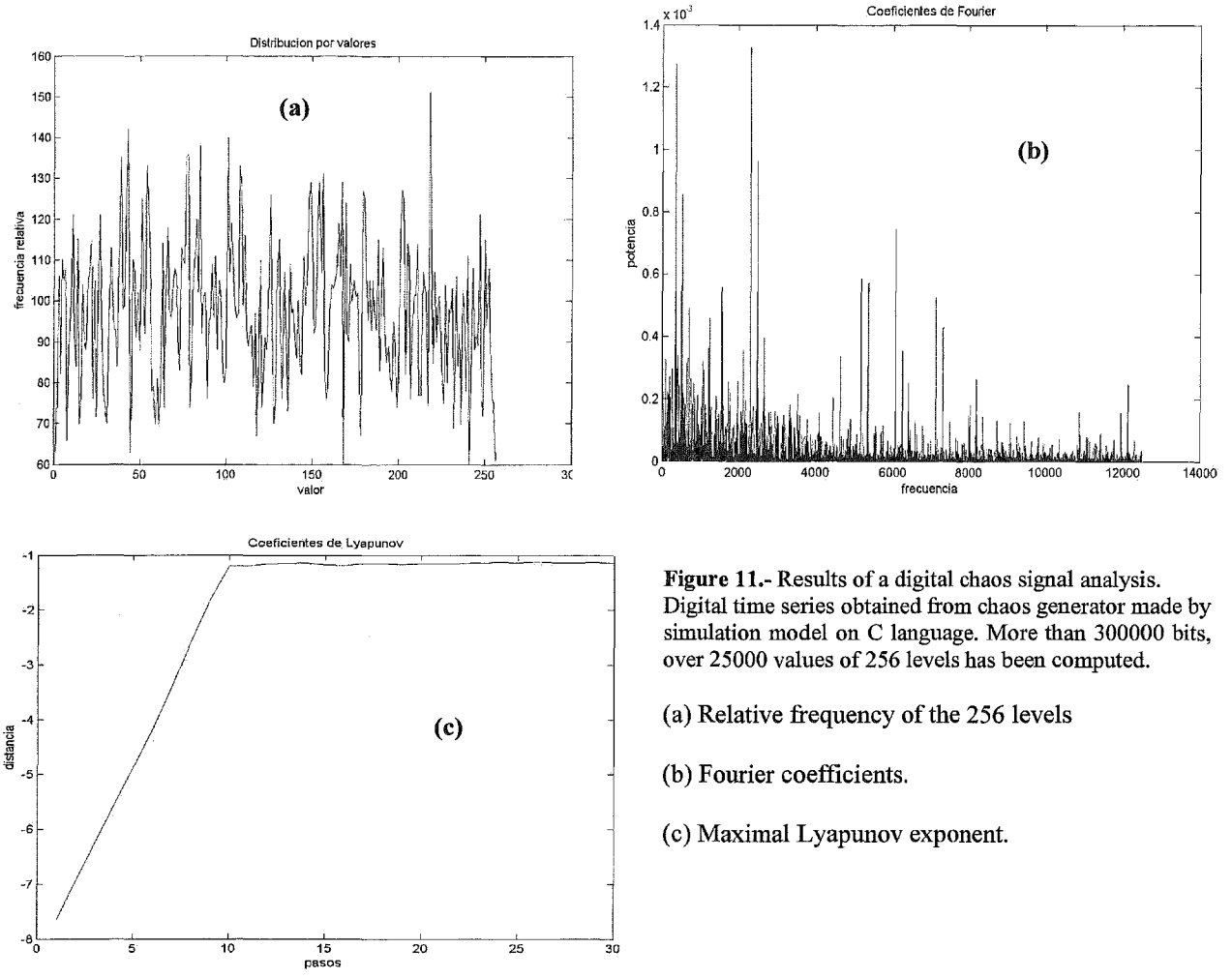


Figure 11.- Results of a digital chaos signal analysis. Digital time series obtained from chaos generator made by simulation model on C language. More than 300000 bits, over 25000 values of 256 levels has been computed.

(a) Relative frequency of the 256 levels

(b) Fourier coefficients.

(c) Maximal Lyapunov exponent.

A brief overview has been presented of the work done trying to describe a digital chaos generator to be implemented for a secure transmission of information.

ACKNOWLEDGMENTS

This work was partly supported by: CICYT, grant TIC2003-04309; CAM "Comunidad Autónoma de Madrid", grant FPI- Formación de Personal Investigador; and grant Cátedra Vodafone (2003).

REFERENCES

1. V.S. Afraimovich, N.N. Verichev and M.I. Rabinovich, *"Stochastic synchronization of oscillations in dissipative systems"*, Inv. VUZ. Rasiofiz. RPQAEC 29, 795-803, 1986.
2. L.M. Pecora and T.L. Carroll, *"Synchronization in Chaotic Systems"*, Physical Review Letters 64, 821, 1990.
3. L.M. Pecora, *"Overview of Chaos and Communications Research"* in "Chaos in Communications", SPIE Proceedings, 2038, 2-25, SPIE. Bellingham, WA. 1993.

4. T.L. Carroll and L.M. Pecora, *"Synchronizing Chaotic Circuits"*, IEEE Trans. on Circuits and Systems, 38, 453, 1991.
5. Several examples are given in "*Chua's Circuit: A Paradigm for Chaos*". Ed.: R.N. Madan. World Scientific Series on Nonlinear Science. World Scientific. London. 1993.
6. K.M. Cuomo and A.V. Oppenheim, *"Circuit implementation of Synchronized with applications to Communications"*. Physical Review Letters, 71, 65-68. 1993
7. K.M. Cuomo, A.V. Oppenheim and S.H. Strogatz, *"Synchronization of Lorentz-based Chaotic Circuits with Applications to Communications"*. IEEE Trans. on Circ. and Systems. 40. 626-633. 1993.
8. T. Stojanovski, L. Kocarev and U. Parlitz, *"Digital Coding via Chaotic Systems"*. IEEE Trans. on Circ. and Systems. 44. 562-565. 1997.
9. J.A. Martín-Pereda, A. González-Marcos and C. Sánchez-Guillén, *"Synchronizing Chaotic Optically-Programmable Digital Circuits"*. Globecom 96. IEEE Global Telecommunications Conference, London. 1996.
10. A. González-Marcos and J.A. Martín-Pereda, *"Transmission of digital chaotic and information-bearing signals in optical communication systems"*. Mathematics of Data/Image Coding, Compression and Encription II, SPIE, vol.3814, pp.36-42, (1999).
11. A. González-Marcos and J. A. Martín-Pereda. *"Digital chaotic output from an optically-processing element"*, in Optical Engineering, Vol. 35, pp. 525-535, (1996).
12. A.Hurtado, A. González-Marcos, J.A. Martín-Pereda, *"Low Power Signal Processing With Vertical-Cavity Semiconductor Optical Amplifiers (VCSOAs)"* Topical Meeting on Optoinformatics, St.Petersburg (Rusia). 18-21 October 2004.
13. A.Hurtado, A. González-Marcos, J.A. Martín-Pereda, *"Optical Reflective Bistability In Vertical-Cavity Semiconductor Optical Amplifiers (VCSOAs)"* Topical Meeting on Optoinformatics, St.Petersburg (Rusia). 18-21 October 2004.
14. J.A. Martin-Pereda and A. Gonzalez-Marcos, *"Time evolution of frequency components in a chaotic digital signal"*. Algorithms and Systems for Optical Information Processing V. Bahram Javidi, Demetri Psaltis; Eds SPIE. Vol. 4471 pp. 214-223. (2001)
15. J.A. Martin-Pereda and A. Gonzalez-Marcos, *"Analysis of digital chaotic optical signals"*, Mathematics of Data/Image Coding, Compression, and Encryption IV, with Applications; Mark S. Schmalz; Ed. SPIE. Vol 4475. pp. 106-115 (2001)
16. Holger Kantz and Thomas Schreiber *"Nonlinear Time Series Analysis"* Cambridge Nonlinear science Series 7, Cambridge University Press, 1997