Ingeniería Investigación y Tecnología, volumen XVI (número 3), julio-septiembre 2015: 335-343
ISSN 1405-7743 FI-UNAM
(artículo arbitrado)
doi: http://dx.doi.org/10.1016/j.riit.2015.05.004

Sistema para codificar información implementando varias órbitas caóticas

System for Information Encryption Implementing Several Chaotic Orbits

Jiménez-Rodríguez Maricela
Departamento de Ciencias Tecnológicas
Centro Universitario de la Ciénega
Universidad de Guadalajara
Correo: m_jimenez_r@yahoo.com

Flores-Siordia Octavio
Departamento de Ciencias Tecnológicas
Centro Universitario de la Ciénega
Universidad de Guadalajara
Correo: o_flores@live.com.mx

González-Novoa María Guadalupe
Departamento de Ciencias Básicas
Centro Universitario de la Ciénega
Universidad de Guadalajara
Correo: gleznogpe@hotmail.com

Información del artículo: recibido: octubre de 2013, reevaluado: abril de 2014, aceptado: agosto de 2014

Resumen

En este artículo se propone un algoritmo de cifrado simétrico que toma como entrada la información original de longitud *L* y al codificarla genera el texto cifrado de longitud mayor *LM*. Se implementa el sistema discreto caótico mapa logístico para generar 3 órbitas diferentes: la primera se utiliza para aplicar una técnica de difusión con la finalidad de mezclar la información original, la segunda órbita se combina con la información mezclada y se incrementa la longitud de *L* hasta *LM* y con la tercer órbita se implementa la técnica de confusión. El algoritmo de cifrado se aplicó para codificar una imagen que después se recupera totalmente mediante las llaves que se utilizaron para cifrar y su respectivo algoritmo para descifrar. El algoritmo puede codificar cualquier información con solo dividirla en bloques de 8 bits, puede cumplir con los requerimientos de alto nivel de seguridad, utiliza 7 claves para cifrar y además proporciona buena velocidad de cifrado.

Descriptores:

- algoritmo
- cifrado simétrico
- caos
- mapa logístico
- confusión
- difusión

Abstract

This article proposes a symmetric encryption algorithm that takes, as input value, the original information of length L, that when encoded, generates the ciphertext of greater length LM. A chaotic discrete system (logistic map) is implemented to generate 3 different orbits: the first is used for applying a diffusion technique in order to mix the original data, the second orbit is combined with the mixed information and increases the length of L to LM, and with the third orbit, the confusion technique is implemented. The encryption algorithm was applied to encode an image which is then totally recovered by the keys used to encrypt and his respective, decrypt algorithm. The algorithm can encode any information, just dividing into 8 bits, it can cover the requirements for high level security, it uses 7 keys to encrypt and provides good encryption speed.

Keywords:

- *algorithm*
- *symmetric encryption*
- *chaos*
- *logistic map*
- *confusion*
- *diffusion*

Introducción

Cada día se generan y avanzan constantemente las nuevas tecnologías y, con estas, también se incrementa la necesidad de utilizarlas para mantenerse en comunicación constante con diferentes personas ubicadas en cualquier lugar del mundo. Pero este crecimiento exponencial también genera un problema de seguridad muy importante, ya que cualquier información que se encuentre en un dispositivo conectado a la red de comunicaciones o que viaje a través de ella, puede ser susceptible a ser detectada o interceptada por alguna persona no autorizada que puede utilizarla indebidamente, ocasionando grandes pérdidas económicas a las empresas o problemas personales. Por tal razón, es indispensable utilizar algún mecanismo que ayude a resguardar la información de algún ataque malicioso, uno de los más utilizados es la criptografía que se encarga de escribir en secreto, proporcionando confidencialidad a la información mediante un método de cifrado (Oppliger, 2005). El caos es el comportamiento de un sistema dinámico que cambia de manera irregular en el tiempo (Hilborn, 1999). Muchos métodos o esquemas de comunicación segura se han desarrollado para cifrar información basándose en sistemas discretos caóticos (Hossam *et al*., 2007; Pisarchik y Zanin, 2008; Pareek *et al*., 2005; Pisarchik y Flores, 2006; Ranjan y Saumitr, 2006). Esto se debe a la relación cercana que existe entre el caos y la criptografía; porque los sistemas caóticos tienen características como: ergodicidad, propiedades de mezcla, sensibilidad a los parámetros y las condiciones iniciales, que pueden considerarse análogos a las técnicas de difusión y confusión integrados en muchos sistemas criptográficos (Chong *et al*., 2011). Se desarrolló un sistema en el que se implementó una técnica que combina el comportamiento impredecible de la función logística con un código aritmético adaptativo, en el cual se usan la condición inicial y el parámetro del mapa caótico logístico como llave para cifrar y comprimir un archivo de texto, después se utiliza un canal inseguro para transmitir los datos codificados y un canal seguro para transmitir la llave (Ranjan y Saumitr, 2006). También se elaboró un algoritmo de llave simétrica para cifrar, mediante múltiples mapas caóticos unidimensionales y una llave externa de 128 bits, el texto plano se divide en 8 bits y se hacen grupos de bloques variables; después se cifra de forma secuencial usando los mapas caóticos de manera aleatoria (Pareek *et al*., 2005). También realizan un algoritmo basado en redes de mapas caóticos para cifrar imágenes de color mediante el mapa logístico; como llaves de cifrado se usan los parámetros, el tamaño de la imagen, un número de iteraciones y de ciclos (Pisarchik y Flores, 2006). Se desarrolló otro criptosistema para cifrar imágenes o videos, en él se normaliza el texto plano para utilizarlo como condición inicial de un mapa caótico (Pisarchik y Zanin, 2008). En otro estudio se creó un sistema para cifrar imágenes mediante un cifrado por bloques de 8 bits y una llave secreta externa alfanumérica o ASCII, de 256 bits de longitud. El cifrado de cada pixel de la imagen depende de la llave secreta, de la salida del mapa logístico y del pixel cifrado antes, lo que significa que al cifrar dos imágenes casi idénticas, una pequeña diferencia en la imagen puede ocasionar que el sistema genere imágenes cifradas muy diferentes (Hossam *et al*., 2007).

Pecora y Carroll, en 1990, demostraron que dos sistemas caóticos idénticos se pueden sincronizar mediante el acoplamiento de una señal común, es decir, cuando un sistema caótico maestro (emisor) se acopla a un sistema esclavo (receptor), los dos se sincronizan evolucionando en un atractor caótico donde el esclavo comienza a oscilar de igual forma que el maestro. Existen varias investigaciones que se basan en la sincronización caótica para codificar información, donde el emisor