AN OPTIMAL CHAOTIC BIDIRECTIONAL COMMUNICATOR FOR HIDDEN INFORMATION, BASED ON SYNCHRONIZED LORENZ CIRCUITS

R. Núñez.

Centro de Investigación Científica y de Educación Superior de Ensenada, B.C.

División de Física Aplicada, Km. 107, Carretera Tijuana-Ensenada, Ensenada, B.C., México, 22860

Tel. (646) 175-0555   E-Mail: rnunez@cicese.mx

ABSTRACT

An Optimal Chaotic Bidirectional Communicator for Hidden Information (OCBCHI) is presented. Its realization is based on a Standard Chaotic Bidirectional Communicator for Hidden Information (SCBCHI), that uses two Lorenz synchronized circuits with an open-loop explicit method. All the chaotic dynamics of the circuits were studied and analysed using DSP techniques. Regarding to our real-time application, -on bidirectional audio communications field-, the optimum conclusion was to make the synchronization and the hidden communication of the private information by the lower chaotic dynamic variable and the most higher chaotic dynamics variables, respectively. By the complete characterization of the bidirectional channels, we got the minimum parameters (i.e., time and spectrum magnitude) of the private information that it must have just to make a confidential and robust communication.

RESUMEN

En este trabajo se presenta un Comunicador Bidireccional Caótico Estandar de Información Oculta (CBCEIO), el cual utiliza dos Circuitos Sincronizados de Lorenz con un método explícito open-loop. Todas las dinámicas caóticas del circuito fueron estudiadas y analizadas usando Técnicas DSP. Por lo que se refiere a nuestra aplicación de tiempo real -en el campo de audio de la Comunicación Bidireccional-, la conclusión óptima fue hacer la sincronización y la comunicación oculta de la información privada, por medio de la variable baja de la dinámica caótica y de la variable alta de la dinámica caótica respectivamente. Por medio de la completa caracterización de los canales Bidireccionales, obtuvimos los parámetros mínimos (ejem: tiempo y magnitud de espectro) de la información privada que debe tener para hacer una comunicación confidencial y robusta.

KEYWORDS: Encrypted communication, Synchronization, Lorenz circuits.

1. INTRODUCTION

The experimental demonstration, that the Bidirectional Communication of Hidden Information, using the Lorenz Synchronized Circuits (**LSC's**), is not only possible but is efficient and reliable, was the goal achieved in [1]. Based on this result, the present work pursues: to characterize a Standard Communicator Bidirectional Chaotic Circuit for Hidden Information (**SCBCHI**), and to transform it into an Optimal one (**OCBCHI**), that takes advantage of the maximum dynamic characteristics of all the variables in game. To fulfil them, first the Lorenz Circuit (**LC**) [2] is described; at once, it is carried out a complete characterization of the **LC** redesigned, implemented with less component than the one reported in [3] and making it work in the kilohertz band. They are discovered, experimentally, the static and dynamic

5

operations ranges [4], -in the time and frequency-, of their X, Y and Z variables. They know each other and identify their waveforms and Spectral Shape Factors (SSF's). They are applied of DSP techniques [5] to discover, experimentally, which variable is the most chaotic, the quickest, the one with widest SSF, etc. Also, it is measured and deployed the LC dynamic, through the excitement imposed by the linear variation of the Rayleigh parameter. This way, the phase relative behavior is known among the signals and it is discovered who they evolve from and make the bifurcations. Given the objectives that are pursued, framed by the applications in Private Communications, it is chosen of [1] the experimental method to carry out the synchrony between two **LC's** in explicit form and open-loop [6, 7].They are detected, experimentally, the aspects to avoid the loss of the synchrony. Once you have being familiarized with the variables dynamics and with the explicit synchrony, it is taken the implementation, characterization and experimental evaluation of the Standard Chaotic Bidirectional Communicator for Hidden Information, or **SCBCHI**, that uses two **LSC's**. It is built with electronic components of low cost and of medium tolerance. For their evaluation are used periodic, chaotic, voice and audio signals, -as information to hide-, with the purpose of discovering their quality and recovery dependability in unidirectional and bidirectional communications. The X variable is chosen, to synchronize, and the Y and Z variables, -those of dynamics chaotic more dissimilar-, respectively, to establish the bidirectional communication and to compare, instantly, the concealment capacities and recovery that present these in the face of identical-autotesting and different information. It is built a demonstrative model of the hidden/transmitted and received/recovered, -in real time-, of radio information, AM-masking by the Y variable and FM-masking by the Z variable, to observe on an Oscilloscope and to listen on a Speaker the original and recovered audiosignals, respectively. As a final result, the basic approaches that the Optimal Chaotic Bidirectional Communicator for Hidden Information, or **OCBCHI**, will settle down completely. In particular, regarding to synchronize the variable (v.g., to use the less chaotic) and to establish the sure bidirectional communication (v.g., to use the most chaotics). As well as the relative characteristics of amplitude and SSF that should keep the information to hide, regarding those of the chaotic signal and asynchrony. We are thinking about the necessity to process the original signal by means of an AGC Circuit. Also, some applications of the **SCBCHI** and **OCBCHI** Circuits intend in industrial processes, through their electromechanical analogies.

2. THE LORENZ CIRCUIT (LC)

The equations (1) describe the **LC** [2] performance. The scaled equations are:

$$x = - r \int (x - y)dt,$$
$$y = - [10 \int x(z - p/10)dt + \int ydt], \qquad (1)$$
$$z = - [10 \int y(- x)dt + b \int zdt],$$

where the parameters of **r** (i.e., Prandtl number) and b (i.e., geometric factor) are left in 10 and 2.7, respectively. While the **p** (i.e., Rayleigh number) is incorporated by means of a voltage varied through the XR1 potenciometer to obtain and maintain dependability, the chaotic Circuit behavior; situation achieved for values in the 3.90 V d.c. vicinity.
The **LC** normalized, built and characterized it is presented in figure 1; it is a simplified and frequency scaled version of the one reported in [3]. For its implementation, commercial components of low cost, medium tolerance and easy acquisition are used.

3. EXPERIMENTAL CHARACTERIZATION OF THE LC

The measurement, display, analysis, save and print of the data, is based widely on Labview (ATS-Labview: Dynamic Generador/Analyzer) and Dadisp (ATS-Dadisp) Automatic Test Systems (ATS's) [4].

Figure 2, shows the instantaneous waveforms, and the lineal magnitude of the spectra, corresponding to the X, Y, and Z measured chaotics signals with the ATS-Dadisp.
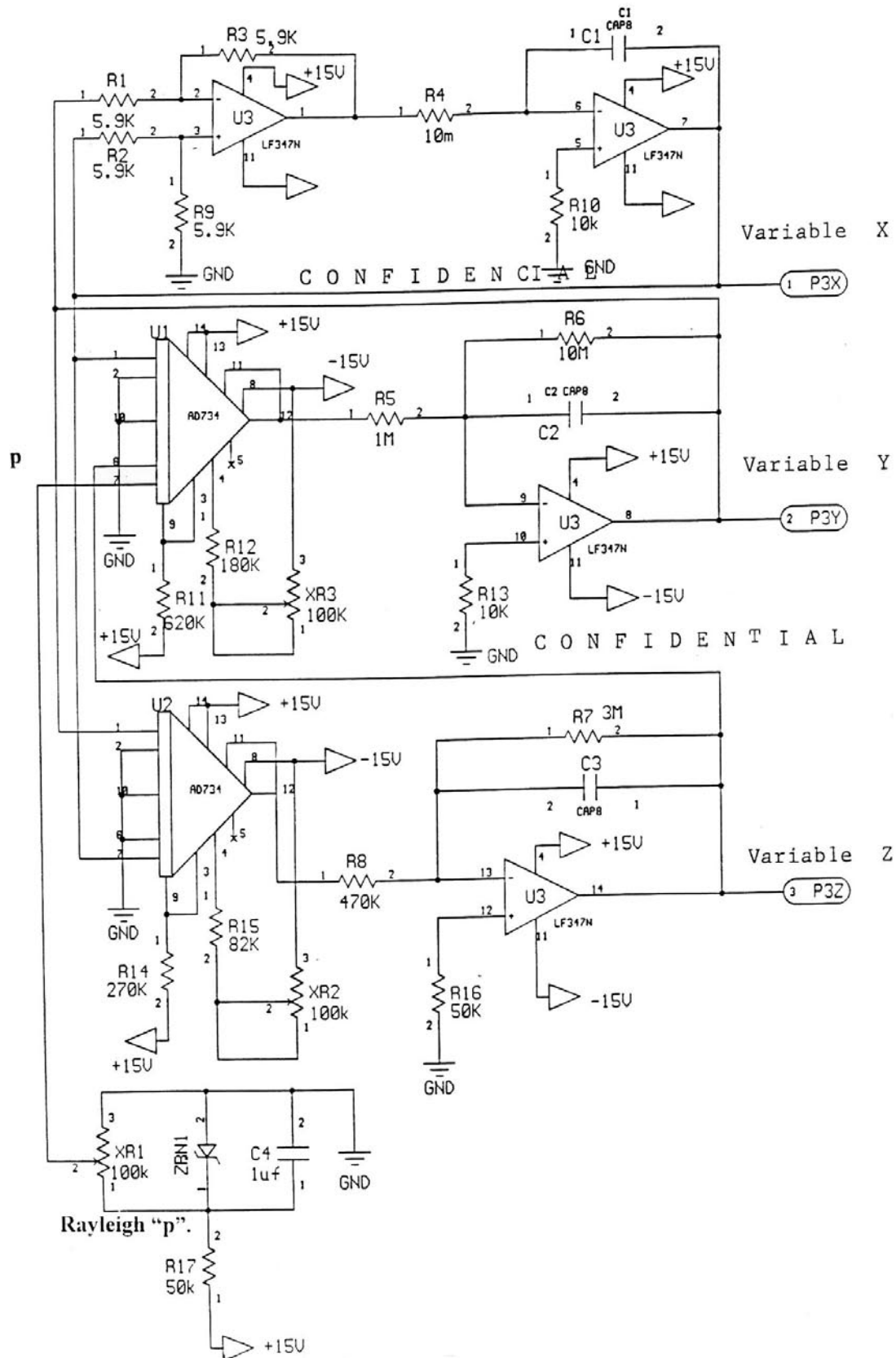
6

Figure 1. Lorenz Electrical Circuit.

3.1 The variables of the LC and their chaotic dynamics

In figure 3, it is presented, graphically, the result of what was carried out to discover, experimentally, the chaotic dynamics of the Lorenz signals. In particular, to identify y qualitatively to the more and less chaotic. If we observe the waveforms of the same ones, in W1, W2 and W3 windows of the mentioned figure 2, we can corroborate that the Y variable presents a bigger dynamics, the X variable continues it and lastly the Z variable. This same can be proved revising its magnitude spectrum, in W4, W5 and W6 windows. But, if we want to quantify the relative degree of chaos, -between the variables-, we need to use the autocorrelation function [5]. This function, manifests us, -in the time-, how similar it is in this way to the same signal, i.e., how many periodic components they constitute. Thus, for this case, the signal that presents the smallest autocorrelation will register the biggest chaotic dynamics. Before applying this function, the magnitude of the playing signals should be normalized. We use the Y variable, like normalization element (v.g., X/Y and Z/Y). For that, in figure 3, we are displaying the magnitudes of the three variables instantaneous autocorrelations and you can appreciate that the difference of those corresponding to the X and Y variables, is small; what means that their chaotic dynamics are similar, but not equal since the one of the Y variable is a little bigger.
In figure 4, the waveforms are presented (c.f., W1 and W3 windows), the phase-planes (c.f., W5 and W6 windows) and the spectral magnitudes (c.f., W2 and W4 windows) corresponding to the Lorenz X and Z variables in chaotic operation. The X/Z phase-plane, is known like the **Lorenz Butterfly atractor** (c.f., W5 window) [5, 1].
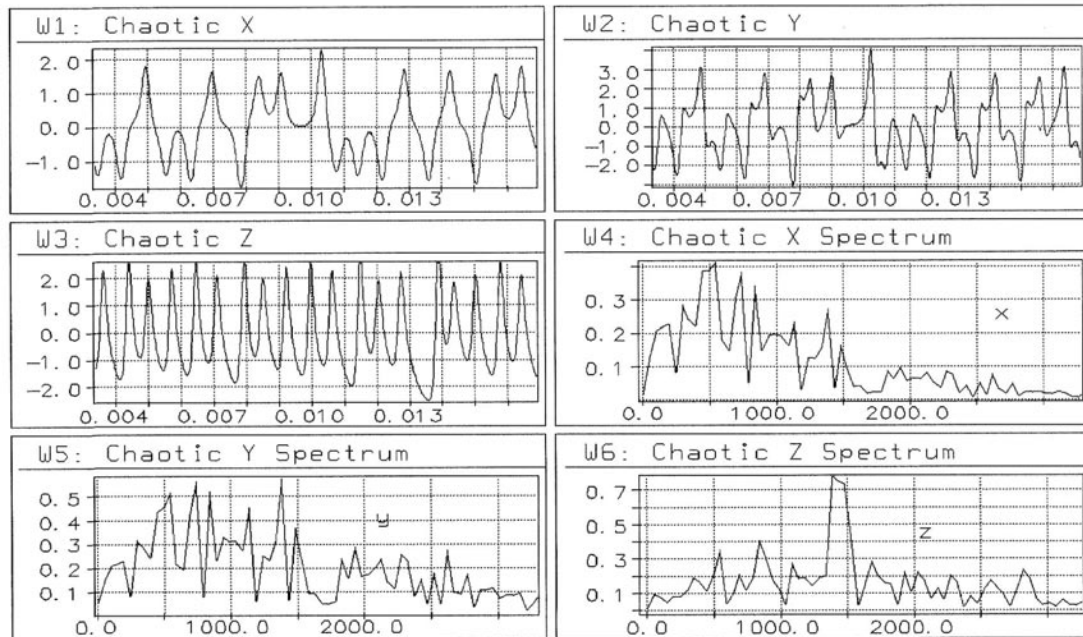

Figure 2. Lorenz Chaotics variables X, Y, Z and their spectra.

3.2 The LC dynamics based on the Rayleigh parameter variations

3.2.1 Steeped and linear parameter variations; bifurcation and relative phase

In figure 5, the **LC** dynamic characteristics are presented, in attention to the steeped variation of the **p** Rayleigh parameter. The variation begins in 0.0 volts, it is increased, in one volt steps, up to 5.0 volts, and it is decreased, in a similar way, down to 0.0 volts, where it finally finishes. As it can be appreciated, the variation of the parameter, -in steeped form-, causes that the behavior of the **LC**, -measured through its X, Y and Z variables-, evolve from the static to the dynamic operation (v.g., it goes by the periodic and chaotic states) and return again to the static one. In particular, the mentioned figure describes, graphically, the Y variable behavior; the most chaotic. Now, if we do vary the parameter in a lineal way, we can observe with thoroughness the evolution of a Circuit complete cycle, as figure 6 describes, in which spreads the Y and Z variables trajectory to the chaos. Chaos route, apparent the bifurcation phenomenon, which is presented in the same figure, i.e., when the Circuit variables pass from the periodic dynamic

8

state to the chaotic one. For our particular case, the phenomenon is appreciated, approximately, to the 6 seconds, measured starting from the outburst of the lineal excitement function (i.e., saw-tooth) that governs the parameter. Here, we can observe that the Y variable, -besides being the most chaotic-, it advances in phase to the other Z and X variables, and that those, in turn, are positioned and evolved in that same order.
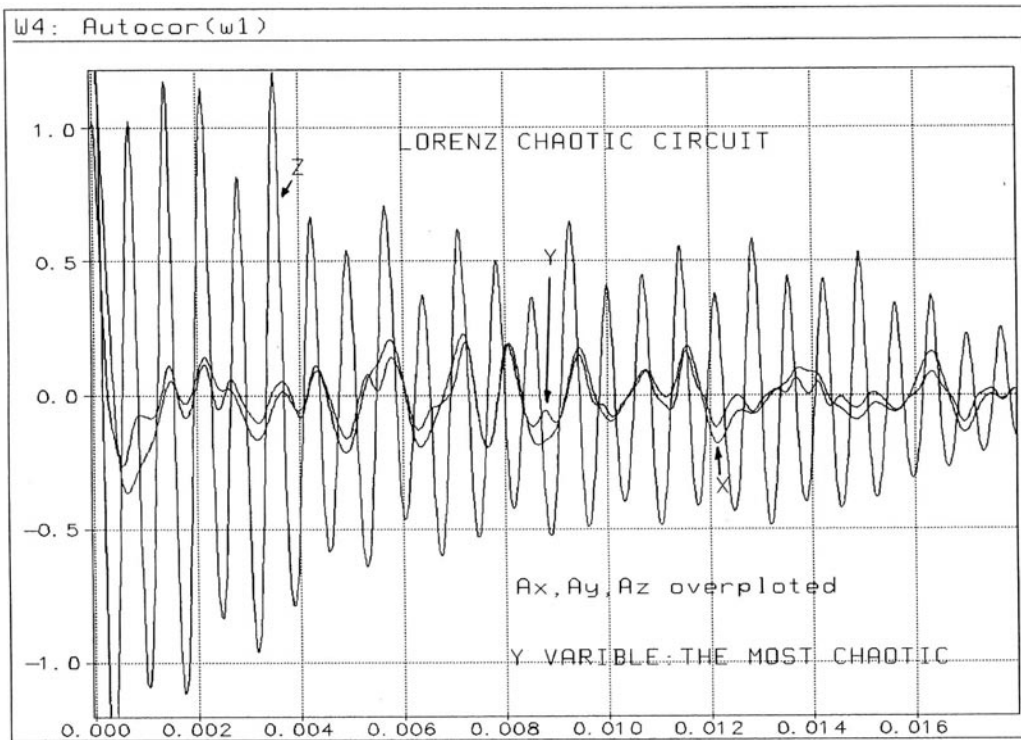

Figure 3. Comparative study between the X, Y and Z autocorrelations.

Figure 4. Waveforms, spectra and phase-plans of X and Z; Lorenz Butterfly atracttor.
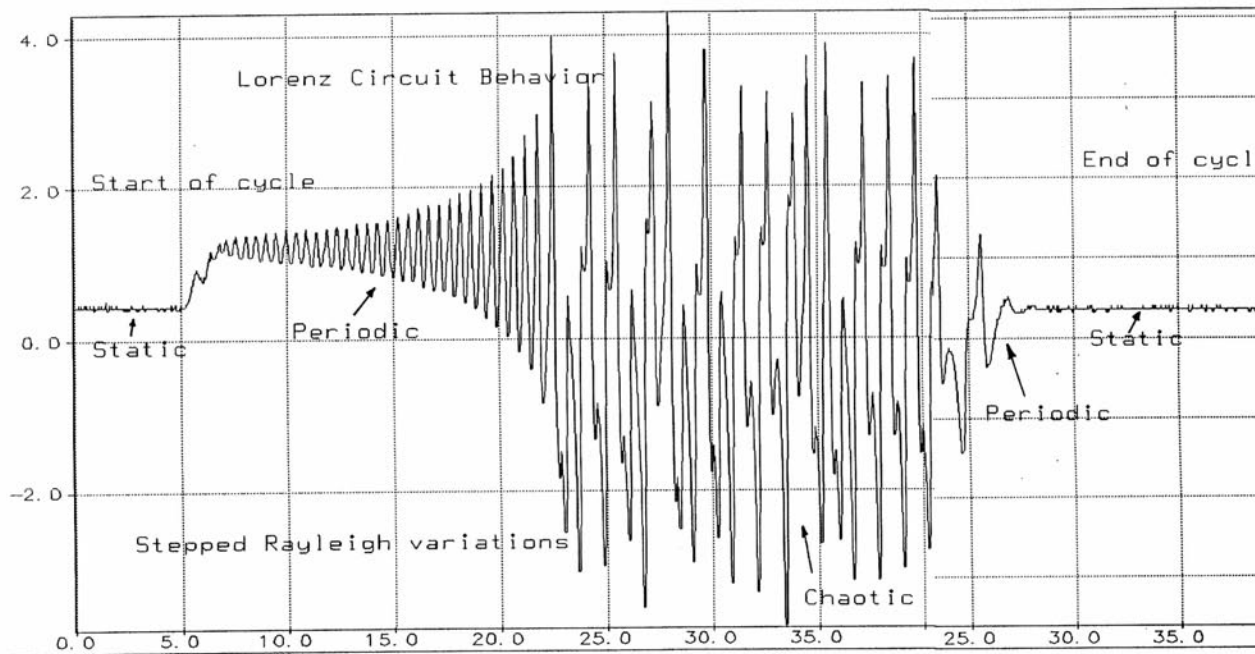
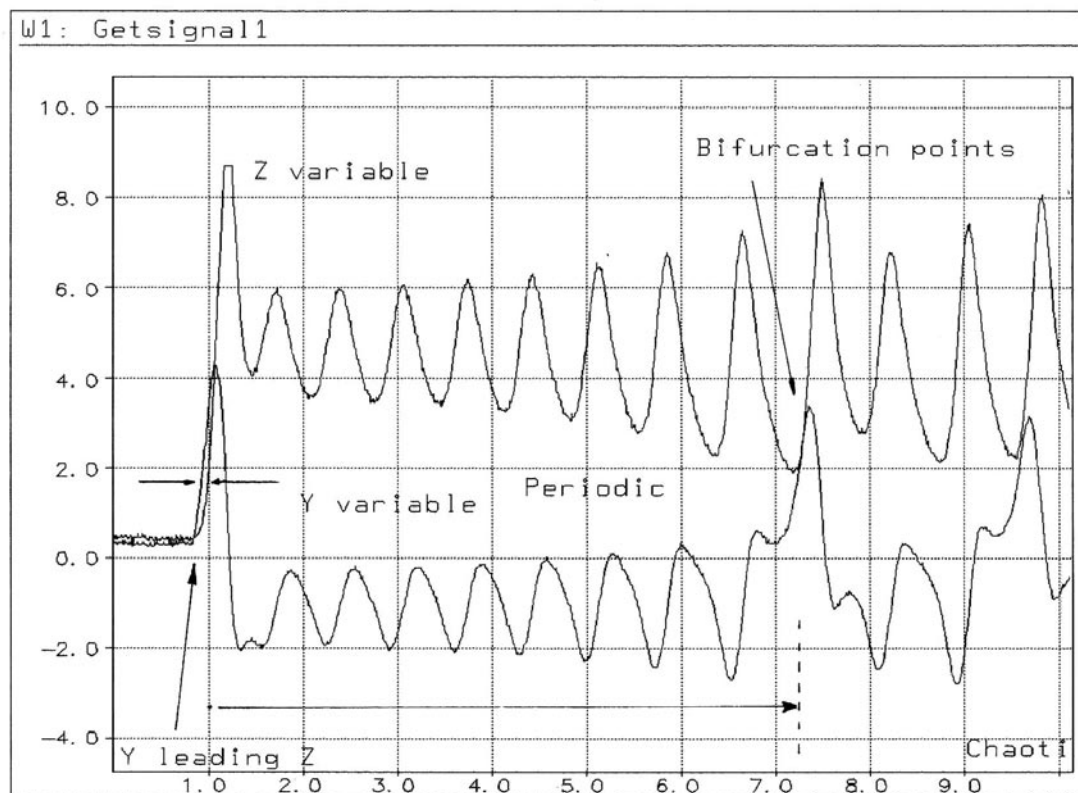*Figure 5. Complete dynamics of Lorenz Circuit Y variable.*

Figure 6. Routes to chaos and bifurcation for the Z and Y variables.

10

4. EXPERIMENTAL SYNCHRONIZATION OF OPEN-LOOP FOR TWO LC´s

The basic method of experimental synchronization that is used, is equivalent to one control in open-loop, as it indicates figure 7. In this method, the Xr signal (v.g., synchronized Circuit or receiver) it is generated and controled, indirectly, starting from the Xt signal (v.g., synchronizator Circuit or transmitter), i.e., Xt causes that the Yr and Zr signals are generated and those, in turn, produce the Xr signal, in the receiver Circuit. Now then, in order for this to work fine, it is required that the two **LC's** involved, (i.e., their components, powers, parameters, delay chains and operation initial conditions, etc.,) be as similar as possible and that they present the same stability. The difference that exists between the Xt and Xr chaotic signals is, intimately, related with the instability and inequality among the Circuits. To this difference we call it: synchrony error or asynchrony, and it is governed by the same chaotic dynamic, since manifests the phase and magnitude relative movements of the two signals involved. So that the systematic asynchrony is minimum, it is required that the delay in the generation and control of the Xr variable, be very small. For this method, the robustness is very limited and it depends, -like in any control system of open-loop-, of the components and electronics circuits stability.

In figure 8, a complete description of the synchrony process is presented for the Lorenz X variable, using the ATS-Dadisp [4]. In W1 and W4 windows, we are displaying the Xt and Xr signals, respectively, while in W7 and W8 windows, we are displaying their lineal spectra. The W6 window, presents the quality obtained in the synchrony process, i.e., the Xt/Xr phase-plane. This process, can also be qualified by the synchrony error measurement, or asynchrony, that is presented in W2 window and which registers a maximum of 60 mVp. In W5 window, this same error is presented but, this time calculated, i.e., the difference between the Xt and Xr instantaneous measurements, W1 and W4 windows, respectively. This error, of 80 mVp, matches with the one measured in the Circuit (c.f., W2 window). For this same case, the big values of the Cross-Correlation (CC) function [5, 1], -between the Xt and Xr variables (i.e., W1 and W4 windows)-, indicate that the variables are very similar, i.e., there is a good synchronization between the Circuits; as well as they indicate this way their regarding spectra.

In figure 9, we are displaying the phase-planes for the six measured Lorenz variables. The Xt/Xr, Yt/Yr and Zt/Zr graphics correspond to the W7, W8 and W9 windows, respectively, and they represent the quality achieved in the synchrony process, between the transmitter and receiver Circuits, during a medium term stability study.
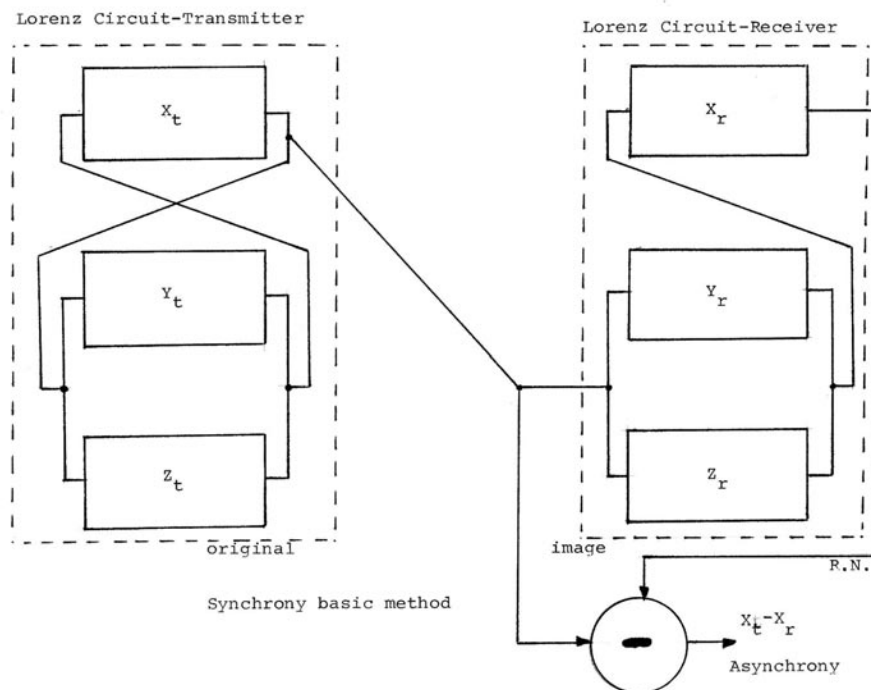

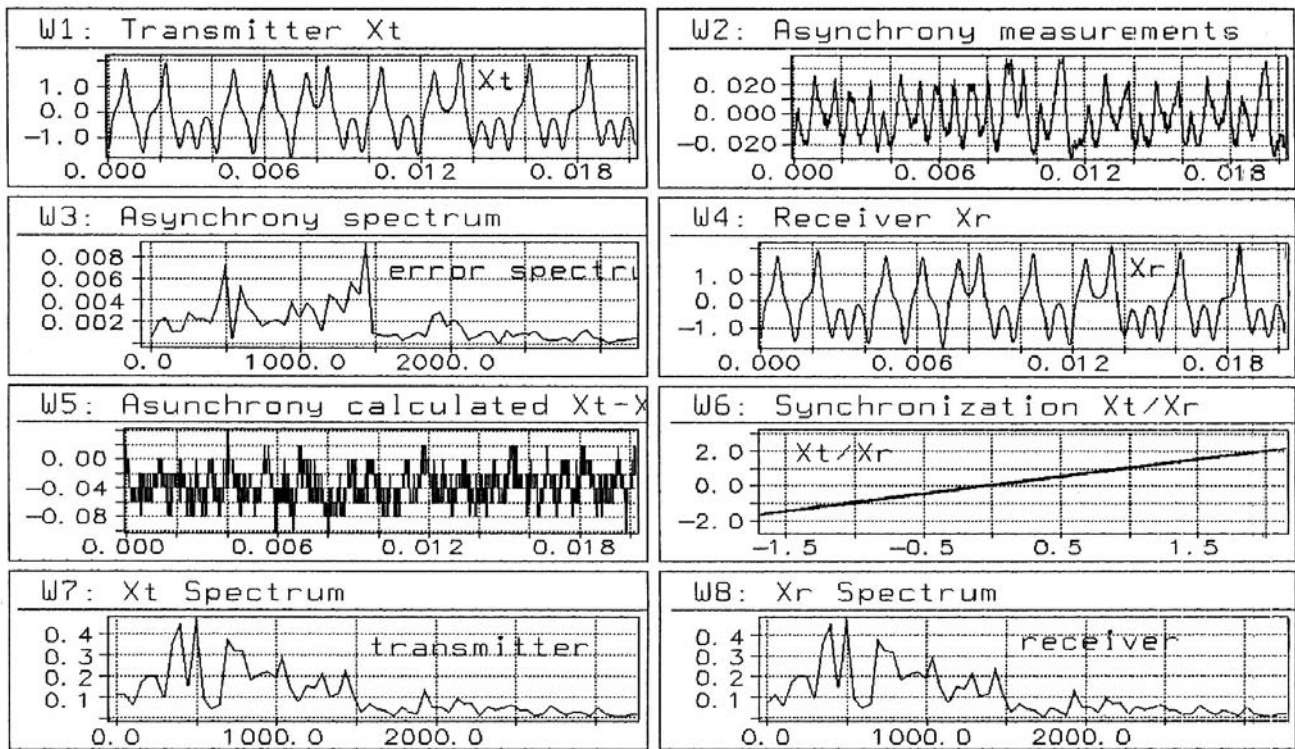*Figure 7. Synchrony basic method between two identical Lorenz Circuits.*

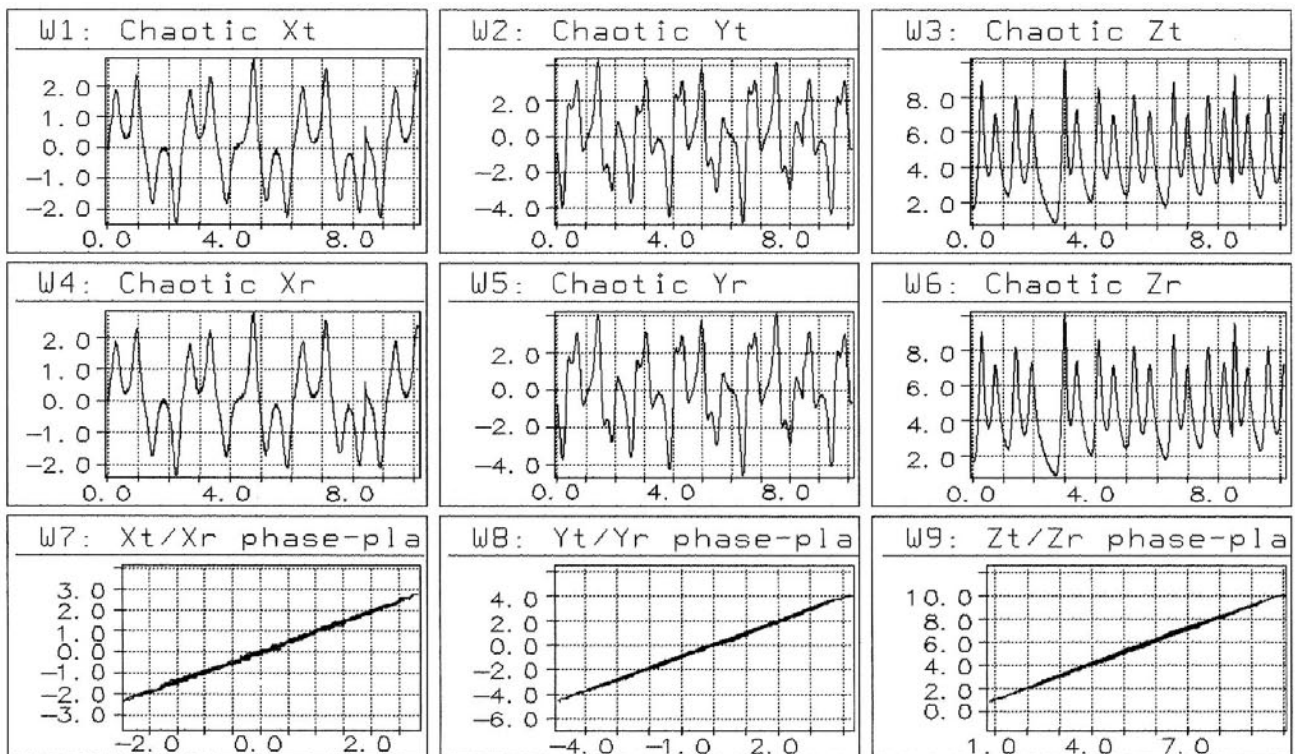*Figure 8. Synchronization process for the X variable; measured/calculated asynchrony.*

Figure 9. Quality gotten in X, Y and Z synchronization processes.

12

5. APPLICATIONS OF THE EXPLICIT SYNCHRONY METHOD (TWO-LINES) IN COMMUNICATIONS

5.1 Unidirectional communication

In figures 10 and 11, the basic outlines are presented to take the unidirectional shipment of hidden messages using the method of explicit synchrony (two-lines) and synchronizing by means of the X variable. This method, was selected from a comparative study, about the efficiency in the hidden and recovery of information, practiced to the methods of implicit and explicit synchrony, carried out in [1]. In figure 10, the Xt synchronizating chaotic signal travels for a line (b) and the information to hide mixes with the same chaotic signal (i.e., Xt + Inf.) and they travel for line (a). Already in the receiver, it is subtracted from the mixed signal the Xr or Yr signal (c.f., figure 11), the one which, -product of the synchrony-, it is almost identical to the Xt or Yt, respectively, in this way to recover the original information signal (i.e., Xt + Inf. - Xr ~ Inf'.).

In figure 12, the obtained results are presented when the signal to hide and to recover is the Lorenz Z chaotic signal. In W1 and W2 windows, we are displaying Lorenz Xr chaotic signal, and the one overlapped between this same one and the sum of Lorenz Xt and Z (i.e., information) chaotics signals, respectively. In W3 and W4 windows, the phase-plane is presented between the Xr chaotic signal and the mixed signals (i.e., Xr / Xt + Z chaotic) and the Z chaotic signal recovered, respectively. For the case, it is interesting to observe that the W3 window phase-plane draws the "**Lorenz Butterfly atractor"**.

In figure 13, the results of the method of explicit synchrony are presented, in an outline of unidirectional communication, when applying audiosignals to it. The application corresponding to the hidden/recovered of audio messages coming from the AM radio, is presented. In W1, W2, W3, W4, W5 and W6 windows, we are displaying the audiosignals to hide/transmit, to receive/recover, the asynchrony, the phase-plane between the original and recovered signals, and the lineal spectra of each one of these signals, respectively. Observe in W4 window, the quality with which recovers the original information.
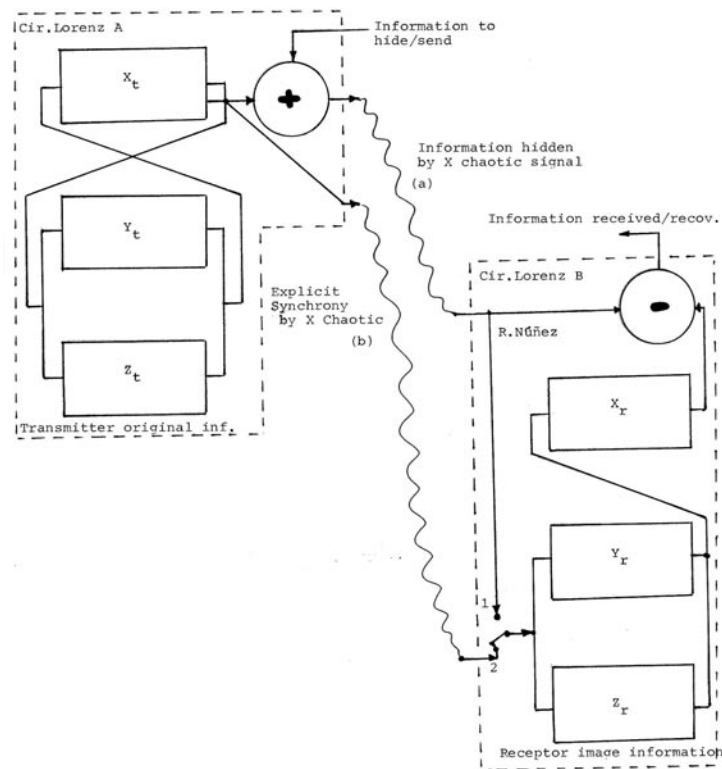

Figure 10. Communication of hidden information through X; using explicit synchronization.
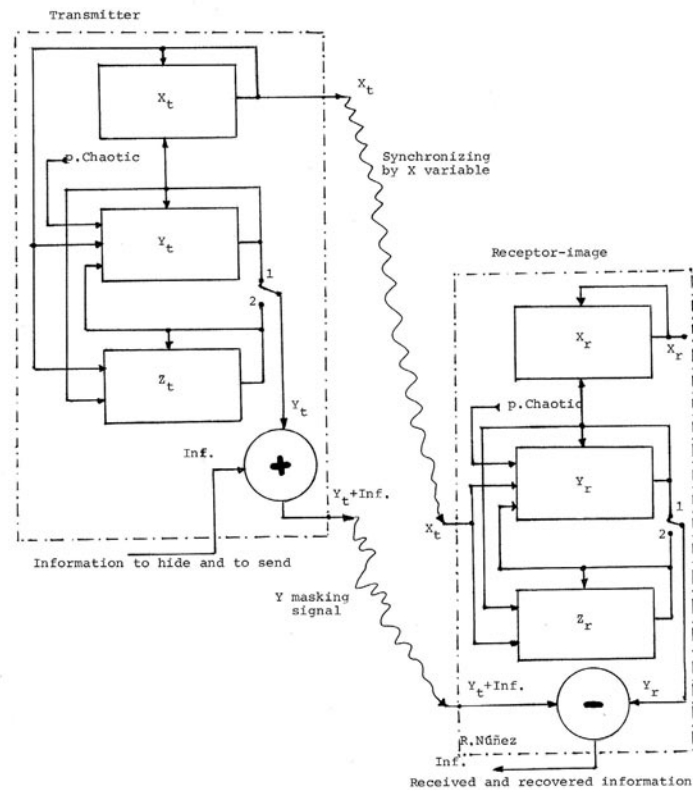
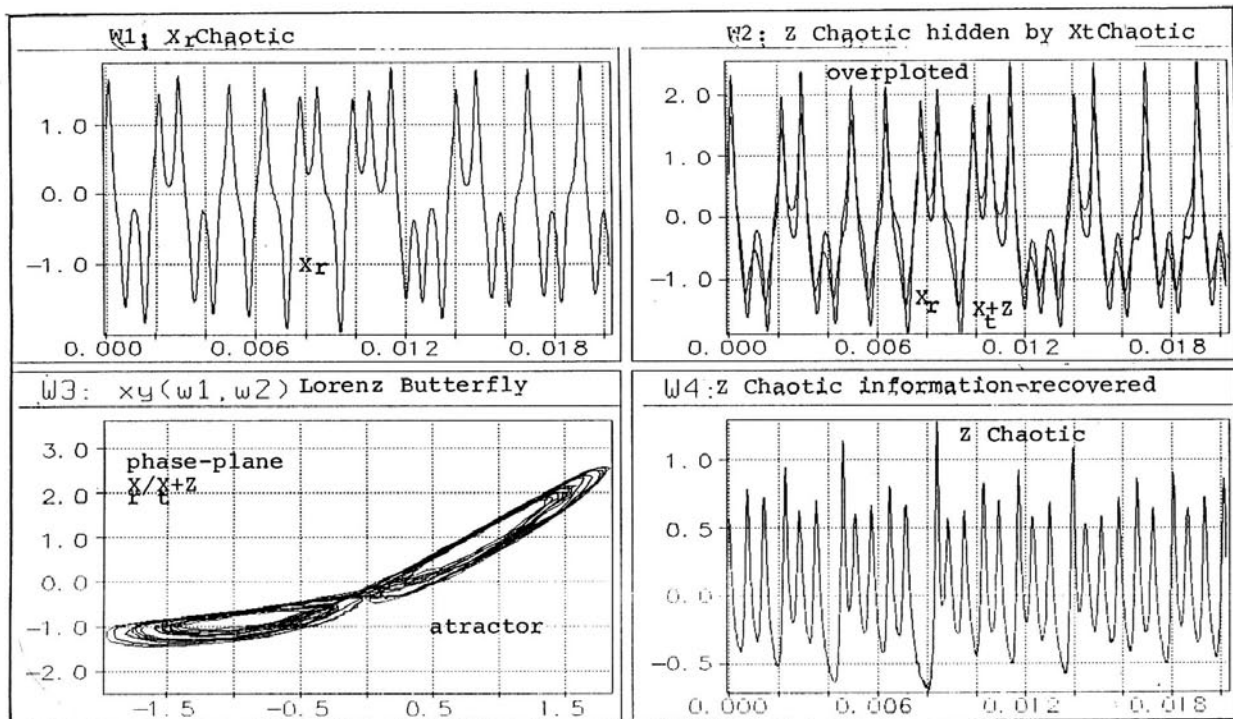*Figure 11. Communication of hidden information through Y or Z; synchronizing by X.*

Figure 12. Z Chaotic hidden by X Chaotic; Lorenz Butterfly atractor.

14

5.2 Standard Chaotic Bidirectional Communicator for Hidden Information (SCBCHI)

In figure 14, the Standard Chaotic Bidirectional Communicator for Hidden Information, or **SCBCHI**, blocks diagram is presented; which was built to check that the hidden process and audio recovery using Lorenz chaotic signals, with explicit synchronization, it is feasible and reliable [1]. A method of three lines is used to achieve the bidireccionality, and the variables are selected to synchronize and to hide the information in a particular way. The X chaotic variable, is used to synchronize the two **LC's**, under almost identical operation conditions (c.f. section 4). The Circuits are identified like A and B. The A controls, or synchronizes, B; the lines indicated are physical. The A Circuit sends the hidden information, through the Y variable, of more chaotic dynamics, to B Circuit, and the B Circuit answers sending the hidden information, through the Z variable, of less chaotic dynamics, to the A Circuit. This outline was designed to study the channels characteristics, regarding to capacity and security in the concealment, i.e., the capacity of hiding a great deal of voice/audio signals of the same magnitude and bandwidth such as different magnitude and bandwidth, through the Lorenz variables with the chaotic dynamics more dissimilar. It is obvious that two degrees of dependability are presented in the concealment. The one of A towards B should be better, therefore, more reliable than the one of B towards A. In the schematic diagram of figure 15, the **SCBCHI** complete Circuit is presented which was implemented, proved and characterized.
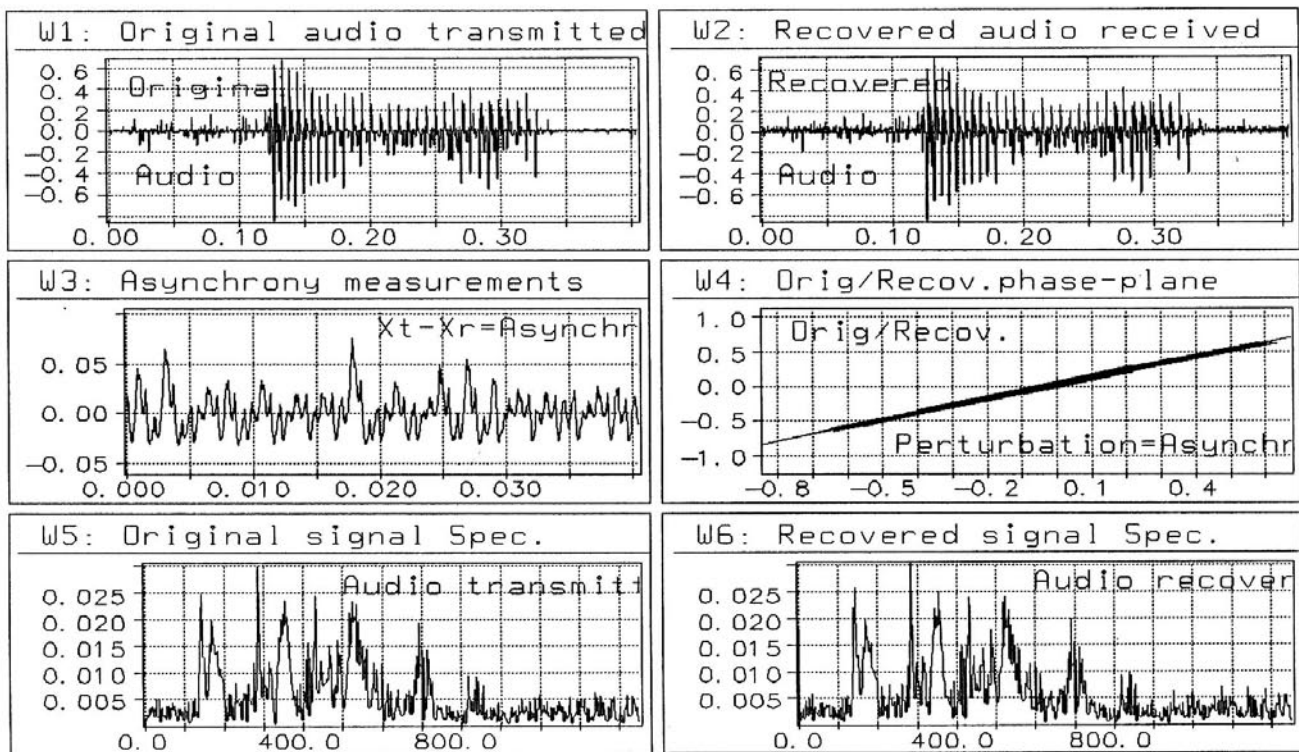

Figure 13. Hidden and recovered of an audio signal.

5.2.1 SCBCHI performance using a voice echo

As the result signals indicate in figure 16, to prove the **SCBCHI** (c.f., figures 14 and 15) the signals are used, firstly, voice signals in a "echo" configuration, or autotesting, i.e., what is sent of A to B one returns from B to A. They are presented, in W1 and W2 windows, the transmitted and recovered voice signals in the A Circuit (v.g., original voice and Zb + "voice echo"-Za), respectively. In W3 and W4 windows, they are presented overlapped the two previous signals and their phase-plane, respectively. The perturbation corresponds completely to a small asynchrony that is observed also in W2 window and which turns out to be a little bigger than the normal asynchrony, because the circulate trajectory that the voice, -or test signal-, travels, i.e., an inherent asynchrony exists of A towards B (v.g., Ya-Yb

in the B Circuit) and another of B towards A (v.g., Zb-Za in the A Circuit), what increases the synchrony absolute error. In a normal bidirectional conversation, or telephonic, this error would not be generated. In general, the quality with which recovers, in the A Circuit, the original voice information of 1 Vp, or "echo", is quite acceptable, since the amplitude of the accumulated asynchrony doesn't surpass the 100 mVp. In W5 and W6 windows, the spectra of the transmitted and received signals are presented. It is observed that they are quite similar.
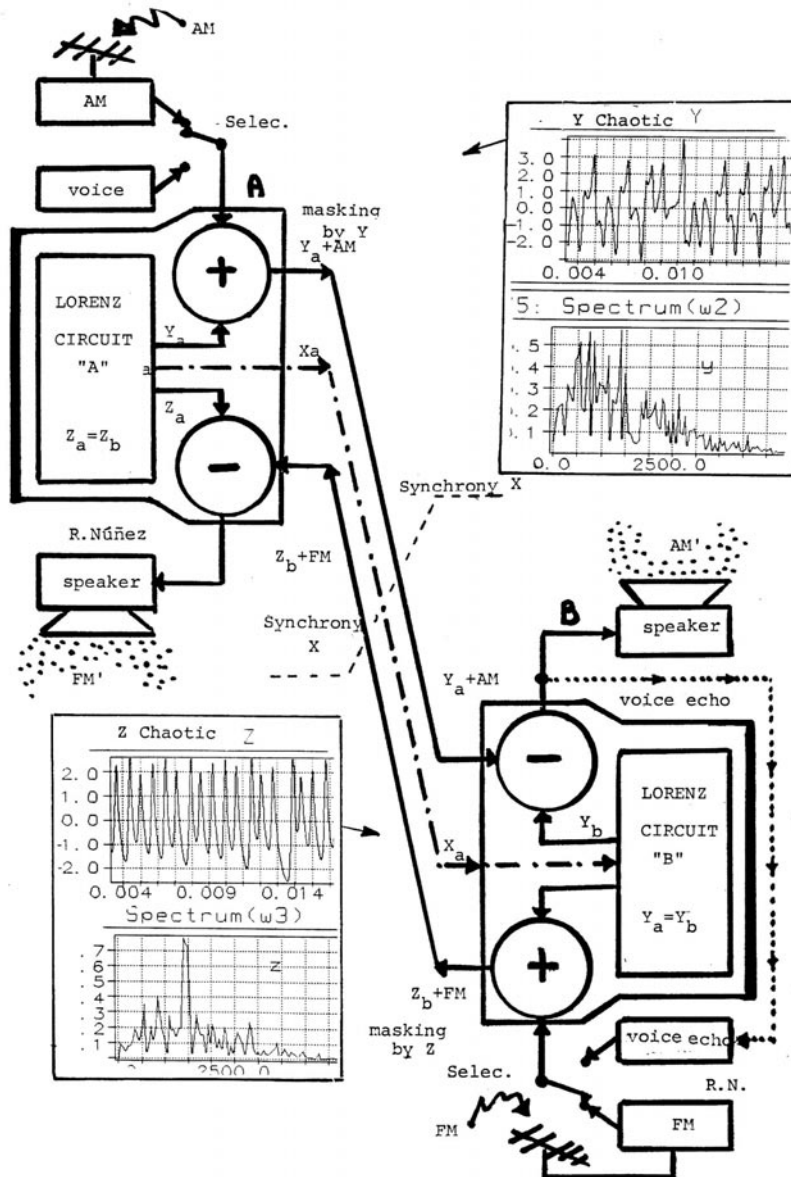

Figure 14. The SCBCHI graphic diagram.

5.2.2 SCBCHI performance using an AM and FM audio dialogue

They are using figures 14 and 15 again, to describe a particular application similar to a telephonic conversation and that it consists in: to hide and to send information of the AM radio of the A Circuit, through the Y variable, -to synchronize the B Circuit by means of the X variable-, to receive and recover this AM information in the B Circuit. At the same time, the B Circuit hides and sends the information of the FM radio to the A Circuit, through the Z variable. The A Circuit will receive and it will recover the FM information. As it can be observed, the AM information, is the one

16

that travels more protected or safe since it uses, by means of concealment and transport, the Y variable, the most chaotic. While, the FM information, is the one that travels less protected, since its bandwidth surpasses that of the Z variable, the less chaotic one.

In W1 and W3 windows, figure 17, we are displaying the AM audiosignals correspondent of A towards B and recovered in B, respectively, and in W2 and W4 windows, we are displaying the FM audiosignal correspondent of B towards A and recovered in A, respectively. Observe attentively the W3 and W4 windows, corresponding to the recovered signals, and compare them with the W1 and W2 windows, respectively, so that it detects the small errors product of the asynchrony.

In W5 and W6 windows, the differences between the original and recovered signals for each communication channel are presented, respectively. One can observe that, for both cases, the error in the information recovery is smaller than 100 mVp. Although, it is convenient to clarify that the AM and FM original audiosignals are not normalized in their amplitude.

In the W7 and W8 windows, the rate of quality is appreciated between the original/recovered audios, -for each communication trajectory-, in both senses and at the same time. To verify the quality of each channel [1], the autocorrelation of the original signal is obtained and it is compared with the CC between the original and recovered signals. If the recovered signal is an exact copy of the original one its CC it will correspond to the original autocorrelation. The above mentioned, is manifested through the W9, W11 and W13 windows, in which are presented, the AM original signal autocorrelation, the CC among the original one and the one recovered, and the difference between both correlations, respectively. As it can be appreciated, the difference between the correlations it is very small. In W10, W12 and W14 windows, the case is presented for the FM communication. Again, the appreciated difference among the correlations is very small and almost of the order of the corresponding to the AM communication.
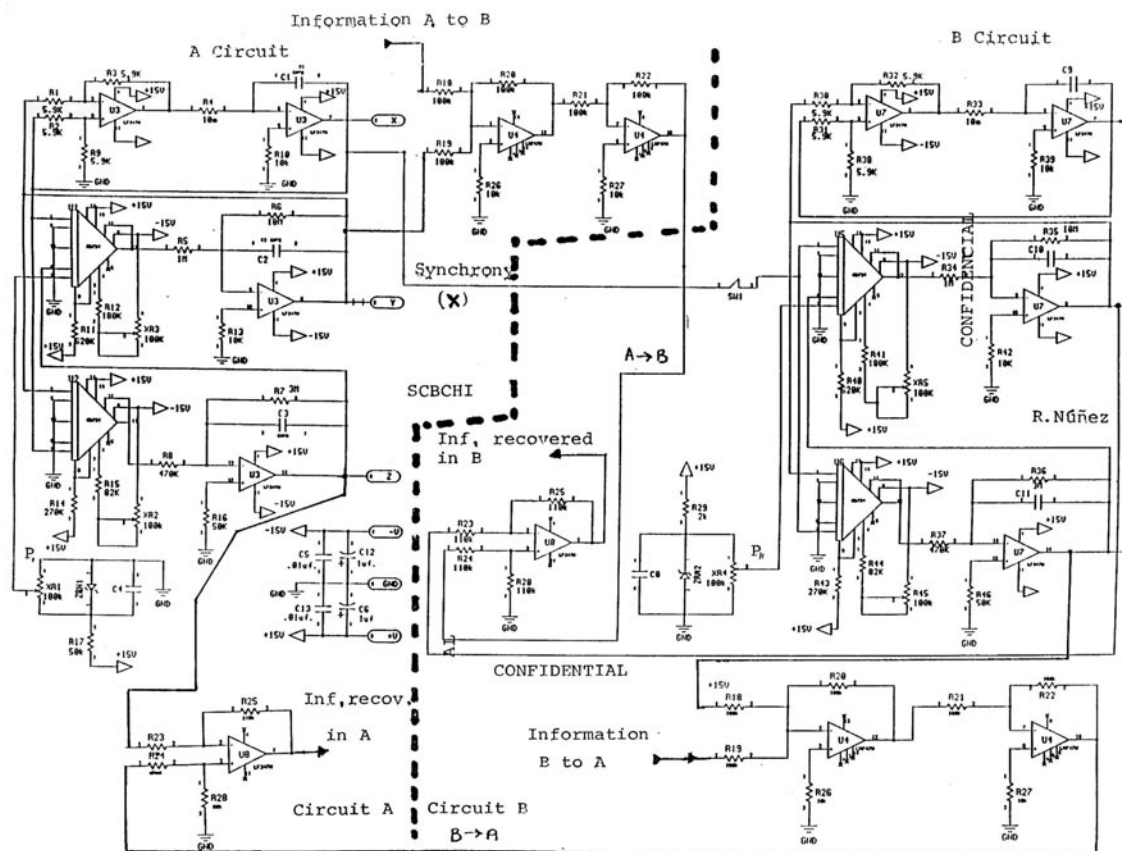

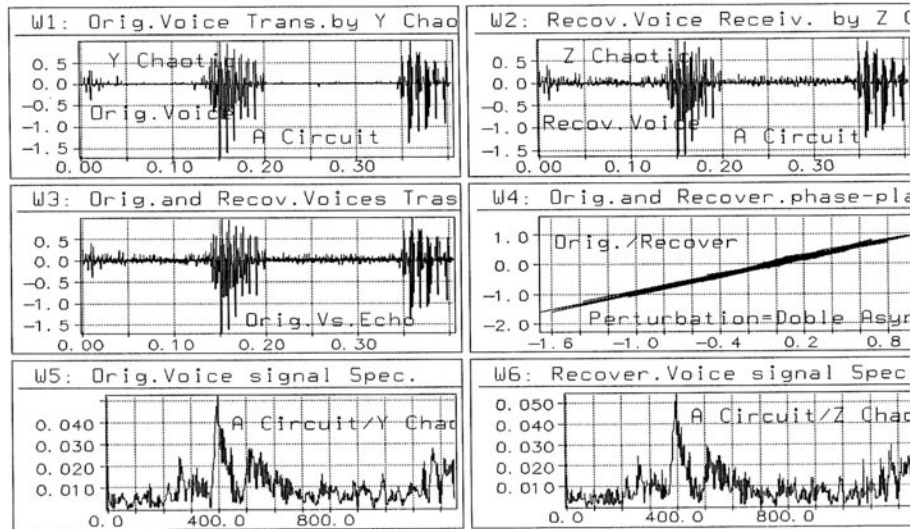*Figure 15. The SCBCHI circuit diagram.*

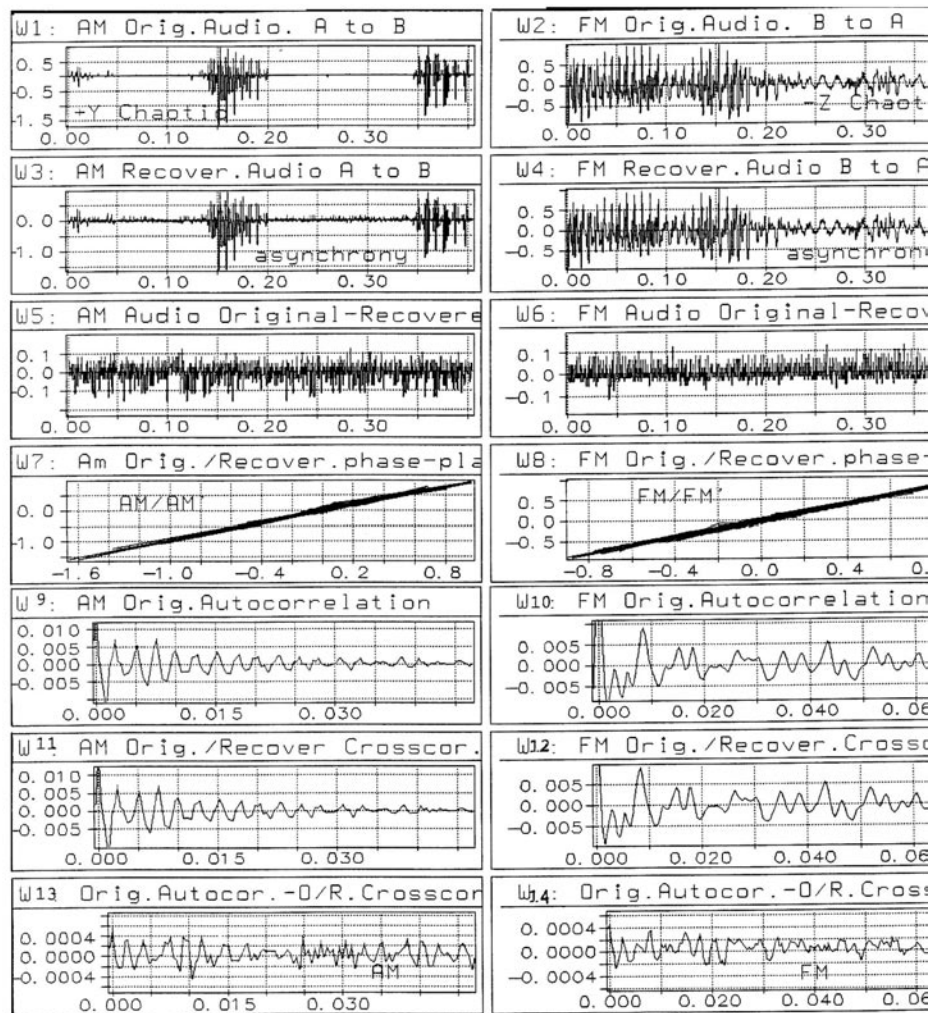Figure 16. Autotesting the SCBCHI using voice echo signals.

Figure 17. Hidden and recovered of bidirectional audio AM/FM information.
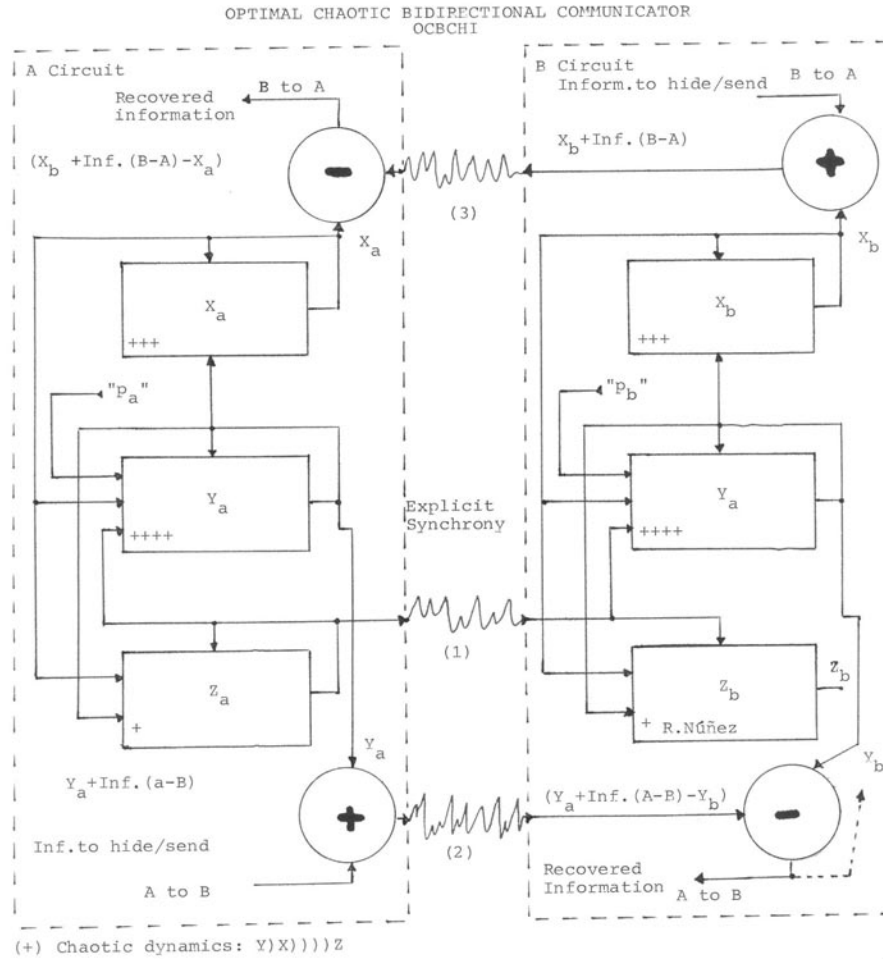
18

Figure 18. The Optimal Chaotic Bidirec, Commun, for hidden Inf. (OCBCHI), using SLC´s.

6. SCBCHI conversion in the Optimal Chaotic Bidirectional Comunicador for Hidden Information (OCBCHI)

Based on the whole study of their dynamics, the Lorenz variables were chosen to carry out the synchrony (v.g., X variable) and the instantaneous bidirectional communication (v.g., Y variable-going and Z variable-return) of the information with the idea of comparing concealment capacities and recovery of identical information, through the variables with the dynamics chaotic more dissimilar. The going channels and return were characterized in an "echo" or autotesting (i.e., same information but different concealment variables) and in a "telephonics" (i.e., between two independent speakers, at the same time and with different concealment variables) configuration. It was verified fully that the Y variable, -that of more chaotic dynamics-, it turns out to be the most efficient and reliable in the hidden works. To qualify the quality of the results of the SCBCHI, the efficiency and dependability achieved are analyzed in the recovery of the hidden information. To be objective, the prototype was proven with periodics, chaotics, voice and audio signals. In general, the quality of the obtained results is good, however it is possible to optimize them, especially, if we take care that the information to hide presents a Spectral Shape Factor (SSF) whose magnitude is at least twice bigger than the asynchrony, or synchrony error, and that it is smaller as many times as possible, of the magnitude of the masking chaotic signal, as well as that its spectrum is contained, entirely, in one of this last. This is due to the fact that spectrum of the chaotic signals is not plane neither monotonics, -but very brittle and with low levels-, since the finite number of frequencies that integrate it are non-linearly excited. Those low levels, can reveal some harmonics of the hidden information signal. It is convenient to mention that the asynchrony registered is coherent with the chaotic dynamics of the variables that produce it.

As a manner of conclusion, in figure 18, the details are described to take care of transforming the **SCBCHI** into one Optimal Chaotic Bidirectional Comunicador for Hidden Information, or **OCBCHI**. The less chaotic variable (Z) should be used, to establish the Circuits synchrony, and the most chaotics variables (Y and X), to hide the information, according to the wanted relative degree of dependability. The biggest degree presents the Y variable. From the frequency point of view, it exists a SSF that should respect the information to be hidden, i.e., the magnitude of this should be bigger than that of the asynchrony but much smaller than that of the Y or X masking chaotics signals. Also, its bandwidth should be equal or smaller to that of the regarding chaotics signals.

For the Private Communication applications, it is very necessary to know the chaotic and periodic dynamics, in the time and in the frequency, of the masking chaotic and the information to hide signals. For the last one, we should make sure that the established SSF works fine, for it is necessary to process this information signal with AGC's Circuits, which should take charge of maintaining the amplitude, bigger than that of the asynchrony and below than that of the masking chaotic signal.

Through their electromechanical analogies, the implemented **SCBCHI** and **OCBCHI** can be applied in the industrial processes of mixed, sanded, loosened, cleaned, etc. These processes could be continuos, or intermittent, depending on the "Chaotic Logic State" that keeps the Rayleigh parameter in each one of the **LCS's**.
It is convenient to mention that the present work, was carried out and it will continue being carried out to support: the laboratory of the Methods of Communications by Chaotics Signals course (**ET807**), and the diverse investigation topics and the master and doctorate thesis related.

7. ACKNOWLEDGEMENT

8. REFERENCES

[1] Núñez P., R., "Implementation and testing of one Chaotic Bidirectional Communicator for Hidden Information, based on two Synchronized Circuits of Lorenz", Technical Report: UET588, DET-CICESE, September, 2000.
[2]   Lorenz E. N., "Deterministic nonperiodic flow", J. Atmospheric Sci., vol. 20, pp. 130-141. Mar., 1963.
[3] Márquez, A. and Alvarez G., J., "Circuit of Lorenz". Technical Report. CICESE, 1996.
[4] Núñez P., R., "The Labview (Generator/Dynamic Analyzer) and Dadisp ATS's". Confidential Technical Reports, DET-CICESE, 1998.
[5] Núñez P., R., "Applications of the DSP in the modern instrumentation using the Dadisp and Labview programs". DSP Institutional course Notes-EP631, DET-CICESE, 1998.
[6] Cuomo, K.M., Oppenheim, A.V. and Strogatz, S.H., "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications". IEEE Trans. on Circuits and Systems-II: Analog/ Digital and Signal Processing, vol. 40, N. - 10, October, 1993.
[7] Carroll, T.L. and Pecora, L.M., "Synchronizing chaotic circuits", IEEE Trans. on Circuits and Systems, vol. 38, pp. 453-6, Apr., 1991.

Note: A partial version of this work was presented as a poster in the 6th Experimental Chaos Conference Postdam, Germany, July 22-26, 2001

Author Byography

Ricardo F. Núñez Pérez

M.Sc. in Electronics and Instrumentation (1987), CICESE, México, and B.Sc. in Electronic Engineering (1980), UABC, México (Honors at both degrees). Since 1987 until now, he is a faculty member of Electronics & Telecommunications Department, CICESE Research Center. He was recipient of the First Prize at the National Contest on Design of Electronics. Equipment Applied to Electric Sector by IIE, CONACYT, SEP and CFE (1988, 1990). Research Areas: Electronics Instrumentation Development for Chaotic Circuits Studies and Applications, and Vibrations and Chaotics Signals DSP Applications.