



Enmascaramiento de información mediante Sistemas Caóticos Sincronizados

Camilo Andrés **Ramírez** Sánchez
Universidad Nacional de Colombia
Colombia
kamandrumsan@gmail.com

Resumen

Se presenta modelaciones numéricas de la sincronización de sistemas caóticos, las condiciones para una correcta sincronización y algunos ejemplos de sistemas caóticos que no se pueden sincronizar. Se aplica la característica de sincronización en sistemas caóticos para simular numéricamente el enmascaramiento de información y la transmisión y recuperación de información. La técnica de enmascaramiento es *Chaotic Shift Keying (CSK)* con los sistemas de Lorenz, de Rössler y algunos sistemas de Sprott. Este tipo de modelación estudia la posibilidad de mejorar la seguridad en el envío y manipulación de información confidencial. El software utilizado para las simulaciones es Matlab junto con la herramienta Simulink el cual es un poderoso entorno de programación visual que trabaja con diagramas de flujo.

Palabras clave: Sistemas caóticos, sistema de Lorenz, sistema de Rössler, simulación numérica, modelación, sincronización, enmascaramiento.

Contenido

Los sistemas de ecuaciones diferenciales ordinarias no lineales, en algunos casos, presentan comportamientos caóticos; esto se debe a que aunque son determinísticos (pues conocen las ecuaciones, los parámetros y las condiciones iniciales que lo generan), son sistemas sensibles a las condiciones iniciales; un pequeño cambio en estas condiciones generan que las trayectorias evolucionen totalmente diferentes. Una aplicación de los sistemas caóticos es la sincronización; significa que partiendo de dos sistemas, *Maestro y Esclavo*, este último se modifica haciéndolo dependiente del sistema maestro, la sincronización se presenta cuando para grandes valores del tiempo ambos sistemas tienen comportamientos idénticos aún sin importar las condiciones iniciales que tengan dichos sistemas. Este fenómeno parecería ir en contra de los fundamentos de los sistemas caóticos pues, como ya se mencionó, un cambio pequeño en las condiciones iniciales generan soluciones divergentes, pero en la sincronización las soluciones de los sistemas con condiciones iniciales diferentes convergen al punto de ser iguales.

Al estudiar el fenómeno de sincronización se encuentra una importante aplicación en el desarrollo tecnológico; la sincronización se puede usar para enmascarar información, transmitirla de manera segura y revertir el proceso sin ningún tipo de pérdida, puede presentar una semejanza con uno de los objetivos de las técnicas de cifrado (transmisión segura de datos confidenciales por un medio inseguro) pero otros objetivos de las técnicas de cifrado no se ven reflejados y por lo tanto en ningún momento la información será cifrada.

Antes de presentar los resultados numéricos de varios experimentos se hará una breve introducción a los sistemas dinámicos caóticos y a la sincronización de estos.

Dinámica no lineal

Los sistemas dinámicos se remontan a Newton con los estudios de la mecánica celeste y a Henri Poincaré con el estudio cualitativo de las ecuaciones diferenciales. Más tarde, en el siglo XX, se establece el área de los sistemas dinámicos con los estudios de matemáticos como Lyapunov, S Smale y V. Arnold, entre otros.

La definición de un sistema dinámico se puede aproximar mediante el concepto de sistema determinista, es decir, situaciones que dependen de una condición inicial que varía con respecto a un parámetro (generalmente el tiempo) y a leyes previamente establecidas, esto implica que el conocimiento de la situación en un momento dado da una clara historia de su pasado y una proyección de su futuro. Al pensar en sistemas dinámicos se debe pensar en el conjunto en el cual la condición inicial varía (Este conjunto se conoce como *Espacio estado*) y en las leyes que determinan la evolución de los estados con respecto al tiempo.

Los sistemas dinámicos están regidos por un conjunto de funciones que determinan cómo evoluciona una condición inicial. Para sistemas de dimensión mayor a tres, algunas veces, cuando en el conjunto de funciones hay componentes no lineales, las soluciones de condiciones iniciales muy cercanas son totalmente diferentes o se comportan de manera *especial*, una forma de medir este comportamiento son los coeficientes de Lyapunov, el cual mide cuando una trayectoria de una solución es caótica y cuando no.

Se escogieron varios sistemas caóticos para hacer las modelaciones numéricas, entre estos está el sistema de Lorenz, el sistema de Rössler y uno de los sistemas de Sprott, a continuación se presentan las ecuaciones diferenciales que los definen:

Tabla 1
Sistemas Caóticos

Lorenz	Rössler	Sprott
$\begin{cases} \dot{x} = \sigma(y - x) & \sigma = 16 \\ \dot{y} = -xz + rx - y & r = 45.6 \\ \dot{z} = xy - bz & b = 4 \end{cases}$	$\begin{cases} \dot{x} = -(y + z) & a = 0.2 \\ \dot{y} = x + ay & b = 0.2 \\ \dot{z} = b + z(x - c) & c = 5 \end{cases}$	$\begin{cases} \dot{x} = -2y \\ \dot{y} = x + z^2 \\ \dot{z} = 1 + y - 2z \end{cases}$

Sincronización de sistemas caóticos

La sincronización se considera como un acoplamiento en el cual dos sistemas caóticos exhiben trayectorias en sus soluciones idénticas para grandes valores del tiempo, es decir, en un tiempo $t_0 = 0$ los sistemas parten de condiciones iniciales diferentes pero en algún tiempo t_1 las soluciones convergen y se vuelven idénticas.

Fundamentos de la sincronización

Pécora, Carroll (1990) demostraron que ciertos sistemas caóticos poseen la propiedad de sincronización, particularmente se denomina auto-sincronización, pues un sistema dinámico se descompone en dos sub-sistemas: un sistema *maestro* y un sistema *esclavo*, los cuales se acoplan por medio de alguna técnica. Un ejemplo de sincronización se da con el sistema de Lorenz, sistema desarrollado en 1960 por el señor Edward Lorenz con el fin de modelar los comportamientos climáticos.

$$\begin{cases} \dot{x}_m = \sigma(y_m - x_m) \\ \dot{y}_m = -x_m z_m + r x_m - y_m \\ \dot{z}_m = x_m y_m - b z_m \end{cases} \quad \text{Sistema maestro}$$

$$\begin{cases} \dot{x}_e = \sigma(y_e - x_e) \\ \dot{y}_e = -x_m z_e + r x_m - y_e \\ \dot{z}_e = x_m y_e - b z_e \end{cases} \quad \text{Sistema esclavo}$$

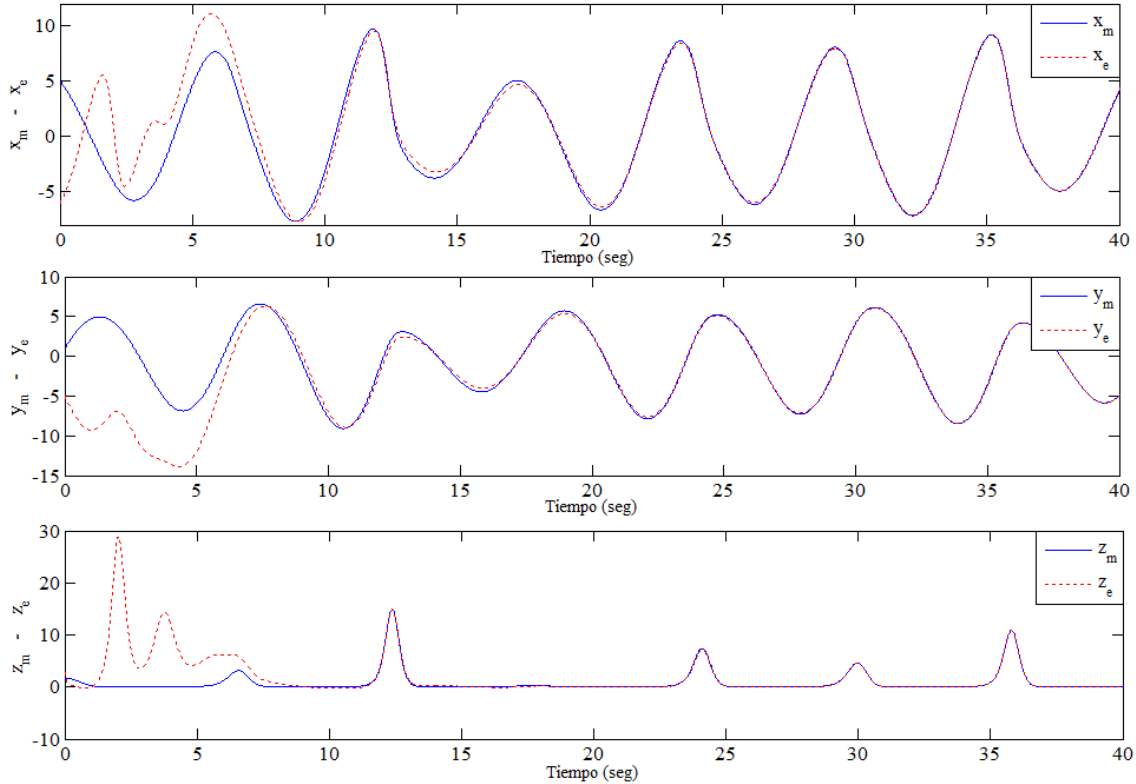


Figura 1. Sistema caótico de Lorenz con las condiciones $x(0) = 0.1$, $y(0) = 1$, $z(0) = 0$

Para este caso, $x_m(t)$ se denomina *coordenada sincronizante* pues es la coordenada que se sustituye en el sistema esclavo por $x_e(t)$ y por lo tanto el sistema esclavo es dependiente por medio de $x_m(t)$ del sistema maestro y esta fuerza a que el sistema esclavo se comporte de la misma manera que sistema maestro. De aquí en adelante las coordenadas de los sistemas estarán diferenciadas por sus subíndices; una m si pertenecen al sistema maestro y una e si pertenecen al sistema esclavo.

Si la evolución de las órbitas solución de $x_m(t) \rightarrow x_e(t)$, $y_m(t) \rightarrow y_e(t)$ y $z_m(t) \rightarrow z_e(t)$ cuando $t \rightarrow \infty$, se dice que los sistemas están sincronizados.

La figura 2 muestra la sincronización del sistema de Lorenz para las tres órbitas solución, con parámetros $\sigma = 16$, $r = 45.6$ y $b = 4$ y condiciones iniciales:

$$\begin{aligned} x_m(0) &= 0.1 & x_e(0) &= -15.9 \\ y_m(0) &= 1 & y_e(0) &= 5.5 \\ z_m(0) &= -2.5 & z_e(0) &= 15 \end{aligned}$$

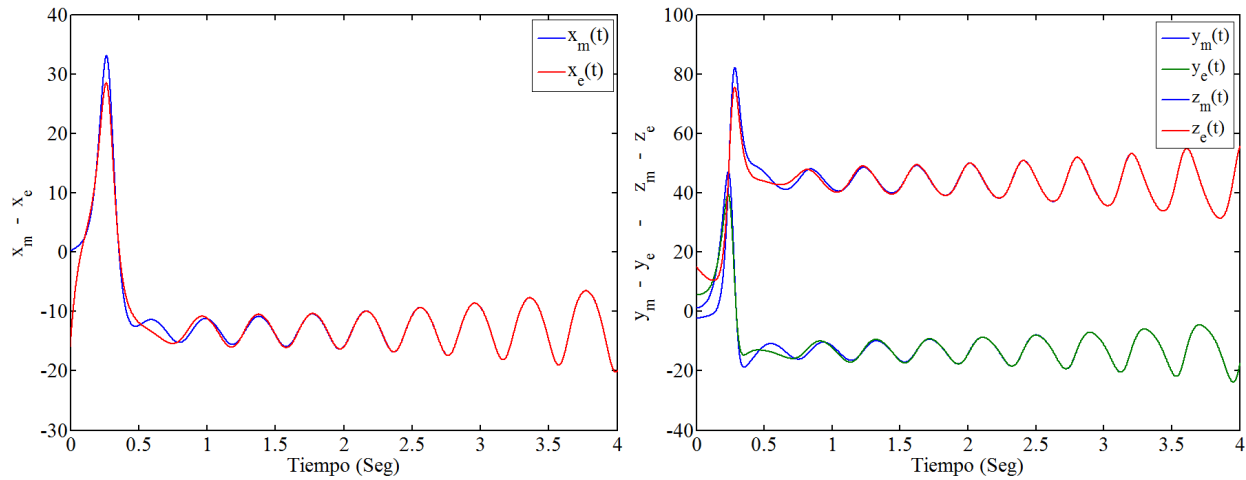


Figura 2. Sincronización en el sistema de Lorenz para $x_m(t)$ y $x_e(t)$ (izquierda) y para las coordenadas $y(t)$ y $z(t)$ (derecha). $t = 4$ seg.

Aquí se observa el proceso de sincronización; las dos órbitas comienzan diferente pero a medida que avanza el tiempo las órbita del sistema esclavo $x_e(t)$, $y_e(t)$ y $z_e(t)$ convergen a las del sistema maestro $x_m(t)$, $y_m(t)$ y $z_m(t)$ respectivamente.

Otra manera de caracterizar la sincronización de un sistema es por medio del *diagrama de sincronización*, en éste se grafica $x_m(t)$ con respecto a $x_e(t)$. Cuando ambos sistemas tienen las mismas condiciones iniciales el diagrama generará una línea recta pero cuando las condiciones son diferentes dicha recta tendrá algunas perturbaciones debido a que la sincronización no se produce desde un principio sino que ha tardado un poco. En caso de no haber sincronización la gráfica se asemejará a un *ruido* y no a una línea recta. La figura 3 muestra la sincronización del sistema maestro - esclavo de Lorenz.

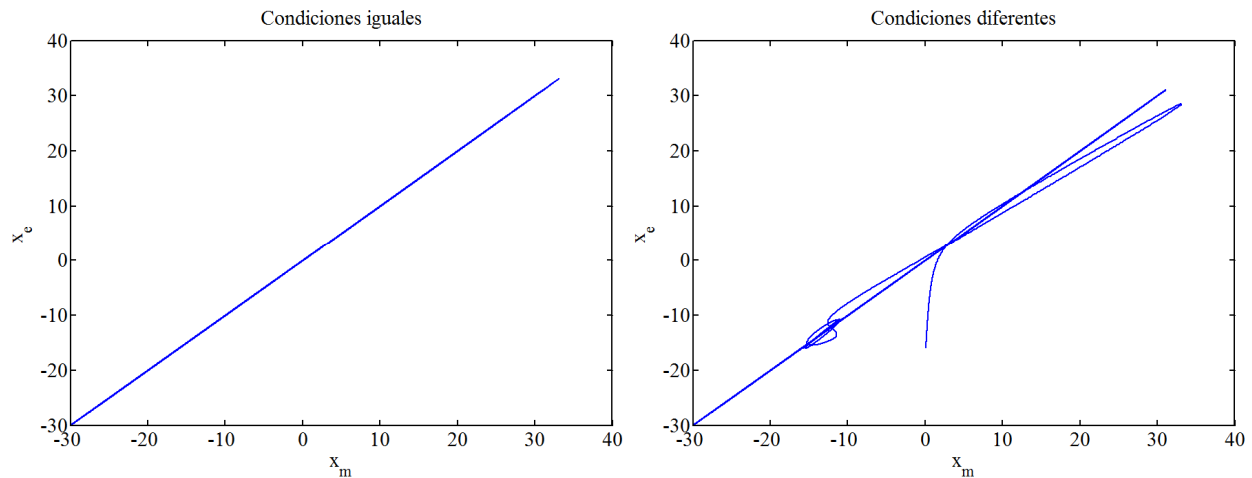


Figura 3. Diagrama de sincronización para el sistema de Lorenz

Con este método de sincronización no es posible sincronizar cualquier sistema caótico pero tiene la característica de que el sistema se puede sincronizar sin importar las condiciones iniciales del sistemas maestro y esclavo.

El sistema de Rössler no se puede sincronizar para ninguna coordenada ya que las órbitas se alejan exponencialmente. La figura 4 muestra como las soluciones intentan converger pero nunca lo hacen y por lo tanto no hay sincronización.

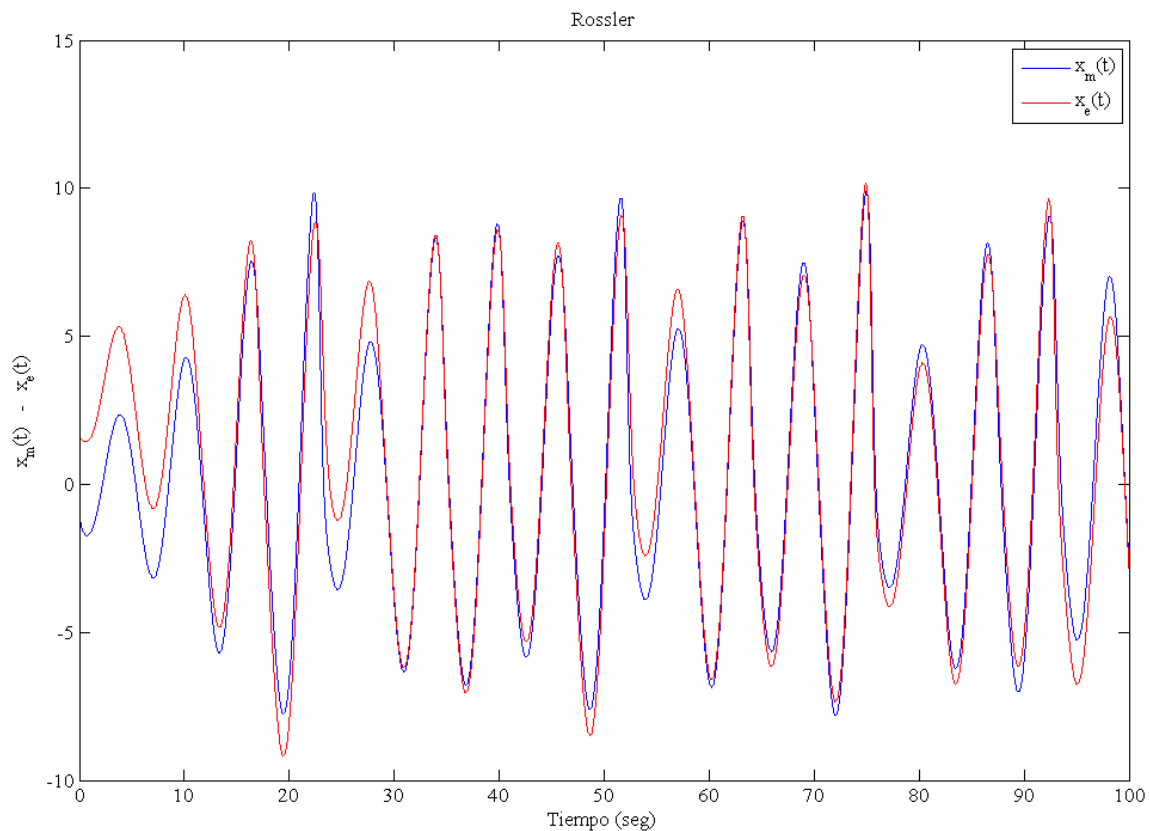


Figura 4. Solución del sistema de Rössler con las condiciones $a = b = 0.2, c = 4.7$

Sincronización *Open- Plus- Colse- Loop (OPCL)*

Lerescu, Constandache, Oancea, Grosu (2008) propusieron este tipo método de sincronización estudiando los sistemas caóticos propuestos por Sprott (1994) y basados en estos proponen sistemas sincronizables con dos o con las tres coordenadas maestras.

La diferencia de este método es que es posible sincronizar cualquier sistema caótico, por ejemplo el sistema de Rössler, el cual no permite el primer método de sincronización, La dificultad de este método es que no se puede sincronizar para cualquier condición inicial y esto imposibilita el uso en las aplicaciones de enmascaramiento. La simulación de sincronización con este método se realiza con un sistema de Sprott, el cual está dado por

$$\begin{cases} \dot{x}_m = -2y_m \\ \dot{y}_m = x_m + z_m^2 \\ \dot{z}_m = 1 + y_m - 2z_m \end{cases} \quad \text{Sistema maestro}$$

$$\begin{cases} \dot{x}_e = -2y_e \\ \dot{y}_e = x_e + z_e^2 + (p - 2z_m)(z_e - z_m) \\ \dot{z}_e = 1 + y_e - 2z_e, \end{cases} \quad \text{Sistema esclavo} \quad p < 0$$

La figura 5 muestra la sincronización de las órbita solución con parámetro $p = -16$ y las condiciones iniciales:

$$\begin{array}{ll} x_m(0) = -4 & x_e(0) = 2.5 \\ y_m(0) = 1.5 & y_e(0) = 0.2 \\ z_m(0) = -12 & z_e(0) = 5 \end{array}$$

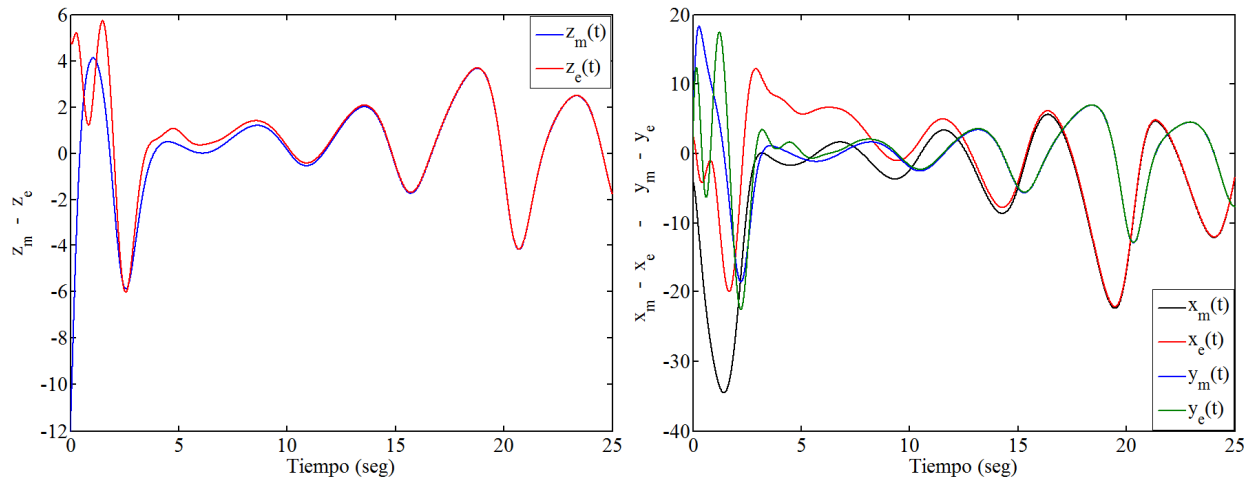


Figura 5. Sincronización en el sistema de Sprott para $z_m(t)$ y $z_e(t)$ (izquierda) y para las coordenadas $x(t)$ y $y(t)$ (derecha). $t = 25$ seg.

Ya que con este método de sincronización no se puede utilizar sincronizar globalmente entonces no se puede aplicar para el enmascaramiento de datos, por lo tanto, de aquí en adelante se trabajará con el sistema de Lorenz y el primer método de sincronización

Enmascaramiento de información

La sincronización de sistemas caóticos tiene una potencial aplicación en la transmisión de comunicaciones seguras ya que en algunos casos permite enmascarar información. El principio fundamental del enmascaramiento es esconder información mediante algún *método* y que esta pase *desapercibida* en un "*canal ruidoso*". Puntualmente la información que se busca esconder es una señal de bits dado que cualquier dato numérico se puede codificar al sistema binario dando como resultados un pulso con solo ceros y unos.

El medio por el cual se va a esconder el pulso son las soluciones de sistemas caóticos pues son irregulares, complejos y sincronizables, características que permite enmascarar un pulso, que este no sea detectable cuando se esté transmitiendo y que se pueda recuperar sin pérdida de información.

Para que la señal se pueda enmascarar y recuperar sin pérdida de información debe tener dos requisitos fundamentales, el primero es que su frecuencia sea alta y el segundo es que su amplitud sea baja, con estas condiciones resulta sencillo enmascarar señales periódicas ya que se puede modular su amplitud y frecuencia. Un pulso cuadrado tiene algunas complicaciones, no es periódico y la frecuencia debe ser escogida lo suficientemente alta para que su espectro de Fourier se esconda en la señal sincronizable.

Actualmente existen diversas técnicas para poder enmascarar información entre las que se destacan cuatro: "*Chaos Masking (CM)*", "*Chaotic Shift Keying (CSK)*", "*Chaotic Parameter Modulation Technique*" y "*Message Inclusion Technique*". En este trabajo se considera la técnica CSK ya que está especialmente diseñada para pulsos cuadrados.

Chaos Shift Keying

La idea básica de este método de enmascaramiento es *modular* algún parámetro del sistema maestro la cual depende del valor de la señal a transmitir. En el sistema esclavo el coeficiente de modulación producirá un error de sincronización entre la señal recibida y la señal regenerada. Usando este error el mensaje puede ser recuperado.

Por lo tanto, este método utiliza dos sistemas maestros que se diferencian por el cambio de uno de los parámetros y un sistema esclavo que se acopla con los sistemas maestros. Utilizando la misma coordenada sincronizante en ambos sistemas maestros la señal que se transmite es la combinación de dichas coordenadas; la primera si el pulso es cero y la segunda cuando el pulso es uno. Esto hace que la coordenada regenerada sea idéntica a la primera cuando el pulso es cero y produzca un error cuando el pulso sea uno, finalmente al restar la coordenada regenerada del sistema esclavo con la coordenada sincronizante del primer sistema maestro la señal resultante es muy cercana a cero cuando el pulso era cero y presentará un *ruido* significativo cuando el pulso sea uno, estos ruidos permiten recuperar el pulso original.

El esquema de la figura 6 da una idea de la estructura de la técnica CSK cuando $x_{m1}(t)$ es la coordenada sincronizante.

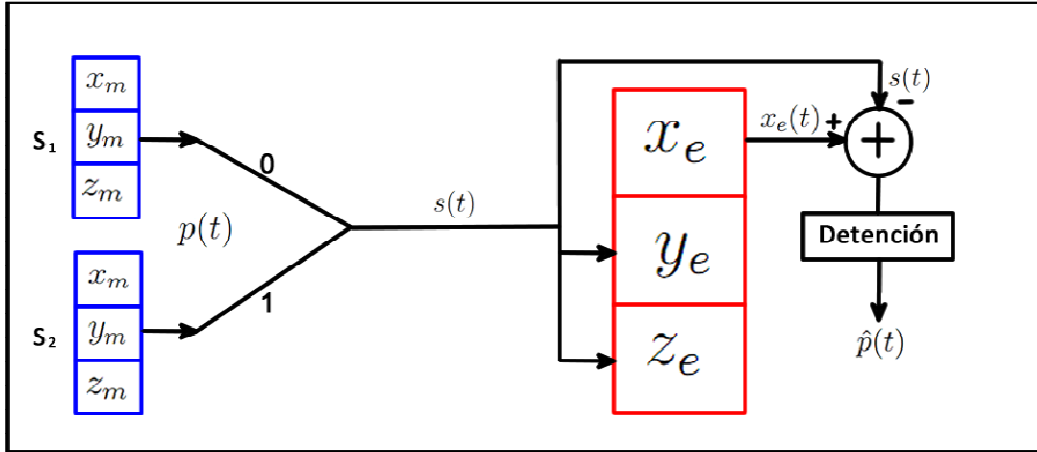


Figura 6. Esquema del método CSK

Del emisor (la combinación de los sistemas maestros, $S_{m1}(x, y, z)$ y $S_{m2}(x, y, z)$) se escoge la coordenada sincronizante $x_{m1}(t)$ y $x_{m2}(t)$ para cada instante de t si $p(t) = 0$ se transmite $x_{m1}(t)$ y si $p(t) = 1$ se transmite $x_{m2}(t)$, entonces $s(t)$ es el resultado de combinar las coordenadas sincronizantes. Luego $s(t)$ se acopla con el receptor (sistema esclavo) y genera a $x_e(t)$, esta se resta con $s(t)$; $r(t) = x_e(t) - s(t)$ es una señal compuesta con una amplitud significativamente grande cuando $p(t) = 1$, en comparación a la baja amplitud cuando $p(t) = 0$. $\hat{p}(t)$ es la señal que resulta al detectar el ruido de $r(t)$, convertirlo en uno, y el resto convertirlo en cero.

A continuación se presenta la simulación de enmascarar los dígitos de una tarjeta de crédito por el método CSK, En primer lugar, toda la información que se transmitirá se codificará en código binario y este generará un pulso con un periodo determinado $p(t)$. Se escoge el sistema de Lorenz para sincronizar puesto que los sistemas de Sprott y la sincronización OPCL es ineficiente para transmitir información.

La coordenada sincronizante será $x_m(t)$, los sistemas maestros y esclavo son:

$$\begin{cases} \dot{x}_{m1} = \sigma(y_{m1} - x_{m1}) \\ \dot{y}_{m1} = -x_{m1}z_{m1} + rx_{m1} - y_{m1} \\ \dot{z}_{m1} = x_{m1}y_{m1} - 4z_{m1} \end{cases} \quad \begin{cases} \dot{x}_{m2} = \sigma(y_{m2} - x_{m2}) \\ \dot{y}_{m2} = -x_{m2}z_{m2} + rx_{m2} - y_{m2} \\ \dot{z}_{m2} = x_{m2}y_{m2} - 4.4z_{m2} \end{cases}$$

$$\begin{cases} \dot{x}_e = \sigma(y_e - x_e) \\ \dot{y}_e = -x_e z_e + rx_m - y_e \\ \dot{z}_e = x_e y_e - 4z_e \end{cases}$$

Con los parámetros $\sigma = 16$, $r = 45.6$ y las condiciones iniciales:

$$\begin{array}{lll}
 x_{m1}(0) = 0.1 & x_{m2}(0) = 0.1 & x_e(0) = -15.9 \\
 y_{m1}(0) = 1 & y_{m2}(0) = 1 & y_e(0) = 5.5 \\
 z_{m1}(0) = -2.5 & z_{m2}(0) = -2.5 & z_e(0) = 15
 \end{array}$$

Se debe escoger un periodo para el pulso que se genera del código binario, y este debe ser lo suficientemente grande para que no haya problema en la recuperación de la señal $r(t)$, pero a su vez no debe ser tan grande porque el tiempo de transmisión se aumentaría significativamente. Por ejemplo un pulso con un periodo de 6 seg y 20 dígitos se demoraría aproximadamente 2 minutos en transmitir la información (10 dígitos cada minuto). Como los resultados encontrados en las simulaciones numéricas sugieren que el pulso tenga un periodo mayor a 3 seg, se trabajará con un periodo de 3.5 segundos, es importante que el receptor conozca el periodo con el que se envía el pulso pues esto facilita la detección de la señal.

Ya que una tarjeta de crédito tiene 16 dígitos se escogerá aleatoriamente un número con estos dígitos el cual se transmitirá; $m(t) = 5514\ 6312\ 5552\ 0014$, estos se codifican y generan un código binario con 53 cifras.

Debido a que los sistemas maestro - esclavo no sincronizan inmediatamente se comenzará a transmitir el mensaje a los 8 segundos después de iniciados los sistemas, por lo tanto la transmisión duraría aproximadamente 190 segundos, en la figura 7 se observa a $p(t)$ generado por $m(t)$

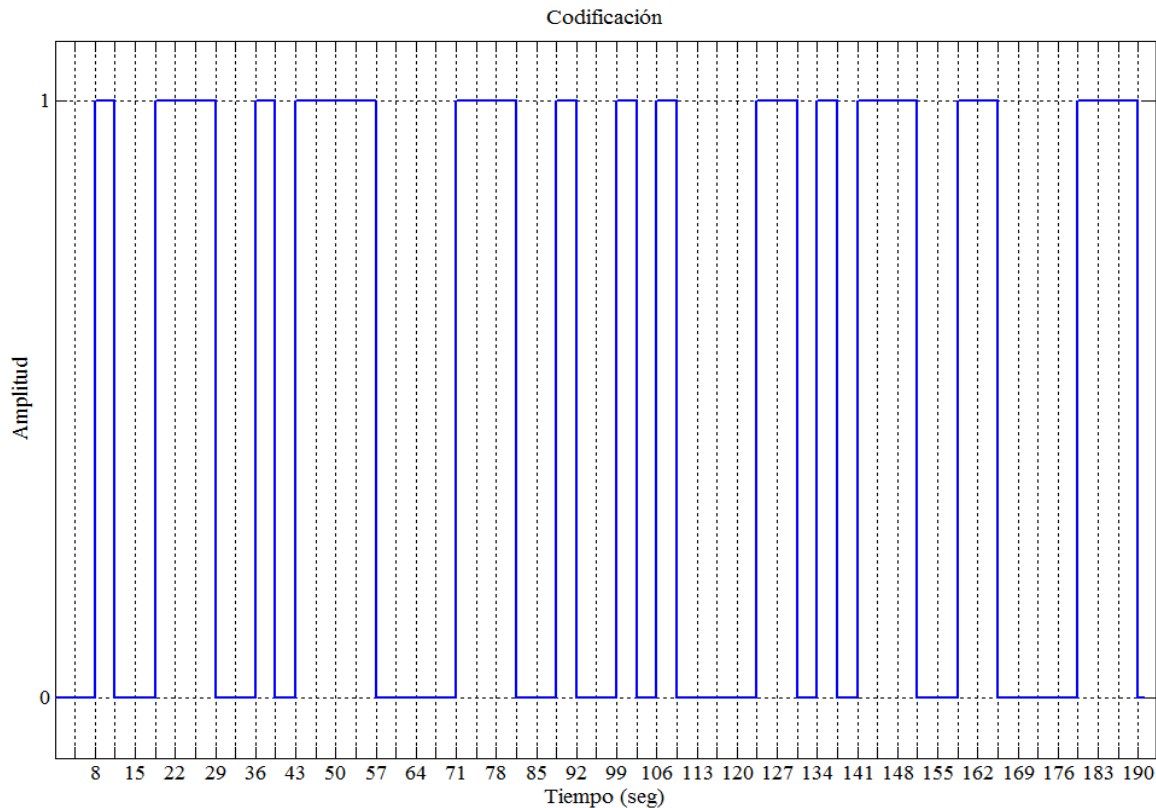


Figura 7. Señal $p(t)$ resultante al codificar los 16 dígitos de la tarjeta de crédito, con un periodo de 3.5 segundos

La figura muestra como cada 3.5 segundos se transmite un 1 o un 0 y en algunas ocasiones se tienen varios 1 o 0. $s(t)$ es la señal que resulta de la solución de los sistemas maestros los cuales solo se diferencian por el parámetro b ($b = 4$) si $p(t)$ transmite un 0 y ($b = 4.4$) si $p(t)$ transmite un 1. Esta se acopla con el sistema esclavo como si fuera la coordenada $x(t)$ y los sistemas se sincronizan. En la figura 8 se ve el diagrama de sincronización de $s(t)$ con respecto a $x_e(t)$, la línea muestra un grosor debido al error de sincronización que se produce.

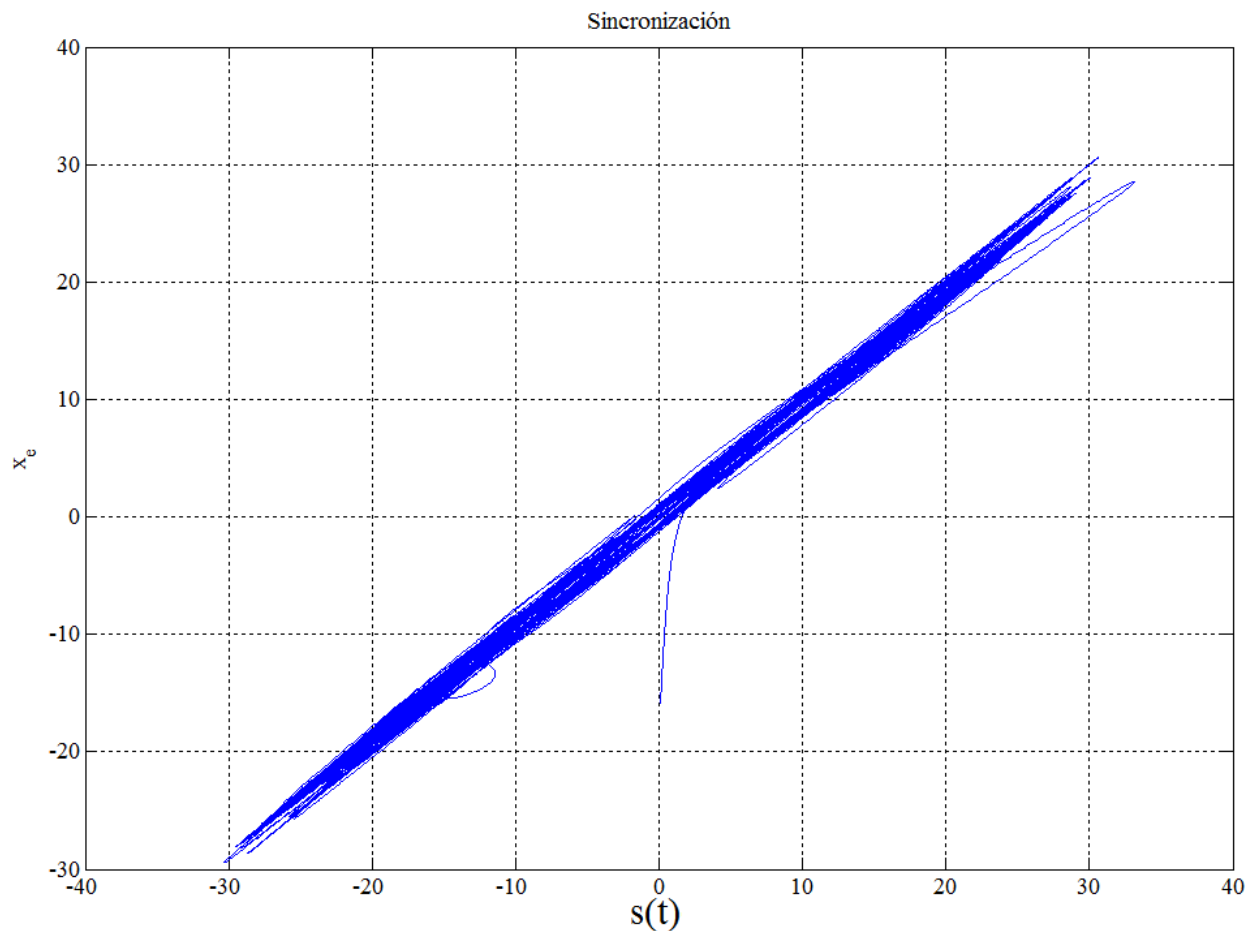


Figura 8. Diagrama de sincronización del sistema de Lorenz por el método CSK

Hay dos tipos de errores, uno es cuando se transmite un 0; el error será muy pequeño, el otro es cuando se transmite un 1; el error será considerablemente mayor al primero.

Gracias a este error se puede generar $r(t) = x_e(t) - s(t)$ el cual se utiliza para detectar el mensaje, la figura 9 muestra el cuadrado de la señal generada por el error de sincronización.

En la figura 9 se grafica el cuadrado del error pues así se amplía el error que se produce cuando se envía un 1 y es más fácil trabajar con este para recuperar el pulso. En general, se ve como los errores dan una idea del pulso enviado y la detección es bastante fácil puesto que se conoce el periodo y el paso alto y bajo.

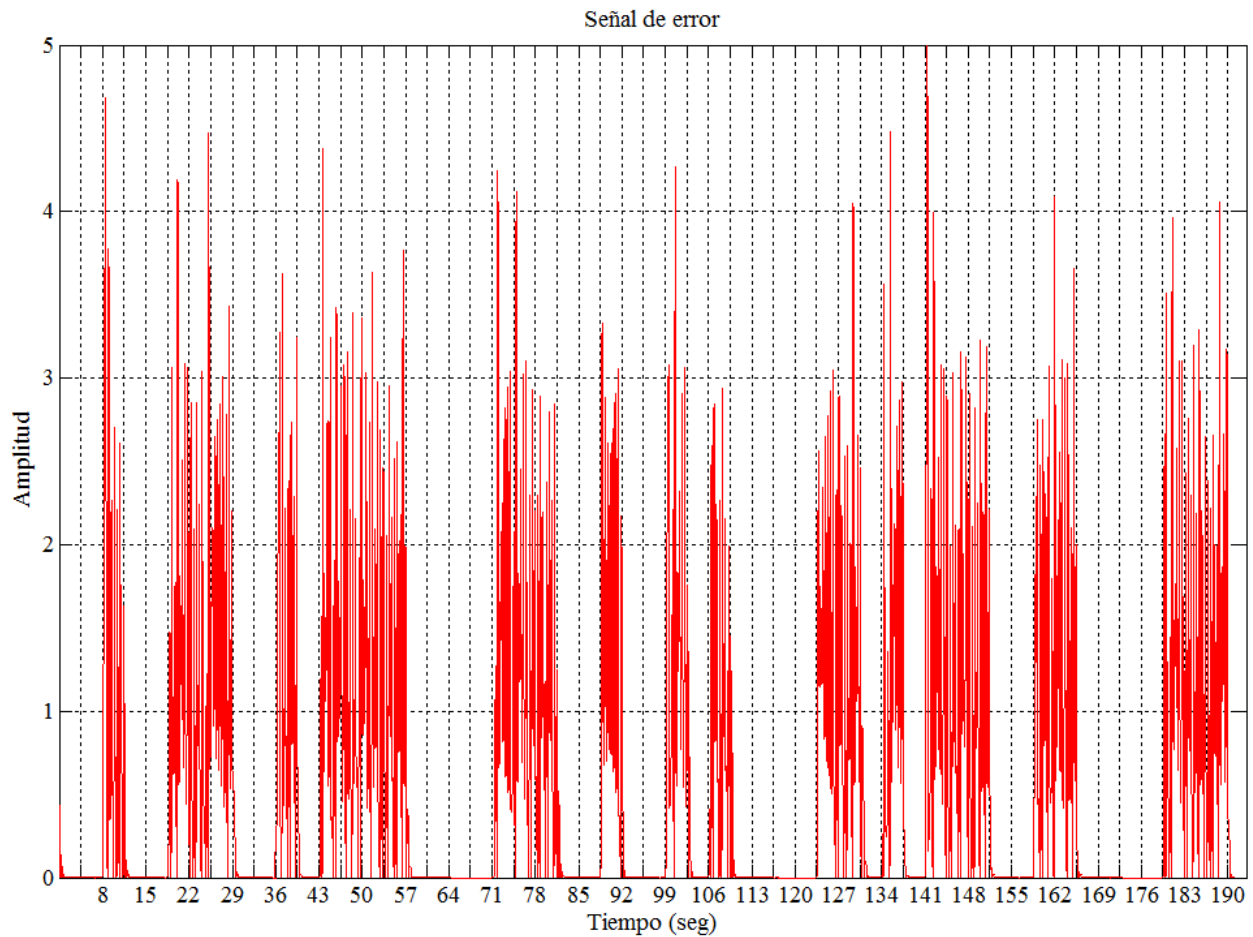
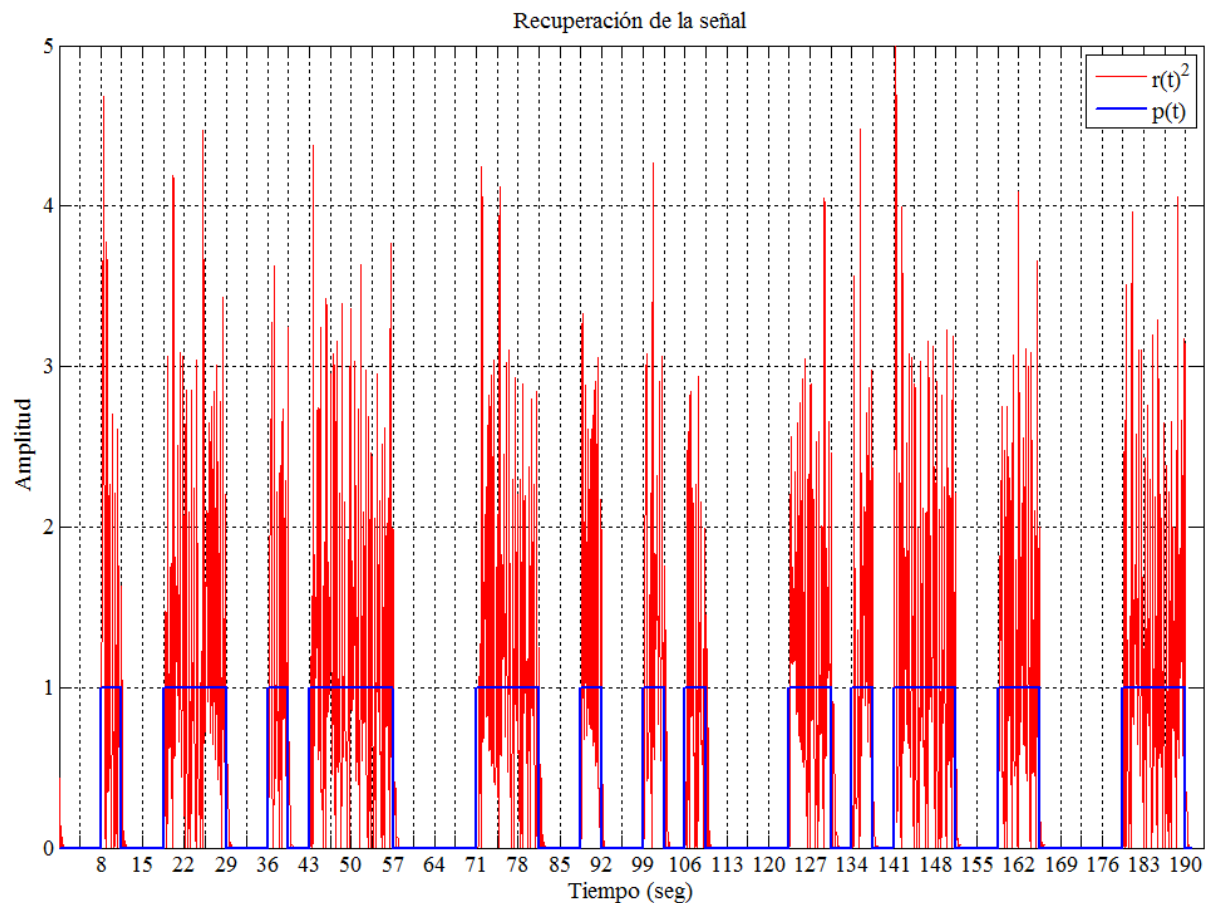


Figura 9. $r(t)^2$ error generado en la sincronización

Con $r(t)^2$ se puede recuperar la señal filtrando adecuadamente esta señal. En la figura 10 se ve que la señal recuperada es igual al pulso que se envió, por lo tanto con esta señal se puede generar los 16 dígitos que se transmitieron.

De esta manera, experimentalmente, un emisor enmascaró los dígitos de una tarjeta de crédito en una señal caótica y los transmitió por un canal ruidoso hasta un receptor el cual conociendo el sistema caótico y los parámetros que lo generaron puede desenmascarar la señal y recuperarla sin comprometer la información.



Referencias y bibliografía

- Arguelles, A. (2001). Transmisión de información con señales caóticas. Trabajo de pre-grado. Universidad Nacional de Colombia. Bogotá. Colombia.
- Lerescu, A.I., Constandache, N., Oancea, S., & S. Grosu, L. (2004). Collection of Master-Slave Synchronized Chaotic Systems. *Chaos, Solitons and Fractals*, 22, 599–604.
doi:10.1016/j.chaos.2004.02.039.
- Lerescu, A.I., Constandache, N., Oancea, S., & S. Grosu, L. (2006). Collection of Mutually Synchronized Chaotic Systems. *Physics Letters A*, 352, 222–226.
doi:10.1016/j.physleta.2005.11.069
- Pecora, L., & Carroll, T. (1991). Driving systems with chaotic signals. *Physical Review A*, 44, 2374–2383. doi: 10.1103/PhysRevA.44.2374
- Pecora, L., & Carroll, T. (1996). Synchronization in chaotic system. *Controlling Chaos. Theoretical and Practical Methods in Non-linear Dynamics*, 142–145.
doi:10.1016/B978-012396840-1/50040-0.
- Perez, G., & Cerdeira, H. (1996). Extracting Messages Masked by Chaos. *Controlling Chaos. Theoretical and Practical Methods in Non-linear Dynamics*, 157–160.
doi:10.1016/B978-012396840-1/50043-6
- Sprott, J.C. (1994). Some simple chaotic flows. *Physical Review E*, 50, r647–r650.
doi:10.1103/PhysRevE.50.R647