Sincronización de Atractores con Múltiples Enrollamientos y una Aplicación a la Comunicación Secreta*

Elizabeth Díaz-Moreno, Luis Gámez-Guzmán, Pedro Ayala-Morales, César Cruz-Hernández, Ricardo Núñez-Pérez
Departamento de Electrónica y Telecomunicaciones
Centro de Investigación Científica y Educación Superior de Ensenada (CICESE)
Km. 107 Carretera Tijuana-Ensenada, 22860 Ensenada, B.C., México.

Resumen

Este artículo presenta la sincronización de atractores con múltiples enrollamientos ("scrolls"), a partir de formas hamiltonianas y el diseño de un observador. Se lleva a efecto una aplicación de tal sincronía, a la comunicación secreta de señales analógicas y digitales, donde la calidad de la información decodificada en el receptor, resulta mayor que la obtenida por técnicas tradicionales que emplean también observadores, mientras que la codificación de la información permanece potencialmente segura.

Palabras claves: Sincronización de caos, atractores con enrollamientos múltiples, observador, comunicación secreta.

1 Introducción

El encriptamiento de información utilizando dinámicas caóticas, fue sugerido en 1990 por Pecora y Carroll [1] como método alterno para codificación de información, que difiere sustancialmente de los métodos convencionales de encriptamiento, los cuales, emplean sofisticados algoritmos numéricos. Desde entonces, diversos métodos se han propuesto para transmitir oculto un mensaje con base en **sincronización caótica**: *codificación caótica aditiva*, *conmutación entre atractores caóticos*, *modulación paramétrica caótica*, etc. Sin embargo, se ha mostrado posteriormente, que en algunos casos, la información oculta en el caos (con sólo un exponente de Lyapunov positivo), se puede extraer por algún receptor intruso, ya sea empleando técnicas de procesamiento de señales o bien mapeos de reconstrucción [2], [3]. Quedando demostrado con esto, dos factores relevantes en la seguridad de estos sistemas, que son: la *dimensión del atractor caótico* y el *esfuerzo requerido para obtener la igualdad en los valores de los parámetros en transmisor y receptor.* Una forma de incrementar la seguridad en la comunicación caótica, es aplicar algoritmos criptográficos a la información y mezclarla posteriormente con el caos [4]. Otra, consiste en aumentar la dimensión del atractor, dando lugar a atractores hipercaóticos [5]. Otra alternativa, es sincronizar osciladores con retardo de tiempo [6], [7], ya que tales osciladores cuentan con un espacio de estados de dimensión infinita y despliegan atractores hipercaóticos con un número arbitrario de exponentes de Lyapunov positivos.

Un asunto relevante en la construcción de sistemas de comunicación tanto analógicos como digitales basados en caos [8], es la **selección del generador de caos**. El circuito de Chua es probablemente el oscilador caótico más conocido y comunmente empleado en este campo. El circuito de Chua resulta un paradigma para el caos [9], en el sentido que constituye un circuito eléctrico no lineal, relativamente sencillo, que exhibe una rica variedad de comportamientos dinámicos. Entre las muchas implementaciones y generalizaciones reportadas en la literatura, sobre este circuito, encontramos atractores cada vez más complicados, obtenidos básicamente de dos maneras: incrementando la dimensión en el estado del circuito [5], [10], donde se han agregado más puntos de ruptura en la no linealidad del circuito de Chua, produciendo con esto dinámicas más complejas (formando atractores con enrollamientos múltiples) que las que exhibe el circuito original. El objetivo que se persigue con esto, es diseñar sistemas de encriptamiento de información confidencial, construidos con base en atractores más complicados, de tal manera que sean inmunes a las técnicas de desencriptamiento por algún receptor no autorizado.

En nuestro caso, con el propósito de contribuir al incremento en la seguridad de los sistemas de comunicación con base en la sincronía de caos, se empleará el circuito de Chua generalizado.

El objetivo del artículo, es extender la metodología propuesta en [11], a la sincronización de atractores con múltiples enrollamientos y dar una aplicación de este resultado, a la comunicación secreta de información analógica y digital. Mencionamos algunas ventajas sobre otros métodos de sincronización: i) la sincronización se ob-

*Trabajo financiado por el *CONACYT* a través del Proyecto de Investigación 31874 − *A*.

tiene de manera sistemática, *ii*) se puede aplicar a muchos osciladores caóticos e hiperca óticos, *iii*) no requiere el cálculo de ningún exponente de Lyapunov y *iv*) no requiere que las condiciones iniciales pertenezcan a la misma cuenca de atracción.

2 Sincronización del circuito de Chua generalizado

Considere el siguiente sistema

$$\dot{x} = f(x), \qquad x \in \mathbb{R}^n \tag{1}$$

con f una función no lineal, que modela las dinámicas complejas de un circuito caótico, en particular, presenta una familia de atractores con múltiples enrollamientos, dependiendo del valor de los parámetros. Siguiendo la metodología propuesta en [11], el sistema (1) se puede escribir en la siguiente forma *"canónica hamiltoniana generalizada"*

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + \mathcal{S}(x)\frac{\partial H}{\partial x} + \mathcal{F}(x), \qquad x \in \mathbb{R}^n \tag{2}$$

$H(x)$ es una *función de energía suave*, definida positiva en $\mathbb{R}^n$. El *vector gradiente* $\frac{\partial H}{\partial x}$ se asume su existencia en cualquier parte. Se utiliza una función de energía cuadrática $H(x) = 1/2\, x^T \mathcal{M}\, x$ con $\mathcal{M}$ matriz constante, simétrica y definida positiva. Tal que $\frac{\partial H}{\partial x} = \mathcal{M}\, x$. Las matrices cuadradas $\mathcal{J}(x)$ y $\mathcal{S}(x)$ satisfacen, para toda $x \in \mathbb{R}^n$, las propiedades: $\mathcal{J}(x) + \mathcal{J}^T(x) = 0$ y $\mathcal{S}(x) = \mathcal{S}^T(x)$.

En (2), el campo vectorial $\mathcal{J}(x)\frac{\partial H}{\partial x}$ exhibe la parte *conservativa* y $\mathcal{S}(x)\frac{\partial H}{\partial x}$ la parte *no conservativa*. En algunos casos, $\mathcal{S}(x)$ es *definida negativa* o *semidefinida negativa*, entonces $\mathcal{S}(x)\frac{\partial H}{\partial x}$ es la parte disipativa. Por otra parte, si $\mathcal{S}(x)$ es definida positiva, semidefinida positiva o de signo indefinido, representa la parte *desestabilizante* en forma global, semiglobal ó local, respectivamente. En el último caso, siempre podemos (aunque no de forma única) descomponer $\mathcal{S}(x)$ en la suma de una matriz simétrica semidefinida negativa $\mathcal{R}(x)$ y una matriz simétrica semidefinida positiva $\mathcal{N}(x)$. $\mathcal{F}(x)$ representa el campo vectorial localmente *desestabilizante*.

En el contexto de diseño de observadores, se considera una clase especial de formas hamiltonianas generalizadas con campo vectorial desestabilizante y una salida $y(t)$, dada por

$$\begin{aligned} \dot{x} &= \mathcal{J}(y)\frac{\partial H}{\partial x} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial x} + \mathcal{F}(y), \qquad x \in \mathbb{R}^n \\ y &= \mathcal{C}\frac{\partial H}{\partial x}, \qquad y \in \mathbb{R}^m \end{aligned} \tag{3}$$

con $\mathcal{S}$ matriz simétrica constante, no necesariamente de signo definido e $\mathcal{I}$ matriz constante antisimétrica.

$\xi(t)$ es el *estimado* del estado $x(t)$ y se considera que $H(\xi)$ es la particularización de H en términos de $\xi(t)$. Similarmente, se representa por $\eta(t)$ a la salida estimada y calculada en términos de $\xi(t)$. El vector gradiente $\frac{\partial H(\xi)}{\partial \xi}$ es naturalmente de la forma $\mathcal{M}\xi$ con $\mathcal{M}$ una matriz constante, simétrica y definida positiva.

Un observador no lineal para (3) está dado por

$$\begin{aligned} \dot{\xi} &= \mathcal{J}(y)\frac{\partial H}{\partial \xi} + (\mathcal{I}+\mathcal{S})\frac{\partial H}{\partial \xi} + \mathcal{F}(y) + K(y-\eta), \\ \eta &= \mathcal{C}\frac{\partial H}{\partial \xi} \end{aligned} \tag{4}$$

con K la *ganancia* del observador.

El *error de estimación del estado* está definido por $e(t) = x(t) - \xi(t)$ y la salida del sistema del error estimado por $e_y(t) = y(t) - \eta(t)$, ambos gobernados por el sistema dinámico

$$\begin{aligned} \dot{e} &= \mathcal{J}(y)\frac{\partial H}{\partial e} + (\mathcal{I}+\mathcal{S}-K\mathcal{C})\frac{\partial H}{\partial e}, \qquad e \in \mathbb{R}^n \\ e_y &= \mathcal{C}\frac{\partial H}{\partial e}, \qquad e_y \in \mathbb{R}^m \end{aligned} \tag{5}$$

$\frac{\partial H}{\partial e}$ con abusos de notación, es el vector gradiente de la función de energía *modificada* $\frac{\partial H(e)}{\partial e} = \frac{\partial H}{\partial x} - \frac{\partial H}{\partial \xi} = \mathcal{M}(x-\xi) = \mathcal{M}e$. Se escribirá, cuando sea necesario $\mathcal{W} = \mathcal{I} + \mathcal{S}$.

Sincronización caótica: Se dice que el sistema receptor (4) sincroniza con el sistema transmisor (3), si $e(t) \to 0$ a medida que $t \to \infty$, donde $e(t)$ representa el error de sincronía.

Circuito de Chua generalizado. Considere el siguiente circuito de Chua generalizado propuesto en [10] por Suykens *et al.*

$$\begin{aligned} \dot{x}_1 &= \alpha(x_2 - h(x_1)), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2, \end{aligned} \tag{6}$$

con característica no lineal definida por la función

$$\begin{aligned} h(x_1) = m_{2q-1}x + \\ + \frac{1}{2}\sum_{i=1}^{2q-1}(m_{i-1} - m_i)(|x+c_i| - |x-c_i|) \end{aligned} \tag{7}$$

la cual, consiste de múltiples puntos de quiebre (función lineal por segmentos), con q un número natural. Es bien conocido que con $q = 1$, $\alpha = 9$ y $\beta = 14.286$ se obtiene el atractor de **doble enrollamiento** [10], Al definir $\mathbf{m} = (m_0; m_1; \cdots; m_{2q-1})$ y $\mathbf{c} = (c_1; c_2; \cdots; c_{2q-1})$ se obtienen los siguientes atractores de ***n*-enrollamientos**: atractor con doble enrollamiento [10]: $q = 1$, $\mathbf{m} = \left(-\frac{1}{7}; \frac{2}{7}\right)$, $\mathbf{c} = 1$. Atractor con 3 enrollamientos [10]:

$q = 2,\ \mathbf{m} = \left(\frac{0.9}{7}; -\frac{3}{7}; \frac{3.5}{7}; -\frac{2.4}{7}\right),\ \mathbf{c} = (1; 2.15; 4)$. Atractor con 4 enrollamientos [10]: $q = 2, \mathbf{m} = \left(-\frac{1}{7}; \frac{2}{7}; -\frac{4}{7}; \frac{2}{7}\right)$, $\mathbf{c} = (1; 2.15; 3.6)$. Atractor con 5 enrollamientos [10] (ver figura 1): $q = 3,\ \mathbf{m} = \left(\frac{0.9}{7}; -\frac{3}{7}; \frac{3.5}{7}; -\frac{2.7}{7}; \frac{4}{7}; -\frac{2.4}{7}\right)$, $\mathbf{c} = (1; 2.15; 3.6; 6.2; 9)$.

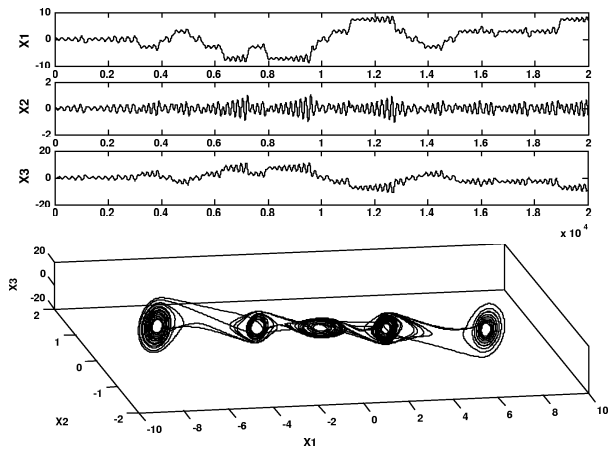

Figura 1: Dinámica compleja de los estados y atractor con 5 enrollamientos de (6) y (7) para $q = 3$.

Los componentes de $\mathbf{m}$ tienen signos alternados. El signo de m_0 es negativo en el caso en que n es impar para los n-enrollamientos (número de enrollamientos impar). Los atractores de n-enrollamientos con número par son generados por (6)-(7) al considerar los mismos valores en los parámetros α y β pero el signo opuesto para $\mathbf{m}$ en la no linealidad $h(x_1)$. Es importante decir que para $q = 2$ se generan atractores con 3 y 4 enrollamientos, dependiendo de los valores de $\mathbf{m}$ que se consideren. Resultados experimentales con estos tipos de atractores con enrollamientos múltiples se reportan en [10].

En este trabajo, se sincroniza el circuito de Chua generalizado (6)-(7) que exhibe atractores con 5 enrollamientos; es decir, con $q = 3$, $\mathbf{m} = \left(\frac{0.9}{7}; -\frac{3}{7}; \frac{3.5}{7}; -\frac{2.7}{7}\right)$ y $\mathbf{c} = (1; 2.15; 3.6; 6.2; 9)$.

El circuito **transmisor** empleando el circuito de Chua generalizado (6)-(7) en la forma (3), está dado por

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -3 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \\ + \begin{bmatrix} 0 & \alpha & 0 \\ \alpha & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial x} + \begin{bmatrix} -\alpha h(x_1) \\ 0 \\ 0 \end{bmatrix}. \quad (8)$$

con $h(x_1)$ dado por (7) para $q = 3$ y considerando como función de energía hamiltoniana a

$$H(x) = \frac{1}{2}\left[\frac{1}{\alpha}x_1^2 + x_2^2 + \frac{1}{\beta}x_3^2\right] \quad (9)$$

siendo el vector gradiente

$$\frac{\partial H}{\partial x} = \begin{bmatrix} \frac{1}{\alpha} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\beta} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \frac{1}{\alpha}x_1 \\ x_2 \\ \frac{1}{\beta}x_3 \end{bmatrix}.$$

De (8) se ve que el vector desestabilizante se encuentra gobernado por $x_1(t)$, entonces se emplea $y(t) = x_1(t)$ en (8). De este modo, $\mathcal{C}$, $\mathcal{S}$ y $\mathcal{I}$ están dadas por

$$\mathcal{C}^T = \begin{bmatrix} \alpha \\ 0 \\ 0 \end{bmatrix},\ \mathcal{S} = \begin{bmatrix} 0 & \alpha & 0 \\ \alpha & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ \mathcal{I} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -3 & \beta \\ 0 & -\beta & 0 \end{bmatrix}.$$

El par de matrices $(\mathcal{C}, \mathcal{S})$ es no observable ni detectable. Sin embargo, el par $(\mathcal{C}, \mathcal{W})$ con $W = I + S$ es observable. La falta de amortiguamiento del sistema en $x_3(t)$ y en cualquiera de los estados $x_1(t)$ ó $x_2(t)$ se presenta por la naturaleza de la estructura de la matriz de disipación $\mathcal{S}$, que es semidefinida negativa. Si $x_1(t)$ se usa como salida, entonces el término de inyección del error de salida incrementa la disipación en la dinámica del estado del error. El circuito **receptor** para (8) se diseña como

$$\begin{bmatrix} \dot{\xi}_1 \\ \dot{\xi}_2 \\ \dot{\xi}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -3 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \\ + \begin{bmatrix} 0 & \alpha & 0 \\ \alpha & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial \xi} + \begin{bmatrix} -\alpha h(y) \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y. \quad (10)$$

con $h(y)$ definida por Ec.(7) para $q = 3$. Con ganancias $k_i,\ i = 1, 2, 3$ por ser seleccionadas, tal que garantizen estabilidad asintótica y exponencial del error de sincronía $e(t)$. Este error es gobernado por

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & -3 & \beta \\ 0 & -\beta & 0 \end{bmatrix} \frac{\partial H}{\partial e} + \\ + \begin{bmatrix} 0 & \alpha & 0 \\ \alpha & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \frac{\partial H}{\partial e} - \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y. \quad (11)$$

con $x(0) = (0.1, 0.1, 0.1)$, $\xi(0) = (0, 0, 0)$, $\alpha = 9$, $\beta = 14.286$, $\mathbf{m} = \left(\frac{0.9}{7}; -\frac{3}{7}; \frac{3.5}{7}; -\frac{2.7}{7}\right)$ y $\mathbf{c} = (1; 2.15; 3.6; 6.2; 9)$ se obtienen los siguientes resultados. La figura 2 muestra el error de sincronía entre los circuitos transmisor y receptor (8) y (10) $e_i(t) = x_i(t) - \xi_i(t),\ i = 1, 2, 3$ para $k_1 = k_2 = k_3 = 4$. La figura 3 muestra los atractores con 5 enrollamientos de los circuitos transmisor y receptor (8) y (10).

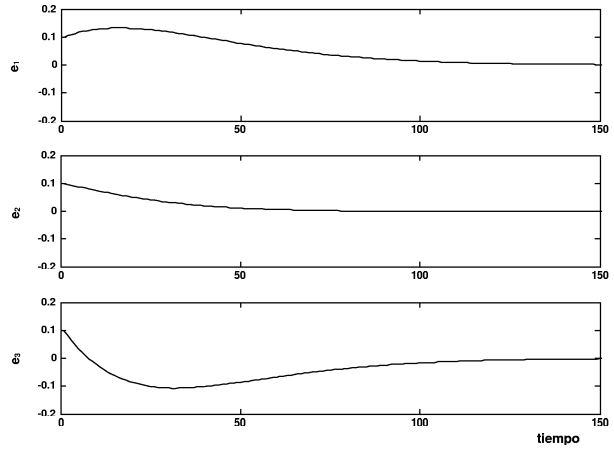

Figura 2: Error de sincronía $e_i(t) = x_i(t) - \xi_i(t)$, $i = 1, 2, 3$, entre los circuitos transmisor y receptor (8) y (10).

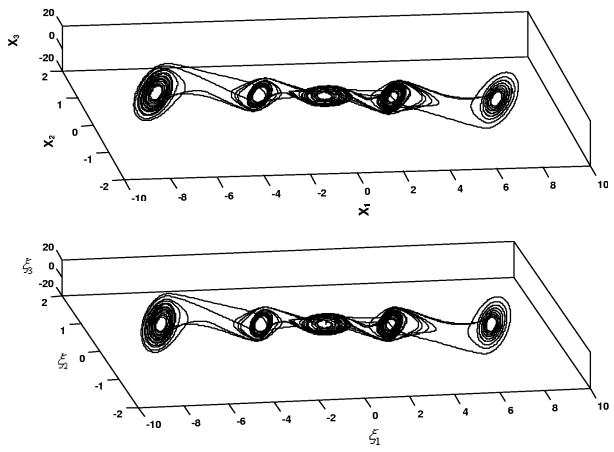

Figura 3: Atractores con 5 enrollamientos de los circuitos transmisor y receptor (8) y (10).

3 Estabilidad del error

En esta sección, se dan condiciones de estabilidad para el error de sincronía (11) entre los circuitos (8) y (10).

Teorema 1 (Sira-Ramírez y Cruz, 2001) *: El estado $x(t)$ del circuito (8) puede ser global, asintótica y exponencialmente estimado por el estado $\xi(t)$ de un observador de la forma (10), si el par de matrices $(\mathcal{C}, \mathcal{W})$ ó $(\mathcal{C}, \mathcal{S})$, son observables o al menos detectables.*

Una condición necesaria y suficiente para estabilidad asintótica global del error de estimación (11), está dada por el siguiente teorema.

Teorema 2 (Sira-Ramírez y Cruz, 2001) *: El estado $x(t)$ del circuito (8) puede ser global, exponencial y asintóticamente estimado, por el estado $\xi(t)$ del observador (10), sí y sólo sí, existe una matriz constante K tal que la matriz simétrica*

$$[\mathcal{W} - K\mathcal{C}] + [\mathcal{W} - K\mathcal{C}]^T = [\mathcal{S} - K\mathcal{C}] + [\mathcal{S} - K\mathcal{C}]^T = 2\left[\mathcal{S} - \frac{1}{2}\left(K\mathcal{C} + \mathcal{C}^T K^T\right)\right] \quad (12)$$

es definida negativa.

Con base en el Teorema 2, tenemos que

$$2\left[S - \frac{1}{2}\left(KC + C^T K^T\right)\right] < 0\,,$$

es decir,

$$\begin{bmatrix} -2\alpha k_1 & 2\alpha - \alpha k_2 & -\alpha k_3 \\ 2\alpha - \alpha k_2 & 4 & 0 \\ -\alpha k_3 & 0 & 0 \end{bmatrix} < 0\,. \quad (13)$$

K debe tomar valores tal que la condición (13) se satisfaga, para esto, es suficiente que $k_1 > 0$, siendo irrelevantes los valores tomados para k_2 y k_3. El valor elegido para las ganancias del circuito **receptor** (10) es $K = [k_1 \quad k_2 \quad k_3]^T$ con $k_1 = k_2 = k_3 = 4$, con lo cual cumple lo establecido por el Teorema 2, condición (13).

4 Comunicación secreta

Esta sección presenta ejemplos ilustrativos de transmisión oculta de información confidencial, tanto analógica como digital, empleando resultados de la Sección 3.

4.1 Codificación caótica aditiva por un canal de transmisión

4.1.1 Ejemplo. La senoidal $m(t) = 0.2\,sen(t)$ es la información oculta que lleva la señal encriptadora, la figura 4 muestra el resultado de este proceso: $m(t) = 0.2\,sen(t)$: señal confidencial a ser transmitida al receptor, $x_1(t) + m(t)$: señal caótica transmitida por el canal público y $\hat{m}(t)$: señal decodificada en el receptor.

4.1.2 Ejemplo. La señal a transmitir, un mensaje de voz $m(t) = voz$ ("bueno"), es la información oculta que lleva la señal, la figura 5 muestra el resultado de este proceso de comunicación secreta: $m(t) = voz$: señal confidencial a ser transmitida al receptor, $x_1(t) + m(t)$: señal caótica transmitida por el canal público y $\hat{m}(t)$: Señal decodificada en el receptor.

4.2 Codificación caótica aditiva por dos canales de transmisión

4.2.1 Ejemplo. La senoidal $m(t) = 0.2\,sen(t)$ es la información que lleva la señal encriptadora, la figura 6 muestra el resultado de este proceso de comunicación secreta:

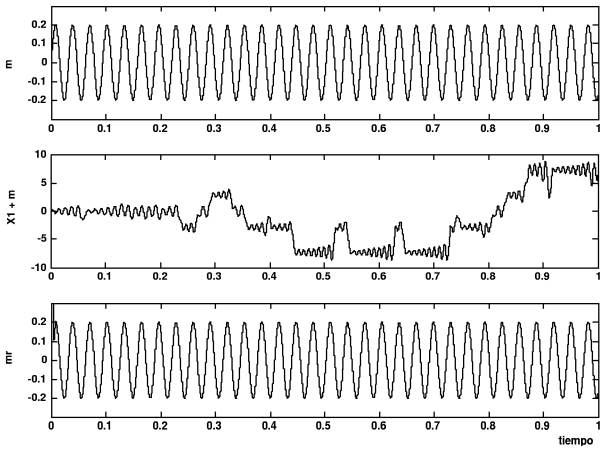

Figura 4: Comunicación secreta con un canal: mensaje por ocultar $m\left(t\right)=0.2\,sen\left(t\right)$, señal transmitida $x_1+m\left(t\right)$ y mensaje decodificado $\hat{m}\left(t\right)$.

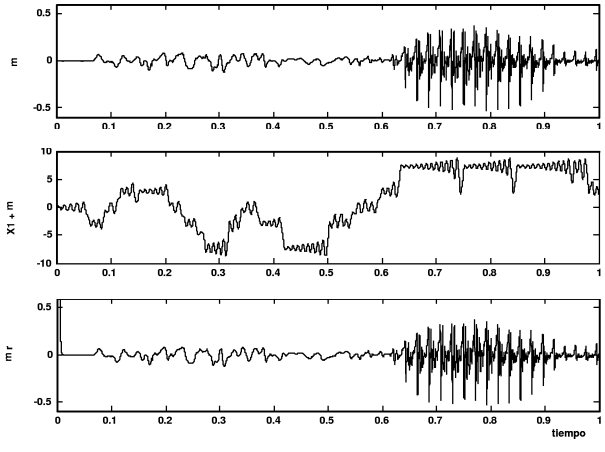

Figura 5: Comunicación secreta con un canal: mensaje por ocultar $m\left(t\right)=$ "bueno", $x_1+m\left(t\right)$ señal transmitida y $\hat{m}\left(t\right)$ mensaje decodificado.

$m\left(t\right)=0.2\,sen\left(t\right)$: señal confidencial a ser transmitida al receptor, $x_2\left(t\right)+m\left(t\right)$: señal caótica transmitida por el canal público y $\hat{m}\left(t\right)$: señal decodificada en el receptor.

4.2.2 Ejemplo. La señal a transmitir es un mensaje de voz $m\left(t\right)=voz$ ("bueno") y es la información oculta que lleva la señal encriptadora. La figura 7 muestra el resultado de este proceso de comunicación secreta: $m\left(t\right)=voz$: señal confidencial a ser transmitida al receptor, $x_2\left(t\right)+m\left(t\right)$: señal caótica transmitida por el canal público y $\hat{m}\left(t\right)$: señal decodificada en el receptor.

4.3 Conmutación entre diferentes atractores caóticos

La comunicación por este método, es para ocultar información binaria, ya que la decodificación del mensaje se obtiene por los cambios de atractores, ocasionados al

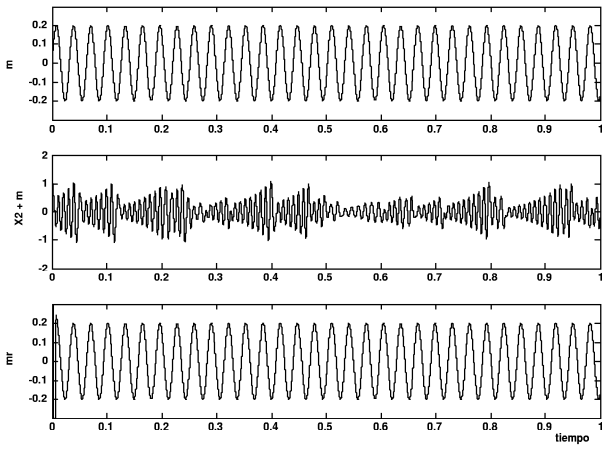

Figura 6: Comunicación secreta con dos canales: mensaje por ocultar $m\left(t\right)=0.2\,sen\left(t\right)$, $x_2+m\left(t\right)$ señal transmitida y $\hat{m}\left(t\right)$ mensaje decodificado.

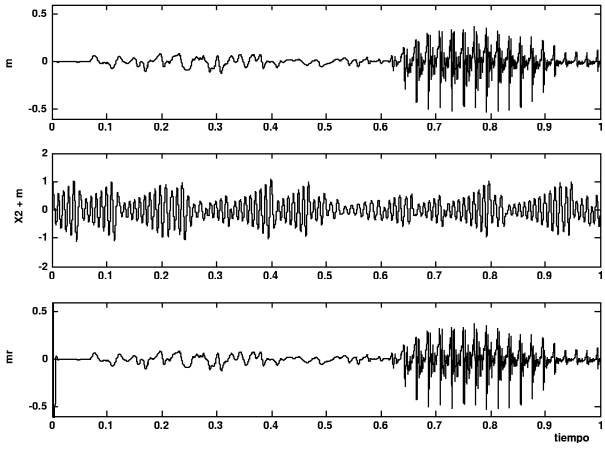

Figura 7: Comunicación secreta con dos canales: mensaje por ocultar $m\left(t\right)=$ "bueno", $x_2+m\left(t\right)$ señal transmitida y $\hat{m}\left(t\right)$ mensaje decodificado.

variar el valor de algún parámetro en el circuito transmisor (8). Se realizó la conmutación paramétrica al variar el parámetro β, con valores de $\beta_1=14.286$ cuyo valor transmitido es el dígito "cero" (sincroniza con el circuito receptor) y $\beta_2=14.285$ cuyo valor transmitido es el dígito "uno" (no sincroniza con el circuito receptor), manteniendo el valor del parámetro $\beta=14.286$ en el receptor todo el tiempo. El mensaje a transmitir oculto es $m(t)=[1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0]$. Con regla de modulación $\beta\left(t\right)=\beta+r\cdot m(t)$, donde $r=0.001$ y $t=2$ seg.

La figura 8 muestra: la señal binaria confidencial a ser transmitida $m(t)=[1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0]$, la señal caótica transmitida, la señal confidencial decodificada $\hat{m}(t)$ en el receptor por detección del error de sincronía $e_1(t)=x_1(t)-\xi_1(t)$ y la señal recibida decodificada $\hat{m}(t)$.

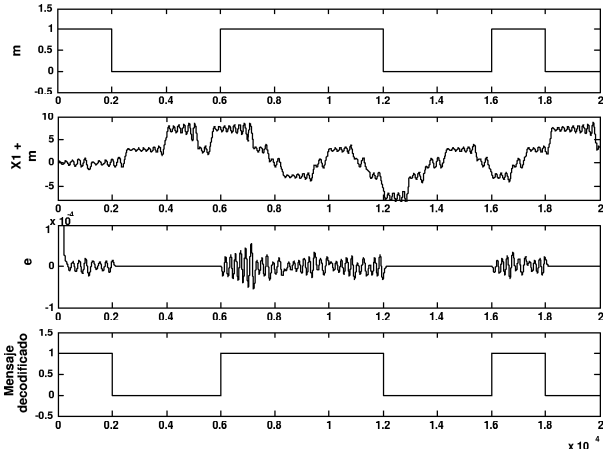

Figura 8: Mensaje binario por ocultar $m(t)$, $x_1(t)$ señal transmitida, detección del error de sincronía $e_1(t)$ en el receptor y $\hat{m}(t)$ mensaje decodificado.

5 Conclusiones

En este artículo, se trató el problema de sincronización de atractores con múltiples enrollamientos desde la perspectiva de los *sistemas hamiltonianos generalizados y el diseño de un observador*. Dicho enfoque permite dar un procedimiento de diseño simple para el receptor y clarifica el asunto de decidir la naturaleza de la señal de salida por ser transmitida. Se mostró la aplicación de este método a diferentes esquemas de comunicación confidencial y al envío secreto de información analógica y digital. Los resultados ilustran la capacidad del procedimiento propuesto. Utilizando sistemas caóticos con dinámicas más complejas como el circuito de Chua generalizado, se logró una mayor seguridad en la comunicación, ya que la dinámica extremadamente compleja de dichos sistemas permite un mejor encriptamiento del mensaje a transmitir resultando muy difícil extraer del canal público, el mensaje por intrusos.

Referencias

[1] Pecora L.M. y Carroll T.L. (1990), "Synchronization in chaotic systems," *Phys. Rev. Lett.*, **64**, 821-824.

[2] Short K.M (1994), "Steps towards unmasking chaotic communication," *Int. J. Bifurc. Chaos*, **4**(4), 959-977.

[3] Pérez G. y Cerdeira H.A. (1995), "Extracting messages masked by chaos," *Phys. Rev. Lett.* **74**, 1970-1973.

[4] Yang T. y Chua L. O. (1997), "Cryptography based on chaotic system," *IEEE Trans. Circuits Syst. I*, **44**(5), 469-472.

[5] Anishchenko V.S., Kapitaniak T., Safonova M.A. y Sosnovzeva O.V. (1994), "Birth of double-double scroll attractor in coupled Chua circuits," *Phys. Lett.* **A192**, 207-214.

[6] Pyragas K. (1998), "Transmission of signals via synchronization of chaotic time-delay systems," *Int. J. Bifurc. Chaos*, **8**(9), 1839-1842.

[7] Cruz C. (2004), "Synchronization of time-delay Chua's oscillator with application to secure communication," por aparecer en *Nonlinear Dynamics and Systems Theory.*

[8] Kolumban, Kennedy y Chua (1997), "The role of synchronization in digital communications," *IEEE Trans. Circuits Syst. I*, **44**(10), 927-935.

[9] Madan R.N. (1993), *Chua's circuit: a paradigm for chaos*, singapore, World Scientific.

[10] Chen G. y Ueta T. (2002), *Chaos in circuits and systems*, World Scientific, vol. 11.

[11] Sira-Ramírez H. y Cruz C. (2001),"Synchronization of Chaotic Systems: A Generalized Hamiltonian Systems Approach", *Int. J. Bifurc. Chaos*, **11**(5), 1381-1395. Y en *Procs. of American Control Conference (ACC'2000)*, Chicago, USA, 769-773.