ENCRIPTADOR CAÓTICO DE IMÁGENES EMPLEANDO UN SISTEMA EMBEBIDO

Abraham Flores-Vergara, Universidad Autónoma de Baja California.
venumc@uabc.edu.mx.
Enrique Efren García-Guerrero, Universidad Autónoma de Baja California.
eegarcia@uabc.edu.mx.
Everardo Inzunza-González, Universidad Autónoma de Baja California.
einzunza@uabc.edu.mx.
Oscar Roberto López-Bonilla, Universidad Autónoma de Baja California.
olopez@uabc.edu.mx.
Eduardo Rodríguez-Orozco, Universidad Autónoma de Baja California.
eduardo.rodriguez.orozco@uabc.edu.mx.

RESUMEN: *El presente trabajo propone un método con criptografía caótica digital implementado en un sistema embebido del alto desempeño computacional Raspberry Pi, para encriptar y desencriptar imágenes digitales a color. El propósito es evaluar la viabilidad y potencialidad que ofrece la tecnología emergente "System on a Chip" (SoC) en procesos de generación de caos y sus aplicaciones potenciales en métodos criptográficos de información confidencial con fines de almacenamiento o de integración en sistemas de telecomunicación. El análisis de seguridad realizado al algoritmo propuesto para el encriptado de imágenes digitales considera análisis estadísticos, tal como NPCR, UACI, entropía de la información, histogramas, análisis de sensibilidad de clave y espacio de claves. Los resultados obtenidos demuestran que el algoritmo de encriptado caótico es robusto y seguro contra los diferentes ataques estadísticos.*

PALABRAS CLAVE: Caos digital, Encriptador, Criptografía caótica, Sistema embebido, Raspberry Pi

1 INTRODUCCIÓN

Sin duda alguna, los cambios en el entorno social y económico que vivimos en la actualidad, tienen una relación directa con los avances tecnológicos en el contexto de las comunicaciones e información. "Estos avances son precisamente el resultado en torno a la digitalización de datos y de su transportación a través de diferentes medios, a grandes distancias y en pequeños intervalos de tiempo y no siempre de manera segura"

Hace ya medio siglo que el Dr. Gordon Earl Moore co-fundador y miembro emérito de la junta directiva de Intel Corporation, describiera su hipotética "ley", la cual describe el comportamiento de la evolución digital basada en transistores. La ley de Moore publicada el 19 de abril de 1965 en la revista "Electronics", anticipaba que la complejidad de los circuitos integrados (CI), medida a partir del número de transistores por CI (chip o microchip), se duplicaría cada dos años. Vaticinó que: "los circuitos integrados conducirán a maravillas como computadores en el hogar o al menos terminales conectadas a un computador central, controladores automáticos para automóviles y dispositivos móviles de comunicación personal. El reloj de pulsera electrónico sólo necesita una pantalla para que sea posible hoy día" [2]. La predicción de Moore, se valida al comparar por ejemplo, uno de los chips más complejos de la actualidad, el Xeon de 15 núcleos, con unos 4100 millones de transistores con respecto al chip de 120 transistores con el que dio inicio la carrera digital. Bajo este panorama, la tecnología en la que nos encontramos actualmente inmersos, supera las predicciones de Moore. El desarrollo tecnológico, es tal que resulta cada vez más común encontrar las denominadas computadoras de placa reducida, también conocidas como microcomputadoras ó SoC, que son computadoras completamente integradas en un sólo circuito. Tal es el caso de la denominada Raspberry Pi, que desde sus inicios en el 2006 y hasta su modelo más reciente lanzado en 2016, Raspberry Pi 3 Modelo B [3] ha tenido una muy buena aceptación. El diseño de las Raspberry Pi en tamaño, es similar al de una tarjeta de crédito (8.6 ×5.4 × 1.7 cm).

El objetivo de este trabajo es evaluar la viabilidad y potencialidad que ofrece la tecnología de Raspberry Pi utilizando la versión 2 modelo B [4], en procesos de generación de caos y sus aplicaciones potenciales en métodos con criptografía caótica, para encriptar imágenes digitales a color con fines de almacenamiento o de integración en sistemas de telecomunicación. La motivación principal de este trabajo se deriva de la vulnerabilidad que presentan los sistemas de seguridad convencionales como DES [5], o AES [6], entre otros, por lo que, es ya una necesidad imperiosa el desarrollar e implementar nuevas técnicas que nos permitan optimizar el ciclo de codificación-decodificación de la información confidencial, que sean lo suficientemente eficientes

para incrementar y garantizar los niveles de seguridad y privacidad necesarios en nuestros días y que seguramente serán más demandantes en el futuro mediato [7-11]. Bajo este esquema, en este trabajo se integran las bondades de la tecnología emergente que ofrece Raspberry Pi, con las propiedades del caos bajo un esquema operacionalmente simple y de alta seguridad, a fin de gestar un sistema criptográfico caótico embebido de bajo costo y bajo consumo de energía.

2 MATERIALES Y MÉTODOS

Son tres las etapas básicas que dan forma al sistema criptográfico implementado: i) selección del mapeo caótico como base para la generación de caos, ii) implementación y validación del sistema caótico en la Raspberry Pi y iii) desarrollo e implementación del algoritmo embebido que ejecuta el ciclo de encriptado-desencriptado de imágenes digitales a color. Se aplican diferentes tipos de análisis a fin de establecer por una parte, los niveles de seguridad propios del sistema criptográfico propuesto y por otra, los niveles de seguridad alcanzados por las imágenes encriptadas (criptogramas).

2.1 MAPEO CÁOTICO

De la gran variedad de mapeos caóticos existentes y ampliamente documentados en la literatura, en el presente trabajo de investigación, se experimenta con el mapeo de Tinkerbell [12]. Este mapeo descrito por Ec. (1), presenta una dinámica en régimen caótico dependiente de dos condiciones iniciales y cuatro parámetros de control. En la figura 1 se observa el atractor característico, obtenido por cálculo numérico con el software MATLAB™.

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

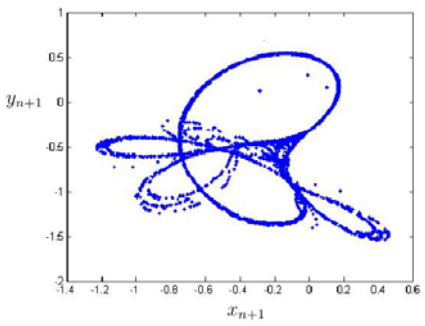


Figura 1. Atractor caótico de mapeo de Tinkerbell.

2.2 PLATAFORMA RASPBERRY PI 2

En la Figura 2 se presenta el sistema embebido Raspberry Pi 2 Modelo B, el cual es un sistema digital basado en microprocesador ARM construido en una placa reducida y de bajo costo, desarrollada en Reino Unido por la Fundación Raspberry Pi.

El diseño de la placa es un SoC (System on a Chip) Broadcom 2836, que contiene un microprocesador ARM Quad Core Cortex-A7 de 32 bits que funciona con reloj de 900 MHz con opción de "overclock" a 1.1 GHz, un procesador gráfico (GPU) Video Core IV y 1 GB de memoria RAM. El diseño no incluye disco duro ni unidad de estado sólido, por lo que se emplea una tarjeta Micro-SD para el almacenamiento de información y del sistema operativo. Además, cuenta con puerto Ethernet para su conectividad a internet, un puerto HDMI como interfaz de video de alta definición y con puertos de comunicación USB para le conexión de periféricos como adaptador Wi-Fi, teclado, cámara web, memorias externas de tipo flash, mouse, entre otros. Este sistema embebido funciona con el sistema operativo Linux, principalmente con la distribución Raspbian.

Figura 2. Sistema embebido Raspberry PI 2 modelo B.

2.3 ALGORITMO EMBEBIDO PROPUESTO

En la Figura 3 se presenta un esquema a bloques del método de encriptado propuesto, el cual está desarrollado con base en el método de cifrado en flujo [13]. La serie de elementos = { !, !, … , !}, que se obtiene a partir de la secuencia pseudoaleatoria generada por el mapeo caótico va enmascarando cada elemento del mensaje = { !, !, … , !} mediante la operación X-OR, para dar lugar a los elementos de = { !, !, … , !} que corresponden al criptograma de la imagen original [14]. Las imágenes a encriptar, son imágenes a color en formato RGB de 8 bits.

Una de las ventajas del sistema criptográfico implementado y del algoritmo embebido, es el hecho de mantenerse invariante en su estructura cuando se

lleva a cabo el proceso inverso de desencriptado (recuperar la imagen original), el cual aprovecha la propiedad de dualidad de la operación X-OR.

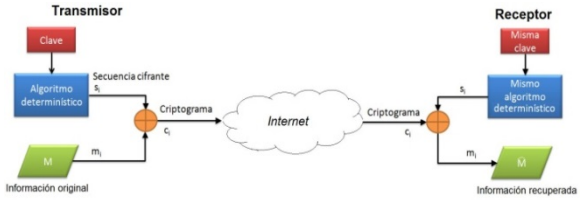


Figura 3. Método de cifrado en flujo

3 PARTE EXPERIMENTAL

3.1 SISTEMA EMBEBIDO PROPUESTO

El sistema criptográfico caótico propuesto, utiliza dos dispositivos SoC Raspberry Pi 2, uno como sistema encriptador y otro como sistema desencriptador. Ambos dispositivos se encuentran remotamente interconectados mediante la internet, con monitor, teclado y mouse conectados como dispositivos periféricos. Las imágenes digitales empleadas en este trabajo se encuentran previamente almacenadas en la Micro-SD.

Cada dispositivo opera con el sistema operativo Raspbian [15], desarrollado y optimizado con base en el sistema operativo universal de uso común y de código abierto Debían [16]. Por lo tanto, se puede disponer de:

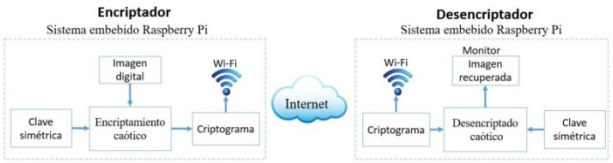


Figura 4. Diagrama de bloques del sistema criptográfico caótico embebido basado en Raspberry Pi

4 RESULTADOS Y DISCUSIÓN

4.1 GENERACIÓN DE CAOS

A fin de validar y evaluar la funcionalidad operativa del sistema experimental propuesto, primeramente se valida la generación de caos a partir de la obtención experimental del comportamiento caótico de varios sistemas discretos. A manera de ejemplo, las Figuras 5 y 6, muestran la dinámica caótica obtenida de los estados !!! e !!! del mapeo de Tinkerbell, implementado en el sistema Raspberry Pi 2. En la Figura 7 se puede observar el atractor extraño del mapeo caótico de Tinkerbell, el cual se obtuvo considerando cálculo numérico de doble precisión IEEE754 de 64 bits [18]. Del atractor experimental presentado en la Figura 7 en relación al mostrado en la Figura 1, se observa la paridad de los atractores obtenidos. El programa encriptador y desencriptador de imágenes digitales se utiliza para generar las señales caóticas y permite visualizar las gráficas de los estados de fase, cabe mencionar que se está empleando la biblioteca Matplotlib [19] para el despliegue de las imágenes procesadas.

Por otra parte, para el encriptado de la información se propone utilizar el estado !!! como secuencia cifrante del método propuesto considerando una condición inicial de ! = −0.72.

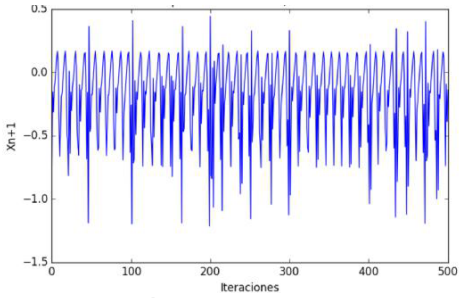


Figura 5. Señal caótica del estado !!! del mapeo de Tinkerbell

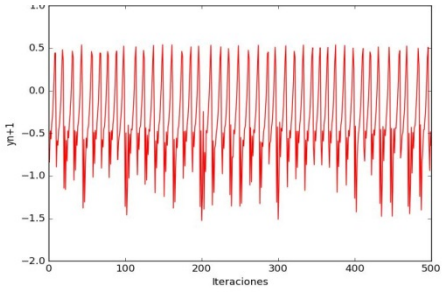


Figura 6. Señal caótica del estado !!! del mapeo de Tinkerbell.

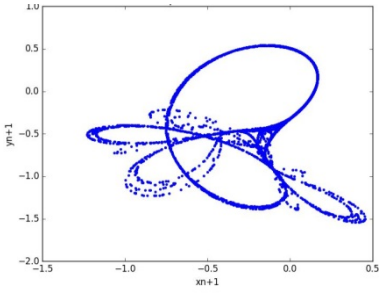


Figura 7. Atractor caótico del mapeo de Tinkerbell evaluado en la Raspberry Pi 2.

4.2 ENCRIPTADO DE IMÁGENES A COLOR

Las Figuras 8-10 muestran las imágenes digitales a color empleadas para validar el sistema criptográfico, así como los criptogramas obtenidos para cada una de ellas. Se puede observar que la

información obtenida a partir de los criptogramas es prácticamente ininteligible, es decir, no refleja información alguna o vestigio de la imagen original. Cada imagen se procesa de manera individual siguiendo el método descrito en la sección 2.3 y esquematizado en la Figura 3

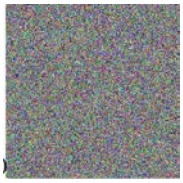
a)  b) 

Figura 8. a) Imagen Lena.png de 256 x 256 pixeles y b) criptograma obtenido con el sistema embebido

a)  b) 

Figura 9. a) Imagen mandril.png de 512 x 512 pixeles y b) criptograma obtenido con el sistema embebido

a)  b) 

Figura 10. a) Imagen Loto.png de 1024 x 1024 pixeles y b) criptograma obtenido con el sistema embebido

En la Figura 11 se muestran las imágenes recuperadas, aplicando el proceso inverso descrito en la sección 2.3.

A partir de un análisis de los histogramas de las imágenes originales y de las imágenes recuperadas, se deduce que son idénticas en cada caso, es decir se logra recuperar el 100% de la información.

Figura 11. Imágenes recuperadas con el desencriptador caótico embebido utilizando la misma clave simétrica

4.3 ESPACIO DE CLAVES

El espacio de claves que proporciona el encriptador caótico implementado en el sistema embebido Raspberry Pi 2 está determinado por las condiciones iniciales del mapeo caótico y sus parámetros de control. Para el caso del mapeo de Tinkerbell y considerando una longitud del tipo de dato flotante de 64 bits acorde al estándar IEEE 754, se tiene que con dos condiciones iniciales para las ecuaciones del mapeo caótico y cuatro parámetros de control, la longitud total de una clave es de (2 + 4)×64 = 384 bits. Por lo tanto, como el sistema embebido propuesto es binario, el espacio de claves en términos de bits es de $2^{!"\#}$ bits [20].

4.4 ANÁLISIS DE SENSIBILIDAD

La sensibilidad del sistema criptográfico propuesto se analiza a partir de los criptogramas obtenidos. En la Figura 12, se muestra el resultado de una prueba de sensibilidad, en donde a partir de un cambio mínimo en el valor de la clave simétrica se obtiene una imagen sin ningún vestigio de información de la original. Es decir, un cambio mínimo en alguno de los parámetros o de las condiciones iniciales, produce una trayectoria caótica diferente y en consecuencia, se obtiene una serie cifrante completamente distinta. El cambio mínimo que permite el sistema desarrollado es de ±1×10!!".

a)  b) 

Figura 12: a) imagen recuperada con la misma clave simétrica y b) imagen recuperada con un cambio mínimo en la clave simétrica (variación de ±1×10!!")

Para validar la sensibilidad del sistema criptográfico propuesto, se aplica un $\Delta = -1\times10!!"$ a la condición inicial con el propósito de recuperar la imagen original de uno de los criptogramas obtenidos.

A manera de ejemplo, utilizamos esta condición inicial para recuperar la imagen original de "Lena.png" a partir de su criptograma (Figura 8b). En la Figura 13 se observan los componentes R, G y B de la imagen recuperada con sus respectivos histogramas, de donde se deduce, que no hay información alguna que permita inferir algo sobre la imagen original correspondiente.

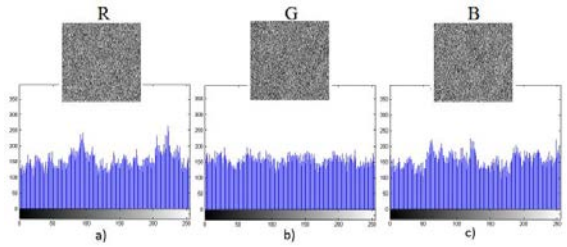


Figura 13. Componentes R, G y B de la imagen recuperada e histogramas obtenidos con un cambio mínimo en ! (Δ = −1×10!!").

4.5 ANÁLISIS ESTADÍSTICO

El análisis estadístico para validar el método criptográfico propuesto con el mapeo de Tinkerbell, se realizó mediante las prueba NPCR y UACI [21] y mediante el valor de incertidumbre de entropía de la información.

Para las pruebas NPCR y UACI, se consideró un parámetro = 0.05. La prueba analizó dos criptogramas de una imagen encriptada con dos claves muy similares. La proximidad se determinó por un cambio de Δx=-1*10 en la condición inicial.

La prueba se realizó a imágenes de diferente resolución.

En la Tabla 1 se pueden observar los resultados obtenidos y se infiere de la misma que en los tres casos de imágenes con diferentes resoluciones, se obtuvieron resultados por arriba del valor mínimo de NPCR y dentro del rango de los valores críticos de UACI, por lo tanto, el sistema implementado ofrece resultados satisfactorios ante este tipo de análisis.

Para el análisis de entropía de la información, considerando imágenes con una resolución de 8 bits cada uno, el valor ideal de incertidumbre es de 8 bits/símbolo.

La Tabla 2 muestra los valores de entropía obtenidos al evaluar los elementos correspondientes a los componentes R, G y B de los criptogramas resultantes de las imágenes analizadas en el presente trabajo.

Se puede observar que para las diferentes imágenes usadas, la entropía en todos los casos los resultados son mayores a 7.99 bits/símbolo, los cuales se encuentran muy cercanos al valor ideal de 8 bits/símbolo.

Mapeo de Tinkerbell. NPCR/UACI ($\alpha = 0.05$)	
Imagen Lena.png de 256×256 pixeles	
Valor mínimo deseado NPCR $N_{0.05} = 99.5693\%,$	Valores críticos UACI $U^{-}_{0.05} = 33.2824\%$ $U^{+}_{0.05} = 33.6447\%$
Valor obtenido: **99.58%**	Valor obtenido: **33.38%**
Imagen Mandril.png de 512×512 pixeles	
Valor mínimo deseado NPCR $N_{0.05} = 99.5893\%,$	Valores críticos UACI $U^{-}_{0.05} = 33.3730\%$ $U^{+}_{0.05} = 33.5591\%$
Valor obtenido: **99.6022%**	Valor obtenido: **33.4721%**
Imagen Loto.png de 1024×1024 pixeles	
Valor mínimo deseado NPCR $N_{0.05} = 99.5994\%,$	Valores críticos UACI $U^{-}_{0.05} = 33.4183\%$ $U^{+}_{0.05} = 33.5088\%$
Valor obtenido: **99.5995%**	Valor obtenido: **33.4259%**

Tabla 1: Resultado de la prueba NPCR y UACI

Mapeo de Tinkerbell	Componentes RGB de 8 bits Entropía obtenida (bits/símbolo)		
Imagen	R	G	B
Lena	**7.997**0	**7.997**2	**7.996**7
Mandril	**7.9993**4	**7.9993**1	**7.9993**4
Loto	**7.9997**9	**7.9997**2	**7.9997**7

Tabla2: Valores de entropía de la información de los criptogramas de Lena, Mandril y Loto.

5 CONCLUSIONES

A partir de los resultados experimentales se valida ampliamente los niveles de seguridad alcanzados tanto para el sistema criptográfico, como para los criptogramas obtenidos. Las características tecnológicas del encriptador caótico lo hacen idóneo a integrarse en sistemas de telecomunicación actuales o en sistemas criptográficos de información confidencial, como por ejemplo en aplicaciones de reconocimiento biométrico. Bajo este contexto se demuestra la viabilidad y la gran potencialidad al implementar sistemas criptográficos caóticos en sistemas embebidos de alto desempeño computacional, tal como el Raspberry Pi.

6 AGRADECIMIENTOS

Este trabajo fue apoyado por el proyecto de investigación aprobado en la 18a Convocatoria Interna de Proyectos de Investigación de la UABC, con el número programático 485 y vigente para los años 2015-2017. Al CONACyT por la beca brindada al los investigadores A.FV. y E.R.O. en apoyo a sus estudios de posgrado a nivel Doctoral. Al PRODEP por el apoyo de Fomento a la Generación y Aplicación Innovadora del Conocimiento otorgado al investigador Dr.

Everardo Inzunza González para el periodo 2016-2017

7 REFERENCIAS

[1] *J. L. Montero O' Farrrel, «Las tecnologías de la información y de las comunicaciones en la sociedad y la educación.,» Edutec-e. Revista Electrónica de Tecnología Educativa., nº 21, Julio 2006.*

[2] *G. E. Moore, «Cramming more components onto integrated circuits,» IEEE Solid-State Circuits Society Newsletter , vol. 20, nº 1, pp. 33-35, Sept 2006.*

[3] *Raspberry Pi Foundation, «Raspberry Pi 3 Modelo B,» 2016. [En línea]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/.*

[4] *Raspberry Pi Foundation, «Raspberry Pi 2 model B,» Raspberry Pi Foundation, 2015. [En línea]. Available: https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. E.*

[5] *Biham y A. Shamir, «Differential Cryptanalysis of the Data Encryption Standard,» Springer Verlag, 1993.*

[6] *National Institute of Standards and Technology, U.S. Department of Commerce, «FIPS PUB 197, Advanced Encryption Standard (AES),» November 2001. [En línea]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .*

[7] *A. Flores-Vergara, E. Inzunza-González, E. E. García-Guerrero y F. Zamora-Arellano, «Diseño e Implementacíon de un Generador de Caos Basado en un Microcontrolador de 8 bits.,» de LV Congreso Nacional de Física., Morelia, Michoacan., 2012*

[8] *A. Flores-Vergara, E. García-Guerrero, E. Inzunza-González y O. López-Bonilla, «Encriptador y Desencriptador Caótico de Imágenes Digitales Usando un Sistema Embebido con Comunicación Wi-Fi.,» Congreso Internacional de Ingeniería Electrónica, vol. 38, pp. 105-110, 2016*

[9] *F. Dachselt y W. Schwarz, «Chaos and Cryptography,» 2001*

[10] *G. Chen, Y. Mao y C. K. Chui, «A symmetric image encryption based on 3{D} chaotic cat maps,» Chaos, Solitons and Fractals, vol. 21, nº 3, pp. 749-761, 2004.*

[11] *E. Inzunza, «Encriptado Caótico en Sistemas Biométricos,» UABC, Tesis de doctorado, Ensenada, Baja California México, 2012*

[12] *Y. Shaoliang y T. Jiang, «Bifurcation and Chaos in the Tinkerbell map,» International Journal of Bifurcation and Chaos, vol. 11, pp. 3137-3156, 2011.*

[13] *A. Fuster, D. Martinez, L. Hernández, F. Montoya y J. Muñoz, Técnicas Criptográficas de Protección de Datos, Alfaomega Ra-Ma, 2001.*

[14] *F.-V. Abraham, «Encriptado Caótico Basado en Microprocesador con Comunicación Wi-Fi,» Tesis de Mestría en Ingeniería, Octubre 2013*

[15] *Raspberry Pi Foundation, «Raspbian Operating System,» Raspberry Pi Foundation, 2016. [En línea]. Available: https://www.raspbian.org/.*

[16] *Debian Project, «The universal operating system.,» [En línea]. Available: https://www.debian.org/.*

[17] *Python Foundation, «Python,» Python software foundation, 2001-2016. [En línea]. Available: https://www.python.org/*

[18] *C. S. IEEE, «{IEEE} Standard for Floating - Point arithmetic,» IEEE std 754 - 2008, pp. 1-58, 2008.*

[19] *J. Hunter, D. Dale y E. F. a. M. Droettboom, «Matplotlib.,» 2016. [En línea]. Available: http://matplotlib.org. V. Patidar, N. K. Pareek, G. Purohit y K. K. Sud, «A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption,» Optics Communications, vol. 284, pp. 4331-4339, 2011.*

[20] *Y. Wu, J. P. Noonan y S. Agaian, «NPCR and UACI Randomness Tests for Image Encryption,»Multidisciplinary Journals in Science and Technology, 2011.*

[21] *Abraham Flores -Vergara: Ingeniero en Computación con estudios de Maestría en Ingeniería en el área de eléctrica por la Universidad Autónoma de Baja California. Estudiante de Doctorado en Ciencias (Electrónica).*

[22] *E. Efren García-Guerrero: Ingeniero Físico egresado de la Universidad Autónoma Metropolitana, de la ciudad de México, con Maestría y Doctorado en Óptica Física por el Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE). Con experiencia en mico y nano-fabricación de componentes opto-electrónicos.*

[23] *Everardo Inzunza-González: Ingeniero Electrónico egresado del Instituto Tecnológico de Culiacán, con estudios de Maestría en Ciencias en Electrónica y Telecomunicaciones por el Centro de Investigación Científica y de Educación*

Superior de Ensenada, Doctor en Ciencias por la Universidad Autónoma de Baja California con énfasis en electrónica. Miembro del Sistema Nacional de Investigadores desde 2015.

[24] Oscar Roberto López-Bonilla: Ingeniero en Electrónica egresado del ITESO, Guadalajara, Jalisco, con maestría en Instrumentación Electrónica por CICESE, Ensenada, Baja California, y Doctorado en Electrical Engineering por la SUNY at Stony Brook, Stony Brook, New York, USA. Con experiencia en instrumentación electrónica y cómputo de alto rendimiento.

[25] Eduardo Rodríguez-Orozco: Ingeniero en Electrónica con estudios de Maestría en Ingeniería en el área de Eléctrica por la Universidad Autónoma de Baja California. Estudiante de Doctorado en Ciencias con énfasis en electrónica.

[26]