Sincronización de caos mediante observadores para cifrado en comunicaciones

Juan Ángel Rodríguez Liñán, Jesús de León Morales
Doctorado en Ingeniería Eléctrica, FIME-UANL
angelrdz@gmail.com, drjleon@hotmail.com

RESUMEN

En este trabajo, se presenta una estrategia de sincronización para la clase más simple de sistemas caóticos, conocida como clase P. El problema de sincronización es tratado mediante la aplicación de la teoría de observadores de estado para reconstruir las señales. Además, se presenta un estudio donde la estrategia de sincronización propuesta es aplicada al problema de cifrado de información en un sistema de comunicaciones seguras. Se presentan resultados en simulación, donde se ilustra el desempeño de este esquema y su potencial en aplicaciones de comunicación segura.

PALABRAS CLAVE

Sistemas caóticos, sincronización de caos, observadores de estado, cifrado de información.

ABSTRACT

A strategy of synchronization for the simplest class of chaotic systems, knowing as P-class, is presented. In this work, the synchronization problem is managed by means of the observer's theory for reconstructing the signals.Furthermore, a study is presented where the proposed strategy of synchronization is applied to the ciphering of information problem in secure communication system. Results of simulation are presented in order to illustrate the performance of this scheme and its potencial application in secure communications.

KEYWORDS

Chaotic systems, chaos synchronization, state observers, information encryption.

INTRODUCCIÓN

El caos está asociado con comportamientos muy complicados e impredecibles debidos a situaciones complejas, y es sinónimo de desorden y confusión, lo que hace pensar que es absurdo estudiarlo e imposible entenderlo. Sin embargo, en la ciencia moderna, el término caos se emplea para referirse a un comportamiento que tiene lugar en algunos sistemas en particular.

Según el modelo newtoniano de la mecánica, si la posición y la velocidad iniciales de un conjunto de partículas fueran conocidas, así como las fuerzas aplicadas a éstas en todo tiempo, se podrían predecir sus trayectorias para todo

tiempo futuro. Asimismo, se suponía también que trayectorias complejas tenían necesariamente su origen en interacciones muy complicadas de muchos cuerpos. Además, que sistemas sencillos producirían trayectorias simples, y que pequeñas modificaciones en las condiciones iniciales no producen más que pequeñas modificaciones en la evolución futura.

Sin embargo, actualmente se sabe que bajo ciertas condiciones, existen sistemas simples que también exhiben comportamiento muy complejo y errático, y sobre todo que no es posible predecir cambios abruptos en su evolución provocados por pequeños cambios en sus condiciones iniciales, a este fenómeno se le ha llamado caos.

Este fenómeno fue descubierto por el meteorólogo Edward Lorenz,[1] mientras estudiaba un modelo del sistema atmosférico en 1963, al notar que la evolución del clima resultaba ser muy sensible a pequeños cambios, y a lo cual posteriormente se le denominó *Efecto Mariposa*, que se describe como "el simple aletear de una mariposa puede provocar un huracán en algún lugar del planeta".

Este fenómeno se presenta en sistemas o procesos dinámicos importantes tales como la turbulencia en fluidos, también se presenta en dispositivos láser retroalimentados, en vibraciones mecánicas debidas a fricción, en procesos biológicos, entre otros.[2]

De tal manera que, los sistemas denominados caóticos son aquellos sistemas no lineales cuyas trayectorias son acotadas y tienen un comportamiento no periódico (oscilaciones erráticas o irregulares que no se repiten nunca) que aparece bajo condiciones totalmente deterministas (puesto que obedecen a leyes bien conocidas y no hay aleatoriedad alguna), y que principalmente, presentan alta sensibilidad a la variación de sus condiciones iniciales.

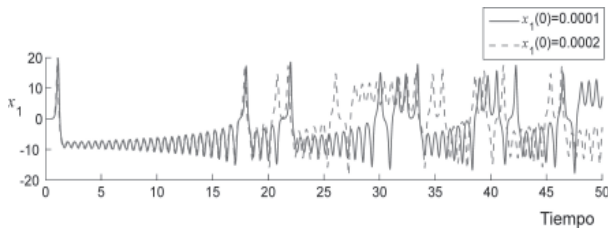

Fig. 1. Trayectorias con evolución diferente debidas a una pequeña diferencia en la condición inicial $x_1(0)$, correspondiente al sistema caótico estudiado por E. Lorenz.

Dicha sensibilidad significa que trayectorias que inician arbitrariamente cercanas entre sí, divergen en el tiempo, por lo cual son impredecibles a mediano y largo plazo, a pesar que cada trayectoria permanece acotada, tal como se muestra en la figura 1.

Por otro lado, la sincronización de caos es la inducción de un régimen en el cual dos sistemas caóticos (uno llamado maestro y otro llamado esclavo) exhiben trayectorias idénticas ($x_M = x_S$) luego de introducir algún tipo de acoplamiento entre ellos,[3] tal como se muestra en la figura 2(a). La figura 2(b) muestra que la trayectoria x_S del sistema esclavo es sincronizada con la trayectoria x_M del sistema maestro aproximadamente a partir de 40 segundos.

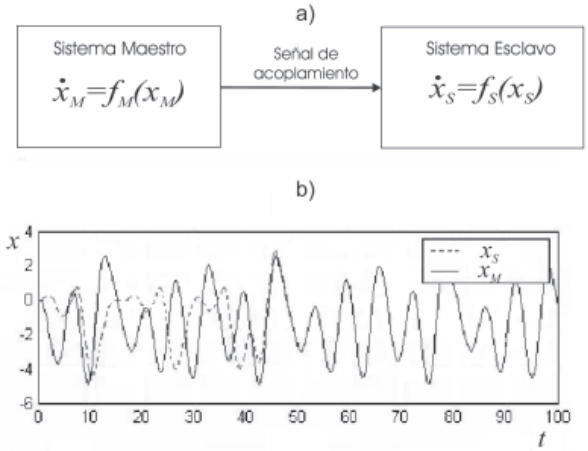

Fig. 2. a) Esquema de sincronización de dos sistemas mediante una señal de acoplamiento, b) Trayectoria x_S del sistema esclavo sincronizada con la trayectoria x_M del maestro luego de un estado de transición.

Por citar algunos casos, se ha reportado que la sincronización aparece en procesos físicos y biológicos tales como la relación entre las neuronas en el sistema nervioso,[4] y en la relación fisiológica entre el corazón y los pulmones.[5]

Por otra parte, la sincronización caótica es de gran interés práctico, ya que mediante ella es posible realizar importantes aplicaciones para cifrado de información en telecomunicaciones[6] en servicios tales como: Enlaces de comunicación militar y empresas privadas, transacciones financieras, operaciones comerciales con firmas electrónicas por Internet, y otros.

La figura 3 muestra un caso de comercio electrónico, donde es indispensable mantener la seguridad informática para realizar operaciones de

compra-venta a través de la Internet y movimientos bancarios a distancia, protegiendo la identidad e información de los clientes e instituciones.

La motivación de utilizar sistemas caóticos en cifrado de información se debe a la característica de impredictibilidad de este tipo de sistemas, lo cual proporciona un alto nivel de seguridad.[7]

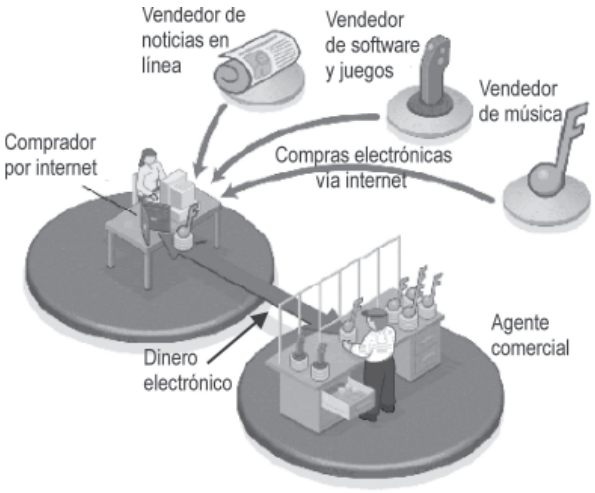

Fig. 3. Comercio electrónico por internet, el cual requiere seguridad informática en comunicaciones.

En este trabajo se describe una técnica de cifrado para sistemas de comunicación, combinando, por un lado, las características de los sistemas caóticos y la sincronización de caos, y por el otro aplicando la teoría de observadores para la reconstrucción de los estados. Además, se ilustra la implementación de dicho esquema mediante un ejemplo con el fin de mostrar el potencial del proceso de cifrado caótico. Finalmente, se desea motivar y despertar el interés en el desarrollo y utilización de este tipo de técnicas.

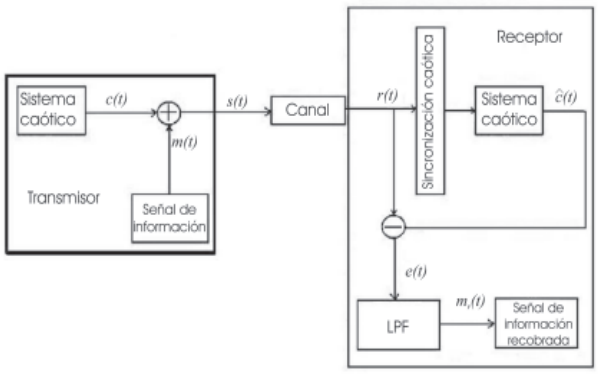

Fig. 4. Esquema de cifrado por enmascaramiento.

ESQUEMA DE SINCRONIZACIÓN EN COMUNICACIONES

La implementación del esquema de sincronización de sistemas caóticos en comunicaciones consiste, básicamente, en que un sistema transmisor (maestro) genere una señal portadora caótica, la cual es modulada por la señal de información, de tal forma que la información sea cifrada debido a la característica caótica de la portadora.

Los métodos de cifrado que se encuentran comúnmente en la literatura[8] y que son utilizados para ello son:

(1) Enmascaramiento, que consiste en sumar la señal de información directamente a la portadora caótica, como se muestra en la figura 4.

(2) Conmutación caótica, que significa transmitir una señal binaria mediante la conmutación entre dos portadoras caóticas generados por dos sistemas diferentes, como se muestra en la figura 5.

(3) Modulación por parámetro, donde un parámetro del sistema transmisor (maestro) es evaluado como una función de la señal de información, lo cual modula a la señal portadora (figura 6).

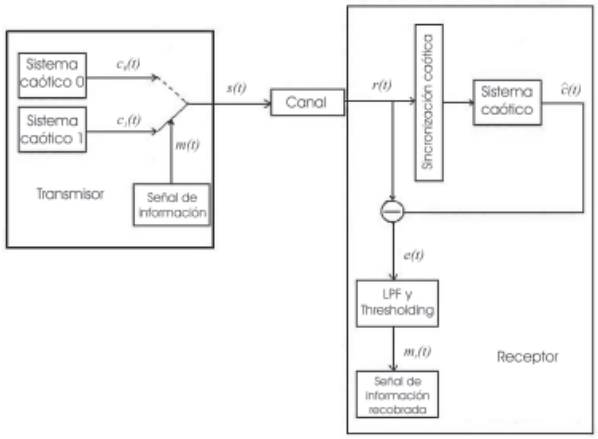

Fig. 5. Esquema de cifrado por conmutación caótica.

Posteriormente, la señal modulada por alguno de los métodos mencionados es transmitida por un canal público de comunicación, y captada por el sistema receptor (esclavo). Este sistema de recepción debe ser capaz de sincronizarse con el sistema maestro y contar con una técnica de descifrado para recuperar la señal de información original. El proceso de descifrado se realiza mediante un proceso de detección del error de sincronización formado por

un filtro pasa bajas (LPF) y detección de umbral (thresholding), según se muestra en los esquemas.

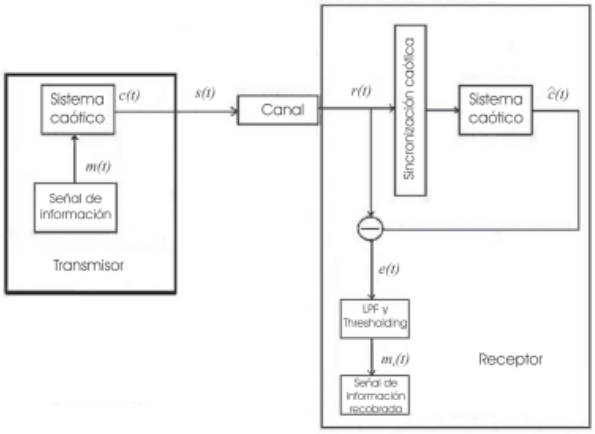

Fig. 6. Esquema de modulación por parámetro.

El problema de sincronización puede resolverse desde el punto de vista de la teoría de observadores,[9] mediante el diseño del sistema esclavo como un observador de estado. La figura 7 muestra el esquema de un observador, el cual es un sistema dinámico capaz de estimar las trayectorias de estado *x* del sistema original, a partir de las señales de entrada *u* y de salida *y*.

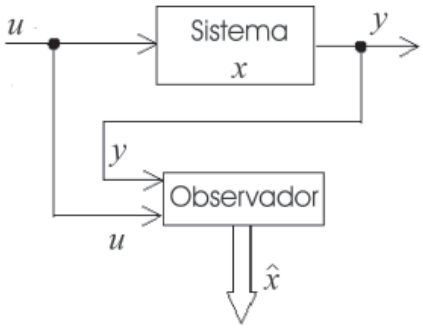

Fig. 7. Esquema sistema-observador: El observador estima las variables de estado *x* a partir de las variables de entrada *u* y salida *y* del sistema.

En la siguiente sección, se presenta más detalladamente el esquema de sincronización mediante un observador de estado.

SINCRONIZACIÓN DE SISTEMAS CAÓTICOS MEDIANTE OBSERVADORES

Considérese un sistema maestro dado por

$$\dot{x} = f(x,\alpha) \qquad (1)$$

donde x es el vector de estado y α es un parámetro real finito. Particularmente, en este trabajo, el sistema (1) representa una clase de ecuaciones diferenciales de tercer orden, definidas por una función polinomial constituida por tres monomios, incluida una no linealidad de tipo cuadrática. Dos de estas ecuaciones son polinomios no lineales de la forma

$$\dddot{x} + \ddot{x} + x - \varphi(x,\dot{x}) = 0 ,$$

donde

$$\varphi(x,\dot{x}) = \dot{x}^2 \text{ o } \varphi(x,\dot{x}) = x\dot{x} .$$

De esta manera, la ecuación (1) constituye una familia de sistemas,[10] conocida como clase P, con cinco monomios en el lado derecho de la ecuación, donde cuatro coeficientes son unitarios, y otro está representado por el parámetro α. Además, todos estos sistemas exhiben comportamiento caótico para un mismo rango del parámetro α, que se encuentra en el intervalo: $2.0168 < \alpha < 2.0577$.

Por otra parte, el sistema (1), bajo un cambio de coordenadas apropiado, puede ser escrito como un sistema afín en el estado de la forma

$$\begin{cases} \dot{x} = A(\alpha, y)x + \varphi(y) \\ y = Cx \end{cases} \qquad (2)$$

Donde y es definida como una variable de salida del sistema, por ejemplo i.e. la señal de acoplamiento entre los sistemas maestro y esclavo. Las componentes de la matriz $A(\alpha, y)$ y del vector $\varphi(y)$ son funciones continuas que dependen de α y y.

Entonces, un sistema esclavo sincronizable con un sistema maestro representado por (2), puede ser diseñado como un observador exponencial descrito por

$$\begin{cases} \dot{\hat{x}} = A(\alpha, y)\hat{x} + \varphi(y) + S^{-1}C^T(y - \hat{y}) \\ \hat{y} = C\hat{x} \end{cases} \qquad (3)$$

Donde $\hat{x}$ es la estimación del vector de estado x, y $S^{-1}C^T$ es un término, conocido como la ganancia del observador, que depende de la solución S de la ecuación

$$\dot{S} = -\rho S - A^T(\alpha, y)S - SA(\alpha, y) + C^T C \qquad (4)$$

Y ρ es alguna constante positiva suficientemente grande[11] que permite acelerar la razón de convergencia de los estados estimados hacia los reales.

De esta forma, la convergencia de $\hat{x}$ al vector de estado x es considerada como la sincronización de (3) a (1).

PROCEDIMIENTO PARA APLICACIÓN EN COMUNICACIONES

Con el fin de ilustrar la implementación del esquema de sincronización, considérese un sistema maestro dado por el sistema caótico clase P (1) descrito por

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = x_3 \\ \dot{x}_3 = -\tilde{\alpha}x_3 - x_1 + x_1x_2 \end{cases} \tag{5}$$

Donde $x = [x_1 \quad x_2 \quad x_3]^T$ es el vector de estado y $\tilde{\alpha}$ el parámetro del sistema. Las figuras 8 y 9 muestran la evolución de las trayectorias caóticas de (5) en el tiempo y en el espacio de fases, respectivamente.

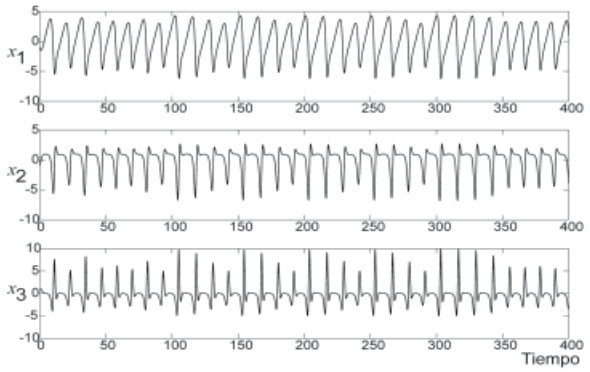

Fig. 8. Trayectorias caóticas x_i (i=1, 2, 3) de (5) *vs.* tiempo.

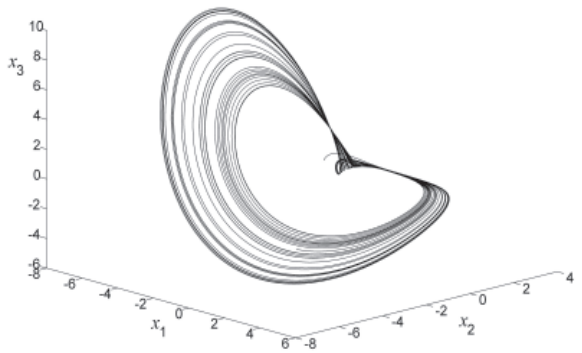

Fig. 9. Trayectorias caóticas x_i (i=1, 2, 3) de (5) en el espacio de fases.

Ahora, considerando la variable de salida $y = x_1$ como la señal de acoplamiento, el sistema (5) se representa en la forma (2):

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & y & -\tilde{\alpha} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ -y \end{bmatrix} \tag{6}$$
$$y = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x$$

Entonces, el sistema esclavo se diseña como el observador dado por (3):

$$\dot{\hat{x}} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & y & -\alpha \end{bmatrix} \hat{x} + \begin{bmatrix} 0 \\ 0 \\ -y \end{bmatrix} + S^{-1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} (y - \hat{y}) \tag{7}$$
$$\hat{y} = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \hat{x}$$

Donde $\hat{x} = \begin{bmatrix} \hat{x}_1 & \hat{x}_2 & \hat{x}_3 \end{bmatrix}^T$ y donde la matriz S es la solución de (4). Luego, el sistema esclavo (7) se sincroniza con el sistema maestro (5) si $\tilde{\alpha} = \alpha$.

Para tal caso, en la figura 10 se muestran los errores de sincronización ($e_i = x_i - \hat{x}_i$, i=1, 2, 3) convergiendo a cero, lo cual significa que los estados de (7) se sincronizan a los estados de (5), después de un tiempo transitorio. En este caso, se consideró que $\tilde{\alpha} = \alpha = 2.02$, y $\rho = 30$. Además, las condiciones iniciales del sistema y del observadores se seleccionaron de la siguiente manera: $x(0) = [0.001 \quad 0.001 \quad 0.001]^T$ y $\hat{x}(0) = [0.03 \quad 0.03 \quad 0.03]^T$.

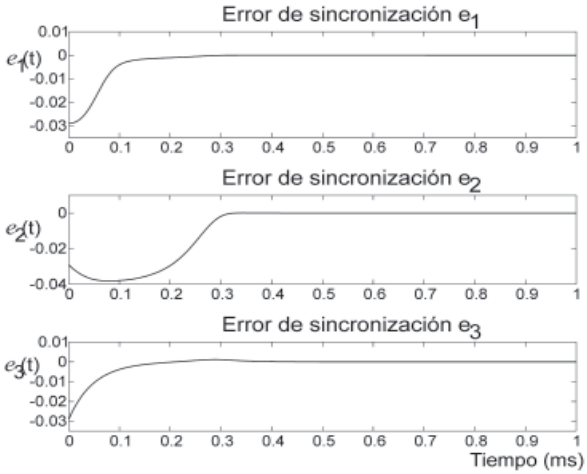

Fig. 10. Evolución del error de sincronización $e_i = x_i - \hat{x}_i$ (i=1, 2, 3), entre (5) y (7).

Ahora, en la técnica de modulación por parámetro, la señal portadora caótica *y* es modulada por el parámetro $\tilde{\alpha}$ del sistema maestro (transmisor), debido a que la evolución de la trayectoria de *y* depende directamente de $\tilde{\alpha}$. Entonces, el parámetro $\tilde{\alpha}$ es conmutado por una señal de información binaria m(t), i.e. $\tilde{\alpha} = \alpha + p \cdot m(t)$, donde α es un valor nominal y *p* el cambio en el valor del parámetro.

Puesto que el receptor está construido sólo con el valor nominal. Entonces, la información m(t) es descifrada en el receptor mediante el error de sincronización ($e_1 = y - \hat{y}$), verificando si $\hat{y}$ converge o no a la señal *y*, lo cual indica si la señal recibida corresponde al valor nominal del parámetro o no (lo cual puede interpretarse como un cero o uno).

RESULTADOS

A continuación se presentan los resultados obtenidos al implementar el esquema de sincronización mostrado, para cifrar, transmitir y descifrar un mensaje.

En este caso, supóngase que la información a ser transmitida es la palabra "Texto", cuyo valor binario en código ASCII a 7 bits por carácter es "1010100 1100101 1111000 1110100 1101111".

Vale la pena mencionar que en lugar de enviar una palabra, esta podría ser remplazada por un número de PIN de una tarjeta comercial o bancaria.

De esta forma, la señal modulante generada se muestra en la figura 11 (a), escribiendo primero el bit menos significativo (LSB) de cada carácter, cuya transmisión se inicia en un tiempo t_s.

El transmisor (5) genera la señal caótica portadora y(t), mostrada en la figura 11 (b), la cual es modulada mediante la conmutación de $\tilde{\alpha}$ entre los valores 2.02 y 2.03, siendo α =2.02 el valor nominal.

Posteriormente, el receptor (7) se sincroniza con (5) cada que $\tilde{\alpha}$ =2.02. El tiempo t_s permite asegurar la sincronización inicial antes de la transmisión. La información se recupera mediante un proceso de detección del error de sincronización, como se muestra en la figura 11 (c), detectando que se pierde sincronía cuando $\tilde{\alpha} \neq 2.02$. De tal modo que la señal digital $m_r(t)$ es recuperada en el receptor al asignar bits con valores (0 o 1) que dependen del error de sincronización. La figura 11 (d) muestra claramente que la información digital original *m(t)* es recuperada en el receptor como $m_r(t)$. Por consiguiente, mediante un proceso de decodificación de ASCII se obtiene el mensaje: "Texto".

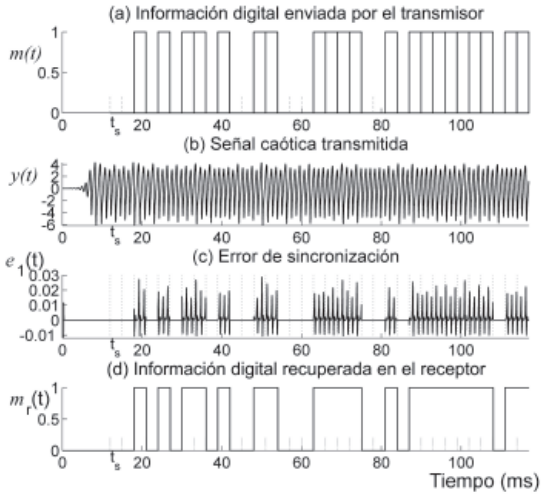

Fig. 11. (a) Señal de información digital m(t), (b) Señal caótica transmitida *y*(t), (c) Detección del error de sincronización e_1(t), (d) Señal de información digital reconstruida m_r(t).

CONCLUSIONES

En este trabajo se presentó una estrategia de sincronización de caos para sistemas clase P. Resolviendo el problema de sincronización mediante observadores de estado, se diseñó un sistema esclavo como un observador del sistema maestro. Además, se presentan resultados, mediante el cifrado de un mensaje de texto, que muestran la eficiencia del esquema de sincronización y sus potenciales aplicaciones en un sistema de comunicaciones seguras.

REFERENCIAS

1. E.N. Lorenz, Deterministic non-periodic flow, Journal of the atmospheric sciences, Vol. 20, pp. 130–141, 1963.
2. B.R. Andrievskii and A.L Fradkov, Control of chaos: Methods and applications, Automation and remote control, Vol. 64, No. 5, pp. 673-713, 2003.
3. L.M. Pecora and T.L. Caroll, Synchronization in chaotic systems, Phys. Rev. Lett. Vol. 64 No. 8 pp. 821-824, Washington, D.C., USA, 1990.

4. H.D.I. Abarbanel, N.F. Rulkov, and M.M. Sushchik, "Generalized synchronization of chaos: The auxiliary system approach", Physical Review E, Vol. 53, pp. 4528-4535, 1996.
5. C. Schafer, et al., "Heartbeat synchronized with ventilation", Nature, London, Vol.392, p.239, 1998.
6. M. Hasler, "Synchronization of chaotic systems and transmission of information", Int. J. Bifurcat. Chaos, Vol. 8, No. 4, pp. 647-660, 1998.
7. T.L. Caroll, "Chaotic communications that are difficult to detect", Phys. Rev. E, Vol. 67, Washington, D.C, 2003.
8. Y. Jin and Z. Qu, "Synchronization of Lorenz systems by adaptive observation", Proceedings of the American control conference, pp. 3305-3310, Denver, Colorado, 2003.
9. H. Nijmeijer and I. Mareels, "An observer looks at synchronization", IEEE transactions on circuits and systems I: Fundamental theory and applications, Vol. 44, No. 10, 1997.
10. J.M. Malasoma, "A new class of minimal chaotic flows", Phys. Lett. A, Vol. 305, pp. 52-58, 2002.
11. H. Hammouri and J. De León-Morales, "Observers synthesis for state affine systems", in Procedings of the 29th IEEE Conference of decision and control, pp. 784-785, Honolulu, Hawai, 1990.