Ingeniería Investigación y Tecnología, volumen XIII (número 4), octubre-diciembre 2012: 489-502
ISSN 1405-7743 FI-UNAM
(artículo arbitrado)

Sincronización atípica de múltiples circuitos caóticos desacoplados y su aplicación en encriptamiento

Atypical Synchronization of Multiple Uncoupled Chaotic Circuits and its Application in Encryption

Núñez-Pérez R.F.
Electrónica y Telecomunicaciones
Centro de Investigación Científica y de Educación Superior de Ensenada
Correo: rnunez@cicese.mx

Información del artículo: recibido: junio de 2011, reevaluado: octubre de 2011, aceptado: noviembre de 2011

Resumen

En el presente trabajo se muestra experimentalmente que es posible lograr sincronizar varios circuitos idénticos de Lorenz desacoplados controlando solamente un parámetro de forma independiente; la asincronía registrada es competitiva con la de una sincronización típica, aunque hay que pagar un precio, ya que la dinámica caótica decrece, y para el caso de encriptamiento, debe compensarse con la suma de otra señal caótica o de alguna función como la convolución con el propio mensaje. Se seleccionan experimentalmente la frecuencia de los pulsos de control (sincronizadores) del parámetro y su ciclo de trabajo para lograr errores mínimos en la sincronización, y se comprueba experimentalmente el procedimiento por medio de dos aplicaciones de encriptamiento y recuperación de señales de audio de baja frecuencia con ruido aleatorio. Finalmente, se necesita realizar más experimentación sobre esta sincronización atípica ante variaciones en el pulso de control paramétrico, ruido eléctrico e inestabilidades propias de los componentes para aplicarla en encriptamiento caótico de señales de voz y audio con usuarios múltiples.

Descriptores:

- circuito de Lorenz
- sincronización típica circuitos caóticos
- encriptamiento caótico

Abstract

This paper shows experimentally that it is possible synchronize several uncoupled Lorenz identical circuits controlling only one parameter independently; registered asynchrony is competitive with that of a typical synchronization. Although there is a price to pay, since the chaotic dynamics decreases and in the case of encryption that must be compensated by the addition of another chaotic signal or some function as the convolution with the message itself. The frequency control pulses (synchronizers) for the parameter and its working cycle are selected experimentally to achieve minimal errors in the timing, and the procedure is experimentally verified using two applications of encryption and recovery of low frequency audio signals with random noise. Finally, more experimentation is needed on this atypical synchronization regarding the changes in pulse parametric control, electrical noise and instability of the components to apply it in chaotic encryption of voice and audio signals from multiple users.

***Keywords*:**

- *Lorenz circuit*
- *chaotic circuits typical*
- *synchronization*
- *chaotic encryption*

Introducción

Con la idea de realizar algunas aplicaciones reales en el campo de las comunicaciones encriptadas, en el año 2001 iniciamos actividades de simulación y experimentación con los circuitos caóticos de Lorenz y Chua (Núñez, 2001). Por las facilidades que presenta, se eligió al de Lorenz para utilizarlo en el desarrollo de un comunicador bidireccional privado basado en encriptamiento caótico (Núñez, 2006a). Dado que el circuito de Lorenz cuenta con tres parámetros, se seleccionó el de Rayleigh por ser el que mejor exhibe su dinámica caótica. Para conocer el grado relativo de caos entre las señales del circuito, se tuvo que excitar el parámetro mencionado con diferentes formas de onda; se encontró que con una señal cuadrada o pulsante se podía encender y apagar, instantáneamente, la dinámica caótica del circuito de Lorenz (Núñez, 2006a, Corron y Hahs, 1997; Verdulla *et al*., 2009). Esto no fue algo nuevo hasta que se realizó con un par de circuitos idénticos y se observó que la evolución de sus señales caóticas era muy semejante durante un cierto tiempo y luego difería notablemente, que es comportamiento típico de los circuitos caóticos en general, (Corron y Hahs, 1997). Este comportamiento mostró que si se encienden de forma simultánea podrían sincronizarse forzadamente durante cierto tiempo y, si antes de que se desincronicen se apagan y se vuelven a encender, entonces se podría mantener controlada la dinámica caótica por esa acción. Si este procedimiento se repite podría establecerse un canal para el envió de mensajes encriptados. El presente trabajo trata acerca de la demostración experimental del procedimiento de sincronización, el cual podría extenderse a varios circuitos receptores. Lo que resulta verdaderamente interesante es que *no necesita acoplamiento alguno entre ellos*, sólo sus tiempos de encendido y apagado deben mantenerse controlados por un tren de pulsos aplicados al parámetro mencionado, el cual depende del tiempo que tarden las señales caóticas en separarse.

El análisis teórico de los diferentes procedimientos típicos de sincronización ya fue realizado con detalle por Carroll y Pecora (1991, 1993), Cuomo *et al*. (1993a, 1993b), Álvarez (1996), Corron *et al*. (1997, 1998), Núñez (2001, 2006a, 2006b, 2011), entre otros. Sin embargo, para este caso, la bibliografía disponible es escasa, por lo que se cree que el trabajo experimental podría ser interesante para los estudiosos de la sincronización de circuitos caóticos desacoplados. Se propone que la señal del pulso paramétrico debe presentar un ciclo de trabajo particular para ser eficiente y dar continuidad al proceso de sincronización. Experimentalmente, se logra buena eficiencia con un ciclo de trabajo de 80%. La duración del pulso paramétrico permite que se puedan enviar continuamente mensajes encriptados de diversas formas, por ejemplo, sumando una señal caótica extra al mensaje o convolucionando la señal caótica original con el mensaje para encriptarlo en el transmisor y deconvolucionando con la señal caótica imagen, para recuperarlo en el receptor. Esto con la idea de incrementar la dinámica caótica de la señal encriptadora, ya que se ve comprometida con ciertos patrones por el propio procedimiento propuesto. El estudio contempla un par de aplicaciones de encriptamiento, la incorporación de ruido en el canal y variaciones en el ciclo de trabajo de los pulsos sincronizadores. Podría pensarse que el procedimiento de sincronización por pulsos paramétricos sería válido para sincronizar múltiples circuitos afines y lograr así una propuesta al tan anhelado encriptamiento de mensajes de usuarios múltiples, etcétera. En la sección 2 se presentan los fun-

damentos del circuito de Lorenz y de sus métodos típicos de sincronización con acoplamiento, también se mencionan algunas maneras sencillas de calificar experimentalmente estos métodos. En las secciones que siguen, se describe la sincronización atípica propuesta para dos o más circuitos de Lorenz por medio de la selección apropiada de la frecuencia de los pulsos paramétricos sincronizadores y de su ciclo de trabajo, con la idea de mantener la continuidad en el proceso se reportan los errores en la sincronización producto de variaciones en el ciclo de trabajo, respectivamente. En secciones posteriores se presentan dos aplicaciones de encriptamiento y recuperación de mensajes y el análisis de los resultados de la sincronización atípica y de la recuperación de los mensajes de las aplicaciones, respectivamente. Aquí se vislumbra el potencial de la propuesta de sincronización atípica. Finalmente se presenta la conclusión de este trabajo: experimentalmente es posible sincronizar varios circuitos idénticos de Lorenz desacoplados, sólo controlando un parámetro en forma sincrónica e independiente como se demuestra con un par de aplicaciones de encriptamiento realizadas. Otra aplicación importante utilizando la sincronización por pulsos propuesta, es la del envió de mensajes binarios por medio de modulación paramétrica. Los agradecimientos y las referencias bibliográficas más relevantes se presentan al final.

Los circuitos de Lorenz, su sincronización típica y calificación

Edward Lorenz (1963) fue el primero en evidenciar la existencia del caos determinístico, es decir, aquel que es desordenado e impredecible, pero que también es acotado, limitado o finito. El sistema que utilizó consta de tres ecuaciones diferenciales ordinarias (1) 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 sus ecuaciones se pueden implementar con circuitos electrónicos sencillos. Por otro lado, el método típico de sincronización para los circuitos de Lorenz que se utiliza en este trabajo es el de Carroll y Pecora (1991, 1993). En dicho método, la señal Xr del circuito receptor se genera y controla indirectamente a partir de la señal **Xt** acoplada desde el circuito transmisor, es decir, **Xt** provoca que se generen las señales Yr y Zr, que son las que a su vez generan la Xr. Ahora bien, se persigue que el error en la sincronización, o asincronía, sea siempre mínimo (esto es, que **Xt** – Xr = 0) y por ello se requiere que los dos circuitos involucrados se parezcan lo más posible y que sus estabilidades sean muy semejantes mientras se desee que permanezcan sincronizados, esto quiere decir que sus componentes electrónicos, alimentaciones, parámetros, cadenas de retardo y condiciones iniciales de operación deben ser muy semejantes. Es claro que el retardo en la generación y control de la señal Xr debe ser pequeño para que no contribuya sistemáticamente al error mencionado.

Como ya se vió, la robustez para este método de sincronización está muy comprometida con la diferencia entre las estabilidades de los circuitos y con el ruido capturado por la señal acoplante **Xt**. Las ecuaciones en forma integro-diferencial de Lorenz para el circuito sincronizado según Carroll y Pecora (1991), Márquez y Álvarez (1996) y Núñez (2006a) son:

Circuito transmisor (t: original)

$$\mathbf{Xt} = -s\int(\mathbf{Xt} - Yt)dt,$$

$$Yt = -[\int \mathbf{Xt}(Zt - \mathbf{pt})dt + \int Ytdt], \quad s, \mathbf{pt}, b > 0 \qquad (1)$$

$$Zt = -[\int(Yt(-\mathbf{Xt})dt + b\int Ztdt],$$

Circuito receptor (r: imagen)

$$Xr = -s\int(Xr - Yr)dt,$$

$$Yr = -[\int \mathbf{Xt}(Zr - \mathbf{pr})dt + \int Yrdt], \quad s, \mathbf{pr}, b > 0 \qquad (2)$$

$$Zr = -[\int(Yr(-\mathbf{Xt})dt + b\int Zrdt].$$

La sincronización se establece por medio de la señal acoplante del transmisor **Xt**, como se indica por (2) en el circuito receptor. Los parámetros s, b y **pt** en (1) (**pr** en (2)) corresponden a los números de Prandtl geométrico y de Rayleigh, respectivamente. Para obtener un comportamiento caótico, los dos primeros representan las ganancias de 10 y 2.7, respectivamente, mientras que el tercero puede variarse entre 20 y 50, pero se posiciona en 40 para que la dinámica caótica de los circuitos implementados sea máxima (Núñez, 2006a), por ejemplo, en las figuras 2 y 3, se ubica cada una de las ganancias mencionadas y se señala en términos de qué componentes del circuito está (Lorenz, 1963).

El análisis teórico de los diferentes métodos típicos de sincronización lo han realizado: Carroll y Pecora (1991, 1993); Cuomo *et al*. (1993a, 1993b); Álvarez (1996); Gonzáles *et al*. (2000); Núñez (2001, 2006a) y otros. Dentro de los procedimientos experimentales más utilizados para calificar el grado y la robustez en las sincronizaciones típicas, se pueden citar las comparaciones de formas de onda (Núñez, 2001; Gamez y Núñez, 2004; Núñez, 2004), de firmas espectrales (Núñez, 2001, 2006b, 2009), de planos de fase o atractores (Núñez,

2001, 2006b, 2009), de riquezas espectrales (Núñez, 2009), de cuantificadores numéricos del caos (Núñez, 2008), de funciones de análisis de coherencia (Gamez y Núñez, 2004; Núñez, 2004), entre otros.

La sincronización atípica propuesta para dos o más circuitos de Lorenz

El estudiar los diversos comportamientos del circuito de Lorenz, vía la variación del parámetro de Rayleigh (Núñez, 2006a; Corron y Hahs, 1997), fue con la finalidad de conocer el nivel del voltaje de éste para posicionar a sus tres señales en caos máximo y averiguar la más caótica. Se observó que si se excita el mismo por medio de una señal pulsante se logra controlar instantáneamente el encendido y apagado de su dinámica caótica. Esto no significó nada nuevo, hasta que se realizó lo mismo, pero con un par de circuitos idénticos de Lorenz y se observó que sus comportamientos eran muy semejantes durante cierto tiempo y luego diferían notablemente, que es la operación normal en circuitos de este tipo. Después se pensó que si los circuitos se encienden de forma simultánea, pueden sincronizarse forzadamente, durante cierto tiempo, y antes que se desincronicen se apagan y se vuelven a encender, en condiciones idénticas, entonces es posible llegar a mantener y controlar el comportamiento caótico.

Este procedimiento podría extenderse a varios circuitos receptores idénticos y lo más relevante: **no necesita acoplamiento alguno entre ellos,** sino que sólo las bases de tiempo de los pulsos paramétricos sincronizadores deben operar simultáneamente.

El procedimiento propuesto se presenta en el diagrama a cuadros de la figura 1 y en las figuras 2 y 3 se presentan los circuitos de Lorenz: transmisor y receptor implementados. En la figura 4 se muestra una fotografía de uno de los experimentos realizados para observar la sincronización de las señales **Xt** y Xr de Lorenz producto de la acción de los pulsos paramétricos sincronizadores; las señales caóticas mencionadas aparecen traslapadas.

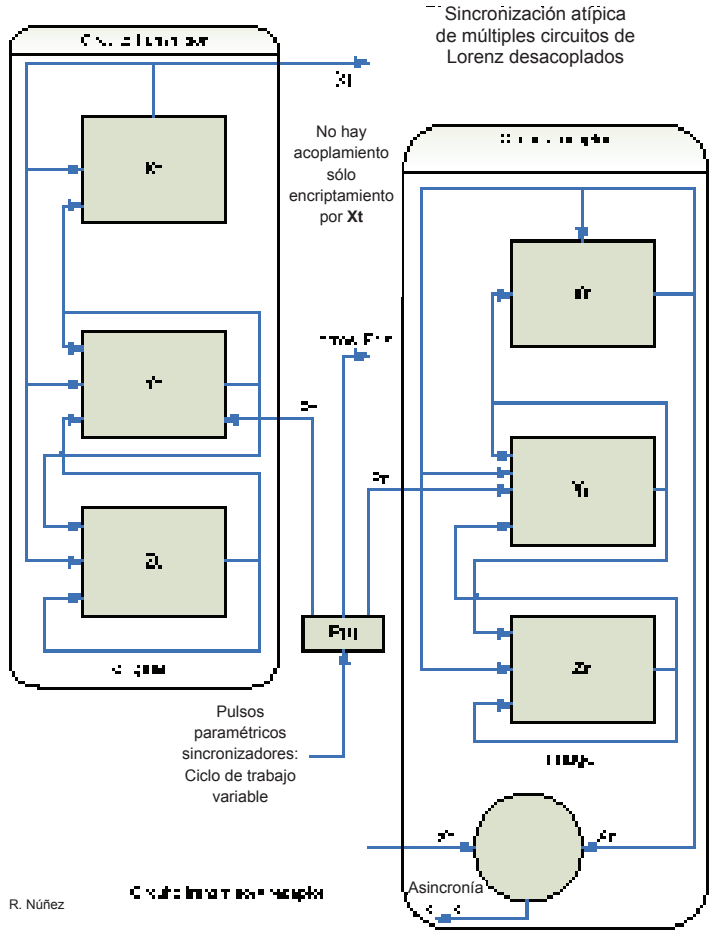

Figura1. Procedimiento propuesto para la sincronización atípica de múltiples circuitos de Lorenz desacoplados

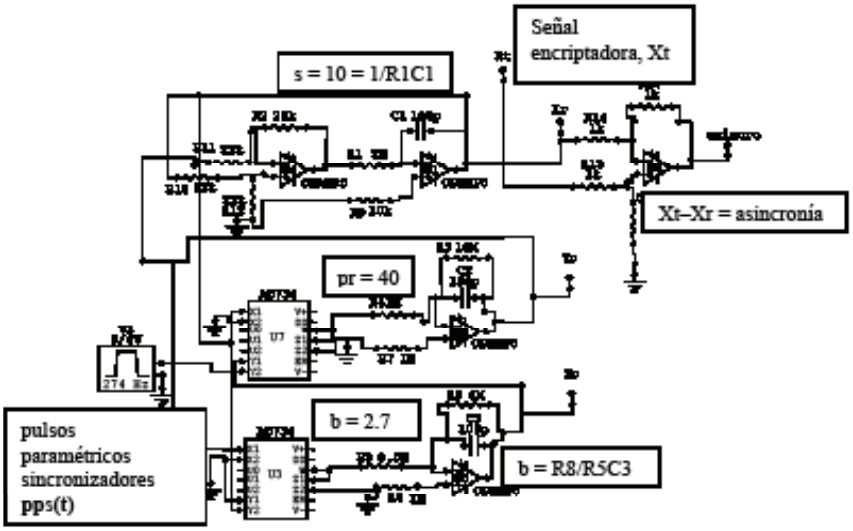

Figura 2. Circuito de Lorenz (transmisor) mostrando sus parámetros, las variables descriptivas y los **pps(t)**

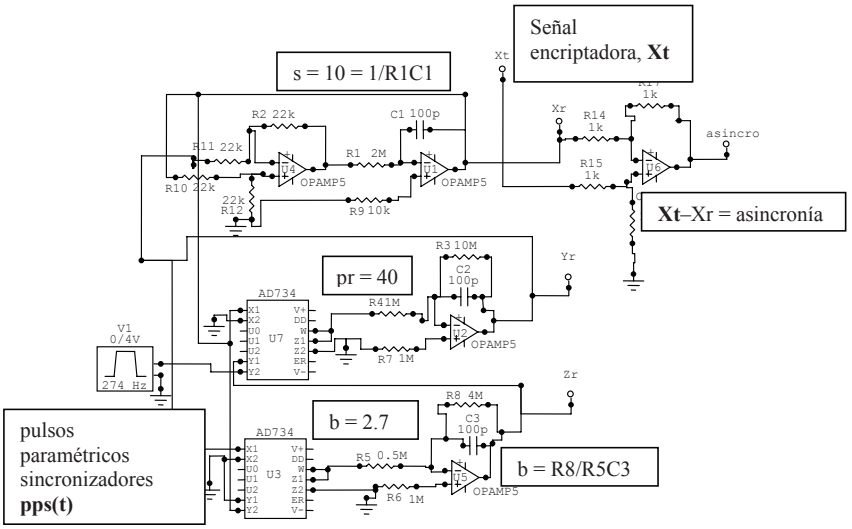

Figura 3. Circuito de Lorenz (receptor) mostrando sus parámetros y variables descriptivas. Se indica la señal de asincronía como calificadora de la sincronización entre los circuitos en atención a los **pps(t)**

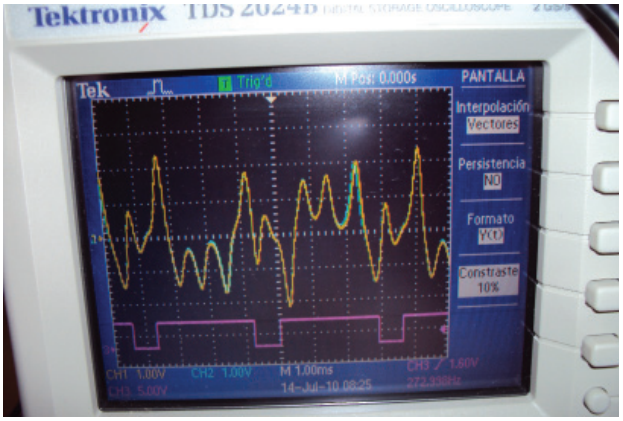

Figura 4. Experimento que despliega al tren de pulsos paramétricos **pps (t)** sincronizando las señales caóticas **Xt** y Xr, las cuales aparecen traslapadas

Las ecuaciones integro-diferenciales de Lorenz para el circuito sincronizado en forma atípica o utilizando pulsos paramétricos sincronizadores **pps(t),** son:

Circuito transmisor (t: original)

$\mathbf{Xt} = -s\int(\mathbf{Xt} - Yt)dt,$

$Yt = -[\int \mathbf{Xt}(Zt - \mathbf{pps(t)t})dt + \int Ytdt], \quad s, \mathbf{pps(t)t}, b > 0 \quad (3)$

$Zt = -[\int(Yt(-\mathbf{Xt})dt + b\int Ztdt],$

Circuito receptor (r: imagen)

$Xr = -s\int(Xr - Yr)dt,$

$Yr = -[\int Xr(Zr - \mathbf{pps(t)r})dt + \int Yrdt], \quad s, \mathbf{pps(t)r}, b > 0 \quad (4)$

$Zr = -[\int(Yr(-Xr)dt + b\int Zrdt],$

Como lo indican las ecuaciones, no existe acoplamiento alguno entre los circuitos. Los parámetros s, b y **pps**(**t**)**t** (1) (**pps**(**t**)**r** (2)) corresponden a los números de Prandtl, geométrico y Rayleigh, respectivamente. Los dos primeros son puestos a las ganancias de 10 y 2.7, respectivamente, para que la dinámica caótica (Núñez, 2006a) de los circuitos implementados sea máxima (Lorenz, 1963), mientras que el tercero, se utiliza para controlar a los circuitos de Lorenz idénticos e independientes, el cual sabemos que está constituido por una señal de pulsos paramétricos sincronizadores **pps**(**t**) (compare la parte inferior de la figura 4), que opera a una frecuencia de sincronización fs (por ejemplo, en las figuras 2 y 3 se ubica cada ganancia y se señala en qué componentes del circuito se encuentra). La idea es que esta señal **pps**(**t**) sea capaz de encender y apagar los circuitos para mantenerlos continuamente sincronizados, a la mayor dinámica caótica posible, para establecer con ello un canal confiable de encriptamiento. En la figuras 5 y 6 las ventanas W1 y W2, presentan las señales caóticas **Xt** y Xr sincronizadas por el método propuesto, respectivamente; las ventanas W4 y W6, muestran las señales caóticas **Xt** y Xr traslapadas con

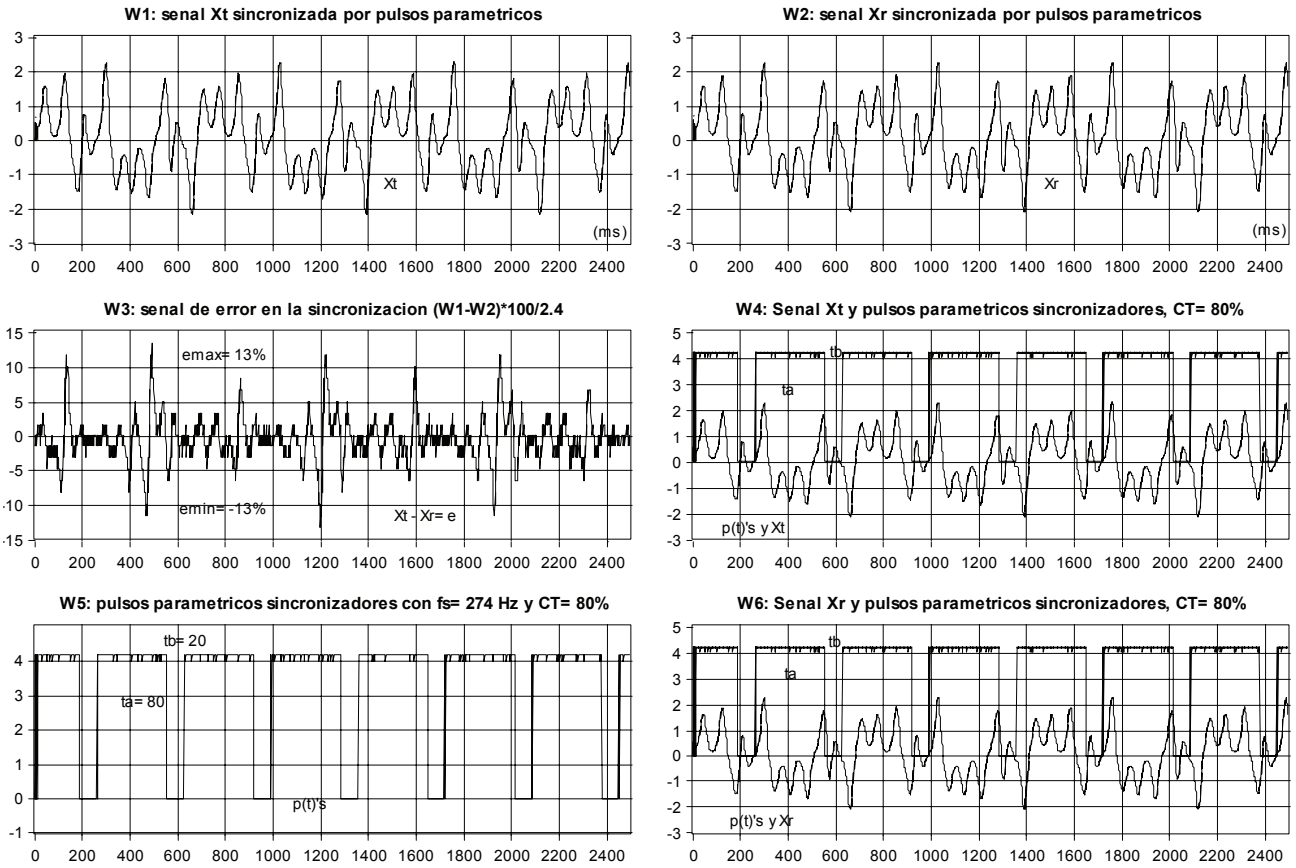

Figura 5. Descripción del procedimiento de sincronización por pulsos paramétricos utilizando el programa Dadisp. Las ventanas W4 y W5 muestran las señales caóticas **Xt** y Xr traslapadas con sus pulsos sincronizadores a un CT de 80%, respectivamente. La ventana W3 presenta la asincronía de 13% obtenida para el CT mencionado

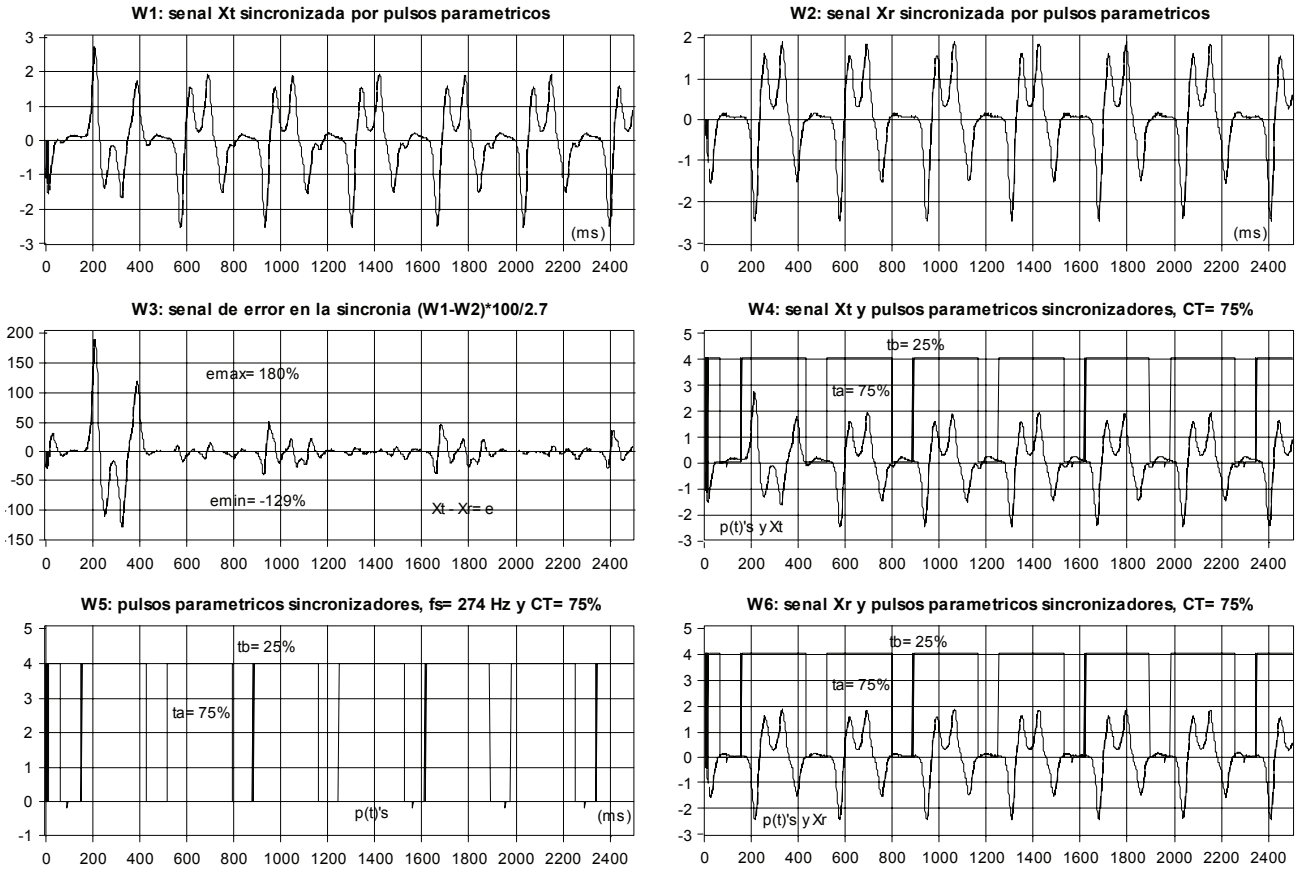

Figura 6. Descripción del procedimiento de sincronización por pulsos paramétricos utilizando el programa Dadisp. Las ventanas W4 y W5 muestran las señales caóticas **Xt** y Xr traslapadas con sus pulsos sincronizadores a un CT de 75%, respectivamente. La ventana W3 presenta la asincronía de 180% obtenida para el CT mencionado

sus pulsos paramétricos sincronizadores, respectivamente (Núñez, 1998). En la figura 7 se despliegan en tiempo real las mismas señales caóticas **Xt** y Xr de la figura 5 con el programa Dadisp (Núñez, 1998), las cuales van sincronizadas por los pulsos paramétricos y sus espectros E**Xt** y EXr, ambos casos de manera traslapada.

También se incluyen sus espectrogramas Es**Xt** y EsXr de forma independiente, utilizando el programa LabVIEW (Núñez, 1998).

Conformación de los pulsos paramétricos sincronizadores

Para mantener la sincronización continua debe controlarse el procedimiento de encendido y apagado de la dinámica caótica de los circuitos de estudio por medio de una frecuencia sincronizadora fs, que proporcione la cadencia para los **pps (t)**. Dicha fs, se calcula a partir de medir el tiempo que tardan las señales caóticas en separarse después de su activado simultáneo, como lo indican Corron y Hahs (1997); Núñez (2001, 2006a) y Verdulla *et al*. (2009). Para el caso particular, se obtiene buen rendimiento con una fs de 274 Hz y la señal propuesta para los **pps(t)** se despliega en la ventana W5 de las figuras 5 y 6.

Ciclo de trabajo de los pulsos paramétricos para continuidad en la sincronización

Al calcular la fs y asegurar que el proceso de sincronización sea continuo, es necesario reducir el tiempo de apagado del circuito variando el ciclo de trabajo de la señal de los **pps(t).** Según Agilent Technologies (2000), el ciclo de trabajo (CT) se define como la tasa entre la duración del pulso Ta y su periodo T. El inverso de este periodo representa la frecuencia máxima de sincronización fs, mencionada en la sección anterior. El ciclo de trabajo CT es:

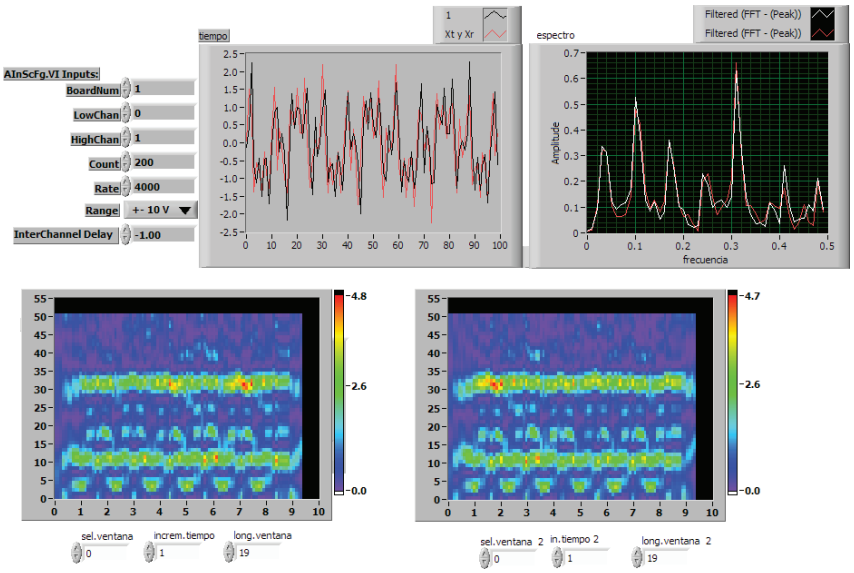

Figura 7. Descripción en tiempo real del procedimiento de sincronización por pulsos paramétricos utilizando el programa LabVIEW. Las ventanas superiores muestran las señales caóticas **Xt** y Xr (V, mseg*10) y sus espectros (V, Khz*4) correspondientes; ambos traslapados. Los pulsos sincronizadores operan con un CT de 80%. Las ventanas inferiores despliegan los espectrogramas (Khz*0.04, mseg*100) para cada señal caótica sincronizada

CT = Ta/T [%],

T = Ta + Tb, (5)

fs = 1/T,

donde

Ta = tiempo de encendido [mseg]; tiempo máximo transcurrido a partir del encendido hasta antes de la separación de las señales caóticas,

Tb = tiempo de apagado [mseg]; tiempo mínimo necesario para apagar y restablecer el circuito caótico

fs = frecuencia máxima de sincronización [Hz]; permite la mayor dinámica caótica.

El CT de la señal de los **pps (t)** debe ser de un valor tal que logre una mayor eficiencia en el tiempo de sostenimiento de la sincronización; la idea es estirar y comprimir al máximo los tiempos de encendido Ta y de apagado Tb, respectivamente. Con base en el cálculo y medición del error mínimo (c.f., con la sección 4), se logra una eficiencia experimental aceptable en la sincronización con un ciclo de trabajo de 80%, como se muestra en la ventana W5 de la figura 5 (i.e., 80% encendido y 20% apagado) (Núñez, 1998). Existen varios tipos de bases de tiempo para sincronizar remotamente los circuitos (Núñez, 1998), pero para realizar las pruebas de laboratorio y por funcionalidad, se utilizó el generador de señales Agilent 32120A (Agilent, 2000), ya que facilita la variación automática y simultánea, tanto de la frecuencia de los pulsos sincronizadores fs como de su CT.

Errores en la sincronización para dos ciclos de trabajo del pulso paramétrico sincronizador

El análisis de error en la sincronización (v.g., e= **Xt**–Xr) se realizó para dos ciclos de trabajo de 80 y 75%, en forma calculada (v.g., %e= (**Xt**–Xr)100% /**Xt**(máx)) y medida (Núñez, 1998). En las ventanas W1 y W2 de la figura 8 se presentan los errores máximos en la sincronización, calculados y medidos de 13 y 18%, respectivamente, para un CT = 80%.

En las ventanas W6 y W3 se presentan los errores máximos en la sincronización calculados y medidos de 180% para ambos casos, cuando el CT = 75%. En la misma figura, las ventanas W4 y W5 muestran las señales medidas de los **pps(t)** a una frecuencia de 274 Hz y sus correspondientes ciclos de trabajo analizados de 80 y 75%, respectivamente. En la figura 9 se muestra la maqueta experimental desarrollada para probar en **tiempo real** la sincronización atípica de los dos circuitos de Lorenz desacoplados.

Encriptamientos y recuperaciones del mensaje m(t) con ruido en el canal

Son dos las aplicaciones realizadas para encriptar y recuperar la señal original del mensaje m(t) constituida por dos senoidales de 125 y 275 Hz de frecuencia y con 0.3 y 0.4 Vp de magnitud, respectivamente. La señal m(t) se produce por el generador de señales Agilent 32120A (Agilent, 2000) y se mide y analiza con el sistema automático de prueba Dadisp (Núñez, 1998). En la

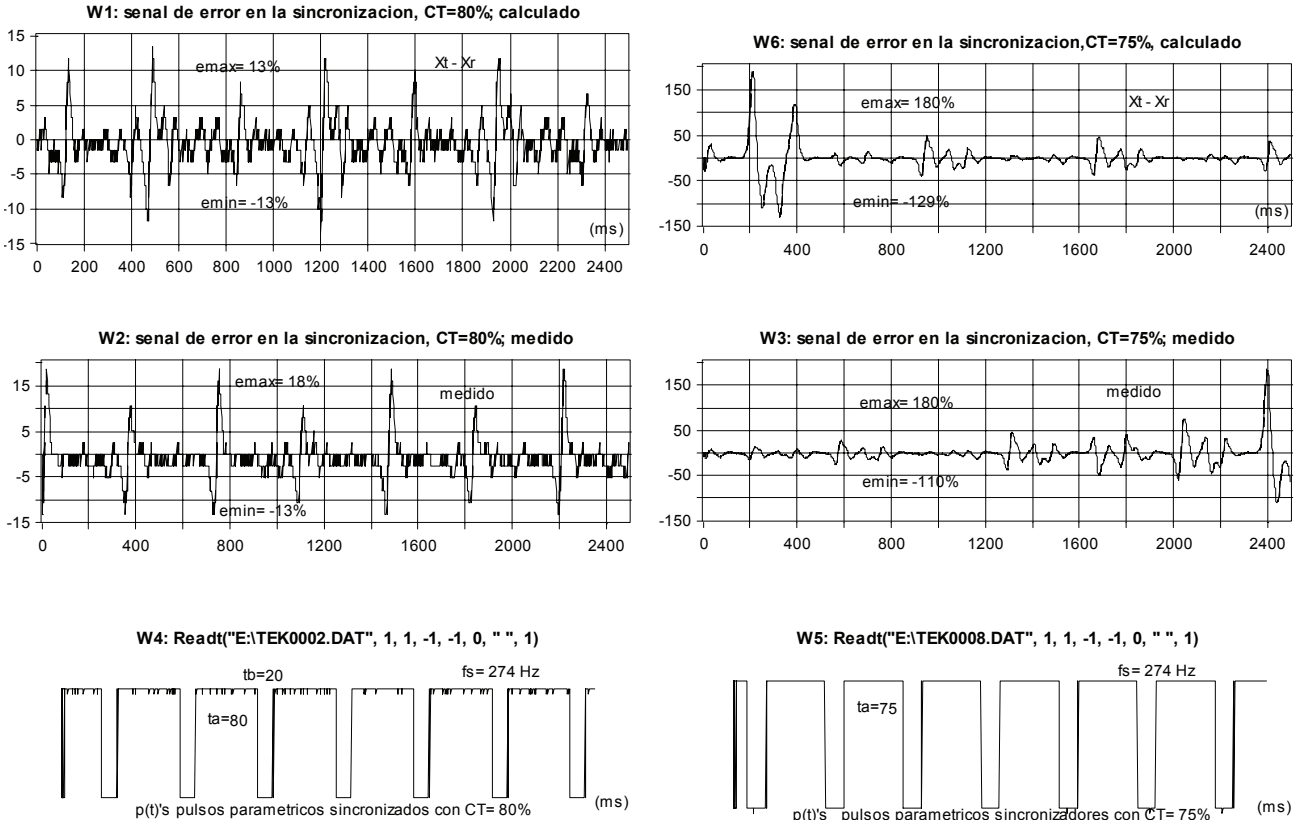

Figura 8. Se presentan los errores en la sincronización calculados y medidos para los CT de 80% y 75%. El CT de 80% es el más eficiente para fs = 274 Hz

figura 10 se describe la primera aplicación de encriptamiento que consiste en sumar el mensaje m(t) a la señal caótica **Xt** en el transmisor, ya en el receptor, se resta la señal Xr de las señales sumadas para recuperar el mensaje m'(t).

La segunda, consiste en convolucionar el mensaje m(t) con la señal caótica **Xt** en el transmisor, ya en el receptor, se deconvoluciona la señal caótica Xr de las convolucionadas para extraer el mensaje m'(t). Para el encriptamiento por suma S(t), se tiene que el mensaje original m(t) se suma a la señal **Xt** (que se produce y mide del circuito transmisor) y a la señal de ruido aleatorio Vr(t) de 0.1 Vp de magnitud, como se puede observar en la ventana W5 de la figura 11. Ya en el receptor, a esta señal S(t) se le resta la señal Xr (la cual se produce y mide del receptor), y es así como se recupera la señal del mensaje m'(t) (compare con la ventana W3 de la figura 11). Las operaciones siguientes describen el proceso de encriptamiento y recuperación del mensaje:

$$S(t) = \mathbf{Xt} + m(t) + Vr(t) \quad (6)$$

Si la frecuencia fs de los **pps(t)** es 274 Hz y presentan un CT = 80%, los circuitos transmisor y receptor se mantienen sincronizados confiablemente (figura 5), por lo tanto, las señales **Xt** y Xr son casi iguales. Aunque debido a la señal de ruido aleatorio Vr(t) existe una pequeña diferencia, como lo indica (7) y se muestra en la ventana W4 de la figura 11, entonces se tiene que:

$$S(t) - Xr \approx m'(t), \quad \text{puesto que } Vr(t) << m(t) \quad (7)$$

Por lo que el error máximo en la recuperación del mensaje m'(t) para esta aplicación es: m(t) – m'(t)= **–5.5%** (compare con la ventana W4 de la figura 11).

Para la aplicación de encriptamiento por convolución C(t), se tiene que el mensaje m(t) se convoluciona con señal caótica **Xt** en el transmisor y ya en el receptor, se deconvoluciona D(t) la señal Xr de las convolucionadas para recuperar el mensaje m'(t). En la figura 12 se presenta la descripción de esta aplicación, y a su vez, se realiza una comparación con la primera. En las ventanas W1 y W2 se presentan las señales **Xt** y Xr sincroni-

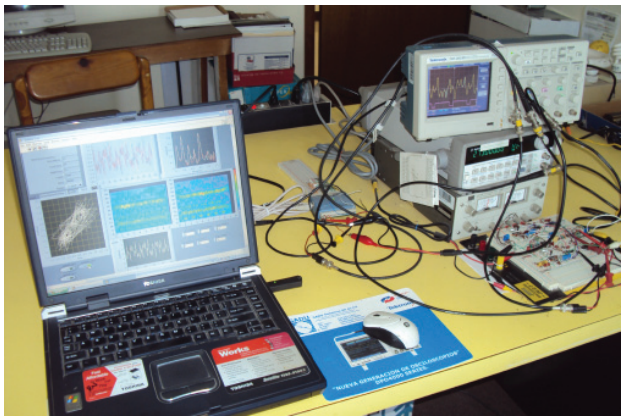

Figura 9. Maqueta experimental para probar en tiempo real la sincronización atípica de dos circuitos de Lorenz desacoplados

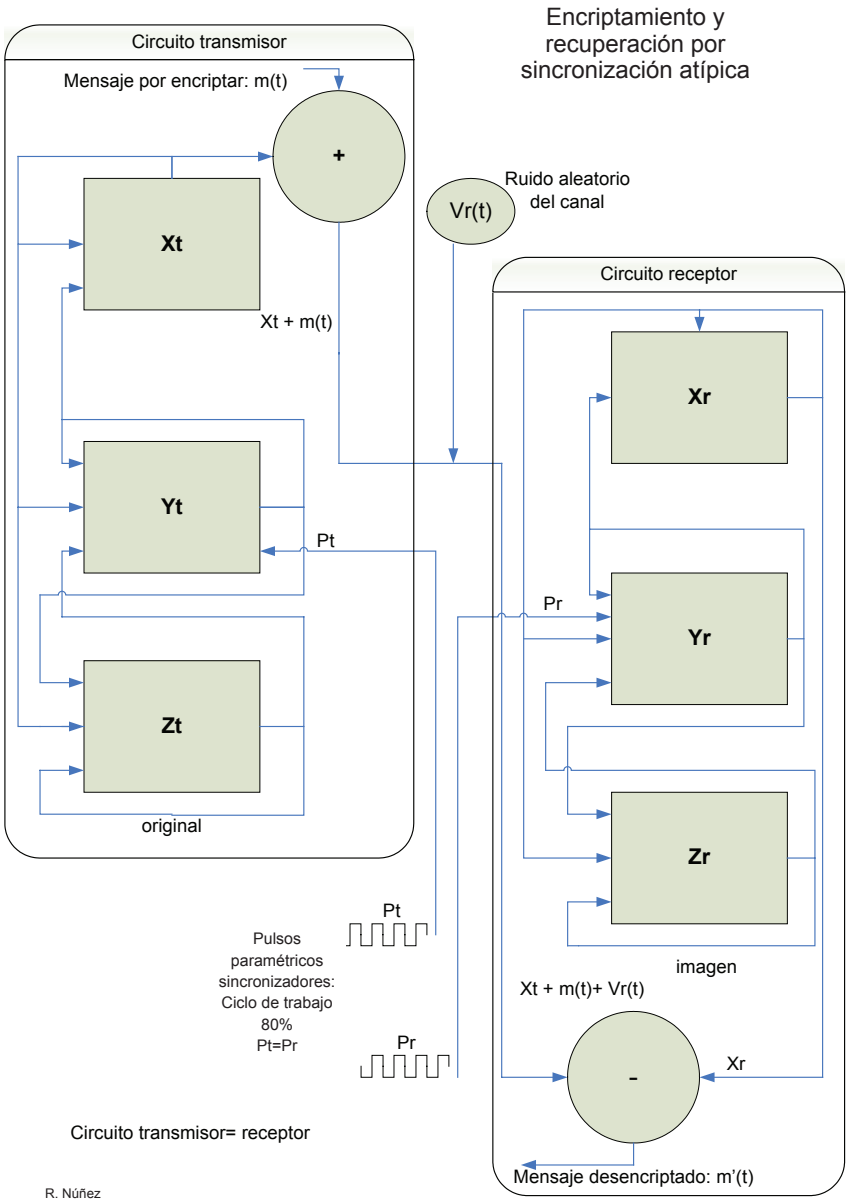

Figura 10. Procedimiento de encriptamiento y recuperación de un mensaje utilizando la sincronización atípica. Se incorpora ruido aleatorio del canal a la señal encriptadora. La cadencia de los pulsos independientes es de 274 Hz y se opera con un CT de 80%

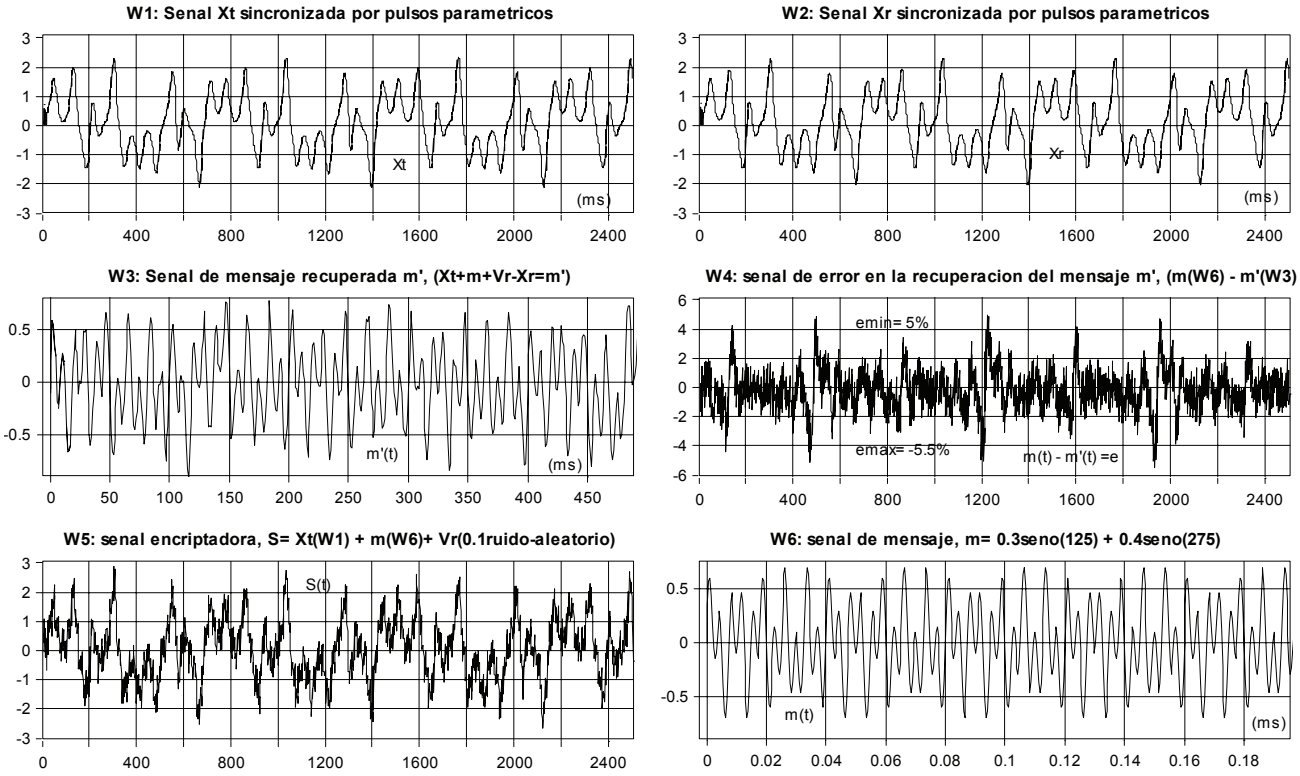

Figura 11. La sincronización atípica en una aplicación de encriptamiento por suma descrita en el programa Dadisp. La ventana W4 presenta un error del 5.5% en la recuperación del mensaje original

zadas por los **pps(t)** con una frecuencia de 274 Hz y CT = 80%, respectivamente, y en las ventanas W7 y W8 se presentan las señales encriptadas por suma S(t) y convolución C(t), respectivamente. En la misma figura, las ventanas W4 y W5 presentan las señales de mensajes m'(t) recuperadas por ambas aplicaciones, respectivamente, y finalmente, en las ventanas W3 y W6, se muestran los errores instantáneos en la recuperación de la señal de m'(t), para cada caso. Debido a que la sincronización por pulsos paramétricos limita la dinámica caótica provocando que las señal sincronizada presente ciertos patrones repetitivos, se propone la utilización de la convolución C(t) para reforzar el encriptamiento, como se puede observar al comparar la forma de onda de la señal **Xt** sincronizada de la ventana W1, con las de las encriptadas por ambas aplicaciones presentadas en las ventanas W7 y W8 de la figura 12. Para este caso el error máximo en la recuperación del mensaje es de **14.9% (**compare con la ventana W6 de la figura 12).

Análisis de resultados en la sincronización y recuperación del mensaje encriptado

Para el método propuesto, los errores en la sincronización calculados y medidos son de 13 y 18%, como lo indican las respectivas ventanas W1 y W2 de la figura 8, para el caso del CT = 80%, los cuales son muy representativos y dignos de mejorarse. Para ello, se recomienda que las bases de tiempo del transmisor y del receptor para el disparo simultáneo presenten buena estabilidad. Para el caso del CT = 75%, los errores en la sincronía son mucho mayores y no se aceptan, ya que sería imposible recuperar el mensaje. El resultado de la aplicación de envió del mensaje m(t) encriptado por suma S(t), utilizando la señal **Xt** de Lorenz con ruido en el canal de acoplamiento para dos circuitos desacoplados, registra un error de 5.5% en la recuperación del m'(t), como se observa en la ventana W4 de la figura 11. En la misma ventana, se puede constatar que la mayor parte

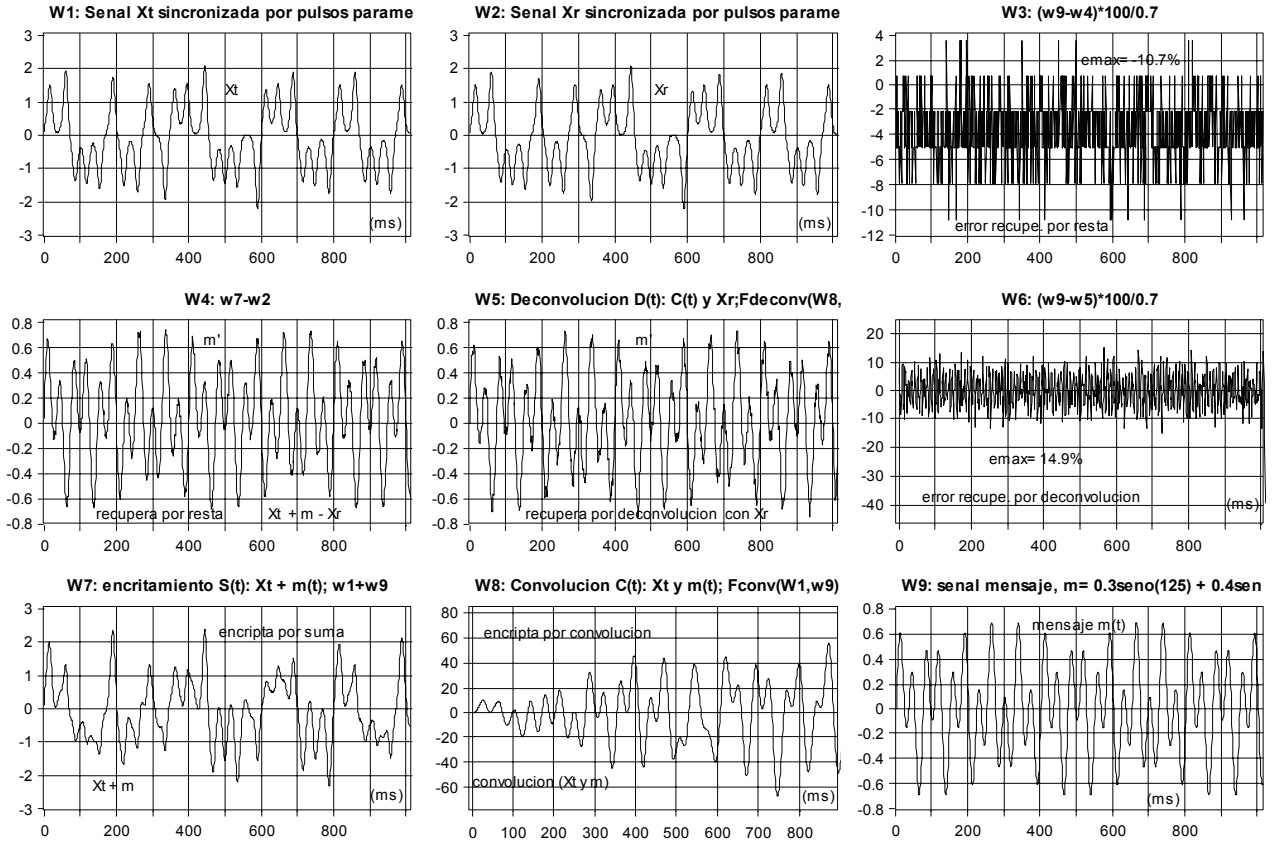

Figura 12. Sincronización atípica en una aplicación de encriptamiento por convolución con el mensaje descrita por el programa Dadisp. La ventana W6 muestra un error de 14.9% en la recuperación del mensaje original. Las ventanas W7 y W8 presentan las señales caóticas encriptadas por suma y convolución del mensaje, respectivamente. Se observa cómo cada una de ellas distorsiona la señal encriptadora, por ejemplo, la convolución mejora la dinámica caótica

del error corresponde al ruido aleatorio de Vr(t) = 0.1 Vp incorporado en el canal. Para el encriptamiento utilizando la convolución C(t), entre **Xt** y m(t), los resultados son interesantes, puesto que se refuerza la capacidad de encriptamiento de la sincronización por pulsos paramétricos, como se puede observar al comparar las señales de las ventanas W7 y W8 de la figura 12. Respecto a la recuperación del mensaje m'(t), se observa que presenta un error máximo del 14.9%, mientras que para el caso de resta es del 10.7%, como se indica en las ventanas W6 y W3 de la misma figura, respectivamente, para esta comparación en particular. Dado que la fs de los **pps(t)** y su CT caracterizan esta propuesta de sincronización, se piensa que su aplicación principal de encriptamiento sería para mensajes de voz y audio de baja frecuencia de usuarios múltiples. Otra aplicación importante de esta misma sincronización por pulsos paramétricos se tiene en el envió de mensajes binarios por medio de modulación paramétrica (Núñez, 2006c); utilizando otro parámetro para la conmutación del estado del circuito de Lorenz.

Conclusiones

Se muestra experimentalmente que es posible sincronizar varios circuitos idénticos de Lorenz desacoplados controlándolos solamente por un parámetro de forma independiente. El precio a pagar es una reducción en la dinámica caótica de la señal encriptadora, la cual tiene que ser compensada con la suma de otra señal caótica o de alguna función encriptadora adicional como la convolución con el propio mensaje. Dada la asincronía obtenida, el método propuesto compite con los métodos de sincronización típicos con acoplamiento. Se seleccionan apropiadamente la frecuencia de los pulsos sincronizadores y su ciclo-trabajo para lograr errores mínimos en la sincronización para comprobar experimentalmente el método por medio de dos aplicaciones de encriptamien-

to de señales de audio de baja frecuencia con ruido aleatorio. Los resultados son representativos, reproducibles y confiables. Otra aplicación importante de esta sincronización propuesta, se encuentra en el envío de mensajes binarios por medio de modulación paramétrica utilizando otro de los parámetros del circuito de Lorenz. Se requiere experimentar más sobre el comportamiento de los circuitos sincronizados atípicamente ante variaciones del pulso paramétrico, ruido eléctrico e inestabilidades propias de los componentes para proponerlos en encriptamiento caótico de señales de voz y audio de baja frecuencia de aplicaciones con usuarios múltiples.

Agradecimientos

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

Referencias

Agilent Technologies. *33120A Function Generator*, manual núm. 90005, 6a ed., 2000, pp. 66-67.

Alvarez J. Synchronization in the Lorenz System: Stability and Robustness. *Nonlinear Dynamics*, volumen 10 (número 1), 1996: 89-103.

Carroll T.L., Pecora L.M. Synchronizing Chaotic Circuits, *IEEE Trans. Circuits and Systems,* volumen 38 (número 4), 1991: 453-456.

Carroll T.L,. Pecora L.M. Synchronizing Nonautonomous Chaotic Circuits. *IEEE Trans. Circuits and Systems II*, volumen 40 (número 10), 1993: 646-650.

Corron N.J., Hahs D.W. A New Approach to Communications Using Chaotic Signals. *IEEE Trans. Circuits Systems I*, volumen 44 (número 5), 1997: 373-382.

Corron N.J. An Approach to Communication with Chaos, en: Procs. 4th Experimental Chaos Conference, Singapore: World Scientific, 1998, pp. 395-406.

Cuomo K.M.,Oppenheim A.V., Strogatz S.H. Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications, en: *Circuits and Syst. II*, volumen 40 **(**número 10), 1993a.

Cuomo K.M., Oppenheim A.V., Strogatz S.H. Robustness and Signal Recovery in a Synchronized Chaotic System. *IJBC*, volumen 3 (número 6), 1993b: 1629-38.

Gámez L., Núñez R. Calificación experimental de la sincronización de dos circuitos caóticos con enrollamientos múltiples, en: Congreso Nacional de la AMCA, 2004.

Gonzáles O.A., Han G., Pineda J., Sánchez E. Lorenz Based Chaotic Cryptosystem: A Monolithic Implementation. *IEEE Trans. Circuits Sytems I*, volumen 47 (número 8), 2000: 1243-47.

Lorenz E.N. Deterministic Nonperiodic Flow. *J. Atmosph., Sci*., volumen 20, 1963:130-41.

Márquez A., Álvarez J. Circuito de Lorenz, Reporte técnico, DET-CICESE, 1996.

Núñez R. The LabVIEW (Generator/Dynamic Analyzer) and Dadisp ATS's. Confidentials Technicals Reports, DET-CICESE, 1998.

Núñez R. An Optimal Chaotic Bidirectional Communicator, Based on Synchronized Lorenz Circuits, en: Procs. of 6th. Experimental Chaos Conference, 22-26 de julio, Postdam, Germany, 2001.

Núñez R. Calificación experimental de la sincronía de dos circuitos caóticos, en: Congreso Internacional de la CLCA2004, La Habana, Cuba, 2004.

Núñez R. Comunicador experimental privado basado en encriptamiento caótico. *Revista Mexicana de Física*, *FC-UNAM*, volumen 52 (número 3), 2006a: 285-294.

Núñez R. Encriptador experimental retroalimentado de Lorenz con parámetros desiguales. *Revista Mexicana de Física*, *FC-UNAM*, volumen 52 (número 4), 2006b: 372-378.

Núñez R. Caracterización de un mensajero caótico binario con ruido en el canal: simulación y experimentación. *Revista Mexicana de Física*, *FC-UNAM*, volumen 52 (número 5), 2006c: 464-473.

Núñez R. Measurement of Chua Chaos and its Applications. *JART, UNAM*, volumen 6 (número 1), 2008.

Núñez R. Spectrum Richness as Determinant of Chaotic Synchronization. *IEEE Latin America Transactions*, volumen 7 (número 5), 2009.

Núñez R. Evaluando las sincronizaciones sin y con retroalimentación en circuitos de Lorenz. *Revista Mexicana de Física*, *FC-UNAM*, volumen 57 (número 1), 2011: 84-90.

Verdulla F.M., López M.J., Prian M. A Pulsed Control Method for Chaotic Systems. *IEEE Latin America Transactions*, volumen 7 (número 1), 2009.

Este artículo se cita:

Citación Chicago

Nuñez-Pérez, Ricardo Francisco. Sincronización atípica de múltiples circuitos caóticos desacoplados y su aplicación en encriptamiento. *Ingeniería Investigación y Tecnología* XIII, 04 (2012): 489-502.

Citación ISO 690

Nuñez-Pérez R.F. Sincronización atípica de múltiples circuitos caóticos desacoplados y su aplicación en encriptamiento. *Ingeniería Investigación y Tecnología,* volumen XIII (número 4), octubre-diciembre 2012: 489-502.

Semblanza del autor

Ricardo Francisco Núñez Pérez. Graduado como M. en C. en instrumentación electrónica por el CICESE, México en 1987 y como licenciado en ingeniería electrónica por la UABC México en 1980, ambos grados con mención honorífica. Desde 1987 hasta la fecha es profesor/investigador en el Departamento de Electrónica y Telecomunicaciones del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE). Recibió el primer lugar con su tesis de maestría en el IV Certamen Nacional sobre diseño de Equipo Electrónico Aplicado al Sector Eléctrico, organizado por el IIE, CONACYT, SEP y la CFE (1988), así como el primer lugar y la Presea en Ciencias y Tecnología en el IV Certamen Nacional del CREA, área electrónica durante el mismo año. Recibió reconocimiento por dirigir la tesis de licenciatura ganadora del primer lugar en el VI Certamen Nacional sobre Diseño de Equipo Electrónico Aplicado al Sector Eléctrico, organizado por el IIE, CONACYT, SEP y CFE (1990). Perteneció al SNI de 1988 a 1993 y sus áreas de investigación e instrucción son: Desarrollo de instrumentación electrónica industrial, comprobaciones experimentales de circuitos caóticos y sus aplicaciones en encriptamiento y en procesos industriales. Utilización de los PDS en el análisis, síntesis y control de señales caóticas, biomédicas y de vibración mecánica.