ISSN: 1692-7257 - Volumen 1 – Número 47 - 2026

ORIGINAL

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Encriptación de imágenes usando caos y compuertas cuánticas

Image encryption using chaos and quantum gates

Miguel Ángel Rico García[1]
Luz Deicy Alvarado Nieto[1]
Edilma Isabel Amaya Barrera[1]

[1] **Universidad Distrital Francisco José de Caldas, Facultad de Ingeniería Grupo ComplexUD, Bogotá Colombia.**

Recibido: 29 agosto 2025. Revisado: 29 octubre 2025. Aceptado: 18 diciembre 2025. Publicado: 30 enero 2026.
Autor de correspondencia: Luz Deicy Alvarado Nieto

Cómo citar: M. Á. Rico García, L. D. Alvarado Nieto, and E. I. Amaya Barrera, "Encriptación de imágenes usando caos y compuertas cuánticas", *Revista Colombiana de Tecnologías de Avanzada (RCTA)*, vol. 1, no. 47, 2026, art. no. 4270, doi: 10.24054/rcta.v1i47.4270

Esta obra está bajo una licencia internacional Creative Commons Atribución-NoComercial 4.0.

Resumen:

Resumen: Se presenta un nuevo algoritmo de encriptación de imágenes tanto a color como en escala de grises, basado en principios de mecánica cuántica y teoría del caos. Para la etapa de difusión se utilizaron: el mapa hipercaótico logístico cuántico, dos números primos de 15 dígitos cada uno y una transformación; generando tres matrices de difusión, que junto con las capas RGB de la imagen original, se evolucionaron usando las compuertas cuánticas SWAP, CNOT y CCNOT. Posteriormente, aplicando XOR se obtuvieron 3 matrices difundidas, sobre las cuales, utilizando 3 secuencias generadas por el sistema caótico híbrido logístico-tienda, se aplicó una estrategia de permutación circular a nivel de filas y columnas. Cabe resaltar que el modelo aquí propuesto, está inspirado en el dominio cuántico, pero es ejecutado en un computador clásico y particularmente encripta, en formato RGB, las imágenes que originalmente están en escala de grises, aumentando con ello la pérdida de patrones lo cual dificulta el éxito de ataques fraudulentos. El algoritmo propuesto fue sometido a pruebas de seguridad y desempeño encontrando indicadores equiparables con algunos reportados en otros trabajos similares.

Palabras clave: mapa caótico, criptografía, encriptación, seguridad de la información, computación cuántica, criptografía inspirada en el dominio cuántico.

Abstract:

Abstract: This article presents a new encryption algorithm for color and grayscale images based on the principles of quantum mechanics and chaos theory. The following were used for the diffusion stage: the quantum logistic hyperchaotic map, two prime numbers of 15 digits each, and a transformation to obtain three pseudo-random sequences used to generate three diffusion matrices which, with the RGB layers of the original image, evolve using the SWAP, CNOT, and CCNOT quantum gates. Subsequently, by applying the XOR operation, three diffused layers of the original image were obtained, to which a circular permutation strategy was applied at the row and column level, using three sequences generated by the hybrid logistic-tent chaotic system. It should be noted that the model proposed herein is inspired by the quantum domain; however, it is implemented using a classical computer and, in particular, encrypts images originally in grayscale, using an RGB representation, increasing the loss of patterns, which hinders the success of fraudulent attacks. The proposed algorithm underwent security and performance tests, obtaining indicators comparable to reported in other similar studies.

Keywords: chaotic mapping, cryptography, encryption, information security, quantum computing, quantum-inspired cryptography.

1. INTRODUCCIÓN

La criptografía se encarga de proponer estrategias para la protección de la información privada. En las últimas décadas han surgido nuevos desarrollos basados en principios de matemáticas e inteligencia artificial, buscando responder a los nuevos desafíos provenientes de los avances tecnológicos que conllevan a intercambiar grandes cantidades de información digital.

Los métodos tradicionales de encriptación tales como RSA (Rivest-Shamir-Adleman) y ECC (criptografía de curvas elípticas) no son indicados cuando se está trabajando con información de gran tamaño, ya que se presentan altos niveles de redundancia en la información y basan su seguridad en el problema de la descomposición de un entero en sus factores primos, el cual es considerado un problema NP (Non-deterministic Polynomial time). Con el surgimiento de los computadores cuánticos, el tiempo de solución para este problema puede reducirse significativamente y llegar a ser de tipo logarítmico, lo cual generaría una catástrofe de seguridad a nivel mundial, hecho que ha impulsado el desarrollo de investigaciones por parte de la comunidad académica y científica, dando lugar a trabajos significativos en esta dirección.

La computación cuántica ha creado desafíos para asegurar la información, es por ello que han surgido propuestas encaminadas a preparar la transición a este nuevo escenario, por lo que el Instituto Nacional de Estándares y Tecnologìas (NIST) se ha dado a la tarea de establecer estándares de seguridad para la era post-cuántica[1],[2].

En la actualidad se han desarrollado propuestas de representación de imágenes en el contexto cuántico, una de ellas se encuentra en el trabajo de Zhang, Gao y Wang [3], la cual aún está vigente e incluso ha tenido propuestas de mejora como lo presentan Wang y colaboradores [4], siendo utilizadas en la propuesta de Wang, Rang y Ding [5] así como en la de Hu, Li y Di [6], para plantear un modelo de encriptación de imágenes en escala de grises, a través de compuertas cuánticas, operaciones de rotación similares al funcionamiento del cubo de Rubik y un sistema bidimensional caótico generado a partir de los sistemas unidimensionales logístico y senoidal. En la misma dirección, se destaca el trabajo propuesto en el artículo A novel image encryption scheme based on quantum dynamical spinning and rotations [7], cuyos autores plantean un algoritmo de encriptación de imágenes RGB, utilizando matrices de rotación y representación de partículas de medio spin.

De otra parte, el uso de los sistemas dinámicos caóticos en el ámbito de la criptografía ha evolucionado para aplicar dichos sistemas en el entorno cuántico, por lo que es frecuente encontrar circuitos cuánticos alusivos a estos sistemas, tal es el caso del trabajo planteado por Gao y colaboradores[8], quienes proponen un nuevo algoritmo para encriptación de imágenes cuánticas representadas mediante el modelo NEQR utilizando además, los atractores caótico bidimensional cat de Arnold y el sistema de Lorenz hipercaótico, con sus correspondientes implementaciones de los circuitos cuánticos.

Adicionalmente, en los trabajos Fast and Robust Image Encryption Scheme Based on Quantum Logistic Map and Hyperchaotic System[9]y Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)[10], los autores plantean modelos de encriptación de imágenes a color, involucrando en ambos casos sistemas dinámicos caóticos cuánticos y compuertas cuánticas.

Teniendo en cuenta el avance en la computación cuántica y sus implicaciones sobre la protección de la información digital, en este artículo se presenta un modelo de encriptación de imágenes digitales a color inspirado en el dominio cuántico, que utiliza sistemas dinámicos caóticos clásicos y cuánticos, así como compuertas cuánticas, el cual es ejecutado usando hardware clásico y validado a través de métricas de seguridad y desempeño. Los resultados obtenidos permiten inferir que este modelo puede ser aplicado en entornos reales. Cabe resaltar que también funciona para imágenes en escala de grises dando origen a un resultado encriptado en escala RGB, lo cual constituye una ventaja criptográfica estratégica ya que favorece la emergencia de dinámicas más complejas aumentando la seguridad estructural del modelo. En los siguientes apartados se abordan los temas: marco teórico, metodología empleada, descripción detallada del algoritmo, aplicación de métricas de rendimiento y conclusiones.

2. MATERIALES Y METODOS

En esta sección se incluyen los elementos teóricos tomados como base para el desarrollo del algoritmo propuesto, explicando las fases de la metodología llevada a cabo.

$$x_{n+1} = mod\left(\left((r * x_n) * (1 - x_n) + \left(\frac{4*r*x_n}{2}\right)\right), 1\right)$$

2.1. Conocimientos Previos

A continuación, se abordan los fundamentos conceptuales que se tuvieron en cuenta para el planteamiento del modelo aquí presentado.

2.1.1. Atractores caóticos clásicos y cuánticos

Un sistema dinámico se caracteriza porque evoluciona de acuerdo a una regla determinista de tipo continuo o discreto, si dicha

evolución es sensible a pequeñas perturbaciones se hace referencia al concepto de caos. Puntualmente, un sistema se considera caótico si satisface tres condiciones que son: sensibilidad a perturbaciones, transitividad y densidad de puntos periódicos[11].

El concepto de Caos fue evidenciado por el meteorólogo Edward Lorenz [12] en un experimento que dio lugar a lo que posteriormente se llamó “efecto mariposa” y que en la actualidad es un referente significativo para los estudiosos de fenómenos complejos no lineales, resaltando que en diferentes áreas del conocimiento existen numerosos comportamientos enmarcados en esta línea, tal es el caso del modelado del clima, de las epidemias, del mercado de valores, entre otros [13], [14], [15].

Cuando se hace análisis cualitativo de un sistema dinámico no lineal enmarcado en un ambiente de caos, para analizar las trayectorias de dicho sistema a partir de condiciones y parámetros iniciales, es usual que aparezcan atractores caóticos extraños, los cuales se caracterizan por la alta sensibilidad, no periodicidad, estructura fractal y dimensión no entera, propiedades que resultan útiles para aprovechar en el contexto de esquemas criptográficos, pues esto se traduce en la obtención de secuencias pseudoaleatorias que pueden ser utilizadas para el diseño de algoritmos de cifrado.

En las últimas décadas, se han formulado nuevos sistemas dinámicos caóticos debido al impacto de estos en el ámbito de la seguridad, buscando obtener comportamientos más complejos que conllevan a una mayor robustez de los sistemas criptográficos basados en tales atractores, es el caso del modelo híbrido obtenido a partir de los sistemas logístico y tienda, el cual se describe por medio de la ecuación (1)[10].

Cabe resaltar que la inmersión de los principios de física cuántica en el escenario de computación conllevó a extrapolar el concepto del caos sobre el dominio cuántico, pese a que allí no hay trayectorias definidas, sino que, por el contrario, el sistema evoluciona con superposición cuántica, presentándose incertidumbre de acuerdo con el principio de Heisenberg y la evolución lineal y unitaria en concordancia con la ecuación de Schrödinger[16]. En este contexto, el caos cuántico trata el estudio de sus análogos caóticos, lo cual implica analizar estructuras en el espacio de Hilbert paralelas a los atractores clásicos, en otras palabras, se estudian las transiciones a la dinámica compleja cuántica. Uno de los atractores clásicos caótico cuántico es el logístico, utilizado como insumo para la parte del proceso de difusión del algoritmo que se describe en el trabajo de Goggin, Sundaram y Milonni[17].

2.1.2. Computación cuántica.

La evolución de los computadores clásicos respecto a su tamaño y velocidad está llegando al límite, es casi imposible crear circuitos integrados con un mayor número de componentes conservando o tratando de disminuir su tamaño, lo cual ha llevado a que las plataformas de supercomputación, utilizadas especialmente para ejecutar modelos de Inteligencia artificial, estén compuestas por enormes cantidades de computadores muy potentes que ocupan edificios enteros destinados únicamente a albergarlos, a su vez, la generación de nuevos y potentes algoritmos que demandan gran capacidad de memoria y velocidad en estas máquinas, ha impulsado la búsqueda de otras alternativas de almacenamiento y procesamiento, es allí donde surge la computación cuántica, de la cual se esperan resultados prometedores.

El trabajo Simulating Physics with Computers[18]se puede considerar como punto de partida de la computación cuántica, en él, Richard Feynman concibió la idea de desarrollar computadores cuánticos para simular sistemas que involucran nanopartículas. En la actualidad se han producido avances significativos en el desarrollo de este tipo de computadores, dando paso a nuevos retos científicos[19].

En contraste con la computación clásica cuya unidad mínima de información es el bit, dentro del sistema cuántico esta unidad corresponde al Qbit, el cual puede asumir los estados cero, uno o ambos (superposición) y combinarse así con otros Qbits, lo que permite llevar a cabo un mayor número de operaciones simultáneamente, para representarlos se usa la notación de Dirac en la cual los valores 0 o 1 son ubicados en medio de una línea vertical y un ángulo a manera de corchete, llamado ket: $|0\rangle$, $|1\rangle$, de esta forma los estados básicos reciben el nombre de ket cero y ket uno respectivamente, los cuales se representan como los polos norte y sur en una esfera de radio 1 denominada “esfera de Bloch” (ver figura 1). Así mismo, el entrelazamiento permite que los Qbits sean manipulados de tal forma que su comportamiento esté sincronizado, logrando un crecimiento exponencial de las operaciones en paralelo respecto al número de Qbits con que trabaja el computador[20], La Fig. 1 representa la esfera de Bloch donde se evidencian varios de los estados posibles para un Qbit.

Para realizar operaciones con estos Qbits, se han definido varias compuertas que actúan sobre ellos, de manera similar a como las compuertas lógicas permiten desarrollar operaciones y crear circuitos con los bits tradicionales. Cabe resaltar que los estados básicos de un qbit pueden representarse también en un vector de tamaño2×1, así $|0\rangle$puede representarse como$\binom{1}{0}$ y $|1\rangle$ como$\binom{0}{1}$. De esta manera, cuando se quiere aplicar compuertas lógicas que requieren más de un qbit, se utiliza producto tensorial para combinar los qbits obteniendo por ejemplo $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ como posibles resultados, facilitando de esta forma su operación con las compuertas mencionadas.

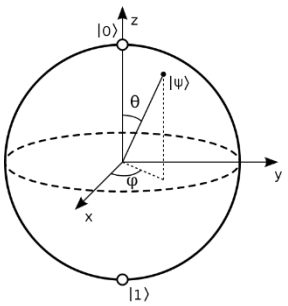


Fig. 1. *Esfera de Bloch con varios estados posibles para un Qbit.*
Fuente: PNGWING [21].

2.1.2.1. Compuerta CNOT

También denominada compuerta NOT controlada, actúa sobre 2 qbits, cambiando el segundo de ellos si el primero (qbit controlador) está en estado 1, es decir, que si se aplica sobre |00⟩ o |01⟩,no habrá ningún cambio, sin embargo, si se aplica sobre |10⟩el resultado será |11⟩y si es sobre |11⟩, el resultado obtenido es |10⟩ [22]. La representación matricial de esta compuerta se muestra en (2)[10],[23].

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La representación gráfica de esta compuerta en forma de circuito, evidencia sus dos entradas, el símbolo$\bigoplus$que actúa sobre los dos qbits y el resultado obtenido, lo cual se presenta en la Fig. 2.

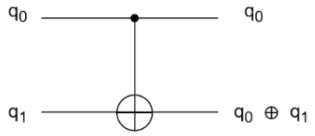


Fig. 2. *Compuerta CNOT.*
Fuente: Adaptada de [23] y [24].

2.1.2.1. Compuerta Toffoli

También conocida como compuerta CNOT controlada, en este caso, actúa sobre 3 qbits, los dos primeros desempeñan el papel de control y el tercero es el objetivo. Si los dos primeros qbits están en 1, el valor del tercero cambia, en caso contrario, sigue igual, es decir, si se tienen los qbits de entrada |000⟩, |001⟩, |010⟩, |011⟩, |100⟩, |101⟩, no habrá ningún cambio mientras que si se aplica la compuerta sobre los qbits |110⟩ o |111⟩se obtiene |111⟩ y |110⟩, respectivamente[24]. La matriz correspondiente a esta compuerta se presenta en(3).

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Al igual que en la compuerta CNOT, para Toffoli su circuito evidencia las 3 entradas, el símbolo XOR que actúa sobre los tres qbits y el resultado generado sobre el último de ellos, tal como se muestra en la Fig. 3.

2.1.2.3. Compuerta Swap

Se aplica sobre 2 qbits intercambiando los valores entre ellos, es decir, si la entrada es |10⟩, la salida será |01⟩y viceversa. En caso de que los 2 qbits tengan el mismo valor, se conservarán tal como están[24]. La matriz correspondiente a esta compuerta se presenta en(4).

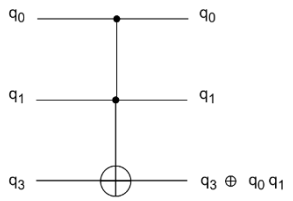


Fig. 3. *Compuerta Toffoli.*
Fuente: Adaptada de [20] y [24].

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

De manera similar a las dos compuertas anteriores, esta cuenta con su representación como circuito tal como se muestra en la Fig. 4.

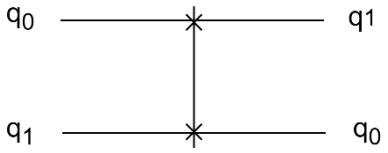


Fig. 4. *Compuerta Swap.*
Fuente: Adaptada de [20] y [24].

2.1.3. Criptografía

Dada la necesidad de preservar la seguridad e integridad de la información privada, la criptografía ha estado presente a lo largo de la evolución humana, tomando cada vez mayor significancia debido al aumento en la cantidad de información digital que circula por medio de canales públicos. El objetivo de la criptografía es transformar información mediante codificación en un resultado ilegible para enmascararla ante intrusos, existen dos tipos: simétrica (misma clave para encriptar y desencriptar), este es el caso de DES (Estándar de cifrado de datos) y asimétrica (una clave para encriptar y otra para desencriptar) como sucede con RSA (Rivest, Shamir Adleman), Los métodos convencionales no son apropiados cuando se está frente a grandes volúmenes de datos tipo imágenes o archivos multimedia, debido a que se presenta redundancia, es así como surgen nuevas propuestas basadas, entre otras, en teoría de curvas elípticas, autómatas celulares, redes neuronales o caos.

Gracias al potencial de las propiedades inherentes a los sistemas caóticos, los algoritmos criptográficos basados en estos, han tomado interés académico desde finales del siglo XX, prueba de esto es el surgimiento de una línea de investigación llamada criptografía caótica, vinculando académicos interesados en hacer esfuerzos colectivos e intercambiar conocimiento para formular esquemas de seguridad. En esta dirección, se han incrementado significativamente las propuestas de criptografía fundamentadas en teoría del caos, todo ello debido a la similitud que existe entre las propiedades de un sistema que exhibe caos y las requeridas en un algoritmo criptográfico. La sensibilidad a condiciones iniciales e imprevisibilidad, presentes en un sistema caótico, hacen que un cambio aparentemente insignificante en una clave de cifrado, genere una salida drásticamente distinta, lo que implica a la vez que al intentar descifrar dicha salida no se logre recuperar la información original. Adicionalmente, si alguien logra acceder a un mensaje cifrado no puede predecir cómo será el siguiente. De otra parte, la complejidad del sistema caótico, en el contexto de la encriptación, significa que hay mayor dificultad en el momento de intentar descifrar el mensaje de manera fraudulenta.

Por lo anterior, la criptografía ha contribuido al estudio y formulación de nuevos sistemas caóticos, basados en su mayoría en los ya existentes, por

medio de la combinación entre ellos o la extensión a un espacio de más dimensiones, teniendo presente en todo caso, aumentar el nivel de complejidad y así, garantizar más seguridad sobre los modelos criptográficos que utilizan secuencias cifrantes, como es el caso del trabajo propuesto por Mohamed y colaboradores[10]. Así mismo se busca corregir deficiencias y consolidar bases para seguir avanzando en el campo de la criptografía caótica, sin perder de vista que, pese a los nuevos desarrollos en el tema, esta enfrenta amenazas provenientes de la computación cuántica[1],[2],[25],[26],[27], por lo que se hace necesario seguir recorriendo terrenos en búsqueda de aportar soluciones en ciberseguridad.

2.2. Metodología

El proceso seguido para consolidar el algoritmo que se propone en este trabajo, empleó un enfoque mixto que abordó aspectos de tipo cualitativo y cuantitativo. En el primer caso, con el objetivo de asegurar alta aleatoriedad en las secuencias pseudoaleatorias

empleadas y en el segundo, para validar el desempeño del algoritmo propuesto y hacer los ajustes correspondientes, con el fin de evitar valores no deseados en las métricas aplicadas, comparando paralelamente el rendimiento, con referentes científicos actuales.

Es de resaltar que el algoritmo, al igual que la mayoría de sistemas criptográficos, involucró fases de difusión y confusión, en las que se emplearon principios de computación cuántica, así como sistemas caóticos clásicos y cuánticos, consolidando una propuesta altamente segura, validada a través de la aplicación de métricas de seguridad y rendimiento. La Fig. 5 sintetiza el proceso llevado a cabo en este trabajo.

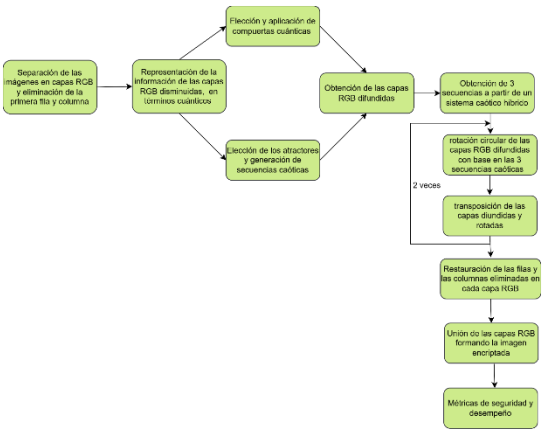


Fig. 5. *Fases del algoritmo de encriptación.*
Fuente: Elaboración Propia.

3. DESCRIPCIÓN DEL ALGORITMO

Partiendo de una imagen de tamaño M×N en escala RGB, cada una de las capas fue sometida a los procesos de difusión y confusión como se detalla a continuación:

3.1. Fase de Difusión

Dado que la información proporcionada por un solo pixel en una imagen es insignificante, especialmente en los bordes, retirar los pixeles de la primera o última fila o columna, no implican cambios visuales significativos, si se encripta el resto de la imagen y se adiciona a este resultado la fila y columna omitidas, dicha estrategia puede generar confusiones a cualquier atacante que intente recuperar parte de la imagen original o inferir información a partir de los bordes, situación favorable en términos de seguridad, la cual es aplicada en la propuesta aquí presentada. Este y los demás procesos llevados a cabo en la fase de difusión, se describen a continuación.

- Separación de las capas RGB y recorte de la primera fila y columna en cada una de ellas.
- Elección aleatoria de una capa recortada y de ella una fila o columna para obtener el valor promedio P de los pixeles de dicha fila o columna elegida.
- Iteración del sistema hipercaótico logístico cuántico con los valores iniciales x0 = 0.043, y0 = 0.035, z0 = 0.025, β = 6.859, r = 3.990, P veces (tomando solo la parte entera de P) las cuales son ignoradas para garantizar mayor aleatoriedad.
- Continuación del proceso de iteración anterior$(M-1)\times(N-1)$veces generando 3 secuencias caóticas {xi}, {yi}, {zi}.
- Obtención de tres matrices caóticas notadasQ_i^R, Q_i^G, Q_i^B, mediante las transformaciones tomadas de[10]y definidas en(5):

$$Q_i^R = mod(floor((\varepsilon_1 . x_i) + \varepsilon_2), 256)$$
$$Q_i^G = mod(floor((\varepsilon_1 . y_i) + \varepsilon_2), 256)$$
$$Q_i^B = mod(floor((\varepsilon_1 . z_i) + \varepsilon_2), 256)$$

Siendoε_(1) y ε_(2)dos números primos de 15 dígitos cada uno.

- Representación de los niveles de intensidad de cada pixel en términos de qbits. Cada una de las entradas de las 6 matrices, es un entero entre 0 y 255, el cual es representado en binario y visto como el producto tensorial de 8 qbits. Por ejemplo, para el caso del pixel con valor 178, se tiene: $178_{10} = |10110010\rangle$.
- Evolución, con base en la representación previa (|q7 q6 q5 q4 q3 q2 q1 q0⟩) de las entradas en las 6 matrices (3 originales recortadas y 3 caóticas) mediante las compuertas cuánticas SWAP, CNOT y Toffoli. Dicha evolución para el ejemplo anterior se muestra en la Tabla 1
- Aplicación de la compuerta lógica XOR en cada par de matrices así: R XOR QR, G XOR QG, B XOR QB, siendo R, G, B, QR, QG y QB los resultados consolidados en el ítem anterior.

Del proceso anterior, se obtienen 3 matrices difundidas de tamaño$(M-1)\times(N-1)$notadas como DR, DG y DB.

Tabla 1: Aplicación secuencial de las compuertas cuánticas

Compuerta	q7	q6	q5	q4	q3	q2	q1	q0
|10110010⟩	1	0	1	1	0	0	1	0
swap(q0,q4)	1	0	1	0	0	0	1	1
swap(q1,q6)	1	1	1	0	0	0	0	1
swap(q2,q5)	1	1	0	0	0	1	0	1
swap(q3,q7)	0	1	0	0	1	1	0	1
swap(q3,q0)	0	1	0	0	1	1	0	1
swap(q4,q7)	0	1	0	0	1	1	0	1
CNOT(q0,q1)	0	1	0	0	1	1	1	1
CNOT(q2,q3)	0	1	0	0	0	1	1	1
CNOT(q4,q5)	0	1	0	0	0	1	1	1
CNOT(q6,q7)	1	1	0	0	0	1	1	1
CCNOT(q0,q1,q2)	1	1	0	0	0	0	1	1
CCNOT(q0,q1,q3)	1	1	0	0	1	0	1	1
CCNOT(q4,q5,q6)	1	1	0	0	1	0	1	1
CCNOT(q4,q5,q7)	1	1	0	0	1	0	1	1

Fuente: Elaboración Propia

3.2. Fase de Confusión

Para permutar las entradas de las matrices DR, DG y DB se lleva a cabo el siguiente procedimiento:

- Iteración del sistema híbrido definido en(1),3×(N−1)veces, obteniendo una secuencia caótica {xi} con i variando de 1 a3×(N−1).
- Aplicación de la transformación T, tomada de[8]y definida en (6) sobre la secuencia {xi}, para obtener una matriz S, de tamaño3×(N−1).

$$T(x_i) = mod(round(abs(x_i) - floor(abs(x_i) \times 10^{14})), 256)$$

(6)

- Permutación de las matrices DR, DG y DB utilizando las filas de la matriz S: S1, S2 y S3, respectivamente. Este proceso se lleva a cabo a través de rotaciones circulares de cada columna así: el valor en la entrada j de S1 (S1j) determina la rotación de la columna j en la matriz DR, cuya magnitud k es dada por(7).

$$k = mod(S_{1,j}, N - 1)$$

(7)

De manera similar se utilizan las entradas de las filas S2 y S3 para rotar circularmente las columnas de DG y DB, respectivamente.

- Transposición de las tres matrices permutadas en el paso anterior, para aplicar nuevamente el mismo mecanismo sobre las columnas de estas y finalmente volver a transponer las matrices resultantes, obteniendo tres matricesD_(p)^(R),D_(p)^(G) y D_(p)^(B)de tamaño(M−1)×(N−1).
- Adhesión de la primera fila y columna, recortadas al inicio de la fase de difusión de las matrices originales, sobre lasD_(p)^(R),D_(p)^(G) y D_(p)^(B)correspondientes.
- Recomposición en una imagen RGB a partir de las tres matrices generadas en el ítem anterior, dando como resultado la imagen encriptada.

Dado que los operados cuánticos y las demás operaciones aplicadas, son reversibles, el proceso de desencriptación se lleva a cabo realizando los mismos pasos de manera inversa. La Fig. 6 muestra las imágenes de prueba obtenidas de USC-SIPI Image Database [28] y los resultados de aplicar el algoritmo de encriptación/desencriptación propuesto.

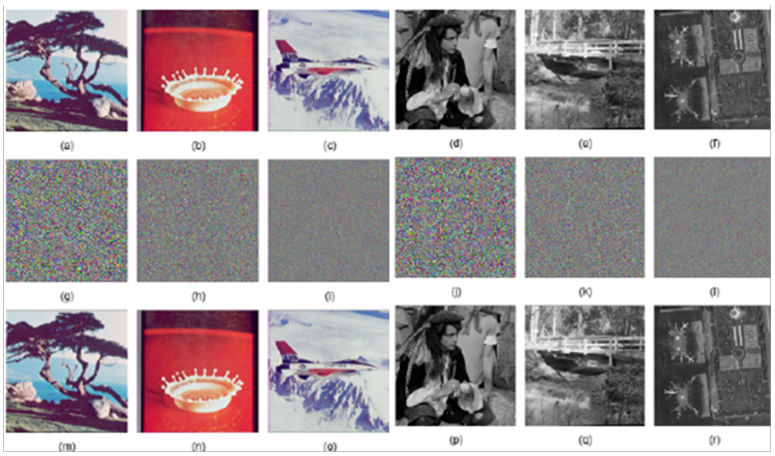


Fig. 6. *Imágenes originales, cifradas y descifradas.*
Fuente: [29].

4. RESULTADOS

Con el fin de validar la eficacia y eficiencia del modelo propuesto, se llevaron a cabo pruebas de seguridad y desempeño las cuales se presentan en esta sección.

4.1. Análisis Diferencial

Esta prueba compara los resultados de encriptar dos imágenes que difieren únicamente en el valor de un pixel, esperando que dichos resultados sean notoriamente diferentes, lo cual se mide usando los indicadores NPCR (Number of Pixels Change Rate) y UACI (Unified Average Changing Intensity). A partir de las dos imágenes encriptadas, el primero de estos compara e indica el porcentaje de pixeles en los que difieren, mientras que el segundo, muestra la diferencia promedio en la intensidad de los pixeles. Las expresiones matemáticas para su cálculo, están dadas por (8), (9) y (10) válidas para imágenes de tamaño M×N, siendo C1 y C2 las dos encriptaciones resultantes.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%$$

$$D(i,j) = \begin{cases} 1, & if\ C_1(i,j) \neq C_2(i,j) \\ 0, & if\ C_1(i,j) = C_2(i,j) \end{cases}$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

De acuerdo con la literatura científica relacionada, los valores ideales para NPCR y UACI son aproximadamente 99,61% y 33,51% respectivamente, se considera que valores cercanos a estos óptimos indican alta resistencia a ataques diferenciales. En este caso se aplicaron sobre varias imágenes, en la Tabla 2 se presentan los resultados obtenidos con algunas de ellas, además de la comparación con el trabajo de[10].

Tabla 2: Valores NPCR yUACI

Imagen	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Splash	99.2073	99.1935	99.2053	33.2634	33.3185	33.3197
Splash1	99.6147	99.6446	99.6082	33.4492	33.5153	33.4790
Airplane	99.4193	99.4097	99.4091	33.3907	33.3481	33.3864
Airplane1	99.6128	99.6099	99.6131	33.4585	33.4692	33.4790
Male	98.8601	98.8601	98.8632	33.1640	33.2857	33.3155
Male1		99.6586			33.6368	
Airport	99.4186	99.4084	99.4131	33.4000	33.3790	33.3675
Airport1		99.6149			33.4560	
Tree	98.8037	98.8265	98.8433	33.2382	33.1580	33.2679
Bridge	99.2015	99.2298	99.2176	33.3026	33.2886	33.2874

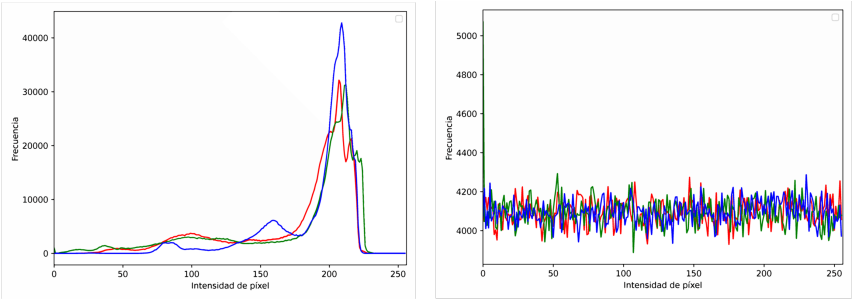
Fuente: Adaptado de [29], 1 Resultados reportados en [10].

Esta prueba es utilizada para determinar la robustez de un sistema criptográfico, frente a posibles amenazas o vulnerabilidad de información privada. Con este fin, se tienen en cuenta los histogramas, diagramas y coeficientes de correlación, así como los valores de varianza y entropía, tanto para imágenes originales como para cifradas.

4.2. Análisis Estadístico

Dado que el modelo propuesto es aplicable sobre imágenes a color y en escala de grises, a continuación, se presentan dos ilustraciones, una para cada escenario: imágenes Airplane (color) y Airport (grises).

La Fig. 7 corresponde a los histogramas de frecuencia para la imagen Airplane (color) original y cifrada, respetivamente, evidenciando que, al cifrar la imagen, los histogramas de frecuencia presentan alta uniformidad, contrario a lo que sucede con la imagen original.



(a) (b)

Fig. 7. *Histogramas para la imagen AirPlane original (a) y cifrada (b).*

Fuente: Elaboración Propia.

Continuando con el análisis de la imagen Airplane las Figs 8 y 9 muestran la correlación por cada capa en sentido horizontal, vertical y diagonal, para la original y la encriptada respectivamente, resaltando en la Fig. 9, la pérdida de correlación entre pixeles adyacentes.

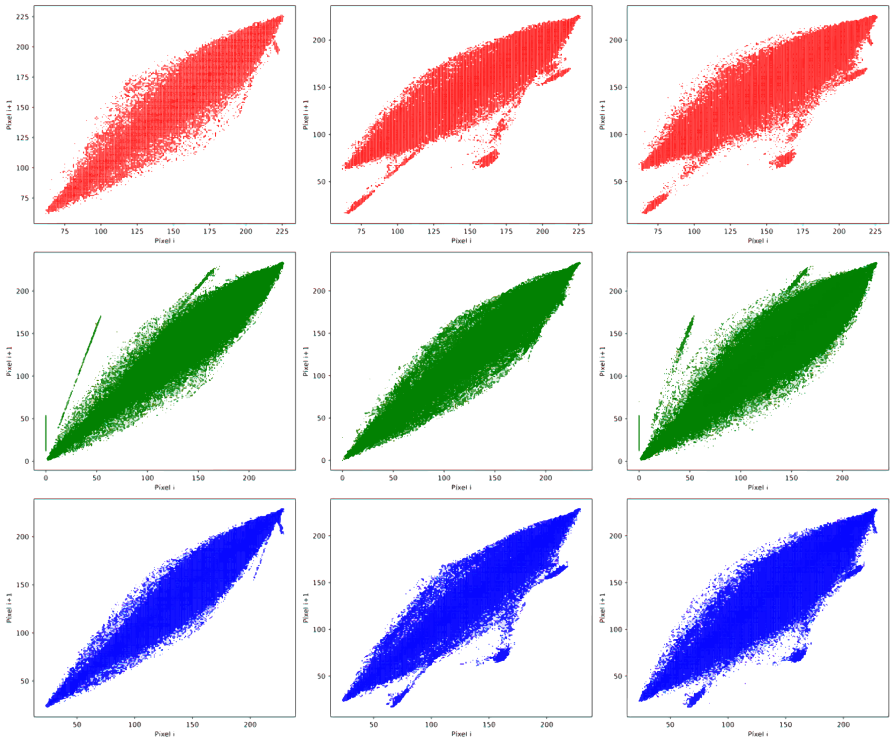


Fig. 8. *Correlación por capas de la imagen Airplane original.*
Fuente: Elaboración Propia

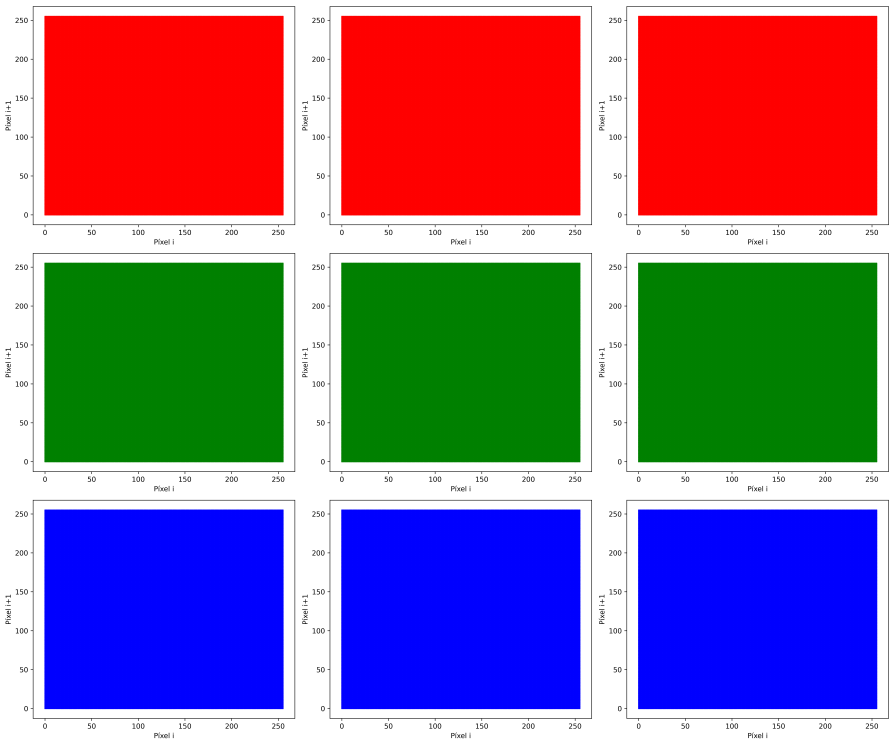


Fig. 9. *Correlación por capas de la imagen Airplane encriptada.*
Fuente: Elaboración propia

La Fig. 10 corresponde a los histogramas de frecuencia para la imagen Airport original y encriptada respectivamente, destacando que este algoritmo encripta en formato RGB las imágenes en escala de grises, lo cual se evidencia en el histograma de la imagen encriptada, caracterizado además por una alta uniformidad. Aunque en este caso se aumenta la cantidad de datos, esto se compensa con la ganancia en términos de seguridad ya que de una parte se genera pérdida completa de la semántica visual original y de otra, se dificulta la aplicación de ataques de reconstrucción inversa y de tipo estadístico, dado que el atacante pierde información estructural fundamental debido a la disminución en la correlación intercanal.

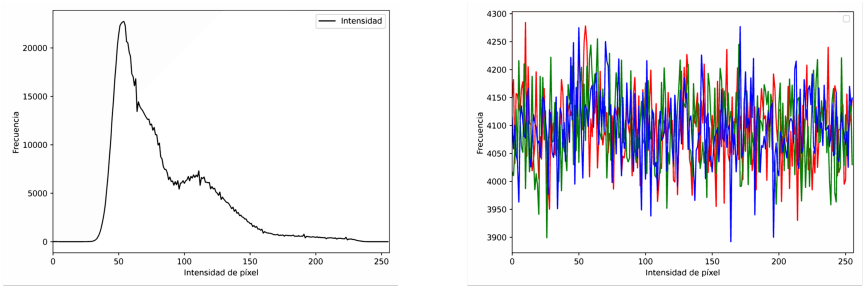


Fig. 10. *Histogramas para la imagen Airport original (a) y encriptada (b).*

Fuente: Elaboración Propia.

Adicionalmente, las Figs. 11 y 12 muestran los diagramas de correlación de pixeles adyacentes, correspondientes a la imagen Airport original y cifrada, respectivamente.

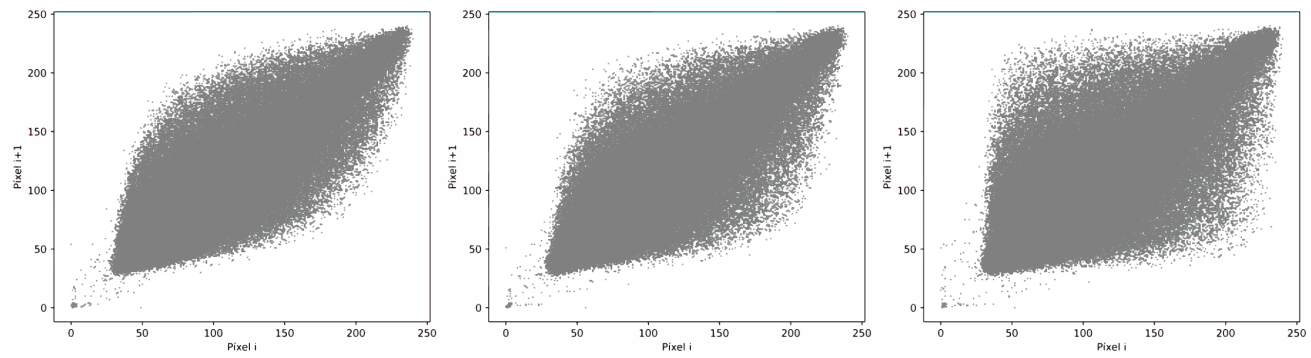


Fig. 11. *Diagrama de correlación Imagen Airport original en escala de grises.*
Fuente: Elaboración Propia.

En coherencia con lo anterior, en las Tablas 3 y 4 se presentan los valores de correlación obtenidos tanto para las imágenes originales como para los resultados de la encriptación, encontrando, como es de esperar, que las imágenes encriptadas arrojan valores próximos a cero.

Tabla 3: Coeficiente de correlación imagen a color (Airplane) original y encriptada

Imagen	Airplane								
	Horizontal			Vertical			Diagonal		
	R	G	B	R	G	B	R	G	B
Plane	0.992	0.991	0.993	0.986	0.992	0.991	0.980	0.984	0984
Encrypted	-0.001	-0.001	0.001	0.001	0.001	0.001	0.001	0.001	-0.001

Fuente: Elaboración Propia.

Tabla 4: Coeficiente de correlación imagen en escala de grises (Airport) original y encriptada

Imagen	Airport								
	Horizontal			Vertical			Diagonal		
	R	G	B	R	G	B	R	G	B
Plane	0.909			0.903			0.859		
Encrypted	0.001	-0.001	-0.001	0.001	0.001	0.001	0.001	0.001	-0.001

Fuente: Elaboración propia.

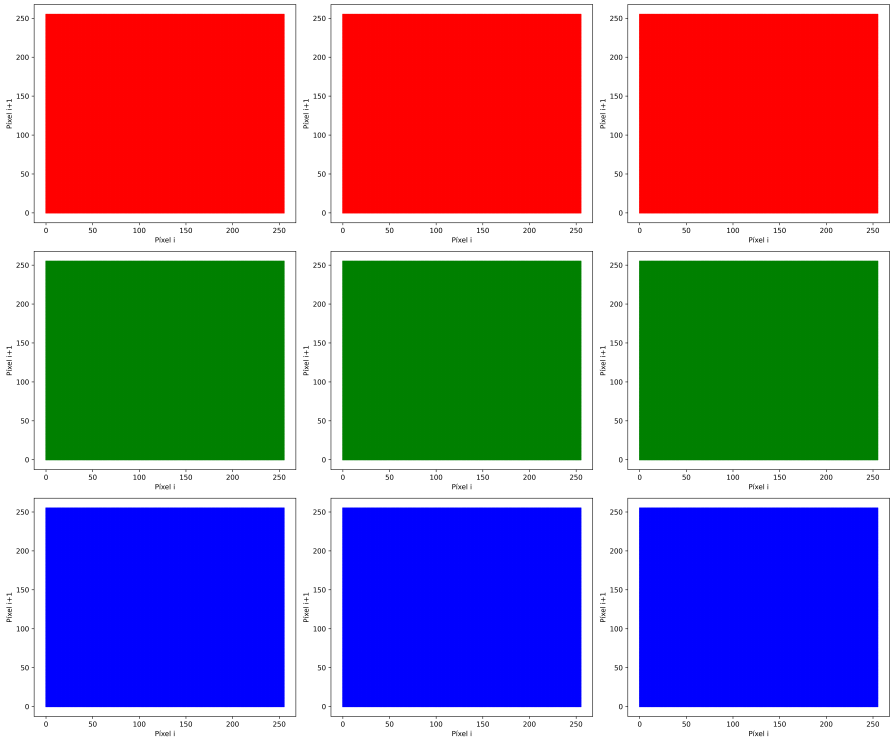


Fig. 12 Diagrama de correlación imagen Airport encriptada
Fuente: Elaboración Propia.

Los valores de varianza para la imagen original y cifrada son presentados en las Tablas 5 y 6, donde se señala el grado de dispersión de los datos con respecto a la media, en el caso de las imágenes encriptadas se desea obtener menores valores de varianza, lo cual indica que los pixeles están agrupados alrededor de la media y tienen poca variación, para el caso de estudio dichos valores se redujeron significativamente y fueron equiparables con los reportados en[10].

Tabla 5: Varianza imagen a color (Airplane) original y encriptada

Imagen	Imagen Original			Imagen Encriptada		
	R	G	B	R	G	B
Airplane	43’292.876	43’240.576	71’128.072	4.183,3	8.029,2	3.776,2
Airplane [10]	43’315.434,5	43’368.407,9	71’618.941,9	3.903,6	8.508,5	4671,1

Fuente: Elaboración Propia.

Tabla 6: Varianza imagen en escala de grises (Airport) original y encriptada

Imagen	Imagen Original	Imagen Encriptada		
		R	G	B
Airport	31’593.420	4.156,5	4.561,1	3.800,1
Airport [10]	31’720.325,7		4.023,2	

Fuente: Elaboración Propia.

Los valores de entropía para las imágenes encriptadas estuvieron cercanos a 8, como se muestra en la Tabla 7, lo cual indica un alto grado de desorden en la información encriptada, resaltando adicionalmente que dichos valores son equiparables con los resultados reportados en los artículos Fast and Robust Image Encryption Scheme Based on Quantum Logistic Map and Hyperchaotic System[9], Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)[10]y A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map[30].

Tabla 7: Valores de entropía, imágenes encriptadas

Imagen	Este trabajo	[9]	[10]	[30]
Airplane	7,99992	7,9977	7,9987	7,9998
Airport	7,99994	----	----	----

Fuente: Elaboración Propia.

4.3. Análisis de Seguridad de Claves

Dado que las claves del sistema propuesto están basadas en atractores caóticos sensibles a pequeñas perturbaciones, esto hace

que, al introducir un cambio insignificante en un componente de la clave, sea imposible recuperar la información original, situación que se presenta en la Fig. 13.

Utilizando la clave K1 para encriptar la imagen Airplane (Fig. 13a) se obtiene la Fig. 13b, al alterar una componente de K1 en 0.01 se obtiene la clave K2 y con ella la imagen encriptada de la Fig. 13c, a pesar de que ante el ojo humano dichos resultados parecen idénticos, la imagen de la Fig. 13d muestra los valores absolutos de la diferencia entre estas dos, evidenciando que los resultados de las Figs. 13b y 13c son diferentes. Al intentar desencriptar la imagen b de la Fig. 13 con la clave K1 se obtiene la original Airplane (Fig. 13e) mientras que, si se utiliza K2 para desencriptarla, se hace imposible su recuperación, tal como se observa en la Fig. 13f, situación deseable en un proceso criptográfico.

Por otra parte, respecto al tamaño del espacio de clave, se toman en cuenta los siguientes valores:

- Parámetros β y r, del sistema logístico, con precisión de 3 cifras decimales para un total de$(10^3)^2$posibles valores.

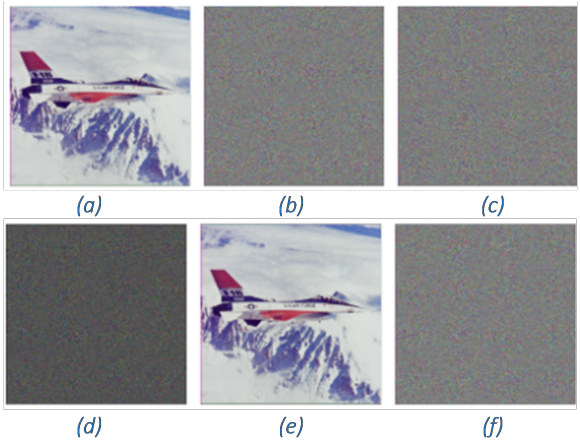


Fig. 13. *Sensibilidad de clave.*
Fuente: [29].

- Condiciones iniciales (x0, y0, z0) del sistema logístico, con 3 decimales de precisión obteniendo$(10^3)^3$posibles valores.
- Llaves de difusión del sistema logístico cuántico con 3 cifras enteras dando como resultado$(10^3)^3$posibles valores.
- Dos números primos de 15 cifras enteras con$(10^{15})^2$posibilidades.
- Parámetro r y condición inicial x0, del sistema logístico tienda, con 3 cifras decimales de precisión para un total de$(10^3)^2$posibles valores.

Por lo anterior, el tamaño del espacio de clave es de10^{60}el cual supera notoriamente varios de los resultados reportados en la literatura consultada, tales como los trabajos de Man y colaboradores [31], Kamal y colaboradores [32] y Ahmed y colaboradores [33], cuyos espacios de clave reportados son 1029, 1035 y 1038, respectivamente.

Cabe resaltar que el NIST[34]ha establecido criterios para considerar si un algoritmo criptográfico es resistente a ataques cuánticos, entre ellos seguridad semántica y ataque adaptativo, para los cuales el modelo que aquí se presenta es robusto debido a que las claves generadas son altamente sensibles a pequeñas perturbaciones ya que provienen de la utilización de sistemas dinámicos caóticos, por esta razón podría afirmarse que el algoritmo es resistente a ataques de búsqueda de Grover[35][19], ya que este ataque disminuiría la complejidad a O(1030), que sigue siendo alta.

4.4. Análisis de Robustes

Para validar la eficacia del modelo propuesto, se llevaron a cabo varias pruebas de robustez, las cuales se presentan a continuación.

4.4.1. Robustez con imágenes planas

Este tipo de análisis consiste en encriptar imágenes de un solo color, usualmente blanco o negro, o patrones generados con estos dos colores y verificar que el modelo es capaz de desencriptarlas adecuadamente. En este caso se encriptaron las imágenes a, b y c de la Fig. 14, obteniendo los resultados que se presentan en las figs 14d, 14e y 14f respectivamente, sobre las cuales se aplicó el proceso de desencriptación y se obtuvieron las imágenes originales g, h e i.

4.4.2. Prueba de Sal y Pimienta

A partir de una imagen encriptada, resultado de aplicar el algoritmo propuesto, se reemplaza, de manera aleatoria, una proporción de pixeles convirtiéndolos en blancos o negros, sobre esta última se aplica el proceso de desencriptación. El propósito de dicha prueba es recuperar, con un alto grado de fidelidad, la imagen original. En este caso se tomó como referente

la imagen a color “Airplane” y se modificaron el 1%, 5% y 10% de los pixeles en la imagen encriptada (Fig. 15a, 15b y 15c, respectivamente). Posteriormente se aplicó el algoritmo de desencriptación, logrando recuperar la imagen original con mínimas distorsiones ante el ojo humano (Fig. 15d, 15e y 15f).

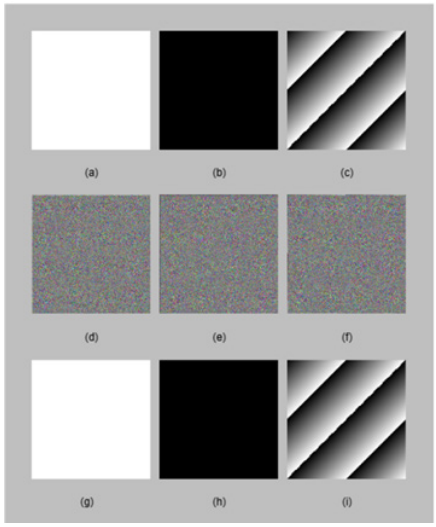


Fig. 14. *Robustez con imágenes planas.*
Fuente: [29].

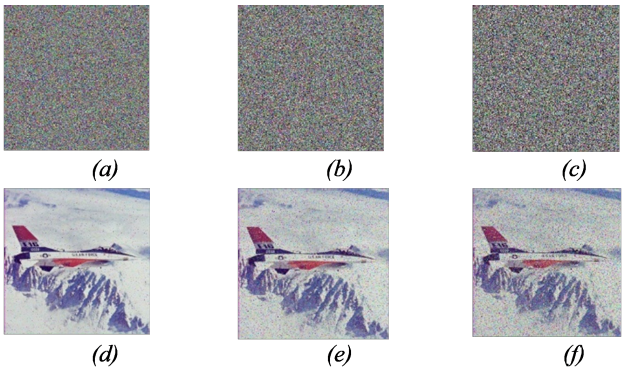


Fig. 15. *Prueba de sal y pimienta imagen color.*
Fuente: Elaboración Propia.

Con el fin de obtener una medición más exacta de los resultados hallados en esta prueba, se calcularon las métricas de error cuadrático medio (MSE) y Relación señal ruido máximo (PSNR), para evaluar el grado de similitud entre las imágenes desencriptadas (luego de aplicar la prueba de sal y pimienta) y la original, tomando como base las mismas proporciones de cambio aplicadas a la imagen encriptada, los resultados se presentan en la Tabla 8.

Tabla 8: Error cuadrático medio y relación señal ruido máximo para la imagen Airplane

Proporción de Ruido	MSE			PSNR		
	R	G	B	R	G	B
1%	3,12406	3,10448	3,10896	43,18361	43,21091	43,20465
5%	14,71433	14,65387	14,67258	36,45339	36,47127	36,46573
10%	27,30998	27,26267	27,29098	33,76758	33,77511	33,77061

Fuente: Elaboración Propia.

En este caso, un valor alto de MSE indica pérdida de información, lo que se evidencia en la Tabla 8 cuando se aplica una proporción de ruido del 5 % o del 10 %. Así mismo, un PSNR superior a 40 indica que la imagen original es muy similar a la imagen descifrada tras aplicar la prueba de sal y pimienta, lo que resultó evidente cuando la proporción de ruido era del 1 %. Sin embargo, proporciones de ruido más altas mostraron algunas diferencias entre las imágenes.

Similarmente se tomó la imagen en escala de grises “Airport” aplicándole el mismo procedimiento que a “Airplane” obteniendo así, resultados consistentes ante el ojo humano, situación que se evidencia en la en la Tabla 9 y en la Fig. 16.

Tabla 9: Error cuadrático medio y relación señal ruido máximo para la imagen Airport

Proporción de Ruido	MSE			PSNR		
	R	G	B	R	G	B
1%	3,14382	3,11217	3,13636	43,15622	43,20016	43,16654
5%	14,69363	14,73378	14,72717	36,45951	36,44765	36,44961
10%	27,37235	27,34791	27,34637	33,75768	33,76156	33,76168

Fuente: Elaboración Propia.

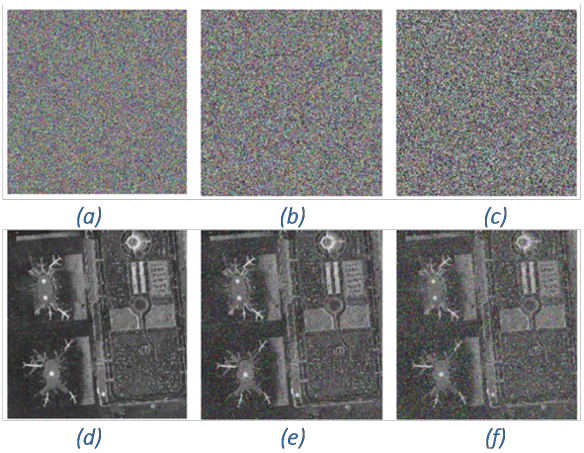


Fig. 16. *Prueba de sal y pimienta imagen grises.*
Fuente: Elaboración Propia.

4.4.3. Prueba de Oclusión

Esta prueba consiste en tomar una imagen encriptada, recortarle una porción rectangular para reemplazarla por pixeles negros y luego de modificada, desencriptarla. El objetivo de esta prueba es verificar qué tan eficiente es el algoritmo para recuperar la imagen original aún después de perder una proporción de la información encriptada.

Para el caso de estudio, se realizaron varias pruebas con la encriptación de la imagen Airplane, recortando 1/16, 1/8, 1/4 y 1/2 como se observa en la Fig. 17 (a, b, c y d). Es de destacar que en las 4 modificaciones se logró recuperar gran parte de la imagen original, situación coherente con lo esperado y que se muestra en la misma Fig. 17 (e, f, g y h).

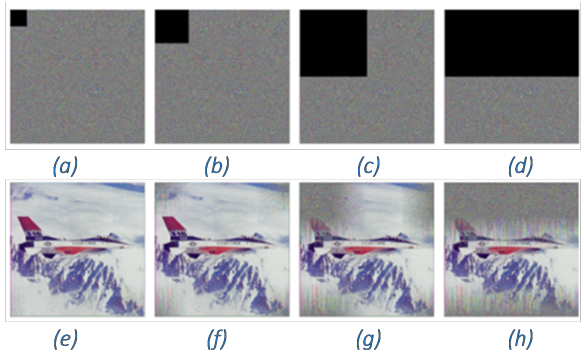


Fig. 17. *Ataques de oclusión sobre la imagen Airplane.*
Fuente: [29].

Con base en las pruebas de seguridad y desempeño aplicadas, es posible afirmar que el modelo aquí presentado es resistente a ataques de texto plano escogido (CPA) y de solo texto plano (COA), ya que el análisis de robustez muestra la inexistencia de patrones visuales, adicionalmente la correlación de pixeles adyacentes es mínima y la clave es altamente sensible a pequeñas perturbaciones, es decir que un pequeño cambio en la imagen original genera cambios globales en la encriptada, mostrando su resistencia a ataques lineales. Así mismo, los resultados de pruebas de entropía, correlación, NPCR, UACI e histogramas, se ajustan a comportamientos ideales en el ámbito de la seguridad, lo cual indica resistencia a ataques diferenciales.

5. CONCLUSIONES

Se propuso un nuevo algoritmo de encriptación, inspirado en el dominio cuántico, mediante la integración de principios de

mecánica cuántica, teoría del caos y tratamiento de imágenes el cual basa su seguridad en la alta aleatoriedad de las secuencias caóticas y en el principio físico de la superposición de qbits.

Para el caso de las imágenes en escala de grises, el algoritmo propuesto genera una encriptación en formato RGB, lo cual contribuye a disminuir las posibilidades de acceso fraudulento a la imagen original, situación deseable especialmente en el caso de imágenes médicas.

Por otra parte, el algoritmo fue ejecutado en un computador clásico y sometido a análisis de seguridad y desempeño, aplicando pruebas de ataque diferencial, estadístico, seguridad de claves y robustez, cuyos resultados permitieron concluir que es altamente seguro, por lo tanto, podría aplicarse en contextos reales.

Finalmente, conviene tener presente que el surgimiento de la computación cuántica genera desafíos y amenazas frente a la seguridad de la información, por lo que es imperativo seguir en la búsqueda de nuevos algoritmos criptográficos que permitan llevar a cabo una transición segura hacia la era poscuántica, buscando asegurar la información de tipo político, económico, militar, científico y social.

RECONOCIMIENTO

Los autores agradecen a la Universidad Distrital Francisco José de Caldas por su apoyo institucional durante la realización de esta investigación.

REFERENCIAS

[1] K. Cherkaoui Dekkaki, I. Tasic, y M.-D. Cano, «Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process», Technologies, vol. 12, n.o 12, p. 241, nov. 2024, doi: 10.3390/technologies12120241.

[2] P. Pekarčík y E. Chovancová, «Post-Quantum Encryption Algorithms», Acta Electrotech. Inform., vol. 25, n.o 3, pp. 16-24, sep. 2025, doi: 10.2478/aei-2025-0011.

[3] Y. Zhang, K. Lu, Y. Gao, y M. Wang, «NEQR: a novel enhanced quantum representation of digital images», Quantum Inf. Process., vol. 12, n.o 8, pp. 2833-2860, ago. 2013, doi: 10.1007/s11128-013-0567-z.

[4] L. Wang, Q. Ran, J. Ma, S. Yu, y L. Tan, «QRCI: A new quantum representation model of color digital images», Opt. Commun., vol. 438, pp. 147-158, 2019, doi: https://doi.org/10.1016/j.optcom.2019.01.015.

[5] L. Wang, Q. Ran, y J. Ding, «Quantum Color Image Encryption Scheme Based on 3D Non-Equilateral Arnold Transform and 3D Logistic Chaotic Map», Int. J. Theor. Phys., vol. 62, n.o 2, p. 36, feb. 2023, doi: 10.1007/s10773-023-05295-y.

[6] M. Hu, J. Li, y X. Di, «Quantum image encryption scheme based on 2D $$\varvec{Sine^{2}-Logistic}$$chaotic map», Nonlinear Dyn., vol. 111, n.o 3, pp. 2815-2839, feb. 2023, doi: 10.1007/s11071-022-07942-1.

[7] M. Khan y H. M. Waseem, «A novel image encryption scheme based on quantum dynamical spinning and rotations», PLOS ONE, vol. 13, n.o 11, p. e0206460, nov. 2018, doi: 10.1371/journal.pone.0206460.

[8] Y. Gao, H. Xie, J. Zhang, y H. Zhang, «A novel quantum image encryption technique based on improved controlled alternated quantum walks and hyperchaotic system», Phys. Stat. Mech. Its Appl., vol. 598, p. 127334, 2022, doi: https://doi.org/10.1016/j.physa.2022.127334.

[9] N. A. E.-S. Mohamed, A. Youssif, y H. A.-G. El-Sayed, «Fast and Robust Image Encryption Scheme Based on Quantum Logistic Map and Hyperchaotic System», Complexity, vol. 2022, n.o 1, p. 3676265, ene. 2022, doi: 10.1155/2022/3676265.

[10] N. A. E.-S. Mohamed, H. El-Sayed, y A. Youssif, «Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)», Fractal Fract., vol. 7, n.o 10, p. 734, oct. 2023, doi: 10.3390/fractalfract7100734.

[11] R. L. Devaney, An Introduction to Chaotic Dynamical Systems, 3.a ed. Boca Raton: Chapman and Hall/CRC, 2021. doi: 10.1201/9780429280801.

[12] Edward Norton Lorenz, «Deterministic Nonperiodic Flow», J. Atmospheric Sci., vol. 20, n.o 2, pp. 130-141, 1963, doi: https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2.

[13] Igor V. Ovchinnikov, «Ubiquitous order known as chaos», Chaos Solitons Fractals, vol. 181, abr. 2024, doi: https://doi.org/10.1016/j.chaos.2024.114611.

[14] Arianna Calistri, Pier Francesco Roggero, y Giorgio Palu, «Chaos theory in the understanding of COVID-19 pandemic dynamics», Gene, vol. 912, Elsevier BV, Amsterdam, Países Bajos, junio de 2024. doi: https://doi.org/10.1016/j.gene.2024.148334.

[15] Marat Akhmet, Madina Tleubergenova, Akylbek Zhamanshin, y Zakhira Nugayeva, Artificial Neural Networks: Alpha Unpredictability and Chaotic Dynamics. Cham, Suiza: Springer Nature Switzerland AG, 2024.

[16] B. Zwiebach, Mastering quantum mechanics: essentials, theory, and applications. Cambridge, Mass: The MIT press, 2022.

[17] M. E. Goggin, B. Sundaram, y P. W. Milonni, «Quantum logistic map», Phys. Rev. A, vol. 41, n.o 10, pp. 5705-5708, may 1990, doi: 10.1103/PhysRevA.41.5705.

[18] R. P. Feynman, «Simulating physics with computers», Int. J. Theor. Phys., vol. 21, n.o 6-7, pp. 467-488, jun. 1982, doi: 10.1007/BF02650179.

[19] M. A. Nielsen y I. L. Chuang, Quantum Computation and Quantum Information, 10th Aniversary. United Kingdom: Cambridge

University, 2010.

[20] T. G. Wong, Introduction to classical and quantum computing. Omaha, Nebraska: Rooted Grove, 2022.

[21] «PNGWING», Imágenes libres png. [En línea]. Disponible en: https://www.pngwing.com/es

[22] A. F. Kockum y F. Nori, «Quantum Bits with Josephson Junctions», en Fundamentals and Frontiers of the Josephson Effect, F. Tafuri, Ed., Cham: Springer International Publishing, 2019, pp. 703-741. doi: 10.1007/978-3-030-20726-7_17.

[23] P. Kaye, R. Laflamme, y M. Mosca, An introduction to quantum computing. en Oxford scholarship online. Oxford: Oxford University Press, 2020. doi: 10.1093/oso/9780198570004.001.0001.

[24] R. Wolf, Quantum Key Distribution: An Introduction with Exercises, vol. 988. en Lecture Notes in Physics, vol. 988. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-73991-1.

[25] B. Hanafi y M. Ali, «Analyzing the research impact in post quantum cryptography through scientometric evaluation», Discov. Comput., vol. 28, n.o 1, p. 32, abr. 2025, doi: 10.1007/s10791-025-09507-3.

[26] T. Hasija, K. R. Ramkumar, A. Kaur, y M. S. Bali, «Exploring the landscape of post quantum cryptography: a bibliometric analysis of emerging trends and research impact», J. Big Data, vol. 12, n.o 1, p. 225, sep. 2025, doi: 10.1186/s40537-025-01269-5.

[27] Y.-K. Liu y D. Moody, «Post-quantum cryptography and the quantum future of cybersecurity», Phys. Rev. Appl., vol. 21, n.o 4, p. 040501, abr. 2024, doi: 10.1103/PhysRevApplied.21.040501.

[28] Signal and Image Processing Institute, «The USC-SIPI Image Database», USC Viterbi. [En línea]. Disponible en: https://sipi.usc.edu/database/

[29] M. A. Rico-García, «Modelo de Encriptación de Imágenes Utilizando Atractores Caóticos y Principios de Computación Cuántica», Informe final Proyecto de grado, Distrital Francisco José de Caldas, Bogotá, 2025. [En línea]. Disponible en: https://repository.udistrital.edu.co/items/c20fb3bc-01f4-4f50-9a1a-8314a665cf8a

[30] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, y I. Hussain, «A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map», Entropy, vol. 22, n.o 3, p. 274, feb. 2020, doi: 10.3390/e22030274.

[31] Z. Man, J. Li, X. Di, Y. Sheng, y Z. Liu, «Double image encryption algorithm based on neural network and chaos», Chaos Solitons Fractals, vol. 152, p. 111318, 2021, doi: https://doi.org/10.1016/j.chaos.2021.111318.

[32] S. T. Kamal, K. M. 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, doi: 10.1109/ACCESS.2021.3063237.

[33] F. Ahmed, A. Anees, V. U. Abbas, y M. Y. Siyal, «A Noisy Channel Tolerant Image Encryption Scheme», Wirel. Pers. Commun., vol. 77, n.o 4, pp. 2771-2791, ago. 2014, doi: 10.1007/s11277-014-1667-5.

[34] NIST Computer Security Resource Center, «Post-Quantum Cryptography (PQC)», Evaluation Criteria. Accedido: 20 de enero de 2026. [En línea]. Disponible en: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria

[35] Lov K. Grover, «A fast quantum mechanical algorithm for database search», Proc. Twenty-Eighth Annu. ACM Symp. Theory Comput., pp. 212-219, jul. 1996, doi: https://doi.org/10.1145/237814.237866.

FINANCIACIÓN

Ninguna

CONFLICTOS DE INTERÉS

No existen

CONTRIBUCIÓN DE AUTORÍA

Redacción - borrador original: Miguel Ángel Rico García, Luz Deicy Alvarado Nieto, Edilma Isabel Amaya Barrera.

Redacción - revisión y edición: Miguel Ángel Rico García, Luz Deicy Alvarado Nieto, Edilma Isabel Amaya Barrera.