

Evaluando las sincronizaciones sin y con retroalimentación en circuitos de Lorenz

R. Núñez

*Electrónica y Telecomunicaciones-Centro de Investigación Científica y de Educación Superior de Ensenada,
Km.107, carr. Tj.-Eda., Eda., B.C., México,
Tel/Fax (646)175-0500/554,
e-mail: rnunez@cicese.mx*

Recibido el 10 de agosto de 2010; aceptado el 11 de noviembre de 2010

Dado que la sincronización es primordial para el envío de información privada por medio de encriptamiento caótico y de conmutación paramétrica, el presente describe un estudio experimental que, sobre dos esquemas de sincronización llamados sin y con retroalimentación, se realiza utilizando como fuente generadora de caos al circuito de Lorenz. La idea es conocer cuál es el más eficiente y robusto para aplicarlo en encriptamiento caótico. Se implementan los circuitos transmisor y receptor en forma muy semejante y se trabajan en condiciones casi idénticas de operación. Se considera una variación lineal del parámetro de Rayleigh para conocer los errores en las sincronizaciones y las alteraciones que registran las dinámicas caóticas de los circuitos. Para ello, se utilizan planos de fase, análisis espectral y de coherencia. Finalmente, la sincronización con retroalimentación presenta un mayor error en la sincronía, disminuye la dinámica caótica, y las capacidades de encriptamiento y recuperación de la señal de información se ven muy comprometidas; aunado a que requiere de una conexión física más. Por lo que es menos eficiente que la sincronización sin retroalimentación, aunque para ésta se necesita realizar más experimentación sobre el comportamiento ante ruido eléctrico, e inestabilidades de los componentes para proponerla en aplicaciones reales de encriptamiento caótico.

Descriptores: Circuito de Lorenz; sincronización de circuitos caóticos; encriptamiento caótico.

Since the synchronization is essential for sending private information through chaotic encryption and parametric commutation, the paper describes an experimental study, on two synchronization schemes namely: without and with feedback, is performed using as a chaotic source the Lorenz circuit. The idea is to know the most efficient and robust for application in chaotic encryption. Transmitter and receiver circuits are implemented in a very similar way and worked in almost identical conditions of operation. It is considered a linear variation of the Rayleigh parameter to find the errors in the synchronization and the chaotic dynamics alterations of the circuits. To do this, we use phase planes, spectral analysis and coherence. Finally, synchronization with feedback has a higher synchronization error, decreases the chaotic dynamics and encryption capabilities and information signal retrieval are very committed; together requiring a physical connection more. It is less efficient than the synchronization without feedback, although for the latter further experimentation is needed on the behavior regarding to electrical noise, and instabilities of the components to come in real applications of chaotic encryption.

Keywords: Lorenz circuit; chaotic circuits synchronization; chaotic encryption.

PACS: 05.45.Vx; 05.45.Xt; 05.45.Gg.

1. Introducción

Los métodos teórico-experimental que más se citan en la actualidad para enviar mensajes encriptados por señales caóticas, a nivel laboratorio, según lo manifiestan Cuomo *et al.* [1], Carroll y Pecora [2] y Núñez [3] son: mezclando la señal caótica con la de información, o enviando la primera, cuya forma de onda se genera por un parámetro que atiende a un estado binario que se desea ocultar. Lo interesante es que la efectividad de ambos métodos requiere y depende de la sincronización de los circuitos, *i.e.*, de un circuito caótico transmisor que sincronice a otro idéntico receptor y que permanezcan así durante todo el proceso de envío del mensaje oculto [4,5,6,7]. En este sentido, el presente estudio comparativo muestra, experimentalmente, el comportamiento de la sincronización cuando ésta se aplica a dos circuitos idénticos de Lorenz configurados bajo los esquemas llamados sin y con retroalimentación. La idea es averiguar si la retroalimentación eficientiza y robustece la sincronización de los circuitos, para así proponer este esquema en aplicaciones de encriptamiento caótico [8,9,10].

La sincronización sin retroalimentación es uno de los esquemas más empleado y fue propuesto por Carroll y Pecora [2]. Mientras que éste sólo utiliza la señal X_t del circuito transmisor para sincronizar al receptor, la sincronización con retroalimentación que se propone, utiliza la señal X_r del circuito receptor para retroalimentarla al transmisor; aparte de emplear la señal X_t mencionada del circuito transmisor. Los esquemas se obtienen realizando las conexiones: 1a-2a-2b y 1a-2b/1b-2a señaladas en la Fig. 1, respectivamente.

En la Sec. 2, se presentan las ecuaciones de Lorenz correspondientes a los circuitos por utilizar y se manifiestan las conexiones por realizar para la selección del esquema de sincronización por evaluar: sin y con retroalimentación. También, se presentan los valores que deben tener los parámetros acondicionadores de las dinámicas de los circuitos y las condiciones de medición y prueba.

En la Sec. 3, se describen las comparaciones experimentales entre las sincronizaciones, bajo condiciones semejantes de operación, en base a las mediciones y cálculo de sus errores porcentuales máximos instantáneos en el tiempo y en la frecuencia, con la idea de cuantificar y decidir cual esquema

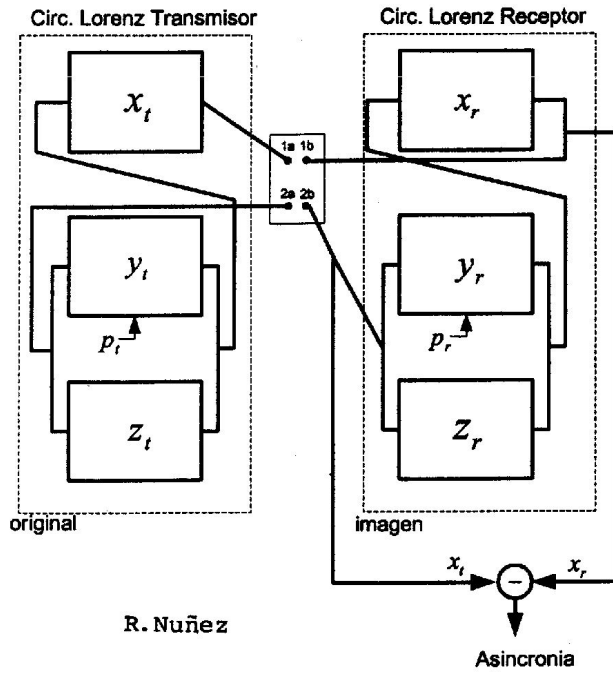


FIGURA 1. Diagrama a cuadros de los circuitos transmisor y receptor de Lorenz mostrando las conexiones para los esquemas de sincronización sin (1a-2a-2b) y con (1a-2b y 1b-2a) retroalimentación.

de sincronización es el más eficiente, *i.e.*, aquel que presente el menor error en la sincronía; para lograr lo anterior se utilizan las mediciones instantáneas de las señales X, Y y Z de los circuitos de Lorenz, sus espectros y planos de fase. En la Sec. 4, se despliegan los transitorios de los circuitos de ambas sincronizaciones, en respuesta a una señal de excitación lineal incorporada por medio del parámetro de Rayleigh, con la idea de conocer las dinámicas caóticas de éstas.

En la Sec. 5, se presenta una analogía con un sistema típico y se evalúan los esquemas de sincronización en base a las funciones de transferencia y de análisis de coherencia [12,13]. Se emplea un promedio de 4 firmas espectrales y se describen cualitativamente los errores en las sincronizaciones utilizando información de la coherencia entre las armónicas. Finalmente, la conclusión indica que la sincronización por retroalimentación, para un par de circuitos idénticos de Lorenz, presenta un error mayor en la sincronización, altera la dinámica caótica y, algo que no se esperaba, pierde capacidad para ocultar y recuperar fielmente la señal de información; aunado a estos resultados, este esquema requiere de una conexión física más. Los agradecimientos y las referencias bibliográficas más relevantes se presentan en las Secs. 6 y 8, respectivamente.

2. Las ecuaciones de Lorenz para los circuitos sincronizados

Edward Lorenz [11] fue el primero en evidenciar la existencia del caos determinístico, *i.e.*, aquel que es desordenado e impredecible pero a su vez también es acotado o finito. El

sistema que utilizó consta de tres ecuaciones diferenciales ordinarias que dedujo como una simplificación de las ecuaciones diferenciales parciales desarrolladas para modelar la convección térmica en la capa atmosférica inferior. A partir de la publicación del trabajo de Lorenz, su modelo ha sido uno de los más utilizados para probar las ideas relacionadas con la dinámica no lineal. En especial, porque las ecuaciones de éste se pueden implementar con circuitos electrónicos sencillos y a través de sus parámetros se puede obtener una descripción muy completa de su dinámica, como se muestra a continuación.

Las ecuaciones de Lorenz para el circuito sincronizado sin retroalimentación [4,8] son:

Círculo transmisor (t: original)

$$\begin{aligned} X_t &= -s \int (X_t - Y_t)dt, \\ Y_t &= -\int [X_t(Z_t - p/10)dt + f Y_t dt], \\ Z_t &= -\int [Y_t(-X_t)dt + b \int Z_t dt], \end{aligned} \tag{1}$$

Círculo receptor (r: imagen)

$$\begin{aligned} X_r &= -s \int (X_r - Y_r)dt, \\ Y_r &= -\int [X_t(Z_r - p/10)dt + f Y_r dt], \\ Z_r &= -\int [Y_r(-X_t)dt + b \int Z_r dt]. \end{aligned}$$

Sincronización vía la señal de acoplamiento del transmisor: **X_t**.

Las ecuaciones de Lorenz para el circuito sincronizado con retroalimentación [4,8,9] son:

Círculo transmisor (t: original)

$$\begin{aligned} X_t &= -s \int (X_t - Y_t)dt, \\ Y_t &= -\int [X_r(Z_t - p/10)dt + f Y_t dt], \\ Z_t &= -\int [Y_t(-X_r)dt + b \int Z_t dt], \end{aligned} \tag{2}$$

Sincronización vía la señal de acoplamiento del receptor: **X_r**.

Círculo receptor (r: imagen)

$$\begin{aligned} X_r &= -s \int (X_r - Y_r)dt, \\ Y_r &= -\int [X_t(Z_r - p/10)dt + f Y_r dt], \\ Z_r &= -\int [Y_r(-X_t)dt + b \int Z_r dt], \end{aligned}$$

Sincronización vía la señal de acoplamiento del transmisor: **X_t**, donde los parámetros s, b y p corresponden a los números de Prandtl, geométrico y Rayleigh, respectivamente. Los dos primeros son puestos en 10 y 2.7, respectivamente, mientras que, el tercero, se coloca en 39 (*i.e.*, en 3.9 Vc.d.), para cada juego. De Núñez [4], se obtiene el valor óptimo de éste para que provoque una mayor dinámica caótica en los circuitos realizados para este estudio. Las variables correspondientes a las señales de acoplamiento o de sincronización **X_t** y **X_r** aparecen en **negritas** en las Ecs. (1) y (2).

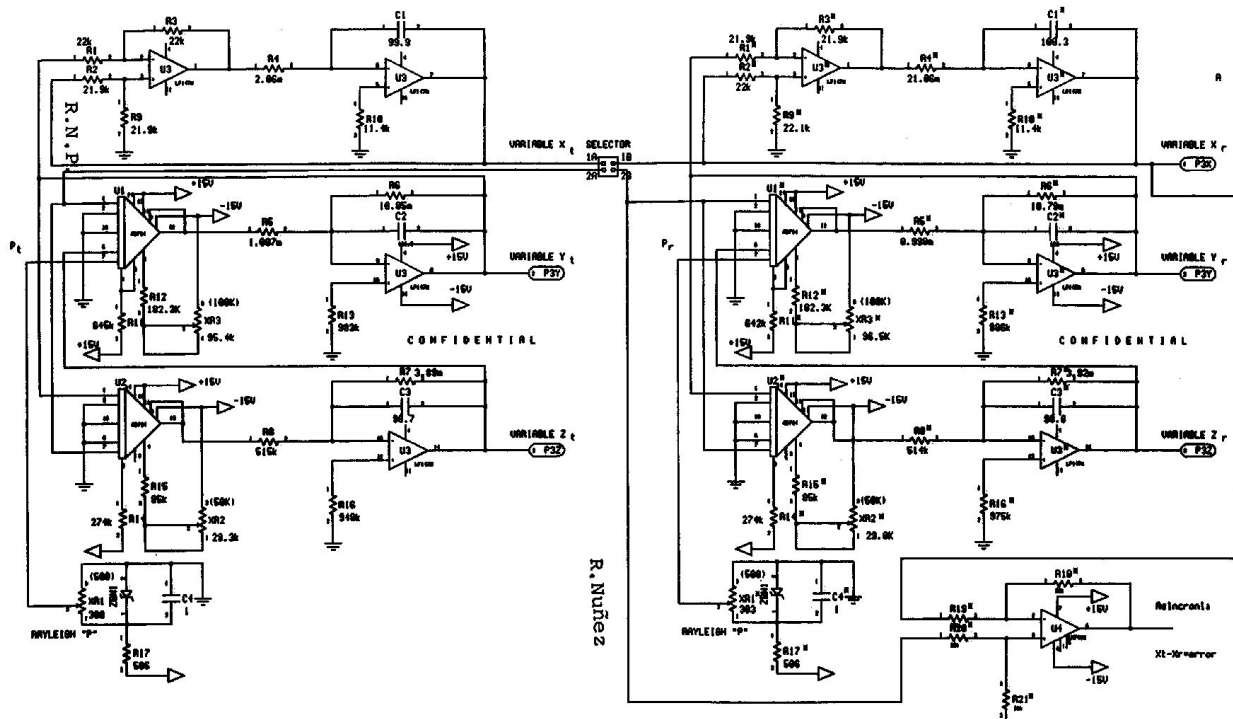


FIGURA 2. Circuito electrónico del transmisor y receptor de Lorenz mostrando las conexiones para los esquemas de sincronización sin (1a-2a-2b) y con (1a-2b y 1b-2a) retroalimentación.

2.1. Las condiciones de prueba para los circuitos de Lorenz sincronizados

Se trabaja con mediciones instantáneas de las señales de los circuitos transmisor y receptor de Lorenz, bajo los esquemas de sincronización llamados sin y con retroalimentación como lo indican las conexiones: 1a-2a-2b y 1a-2b/1b-2a en el diagrama a cuadros de la Fig. 1, respectivamente. Esto significa que, para el primer esquema, sólo se utiliza la señal X_t del circuito transmisor para sincronizar al receptor, mientras que para el segundo, se retroalimenta la señal X_r del circuito receptor al transmisor, además de mantener la señal ya mencionada para el primero. Esta simetría asegura que la trayectoria eléctrica (i.e., el retardo) que recorre cada señal de acoplamiento o sincronización sea equivalente.

Los circuitos electrónicos del transmisor y receptor de Lorenz que se construyeron y probaron se presentan en la Fig. 2. Se implementan lo más parecido posible y se hacen trabajar bajo condiciones muy similares, con la idea de que sus características estáticas y dinámicas, y de estabilidad se comporten lo más semejantemente posible durante las pruebas a los esquemas de sincronización (v.g., la diferencia promedio entre los valores ideales y medidos de los componentes de los circuitos mencionados es de aproximadamente el 0.4%).

Se utiliza el Sistema Automático de Prueba-Dadisp, SAP-Dadisp [12], para asegurar precisión y confiabilidad en las mediciones y análisis digital de las señales caóticas. Se cuidan todos los aspectos necesarios para lograr una buena digitalización (v.g., se utilizan apropiados: número de muestras, frecuencia de muestreo y número de bits de resolución en la

amplitud) y despliegue espectral (v.g., se utilizan apropiados: número de muestras, frecuencia de muestreo y tipo de ventanas) de las señales mencionadas.

3. Comparación entre las sincronizaciones sin y con retroalimentación bajo condiciones idénticas de operación

En la Fig. 3, en las ventanas W1-W2 y W3-W4, se presentan las mediciones instantáneas de las señales X_t y X_r para las sincronizaciones sin y con retroalimentación, respectivamente. En las ventanas W5-W6 y W7-W8, se despliegan el error porcentual máximo instantáneo temporal de la sincronización (v.g., $\%et = (X_t - X_r)100\% / X_t(\text{máx})$) [14] y el plano de fase X_t/X_r para cada una de las sincronizaciones, respectivamente. En las ventanas W9-W10 y W11-W12, se presentan las magnitudes lineales de los espectros E_t y E_r de las señales X_t y X_r , para las sincronizaciones mencionadas; los espectros presentan un alcance de 0 a 3250 Hz. Finalmente, en las ventanas W13-W14 y W15-W16, se despliegan el error porcentual máximo instantáneo frecuencial en la sincronización (v.g., $\%ef = (E_t - E_r)100\% / E_t(\text{máx})$) y el plano de fase de los espectros E_t y E_r para cada una de las sincronizaciones.

Se reporta el resumen de resultados en la Tabla I, i.e., los errores porcentuales máximos instantáneos en las sincronizaciones, tanto para el tiempo (%et) como para la frecuencia (%ef). Valores máximos en **negritas**. Si el % de error es negativo significa que el valor de referencia o señal del transmisor (X_t) es menor que el de la señal generada en el receptor (X_r) [14].

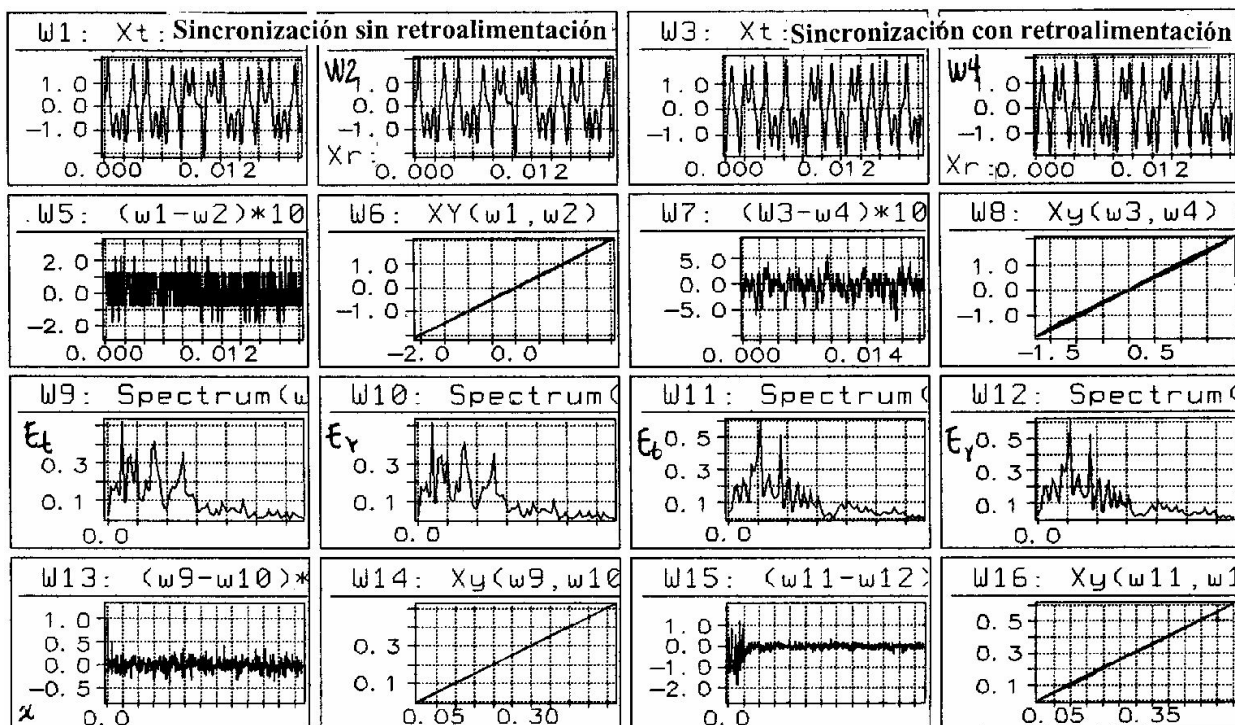


FIGURA 3. Ventanas mostrando las señales X_t y X_r , el error de sincronización ($X_t - X_r$), los planos de fase (X_t/X_r), los espectros E_t y E_r , el error de sincronización ($E_t - E_r$), y los planos de fase (E_t/E_r) para los esquemas de sincronización sin y con retroalimentación.

TABLA I. Error porcentual instantáneo en tiempo y en frecuencia para cada sincronización.

	[sincronización]	
(X_t/X_r)	[sin retroalimentación]	[con retroalimentación]
[% error]		
[%et]	2.20 / -1.70	5.40 / -7.20
[%ef]	0.90 / -0.41	1.20 / -1.90

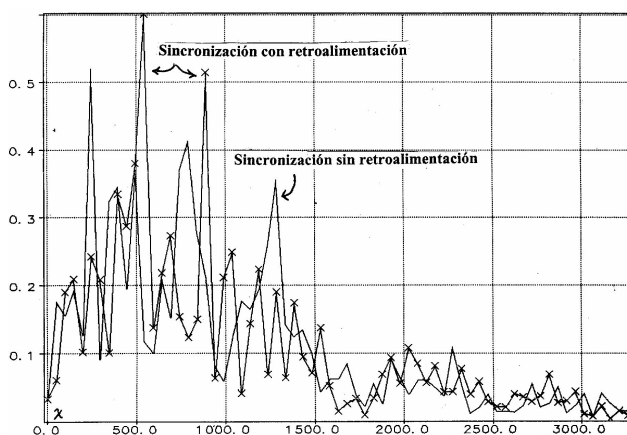


FIGURA 4. Espectros de X_t traslapados para las sincronizaciones sin retroalimentación y con retroalimentación (con cruces). Observe como varía la magnitud de algunas armónicas.

Las desviaciones porcentuales de la Tabla I, calculadas para cada sincronización, indican que para el parámetro de Rayleigh de 3.9 Vc.d. [4], en los circuitos transmisor-

receptor, la sincronización con retroalimentación resulta menos eficiente, puesto que sus errores son mayores a los de su contraparte. Estos mismos, también se manifiestan cualitativamente en los planos de fase temporal (X_t/X_r) y frecuencial (E_t/E_r) mostrados en las ventanas W6 y W14 y W8 y W16 de la Fig. 3, respectivamente. En la Fig. 4, se presentan los espectros traslapados de la señal caótica X_t correspondientes a los esquemas de sincronización con retroalimentación (con cruces) (*i.e.*, la ventana W9 de la Fig. 3) y sin retroalimentación (*i.e.*, la ventana W11 de la Fig. 3). Si comparamos sus firmas espectrales podemos observar que algunas armónicas, del esquema de sincronización sin retroalimentación, fueron atenuadas (*v.g.*, las de 250, 760, 1100 y 1200 Hz) y amplificadas (*v.g.*, las de 480, 510, 800, 1000 y 1010 Hz) [15]. Lo que se puede explicar de la manera siguiente: al retroalimentar la señal X_r , del circuito receptor al transmisor, el acoplamiento transmisor-receptor cambia puesto que ahora ambos circuitos pasan de una sincronización unilateral [2] a una bilateral o de autosincronización; esto acarrea que la dinámica caótica, del esquema con retroalimentación, se vea alterada y tienda a decrecer con respecto a la del sin retroalimentación.

4. Comparación entre los transitorios de ambas sincronizaciones en atención a una excitación lineal del parámetro de Rayleigh

Se presentan en las ventanas W1 y W2 de la Fig. 5, el comportamiento de las señales caótica transitoria X_t y excitadora p del parámetro de Rayleigh (*i.e.*, una señal diente de sierra),

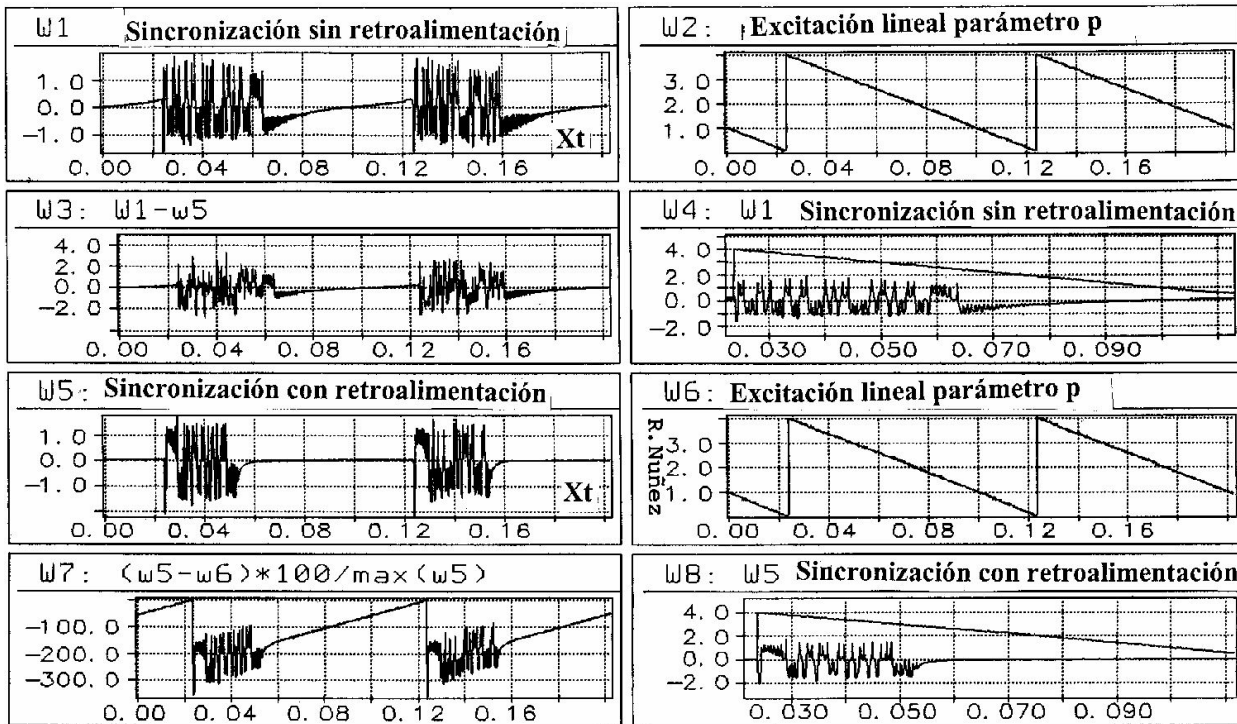


FIGURA 5. Las ventanas W4 y W8 despliegan la evolución de la señal X_t en respuesta a una diente de sierra que excita al parámetro p de Rayleigh en los esquemas de sincronización sin y con retroalimentación. En W8 se observa que el estado caótico se encuentra más comprometido.

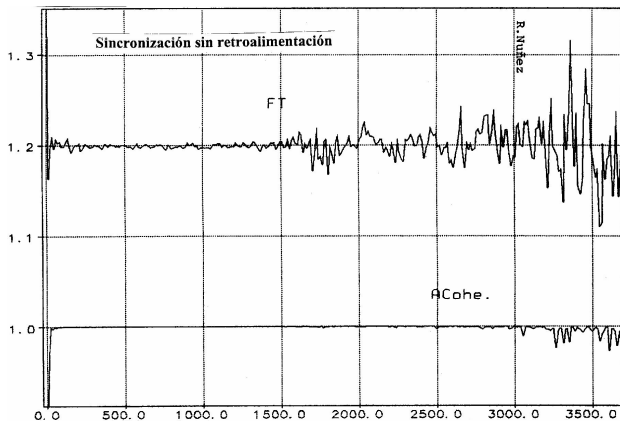


FIGURA 6. Función de transferencia de la señal de entrada X_t y salida X_r (X_t/X_r) y el análisis de coherencia para un promedio de 4 espectros de E_t y E_r , para la sincronización sin retroalimentación. Las armónicas en la vecindad de 3500 Hz manifiestan el error en este esquema de sincronización.

respectivamente. De Núñez [4], se escoge la señal diente de sierra para excitar el parámetro mencionado porque es la que provoca que el circuito de Lorenz despliegue un ciclo dinámico completo (*i.e.*, que su operación pase de régimen estático a dinámico y de nuevo a estático). De la ventana W1 a la W4 y de la W5 a la W8, se presentan los esquemas para las sincronizaciones sin retroalimentación y con retroalimentación, respectivamente. En la ventana W4, se despliega el traslape entre el transitorio sin retroalimentación y su señal

excitadora p . En las ventanas W5, W6 y W8, se presenta el comportamiento transitorio de la sincronización con retroalimentación, su señal excitadora p y el traslape entre el transitorio de la sincronización con retroalimentación y su señal excitadora p , respectivamente. Comparando la evolución de la señal caótica X_t que se presenta en las ventanas W4 y W8, se observa que la duración de la señal transitoria para cada esquema es diferente. Para el que más interesa, el de la sincronización con retroalimentación, la entrada del circuito al estado caótico tarda más, se mantiene menos en éste, y al salir del mismo lo hace más rápidamente que el de su contraparte. Esto trae como consecuencia que este esquema sea más sensible a cambios en el parámetro p , lo que compromete el estado caótico de X_t y aumenta el error de sincronización.

5. Los errores de sincronización manifestados por las funciones de transferencia y de análisis de coherencia para una relación entrada/salida (X_t/X_r)

Se considera al esquema de sincronización en general como un sistema típico con una entrada y una salida, en el cual la entrada es la señal de sincronización X_t y la salida es la sincronizada X_r . Se obtienen los auto-espectros promedio de las señales de entrada X_t ($A_{E_p}X_t$) y salida X_r ($A_{E_p}X_r$), y el espectro-cruzado promedio entre las señales de entrada X_t y salida X_r (ECX_{p_t-r}), respectivamente, para el esquema de

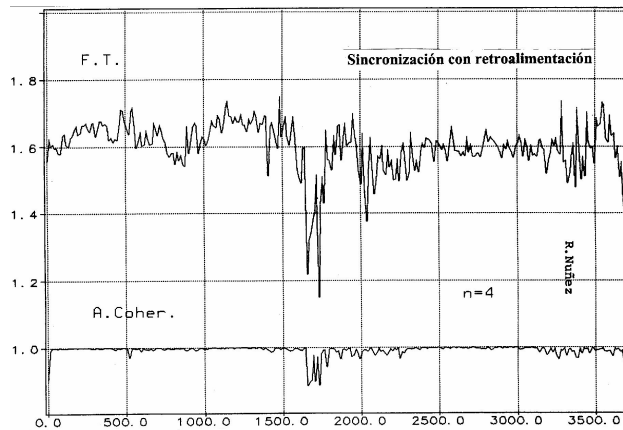


FIGURA 7. Función de transferencia de la señal de entrada X_t y salida X_r (X_t/X_r) y el análisis de coherencia para un promedio de 4 espectros de E_t y E_r , para la sincronización con retroalimentación. Las armónicas en las vecindades de 1750 Hz y de 3500 HZ manifiestan el error en este esquema de sincronización.

la sincronía sin retroalimentación. Los espectros promedio se calculan de una serie de 4 espectros de potencia obtenidos de la pareja de señales X_t y X_r , las cuales fueron medidas instantáneamente y en fase. Se obtienen la potencia promedio (v.g., $P_p = (AEX_{pt}) (AEX_{pr}) 0.5$), la función de transferencia (v.g., $FT = ECX_{pt-r} / AEX_{pt}$) y la función análisis de coherencia (v.g., $FAC = (ECX_{pt-r})^2 / ((AEX_{pt}) (AEX_{pr}))$) [12,13], para el esquema de sincronización estudiado. La FAC califica las armónicas de la señal de salida X_r que fueron excitadas, o generadas, por las armónicas de la señal de entrada X_t , si son idénticas significa que no hay error en la sincronización. Los resultados son de carácter cualitativo, i.e., si se desea mayor precisión es necesario promediar más espectros (v.g., 16 o más). En la Fig. 6, se presentan con mayor detalle las funciones antes mencionadas, y de las cuales se observa que la señal de salida X_r se excita, casi por completo, por la de entrada X_t ; esto se realiza desde las componentes de frecuencia muy baja hasta las cercanas a los 3750 Hz. A partir de la frecuencia de 3250 Hz, la FAC indica que existen ciertas armónicas con baja coherencia y las cuales representan los errores en la

sincronía para el esquema de sincronización sin retroalimentación. Como en la Fig. 6, en la 7, se presenta el esquema de la sincronización con retroalimentación y se observan con mayor detalle las zonas de baja coherencia; una alrededor de los 1750 Hz y otra alrededor de los 3250 Hz (i.e., parecida al de la sincronización sin retroalimentación); donde ambos grupos de frecuencias manifiestan el error en la sincronización y, como era de esperarse, éste resulta mayor que el del primer esquema. Con estos resultados se corroboran los reportados en la Tabla I obtenidos en la Sec. 3; producto de la retroalimentación, la eficiencia en la sincronización de los circuitos transmisor y receptor disminuye.

6. Conclusiones

La utilización de la sincronización con retroalimentación, en un par de circuitos idénticos de Lorenz, presenta un mayor error en la sincronía y tiende a disminuir la dinámica caótica al compararse con la de su contraparte, la sincronización sin retroalimentación; aunado a que la primera requiere de una conexión física extra. Estos resultados se pueden apreciar al ver cómo se altera la forma de onda y cómo se abaten algunas armónicas; esto, al final de cuentas, limita considerablemente la capacidad de ocultamiento y recuperación fiel de las señales de información. Los resultados son representativos y reproducibles, ya que son validados por la función de análisis de coherencia y se cuida su buena precisión y confiabilidad. Se requiere seguir experimentando sobre el comportamiento de los circuitos sincronizados sin retroalimentación ante ruido eléctrico intrínseco y extrínseco e inestabilidades de los componentes para proponerlos en aplicaciones reales de encriptamiento por medio de señales caóticas.

Agradecimientos

Agradecemos al CONACYT por apoyar económicamente el presente, a través del proyecto: 7453, dirigido por el Dr. J. Álvarez G.

1. K.M. Cuomo, A.V. Oppenheim y S.H. Strogatz, *IEEE Trans. on Circuits and Systems., II: Analog/ Digital and Signal Processing* **40** (1993).
2. T.L. Carroll y L.M. Pecora, *IEEE Trans. on Circuits and Systems* **38** (1991) 453.
3. R. Núñez, *An optimal chaotic bidirectional communicator based on synchronized Lorenz circuits* (Process. of 6th. Experimental Chaos Conference, July 22-26, Postdam, Germany, 2001).
4. R. Núñez, *Rev. Mex. Fís.* **52** (2006) 285.
5. I. Campos, E. Campos, J.S. Murguía y M.E. Chavira, *FI-UNAM* **10** (2008) 21.
6. C. Posadas, C. Cruz y R. Núñez, *JART* **2** (2004).
7. O.A. Gonzalez, G. Han, J. Pineda y E. Sánchez, *IEEE Trans. on Circuits and Systems.- I* **47** (2000).
8. R. Núñez, *Rev. Mex. Fís.* **52** (2006) 372.
9. D. López y C. Cruz, *Rev. Mex. Fís.* **51** (2005).
10. K.M. Cuomo, A.V. Oppenheim y S.H. Strogatz, *IJBC* **3** (1993) 1629.
11. E.N. Lorenz, *Deterministic nonperiodic flow J. Atmosph., Sci.* **20** (1963) 130.
12. R. Núñez, "The LabVIEW (Generator/Dynamic Analyzer) and Dadisp ATS's" (Confidentials Technicals Reports, DET-CICESE, 1998).

13. R. Núñez, “Calificación experimental de la sincronía de dos circuitos caóticos” (Congreso internacional XI CLCA’04, La Habana, Cuba, octubre, 2004).
14. ISA, Norma ANSI/ISA-S51.1-1979 (R1993), “*Process Instrumentation Technology*” (1995).
15. R. Núñez, *IEEE-Latin America Transactions* **7** (2009).