Congreso Internacional en Ingeniería Electrónica. Mem. Electro 2015, Vol. 37, pp 304-309, Chihuahua, Chih. México
http://depi.itchihuahua.edu.mx/display/memorias_electro/MemoriaElectro2015
ISSN 1405-2172

SISTEMA ELECTRÓNICO DIGITAL DE 8 BITS PARA GENERACIÓN DE CAOS

Flores Vergara Abraham[1], Inzunza González Everardo[2], García Guerrero E. Efren[3] y López Bonilla Oscar R[4].
Universidad Autónoma de Baja California, Facultad de Ingeniería, Arquitectura y Diseño
Carretera Transpeninsular Ensenada-Tijuana 3917, Colonia Playitas. C.P. 22860. Ensenada, B.C. México.
Tel.+52(646)175-07-44, Fax. +52(646)174-43-33
[1] venumc@uabc.edu.mx, [2]einzunza@uabc.edu.mx , [3]eegarcia@uabc.edu.mx y [4]olopez@uabc.edu.mx

RESUMEN

La criptografía caótica implementada en sistemas electrónicos se presenta como una alternativa para solucionar las necesidades de comunicación segura hoy en día. Sin embargo, el uso de sistemas electrónicos analógicos adiciona complejidad y vulnerabilidad en comparación con el uso de sistemas electrónicos digitales. En este trabajo se presenta el diseño e implementación de un sistema electrónico digital empotrado para generación de caos. El propósito del sistema es integrarse a los métodos criptográficos de información confidencial en sistemas de telecomunicación. El diseño digital se basa en un microcontrolador PIC16F877A de 8 bits fabricado por Microchip Technology Inc. Las series pseudoaleatorias generadas por el sistema electrónico digital, corresponden a las ecuaciones en diferencias de los mapeos caóticos de Tinkerbell, Ikeda, Logístico 2D y Chen. Para cada mapeo, se visualiza experimentalmente su atractor extraño en un osciloscopio digital a partir del uso de convertidores digital a analógico (DAC-MCP4929) con comunicación serie tipo SPI (Serial Peripherical Interface).

Palabras Clave: Generador digital de caos, series pseudoaleatorias, microcontrolador PIC, mapeos caóticos, atractores extraños.

ABSTRACT

The chaotic cryptography implemented in electronic systems is presented as an alternative to solve the needs of secure communication today. However, the use of analog electronic systems, adds complexity and vulnerability noise, in comparison with the use of digital electronics. This work presents the design and implementation of a digital generator system for chaotic attractors, that can be used in cryptographic methods for confidential information in telecommunication systems. Specifically, the proposed circuit is based on a 8-bits microcontroller PIC16F877A by Microchip Technology and the attractors generated corresponding to chaotic maps widely documented in the literature, including: the Tinkerbell map, Ikeda map, Logistic 2D map and Chen map. The strange attractor is experimentally displayed on a digital oscilloscope from the use of digital to analog converters (DAC- MCP4929) with SPI (Serial Interface Peripherical) communication.

Keywords: Digital chaos-generator, pseudoramdom series, microcontroller PIC16F877A, chaotic maps, strange attractor.

1 INTRODUCCIÓN

El descubrimiento del caos como se conoce hoy día se debe a Edward N. Lorenz (1917-2008) matemático y meteorólogo estadounidense y a la invención de las computadoras de alta velocidad en la década de los 60's. Después de estudiar detenidamente su modelo matemático muy simplificado con el cual pretendía modelar la atmósfera (1963), llegó a la conclusión de que las soluciones a su modelo eran muy divergentes para valores muy próximos en cualquiera de sus condiciones iniciales. Observó que la evolución de su sistema dinámico al representarlo en un diagrama de fases, quedaba formado por una serie de trayectorias divergentes que al parecer eran muy poco predecibles, pero más aún, la evolución propia del sistema se acumulaba o se atraían hacia un mismo espacio, hacia un mismo objeto, es decir, se formaba un atractor. Esto es el caos, la dependencia sensible a las condiciones iniciales. En la figura 1 se muestra el comportamiento dinámico (atractor) del sistema de ecuaciones simplificadas de Lorenz [1].

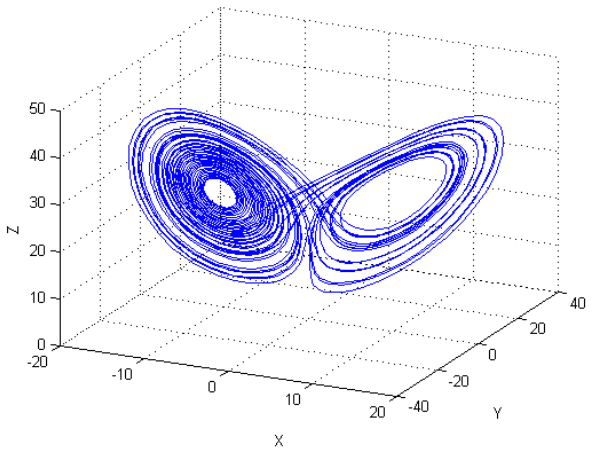

Figura 1. Atractor de Lorenz.

En un diagrama de fases como el atractor de Lorenz el tiempo está implícito, y cada eje representa una dimensión asociada a cada estado del sistema dinámico (X, Y, Z) definido a través de su sistema de ecuaciones diferenciales respectivo. De acuerdo a

la forma en que sus trayectorias evolucionan, los atractores pueden ser clasificados como atractor punto fijo, periódico o ciclo límite, cuasi periódico y caótico. Un atractor es caótico en el sentido de que no puede ser predecible la evolución de las trayectorias de dos puntos iniciales, aún cuando exista entre ellos una diferencia muy pequeña en alguna de sus condiciones iniciales. Los fenómenos físicos se estudian a partir de modelos matemáticos, los cuales se describen mediante sistemas de ecuaciones diferenciales para fenómenos tratados en tiempo contínuo, o mediante sistemas de ecuaciones en diferencias, conocidas como mapeos, para análisis en tiempo discreto. Un método para obtener el mapa de un sistema contínuo es mediante la aplicación del modelo de sección de Poincaré o Mapeo de Poincaré [2]. Una de las ventajas de implementar el mapeo de un sistema contínuo, es que se trabaja con sistemas de ecuaciones en diferencias con igual o generalmente menos ecuaciones que el sistema contínuo, sin modificarse las propiedades del sistema original. A este proceso se le conoce como discretización de sistemas contínuos. El sistema de ecuaciones (1), representa un sistema caótico en tiempo discreto conocido como Mapeo de Hénon [3]. Este mapeo fue implementado por Michel Hénon aplicando el método de sección de Poincaré [2], al sistema dinámico en tiempo contínuo de Lorenz [1]. Se observa en el sistema de ecuaciones (1), que la dinámica depende de los parámetros *a* y *b*. Cuando *a=1.4* y *b=0.3*, el sistema presenta un comportamiento caótico. En la Figura 2, se muestra el atractor extraño de Hénon. Para otros valores posibles de *a* y *b*, el mapeo de Hénon puede ser caótico o converger en una órbita periódica. La figura 2 da el comportamiento en tiempo discreto del comportamiento en tiempo contínuo de la figura 1.

$$x_{n+1} = y_n + 1 - ax_n^2,$$
$$y_{n+1} = bx_n. \qquad (1)$$

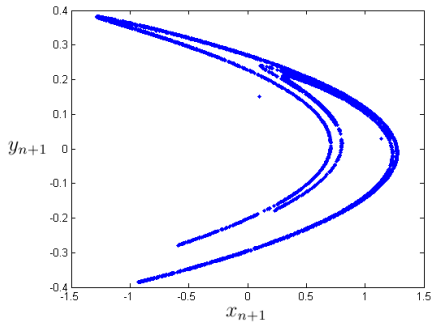

Figura 2. Atractor caótico de Hénon.

Actualmente podemos encontrar en la literatura una amplia gama de mapeos caóticos. A manera de ejemplo, en este trabajo se implementan experimentalmente los mapeos: Tinkerbell, Logístico 2D, Ikeda y Chen.

1.1 Mapeo de Tinkerbell

Recientemente se ha reportado en la literatura el mapeo Tinkerbell [4], descrito por el sistema de ecuaciones (2) y cuya dinámica en régimen caótico se puede observar en la figura 3.

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n,$$
$$y_{n+1} = 2x_n y_n + cx_n + dy_n. \qquad (2)$$

Donde: $a = 0.9, b = -0.6013, c = 2$ y $d = 0.5$.
La figura 3 muestra el atractor del mapeo Tinkerbell.

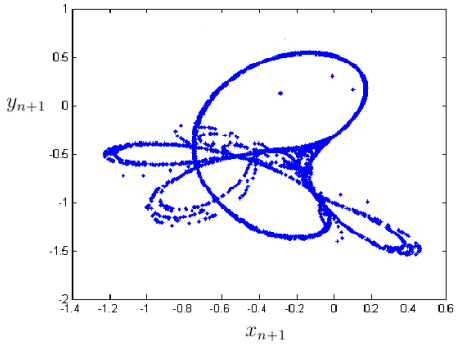

Figura 3. Atractor caótico de Tinkerbell.

1.2 Mapeo Logístico 2D

El mapeo Logístico 2D, es un modelo de crecimiento poblacional publicado por Pierre Verhulst [5] y se popularizó en 1976 por el biólogo Robert May [6]. Su dinámica se describe por el sistema de ecuaciones en diferencias (3).

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \gamma_1 y_n^2,$$
$$y_{n+1} = \mu_2 y_n(1 - y_n) + \gamma_1(x_n^2 + x_n y_n). \qquad (3)$$

Cuando: $2.75 < \mu_1 \leq 3.4$, $2.75 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ y $0.13 < \gamma_2 \leq 0.15$, el sistema tiene un comportamiento caótico como el que se muestra en la figura 4.

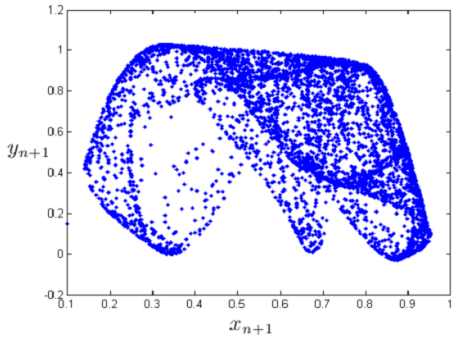

Figura 4. Atractor caótico Logístico 2D.

1.3 Mapeo de Ikeda

El mapeo de Ikeda [7] está descrito por el sistema de ecuaciones en diferencias (4). Este mapeo fue conceptualizado y propuesto por Ikeda, como un modelo de luz que pasa a través de un resonador óptico no-lineal.

$$x_{n+1} = 1 + u(x_n \cos(t_n) - y_n \sin(t_n)),$$
$$y_{n+1} = u(x_n \sin(t_n) + y_n \cos(t_n)). \quad (4)$$

Donde: $t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}$ y $u = 0.9$. El atractor caótico se muestra en la figura 5.

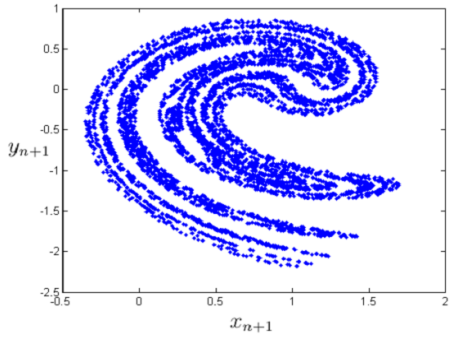

Figura 5. Atractor caótico de Ikeda.

1.4 Mapeo hipercaótico de Chen

El mapeo hipercaótico de Chen [8] está descrito por el sistema de ecuaciones en diferencias (5). Cuando $a = 1.95$ y $b = 1$ el comportamiento dinámico del sistema, exhibe una dinámica hipercaótica.

$$x_{n+1} = 1 - a(x_n^2 + y_n^2),$$
$$y_{n+1} = 2 - abx_n y_n. \quad (5)$$

El atractor generado se muestra en la figura 6.

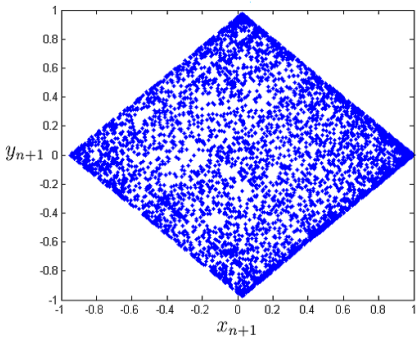

Figura 6. Atractor caótico de Chen.

2 TRABAJOS RELACIONADOS

En la literatura actual, se puede encontrar una amplia gama de trabajos que describen diferentes metodologías para implementar generadores de caos que utilizan técnicas de diseño basados en circuitos analógicos [9-13]. En el diseño de circuitos analógicos y particularmente para la generación de caos, es necesario emplear una gran variedad de componentes electrónicos tales como: bobinas, amplificadores operacionales, diodos, resistores, capacitores, multiplicadores, entre muchos otros. En la mayoría de los casos, se requieren valores nominales en los componentes electrónicos muy precisos o llevar acabo ajustes muy finos, lo que hace complicada la implementación experimental. Por otra parte, algunos de los componentes electrónicos no son comerciales por lo que no son de fácil adquisición y encarecen los diseños respectivos. Adicionalmente, el punto más vulnerable de los circuitos analógicos es su gran sensibilidad al ruido del entorno, manifestándose sobre los circuitos a partir de interferencias electromagnéticas. Desde la perspectiva de la electrónica digital [14], al utilizar componentes electrónicos digitales y en específico el microcontrolador, se reduce entre otras cosas, la cantidad de componentes en el diseño de los circuitos generadores de caos, debido a que la implementación propia de los sistemas caóticos se lleva a cabo mediante programación en el microcontrolador y no por componentes electrónicos analógicos. Esto minimiza tanto la complejidad en la circuitería, como en el tiempo de implementación. Por otra parte, no son necesarios ajustes finos sobre algunos componentes y se reduce considerablemente la sensibilidad al ruido del entorno. En [15-17] se documenta la utilización de tarjetas de desarrollo basadas en microcontrolador para generar caos como por ejemplo el 8051 de Intel o con el PIC12F629 de Microchip Inc., programados en lenguaje ensamblador. Sin embargo hoy en día existen compiladores de lenguaje C para microcontroladores, que facilitan la programación y por ende, permiten abordar y experimentar con modelos matemáticos más complejos y con mayor precisión numérica. En este trabajo se propone una metodología empleando el microcontrolador PIC16F877A de Microchip Inc., como base para el diseño de un sistema embebido generador de caos y empleando el lenguaje C de programación. Para la validación de los resultados, se incluye una etapa de conversión Digital-Analógica visualizando en un osciloscopio digital el atractor caótico generado.

3 METODOLOGÍA

En la figura 7 se presenta un diagrama de flujo del método propuesto para generar caos a partir de un sistema electrónico digital. La parte central la constituye la programación del sistema de ecuaciones en diferencias del mapeo caótico de interés, conjuntándose con una etapa de conversión Digital-Analógico. El microcontrolador PIC16F877A de 8 bits con arquitectura RISC (Reduced Instruction Set Computer), al programarse bajo las directrices del mapeo caótico en cuestión, genera las series pseudoaleatorias de cada uno de sus estados $x_{n+1}, y_{n+1}, \ldots, z_{n+1}$, que describen la dinámica del sistema. Las señales $\{x_i\}, \{y_i\}$ y $\{z_i\}$ obtenidas en este nivel, son de naturaleza digital, por lo que, a fin de observar y validar el comportamiento del mapeo caótico, dichas series pasan por una etapa de conversión Digital-Analógico mediante la implementación de convertidores del tipo DAC-MCP4929 de 12 bits con comunicación serie tipo SPI (Serial Peripherical Interface).

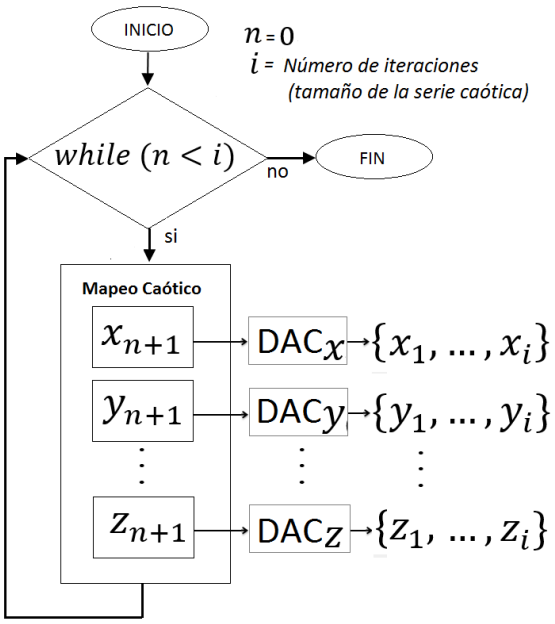

Figura 7. Diagrama de flujo del generador de caos.

Cada sistema caótico genera tantas series pseudoaleatorias como estados $x_{n+1}, y_{n+1}, \ldots, z_{n+1}$ contenga su sistema de ecuaciones. Por lo que, experimentalmente cada una de las series pseudoaleatorias generadas se envía a su correspondiente DAC, como se ejemplifica en la figura 7.

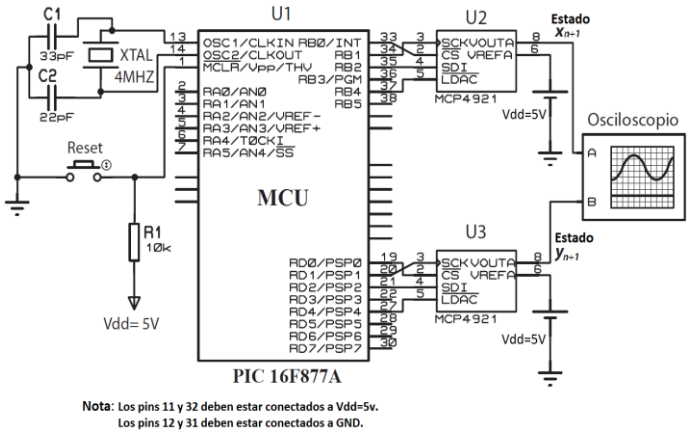

Figura 8. Diagrama eléctrico del generador de caos.

En la figura 8 se observa el diseño eléctrico del circuito digital implementado físicamente para la generación de caos. Se observa claramente el tipo de interconexión entre el microcontrolador **PIC16F877A**, con los convertidores del tipo **DAC-MCP4929**. Adicionalmente se integra un circuito generador de reloj en las terminales ***OSC1/CLKIN*** y ***OSC2/CLKOUT***, que corresponde a un cristal de 4MHz. Se adiciona un circuito reset en la terminal $\overline{\boldsymbol{MCLR}}$***/Vpp/TVH*** del microcontrolador para el control de arranque y paro del sistema. El lenguaje de programación que se utiliza es el lenguaje C para microcontroladores y el software de programación es el compilador PCWH de CCS. En la Figura 9 se observa el arreglo experimental implementado para la generación y visualización de los atractores extraños correspondientes al mapeo implementado. A manera de ejemplo, en la misma figura se muestra la generación del atractor caótico de Hénon. En primer plano (lado derecho) se visualiza en la pantalla de una computadora el atractor caótico generado numéricamente por el sistema de ecuaciones (1). Paralelamente, al fondo de la figura (lado izquierdo) se observa el mismo atractor, pero ahora en la pantalla de un osciloscopio digital generado por el sistema embebido cuyo diseño sigue las directrices mostradas en la figura 8.

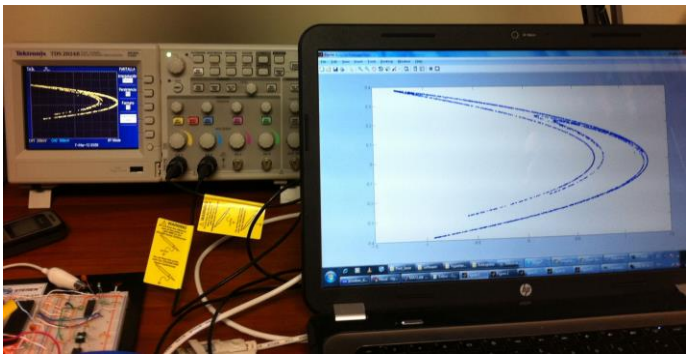

Figura 9. Arreglo experimental.

4 RESULTADOS EXPERIMENTALES

Desde la perspectiva de la electrónica digital, al utilizar dispositivos digitales y en específico los microcontroladores, se reduce la cantidad de componentes en la construcción de generadores caóticos, esto es en gran medida al hecho de que las ecuaciones en diferencias de los mapeos caóticos se implementan mediante programación en el microcontrolador y no por componentes electrónicos. Esto permite entre otras cosas, que el circuito embebido sea genérico ya que con la misma estructura de diseño (figura 8), se pueden implementar una variedad considerable de mapeos caóticos [18].

4.1 Atractores caóticos experimentales

Partiendo de la definición de los sistemas dinámicos presentados en la sección 1 (ecuaciones (2)-(5)), cuyas dinámicas se plasman en sus atractores caóticos respectivos (Figuras 3 – 6), se sigue la metodología presentada en la sección 3 para reproducir experimentalmente las dinámicas caóticas a través del sistema embebido propuesto (Figura 8). La visualización experimental de los atractores obtenidos es en la pantalla de un osciloscopio de almacenamiento digital de la

serie TDS2000B – Tektronik. La validación experimental que se lleva a cabo en esta etapa, es de carácter visual, se hace un comparativo entre los atractores caóticos generados experimentalmente con respecto a los que se generan numéricamente en una PC.

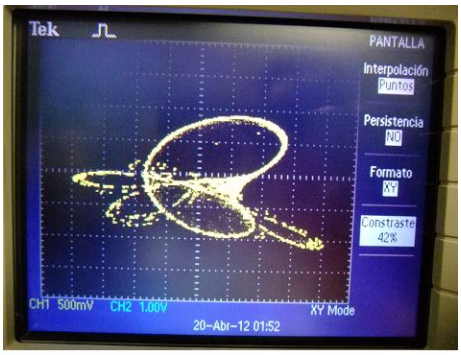

Figura 10. Atractor experimental del mapeo de Tinkerbell.

En la figura 10 se muestra el atractor caótico experimental de Tinkerbell correspondiente al sistema de ecuaciones (2) y cuyo atractor caótico generado numéricamente en una PC se muestra en la figura 3.

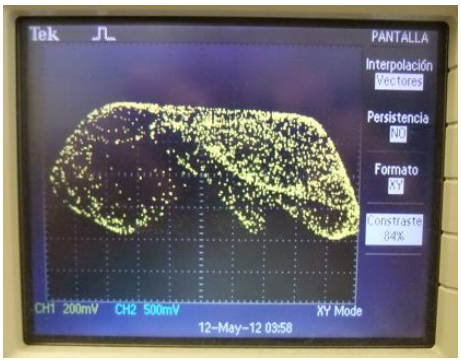

Figura 11. Atractor experimental del mapeo Logístico 2D.

En la figura 11, 12 y 13 se observan los atractores caóticos obtenidos experimentalmente de los mapeos Logístico 2D, Ikeda y Chen y que corresponden a los sistemas de ecuaciones (3), (4) y (5) respectivamente. Los atractores generados numéricamente en una PC se pueden observar en las figuras 4, 5 y 6.

4.2 Tamaño de serie caótica y longitud de sus elementos

En relación a la figura 7, el mapeo caótico se puede programar para un específico número de iteraciones o en un ciclo infinito, esto genera series caóticas de longitud específica o infinita según sea el caso.

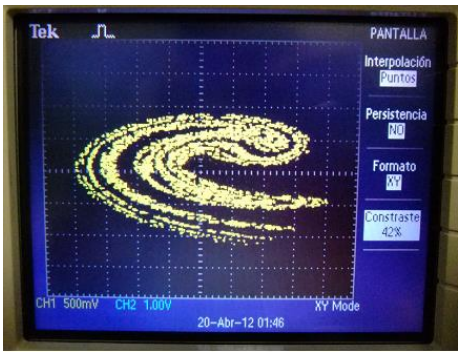

Figura 12. Atractor experimental del mapeo de Ikeda.

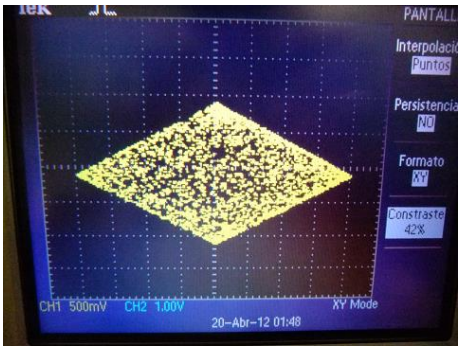

Figura 13. Atractor experimental del mapeo de Chen.

La longitud de cada elemento de la serie corresponde a la longitud máxima que pueda procesarse en el microcontrolador con el tipo de dato ***"float"***, en este caso es de 32-bits (IEEE valor punto flotante) para el PIC16F877A y su rango es:

$$1.8\text{x}10^{-38} < \text{x}_\text{i} < 3.40x10^{38}.$$

4.3 Espacio de claves

Un generador de secuencias caóticas que proporcione un espacio de claves mayor a 128 bits, se clasifica como viable para la mayoría de las aplicaciones criptográficas en términos de la velocidad de las computadoras actuales. En la tabla 1 se presentan los espacios de claves que pueden proporcionar los mapeos caóticos implementados en el sistema embebido propuesto en este trabajo basado en el microcontrolador PIC16F877A y su clasificación de viabilidad acorde a [19].

Tabla 1. Mapeos caóticos para aplicaciones criptográficas.

Viabilidad		
Mapeo caótico	Espacio de claves	viable
Tinkerbell	192	Si
Logístico 2D	192	Si
Ikeda	128	No
Chen	128	No

5 CONCLUSIONES

De los resultados obtenidos experimentalmente, se vislumbra la potencialidad que brindan los diseños y construcción de sistemas embebidos para la generación de caos. La base del sistema electrónico digital propuesto, resulta ser sencillo, compacto y destaca la ventaja de que bajo el mismo esquema, es fácil conmutar de un mapeo caótico a otro. El desarrollo de este tipo de generadores caóticos digitales, permiten implementar la criptografía caótica digital, la cual está basada no en la complejidad algorítmica en los niveles superiores, sino en conceptos físicos relativos a las señales digitales caóticas portadoras de la llave de encriptado/desencriptado, que trabajan en las capas inferiores (capa física), lo que permite en principio una seguridad incondicional. Las comunicaciones digitales empleando portadoras caóticas constituyen un medio prometedor para proporcionar privacidad y seguridad en redes de telecomunicación. Dado que la implementación del generador caótico es en un sistema embebido, esto facilitará la aplicación e integración en sistemas de telecomunicación actuales que operan en tiempo real, tal como la telefonía celular.

6 AGRADECIMIENTOS

Este trabajo fue apoyado por el proyecto de investigación aprobado en la 18va Convocatoria Interna de Proyectos de Investigación de la UABC, con el número 485 y vigente para los años 2015-2017. Al CONACyT por la beca brindada al investigador F.V.A. en apoyo a sus estudios de posgrado a nivel Doctoral.

7 REFERENCIAS

[1] E. N. Lorenz, «Deterministic Nonperiodic Flow,» *Journal of the Atmospheric Sciences,* vol. 20, pp. 130-141, 1963.

[2] F.C.Moon, Chaotic And Fractal Dynamics. An Introduction for applied Scientists and Engineers., Ithaca, New York.: WILEYVCH Verlang Gmbh & Co. KGaA., 1992.

[3] M. Hénon, «A Two-dimensional Mapping with a Strange Attractor,» *Communications in Mathematical Physics,* vol. 50, nº 1, pp. 69-77, 1976.

[4] Y. S. a. T. Jiang, «Bifurcation and Chaos in the Tinkerbell Map,» *International Journal of Bifurcation and Chaos,* pp. 3137-3156, 2011.

[5] P. F. Verhulst, «Recherches Mathematiques sur la loi d' Accroissement de la Population,» *Nouv. mém. de l' Academie Royale des Sci. et. BellesLettres de Bruxelles,* vol. 18, pp. 1-41, 1845.

[6] R. M. May, «Simple Mathematical Models with very Complicated Dynamics,» *Nature,* vol. 261, pp. 459-467, 1976.

[7] K. I. a. H. Daido, «Optical Turbulence: Chaotic Behavior of Transmited Light from a Ring Cavity,» *Phys. Rev.,* vol. 45, nº 9, pp. 709-712, 1980.

[8] L. Chen, «An Open-plus-closed-loop Control for Discrete Chaos and Hyperchaos,» *Physis Letters A,* vol. 128, nº 5, pp. 327-333, 2001.

[9] G. C. a. T. Veta, «Chaos in Circuits ans Systems,» *World Scientific Series on Nonlinear Science,* vol. 11, nº Series B.

[10] P. S. Lindsay, «Period Doubling and Chaotic Behavior in Driven Anharmonic Oscilator.,» *Phys. Rev. ,* vol. 41, pp. 1349-1352, 1981.

[11] R. N. a. S. Sathyan, «An RC Op. Amp. Chaos Generator,» *IEEE Trans. Circuit Syst.,* vol. 30, pp. 54-56, 1983.

[12] M. K. a. T. M. L. O. Chua, «The Double Scroll Family,» *IEEE Trans. Circuit Syst.,* vol. 33, pp. 1072-1118, 1986.

[13] M. P. Kennedy, «Three Steps to Chaos, part ii; A Chua's Circuit Primer.,» *IEEE Trans. Circuit Syst.,* vol. 3, nº 6, pp. 1619-1627, 1993.

[14] S. L. Ljupco Kocarev, «Chaos-Based Cryptography Theory, Algorithms and Applications.,» *Studies in Computational Intelligence, Springer.,* nº 354.

[15] L. Acho-Zuppa, «Chaotic Logistic Map Implementation in the PIC12F629 Microcontroler Unit.,» *10th IFAC Workshop on Programmable Devices and Embedded Systems.,* vol. 10, 2010.

[16] E. S. A. E.-B. A. M. W. E.-M. M. E.-B. a. E. D. S. A. K. Aboul-Seoud, «A Simple 8 bit Digital Microcontroller Implementation for Chaotic Sequence Generation.,» *28th National Radio Science Conference.,* pp. 5959-5965, 2011.

[17] H. S. K. a. K. F. M. K. W. Tang, «A Chaos Based-random-number Generator for Eigth-bit Microcontroler System.,» *International Journal of Bifurcation and Chaos.,* vol. 3, pp. 852-867, 2008.

[18] A. F. Vergara, «Encriptado Caótico Basado en Microprocesador con Comunicación Wi-Fi.,» Universidad Autónoma de Baja California., Ensenada, Baja California México., 2013.

[19] V. P. N. K. P. G. y. S. K. Patidar, «A Robust and secure Chaotic Standar Map Based Pseudorandom Permutation-substitution Scheme for Image Encryption.,» *Optics Communications,* nº 284, pp. 4331-4339, 2001.

[20] T. Saito, «A Chaos Generator Based on a Quasi-harmonic Oscillator.,» *IEEE Trans. Circuit Syst.,* vol. 32, pp. 320-331, 1985.