Algoritmo de encriptado empleando sistemas caóticos de orden no entero en imágenes médicas

Cornelio Posadas-Castillo[1], Ernesto Zambrano-Serrano[1*], Miguel Angel Platas-Garza[1], Pedro Javier García-Ramírez[2], José Ramón Rodríguez-Cruz[1]
[1]Facultad de Ingeniería Mecánica y Eléctrica, Universidad Autónoma de Nuevo León, N.L., México
[2]Facultad de Ingenieria, Universidad Veracruzana, México
cornelio.posadascs@uanl.edu.mx; ernesto.zambranos@uanl.edu.mx;
miguel.platasgrz@uanl.edu.mx; jagarcia@uv.mx; jose.rodriguezcu@uanl.edu.mx

RESUMEN

Una de las técnicas más eficientes para proteger las imágenes médicas es aplicar algoritmos basados en dinámica no lineal. En este trabajo se presenta un esquema de encriptación y compresión de imágenes médicas. El esquema se basa en sistemas caóticos de orden fraccionario, combinados con compresión por transformada de wavelet discreta. El encriptado realiza ciclos de operaciones digitales entre las soluciones del sistema dinámico y la imagen a encriptar, agregando las características de confusión y difusión a la imagen. Los resultados experimentales y análisis estadísticos muestran desempeños adecuados para aplicación en imágenes médicas en presencia de múltiples ataques y ruido.

PALABRAS CLAVE

Cálculo fraccionario, Sistema Caótico; Encriptación; Imágenes Biomédicas.

ABSTRACT

One of the most efficient techniques to protect medical images is to apply algorithms based on nonlinear dynamics. This paper presents an encryption and compression scheme for medical images. The scheme is based on fractional-order chaotic systems, combined with a discrete wavelet transform compression. The encryption performs digital cycle operations between the solutions of the dynamic system and the image to be encrypted, adding the characteristics of confusion and diffusion to the image. The experimental results and statistical analyzes show adequate performance for application in medical imaging in the presence of multiple seizures and noise.

KEYWORDS

Fractional calculus, Chaotic system; Encryption; Biomedical Imaging.

INTRODUCCIÓN

Con el rápido desarrollo de la tecnología en dispositivos médicos, ha llegado a ser muy común diagnosticar diferentes enfermedades por medio de utilizar imágenes médicas. Las imágenes médicas son parte relevante del *expediente clínico*, el cual es un instrumento de gran relevancia para la materialización del derecho a la protección de la salud, de acuerdo con la norma oficial mexicana NOM-004-SSA3-2012. El expediente clínico "es el conjunto único de información y datos personales de un paciente, puede estar integrado por documentos escritos, gráficos, imagenológicos, electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos y de otras tecnologías, mediante los cuales se hace constar en diferentes momentos del proceso de la atención médica, las diversas intervenciones del personal del área de la salud, así como describir el estado de salud del paciente; además de incluir en su caso, datos acerca del bienestar físico, mental y social del mismo".[1] Con la creciente popularidad de las comunicaciones inalámbricas, la seguridad de la información se ha vuelto esencial durante la transmisión de datos. Las imágenes médicas son comúnmente

trasmitidas a través de diferentes canales públicos, lo que implica que la seguridad de las imágenes y otros archivos multimedia requieren una seguridad sólida para garantizar su confidencialidad y la privacidad. Por lo tanto, el encriptado de imágenes como: mamografías, resonancias magnéticas, radiografías de tórax, tomografías, etc; es una de las estrategias más convenientes para proteger la seguridad de los datos personales de los pacientes contra ataques maliciosos. Dado que las imágenes médicas son los datos privados de los pacientes, garantizar la integridad, el almacenamiento y transmisión se ha convertido en un tema de interés.

Las imágenes tienen varias características, por ejemplo, alta redundancia, gran capacidad de datos, fuerte correlación entre píxeles adyacentes y baja entropía en comparación con el texto.[2] A diferencia de las imágenes tradicionales las imágenes médicas presentan una característica distintiva, es decir, en promedio presentan más del 70% de bits de valor 0, lo que hace que los algoritmos de encriptación que no consideran esa característica en su diseño, al ser aplicados a imágenes médicas, presenten resultados adversos. En términos generales, se ha observado que la alta proporción de bits de valor 0 degrada el impacto de encriptado de las operaciones de permutación y sustitución.[3] En consecuencia, existe la necesidad de un algoritmo de encriptación de imágenes, adecuado y eficiente con la finalidad de adaptarse al desafío del alto número de bits de valor 0 presentes en las imágenes médicas. Además, debe responder a la baja complejidad y alta eficiencia que requieren las aplicaciones de comunicaciones inalámbricas.

Es bien sabido que el Estándar de Encriptado Avanzado (*Advanced Encryption Standard*, AES) es un encriptado de bloque que tiene varias ventajas cuando se trata de cifrar texto. Tiene un enfoque de encriptado relativamente rápido y un algoritmo robusto contra la piratería. Además, de acuerdo con,[3] para una clave de 128 bits, se necesitan alrededor de 2^{128} intentos para descifrarla. Sin embargo, el encriptado AES no es adecuado para datos multimedia ya que es computacionalmente extenuante; como consecuencia se requiere más tiempo computacional y no es lo suficientemente factible para el encriptado de imágenes médicas. Por lo tanto, numerosos investigadores en el campo del encriptado de imágenes han propuesto nuevos encriptados para reducir la correlación y la redundancia entre pixeles.[5] En[6] se presenta un algoritmo de encriptación de imágenes médicas el cual consiste en insertar datos aleatorios, codificación de alta velocidad y la difusión adaptativa de pixeles.

En particular, se ha observado que, los sistemas caóticos se utilizan ampliamente en criptografía. Debido a propiedades específicas del caos como la ergodicidad, la sensibilidad a las condiciones iniciales/parámetros del sistema y las características pseudoaleatorias.[7] Estas propiedades están vinculadas a la aleatoriedad, la confusión y la difusión, que son necesarias para un buen encriptado. En el proceso de confusión, los píxeles de la imagen se reorganizan sin ningún cambio en sus valores, con el objetivo de ocultar las correlaciones entre los píxeles adyacentes. Mientras que, en el proceso de difusión, los valores de los píxeles se modifican secuencialmente, tratando de cambiar las características estadísticas de la imagen, de modo que una alteración menor en la imagen conduce a cambios significativos en la imagen encriptada.[8]

En general, un buen algoritmo de encriptado debe ser sensible a las claves de encriptado y el espacio de claves debe ser lo suficientemente grande como para resistir los ataques de fuerza bruta de los atacantes. Por lo tanto, los algoritmos de encriptado de imágenes basados en caos se han desarrollado en dos principales direcciones en los últimos años.[8] La primera tendencia es mejorar la seguridad del algoritmo mediante el diseño de un sistema con un mejor comportamiento caótico.[9] En,[10] se propone el encriptado de imágenes considerando el comportamiento dinámico de un sistema caótico de orden fraccionario para mejorar la robustez y la seguridad del algoritmo de encriptado. Otra forma es por medio de integrar el encriptado basado en el caos con otras tecnologías de encriptado para diseñar algoritmos con mayor seguridad. En,[11] se presenta un algoritmo para diseñar una caja de sustitución de $n \times n$-bits basada en series temporales generadas a partir de un mapa logístico. En,[12] se propone un esquema de encriptación de imágenes en color usando codificación de ADN basado en sincronización caótica.

Con base en la revisión y el análisis mostrados previamente, resumimos los estudios relacionados en las dos direcciones anteriores y combinamos las fortalezas de cada uno. Proponiendo un esquema

de encriptado eficiente en el que se consideran los procesos de compresión y encriptado de imágenes médicas. El algoritmo utiliza osciladores caóticos de orden fraccionario y rondas (ciclos) de operaciones digitales entre los estados vectoriales del sistema de orden fraccionario y la imagen a encriptar. Implementamos la transformada wavelet discreta DWT con el objetivo de reducir la cantidad de datos a enmascarar, así como disminuir la cantidad de iteraciones para el algoritmo de integración numérica de orden fraccionario Grünwald-Letnikov (GL). El análisis de seguridad y los resultados experimentales muestran que el algoritmo propuesto tiene un adecuado espacio de claves y sensibilidad a las claves, lo cual es eficiente frente a los ataques de fuerza bruta y estadísticos. Finalmente, la evaluación de este trabajo se realiza a través de medir la entropía de la información, el coeficiente de correlación, la tasa de número de píxeles cambiantes (*Number of Changing Pixel Rate*, NPCR) y la intensidad cambiada promedio unificada (*Unified Averaged Changed Intensity*, UACI).

METODOLOGÍA UTILIZADA

La metodología usada es descrita en la figura 1, donde se plantea un esquema de encriptado, compresión y transmisión. La transmisión se realiza por medio de dos radios NI-USRP del fabricante National Instruments. Una de las principales contribuciones de este trabajo es el analizar el efecto de cada etapa (encriptado, compresión y transmisión) de manera conjunta.

Oscilador de Liu de orden fraccionario (Generador de Caos)

En este artículo se considera el sistema caótico de Liu de orden fraccionario, el cual es definido de la siguiente forma:[8]

$$
\begin{aligned}
{}^{GL}D^{q}x(t) &= -ax(t) - ey(t)^{2},\\
{}^{GL}D^{q}y(t) &= by(t) - kx(t)z(t),\\
{}^{GL}D^{q}z(t) &= -dz(t) + mx(t)y(t),
\end{aligned}
$$

donde $x(t)$, $y(t)$, y $z(t)$ son variables de estado, a, b, d, e, k y m son parámetros positivos, $q \in (0,1)$ es el orden fraccionario, ${}^{GL}D^{q}$ es la derivada de orden fraccionario en el sentido de Grünwald-Letnikov. Los puntos de equilibrio del sistema y sus valores propios son mostrados en la tabla I, los cuales son obtenidos definiendo ${}^{GL}D^{q}x(t) = 0$, ${}^{GL}D^{q}y(t) = 0$, y ${}^{GL}D^{q}z(t) = 0$, considerando el siguiente conjunto de parámetros $a = 1, b = 2.5, d = 5, e = 1, k = 4$ y $m = 4$. Se observa que el sistema presenta tres puntos de equilibrio reales y dos imaginarios, respectivamente.

Las simulaciones numéricas se realizaron considerando el algoritmo propuesto por Grünwald-Letnikov e implementado en,[8] considerando el principio de memoria corta con valor de $L = 200$, un orden fraccionario $q = 0.95$, un paso de integración $h = 0.01$. En la figura 2, se muestran el plano de fase del sistema de Liu.

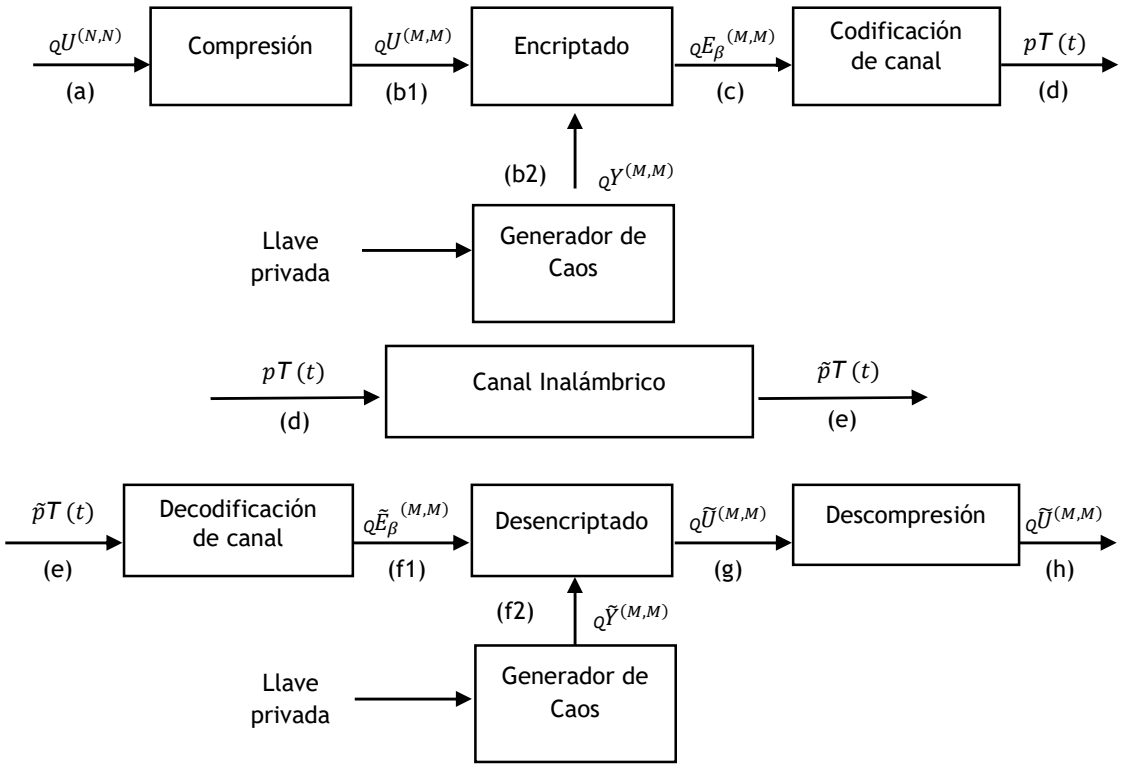


Fig. 1. Diagrama de bloques que describe la compresión, el encriptado y la transmisión inalámbrica de los datos. El estado $y(t)$ se utiliza en todas las operaciones de enmascaramiento realizadas. La marca (a) representa los datos a cifrar, (b1) los datos comprimidos, (b2) la llave en el codificador, (c) los datos encriptados, (d) los pulsos encriptados que se transmitirán, (e) el tren de pulsos recibido, (f1) los datos encriptados recuperados, (f2) la llave en el decodificador, (g) los datos comprimidos recuperados, (g) los datos recuperados.

Tabla I. Puntos de Equilibrio del sistema de Liu de orden fraccionario.

Puntos de Equilibrio	Valores propios	
	λ_1	$\lambda_{2,3}$
$E_1(0,0,0)$	-1	2.5, -5
$E_2(-0.8838,0.9401,-0.6647)$	-4.3877	$0.4438 \pm 3.3463i$
$E_3(-0.8838,-0.9401,0.6647)$	-4.3877	$0.4438 \pm 3.3463i$
$E_4(0.8838,0.9401i,0.6647i)$	-4.3877	$0.4438 \pm 3.3463i$
$E_5(0.8838,-0.9401i,-0.6647i)$	-4.3877	$0.4438 \pm 3.3463i$

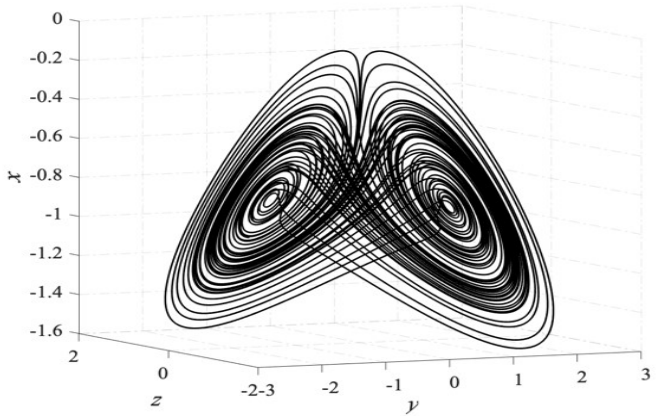


Fig. 2. Plano de fase del sistema de Liu de orden fraccionario $q = 0.95$.

Encriptado

Una llave de 128 bits es usada en este trabajo. Los bits de la llave representan una combinación de orden, y condiciones iniciales previamente preseleccionadas dentro de rangos finitos donde la existencia de caos es asegurada. Una vez seleccionada la llave adecuadamente considerando un cierto orden fraccionario, un conjunto de parámetros y condiciones iniciales, se generan $K = M^2$ muestras de la señal caótica de orden fraccionario utilizando el algoritmo de integración numérico propuesto por GL. Los estados del oscilador $x(t)$, $y(t)$, y $z(t)$ se cuantifican en Q bits, y los M^2 valores de cada estado se almacenan en arreglos ${}_{Q}X^{(M,M)}$, ${}_{Q}Y^{(M,M)}$, ${}_{Q}Z^{(M,M)}$.

Las β operaciones se aplican entre la imagen de entrada y los estados para generar la imagen encriptada ${}_{Q}E_{\beta}{}^{(M,M)}$. Las operaciones se implementan de forma serial, 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 $\{\psi_1, \psi_1, \ldots, \psi_\beta\}$, la imagen encriptada en el nivel β debe estar dada por:

$$ {}_{Q}E_{\beta}{}^{(M,M)} = \psi_\beta\{ {}_{Q}S_{\beta}{}^{(M,M)},\ {}_{Q}E_{\beta-1}{}^{(M,M)}\}, \tag{1}$$

donde

$$ {}_{Q}E_{\beta-1}{}^{(M,M)} = \psi_{\beta-1}\{ {}_{Q}S_{\beta-1}{}^{(M,M)},\ {}_{Q}E_{\beta-2}{}^{(M,M)}\}, \tag{2}$$

$$ {}_{Q}E_{\beta-2}{}^{(M,M)} = \psi_{\beta-2}\{ {}_{Q}S_{\beta-2}{}^{(M,M)},\ {}_{Q}E_{\beta-3}{}^{(M,M)}\}, \tag{3}$$

$$\vdots$$

$$ {}_{Q}E_{1}{}^{(M,M)} = \psi_{1}\{ {}_{Q}S_{1}{}^{(M,M)},\ {}_{Q}E_{0}{}^{(M,M)}\}, \tag{4}$$

siendo ${}_{Q}E_{0}{}^{(M,M)} = {}_{Q}U^{(M,M)}$ la imagen médica a encriptar.

Operaciones de encriptado

Las operaciones consideradas en este trabajo son:

- La operación lógica OR-exclusivo (XOR). La operación j-ésima del esquema puede implicar la operación XOR, que se define a nivel de bit entre todos los píxeles de la imagen.
- Rotación circular de bits a la derecha (CIRCR). La operación j-ésima del esquema puede involucrar la operación CIRCR, que se aplica a nivel de bits entre dos píxeles de la imagen. La operación CIRCR indica que los bits Q que construyen el píxel ${Q^e}_{j-1}(n,m)$ rotan, del bit más significativo (MSB) al bit menos significativo (LSB), el número entero dado por el elemento ${}_{Q}S_{\beta}(n,m)$.
- Rotación circular de bits a la izquierda (CIRCL). Similar a CIRCR, pero con la rotación circular del LSB al MSB.

- Rotación de píxeles en una línea a la derecha (PIXRR) y a la izquierda (PIXRL). Similar a CIRCR y CIRCL, pero la rotación circular se realiza a nivel de píxel en las líneas horizontales de la imagen
- Rotación de píxeles en una columna a la derecha (PIXCR) y a la izquierda (PIXCL). Similar a PIXRR y PIXR, pero la rotación circular se realiza sobre las columnas de la imagen.
- Operación de sustitución (SBOX). Se utiliza la *s-box* propuesta en.[8] No se requiere la señal caótica para realizar esta operación, que se aplica a nivel de píxel. La *s-box* de representa una función invertible que sustituye cada píxel del plano por otro valor.
- Operación de permutación (PBOX). La matriz separable de distancia máxima (MDS)

$$ {}_{Q}P^{(4\times4)} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}, \tag{5} $$

se utiliza como caja de permutación. Este cuadro se multiplica por bloques adyacentes de 4 píxeles. La multiplicación se realiza en el campo de Galois GF (2^8). Nuevamente, usamos una matriz MDS bien conocida como caja de permutación para asegurar un sistema criptográficamente seguro.[8] En nuestro caso, si la operación se aplica a bloques más grandes, la convolución bidimensional se realiza entre los elementos de la caja y los datos de entrada. Usamos convolución, a diferencia de otros trabajos donde el cuadro de permutación se aplica a bloques de datos adyacentes. Esto puede aumentar el tiempo de cálculo porque cada línea de píxeles se procesará cuatro veces. Sin embargo, un mayor número de iteraciones puede causar relaciones más complejas en el encriptado.

Compresión

En la etapa de compresión, se aplica la DWT de η niveles a ${}_{Q}U^{(N,N)}$, lo que da como resultado una aproximación $U^{(M,M)}$ con $M \approx \frac{N}{\eta}$, y 3η grupos de coeficientes a diferentes escalas. Debido a que la mayoría de las imágenes son de naturaleza de paso bajo, solo se considera una aproximación a $U^{(M,M)}$ y los detalles de alta frecuencia se descartan en los componentes horizontal, vertical y diagonal.

Posteriormente, se aplica una cuantificación uniforme con niveles de 2^Q a cada píxel de $U^{(M,M)}$ generando la señal ${}_{Q}U^{(M,M)}$.

RESULTADOS

En esta sección presentamos algunos resultados experimentales. El sistema completo considera el esquema que se muestra en la figura 1. El esquema de compresión y encriptación realizado por el transmisor se realiza utilizando una secuencia plana, donde la salida de cada etapa alimenta la entrada de la siguiente. El receptor realiza un proceso similar. El rendimiento de las diferentes etapas del sistema se evalúa a través de varias métricas, como la entropía de la información, coeficientes de correlación (CC), número de tasa de cambio de píxeles (NPCR), intensidad de cambio promedio unificado (UACI), robustez de ruido y complejidad computacional por medio de análisis de tiempo. Se utilizó una radiografia de tórax en escala de grises de 8 bits. El tamaño de la imágen utilizada es de 512×512 píxeles. Las imágen de prueba se muestran en la figura 3, la cual consiste en una radiografia de tórax. Las radiografías o los rayos X del tórax, utilizan una dosis muy pequeña de radiación ionizante para producir imágenes del interior del tórax. Se utiliza para evaluar los pulmones, la pared del pecho y el corazón, se puede diagnosticar la bradipnea, tos persistente, fiebre, dolor de pecho o algunas lesiones internas. También ayuda a diagnosticar y monitorear tratamientos de una variedad de condiciones de los pulmones como la neumonía, el enfisema y el cáncer. Debido a que los rayos X del tórax son rápidos y fáciles, resultan particularmente útiles para diagnósticos y tratamientos de emergencia.

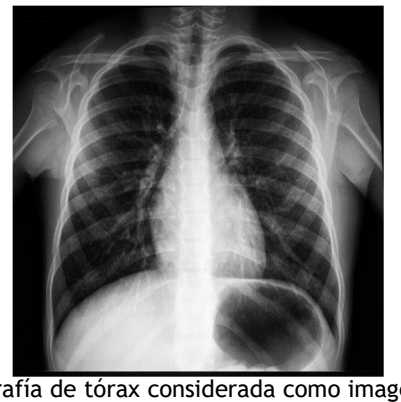


Fig. 3. Radiografía de tórax considerada como imagen de prueba.

Métricas de encriptado

En una primera instancia, evaluamos el proceso de encriptado que se mostró previamente, asumiendo un canal ideal, eliminando la etapa de compresión y considerando diferentes rondas (ciclos) de encriptación κ.

Para cada valor de κ se calcularon 30 ejecuciones, en cada ciclo se seleccionó una clave de forma aleatoria. La tabla II, muestra la entropía mínima, máxima y promedio de la imagen encriptada para diferentes valores de κ (ciclos de encriptación). En todos los casos abordados, la entropía de los datos encriptados está cerca de su valor ideal $H = 8$.

Tabla II. Promedio, mínimo y máximo para la entropía de información H. Para calcular cada valor se realizaron 30 rondas con claves aleatorias.

Imagen	κ	min(H)	max(H)	Promedio (H)
Torax	1	7.99920579	7.99938443	7.99931478
	2	7.99917575	7.99938282	7.9993149
	4	7.99918183	7.99944923	7.99929086

Los coeficientes de correlación en las direcciones horizontal CC_x, vertical CC_y y diagonal $CC_{x,y}$ también se calcularon para la imagen. Se utilizaron diferentes claves aleatorias y $\kappa = 1,2,4$ rondas. Para cada caso abordado, separamos pares de 1000 píxeles adyacentes en las direcciones horizontal, vertical y diagonal de la imagen original y encriptada. Los coeficientes de correlación se calcularon a partir de estos conjuntos. Los resultados obtenidos se resumen en la tabla III donde, se puede apreciar una correlación más débil de la imagen encriptada con respecto a la imagen original. El valor ideal para los coeficientes de correlación en una imagen cifrada es de cero.

Tabla III. Coeficientes de correlación de las imagen original y encriptada, para cada imagen se considera $\kappa = 1,2,4$ ciclos. En cada ejecución, se seleccionaron aleatoriamente conjuntos de 1000 píxeles adyacentes en la dirección apropiada y se calcularon sus coeficientes de correlación.

Imagen	Caso	Horizontal CC_x	Vertical CC_y	Diagonal $CC_{x,y}$
Torax	Sin encriptar	0.9967	0.9951	0.9923
	Encriptado con $\kappa = 1$	0.0052	-0.0012	-0.0154
	Encriptado con $\kappa = 2$	-0.0273	-0.0284	-0.0118
	Encriptado con $\kappa = 4$	0.0203	0.0150	0.0533

Análisis de sensibilidad

La sensibilidad a la llave es importante como medida de seguridad. Esta capacidad generalmente se mide cuantitativamente a través de la tasa de cambio del número de píxeles (NPCR) y la intensidad

de cambio promedio unificada (UACI). Las tablas IV y V, muestran el valor mínimo, máximo y promedio de ambas métricas, para las cuatro imágenes de prueba y para $\kappa = 1{,}2{,}4$. Nuevamente, para cada caso se realizaron 30 ejecuciones. En cada ejecución, se alternaba un bit aleatorio de la clave. Como se puede observar en las tablas IV y V el NPCR indica que, en todos los casos abordados, este mínimo cambio en la clave produce al menos un cambio en el 99.25% de los píxeles de encriptado. Por otra parte, los valores de UACI indican que un cambio mínimo en la clave produce una diferencia de intensidad media de 33.43% en los píxeles de encriptado. De las tablas IV y V, se puede ver que el encriptado tiene un nivel de seguridad aceptable para un cambio de bit en la clave secreta.

Tabla IV. Sensibilidad de la clave. Promedio, mínimo y máximo para la métrica NPCR. Donde para cada imagen se realizaron 30 ejecuciones. En cada ejecución, se alternaba un bit aleatorio de la clave.

Imagen	κ	min (NPCR)	max (NPCR)	promedio (NPCR)
Torax	1	99.25651%	99.61280%	99.48883%
	2	99.59182%	99.63531%	99.61793%
	4	99.59411%	99.63569%	99.61530%

Tabla V. Sensibilidad clave. Promedio, mínimo y máximo para la métrica UACI. Para cada imagen se calcularon 30 ejecuciones. En cada ejecución, se alternaba un bit aleatorio de la clave.

Imagen	κ	min (UACI)	max (UACI)	promedio (UACI)
Torax	1	33.09046%	33.51029%	33.36043%
	2	33.40805%	33.49997%	33.45852%
	4	33.42108%	33.56761%	33.47018%

Tabla VI. PSNR promedio, mínimo y máximo para $\kappa = 1{,}2{,}4$ y ruido con $p = 0.01, 0.001, 0.0001$.

Imagen		$p = 0.01$			$p = 0.001$			$p = 0.001$		
		min	max	min	min	max	avg	min	max	avg
Torax	1	19.75	19.92	19.82	29.31	29.92	29.59	38.92	41.52	39.91
	2	14.41	14.38	14.35	23.60	24.36	23.89	32.76	34.74	33.57
	4	8.77	8.77	8.72	12.70	13.00	12.80	21.10	22.69	21.96

Robustez ante ruido

Un encriptado debe ser resistente al ruido para evitar distorsiones en la imagen desencriptada inducidas por cambios en la imagen encriptada. Estos cambios podrían estar relacionados con el proceso de transmisión o con el proceso de encriptado en sí. En este documento, la robustez contra el ruido se evalúa agregando ruido de sal y pimienta a la imagen encriptada. El ruido de Sal y Pimienta (SP) es uno de los ruidos más populares que afectan la calidad de la imagen digital, y la probabilidad de que aparezca un píxel blanco o negro viene dada por una probabilidad $p \leq \frac{1}{2}$. Agregamos ruido de Sal y Pimienta a los datos encriptados, y luego estos datos ruidosos se descifran. La tabla VI muestra el PSNR entre los datos de desencriptado sin ruido y los datos de desencriptado con ruido. Los valores más altos para el PSNR indican que el encriptado es más robusto contra el ruido. La robustez del ruido disminuye cuando κ aumenta.

Análisis y compresión del tiempo

El esquema de encriptado se realizó en dos dispositivos. El primer dispositivo, denominado Dispositivo 1 el cual es una PC con una CPU Intel Core i7 a 2,60 GHz, 8 MB de RAM DDR4 y una unidad de estado sólido de 1 TB con Ubuntu 18.04 LTS. El segundo dispositivo, etiquetado como Dispositivo 2, es una placa Raspberry Pi 4 modelo B con un Cortex-A72 de cuatro núcleos que funciona a 1,5 GHz, 4 GB de RAM y una microSD de 32 GB que ejecuta Raspbian 10. El rendimiento

de tiempo logrado por ambos dispositivos se muestra en la tabla VII. En ambos casos, se utilizó el mismo script de Python 2.7.

Tabla VII. Tiempo necesario para realizar el proceso de encriptación de la imagen de tórax para diferentes esquemas de compresión y número de rondas. PSNR logrado cuando se agrega una etapa de compresión DWT de un nivel. Se informa el tiempo de encriptado logrado con una computadora portátil (Dispositivo 1) y una placa Raspberry Pi 4 modelo B (Dispositivo 2).

		Pasa bajas únicamente			Pasa bajas + detalles		
	κ	Tiempo dispositivo 1	Tiempo dispositivo 2	PSNR	Tiempo dispositivo 1	Tiempo dispositivo 2	PSNR
Sin compresión $\eta = 0$	1	11.89 seg.	11.89 seg.	∞ dB	-	-	-
	2	19.87 seg.	19.87 seg.		-	-	-
	4	29.08 seg.	29.06 seg.		-	-	-
Con compresión $\eta = 1$	1	3.02 seg.	13.85 seg.	31.50 dB	28.27	28.71	55.76 dB
	2	4.43 seg.	20.62 seg.		22.52	23.23	
	4	7.44 seg.	35.52 seg.		11.59	11.87	

El tiempo necesario aumenta con κ para ambos niveles de compresión $\eta = 0\ y\ 1$, donde ambos dispositivos (Dispositivo 1 y Dispositivo 2). Cuando se agrega la etapa de compresión, y solo se considera la versión paso bajo de la imagen, se reduce el tiempo promedio en todos los casos abordados, y se logra un PSNR de 36.60 dB entre la salida del desencriptado y el plano. Por otro lado, cuando se agregan detalles en la compresión, se aumenta el tiempo promedio y se mejora el PSNR a 55.77 dB. La reducción de tiempo se consigue en todos los casos en los que se utiliza una etapa de compresión.

Remarcamos que se usaron dos dispositivos en esta sección debido al uso potencial de este algoritmo de encriptado en futuras aplicaciones de PC de escritorio, así como en aplicaciones embebidas. Como era de esperar, el Dispositivo 2 tiene un rendimiento menor respecto al Dispositivo 1 debido a sus recursos limitados.

Comparación con otros algoritmos de encriptado

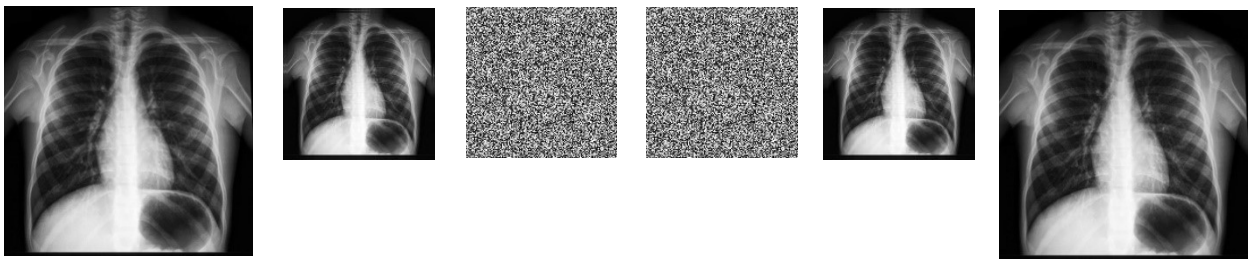
Aquí mostramos los resultados de la comparación del método de encriptado y las referencias.[13, 14, 15, 16] En todos los casos se utiliza la imagen Lena en escala de grises 512×512 512. La tabla VIII presenta los resultados.

Tabla VIII. Comparación con otros algoritmos de encriptado. La información en las últimas dos columnas refleja el valor máximo para y $\kappa = 16$.

Métrica	[13]	[14]	[15]	[16]	$\kappa = 16$
Entropy	7.999419	7.9964	7.999319	7.9994	7.9991
NPCR	99.62%	$\approx 0\%$	99.62%	99.60%	99.63%
UACI	33.45%	$\approx 0\%$	33.48%	33.46%	33.59%

Resultados para el sistema completo

Los resultados para todo el sistema representado por la figura 1 se muestran en las figuras 4. Aquí las señales de prueba fueron procesadas por todas las etapas (compresión, encriptación y transmisión). En todos los casos se utilizó el valor $\kappa = 4$. Los valores más altos de κ mejoran NPCR y UACI, pero disminuyen la tolerancia al ruido. Como se puede observar cualitativamente, en todos los casos abordados se logra la reconstrucción. Es importante resaltar que, en todos los casos, el texto encriptado se transmitió experimentalmente utilizando los módulos de radio definidos por software usando modulación PSK.



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

Fig. 4. Resultados para la radiografía de tórax. (a) Imagen original $QU^{(N,N)}$; (b) Imagen comprimida y cuantizada por $QU^{(M,M)}$; (c) Imagen encriptada a ser transmitida; (d) Imagen encriptada $QE_{\beta}{}^{(M,M)}$ recibida; (f) Imagen desencriptada $Q\widehat{U}_{\beta}{}^{(M,M)}$ en la salida del desencriptador. (d) Imagen recuperada.

CONCLUSIONES

En este trabajo se presentó un esquema de encriptación, compresión y transmisión. La compensación entre complejidad y rendimiento es adecuada para varias aplicaciones. La seguridad se evaluó a través de NPCR y UACI, ambas métricas muestran una sensibilidad satisfactoria a los cambios presentados en la clave cuando se utilizan suficientes rondas de encriptado. Por otra parte, el efecto de las degradaciones de transmisión se amplifica si se utiliza un gran número de rondas. Entonces, se debe considerar un equilibrio adecuado entre la sensibilidad y la robustez del ruido. El proceso de encriptado se comparó con otros algoritmos encontrados en la literatura. Como se muestra en la tabla VIII, se logró un desempeño competitivo. Además, si se utiliza la etapa de compresión de transformada de wavelet discreta, el tiempo de encriptado se reduce considerablemente. Finalmente, es importante resaltar que, luego de varios experimentos, los resultados mostraron desempeños adecuados para varias aplicaciones en un entorno físico de comunicaciones inalámbricas. Como trabajo futuro, proponemos aplicar este esquema de compresión-encriptado-transmisión a imágenes RGB. La investigación actual en el campo considera otros esquemas de compresión, encriptado y transmisión, así como soluciones de optimización conjunta.

AGRADECIMIENTOS

Los autores agradecen al Departamento de Electrónica y Automatización de la Facultad de Ingeniería Mecánica y Eléctrica de la UANL, y a CONACYT/MÉXICO No. 166654, A1-S-31628.

REFERENCIAS

1. Secretaria de la salud, «NORMA Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico.,» [En línea]. Available: http://dof.gob.mx/nota_detalle_popup.php?codigo=5272787. [Último acceso: 10 Marzo 2022].
2. M. Garcia-Martinez y E. Campos-Cantons, «Pseudo-random bit generator based on multi-modal maps,» Nonlinear Dynamics, vol. 82, nº 8, pp. 2119-2131, 2015.
3. A. Belazi, M. Talha, S. Kharbech y W. Xiang, «Novel medical image encryption scheme based on chaos and DNA encoding. , 7,,» IEEE access, vol. 7, pp. 36667-36681, 2019.
4. C. H. Yang y Y. S. Chien, «FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm,» Symmetry, vol. 12, nº 2, p. 189, 2020.
5. S. T. Kamal, K. Hosny, T. M. Elgindy, M. M. Darwish y M. M. Fouda, «A new image encryption algorithm for grey and color medical images,» IEEE Access, vol. 9, pp. 37855-37865., 2021.
6. Z. Hua, S. Yi y Y. Zhou, «Medical image encryption using high-speed scrambling and pixel adaptive diffusion,» Signal Processing, vol. 144, pp. 134-144, 2018.

7. H. E. Gilardi-Velázquez, J. L. Echenausía-Monroy, R. Jaimes-Reátegui, J. H. García-López, E. Campos y G. Huerta-Cuellar, «Deterministic coherence resonance analysis of coupled chaotic oscillators: fractional approach,» Chaos, Solitons & Fractals, vol. 157, p. 111919, 2022.
8. M. A. Platas-Garza, E. Zambrano-Serrano, J. Rodríguez-Cruz y C. Posadas-Castillo, «Implementation of an encrypted-compressed image wireless transmission scheme based on chaotic fractional-order systems,» Chinese Journal of Physics, vol. 71, pp. 22-37, 2021.
9. O. García-Sepúlveda, C. Posadas-Castillo, A. D. Cortés-Preciado, M. A. Platas-Garza, E. Garza-González y A. G. Sánchez, «Synchronization of fractional-order Lü chaotic oscillators for voice encryption,» Revista mexicana de física, vol. 66, nº 3, pp. 364-673, 2020.
10. R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Muñoz-Pacheco y R. Torrealba-Meléndez, «Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks,» Ad Hoc Networks, vol. 97, p. 102005, 2020.
11. B. B. Cassal-Quiroga y E. Campos-Cantón, «Generation of dynamical S-boxes for block ciphers via extended logistic map,» Mathematical Problems in Engineering, p. 2702653, 2020.
12. J. Luo, S. Qu, Y. Chen y Z. Xiong, «Synchronization of memristor-based chaotic systems by a simplified control and its application to image en-/decryption using DNA encoding,» Chinese Journal of Physics, vol. 62, pp. 374-387, 2019.
13. Ahmad, M., Al Solami, E., Wang, X. Y., Doja, M. N., Beg, M. M., y Alzaidi, A. A. «Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos. » Symmetry, vol 10 nº 7, 266, 2018.
14. Wang, W., Si, M., Pang, Y., Ran, P., Wang, H., Jiang, X., ... y Jeon, G. «An encryption algorithm based on combined chaos in body area networks. » Computers & Electrical Engineering, vol. 65, 282-291.2018.
15. Chen, J. X., Zhu, Z. L., Fu, C., Yu, H., y Zhang, L. B. «A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. » Communications in Nonlinear Science and Numerical Simulation, vol 20, n°3, 846-860. 2015
16. Bashir, Z., Wątróbski, J., Rashid, T., Zafar, S., y Sałabun, W. «Chaotic dynamical state variables selection procedure based image encryption scheme. » Symmetry, vol 9, n°12, 312. 2017.