2009-04-30

Sistemas caóticos y su aplicación a la encriptación de señales

Gallego, Juan P.; Sánchez-Torres, Juan D.; Vera-Ciro, Carlos; Rodríguez-Rey, Boris A.

Gallego, J.P.; Sánchez-Torres, J.D.; Vera-Ciro, C.;Rodríguez-Rey, B.A.(2009). Sistemas caóticos y su aplicación a la encriptación de señales. Revista de la Sociedad Colombiana de Física, 41(2), 436-439.

Enlace directo al documento: http://hdl.handle.net/11117/3260

Revista Colombiana de Física,Vol. 41, No.2, Abril 2009

Sistemas Caóticos y su Aplicación a la Encriptación de Señales

Juan P. Gallego [a], Juan D. Sánchez [a], Carlos A. Vera [b,c], Boris A. Rodríguez [b,c]

[a] *GAUNAL, Universidad Nacional de Colombia, Sede Medellín, Colombia*
[b] *FACom,Instituto de Física, Universidad de Antioquia,Medelín, Colombia*
[c] *GFAM,Instituto de Física, Universidad de Antioquia, Medelín, Colombia*

Recibido 23 de Oct. 2007; Aceptado 6 de Mar. 2009; Publicado en línea 30 de Abr. 2009

Resumen

La sincronización y control de señales caóticas es una activa área de investigación por sus posibles aplicaciones en telecomunicaciones y transmisión de señales [1,2,3,4]. En el presente trabajo se estudia un sistema de comunicación basado en la sincronización de dos sistemas no lineales caóticos, cada uno modelado a partir de las ecuaciones de movimiento de un péndulo forzado amortiguado y que se encuentran en el mismo punto de operación del espacio de parámetros. Se usaron dos canales de comunicación: el primero para la señal de sincronización y el segundo para el envío del mensaje, con lo que se resuelve el problema de la sensibilidad a las condiciones iniciales. En el sistema receptor se usa un lazo de realimentación a modo de controlador proporcional que hace que el error entre los estados del codificador y del decodificador vaya rápidamente a cero. Estos dos últimos hechos hacen que el sistema sea robusto ante perturbaciones externas tales como ruido en los canales de comunicación.

***Palabras Clave*:** Sistemas Dinámicos, Caos, Sincronización de caos, Teoría de control.

Abstract

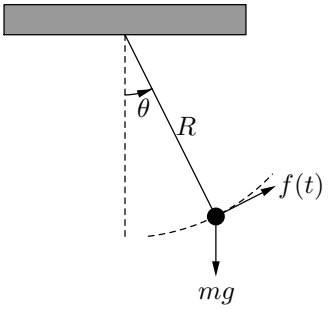
Synchronization and control of chaotic signals is an active research area because of its applications in telecommunications and secure signal transmission [1,2,3,4]. In this work a communication system based in the synchronization of two chaotic nonlinear systems, each one being modeled by the motion equations of a driven damped pendulum and operated in the same parameter space region is shown. Two communication channels were used: the first one for the synchronizing signal and the second one for the sent message. By using two channels the initial conditions sensibility problem is solved. In the receiver system a feedback loop as a proportional controller is used in order to drive quickly the error between the decoder and encoder states to zero. The last two facts make the system to be robust to external pertubative signals such as noise in the communication channels.

***Keywords*:** Dynamical Systems, Chaos, Chaos Synchronization, Control Theory.

1. Sistema caótico y sistema de sincronización

Uno de los osciladores caóticos [5] más estudiados en la literatura es el péndulo forzado y amortiguado, en esta sección mostramos algunos resultados básicos relacionados con su dinámica. Usando la segunda ecuación de Newton podemos escribir las ecuaciones de movimiento para este sistema en forma adimensional como,

$$\frac{d^2\theta}{d\tau^2} = -\sin\theta + G\cos(\omega_D\tau) - \frac{1}{q}\frac{d\theta}{d\tau}, \qquad (1)$$



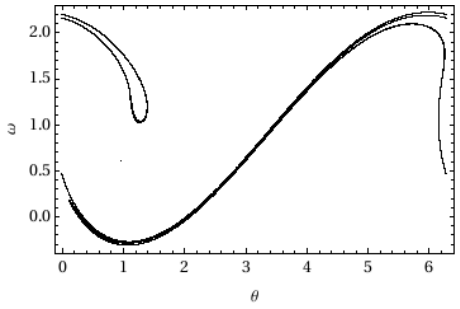
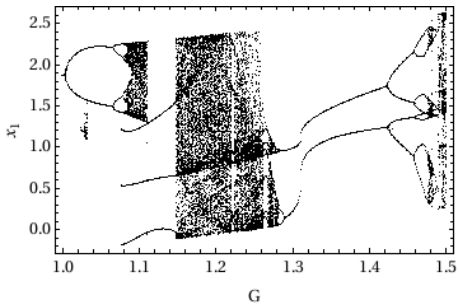


Figura 1. El péndulo forzado amortiguado. La variable dinámica es θ; $f(t)$ es un forzamiento armónico definido por $f(t) = f_0 \cos(\omega_f)t$ (panel izquierdo). Sección de Poincaré para $G = 1{,}2$, $q = 2$ y $\omega_D = 2/3$, los puntos son tomados cada periodo de forzamiento (panel derecho).



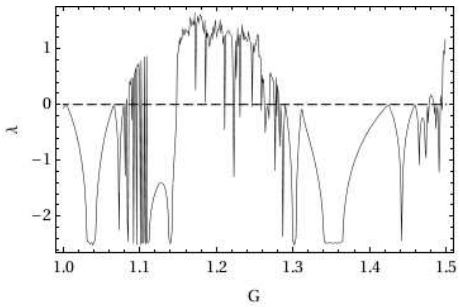


Figura 2. Diagrama de bifurcación para $x_1 = \omega$ tomando $q = 2$ y $\omega_D = 2/3$ (panel izquierdo) y Máximo exponente de Lyapunov en la misma región de parámetros (panel derecho)

donde $\omega_D = \omega_f \sqrt{g/R}$ es la frecuencia adimensional de forzamiento; $\tau = t\sqrt{g/R}$ es la escala de tiempo; $G = f_0/m$ es la amplitud adimensional de forzamiento; q es el parámetro de fricción y θ es el desplazamiento angular del péndulo medido desde la vertical. La presencia de caos en el sistema se garantiza a través del cálculo del máximo exponente de Lyapunov en una región sugerida por el diagrama de bifurcación del sistema (Figura 2).

2. El Sistema de Comunicación Propuesto

El sistema de comunicación propuesto consta esencialmente de: un sistema codificador, un sistema decodificador, un modelo emisor y un modelo receptor (Figura 4). Para el sistema codificador y decodificador usamos una representación 2-dimensional de la ecuación de movimiento para el péndulo (1) en la misma región de parámetros. Es decir,

$$\dot{x}_1 = -\frac{1}{q}x_1 - \sin x_2 + G\cos(\omega_D \tau) \quad \text{y} \quad \dot{x}_2 = x_1, \tag{2}$$

$$\dot{z}_1 = -\frac{1}{q}z_1 - \sin z_2 + G\cos(\omega_D \tau) \quad \text{y} \quad \dot{z}_2 = z_1 + u(\tau), \tag{3}$$

para el codificador y decodificador, respectivamente. Llamando $m(\tau)$ el mensaje enviado, la señal transmitida $s(\tau)$, será la suma de $m(\tau)$ y una función suave $h(x)$. La dinámica del error es

$$\begin{aligned} \dot{e}_1 &= \dot{z}_1 - \dot{x}_1 = -\frac{1}{q}e_1 - \sin z_2 + \sin x_2 \quad \text{y} \\ \dot{e}_2 &= \dot{z}_1 - \dot{x}_1 = e_1 + u(\tau). \end{aligned} \tag{4}$$

Tomando $x_2 = z_2$ y $u(\tau) = -\gamma e_2(\tau)$ este sistema se puede escribir como

$$\dot{e} = \begin{pmatrix} -1/q & 0 \\ 1 & -\gamma \end{pmatrix} e, \tag{5}$$

que es lineal con autovalores $\{-\gamma, -1/q\}$ ambos negativos y por lo tanto posee un punto fijo global estable en el origen $e = 0$, lo que asegura la sincronización de los estados.

3. Simulación y conclusiones

Demostramos el desempeño del sistema propuesto haciendo una simulación numérica de los procesos de codificación y decodificación para una señal sonora de 7 segundos de duración. Las codiciones iniciales en cada sistema se eligieron aleatoriamente. Note que el estado x_2 representa una ángulo que varía entre 0 y 2π, por

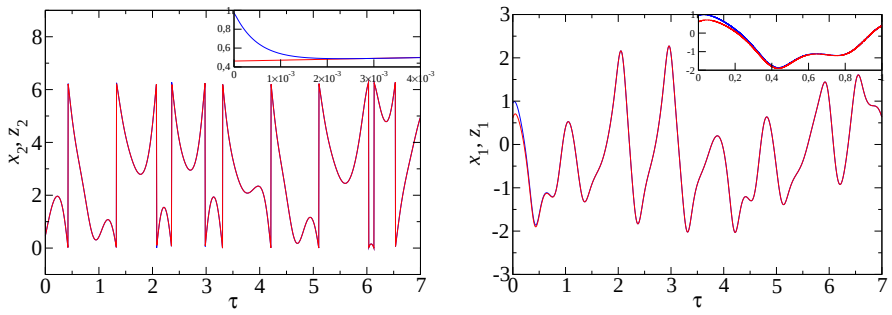


Figura 3. El panel izquierdo muestra la evolución para los estados x_2 (rojo) y z_2 (azul). El panel derecho muestra la evolución para los estados x_1 (rojo) y z_2 (azul). En los recuadros se muestra la dinámica para pequeños tiempos, lo que muestra la rápida sincronización del sistema.

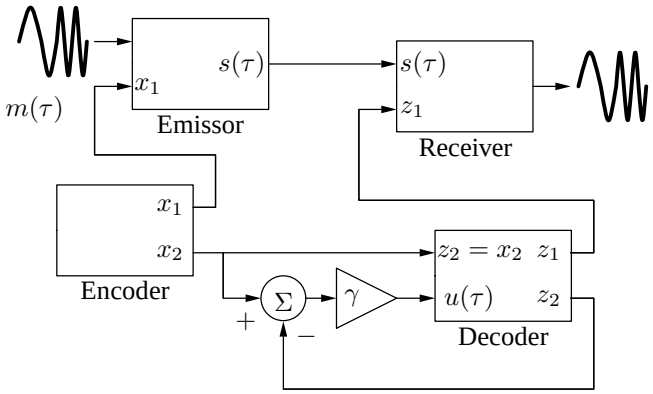


Figura 4. Sistema propuesto de comunicación. La señal codificadora usada es el estado $h(x) = x_1$ del codificador y $s(\tau)$ is la señal enviada.

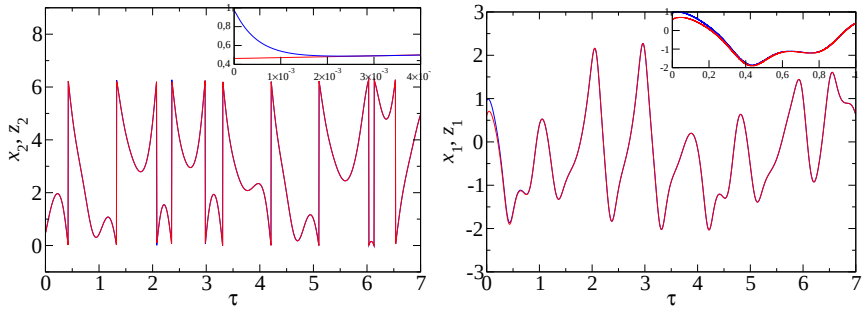


Figura 5. El panel izquierdo muestra la evolución para los estados x_2 (rojo) y z_2 (azul). El panel derecho muestra la evolución para los estados x_1 (rojo) y z_2 (azul). En los recuadros se muestra la dinámica para pequeños tiempos, lo que muestra la rápida sincronización del sistema.

lo tanto el proceso de integración numérica hace una transición abrupta cada vez que una órbita pase por los extremos del intervalo. Este efecto puede ser interpretado como un ruido en el sistema receptor. Sin embargo el tiempo de estabilización es corto convirtiendo este efecto en una perturbación numérica insignificante para la dinámica completa del sistema. El tiempo de estabilización del estado e_2 varía como $1/\gamma$, la elección de un parámetro de control grande asegura entonces una rápida sincronización. Teniendo en cuenta esto se eligió un valor de $\gamma = 200$.

La figura 5 muestra que la sincronización se hace en las escalas de tiempo esperadas, este hecho verifica la eficiencia del esquema implementado. Sin embargo una prueba del desempeño de la estructura de comunicación propuesta es la densidad espectral de potencias de la señal de enmascaramiento caótica. Claramente si en el mensaje codificado aparecen todas las componentes de frecuencia con aproximadamente la misma magnitud,

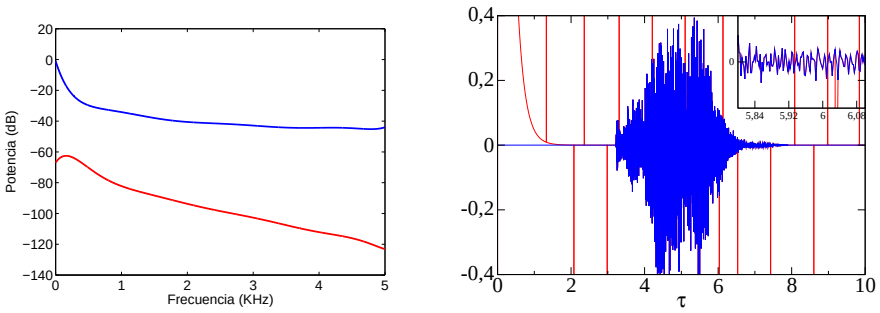


Figura 6. El panel izquierdo muestra la densidad espectral para la señal codificada enviada (azul) y para la señal audible enviada (rojo). El panel derecho muestra la serie de tiempo asociada a la señal original (azul) y la señal recuperada (rojo). Las diferencias entre las dos señales no tienen efecto significativo sobre el mensaje recuperado.

esta no será audible. Como se muestra en la figura 6 la densidad espectral de potencias la señal de enmascaramiento caótica se superpone sobre la señal audible con una media de $\approx$ 25dB, por lo tanto es imposible distinguir las componentes de la señal audible. Debe ser considerado que durante los procesos de codifición, emisión, recepción y decodificación de la señal esta sufre varios cambios de amplitud, lo que asegura que la señal transmitida tenga una magnitud en la densidad espectral más grande que el mensaje enviado.

En conclusión, se propuso un esquema eficiente para enviar señales codificadas a través del enmascaramiento caótico, basado en el paradigma de la sincronización de dos sistemas caóticos equivalentes. Usando la alta aperiodicidad de la señal caótica es posible enmascarar un mensaje que será decodificado por un sistema caótico sincronizado con el emisor que se encuentra en el mismo punto de operación del espacio de parámetros. El empleo de un lazo de realimentación en el decodificador permite hacer de manera eficiente que el error vaya rápidamente a cero, esto evita problemas de estabilidad en el sistema, lo que se puede verificar con el rápido amortiguamiento del error.

Referencias

[1] K. M. Cuomo, and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65(1993).
[2] N. Sharma, and P. G. Poonacha, Phys. Rev. E **56**, 1242(1996).
[3] E. Ott, *Chaos in Dynamical Systems, 2nd Ed.*, Cambridge University Press, 2002.
[4] J. Bechhoefer, Rev, Mod, Phys. **77**, 783(2005).
[5] G. L. Baker, and J. P. Gollub, *Chaotic Dynamics: an Introduction (2nd Ed)*. Cambridge University Press (1996).