Digital Object Identifier: 10.24054/rcta.v1i47.4270

Image Encryption Using Chaos and Quantum Gates

Encriptación de imágenes usando caos y compuertas cuánticas

Ing. Miguel Ángel Rico García [1], **PhD. Luz Deicy Alvarado Nieto** [1]
MSc. Edilma Isabel Amaya Barrera [1]

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

Correspondence: *lalvarado@udistrital.edu.co*

Received: *August 29, 2025.* ***Accepted:*** *December 18, 2025.* ***Published:*** *January 30, 2026.*

How to cite: *M. A. Rico García, L. D. Alvarado Nieto, and E. I. Amaya Barrera, "Image Encryption Using Chaos and Quantum Gates", RCTA, vol. 1, n.º. 47, pp. 188-201, Jan. 2026.*
Retrieved from https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4270

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.

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.

1. INTRODUCTION

Cryptography is responsible for proposing strategies for the protection of private information. In recent times, new developments based on principles of mathematics and artificial intelligence have emerged, trying to respond to new challenges arising from technological advances that lead to the exchange of large amounts of digital information.

Traditional encryption methods such as RSA (Rivest-Shamir-Adleman) and ECC (elliptic curve cryptography) are not suitable when working with large amounts of data because they present high levels of redundancy in the information and base their security on the problem of decomposing an integer into its prime factors, which is considered a Non-deterministic Polynomial time (NP) problem. With the emergence of quantum computers, the solution time for this problem can be significantly reduced and become logarithmic, which would lead to a global security catastrophe. This fact has driven research by the academic and scientific community, resulting in significant work in this direction.

Quantum computing has introduced significant challenges for information security; consequently, proposals have emerged aimed at preparing the transition to this new scenario. In response, the National Institute of Standards and Technology (NIST) has undertaken the task of establishing security standards for the post-quantum era [1], [2].

Currently, proposals for image representation in the quantum context have been developed, one of them can be found in the work of Zhang, Gao y Wang [3], which is still in use and has even had proposals for improvement, as presented by Wang et al [4], used in the proposal by Wang, Rang, and Ding [5], as well as in Hu, Li, and Di [6], to propose a model for encrypting grayscale images using quantum gates, rotation operations similar to the functioning of a Rubik's cube, and a chaotic two-dimensional system generated from one-dimensional logistic and sinusoidal systems. With the same approach, the work proposed in the article *A Novel Image Encryption Scheme Based on Quantum Dynamical Spinning and Rotations* [7] stands out, in which the authors propose a RGB image encryption algorithm using rotation matrices and half-spin particle representation.

In addition, the use of chaotic dynamic systems in the field of cryptography has evolved to apply these systems in the quantum environment, so it is common to find quantum circuits related to these systems, such as the work proposed by Gao et al [8], who proposed a new algorithm for encrypting quantum images represented by the NEQR model, also using Arnold's two-dimensional chaotic attractors and the hyperchaotic Lorenz system, with their corresponding implementations of quantum circuits.

Similarly, in the works *Fast and Robust Image Encryption Scheme Based on Quantum Logistic Map and Hyperchaotic System* [9] and *Mixed Multi-Chaos Quantum Image Encryption Scheme Based on Quantum Cellular Automata (QCA)* [10], the authors propose color image encryption models, involving in both cases quantum chaotic dynamic systems and quantum gates.

Considering the advances in quantum computing and their implications for the protection of digital information, this article presents a color digital image encryption model inspired by the quantum domain, which employs classical and quantum chaotic dynamical systems, as well as quantum gates, which is implemented using classical hardware and validated through security and performance metrics. The results suggest that this model can be applied to real environments. It is important to note that the algorithm proposed here can also be used for grayscale images, producing an encrypted result in RGB scale, which constitutes a strategic cryptographic advantage, as it promotes the emergence of more complex dynamics, thereby enhancing the structural security of the model. The following sections describe the preliminary knowledge, methodology used, detailed description of the algorithm, application of performance metrics, and conclusions.

2. MATERIALS AND METHODS

This section includes the theoretical elements used as a basis for developing the proposed algorithm, explaining the phases of the methodology carried out.

2.1. Preliminary Knowledge

The conceptual foundations that were considered for the approach of the model are presented here.

2.1.1. Classical And Quantum Chaotic Attractors

A dynamic system is characterized by evolving according to a deterministic rule of a continuous or discrete type. If this evolution is sensitive to small perturbations, it may fall within the field of chaos theory. Specifically, a system is considered chaotic if it satisfies three conditions: sensitivity to perturbations, transitivity, and density of periodic points [11].

The concept of chaos was introduced by the meteorologist Edward Lorenz [12] through an experiment that gave rise to what was later termed the “butterfly effect” and that is currently regarded as a significant reference for researchers of nonlinear complex phenomena, highlighting that numerous behaviors across different fields of knowledge fall within this framework, such as climate modeling, epidemics, and the stock market, among others [13], [14], [15].

In nonlinear dynamic systems within a chaotic environment, it is common for chaotic-strange attractors to appear, which are characterized by high sensitivity, non-periodicity, fractal structure, and non-integer dimension. These properties are useful in the context of cryptographic schemes, as they produce pseudo-random sequences that can be used in the design of encryption algorithms.

In recent decades, new chaotic dynamic systems have been formulated due to their impact on security, seeking to obtain more complex behaviors that lead to greater robustness of cryptographic systems based on such attractors. An example of this is the hybrid model obtained from the logistic and tent systems, which is described by (1) [10].

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

The immersion of quantum physics principles in the computing scenario led to the extrapolation of the concept of chaos to the quantum domain, despite the fact that there are no defined trajectories and the system evolves with quantum superposition, presenting uncertainty in accordance with Heisenberg's principle and linear and unitary evolution in accordance with Schrödinger's equation [16]. In this context, quantum chaos deals with the study of its chaotic analogues, which involves analyzing structures in Hilbert space parallel to classical attractors, in other words, transitions to complex quantum dynamics are studied. One of the classical quantum chaotic attractors is the logistic attractor, used as input for the diffusion part of the algorithm described in the work of Goggin, Sundaram and Milonni [17].

2.1.2. Quantum Computing

The evolution of classic computers in terms of size and speed is reaching its limits. It is almost impossible to create integrated circuits with a greater number of components while maintaining or attempting to reduce their size. This has led to supercomputing platforms, used especially to run artificial intelligence models, are composed of enormous quantities of very powerful computers that occupy entire buildings dedicated exclusively to housing them. At the same time, the generation of new and powerful algorithms that demand great memory capacity and speed in these machines has driven the search for other storage and processing alternatives. Quantum computing, then, becomes an alternative from which promising results are expected.

The work “*Simulating Physics with Computers*” [18] can be regarded as the starting point of quantum computing. In this work, Richard Feynman conceived the idea of developing quantum computers to simulate systems involving nanoparticles. Currently, significant advances have been achieved in the development of this type of computer, giving rise to new scientific challenges [19].

Contrasting classical computing, whose minimum unit of information is the bit, with the quantum system, this unit corresponds to the Qbit, which can assume the states zero, one, or both (superposition) and thus combine with other Qbits, allowing a greater number of operations to be carried out simultaneously. To represent them, Dirac notation is used, in which the values 0 or 1 are placed in the middle of a vertical line and an angle in the form of a bracket, called a ket: |0⟩, |1⟩. Thus, the basic states are named ket zero and ket one, respectively, which are represented as the north and south poles on a unitary sphere called the "Bloch sphere" (see Fig. 1). Likewise, entanglement allows Qbits to be manipulated in such a way that their behavior is synchronized, achieving exponential growth in parallel operations with respect to the number of Qbits the computer works with [20]. Fig. 1 represents the Bloch sphere, which shows several of the possible states for a Qbit.

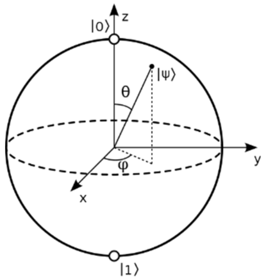


Fig. 1*. Bloch sphere with several possible states for a Qbit.*
Source: *PNGWING [21].*

In order to perform operations with these Qbits, several gates that act on them, have been defined, similarly, logic gates act to perform operations and design circuits with traditional bits. The basic states of a qubit can also be represented in a 2 × 1 vector, so $|0\rangle$ can be represented as $\binom{1}{0}$ and $|1\rangle$ as $\binom{0}{1}$. When it is necessary to apply logic gates to more than one qubit, tensor product is used to combine the qubits, obtaining, for example, $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ as possible results, thus facilitating their operation with these gates.

In this work, besides to the application of the tensor product, the following gates were used: CNOT, Toffoli, and Swap, which are reversible and are described below.

2.1.2.1. CNOT Gate (Controlled Not Gate)

The CNOT gate acts on two qubits, changing the second one if the first (the control qubit) is in state 1. In other words, if it is applied to $|00\rangle$ or $|01\rangle$, there will be no change, but if it is applied to $|10\rangle$, the result will be $|11\rangle$, and if it is applied to $|11\rangle$, the result obtained is $|10\rangle$ [22]. The matrix representation of this gate is shown in (2) [10], [23].

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad (2)$$

The circuit corresponding to this gate shows its two inputs, the symbol ⊕ acting on the two qubits, and the result obtained, which is shown in Fig 2.

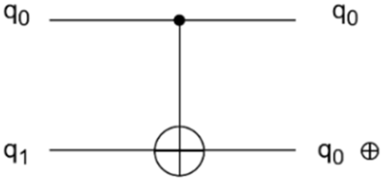


Fig. 2*. CNOT gate.*
Source: *Adapted from [23] and [24].*

2.1.2.2. Toffoli Gate (CNOT-Controlled Gate)

This gate acts on three qubits, the first two of which play the role of control and the third is the output. If the first two qubits are at 1, the value of the third changes; otherwise, it remains the same. In other words, if you have the input qubits $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle$ or $|101\rangle$, it will remain, whereas if the gate is applied to the qubits $|110\rangle$ o $|111\rangle$, the result will be $|111\rangle$ and $|110\rangle$, respectively [24]. The matrix representation of this gate is shown in (3).

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad (3)$$

Similar to the CNOT gate, Toffoli's circuit shows the three inputs, the symbol ⊕ acting on the three qubits, and the result generated on the last one, as shown in Fig. 3.

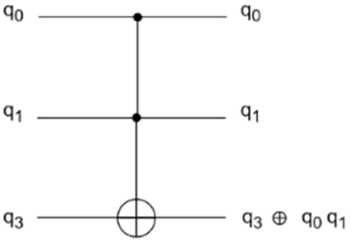


Fig. 3*. Toffoli gate.*
Source: *Adapted from [20] and [24].*

2.1.2.3. Swap Gate

This gate is applied to two qubits by swapping their values, i.e., if the input is $|10\rangle$, the output will be $|01\rangle$ and vice versa. If the two qubits have the same value, they will remain as they are [24]. The matrix representation of this gate is shown in (4).

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (4)$$

Similar to the two previous gates, this one is represented as a circuit, as shown in Fig. 4

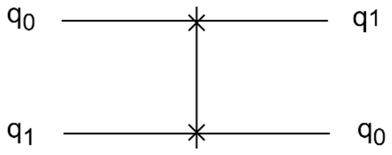


***Fig. 4**. Swap gate.*
***Source:** Adapted from [20] and [24].*

2.1.3. Cryptography

Needing to preserve the security and integrity of private information has made cryptography a constant presence throughout human evolution, becoming constantly more important due to the increase in the amount of digital information circulating through public channels. The purpose of cryptography is to transform information through encoding into an illegible result in order to mask it from intruders. There are two types: symmetric (same key for encryption and decryption), as in the case of DES (Data Encryption Standard), and asymmetric (one key for encryption and another for decryption), as in the case of RSA (Rivest, Shamir, Adleman). Conventional methods are not appropriate when dealing with large volumes of data such as images or multimedia files, due to redundancy. This has led to new proposals based on, among other things, elliptic curve theory, cellular automata, neural networks, or chaos.

Due to the potential of the properties inherent in chaotic systems, cryptographic algorithms based on them have attracted academic interest since the late 20th century. Proof of this is the rise of a line of research called chaotic cryptography, connecting academics interested in making collective efforts and exchanging knowledge to formulate security schemes. In this regard, there has been a significant increase in cryptography proposals based on chaos theory, due to the similarity between the properties of a chaotic system and those required in a cryptographic algorithm. The sensitivity to initial conditions and unpredictability in a chaotic system make it so that an apparently insignificant change in an encryption key generates a drastically different output, which in turn implies that when attempting to decrypt that output, the original information cannot be recovered. Additionally, if someone is able to access an encrypted message, they cannot predict what the next one will be. On the other hand, the complexity of the chaotic system, in the context of encryption, implies that it is more difficult to attempt to decrypt the message fraudulently.

Therefore, cryptography has contributed to the study and formulation of new chaotic systems, mostly based on existing ones, by combining them or extending them to a higher-dimensional space, bearing in mind to increasing the level of complexity and thus ensuring greater security for cryptographic models that use pseudorandom sequences, as is the case with the work proposed by Mohamed et al [10]. Similarly, the objective is to correct deficiencies and consolidate foundations to continue advancing in the field of chaotic cryptography, without forgetting that, despite new developments in the field, it faces threats from quantum computing [1], [2], [25], [26], [27], making it necessary to continue exploring new areas searching for cybersecurity solutions.

2.2. Methodology

The process followed to consolidate the algorithm proposed in this work employed a mixed approach that involved both qualitative and quantitative aspects. The qualitative aspect aims to ensure high randomness in the pseudo-random sequences used, while the quantitative aspect is involved in validating the performance of the proposed algorithm and making the corresponding adjustments, in order to avoid undesirable values in the metrics applied, while comparing performance with current scientific references.

The algorithm, like most cryptographic systems, involved diffusion and confusion phases, in which quantum computing principles were used, as well as classical and quantum chaotic systems, consolidating a highly secure proposal, validated through the application of security and performance metrics. Fig.5 summarizes the process carried out in this work.

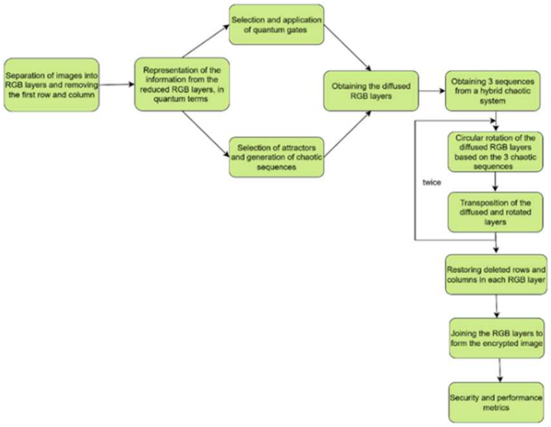

Separation of images into RGB layers and removing the first row and column
Representation of the information from the reduced RGB layers, in quantum terms
Selection and application of quantum gates
Selection of attractors and generation of chaotic sequences
Obtaining the diffused RGB layers
Obtaining 3 sequences from a hybrid chaotic system
Circular rotation of the diffused RGB layers based on the 3 chaotic sequences
Transposition of the diffused and rotated layers
twice
Restoring deleted rows and columns in each RGB layer
Joining the RGB layers to form the encrypted image
Security and performance metrics

Fig. 5. *Phases of the encryption algorithm.*

Source: *Own Elaboration.*

3. ALGORITHM DESCRIPTION

Each layer of a M×N image in RGB scale was subjected to the diffusion and confusion phases as detailed below:

3.1. Diffusion Phase

The information provided by a single pixel in an image is insignificant, especially at the edges. Removing pixels from the first or last row or column does not imply meaningful visual changes. If the rest of the image is encrypted and the removed row and column are added to this result, this strategy can confuse any attacker attempting to recover part of the original image or infer information from the edges, a favorable situation in terms of security, which is applied in the proposal described here. This and the rest of the processes carried out during the diffusion phase are described below.

- Separation of the RGB layers and crop the first row and column in each of them.
- Random selection of a cropped layer and, from it, a row or column to obtain the P average value.
- Iteration of the quantum logistic hyperchaotic system P times (taking only the integer part of P), with initial values $x_0 = 0.043$, $y_0 = 0.035$, $z_0 = 0.025$, $\beta = 6.859$, $r = 3.990$, which are ignored to ensure greater randomness.
- Continuing the previous iteration process $(M-1)\times(N-1)$ times, generating 3 chaotic sequences $\{x_i\}$, $\{y_i\}$, $\{z_i\}$.
- Obtaining three chaotic matrices designated as Q^R, Q^G, Q^B, by means of transformations taken from [8] and defined in (5):

$$Q_i^R = mod\big(floor((\varepsilon_1 . x_i) + \varepsilon_2), 256\big)$$
$$Q_i^G = mod\big(floor((\varepsilon_1 . y_i) + \varepsilon_2), 256\big)$$
$$Q_i^B = mod\big(floor((\varepsilon_1 . z_i) + \varepsilon_2), 256\big) \quad (5)$$

  with $\varepsilon_1\ y\ \varepsilon_2$ being 15-digit prime numbers each.
- Representation of the intensity levels of each pixel in terms of qubits. Each entry of the six matrices is an integer between 0 and 255, which is represented in binary and interpreted as the tensor product of 8 qubits. For example, in the case of a pixel with value 178, the following representation is obtained: $178_{10} = |10110010\rangle$.
- Evolution, based on the previous representation ($|q_7\ q_6\ q_5\ q_4\ q_3\ q_2\ q_1\ q_0\rangle$), of the entries of the six matrices (three cropped originals and three chaotic) through the application of the quantum gates SWAP, CNOT, and Toffoli. This evolution for the preceding example is presented in Table 1.

Table 1: *Sequential application of quantum gates*

Compuerta	q_7	q_6	q_5	q_4	q_3	q_2	q_1	q_0
$\lvert 10110010\rangle$	1	0	1	1	0	0	1	0
swap(q_0,q_4)	1	0	1	0	0	0	1	1
swap(q_1,q_6)	1	1	1	0	0	0	0	1
swap(q_2,q_5)	1	1	0	0	0	1	0	1
swap(q_3,q_7)	0	1	0	0	1	1	0	1
swap(q_3,q_0)	0	1	0	0	1	1	0	1
swap(q_4,q_7)	0	1	0	0	1	1	0	1
CNOT(q_0,q_1)	0	1	0	0	1	1	1	1
CNOT(q_2,q_3)	0	1	0	0	0	1	1	1
CNOT(q_4,q_5)	0	1	0	0	0	1	1	1
CNOT(q_6,q_7)	1	1	0	0	0	1	1	1
CCNOT(q_0,q_1,q_2)	1	1	0	0	0	0	1	1
CCNOT(q_0,q_1,q_3)	1	1	0	0	1	0	1	1
CCNOT(q_4,q_5,q_6)	1	1	0	0	1	0	1	1
CCNOT(q_4,q_5,q_7)	1	1	0	0	1	0	1	1

Source: *Own Elaboration.*

- Application of the XOR logic gate to each pair of matrices: R XOR Q^R, G XOR Q^G, B XOR Q^B, where R, G, B, Q^R, Q^G y Q^B are the consolidated results in the previous item.

The above process, three diffused matrices of size $(M-1)\times(N-1)$ are obtained and denoted as D^R, D^G y D^B.

3.2. Confusion Phase

To permute the entries of the matrices D^R, D^G y D^B the following procedure is carried out:

- Iteration of the hybrid system defined in (1), $3 \times (N-1)$ times, achieving a chaotic sequence $\{x_i\}$ with i ranging from 1 to $3 \times (N-1)$.
- Application of the T-transformation, taken from [8] and defined in (6) on the sequence $\{x_i\}$, to obtain a S matrix, with size $3 \times (N-1)$.

$$T(x_i) = mod(round(abs(x_i) - floor(abs(x_i) \times 10^{14})), 256) \qquad (6)$$

- Permutation of matrices D^R, D^G y D^B using the rows of the S matrix: S_1, S_2 y S_3, respectively. his process is carried out through circular rotations of each column as follows: the value at entry j of S_1 (S_{1j}) determines the rotation of column j in the D^R matrix, whose magnitude k is given by (7).

  $$k = mod(S_{1,j}, N-1) \qquad (7)$$

  Similarly, the entries in rows S_2 and S_3 are used to rotate the columns D^G y D^B, respectively, in a circular way.

- Transpose the three matrices permuted in the previous step, to apply the same mechanism again to their columns and finally transpose the resulting matrices again, obtaining three matrices $D_p^R, D_p^G \ y \ D_p^B$ of size $(M-1) \times (N-1)$.
- Joining of the first row and column, cropped at the beginning of the diffusion phase of the original matrices, on the corresponding $D_p^R, D_p^G \ y \ D_p^B$.
- Recompositing into a RGB image from the three matrices generated in the previous item, resulting in the encrypted image.

Since quantum operators and other applied operations are reversible, the decryption process is carried out by performing the same steps in reverse order. Fig. 6 shows the test images obtained from USC-SIPI Image Database [28] and the results of applying the proposed encryption/decryption algorithm.

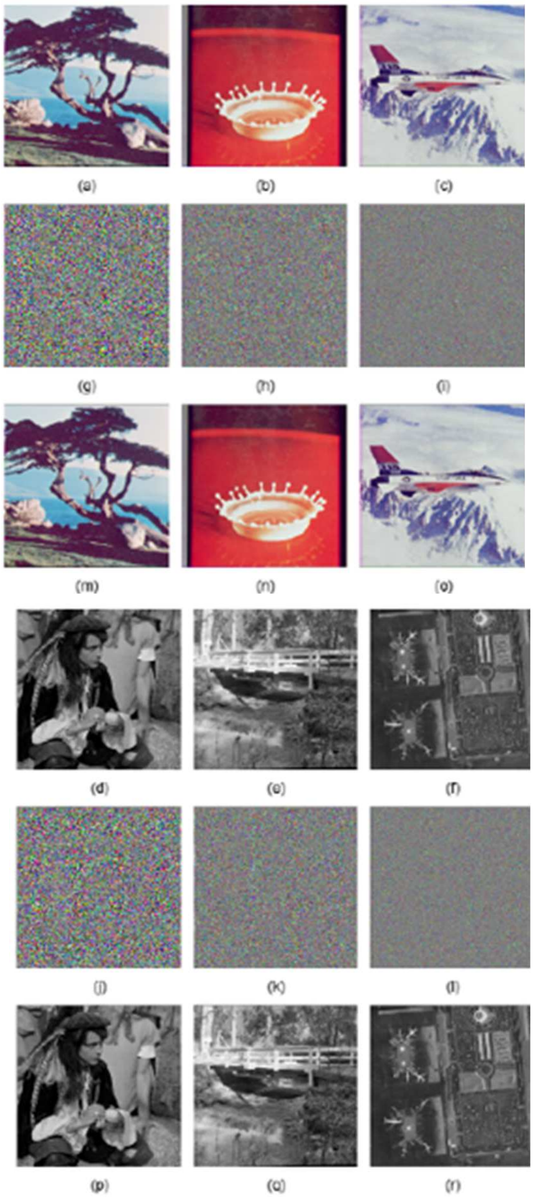


Fig. 6. *Original encrypted, and decrypted images.*
Source: *[29]*

4. RESULTS

In order to validate the effectiveness and efficiency of the proposed model, safety and performance tests were carried out, which are presented in this section.

4.1. Differential Analysis

This test compares the results of encrypting two images that differ only in the value of one pixel, expecting these results to show remarkable differences, which are measured using the Number of Pixels Change Rate (NPCR) and Unified Average

Changing Intensity (UACI) indicators. Based on the two encrypted images, the first compares and indicates the percentage of pixels in which they differ, while the second shows the average difference in pixel intensity. The mathematical expressions for their calculation are given by (8), (9) y (10) valid for images of size $M \times N$, where C_1 y C_2 are the two resulting encryptions.

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \tag{8}$$

$$D(i,j) = \begin{cases} 1, & if\ C_1(i,j) \neq C_2(i,j) \\ 0, & if\ C_1(i,j) = C_2(i,j) \end{cases} \tag{9}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{10}$$

According to the related scientific literature, the ideal values for NPCR and UACI are approximately 99.61% and 33.51%, respectively; values close to these optima are considered indicative of high resistance to differential attacks. Table 2 shows the results obtained with some of them, as well as a comparison with the work of [10].

***Table 2:** NPCR and UACI values*

Imagen	NPCR (%)			UACI (%)		
	R	G	B	R	G	B
Splash	99.2073	99.1935	99.2053	33.2634	33.3185	33.3197
Splash[1]	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
Airplane[1]	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
Male[1]		99.6586			33.6368	
Airport	99.4186	99.4084	99.4131	33.4000	33.3790	33.3675
Airport[1]		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

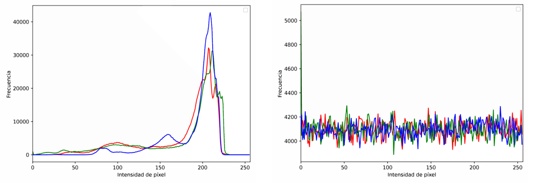
***Source**: Adapted from[29], [1] Results reported in [10].*

4.2. Statistical Analysis

The purpose of this test is to determine the robustness of a cryptographic system against potential threats or vulnerabilities to private information. To this end, histograms, diagrams and correlation coefficients are considered, as well as variance and entropy values, for both original and encrypted images.

Since the proposed model is applicable to both color and grayscale images, two illustrations are presented below, one for each scenario: Airplane (color) and Airport (grayscale) images.

Fig. 7 shows the frequency histograms for the original and encrypted Airplane (color) images, respectively, demonstrating that, when the image is encrypted, the frequency histograms are highly uniform, contrary to that of the original image.



(a) *(b)*

***Fig.** 7. Histograms for the AirPlane image original (a) and encrypted (b). **Source:** Own Elaboration.*

Continuing with the analysis of the Airplane image, Figs. 8 and 9 show the correlation for each layer in the horizontal, vertical, and diagonal directions for the original and encrypted images, respectively, highlighting in Fig. 9 the loss of correlation between adjacent pixels.

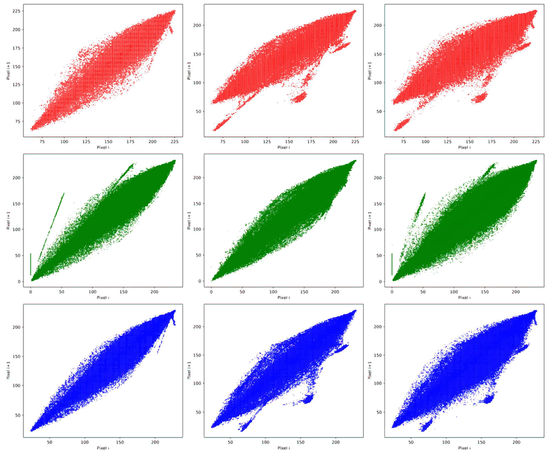


***Fig. 8.** Layer correlation of the original Airplane image. **Source:** Own Elaboration.*

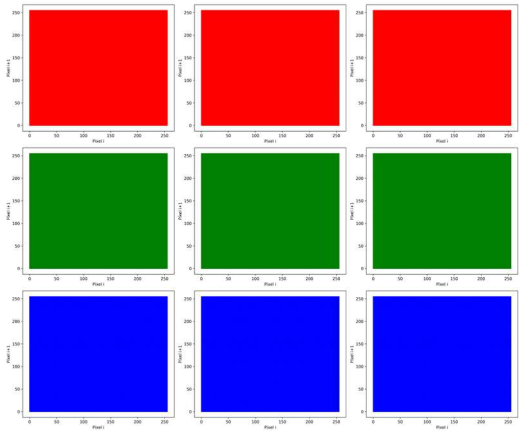
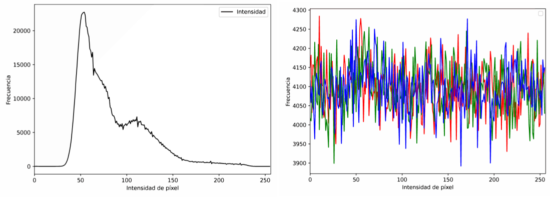


***Fig. 9.** Layer correlation of the encrypted Airplane image. **Source:** Own Elaboration.*

Fig.10 shows the frequency histograms for the original and encrypted Airport images, respectively.

It should be noted that although the original image is in grayscale, this algorithm encrypts in RGB scale, which is evident in the histogram of the encrypted image is also characterized by high uniformity. Although the amount of data is increased in this case, this is offset by the gain in terms of security, since, on the one hand, there is a complete loss of the original visual semantics and, on the other hand, the application of inverse reconstruction and statistical attacks is hindered, as the attacker loses fundamental structural information due to the reduction in inter-channel correlation.



(a) *(b)*

Fig. 10. *Histograms for the Airport image original (a) and encrypted (b).* ***Source:*** *Own Elaboration.*

Additionally, Figs. 11 and 12 show the correlation diagrams of adjacent pixels, corresponding to the original and encrypted Airport images, respectively.

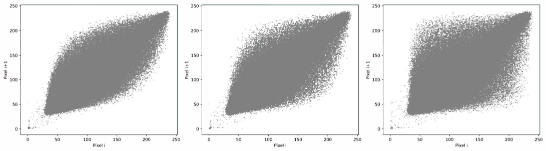


Fig. 11. *Correlation diagram original grayscale image of the airport.* ***Source:*** *Own Elaboration.*

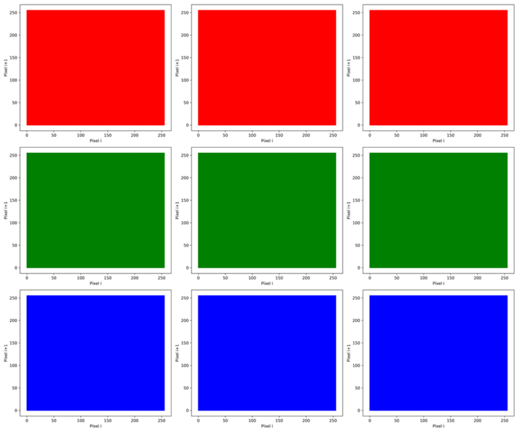


Fig. 12. *Correlation diagram of encrypted Airport image.* ***Source:*** *Own Elaboration*

In line with the above, Tables 3 and 4 show the correlation values obtained for both the original images and the encryption results. As expected, the encrypted images exhibit values close to zero.

Table 3: *Color Image correlation coefficient (Airplane) Original and Encrypted*

	Airplane								
Imagen	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

Source: *Own Elaboration.*

Table 4: *Correlation coefficient for original and encrypted grayscale images (Airport)*

	Airport								
Imagen	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

Source: *Own Elaboration.*

The variance values for the original and encrypted images are presented in Tables 5 and 6, which show the degree of dispersion of the data with respect to the mean. in the case of encrypted images, lower variance values are desired, indicating that the pixels are arranged around the mean and have little variation. For the case study, these values were significantly reduced and were comparable to those reported in [10].

Table 5: *Color image variance (Airplane) original and encrypted*

Imagen	Plane Imagen			Encrypted Imagen		
	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

Source: *Own Elaboration.*

Table 6: *Gray scale image variance (Airport) original and encrypted*

Imagen	Plane Imagen	Encrypted Imagen		
		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	

Source: *Own Elaboration.*

The entropy values for the original images Airplane and Airport were 6,66508 and 6,83033, respectively. The encrypted images were close to 8, as shown in Table 7, indicating a high degree of disorder in the encrypted information. It should be noted that these values are comparable to the results reported in the articles 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] and A Novel Hybrid Secure Image Encryption Based on Julia Set of Fractals and 3D Lorenz Chaotic Map [30].

***Table 7:** Entropy values encrypted images*

Image	This Work	[9]	[10]	[30]
Airplane	7,99992	7,9977	7,9987	7,9998
Airport	7,99994	----	----	----

***Source:** Own Elaboration.*

4.3. Key Security Analysis

Since the keys of the proposed system are based on chaotic attractors sensitive to small perturbations, when an insignificant change is introduced in a component of the key, it is impossible to recover the original information, situation shown in Fig. 13.

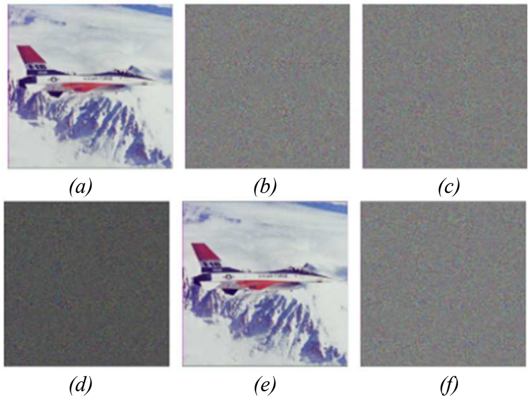


***Fig. 13.** Key sensitivity.*
***Source:**[29].*

Using key K1 to encrypt the Airplane image (Fig. 13a) we obtain Fig. 13b. By altering one component of K1 by 0.01 we obtain key K2 and with it the encrypted image in Fig. 13c. Although these results appear identical to the human eye, the image in Fig. 13d shows the absolute values of the difference between the two, demonstrating that the results in Fig. 13b and 13c are different. When attempting to decrypt image b in Fig. 13 with key K1, the original Airplane image is obtained (Fig. 13e), whereas if K2 is used to decrypt it, recovery becomes impossible, as shown in Fig. 13f, which is desirable in a cryptographic process.

On the other hand, with regard to the size of the key space, the following values were considered:

- Parameters β and r of the logistic system, with a precision of 3 decimal places for a total of $(10^3)^2$ possible values.
- Initial conditions (x_0, y_0, z_0) of the logistic system, with 3 decimal places of precision, obtaining $(10^3)^3$ possible values.
- Quantum logistics system diffusion keys with 3 integers digits resulting in $(10^3)^3$ possible values.
- Two prime numbers with 15 digits resulting in $(10^{15})^2$ possibilities.
- Parameter r and initial condition x_0, of the tent logistic system, with 3 decimal places of precision with a total of $(10^3)^2$ possible values.

Therefore, the size of the key space is 10^{60} which significantly exceeds several of the results reported in the literature consulted, such the works of Man et al [31], Kamal et al [32] and Ahmed et al [33] for which the reported key spaces were 10^{29}, 10^{35} y 10^{38}, respectively.

It should be emphasized that the National Institute of Standards and Technology (NIST) [34] has established criteria to assess whether a cryptographic algorithm is resistant to quantum attacks, including semantic security and resistance to adaptive attacks. The model presented herein is robust with respect to these criteria, since the generated keys are highly sensitive to small perturbations due to the use of chaotic dynamical systems. For this reason, it may be asserted that the algorithm is resistant to Grover-type search attacks [35], [19], as such an attack would reduce the computational complexity to $O(10^{30})$, which is still large.

4.4. Robustness Analysis

To validate the effectiveness of the proposed model, several robustness tests were carried out, which are presented below.

4.4.1. Robustness with plane images

This type of analysis consists of encrypting single-color images, usually black or white, or patterns generated with these two colors, and verifying that the model is capable of decrypting them properly. In this case, images a, b, and c in Fig. 14 were encrypted, obtaining the results shown in Figs 14d, 14e, and 14f, respectively, to which the decryption process was applied, obtaining the original images g, h, and i.

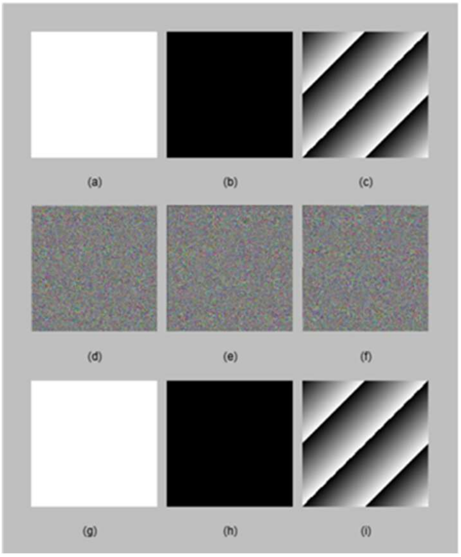


Fig. 14. *Robustness with plane images.*
Source:*[29].*

4.4.2. Salt and Pepper Test

Starting with an encrypted image, which is the result of applying the proposed algorithm, a proportion of pixels was randomly replaced, turning them into white or black, and then the decryption process is applied. The purpose of this test is to recover the original image with a high degree of fidelity. In this case, the color image "Airplane" was taken as a reference, and 1%, 5%, and 10% of the pixels in the encrypted image were modified (Fig. 15a, 15b, and 15c, respectively). The decryption algorithm was then applied, successfully recovering the original image with minimal distortion visible to the human eye (Fig. 15d, 15e, and 15f).

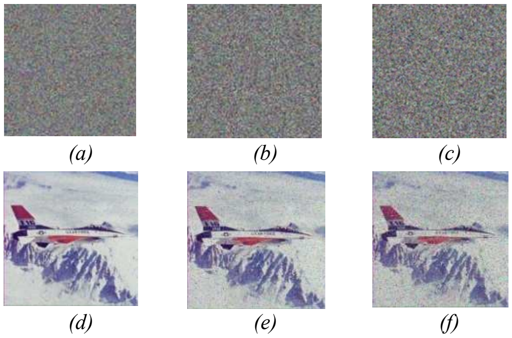


Fig. 15*. Salt and pepper test, color image.*
Source: *Own Elaboration.*

In order to obtain a more accurate measurement of the results found in this test, the mean square error (MSE) and peak signal-to-noise ratio (PSNR) metrics were calculated to evaluate the degree of similarity between the decrypted images (after applying the salt and pepper test) and the original, based on the same change proportions applied to the encrypted image. Results are presented in Table 8.

Table 8**:** *Mean Square Error and Maximum Signal-To-Noise Ratio for The Airplane Image*

Noise ratio	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

Source*: Own Elaboration.*

In this case, a high MSE value indicates loss of information, which is evident in Table 8 when a noise ratio of 5% or 10% is applied. Similarly, a PSNR greater than 40 indicates that the original image is very similar to the decrypted image after applying the salt and pepper test, which was evident when the noise ratio was 1%. However, higher noise ratios showed some differences between the images.

Similarly, the grayscale image "Airport" was taken using the same procedure as for "Airplane," thus obtaining consistent results to the human eye, as shown in Table 9 and Fig. 16.

Table 9: *Mean square error and maximum signal-to-noise ratio for the Airport image*

Noise ratio	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

Source*: Own Elaboration.*

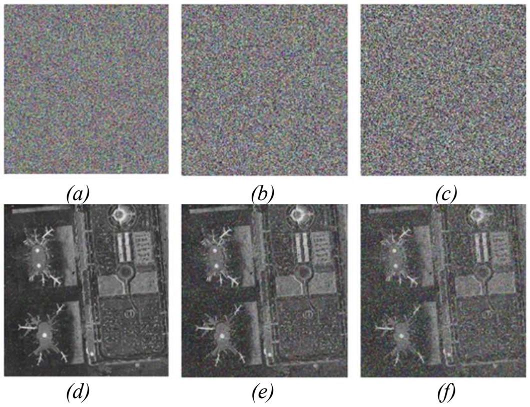
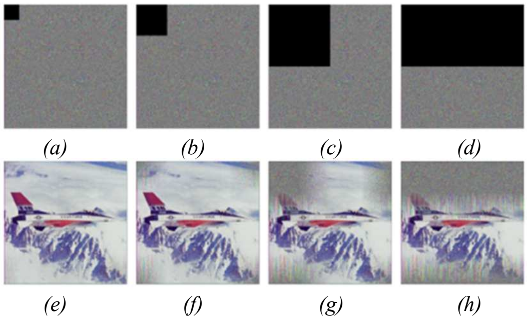


Fig. 16*. Salt and pepper test, gray image.*
Source: *Own Elaboration.*

4.4.3. *Occlusion* Test

This test consists of taking an encrypted image, cropping a rectangular portion of it to replace it with black pixels, and then, after modifying it, decrypting it. The purpose of this test is to verify how efficient the algorithm is at recovering the original image even after losing a portion of the encrypted information.

For the case study, several tests were performed with the encryption of the Airplane image, cropping 1/16, 1/8, 1/4, and 1/2 as shown in Fig. 17 (a, b, c, and d). It should be noted that in the four modifications, a large part of the original image was recovered, which is consistent with expectations and shown in Fig. 17 (e, f, g, and h).


(a) *(b)* *(c)* *(d)*

(e) *(f)* *(g)* *(h)*

***Fig. 17**. Occlusion attacks on the Airplane image.*
***Source:**[29].*

Based on the applied security and performance tests, it can be stated that the model presented herein is resistant to chosen-plaintext attacks (CPA) and ciphertext-only attacks (COA), as the robustness analysis demonstrates the absence of visual patterns. Furthermore, the correlation between adjacent pixels is minimal, and the key is highly sensitive to small perturbations; that is, a slight change in the original image results in global changes in the encrypted image, thereby demonstrating resistance to linear attacks. Likewise, the results of entropy, correlation, NPCR, UACI, and histogram analyses are consistent with ideal security-related behaviors, indicating resistance to differential attacks.

5. CONCLUSIONS

A new encryption algorithm, quantum-inspired, was proposed by integrating principles of quantum mechanics, chaos theory, and image processing, which bases its security on the high randomness of chaotic sequences and the physical principle of qbit superposition.

In the case of grayscale images, the proposed algorithm generates encryption in RGB format, which helps reduce the possibilities of fraudulent access to the original image, a desirable situation, particularly in the case of medical images.

Furthermore, the algorithm was implemented using a classical computer and subjected to tests of security and performance analysis, differential and statistical attacks, key security, and robustness, the results of which led to the conclusion that it is highly secure, therefore could be applied in real-world contexts.

Finally, it is important to note that the emergence of quantum computing poses challenges and threats to information security, making it imperative to continue the search for new cryptographic algorithms that enable a secure transition to the post-quantum era, with the aim of protecting political, economic, military, scientific, and social information.

ACKNOWLEDGMENTS

The authors are grateful to the Universidad Distrital Francisco José de Caldas for its institutional support during the course of this research.

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.