

## TRANSMISIÓN ÓPTICA DE INFORMACIÓN ENCRIPTADA EN CAOS

Rosa Martha López Gutiérrez<sup>1</sup>, Liliana Cardoza Avendaño<sup>1</sup>, Humberto Cervantes de Ávila<sup>1</sup>, Adrián Arellano-Delgado<sup>2</sup>, José Antonio Michel Macarty<sup>1</sup>, Roberto Carmona Rodríguez<sup>1</sup>, César Cruz Hernández<sup>2</sup>

<sup>1</sup> Universidad Autónoma de Baja California, Facultad de Ingeniería, Arquitectura y Diseño  
Carretera Transpeninsular Ensenada-Tijuana numero 3917, Col Playitas  
Ensenada, B.C., C.P. 22860, +52 (646) 1744333

<sup>2</sup> Centro de Investigación Científica y de Educación Superior de Ensenada  
Carretera Ensenada-Tijuana 3918, Zona Playitas  
Ensenada, B.C., C.P. 22860, +52 (646)1750500

Correo-e: roslopez@uabc.edu.mx, lcardoza@uabc.edu.mx,  
hcervantes@uabc.edu.mx, aarellan@cicese.mx, michelmacartyj@uabc.edu.mx,  
robertocarmonar@gmail.com, ccruz@cicese.mx

### RESUMEN.

Se presenta una comunicación encriptada y transmitida por medio de fibra óptica de plástico (FOP). Tanto en el circuito transmisor como en el receptor se utilizó un oscilador caótico para poder realizar una comunicación encriptada. A través de la fibra óptica se transmite una señal de audio encriptada por medio de un oscilador caótico de Lorenz. El encriptado de la información se basa en el método de enmascaramiento caótico aditivo, por lo que del lado del receptor se tiene un oscilador caótico idéntico al utilizado en el transmisor.

**Palabras claves:** Comunicación, encriptamiento, sistema caótico.

### ABSTRACT

Encrypted and transmitted communication is reached via plastic optical fiber (POF). Both the transmitter and receiver circuit for an encrypted communication is used a chaotic oscillator. It is transmitted through fiber optic audio signal encrypted with Lorenz chaotic oscillator. To encrypt information chaotic masking the additive method is used, so the receiver side have identical chaotic oscillator which has the transmitter.

**Keywords:** Communication, encrypted information, chaotic system.

### 1. INTRODUCCION

Desde décadas anteriores, la sincronización caótica ha tenido un creciente interés, véase, por ejemplo [1-8] y referencias en él. Esta propiedad tienen aplicaciones interesantes en diferentes campos, sobre todo en el diseño de

sistemas de comunicación privada/segura, véase, por ejemplo [4, 5, 8-17]; en el que la información confidencial se cifra en la señal caótica para la transmisión por medio de la modulación directa, enmascaramiento, o alguna otra técnica. En el receptor, una vez que se ha logrado la sincronización, es posible extraer la información oculta de la señal transmitida, la combinación de circuitos caóticos y el láser (ver por ejemplo [18 a 26]) son candidatos ideales para la experimentación de comunicaciones seguras. Las características del ancho de banda y ruido de las señales caóticas son vistas como medios de comunicación, posiblemente, de alta seguridad para la comunicación [4], [5], [11], [12], [13], [14], [15], [16].

El principal objetivo de este trabajo es obtener la sincronización entre un transmisor y un receptor utilizando circuitos de Lorenz acoplados en topología maestro-esclavo utilizando como canal de comunicación una fibra óptica de plástico (FOP), como canal de comunicación. El objetivo se logra con realización experimental mediante el uso de dispositivos opto-electrónico.

Los datos encriptados utilizando dinámicas caóticas fueron reportados en los años noventa como una aproximación para codificar información. Existen varias técnicas que han sido estudiadas, tales como el enmascaramiento caótico [10], conmutación paramétrica [11] y modulación de parámetros caóticos [12].

El caos habitualmente se refiere a lo impredecible, y es uno de los principales conceptos del Cosmos. Caos deriva de la raíz *ghen* del lenguaje protoindoeuropeo ("hueco", "muy abierto").

En la actualidad, las oscilaciones caóticas que presentan un comportamiento aparentemente estocástico, caracterizado por un gran ancho de banda en el espectro de frecuencias, son utilizadas para encriptar información, con la finalidad de transmitir mensajes secretos en forma segura.

## 2. SISTEMA DE COMUNICACIÓN ÓPTICO CAÓTICO

El trabajo se divide en dos partes que son: el medio de transmisión y el generador caótico para el encriptamiento y desencriptamiento de la señal de audio transmitida.

### 2.1. SISTEMA CAÓTICO

Para encriptar y desencriptar la información se utiliza un generador caótico. El generador caótico es un circuito de Lorenz cuyas ecuaciones normalizadas son las siguientes:

$$\begin{aligned}\dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_2x_1 - bx_3\end{aligned}\quad (1)$$

Dónde:

$\sigma$ : Número de Prandtl

(Viscosidad/conductividad térmica).

$r$ : Numero de Rayleigh Jonh Strutt (Diferencia de temperatura entre base y tope).

$b$ : La razón entre la longitud y altura del sistema.

$x$ : Razón de rotación del anillo.

$y$ : Gradiente de temperatura.

$z$ : Desviación de la temperatura respecto a su valor de equilibrio.

### 2.2. ESQUEMA DE LA COMUNICACION ENCRYPTADA

El diagrama esquemático de la comunicación encriptada se muestra en la figura 1, se utiliza el encriptamiento aditivo, el cual consiste en sumar la señal caótica con el mensaje a encriptar.

Para que la señal pueda ser recuperada es necesario sincronizar el sistema caótico maestro con el esclavo, lo cual se muestra en las siguientes ecuaciones:

Transmisor

$$\begin{aligned}\dot{x}_1 &= \sigma(x_2 - x_1) \\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3 \\ \dot{x}_3 &= x_2x_1 - bx_3\end{aligned}\quad (2)$$

Receptor

$$\begin{aligned}\dot{x}_1^R &= \sigma(x_2^R - x_1^R) + u \\ \dot{x}_2^R &= rx_1^R - x_2^R - x_1^Rx_3^R \\ \dot{x}_3^R &= x_2^Rx_1^R - bx_3^R \\ u &= C(x_1 - x_1^R)\end{aligned}\quad (3)$$

donde:  $u$  es la señal de acoplamiento y  $C$  la constante de acoplamiento.

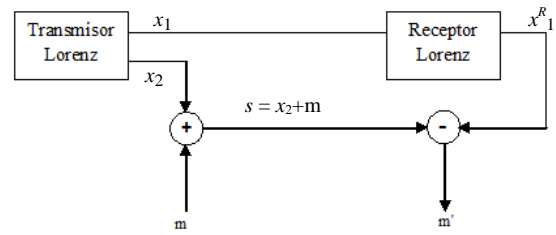


Figura 1. Encriptamiento aditivo.

El resultado de esta suma se enviará al destinatario utilizando el transmisor óptico. Para recuperar la información del lado del receptor es necesario que se realice el proceso inverso al transmisor, la señal caótica generada en el receptor una vez sincronizada se realiza la diferencia con la señal codificada en el receptor como se muestra en la figura 2.

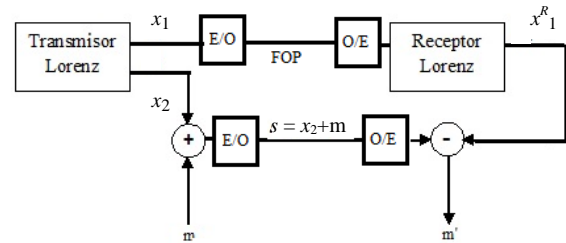


Figura 2. Diagrama esquemático con la parte E/O y O/E

## 3. COMUNICACION ÓPTICA ENCRYPTADA: EXPERIMENTAL.

La etapa de generador de caos está constituida por el circuito de Lorenz. Se construyeron dos generadores caóticos, una para el transmisor (Figura 3) y otra para el receptor (Figura 4). El receptor tiene una etapa de sincronización como se muestra en la ecuación (3), para logra esta sincronización se construyó el circuito mostrado en la figura 5.

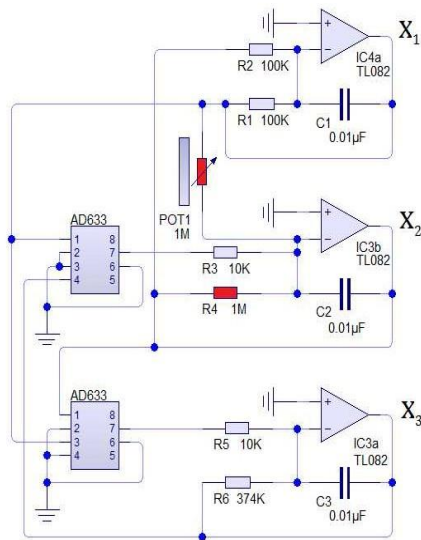


Figura 3. Circuito transmisor sin sincronizar

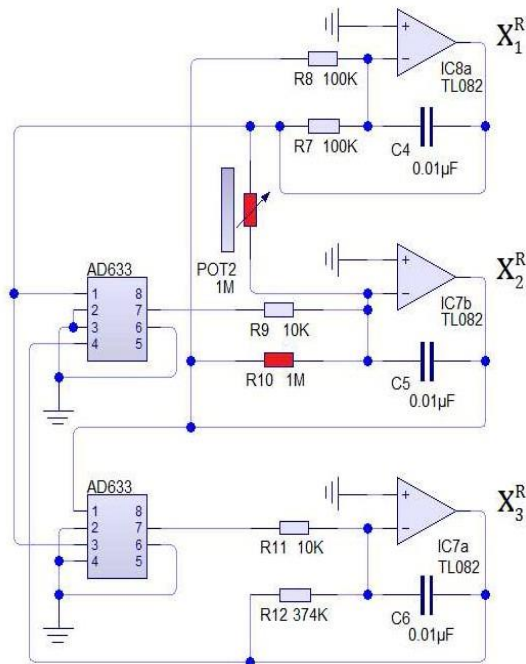


Figura 4. Circuito receptor sin sincronizar.

### 3.1. SISTEMA ELECTRO-ÓPTICO Y ÓPTICO ELÉCTRICO

Para el canal de transmisión se utilizó una fibra óptica de plástico (FOP) Super Eska con atenuación de 3 dB/m, el LED IF-E96 y el fotodiodo IF-E91, la longitud de la FOP es de 2 metros. La longitud de onda del LED utilizado es de 660nm con un ancho de banda de 20nm. Cabe mencionar que la FOP super Eska está diseñada para la transmisión de datos, por lo que muchas de las interfaces de audio digital manufacturadas hoy en día, son realizadas con esta fibra.

La figura 6 muestra el circuito convertidor electro-óptico, la señal caótica  $x_{2T}$  del transmisor es convertida a señal óptica, y después se introduce al canal de comunicación mediante la FOP.

En la figura 7 se muestra el circuito conversor óptica a eléctrico, la señal es utilizada para sincronizar el receptor.

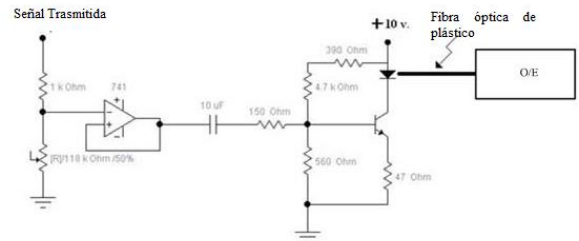


Figura 6. Circuito Eléctro/Óptico (E/O).

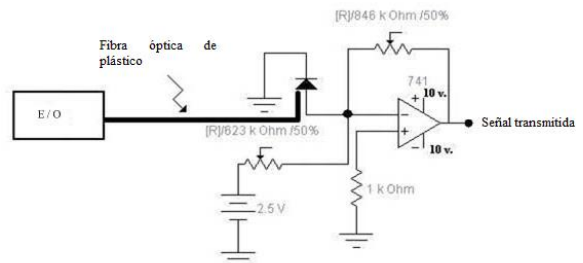


Figura 7. Circuito Óptico/Eléctrico (O/E).

## 4. RESULTADOS Y DISCUSIÓN.

La secuencia caótica generada por los circuitos de Lorenz, se muestran en la figura 8, en esta se puede observar el atractor.

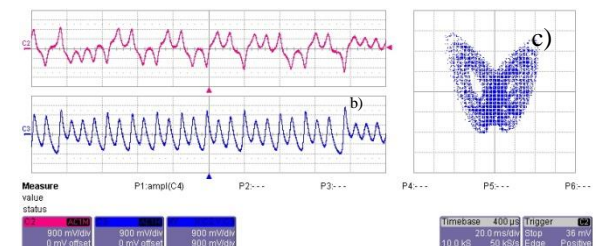


Figura 8. Estados de Lorenz. a) Gráfica  $x_1$ ; b) Gráfica  $x_3$ , c) Atractor de Lorenz

Los estados  $x_1$  y  $x_1^R$  y la sincronización entre estos estados se muestra en la figura 9. En la figura 10 se muestra las señales sin y con mensaje, donde se puede ver que el mensaje no se logra distinguir.

En la figura 11 se muestran la señal original y la señal recupera, cabe aclarar que la escala de estas graficas están en 150mV/div.

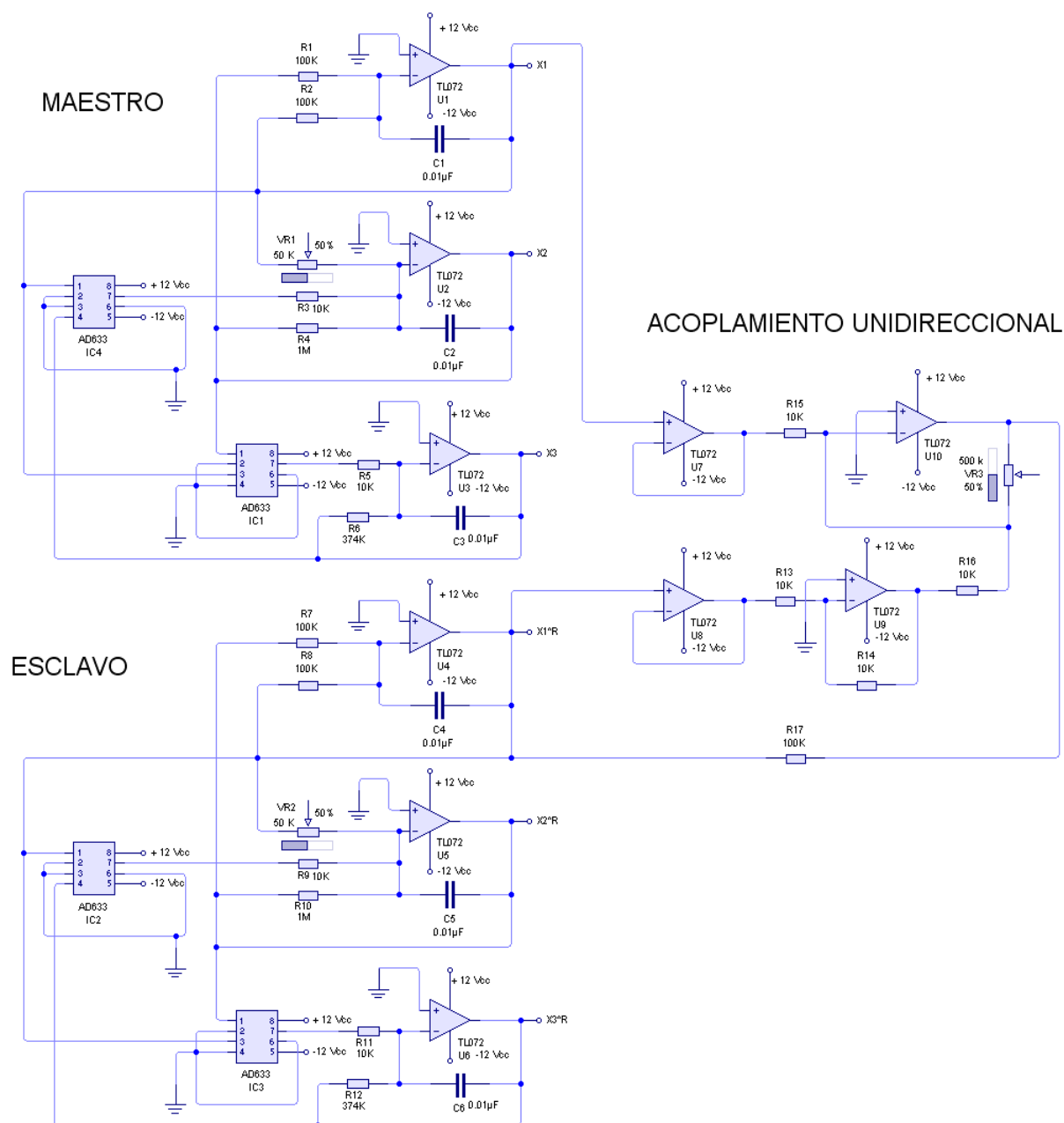


Figura5. Sistema de comunicación sincronizado.

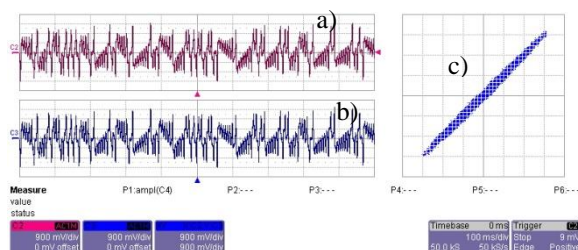
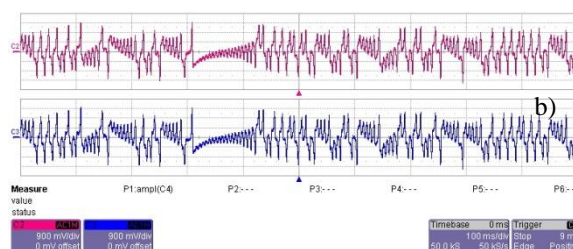


Figura 9. Sincronización Transmisor-Receptor.  
 a)  $x_1$  del transmisor, b)  $x_1^R$  del receptor, c) Sincronización del transmisor vs receptor.



Figuro 10. a) Señal  $x_2$  del maestro. b) Señal  $x_2$  mas el mensaje  $m$ , es decir  $s$ .

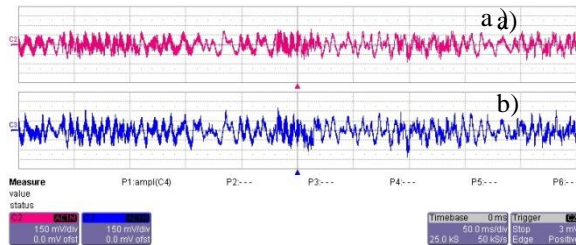


Figura 11. a) Señal original y b) Señal recuperada

El sistema de comunicaciones presentado en este trabajo logró transmitir una señal de audio encriptada utilizando fibra óptica de plástico. Del lado del receptor se recuperó la señal de audio original, para ello se utilizaron dos canales, uno para sincronizar y el otro para transmitir la señal encriptada; sin embargo, como se utiliza un mismo canal, la señal muestra un ruido al recuperarse.

#### 4. Conclusiones

Se presentó una comunicación segura a través del circuito caótico Lorenz utilizando la configuración maestro y esclavo. El canal de comunicación utilizado fue una FOP.

Para lograr la transmisión de audio por medio de fibra óptica se implementaron etapas electro-ópticas y óptico-eléctricas en el receptor. Los resultados experimentales obtenidos muestran que el receptor logra sincronizarse con el transmisor.

#### AGRADECIMIENTOS

Este trabajo fue apoyado por el CONACYT, México en bajo el apoyo de investigación No. 166654

#### 5. Bibliografía.

[1] L.M. Pecora, T.L. Carroll, Synchronization in chaotic systems, *Phys. Rev. Lett.* 64 (1990) 821–824.  
 [2] C. Cruz-Hernandez, H. Nijmeijer, Synchronization through filtering, *Int. J. Bifurcat. Chaos* 10 (4) (2000) 763–775.  
 [3] H. Sira-Ramírez, C. Cruz-Hernandez, Synchronization of chaotic systems: a generalized Hamiltonian systems approach, *Int. Bifurcat. Chaos* 11 (5) (2001) 1381–1395.  
 [4] D. Lopez-Mancilla, C. Cruz-Hernandez, Output synchronization of chaotic systems: model-matching approach with application to

secure communication, *Nonlinear Dyn. Syst. Theory* 5 (2) (2005) 141–156.

[5] U. Feldmann, M. Hasler, W. Schwarz, Communication by chaotic signals: the inverse system approach, *Int. J. Circ. Theory Appl.* 24 (5) (1996) 551–579.  
 [6] H. Nijmeijer, I.M.Y. Mareels, An observer looks at synchronization, *IEEE Trans. Circ. Syst.* 44 (10) (1997) 882–890.  
 [7] A. Boukabou, On nonlinear control and synchronization design for autonomous chaotic systems, *Nonlinear Dyn. Syst. Theory* 8 (2) (2008) 151–167.  
 [8] C. Cruz-Hernandez, A.A. Martynyuk, *Advances in Chaotic Dynamics with Applications*, vol. 4, Cambridge Scientific Publishers, London, 2010.  
 [9] K.M. Cuomo, A.V. Oppenheim, Circuit implementation of synchronized chaos with applications to communications, *Phys. Rev. Lett.* 71 (1993) 65–68.  
 [10] C. Cruz-Hernandez, D. Lopez-Mancilla, V. García, H. Serrano, R. Nunez, Experimental realization of binary signal transmission using chaos, *J. Circ. Syst. Comput.* 14 (3) (2005) 453–468.  
 [11] C. Cruz-Hernandez, Synchronization of time-delay Chua's oscillator with application to secure communication, *Nonlinear Dyn. Syst. Theory* 4 (1) (2004) 1–13.  
 [12] C. Posadas-Castillo, R.M. Lopez-Gutierrez, C. Cruz-Hernandez, Synchronization of chaotic solid-state Nd:YAG lasers: application to secure communication, *Commun. Nonlinear Sci. Numer. Simul.* 13 (8) (2008) 1655–1667.  
 [13] L. Gamez-Guzman, C. Cruz-Hernandez, R.M. Lopez-Gutierrez, E.E. Garcia-Guerrero, Synchronization of Chua's circuits with multi-scroll attractors: application to communication, *Commun. Nonlinear Sci. Numer. Simul.* 14 (6) (2009) 2765–2775.  
 [14] C. Cruz-Hernandez, N. Romero-Haros, Communicating via synchronized timedelay Chua's circuits, *Commun. Nonlinear Sci. Numer. Simul.* 13 (3) (2008) 645–659.  
 [15] K. Kusumot, J. Ohtsubo, 1.5-GHz message transmission based on synchronization of chaos in semiconductor lasers, *Opt. Lett.* 27 (2002) 989–991.  
 [16] M.W. Lee, J. Paul, S. Sivaprakasam, K.A. Shore, Comparison of closed-loop and open-loop feedback schemes of message decoding using chaotic laser diodes, *Opt. Lett.* 28 (2003) 2168–2170.  
 [17] J. Paul, S. Sivaprakasam, K.A. Shore, Dual-channel chaotic optical communications using external-cavity semiconductor lasers, *J. Opt. Soc. Am. B* 21 (2004) 514–521.



- [18] Madan RN, (Guest Ed.). Chua's Circuit: A Paradigm for Chaos, World Scientific, 1993.
- [19] M.P. Kennedy, Robust Op-Amp realization of Chua's circuit, *Frequenz* 46 (34) (1992) 66–80.
- [20] B. Muthuswamy, L.O. Chua, Simplest chaotic circuit, *Int. J. Bifurcat. Chaos* 20 (5) (2010) 1567–1580.
- [21] J. Lu, R. Chen, Generating multiscroll chaotic attractors: theories, methods and applications, *Int. J. Bifurcat. Chaos* 16 (4) (2006) 775–858.
- [22] L. Cardoza-Avendano, V. Spirin, R.M. Lopez-Gutiérrez, C.A. Lopez-Mercado, C. Cruz-Hernandez, Experimental characterization of DFB and FP chaotic lasers with strong incoherent optical feedback, *Opt. Laser Technol.* 43 (5) (2011) 949–955.
- [23] V. Spirin, C.A. Lopez-Mercado, S.V. Miridonov, L. Cardoza-Avendano, R.M. Lopez-Gutierrez, C. Cruz-Hernandez, Elimination of low-frequency fluctuations of backscattered Rayleigh radiation from optical fiber with chaotic lasers, *Opt. Fiber Technol.* 17 (2011) 258–261.
- [24] S. Tang, J.M. Liu, Chaotic pulsing and quasi-periodic route to chaos in a semiconductor laser with delayed opto-electronic feedback, *IEEE J. Quantum Electron.* 37 (2001) 329–336.
- [25] Yuncai Anbang Wang, He Wang Hucheng, Enhancing the bandwidth of the optical chaotic signal generated by a semiconductor laser with optical feedback, *IEEE Photon. Technol. Lett.* 20 (2008) 1633–1635.
- [26] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, Garcia-Ojalvo, C.R. Mirasso, L. Pesquera, K.A. Shore, Chaos-based communications at high bit rates using commercial fibre-optic links, *Nature* 438 (7066) (2005) 343–346.