Encriptador caótico de imágenes empleando un sistema embebido.

Flores Vergara Abraham, Rodríguez Orozco Eduardo, García Guerrero E. Efrén, Inzunza González Everardo y López Bonilla Oscar.

Facultad de ingeniería, Arquitectura y Diseño, Programa de Maestría y Doctorado en Ciencias e Ingeniería.

RESUMEN

Este trabajo presenta el diseño e implementación de un sistema electrónico digital con criptografía caótica, con el propósito de integrarse a los métodos criptográficos de información confidencial en sistemas de telecomunicación. El diseño digital se implementa en un sistema Raspberry Pi 2. El mapeo caótico utilizado para la generación de caos corresponde a las ecuaciones en diferencias del mapeo caótico de Tinkerbell. Los mensajes utilizados son imágenes a color en formato RGB.

INTRODUCCIÓN

La criptografía caótica implementada en sistemas electrónicos se presenta como una alternativa para solucionar las necesidades de comunicación segura hoy en día (ver figura 8). Sin embargo, el uso de sistemas electrónicos analógicos adiciona complejidad y vulnerabilidad en comparación con el uso de sistemas electrónicos digitales.

En el diseño de circuitos analógicos para la generación de caos, es necesario emplear una gran variedad de componentes electrónicos que, en la mayoría de los casos, se requieren valores nominales en los componentes muy precisos o llevar acabo ajustes muy finos, lo que hace complicada la implementación experimental.

Desde la perspectiva de la electrónica digital, 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. Esto minimiza tanto la complejidad en la circuitería, como en el tiempo de implementación.

METODOLOGÍA

El método de encriptamiento que se utiliza es el cifrado en flujo; que utiliza una serie de elementos pseudoaleatorios generados mediante un algoritmo deterministico, en este caso, el mapeo caótico de Tinkerbell .

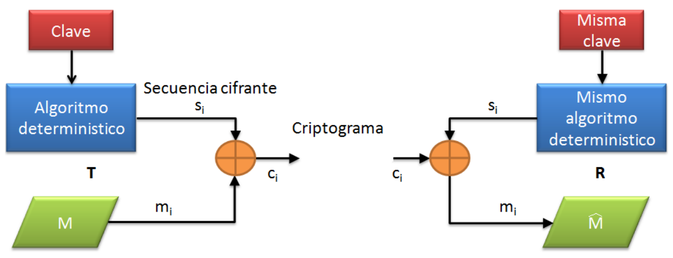

Figura 1. Método de cifrado en flujo

El sistema digital donde se implementa el método de encriptado es un sistema embebido basado en microprocesador de última generación Raspberry Pi 2.

Figura 2. Sistema basado en microprocesador ARM V7L Raspberry Pi 2

RESULTADOS

La Figura 3, muestra el atractor caótico del mapeo de Tinkerbell generado numéricamente y el generado con el sistema Raspberry Pi 2 .

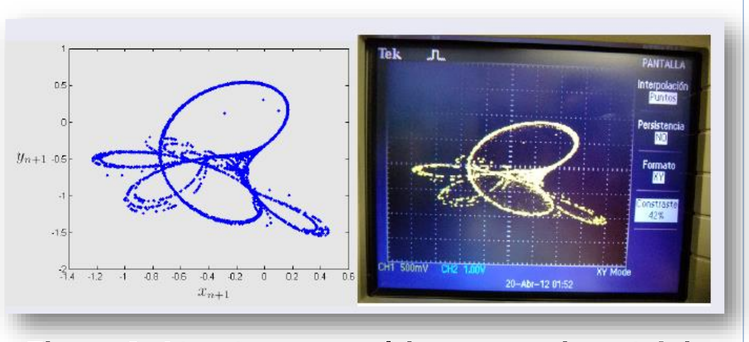

Figura 3. Atractores numérico y experimental de Tinkerbell.

Las figuras 4-6 muestran las imágenes encriptadas y sus respectivos criptogramas, mismos que se envían como mensaje por e-mail.

Figura 4. Imagen de 250 x 250 pixeles

Figura 5. Imagen de 222 x 181 pixeles

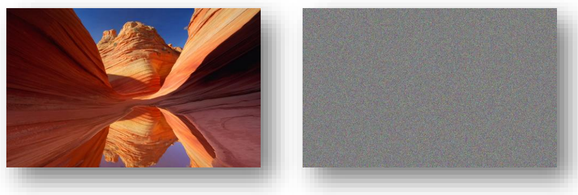

Figura 6. Imagen de 1920 x 1200 pixeles

La figura 7 muestra las imágenes recuperadas después de ser desencriptadas aplicando el proceso inverso de desencriptado, se observa que son idénticas a las originales.

Figura 7. Imágenes recuperadas

El espacio de claves que proporciona el generador caótico implementado en el sistema Raspberry Pi 2 está determinado por las condiciones iniciales del mapeo caótico y sus parámetros de control. El valor numérico que se procesa es de tipo flotante de 64 bits de doble precisión.

Espacio de claves del generador con Raspberry Pi 2.

Mapeo caótico	Espacio de claves (bits)
Tinkerbell	384
Logístico 2D	384
Ikeda	256
Chen	256
Hénon	256
Logístico 1D	128

IMÁGENES

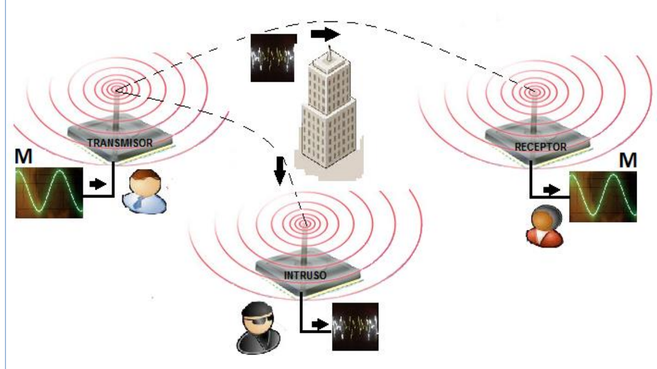

Figura 8. Sistema de comunicación segura.

CONCLUSIONES

La investigación realizada, presenta la viabilidad de implementar sistemas digitales embebidos basados en microprocesador Raspberry Pi 2 en el diseño de sistemas criptográficos caóticos para comunicaciones seguras y su implementación en internet.

De lo anterior se comprueba que el método propuesto puede ser viable si se utilizan sistemas caóticos que proporcionen espacios de claves mayores a 128 bits. Adicionalmente, la utilización de la operación XOR en el método de cifrado, involucra que se puede utilizar el mismo sistema embebido para encriptar y desencriptar la imagen.

BIBLIOGRAFÍA

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

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

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.

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

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 los investigadores A.FV. y E.R.O. en apoyo a sus estudios de posgrado a nivel Doctoral.

EXPOCIENCIA