ISSN: 1692-7257 - Volume 1 – Issue 47 - 2026

ORIGINAL

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Image encryption using chaos and quantum gates

Encriptación de imágenes usando caos y compuertas cuánticas

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.**

Received: 29 agosto 2025. Revised: 29 octubre 2025. Accepted: 18 diciembre 2025. Published: 30 enero 2026.
Corresponding Author: Luz Deicy Alvarado Nieto

How to cite: 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

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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.

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.

1. INTRODUCTION

Cryptography is responsible for proposing strategies for the protection of private information. In recent decades, new developments based on principles of mathematics and artificial intelligence have emerged, seeking to respond to the 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-scale information, since high levels of redundancy arise in the information and their security is based on the problem of decomposing an integer into its prime factors, which is considered an NP (Non-deterministic Polynomial time) problem. With the emergence of quantum computers, the solution time for this problem can be significantly reduced and may even become logarithmic, which would generate a worldwide security catastrophe, a fact that has driven research by the academic and scientific community, giving rise to significant work in this direction.

Quantum computing has created challenges for securing information, which is why proposals aimed at preparing the transition to this new scenario have emerged, so the National Institute of Standards and Technology (NIST) has taken on the task of establishing security standards for the post-quantum era[1],[2].

To date, proposals for image representation in the quantum context have been developed; one of them is found in the work of Zhang, Gao and Wang [3], which is still valid and has even had improvement proposals as presented by Wang and colleagues [4], being used in the proposal of Wang, Rang and Ding [5] as well as in that of Hu, Li and Di [6], to propose a grayscale image encryption model through quantum gates, rotation operations similar to the operation of the Rubik's cube and a two-dimensional chaotic system generated from the one-dimensional logistic and sine systems. In the same direction, the work proposed in the article A novel image encryption scheme based on quantum dynamical spinning and rotations [7] stands out, whose authors propose an RGB image encryption algorithm using rotation matrices and half-spin particle representation.

On the other hand, the use of chaotic dynamical systems in the field of cryptography has evolved to apply such systems in the quantum environment, so it is common to find quantum circuits alluding to these systems, as is the case of the work proposed by Gao and colleagues[8], who propose a new algorithm for encryption of quantum images represented by the NEQR model, also using the two-dimensional chaotic Arnold cat attractors and the hyperchaotic Lorenz system, with their corresponding implementations of the quantum circuits.

Additionally, 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 dynamical systems and quantum gates.

Given the progress in quantum computing and its implications for the protection of digital information, this article presents a color digital image encryption model inspired by the quantum domain, which uses classical and quantum chaotic dynamical systems as well as quantum gates, is executed on classical hardware, and is validated through security and performance metrics. The results obtained allow inferring that this model can be applied in real environments. It is worth highlighting that it also works for grayscale images, giving rise to an encrypted result in RGB scale, which constitutes a strategic cryptographic advantage since it favors the emergence of more complex dynamics, increasing the structural security of the model. The following sections address the topics: theoretical framework, methodology used, detailed description of the algorithm, application of performance metrics and conclusions.

2. MATERIALS AND METHODS

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

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

2.1. Background Knowledge

The conceptual foundations that were taken into account for the formulation of the model presented here are addressed below.

2.1.1. Classical and quantum chaotic attractors

A dynamical system is characterized by evolving according to a deterministic rule of a continuous or discrete type; if such evolution is sensitive to small perturbations, reference is made to the concept of chaos. Specifically, a system is considered chaotic if it satisfies three conditions, namely: sensitivity to perturbations, transitivity and density of periodic points[11].

The concept of chaos was evidenced by the meteorologist Edward Lorenz [12] in an experiment that gave rise to what was later called the "butterfly effect" and which is currently a significant reference for scholars of complex nonlinear phenomena,

noting that numerous behaviors framed within this line exist in different areas of knowledge, such is the case of climate modeling, epidemics, the stock market, among others [13], [14], [15].

When a qualitative analysis is made of a nonlinear dynamical system framed in an environment of chaos, in order to analyze the trajectories of said system from initial conditions and parameters, it is usual for strange chaotic attractors to appear, which are characterized by high sensitivity, non-periodicity, fractal structure and non-integer dimension, properties that are useful to exploit in the context of cryptographic schemes, since this translates into obtaining pseudorandom sequences that can be used for the design of encryption algorithms.

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

It should be noted that the immersion of the principles of quantum physics in the computing scenario led to extrapolating the concept of chaos into the quantum domain, even though there are no defined trajectories there; rather, the system evolves with quantum superposition, with uncertainty arising in accordance with the Heisenberg principle and linear and unitary evolution in accordance with the Schrödinger equation[16]. In this context, quantum chaos deals with the study of its chaotic analogues, which implies analyzing structures in Hilbert space parallel to classical attractors; in other words, transitions to complex quantum dynamics are studied. One of the classical chaotic quantum attractors is the logistic one, used as input for the diffusion part of the algorithm process described in the work of Goggin, Sundaram and Milonni[17].

2.1.2. Quantum computing.

The evolution of classical computers with respect to their size and speed is reaching its limit; it is almost impossible to create integrated circuits with a larger number of components while preserving or trying to reduce their size. As a result, supercomputing platforms, used especially to run artificial intelligence models, are composed of enormous quantities of very powerful computers that occupy entire buildings intended solely to house them. In turn, 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, and it is there that quantum computing emerges, from which promising results are expected.

The work Simulating Physics with Computers[18]can be considered as the starting point of quantum computing; in it, Richard Feynman conceived the idea of developing quantum computers to simulate systems involving nanoparticles. To date, significant advances have been made in the development of this type of computer, giving way to new scientific challenges[19].

In contrast to classical computing, whose minimum unit of information is the bit, within the quantum system this unit corresponds to the qubit, which can assume the states zero, one or both (superposition) and thus be combined with other qubits, 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 between a vertical line and an angle as a bracket, called a ket: $|0\rangle$, $|1\rangle$. Thus the basic states are called ket zero and ket one respectively, and are represented as the north and south poles on a sphere of radius 1 called the "Bloch sphere" (see figure 1). Likewise, entanglement allows qubits to be manipulated in such a way that their behavior is synchronized, achieving exponential growth in parallel operations with respect to the number of qubits the computer works with[20]. Fig. 1 represents the Bloch sphere, where several of the possible states for a qubit are shown.

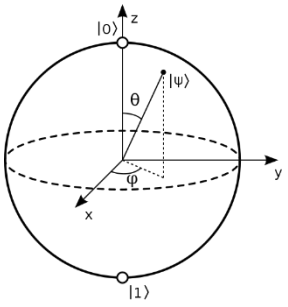


Fig. 1. *Bloch sphere with several possible states for a qubit.*
Source: PNGWING [21].

To perform operations with these qubits, several gates that act on them have been defined, in a manner similar to how logic gates allow operations to be developed and circuits to be created with traditional bits. Note that the basic states of a qubit can also be represented in a vector of size2×1; thus $|0\rangle$can be represented as$\binom{1}{0}$and $|1\rangle$ as$\binom{0}{1}$. In this way, when logic gates that require more than one qubit are to be applied, the 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 the aforementioned gates.

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

2.1.2.1. Compuerta CNOT

Also called the controlled NOT gate, it acts on 2 qubits, changing the second of them if the first (control qubit) is in state 1; that is, if it is applied to |00⟩ o |01⟩,there will be no change, however, if it is applied to |10⟩the result will be |11⟩and if it is applied to |11⟩, the result obtained is |10⟩ [22]. The matrix representation of this gate is shown in (2)[10],[23].

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

The graphical representation of this gate as a circuit shows its two inputs, the symbol⊕that acts on the two qubits and the result obtained, which is presented in Fig. 2.

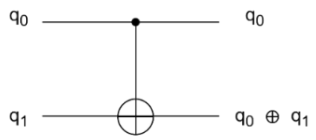


Fig. 2. *Compuerta CNOT.*
Source: Adapted from [23] and [24].

2.1.2.1. Toffoli gate

Also known as a controlled CNOT gate, in this case it acts on 3 qubits, the first two play the control role and the third is the target. If the first two qubits are at 1, the value of the third changes; otherwise, it remains the same, that is, if the input qubits are |000⟩, |001⟩, |010⟩, |011⟩, |100⟩, |101⟩, there will be no change while if the gate is applied to the qbits |110⟩ o |111⟩ one obtains |111⟩ y |110⟩, respectively[24]. The matrix corresponding to this gate is presented in(3).

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

As with the compuerta CNOT, for Toffoli its circuit shows the 3 inputs, the XOR symbol acting on the three qubits and the result generated on the last one, as shown in Fig. 3.

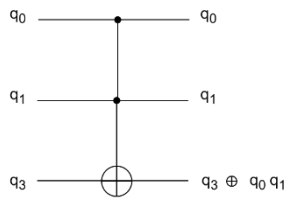


Fig. 3. *Toffoli gate.*
Source: Adapted from [20] and [24].

2.1.2.3. compuerta SWAP

It is applied to 2 qubits by swapping their values, that is, if the input is |10⟩, the output will be |01⟩ and vice versa. If the 2 qubits have the same value, they are preserved as they are[24]. The matrix corresponding to this gate is presented in(4).

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

Similarly to the two previous gates, this one has its representation as a circuit as shown in Fig. 4.

2.1.3. Cryptography

Given the need to preserve the security and integrity of private information, cryptography has been present throughout human evolution, becoming increasingly significant due to the growth in the amount of digital information circulating through public

channels. The aim of cryptography is to transform information by means of encoding into an unreadable result in order to mask it from intruders; there are two types: symmetric (same key to encrypt and decrypt), as is the case of DES (Data Encryption Standard), and asymmetric (one key to encrypt and another to decrypt), as with RSA (Rivest, Shamir Adleman). Conventional methods are not appropriate when facing large volumes of image or multimedia data, because redundancy occurs; this is how new proposals arise based, among others, on elliptic curve theory, cellular automata, neural networks or chaos.

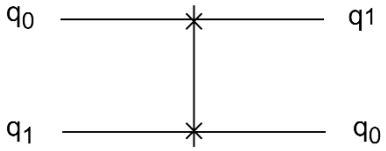


Fig. 4. *Compuerta Swap.*
Source: Adapted from [20] and [24].

Thanks to the potential of the properties inherent to chaotic systems, cryptographic algorithms based on them have gained academic interest since the end of the XX century; proof of this is the emergence of a line of research called chaotic cryptography, linking academics interested in making collective efforts and exchanging knowledge to formulate security schemes. In this direction, proposals for cryptography based on chaos theory have increased significantly, all due to the similarity between the properties of a system that exhibits chaos and those required in a cryptographic algorithm. The sensitivity to initial conditions and unpredictability present in a chaotic system mean 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 manages to access an encrypted message, they cannot predict what the next one will be like. On the other hand, the complexity of the chaotic system, in the context of encryption, means that there is greater difficulty when attempting to decrypt the message fraudulently.

For the above reasons, cryptography has contributed to the study and formulation of new chaotic systems, mostly based on existing ones, by

by combining them or extending them to a higher-dimensional space, always bearing in mind the need to increase the level of complexity and thus guarantee greater security for cryptographic models that use ciphering sequences, as is the case of the work proposed by Mohamed and colleagues[10]. Likewise, the aim is to correct deficiencies and consolidate foundations to continue advancing in the field of chaotic cryptography, without losing sight of the fact that, despite new developments in the subject, it faces threats from quantum computing[1],[2],[25],[26],[27], which makes it necessary to continue exploring new ground in search of contributing solutions in cybersecurity.

2.2. Methodology

The process followed to consolidate the algorithm proposed in this work used a mixed approach that addressed both qualitative and quantitative aspects. In the first case, with the aim of ensuring high randomness in the pseudorandom sequences used, and in the second, to validate the performance of the proposed algorithm and make the corresponding adjustments in order to avoid undesired values in the metrics applied, comparing performance in parallel with current scientific benchmarks.

It is worth highlighting that the algorithm, like most cryptographic systems, involved diffusion and confusion phases, in which principles of quantum computing 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.

3. DESCRIPTION OF THE ALGORITHM

Starting from an image of size M×N in RGB scale, each of the layers was subjected to the diffusion and confusion processes as detailed below:

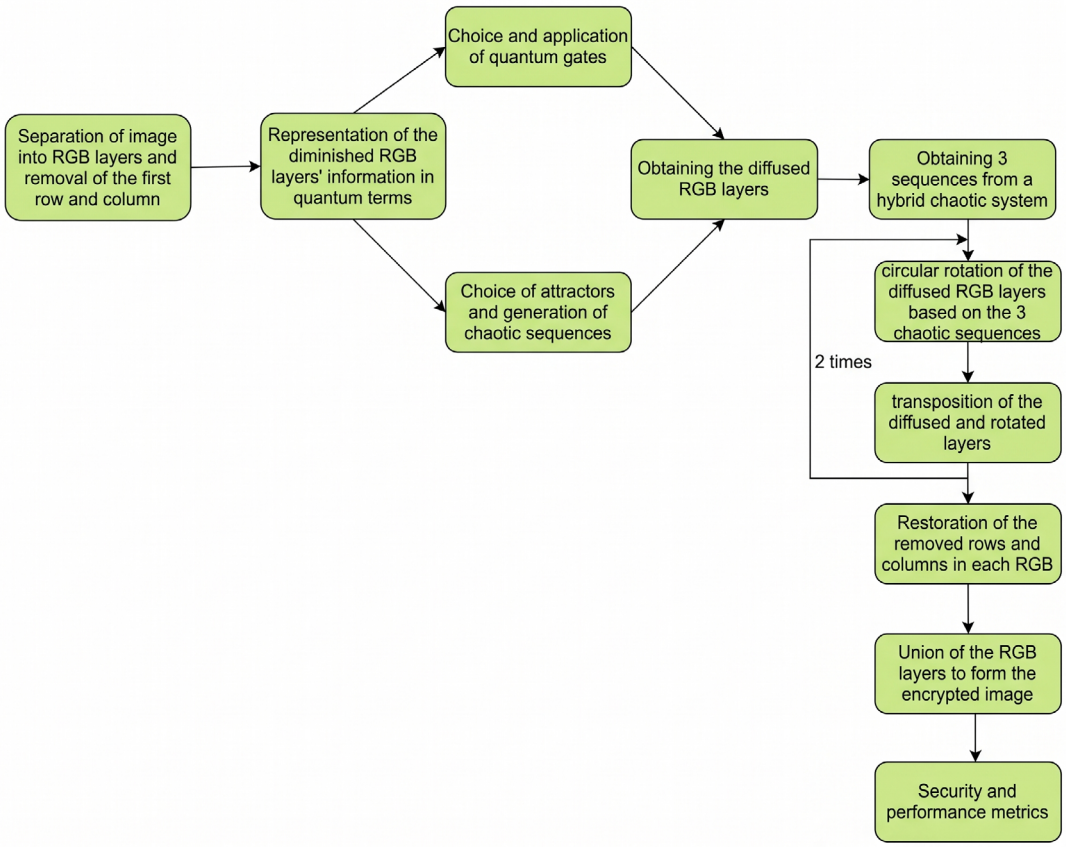


Fig. 5. *Phases of the encryption algorithm.*
Source: Own elaboration.

3.1. Diffusion Phase

Since the information provided by a single pixel in an image is negligible, especially at the edges, removing the pixels of the first or last row or column does not imply significant visual changes; if the rest of the image is encrypted and the omitted row and column are added to this result, this strategy can generate confusion for 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 presented here. This and the other processes carried out in the diffusion phase are described below.

- Separation of the RGB layers and cropping of 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 average value P of the pixels of that selected row or column.
- Iteration of the quantum logistic hyperchaotic system with the initial values x0 = 0.043, y0 = 0.035, z0 = 0.025, β = 6.859, r = 3.990, P times (taking only the integer part of P), which are ignored to guarantee greater randomness.
- Continuation of the previous iteration process$(M-1)\times(N-1)$times, generating 3 chaotic sequences {xi}, {yi}, {zi}.
- Obtaining three chaotic matrices denotedQ_i^R, Q_i^G, Q_i^B, by means of the transformations taken from[10]and defined in(5):

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

Whereε_(1) y ε_(2)are two prime numbers of 15 digits each.

- Representation of the intensity levels of each pixel in terms of qubits. Each entry of the 6 matrices is an integer between 0 and 255, which is represented in binary and viewed as the tensor product of 8 qubits. For example, for the pixel with value 178, we have: 17810 = $|10110010\rangle$.
- Evolution, based on the previous representation ($|q7\ q6\ q5\ q4\ q3\ q2\ q1\ q0\rangle$), of the entries in the 6 matrices (3 original cropped and 3 chaotic) by means of the SWAP, CNOT and Toffoli quantum gates. This evolution for the previous example is shown in Table 1
- Application of the XOR logic gate to each pair of matrices as follows: R XOR QR, G XOR QG, B XOR QB, where R, G, B, QR, QG and QB are the results consolidated in the previous item.

From the above process, 3 diffused matrices of size$(M-1)\times(N-1)$are obtained, denoted as DR, DG and DB.

Table 1: Sequential application of the quantum gates

Gate	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

Source: Own elaboration

3.2. Confusion Phase

To permute the entries of matrices DR, DG and DB, the following procedure is carried out:

- Iteration of the hybrid system defined in(1),3×(N−1)times, obtaining a chaotic sequence {xi} with i ranging from 1 to3×(N−1).
- Application of the transformation T, taken from[8]and defined in (6) over the sequence {xi}, to obtain an S matrix, of size3×(N−1).

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

(6)

- Permutation of matrices DR, DG and DB using the rows of matrix S: S1, S2 and S3, respectively. This process is carried out through circular rotations of each column as follows: the value at entry j of S1 (S1j) determines the rotation of column j in matrix DR, whose magnitude k is given by(7).

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

(7)

Similarly, the entries of rows S2 and S3 are used to circularly rotate the columns of DG and DB, respectively.

- Transposition of the three matrices permuted in the previous step, so that the same mechanism can be applied again to their columns and the resulting matrices then transposed again, yielding three matricesD_(p)^(R),D_(p)^(G) y D_(p)^(B) of size(M−1)×(N−1).
- Adhesion of the first row and column, trimmed at the beginning of the diffusion phase of the original matrices, onto the correspondingD_(p)^(R),D_(p)^(G) y D_(p)^(B).
- Recomposition into an RGB image from the three matrices generated in the previous item, resulting in the encrypted image.

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

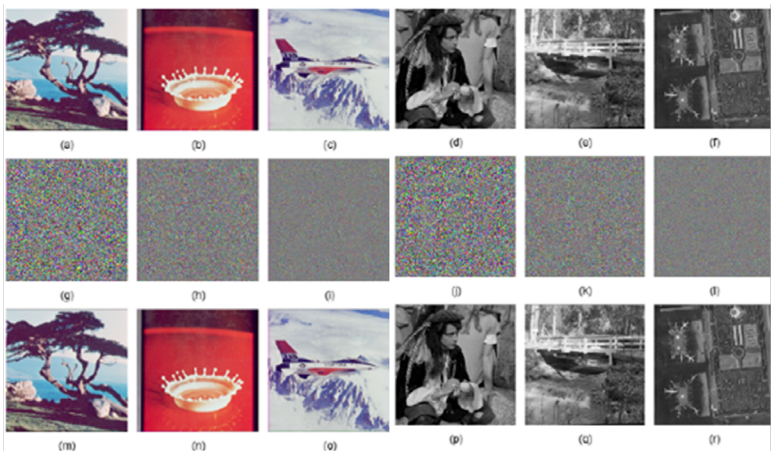


Fig. 6. *Original, encrypted and decrypted images.*
Source: [29].

4. RESULTS

To validate the effectiveness and efficiency of the proposed model, security and performance tests were carried out, and they 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 be noticeably different, which is measured using the NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) indicators. From the two encrypted images, the first of these 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) and (10), valid for images of size M×N, where C1 and C2 are the two resulting encryptions.

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

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

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

According to the related scientific literature, the ideal values for NPCR and UACI are approximately 99.61% and 33.51%, respectively, and values close to these optima are considered to indicate high resistance to differential attacks. In this case they were applied to several images; Table 2 presents the results obtained with some of them, along with the comparison with the work of[10].

Table 2: NPCR and UACI values

Image	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

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

This test is used to determine the robustness of a cryptographic system against possible threats or vulnerabilities of private information. To this end, histograms, diagrams and correlation coefficients are taken into account, as well as variance and entropy values, for both original and encrypted images.

4.2. Statistical Analysis

Since the proposed model can be applied 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 the encrypted Airplane (color) image, respectively, showing that, when the image is encrypted, the frequency histograms are highly uniform, contrary to what happens with the original image.

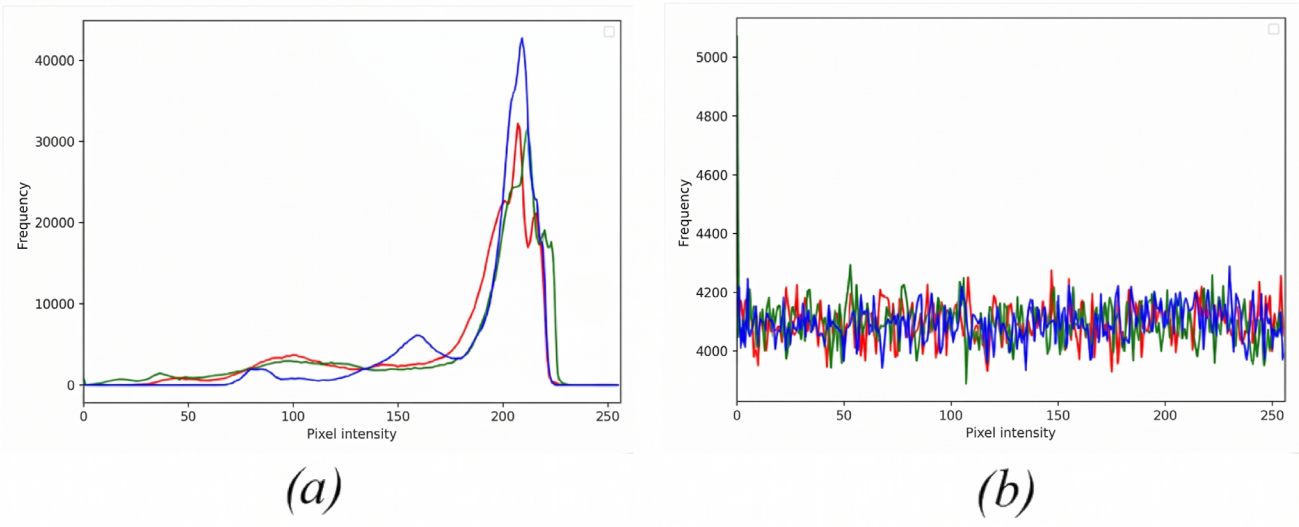


Fig. 7. *Histograms for the original (a) and encrypted (b) AirPlane image.*
Source: Own elaboration.

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 the encrypted image, respectively, with Fig. 9 highlighting the loss of correlation between adjacent pixels.

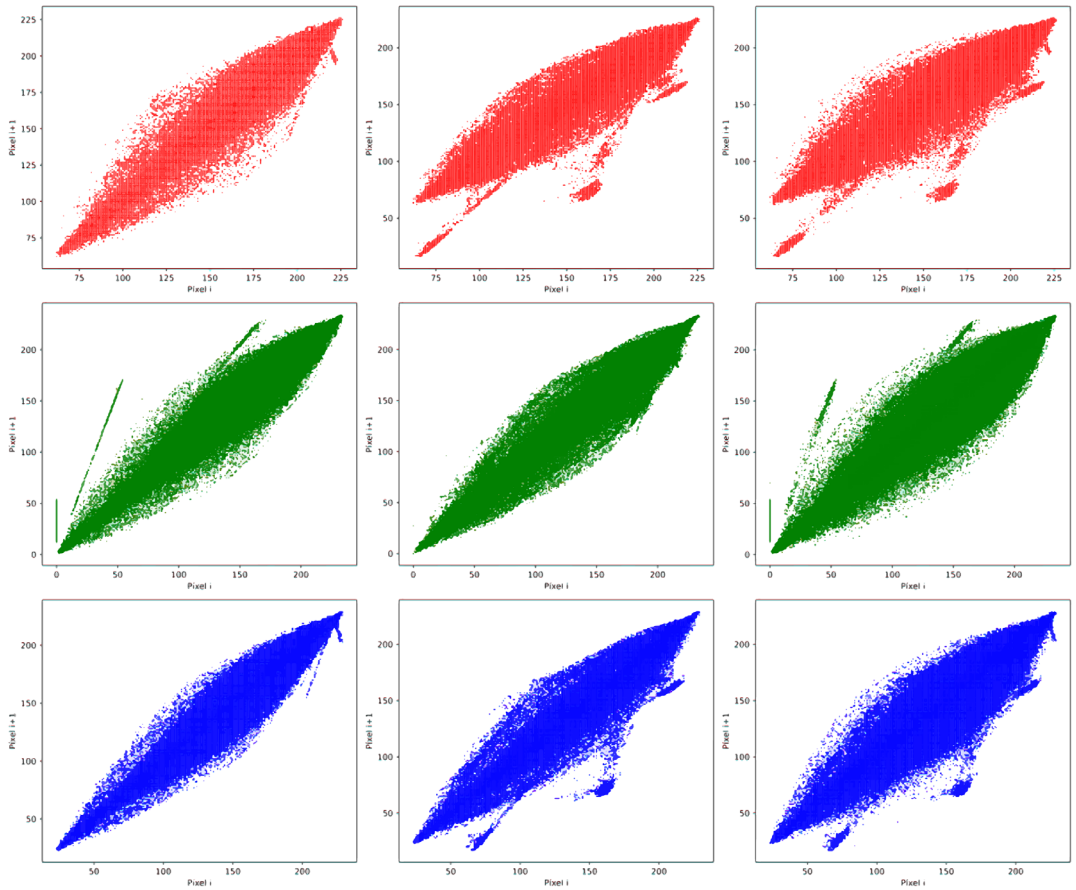


Fig. 8. *Correlation by layers of the original Airplane image.*
Source: Own elaboration

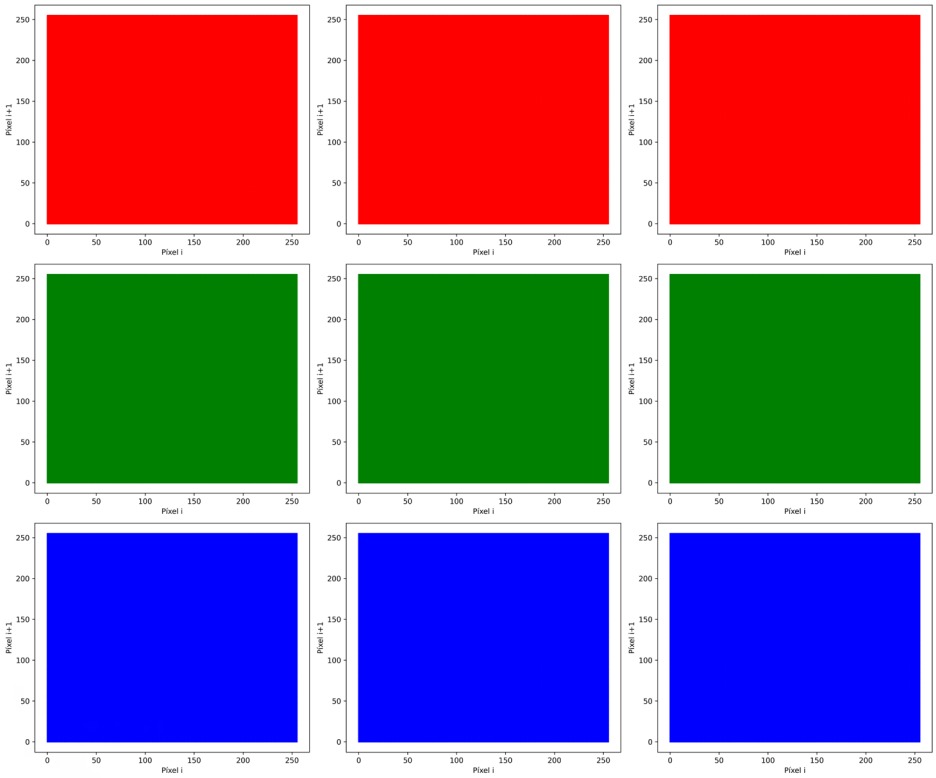


Fig. 9. *Correlation by layers of the encrypted Airplane image.*
Source: Own elaboration

Fig. 10 corresponds to the frequency histograms for the original and encrypted Airport image, respectively, highlighting that this algorithm encrypts grayscale images in formato RGB, which is evidenced in the histogram of the encrypted image, also characterized by high uniformity. Although in this case the amount of data increases, this is offset by the gain in terms of security, since on the one hand a complete loss of the original visual semantics is generated and, on the other, the application of inverse reconstruction and statistical attacks is hindered, given that the attacker loses fundamental structural information due to the decrease in inter-channel correlation.

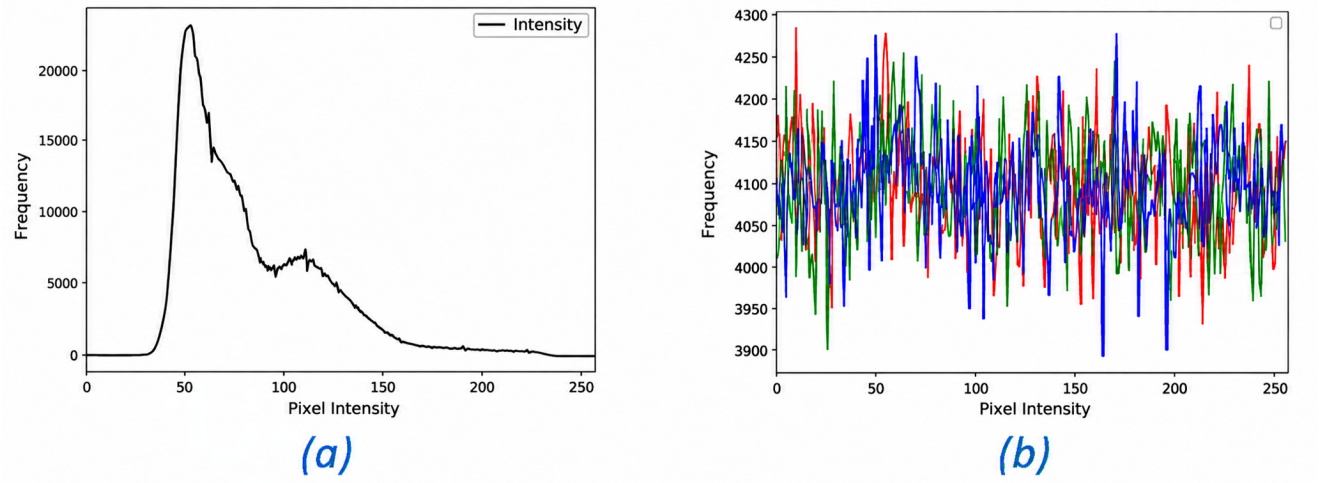


Fig. 10. *Histograms for the original (a) and encrypted (b) Airport image.*
Source: Own elaboration.

Additionally, Figs. 11 and 12 show the adjacent pixel correlation diagrams corresponding to the original and encrypted Airport image, respectively.

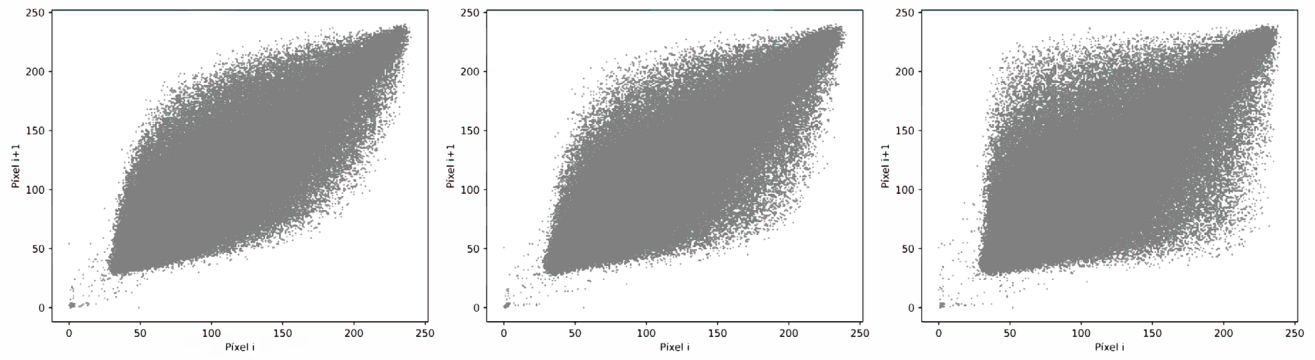
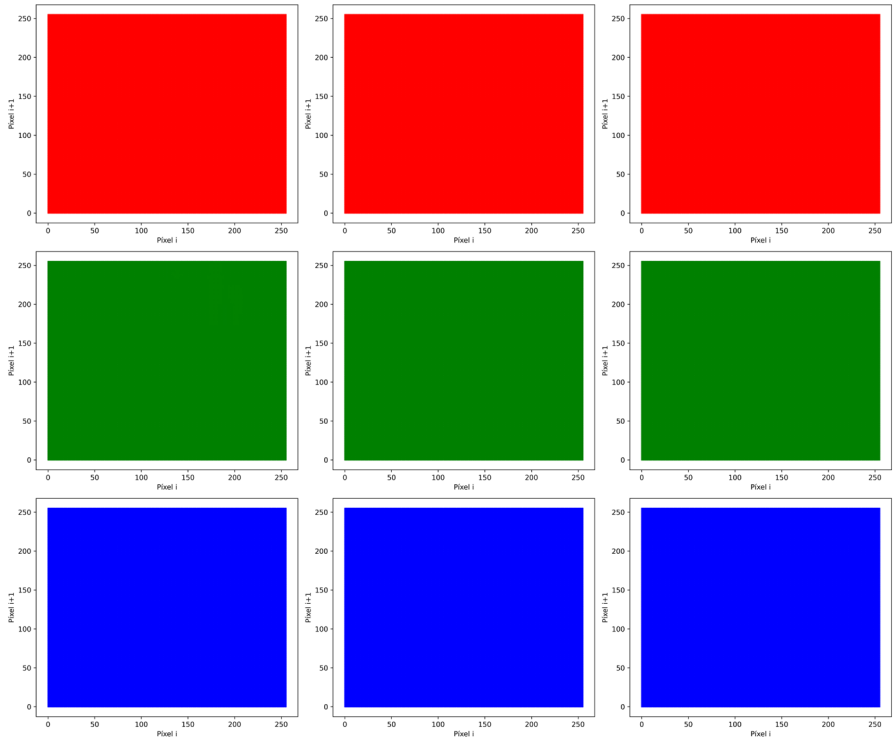


Fig. 11. *Correlation diagram of the original Airport image in grayscale.*
Source: Own elaboration.

Consistent with the above, Tables 3 and 4 present the correlation values obtained for both the original images and the encryption results; as expected, the encrypted images yield values close to zero.



Source: Own elaboration.

Table 3: Correlation coefficient of the original and encrypted color image (Airplane)

Image	Airplane								
	Horizontal			Vertical			Diagonal		
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 of the original and encrypted grayscale image (Airport)

Image	Airplane								
	Horizontal			Vertical			Diagonal		
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.

Tables 5 and 6 present the variance values for the original and encrypted image, which indicate how far the data are dispersed from the mean. For encrypted images, lower variance values are desirable, since they indicate that the pixels are grouped

around the mean and vary little. In the case study, these values were significantly reduced and were comparable with those reported in[10].

Table 5: Variance of the original and encrypted color image (Airplane)

Image	Original Image			Encrypted Image		
	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: Variance of the original and encrypted grayscale image (Airport)

Image	Original Image			Encrypted Image		
	R	G	B	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 encrypted images were close to 8, as shown in Table 7, which indicates a high degree of disorder in the encrypted information. These values are also comparable with 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

Because the keys of the proposed system are based on chaotic attractors that are sensitive to small perturbations, introducing an insignificant change in one component of the key makes it impossible to recover the original information, a situation shown in Fig. 13.

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

On the other hand, regarding the size of the key space, the following values are taken into account:

- Parameters β and r of the logistic system, with a precision of 3 decimal digits for a total of$(10^3)^2$possible values.

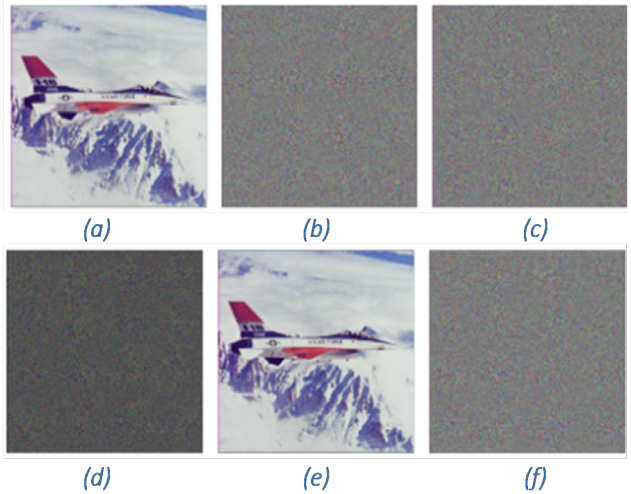


Fig. 13. *Key sensitivity.*
Source: [29].

• Initial conditions (x0, y0, z0) of the logistic system, with 3 decimal digits of precision, yielding$(10^3)^3$possible values.
• Diffusion keys of the quantum logistic system with 3 integer digits, resulting in$(10^3)^3$possible values.
• Two prime numbers of 15 integer digits with$(10^{15})^2$possibilities.
• Parameter r and initial condition x0 of the logistic map, with 3 decimal digits of precision for a total of$(10^3)^2$possible values.
Therefore, the size of the key space is10^{60}, which notably exceeds several of the results reported in the consulted literature, such as the works of Man et al. [31], Kamal et al. [32] and Ahmed et al. [33], whose reported key spaces are 1029, 1035 and 1038, respectively.

NIST[34]has established criteria for considering whether a cryptographic algorithm is resistant to quantum attacks, including semantic security and adaptive attack; the model presented here is robust for these criteria because the generated keys are highly sensitive to small perturbations, since they come from the use of chaotic dynamical systems. For this reason it could be stated that the algorithm is resistant to Grover search attacks[35][19], since this attack would reduce the complexity to O(1030), which is still high.

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 flat images

This type of analysis consists of encrypting single-color images, usually white or black, 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 of Fig. 14 were encrypted, and the results are presented in Figs. 14d, 14e and 14f, respectively. The decryption process was applied to these, and the original images g, h and i were obtained.

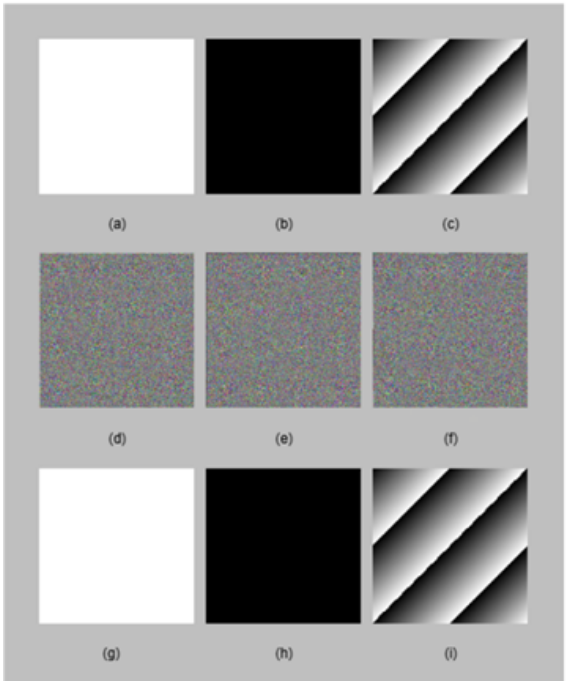


Fig. 14. *Robustness with flat images.*
Source: [29].

Starting from an encrypted image resulting from applying the proposed algorithm, a proportion of pixels is randomly replaced, turning them white or black, and the decryption process is then applied to the resulting image. 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). Subsequently, the decryption algorithm was applied, and the original image was recovered with minimal distortions to the human eye (Fig. 15d, 15e and 15f).

4.4.2. Salt and Pepper Test

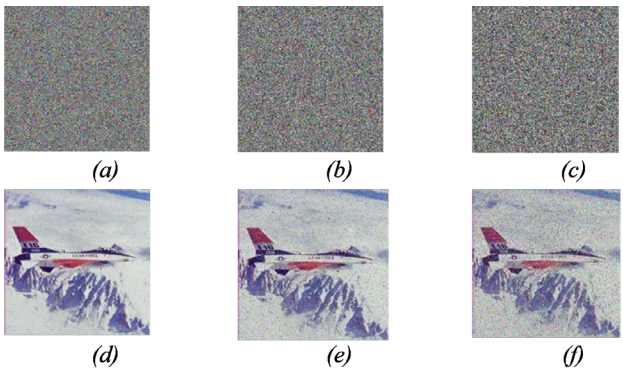


Fig. 15. *Salt and pepper test, color image.*
Source: Own elaboration.

In order to obtain a more accurate measurement of the results found in this test, the mean squared 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. The results are presented in Table 8.

Table 8: Mean squared error and peak signal-to-noise ratio for the Airplane image

Noise Proportion	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, as shown in Table 8 when a noise proportion of 5 % or 10 % is applied. Likewise, a PSNR above 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 proportion was 1 %. However, higher noise proportions showed some differences between the images.

Similarly, the grayscale image “Airport” was subjected to the same procedure as “Airplane”, yielding results that were consistent to the human eye, as shown in Table 9 and in Fig. 16.

Table 9: Mean squared error and peak signal-to-noise ratio for the Airport image

Noise Proportion	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.

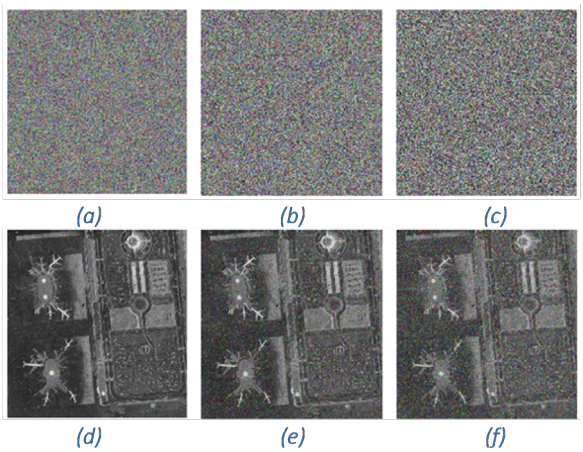


Fig. 16. *Salt and pepper test on grayscale image.*
Source: Own elaboration.

4.4.3. Occlusion Test

This test consists of taking an encrypted image, cropping a rectangular por
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). Note that in all 4 modifications a large part of the original image was recovered, a situation consistent with what was expected and shown in the same Fig. 17 (e, f, g and h).

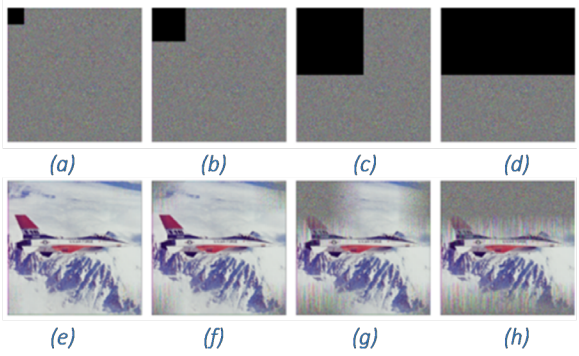


Fig. 17. *Occlusion attacks on the Airplane image.*
Source: [29].

Based on the security and performance tests applied, it is possible to state that the model presented here is resistant to chosen-plaintext attacks (CPA) and ciphertext-only attacks (COA), since the robustness analysis shows the absence of visual patterns; additionally, the correlation of adjacent pixels is minimal and the key is highly sensitive to small perturbations, that is, a small change in the original image generates global changes in the encrypted image, showing its resistance to linear attacks. Likewise, the results of entropy, correlation, NPCR, UACI and histogram tests conform to ideal behaviors in the field of security, which indicates resistance to differential attacks.

5. CONCLUSIONS

A new encryption algorithm inspired by the quantum domain was proposed, integrating principles of quantum mechanics, chaos theory and image processing, whose security is based on the high randomness of chaotic sequences and on the physical principle of qubit superposition.

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

The algorithm was also run on a classical computer and subjected to security and performance analysis, applying differential and statistical attack tests, key security and robustness tests, whose results led to the conclusion that it is highly secure and could therefore be applied in real contexts.

Finally, it should be borne in mind that the emergence of quantum computing creates challenges and threats to information security, so it is imperative to continue the search for new cryptographic algorithms that enable a secure transition to the post-quantum era, seeking to safeguard political, economic, military, scientific and social information.

ACKNOWLEDGMENT

The authors thank Universidad Distrital Francisco José de Caldas for its institutional support during the conduct of this research.

REFERENCES

[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.

FUNDING

No financing

CONFLICT OF INTEREST

None

AUTHORSHIP CONTRIBUTIONS

Drafting – original draft: Miguel Ángel Rico García, Luz Deicy Alvarado Nieto, Edilma Isabel Amaya Barrera.

Writing–review and editing: Miguel Ángel Rico García, Luz Deicy Alvarado Nieto, Edilma Isabel Amaya Barrera.