SISTEMA DE ENCRIPTAMIENTO DE SEÑALES MEDIANTE OSCILADORES CAÓTICOS

PRESENTAN:
José Antonio Dávila Pintle y Delfino Raúl Vazquez López
Facultad de Ciencias de la Electrónica
C.U. San Manuel
jpintle@ece.buap.mx

RESUMEN

En este trabajo se pretende dar a conocer la forma de construir osciladores no lineales de tercer orden que presentan el fenómeno de caos, bajo ciertas condiciones. Se presenta un método para enmascarar información mediante la modulación de los parámetros de un oscilador caótico de doble órbita (oscilador de Chua), así como la forma de recuperar la señal encriptada mediante otro oscilador caótico.

1. INTRODUCCION

El uso de formas de ondas caóticas para los sistemas de comunicaciones basados en el fenómeno de sincronización en sistemas caóticos [2,3] esta ofreciendo nuevos fundamentos para el diseño de sistemas de comunicaciones seguros y prácticos. Algunos métodos de modulación analógicos y digitales han sido propuestos y la evaluación de su comportamiento en sistemas de comunicaciones esta en progreso [4,12].

Para transmisión de datos binarios dos métodos de modulación se encuentran en la literatura [3,8]. Un enfoque directo [3,7] es generar una portadora caótica al conmutar entre dos diferentes fuentes caóticas, siguiendo la secuencia de 0´s y 1's del flujo de datos binarios. El de modulador identifica el flujo de símbolos y la portadora caótica por medio de un conjunto de subsistemas síncronos que son "sintonizados" para seguir cada una de las fuentes caóticas. Un segundo enfoque, aparentemente, mas robusto que el anterior usaría el flujo de datos binarios de información para conducir la orbita de un sistema caótico de tal forma que sea compatible consigo misma [8]. Un subsistema síncrono en el receptor recibe y recrea la orbita del sistema trasmisor y la información es recuperada.

Para fuentes de información analógicas, el enfoque directo para comunicaciones seguras es combinar la información con las señales caóticas en mezcladores convencionales [9]. El receptor consiste en un subsistema síncrono que reproduce la señal caótica que es necesaria para recuperar la señal de información. Un segundo enfoque [11] es detectar diferencias en los parámetros del transmisor y el receptor. Se pretende seguir este enfoque en este trabajo, la modulación paramétrica fue propuesta por Corron y Hans en la referencia 11..
Los principios de la modulación paramétrica se dan en la sección 3 y 4 las cuales describen la implementación de un oscilador de doble órbita (DSO, también conocido como oscilador de Chua)[12].

2. PUNTOS FIJOS

Comenzaremos este trabajo discutiendo un poco acerca del plano fase que describe la soluciones de un sistema de ecuaciones diferenciales como trayectorias en dicho plano[13].
Consideremos en el siguiente sistema lineal:

$$\frac{dx_1}{dt} = \dot{x}_1 = f_1(x_1,...,x_n)$$

... .(1)

$$\frac{dx_n}{dt} = \dot{x}_n = f_n(x_1,...,x_n)$$

Las soluciones de este sistema pueden ser visualizadas como trayectorias fluyendo en un espacio n dimensional, con coordenadas $x_1,...,x_n$ mencionaremos un caso sencillo para ilustrar esta idea.

Comencemos con un sistema de una sola dimensión , sea el circuito RC que se muestra en la figura 1, la ecuación diferencial que describe dicho circuito es:

$$\dot{v}_c = \frac{1}{RC}(V_i - v_c) \quad .....(2)$$

La solución de la ecuación (2) que representa el comportamiento del sistema para cualquier tiempo t >0 cuando $v_c(0)=0$ es:

$$v_c = V_i(1 - \exp(-t/RC)) \quad .....(3)$$

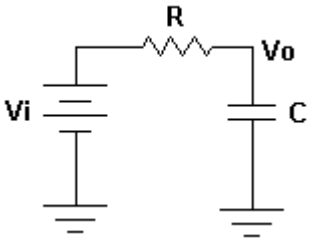

Figura 1. Circuito simple RC.

El comportamiento en estado estacionario del voltaje del capacitor (ec 3), en el límite cuando t→∞ es $v_c \to V_i$.

Si pensamos que v_c es la posición de una partícula imaginaria moviéndose a lo largo de la línea real, y dv_c/dt reprenda entonces su velocidad, la ecuación diferencial (ec. 2) representa un campo vectorial sobre la línea y dicta el vector velocidad dv_c/dt para cada v_c. Para obtener el campo vectorial, es conveniente graficar dv_c/dt contra v_c, y entonces dibujar flechas sobre el el eje v_c para indicar el vector velocidad correspondiente para cada v_c. Las flechas apuntan hacia la derecha cuando dv_c/dt>0 y hacia la izquierda cuando dv_c/dt<0. En los puntos en los cuales dv_c/dt=0 no hay flujo, tales puntos son llamados **puntos fijos**.

Armados con esta representación podemos fácilmente entender la ecuación diferencial dada por la ecuación 2, comenzamos con nuestra partícula en $v_c(0)$ y miramos como el llevada por le flujo en el eje real, esto se muestra en la figura (2)

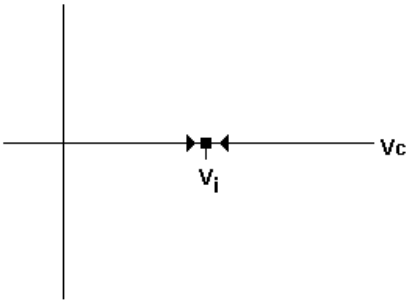

Figura 2. Plano fase de la ecuación (2)

Según la figura (2) independientemente de la condición inicial $v_c(0)$, el voltaje en el capacitor siempre tendera hacia el punto Vi.

3. El OSCILADOR DE DOBRE ÓRBITA (DS0)

El circuito eléctrico conocido como oscilador de doble órbita (figura 3) esta descrito por una ecuación diferencial de tercer orden no lineal que puede ser expresada como el siguiente conjunto de ecuaciones de primer orden acopladas:

$$\begin{aligned} C_1\dot{V}_1 &= (V_2 - V_1)G - i(V_1) \\ C_2\dot{V}_2 &= (V_1 - V_2)G + i_L \\ L\dot{i}_L &= -V_2 \end{aligned} \quad \text{.....(4)}$$

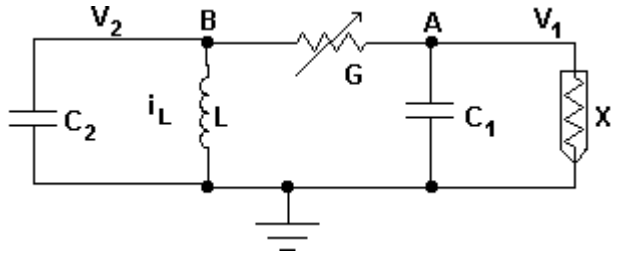

Figura 3. Diagrama esquemático del oscilador de doble órbita, el elemento no lineal esta marcado con una X.

Un punto en el espacio fase tiene coordenadas (V_1, V_2, i_L) Las primeras dos ecuaciones de (6) expresan la conservación de la corriente en los nodos A y B. La tercera es la ley de inducción para una bobina sin perdidas. El elemento marcado con X en la figura 3 es un resistor no lineal negativo con las siguientes características I-V

$$i(v) = \begin{cases} -G_1 v - V_B(G_0 - G_1) & v > V_B \\ -G_0 v & |v| \le V_B \\ -G_1 v + V_B(G_0 - G_1) & v < -V_B \end{cases} \quad \text{.....(5)}$$

La característica I-V del elemento no lineal (ec. 5) es implementada según el circuito de la figura (4)

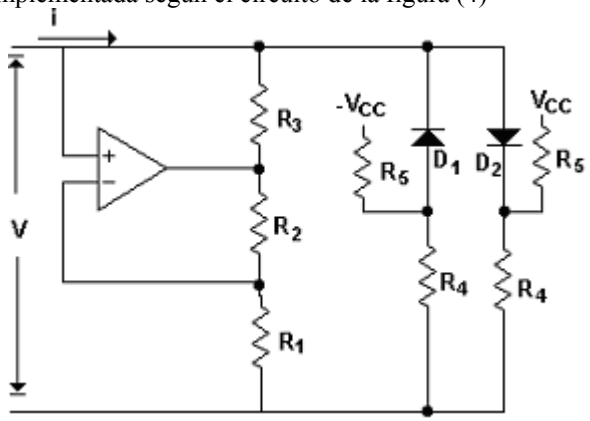

Figura 4. El elemento no lineal en el DSO, los diodos en el circuito son los componentes no lineales.

Los parámetros en la relación i-v del elemento no lineal (ec. 5) son identificados de las siguientes relaciones:

V_B = Punto de ruptura de los diodos

$$G_0 = \frac{R_2}{R_1 R_3} \quad \text{.....(6)}$$

$$G_1 = \frac{R_0 R_2 - R_1 R_3}{R_0 R_1 R_3}$$

El circuito de la figura 3 tiene tres puntos fijos, dependiendo de los parámetros de admitancia. Este se comporta como DSO cuando $G_1<G<G_0$. En este caso el oscilador tiene tres puntos de equilibrio, uno de ellos, N, esta localizado en el origen del espacio fase, y los otros dos están localizados P=($-V_f$, 0, V_fG) y Q=(V_f, 0, $-V_fG$), Donde se satisface $i(V_f) = -GV_f$, esta relación se muestra gráficamente en la figura (5)

$$V_f = V_B \frac{G_0 - G_1}{G - G_1} \quad \text{.....(7)}$$

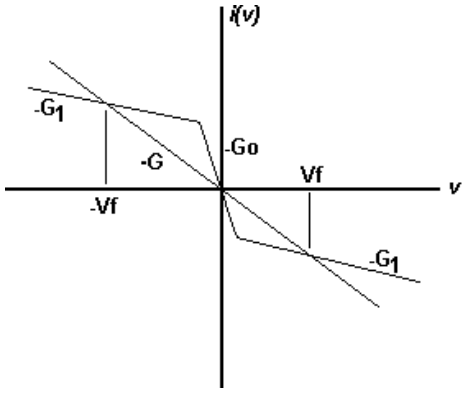

Figura 5. Solución gráfica a *i(v)=-Gv*. Las pendientes de los segmentos han sido marcados, Las inigualdades $G_1<G<G_0$ son necesarias para tener tres cruces.

4. MODULANDO EL DSO

La señal de información es acoplada al DSO (fig. 3) al inyectársela en la forma de una corriente variable en el tiempo en el nodo A. En el diagrama esquemático de la figura 6 esta modulación es implementada al inyectarle una corriente a través del resistor Rm y Vm. El conjunto de ecuaciones que describen el DSO modulado es:

$$C_1 \dot{V}_1 = (V_2 - \mu V_1)G - i(V_1) + \Lambda(t)$$

$$C_2 \dot{V}_2 = (V_1 - V_2)G + i_L \quad \text{.....(8)}$$

$$L \dot{i}_L = -V_2$$

donde $\mu = 1 + G_m / \ G > 1$ y $\Lambda(t) = G_m V_m(t)$. En el límite de admitancia cero Gm→0 se recupera el DSO sin modular.

El DSO modulado tiene tres puntos fijos si las condiciones $G_1 < \mu G < G_0$ y $|V_m| < V_B(G_0 - \mu G)/G_m$ son cumplidas. La primera condición es sobre los parámetros del circuito y la segunda sobre la amplitud de la modulación.

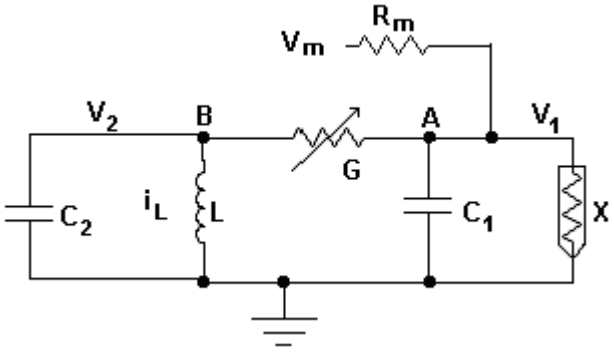

Figura 6. DSO modulado

La amplitud de la modulación $\Lambda(t)$ hace que los puntos fijos P, Q, y N se muevan a lo largo de la línea $i_L=-GV_1$ en el plano V2=0,

$$N(t) = \left(\frac{\Lambda(t)}{\mu G - G_0}, 0, \frac{-G\Lambda(t)}{\mu G - G_0} \right) \quad \text{.....(9)}$$

$$P(t) = \left(-V'_f + \frac{\Lambda(t)}{\mu G - G_1}, 0, -G\left[V'_f + \frac{\Lambda(t)}{\mu G - G_1} \right] \right)$$

$$Q(t) = \left(V'_f + \frac{\Lambda(t)}{\mu G - G_1}, 0, -G\left[V'_f + \frac{\Lambda(t)}{\mu G - G_1} \right] \right)$$

donde $V'_f = V_f \frac{G - G_1}{\mu G - G_1}$ y V_1 es la coordenada del punto fijo Q del sistema sin modular, $\Lambda = 0$.

3. RESULTADOS Y CONCLUSIONES

Las figuras 7 muestra el plano fase del oscilador del transmisor, y la figura 8 del receptor.

Figura 7 Gráfico x-y de los nodos A y B del circuito de la figura 3

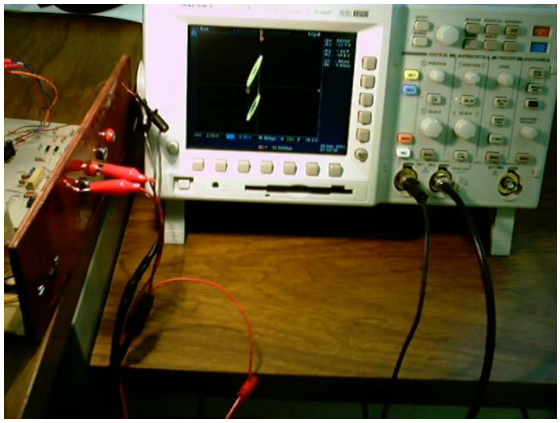

Figura 8 Gráfico x-y de los nodos A y B del circuito receptor

Al inyectarle una corriente al nodo A (figura 3) se observo un desplazamiento de los puntos fijos de acuerdo a la ecuación (9), y al graficar el voltaje del nodo A contra el voltaje del nodo B de un circuito idéntico en el receptor, se logra reconstruir el plano fase (figura 8), que como conclusión, se lograron generar señales caóticas por modulación paramétrica del DSO que pueden ser usadas para llevar información encriptada,

REFERENCIAS

[1] Jesús Urías, Analog modulation and demodulation of a chaotic oscillator, Revista Mexicana de Física, 45(4), 1999, 331-335.

[2] L.M. Pecora and T.L Carroll, Phys. Rev. Letters 64(1990) 821.

[3] L.M. Pecora et al., CHAOS 7,(1997) 520.

[4] U.Parlitz et al., Intl. J. Bifurc. And Chaos 2 (1992) 973

[5] K.M. Cuomo, and A. V. Oppenheim, Phys. Rev. Letters 71 (1993) 65.

[6] K.M. Cuomo, A. V. Oppenheim, and S.H. Strogatz, IEEE trans. Circuits Sys. II 40 (1993) 634

[7] P. Celka, IEEE Trans. Circuits Syst. I 42 (1995) 455

[8] S. Hayes, C. Grebogi, and E. Ott. Phys. Rev. Letters 70 (1993) 3031

[9] R. He. And P.G. Vaidya, Phys. Rev. E 57 (1998) 1532.

[10] T.L. Carroll and L.M. Pecora, Physica D 67 (1993) 126

[11] N.J. Corron and D. W. Hans, IEEE Trans, Ciruits and Systems 44 (1997) 275

[12] M. Itoh, C.W. Wu, and L.O. Chua, Int. J. Bifuc. And Chaos 7 (1997) 275

[13] Steven H. Strogatz, *Nonlinear dynamics and chaos* (Adisson-Wesley , 1994)