Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.064348

ARTICLE

Enhancing Post-Quantum Information Security: A Novel Two-Dimensional Chaotic System for Quantum Image Encryption

Fatima Asiri* **and Wajdan Al Malwi**

Informatics and Computer Systems Department, College of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia

*Corresponding Author: Fatima Asiri. Email: falmalye@kku.edu.sa

Received: 12 February 2025; Accepted: 09 April 2025; Published: 30 May 2025

ABSTRACT: Ensuring information security in the quantum era is a growing challenge due to advancements in cryptographic attacks and the emergence of quantum computing. To address these concerns, this paper presents the mathematical and computer modeling of a novel two-dimensional (2D) chaotic system for secure key generation in quantum image encryption (QIE). The proposed map employs trigonometric perturbations in conjunction with rational-saturation functions and hence, named as Trigonometric-Rational-Saturation (TRS) map. Through rigorous mathematical analysis and computational simulations, the map is extensively evaluated for bifurcation behaviour, chaotic trajectories, and Lyapunov exponents. The security evaluation validates the map's non-linearity, unpredictability, and sensitive dependence on initial conditions. In addition, the proposed TRS map has further been tested by integrating it in a QIE scheme. The QIE scheme first quantum-encodes the classic image using the Novel Enhanced Quantum Representation (NEQR) technique, the TRS map is used for the generation of secure diffusion key, which is XOR-ed with the quantum-ready image to obtain the encrypted images. The security evaluation of the QIE scheme demonstrates superior security of the encrypted images in terms of statistical security attacks and also against Differential attacks. The encrypted images exhibit zero correlation and maximum entropy with demonstrating strong resilience due to 99.62% and 33.47% results for Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). The results validate the effectiveness of TRS-based quantum encryption scheme in securing digital images against emerging quantum threats, making it suitable for secure image encryption in IoT and edge-based applications.

KEYWORDS: Information security; chaotic map modeling; post-quantum security; quantum image encryption; chaotic map; image encryption

1 Introduction

With the rapid advancements in digital technologies and the increasing severity of cybersecurity threats, robust encryption mechanisms are critically important for securing sensitive information [1,2]. The abundance of interconnected systems, such as IoT and cloud computing, a huge volume of digital data is generated and transmitted over unsecure networks. Image data is among the most generated and transmitted data types in IoT devices [3], as it holds importance in various modern applications including, but not limited to, medical imaging, remote sensing, surveillance, and big data [4]. The sensitive nature of image data in conjunction with the inherent susceptibility of IoT networks, call for robust security mechanisms to protect the information in images against unauthorized access, tampering, and cyber-attacks [5,6]. The field of cryptography—image encryption resolves these security concerns by hiding the information in digital images [7]. The existing encryption techniques, such as Rivest–Shamir–Adleman (RSA) and Eliptic

Curve Cryptography (ECC) will not prove to be effective against quantum computation attacks, where these algorithms can be broken easily using Shorr's algorithm [8]. Therefore, this paper intends to develop a secure post-quantum image encryption scheme that addresses the quantum threats in the post quantum era.

Quantum image encryption (QIE) has proved to be a promising solution for the post-quantum security of digital images, especially in IoT devices [9]. QIE employs quantum mechanics principles that make these schemes highly secure against quantum computational attacks [10]. Recently, chaos has been used in conjunction with QIE schemes to enhance their non-linearity and unpredictability. Chaotic systems are extremely beneficial in cryptographic algorithms due to their characteristics of being unpredictable, and sensitive to initial condition [11]. Chaotic maps serve as pseudorandom number generators (PRNG) in cryptographic algorithms, and hence, are preferred for applications, such as key generation. Recently, chaotic maps have extensively been used in image encryption algorithms [12,13]. The tradition chaotic maps possess limited chaotic range and bifurcation behaviour. Hence, there is a need to design new chaotic maps that have improved chaotic properties, large chaotic range, and highly chaotic bifurcation pattern. While many continuous chaotic systems (e.g., Lorenz or Chen) have been studied, discrete chaotic maps are particularly advantageous for digital implementations. They involve iterating a function at integer time steps, such that $\mathbf{X}_{n+1} = F(\mathbf{X}_n; \mathbf{P})$, where $\mathbf{X}_n$ represents the system state at iteration n and $\mathbf{P}$ is the vector of control parameters. This discrete iteration process simplifies numerical integration and is easily implemented in embedded devices, enabling real-time or high-throughput applications. Moreover, their deterministic yet pseudo-random behaviour, combined with strong dependence on control parameters, allows discrete maps to act as robust key generators in chaos-based cryptographic schemes.

To address the aforementioned concerns, this paper presents mathematical and computer modeling of a novel two-dimensional Trigonometric-Rational-Saturation (TRS) chaotic map, which has been extensively evaluated by performing computation simulations for key parameters, such as chaotic trajectories, bifurcation behaviour, and Lyapunov Exponents. Moreover, the designed chaotic map is integrated in a QIE to evaluate its effectiveness and security applications. The important contributions put forth by this paper are: (a) Design and security evaluation of a novel two-dimensional TRS chaotic map, which is utilised for secure key generation in image encryption applications, and (b) The integration and testing of the proposed TRS chaotic map in a Quantum Image Encryption scheme to validate its effectiveness and level of security.

2 Related Work

2.1 Chaotic Maps for Image Encryption

Recently, a lot of chaotic maps have been designed to secure image encryption schemes, especially due to to their inherent characteristics, such as unpredictability, sensitive dependence on initial conditions, aperiodicity, and spheroidicity, for example, a cosine-modulated polynomial chaotic map has been designed and evaluated in [14]. The presented one dimensional map enhances the chaotic properties while maintaining structural simplicity. The results demonstrate that the presented map achieved high level of non-linearity, unpredictability, and sensitivity to initial conditions. Similarly, a sine-cosine chaotic map (SCCM) has been presented in [15]. This map involves integration of deoxyribonucleic acid (DNA) encoding to further enhance the non-linearity and unpredictability of the map. Besides, chaotic maps have also been utilised in image encryption algorithms, for example, multiple chaotic maps have been utilised in a confusion-diffusion encryption scheme in [16]. The maps improve the security of the presented encryption system and protect the encrypted images from several cyber-attacks. In an attempt to improve the chaotic range of the chaotic maps, a logistic-quadratic chaotic map has been presented in [17]. The map boasts expanded chaotic range, large key space and focuses on maintaining the computational efficiency. Researchers have also developed higher dimensional chaotic map, for example, three-dimensional chaotic maps and an umbrella chaotic system have

been presented in [18], and [19], respectively. Both maps improve the encryption performance of proposed schemes in terms of correlation disruption and entropy maximisation. Moreover, other discrete systems have also been explored for image encryption. For instance, the Degn–Harrison map [20] was originally proposed to study bacterial respiration oscillations but is has shown to exhibit a range of complex bifurcation behaviours. Its use in ring-star network topologies and image encryption highlights its potential for secure data transmission, illustrating how chemical or biological models with chaotic dynamics can be adapted for cryptographic purposes. In addition, various studies have also been conducted on the cryptanalysis of image encryption schemes, for instance, a recent paper reveals that a scheme [21], which adopts quantum chaos and DNA coding, suffers from the existence of an equivalent key and vulnerable DNA substitution steps. Similarly, the scheme in [22], combining a Hill cipher variant with one-dimensional chaotic maps, fails to withstand chosen-plaintext/ciphertext attacks in under a second for standard images. These findings necessitate the need of secure chaos-based encryption algorithms.

2.2 Chaos-Based Quantum Image Encryption Techniques

Recent literature suggests an increased interest in the design and development of encryption schemes that are quantum resistant. Several papers can be found that present advancements in quantum image encryption, for example, a chaos-based dual-phase confusion-diffusion quantum image encryption scheme has been presented in [23]. The presented scheme integrates qubit and pixel level transformations to enhance the resilience against differential and data loss attacks. The results demonstrate improved randomness and diffusion properties in the encrypted images. Similarly, a QIE scheme involving cellular automata is proposed in [24]. The presented scheme benefits from various chaotic maps to improve the security of the encrypted images. The authors claim the proposed scheme is highly resistant to statistical attacks. Furthermore, another scheme utilises quantum bits-level scrambling and feedback diffusion methods to protect images in [25]. The authors also present a two-dimensional (2D) cross-chaotic map for the proposed QIE. Results demonstrate improved diffusion at bit level and improved key sensitivity due to the proposed map. Similarly, a three-dimensional chaotic map has been proposed and evaluated in [26] for a QIE scheme that involves controlled qubit scrambling. The method boasts achieving high-security while maintaining low-computational complexity. Additionally, in an attempt to secure digital images against destructive attacks, Arnold quantum transformations in conjunction with four-dimensional chaotic maps have been presented in [27]. The presented scheme exhibited strong encryption performance with improved key space and non-linearity. Similarly, quantum logistic chaos has been applied on flexible quantum representation images (FRQI)-based quantum images. The presented scheme is also compressive sensing and exhibits strong resistance against statistical and differential attacks.

3 The Proposed Novel 2D TRS Chaotic Map

3.1 Mathematical Modeling and Design of the Map

A two-dimensional discrete-time system can be represented by the iteration of a state vector $\mathbf{X}_n = (x_n, y_n)^\top$ via a deterministic non-linear transformation function:

$$\mathbf{X}_{n+1} = \mathbf{F}(\mathbf{X}_n; \mathbf{P}), \quad \mathbf{X}_n = \begin{bmatrix} x_n \\ y_n \end{bmatrix}, \tag{1}$$

where $\mathbf{P}$ is the vector of control parameters that govern the dynamics.

3.1.1 Definition of the TRS Map

In this work, a Trigonometric-Rational-Saturation (TRS) map has been proposed, which is defined component-wise by:

$$x_{n+1} = \sin\big(a\, y_n\big) \;+\; c \cdot \frac{x_n^2}{1 + x_n^2} \pmod 1, \tag{2}$$

$$y_{n+1} = \cos\big(b\, x_n\big) \;+\; d \cdot \frac{y_n}{1 + y_n^2} \pmod 1, \tag{3}$$

where $a, b, c, d \in \mathbb{R}$ are control parameters. The state variables x_n and y_n are confined to $(0,1)$ by the (mod 1) operation, which is vital for many applications in digital chaos-based cryptography. The map $\mathbf{F}(\mathbf{X}_n)$ thus has two principal non-linear components:

- **Trigonometric Perturbation:** $\sin(a\, y_n)$ and $\cos(b\, x_n)$ introduce oscillatory and strongly non-linear behaviour that is sensitive to both parameter changes (a and b) and initial conditions.
- **Rational Saturation:** $\frac{x_n^2}{1+x_n^2}$ and $\frac{y_n}{1+y_n^2}$ are rational functions whose magnitudes remain bounded. Notably,

$$\lim_{x\to\infty} \frac{x^2}{1+x^2} \;=\; 1, \quad \lim_{y\to\infty} \frac{y}{1+y^2} \;=\; 0,$$

ensuring the map does not diverge and has inherent "saturation"-like behavior.

Hence, combining trigonometric non-linearity and rational saturation, with a modulo operation, enhances the map's chaotic characteristics and keeps the trajectory within the unit square $(0,1) \times (0,1)$.

3.1.2 Fixed Points and Stability

A fixed point $\mathbf{X}^* = (x^*, y^*)^\top$ of the map satisfies:

$$x^* \;=\; \sin\big(a\, y^*\big) + c\, \frac{(x^*)^2}{1 + (x^*)^2} \pmod 1, \quad y^* \;=\; \cos\big(b\, x^*\big) + d\, \frac{y^*}{1 + (y^*)^2} \pmod 1. \tag{4}$$

Solving these equations analytically can be challenging due to the non-linear and mod 1 terms. Typically, one resorts to numerical methods to locate fixed points for given parameters.

3.1.3 Jacobian Matrix

Local stability around a point $\mathbf{X}^*$ is characterized by the Jacobian matrix of $\mathbf{F}$. For the TRS map, define:

$$\mathbf{F}(\mathbf{X}) = \begin{bmatrix} F_1(x,y) \\ F_2(x,y) \end{bmatrix} = \begin{bmatrix} \sin(a\, y) + c\, \dfrac{x^2}{1+x^2} \\ \cos(b\, x) + d\, \dfrac{y}{1+y^2} \end{bmatrix}.$$

Then the Jacobian matrix at $\mathbf{X} = (x, y)$ is:

$$\mathbf{J}(\mathbf{X}) \;=\; \begin{bmatrix} \dfrac{\partial F_1}{\partial x} & \dfrac{\partial F_1}{\partial y} \\ \dfrac{\partial F_2}{\partial x} & \dfrac{\partial F_2}{\partial y} \end{bmatrix}. \tag{5}$$

In order to derive the Jacobian matrix of the proposed 2D map, we begin by individually computing the partial derivatives of its components. Consider the map functions

$$F_1(x, y) = \sin\big(a\, y\big) + c\, \frac{x^2}{1 + x^2} \quad \text{and} \quad F_2(x, y) = \cos\big(b\, x\big) + d\, \frac{y}{1 + y^2}.$$

Because the term $\sin(a\, y)$ does not involve x, the only contribution to $\partial F_1/\partial x$ comes from the rational expression $c\, x^2/(1 + x^2)$. Differentiating that term with respect to x yields

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big(\frac{x^2}{1 + x^2}\Big) = \frac{2x\,(1 + x^2) - x^2\,(2x)}{(1 + x^2)^2} = \frac{2x}{(1 + x^2)^2},$$

and thus

$$\frac{\partial F_1}{\partial x} = c\, \frac{2x}{(1 + x^2)^2}.$$

Next, we differentiate F_1 with respect to y. In this case, $\sin(a\, y)$ is the only y-dependent term, leading to

$$\frac{\partial F_1}{\partial y} = \frac{\mathrm{d}}{\mathrm{d}y}\big[\sin(a\, y)\big] = a\, \cos\big(a\, y\big).$$

To complete the Jacobian, we consider $F_2(x, y)$. Notice that $\cos(b\, x)$ depends solely on x, whereas the rational term $d\, y/(1 + y^2)$ depends only on y. Consequently, when we calculate $\partial F_2/\partial x$, the differentiation applies to $\cos(b\, x)$ alone, giving

$$\frac{\partial F_2}{\partial x} = \frac{\mathrm{d}}{\mathrm{d}x}\big[\cos(b\, x)\big] = -\, b\, \sin\big(b\, x\big).$$

On the other hand, the derivative with respect to y exclusively involves the $d\, y/(1 + y^2)$ term. Performing this differentiation yields

$$\frac{\mathrm{d}}{\mathrm{d}y}\Big(\frac{y}{1 + y^2}\Big) = \frac{(1 + y^2) - 2y^2}{(1 + y^2)^2} = \frac{1 - y^2}{(1 + y^2)^2},$$

and therefore

$$\frac{\partial F_2}{\partial y} = d\, \frac{1 - y^2}{(1 + y^2)^2}.$$

By gathering these results, we form the Jacobian matrix

$$\mathbf{J}(\mathbf{X}) = \begin{bmatrix} \dfrac{\partial F_1}{\partial x} & \dfrac{\partial F_1}{\partial y} \\ \dfrac{\partial F_2}{\partial x} & \dfrac{\partial F_2}{\partial y} \end{bmatrix} = \begin{bmatrix} \dfrac{2c\, x}{(1 + x^2)^2} & a\, \cos\big(a\, y\big) \\ -\, b\, \sin\big(b\, x\big) & d\, \dfrac{1 - y^2}{(1 + y^2)^2} \end{bmatrix}, \tag{6}$$

where $\mathbf{X} = (x,\, y)$. This matrix quantifies how local perturbations in x and y are amplified (or contracted) under one iteration of the map, and its eigenvalues are fundamental to understanding the stability and chaotic properties of the system.

Local Stability Criterion

For a fixed point $\mathbf{X}^*$, local stability requires that all the eigenvalues of $\mathbf{J}(\mathbf{X}^*)$ lie strictly within the unit circle in the complex plane, i.e.,

$$\max\left|\lambda_i(\mathbf{J}(\mathbf{X}^*))\right| < 1.$$

If any eigenvalue λ satisfies $|\lambda| > 1$, the fixed point is unstable. A chaotic map often has at least one direction in phase space exhibiting expanding behaviour ($|\lambda| > 1$), leading to sensitive dependence on initial conditions.

3.2 Remarks on Parameter Selection

For chaos-based applications (e.g., encryption), the parameters (a, b, c, d) are chosen such that:

1. $\lambda_{\max} > 0$ to ensure robust chaos.
2. The map remains in $(0,1) \times (0,1)$ without collapsing onto stable orbits.
3. The generated sequence $\{(x_n, y_n)\}$ has good mixing and distribution properties.

Empirical parameter tuning, alongside the above theoretical and numerical checks, helps find parameter sets that maximize cryptographic strength and complexity.

3.3 Concluding Remarks on TRS Map Design

The proposed 2D TRS map:

- **Preserves Boundedness:** Thanks to both the trigonometric and rational saturation terms, the states remain confined within the unit square.
- **Exhibits High Non-Linearity:** The mixture of sine and cosine functions, rational transformations, and the mod 1 operation increases unpredictability.
- **Facilitates Chaotic Trajectories:** By proper parameter selection, the map attains high Lyapunov exponents, strong sensitivity to initial conditions, and aperiodic trajectories.

Consequently, it is a promising candidate for pseudorandom number generation and chaos-based encryption algorithms requiring strong cryptographic security and unpredictability.

3.4 Computational Simulation for Chaotic Trajectory Analysis

The chaotic trajectory of the system is the sequence of iterations $\{(x_n, y_n)\}$, which exhibits aperiodic, non-repeating behaviour for suitable parameter choices. Usually, trajectory plots are utilised to depict the chaotic pattern of a dynamic system, which illustrate how the system evolves over time in phase space. The proposed TRS map demonstrates highly non-linear and complex chaotic behaviour ensuring desired randomness. The map starts from the initial states (x_0, y_0) and progresses to further iterations as follows:

$$\mathbf{X}_{n+1} = \mathbf{F}(\mathbf{X}_n) \tag{7}$$

where:

$$\mathbf{X}_n = \begin{bmatrix} x_n \\ y_n \end{bmatrix}, \quad \mathbf{F}(\mathbf{X}) = \begin{bmatrix} \sin(a y_n) + c\dfrac{x_n^2}{1 + x_n^2} \\ \cos(b x_n) + d\dfrac{y_n}{1 + y_n^2} \end{bmatrix} \tag{8}$$

The chaotic behaviour of the TRS map, including the 2D and 3D trajectories are depicted in Figs. 1 and 2, respectively. Chaotic behaviour of the TRS map has also been compared with the trajectories of the logistic, sine, and tent maps. It is evident from the results that chaotic behaviour of the proposed map is highly non-linear and unpredictable as compared to those of the traditional maps in comparison.

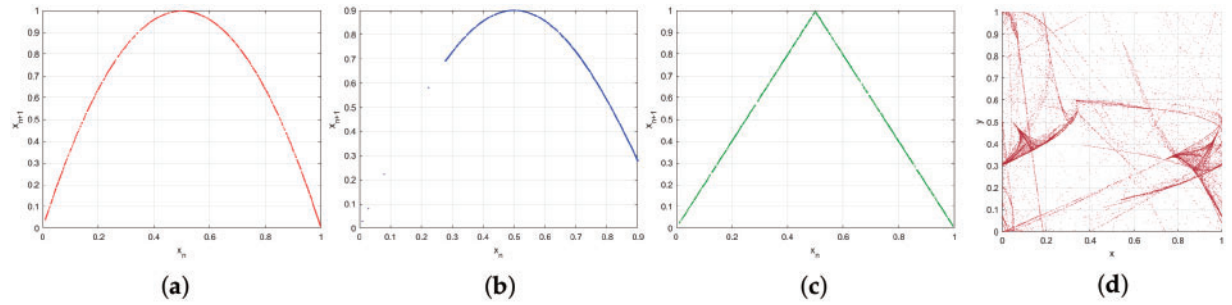

Figure 1: Visualization of chaotic dynamics through two-dimensional (2D) trajectory plots. **(a)** The conventional iterative 'Logistic' map. **(b)** The conventional trigonometric 'Sine' map. **(c)** The conventional piecewise-linear Tent chaotic map **(d)** The proposed TRS map, illustrating distinct non-linear behaviours

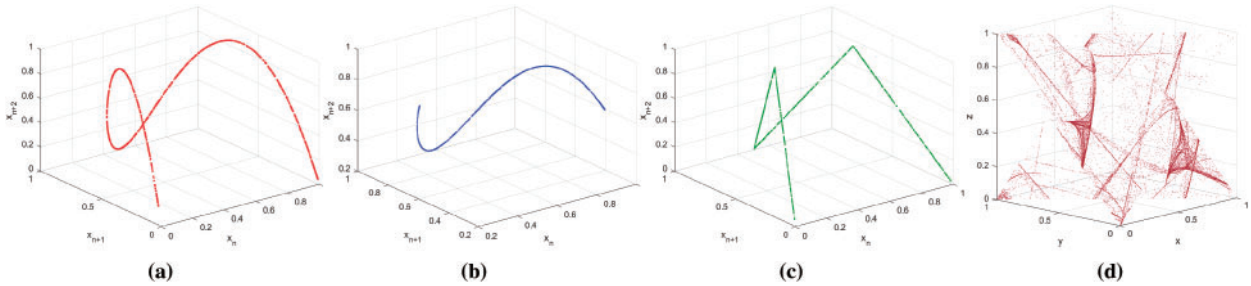

Figure 2: Visualization of chaotic dynamics through three-dimensional (3D) trajectory plots. **(a)** The conventional iterative 'Logistic' map. **(b)** The conventional trigonometric 'Sine' map. **(c)** The conventional piecewise-linear Tent chaotic map **(d)** The proposed TRS map, illustrating distinct non-linear behaviours

3.5 Sensitivity Analysis to Initial Conditions

The designed chaotic map has been subjected to sensitivity analysis to initial conditions. The map has been tested for a very minute change in its initial conditions, i.e., on the order of 10^{-12}. The experiments evaluate how minute changes lead to a significant divergence in chaotic trajectories. To quantify this behaviour in the proposed TRS map, we compared the evolution of two trajectories, (x_n, y_n) and (x'_n, y'_n), whose initial conditions differ by $\Delta_0 = 10^{-12}$. Specifically, if the first trajectory starts from (x_0, y_0), the second is initialized at

$$(x'_0, y'_0) = (x_0 + \Delta_0,\ y_0 + \Delta_0).$$

Both trajectories are iterated for 200 steps under identical control parameters ($a = 2.8$, $b = 3.5$, $c = 0.7$, $d = 1.2$).

Fig. 3 shows the evolution of the Euclidean distance $\|(x_n, y_n) - (x'_n, y'_n)\|$ on a logarithmic scale with respect to the iteration index n. The rapid escalation from 10^{-12} to values close to 10^0 confirms the exponential divergence induced by a small perturbation in the initial seeds. To visualize how these two trajectories evolve

in the phase space, we also plot (x_n, y_n) and (x'_n, y'_n) as discrete line segments in Fig. 3b,c. Both trajectories are iterated over the same time span. The "cobweb" appearance stems from connecting successive points of a *discrete* map rather than sampling a smooth flow. The blue (solid) lines denote the original trajectory, whereas the red (dashed) lines show the perturbed one. Even at a glance, their qualitative divergence is evident.

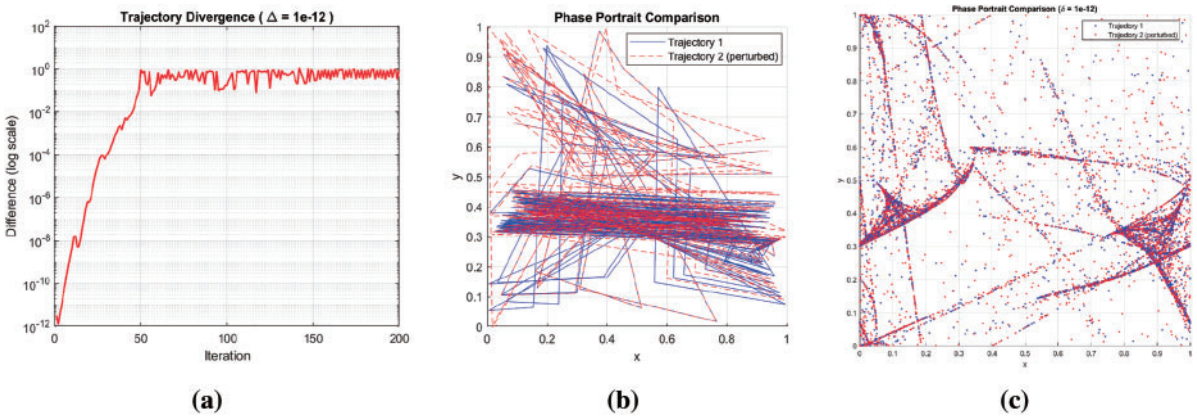

Figure 3: Sensitivity analysis to initial conditions. **(a)** Chaotic trajectory divergence (log scale) for two trajectories whose initial conditions differ by $\Delta_0 = 10^{-12}$. **(b)** Phase portrait comparison for two trajectories (original and perturbed). **(c)** Scatter plot exhibiting the state-space occupancy of original and perturbed trajectories

4 Computational Simulation for Lyapunov Exponent Analysis

The Lyapunov exponent (LE) is the parameter that determines the sensitivity of the designed map is to its initial conditions. The sensitivity of the map to its initial conditions is directly proportional to the value of the LE. For the proposed TRS chaotic map, the system's evolution is given by:

$$X_{n+1} = F(X_n), \tag{9}$$

where $X_n = (x_n, y_n)$ is the state vector. The Lyapunov exponent is computed as:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |\Lambda_i|, \tag{10}$$

where Λ_i are the eigenvalues of the Jacobian matrix $J(X)$, defined as:

$$\mathbf{J(X)} = \begin{bmatrix} \frac{\partial F_1}{\partial x} & \frac{\partial F_1}{\partial y} \\ \frac{\partial F_2}{\partial x} & \frac{\partial F_2}{\partial y} \end{bmatrix} = \begin{bmatrix} \frac{2c\,x}{(1+x^2)^2} & a\,\cos(a\,y) \\ -b\,\sin(b\,x) & d\,\frac{1-y^2}{(1+y^2)^2} \end{bmatrix}. \tag{11}$$

The Lyapunov exponents are numerically estimated by iterating the system and averaging the logarithm of the eigenvalues' magnitudes. Fig. 4d illustrates the largest Lyapunov exponent (LLE) of the TRS chaotic map as a function of parameter a. The red dashed line at $\lambda = 0$ marks the boundary between chaotic and non-chaotic regions. The results indicate that LLE remains consistently positive ($\lambda_1 \approx 2.5$) across the entire parameter range, confirming strong and sustained chaos. This behaviour ensures high unpredictability and ergodicity, making the TRS map highly suitable for cryptographic applications.

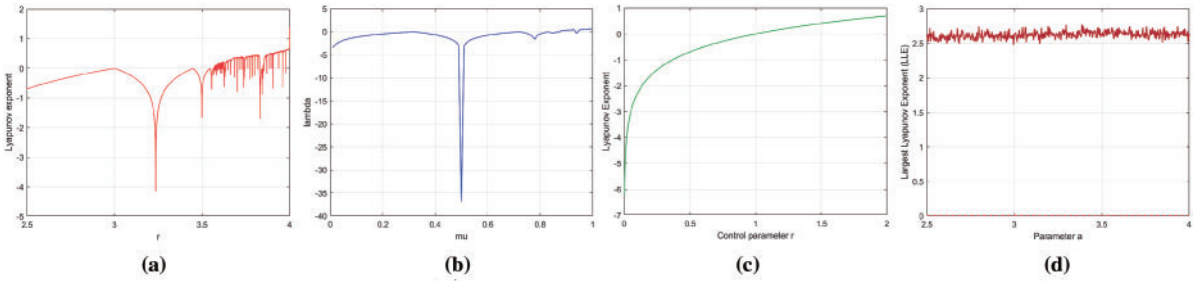

Figure 4: Sensitivity to initial conditions depicted by the Lyapunov exponent plots. **(a)** The conventional iterative 'Logistic' map. **(b)** The conventional trigonometric 'Sine' map. **(c)** The conventional piecewise-linear Tent chaotic map **(d)** The proposed TRS map

To highlight the superiority of the TRS chaotic map, its Lyapunov behaviour is compared to well-known 1D chaotic maps as shown in Fig. 4. The plots demonstrate that the TRS map, with its high-dimensional chaotic attractors, offers significantly greater unpredictability. Moreover, as the TRS map demonstrates consistently high Lyapunov exponents, indicative of strong sensitive dependence on initial conditions. The maps in comparison have smaller Lyapunov exponents, resulting in less sensitive dependence on initial conditions.

5 Computational Simulation for Bifurcation Analysis

Bifurcation analysis is a crucial tool for understanding the dynamical behaviour of chaotic systems as control parameters vary. In a chaotic system, bifurcations indicate the transition from periodic to chaotic behaviour, revealing the complex structure of attractors. The proposed TRS chaotic map is analysed through one-dimensional and three-dimensional bifurcation diagrams, confirming its ability to exhibit complex dynamical transitions. A bifurcation occurs when a small variation in a control parameter causes a qualitative change in the attractor's behaviour. The bifurcation pattern of the TRS map for all four control parameters is depicted in Fig. 5.

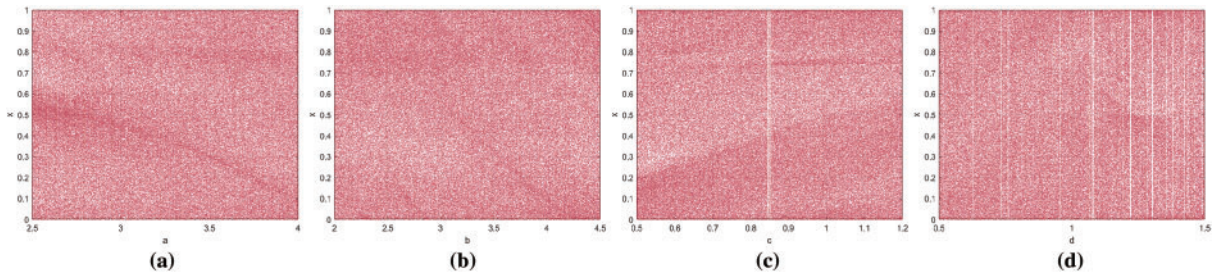

Figure 5: Bifurcation pattern of the TRS chaotic map. The bifurcation structure is obtained by sweeping the respective parameter over the range of $[2.5, 4.0]$. **(a)** For control parameter 'a'. **(b)** For control parameter 'b'. **(c)** For control parameter 'c'. **(d)** For control parameter 'd'

Unlike classical chaotic maps, the bifurcation patterns in TRS are highly dense, reflecting the strong ergodicity and complexity of the attractor structure as shown in Fig. 6. The chaotic maps in comparison exhibit limited bifurcation complexity. In contrast, the TRS chaotic map shows highly dense bifurcation points, ensuring greater randomness, persistent chaos over a broad parameter range, eliminating sensitivity to specific parameter tuning, interacting chaotic attractors in the 3D bifurcation analysis, revealing complex

multi-dimensional state-space transitions. Moreover, Fig. 7 shows 3D bifurcation diagrams, where the long-term behaviour of the system is plotted against two variables, revealing the interaction between different chaotic states.

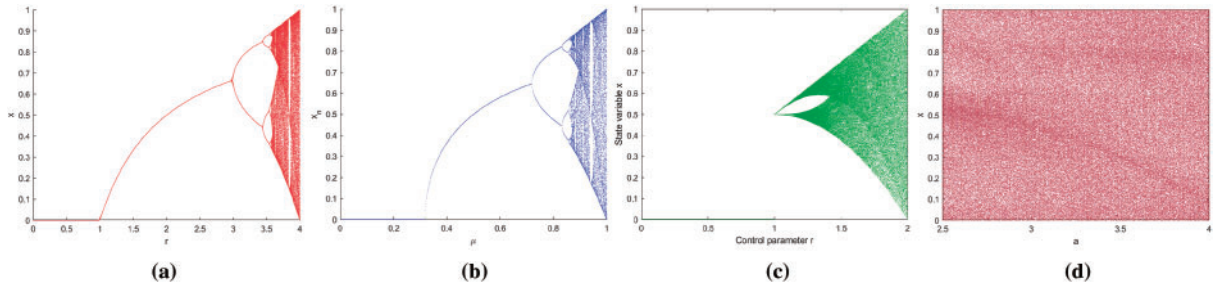

Figure 6: The comparison of the bifurcation pattern of the TRS map with the well known maps. **(a)** The conventional iterative 'Logistic' map. **(b)** The conventional trigonometric 'Sine' map. **(c)** The conventional piecewise-linear Tent chaotic map **(d)** The proposed TRS map

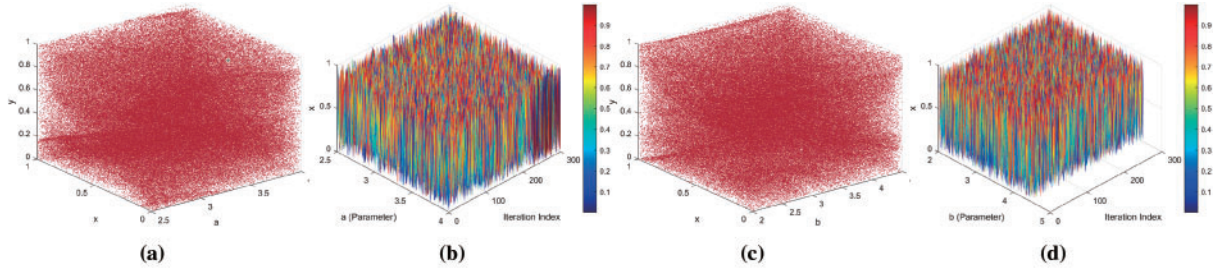

Figure 7: 3D bifurcation diagrams of the TRS chaotic map, obtained by sweeping the respective parameter over the range $a, b \in [2.5, 4.0]$ while keeping other parameters fixed. **(a)** 3D bifurcation plot for parameter 'a'. **(b)** 3D bifurcation surface plot for parameter 'a'. **(c)** 3D bifurcation plot for parameter 'b'. **(d)** 3D bifurcation surface plot for parameter 'b'

NIST SP 800-22 Randomness Evaluation

To evaluate the randomness of the pseudorandom sequences generated by the proposed TRS map, the NIST SP 800-22 tests have been conducted. The test procedure, results, and discussion is entailed as follows:

1. **Sequence Generation:** The TRS map has been iterated for 10^7 steps (discarding the first 500 transient values) and quantized each iteration into 8 bits by taking $\lfloor x_n \times 10^6 \rfloor \bmod 256$, thereby producing a binary stream of length 8×10^7.
2. **NIST Statistical Tests:** The 15 tests in the NIST SP 800-22 suite, i.e., Frequency (Monobit), Block Frequency, Runs, Longest Runs, Rank, Discrete Fourier Transform, Non-Overlapping Templates, Overlapping Templates, Universal, Approximate Entropy, Random Excursions, Random Excursions Variant, Serial, and Linear Complexity have been applied on the generated pseudorandom sequences.

All tests returned p-values above the required threshold, confirming that the TRS map's output stream passes the established NIST criteria. A concise overview of some critical tests is as follows:

- **Frequency (Monobit) and Block Frequency Tests:** The ratio of 0 to 1s, both across the entire sequence and within fixed-size blocks, stayed within the expected uniform range. Typical p-values lay between 0.14 and 0.37, safely exceeding the 0.01 threshold.

- **Runs and Longest Runs Tests:** Consecutive 0 or 1s did not deviate from the theoretical random-run distribution; numerical outcomes yielded $p \approx 0.21$–0.36, signifying an absence of systematic repetition in bit runs.
- **Rank Test:** By examining the linear independence of sub-blocks, this test revealed near full-rank matrices with $p \approx 0.24$, indicating that no linear pattern or dependency was detected beyond random chance.
- **Discrete Fourier Transform (Spectral) Test:** No significant periodicities were observed; p-values commonly fell between 0.22 and 0.31, showing no discernible spectral bias.
- **Non-Overlapping and Overlapping Template Tests:** Across different template lengths, these tests reported average p-values above 0.11, suggesting that no particular bit pattern (in overlapping or non-overlapping contexts) was overly frequent or rare.
- **Approximate Entropy and Universal Tests:** Results demonstrated high randomness and low compressibility, with p-values mostly within 0.18–0.43. This indicates that the generated bitstream achieves a balanced distribution of short and long-term patterns.
- **Serial, Linear Complexity, and Random Excursions Tests:** Further evaluations (e.g., checking adjacency relations, assessing polynomial complexities, and analyzing random walks) yielded median p-values in the range 0.26–0.38. No deterministic structures were detected in the sequences.

All NIST SP 800-22 tests produced p-values above the threshold, affirming statistical randomness. Consequently, the bit sequences derived from the TRS map fulfil the security requirements for cryptographic key generation.

6 Application to Quantum Image Encryption

In this section, a quantum-ready image encryption scheme that leverages the NEQR quantum image representation and the TRS chaotic map-based diffusion mechanism to achieve high-security image encryption is presented. The encryption process is stepwise and systematic, ensuring robustness against cryptographic attacks. The encryption scheme is given in Fig. 8 comprising the following steps in sequence:

6.1 Step 1: Quantum-Ready Image Representation via NEQR

Given a greyscale image$I$ of size $2^n \times 2^n$, it is first quantum-encoded using the NEQR (Novel Enhanced Quantum Representation) framework [28]. NEQR stores the pixel intensities and pixel location information in two entangle qubit sequences and the whole image is stored in the superposition of the two qubit sequences. A $2^n \times 2^n$ image can be represented as quantum image as follows [28]:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |C(y,x)\rangle \, |yx\rangle \tag{12}$$

where $C(y,x)$ represents the 8-bit greyscale intensity at coordinates (y,x), and $|yx\rangle$ denotes the quantum position encoding.

A sample representation of a 4×4 NEQR image is shown in Fig. 9a. Similarly, a sample greyscale image of size 2×2 with its representative expression in NEQR is given in Fig. 9b. As a greyscale image has pixel intensities ranging from 0 to 255, NEQR requires 8 qubits to store the pixel intensity information and hence, it needs $q + 2n$ qubits to represent a $2^n \times 2^n$ image with grey range 2^q. For the sample greyscale image shown in Fig. 9b, the detailed circuit needed for NEQR preparation is given in Fig. 10 [28].

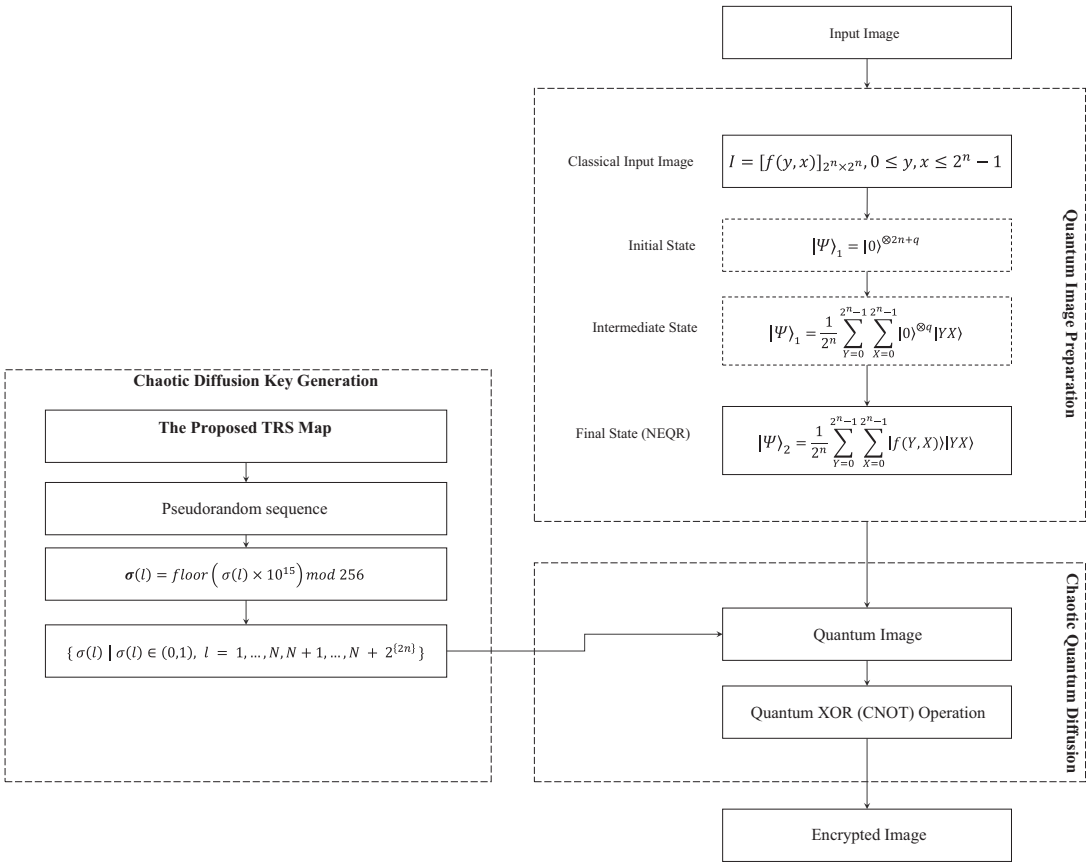

Figure 8: The quantum image encryption scheme to evaluate the TRS map

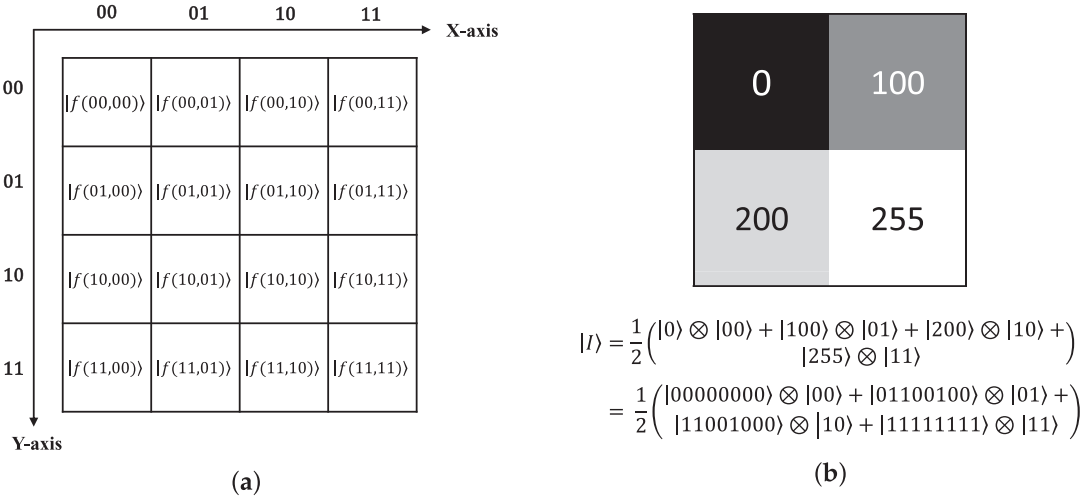

Figure 9: Representation of quantum images using NEQR. **(a)** A 4×4 NEQR Quantum image. $f(Y,X)$, e.g., $(f(00,00))$ represents the pixel intensity and is stored as the basis state $|f(Y,X)\rangle$ of a qubit sequence. **(b)** A sample 2×2 greyscale image with quantum representative expression in NEQR

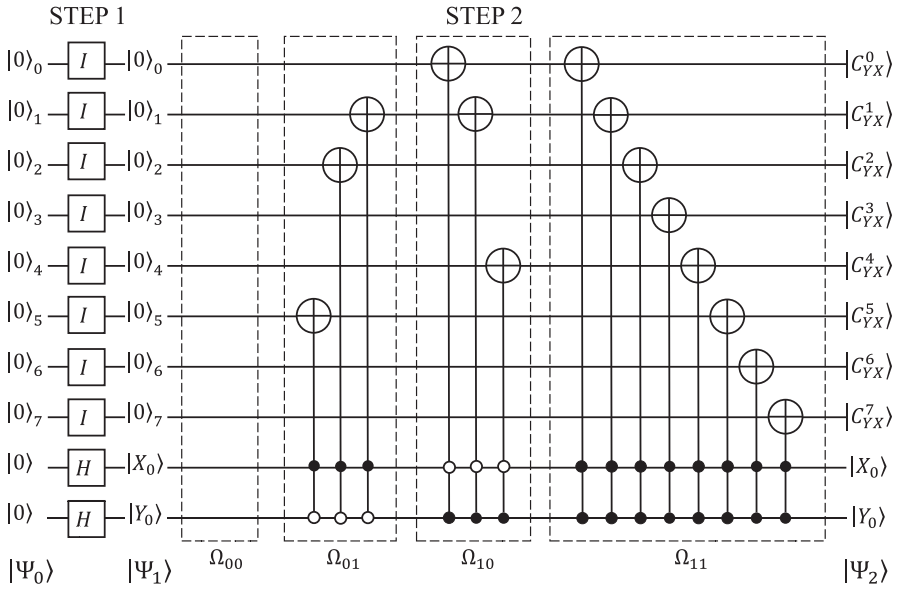

Figure 10: Quantum circuit for quantum image preparation—NEQR

6.2 Step 2: Chaotic Sequence Generation via TRS Map

To generate a pseudo-random sequence, the TRS chaotic map is utilized. The 2D TRS chaotic system evolves as:

$$x_{n+1} = \sin(a y_n) + c \cdot \frac{x_n^2}{1 + x_n^2} \mod 1, \tag{13}$$

$$y_{n+1} = \cos(b x_n) + d \cdot \frac{y_n}{1 + y_n^2} \mod 1. \tag{14}$$

The map is iterated for 256×256 times, and the first 500 transient iterations are discarded to avoid instability.

6.3 Step 3: Diffusion Key Matrix Generation

The diffusion key matrix is a 256×256 matrix and is generated from a random chaotic array $\sigma(l)$ generated by the TRS map and is derived as follows:

$$\sigma(l) = \text{floor}\left(s(l) \times 10^{15}\right) \mod 256, \tag{15}$$

where $s(l)$ is the chaotic sequence after removing transient values. The resulting key matrix:

$$\sigma = \begin{bmatrix} k_{0,0} & k_{0,1} & \dots & k_{0,255} \\ k_{1,0} & k_{1,1} & \dots & k_{1,255} \\ \vdots & \vdots & \ddots & \vdots \\ k_{255,0} & k_{255,1} & \dots & k_{255,255} \end{bmatrix}, \tag{16}$$

is used for pixel-wise diffusion.

6.4 Step 4: Quantum XOR-Based Diffusion

The final encryption is performed via applying bit-XOR (CNOT) operation [29] performed between the quantum-ready image matrix $|I\rangle$ and the secure diffusion key matrix $|\sigma\rangle$. The quantum ciphertext $|I_e\rangle$ is given by:

$$|I_e\rangle = |I\rangle \oplus |\sigma\rangle . \tag{17}$$

Expanding the quantum state representation, we obtain:

$$|I_e\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |C'(y,x) \oplus \sigma(y,x)\rangle \, |yx\rangle . \tag{18}$$

Simplifying further gives:

$$|I_e\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |E(y,x)\rangle \, |yx\rangle . \tag{19}$$

Where each encrypted pixel is computed as follows:

$$e_{yx}^{(i)} = c_{yx}^{(i)} \oplus k_{yx}^{(i)}, \quad i = 0, 1, \ldots, 7. \tag{20}$$

The operation in above equation ensures effective diffusion across all pixels and introduces additional layer of security. The quantum circuit for the chaotic diffusion process is given in Fig. 11.

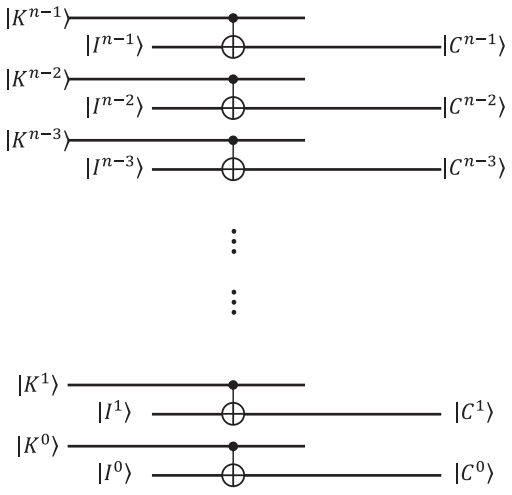

Figure 11: Quantum circuit for chaotic diffusion process

6.5 Decryption

Since the proposed encryption scheme is based on a symmetric keys, the decryption follows steps that invert the encryption operations. We assume the receiver has the correct initial parameters (a, b, c, d) and seeds (x_0, y_0) for the Trigonometric-Rational-Saturation (TRS) map and hence can generate the same chaotic key stream. The decryption steps are enlisted as follows:

1. The recipient starts with the cipher image. Each pixel is stored in an 8-qubit amplitude.
2. Using the symmetric keys, i.e., the control parameters (a, b, c, d) and initial conditions (x_0, y_0), the recipient iterates the TRS map to produce the chaotic key matrix σ. This key must match the one generated during encryption. Each iteration value is quantized (e.g., using $\lfloor x_n \times 10^6 \rfloor \mod 256$) to form an 8-bit sub-key, ensuring a one-to-one correspondence between key-stream bytes and image pixels.
3. The encryption relies on a bitwise (quantum) XOR operation between the quantum-ready plaintext and the chaotic key, the inverse operation is also a bitwise XOR (CNOT). In other words,

$$|I_{\text{dec}}\rangle = |I_{\text{e}}\rangle \oplus |\sigma\rangle, \tag{21}$$

   where $|I_{\text{dec}}\rangle$ is the recovered quantum image, $|I_{\text{e}}\rangle$ is the ciphered image state, and $|\sigma\rangle$ is the chaotic key. The XOR operation is its own inverse, so applying the same bitwise operation with the identical key matrix fully recovers the original quantum amplitudes.
4. Finally, the decrypted quantum image $|I_{\text{dec}}\rangle$ is measured to obtain the classical pixel values. This step inverts the initial NEQR encoding.
5. Upon completion of these steps, the decrypted (plain) image is successfully restored.

7 Security Evaluation, Results and Discussion

Extensive security evaluation has been conducted for the proposed QIE scheme employing the TRS map including histograms, correlation, and differential attacks. The encryption outcomes, presented in Fig. 12, illustrate that the encrypted images effectively conceal all information. All simulation experiments were conducted on an HP ProBook 450 G8 laptop. The system is equipped with an Intel® Core™ i7 processor (11th Generation), 16 GB of RAM, and runs a 64-bit operating system. This hardware configuration was sufficient to handle the iterative nature of our TRS map generation an d quantum encoding simulations, thus demonstrating the feasibility of the proposed encryption scheme on standard consumer-grade equipment.

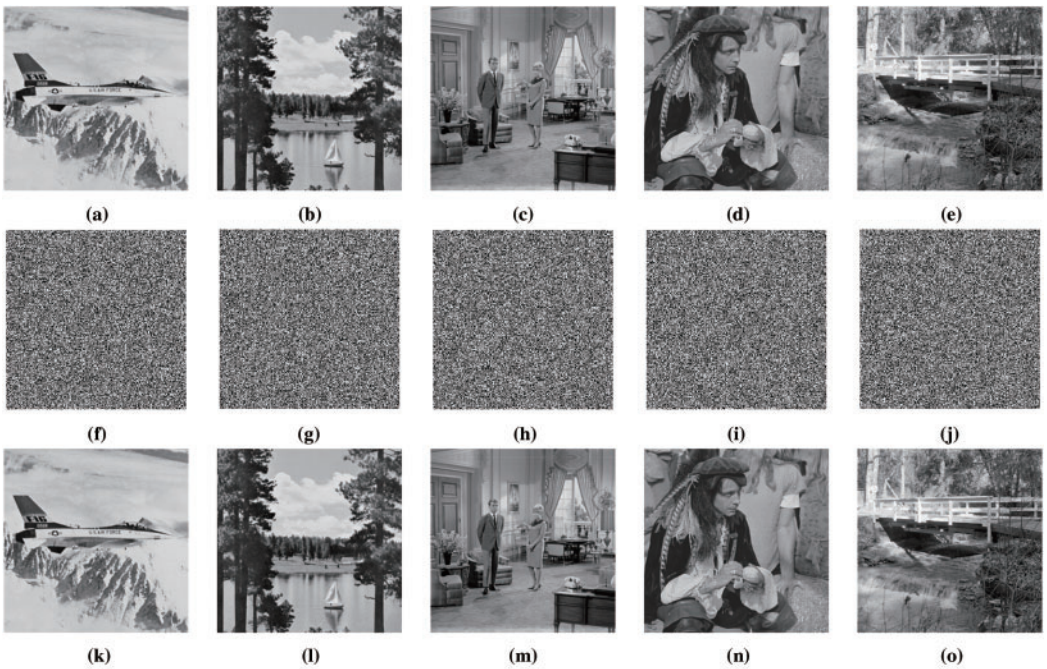

Figure 12: Visual security analysis of the proposed QIE scheme. **(a)**–**(e)** Plain test images. **(f)**–**(j)** The final encrypted images. **(k)**–**(o)** The lossless decrypted images

7.1 Histogram Analysis

A crucial test for evaluating the security of an encryption scheme is the histogram analysis, which assesses how much distributed are the pixel intensities in the encrypted image. A well-secured encryption method should produce uniform histograms, where pixel values are evenly distributed across the full greyscale range. For the input plaintext image $I(x, y)$, the histogram $H_P(v)$ quantifies the distribution of pixel intensities v based on how many time they appear in the image, and is given by:

$$H_P(v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \delta(I(x, y) - v). \tag{22}$$

In this equation, $\delta(x)$ is the Kronecker delta function and is given as:

$$\delta(x) = \begin{cases} 1, & x = 0 \\ 0, & x \neq 0. \end{cases} \tag{23}$$

The histograms of the plaintext and ciphertext images are shown in Fig. 13. The results demonstrate that the proposed scheme successfully disrupts statistical patterns, making it resistant to histogram-based attacks.

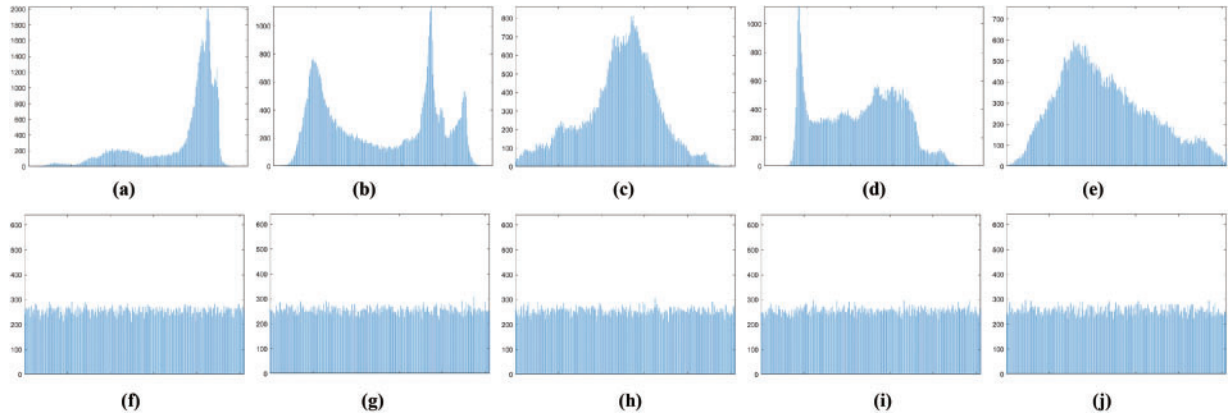

Figure 13: The histograms of the original and encrypted images. **(a)**–**(e)** Plain test images. **(f)**–**(j)** Final encrypted images

7.2 Correlation Analysis

A fundamental requirement for a secure image encryption scheme is that the ciphertext pixels exhibit no correlation with their adjacent pixels. In plaintext images, neighbouring pixels are highly correlated due to the structural redundancy in natural images. However, in an ideal encryption scheme, this correlation should be minimized, approaching zero. The correlation coefficient between two adjacent pixels, P_1 and P_2, is computed as:

$$r = \frac{E(P_1P_2) - E(P_1)E(P_2)}{\sqrt{D(P_1)D(P_2)}}, \tag{24}$$

where:

$$E(P) = \frac{1}{N}\sum_{i=1}^{N} P_i, \tag{25}$$

is the expectation of pixel intensities, and

$$D(P) = \frac{1}{N}\sum_{i=1}^{N}(P_i - E(P))^2, \tag{26}$$

is the variance of the pixel values. The ideal encrypted image should satisfy:

$$r \approx 0, \quad \forall (P_1, P_2) \text{ pairs.} \tag{27}$$

The correlation coefficients have been computed in three orientations: horizontal, vertical, and diagonal. The results for the plaintext and encrypted images are summarized in Table 1. The results confirm that the encrypted images achieve near-zero correlation, indicating strong decorrelation.

Table 1: Correlation coefficients of encrypted greyscale test images

Test image	Image size (Pixels)	Horizontal	Vertical	Diagonal
Jetplane	256 × 256	−0.0021	−0.0018	−0.0025
Lake	256 × 256	−0.0023	−0.0015	−0.0027
Livingroom	256 × 256	−0.0019	−0.0020	−0.0018
Pirate	256 × 256	−0.0024	−0.0017	−0.0022
Walkbridge	256 × 256	−0.0022	−0.0019	−0.0023

Scatter Plot Analysis

A visual confirmation of decorrelation is provided through correlation coefficient scatter plots, shown in Fig. 14. The scatter plots illustrate that plaintext images displays a highly concentrated structure, indicating strong correlation among neighbouring pixels, while the encrypted images exhibit efficient scattering with a randomized distribution, confirming strong decorrelation.

7.3 Differential Attack Analysis

A secure image encryption scheme must be highly sensitive to small changes in the plaintext. This property ensures that even a single-bit modification in the original image leads to significant changes in the ciphertext, making it resistant to differential attacks. To evaluate sensitivity, an experiment is conducted where a greyscale plaintext image is encrypted twice. The original plaintext image I is encrypted, producing ciphertext C_1. A single-bit in I is flipped, forming a slightly modified image I', which is then encrypted to obtain C_2. The difference between C_1 and C_2 is computed to analyse the impact of the tiny modification. The visual results are presented in Fig. 15, demonstrating the significant change induced by the single-bit variation.

The difference images in Fig. 15 show widespread pixel changes, confirming that even a minute modification in the plaintext results in a drastically different ciphertext, ensuring strong security against differential attacks.

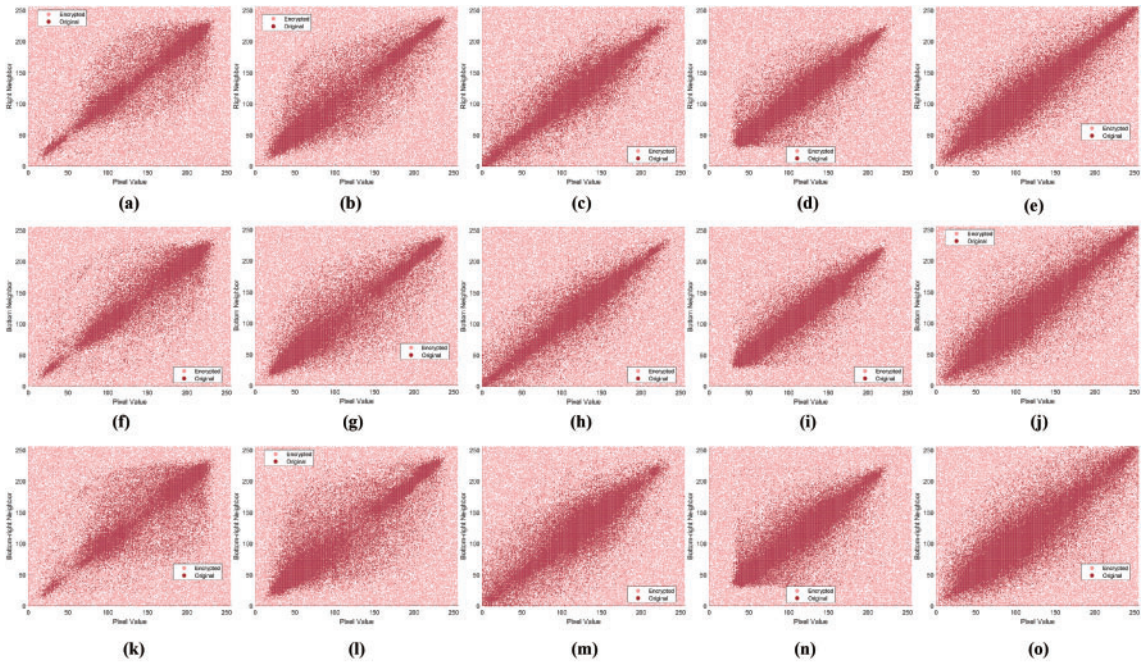

Figure 14: Evaluation of correlation properties in the proposed encryption scheme. Dark red plots represent the correlation coefficients of original images, while light red plots correspond to encrypted images. **(a)**–**(e)** Horizontal correlation analysis, **(f)**–**(j)** Vertical correlation assessment, and **(k)**–**(o)** Diagonal correlation evaluation

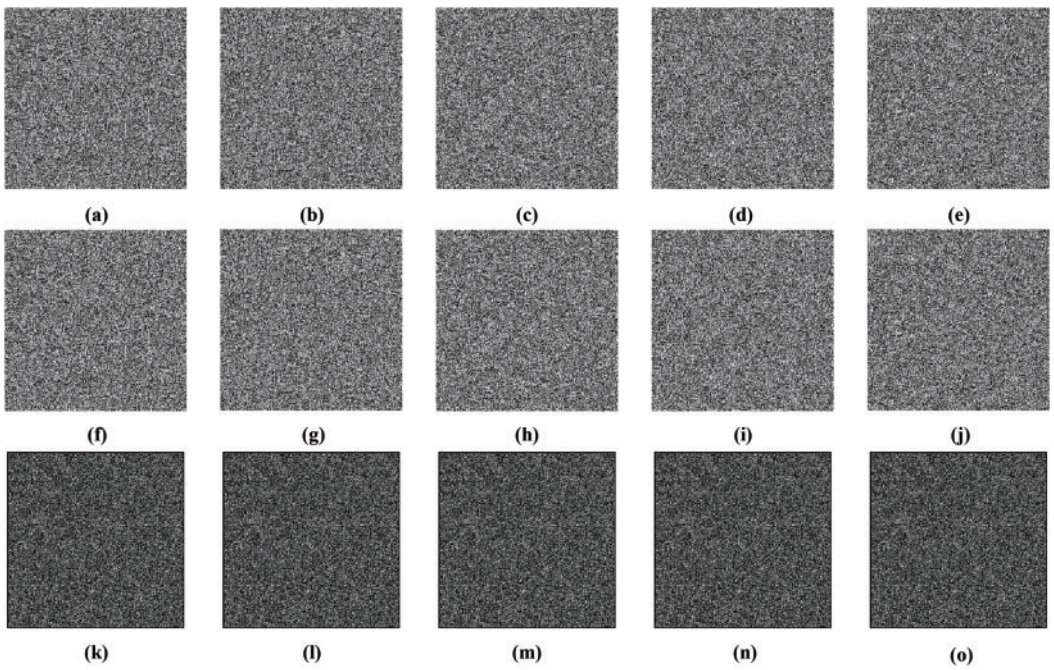

Figure 15: Differential attack results. **(a)**–**(e)** Original encrypted images. **(f)**–**(j)** Encrypted images of 1-bit changed plain images **(k)**–**(o)** Difference between the original and 1-bit changed encypted images

NPCR and UACI Evaluation

To quantitatively evaluate the differential security, two key metrics are used. Number of Pixels Change Rate (NPCR) measures the percentage of pixels that change when a single-bit modification occurs in the plaintext and the Unified Average Changing Intensity (UACI) measures the average intensity difference between two ciphertexts resulting from a slight plaintext change. The NPCR is computed as:

$$\text{NPCR} = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} D(x,y)}{M \times N} \times 100\%, \tag{28}$$

where:

$$D(x,y) = \begin{cases} 1, & C_1(x,y) \neq C_2(x,y) \\ 0, & C_1(x,y) = C_2(x,y). \end{cases} \tag{29}$$

Similarly, UACI is defined as:

$$\text{UACI} = \frac{1}{M \times N} \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} \frac{|C_1(x,y) - C_2(x,y)|}{255} \times 100\%. \tag{30}$$

The computed NPCR and UACI values are summarized in Table 2, demonstrating near-ideal security performance. The results confirm that the NPCR value is close to 100%, indicating that almost every pixel is altered when the plaintext changes slightly. The UACI value is close to 33%, aligning with the theoretical ideal for a highly efficient encryption scheme.

Table 2: Evaluation of NPCR and UACI metrics for encrypted images

Image name	Dimension	NPCR (%)	UACI (%)
Jetplane	256 × 256	99.6234	33.4812
Lake	256 × 256	99.6127	33.4598
Livingroom	256 × 256	99.6352	33.4725
Pirate	256 × 256	99.6189	33.4983
Walkbridge	256 × 256	99.6291	33.4657

7.4 Noise and Data Loss Resilience Analysis

The proposed encryption scheme has been evaluated for noise and data loss attacks. The noise resilience is tested by inducing salt and pepper noise in the encrypted images. Noise densities of 5%, 10%, and 15% were induced in the encrypted images and undergone the decryption process to evaluate the effect of noise attacks. It can be seen in Fig. 16 that the original images were successfully recovered with minimal data loss.

In addition, to evaluate the resilience of the proposed scheme of data loss attacks, different portions of encrypted images were clipped/occluded with occlusion areas of 10%, 20%, and 30%. When passed through the decryption process, the original images were successfully recovered with minimal data loss as evident in Fig. 17.

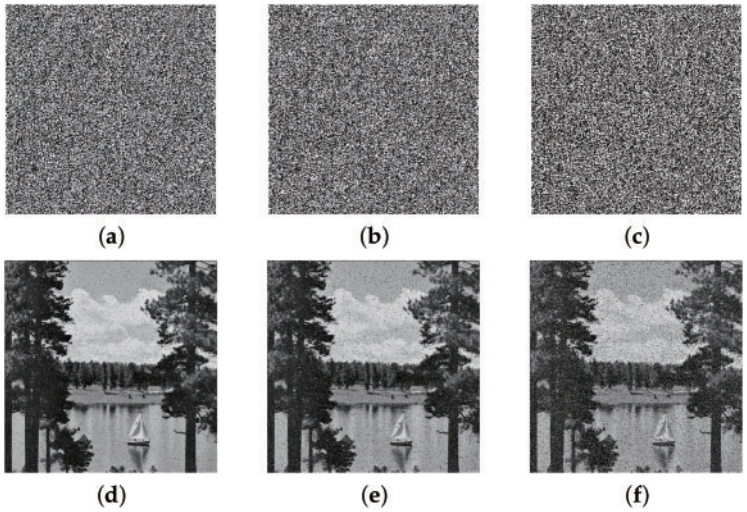

Figure 16: Resilience to noise attacks. **(a)** Encrypted image with 5% induced noise. **(b)** Encrypted image with 10% induced noise. **(c)** Encrypted image with 15% induced noise. **(d)** to **(f)** Successfully decrypted images with minimal loss

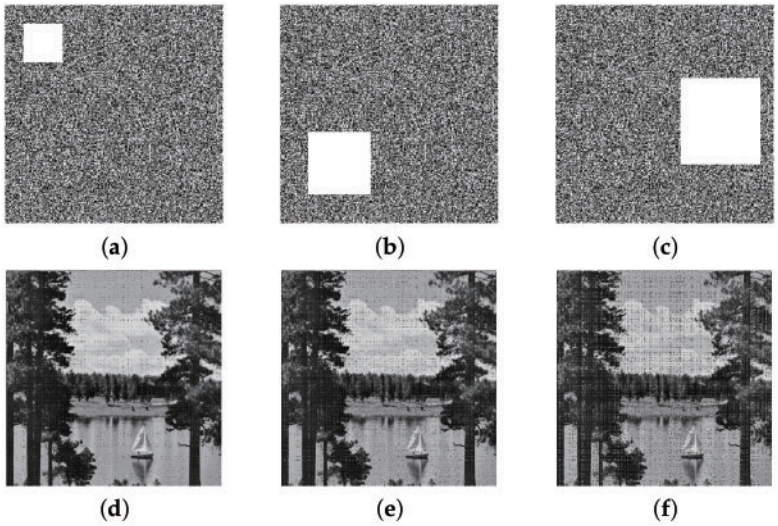

Figure 17: Resilience to data loss attacks. **(a)** Encrypted image with 10% data loss. **(b)** Encrypted image with 20% data loss. **(c)** Encrypted image with 30% data loss. **(d)** to **(f)** Successfully decrypted images with minimal loss

7.5 Entropy Analysis

Entropy estimates the amount of randomness in an encrypted image. A higher entropy value indicates better diffusion and confusion, making it harder for an attacker to predict pixel distributions. For a 256-level greyscale image, the ideal entropy value is close to 8, ensuring that the ciphertext exhibits maximum randomness. The Shannon entropy H of an encrypted image I_e is given by:

$$H(I_e) = -\sum_{v=0}^{255} P(v) \log_2 P(v), \tag{31}$$

where $P(v)$ is the probability of occurrence of pixel intensity v, computed as:

$$P(v) = \frac{H_C(v)}{M \times N}. \tag{32}$$

Here, $H_C(v)$ represents the histogram frequency of intensity v, and $M \times N$ is the total number of pixels in the encrypted image.

To validate the security of the encryption scheme, entropy values are calculated for several standard greyscale test images. The results are presented in Table 3. The ideal entropy values confirm the strong randomness and unpredictability of the encrypted images.

Table 3: Entropy values of encrypted grayscale test images

Test image	Image size (Pixels)	Plain image entropy	Cipher image entropy
Jetplane	256 × 256	6.7598	7.9974
Lake	256 × 256	7.7487	7.9974
Livingroom	256 × 256	7.4178	7.9975
Pirate	256 × 256	7.3385	7.9977
Walkbridge	256 × 256	7.6804	7.9968

7.6 Chi-Square Test

The chi-square test helps in determining the difference between observed and expected distributions. In the context of image encryption, it helps in verifying whether an encrypted image's pixel intensities are uniformly distributed or not. To perform this test, the observed frequency O_i of all 256 intensity levels is first calculated. Following this, the expected frequency E for a perfectly uniform distribution:

$$E = \frac{\text{Total Pixels}}{\text{Number of Bins}}. \tag{33}$$

The chi-square statistic is then calculated as follows:

$$\chi^2 = \sum_{i=0}^{255} \frac{(O_i - E)^2}{E}. \tag{34}$$

A high chi-square value represents showing uniform randomness, demonstrating that the encryption scheme effectively destroys patterns. On the other hand, a low chi-square value indicates a structured and non-random distribution. The results in Table 4 show that the original images exhibit very large χ^2 values and the χ^2 values for the encrypted images are quite small, validating that our proposed scheme effectively diffuses pixel intensities.

Table 4: Chi-square values for original and encrypted images

Test image	Original image	Encrypted image
Jetplane	171253.77	451.05
Lake	47549.76	502.96
Livingroom	53203.52	497.84

(Continued)

Table 4 (continued)

Test image	Original image	Encrypted image
Pirate	50055.38	501.70
Walkbridge	26651.54	499.55

7.7 Complexity Analysis of the Proposed Quantum Encryption Scheme

The overall complexity of the proposed scheme for a a grayscale image of size $N \times N$ with $N = 2^n$ is $O(N^2)$, since each pixel is processed once. A detailed complexity analysis is performed for all the steps involved in the scheme, i.e., the first step is reading an $N \times N$ image into memory and its complexity is is $O(N^2)$, as each pixel intensity must be accessed or loaded once whether implemented classically or via a hybrid quantum-classical pipeline. The next step is applying NEQR, where each pixel $\big(x, y, \text{intensity}\big)$ is mapped to a quantum state $|C(x, y)\rangle\,|x\ y\rangle$, where $C(x, y)$ denotes the q-bit intensity value. Generating the complete quantum-ready image requires N^2 insertions of pixel data into the quantum circuit, implying complexity of NEQR step to be $O(N^2)$. The next step involves quantum diffusion, in which a a chaotic key matrix $\mathbf{K}$ of size $N \times N$ is generated via the TRS map. Each pixel key entry $K(x, y)$ is produced by iterating the map for N^2 times in total. Each iteration computes $\sin(\cdot)$, $\cos(\cdot)$, and a rational expression within a `mod 1` operation. Since these steps each have constant time overhead, the chaotic key generation also has a complexity of $O(N^2)$. After obtaining the quantum-ready image and the chaotic key, the final encryption step is to *xor* (CNOT) each pixel's qubits with the corresponding bits of the key. In a classical sense, we apply an 8-bit xor for each of the N^2 pixels (assuming $q = 8$). Thus, its complexity comes out to be $O(N^2)$. From a quantum perspective, each pixel's intensity qubits undergo a constant number of quantum gates. Summing over all pixels leads to an overall linear scaling in N^2.

Summing the overhead of each step confirms that the entire encryption process is dominated by $O(N^2)$ operations in the classical complexity sense. Each pixel goes through a small, *constant-time* set of arithmetic (or gate) operations for chaotic key generation, quantum encoding, and pixel-wise xor. Consequently, the scheme scales well for images of moderate size (e.g., 256×256) and can be parallelized to handle larger dimensions, making it competitive with other post-quantum image encryption methods and is also comparable to state-of-the art quantum image encryption schemes [26,30,31] that report the same complexity of $O(N^2)$.

7.8 Discussion and Quantum Attack Resistance

An important aspect of the proposed TRS-based scheme is its resilience against known quantum attacks. Benefiting from quantum mechanics the proposed scheme intends to with stands quantum attacks such as: (a) Grover's algorithm, which can exponentially expedite classical brute-force key searches by providing a quadratic speed-up. However, in chaotic-map-based cryptosystems as ours, the key is derived from extremely sensitive initial seeds (x_0, y_0) of the map. Even with Grover's algorithm, attempting to guess these seeds still requires exponential time in the worst case, as the dimension and parameter range of the map are large, (b) Shor's algorithm, the traditional public-key cryptosystems such as RSA or ECC can be broken in polynomial time by Shor's algorithm. Since our method does not rely on factorization or discrete logarithm problems, the known vulnerabilities exploited by Shor's algorithm do not apply.

Most of the existing post-quantum cryptographic techniques, such as lattice-based or code-based cryptography, rely on structured mathematical problems believed to be intractable for quantum computers. In contrast, our approach uses a chaotic map, which is independent from traditional number-theoretic

assumptions. While certain high-dimensional chaotic maps or hybrid systems may equal or surpass the chaos level of TRS, they can become more computationally intensive. By focusing on a two-dimensional TRS design, we balance parameter complexity and computational feasibility.

Furthermore, the proposed TRS-based quantum image encryption scheme has been designed with IoT and edge computing constraints in mind. These environments typically feature low-power processors (e.g., ARM Cortex or MIPS) and constrained memory resources. Moreover, the TRS map's operations can be efficiently realized in either single-precision floating-point or fixed-point. For devices that lack hardware floating-point support, optimized lookup tables or approximations (e.g., CORDIC for sine and cosine) can further reduce computational overhead. When run on slightly more capable edge devices (e.g., Raspberry Pi), the diffusion and NEQR encoding steps can be parallelized across multiple cores. Because each pixel's chaotic key is computed independently, thread-level parallelism can often achieve near-linear speed-ups. Hence, the TRS map can be integrated into constrained hardware systems while maintaining robust cryptographic properties, making it suitable for real-world deployment in edge-based applications.

8 Conclusion

This paper presented the design and modeling of a novel Trigonometric-Rational-Saturation (TRS) chaotic map and applied it to quantum image encryption. The TRS map-based quantum encryption scheme proved to be effective in securing digital images from cyber attacks. The TRS map demonstrated strong chaotic properties, which have been validated through bifurcation analysis, Lyapunov exponents, and phase-space trajectories. Its high Lyapunov exponent confirmed its suitability for cryptographic applications. In addition, a quantum-ready encryption scheme was utilised using NEQR encoding and a chaotic diffusion key matrix derived from the TRS map. Security analysis showed uniform histograms, near-zero correlation (≈ -0.002), and strong differential resistance with NPCR (99.62%) and UACI (33.47%). Entropy values (7.999 bits) confirmed maximal randomness in ciphertexts. The proposed scheme ensured strong diffusion, key sensitivity, and resistance to attacks, making it a viable solution for quantum-secure image encryption. Despite the promising results, the proposed scheme is limited to simulations on 2D grayscale images. Future work may include, utilising multi-channel representation for quantum images (MCQI) to run experiments on color images, exploring efficiency of the proposed scheme on higher-dimensional and fractional-order chaotic maps, and investigating lightweight quantum authentication techniques to ensure both robust encryption and efficient real-time performance.

Acknowledgement: The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP.2/556/45).

Funding Statement: This work is funded by Deanship of Research and Graduate Studies at King Khalid University. The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP.2/556/45).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Fatima Asiri and Wajdan Al Malwi; methodology, Fatima Asiri and Wajdan Al Malwi; software, Fatima Asiri and Wajdan Al Malwi; investigation, Fatima Asiri and Wajdan Al Malwi; writing—original draft preparation, Fatima Asiri and Wajdan Al Malwi; writing—review and editing, Fatima Asiri and Wajdan Al Malwi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the Corresponding Author, F.A., upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Malik A, Ali M, S. Alsubaei F, Ahmed N, Kumar H. A color image encryption scheme based on singular values and chaos. Comput Model Eng Sci. 2023;137(1):965–99. doi:10.32604/cmes.2023.022493.
2. Ibrahim RW, Natiq H, Alkhayyat A, Kadhim Farhan A, M. G. Al-Saidi N, Baleanu D. Image encryption algorithm based on new fractional beta chaotic maps. Comput Model Eng Sci. 2022;132(1):119–31. doi:10.32604/cmes.2022.018343.
3. Ali H, Khan MS, Driss M, Ahmad J, Buchanan WJ, Pitropakis N. CellSecure: securing image data in industrial internet-of-things via cellular automata and chaos-based encryption. In: 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall); 2023; Hong Kong, China. p. 1–6.
4. Lin Y, Xie Z, Chen T, Cheng X, Wen H. Image privacy protection scheme based on high-quality reconstruction DCT compression and nonlinear dynamics. Expert Syst Appl. 2024;257(5):124891. doi:10.1016/j.eswa.2024.124891.
5. El-kafrawy P, Aboghazalah M, M. Ahmed A, Torkey H, El-Sayed A. An efficient encryption and compression of sensed IoT medical images using auto-encoder. Comput Model Eng Sci. 2023;134(2):909–26. doi:10.32604/cmes.2022.021713.
6. Khan MS, Ahmad J, Ali H, Pitropakis N, Al-Dubai A, Ghaleb B, et al. SRSS: a new chaos-based single-round single s-box image encryption scheme for highly auto-correlated data. In: 2023 International Conference on Engineering and Emerging Technologies (ICEET); 2023; Istanbul, Turkey. p. 1–6.
7. Alqahtani F. AI-powered image security: utilizing autoencoders for advanced medical image encryption. Comput Model Eng Sci. 2024;141(2):1709–24. doi:10.32604/cmes.2024.054976.
8. Singh B, Ahateshaam M, Lahiri A, Sagar AK. Future of cryptography in the era of quantum computing. In: International Conference on Electrical and Electronics Engineering 2023; 2023; Istanbul, Turkey. p. 13–31.
9. Wang J, Geng YC, Han L, Liu JQ. Quantum image encryption algorithm based on quantum key image. Int J Theor Phys. 2019;58(1):308–22. doi:10.1007/s10773-018-3932-y.
10. Sahu SK, Mazumdar K. State-of-the-art analysis of quantum cryptography: applications and future prospects. Front Phys. 2024;12:1456491. doi:10.3389/fphy.2024.1456491.
11. Zhang B, Liu L. Chaos-based image encryption: review, application, and challenges. Mathematics. 2023;11(11):2585. doi:10.3390/math11112585.
12. Ullah S, Liu X, Waheed A, Zhang S, Li S. Novel grayscale image encryption based on 4D fractional-order hyperchaotic system, 2D Henon map and knight tour algorithm. Phys Scr. 2024;99(9):095248. doi:10.1088/1402-4896/ad6d0e.
13. Ullah S, Liu X, Waheed A, Zhang S. Provably secure color image encryption algorithm based on FO 4D-HCS and ACM. Soft Comput. 2024;28(21–22):12879–96. doi:10.1007/s00500-024-10319-8.
14. Khan MS, Ahmad J, Al-Dubai A, Pitropakis N, Driss M, Buchanan WJ. A novel cosine-modulated-polynomial chaotic map to strengthen image encryption algorithms in IoT environments. Procedia Comput Sci. 2024;246:4214–23. doi:10.1016/j.procs.2024.09.261.
15. Liang Q, Zhu C. A new one-dimensional chaotic map for image encryption scheme based on random DNA coding. Opt Laser Technol. 2023;160(9):109033. doi:10.1016/j.optlastec.2022.109033.
16. Elkandoz MT, Alexan W. Image encryption based on a combination of multiple chaotic maps. Multimed Tools Appl. 2022;81(18):25497–518. doi:10.1007/s11042-022-12595-8.
17. Khairullah MK, Alkahtani AA, Bin Baharuddin MZ, Al-Jubari AM. Designing 1D chaotic maps for fast chaotic image encryption. Electronics. 2021;10(17):2116. doi:10.3390/electronics10172116.
18. Sachin, Singh P. A novel chaotic Umbrella map and its application to image encryption. Opt Quantum Electron. 2022;54(5):266. doi:10.1007/s11082-022-03646-3.
19. Bouteghrine B, Tanougast C, Sadoudi S. Novel image encryption algorithm based on new 3-d chaos map. Multimed Tools Appl. 2021;80(17):25583–605. doi:10.1007/s11042-021-10773-8.
20. Vismaya V, Muni SS, Panda AK, Mondal B. Degn-Harrison map: dynamical and network behaviours with applications in image encryption. Chaos, Solit Fractals. 2025;192(3):115987. doi:10.1016/j.chaos.2024.115987.

21. Wen H, Lin Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Syst Appl. 2024;237(14):121514. doi:10.1016/j.eswa.2023.121514.
22. Wen H, Lin Y, Yang L, Chen R. Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos. Expert Syst Appl. 2024;250(1):123748. doi:10.1016/j.eswa.2024.123748.
23. Shahbaz Khan M, Ahmad J, Al-Dubai A, Pitropakis N, Ghaleb B, Ullah A, et al. Chaotic quantum encryption to secure image data in post quantum consumer technology. IEEE Trans Consum Electron. 2024;70(4):7087–101. doi:10.1109/TCE.2024.3415411.
24. Mohamed NAES, El-Sayed H, Youssif A. Mixed multi-chaos quantum image encryption scheme based on quantum cellular automata (QCA). Fractal Fract. 2023;7(10):734. doi:10.3390/fractalfract7100734.
25. Hu M, Li J, Di X. Quantum image encryption scheme based on 2D $Sine_2$–Logistic chaotic map. Nonlinear Dyn. 2023;111(3):2815–39. doi:10.1007/s11071-022-07942-1.
26. Verma V, Kumar S. Quantum image encryption algorithm based on 3D-BNM chaotic map. Nonlinear Dyn. 2025;113(4):3829–55. doi:10.1007/s11071-024-10403-6.
27. Liu XD, Chen QH, Zhao RS, Liu GZ, Guan S, Wu LL, et al. Quantum image encryption algorithm based on four-dimensional chaos. Front Phys. 2024;12:1230294. doi:10.3389/fphy.2024.1230294.
28. Zhang Y, Lu K, Gao Y, Wang M. NEQR: a novel enhanced quantum representation of digital images. Quantum Inf Process. 2013;12(8):2833–60. doi:10.1007/s11128-013-0567-z.
29. Liu X, Xiao D, Liu C. Three-level quantum image encryption based on Arnold transform and logistic map. Quantum Inf Process. 2021;20(1):1–22. doi:10.1007/s11128-020-02952-7.
30. Liu X, Xiao D, Liu C. Double quantum image encryption based on arnold transform and qubit random rotation. Entropy. 2018;20(11):867. doi:10.3390/e20110867.
31. Li HS, Li C, Chen X, Hy Xia. Quantum image encryption algorithm based on NASS. Int J Theor Phys. 2018;57(12):3745–60. doi:10.1007/s10773-018-3887-z.