# Encriptación en sistemas caóticos con excitaciones sinusoidales.

G. Obregón-Pulido, A. Torres-González, R. Cárdenas-Rodríguez y G. Solís-Perales
Universidad de Guadalajara, Centro Universitario de Ciencias Exactas e Ingenierías (CUCEI)
División de Electrónica y Computación
Av. Revolución 1500, Guadalajara, Jalisco, México.
guillermo.obregon[angel.torresg]@red.cucei.udg.mx, cardenas[gualberto.solis]@cucei.udg.mx

***Resumen*— Un sistema dinámico caótico es extremadamente sensible a sus condiciones iniciales, por lo cual su comportamiento es prácticamente impredecible y al mismo tiempo lo hace más atractivo para aplicaciones de encriptación. Por otro lado, en teoría de regulación se considera un sistema generador de señales de perturbación y/o referencia el cual es llamado exosistema, dicho exosistema se supuso conocido para la elaboración de este documento.**

**En este trabajo presentamos a un oscilador caótico excitado mediante una suma de "*n*" señales sinusoidales y un mensaje, el cual se pretende ser encriptado por el caos del oscilador con el fin de transmitir el mensaje con mayor seguridad, dicho mensaje deberá ser recuperado por el receptor; en éste esquema propuesto, el receptor conoce cada una de las frecuencias de las señales sinusoidales y estimará la señal de excitación. El propósito es aumentar la seguridad del mensaje en el canal de la transmisión, dicha seguridad está sustentada en la combinación de señales sinusoidales a través del caos y no como anteriormente se trababa, que era teniendo solamente una señal de información a través de un encriptador caótico.**

**Se propone un sistema que resuelve el problema anteriormente planteado.**

**Palabras clave: Estimación de frecuencias, Sistemas caóticos, Procesamiento de señales.**

## I. INTRODUCCIÓN

Desde que Pecora y Carroll presentaron su trabajo de sincronización de caos [1], la investigación con respecto al caos ha recibido considerable atención y el fenómeno se ha extendido a la aplicación en la seguridad en las comunicaciones ([2], [3], [4]). Al utilizar los sistemas caóticos para codificar y decodificar señales, surge un nuevo método diferente de las técnicas convencionales, tal como lo presentado por Cuomo y Oppenheim en donde envían una señal de voz en su forma original y se logra recuperar satisfactoriamente [5].

En los últimos años, los esquemas de encriptamiento están siendo estudiados cada vez más, ante la demanda que existe de desarrollar un sistema de encriptamiento mas seguro, para la transmisión de datos en tiempo real a través de Internet, redes inalámbricas y otros dispositivos ([6],[7]).

El algoritmo estándar tradicional de encriptamiento de imágenes y el encriptamiento de datos (DES), tienen desventaja cuando se manejan grandes cantidades de datos [8], ya que se realizan digitalmente (primero en una PC), y luego se envía la señal encriptada.

El encriptamiento en línea en un sistema dinámico tiene la ventaja de procesar la señal en tiempo real, es decir, la señal analógica (mensaje) se encripta y al mismo tiempo se envía.

En el presente trabajo se propone un sistema no lineal, que se encuentra excitado por una señal dada por la ecuación:

$$p = \sum_{i=1}^{n} A_i \sin(\alpha_i t + \varphi_i) + B \tag{1}$$

donde las amplitudes $A_i \neq 0$, los ángulos de fase $\varphi_i$ son constantes desconocidas y $B$ es una constante que representa al bias de la señal. Además de esta sinusoidal, tendremos una señal de información $m$. Se observa que la señal $p$ puede ser generada por un sistema lineal $\dot{w} = Sw$ el cual llamaremos exosistema [9].

Estas señales excitarán al oscilador caótico con el fin de encriptar el mensaje de manera más segura; en el esquema propuesto el receptor conoce las frecuencias que se utilizaran y estimará la señal (1) de forma global.

La organización del artículo es la siguiente: en la sección 2, se plantea el problema; el estimador no lineal se diseña en la sección 3; en la sección 4 se muestran diversos ejemplos y para finalizar, en la sección 5 se plantean algunas conclusiones.

## II. PLANTEAMIENTO DEL PROBLEMA

Varios tipos de sistemas caóticos se pueden tratar bajo el impulso de una señal sinusoidal de entrada. En forma general el sistema caótico se puede ver en (2), donde $f(x_1,x_2,\eta)$ y $\alpha(x_1,x_2,\eta)$ son funciones no lineales de los estados y $m$ es el mensaje a ser encriptado.

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -a_1 x_1 - a_2 x_2 + f(x_1,x_2,\eta) + m + p \\ \dot{\eta} &= -a_3 \eta + \alpha(x_1,x_2,\eta) \end{aligned} \tag{2}$$

Una vez descrito el modelo del sistema caótico de manera general, se procede a incorporar la señal de información, tanto en el encriptador (sistema caótico) como en la señal de salida que está dada por:

$$\begin{aligned} y_0 &= x_1 + x_2 + f(x_1,x_2,\eta) + m \\ y_1 &= x_1 \end{aligned} \tag{3}$$

Algunos osciladores caóticos son estudiados en los párrafos siguientes y serán adaptados para lograr el encriptamiento deseado y que tomen la forma (2).

Se pretende que con las salidas dadas por (3) se pueda recuperar el mensaje $m$ y la señal de perturbación $p$, tal como se muestra en la figura 1.

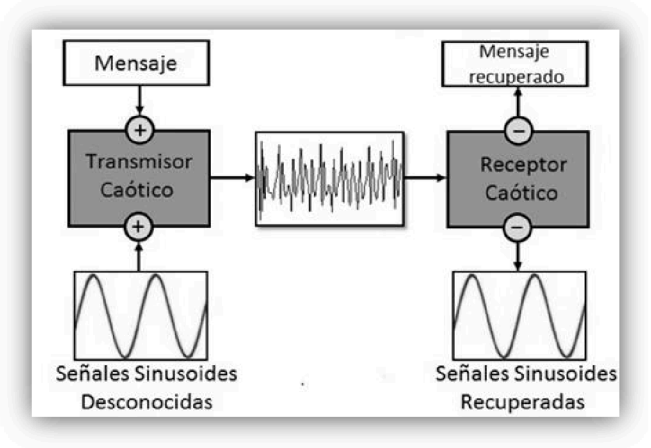


Figura 1. Estimación de la perturbación $p(t)$ en el sistema caótico.

Si en un momento dado, se interviene en la señal de transmisión y se logra eliminar el caos, encontrarán que el mensaje estará perturbado por una señal sinusoidal y sus armónicos ya que esta se inyecto en el sistema caótico y este presente multiplicación de señales, de tal manera no se decodifica el mensaje y la información estará preservada.

**Nota:** Observe que aunque se están tomando dos salidas, es posible transmitir una sola si realizamos el multiplexado en frecuencia para enviar las dos señales en un solo canal y poderlas recuperar después en el receptor.

En lo que sigue se presentan algunos sistemas caóticos y como estos serán transformados para qué tomen una estructura adecuada.

*2.1 El sistema caótico de Van der Pol.*

La ecuación de Van der Pol proporciona un ejemplo de un oscilador no lineal con amortiguación. El sistema se puede escribir en la forma:

$$\ddot{x} - \mu(1 - x^2)\dot{x} + x = p + m \tag{4}$$

tomando $x_1 = x$ y $\dot{x} = x_2$ el sistema toma la forma (2)

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -x_1 + \mu x_2 - \mu x_1^2 x_2 + p + m \end{aligned} \tag{5}$$

con los siguientes coeficientes:

$$a_1 = 1, \quad a_2 = -\mu,$$
$$f(x_1, x_2, \eta) = -\mu x_1^2 x_2$$

*2.2 El sistema caótico de Duffing.*

La ecuación de Duffing es introducida en 1918 como un modelo de oscilador no lineal.
La ecuación se define como:

$$\ddot{x} + \delta\dot{x} - \beta x + x^3 = p + m \tag{6}$$

tomando $x_1 = x$ y $\dot{x} = x_2$ el sistema toma la forma (2)

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= \beta x_1 - \delta x_2 - x_1^3 + p + m \end{aligned} \tag{7}$$

con los siguientes coeficientes:

$$a_1 = -\beta, \quad a_2 = \delta,$$
$$f(x_1, x_2, \eta) = -x_1^3$$

*2.3 El sistema caótico de Lorenz.*

Este sistema se le conoce como un modelo simplificado de varios sistemas físicos ([10], [11]). Este sistema está descrito por:

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= cx - y - xz + m + p \\ \dot{z} &= -bz + xy \end{aligned} \tag{8}$$

Si tomamos como $x_1 = x$ y $x_1 = x, x_2 = a(y - x), \eta = z$, el sistema (8) toma la forma:

$$\begin{aligned} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -a(1 - c)x_1 - (a + 1)x_2 - ax_1\eta + p + m \\ \dot{\eta} &= -b\eta + x_1\left(\frac{x_2}{a} + x_1\right) \end{aligned} \tag{9}$$

entonces toma la misma estructura que (2) con los respectivos coeficientes que son:

$$a_1 = a(1 - c), \qquad a_2 = (a + 1), \qquad a_3 = b,$$
$$f(x_1, x_2, \eta) = -ax_1\eta, \qquad \alpha(x_1, x_2, \eta) = x_1\left(\frac{x_2}{a} + x_1\right)$$

**Nota:** Se observa que los sistemas caóticos de Lu, Chen y Raylegh también se pueden poner en la forma (2). Además en algunos casos el estado $\eta$ no existe.

Para la clase de sistemas dados, se hacen las siguientes suposiciones:

**Suposición 1.** Las constantes $(a_1, a_2, a_3) \in \mathcal{R}$, la función $f(x_1, x_2, \eta)$ y la dinámica de $\eta$ son conocidas.

**Suposición 2.** Las frecuencias $\alpha_i$ son conocidas y cumplen con $\alpha_i \neq \alpha_j$ para $i \neq j$.

**Suposición 3.** El mensaje y la perturbación no destruyen el caos.

Se observa que las señales de salida son caóticas y entonces ésta señal tiene un infinito número de frecuencias.

## III. Diseño del receptor

Ahora se propone un estimador el cual utiliza la señal que envía el emisor. El estimador desencripta la información separando la señal $p$, las señales caóticas y el mensaje.

**Proposición:** Considere las señales de salida dadas por (3) y las suposiciones 1 a 3, entonces el estimador dado por

$$\begin{aligned}
\dot{\hat{x}}_1 &= \hat{x}_2 + g_1(y_1 - \hat{y}_1)\\
\dot{\hat{x}}_2 &= -a_1\hat{x}_1 - a_2\hat{x}_2 + (y_0 - \hat{y}_0) + g_2(y_1 - \hat{y}_1) + \hat{p}\\
\dot{\hat{\eta}} &= -a_3\hat{\eta} + \alpha(\hat{x}_1, \hat{x}_2, \hat{\eta})\\
\dot{\hat{w}} &= S\hat{w} + G_0(y_1 - \hat{y}_1)
\end{aligned} \tag{10}$$

$$\hat{p} = \sum_{k=0}^{n} \hat{w}_{2k+1}, \qquad S = \begin{bmatrix} S_1 & 0 & \cdots & 0 & 0 \\ 0 & S_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & S_n & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix},$$

$$S_j = \begin{bmatrix} 0 & \alpha_j \\ -\alpha_j & 0 \end{bmatrix}$$

con salida:

$$\begin{aligned}
\hat{y}_0 &= \hat{x}_1 + \hat{x}_2\\
\hat{y}_1 &= \hat{x}_1
\end{aligned} \tag{11}$$

Y las constantes $g_1$, $g_2$ y $G_0$ seleccionadas de forma adecuada es tal que estima las señales caóticas, la señal de perturbación $p$ y el mensaje.

**Prueba**: Consideremos el sistema error entre (2), (10) y el exosistema

$$\begin{aligned}
\dot{e}_1 &= e_2 - g_1 e_1\\
\dot{e}_2 &= -(a_1 + 1)e_1 - (a_2 + 1)e_2 + \sum_{k=0}^{n} e_{w_{2k+1}} - g_2 e_1\\
\dot{e}_3 &= -a_3 e_3 + \alpha(x_1, x_2, \eta) - \alpha(\hat{x}_1, \hat{x}_2, \hat{\eta})\\
\dot{e}_w &= S e_w - G_0 e_1
\end{aligned} \tag{12}$$

Donde $e_1 = x_1 - \hat{x}_1, e_2 = x_2 - \hat{x}_2, e_3 = \eta - \hat{\eta}, e_w = w - \hat{w}$ se puede ver que las señales $e_1$, $e_2$, $e_w$, son señales observables con la señal $e_1$, por lo que es posible elegir constantes $g_1$, $g_2$ y $G_0$ tales que $e_1 \to 0, e_2 \to 0, e_w \to 0$. Para la señal $e_3$ se observa que su dinámica tiene de entrada la diferencia de las funciones no lineales y ésta diferencia también tiende a cero por lo que $e_3$ también tenderá a cero.

Entonces podremos estimar el mensaje y la perturbación con las siguientes formulas:

$$\begin{aligned}
\hat{m} &= y_0 - \hat{y}_0 - f(\hat{x}_1, \hat{x}_2, \hat{\eta})\\
\hat{p} &= \sum_{k=0}^{n} \hat{w}_{2k+1}
\end{aligned} \tag{13}$$

Con lo que la prueba queda terminada. ▲

## IV. Simulación

Considere el sistema caótico de Duffing, dado por las ecuaciones:

$$\begin{aligned}
\dot{x}_1 &= x_2\\
\dot{x}_2 &= \beta x_1 - \delta x_2 - x_1^3 + p + m
\end{aligned}$$

aplicando nuevamente el estimador (10). Los valores con los cuales se genera un comportamiento caótico $\beta = 1$; $\delta = 0.1$; la perturbación dada por $p(t) = sin(1.5t)$ y el mensaje como una señal triangular dada por $m(t) = arcsin(sin(t))$, [12]. Los valores obtenidos son $g_1 = 18.9$; $g_2 = 130.21$; $G_0 = [385.7, 139.3516]$.

El seguimiento de la perturbación se puede observar en la figura 2 y en la figura 3 la recuperación del mensaje propuesto.

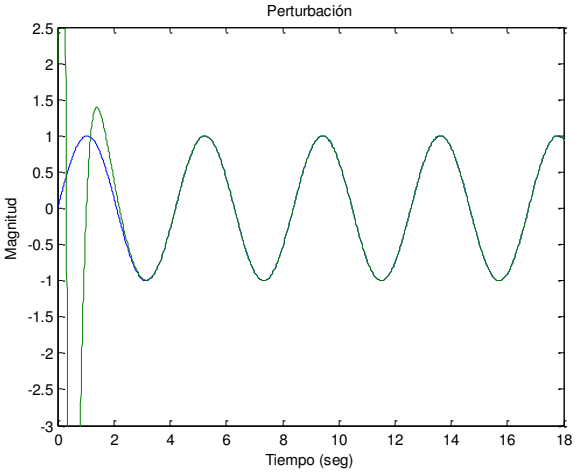


Figura 2. Estimación de la señal de perturbación.

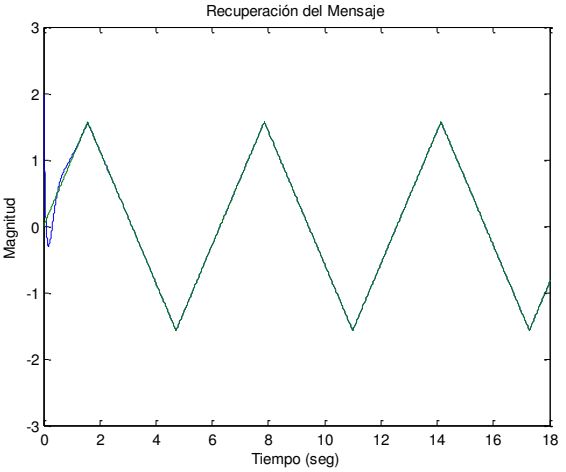


Figura 3. Estimación del mensaje dado por una señal de forma triangular, siendo $m(t) = arcsin(sin(t))$

En la figura 4 se observa el comportamiento caótico del oscilador Duffing.

Evidentemente se toman valores apropiados tanto para la perturbación como para el mensaje y que dichas señales no destruyan el caos producido por el sistema.

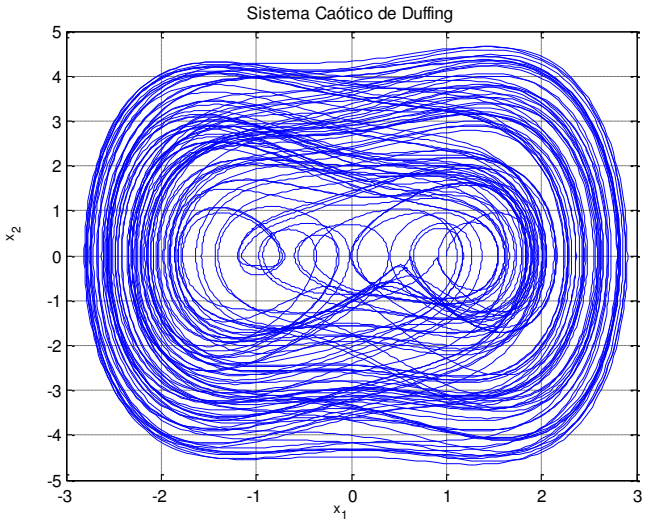


Figura 4. Oscilador caótico de Duffing bajo la excitación de la perturbación y de la señal de información.

El lector puede comprobar que para los valores $\beta = 1$; $\delta = 0.1$; $p(t) = sin(12t)$ y el mismo mensaje definido como onda triangular, con ganancias de valor $g_1 = 18.9$; $g_2 = -11.54$; $G_0 = [-2307, 146.1752]$, dará como resultado la destrucción del comportamiento caótico.

Considerando una aplicación real con una señal de audio, presentaremos la encriptación de los primeros 5 segundos de la canción *Un bel di vedremo* (tomada de la ópera *Madama Butterfly,* segundo acto). Se aplicarán dos frecuencias de perturbación $p(t) = sin(t) + sin(4t)$, al sistema caótico de Lorenz que se muestra a continuación:

$$\dot{x} = a(y - x)$$
$$\dot{y} = cx - y - xz + m + p$$
$$\dot{z} = -bz + xy$$

aplicando el estimador (10) y los valores que producen un comportamiento caótico $(a = 10,\ b = 28,\ \ c = 8/3)$, con ganancias diseñadas de $g_1 = 18$; $g_2 = 392$; $G_0 = [1085,\ 441,\ 904,\ 707]$.

En la figura 5 se puede ver la estimación de la perturbación de las dos señales.

En la figura 6 se observa la señal dada como audio original, las salidas del sistema caótico así como también se muestra la recuperación del audio (el eje de tiempo se encuentra escalado).

Posteriormente, en la figura 7 se hace un acercamiento a la señal recuperada (sección del rectángulo con línea punteada), donde efectivamente la señal del decodificador corresponde al audio original y en la figura 8 está la señal de error entre la señal del mensaje original y la señal del mensaje recuperado, vemos que efectivamente tiende a cero.

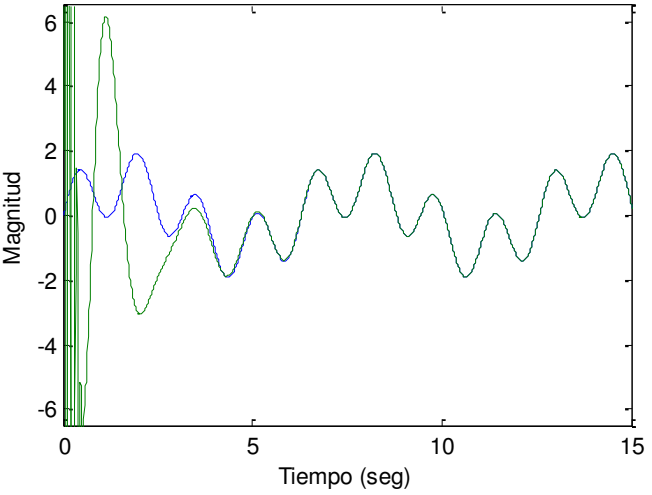


Figura 5. Estimación de la perturbación en el sistema caótico. $(p(t) = sin(t) + sin(4t))$

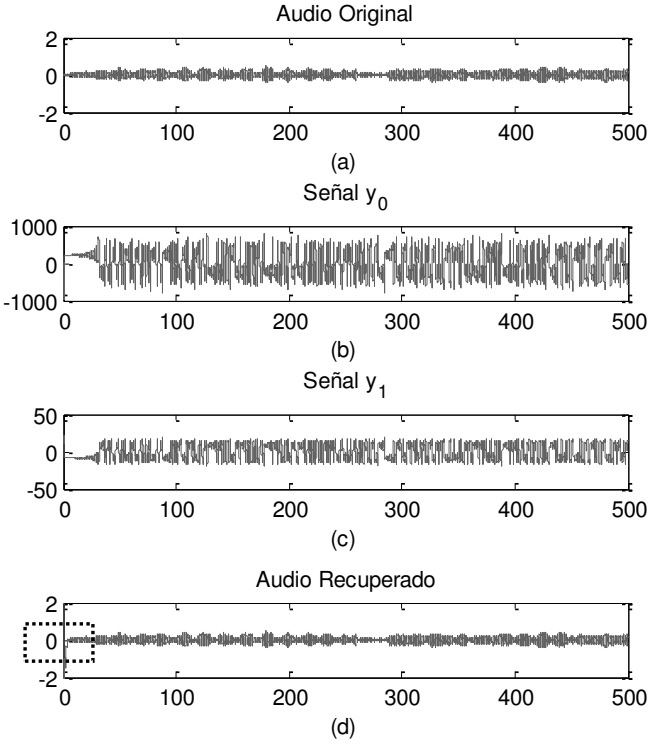


Figura 6. Audio original 9(a), el envío de las señales $y_0$ y $y_1$ las cuales son caóticas en 9(b-c) y en 9(d) Recuperación de mensaje original

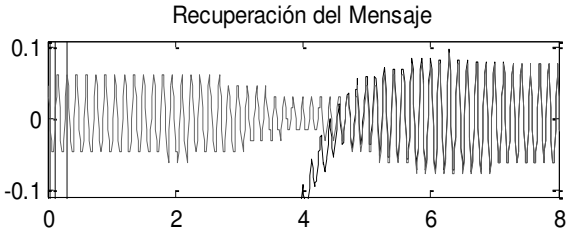

Figura 7. Acercamiento de la señal recuperada del audio original puesta en el codificador.

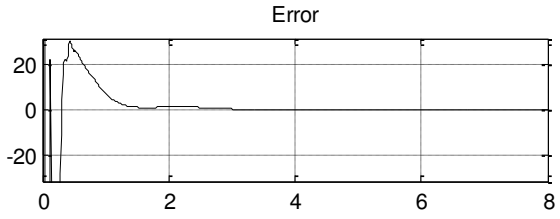

Figura 8. Señal de error entre el mensaje original y el mensaje recuperado.

El método también se puede aplicar a una imagen digital. Para realizar la codificación, se adapta la imagen de tal forma que se tome como un vector y se envía de la misma manera que la señal de audio. En este caso el receptor conoce el número de filas y columnas para llevar a cabo la decodificación.

Para este ejemplo, se utiliza el sistema caótico de Duffing con la perturbación dada por $p(t) = sin(0.5t)$. Las ganancias colocadas en el sistema son las siguientes: $g_1 = 20;\ g_2 = 100;\ G_0 = [350.7, 89.3516]$.

En la figura 9 se puede ver como se adapta la perturbación.

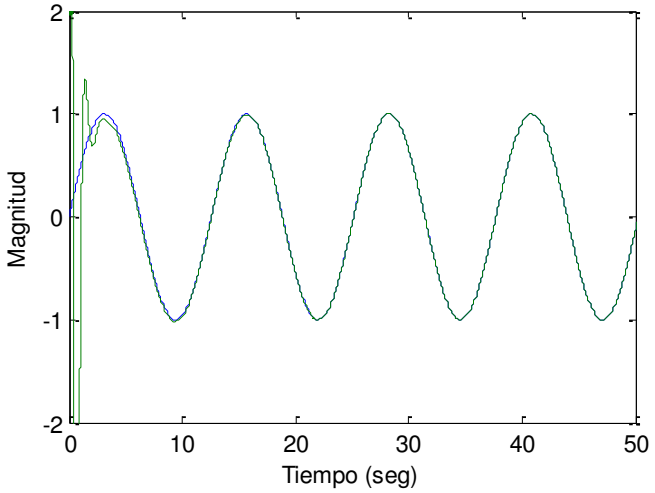

Figura 9. Seguimiento de la señal de perturbación.

En la figura 10, se presenta el comportamiento caótico del ejemplo y en comparación con la figura 4, se detectan pequeñas diferencias en cuanto a su evolución, no obstante, se sigue teniendo un compartamiento similar, es decir, caótico.

En la figura 11(a-b) se muestra la imagen de ejemplo que se utilizó en el codificador y la recuperación de la misma, por medio del decodificador.

En la figura 12(a-b) se muestran las señales enviadas que son mostradas en forma de imágenes. Recordemos que la forma de envío es a través de un vector, tal como se realizó en una señal de audio. La información se mantiene oculta ya que a simple vista, no se puede revelar la información.

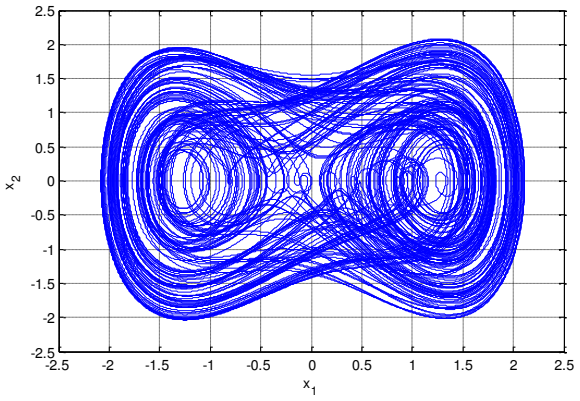

Figura 10. Comportamiento caótico generado por la presencia del sistema de Duffing, la perturbación y la imagen digital.

Figura 11a. Comparación entre la imagen original codificada y la imagen decodificada a través del sistema caótico.

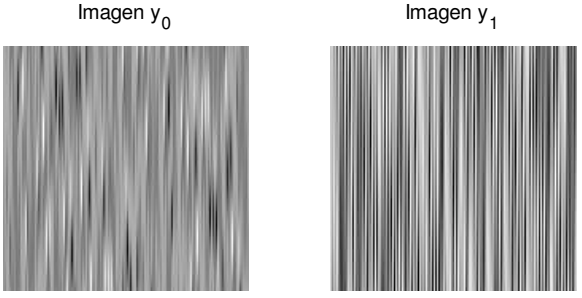

Figura 12a. Señales encriptadas mostradas en forma de imagen.


Figura 11b. Comparación entre la imagen original codificada y la imagen decodificada a través del sistema caótico.

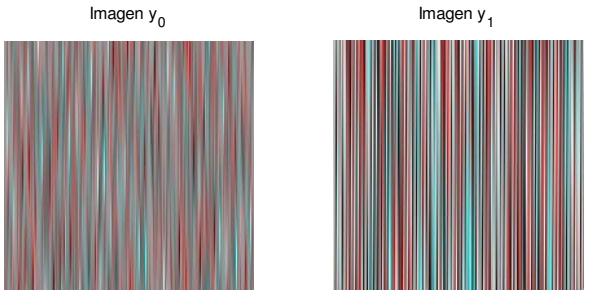


Figura 12b. Señales encriptadas mostradas en forma de imagen.

## V. Conclusiones

Los sistemas de encriptación basados en caos, proponen un modo seguro para el envío de información. En los primeros trabajos encaminados a usar dicha encriptación, sólo utilizaban una señal caótica y otra señal propuesta como mensaje [5]; sin embargo, en el presente documento se proporciona un algoritmo que mejora la seguridad, la cual consiste en combinar las señales caóticas, la señal de información y las señales sinusoidales. Si se interviene en la línea de comunicación y logran eliminar el comportamiento caótico de la señal, aún se tendrá que eliminar las señales sinusoidales presentes aunado a los armónicos de las mismas producidos por el sistema caótico.

La encriptación en sistemas caóticos con excitaciones sinusoidales conocidas, propone una nueva forma de lograr una seguridad en el envío de la información.

Como trabajo futuro se pretende extender el mismo tema de encriptación, con la presencia de perturbaciones cuyas frecuencias también sean desconocidas y a su vez, recuperar cada una de las componentes sinusoidales así como también el mensaje propuesto desde un principio.

## VI. Agradecimientos

Este trabajo ha sido auspiciado por el departamento de electrónica de la Universidad de Guadalajara.

## Referencias

[1] Pecora L.M. and Carroll T.L. (1990). “Synchronization in chaotic systems”, Phys. Rev. Lett.64, 821-824.
[2] Alvarez G.,Li S (2006). “Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems”. International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151.
[3] Gámez G. L., Cruz Hernández. C., López Gutiérrez .R.M.,y García G.E.E. (2008). “Synchronization of multi-scroll chaos generators: application to private communication”. Revista Mexicana de Física 54(4), pp. 299-305.
[4] Gámez G, L., Cruz-Hernández, C., López-Gutiérrez, R.M., García G.E.E (2009). “Synchronization of Chua’s circuits with multi-scroll Application to communication”, Commun Nonlinear Sci Numer Simulat 14, 2765-2775.
[5] K. M. Cuomo, A. V. Oppenheim, S. H. Isabelle (1992) “Spread Spectrum Modulation, and Signal Masking Using Synchronized Chaotic Systems”, MIT Research Laboratory of Electronics Technical Report.
[6] Li S., Alvarez G.,Li Z., Halang W. A. (2007). “Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey”. http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.5455v1.pdf
[7] Chiaraluce F, Ciccarelli L, et al (2002). “A new chaotic algorithm for video encryption”. IEEE Trans Consum Electron 48,838–43.
[8] Chen G.R, Mao Y.B, et al (2004). “A symmetric image encryption scheme based on 3D chaotic cat maps”. Chaos, Solitons & Fractals 21, 749–61.
[9] Isidori A. and Byrnes C. (1990) “Output regulation of nonlinear systems”. IEEE Transactions on Automatic Control 35, No. 2. Pp 131-140.
[10] Richter H. (2001) “Controlling the Lorenz system: combining global and local schemes”. Chaos, Solitons and Fractals No.12. pp. 2375–2380
[11] E.N. Lorenz (1963) “Deterministic nonperiodic flow” Journal Atmosph., Sci. 20. pp. 130.
[12] Obregón-Pulido G. and R Cárdenas-Rodríguez, (2012) “Relación entre las funciones trigonométricas y las señales Diente de Sierra, Triangular y Cuadrada”, Sociedad Mexicana de Instrumentación (SOMI XXVII), Culiacán, Sinaloa, México.