EVALUACIÓN DE LLAVES CAÓTICAS EN LA ENCRIPTACIÓN DE IMÁGENES EN ESCALA DE GRISES

CHAOTIC KEYS EVALUATION FOR BLAK AND WHITE IMAGE ENCRYPTION

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

Víctor Manuel Hinostroza Zubia
Universidad Autónoma de Ciudad Juárez, México
vhinostr@uacj.mx

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

Recepción: 21/octubre/2019 **Aceptación:** 2/diciembre/2019

Resumen

La próxima generación de sistemas de telecomunicación enfrentará grandes retos como: conexión masiva de dispositivos, tiempo de retardo extremadamente bajo, menor consumo de energía, etc. Entre ellos destaca la seguridad en el intercambio de información, se han propuesto modelos de cifrado de imágenes en escala de grises que requieren de procesos diferentes a los actuales, como la utilización de claves caóticas. Este escrito tiene la finalidad de exponer los frutos del análisis de veinte llaves caóticas, desarrolladas usando modelos discretos unidimensionales. Se valoró su capacidad de encriptación mediante las siguientes herramientas estadísticas de prueba: histograma, distribución de valores de pixeles vecinos, entropía y correlación de pixeles. El desempeño que presentaron las mil imágenes examinadas fue satisfactorio en todas las pruebas a las que se sometieron, con la excepción de los mapas caóticos cuadrático y logístico modificado, que rindieron pobremente en la evaluación de la entropía y correlación de pixeles respectivamente.

Palabras Claves: Caos, encriptación, telecomunicaciones.

Abstract

The next generation of telecommunication systems will face significant challenges, such as: massive device connectivity, very low latency, less energy consumption, etc. Among them, secure information transfer stands out. In this context, models have been proposed for encryption of black and white images that require different processes than those currently used, one of which is the use of chaotic keys. This paper has the purpose of exposing the results of the analysis of twenty chaotic keys, developed using one-dimensional discrete models. Its encryption ability was assessed using the following statistical test tools: histogram, entropy, correlation and distribution of neighboring pixel values. The performance of one thousand images examined was satisfactory in all the tests they underwent, with the exception of quadratic and modified logistic maps, which performed poorly in the evaluation of entropy and pixel correlation, respectively.

Keywords**:** *Chaos, encrytion, telecommunications.*

1. Introducción

Un principio científico es encontrar la relación entre causa y efecto, y a través de esta conexión predecir el comportamiento de los fenómenos naturales. Isaac Newton aportó una herramienta básica para la comprensión de ciertos eventos que ocurren en la naturaleza. Debido a esto, y empleando cálculo diferencial es posible establecer que el estado presente de cierto sistema es la consecuencia del estado anterior y la causa del estado futuro. La única dificultad presente para pronosticar los estados es recopilar suficiente información [Bonev, 1995].

No obstante, existen fenómenos que son complicados de describir matemáticamente, el ejemplo por excelencia es el estado del tiempo. Cuando se le describe se considera impredecible a largo plazo y con un comportamiento aleatorio. En otras palabras, no existe una relación clara entre causa y efecto, su rareza es que, si una de las variables llegara a tener una alteración microscópica esto conlleva a cambios a gran escala en su evolución en el tiempo. Actualmente estos fenómenos naturales aparentemente aleatorios, se les denomina caóticos a pesar de ser deterministas [Stewart, 2007].

El siguiente punto a considerar es la nueva ola tecnológica, la cual ha proporcionado a la población herramientas robustas para la distribución de la información. En efecto, día a día es más fácil y rápido compartir conocimiento de cualquier tipo, sin importar la distancia o alguna limitación física. La existencia de la Internet ha traído consigo una evolución en la forma en que la sociedad se comunica, dándole un papel fundamental a las imágenes. Para la sociedad la confidencialidad de la información siempre ha sido esencial, por consiguiente, el cifrado de mensajes es una importante área de estudio debido a los requerimientos de invulnerabilidad. Por ende, se requiere de métodos que aseguren la privacidad del mensaje transmitido, es decir, que la información enviada sólo sea conocida por el destinatario y que permanezca oculta a cualquier otra entidad que intente tener acceso. Como respuesta a este problema, en la encriptación electrónica se han propuesto métodos de cifrado de imágenes que requieren de procesos diferentes de los actualmente utilizados. Uno de estos métodos, el cual destaca por su innovación y alta seguridad es la utilización de llaves caóticas, obtenidas a partir de sistemas caóticos. Estas destacan por tener varias propiedades como: ergodicidad, amplio ancho de banda, comportamiento pseudo aleatorio y alta sensibilidad a las condiciones iniciales [Broer, 2009]. Los algoritmos de encriptado para la seguridad de un sistema de comunicaciones deben tener como punto fuerte la clave y no tanto el proceso usado para el cifrado.

En cuanto al uso de llaves caóticas en la encriptación en otro tipo de información, por ejemplo, se han desarrollado aplicaciones en el reconocimiento de voz [Rodriguez, 2018].

2. Métodos

El problema de los tres cuerpos consiste en calcular en cualquier instante su posición y velocidad cuando están sometidos a la atracción gravitacional mutua. A finales del siglo XIX, Henri Poincaré como respuesta a este enigma llegó a la conclusión que la interacción de más de dos cuerpos celestes, presenta un comportamiento aparentemente aleatorio. Por consiguiente, no es posible hacer predicciones de su comportamiento. Con esto Poincaré encontró que 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. Debido a esto, el conocimiento que pueda tenerse de éstos es siempre impreciso [Espinosa, 2014]. Este fue el primer paso en el descubrimiento de lo que ahora se llama sistemas caóticos. Un oscilador caótico discreto y unidimensional se define como una función no lineal iterativa o de mapeo $f:\phi \to \phi$ que puede ser escrita con ecuación 1.

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

Hay un gran número de sistemas en los cuales se ha observado un comportamiento caótico; en particular en la tabla 1 se muestra la definición matemática y la región caótica de los veinte mapas contemplados para este estudio [Garces, 2018].

Tabla 1 Mapas caóticos.

Mapa	Definición	Régimen caótico
Bernoulli	$\varphi_{(k+1)} = \begin{cases} B\varphi_k + A & \varphi_k < 0 \\ B\varphi_k - A & \varphi_k > 0 \end{cases}$	$\varphi_k \in [-A, A]$ $0 < B < 2$
Bernoulli shift 3	$\varphi_{(k+1)} = \mathrm{mod}((A \cdot \varphi_k), 1)$	
Bernoulli shift 4	$\varphi_{(k+1)} = 1 - \mathrm{mod}((A \cdot \varphi_k), 1)$	
Chebyshev	$\varphi_{(k+1)} = \cos(B\ arccos(\varphi_k))$	$\varphi_k \in [-1, 1]$ $1 < B < 10$
Congruente	$\varphi_{(k+1)} = \begin{cases} B\varphi_k - C & \varphi_k > A \\ B\varphi_k & \lvert\varphi_k\rvert \le A \\ B\varphi_k + C & \varphi_k < -A \end{cases}$	$\varphi_k \in [-C, C]$ $1 < B < 2$ $C = 2A$
Coseno	$\varphi_{(k+1)} = A\cos(\varphi_k + B)$	$\varphi_k \in [-A, A]$ $2 < A < 10$ ó $-\pi < B < \pi$
Cuadrático	$\varphi_{(k+1)} = B - (A\varphi_k^2)$	$\varphi_k \in \left[-\frac{2}{A}, \frac{2}{A}\right]$ $\frac{3}{4} < AB < 2$
Cúbico 1	$\varphi_{(k+1)} = C(3\varphi_k - 4\varphi_k^3)$	$\varphi_k \in [-C, C]$ $0 < C < \infty$
Cúbico 2	$\varphi_{(k+1)} = (1 - C)\varphi_k + C\varphi_k^3$	$\varphi_k \in \left[-\frac{3-2c}{3\sqrt{3}}, \frac{3-2c}{3\sqrt{3}}\right]$ $-\infty < C < 3/2$
Cúbico 3	$\varphi_{(k+1)} = C(\varphi_k - \varphi_k^3)$ $= C\varphi_k(1 - \varphi_k^2)$	$\varphi_k \in \left[-\frac{2c}{\sqrt{3}}, 0\right]$ $0 < C < 2.6$

Mapa	Definición	Régimen caótico
Exponencial	$\varphi_{(k+1)} = \varphi_k \exp(B(A - \varphi_k))$	$\varphi_k \in [0, \frac{\exp(AB-1)}{B}]$ $AB > 2$
Hopping	$\varphi_{(k+1)} = \begin{cases} D(\varphi_k - A) + C & \varphi_k > A \\ B\varphi_k & \lvert\varphi_k\rvert \le A \\ D(\varphi_k + A) - C & \varphi_k < -A \end{cases}$	$\varphi_k \in [-C, C]$ $B, -D > 1\ C = BA$
Logístico	$\varphi_{(k+1)} = B(A^2 - \varphi_k^2) - A$	$\varphi_k \in [-A, A]$ $\frac{3}{2} < AB < 2$
Logístico bipolar	$\varphi_{(k+1)} = 1 - \mu\varphi_k^2$	$\mu \in (0, 2]$ $\varphi_k \in [1 - \mu, 1]$
Logístico modificado	$\varphi_{(k+1)} = \lambda\varphi_k(1 - A\varphi_k)$	$\lambda \in (0, 4], A > 1$ $\varphi_k \in [0, \lambda/4k]$
Sinusoidal 1	$\varphi_{(k+1)} = C\sin(\pi\varphi_k)$	$\varphi_k = [0, C]$ $0 < C < 1$
Tienda	$\varphi_{(k+1)} = A - B\lvert\varphi_k\rvert$	$\varphi_k \in [A(1 - B), A]$ $0 < B < 2$
Tienda Bipolar	$\varphi_{(k+1)} = \frac{1 + C^2 - 2C\varphi_k - 2\lvert\varphi_k - C\rvert}{1 - C^2}$	$C \in (-2, 2)$ $\varphi_k \in [-1, 1]$
Tienda Oblicuo	$\varphi_{(k+1)} = \frac{C + \varphi_k(1 - 2C) - \lvert\varphi_k - C\rvert}{2C(1 - C)}$	$C \in (-2, 2)$ $\varphi_k \in [0, 1]$
Tienda Simétrico	$\varphi_{(k+1)} = \beta(1 - \lvert\varphi_k\rvert) - 1$	$\beta \in [0, 2]$ $\varphi_k \in [-1, \beta - 1]$

Si bien las funciones mostradas en la tabla 1 son deterministas, poseen características singulares. Una manera de darse cuenta de ese peculiar comportamiento es variar el valor de algún parámetro de la función de mapeo dentro de un rango especifico, por consiguiente, se obtiene el denominado diagrama de

bifurcación. Mitchell Jay Feigenbaum presentó en 1975 el primer mapa de bifurcación, mostrado en la figura 1, que pertenece al sistema caótico logístico.

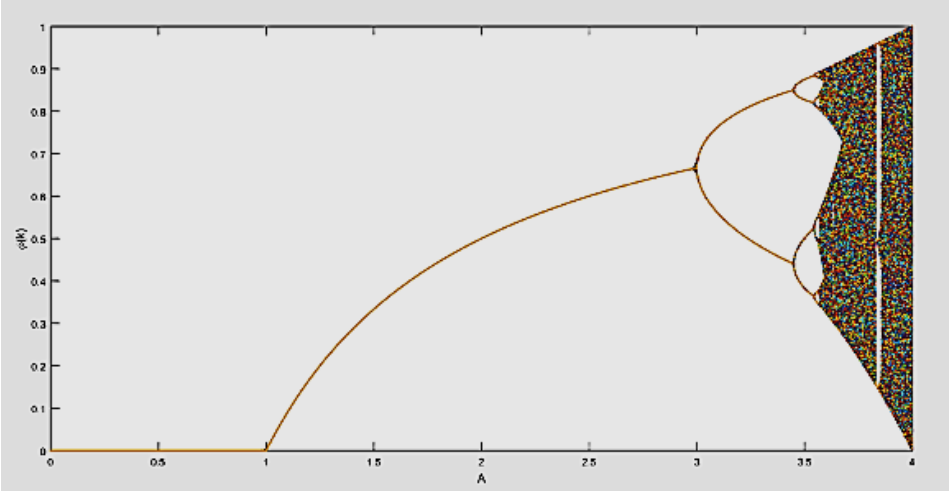


Figura 1 Diagrama de bifurcación del mapa logístico.

Una bifurcación ocurre cuando se varía un parámetro de control al sistema dinámico modificando así su comportamiento (figura 1), para llegar a un punto crítico ocasionando la pérdida de estabilidad del sistema [Peitgen, 2004]. En este diagrama se aprecia que después de una bifurcación se tiene un comportamiento aleatorio, con valores sin repeticiones, pero que siempre están acotados por rangos específicos [Ives, 2004]. Es decir, a pesar de que el caos está relacionado con el desorden, la confusión o lo impredecible, el diagrama de bifurcación muestra que el caos tiene fronteras.

Con respecto al proceso de encriptación de imágenes y su posterior análisis en primer lugar, se construyó un cifrador en una Raspberry Pi a continuación, los datos obtenidos fueron estudiados mediante el software Matlab. Se seleccionó la Raspberry pi por: su bajo costo, su lenguaje de programación de alto nivel Python y porque tiene una considerable potencia computacional en una superficie no mayor que una tarjeta de crédito. En particular, Python es un lenguaje para scripts, no tiene la necesidad de un compilador en sí y la sintaxis es más sencilla. Debido a esto, es muy atractivo para un rápido desarrollo de aplicaciones [Donat, 2005]. El diseñó del encriptador digital utiliza un sencillo algoritmo como el presentado en [Inzunza,

2012] y tiene como elemento esencial del proceso al operador booleano XOR para la adición de la llave cifradora a la imagen original.

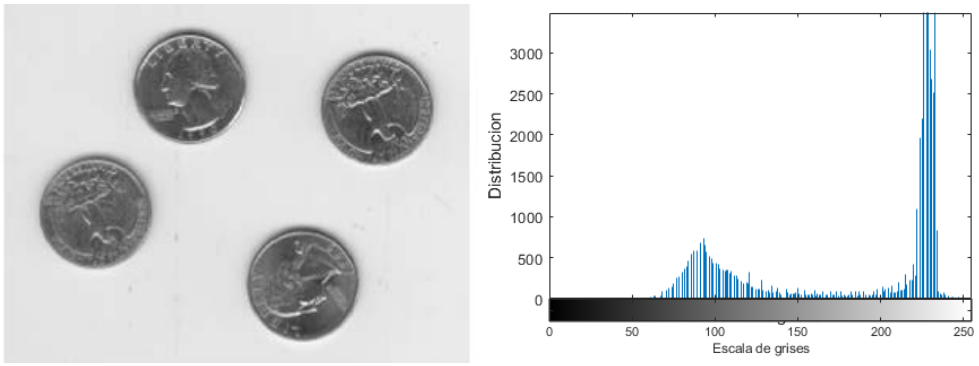
3. Resultados

Con el propósito de realizar un análisis exhaustivo de las veinte llaves caóticas se seleccionaron cinco figuras comúnmente empleadas en el procesamiento de imágenes: cell, circbw, eight, Lena y logo. Estas difieren en dos aspectos; tamaño y entropía, en la tabla 2 se especifican sus características. Además, se eligió variar un parámetro de control de cada uno de los veinte mapas, es decir uno de los parámetros de su definición mostrada en la tabla 1. Hay que destacar que el rango de variación del parámetro de control está dentro de la región de operación caótica. Combinando las cinco figuras, los veinte mapas y la variación del parámetro de control se obtuvieron más de mil imágenes cifradas. Esta es una cantidad significativa de muestras requeridas con la finalidad de evaluar la habilidad de encriptación de las llaves bajo estudio. En este escrito se reporta el valor medio de cada una de las siguientes herramientas estadísticas, a las que se sometieron las mil imágenes: histograma, distribución de valores de pixeles vecinos, entropía y correlación de pixeles.

Tabla 2 Características principales de las imágenes de prueba.

Imagen	Tamaño en pixeles	Entropía
cell.tif	159x91	4.6024
circbw.tif	280x272	0.9996
eight.tif	242x308	4.8796
lena.bmp	512x512	7.4455
logo.tif	107x122	1

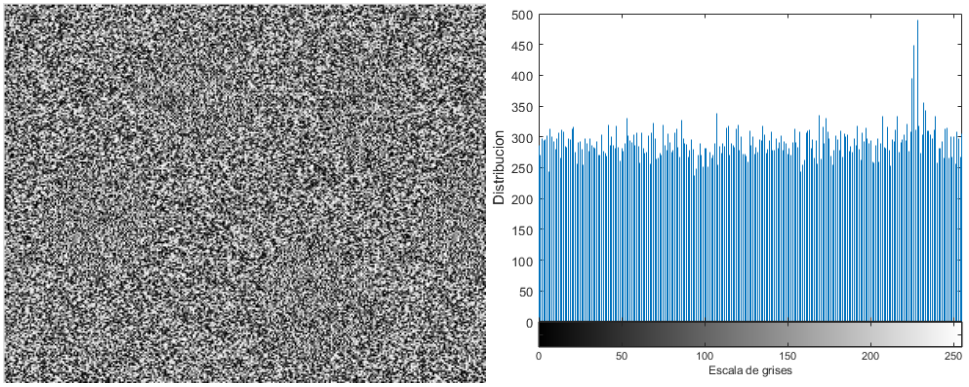
El histograma es un método muy útil para representar de una manera organizada un conjunto de datos. Por ende, su uso puede corroborar analíticamente la diferencia existente entre la imagen original y la encriptada. En la figura 2 se puede apreciar como los valores de los pixeles para la imagen de eight varían dentro del rango posible para la escala de grises, presentando dos picos en los valores más recurrentes de la escala de grises.



a) Eight original *b) Histograma*

Figura 2 Eight original e Histograma.

Por lo contrario, en la figura 3 se exhibe la imagen de eight encriptada con una llave basada en el sistema Hopping y su histograma. Esta representación gráfica semeja una pdf uniforme, note la casi ausencia de crestas y valles. Del histograma se puede inferir que no es posible obtener información concreta de la imagen original a partir de la cifrada, gracias a la distribución uniforme. En la mayoría de los mil casos examinados se observó una distribución de probabilidad casi uniforme de valores en la escala de grises, confirmando la eficacia del proceso de cifrado.

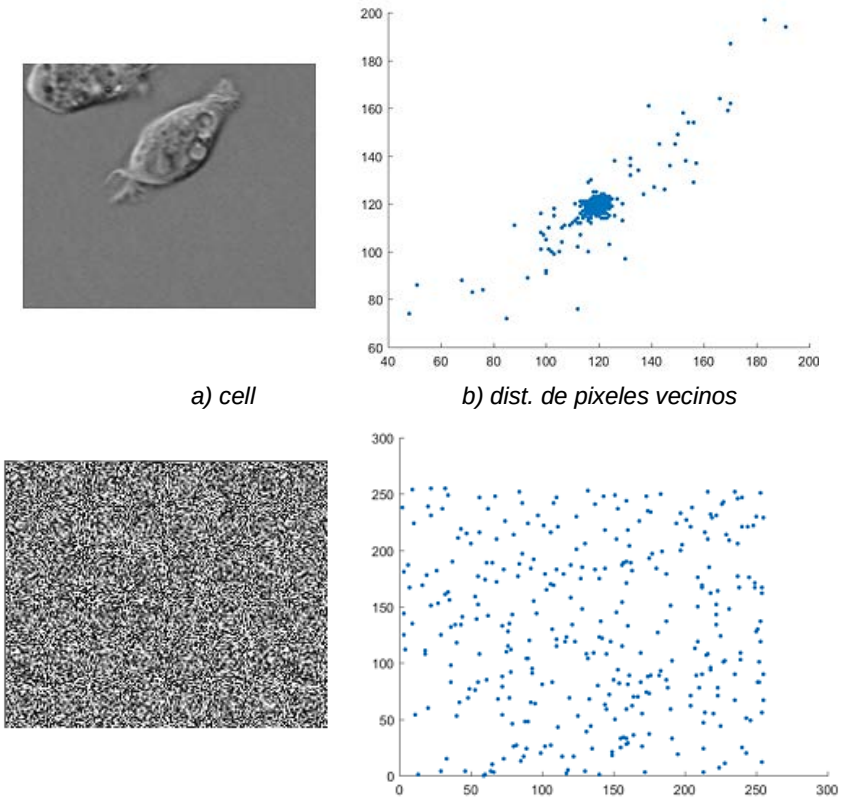


a) Eight encriptada *b) Histograma de eight encriptada*

Figura 3 Eight encriptada, Histograma de eight encriptada.

Más adelante, para observar de manera gráfica la distribución de valores de pixeles vecinos se recurrió al empleo de un plano cartesiano como herramienta de análisis. Cada punto en el esquema se obtuvo de la siguiente manera; en el eje horizontal del plano se consideró el valor en la escala de grises de un pixel ubicado en la

imagen en las coordenadas [x, y], mientras que en el eje vertical se usó el valor del pixel contiguo localizado en [x, y+1]. Como resultado, en la figura 4 b) es posible apreciar como la concentración de valores de la imagen cell es más densa en una línea recta con pendiente uno, lo que indica la existencia de alta redundancia entre pixeles adyacentes. Por el contrario, la distribución de valores de pixeles vecinos en la imagen cell cifrada, figura 4 d) ocupa todo el espacio delimitado por la gráfica. Es decir, los pixeles de la imagen encriptada no presentan relación alguna con los pixeles próximos. También este resultado se repite en la generalidad de las muestras analizadas, lo que comprueba una vez más la eficacia de la encriptación a base de llaves caóticas.



a) cell *b) dist. de pixeles vecinos*

c) cell encriptado *d) dist, de pixeles vecinos*

Figura 4 Cell., dist. de pixeles vecinos, cell encriptado, dist, de pixeles vecinos.

Otro punto considerado en este estudio fue la entropía, es decir la medición del desarreglo de los pixeles en su nivel en la escala de grises. Para comparar el orden o desorden en el contenido de la imagen, antes y después de la encriptación. La

figura 5 ilustra la diferencia existente entre la entropía calculada de una imagen simple como circbw original a la obtenida en la encriptada. Aquí se observa como el proceso de cifrado incrementa la entropía de un valor menor a uno hasta su valor máximo de ocho. En particular el desempeño de la llave basada en el mapa cuadrático es muy pobre, solo incrementa la entropía a un valor cercano a dos. Al continuar comparando las cuatro imágenes encriptadas restantes con las veinte llaves caóticas se observó el mismo comportamiento, todos los valores de la entropía obtenidos están cerca del valor máximo ocho, con la excepción del mapa cuadrático.

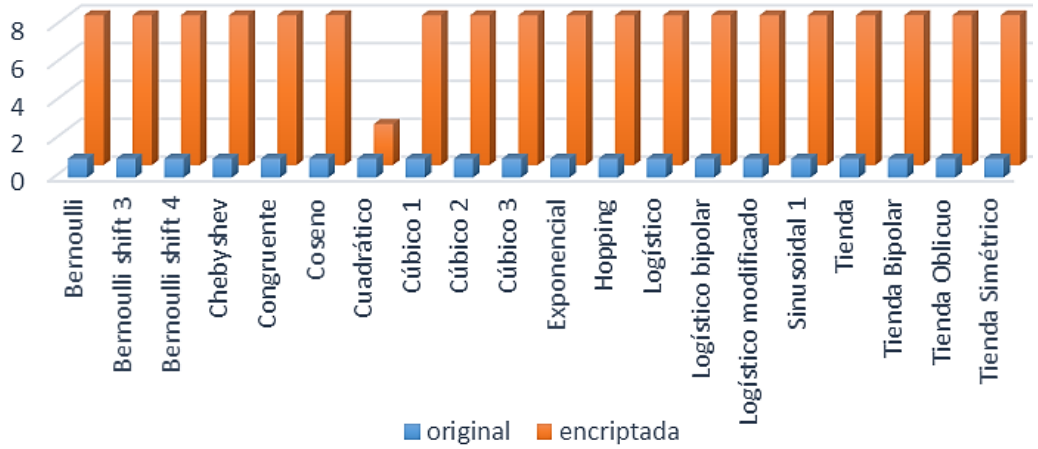


Figura 5 Entropía de la imagen circbw.

Finalmente, para conocer si el proceso estudiado reduce la redundancia entre pixeles vecinos o si esta persiste aun después de la encriptación, se evaluó su correlación. Considerando las variables aleatorias x y y definidas por los valores del nivel de gris de un par de pixeles, su coeficiente de correlación está dado por ecuación 2.

$$\rho_{xy} = \frac{C_{xy}}{\sigma_x \sigma_y} \tag{2}$$

Donde σ_x es la desviación estándar de x, y C_{xy} es la covariancia entre x y y. Para cada una de las imágenes se seleccionaron aleatoriamente 333 pixeles y se compararon con tres de los pixeles adyacentes, estos que se encuentran

localizados abajo, a la derecha y en la esquina inferior derecha como se muestra en la figura 6. Por ende, se formaron 999 pares de pixeles.

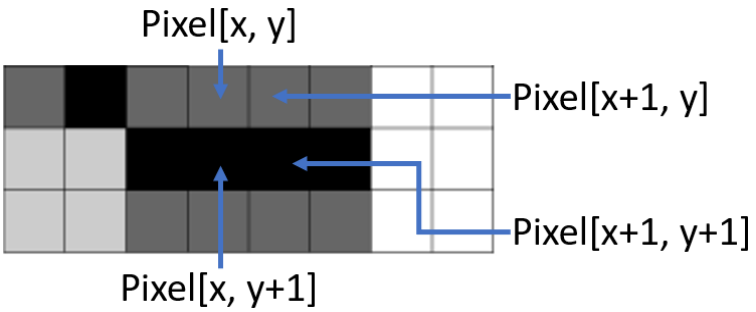


Figura 6 Tres pixeles adyacentes.

Como parámetro de referencia se calculó la correlación de pixeles de las cinco imágenes originales. Luego de cada una de ellas se seleccionaron imágenes encriptadas con los valores intermedios de su parámetro de control, para cada uno de los veinte sistemas caóticos. Como resultado, solo se evaluaron cien imágenes cifradas. Tomando como ejemplo a la imagen cell, en la figura 7 se muestra la comparación de los coeficientes de correlación por sistema caótico entre el pixel central [x, y] y el inferior inmediato [x, y+1]. En la figura 8 se ilustra lo mismo, pero partir del pixel central [x, y] y su vecino a la derecha [x+1, y]. Por último, el tercer coeficiente, mostrado en la figura 9, se obtuvo con la combinación del pixel central [x, y] y el adyacente hacia la derecha [x+1, y+1].

Al analizar las gráficas en las figuras 7 al 9, es posible observar que el coeficiente de correlación calculado en la imagen original tiene un valor cercano a uno.

Figura 7 Correlación de pixeles hacia abajo.

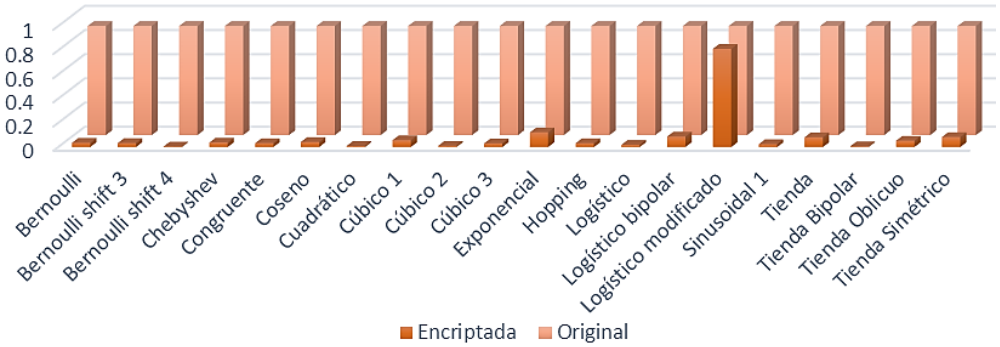


Figura 8 Correlación de pixeles hacia la derecha.

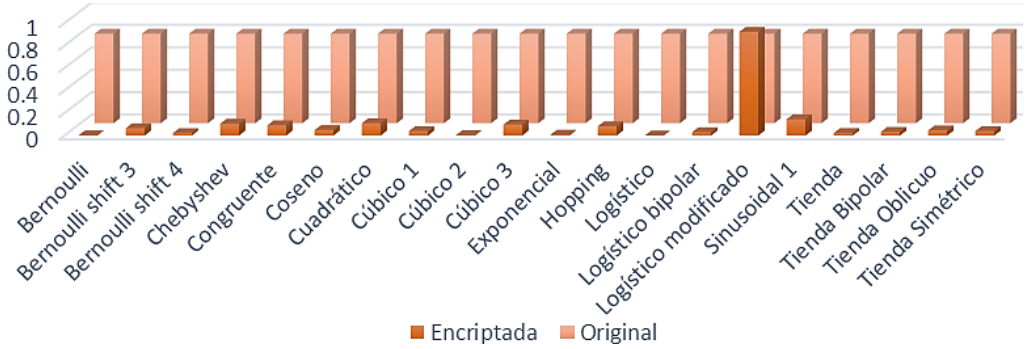


Figura 9 Correlación de pixeles en diagonal.

Obviamente por la alta redundancia contenida en la imagen. Por el contrario, los valores evaluados a partir de las imágenes encriptadas se muestran muy cercanos al cero. Indiscutiblemente esto indica una correlación casi nula entre los pares de pixeles, en cualquiera de sus tres direcciones. La diferencia existente entre las cien imágenes evaluadas es pequeña. El único sistema que no presentó consistencia fue el logístico modificado, pero de una forma negativa, pues sus valores de correlación en las tres direcciones se muestran similares a la imagen original.

4. Discusión

Se logró una sencilla y barata implementación del encriptador digital, con hardware y software de uso común y fácilmente accesible. Aunado a esto de las veinte llaves caóticas analizadas, solo dos presentan un bajo desempeño en dos de las pruebas a que fueron sometidas. Para confirmar estos resultados se podría continuar el estudio de estas llaves caóticas médiate otras herramientas como

examinar su fortaleza al someterlas a ataques cibernéticos. También se podría modificar el diseño del encriptador digital para procesar imágenes más complicadas, de mayor resolución o a color, las cuales presentan una estructura diferente a las compuestas por escala de grises. Asimismo, se podrían generar otras llaves caóticas empleando sistemas caóticos no contemplados en esta investigación, tales como: discretos de más de una dimensión y los de tiempo continúo sometidos a un proceso de discretización.

5. Conclusiones

Para comprobar la efectividad de las veinte llaves caóticas, las mil imágenes encriptadas se sometieron a cuatro diferentes análisis: histograma, distribución de valores de pixeles vecinos, entropía y correlación de pixeles. Tomando en cuenta los resultados obtenidos de las pruebas realizadas, se puede concluir que la mayoría de las llaves son eficaces. Sin embargo, es necesario mencionar las excepciones presentes en el sistema cuadrático, que presenta pobres resultados en la prueba de entropía, y en el sistema logístico modificado, que no rindió satisfactoriamente en el análisis de la correlación de pixeles.

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] Donat Wolfram, Learn Raspberry Pi, Programming with Python, Primera ed. United Kingdom: Technology in action, 2005.

[5] 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.

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

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

[8] Garcés Guzmán Héctor, Hinostroza Zubía Victor Manuel, Priscila Betsabe Hernández Valadez, Encriptador de imágenes en escala de grises con llaves caóticas, Pistas educativas, vol. no 40, noviembre 2018, pp. 478 – 489.

[9] Inzunza, Gonzalez Everardo, Encriptado caótico en sistemas biométricos, Tesis doctoral, Universidad Autónoma de Baja California, Ensenada, Baja California, 2012, pp. 59 – 60.

[10] 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

[11] Ives Crystal, “Human beings as chaotic systems,” Life Sci. Tehcnology, vol. 8, no. 2, pp. 1–7, 2004.

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

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

[14] Rodríguez-Orozco Eduardo, García-Guerrero Enrique Efrén, Inzunza-Gonzalez Everardo, López-Bonilla Oscar Roberto, Flores-Vergara Abraham, Cárdenas-Valdez Jose Ricardo Tlelo-Cuautle Esteban, FPGA-based Chaotic Cryptosystem by Using Voice Recognition as Access Key, Electronics, www.mdpi.com/journal/electronics, 2018.

[15] Smart Nigel Paul, Cryptography: An Introduction, New York: McGraw Hills, 2010.

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