# Encriptamiento de Imágenes Basado en Mapeo Caótico Trigonométrico para Comunicaciones Seguras

J. B. Mercado-Sánchez[1], M. T. Rodríguez-Sahagún[1], D. López-Mancilla[2]
[1]Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara (CUCEI-UdeG)
C.P. 44420, Guadalajara, Jal., México
[2]Centro Universitario de los Lagos, Universidad de Guadalajara (CULagos-UdeG)
C.P 47460, Lagos de Moreno, Jalisco, México
comdsp@yahoo.com
Teléfono: (52)-33-36320360

***Resumen*—En este trabajo se presenta una modificación al esquema de encriptamiento basado en el mapeo caótico trigonométrico de Jafarizadeh (2001) y Sohrab (2008). Estos mapeos están definidos como cocientes de polinomios de grado N. Tienen propiedades como: región caótica variable, bifurcación de un estado estable a uno caótico (y viceversa) sin presentar el escenario usual de período doble o período *n* en la ruta al caos, y la posibilidad de construir composición de mapeos. Con el objetivo de lograr el encriptamiento de imágenes, se aplica una composición de mapeos caóticos trigonométricos (CMCT) para permutar los pixeles de la imagen. Otra CMCT se utiliza en el proceso de difuminación. En este trabajo se propone el encriptamiento de imágenes a colores de tamaño variable aplicando CMCT en la permutación, y un nuevo algoritmo en el proceso de difuminacion utilizando un segundo mapeo. El algoritmo de encriptamiento y desencriptamiento presentado, puede cumplir con los requerimientos de alto nivel de seguridad, gran espacio de la clave y aceptable velocidad de encriptamiento para una imagen a color. Se realizan simulaciones numéricas y representaciones gráficas para el encriptamiento y el desencriptamiento de una imagen utilizando el software MatLab.**

**Palabras clave: Mapeos caóticos trigonométricos, encriptamiento de imagen, comunicaciones seguras.**

## I. INTRODUCCIÓN

Desde que Pecora y Carroll reportaron su trabajo de sincronización de caos (Pecora y Carroll, 1990), la investigación en la dinámica caótica ha recibido considerable atención. Particularmente, a la luz de la aplicación potencial de este fenómeno en la seguridad en las comunicaciones (Alvarez y Li, 2006; Gámez *et al*., 2008; Gámez *et al*., 2009 ). El encriptamiento de datos utilizando sistemas caóticos fue reportada en los 90's como un nuevo método de aprovechamiento para codificar y decodificar señales diferentes de los métodos convencionales que usan algoritmos numéricos como la clave de encriptamiento (Cruz *et al*., 2005).

El número de delitos por computadora se ha incrementado considerablemente. La seguridad en la transmisión de imágenes se ha convertido en un tópico importante en el mundo (Li *et al.*, 2005). Los esquemas de encriptamiento de imágenes están siendo estudiados cada vez más ante la demanda para encontrar seguridad en la transmisión de imágenes en tiempo real a través de Internet y también para las redes inalámbricas (Li *et al.*, 2007; Chiaraluce *et al*., 2002 ).

El algoritmo tradicional de encriptamiento de imágenes como el estándar de encriptamiento de datos (DES), tiene la desventaja de bajo nivel de eficiencia cuando la imagen es grande (Chen *et al*., 2004). El encriptamiento basado en caos propone una nueva y eficiente forma de lograr una rápida y alta seguridad en el encriptamiento de imágenes. Después que Matthews propuso el algoritmo de encriptamiento caótico (Matthews, 1989), el incremento en las investigaciones de la tecnología de encriptamiento de imágenes está basado en los sistemas caóticos (Wang *et al*., 2004). Los sistemas caóticos tienen importantes propiedades como la sensibilidad a las condiciones iniciales, la propiedad de pseudo aleatoriedad, no periodicidad y la dependencia de los parámetros del sistema. Estas propiedades están relacionadas con los requisitos de Shannon para la permutación y la difusión en la construcción de criptosistemas (Shannon, 1949). El principal obstáculo en el diseño de algoritmos de encriptamiento de imágenes consiste en la gran dificultad de realizar rápidamente el proceso de permutación y difuminación de los pixeles por los métodos tradicionales de la criptología. Considerando las ventajas de un alto nivel de eficiencia y simplicidad de los sistemas caóticos unidimensionales (Elnashaje & Abasha, 1995), se han aplicado diferentes sistemas caóticos de tiempo discreto como el mapeo logístico en algoritmos de encriptamiento de imágenes, sin embargo estos mapeos presentan desventajas como pequeño espacio de la clave y una débil seguridad (Kocarev, 2001; Ponomarenko y Prokhoroy, 2002).

Para superar estas desventajas, se propone un algoritmo caótico con un alto nivel de seguridad, un gran espacio de clave y una aceptable velocidad de encriptamiento basado en CMCT.

## II. ALGORITMO DE CMCT

Conjuntos de mapeos caóticos uniparamétricos en el intervalo [0,1], pueden ser definidos como el cociente de polinomios de grado *N* (Jafarizadeh, 2001):

$$\phi_N^{(1,2)}(x,\alpha)=\frac{\alpha^2F^2}{1+(\alpha^2-1)F^2} \quad (1)$$

Donde *F* se sustituye con el polinomio de Chebyshev de primer tipo $T_N(\sqrt{x})$:

$$\phi_N^{(1)}(x,\alpha)=\frac{\alpha^2(T_N(\sqrt{x}))^2}{1+(\alpha^2-1)(T_N(\sqrt{x}))^2} \quad (2)$$

Y el polinomio de segundo tipo $U_N(\sqrt{x})$:

$$\phi_N^{(2)}(x,\alpha)=\frac{\alpha^2(U_N(\sqrt{x}))^2}{1+(\alpha^2-1)(U_N(\sqrt{x}))^2} \quad (3)$$

En seguida se aplica un mapeo isomórfico con la función:

$$h(x)=\frac{1-x}{x} \quad (4)$$

De acuerdo a:

$$\tilde{\phi}_N^{(1)}(x,\alpha)=h\circ\phi_N^1\circ h^{-1} \quad (5)$$
$$=\frac{1}{\alpha^2}\tan^2(N\arctan\sqrt{x})$$

$$\tilde{\phi}_N^{(2)}(x,\alpha)=h\circ\phi_N^2\circ h^{-1} \quad (6)$$
$$=\frac{1}{\alpha^2}\cot^2(N\arctan\frac{1}{\sqrt{x}})$$

De la definición de estos mapeos, se puede probar que para N impar, x=0 (α ε (0,1/ N)) y x=1 (α >N) son puntos fijos, $\phi_N^{(1,2)}(x,\alpha)$ exhibe dinámica caótica para valores impares de N con α ε (1/N, N) (no presenta ventanas periódicas).

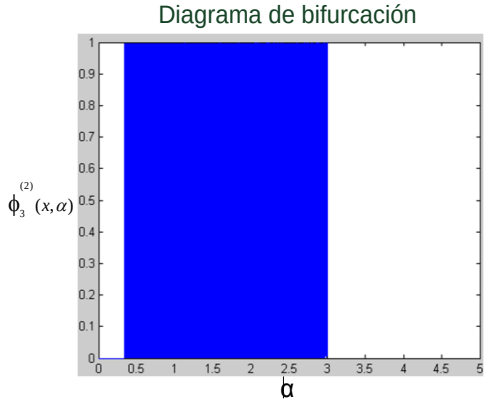


Figura 1. Diagrama de bifurcación de $\phi_3^{(2)}(x,\alpha)$

Para N par, los mapeos $\phi_N^{(1)}(x,\alpha)$ exhiben comportamiento caótico para α ε(0,N) con punto fijo x=1 en α > N y los mapeos $\phi_N^{(2)}(x,\alpha)$ presentan dinámica caótica para α ε (1/N,∞) con punto fijo x=0 en α ε(0,1/N). El mapeo $\phi_2^{(2)}(x,\alpha)$ se reduce a un mapeo logístico con α =1.

Aprovechando la jerarquía de mapeos caóticos Ec. (5) y Ec. (6), se puede generar una nueva jerarquía de familias de mapeos caóticos con múltiples parámetros realizando la composición de los mapeos Ec. (5) y Ec. (6), los cuales pueden ser escritos en la siguiente forma:

CMCT1,

$$\phi_{N_1,N_2}^{\alpha1,\alpha2}=\frac{1}{\alpha_2^{\,2}}\tan^2\left(N_2\arctan\left(\sqrt{\frac{\tan^2(N_1\arctan(\sqrt{x}))}{\alpha_1^{\,2}}}\right)\right) \quad (7)$$

CMCT2,

$$\phi_{N_1,N_2}^{\alpha'1,\alpha'2}=\frac{1}{\alpha'_2{}^2}\cot^2\left(N_2\arctan\left(\frac{\alpha'_1}{\cot^2(N_1\arctan(\frac{1}{\sqrt{x}}))}\right)\right) \quad (8)$$

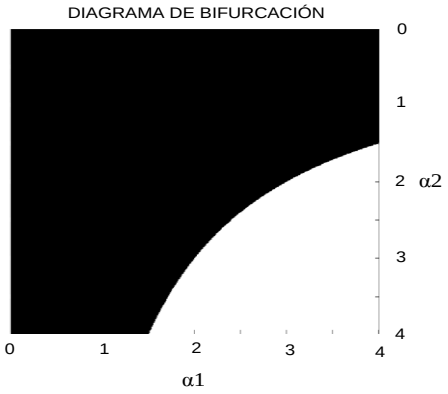


Figura 2. Segmento de la proyección del diagrama de bifurcación $\phi_{2,3}^1$ en el plano $\alpha_1$, $\alpha_2$.

Se puede probar que las regiones con dinámica caótica son: Para valores enteros impares de $N_1, N_2,\ldots, N_n$.

$$\prod_{k=1}^{n}1/N_k<\prod_{k=1}^{n}\alpha_k<\prod_{k=1}^{n}N_k$$

Si uno de los enteros es par (ver Fig. 2), entonces los parámetros de la región caótica están definidos por $\alpha_k>0$, para $k=1,2,...,n$ y

$$\prod_{k=1}^{n}\alpha_k<\prod_{k=1}^{n}N_k,$$

fuera de estas regiones, tienen puntos fijos estables de período uno.

## III. MÉTODO DE ENCRIPTAMIENTO

Se procesa una imagen a colores de dimensión A(f,c,3), donde f = número de filas, c = número de columnas y 3 es el número de capas.

Para el encriptamiento de la imagen, se aplica un proceso de permutación seguido de un proceso de difuminación. En el proceso de permutación, los pixeles de la imagen son reacomodados de la siguiente forma:

Aplicando CMCT1 Ec. (7), se generan los vectores $x_p$ y $y_p$ de acuerdo a los siguientes valores iniciales y parámetros,

$N_1 = 3$, $N_2 = 5$

Permutación: m: $x_0$, $\alpha_{1x}$, $\alpha_{2x}$

n: $y_0$, $\alpha_{1y}$, $\alpha_{2y}$

Y aplicando las ecuaciones,

$$x_p = \left[ \phi_{N1} \times 10^4 \right] \bmod f \qquad (9)$$

$$y_p = \left[ \phi_{N_2} \times 10^3 \right] \bmod c \qquad (10)$$

para permutar la imagen $M_{m\times n\times k}$ intercambiando el pixel (i,j,k) con el pixel $(x_p, y_p, k)$.

Para el proceso de difuminación de la imagen se usa CMCT2 Ec. (8) con $N_1 = 4$, $N_2 = 8$ para calcular el vector,

$$x_k = \left[ x \times 10^{10} \right] \bmod 256 \qquad (11)$$

El vector $x_k$ y la matriz permutada $M_{m\times n\times k}$ se procesan de acuerdo al algoritmo desarrollado en la figura (3) y el resultado generado es almacenado en $C_{m\times n\times k}$.

En primer lugar se suma el vector $x_k$ con los elementos de la matriz $M_{m\times n\times k}$ en modulo 256, este resultado se recombina nuevamente con $x_k$ (xor), después esta trama se mezcla (xor) con una versión de ella misma con retardo $D^{-3}$ y $D^{-5}$,

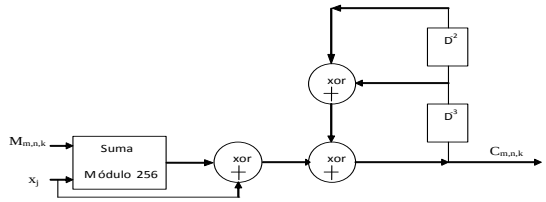


Figura 3. Diagrama a bloques del algoritmo de difuminación.

$$C_{m,n,k} = x_k \; XOR \; \left( \left( M_{m,n,k} + x_k \right) \bmod 256 \right) \ldots \qquad (12)$$
$$\ldots XOR \; C_{m,n,k}\left(D^{-3}\right) XOR \; C_{m,n,k}\left(D^{-2}\right)$$

Este algoritmo de encriptamiento incrementa el nivel de difuminación de la imagen encriptada dando por resultado un mayor nivel de seguridad contra los ataques criptográficos más comunes.

## IV. RESULTADOS NUMÉRICOS

Se aplicó el algoritmo de encriptamiento a una imagen a colores ("Pisa" de tamaño 141x 264 x 3). Para realizar el encriptamiento de la imagen se utilizaron los siguientes valores iniciales y parámetros en el proceso de permutación:

$N_1 = 3$, $N_2 = 5$

x: $\alpha_1 = 2.10155$, $\alpha_2 = 3.569221$, $x_0 = 25.687$

y: $\alpha_1 = 1.8874$, $\alpha_2 = 4.23562$, $y_0 = 574.461$,

Para el proceso de difuminación: $N_1 = 4$, $N_2 = 8$

m x n: $\alpha_1 = 2.8912$, $\alpha_2 = 3.89954$, $x_0 = 814.217217$.

Los resultados de encriptamiento se presentan a continuación:

Primero se presenta la imagen original (IO).

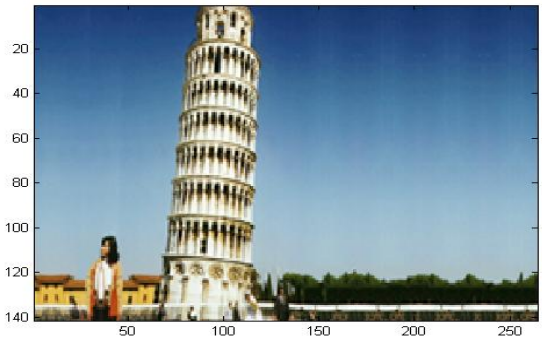


Figura 4. La imagen original (IO).

En seguida se presenta la Imagen Encriptada (IE), en donde el análisis estadístico demuestra un nivel alto de confusión y difuminación del algoritmo de encriptamiento.

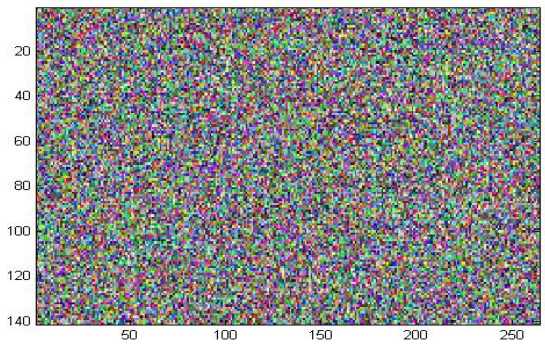


Figura 5. La imagen encriptada (IE).

Al aplicar el algoritmo de desencriptamiento con los valores iniciales y parámetros correctos, se recupera la IO sin errores.

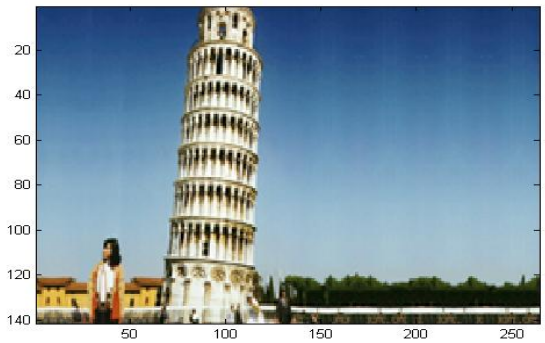


Figura 6. La imagen recuperada.

Al presentar una pequeña variación en uno de los parámetros (α=2.10155 por α=2.1015500001) se recupera una imagen errónea con clave falsa.

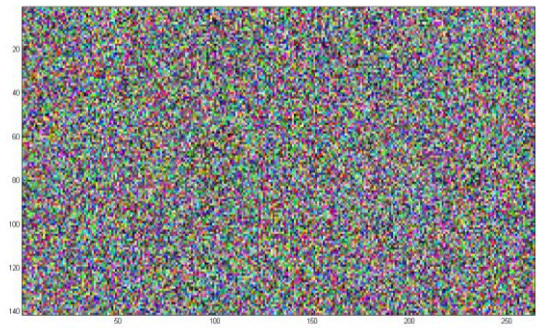

Figura 7. La imagen recuperada con clave falsa.

## V. ANÁLISIS ESTADÍSTICO

Se aplica un análisis estadístico para la IO y para la IE, y se muestran los histogramas en la figura 8.

Se demuestra que el algoritmo de encriptamiento ha encubierto los caracteres de la IO y muestra buen rendimiento; el histograma de la IE es uniforme y significativamente diferente con respecto al histograma de la IO. El histograma de una imagen sin encriptamiento muestra zonas de colores comunes en cantidad variable de acuerdo al tamaño de las figuras (zonas) presentes en la IO. Por otra parte, entre más uniforme resulte el histograma de la IE, mayor será el nivel de seguridad del algoritmo. La proporción es aproximadamente de 0-1; bajo nivel de correlación en la IE y alto nivel de seguridad.

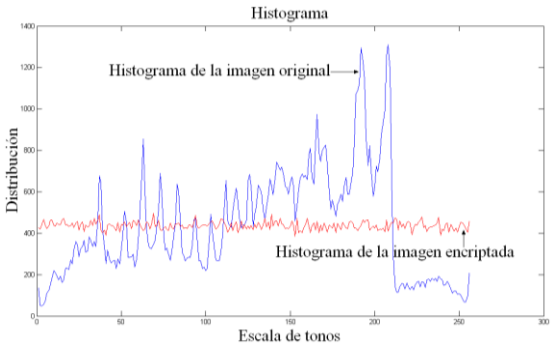


Figura 8. Histograma de la IO (azul) e histograma de la IE (rojo).

Para determinar la correlación entre los pixeles de la IO y la correlación de los pixeles en la IE, se realizó el siguiente procedimiento:

1.- Se seleccionaron aleatoriamente 1000 pares de pixeles adyacentes en dirección horizontal (x, y) → (x+1, y). Los resultados del análisis de correlación en sentido horizontal para la IO se presentan en la figura 9.

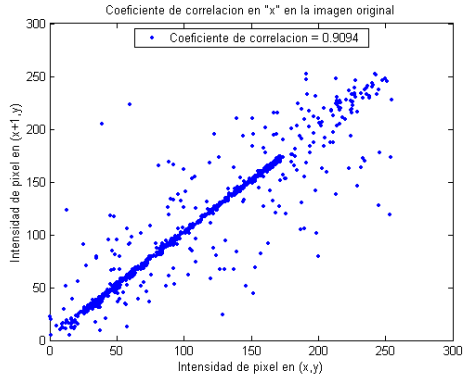


Figura 9. Análisis de correlación en dirección horizontal de la IO.

El análisis de correlación en dirección horizontal para la IE se presenta en la figura 10.

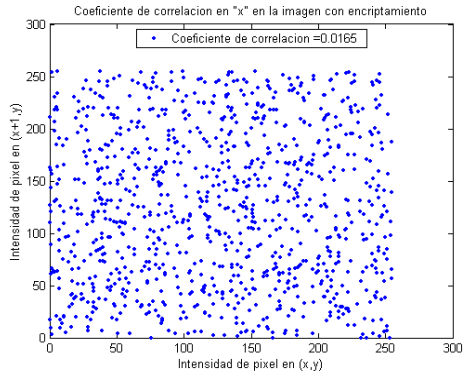


Figura 10. Análisis de correlación en dirección horizontal de la IE.

2.- Se seleccionaron aleatoriamente 1000 pares de pixeles adyacentes en dirección vertical $(x, y) \rightarrow (x, y+1)$. Los resultados del análisis de correlación en sentido vertical para la IO se presentan en la figura 11.

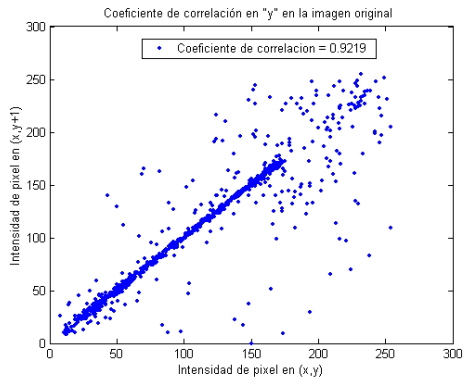


Figura 11. Análisis de correlación en dirección vertical de la IO.

El análisis de correlación en dirección vertical para la IE se presenta en la figura 12.

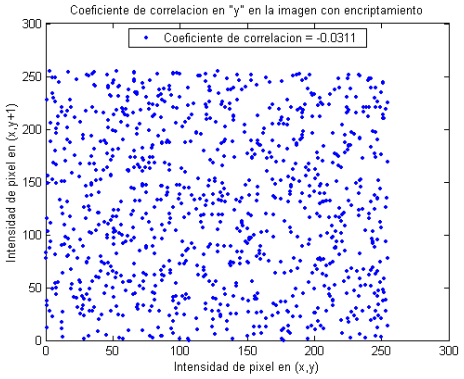


Figura 12. Análisis de correlación en dirección vertical de la IE.

3.- Se seleccionaron aleatoriamente 1000 pares de pixeles adyacentes en dirección diagonal $(x, y) \rightarrow (x+1, y+1)$. Los resultados del análisis de correlación en sentido diagonal para la IO se presentan en la figura 13.

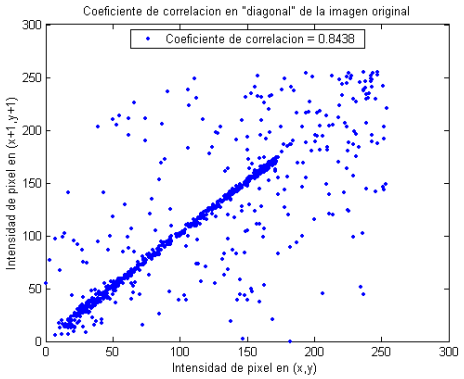


Figura 13. Análisis de correlación en dirección diagonal de la IO.

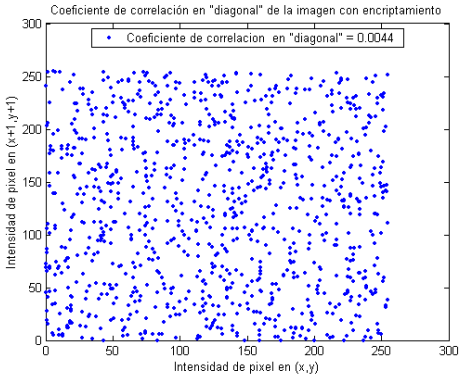


Figura 14. Análisis de correlación en dirección diagonal de la IE.

En la tabla 1, se muestran los resultados obtenidos al calcular los coeficientes de correlación (CC) de la IO e IE para 1000 pares de pixeles tomados aleatoriamente en las direcciones horizontal, vertical y diagonal. Se muestra claramente la relación 1 a 0 en el CC. Puesto que para la IO el CC debe aproximarse a 1; y para la IE el CC debe aproximarse a 0.

Tabla 1. Coeficiente de correlación de 1000 pixeles adyacentes para IO vs IE.

| | Imagen original | Imagen con encriptamiento |
|---|---|---|
| Horizontal | 0.9094 | 0.0165 |
| Vertical | 0.9219 | -0.0311 |
| Diagonal | 0.8433 | 0.0013 |

## VI. ANÁLISIS DEL ESPACIO DE LA CLAVE

El espacio de la clave es el número total de las combinaciones que pueden ser usadas en el sistema de encriptamiento. La clave para el algoritmo está compuesto de tres partes: parámetros de permutación, XOR etapa 1 y parámetros de la etapa II, XOR. Considerando solamente 6 parámetros; si la precisión es $10^{-16}$, el tamaño del espacio de la clave será $10^{16x6} = 10^{96} \approx 2^{320}$. Por consiguiente, el espacio de la clave es muy grande y puede resistir toda clase de ataque por fuerza bruta.

## VII. CALIDAD DE ENCRIPTAMIENTO

Al aplicar el algoritmo de encriptamiento de una imagen, se modifican los valores de los pixeles de la IO. La calidad de encriptamiento puede ser expresada como la desviación de la intensidad de los pixeles en la IE con respecto a los pixeles de la IO. La desviación se obtiene calculando la matriz "X", la cual representa el valor absoluto de la desviación entre cada valor del pixel antes y después del encriptamiento. Se obtiene el histograma de las diferencias y se calcula el valor promedio "D" seguido de "S" (valor absoluto de la diferencia de los valores del histograma menos "D"). Finalmente se determina el parámetro de calidad de encriptamiento AS (suma de las diferencias S) (Elkamchouchi & Makar, 2005).

Resumen de los pasos para obtener AS :

1. $X = \left| IO - IE \right|$
2. $H = histograma\left( X \right)$
3. $D = \frac{1}{256}\sum_{i=0}^{255} h_i$ (13)
4. $S(i) = \left| H(i) - D \right|$ (14)
5. $AS = \sum_{i=0}^{255} D(i)$ (15)

X: Matriz de diferencias entre pixeles.
H: Distribución histograma.
hi: La amplitud de las diferencias absolutas.

El algoritmo produce un AS=21,450, para una imagen a color el valor esperado es ≈ 18,000, por lo cual el AS es un buen resultado para la Calidad de Encriptamiento.

## VIII. ATAQUE DIFERENCIAL

Para probar la influencia del cambio de un pixel en la IO por el algoritmo propuesto sobre la IE, se usaron dos factores: NPCR y UACI (Chen & Ueta, 1999). El porcentaje de cambio en los pixeles de la IE (NPCR). El promedio de las diferencias en las intensidades de la IE (UACI).

Se toman dos IE, $C_1$ y $C_2$ del mismo tamaño cuyas correspondientes imágenes originales tienen solamente un pixel de diferencia. Asignamos los valores de escala de grises de los pixeles a los valores de (i , j) de $C_1$ y $C_2$ con $C_1$ (i , j) y $C_2$ (i , j). D (i, j) es determinada por $C_1$ (i, j) y $C_2$ (i, j), esto es; si $C_1$ (i, j) = $C_2$ (i, j) entonces D (i, j)= 0 o de otra forma D (i, j)= 1. El NPCR y el UACI son definidos por las siguientes ecuaciones:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (16)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (17)$$

donde W y H son el ancho y largo de la imagen. En una corrida se obtuvieron NPCR =72.4% y UACI = 36.3458 %. Con estos resultados, se observa que el algoritmo propuesto puede resistir el ataque diferencial.

## IX. CONCLUSIONES

En este trabajo, se propone un algoritmo de encriptamiento con CMCT con el fin de contribuir en la investigación de los sistemas dinámicos con enfoque al encriptamiento de imágenes, permutando caóticamente los pixeles de la imagen original. Otro CMCT es usado en el proceso de difuminación. Según el análisis realizado, el algoritmo de encriptamiento y desencriptamiento presentado puede cumplir los requisitos de alto nivel de seguridad, gran espacio de clave y velocidad de encriptamiento aceptable para una imagen a color de longitud (m,n,k). En trabajos posteriores se presentarán aplicaciones para transmisión de información en internet, como mensajeros y correos electrónicos, tomando en cuenta el impacto en la transmisión de mensajes privados.

## AGRADECIMIENTOS

Este trabajo fue patrocinado por el PROMEP, bajo el proyecto con autorización **PROMEP103.5/07/2636**.

## REFERENCIAS

Alvarez G.,Li S (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151.

Bu S.L, Wang B.H (2004). Improving the security of chaotic encryption by using a simple modulating method. Chaos, Solitons & Fractals 19, 919–924.

Chen G.R, Mao Y.B, et al (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 21, 749–61.

Chen, G. & Ueta, T,(1999). Yet another chaotic attractor. Int. J. Bifurcation and chaos 9, 1465-1466.

Chiaraluce F, Ciccarelli L, et al (2002).A new chaotic algorithm for video encryption. IEEE Trans Consum Electron 48,838–43.

Cruz-Hernández. C., López-Mancilla, D., García-Gradilla. V., Serrano-García. H., y Nuñez-Pérez, R.
(2005). Experimental realization of binary signals transmission using chaos. Journal of Circuits, Systems and Computers 14, 453-468.

Elkamchouchi H. and Makar M. A (2005). Measuring encryption quality of bitmap images encrypted with Rijndael and KAMKAR block ciphers. Twenty Second National Radio Science Conference (NRSC 2005).,pp.C11, Cairo, Egypt, March 15-17.

Gámez G, L., Cruz-Hernández, C., López-Gutiérrez, R.M., García G.E.E (2009).
Synchronization of Chua's circuits with multi-scroll Application to communication.. Commun Nonlinear Sci Numer Simulat 14, 2765-2775.

Gámez G. L., Cruz Hernández. C., López Gutiérrez .R.M.,y García G.E.E.( 2008).
Synchronization of multi-scroll chaos generators: application to private communication. Revista Mexicana de Física 54(4),299-305.

Jafarizadeh, M. A., Behnia, S., Khorram, S. & Nagshara, H. (2001).
Hierarchy of chaotic maps with an invariant measure , J. Stat. Phys 104, 1013-1028.

Jafarizadeh, M. A. & Behnia, S. (2002). Hierarchy of chaotic maps with an invariant measure and their compositions, J. Nonlin. Math. Phys. 9, 1-16.

Kpcarev, L. (2001). Chaos-based cryptography: A brief overview, IEEE Circuits Syst. Mag 1, 6-21.

Li S., Alvarez G.,Li Z., Halang W. A. (2007). Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey.(2007). http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.5455v1.pdf.

Li S., Alvarez G., and Chen G (2005). Breaking a chaos-based secure communication acheme designed by an improved modulation method. Chaos, Solitons & Fractals, vol. 25, no. 1, pp. 109-120.

López-Gutiérrez,.R.M., Posadas Castillo, C., López-Mancilla, D. y Cruz-Hernández, C. (2009).
Communicating via robust synchronization of chaotic lasers. Chaos, Solitons and Fractals 42, 277-285.

Matthews R (1989). On the derivation of a chaotic encryption algorithm. Cryptologia 13, 29–42.

Nien, H.H., Huang,C.K., Changchien S.K., Shieh H.W.,Chen C.T., Tuan Y.Y.(2007). Digital color image encoding and decoding using a novel chaotic random generator. Chaos, Solitons and Fractals 32, 1070-1080.

Orue A. B., Fernández V., Alvarez G., Pastor G. M.R., Montoya F.(2008). Determination of the Parameters for a Lorenz System and Application to Break the Security of Two-channel Chaotic Cryptosystems.

Pecora L.M. and Carroll T.L. (1990).Synchronization in chaotic systems, Phys. Rev. Lett.64, 821-824.

Ponomarenko, V.I. & Prokhorov, M. I (2002). Extracting information masked by the chaotic signal of a time-delay system, Phys. Rev. E 66, 026215.

Shannon C.E (1949). Communication theory of security systems. The Bell Syst Tech J. 28, 656-715.

Shannon C.E (1949). Communication Theory of Secrecy Systems. Bell Systems Techn. J. 28, 656-715.

Sohrab, Behnia.,Afshin A.,& Hadi M (2008). Chaotic cryptographic scheme based on composition maps. Int. J. Bifurcation and Chaos 18, 251-261.

Wang YW, Guan ZH, Wen XJ (2004). Adaptive synchronization for Chen chaotic system with fully unknown parameters. Chaos, Solitons & Fractals 19, 899–903.

Zhang LH, Liao XF, Wang XB (2005). An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals 24,759–65.