Memorias del Congreso Nacional de Control Automático
ISSN: 2594-2492

Encriptado de imágenes mediante DWT y osciladores caóticos de orden fraccionario ⋆

M.A. Platas-Garza, * **O. García-Sepulveda,** *
J.R. Rodríguez-Cruz, * **D.A. Diaz-Romero,** *
A.E. Loya-Cabrera, * **C. Posadas-Castillo.** *

* *Universidad Autónoma de Nuevo León,*
Facultad de Ingeniería Mecánica y Eléctrica,
Av. Universidad s/n. Cd. Universitaria, San Nicolás de los Garza,
Nuevo León, México, C.P. 66450.

Resumen: Se presenta un proceso de compresión y encriptado de imágenes en escala de grises. El proceso de compresión emplea el uso de la Transformada Wavelet Discreta (DWT), mientras que el proceso de encriptado emplea el uso de osciladores de orden fraccionario y un conjunto de operaciones digitales entre los estados del sistema y la señal a encriptar. Mientras que el uso de una etapa de compresión disminuye la carga computacional necesaria para realizar el encriptado, el orden fraccionario usado, así como el orden y el tipo de operaciones realizadas aumenta el espacio llave.

Keywords: Encriptado, DWT, Caos, Sistemas de Orden Fraccionario, Cyberseguridad.

1. INTRODUCCIÓN

Este documento aborda el encriptado de imágenes. Sea entendido el encriptado como el proceso de distorsionar la información privada para que sea ilegible por usuarios no deseados. Debido a su naturaleza aparentemente aleatoria los osciladores caóticos han sido propuestos y usados en esquemas de comunicaciones seguras. Generalmente en estas aplicaciones el espacio llave consiste en el atractor usado, sus parámetros y sus condiciones iniciales [Khan and Ahmad (2019))], [Guan et al. (2005)].

Una alternativa para aumentar el espacio llave, en sistemas de encriptado basados en caos, es el uso de osciladores caóticos de orden fraccionario [Li and Chen (2004)]. En estos casos, el orden puede variar en ciertos intervalos garantizando caos y una dinámica con sensibilidad extrema al mismo.

Con respecto al proceso de encriptado, éste se realiza generalmente al aplicar una operación entre los estados del sistema y la imagen original píxel por píxel [Tlelo-Cuautle et al. (2015)]. Existen operaciones que pueden provocar un cambio de resolución y por lo tanto perdida de información, tales como el encriptamiento aditivo [Soriano-Sánchez et al. (2015)]. Por otro lado, para garantizar la no distorsión del mensaje original, es preferible el realizar operaciones digitales reversibles tales como permutaciones de bits a nivel píxel y de píxeles a nivel imagen. Generalmente rondas de estas operaciones son realizadas, algunos ejemplos de esta metodología son abordados por [Aslam et al. (2019)], [Murillo-Escobar et al. (2015)].

Una alternativa al procesamiento píxel a píxel de la imagen original es hacer uso de sistemas de compresión/descompresión de imágenes. Mismos que pueden ser usados para disminuir la carga computacional del proceso y reducir el peso del mensaje encriptado añadiendo un procesamiento extra que puede contribuir al cifrado. Algunas de las transformaciones usadas en la literatura para compresión son: La transformada coseno discreto [Lima et al. (2013)], y la transformada wavelet discreta (DWT) [Pradhan et al. (2012)], [Wu et al. (2016)].

En este documento se propone un esquema de encriptado en el cual se aplican $\beta \in \aleph$ operaciones de encriptado basado en caos fraccionario, considerando operaciones reversibles en cascada entre los estados de un sistema caótico de orden fraccionario y una imagen a encriptar. Asimismo, se proponen etapas de compresión y descompresión mediante DWT para reducir la cantidad de datos a enmascarar por el sistema. Como resultados, se presentan dos casos de estudio en los que se encriptan las imágenes de prueba Lena y Barbara. Los resultados son analizados vía histogramas y la relación señal a ruido.

2. PRELIMINARES

A continuación se abordan definiciones y los preliminares matemáticos sobre el cálculo fraccionario, osciladores

⋆ M.A. Platas-Garza, miguel.platasgrz@uanl.edu.mx, O. García-Sepulveda, otoniel.garcia90@hotmail.com, J.R. Rodríguez-Cruz, jose.rodriguezcu@uanl.edu.mx, D.A. Diaz-Romero, ddiaz.uanl@gmail.com, A.E. Loya-Cabrera, aloya67@gmail.com, C. Posadas-Castillo, cornelio.posadascs@uanl.edu.mx.

caóticos, sincronización maestro esclavo y esquemas de compresión.

2.1 Cálculo fraccionario

La teoría de cálculo fraccional generaliza las operaciones de integración y diferenciación a ordenes no enteros. El operador integro-diferencial fraccionario continuo que define tales operaciones es definido por

$$ {}_aD_t^q = \begin{cases} \dfrac{d^q}{dt^q}, & q > 0, \\ 1, & q = 0, \\ \displaystyle\int_a^t (d\tau)^{-q}, & q < 0, \end{cases} \tag{1} $$

donde $a, t \in \Re$ son las cotas de la operación y $q \in \Re$ representa el orden.

Con la finalidad de resolver el problema de integración fraccionaria de manera numérica, la definición de Grünwald-Letnikov (GL) para el operador ${}_aD_t^q$ puede ser usada para la aplicación del operador fraccionario a una secuencia $f(k)$ muestreada con un paso h. Lo anterior deriva en la siguiente relación

$$ {}_{k-L_m/h}D_{t_k}^q f(t) \approx h^{-q} \sum_{j=0}^{L_m-1} c_j^{(q)} f(k-j), \tag{2} $$

con $L_m \in \aleph$ representando la cantidad de muestras considerada en la longitud de memoria, y $c_j^{(q)} \in \Re$ los coeficientes binomiales

$$ c_0^{(q)} = 1, \tag{3} $$

$$ c_j^{(q)} = \left(1 - \frac{1+q}{j}\right) c_{j-1}^{(q)}. \tag{4} $$

Entonces, una aproximación a la solución numérica de la ecuación diferencial fraccionaria dada por

$$ {}_aD_t^q y(t) = f(y(t), t), \tag{5} $$

se puede expresar por

$$ y(t_k) = f(y(t_k), t_k) h^q - \sum_{j=v}^{k} c_j^{(q)} y(t_k - j). \tag{6} $$

2.2 Oscilador caótico fraccionario de Liu

El modelo matemático para un oscilador de Liu de orden fraccionario es definido por

$$ \begin{cases} {}_0D_t^{q_1} x(t) &= -ax(t) - ey^2(t), \\ {}_0D_t^{q_2} y(t) &= by(t) - kx(t)z(t), \\ {}_0D_t^{q_3} z(t) &= -dz(t) + mx(t)y(t). \end{cases} \tag{7} $$

El conjunto de ecuaciones (7) exhibe caos para los parámetros $(a, e, b, k, d, m) = (1, 1, 2{,}5, 4, 5, 4)$ y un orden conmensurado $q_1 = q_2 = q_3 = q_4 = q =$0.95. La Fig. 1 muestra el atractor extraño y la evolución temporal del estado $z(t)$ de dicho oscilador.

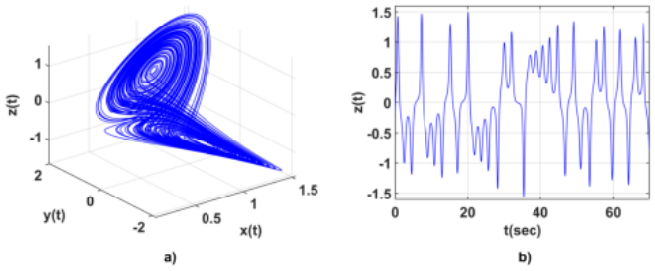


Figura 1. a) Atractor del oscilador de Liu fraccionario para parámetros $(a, e, b, k, d, m) = (1, 1, 2{,}5, 4, 5, 4)$, y condiciones iniciales $(x(0), y(0), z(0), w(0)) =$ (0.485,0.922,-0.126) proyectado en $(x(t), y(t), z(t))$. b) Evolución temporal de la variable de estado $z(t)$.

2.3 Sincronización maestro-esclavo

En Pecora and Carroll (1990) es mostrado que, los sistemas son capaces de alcanzar sincronía, si los signos de los exponentes de Lyapunov de los subsistemas son todos negativos. En dicho trabajo se explica que, la capacidad para alcanzar sincronía no es obvia en sistemas no-lineales.

Por ejemplo, considere el sistema n dimensional

$$ \frac{du}{dt} = f(u). \tag{8} $$

La eq. (8) puede ser dividida en dos subsistemas como sigue

$$ \frac{dv}{dt} = g(v, w), \quad \frac{dw}{dt} = h(v, w), \tag{9} $$

donde $v = (u_1, ..., u_m)$, $g = (f_1(u), ..., f_m(u))$, $w = (u_{m+1}, ..., u_n)$, y $h = (f_{m+1}(u), ..., f_n(u))$.

Sea w' un nuevo subsistema idéntico al sistema w. El conjunto de variables v son substituidas por las variables v' correspondientes en la función $h(\cdot)$. El nuevo sistema es añadido en la eq. (9) resultando en

$$ \frac{dv}{dt} = g(v, w), \quad \frac{dw}{dt} = h(v, w), \quad \frac{dw'}{dt} = h(v, w'). \tag{10} $$

Los subsistemas w y w' alcanzan sincronía solo si, $\Delta w = w' - w \to 0$ conforme $t \to \infty$.

2.4 Compresión de imágenes

La compresión de una señal se realiza mediante la aplicación de etapas de transformación, cuantización y codificación [Antonini et al. (1992)]. En el caso de imágenes, la etapa de transformación puede realizarse mediante la DWT [Grgic et al. (2001)], [Du and Fowler (2007)] tal como lo establece el estándar JPG2000. La codificación piramidal usada por este algoritmo consiste en separar la

generalidad del detalle mediante cambios en resolución y filtrado.

En el compresor, los filtros de análisis procesan los componentes frecuenciales en cada dimensión de la imagen, separando el detalle de alta frecuencia de la generalidad en baja frecuencia. Al finalizar el proceso de análisis, cuatro matrices de coeficientes son obtenidas LL, LH, HL y HH, las cuales representan la aproximación y los detalles en las direcciones horizontal, vertical y diagonal respectivamente. Asimismo, en una codificación de N niveles el proceso se aplica iterativamente a la generalidad de baja frecuencia LL del nivel anterior, tal y como lo muestra la Fig. 2.

De manera inversa, en la decodificación existen filtros de síntesis que se encargan de unir el detalle en cada banda con la aproximación de baja resolución para recuperar la imagen original. En procesos de compresión la cuantificación de coeficientes en los conjuntos LL, LH, HL y HH provoca una distorsión no reversible a pesar de que los filtros cumplan con condiciones de perfecta reconstrucción.

3. MÉTODO DE ENCRIPTADO PROPUESTO

Se considera el encriptado de una imagen ${}_Q U^{(N,N)}$ en escala de grises, en la que, abusando de la notación, el superíndice $(\cdot)^{(N,N)}$ y el subíndice ${}_Q(\cdot)$ indican las dimensiones del arreglo, y el número de Q bits usados para representar los elementos $u(n,m)$ del arreglo respectivamente. El procesamiento de enmascaramiento se describe a continuación:

3.1 Proceso de compresión y cuantificación

En la etapa de compresión, se aplica una DWT de η niveles a ${}_Q U^{(N,N)}$, resultando en una aproximación LL $U^{(M,M)}$ con $M \approx \frac{N}{\eta}$, y 3η grupos de coeficientes en distintas escalas. Debido a que la mayoría de las imágenes naturales son de naturaleza pasa bajas, solamente se considera como aproximación a $U^{(M,M)}$ y se descartan los detalles de alta frecuencia en las componentes horizontal, vertical y diagonal.

Posteriormente, se aplica cuantización a cada píxel de $U^{(M,M)}$ generando la señal ${}_Q U^{(M,M)}$. La cuantización uniforme se realiza con 2^Q niveles dentro del rango de $U^{(M,M)}$.

3.2 Proceso de encriptado

Dados cierto orden fraccionario y ciertas condiciones iniciales, se generan $K = M^2 + \delta$ muestras de una señal caótica de orden fraccionario usando el método de integración de GL. $\delta > 0$ es un entero lo suficientemente grande tal que δh cubre el tiempo necesario para garantizar la sincronización maestro-esclavo de los osciladores en el codificador y decodificador. Los estados del oscilador

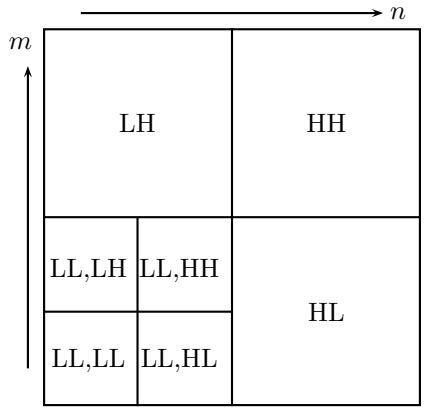


Figura 2. DWT de dos niveles. El siguiente nivel es aplicado a la generalidad LL del nivel anterior.

son cuantizados en Q bits y los últimos M^2 valores de cada estado son almacenados en los arreglos ${}_Q X^{(M,M)}$, ${}_Q Y^{(M,M)}$ y ${}_Q Z^{(M,M)}$.

Se aplican β operaciones entre la imagen de entrada y los estados del sistema caótico de orden fraccionario para generar la imagen encriptada ${}_Q E_\beta^{(M,M)}$. Las operaciones se aplican en cascada, ejecutando cada operación entre algún estado del sistema ${}_Q S_\beta^{(M,M)}$ y el resultado de la operación anterior ${}_Q E_{\beta-1}^{(M,M)}$. Denotando el conjunto de operaciones por las funciones $\{\psi_1, \psi_2, \ldots, \psi_\beta\}$, se tiene que la imagen encriptada de β niveles es dada por:

$$ {}_Q E_\beta^{(M,M)} = \psi_\beta \left\{ {}_Q S_\beta^{(M,M)},\ {}_Q E_{\beta-1}^{(M,M)} \right\}, \tag{11} $$

donde

$$ {}_Q E_{\beta-1}^{(M,M)} = \psi_{\beta-1} \left\{ {}_Q S_{\beta-1}^{(M,M)},\ {}_Q E_{\beta-2}^{(M,M)} \right\}, \tag{12} $$

$$ {}_Q E_{\beta-2}^{(M,M)} = \psi_{\beta-2} \left\{ {}_Q S_{\beta-2}^{(M,M)},\ {}_Q E_{\beta-3}^{(M,M)} \right\}, \tag{13} $$

$$ \vdots \tag{14} $$

$$ {}_Q E_1^{(M,M)} = \psi_1 \left\{ {}_Q S_1^{(M,M)},\ {}_Q E_0^{(M,M)} \right\}, \tag{15} $$

con ${}_Q E_0^{(M,M)} =_Q U^{(M,M)}$ siendo la salida del compresor.

Operaciones de encriptado Las operaciones consideradas en este trabajo son:

1. Operación or exclusivo (XOR). La j-ésima operación del esquema puede involucrar la operación XOR

$$ {}_Q E_j^{(M,M)} = \psi_j \left\{ {}_Q S_\beta^{(M,M)},\ {}_Q E_{j-1}^{(M,M)} \right\}, \tag{16} $$

$$ = {}_Q S_\beta^{(M,M)} \oplus {}_Q E_{j-1}^{(M,M)}, \tag{17} $$

misma que se se realiza a nivel bit entre todos los píxeles de la imagen

$$ {}_Qe_j(n,m) =_Q s_\beta(n,m) \oplus {}_Qe_{j-1}(n,m), \quad (18) $$

donde ${}_Qe_j(n,m)$, ${}_Qs_\beta(n,m)$ y ${}_Qe_{j-1}(n,m)$ indican el n-ésimo píxel de la m-ésima fila de ${}_QE_j^{(M,M)}$, ${}_QS_\beta^{(M,M)}$ y ${}_QE_{j-1}^{(M,M)}$ respectivamente.

2. Operación rotación circular de bits a la derecha (CIRCR). La j-ésima operación del esquema puede involucrar la operación CIRCR

$$ {}_QE_j^{(M,M)} = \psi_j \left\{ {}_QS_\beta^{(M,M)},\ {}_QE_{j-1}^{(M,M)} \right\}, \quad (19) $$

$$ = {}_QS_\beta^{(M,M)} \odot_R {}_QE_{j-1}^{(M,M)}, \quad (20) $$

misma que al igual que la operación XOR, se aplica a nivel bit entre dos píxeles de la imagen. La operación $\odot_R$ en la Eq. (19) indica que los Q bits que conforman el elemento ${}_Qe_{j-1}(n,m)$ de rotan circularmente del bit de mayor peso al de menor peso el número entero dado por el elemento ${}_Qs_\beta(n,m)$.

3. Operación rotación circular de bits a la izquierda (CIRCL). Denotada por $\odot_L$ y similar a CIRCR, pero con la rotación circular del bit de menor peso al de mayor peso.
4. Operación rotación píxeles en una linea a la derecha (PIXR), y a la izquierda (PIXL). Denotadas por $\ominus_R$ y $\ominus_L$, similares a CIRCR y CIRCL, pero la rotación circular se hace a nivel píxel sobre las lineas horizontales de la imagen.

3.3 Proceso de desencriptado

Suponga que el decodificador dispone de los estados ${}_Q\tilde{X}^{(M,M)}$, ${}_Q\tilde{Y}^{(M,M)}$, ${}_Q\tilde{Z}^{(M,M)}$ similares a los del codificador, o de la información llave para generarlos (condiciones iniciales, orden fraccionario, niveles de cuatización, y tamaño de imagen M). Además suponga que se dispone tipo y del orden en el que las operaciones de encriptado fueron realizadas, así como el estado seleccionado para realizar cada operación. Entonces, la imagen recuperada ${}_Q\hat{U}_\beta^{(M,M)}$ puede computarse a partir del dato transmitido al decodificador ${}_Q\tilde{E}_\beta^{(M,M)}$ al aplicar las operaciones en orden inverso

$$ {}_Q\hat{U}_\beta^{(M,M)} = \tilde{\psi_1} \left\{ {}_Q\tilde{S}_1^{(M,M)},\ {}_Q\tilde{E}_1^{(M,M)} \right\}, \quad (21) $$

$$ {}_Q\hat{E}_1^{(M,M)} = \tilde{\psi_2} \left\{ {}_Q\tilde{S}_2^{(M,M)},\ {}_Q\tilde{E}_2^{(M,M)} \right\}, \quad (22) $$

$$ \vdots \quad (23) $$

$$ {}_Q\hat{E}_{\beta-2}^{(M,M)} = \tilde{\psi_{\beta-1}} \left\{ {}_Q\tilde{S}_{\beta-1}^{(M,M)},\ {}_Q\tilde{E}_{\beta-1}^{(M,M)} \right\} \quad (24) $$

$$ {}_Q\hat{E}_{\beta-1}^{(M,M)} = \tilde{\psi_\beta} \left\{ {}_Q\tilde{S}_\beta^{(M,M)},\ {}_Q\tilde{E}_\beta^{(M,M)} \right\}. \quad (25) $$

La operación dual $\tilde{\psi_j}$ es tal que cancela la operación ψ_j. El mensaje original se recuperará sin error si los estados en el decodificador y codificador son idénticos

$$ {}_Q\tilde{S}_j^{(M,M)} =_Q S_j^{(M,M)}, \quad j = 1,2,\ldots,\beta, \quad (26) $$

y el mensaje no fue corrompido durante su transmisión

$$ {}_Q\tilde{E}_\beta^{(M,M)} =_Q E_\beta^{(M,M)}. \quad (27) $$

Descompresión Si en adición se dispone de información sobre la wavelet y los niveles usadas en la compresión. Entonces es posible recuperar un estimado ${}_Q\hat{U}_\beta^{(N,N)}$ de la imagen en su resolución original al aplicar IDWT a ${}_Q\hat{U}_\beta^{(M,M)}$.

4. ANÁLISIS DE DESEMPEÑO DEL ALGORITMO PROPUESTO

En lo siguiente se aborda el estudio del desempeño del algoritmo de encriptado propuesto. Como casos de estudio se usan las imágenes de prueba Lena y Barbara. Las imágenes usadas son mostradas en las Figs. 3(a) y 4(a). Se propone analizar dos imágenes variando los parámetros de encriptado y analizar los resultados.

4.1 Espacio llave

El espacio de la llave refleja una medición de la seguridad del sistema en la criptografía. En el caso propuesto está formado por $\{x(0), y(0), z(0), q, \psi_1, \psi_2 \ldots \psi_\beta\}$. Los factores que contribuyen a aumentar dicho espacio son:

1. Condiciones iniciales del sistema caótico. Cuantizadas con 18 decimales generan 10^{54} valores posibles.
2. Orden fraccionario del sistema. Considerando un orden conmensurado cuantizado a 18 decimales genera 10^{18} valores posibles.
3. Tipo de operación y estado con el que se realizan las operaciones de encriptado. Considerando un sistema de 3 estados y las 3 operaciones definidas anteriormente, se tienen 9 posibles operaciones por etapa. Por lo que un sistema de encriptado en β etapas genera por 9^β valores posibles.

Note que el espacio llave aumenta debido a la naturaleza fraccionaria del sistema caótico involucrado en el encriptado.

4.2 Imágenes encriptadas

Se consideran 2 imágenes en el presente trabajo. Para cada una de ellas la imagen original, la imagen comprimida, la imagen encriptada, la imagen recuperada y la imagen descomprimida son mostradas en las Figs. 3-4. En todos los casos presentados se procesan imágenes con resolución de 512 x 512 píxeles. En los casos presentados en las Figs. 3-4 se usa una wavelet db04 de 2 niveles reduciendo las imágenes a aproximaciones pasa bajas de $M \times M$ píxeles con $M = 133$ que son cuantizadas con 8 bits. Resultados similares a los de las Figs. 3-4 usando distintos parámetros de compresión fueron obtenidos, el desempeño para distintos niveles es reportado en la Tabla 1. En la etapa de encriptado se usa el oscilador de Liu descrito en (7) con un orden conmensurado q =0.95 y un

(a) (b) (c) (d) (e)

Figura 3. Resultados para la imagen de Lena. (a) Imagen original ${}_{Q}U^{(N,N)}$; (b) Imagen comprimida mediante DWT y cuantizada uniformemente ${}_{Q}U^{(M,M)}$; (c) Imagen encriptada al aplicar el conjunto de operaciones a la compresión ${}_{Q}E_{\beta}^{(M,M)}$; (d) Imagen desencriptada ${}_{Q}\hat{U}_{\beta}^{(M,M)}$ al aplicar las operaciones en orden inverso. (e) Imagen descomprimida ${}_{Q}\hat{U}_{\beta}^{(N,N)}$ al aplicar IDWT.

(a) (b) (c) (d) (e)

Figura 4. Resultados para la imagen Barbara. (a) Imagen original ${}_{Q}U^{(N,N)}$; (b) Imagen comprimida mediante DWT y cuantizada uniformemente ${}_{Q}U^{(M,M)}$; (c) Imagen encriptada al aplicar el conjunto de operaciones a la compresión ${}_{Q}E_{\beta}^{(M,M)}$; (d) Imagen desencriptada ${}_{Q}\hat{U}_{\beta}^{(M,M)}$ al aplicar las operaciones en orden inverso. (e) Imagen descomprimida ${}_{Q}\hat{U}_{\beta}^{(N,N)}$ al aplicar IDWT.

paso de integración de h =0.017 segundos. En el codificador y decodificador se implementa un sistema caótico de orden fraccionario para generar $M^2+\delta$ muestras de cada uno de sus estados, con $\delta = 1000$. De las cuales, las M^2 muestras finales son cuantizadas con $Q = 8$ bits y almacenadas en matrices de dimensión $M \times M$ denotadas por ${}_{Q}X^{(M,M)}$, ${}_{Q}Y^{(M,M)}$ y ${}_{Q}Z^{(M,M)}$ para el codificador y ${}_{Q}\tilde{X}^{(M,M)}$, ${}_{Q}\tilde{Y}^{(M,M)}$ y ${}_{Q}\tilde{Z}^{(M,M)}$ para el decodificador.

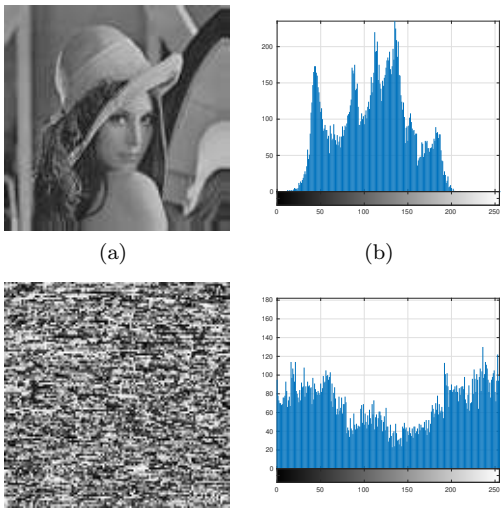
Con respecto a las operaciones de encriptado, para los casos mostrados en las Figs. 3-4 se consideran $\beta = 3$ operaciones en el codificador

$${}_{Q}E_{3}^{(M,M)} = \left({}_{Q}Z^{(M,M)} \odot_{R} \left({}_{Q}X^{(M,M)} \oplus \left({}_{Q}X^{(M,M)} \ominus_{RQ}U^{(M,M)}\right)\right)\right)$$

con sus correspondientes operaciones en el decodificador dadas por:

$${}_{Q}\hat{U}^{(M,M)} = \left({}_{Q}\tilde{X}^{(M,M)} \ominus_{L} \left({}_{Q}\tilde{X}^{(M,M)} \oplus \left({}_{Q}\tilde{Z}^{(M,M)} \odot_{LQ}E_{3}^{(M,M)}\right)\right)\right).$$

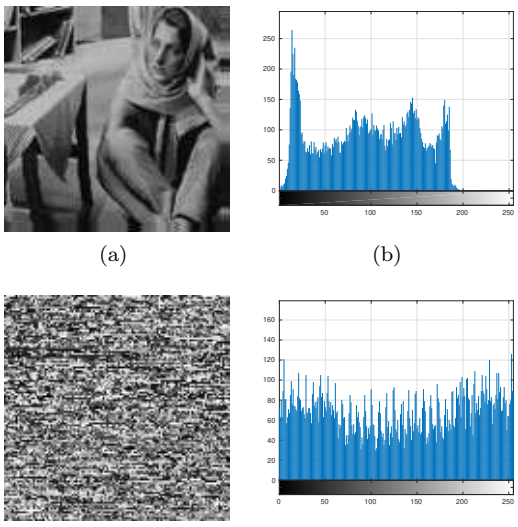
Si los estados en el codificador son idénticos a los estados en el decodificador la operación de encriptado no provoca distorsión, siendo la cuantización y selección de



(a) (b)

(c) (d)

Figura 5. Histogramas para la imagen Lena antes y después del encriptado. (a) Etapa anterior al encriptado ${}_QU^{M,M}$, (b) Histograma de ${}_QU^{M,M}$, (c) Etapa posterior al encriptado ${}_QE_\beta^{M,M}$, (d) Histograma de ${}_QE_\beta^{M,M}$.



(a) (b)

(c) (d)

Figura 6. Histogramas para la imagen Barbara antes y después del encriptado. (a) Etapa anterior al encriptado ${}_QU^{M,M}$, (b) Histograma de ${}_QU^{M,M}$, (c) Etapa posterior al encriptado ${}_QE_\beta^{M,M}$, (d) Histograma de ${}_QE_\beta^{M,M}$.

componentes LL en la compresión los únicos procesos que provocan perdida de información. Sin embargo, incluso usando las mismas condiciones iniciales es posible que los estados de los sistemas diverjan debido a redondeos computacionales. Por lo tanto, para garantizar que ${}_Q\tilde{X}^{(M,M)} \approx {}_QX^{(M,M)}$ es necesario garantizar la sincronización de ambos sistemas. En este trabajo, lo anterior se logra mediante la sincronización maestro-esclavo descrita en la sección 2.3 compartiendo el estado ${}_QY^{(M,M)}$ del codificador (maestro) al decodificador (esclavo).

4.3 Histogramas y entropía

Los histogramas miden la distribución de los valores de los píxeles dentro del campo finito de posibles valores. Para un buen encriptado, el histograma de la imagen encriptada debe de ser uniformemente distribuido indicando que cada valor de cuantización tiene la misma posibilidad de aparecer. Además, el histograma encriptado no debe de ser semejante al histograma original. Los histogramas para las imágenes antes y después del encriptado son mostrados en las Figs. 5-6. Note que en todos los casos se cumple con las condiciones anteriores.

La entropía de una imagen en escala de grises cuantizada con Q bits está definida por

$$H = -\sum_{l=0}^{Q-1} p_l \log_2(p_l), \tag{28}$$

donde p_l representa la probabilidad de ocurrencia del l-ésimo nivel de gris en la imagen.

La entropía en el caso de la imagen mostrada en la Figs. 5(c) es de 7.8682, y de 7.9438 para el caso de la Fig. 6(c). Lo anterior es cercano al valor ideal de 8 obtenido para una imagen con intensidades en sus píxeles definidas por una distribución aleatoria uniformemente.

4.4 Relación señal a ruido

La Tabla 1 presenta la proporción máxima de la relación señal a ruido (PSNR) entre la imagen original ${}_QU^{(N,N)}$ y la recuperada ${}_Q\hat{U}_\beta^{(N,N)}$. Este índice está definido por

$$\text{PSNR}_T = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right), \tag{29}$$

con MSE denotando el error cuadrático medio, que es definido por

$$\text{MSE} = \frac{1}{N^2}\sum_{n=1}^{N}\sum_{m=1}^{N}\left(u(n,m) - \hat{u}(n,m)\right)^2 \tag{30}$$

y es afectado de igual manera por los procesos de compresión y encriptado.

Para los casos de la Tabla 1 en los que $\beta = 1$ se aplica solamente la operación CIRCR, para $\beta = 2$ se aplica CIRCR + XOR, y finalmente para $\beta = 3$ se aplica CIRCR + XOR + PIXR.

En adición, la Tabla 1 presenta el PSNR_E calculado a partir de ${}_QU^{(M,M)}$ y ${}_QE_\beta^{(M,M)}$ como una medida de la calidad del encriptado. Note que, en general, para todos los casos presentados se tiene que el PSNR_E promedio es de 9.73 dB. Valores típicos de PSNR menores a 10 dB indican mayores posibilidades de enmascaramiento.

Imagen	Niveles η	Etapas β	PSNR_E	PSNR_T
Lena	1	1	8.65 dB	32.02 dB
	2	1	12.37 dB	25.54 dB
	3	1	8.66 dB	28.70 dB
	1	2	8.71 dB	35.02 dB
	2	2	12.63 dB	29.32 dB
	3	2	8.72 dB	25.54 dB
	1	3	8.60 dB	29.32 dB
	2	3	8.64 dB	29.32 dB
	3	3	10.73 dB	25.50 dB
Barbara	1	1	11.58 dB	21.20 dB
	2	1	8.11 dB	21.21 dB
	3	1	12.57 dB	35.02 dB
	1	2	11.58 dB	21.23 dB
	2	2	8.11 dB	23.32 dB
	3	2	11.55 dB	19.66 dB
	1	3	8.03 dB	21.21 dB
	2	3	8.02 dB	19.66 dB
	3	3	7.94 dB	19.67 dB

Cuadro 1. PSNR para diferentes conjuntos de parámetros.

Finalmente, se menciona que el promedio para PSNR_T es de 24.61 dB, dicho valor refleja las distorsiones sufridas en el proceso de cuantificación y la omisión de los coeficientes de detalle en la IDWT.

5. CONCLUSIÓN

Se plantea que el orden fraccionario usado permite aumentar la seguridad del sistema de cifrado al incrementar el espacio llave. La estructura flexible permite un proceso de encriptado reversible mediante β rondas de operaciones reversibles de la información. El uso de etapas de compresión posiblemente añade distorsión al sistema pero permite el encriptar la señal generando secuencias caóticas de menor longitud. Lo anterior permite reducir la carga del cifrado, la cual es considerable y debe de tomarse en cuenta ya que la integración numérica de orden fraccionario GL requiere una mayor carga computacional en comparación con métodos de orden entero debido a la longitud de memoria. La sincronización maestro-esclavo de dos sistemas caóticos fraccionarios fue realizada. Como trabajo futuro, es necesario profundizar en el proceso, para mejorar la aproximación de la señal es necesario incluir los componentes de detalle de la DWT en el proceso de encriptado. En adición, el estudio exhaustivo del error de aproximación así como de la comparación con otras metodologías de cifrado debe realizarse al considerar un conjunto mayor de métricas.

6. AGRADECIMIENTOS

Los autores agradecen al proyecto CONACyT: "Sincronización de sistemas complejos y algunas aplicaciones" ref. 166654 y A1-S-31628, y a FIME-UANL.

REFERENCIAS

Antonini, M., Barlaud, M., Mathieu, P., and Daubechies, I. (1992). Image coding using wavelet transform. *IEEE Transactions on Image Processing*, 1(2), 205–220.

Aslam, M.N., Belazi, A., Kharbech, S., Talha, M., and Xiang, W. (2019). Fourth order mca and chaos-based image encryption scheme. *IEEE Access*, 1–1.

Du, Q. and Fowler, J.E. (2007). Hyperspectral image compression using jpeg2000 and principal component analysis. *IEEE Geoscience and Remote Sensing Letters*, 4(2), 201–205.

Grgic, S., Grgic, M., and Zovko-Cihlar, B. (2001). Performance analysis of image compression using wavelets. *IEEE Transactions on Industrial Electronics*, 48(3), 682–695.

Guan, Z.H., Huang, F., and Guan, W. (2005). Chaos-based image encryption algorithm. *Physics Letters A*, 346(1), 153 – 157.

Khan, J.S. and Ahmad, J. (2019). Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, 30(2), 943–961.

Li, C. and Chen, G. (2004). Chaos and hyperchaos in the fractional-order rössler equations. *Physica A: Statistical Mechanics and its Applications*, 341, 55 – 61.

Lima, J., Lima, E., and Madeiro, F. (2013). Image encryption based on the finite field cosine transform. *Signal Processing: Image Communication*, 28(10), 1537 – 1547.

Murillo-Escobar, M., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R., and Campo, O.A.D. (2015). A rgb image encryption algorithm based on total plain image characteristics and chaos. *Signal Processing*, 109, 119 – 131.

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

Pradhan, C., Rath, S., and Bisoi, A.K. (2012). Non blind digital watermarking technique using dwt and cross chaos. *Procedia Technology*, 6, 897 – 904. 2nd International Conference on Communication, Computing & Security [ICCCS-2012].

Soriano-Sánchez, A., Posadas-Castillo, C., Platas-Garza, M., and Diaz-Romero, D. (2015). Performance improvement of chaotic encryption via energy and frequency location criteria. *Mathematics and Computers in Simulation*, 112, 14 – 27.

Tlelo-Cuautle, E., Carbajal-Gomez, V.H., Obeso-Rodelo, P.J., Rangel-Magdaleno, J.J., and Núñez-Pérez, J.C. (2015). Fpga realization of a chaotic communication system applied to image processing. *Nonlinear Dynamics*, 82(4), 1879–1892.

Wu, X., Wang, D., Kurths, J., and Kan, H. (2016). A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system. *Information Sciences*, 349-350, 137 – 153.

