Encriptador experimental retroalimentado de Lorenz con parámetros desiguales

R. Núñez
Electrónica y Telecomunicaciones-CICESE,
Km.107, Carretera Tij.-Eda., Eda., B.C. México,
Tel/Fax (646)175-0500/537,
e-mail: rnunez@cicese.mx

Recibido el 20 de abril de 2005; aceptado el 16 de mayo de 2006

Se caracteriza y especifica un circuito encriptador de Lorenz para mostrar experimentalmente que retroalimentando el mensaje y el ruido al transmisor es posible obtener una buena recuperación del primero, pese a que los parámetros de Rayleigh de los circuitos transmisor y receptor sean diferentes hasta en un 10 % y que la magnitud del ruido aleatorio en el canal sea equivalente a la del mensaje. Con este esquema se deja por un lado el requisito impuesto por Carroll y Pecora (1991) que exige que los circuitos por sincronizar sean idénticos. Finalmente, la robustez del encriptador caracterizado indica que puede ser construido con componentes de mayor tolerancia, por lo cual resulta económico e ideal para utilizarlo en la docencia. Se requiere la realización de más estudios sobre el comportamiento del circuito propuesto ante el ruido eléctrico, las inestabilidades propias de sus componentes, etc., para poder utilizarlo confiablemente en aplicaciones reales de envío de mensajes ocultos por señales caóticas.

Descriptores: Circuito de Lorenz; sincronización de caos; retroalimentación del mensaje y ruido; comunicación encriptada.

The Lorenz encrypter circuit is characterized and specified to show experimental confirmation that with message and random noise feedback at the transmitter it is possible to achieve a high quality message recovery, even though of transmitter and receiver Rayleigh parameters have a 10 % of mismatching, and a channel random noise of the same magnitude of the message. This modified chaos-based communication scheme puts away from the Carroll and Pecora (1991) requirement that says that the circuits to synchronize must be identical. In conclusion, the encryption robustness indicates that the proposed scheme can be built with low cost components and therefore could be appropiate to academics purposes. It is need to performance more studies regarding to electrical noise and long time stability for confidentially to use the circuit in real applications for transmission of messages hidden by chaotic signals.

Keywords: Lorenz circuit; chaos synchronization; message and noise feedback; encrypted communication.

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

1. Introducción

Los dos métodos teórico-experimentales que más se citan en la actualidad para enviar mensajes encriptados a nivel laboratorio [1-6] son sumar la señal caótica a la de información o enviar la primera cuya forma de onda sea generada obedeciendo a un valor paramétrico seleccionado por un estado binario que se desea encriptar. Lo interesante es que la efectividad de ambos métodos requiere y depende de la *sincronización* entre un circuito caótico transmisor, original, y otro caótico receptor, copia fiel del primero, y los cuales deben mantenerse sincronizados durante el proceso de envío del mensaje encriptado. En particular, este proceso puede realizarse a través de una o dos líneas de comunicación [1]. En este sentido, Wu (1993) propone la teoría de una sola línea, para realizar la sincronización y el envío del mensaje encriptado *retroalimentando ambas señales al transmisor.* El presente estudio muestra, *experimentalmente*, que el encriptamiento y la recuperación del mensaje es confiable cuando se retroalimenta éste, la señal de sincronía y el ruido aleatorio del canal al circuito transmisor; aun cuando los parámetros de Rayleigh de los circuitos transmisor y receptor sean diferentes [7-10]. Primeramente, en la Sec. 2 se describe el circuito de Lorenz [5,11,12], sus sincronizaciones: [a) natural y b) con retroalimentación del mensaje y del ruido en el transmisor, Fig. 1] y la tipificación de las señales de sincronización/encriptamiento, mensaje y ruido aleatorio. Los circuitos transmisor y receptor de Lorenz, por sincronizar en forma natural, se construyen de manera semejante y se evalúan en condiciones muy similares para que sus características de operación y estabilidad se comporten lo más parecido posible durante las pruebas (según Núñez [5] la diferencia promedio entre los valores medidos de los componentes integrantes de los circuitos es del 0.4 %). Se utiliza la señal caótica X de Lorenz para sincronizar, puesto que es la que presenta la dinámica caótica más apropiada para este estudio [5]. Se posiciona el parámetro de Rayleigh por medio de un voltaje que excita al máximo la dinámica caótica de los circuitos por sincronizar (*i.e.*, se situa en 3.90V c.d., para cada circuito [5]). En la Sec. 3 se describe la caracterización del circuito encriptador bajo las condiciones de: a) encriptado y recuperado de un mensaje de audio ante el ruido aleatorio del canal y los parámetros iguales; b) vía la sincronización implícita según Cuomo [1] con los parámetros iguales; y c) encriptado y recuperado de un mensaje de audio ante el ruido del canal y variaciones considerables del parámetro Rayleigh del receptor. Se utiliza el Sistema Automático de Prueba-Dadisp (SAP-Dadisp) [13-15], para asegurar precisión y confiabilidad en las mediciones y en el análisis digital de las señales caóticas. En la Sec. 4 se evalúan los resultados en la recuperación del mensaje, cuando éste contiene ruido aleatorio del canal y, cuando además de esto, los parámetros de Rayleigh

presentan una diferencia considerable. También en ésta sección se compara el procedimiento con retroalimentación del mensaje y del ruido al transmisor, con el de sincronización implícita propuesto por Cuomo [1] el cual, como se muestra experimentalmente, ya no es competitivo. En esta misma sección se presentan las características y especificaciones del circuito de laboratorio. En la Sec. 5 se concluye que el circuito encriptador presenta una robustez tal que puede permitir que los parámetros de Rayleigh, de los circuitos transmisor y receptor, sean diferentes hasta en un 10 %, y el procedimiento de recuperación siga siendo eficiente, aun cuando exista ruido aleatorio en el canal de una magnitud semejante al del mensaje. Con este esquema, se puede dejar de lado el requisito impuesto por Carroll y Pecora [2] que exige que los circuitos por sincronizar sean idénticos. En ese sentido, los circuitos resultan favorables para utilizarse en la docencia, puesto que se pueden construir con componentes de mayor tolerancia y menor costo.

2. Circuito de Lorenz, sincronización natural y con retroalimentación del mensaje y del ruido

Edward Lorenz 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, limitado 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. El modelo físico que utilizó es simple: se pone un gas sobre una caja rectangular sólida con una fuente de calor al fondo. Se simplifican algunas de las ecuaciones de Navier Stokes de la dinámica de fluidos y al final se consideran sólo tres ecuaciones no lineales. A partir de la publicación del trabajo de Lorenz [9], su modelo y circuito electrónico han sido unos de los más utilizados para probar las ideas relacionadas con la dinámica no lineal.

Los circuitos de Lorenz normalizados, construidos y caracterizados, y que constituyen al encriptador estudiado, se presentan en la Fig. 1, y son una versión simplificada y escalada en la frecuencia de los reportados en Ref. 5. Para su construcción, se utilizan componentes comerciales de bajo costo.

2.1. Sincronización natural

Las ecuaciones de Lorenz para el circuito encriptador sincronizado [5,16] son:

transmisor (t: original)

$$\begin{aligned} Xt &= -s\int(Xt - Yt)dt, \\ Yt &= -[10\int Xt(Zt - \boldsymbol{P}t/10)dt + \int Ytdt], \\ Zt &= -[10\int(Yt(-Xt)dt + b\int Ztdt], \end{aligned} \tag{1}$$

receptor (r: copia)

$$\begin{aligned} Xr &= -s\int(Xr - Yr)dt, \\ Yr &= -[10\int Xt(Zr - \boldsymbol{P}r/10)dt + \int Yrdt], \\ Zr &= -[10\int(Yr(-Xt)dt + b\int Zrdt], \end{aligned}$$

donde los parámetros s, b y ***P*** corresponden a los números de Prandtl (que es la relación entre la viscosidad del fluido y la conductividad térmica) geométrico (que es la relación entre el alto y el ancho de la caja utilizada para el experimento) y de Rayleigh (que es la diferencia de temperatura entre la parte superior y la inferior de la caja) respectivamente. Cabe hacer mención que los parámetros descritos anteriormente son importantes para determinar al sistema caótico. Este mismo sistema de ecuaciones puede emplearse de manera general para otras áreas de la ciencia.

2.2. Sincronización por retroalimentación del mensaje y del ruido en el transmisor

Las ecuaciones de Lorenz para el circuito encriptador sincronizado con retroalimentación del mensaje, m, y del ruido aleatorio, Vr, en el transmisor son [7,16]:

transmisor (t: original)

$$\begin{aligned} Xt &= -s\int(Xt - Yt)dt, \\ Yt &= -[10\int \mathbf{X't}(Zt - \boldsymbol{P}t/10)dt + \int Ytdt], \\ Zt &= -[10\int(Yt(-\mathbf{X't})dt + b\int Ztdt], \end{aligned} \tag{2}$$

receptor (r: copia)

$$\begin{aligned} Xr &= -s\int(Xr - Yr)dt, \\ Yr &= -[10\int \mathbf{X't}(Zr - \boldsymbol{P}r/10)dt + \int Yrdt], \\ Zr &= -[10\int(Yr(-\mathbf{X't})dt + b\int Zrdt], \end{aligned}$$

donde los parámetros s, b y ***P*** corresponden a los números de Prandtl, geométrico y de Rayleigh, respectivamente. Los dos primeros son puestos en 10 y 2.7, respectivamente, mientras que el tercero se coloca en 3.90V c.d. para cada circuito. De Núñez [5] se obtiene el valor de este último para provocar una mayor dinámica caótica en los circuitos construidos. La variable correspondiente a la señal sincronizadora **X't** (se indica por s1 en el diagrama de la Fig. 1) representa el proceso de *retroalimentación* en el transmisor de las señales de: sincronización/encriptadora, Xt (*v.g.*, x1, con amplitud de +/- 2Vp), el mensaje de audio, m (*v.g.*, m(t), con amplitud de +/- 1Vp), y el ruido aleatorio, Vr (*v.g.*, v(t), con amplitud de +/- 180mVp), para cuando los valores de los parámetros de Rayleigh, del transmisor y receptor (*i.e.*, ***P***t y ***P***r), ya fueron definidos y puestos igual por los voltajes Vs1 de cada uno de los circuitos. Las señales mencionadas se presentan, en ese mismo orden, en las ventanas de la W1 a la W3 de la Fig. 2, y con sus espectros, calculados y desplegados en un alcance de 0 a 6 (0.12) Khz se hace lo propio de las ventanas W4 a la W6. En las ventanas W9 y W7, se muestra la forma de onda de la señal **X't** (*i.e.*, **X't**= Xt + m + Vr) y su espectro, respectivamente. Se obtiene la sincronización implícita, definida por Cuomo [1] al enviar al receptor, por una sola línea, las señales de: sincronización/encriptadora, Xt, el mensaje de audio, m, y el ruido aleatorio, Vr, que se incorpora del canal. Para esto, es necesario realizar la conexión de s1 sin la retroalimentación al transmisor (*i.e.*, sólo debe conectarse al transmisor la señal x1, en lugar de la s1 completa como se indica en el diagrama de la Fig. 1).

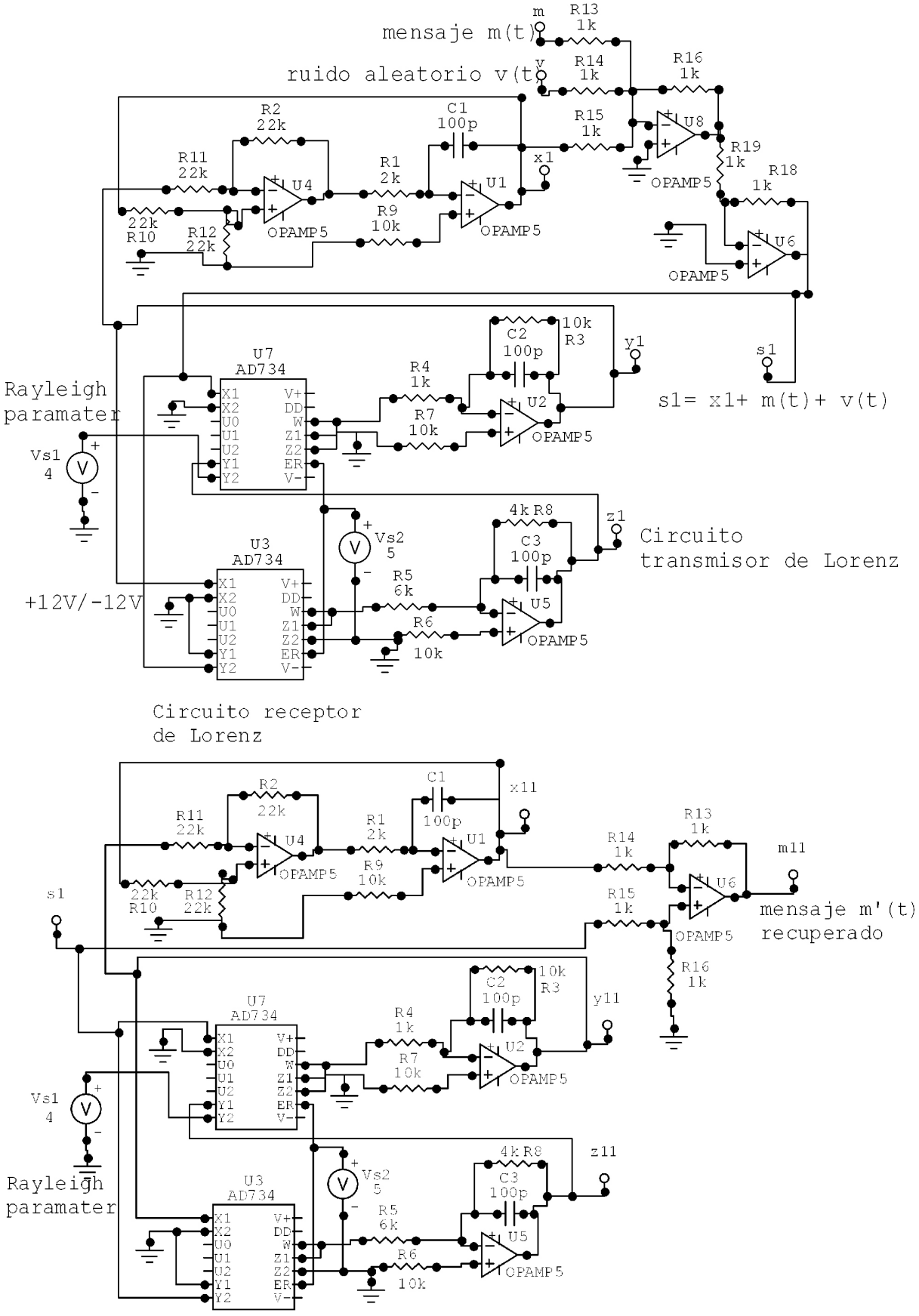

FIGURA 1. Circuito del encriptador de Lorenz que utiliza retroalimentación del mensaje y del ruido aleatorio.

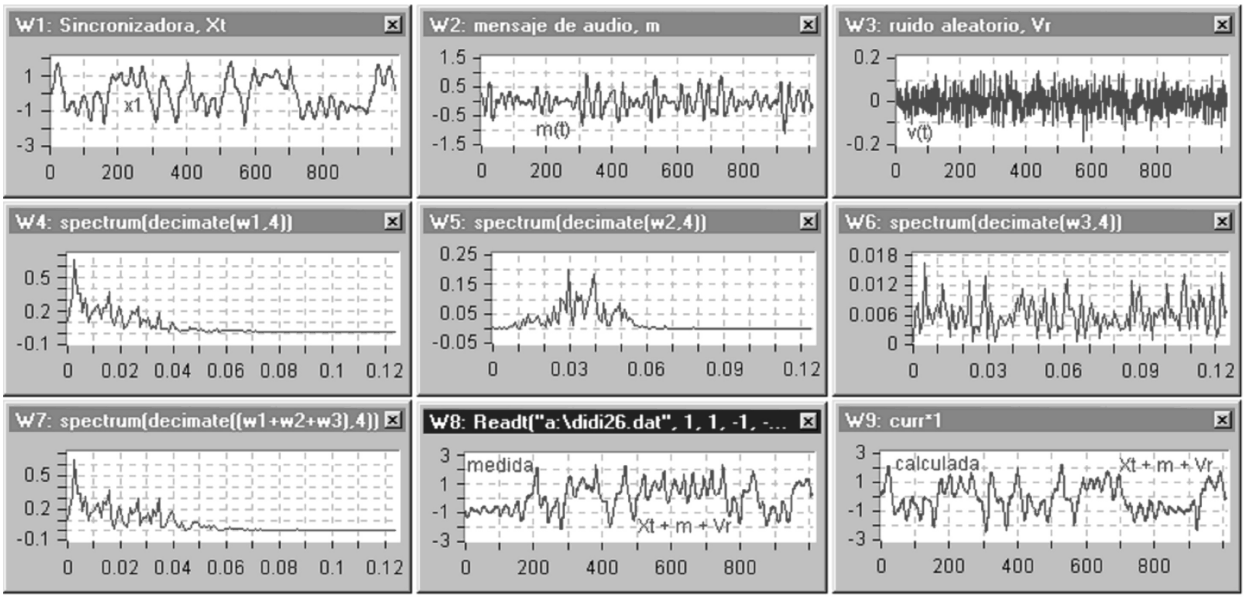

FIGURA 2. Señales independientes: sincronizadora, Xt, mensaje de audio, m, y ruido aleatorio, Vr. Señal encriptadora operando **X't**: calculada (Xt + m + Vr)en la ventana W9 y medida en la ventana W8.

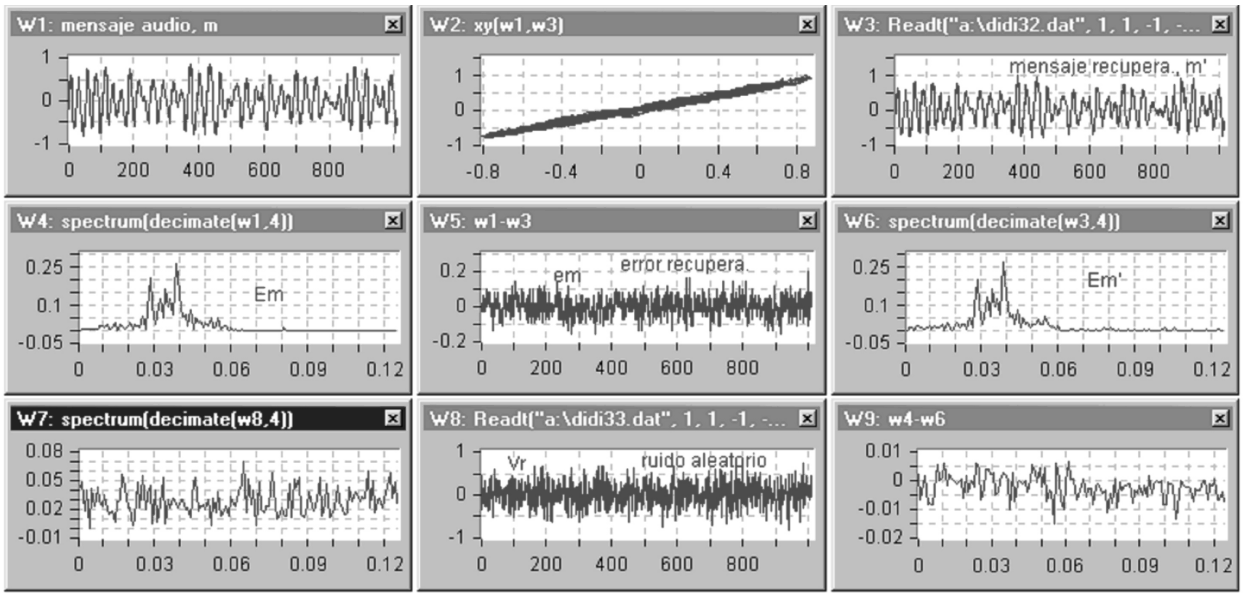

FIGURA 3. Mensaje encriptado de audio, m (W1), con ruido aleatorio incorporado, Vr (W8), y recuperación del mensaje, m' (W3). El encriptamiento y recuperación vía retroalimentación del mensaje y ruido aleatorio es aceptable como lo indica m', en la ventana W3, y el error en la recuperación , em= m-m', en la ventana W5.

3. Caracterización del circuito encriptador

La medición, despliegue, análisis, salvaguarda e impresión de los datos, se basa extensamente en el Sistema Automático de Prueba Dadisp (SAP-Dadisp) [13-15] y para generar el ruido aleatorio se utiliza el generador de ondas diversas Agilent 33210A.

Se describe la caracterización del circuito encriptador con base en las diversas condiciones de operación a las que se somete:

3.1. Encriptado y recuperado de un mensaje de audio ante el ruido del canal y los parámetros iguales

En la Fig. 3, de la ventana W1 a la W6, se presenta el mensaje de audio original de 0.8Vp, m, el plano de fase, m/m', el mensaje de audio recuperado, m', el espectro del mensaje de audio original, Em, el error en la recuperación, em= m-m', y el espectro del mensaje de audio recuperado, Em', respectivamente. En las ventanas W8 y W7, se muestra la señal de ruido aleatorio de 0.8Vp, Vr (puesta a una magnitud aproximada a la del mensaje m) y su espectro, respectivamente. Se

puede observar la semejanza entre las formas de onda y los espectros de las señales de los mensajes de audio, m, y recuperado, m', tanto en el tiempo (*v.g.*, W1 y W3) como en la frecuencia (*v.g.*, W4 y W6). Los parámetros de Rayleigh de los circuitos transmisor y receptor fueron situados en un valor de 3.90V (Vs1) de c.d. para realizar la caracterización mencionada.

3.2. Encriptado y recuperado de un mensaje de audio vía la sincronización implícita según Cuomo [1] con los parámetros iguales

En la Fig. 4, de la ventana W1 a la W6, se presenta el mensaje de audio original de 0.2Vp, m, el plano de fase, m/m', el mensaje de audio recuperado, m', el espectro del mensaje de audio original, Em, el error en la recuperación, em= m-m', y el espectro del mensaje de audio recuperado, Em', respectivamente. En las ventanas W8 y W7, se presentan la señal de ruido aleatorio de 0.03Vp, Vr (puesta a una magnitud muy pequeña respecto a la del mensaje m) y su espectro, respectivamente. Se puede observar que este procedimiento de sincronización no es capaz de recuperar la señal del mensaje de audio original (c.f., ventanas W1 y W3), pese a que las magnitudes del mensaje, m, y del ruido aleatorio, Vr, son muy pequeñas comparadas con la de la señal de sincronización/encriptadora Xt (c.f., ventana W1 de la figura 2). Los parámetros de Rayleigh de los circuitos transmisor y receptor fueron situados en un valor de 3.90V (Vs1) de c.d. para realizar la caracterización mencionada.

3.3. Encriptado y recuperado de un mensaje de audio ante ruido del canal y variaciones considerables entre los parámetros de Rayleigh

En la Fig. 5, de la ventana W1 a la W3, se presenta el mensaje de audio original de 0.5Vp, m, el plano de fase, m/m', y el mensaje de audio recuperado, m', respectivamente. En la ventana W5, se muestra el error en la recuperación del mensaje de audio, em= m-m', y en las siguientes ventanas W4, W6 y W9, se presenta los espectros del mensaje de audio original, Em, del mensaje de audio recuperado, Em', y del error espectral, Em-Em', respectivamente. Finalmente, en las ventanas W8 y W7, se muestran el ruido aleatorio de 0.4Vp, Vr (puesto a una magnitud semejante a la del mensaje m) y su espectro, respectivamente. Para este caso, se observa una muy buena recuperación del mensaje de audio, m' (*v.g.*, W3), pese a que el parámetro de Rayleigh del receptor $\boldsymbol{P}$r (Vs1= 3.5V de c.d.) es 10 % menor al del transmisor $\boldsymbol{P}$t. Ahora,si el $\boldsymbol{P}$r, del receptor, se reduce más del 15 % del $\boldsymbol{P}$t, del transmisor, la distorsión en el mensaje, m', es tal que ya no es posible recuperarlo, puesto que el comportamiento obtenido se asemeja mucho al de la sincronización implícita de la Fig. 4 (c.f., con la ventana W3 de la misma figura).

4. Evaluación de los resultados

Según la ventana W3 de la Fig. 3, la recuperación del mensaje (*i.e.*, m'= Xt + Vr + m - Xr), m', es buena pese a que la magnitud del ruido aleatorio, Vr (c.f., con la ventana W8), es equivalente a la del mensaje de audio original, m (c.f., con la ventana W1), lo que habla bien de la robustez que presenta el circuito encriptador propuesto para cuando el valor de los parámetros de Rayleigh son iguales. Comparando este resultado con los manifestados en la Fig. 4 (correspondientes a la sincronización implícita) para las mismas condiciones paramétricas, podemos decir que este procedimiento no es competitivo puesto que según las ventanas, W5 y W8, que representan el error en la recuperación del mensaje (*i.e.*, em= m-m') y la magnitud del ruido aleatorio, respectivamente, la señal del mensaje recuperado, m', se distorsiona completamente (c.f., con la ventana W3 de la Fig. 4).

Finalmente, el resultado más interesante es el que se obtiene cuando se varía considerablemente el parámetro de Rayleigh del receptor, $\boldsymbol{P}$r (c.f., Vs1 del receptor en la Fig. 1), se decrementa un 10 % de el valor del transmisor, $\boldsymbol{P}$t (*i.e.*, $\boldsymbol{P}$r= 0.9$\boldsymbol{P}$t), como lo indica la Fig. 5. Para el caso, los resultados son prometedores como lo manifiestan las ventanas W5 y W8, que representan el error en la recuperación del mensaje, em, y el ruido aleatorio incorporado, Vr, respectivamente, y sobre todo la señal del mensaje recuperado, m', que se presenta en la ventana W3 de la misma figura. Este resultado es importante puesto que manifiesta *la robustez* experimental del encriptador propuesto ante *el ruido del canal* y ante *la desigualdad entre los parámetros de Rayleigh del transmisor y del receptor*. Esto último, permite que los circuitos puedan construirse con componentes de mayor tolerancia y menor costo, *i.e.*, ya no se requiere que los circuitos sean idénticos ni que los componentes electrónicos sean de gran precisión y estabilidad. Las características y especificaciones del encriptador de Lorenz estudiado se presentan en la Tabla I.

TABLA I. Características y especificaciones del encriptador de Lorenz estudiado.

Señal sincronizadora/encriptadora, Xt	Xt (señal caótica de Lorenz
Mensaje de audio, m	m= 0.2Xt (puede ser menor)
Ruido aleatorio, Vr	Vr= 0.4Xt= 2m (puede ser mayor)
Variación permitida del parámetro de Rayleigh del receptor, $\boldsymbol{P}$r	$\boldsymbol{P}$t(0.90) $\leq \boldsymbol{P}$r $\leq \boldsymbol{P}$t (alcance máximo),

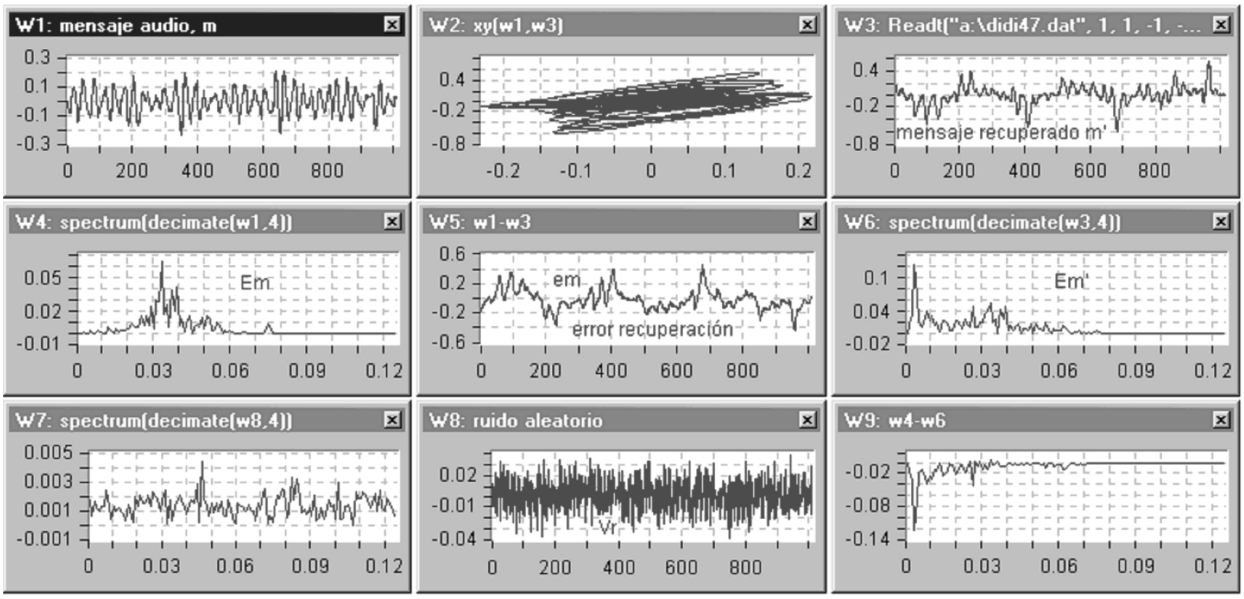

FIGURA 4. Mensajes encriptado de audio, m (W1), con ruido aleatorio incorporado, Vr (W8), y recuperación del mensaje, m' (W3). Encriptamiento y recuperación vía la sincronía implícita según Cuomo *et. al.*, 1993. Procedimiento deficiente como lo indica, m', y el error en la recuperación (em= m-m'), ventanas W3 y W5, respectivamente.

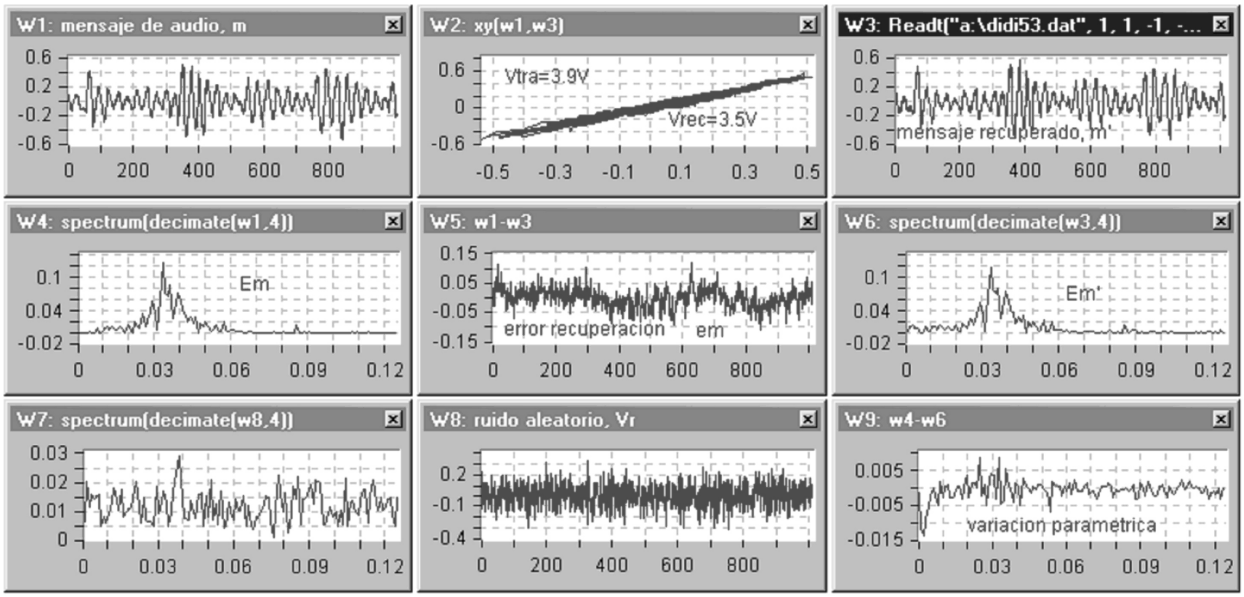

FIGURA 5. Mensaje encriptado de audio, m (W1), con ruido aleatorio incorporado, Vr (W8), y con una variación en el parámetro de *Rayleigh* del receptor del 10 % del Pt (W2). La recuperación del mensaje de audio, m', y el error en la recuperación, em= m-m', son apropiados como lo indican las ventanas W3 y W5, respectivamente.

5. Conclusiones

Se muestra con este encriptador que es posible realizar la sincronía y retroalimentar tanto el mensaje como el ruido aleatorio del canal al transmisor sin que esto afecte considerablemente la recuperación del mensaje, aun cuando los parámetros de Rayleigh de los circuitos transmisor y receptor no sean idénticos y que el ruido aleatorio del canal sea de una magnitud semejante al del mensaje. Se puede mencionar que el circuito de laboratorio caracterizado es robusto ante ruido aleatorio del canal y ante variaciones en los parámetros mencionados, lo que trae como consecuencia que éstos puedan ser diferentes hasta en un 10 % y que la recuperación del mensaje de audio original sea eficiente, pese al ruido aleatorio del canal. El circuito de laboratorio es confiable, de bajo costo, e ideal para utilizarse en docencia, puesto que no requiere componentes electrónicos idénticos ni de gran precisión y estabilidad. Con este esquema, se deja por un lado el requisito impuesto por Carroll y Pecora [2] que exige que los circuitos por sincronizar sean idénticos. Producto de la retroalimen-

tación en el circuito transmisor, el ruido aleatorio se atenúa por el encriptador de *Lorenz* de una manera semejante a la de un filtro paso bajas. Se requiere más trabajo experimental sobre el comportamiento del circuito propuesto ante el ruido eléctrico [17], las inestabilidades propias de sus componentes, etc., para utilizarlo confiablemente en aplicaciones reales de envío de mensajes ocultos por señales caóticas.

Agradecimientos

Agradecemos al CONACYT por apoyar económicamente el presente, a través del proyecto 31874-1 dirigido por el Dr. César Cruz Hernández.

1. K.M. Cuomo, A.V. Oppenheim y S.H. Strogatz, *IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing* **40** (1993).
2. T.L. Carroll y L.M. Pecora, *IEEE Trans. on Circuits and Systems* **38** (1991) 453.
3. N.J. Corron y R. Hans, *IEEE Trans. on Circs. And Systs.- I* **44** (1997).
4. O.A. Gonzalez, G. Han, J. Pineda, y E. Sánchez, *IEEE Trans. on Circs. And Systs.- I* **47** (2000).
5. R. Núñez, *Procs. of 6th. Experimental Chaos Conference*, July 22-26, Postdam, Germany (2001).
6. R. Núñez, *AMCA2003*, Eda., B.C., México (2003).
7. C.W. Wu y L.O. Chua, *IJBC* **3** (1993) 1619.
8. M. Hasler y Th. Schamming, *IJBC* **10** (2000) 719.
9. D. López y C. Cruz, Rev. Mex. Fis. vol. **51** (por aparecer en junio 2005).
10. D. López, C. Cruz y C. Posadas, *Journal of Physics: Conference Series* (por aparecer en 2005).
11. E.N. Lorenz, *J. Atmosph., Sci.* **20** (1963) 130.
12. K.M. Cuomo, A.V. Oppenheim y S.H. Strogatz, *IJBC* **3** (1993) 1629.
13. R. Núñez, "Los SAP's-Labview (Generador/Analizador Dinámico) y Dadisp". Reporte técnico confidencial, DET-CICESE, 1998.
14. R. Núñez, "Aplicaciones del PDS en la instrumentación moderna utilizando los programas Dadisp y Labview", Apuntes del curso institucional: PDS, DET-CICESE, 1998.
15. A.V. Oppenheim, G.W. Wornell, S.H. Isabelle y K.M. Cuomo, *IEEE, ICASSP* **IV** (1992) 117.
16. R. Núñez, "Calificación experimental de la sincronía de dos circuitos caóticos", **XI** Con. Lat. de Cont. Auto., CLCA'04, La Habana, Cuba, 2004.
17. H. Ott, *Noise Reduction Techniques in Electronic Systems*, Sec. Ed., W&S., 1998.