



# ESTUDIO E IMPLEMENTACIÓN DE UN CIRCUITO CAÓTICO PARA COMUNICACIONES SEGURAS.

Castro Muñoz Gloria  
Rendón Marín Manuel  
Flores Osorio Jesús Alfredo  
Vázquez Martínez Hugo Cesar

Dirección 18 sur y Av. San Claudio C.U. FCE  
jesusf@ece.buap.mx

## RESUMEN.

Desde la década de los 70's fue demostrado que el estudio del caos es importante en diversos campos de la ciencia e ingeniería, tales como la química, mecánica de fluidos, dispositivos de estado sólido, biología, etc.

Recientemente, un nuevo enfoque en el estudio de sistemas dinámicos caóticos se orienta hacia el aprovechamiento del caos para realizar alguna actividad. Como puede ser en sistemas para comunicaciones seguras, en donde la información enviada se mezcla con componentes caóticos para enmascararla.

En este trabajo se construye un circuito emisor que enmascara y un circuito receptor, réplica del anterior, que extrae la información transmitida cuando estos se sincronizan.

## INTRODUCCIÓN

Existen algunas ocasiones en que el caos puede ser predecible: Dos sistemas pueden ser diseñados tal que tengan exactamente el mismo comportamiento. En otras palabras el sistema puede ser exactamente sincronizado. Una de las aplicaciones de éstos sistemas involucra comunicación encriptada. Por ejemplo, uno de los sistemas puede ser usado para ocultar un mensaje con la señal caótica. Sólo alguien que posea el segundo sistema podría decodificar la transmisión, substrayendo la señal caótica.

En base a las aportaciones de Pecora y Carroll en cuanto a la sincronización del caos; Kevin Cuomo y Alan Oppenheim [2] han propuesto una forma de transmitir y recuperar

información encriptada. Donde el transmisor esta conformado por el circuito drive, que tendrá la tarea de generar una señal caótica, y un sumador en el que se mezcla la salida del drive y el mensaje que se desea enviar. El receptor consta de el circuito de respuesta que se encargará de reproducir la misma señal caótica generada por el circuito drive, y un diferenciador que obtiene el mensaje original, eliminando la señal caótica.

Las propiedades de sincronización del sistema de ecuaciones de Rossler, la implementación del mismo con un circuito analógico y su aplicación son abordadas en este trabajo.

## 2. SINCRONIZACION DE UN CIRCUITO CAÓTICO.

Dado un sistema de ecuaciones con características no lineales, como lo es el sistema de Rossler [1], se puede descomponer en varios subsistemas; dichos subsistemas pueden conformar un nuevo sistema y si estos tienden al mismo comportamiento que el sistema original se puede decir que están sincronizados.

Una implementación del sistema Rossler determinado por las ecuaciones 1,2 y 3 se muestra en la figura (1).

$$\frac{dx}{dt} = -\alpha(\Gamma x + \beta y + \lambda z) \quad (1)$$

$$\frac{dy}{dt} = -\alpha(-x - \gamma y + 0.02y) \quad (2)$$

$$\frac{dz}{dt} = -\alpha(-g(x) + z) \quad (3)$$

$$g(x) = \begin{cases} 0, & x \leq 3 \\ \mu(x-3), & x > 3 \end{cases} \quad (4)$$

La única no linealidad en el circuito es dada por el diodo D1 que va a la entrada inversora del amplificador U4, que actúa como un interruptor, tal que solo conduce cuando  $x$  excede 3V. Donde el factor de tiempo  $\alpha = 10^4 \text{ s}^{-1}$ ,  $\Gamma = 0.05$ ,  $\beta = 0.5$ ,  $\lambda = 1$ ,  $\gamma = 0.133$ ,  $\mu = 15$ .

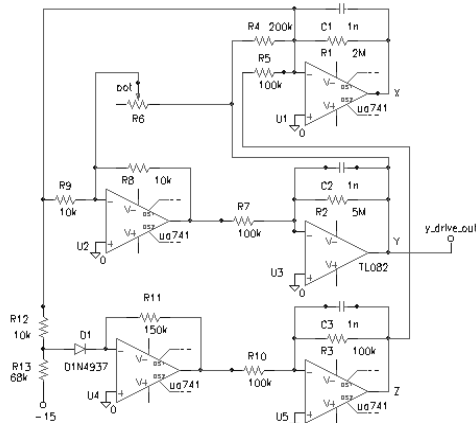


Figura (1). Circuito drive

A continuación se muestran las ecuaciones en términos de los componentes del sistema :

$$y' = -\frac{R_8}{R_9 \cdot R_7} \cdot \frac{1}{C_2} \left[ -x - \frac{R_9}{R_6} y + \frac{R_7 \cdot R_9}{R_2 \cdot R_8} y \right]$$

$$x = -\frac{R_8}{R_9 \cdot R_7} \cdot \frac{1}{C_2} \left[ -\frac{R_9 R_7}{R_8 R_1} x - \frac{R_9 R_7}{R_8 R_4} y + \frac{R_7 \cdot R_9}{R_5 \cdot R_8} z \right]$$

$$z = -\frac{R_8}{R_9 \cdot R_7} \cdot \frac{1}{C_2} \left[ g(x) \frac{R_9 R_7}{R_8 R_{10}} + \frac{R_7 \cdot R_9}{R_3 \cdot R_8} z \right]$$

donde los parámetros quedan en términos de

$$\alpha = \frac{R_8}{R_9 R_7 C_2}$$

$$\gamma = \frac{R_9}{R_6}$$

$$\delta = \frac{R_7 R_9}{R_2 R_8} = 0.02$$

$$\Gamma = \frac{R_9 R_7}{R_8 R_1} = 0.05$$

$$\beta = \frac{R_9 R_7}{R_4 R_8} = 0.5$$

$$\lambda = \frac{R_9 R_7}{R_8 R_5} = 1$$

$$\mu = \frac{R_{11}}{R_{12}} = 15$$

El sistema de respuesta está descrito por las siguientes ecuaciones:

$$\frac{dx'}{dt} = -\alpha(\Gamma x' + \beta y + \lambda z') \quad (5)$$

$$\frac{dy''}{dt} = -\alpha(-x' - \gamma y + 0.02 y') \quad (6)$$

$$\frac{dz'}{dt} = -\alpha(-g(x') + z') \quad (7)$$

donde las ecuaciones 5 y 7 forman el subsistema  $(x', z')$  y la ecuación 6 forma el subsistema  $y''$ .

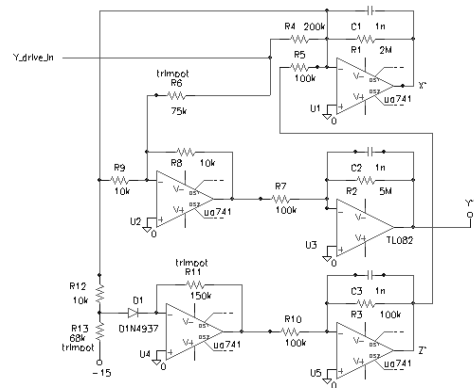


Figura 2. Circuito generador.

Si en el circuito drive, el potenciómetro  $R_6$  es ajustado a  $47.3\text{K}\Omega$  se observará el atractor de la figura 3; éste atractor es un gráfico del osciloscopio de la señal  $x$  del circuito drive (ch1) contra la señal  $y$  del circuito drive (ch2).

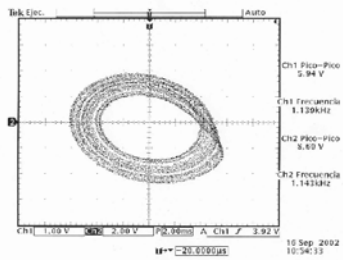


Figura 3. Atractor del circuito drive.

Para lograr que las características de ambos circuitos drive y generador sean lo mas semejantes posibles se vario el valor del potenciómetro  $R_6$ , y para optimizar mas la sincronización se variaron conjuntamente los potenciómetros  $R_{11}$  y  $R_{13}$  del circuito receptor. Cuando los dos están sincronizados el gráfico de  $y$  contra  $y''$  se ve como en la figura (4).

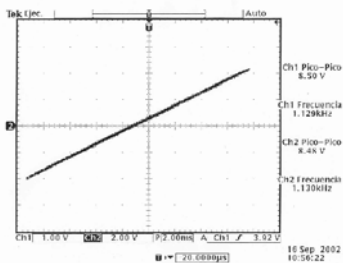


Figura 4. Señal  $y$  del circuito drive contra señal  $y''$  del circuito generador.

Para reafirmar la existencia de sincronización se muestra que no existe gran diferencia entre los espectros en frecuencia de la señal y del circuito drive que llamaremos  $u(t)$  y la señal regenerada  $u_r(t)$ . Dichos espectros se muestran en la figura 5 y 6 que fueron obtenidos del osciloscopio.

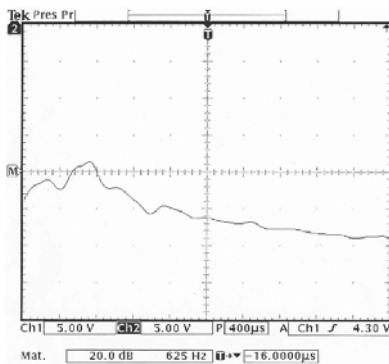


Figura 5.  $u(f)$  transmisor

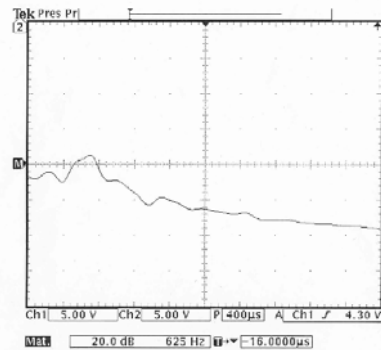


Figura 6.  $u_r(f)$  receptor

Para poder comunicarnos de manera confidencial; es decir que el mensaje que se desea enviar no sea captado por otras personas, necesitamos encriptar dicho mensaje. Esto se puede hacer implementando el diagrama mostrado en la figura 7 [3].

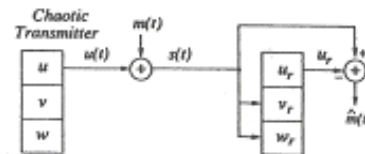


figura 7.

La implementación del enmascaramiento se realiza mediante la suma de una señal que aparenta ser ruido  $u(t)$ , que proviene del circuito drive ajustado en una región caótica, y la señal de voz que se desea transmitir  $m(t)$  se genera la señal a transmitir  $s(t)$  la cual será utilizada en el receptor para sincronizar el circuito generador y regenerar la señal caótica que una vez restada a la señal recibida  $s(t)$  se tendrá el mensaje transmitido  $m(t)$ .

Realizando una comparación del espectro de frecuencias de la señal caótica  $u(t)$  y la señal  $s(t)$ , mostradas en la figura 5 y 9 respectivamente; se puede observar que no existe diferencia significativa lo cual quiere decir que no se distingue el mensaje transmitido (figura 8) de la señal caótica.

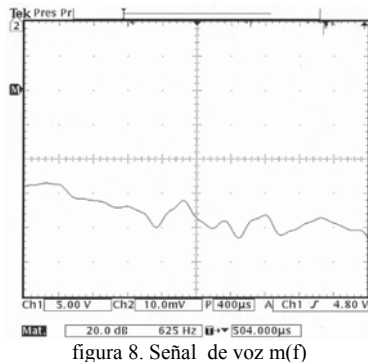


figura 8. Señal de voz  $m(f)$

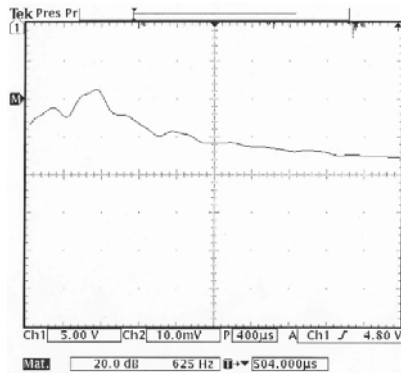


Figura 9.  $s(f)$

[1] L. M. Pecora and T. L. Carroll, Synchronization in Chaotic Systems, *Phy. Rev. Lett.* 64,821 (1990)

[2] H. Strogatz Steven *Nonlinear Dynamics and Chaos* Edit Addison Wesley 1994 301-335

[3] M. Cuomo Kevin and Oppenheim, Circuit Implementation of Synchronized Chaos with Applications to Communications, *Phy. Rev. Lett.* 71,65 (1993)

### 3. CONCLUSIONES

Aun cuando la señal  $m(t)$  es significativamente mas pequeña que la señal caótica, el mensaje recuperado fue entendible aunque esta se escuchaba con un poco de ruido.

En base a los resultados se pretende cuantificar el rango de variación de los componentes de un circuito a otro, es decir entre el circuito drive y generador. Así como encontrar la forma de disminuir el ruido generado en la señal recuperada. Para posteriormente poder utilizarlo en la transmisión de otro tipo de señales.

### 4. AGRADECIMIENTOS

A nuestros padres que nos dieron el apoyo suficiente para que este proyecto se llevara a cabo y a aquellas personas que en algún momento se preocuparon por nosotros y nos apoyaron en la elaboración de este trabajo.

### REFERENCIAS