ENCRIPTADOR DE IMÁGENES EN ESCALA DE GRISES CON LLAVES CAÓTICAS

BLAK AND WHITE IMAGE ENCRYPTION WITH CHAOTIC KEYS

Héctor Garcés Guzmán
Universidad Autónoma de Ciudad Juárez
hgarces@uacj.mx

Victor Manuel Hinostroza Zubia
Universidad Autónoma de Ciudad Juárez
vhinostr@uacj.mx

Priscila Betsabe Hernández Valadez
Universidad Autónoma de Ciudad Juárez
al131466@alumnos.uacj.mx

Resumen

Los avances tecnológicos del siglo XXI han proporcionado a la población con herramientas robustas para la distribución de la información. Hoy en día es más fácil y rápido compartir conocimiento de cualquier tipo, sin importar las distancias. Todo esto gracias a la red de computadoras que intercomunica al mundo entero; sin embargo, se presentó un problema importante, la seguridad de la información. Como respuesta a lo anterior, se han propuesto modelos de cifrado de imágenes que requieren de procesos diferentes de los actualmente utilizados, uno de estos es la utilización de llaves caóticas. El propósito de este artículo es dar a conocer los resultados de un proyecto de investigación donde se desarrolló un sistema de cifrado de imágenes en escala de grises en una Raspberry Pi a base de llaves caóticas, empleando múltiples mapas caóticos. Se evaluó su comportamiento mediante dos pruebas, histograma y entropía.

Palabras Claves: Caos, encriptación, telecomunicaciones.

Abstract

The technological advances of the 21st century have provided the population with robust tools for information distribution. Nowadays, it is easier and faster to

share knowledge of any kind, regardless of distance. All this thanks to the computer network that interconnects the whole world; however there was a major problem, information security. In response to the above, have been proposed models of image encryption that require different processes from those currently used, one of these is the use of chaotic keys. The purpose of this article is to present the results of a research project where an encryption system of grayscale images was developed in a Raspberry PI based on chaotic keys, using multiple chaotic maps. Their behavior was evaluated by two tests, histogram and entropy.
Keywords: *Chaos, encrytion, telecommunications.*

1. Introducción

Una de las bases de la ciencia es la relación que se busca entre causa y efecto. Es posible predecir la ocurrencia de ciertos fenómenos naturales gracias a las leyes establecidas con las que se describe su comportamiento. El desarrollo del cálculo por Isaac Newton aceleró el avance de las ciencias. Aportó la herramienta base para el desarrollo de sistemas y fórmulas utilizadas en la representación de los fenómenos naturales. Una de las características de la época Newtoniana era el determinismo. Este principio establecía que el estado presente de cierto sistema era la consecuencia del estado anterior y la causa del estado futuro. La única dificultad presente para pronosticar los estados era recopilar suficiente información [Bonev, 1995].

Con las leyes de Newton y el cálculo diferencial como herramienta, los científicos comenzaron a buscar ecuaciones que explicaran y describieran los fenómenos naturales, encontrando un orden en el universo. Sin embargo, existen fenómenos que son complicados de describir matemáticamente, normalmente no lineales y por ende es difícil predecir su estado futuro a largo plazo. El ejemplo por excelencia de estos fenómenos naturales es el estado del tiempo. Cuando se habla de él se le considera impredecible y aleatorio, pues aparentemente no existe en su comportamiento una relación clara entre causa y efecto. Por lo contrario, el clima de una región es estable y predecible. Inicialmente se creyó que la imprevisibilidad del estado del tiempo era debido a falta de información precisa, sin embargo,

algunas de las conclusiones de la teoría del caos proveen otro punto de vista para este aparente problema. Pues se propone que los sistemas deterministas simples, incluso con pocos elementos, pueden presentar un comportamiento aleatorio que no desaparece con obtener más información del sistema. Esta aparente aleatoriedad es llamada caos [Broer, 2009].

Actualmente los científicos se refieren como caóticos a aquellos sistemas con movimientos complicados no aleatorios que presentan un crecimiento rápido de error. Para estos sistemas, a pesar de ser de carácter determinista, es imposible hacer predicciones acertadas a largo plazo del estado del sistema. Por lo contrario, a corto plazo es posible estimar su valor con una buena certeza. Dentro de la definición de caos la dependencia sensible hacia las condiciones iniciales juega un papel importante en el crecimiento del error y en la imposibilidad de predecir el estado futuro del sistema [Stewart, 2007]. La confidencialidad de la información siempre ha sido importante, esto con el fin de asegurar que únicamente la persona adecuada tenga acceso al mensaje. Por consiguiente, el cifrado de mensajes siempre ha sido una importante área de estudio. La ciencia encargada de estudiar, diseñar y crear algoritmos para cifrar información se conoce como criptografía. Su contraparte es el criptoanálisis, la ciencia encargada de estudiar y romper la encriptación, es decir, encontrar la llave del algoritmo aplicado a la información para tener acceso al mensaje original. Al conjunto de estas dos ciencias se le llama Criptología. Los algoritmos de encriptado para la seguridad de un sistema de comunicaciones deben tener como punto fuerte la llave y no tanto el proceso usado para el cifrado. En consecuencia, hay una gran demanda por explorar nuevas técnicas y herramientas en el desarrollo de llaves, como puede ser el caso de las señales caóticas. En particular porque éstas destacan por tener varias propiedades como: ergodicidad, amplio ancho de banda, comportamiento pseudo aleatorio, alta sensibilidad a las condiciones iniciales y atractores.

2. Métodos

Algunos sistemas no lineales deterministas bajo ciertas condiciones pueden generar una señal que presenta un comportamiento estocástico, a pesar de que

su naturaleza es esencialmente determinista. Se han observado estos sistemas en áreas de estudio tan dispares como: biología, física, química, matemáticas, economía, meteorología, geología, ingeniería, etc. Un oscilador caótico discreto y unidimensional se define como una función no lineal iterativa o de mapeo $f: \phi \rightarrow \phi$ que puede ser escrita como se muestra en la ecuación 1.

$$\phi_{(k+1)} = f(\phi_k) \tag{1}$$

En numerosos sistemas no lineales dinámicos discretos unidimensionales se ha observado un comportamiento caótico; en particular en la tabla 1 se muestra la definición matemática de los mapas considerados para el análisis reportado en este documento [Garces, 2016].

Tabla 1 Mapas caóticos.

Mapa	Definición	Régimen caótico
Bernoulli	$\phi_{(k+1)} = \begin{cases} B\phi_k + A & \phi_k < 0 \\ B\phi_k - A & \phi_k > 0 \end{cases}$	$\phi_k \in [-A, A] \quad 0 < B < 2$
Chebyshev	$\phi_{(k+1)} = \cos(B\ arccos(\phi_k))$	$\phi_k \in [-1,1] \quad 1 < B < 10$
Coseno	$\phi_{(k+1)} = A\cos(\phi_k + B)$	$\phi_k \in [-A, A]$ $2 < A < 10$ ó $-\pi < B < \pi$
Cuadrático	$\phi_{(k+1)} = B - (A\phi_k^2)$	$\phi_k \in \left[-\frac{2}{A}, \frac{2}{A}\right] \quad \frac{3}{4} < AB < 2$
Cúbico 1	$\phi_{(k+1)} = C(3\phi_k - 4\phi_k^3)$	$\phi_k \in [-C, C] \quad 0 < C < \infty$
Exponencial	$\phi_{(k+1)} = \phi_k \exp(B(A - \phi_k))$	$\phi_k \in [0, \frac{\exp(AB-1)}{B}]$ $AB > 2$
Hopping	$\phi_{(k+1)} = \begin{cases} D(\phi_k - A) + C & \phi_k > A \\ B\phi_k & \lvert\phi_k\rvert \le A \\ D(\phi_k + A) - C & \phi_k < -A \end{cases}$	$\phi_k \in [-C, C]$ $B, -D > 1 \quad C = BA$
Logístico	$\phi_{(k+1)} = B(A^2 - \phi_k^2) - A$	$\phi_k \in [-A, A]$ $\frac{3}{2} < AB < 2$
Tienda	$\phi_{(k+1)} = A - B\lvert\phi_k\rvert$	$\phi_k \in [A(1-B), A]$ $0 < B < 2$

A pesar de que las funciones mostradas en la tabla 1 son deterministas, poseen características peculiares. Una manera de observar su comportamiento es variar el valor de los parámetros constantes (A, B, etc.) dentro de un rango

predeterminado, como resultado se obtiene el denominado diagrama de bifurcación. Particularmente para el mapa coseno, en la figura 1 se ilustra su evolución al variar el parámetro A en el rango de [1.5 3]. En esta grafica claramente se distinguen dos regiones, en la primera por ejemplo para $A = 1.7$ el resultado de todas las iteraciones siempre es el mismo $\phi(k) = \pm 1.5$, esto es dentro de la zona determinista. Por lo contrario, para $A = 2.25$ el resultado de cada iteración varia en un rango aproximado de $\phi(k) \in [-2.2 \;\; 2.2]$, esta es un área de operación caótica. Un análisis cuidadoso de la figura 1 muestra una alternancia o bifurcación entre regiones caóticas y deterministas.

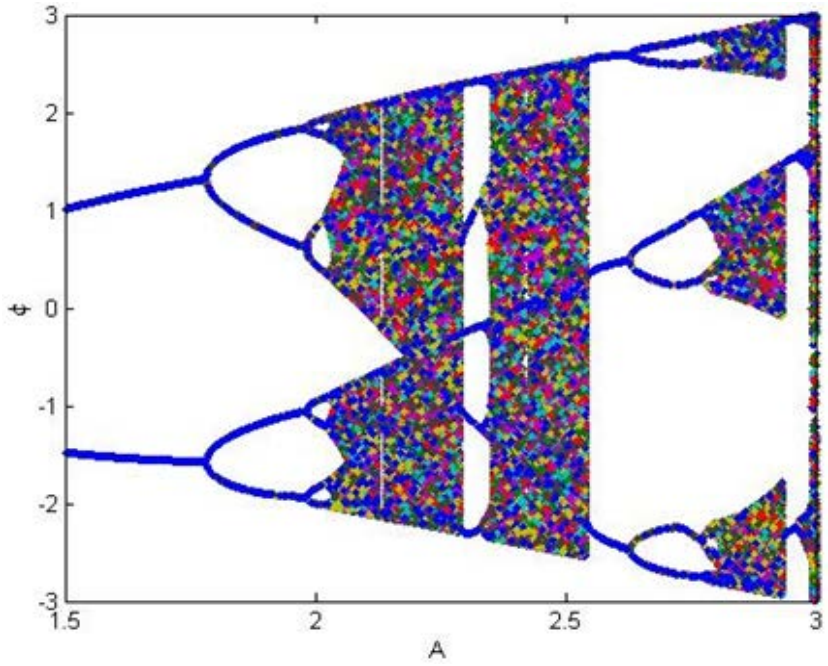


Figura 1 Diagrama de bifurcación del mapa coseno.

El diseñó del encriptador digital tiene como elemento esencial del proceso al operador booleano XOR para la adición de la llave cifradora a la imagen original. Esto se puede observar en el diagrama presentado en la figura 2. Para realizar su implementación la opción más viable fue la Raspberry Pi, por las siguientes razones: procesador de cuatro núcleos, memoria RAM de la que dispone, puertos con los que cuenta, capacidad de procesamiento que ofrece y el software que la controla. Estas especificaciones técnicas junto con el poder de procesamiento de

la tablilla se consideraron suficientes para la ejecución correcta y rápida del sistema de encriptación.

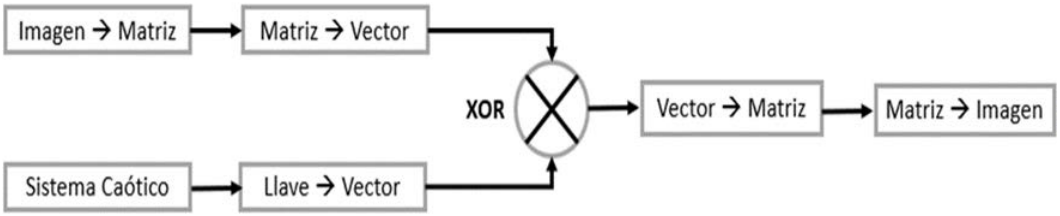


Figura 2 Encriptador digital de imágenes.

Se recurrió a la programación modular utilizando el lenguaje Python en su versión 3.6. En este caso, con la finalidad de facilitar la implementación del algoritmo, buscando hacerlo de una forma clara, definiendo secciones de código para funcionalidades específicas y repetitivas durante el proceso. Los archivos de código fuente se organizaron en dos secciones, la primera abarcando los scripts para la generación de las llaves caóticas, siendo un script por sistema caótico, la segunda sección se conformó por un script principal encargado de llamar a los scripts de las llaves caóticas y del proceso de encriptación. También se incluyó una sección de scripts para la definición de variables, tales como los directorios en los que se almacenaron las imágenes, así como los valores iniciales que se tomaron de las zonas caóticas de los sistemas. La estructura del contenido de estos scripts es similar en todos los casos analizados en este proyecto, el proceso total se ilustra en la figura 3.

3. Resultados

Para obtener una cantidad significativa de muestras para el análisis del algoritmo se seleccionaron tres imágenes distintas en escala de grises: eight, logo y Lena. Estas figuras son empleadas normalmente en el procesamiento de imágenes y están incorporadas en casi todas las librerías de los paquetes de software, por ejemplo, Matlab incluye las dos primeras. A ellas se les aplicaron cada una de las llaves caóticas, por sistema y por parámetro. Estas imágenes de prueba difieren en dos aspectos; tamaño y entropía.

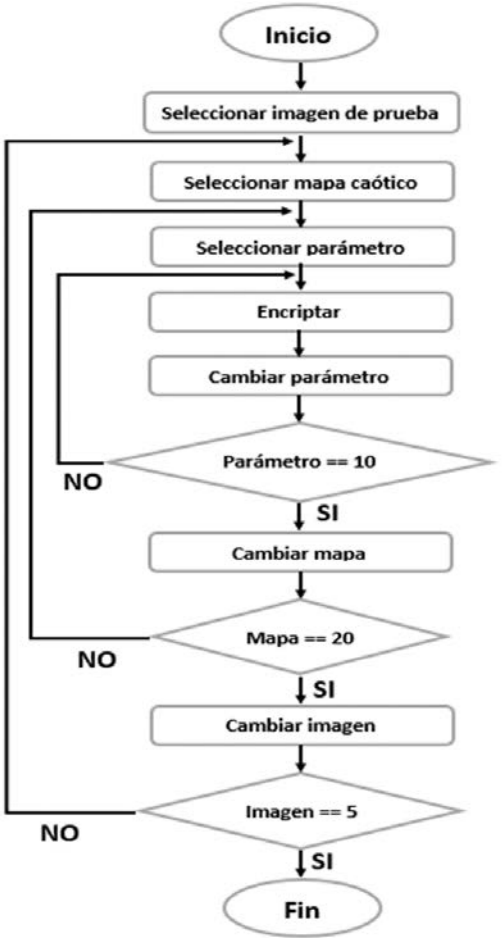


Figura 3 Diagrama de flujo del algoritmo de encriptación.

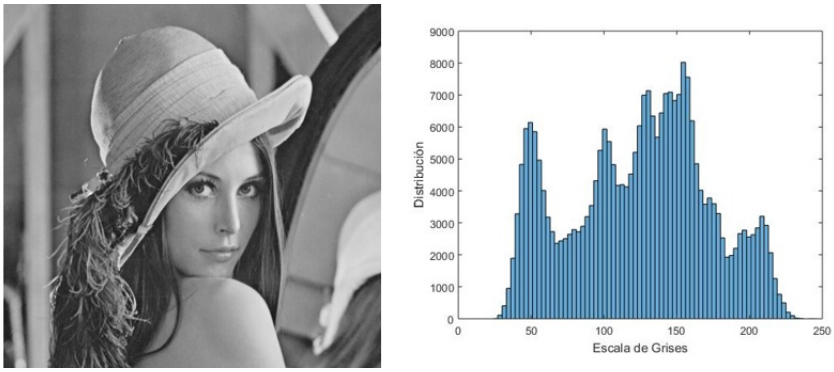
En la tabla 2 se resumen estas características. Además, con la finalidad de analizar las fortalezas que presentan cada uno de los sistemas caóticos utilizados, se variaron los parámetros del mapa considerando valores que permitan la operación en la zona caótica.

Tabla 2 Características principales de las imágenes de prueba.

Imagen	Tamaño en pixeles	Entropía
eight.tif	242x308	4.8796
lena.bmp	512x512	7.4455
logo.tif	107x122	1

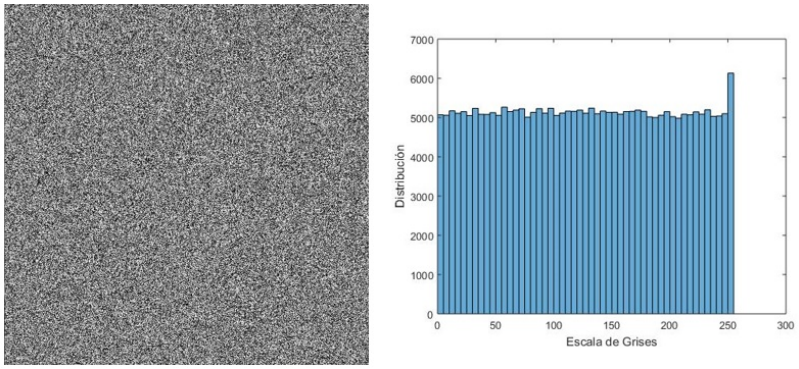
Para este proyecto se consideraron adecuadas dos pruebas en las que se analizó el contenido de las imágenes de salida del sistema encriptador. El histograma fue

la primera evaluación realizada esperando conocer la distribución de probabilidad de los valores de los pixeles. Para continuar, se tomó en cuenta la entropía como un parámetro útil y necesario para conocer el desorden contenido en la imagen, antes y después de la encriptación. En la figura 4 se puede apreciar como los valores de los pixeles para la imagen de Lena varían dentro del rango posible para la escala de grises, presentando picos en los valores más recurrentes y depresiones en los que no son tan comunes. En cambio, en la figura 5, se exhibe la imagen de Lena encriptada con una llave basada en el sistema tienda y su histograma. Lo que se observó en todos los histogramas de las imágenes encriptadas fue una distribución de probabilidad casi uniforme de valores en la escala de grises. Del contenido de estos histogramas no es posible obtener información concreta de la imagen original gracias a la distribución uniforme, confirmando la eficacia del proceso de cifrado al que fue sometida.



a) Lena. b) histograma.

Figura 4 Lena original.



a) Lena. b) histograma.

Figura 5 Lena encriptada.

Para continuar con el análisis de las imágenes encriptadas se calculó su valor de entropía. Con la obtención de estos valores se determinó el desorden existente en el valor de los pixeles. Para lograr una mayor comprensión de la diferencia existente entre la entropía calculada en la imagen original a la obtenida en la encriptada se compararon estos valores en las tablas 3, 4 y 5. Si se analizan primero los valores de entropía ilustrados en la tabla 2 de las imágenes originales se detectan variaciones considerables entre ellos. Por ejemplo, una imagen simple como logo tiene una entropía baja, en cambio Lena es una imagen con muchos contrastes dando como resultado que su entropía sea alta. Al continuar comparando ahora las imágenes encriptadas es posible observar como los valores de entropía son muy similares entre sí, independientemente si provienen de valores iniciales distintos, de sistemas caóticos diferentes o incluso de diferentes imágenes. Como se puede observar todos los datos obtenidos están cerca del valor máximo de entropía; que es ocho.

Tabla 3 Entropía de la imagen eight.

	eight.tif	
Sistema	**Original**	**Encriptada**
Bernoulli	4.8796	7.99363618
Chebyshev	4.8796	7.99445732
Congruente	4.8796	7.99468391
Coseno	4.8796	7.9943531
Cúbico 1	4.8796	7.99551106
Exponencial	4.8796	7.99359114
Hopping	4.8796	7.9944538
Logístico	4.8796	7.99426404
Tienda	4.8796	7.99488021

Tabla 4 Entropía de la imagen Lena.

	lena.bmp	
Sistema	**Original**	**Encriptada**
Bernoulli	7.4455	7.99910979
Chebyshev	7.4455	7.99926031
Congruente	7.4455	7.99936243
Coseno	7.4455	7.99927294
Cúbico 1	7.4455	7.99923364
Exponencial	7.4455	7.99913019
Hopping	7.4455	7.99924383
Logístico	7.4455	7.99918969
Tienda	7.4455	7.99927253

Tabla 5 Entropía de la imagen logo.

	logo.tif	
Sistema	**Original**	**Encriptada**
Bernoulli	1	7.9591309
Chebyshev	1	7.95530339
Congruente	1	7.9596725
Coseno	1	7.95750567
Cúbico 1	1	7.95355538
Exponencial	1	7.95413802
Hopping	1	7.95273317
Logístico	1	7.95706527
Tienda	1	7.95391654

4. Discusión

A partir de este trabajo es posible continuar con la investigación acerca del caos como una opción para la encriptación de información digital. En el caso específico de las imágenes, se considera como posible trabajo futuro el diseño y desarrollo de un sistema de encriptación para imágenes a color, las cuales presentan una estructura diferente a las compuestas por escala de grises, que se utilizaron en este proyecto. También podrían tomarse en cuenta sistemas caóticos no contemplados en esta investigación, como son los de más de una dimensión. Aquí se estaría buscando analizar la eficacia de las nuevas llaves cifradoras, por consiguiente, se tendría un panorama más amplio.

Considerando los resultados la encriptación de imágenes usando llaves que provengan de un sistema caótico es una manera relativamente simple y barata de encriptar imágenes, con hardware y software de uso común y fácilmente accesible. Los resultados demuestran también que la imagen encriptada aumenta su entropía casi a su límite máximo, sin aumentar excesivamente el tiempo de procesamiento y costo.

5. Conclusiones

En este proyecto se diseñó y construyó un encriptador de imágenes que emplea llaves caóticas, con el algoritmo de cifrado implementado en Python utilizando como plataforma la Raspberry Pi 3. Como sujetos de prueba se seleccionaron tres imágenes en escala de grises, y como resultado de la ejecución del proceso de

encriptación se obtuvieron cerca de quinientas imágenes cifradas. Para comprobar la efectividad del proceso de cifrado, las imágenes encriptadas se sometieron a dos diferentes análisis el histograma y su entropía.

Tomando en cuenta los resultados obtenidos de las pruebas realizadas, se puede concluir que la mayoría de los sistemas caóticos seleccionados para la implementación del encriptador son eficaces. El rendimiento que presentaron como generadores de llaves de cifrado para imágenes fue apropiado al presentar valores satisfactorios en las pruebas.

Como trabajo futuro se podrían implementar estos algoritmos en imágenes en tonos de gris o a color, usando llaves generadas con otros sistemas caóticos e implementados en hardware y software con otras características.

6. Bibliografía y Referencias

[1] Bonev Ivan Ivanov, La Teoría del caos, Primera. Buenos Aires: Rundinuskín, 1995.

[2] Broer Henk, Takens Floris, Dynamical Systems and Chaos, vol. 139. New York: Springer, 2009.

[3] Chen Guanrong, Mao Yaobin, Chui Charles K., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons and Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[4] Espinoza Illanes, Marcos, Cifrado de imágenes digitales basado en teoría del caos: mapas logísticos, Tesis maestría, pp. 1–20, 2014.

[5] Gao, T. G. y Chen, Z. Q, A new image encryption algorithm based on hyper chaos. Physics Letters A, 372(4): 394–400, 2008.

[6] Isabelle Steven. H., A Signal Processing Framework for the Analysis and Application of Chaotic Systems, Ph.D. Dissertation, Massachusetts Institute of Technology (MIT), Cambridge, MA, May 1995.

[7] Garcés Guzmán Héctor, Hinostroza Zubía Victor Manuel, Peña Alarcón Deana Larisa, Enríquez Edwin Antonio, Modificaciones en la rapidez de sincronización por sistemas acoplados de señales caóticas unidimensionales, Congreso Internacional de Investigación Tijuana, Revista

Aristas: Investigación Básica y Aplicada, Tijuana, BC., Vol. 5, Núm. 9, pp. 38 - 42, febrero 2016.

[8] Garcés Guzmán Héctor, Hinostroza Zubía Victor Manuel, Priscila Betsabe Hernández Valadez, Estudio de la estructura estadística de las señales caóticas, Congreso Internacional de Investigación Tijuana, Revista Aristas: Investigación Básica y Aplicada, Marzo 2017, Tijuana, BC., Vol. 6, Núm. 11, pp. 150–154.

[9] Madrid Casado Carlos M., Historia de la Teoría del Caos contada para escépticos: Cuestiones de génesis y estructura, Encuentros Multidisciplinarios., pp. 1–15, 2010.

[10] Peitgen Heinz-Otto, Hartmut Jürgens Dietmar Saupe, Chaos and Fractals, Second. New York: Springer, 2004.

[11] Smart Nigel Paul, Cryptography: An Introduction, New York: McGraw Hill, 2010.

[12] Stewart Ian, Historia de las matemáticas en los últimos 10000 años. España: Crítica, 2007.