Implementación de la codificación de señales por medio de sistemas caóticos sincronizados usando control activo.

Pablo Andrés DeOssa, *Estudiante de Ing. de Control, UNALMED,* Eduardo Ramirez Uribe, *Estudiante de de Ing. de Control, UNALMED,* y Juan Camilo Zapata, *Estudiante de Ing. de Control, UNALMED,*

(Artìculo Estudiantil)

***Abstract*— Se propone un sistema de comunicación digital basado en la sincronización de dos sistemas dinámicos caóticos discretizados mediante el metodo de Runge Kutta, cada sistema construido a partir de las ecuaciones dinámicas del sistema de Newton-Leipnik. Se utiliza el método propuesto en [3] que usa 2 canales de comunicación, uno para la señal de sincronización y otro para la señal portadora del mensaje y se diseña un sistema atraves de control activo que introduce una realimentación en el sistema que asegura una convergencia rápida de los errores a cero.**

***Index Terms*— Chaos theory, Signal analysis, Synchronization, Control theory, Dynamic systems.**

CONTENTS

I. INTRODUCCIÓN

El asombroso hecho de que el determinismo no implica necesariamente el comportamiento regular o predictible en la descripción dinámica de los fenómenos naturales, ha sido uno de los mayores impactos en las ideas científicas de las últimas décadas. El descubrimiento del comportamiento caótico cambió nuestra manera de entender el mundo y nos reta a buscar nuevas explicaciones. La biología, las matemáticas, la física, la ingeniería, las ciencias sociales y hasta el arte han sentido la intromisión de los nuevos conceptos en sus cuerpos teóricos y podríamos decir que prácticamente ninguna rama del saber y/o la técnica han estado libre de la influencia de estas ideas [1]

Desde la aparición de los primeros análisis computacionales de los sistemas caóticos en la decada del 60 con los trabajos pioneros de Lorenz hasta la actualidad, la emergencia del caos en el estudio de sistemas no lineales o sistemas complejos es un hecho. El presente trabajo pretende mostrar como utilizar las técnicas de control y sincronización de caos para la transmisión de señales. El problema de la sincronización de sistemas caóticos fue estudiado por primera vez por Yamada y Fujisaka en 1983 y puesto en su forma actual por Pecora y Carrol en su seminal trabajo de 1990 [5]

El problema central de la sincronización es lograr que la respuesta de dos o más sistemas dinámicos caóticos acoplados sea la misma con independencia de las condiciones iniciales [4]

El uso de la idea de sincronización de sistemas caóticos en la encriptación o envio codificado de señales se debe al trabajo de Cuomo y Oppenheim quienes mostraron como un emisor puede enmascarar una señal arbitraria con una señal caótica y transmitirla públicamente sin necesidad de ningún proceso de codificación, porque al ser la señal caótica esta es invulnerable a esquemas clásicos de decodificación ya que todas las herramientas lineales dan resultado nulo. Por ejemplo una señal caótica tiene un ancho espectral que no permite diferenciarla del ruido. El proceso de decodificación de la señal viene dado justamente por la sincronización adecuada del decodificador caótico con el codificador [6] . Para este trabajo nos basaremos en el procedimiento propuesto en [3]

El trabajo está estructurado de la siguiente forma. En la sección 2 se exhibirán las técnicas de espacio de fase para el sistema caótico elegido, i.e. el péndulo forzado y amortiguado, mostrando la evidencia del caos en este sistema. Esto nos permite elegir la región en el espacio de parámetros para la operación del sistema. En la sección 3 se desarrollará el sistema de comunicación y en particular se mostrará como la sincronización de dos sistemas caóticos, codificador-decodificador, permite desarrollar un esquema para la transmisión codificada de señales. En la sección 4 se muestran los principales resultados y las simulaciones y finalmente se discuten algunas conclusiones y perspectivas del trabajo.

II. EL SISTEMA DE NEWTON-LEIPNIK

El sistema de Newton-Leipnik está descrito por el siguiente conjunto de ecuaciones diferenciales:

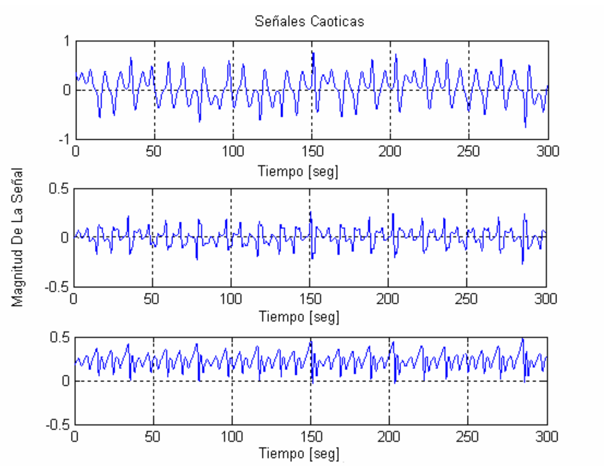
$$\begin{aligned} \dot{x} &= -ax + y + 10yz \\ \dot{y} &= -x - 0{,}4y + 5xz \\ \dot{z} &= bz - 5xy \end{aligned} \tag{1}$$

donde x, y, z son las variables de estado y a, b son dos parámetros positivos. La divergencia del flujo está dada por:

$$\nabla \cdot V = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} = -a - 0{,}4 + b \tag{2}$$

Obviamente, el sistema 1 es disipativo si $-a-0{,}4+b<0$. Cuando $a=0{,}4$ y $b=0{,}175$, las trayectorias del sistema son asintoticamente acotadas, es decir, existe una bola abierta en el espacio de estados donde el sistema estará en todo tiempo.

La respuesta en el tiempo de este sistema puede verse em la siguiente gráfica:



Series de tiempo del sistema

III. SINCRONIZACIÓN DE DOS SISTEMAS NEWTON-LEIPNIK

Sincronización del caos entre dos sistemas identicos Newton–Leipnik es alcanzada en esta seccion. Se supone el sistema maestro de la forma:

$$\begin{aligned} \dot{x}_1 &= -ax_1 + y_1 + 10y_1z_1 \\ \dot{y}_1 &= -x_1 - 0{,}4y_1 + 5x_1z_1 \\ \dot{z}_1 &= bz_1 - 5x_1y_1 \end{aligned} \tag{3}$$

y el sistema esclavo

$$\begin{aligned} \dot{x}_2 &= -ax_2 + y_2 + 10y_2z_2 + u_1 \\ \dot{y}_2 &= -x_2 - 0{,}4y_2 + 5x_2z_2 + u_2 \\ \dot{z}_2 &= bz_2 - 5x_2y_2 + u_3 \end{aligned} \tag{4}$$

donde u_i, $i=\overline{1,3}$ son las entradas de control que deben diseñarse de forma de que los sistemas sincronizen. Para esto se define el sistema de los errores:

$$\begin{aligned} \dot{e}_1 &= -ae_1 + e_3 + 10\left(e_2e_3 + y_1e_3 + e_2z_1\right) + u_1 \\ \dot{e}_2 &= -e_1 - 0{,}4e_2 + 5\left(e_1e_3 + x_1e_3 + e_1z_1\right) + u_2 \\ \dot{e}_3 &= be_3 - 5\left(e_1e_2 + x_1e_2 + e_1y_1\right) + u_3 \end{aligned} \tag{5}$$

donde $e_1=x_2-x_1$, $e_2=y_2-y_1$, $e_3=z_2-z_1$tomados de 3 y 4

Para eliminar las nolinealidades del sistema 5 ley de control activo se toma como:

$$\begin{aligned} u_1 &= -10\left(e_2e_3 + y_1e_3 + e_2z_1\right) + v_1 \\ u_2 &= -5\left(e_1e_3 + x_1e_3 + e_1z_1\right) + v_2 \\ u_3 &= 5\left(e_1e_2 + x_1e_2 + e_1y_1\right) + v3 \end{aligned} \tag{6}$$

De donde reemplazando en 5 el sistema del error queda linealizado de la forma

$$\begin{aligned} \dot{e}_1 &= -ae_1 + e_3 + v_1 \\ \dot{e}_2 &= -e_1 - 0{,}4e_2 + v_2 \\ \dot{e}_3 &= be_3 + v3 \end{aligned} \tag{7}$$

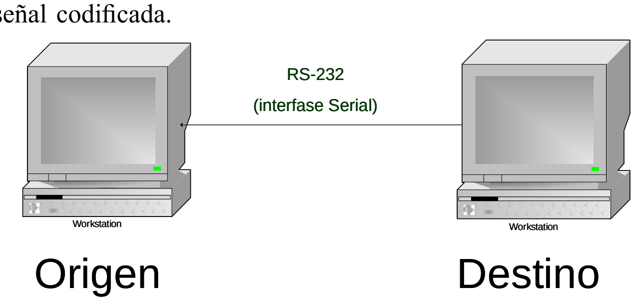
Para que el sistema anterior sea estable se eligen las siguientes señales de control v_i, $i=\overline{1,3}$:

$$\begin{aligned} v_1 &= -e_3 \\ v_2 &= e_1 \\ v_3 &= -\left(b+1\right)e_3 \end{aligned} \tag{8}$$

Así los valores propios del sistema 7 son $-a$, $-0{,}4$ y -1.

IV. IMPLEMENTACIÓN Y RESULTADOS

La implementación básicamente consistió en enviar cuatro señales caóticas de un computador personal a otro, mediante el puerto serial. Tres de estas señales se utilizaron para ser la sincronización y la cuarta se uso como onda portadora de la señal codificada.



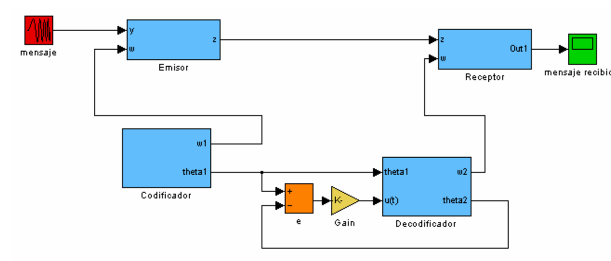
Los códigos para hacer este montaje fueron escritos en MatLab, el código para el transmisor es el siguiente:

```
ser1=serial('com1')
ser1.BaudRate=115200;
ser1.OutputBufferSize=10000;
fopen(ser1)
 fprintf(ser1,'%+3.4f\t',x)
 pause
fclose(ser1)
%envio y
fopen(ser1)
 fprintf(ser1,'%+3.4f\t',y)
 pause
fclose(ser1)
%envio z
fopen(ser1)
 fprintf(ser1,'%+3.4f\t',z)
 pause
fclose(ser1)
%envio suma
fopen(ser1)
 fprintf(ser1,'%+3.4f\t',suma)
 pause
```

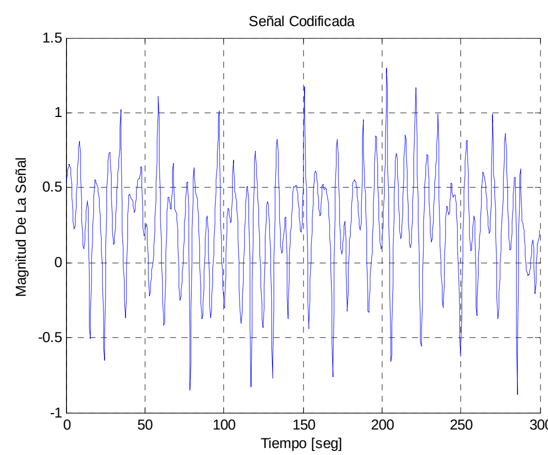
Y el código para el receptor es:

```
%%%%%%Codigo de Recepcion%%%%%%%
%habilitar puerto com1
s = serial('COM1');
%asignar velocidad de transmision
s.BaudRate=115200;
%magnitud del buffer en bytes
s.InputBufferSize=10000;
%se abre el puerto com1
fopen(s)
%comunicacion asincrona
readasync(s)
out = fscanf(s,'%+6.4f\t')
%datos a valores numericos
x=str2num(out)
%se cierra el puerto
fclose(s)
pause
fopen(s)
readasync(s)
out2 = fscanf(s,'%+6.4f\t')
y=str2num(out2)
fclose(s)
pause
fopen(s)
readasync(s)
out3 = fscanf(s,'%+6.4f\t')
z=str2num(out3)
fclose(s)
pause
fopen(s)
readasync(s)
out4 = fscanf(s,'%+6.4f\t')
suma=str2num(out4)
fclose(s)
t1=[1:length(x)];
matx=[t1 ; x]';
maty=[t1 ;y]';
matz=[t1 ;z]';
matsuma=[t1 ;suma]';
```

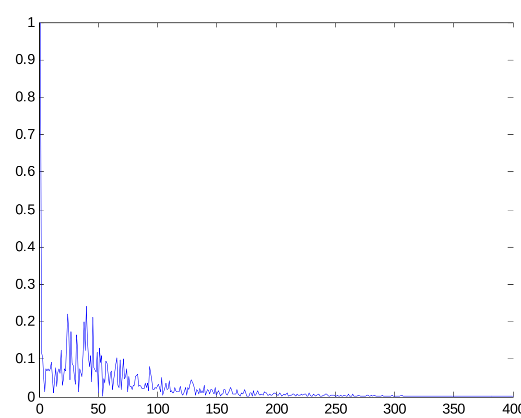
El diagrama de bloques que representa el montaje se muestra en la siguiente figura:



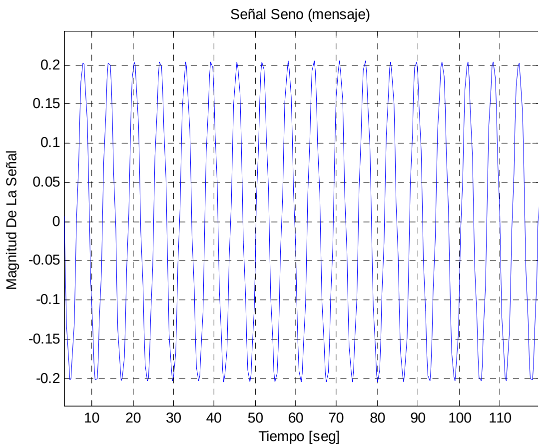
Le señal usada para la encriptación es la suma de las respuestas de los tres estado del sistema emisor,



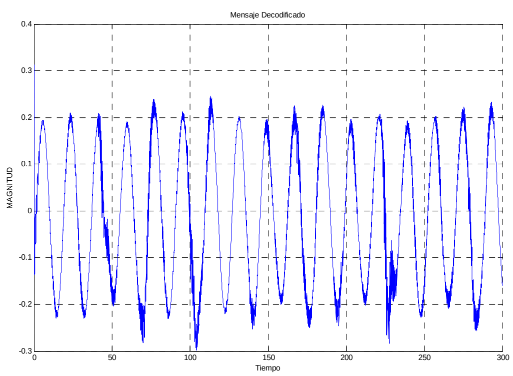
el espectro de potencia de esta señal se mustra a continuación:



Para efectos de experimentación se usó una señal seno para el envío:



La señal obtenida luego de decodificar con el esquema propuesto es:



Señal decodificada

V. Conclusiones

En el presente trabajo se mostró como mediante la sincronización de dos sistemas caóticos es posible desarrollar un esquema eficiente para el envio de señales codificadas. Aprovechando las propiedades altamente irregulares de las señales caóticas es posible enmascarar un mensaje que será posteriormente decodificado con un sistema caótico debidamente sincronizado con el codificador.

La posibilidad de desarrollar otros esquemas de sincronización caótica para procesos de comunicación, en la actualidad es un área de investigación muy activa por las posibilidades de desarrollo de sistemas de transmisión de señales invulnerables a ataques de decodificación.

References

[1] Strogatz, S.H. (2000) Nonlinear Dynamics And Chaos. Perseus Publishing, New York.
[2] Mandelbrot, B.B. (1983) The fractal geometry of nature. Freeman, New York.
[3] Gallego, J.P, Vera C.A., Sánchez J.D. y Rodriguez B.A. (2007)Sistemas Caóticos y su Aplicación en la Encriptección de Señales. Congreso de la Asociación Colombiana de Física.
[4] Ott, E. (2002) Chaos in Dynamical Systems, Second Edition. Cambridge University Press, Cambridge.
[5] Pecora, L.M. and Carroll, T.L. (1990). Synchronization in Chaotic Systems. Phys. Rev. Lett. 64, 821-824.
[6] Cuomo, K.M. and Oppenheim, A.V. (1993). Circuit Implementation Of Synchronized Chaos with Application to Communications. Phys. Rev. Lett. 71, 65-68.
[7] Qiang Jia (2008) Chaos control and synchronization of the Newton–Leipnik chaotic system. Chaos, Solitons and Fractals 35. 814–824