Caracterización de un mensajero caótico binario con ruido en el canal: simulación y experimentación

R. Núñez-Pérez
Electrónica y Telecomunicaciones, Centro de Investigación Científica y de Educación Superior de Eda.(CICESE), Km. 107, Carr. Tj.-Eda., Eda., B.C., México,
Tel/Fax (646)175-0500/537
e-mail: rnunez@cicese.mx

Recibido el 27 de enero de 2005; aceptado el 29 de marzo de 2006

Se obtienen las características de un mensajero caótico binario, basado en conmutación paramétrica, tanto a nivel simulación como experimental para explorar su capacidad de encriptamiento en la realidad. Se averiguan las características más importantes y no reportadas como son: a) el cambio mínimo en el parámetro tal que su acción sobre la forma de onda de la señal caótica sincronizadora sea imperceptible a un posible espía en el canal ruidoso; b) el nivel máximo del ruido permitido para que el cambio mínimo en el parámetro siga operando; y c) los tiempos en los retardos para que la recuperación de la información binaria sea rápida. Se concluye que el ruido en el canal limita notablemente el funcionamiento real del mensajero estudiado; para superar esto, se propone un mensajero caótico completamente digital.

Descriptores: Circuito de Chua; sincronización de circuitos caóticos; conmutación paramétrica; ruido en el canal; comunicación encriptada robusta.

A binary chaotic messenger is characterized, based on parameters' commutation, using simulation and experimental procedures to explore his real encrypted communication capacity. The characteristics to find out are: a) Parameter minimum change in such a way the change, of synchronization chaotic signal, be invisible to some spy at the noisy channel, and b) Noise maximum level and c) Time delays allow just to make reliable the binary information recovery. Because, the noisy channel allow hardly the messenger studied right performance, the solution is through a new digital chaotic messenger

Keywords: Chua's circuit; synchronization of chaotics circuits; parameter commutation; channel noise; robust encrypted communication.

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

1. Introducción

Para que un mensajero caótico binario, basado en la conmutación paramétrica, funcione en la práctica fuera del ambiente demostrativo y de laboratorio, el cambio en la forma de onda de la señal caótica encriptadora y sincronizadora, cuando el parámetro pasa de un valor a otro debe ser muy pequeño e invisible para que un posible espía en el canal no se dé cuenta, pero a la vez este cambio debe permitir que el receptor pueda detectarlo y recuperar de él, casi instantáneamente, la información binaria correspondiente, pese a que exista un nivel considerable de ruido en el canal. Ya algunos autores han realizado estudios demostrativos al respecto [1-4]. Parlitz [1] propone la conmutación paramétrica basada en el circuito de Chua [5] y recupera la información binaria bastante bien, sólo que considera un cambio paramétrico muy grande, el cual permite que, a simple vista, cualquier observador pueda detectar esta variación en la forma de onda de la señal caótica y por lo tanto descubrir el envío de información binaria, además de no considerar ningún tipo de ruido en el canal y, en el proceso de recuperación de la información binaria, no reporta retardo alguno, pese a que utiliza filtraje digital promediador en movimiento con un factor suavizador de 40 muestras, como lo indica la Fig. 1. Cuomo trabaja con el circuito de Lorenz y prácticamente hace lo mismo que Parlitz, aunque éste, para recuperar la información binaria, utiliza un filtro analógico paso bajas de orden no especificado y el cual aparentemente no retarda la señal operada, como se muestra en la Fig. 2. Dedieu y Cruz [3,4] se basan fuertemente en los resultados de Parlitz para sus estudios y por lo tanto sus conclusiones son semejantes. En general ningún autor de los mencionados realiza estudios sobre la afectación real que sufre la conmutación paramétrica ante ruido en el canal, ni averigua por el cambio mínimo en el parámetro, tal que éste sea invisible para un espía en el canal, y tampoco analizan la velocidad de respuesta de su mensajero propuesto. Todo esto es normal, puesto que lo que persiguen básicamente es demostrar la metodología propuesta a nivel simulación y laboratorio. Ahora bien, si realmente se busca aplicar estos circuitos de encriptamiento, en el campo del envío privado de mensajes, se tiene que competir con sistemas comerciales que trabajan confiablemente en ambientes ruidosos. Esto reviste un verdadero reto en el acondicionamiento de un circuito como el que se propone para que opere con la seguridad necesaria y en los ambientes mencionados.

En la Sec. 2 se presentan las características importantes que los autores de los mensajeros, ya mencionados no reportaron. Por ejemplo: a) el cambio mínimo en el parámetro P tal que no se refleje en la forma de onda de la señal caótica sincronizadora y que sea imperceptible a un espía en el canal ruidoso; b) el nivel máximo del ruido permitido en el canal para que la recuperación de la información sea confiable; y c) los retardos generados por la recuperación de la información binaria. En la misma sección también se describen algunos fundamentos básicos sobre el circuito de Chua, la sincronización y la conmutación paramétrica.

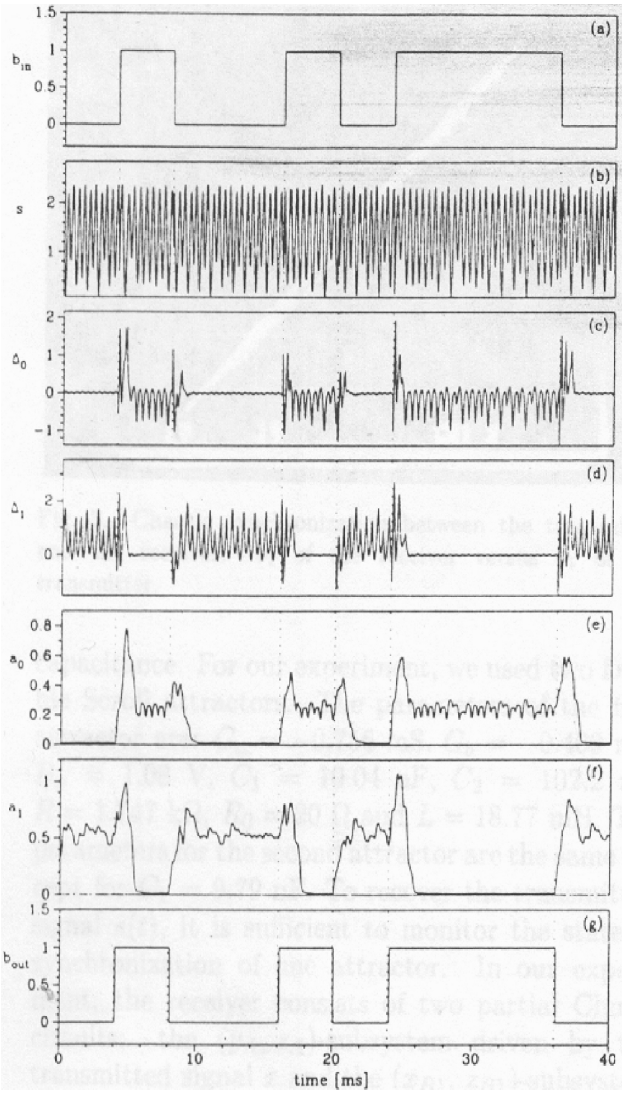

FIGURA 1. Antecedente: a).- Resultado del mensajero caótico binario de Parlitz *et al*. [1]. ΔP = 3 %, filtraje promediador en movimiento sin presentar retardo y no considera el ruido del canal.

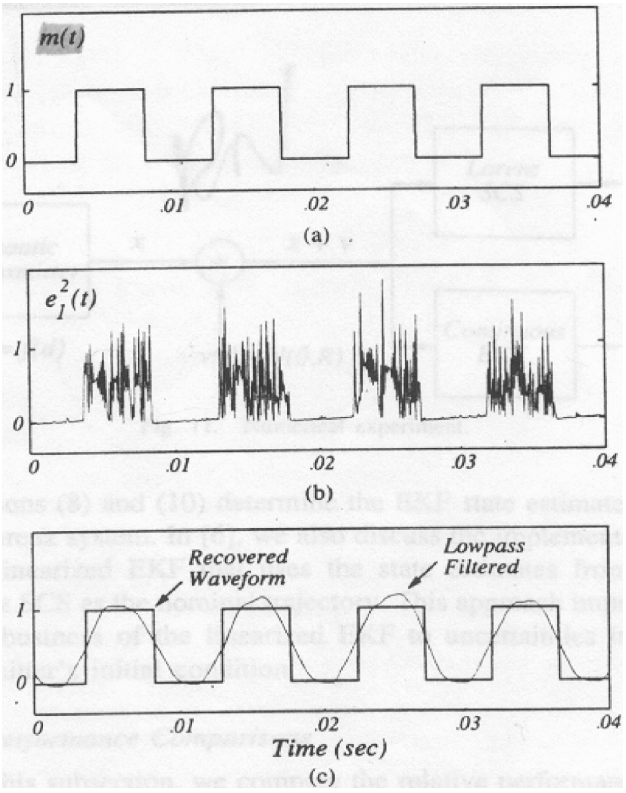

FIGURA 2. Antecedente: b).- Resultado del mensajero caótico binario de Cuomo *et al*. [2]. ΔP = 9 %, filtraje analógico sin presentar retardo y no considera el ruido del canal.

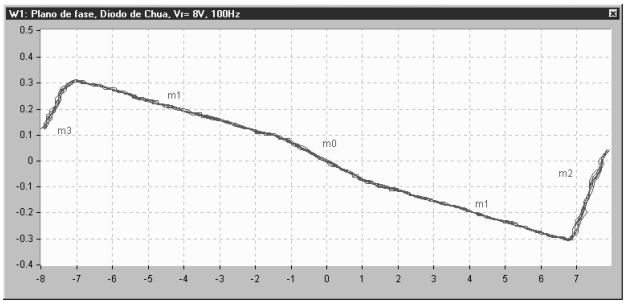

FIGURA 3. Plano de fase del diodo de Chua, o función no-lineal f(x_1), mostrando las pendientes y los puntos de ruptura, obtenido según Kennedy [7].

En la Sec. 3 se presentan los procedimientos de caracterización del mensajero propuesto tanto a nivel simulación como experimental. Se averigua por el cambio en el parámetro, tal que produzca uno mínimo en la forma de onda de la señal caótica sincronizadora y que por ende sea invisible para un posible espía en el canal, pero no para el receptor, ya que éste debe detectar dicho cambio, aun con ruido del canal, y recuperar la información binaria de una manera casi instantánea. Para esto se utilizan el programa Workbench (Wb), para la simulación, y el Sistema Automático de Prueba-Dadisp (SAP-Dadisp), para la experimentación. Se realizan variaciones paramétricas y se registran los resultados a través de las formas de onda de la señal caótica sincronizadora, de la señal de error y de la información binaria recuperada. Ya habiendo obtenido el porcentaje óptimo de variación en el parámetro, se suma una señal de ruido a la caótica mencionada y se hace variar la magnitud de la primera para estudiar su efecto sobre la recuperación de la información binaria. Finalmente, se registra y mide el retardo impuesto por el filtro paso bajas incorporado en el circuito recuperador, comparando instantáneamente las señales de los mensajes enviado y recuperado para poder especificar la velocidad máxima del envío de mensajes. Se observa que, ante cambios en el parámetro P de 0.5 y de 1 % correspondientes a la simulación y experimentación, respectivamente, el proceso resulta casi invisible y el receptor sigue operando apropiadamente, aún con ruido en el canal.

En la Sec. 4 se obtienen algunas especificaciones para facilitar la evaluación del rendimiento y la confiabilidad ante el cambio paramétrico, el nivel de ruido en el canal y el retardo, en la recuperación, de los mensajeros de este tipo, *v.g.*, tal cambio mínimo en el parámetro puede soportar un nivel má-

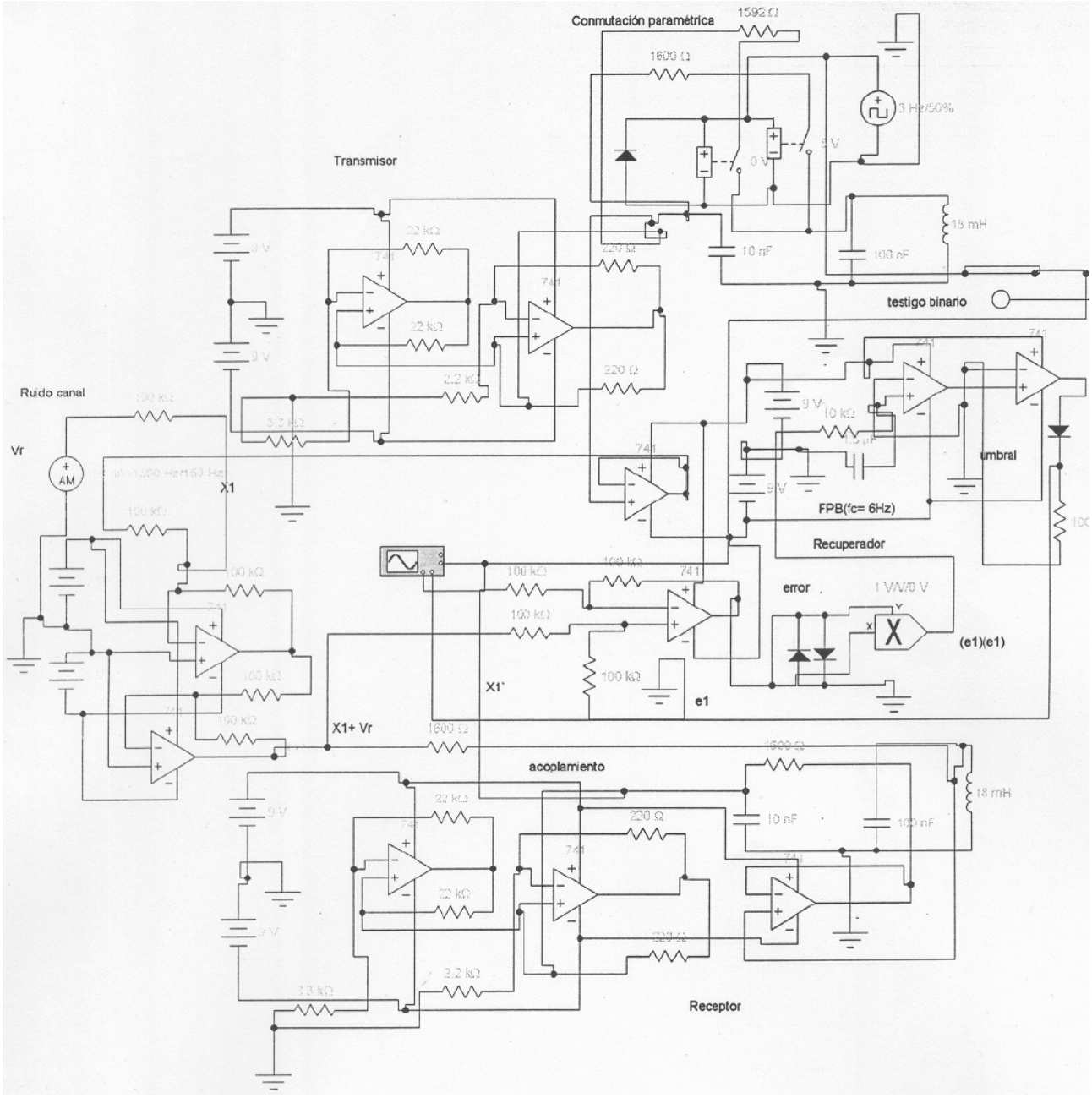

FIGURA 4. Diagrama del circuito del mensajero caótico binario:simulación con el Workbench.

ximo de ruido que acarrea un retardo mínimo en la recuperación del mensaje, etc. Los resultados se comparan con los de trabajos anteriores y se plantean algunas mejoras al mensajero propuesto.

En la Sec. 5 se presentan las conclusiones más relevantes, se manifiesta que el ruido en el canal es el enemigo a vencer en el mensajero estudiado, ya que la disminución en el cambio paramétrico facilita su incorporación y por lo tanto la recuperación de la información binaria ya no es fiel. Se tienen que negociar privacidad y confiabilidad para este tipo de circuito. Se propone un mensajero caótico digital como alternativa para abatir la incorporación del ruido en el canal.

2. Antecedentes

2.1. Lo no reportado en los mensajeros de demostración

Como ya se mencionó en la introducción, los mensajeros caóticos binarios de demostración propuestos por Parlitz *et al.* [1] y Cuomo *et al.* [2] no reportaron tres aspectos importantes que deben caracterizar a un sistema de este tipo, como lo son: a) el cambio mínimo en el parámetro P tal que su acción sobre la forma de onda de la señal caótica sincronizadora sea imperceptible a un posible espía en el canal ruidoso; b) el nivel máximo del ruido permitido en el canal para que la recuperación de la información sea confiable, aún cuando se opera bajo la condición del cambio mínimo en el parámetro;

y c) los retardos generados en la recuperación de la información binaria para de ellos conocer la velocidad máxima del envío de los mensajes. Es por eso que estos tres aspectos son los que averiguaremos y validaremos, tanto a nivel simulación como experimentación en este trabajo.

2.2. Algunos fundamentos sobre el tema

2.2.1. El circuito de Chua

El circuito de Chua [6] también se conoce como de doble espiral, porque produce un atractor en el que su dinámica pasa de una espiral a otra. Este circuito es autónomo no lineal compuesto por dos capacitores, una inductancia, dos resistencias lineales y un elemento no lineal. Este último es una conductancia lineal por fragmentos definida por una función $f(x_1)$ (2). La dinámica del circuito la describen las ecuaciones diferenciales normalizadas (1):

$$\begin{aligned} dtx_1 &= \alpha(\, x_2 - x_1 - f(x_1)), \\ dtx_2 &= x_1 - x_2 + x_3, \\ dtx_3 &= -\beta x_2, \end{aligned} \tag{1}$$

donde x_2, x_1, y x_3, son las variables o señales dinámicas que representan el voltaje a través de C_2, C_1, y la corriente en L, respectivamente. La falta de linealidad para el comportamiento caótico descrito por el circuito se asegura con la función $f(x_1)$ (2), llamada diodo de Chua [5], de la cual se presenta su plano de fase en la Fig. 3. Dicho plano, muestra los puntos de ruptura y los cambios de pendiente, ante una caracterización completa, obtenidas como lo indica Kennedy [7]. Aunque para el circuito de estudio solo se trabaja con las pendientes m_0 y m_1, y con sus dos puntos de ruptura. Dicha función se define (2) como

$$f(x_1) = bx_1 + 0.5(a - b)[|\, x_1 + 1| - |\, x_1 - 1|], \tag{2}$$

donde: $\alpha = 10$, $\beta = 14.9$, $a = -1.27$ y $b = -0.68$.

En las Figs. 4(Wb) y 17(SAP-Dadisp), se muestran los diodos y circuitos de Chua configurados como transmisor y receptor. En la literatura existen una gran cantidad de reportes sobre estos circuitos [5,7-10].

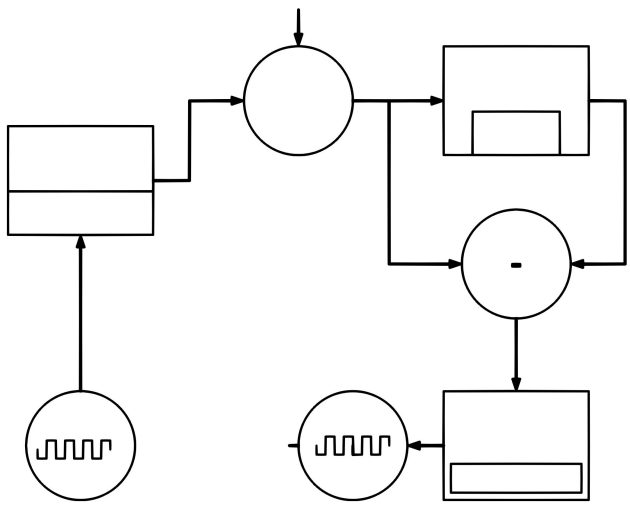

FIGURA 5. Diagrama a cuadros del mensajero caótico binario caracterizado.

2.2.2. Sincronización y conmutación paramétrica

Las ecuaciones normalizadas de sincronía para el receptor, según Pecora y Carroll [8], son

$$\begin{aligned} dtx_1' &= \alpha'(\, x_2' - x_1' - f(x_1')), \\ dtx_2' &= \mathbf{x}_1 - x_2' + x_3', \\ dtx_3' &= -\beta' x_2', \end{aligned} \tag{3}$$

donde su nomenclatura y valores son iguales que los del transmisor (1). Como ya se sabe de Pecora y Carroll y de otros [9-10], solamente se puede sincronizar por medio de las variables $\mathbf{x}_1$ y x_2. Para este caso se utiliza $\mathbf{x}_1$, la cual acopla y sincroniza ambos circuitos idénticos, como se muestra en los diagramas de los circuitos, ya mencionados, de las Figs. 4(Wb) y 17(SAP-Dadisp).

En la conmutación paramétrica [1-4,11-15], el transmisor presenta el parámetro P, el cual relaciona a los parámetros: β, a y b con la resistencia R del circuito de Chua y con los valores cercanos $P_0(R_0)$ y $P_1(R_1)$ [11] que se conectan al circuito en función del estado lógico del mensaje, m, *i.e.*, para un cero lógico se conecta P_0, que equivale a una R_0 de 1600Ω, y para su complemento se conecta P_1, que equivale a una R_1 de 1592Ω; para cada caso se generan formas de onda caóticas particulares y cuando se envían éstas al receptor (el cual ya tiene conectado el parámetro $P_0(R_0)$) permite su sincronización sólo con la generada por su parámetro símil (*i.e.*, sólo para el caso $P_0 = P_0'$). Cuando se encuentran sincronizados los circuitos, la señal de error, e_1, es casi cero (*i.e.*, $e_1 = x_1 - x_1'$, para una señal de ruido $v_r = 0$), y cuando están fuera de sincronía (*i.e.*, el caso $P_1 \neq P_0'$) existen magnitudes mayores a cero; ambos casos se operan para recuperar la información binaria. El proceso de sincronización no es instantáneo, requiere de un pequeño tiempo de sincronización, aunado al del circuito recuperador del mensaje binario. La clave está en que este cambio (en la forma de onda de la señal caótica) produzca señales casi idénticas, aun con ruido proveniente del canal. Por lo que si se desea privacidad, el cambio en el parámetro debe ser muy pequeño para que el de la forma de onda en el canal, sea imperceptible a un posible espía pero no para el receptor, el cual debe detectar el cambio aun con el mensaje distorsionado por el ruido. En la Fig. 4(Wb) se muestra en el circuito transmisor, la conmutación paramétrica (atendiendo a una señal de onda cuadrada que simula una transmisión binaria continua) y, en el circuito receptor, la recuperación de la información mencionada.

3. Procedimiento de caracterización

Para poder conocer los aspectos no reportados en los mensajeros demostrativos de la Sec. 2.1, se realiza y construye un mensajero caótico binario, el cual se basa en los diagramas a cuadros y del circuito de las Figs. 5 y 4(Wb), respectivamente. Se trabajan esquemas semejantes para poder validar sus resultados, *i.e.*, los de la simulación, con el programa Work-

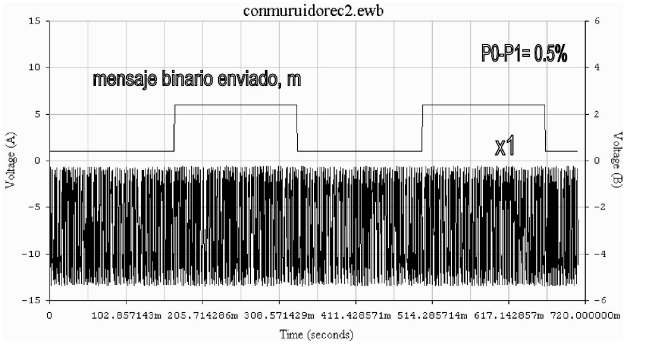

FIGURA 6. Muestra el mensaje binario m (f_m= 3Hz)y la forma de onda de la señal caótica sincronizadora x_1; observe el cambio que sufre ésta, al conmutar el mensaje de 0 a 1 para un ΔP de 0.5 %, es casi imperceptible.

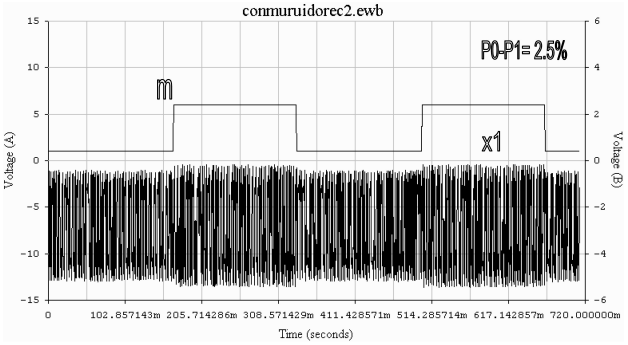

FIGURA 7. Muestra el mensaje binario m y la forma de onda de la señal caótica sincronizadora x_1; observe el cambio que sufre ésta, al conmutar el mensaje de 0 a 1 para un ΔP de 2.5 %, es bastante perceptible.

bench (Wb), y los de la implementación, obtenidos y analizados por el Sistema Automático de Prueba-Dadisp (SAP-Dadisp) [6].

3.1. Simulación con el programa Workbench (Wb)

Para averiguar por el cambio mínimo en el parámetro (*i.e.* el ΔP_{min}= P_0-P_1), tal que sea invisible para un posible espía en el canal, pero no para el receptor, ya que éste debe detectar dicho cambio, aún con ruido de cierto nivel proveniente del canal, para recuperar la información binaria de una manera casi instantánea**,** primero se conocen los porcentajes de cambio en los parámetros reportados en los trabajos de Parlitz y de Cuomo que son del 3 % (*v.g.*, capacitor ΔC, C_0= 10.04nF y C_1= 9.79nF) y del 9 % (*v.g.*, voltaje ΔV, V_0= 4.0V y V_1= 4.4V), respectivamente (c.f., Figs. 1 y 2); sin considerar ruido en el canal. En seguida, y utilizando el programa Wb, se varía el parámetro P de 0 a 2.5 % (*i.e.*, R pasa de 1600Ω(P_0) a 1560Ω(P_1)) y se registran los resultados, tanto de la forma de onda como del error, así como también el de la información binaria recuperada; en esta etapa no se considera la incorporación del ruido en el canal. Se observa que, a cambios cercanos al 0.5 % de P_0 (*i.e.*, R_0= 1600Ω(P_0) y R_1= 1592Ω(P_1)), el proceso resulta casi invisible en el canal, más sin embargo el receptor sigue operando apropiadamente. En las Figs. 6 y 7 se presentan los resultados correspondientes a los ΔP_0's de 0.5 y 2.5 %, respectivamente. En la figura superior se presenta la información binaria m, por enviar, y su cambio de estado. Obsérvese que para el caso del 2.5 %, se aprecia perfectamente, en la forma de onda de x_1, el cambio o distorsión de su amplitud. Por lo que cualquier espía, a simple vista, puede detectar este cambio y descubrir la existencia del mensaje binario. En la Fig. 8, se presentan las señales x_1 y x_1' sincronizadas (*i.e.*, cuando P_0= P_0') en forma sobrepuesta y a una frecuencia del mensaje f_m de 3Hz. Como puede observarse son casi idénticas. En las Figs. 9 y 10, se presentan los planos de fase (*i.e.*, x_1/ x_1') para los casos de las señales sincronizadas y no sincronizadas, respectivamente. En la Fig. 11, se presenta la señal de error al cuadrado (*i.e.*, e_1^2= (x_1- x_1')^2) y el mensaje binario enviado, m.

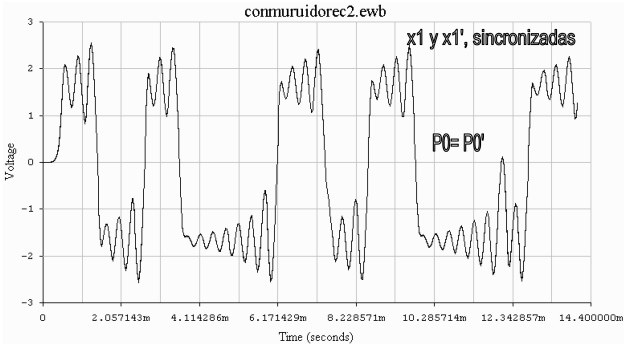

FIGURA 8. Se presenta las señales x_1 y x_1' sincronizadas (*i.e.*, P_0= P_0') y encimadas, para el caso de ΔP_{min}= 0.5 %.

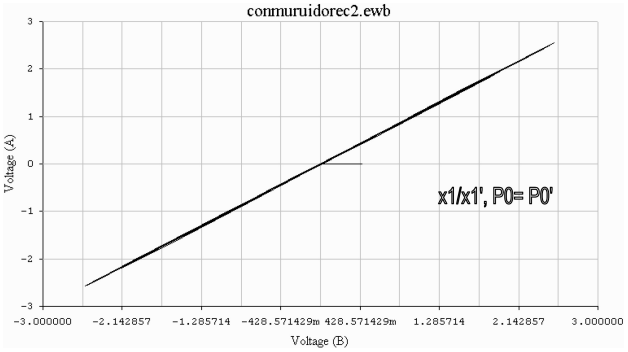

FIGURA 9. Se presenta el plano de fase entre x_1 y x_1', x_1/x_1', para el caso ΔP_{min}= 0.5 % y permaneciendo sincronizadas.

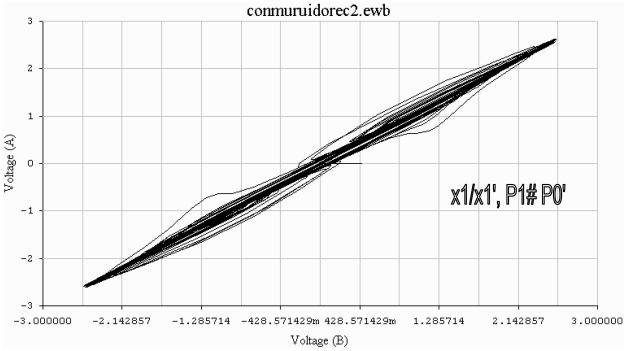

FIGURA 10. Se presenta el plano de fase entre x_1 y x_1', x_1/x_1', para el caso ΔP_{min}= 0.5 % y permaneciendo fuera de sincronía.

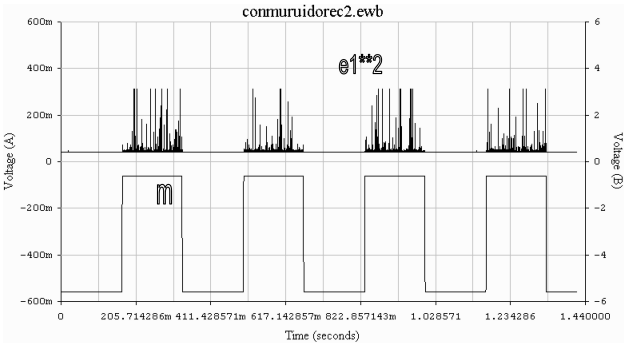

FIGURA 11. Muestra el mensaje binario m (f_m= 3Hz) y el error en la sincronía al cuadrado, para el caso ΔP_{min}= 0.5 % y sin ruido en el canal.

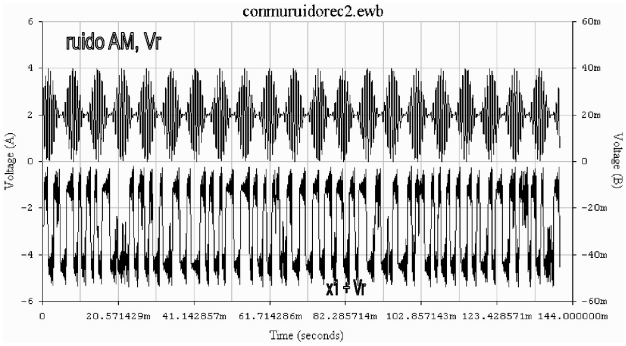

FIGURA 12. Se presentan las señales de ruido, v_r, y la caótica sincronizadora x_1 sumada a v_r (*i.e.*, $x_1 + v_r$).

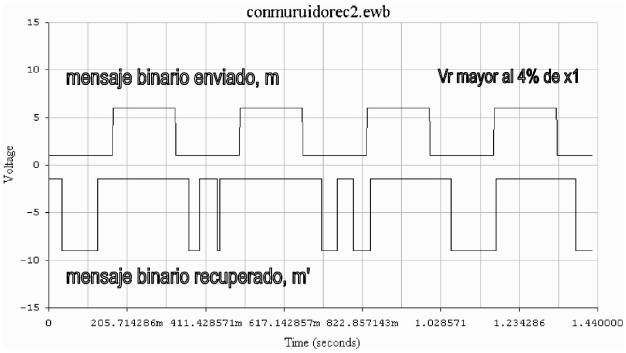

FIGURA 13. Se muestran los mensajes binarios enviado, m, y recuperado, m', para el caso ΔP_{min}= 0.5 % y con una magnitud de $v_r > 4$ %. Bajo esta condición, ya no es confiable el mensajero de estudio.

Ya habiendo obtenido el porcentaje mínimo de variación del parámetro P, *i.e.*, el de 0.5 % de P_0, sumamos a la señal caótica x_1 (*v.g.*, $x_{1máx}$= 2.5Vp) una señal de ruido, v_r (*v.g.*, $x_1 + v_r$), del tipo amplitud modulada (AM), con características variables de amplitud (*v.g.*, 0-250mVp) y con frecuencias fijas (*v.g.*, portadora de 1500Hz y modulante de 150Hz), como lo indica la Fig. 12. Se varía la magnitud de v_r, de 0 a 10 % de la magnitud de x_{1max}, y se sigue el procedimiento y los puntos de evaluación como en el caso anterior, *i.e.*, se incrementa la magnitud de la señal ruidosa hasta que el receptor provoque errores en la recuperación de la señal binaria m'(c.f., Fig. 13). Para el caso particular, resultó que un nivel de ruido del 4 % de la señal encriptadora x_{1max} es justo el tolerable.

Finalmente, se registra el retardo impuesto por el filtro paso bajas, con una frecuencia de corte de 6Hz, incorporado en el circuito recuperador. Su registro se realiza comparando, instantáneamente, las señales de los mensajes: enviado, m, y recuperado, m', como lo indican las Figs. 14 y 15; considerando un nivel de ruido v_r de 100 mVp, equivalente al 4 % de x_{1max}. Este retardo (en la recuperación) es variable y

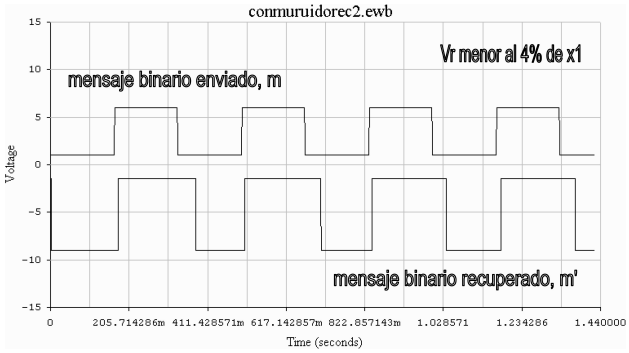

FIGURA 14. Se muestran los mensajes binarios enviado, m, y recuperado, m', para el caso ΔP_{min}= 0.5 % y con una magnitud de $v_r < 4$ %. Bajo esta condición, si es confiable el mensajero de estudio.

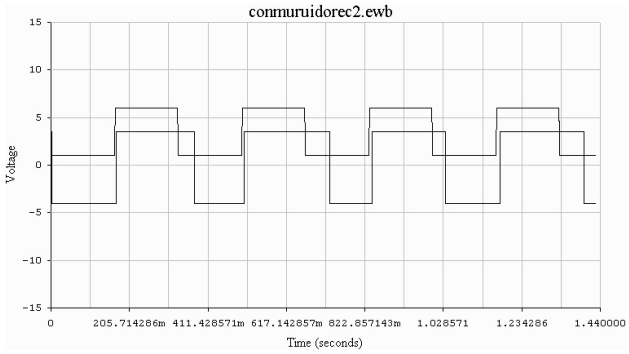

FIGURA 15. Se muestran los mensajes binarios enviado, m, y recuperado, m', encimados. Se observan claramente los retardos de adquisición y recuperación, para el caso ΔP_{min}= 0.5 %, con una magnitud de $v_r < 4$ % y f_m= 3Hz.

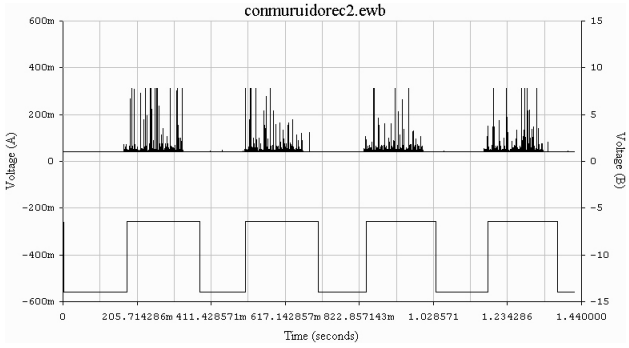

FIGURA 16. Muestra el mensaje binario m' (f_m= 3Hz) y el error en la sincronía al cuadrado, para el caso ΔP_{min}= 0.5 % y con una magnitud de vr< 4 %.

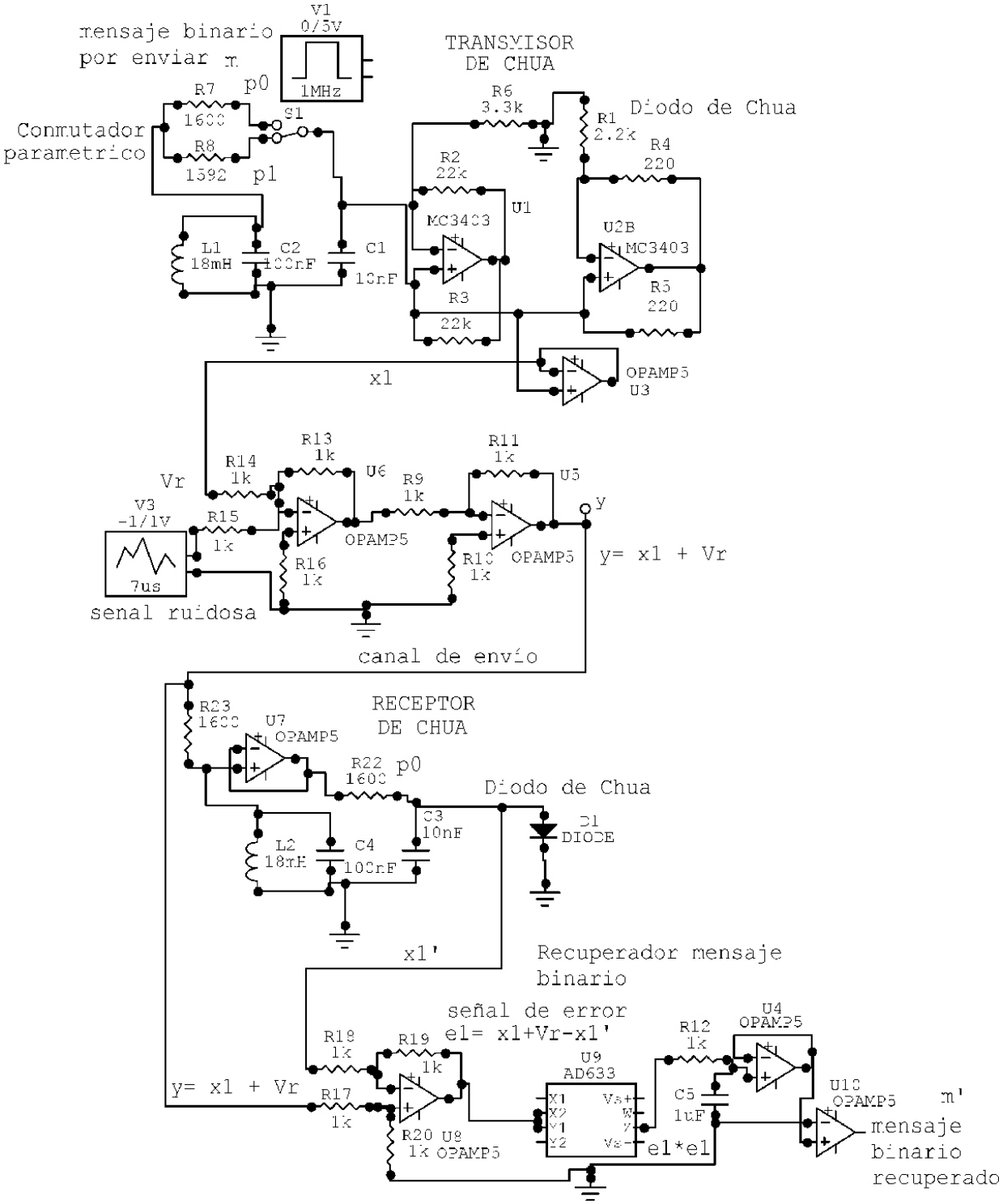

FIGURA 17. Diagrama del circuito del mensajero caótico binario: experimental con el SAP-Dadisp.

presenta un alcance de 10 a 70mseg, lo cual es normal puesto que atiende a una señal caótica. El retardo mencionado se utiliza para conocer la velocidad del mensajero, *i.e.*, los bits por segundo a los cuales puede operar confiablemente. En la Sec. 4 se presentan algunas especificaciones que sirven para evaluar el rendimiento y la confiabilidad ante el cambio paramétrico, el nivel de ruido en el canal y el retardo en los *mensajeros* estudiados, *v.g.*, tal cambio paramétrico puede tolerar un nivel de ruido que permite recuperar rápidamente al mensaje binario m'.

En la Fig. 16, se presenta la señal del error al cuadrado, e_1^2, y la señal de información binaria recuperada, m', para el caso cuando: ΔP_{min}= 0.5 %, v_r= 100mVp y f_m= 3Hz.

TABLA I. Especificaciones obtenidas de los mensajeros estudiados.

Mensajeros estudiados:	Variación paramétrica, ΔP_m [%]	Nivel ruido, v_r [%,mVp]	Frecuencia del mensaje, f_m [Hz]	Retardo de recuperación [mseg]
Simulado (Wb)	0.5	4, 100 (AM)	3	10-70
Experimental (SAP-Dadisp)	1.0	8, 200 (Aleatorio)	5	2-20

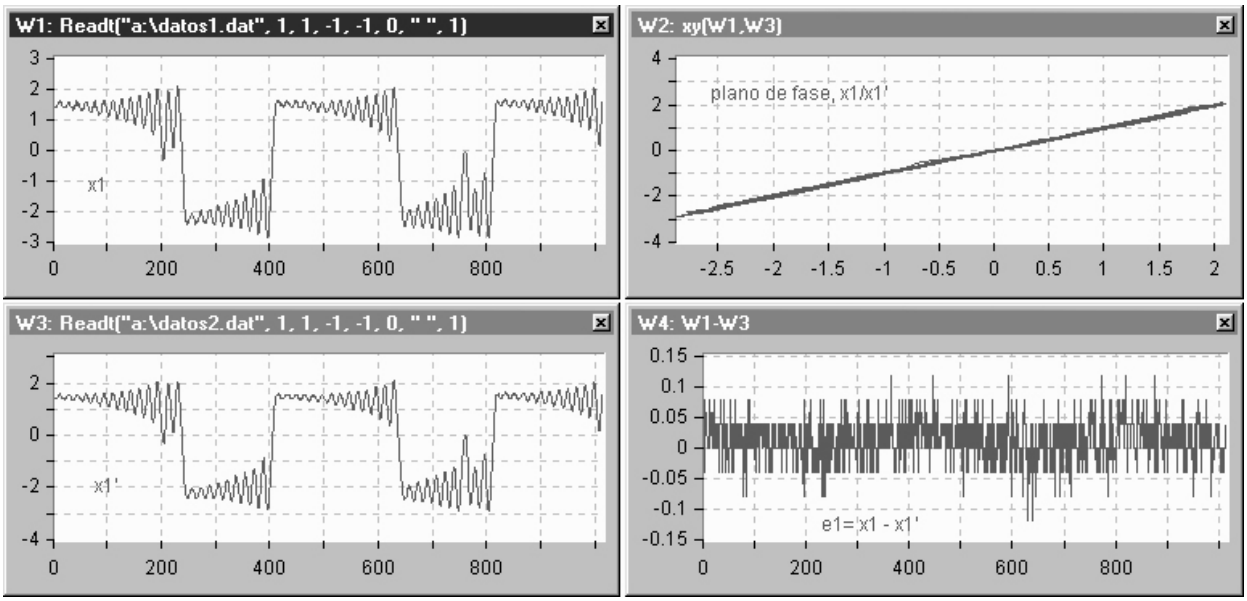

FIGURA 18. Mediciones de las señales caóticas x_1 y x_1' en sincronía, obtención del plano de fase y de la señal error e_1, utilizando el SAP-Dadisp.

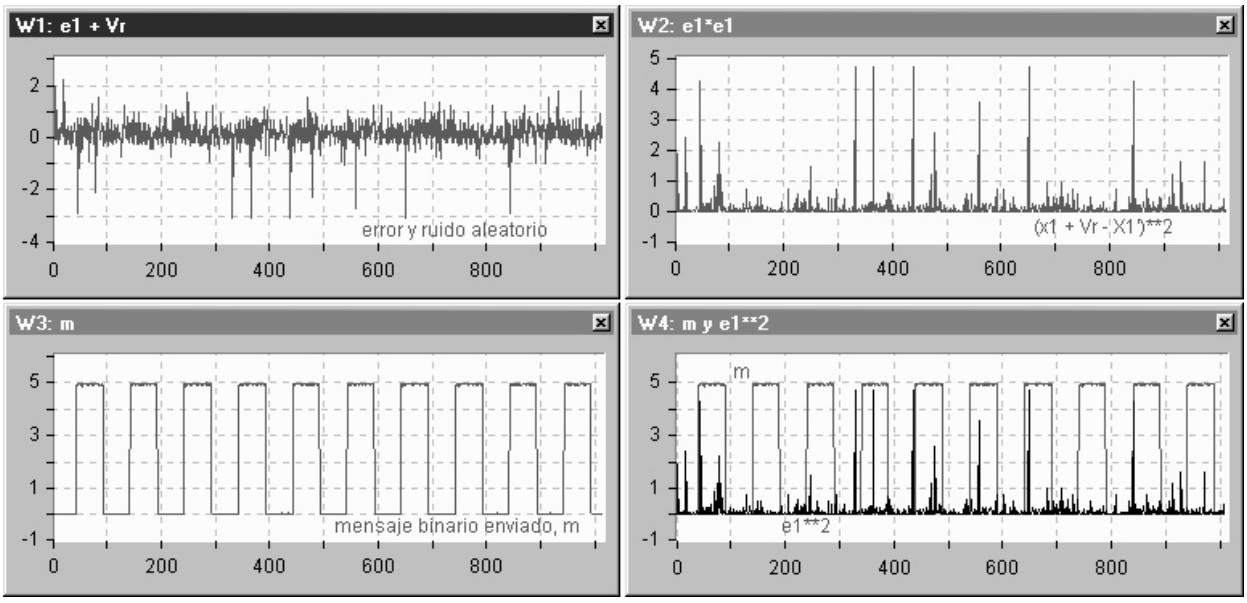

FIGURA 19. Medición de la señal error e_1 y del mensaje binario m, obtención del cuadrado del error e_1^2 y su comparación con m.

3.2. Experimentación y análisis con el SAP-Dadisp

Se utiliza el Sistema Automático de Pruebas, SAP-Dadisp[6], para realizar las mediciones y el análisis de las principales señales del *mensajero* en estudio (c.f., con el diagrama de la Fig. 17(SAP-Dadisp), *v.g.*, las señales: x_1, de error, de los mensajes m y m', etc.

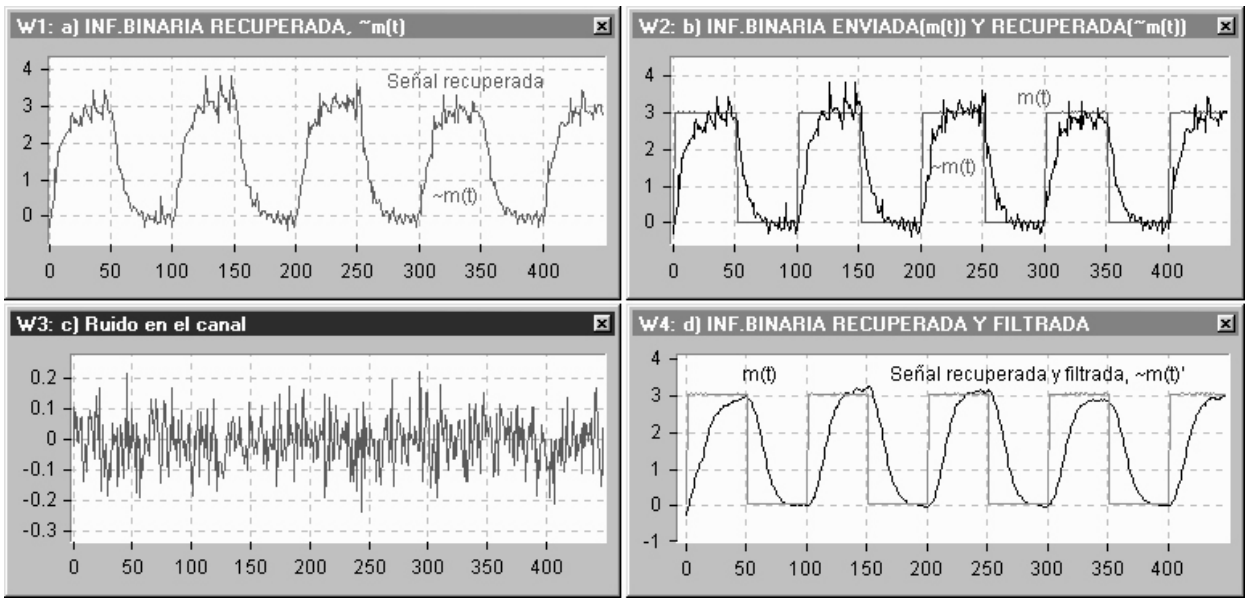

FIGURA 20. Mediciones de los mensajes binarios recuperado, m', enviado, m, del ruido aleatorio en el canal, v_r, y de la salida del filtro analógico promediador, ∼m'. Se comparan, instantáneamente, los mensajes medidos entre sí para observar los retardos de adquisición y recuperación.

En la Fig. 18, se presentan en las ventanas W_1 y W_3 las mediciones de la señal x_1 y x_1', en condiciones de sincronía y con ruido mínimo en el canal, respectivamente. La diferencia entre éstas y su plano de fase se muestra en las ventanas W_4 y W_2, respectivamente. Observe que el error en la sincronía, e_1, se mantiene acotado alrededor de +/-100mVp. Este error, producto principalmente de la desigualdad existente entre las tolerancias de los componentes de los circuitos transmisor y receptor del *mensajero* construido. En la Fig. 19, ventanas W_1 y W_2, se presentan el error e_1 y su valor al cuadrado habiendo sumado ya a x_1 la señal de ruido, v_r, de 200mVp; todo esto en atención a la señal del mensaje m, cuya frecuencia, para este caso, es de 5Hz y la cual se presenta en la ventana W_3. En la ventana W_4, se muestran la señal de mensaje m sobrepuesta a la señal del error al cuadrado correspondiente. Experimentalmente, el cambio paramétrico mínimo obtenido fue del orden del 1 % del parámetro P_0 (*i.e.*, los valores registrados son: R_0= 1600Ω(P_0) y R_1= 1584Ω(P_1)) (c.f., Sec. 3.1). En la Fig. 20, ventana W_2, se muestran sobrepuestas las señales de los mensajes binarios enviado y recuperado, m y m', respectivamente. De las mismas, se puede observar el retardo en la recuperación producto del filtro paso bajas, ya mencionado en la sección anterior. En las ventanas W_1 y W_4, se presentan las mediciones de las señales de información binaria recuperada y filtrada analógicamente, como lo hizo Cuomo, y digitalmente, como lo hizo Parlitz (c.f., Figs. 1 y 2). En ambos casos se puede observar el retardo producto de los filtrajes ya mencionados. Finalmente, se presenta, en la ventana W_3, la señal de ruido aleatorio máximo $v_{r(máx)}$ que permite (v.g., v_r= 200mVp, equivalente al 8 % de x_{1max}) la recuperación de la información binaria y facilita la prueba del *mensajero* implementado.

4. Resultados y mejoras

De los resultados de la simulación (Wb) y de la experimentación (SAP-Dadisp[6]), podemos reportar las especificaciones para los *mensajeros* estudiados que aparecen en la Tabla I.

Del estudio comparativo entre los *mensajeros*, simulado y experimental, se desprende que existen coincidencias interesantes:

a) En lo que respecta al cambio mínimo en el parámetro (ΔP_{min}). En el simulado (Wb), éste resultó menor que en el experimental como era de esperarse para los casos con y sin ruido.

b) Respecto al nivel de ruido máximo, $v_{r(máx)}$, al cual todavía se permite la recuperación de la información binaria, el experimental resultó más robusto.

c) En la recuperación casi instantánea, se observó que el experimental responde más rápido puesto que su retardo es 3 veces menor.

Es conveniente mencionar que la fuente de ruido, en el caso experimental, es aleatoria y su magnitud se hizo variar de manera semejante a la del ruido AM, la cual se utiliza en el caso de la simulación (Wb).

Por otro lado, es posible incrementar la velocidad de envío de los mensajes binarios cambiando el valor de los componentes pasivos de los circuitos de Chua [11,15] del mensajero implementado; aunque hay que considerar el retardo en la recuperación, ya que éste siempre existirá y representará por su magnitud una limitación importante.

Observando los porcentajes de ruido obtenido para los *mensajeros estudiados* podemos decir que no resultan muy resistentes ante el ruido del canal, como se desearía para competir con aplicaciones de encriptamiento comerciales [4,13],

en ambientes ruidosos, por lo que una mejora sería mantener al ruido fuera del canal por medio de algunas técnicas eficientes de abatimiento de éste propuestas por Ott [16]. Ahora bien, se puede comentar que el tipo de *mensajero* estudiado resulta limitado por su principio de operación, puesto que entre más pequeño se hace el cambio paramétrico, para evitar la detección del cambio en la forma de onda caótica sincronizadora por un espía, se favorece a que un menor *ruido* distorsione la señal y por lo tanto el receptor no pueda recuperar la información binaria; aunado al incremento en el tiempo de recuperación producto del filtraje. Para el caso, se tiene que negociar entre privacidad y confiabilidad. Siendo el factor toral el ruido en el canal, por lo que si éste se abate, *i.e.*, $v_r = 0$, como sería, aproximadamente, en un canal completamente digital podría mejorarse, notablemente, la negociación anterior, *i.e.*, convertir el mensajero estudiado en un mensajero caótico digital.

5. Conclusiones

La disminución en el cambio paramétrico facilita la incorporación del ruido en el canal y por ende la recuperación de la información binaria ya no es fiel, lo que lleva a una negociación difícil de lograr entre privacidad y confiabilidad, para el *mensajero* estudiado. Los cambios paramétricos obtenidos para el mismo de 0.5 y de 1 % en la simulación y la experimentación, respectivamente, producen cambios imperceptibles, en la señal caótica sincronizadora, para un espía en el canal, y permiten que aún hasta con un nivel de ruido del 4 %, de la señal caótica, se pueda recuperar la información binaria; arriba de éste, el mensajero ya no es confiable. Como puede observarse, el mensajero caracterizado presenta una robustez muy limitada, ante el ruido del canal, y esto contribuye a que la velocidad en el envío de mensajes sea muy baja. Pese a la incorporación de algunas técnicas de eliminación de ruido no se logra mejorar la robustez lo suficiente para asegurar su competencia con los encriptadores comerciales. Una solución viable es utilizar un mensajero caótico digital, *i.e.*, enviar digitalizada la señal encriptadora y sincronizadora $\mathbf{x}_1$.

Agradecimientos

Agradecemos al CONACYT por apoyar económicamente el presente. Proyecto 31874-1, dirigido por el Dr. C. Cruz H.

1. U. Parlitz, L.O. Chua, Lj. Kocarev, K.S. Halle y A. Shang, *Int. J. Bifurc. Chaos* **2** (1992) 973.
2. K.M. Cuomo, A.V. Oppenheim y S.H. Strogatz, *IEEE Trans. on Circuits and Systems-II: Analog and Digital Signal Processing* **40** (1993).
3. H. Dedieu, M. Kennedy y M. Hasler, *IEEE Trans. Circuits Syst. II* **40** (1993) 634.
4. C. Cruz H., D. Lopez M., V. García G., H. Serrano G. y R. Núñez P., *Int. Conf. on Com., Circs. and Syts. and W. Sino Expo.* Chendú, China (2002).
5. L.O. Chua, Lj. Kcarev, K. Eckert y M. Itoh, *Int. J. Bifurc. Chaos* **2** (1992) 705.
6. R. Núñez P., "Los SAP's-Labview (Generador/ Analizador Dinámico) y Dadisp", Informe Técnico: CTETT9913, DET-CICESE (1998).
7. M.P. Kennedy,"Experimental chaos via Chua's circuit", in Proc.of the **1**st. Experimental Chaos Conference, ed. S. Vohra, M. Spano, M. Shlesinger, L. Pecora y W. Ditto, (W. S.) (1992) 340.
8. T.L. Carroll y L.M. Pecora, *IEEE Trans. on Circuits and Systems* **38** (1991) 453.
9. M. Hasler,"Synchronization principles and applications", in Circuits and Systems Tutorials, C. Toumazou, Ed. Piscataway, NJ: IEEE, (1994) 314.
10. F.C. Moon, "Chaotic and fractal dynamics, an introduction for applied scientist and engineers", Wiley and Sons, Inc., (1992) 758.
11. M.O. Meranza C. y C. Cruz H., "Estudio experimental de la sincronía de dos circuitos hipercaóticos de Chua", Proc. of the$\mathbf{2}^{nd}$. Int. Conf. On Aut.Cont., AUT'2002, Santiago de Cuba, Cuba (2002).
12. M. Hasler y Th. Schmming, *IJBC* **10** (2000) 719.
13. N.J. Corron y D.W. Hahs, *IEEE Trans. Circuits Systems I* **44** (1997) 373.
14. A.V. Oppenheim, G.W. Wornell, S.H. Isabelle y K.M. Cuomo, "Signal processing in the context of chaotic signals", in Proc. IEEE ICASSP, **IV** (1992).
15. R. Núñez P., "Kosímetro de Chua", Con. Nac. de la AMCA2004, Méx. D.F. (2004).
16. H. Ott, "Noise Reduction Techniques in Electronic Systems", $\mathbf{2}^a$ Ed., W.& S.(1998).