Memorias del XVI Congreso Latinoamericano
de Control Automático, CLCA 2014
Octubre 14-17, 2014. Cancún, Quintana Roo, México

Encriptado de imágenes usando modelos caóticos continuos y discretos

D. López-Mancilla, J.M. Roblero Villa.

Universidad de Guadalajara (UDG), Departamento de Ciencias Exactas y Tecnología
47460, MEX (Tel: 4747379778; e-mail: didierlman@gmail.com).

Resumen: En este trabajo se realizaron algoritmos de programación en Matlab para el encriptado y desencriptado de imágenes usando modelos caóticos continuos y discretos. Se realizó el análisis estadístico de eficiencia y seguridad para determinar la eficiencia de los algoritmos propuestos y corroborar los datos mediante coeficientes de correlación, histogramas, análisis de espacio clave y la calidad de encriptado. Esto determinará la eficiencia del programa, la cual nos llevará a establecer que el sistema de comunicación confidencial es confiable como medio de cifrado de información.

Palabras clave: Encriptamiento de imágenes, Sistemas caóticos, Análisis estadístico de seguridad.

1. INTRODUCCIÓN

En la actualidad con la constante proliferación de los sistemas de comunicación tales como redes de computadoras teléfono celular, tv. por cable o satelital, etc., se requiere que la información a través de estos canales y redes bajo condiciones hostiles de seguridad, sea transmitida en forma segura, por lo que se ha vuelto un problema de vital importancia, en donde, la criptografía asume un papel muy importante. En este trabajo nos enfocaremos en el encriptado de imágenes digitales, debido a su gran uso en varios sistemas y aplicaciones que utilizan imágenes como: sistemas de reconocimiento facial, sistemas de reconocimiento de retina, sistemas de reconocimiento de huellas dactilares, entre otros.

Por lo tanto el presente trabajo se realizó con la finalidad de contribuir a la solución del problema de seguridad y confiabilidad de transmisión de información a través de medios públicos. Se proponen algoritmos para el encriptado y desencriptado de imágenes basados en sistemas caóticos continuos y discretos.

2. DESCRIPCIÓN DEL ENCRIPTADO DE IMÁGENES CON ENMASCARAMIENTO CAÓTICO

Se utilizó un sistema de encriptado aditivo, para cifrar la información que se muestra en la Fig. 1, en el que se procesa una imagen, convirtiéndola a un vector, el cual se atenuará, obteniendo la señal *m(t)*, la cual se suma con el vector caótico *c(t)*, obteniendo la señal *y(t)* que se amplifica, para que el vector encriptado *y(t)* se vuelva a convertir a una imagen, y después se enviará a través de cualquier medio de transmisión.

2.1 *Encriptado con el sistema caótico de Lorenz*

Edward Norton Lorenz [Lorenz 1963], ideó un sistema de tres ecuaciones diferenciales ordinarias, no lineales, como modelo para predecir el clima a largo plazo, pero este sistema no produjo los resultados deseados de acuerdo con lo previsto por Lorenz, ya que resultó sensible a las condiciones iniciales y, por lo tanto, resulto ser lo que hoy se conoce como un sistema caótico.

Las ecuaciones de Lorenz se describen en las siguientes ecuaciones:

$$\begin{aligned} \dot{x}_1 &= p(x_2 - x_1) \\ \dot{x}_2 &= -x_1 x_3 + r x_1 - x_2 \\ \dot{x}_3 &= +x_1 x_2 - t x_3 \end{aligned} \tag{1}$$

Es un sistema dinámico donde p (No. de Prandtl), r (No de Rayleigh) y t son parámetros dados. Para los valores: $p = 10$; $r = 28$ y $t = 8/3$, el sistema se vuelve inestable y muestra un comportamiento caótico.

Ahora, al momento de utilizar el sistema de Lorenz se propuso la imagen que se muestra en la Fig. 3. Al realizar el encriptado de la imagen, se genera una imagen totalmente diferente a la original, que se muestra en la Fig. 4. En la Fig. 5 se muestra la imagen desencriptada obteniendo la imagen que se recupera utilizando el sistema de Lorenz.

2.2 Encriptado con el m*apeo Caótico de Chen* [Chen y Ueta, 1999]

Uno de los mapeos caóticos que se presenta en el artículo, y que se utilizó en este trabajo es el mapeo caótico de Chen, al cual se le aplicó el proceso de encriptado con enmascaramiento caótico teniendo una imagen diferente como se muestra en la Fig. 6, y su respectivo desencriptado mostrado en la Fig. 7, volviendo a recuperar la imagen original. El modelo matemático que se utilizó fue el siguiente:

$$\begin{aligned} y_1(k+1) &= 1 - a\,[y_1^2(k) + y_2^2(k)] \\ y_2(k+1) &= -2ab\,y_1(k)\,y_2(k) \end{aligned} \tag{2}$$

dónde: a=1.95, b=1, $y_1(1)$=0.1, $y_2(1)$=0.1

Aunque los sistemas utilizados puedan llegar a parecer similares, son topológicamente muy distintos y su comportamiento difiere bastante.

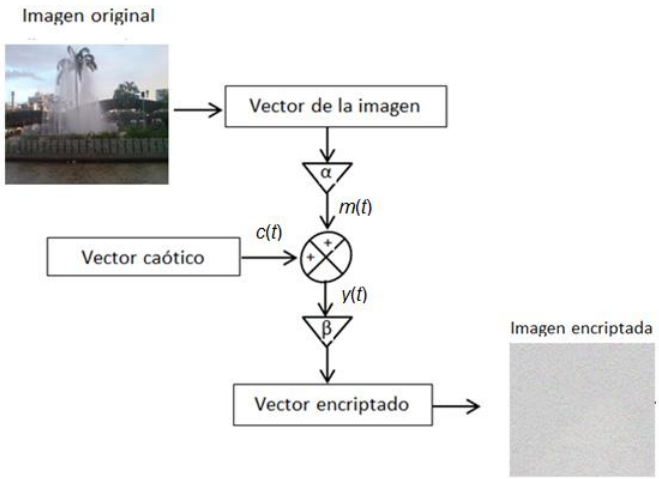

Figura 1: Enmascaramiento de la información utilizando caos.

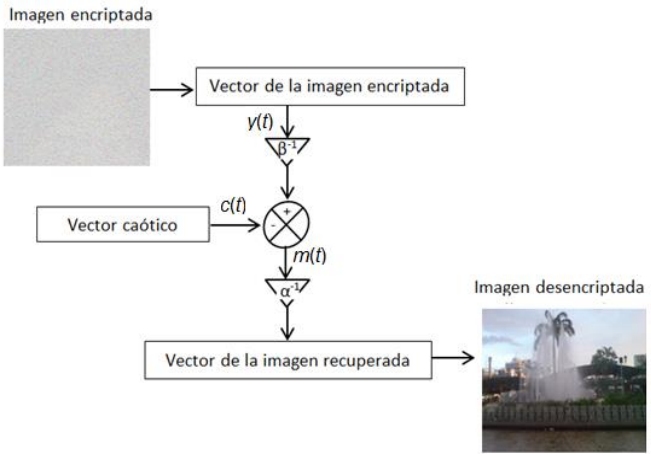

Figura 2: Proceso inverso para el desencriptado de la imagen.

2.3 Encriptado con el mapeo hipercaótico de Rössler

Es un sistema de ecuaciones diferenciales ordinarias no lineales, descubierto por el científico alemán O. Rössler [Rössler, 1976], es un modelo simple y fue uno de los primeros atractores altamente conocidos de tres dimensiones [Lakshman. y Murali, 1996] [Kathleen, 1996], la ecuación característica es la siguiente:

$$x_1(k+1) = \alpha x_1(k)\big(1 - x_1(k)\big) - \beta(x_2(k) + \gamma)\big(1 - 2x_2(k)\big)$$

$$x_2(k+1) = \delta x_2(k)\big(1 - x_2(k)\big) + \zeta x_3(k) \qquad (3)$$

$$x_3(k+1) = \eta((x_3(k) + \gamma)(1 - 2x_2(k) - 1)(1 - \theta x_1(k)$$

la cual tiene los siguientes valores: $\alpha = 3.8$, $\beta = 0.05$, $\sigma = 0.35$, $\lambda = 3.78$, $\gamma = 0.2$, $\eta = 0.1$ y $\theta = 1.9$

Se realizó el proceso de encriptado con el modelo hipercaótico de Rössler, obteniendo una imagen totalmente diferente a la obtenida en la Fig. 3, la cual se muestra en la Fig. 8, así como la imagen desencriptada, volviendo a recuperar la imagen original como se muestra en la Fig 9.

3. ANÁLISIS ESTADISTICO DE EFICIENCIA Y SEGURIDAD.

Se realizó el análisis estadístico para la Fig. 3, que es la imagen original (IO), y el encriptado y desencriptado con cada uno de los sistemas propuestos. Se muestran los histogramas de la IO, el histograma del encriptado de la imagen (IE), y el histograma de la imagen desencriptada (ID), pudiéndose observar el nivel de confusión del sistema entre la IO vs la IE, y el nivel de recuperación de la IO vs ID.

También se procedió a graficar el coeficiente de correlación para cada una de la IO, IE y de la ID donde la proporción es aproximadamente de 0-1 donde "0" significa un bajo nivel de correlación en la IE y "1" un alto nivel de recuperación en la ID

3.1 Comparación de histogramas

Comúnmente las estadísticas por sí mismas no proporcionan una imagen completa e informativa del desempeño de un proceso, por eso el histograma, siendo un gráfico especial, se utiliza para demostrar las variaciones cuando se proporcionan datos continuos como tiempo, peso, tamaño, temperatura, etc.

A continuación se muestran los histogramas de la IO vs IE vs ID con el sistema de Lorenz en la Fig. 10, en el que se puede observar que los histogramas de la IO vs IE nos muestra que los niveles de intensidad son totalmente diferentes lo que quiere decir que la IE no se asemeja a la IO, por lo que obtenemos una imagen nueva diferente a la IO, en comparación con la IO vs ID en el cual hay.

Figura 3: Imagen original propuesta para el encriptado y desencriptado.

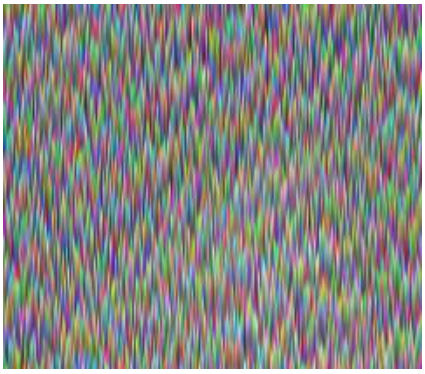

Figura 4: Imagen encriptada con el sistema Lorenz.

Figura 5: Imagen desencriptada con el sistema de Lorenz.

Figura 6: Imagen encriptada con el mapeo caótico de Chen.

Figura 7: Imagen desencriptada con el mapeo caótico de Chen.

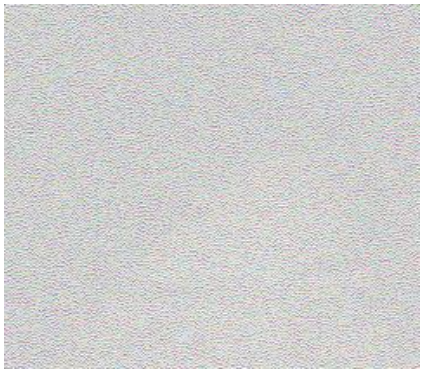

Figura 8: Imagen encriptada con Rössler.

Figura 9: imagen desencriptada con Rössler.

una gran similitud en los niveles de intensidad y por lo tanto en el recuperado de la ID el histograma se parece al histograma de la IO

En la comparación de los histogramas IO vs IE vs ID con el mapeo caótico de Chen en la Fig. 11, se puede observar que los histogramas de la IO vs IE, sus niveles de intensidad también son diferentes y por lo tanto sus histogramas no se parecen, indicándonos que no es la misma figura, en el de la IO vs ID del mapeo de Chen los niveles de intensidad son idénticos a lo que los histogramas de la IO vs ID son similares y la imagen es muy parecida a la IO.

Y por último la comparación de histogramas de la IO vs IE vs ID del mapeo hipercaótico de Rössler en la Fig. 12, se puede analizar que no hay similitud existente ya que al igual que con los otros sistemas el nivel de intensidad de la IE es totalmente diferente a la IO, en los cuales se puede observar que los histogramas son diferentes y no hay similitud entre los histogramas de las imágenes, en el caso de la IO vs ID, en el desencriptado de la imagen, su recuperación en cuestión de los niveles de intensidad es muy similar a la IO por lo que nos da un histograma parecido a la IO.

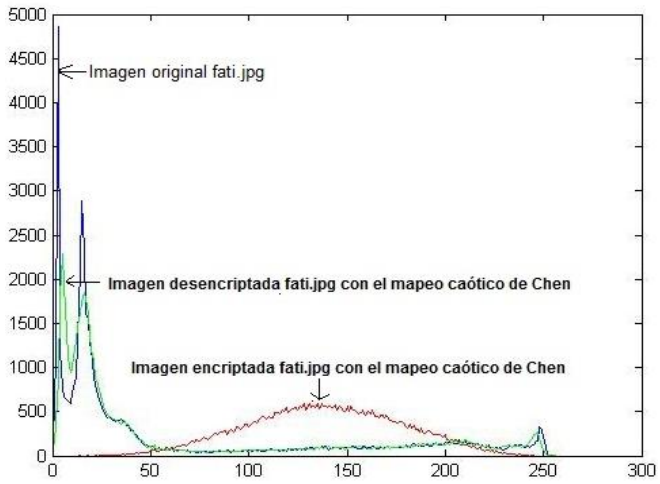

Figura 10: IO vs IE vs ID(Chen).

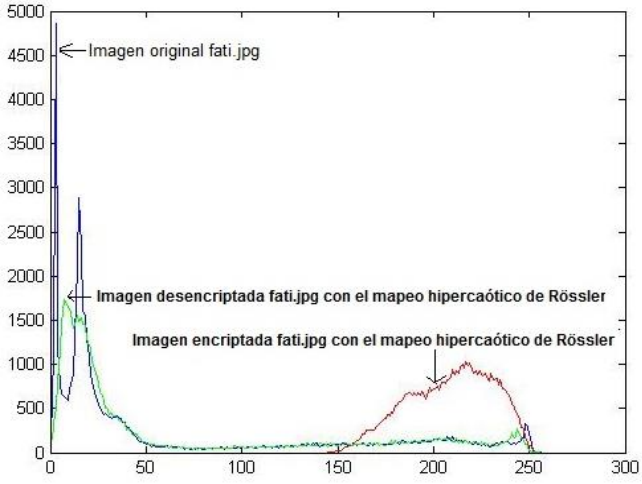

Figura 11: IO vs IE vs ID (Rössler).

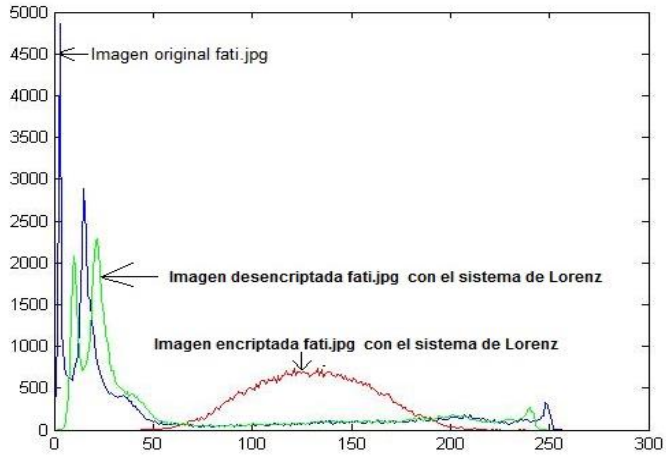

Figura 12: IO vs IE vs ID (Lorenz).

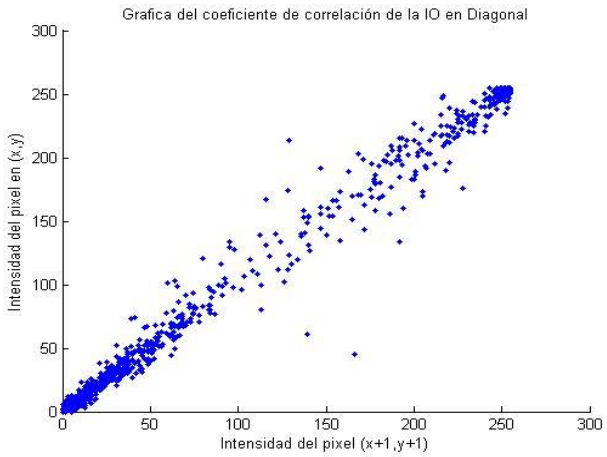

Figura 13: Gráfica del CC de la IO en diagonal.

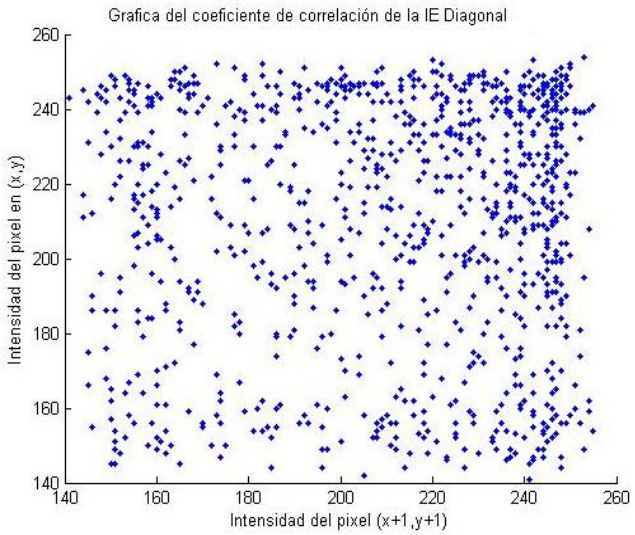

Figura 14: Gráfica del CC de la IE en diagonal.

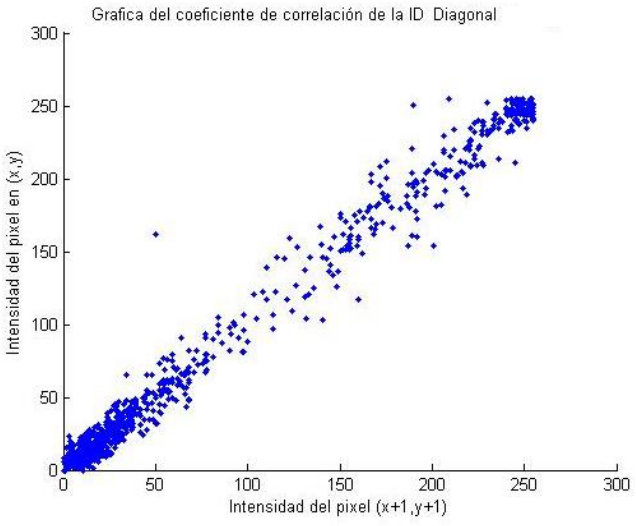

Figura 14: Gráfica del CC de la ID en diagonal.

Tabla 1. CC en dirección: Diagonal, del sistema de Lorenz

Imágenes	Coeficiente de correlación
Imagen original (IO)	0.9981
Imagen encriptada (IE)	0.0761
Imagen desncriptada (ID)	0.9945

3.2 Coeficiente de Correlación [Mercado-Sánchez et al, 2009]

Es una medida que indica la asociación entre las variables (similitud o coherencia) de los pixeles de la imagen, el coeficiente de correlación (CC), debe de estar en los rangos de 0 a 1, el cual indica que cuando el valor es menor que 1 no hay relación entre los pixeles de la IE en comparación de los pixeles de la IO, en el otro caso el valor de 1 nos indica que hay una gran similitud entre los pixeles de la IO comparándola con los pixeles de la ID. Se determinó el CC de la IO, para ver el nivel de confusión en la IE y el nivel de recuperación de la ID, en las Figs. 13, 14 y 15, se muestran las gráficas de coeficiente de corrección, las cuales muestran el nivel de coherencia existente en las imágenes en este caso la IO, IE e ID con el sistema de Lorenz, a lo cual se realizó la siguiente selección. Aleatoriamente se seleccionaron 1000 pares de pixeles adyacentes (x,y) de la IO,IE e ID, en dirección diagonal $(x+1,y+1)$, para el caso de la IO se pude apreciar la similitud existente entre los pares de pixeles seleccionados aleatoriamente en la Fig. 13, en el caso contrario en la gráfica de CC de la IE no hay relación existente en los pares de pixeles aleatorios y por lo tanto se puede observar en la Fig. 14, que los pixeles están dispersos en todo el plano, en el caso contrario la gráfica de la ID Fig. 15, hay una gran relación entre los pares de pixeles adyacentes formando una línea en 45 grados como en la IO.

En la tabla 1, se muestran los valores para el CC de la IO, IE e ID en dirección diagonal para el sistema de Lorenz, en los que se puede ver que el valor de la IO es 0.9981 cercano a 1, lo que nos indica que el CC es alto, en el caso contrario con la IE el coeficiente de correlación es 0.0761 muy cercano a "0" indicándonos que hay gran dispersión de pixeles y obtenemos valores muy lejanos a la IO, y por último en la ID se obtiene un valor de 0.9945, indicándonos que se obtuvo un valor muy cercano a la IO por lo que la recuperación es muy parecida a la IO.

3.3 *Análisis de espacio clave* [Chen et al, 2004]

Es el número de combinaciones totales que se pueden realizar para el sistema de encriptado, el cual depende de los números de estado (parámetros) que se utilizan con cada uno de los sistemas de encriptado [Elkamchouchi y Makar, 2005].

Para nuestro caso se tienen los siguientes parámetros: para el mapeo de Chen: 2 parámetros, para el mapeo hipercaótico de Rössler 3 parámetros y para el sistema de Lorenz: 3 parámetros, los cuales para saber la precisión del sistema depende de los parámetros empleados en los estados que se utilizan en los sistemas de encriptado, por ejemplo para un parámetro es:

$$10^{|-38*1|} = 10^{38} \approx 2^{106}.$$

Esta razón hace que el espacio de clave del sistema sea reducido y, por lo tanto, tiene una gran probabilidad a no resistir ataques de fuerza bruta.

Tabla 2. Espacio de clave para los diferentes sistemas de encriptado.

Precisión de la Lap-top $10^{\|-38\|}$	**Parámetros**	**Espacio de clave**
Mapeo de Chen	2	$10^{\|-38*2\|} = 10^{76} \approx 2^{252}$
Mapeo hipercaótico de Rössler	3	$10^{\|-38*3\|} = 10^{114} \approx 2^{379}$
Sistema de Lorenz	3	$10^{\|-38*3\|} = 10^{114} \approx 2^{379}$

El espacio clave en el mapeo de Chen que se utilizó con dos parámetros fue el siguiente:

$$10^{|-38*2|} = 10^{76} \approx 2^{252}.$$

Para el mapeo hipercaótico de Rössler y el sistema de Lorenz, el espacio de clave está definido por tres parámetros, los cuales nos dieron los siguientes resultados de espacio clave:

$$10^{|-38*3|} = 10^{114} \approx 2^{379})$$

Como se puede observar el espacio clave tiene un amplio número de combinaciones, y por lo tanto puede resistir cualquier tipo de ataque de fuerza bruta, como se ve en la tabla 2.

3.4. *Calidad de encriptado*

Uno de los factores importantes al examinar el encriptado de la imagen, es la inspección visual, donde se ve la dispersión de los pixeles de la imagen encriptada y la calidad del código.

Por ejemplo, la calidad del encriptado es expresada como la desviación que hay entre los pixeles en la IE con respecto a la desviación de los pixeles en la IO. Para obtener la desviación se calcula la matriz X, la cual hace una representación del valor absoluto de la desviación entre cada pixel que hay antes y después del encriptado, se obtiene el histograma de las diferencias y se calcula el valor el valor promedio DC seguido de AC (Valor Absoluto de los Histogramas menos D). Finalmente se determina el parámetro de calidad que hay en el desencriptado R (suma de las diferencias AC) [Elkamchouchi y Makar, 2005].

Resumiendo: para obtener la calidad de encriptado realizamos los siguientes pasos:

1. $D = |IO - IE|$
2. $H = hist(D)$
3. $DC(i) = \frac{1}{256} \sum_{i=0}^{256} hi$
4. $AC(i) = |H(i) - D|$
5. $R = \frac{1}{256} \sum_{i=0}^{255} AC(i)$

El valor esperado de la R es ≈ 18, 000, mientras que el algoritmo en los tres métodos de encriptado produce valores por arriba de 20,000 y por lo cual la R es un buen resultado para la calidad de encriptado. Los valores de los resultados de la calidad de encriptado con los sistemas propuestos se encuentran en la tabla 3.

Tabla 3 Resultados de la calidad de encriptado para la imagen propuesta Fig. 3, con los diferentes sistemas.

Calidad de encriptado para fati.jpg	**ID del algoritmo**	**Valor esperado**
Mapeo de Chen	23654	18000
Mapeo hipercaótico de Rössler	23555	18000
Sistema de Lorenz	23457	18000

AGRADECIMIENTOS:

Este trabajo fue patrocinado por el Conacyt,, México, con el proyecto CB-2011/166654.

4. CONCLUSIONES

En este trabajo, se realizó una contribución a la solución del encriptado de imágenes utilizando caos, modificando los esquemas comunes de encriptado. Se propusieron sistemas y mapeos caóticos continuos y discretos para encriptar imágenes, corroborándose los datos obtenidos con el análisis estadístico del mapeo caótico de Chen, el hipercaotico de Rössler y el sistema de Lorenz. Se analizaron los coeficientes de correlación, el espacio de clave y la calidad de encriptado de cada uno para probar la resistencia que tienen ante ataques de fuerza bruta. Se determinó la eficiencia de los algoritmos de encriptado propuestos, realizando simulaciones numéricas y representaciones gráficas para ver el nivel de encriptado.

REFERENCIAS

Chen G.R, Mao Y.B., Chui C. K. 2004. "A symmetric image encryption scheme based on 3D chaotic cat maps". Chaos, Solitions and Fractals. 21. Pp. 749-761.

E. N. Lorenz. Deterministic Nonperiodic Flow. Journal of the Atmospheric Sciences. Vol.20. Pp. 130-141. 1963.

Elkamchouchi H. and Makar M.A. 2005. "Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR clock ciphers". Twenty second national radio science conference (NRSC). Pp C11. Cairo, Egypt. March 15-17.

G. Chen. T. Ueta. “Yet another chaotic attractor”. Int. J. of Bifur Chaos. Vol. 9. Pp. 1465-1466. 1999.

J. B. Mercado-Sánchez, M. T. Rodríguez-Sahagún, D. López-Mancilla.2009. “Encriptamiento de Imágenes Basado en Mapeo Caótico Trigonométrico para Comunicaciones Seguras. Congreso Anual 2009 de la Asociación de México de Control Automático. Zacatecas”, México. Pp 5.

Kathleen T. Alligood. Tim d. Sauer James A. Yorke. 1996. “Chaos and introduction to dynamical systems”. Pp. 43-273.

M.Lakshman. K. Murali. 1996. “Chaos in nonlinear oscillators controlling and synchronization”. Pp. 1-18.

O. E. Rössler. 1976. “An equation for continuous chaos”. Physics letters, 57a, Pp. 397-398.