Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063729

ARTICLE

Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption

De Rosal Ignatius Moses Setiadi[1,*], T. Sutojo[1], Supriadi Rustad[1], Muhamad Akrom[1], Sudipta Kr Ghosal[2], Minh T. Nguyen[3] and Arnold Adimabua Ojugo[4]

[1]Research Center for Quantum Computing and Materials Informatics, Faculty of Computer Science, Dian Nuswantoro University, Semarang, 50131, Indonesia

[2]Department of Cyber Forensics and Information Security, Behala Government Polytechnic, 756, Upendra Nath Banerjee Road, Parnasree, Behala, Kolkata, 700060, India

[3]Thai Nguyen University of Technology, Thai Nguyen University, Thai Nguyen, 240000, Vietnam

[4]Department of Computer Science, Federal University of Petroleum Resources, Effurun, 330102, Nigeria

*Corresponding Author: De Rosal Ignatius Moses Setiadi. Email: moses@dsn.dinus.ac.id

Received: 22 January 2025; Accepted: 10 March 2025; Published: 16 April 2025

ABSTRACT: Data security has become a growing priority due to the increasing frequency of cyber-attacks, necessitating the development of more advanced encryption algorithms. This paper introduces Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps (SQQLSR), a quantum-based chaos map designed to generate one-dimensional chaotic sequences with an ultra-wide parameter range. The proposed model leverages quantum superposition using Hadamard gates and quantum rotations along the X, Y, and Z axes to enhance randomness. Extensive numerical experiments validate the effectiveness of SQQLSR. The proposed method achieves a maximum Lyapunov exponent (LE) of ≈55.265, surpassing traditional chaotic maps in unpredictability. The bifurcation analysis confirms a uniform chaotic distribution, eliminating periodic windows and ensuring higher randomness. The system also generates an expanded key space exceeding 10^{40}, enhancing security against brute-force attacks. Additionally, SQQLSR is applied to image encryption using a simple three-layer encryption scheme combining permutation and substitution techniques. This approach is intentionally designed to highlight the impact of SQQLSR-generated chaotic sequences rather than relying on a complex encryption algorithm. The encryption method achieves an average entropy of 7.9994, NPCR above 99.6%, and UACI within 32.8%–33.8%, confirming its strong randomness and sensitivity to minor modifications. The robustness tests against noise, cropping, and JPEG compression demonstrate its resistance to statistical and differential attacks. Additionally, the decryption process ensures perfect image reconstruction with an infinite PSNR value, proving the algorithm's reliability. These results highlight SQQLSR's potential as a lightweight yet highly secure encryption mechanism suitable for quantum cryptography and secure communications.

KEYWORDS: Single qubit quantum chaotic; quantum chaotic map; quantum image encryption; quantum logistic map; quantum sine map

1 Introduction

In today's modern world, the acceleration of data transmission has increased the demand for data protection techniques. In addition, due to the rapid increase in both the volume and complexity of cyberattacks [1,2], conventional encryption methods began to face more and more difficulties [3]. A new paradigm of increasing attention is chaos-based cryptography, which possesses the properties of being sensitive to

initial conditions, ergodicity, and unpredictability [4–6]. In general, chaos maps are categorized into one-dimensional (1D), two-dimensional (2D), and high-dimensional (HD) maps [7–10]. HD chaotic maps, such as hyperchaotic maps, have complex dynamics and more control parameters, thus providing a high level of security in encryption applications [11]. However, implementing these maps often requires longer computation time and more resources. To overcome this, compression and encryption can be combined to reduce computational complexity while increasing encryption efficiency [12]. However, designing and improving chaotic models can directly improve encryption performance.

The 1D chaotic maps have a simple structure, are easy to implement, and require minimal computational resources, making them an attractive choice for many practical applications, including image encryption [13]. However, traditional 1D chaotic maps, such as Logistic Map and sine maps, have inherent limitations, like uneven bifurcation distribution, periodic windows, and limited Lyapunov exponent (LE) range. These limitations reduce the effectiveness of 1D maps for high-security scenarios and advanced applications such as image encryption. Research [14] has created a cryptanalysis method to break the encryption of hill and chaotic variants such as logistic, sine, and Chebyshev. Hence, the development of chaos methods becomes urgent.

Several studies have developed 1D chaotic maps, such as Han's [15] study, which proposed the Modified Logistic Map to improve the sensitivity to initial conditions and expand the chaotic range of the Logistic Map. Other 1D methods have also been proposed, such as Fractional 1D chaotic map [13] for high-speed image encryption and 1D Sine Powered (1DSP) [16], which integrates two control parameters to produce a wider range of chaos and higher complexity. The 1D Sine-Map-Coupling-Logistic-Map (1D-SMCLM) coupling system was also developed by Hu et al. [17], which overcomes the shortcomings of small parameters in the Sine Map and Logistic Map. In addition, an Improved Logistic Map (1D-ILM) and an Improved Quadratic Map (1D-IQM) were also proposed by Khairullah et al. [18]. These developments reflect significant efforts to improve the efficiency and security of 1D-based chaotic systems.

The advancement of quantum computing technology, such as Quantum Key Distribution (QKD), has been widely developed in data communication. QKD can be distributed very securely, making it difficult for attackers to steal. QKD has also been applied to protect key distribution in image encryption [19–21], but quantum development for image encryption has not been widely developed. The way quantum computing works by converting bits into qubits makes the randomness patterns produced by chaotic systems stronger [22,23]. The superposition principle allows qubits to be in a linear combination of two or more states simultaneously, providing the ability to increase randomness significantly [24,25]. Moreover, entanglement between qubits strengthens the correlation between elements in a chaotic system even though they are physically separated. Quantum rotation, mediated by rotation gates such as Hadamard and CNOT, provides additional complexity in manipulating the system's randomness.

Several studies have utilized quantum approaches to chaotic maps [26–28]. Rehman [29] integrated quantum principles with sine-based chaos maps. Wang [30] proposed fast adaptive synchronization on discrete logistic quantum chaos maps. Rajan et al. [31] also introduced an image encryption model that combines quantum rotation and chaos maps. While Abd el-Latif et al. [32] used a quantum-inspired method to integrate the properties of quantum walks and logistic-sine maps. The development of quantum chaos is crucial because it can expand the control parameters that directly increase the key space, increase the complexity of system dynamics, and overcome the periodicity weaknesses in traditional chaotic systems, especially 1D ones.

This research objective is to introduce Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps (SQQLSR), a powerful and simple 1D quantum chaos map. SQQLSR utilizes quantum principles to produce more random and unpredictable 1D chaotic behavior. Quantum superposition is implemented through

the Hadamard gate, which allows qubits to be in a linear combination of multiple states simultaneously, expanding the space of possible system dynamics. In addition, three types of quantum rotations are used—*X*, *Y*, and *Z* Rotations—each providing an additional dimension to manipulating randomness. Combining these elements makes SQQLSR produce superior performance in terms of randomness and security. The SQQLSR map is also tested and applied in a new image encryption framework, where the resulting chaotic sequence is used for substitution and permutation processes. RGB images expand one chaotic sequence into three sequences for red, green, and blue channels. A high floating point normalization technique is applied to adjust the initial distribution range of the chaotic sequence, making it compatible with the number of image layers without compromising the randomness quality of the system.

2 Literature Review

2.1 Traditional Chaotic Maps and Background

In traditional chaos maps such as Logistic Map and Sine Map, bifurcations are often concentrated in certain regions, especially when the value of the control parameter (r) is close to the threshold for producing complete chaos. The bifurcation graph of the Logistic Map shows that the chaotic pattern only occurs at values of $r \approx [3.5, 4.0]$, while at other r ranges, the pattern is more regular or even stable, see Fig. 1a,b.

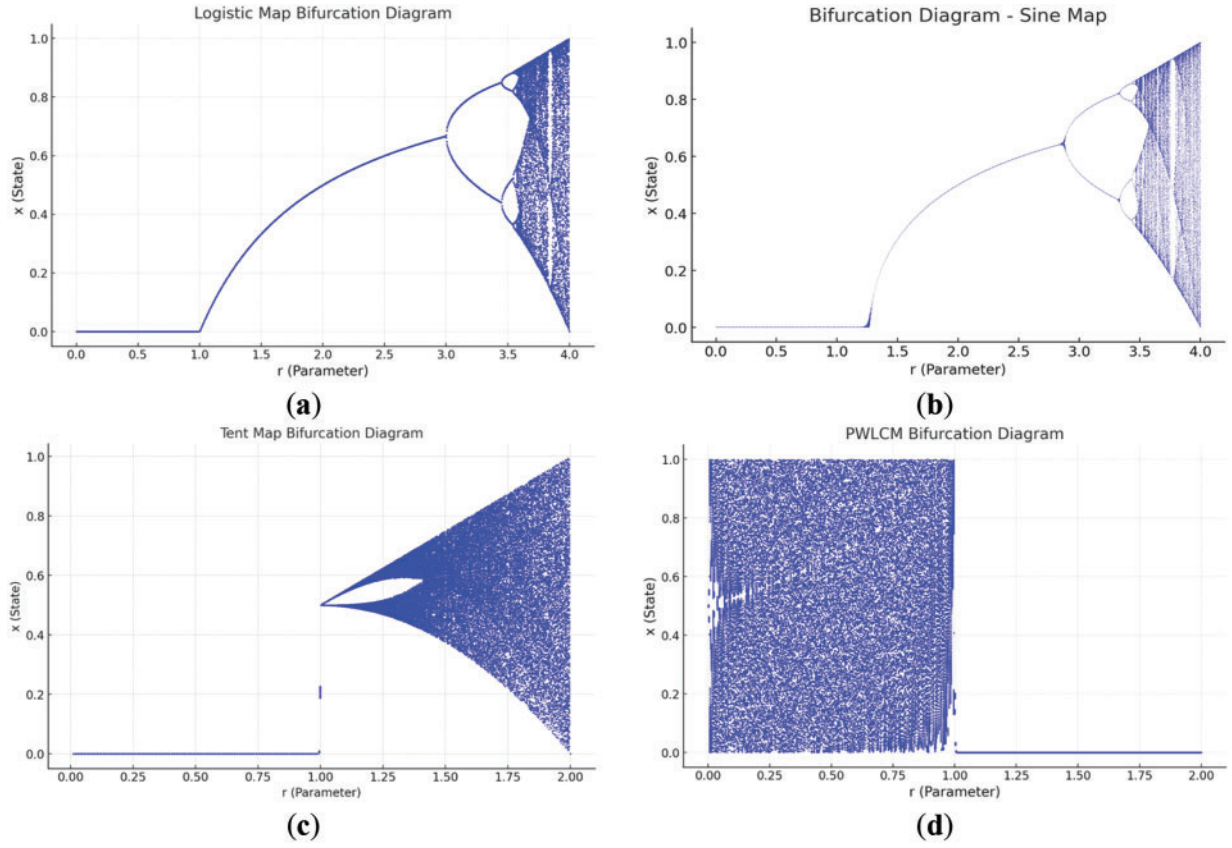

Figure 1: Bifurcation diagram of traditional chaotic map (**a**) Logistic map; (**b**) Sine map; (**c**) Tent map; (**d**) Piecewise-linear chaotic map

The Tent Map bifurcation graph in Fig. 1c shows chaotic behavior starting from the control parameter value $r \approx 1.0$. Conversely, at a value of $r < 1.0$, the system shows stability, but. The PWLCM bifurcation

graph (Fig. 1d) shows a more even chaos distribution than other traditional maps. This system begins to show chaotic behavior at a value of $r \approx 0.05$, with the full chaos region expanding significantly to $r \approx 1.0$. Furthermore, the PWLCM bifurcation returns to a stable trend, which shows that the PWLCM parameter control range is still limited. This weakness impacts the efficiency of chaos maps in cryptographic applications. The uneven bifurcation distribution limits the randomness that can be used, making the key space narrower and the resulting key pattern more susceptible to prediction.

The Lyapunov exponent (LE) is an essential metric for assessing the sensitivity of a system to small changes in initial conditions. Positive LE values indicate a better chaotic pattern. Conversely, low values mean that the chaotic pattern is more predictable, thus reducing the strength of the encryption key. In traditional chaotic maps such as Logistic and Sine Map, LE values tend to be low in the r range below 3.5, indicating a less sensitive system nature. Only in the $r \approx [3.5, 4.0]$ range the LE value increase to positive, indicating chaotic behavior, see Fig. 2a,b.

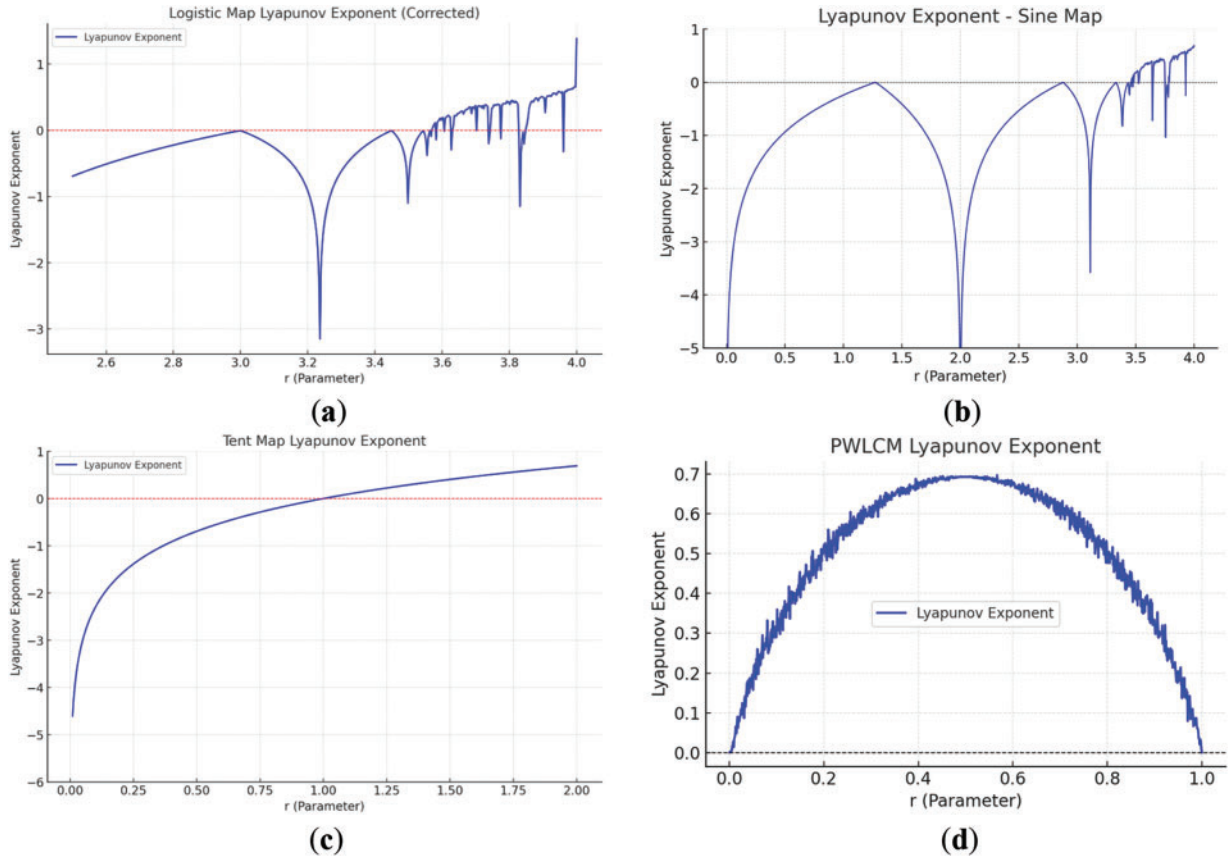

Figure 2: LE of traditional chaotic map (**a**) Logistic map; (**b**) Sine map; (**c**) Tent map; (**d**) Piecewise-linear chaotic map

The LE of the Tent Map (see Fig. 2c) shows a pattern different from that of the Logistic and Sine Map. In the $r \in [0, 1.0]$ range, the LE value tends to be negative, indicating stable and periodic system dynamics. However, when $r > 1.0$, the LE value starts to be positive and increases consistently until it approaches 1.0 at $r = 2.0$. This indicates that the Tent Map has strong chaotic properties and is more stable in that interval, with increased sensitivity to small changes in initial conditions. PWLCM shows a parabolic LE pattern in the parameter range $p \in [0, 1.0]$. The highest LE value is around $p = 0.5$, reaching almost 0.7, indicating

that PWLCM has strong chaotic properties in that parameter. On the other hand, the LE value approaches zero at the ends of the range $p \approx 0$ and $p \approx 1.0$. More advanced chaotic methods, such as hybrid chaotic maps [33], can increase LE ≈ 1.7, making the system more sensitive to small changes. Similarly, 1D Sine Powered Map (1D-DSP) also achieves LE ≈ 1.7, while traditional chaotic generally have a value of LE ≈ 0.7 in the chaotic region.

Another important factor in chaotic systems is the range of control parameters. A more extensive range of control parameters directly expands the available key space, which is one of the critical elements in cryptographic security [33,34]. In traditional chaotic maps such as Logistic Map, the range of control parameters is generally limited to the interval [0, 4]. Ullah et al. [34] proposed 1D Cosine Chaotic Equation (1D-CCE) with a range of control parameters [0, 10], showing improved flexibility and randomness compared to the Logistic Map. Another study [33] developed a hybrid chaotic map using three dynamic parameters, where one parameter has a range of [0, 4], and the other two parameters have a range of [0, 2]. Although there is an improvement over traditional maps, the limited range of parameters is still a constraint in expanding the key space. Therefore, expanding the control parameters in 1D chaotic maps remains a significant need to improve security, especially in the key space and complexity of chaotic systems.

2.2 Related Works

Traditional chaotic maps have been modified to improve deficiencies such as narrow bifurcation range, low LE, and instability in specific parameter ranges. Modified Logistic Map [15] is designed to increase sensitivity to initial conditions, expand the range of control parameters to [0, 10], and obtain complete mapping $x_n \in [-2r, 2r]$, in addition the LE value is relatively more stable, namely ≈0.7 in the entire range.

Another development of 1D chaotic map is called sine powered chaotic map (1DSP) [16] such as research using two control parameters, namely $\alpha > 1$ and $\beta \in [0, 1]$. When the value of $\alpha = 4.4926$, the LE value moves up from ≈ 0.4 at $\beta = 0$ to approaching 1.5 when the value of $\beta \approx 0.1$, then LE starts to drop to 0 when $\beta \approx 0.7$, LE drops drastically to ≈ −2 at $\beta \approx 0.8$ and starts to rise again towards ≈ −0.2 when $\beta = 1.0$. On the other hand, when tested with a value of $\beta = 0.3306$ for $\alpha \in [0, 9]$, there is a relatively stable upward movement of LE from ≈ −2.25 hingga ≈ 1.5, although there is an unstable up and down movement of LE when α is between 0 and 1 from ≈ −2.25 to ≈ 0.

Another map, the Fractional 1D chaotic map [13], also uses two control parameters, namely $\alpha \in [0, 1]$ and $\beta \in \left[-0.5, 1 + \frac{\alpha}{2}\right]$. The bifurcation at $\alpha = 0.2$ is wider and more spread out than at $\alpha = 0.5$, but at some values, namely $\beta <\approx 0.2$ when $\alpha = 0.2$ and $\beta <\approx 0.3$ when $\alpha = 0.5$, it shows uneven bifurcation, which means the system dynamics are relatively stable.

Furthermore, a recent study [34] proposed 1-Dimensional Cosine Chaotic Equation (1D-CCE). CCE has a wider range of control parameters, namely $r \in [0, 10]$ with maximum LE values of CCE ≈ 4.999. The bifurcation and LE graphs of CCE show extensive and dynamic chaotic behavior in the range [0, 1], although there are small parts that have "blank windows" indicating stable dynamics [18].

The development of the 1D chaotic map models above has indeed succeeded in expanding the range of chaos and increasing sensitivity to initial conditions. However, quantum chaotic maps have been developed with a relatively limited parameter range and relatively unstable chaotic behavior. Study [35] is one of the early studies that utilized quantum chaotic maps as pseudo-random number generators (PRNG). It is said that a high level of non-periodicity was obtained based on the evaluation of the Scale Index Technique. In addition, there are also dissipative quantum corrections, which provide additional dynamics.

Furthermore, Rehman [29] implemented quantum coding and 1-D Sine-based Chaotic Maps for image encryption. Furthermore, Rajan et al. [31] combined classical chaotic maps, such as logistic-sine hybrid

chaotic maps, with quantum chaotic maps to increase randomness and sensitivity to initial conditions. The unique characteristics of qubits, such as entanglement and superposition, are exploited to expand the key space and strengthen encryption security against classical and quantum threats. Unfortunately, this study does not discuss the bifurcation diagram, Lyapunov exponent, and trajectory. However, there is a discussion of the phase diagram, which shows very complex and unexpected dynamics, in addition to the claim of a significant increase in the key space.

Recent research introduces a distributed quantum logistic model in three dimensions (3D) [30], utilizing the coupling parameter (κ) and the degree of quantum entanglement (γ) to expand the chaotic dynamics. With this approach, a larger chaotic zone and higher complexity are achieved, as seen in the bifurcation and phase diagrams. Quantum entanglement is key in increasing the sensitivity to initial conditions and enriching the system's dynamics. This is indeed different from the simpler 1D approach. Still, based on bifurcation observations made at $\kappa \in [3, 4]$ and $\gamma = 3.5, 3.8, 4.0$, but the bifurcation pattern in the range $\kappa \in [3, 3.5]$ is still relatively stable, as well as when tested at $\gamma \in [2.75, 4]$ and $\kappa = 3.7, 3.85, 4.0$, there is a stable bifurcation pattern at $\gamma \in [2.75, 3]$. This means that the dynamic, chaotic space is still relatively limited, and this can also affect the key space. Therefore, further development related to the quantum chaotic map still needs to be explored again to create a quantum chaotic formula with a wide, dynamic, simple, and powerful key space range.

2.3 Motivation and Research Contribution

Traditional chaos maps face limitations such as uneven bifurcation distribution, low Lyapunov exponent (LE), and narrow key space. The development of chaos maps has been carried out and has obtained positive results, but considering the increasingly developing technology, the sophistication of chaos maps still needs to be developed. Quantum technology is a leap of innovation and has the potential to develop chaos map performance. The previously carried out quantum approach offers more complex dynamics, although it can be more complex and still has limited chaos space. SQQLSR is designed to overcome this problem by utilizing the principles of superposition and quantum rotation, resulting in a more even bifurcation distribution, stable LE, and a more expansive dynamic key space. More detailed contributions of this research are:

1. Designing SQQLSR by simply using single qubits to reduce computational complexity.
2. The principles of superposition (Hadamard) and quantum rotation (X, Y, Z) are used to expand chaos dynamics and increase sensitivity.
3. SQQLSR offers higher and stable LE and dynamic bifurcation distribution over an ultra-wide parameter range.
4. Implementing and testing SQQLSR for image encryption.

3 Proposed Method

3.1 Design Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps

Single Qubit Quantum Logistic-Sine *XYZ*-Rotation Maps (SQQLSR) is a quantum-based chaos map design that utilizes the properties of quantum superposition and rotation to produce more complex and unpredictable chaotic dynamics. Compared with classical chaos maps, SQQLSR provides significant advantages regarding a more expansive key space, higher randomness, and better sensitivity to initial conditions. It should be noted that the number of qubits in a quantum computing system significantly impacts computational complexity. Each additional qubit increases the information storage capacity exponentially and enlarges the state space that must be managed, thereby increasing operational complexity and resource requirements [36,37]. Based on this theory, this research considers designing the system using a single qubit,

making it simpler than multi-qubit based models but still sophisticated. This single-qubit design reduces the computational complexity while maintaining strong chaotic properties. Efficiently exploiting quantum superposition and rotation in a simpler framework makes near-term quantum hardware more feasible. The unitary operator of SQQLSR can be written in Eq. (1).

$$U_{SQQLSR} = H \cdot R_Z(\theta) \cdot R_Y(\phi) \cdot R_X(\gamma) \cdot H \tag{1}$$

where H is the Hadamard gate to prepare the initial and final superposition; $R_Z(\theta), R_Y(\phi), R_X(\gamma)$ are three types of rotation gates with defined scaling parameters (θ, ϕ, γ) which are described in more detail in Eqs. (2)–(4), updated iteratively to regulate the rotation dynamics.

$$\theta = r \cdot x_n \cdot (1 - x_n) \cdot scale + i \cdot iv \tag{2}$$

$$\phi = \alpha \cdot \sin(\pi \cdot x_n) \cdot scale + r \cdot iv \tag{3}$$

$$\gamma = r \cdot iv + \frac{\pi}{3} \tag{4}$$

where r is the control parameter being varied; i is the i-th iteration; x_n is the chaos value at the n-th iteration; $scale$ = 25,000 is the scale factor to increase the precision of the chaos value; iv = 0.002 for the variation per iteration to provide dynamic shift; α = 2.0 as a factor controlling the contribution of the sine map to the rotation γ to add a fixed offset for dynamic stability. Fig. 3 illustrates the circuit design plotted with the Pennylane Quantum simulator.

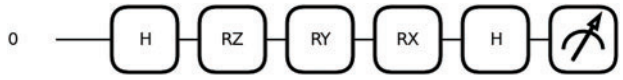

Figure 3: Quantum circuit design of SQQLSR

Based on the circuit plot in Fig. 3, the more detailed workings of the proposed quantum circuit are as follows:

1. Initial Hadamard gate: prepares the qubit in the initial superposition state, allowing the qubit to be in a linear combination of its basis states $(|0\rangle, |1\rangle)$
2. The first rotation about the Z-axis $(R_Z(\theta))$ is performed based on the scaled logistic map.
3. The second rotation about the Y-axis $(R_Y(\phi))$ is performed based on the sine map to provide additional dynamics.
4. The third rotation about the X-axis $(R_X(\gamma))$ is performed to maintain dynamic stability and provide additional offsets.
5. The End Hadamard Gate is used to bring the qubit back to the superposition basis to maximize quantum interference that reflects the overall dynamics of the system.
6. Pauli-Z measurement $\langle Z \rangle$ is the expectation of the Pauli-Z operator, which gives the chaos value at the current iteration, which becomes the input for the next iteration.

3.2 Proposed Image Encryption Method Using SQQLSR

The SQQLSR is used as a chaotic sequence generator as the primary key (S_1) of image encryption. This part has been explained in Section 3.1. The encryption design is relatively simple to show a more natural performance of SQQLSR. Fig. 4 illustrates the proposed image encryption method, while the more detailed steps are explained as follows:

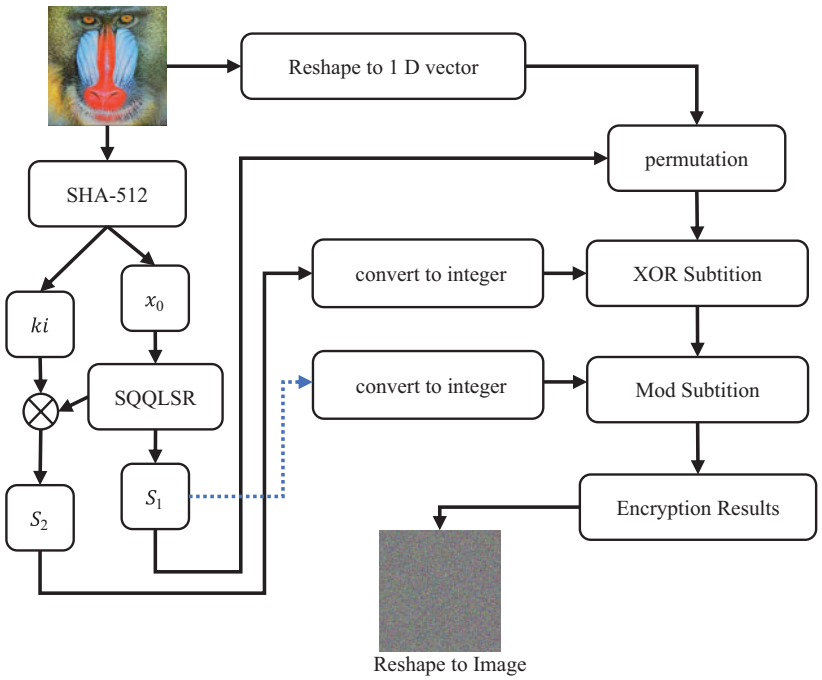

Figure 4: Proposed encryption scheme

3.2.1 Initialization and Key Generation

1. A plain image (I) with size $m \times n \times o$ is processed using the SHA-512 hashing method, resulting in a hash vector converted into a numeric ASCII value. From the ASCII hashing (h) results, get the initial seed (x_0) based on the standard deviation of the hash value $(x_0 = \sigma(h))$. To maintain the stability of the system, x_0 is divided gradually until its value is less than one, using Eq. (5). We also calculated the normalized parameter k_i based on the initial seed using Eq. (6).

$$\text{while } x_0 > 1, x_0 = \frac{x_0}{10} \tag{5}$$

$$k_i = \frac{1 - x_0}{100} \tag{6}$$

2. The chaotic sequence S_1 generated by SQQLSR using the initial seed x_0, then create a chaotic sequence S_2 by normalizing S_1 based on k_i. The normalization process is calculated by Eq. (7).

$$S_2 = \frac{S_1 - \min(S_1)}{\max(S_1) - \min(S_1)} + k_i \tag{7}$$

where S_1 is the original SQQLSR chaotic sequence; k_i is the adjustment parameter of image hashing, $\max(S_1)$ and $\min(S_1)$ each is the minimum and maximum value of S_1.

3. After obtaining two chaotic sequences S_1 and S_2, converted to integer form to simplify the substitution process, using Eq. (8).

$$\begin{aligned} S_{1\_\text{int}} &= \text{mod}\left(S_1 \cdot 10^8, 256\right) \\ S_{2\_\text{int}} &= \text{mod}\left(S_2 \cdot 10^8, 256\right) \end{aligned} \tag{8}$$

3.2.2 Encryption Stages

1. Stage 1: In this stage involves a sort permutation operation to shuffle the positions of image pixels. This step introduces a high level of randomness to the spatial distribution of pixel intensities, effectively obscuring the original image structure. The chaotic sequence S_1, generated using the proposed SQQLSR, serves as the basis for determining the new order of the pixels. The sorting index, denoted as sortIndex, is computed using Eq. (9).

$$\text{sortIndex} = \text{argsort}(S_1) \tag{9}$$

here, $\text{argsort}(S_1)$ generates an array of indices that sorts the elements of S_1 in ascending order. These indices are then used to rearrange the pixels of the original image I_{mno}. Next, I_{mno}. is reshaped into a one-dimensional vector I_z, where $z = m \times n \times o$ and z is the index of the vector. The pixel intensities in I_z are then permuted based on sortIndex to produce the first-stage encrypted image $E1_z$ using Eq. (10).

$$E1_z = \text{sortIndex}(I_z) \tag{10}$$

2. Stage 2: XOR Substitution is performed by XOR operation between the first stage encrypted image $E1_z$ and chaotic sequence S_{2_int}, see Eq. (11). This operation adds a layer of complexity by bitwise changing the pixel values.

$$E2_z = E1_z \oplus S_{2\_\text{int}} \tag{11}$$

3. Stage 3: The final stage is modulus substitution, where the chaotic sequence S_{1_int} is used to add a third layer of encryption to the encrypted image $E2_m$, see Eq. (12).

$$E3_z = \text{mod}\ (E2_z - S_{1\_\text{int}}, 256) \tag{12}$$

4. The $E3_z$ the encrypted image is reconstructed to its original dimensions $(m \times n \times o)$ using the reshape function to be visualized as a final encrypted image $E3_{mno}$.

3.2.3 Decryption Stages

1. Read the final encrypted image $E3_{mno}$, then reconstruct it into a one-dimensional vector form $E3_z$. Then perform the three stages decryption process using the reverse flow of the encryption stages as steps 2 until 4.
2. Stage 1: Perform modulus Substitution Inversion on $E3_z$ and S_{1_int}, to get a vector $D2_z$, using Eq. (13).

$$D2_z = \text{mod}\ (E3_z + S_{1\_\text{int}}, 256) \tag{13}$$

3. Stage 2: Perform XOR substitution inversion on $D2_z$ with S_{2_int} to obtain vector $D1_z$, using Eq. (14).

$$D1_z = D2_z \oplus S_{2\_\text{int}} \tag{14}$$

4. Stage 3: Restore the pixel position of $D1_z$ based on the inverse of the permutation index to obtain I'_z using Eq. (15).

$$I'_z = \text{sortIndex}(D1_z) \tag{15}$$

5. After three stages decryption, reconstructed I'_z to its original dimensions $(m \times n)$ using the reshape function to get as a final decrypted image I'_{mno}.

4 Results and Discussion

This section presents the results and analysis of the SQQLSR model, evaluated through comprehensive simulations. The experiments were conducted in a Python environment using Google Colab, utilizing the PennyLane quantum simulator to implement and test the chaotic properties of SQQLSR. The implementation leveraged PennyLane for quantum circuit simulations, NumPy for numerical computations, Matplotlib for visualization, and Pandas for data handling. OpenCV and PIL libraries were also employed for image preprocessing, encryption, and visualization. The proposed quantum chaotic system was examined using bifurcation diagrams, Lyapunov exponent analysis, trajectory plots, and phase-space representations to validate its capability to generate highly complex and unpredictable dynamics.

Section 4.1 provides an in-depth analysis of SQQLSR, including its parameter sensitivity, chaotic range, and key performance metrics, demonstrating its advantages over traditional chaotic maps. Meanwhile, Section 4.2 implements SQQLSR for image encryption, applying a simple three-layer scheme combining permutation and substitution techniques. This approach is intentionally designed to isolate and highlight the impact of SQQLSR on encryption performance rather than relying on a complex encryption algorithm. By focusing on the chaotic sequence generated by SQQLSR, the evaluation emphasizes its effectiveness in enhancing diffusion and confusion, ensuring robust security against statistical and differential attacks.

4.1 Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps (SQQLSR)

In this section, the results of the SQQLSR test are measured and analyzed using bifurcation diagrams, LE, and chaos trajectories. In addition, this section also aims to validate the hypothesis that the selection of parameters such as scaling factor, iteration variation, and rotation offset can expand the range of control parameters, increase sensitivity to initial conditions, and strengthen chaotic dynamics. In SQQLSR, apart from the parameter r, its value is specified. This aims to simplify the implementation process of SQQLSR. Although other parameters can also be changed, if necessary, there may be changes in the range of the parameter r. Figs. 5–7 show the results of the bifurcation diagram, LE, and its trajectories, respectively.

The simulation results of SQQLSR show excellent capability in generating complex and unpredictable chaotic dynamics. The bifurcation diagram (Fig. 5) shows a uniform distribution of variable x in the range $[-1, 1]$ without "blank windows" for Fig. 5a–c, indicating that SQQLSR successfully overcomes the weakness of the stability of traditional chaos maps. However, "blank windows" begin to appear in Fig. 5d, so our test is limited to 10^{24} although there is still a possibility of increasing it. This value has provided much greater flexibility than previous methods, ensuring the stability of chaotic dynamics without switching to the periodic zone.

Based on the observation in Fig. 6, the LE value shows a relatively stable increase along with a significant increase compared to the traditional chaos map at ≈0.7 and even better than advanced chaos maps such as CCE. The maximum LE value reaches 55.26503239483661, which is achieved at $r \approx 10^{24}$. This value is much higher than the average LE value. The chaotic trajectory graphs in Fig. 7 show a completely random and non-repeating pattern. At $r \approx 10^{24}$, it appears that the range is lower than the other three graphs. However, the resulting pattern appears to reflect complex chaotic dynamics. This pattern is consistent with the even distribution of bifurcation diagrams, confirming that SQQLSR can maintain randomness without stability zones even at high iterations.

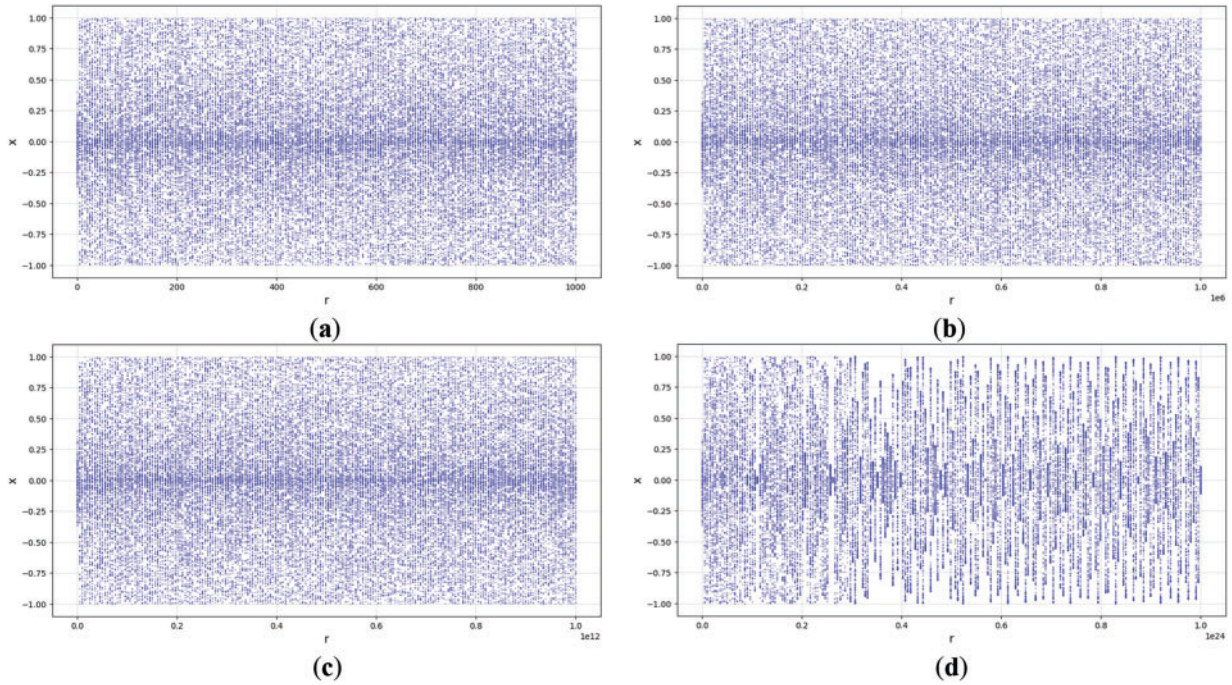

Figure 5: Bifurcation diagram of SQQLSR (**a**) $r \in [0, 1000]$; (**b**) $r \in [0, 10^6]$; (**c**) $r \in [0, 10^{12}]$; (**d**) $r \in [0, 10^{24}]$

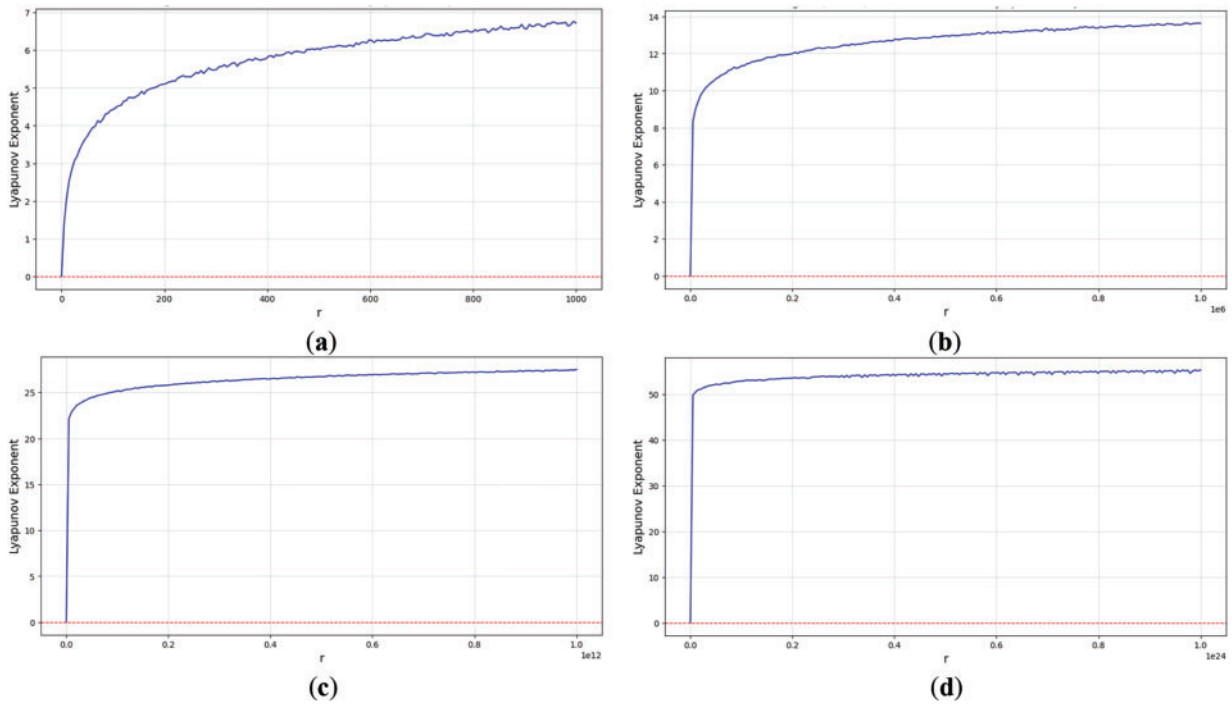

Figure 6: Lyapunov exponent of SQQLSR (**a**) $r \in [0, 1000]$ max LE = 6.767303907168853; (**b**) $r \in [0, 10^6]$ max LE = 13.646327485383424; (**c**) $r \in [0, 10^{12}]$ max LE = 27.532701815165996; (**d**) $r \in [0, 10^{24}]$ max LE = 55.26503239483661

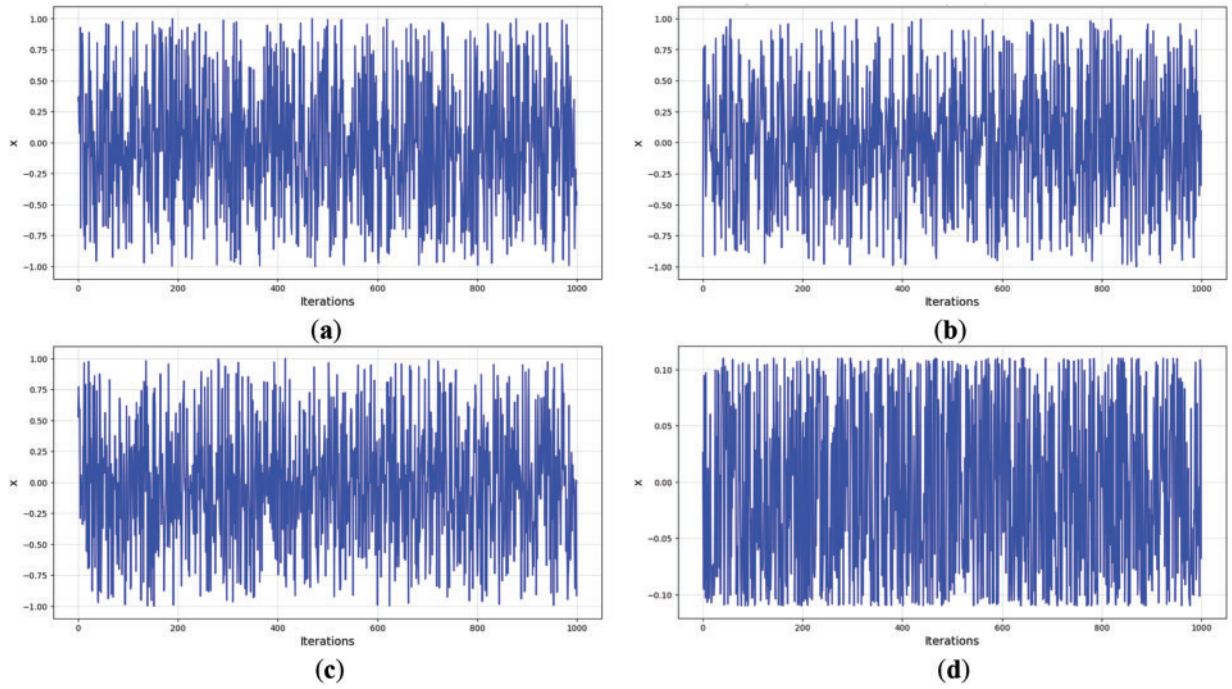

Figure 7: Trajectory diagram of SQQLSR (**a**) $r = 994.9748743718594$; (**b**) $r = 969849.2462311557$; (**c**) $r = 1000000000000.0$; (**d**) $r = 1000000000000000000000000.0$

The chaotic attractor diagram in Fig. 8 also confirms the superior chaotic dynamics of SQQLSR. The diagram presents a dense, non-repeating point distribution highlighting the system's ability to explore a wide range of state spaces. In Fig. 8a–c, the attractor maintains its density and complexity while avoiding periodic regions, thus ensuring robust and unpredictable dynamics. At $r \approx 10^{24}$, the attractor begins to show slight clustering in certain regions, as seen in Fig. 8d. This indicates that while the system maintains chaotic behavior, the very high parameter range can slightly reduce the uniformity of the state space coverage. Nevertheless, the attractor remains much more stable and wide-ranging compared to traditional chaotic systems, confirming the superiority of SQQLSR in extending chaotic dynamics.

The phase space diagrams of SQQLSR presented in Fig. 9 demonstrate strong chaotic behavior across an ultra-wide range of the control parameter r. The distribution of points remains highly irregular and densely populated, with no apparent periodic structures, indicating a robust chaotic system suitable for cryptographic applications. As r increases from $[0, 1000]$ to $[0, 10^{12}]$, the phase space maintains a homogeneous and fully dispersed pattern, signifying stable chaotic dynamics without degenerating into periodicity. At $r \in [0, 10^{24}]$, a subtle structural change is observed in the phase space, suggesting an evolution in the chaotic behavior as the system operates in extreme parameter conditions. However, despite this variation, the chaotic distribution remains widely spread and relatively non-repetitive, ensuring that the randomness, diffusion properties, and sensitivity to initial conditions remain intact. This further confirms that SQQLSR maintains its strong chaotic characteristics and security potential.

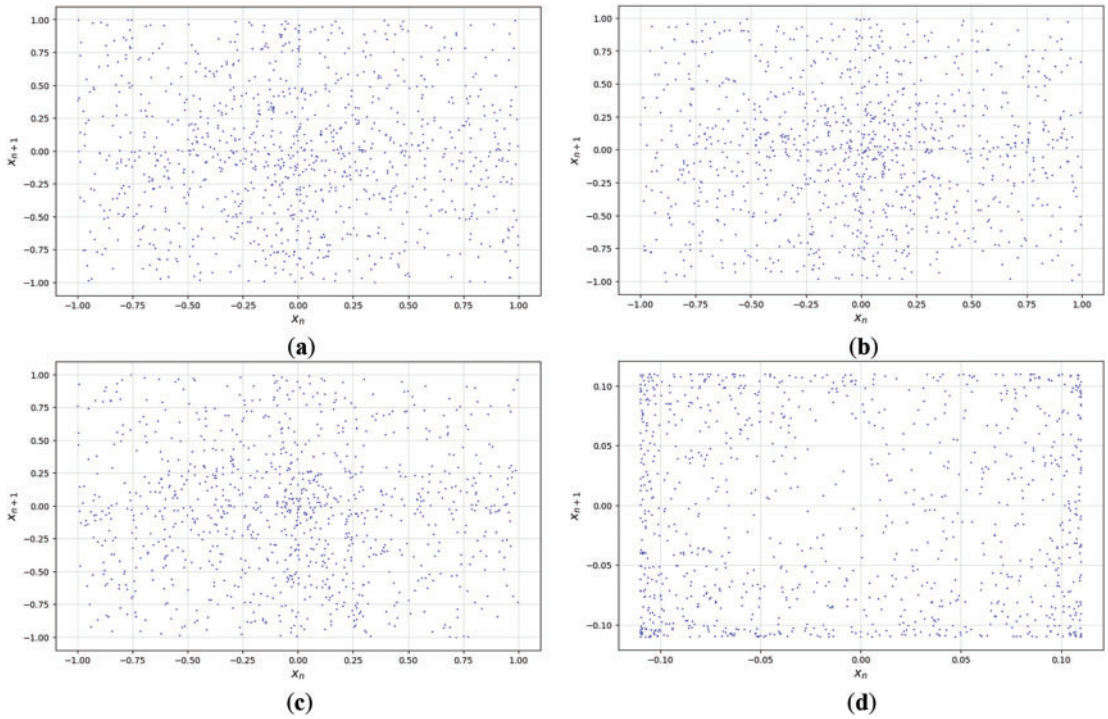

Figure 8: Chaotic attractor of SQQLSR (**a**) $r = 994.9748743718594$; (**b**) $r = 969849.2462311557$; (**c**) $r = 1000000000000.0$; (**d**) $r = 1000000000000000000000000.0$

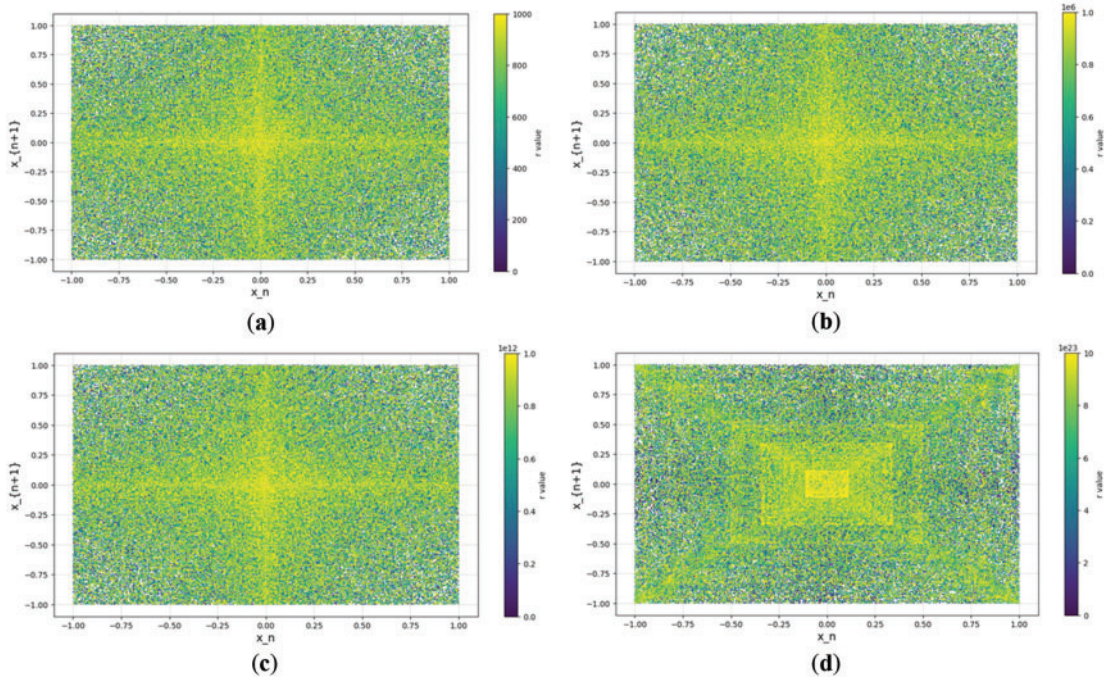

Figure 9: Phase space diagram of SQQLSR (**a**) $r \in [0, 1000]$; (**b**) $r \in [0, 10^6]$; (**c**) $r \in [0, 10^{12}]$; (**d**) $r \in [0, 10^{24}]$

The carefully designed parameter selection also supports this success. To determine optimal values, we conducted multiple experimental trials to evaluate the sensitivity of each parameter to chaotic behavior. In the graphs above, we used 1000 iterations (i) after testing different values to ensure stability. A scaling factor ($scale$) of 25,000 was necessary to enhance precision and maintain significant chaotic dynamics in the quantum domain. A higher $scale$ improves the resolution of chaotic behavior but can introduce numerical instability, whereas a lower $scale$ may weaken chaos, making the system more predictable. An iteration variation (iv) of 0.002 was chosen after observing its impact on bifurcation smoothness and overall system stability, where a large iv causes abrupt changes in chaotic states, while a smaller iv may reduce diversity in the system's evolution. The rotation offset ($\pi/3$) on R_X was found to be optimal in maintaining rotational stability; increasing it may introduce excessive transformation in state-space rotation while reducing it could lead to a weaker chaotic effect. Similarly, $\alpha = 2.0$ was selected to strengthen the contribution of the sine map, as a larger α amplifies the sine component in system dynamics, while a smaller value reduces its influence, making the system more dependent on other chaotic factors. Due to the high sensitivity of these parameters, careful tuning was essential, and the ultra-wide r further ensured large-scale chaos exploration. A larger r expands the key space but may introduce numerical instability, while a smaller r limits the system's unpredictability. These optimizations collectively make SQQLSR superior to both classical and previous quantum methods by balancing sensitivity, chaos enhancement, and numerical stability. Next, Table 1 explains the comparative performance of LE values, bifurcation range, range of r, and SQQLSR key spaces compared to other traditional chaos methods.

Table 1: Comparison of SQQLR and other chaotic method

Method	Max LE	Bifurcation range	Range of r	Keyspace
Logistic map	≈ 1.5	$[0,1]$	$[0,4]$	$\approx 4 \times 10^{16}$
Sine map	≈ 0.7	$[0,1]$	$[0,4]$	$\approx 4 \times 10^{16}$
Tent map	≈ 0.7	$[0,1]$	$[0,2]$	$\approx 2 \times 10^{16}$
PWLCM	≈ 0.7	$[0,1]$	$[0,2]$	$\approx 2 \times 10^{16}$
1D-CCE [34]	≈ 4.999	$[0,1]$	$[0,10]$	$\approx 10^{17}$
SQQLSR	≈ 55.265	$[-1,1]$	$[0,10^{24}]$	$\approx 10^{40}$

Table 1 highlights the superiority of SQQLSR over traditional chaotic maps in key aspects such as Lyapunov exponent (LE), bifurcation range, and key space size. SQQLSR exhibits a significantly higher LE ($\approx$55.265), indicating extreme sensitivity to initial conditions compared to classical methods, which typically have LE ≤ 1.5. Its bifurcation range $[-1, 1]$ is broader than conventional maps, suggesting enhanced chaotic behavior. Moreover, its key space ($\approx 10^{40}$) is orders of magnitude larger than classical methods, reinforcing its robustness against brute-force attacks. Overall, SQQLSR offers significant advantages regarding large key space, unpredictable randomness, and high sensitivity to initial conditions, making it a strong candidate for developing quantum-based security technologies.

4.2 Implementation SQQLSR for Image Encryption

In this section, we test SQQLSR with $r = 969849.2462311557$, this value was chosen because it has obtained a relatively very high LE value compared to traditional chaos and is relatively an intermediate value. The test was carried out on a standard image dataset with dimensions of 512×512 with a depth of 24 bits, presented in Fig. 10. All images can be downloaded from [38]. Furthermore, Fig. 11 also presents the encrypted image and its histogram. The results presented in Fig. 11 show good encryption results in terms

of visual results and histograms. However, visual assessment is a subjective assessment. Several standard matrices are used to measure image quality, presented in Sections 4.2.1–4.2.8.

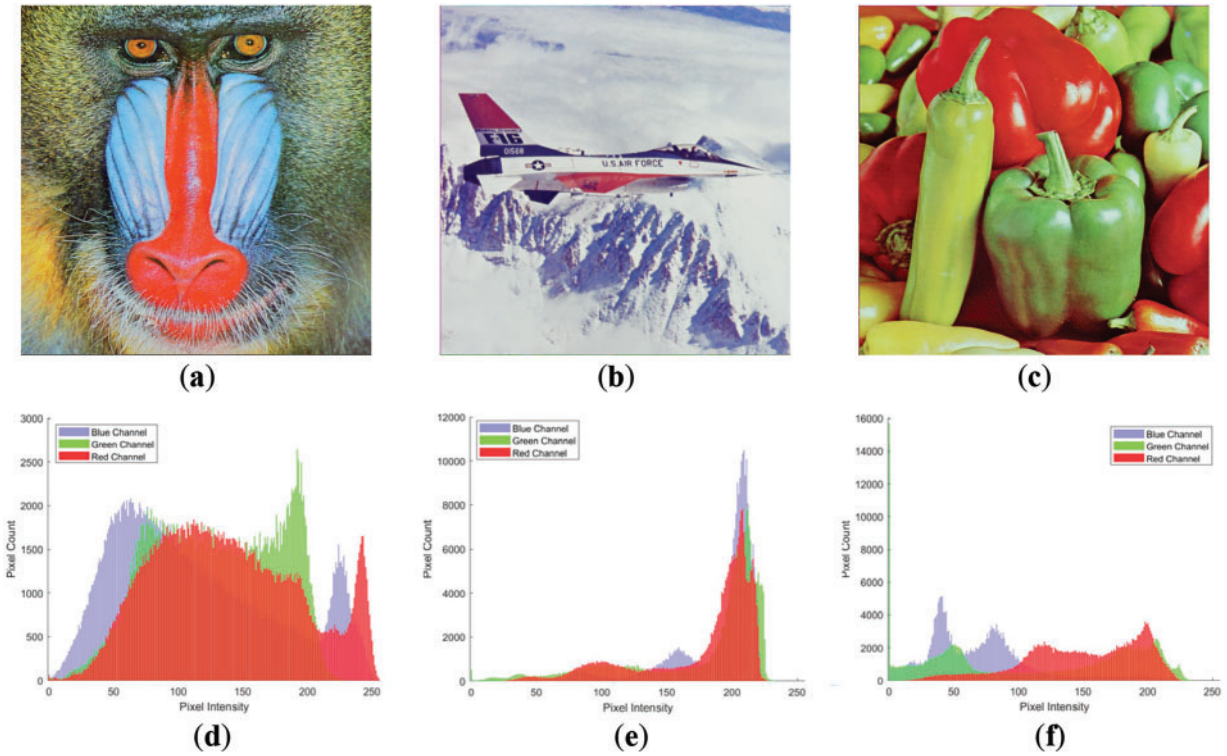

Figure 10: Standard image used (**a**) 4.2.03 Baboon; (**b**) 4.2.05; (**c**) 4.2.07 Peppers; (**d–f**) Corresponde Histogram

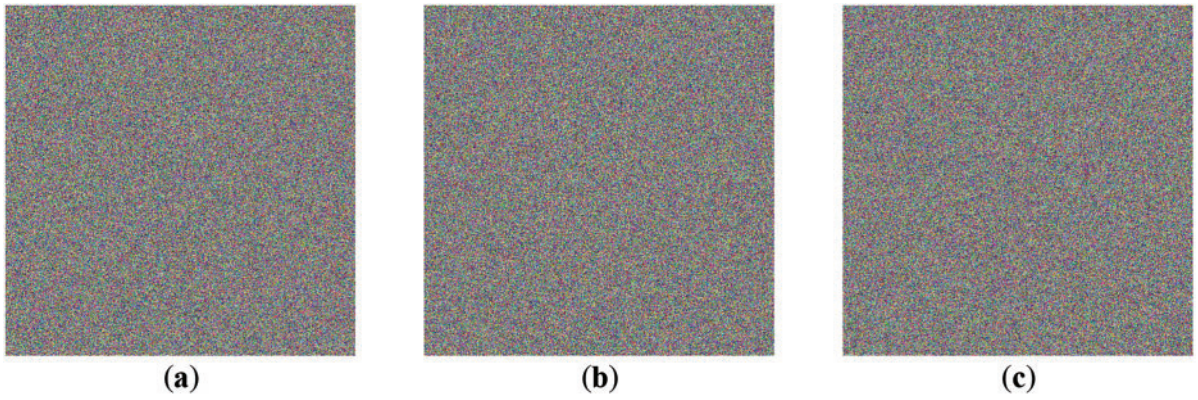

Figure 11: (Continued)

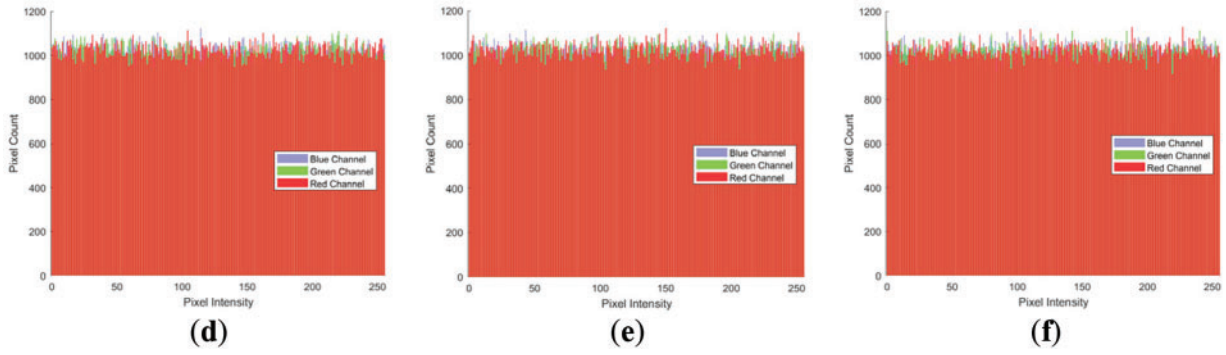

Figure 11: Encryption results (**a**) 4.2.03 Baboon; (**b**) 4.2.05; (**c**) 4.2.07 Peppers; (**d–f**) Corresponde Histogram

4.2.1 Chi-Square Analysis

In the context of chi-square analysis on images with a dimension of 512 × 512 pixels, it is important to understand that the ideal chi-square value results from a uniform distribution of pixel intensities after encryption. For grayscale images, the ideal distribution is that each intensity level has the same frequency. With a total of 512 × 512 = 262,144 pixels evenly distributed among 256 intensity levels, the ideal frequency (if) for each intensity level is 1024. Chi-square is calculated to evaluate the extent to which the actual distribution of pixel intensities approaches the ideal distribution, see Eq. (16).

$$X^2 = \sum_{i=1}^{256} \frac{(af_i - if)^2}{if} \tag{16}$$

where af is the actual frequency for intensity level i, if is 1024 in this case.

To evaluate whether the results are ideal, it is necessary to compare the calculated chi-square value with the critical value at a certain significance level. If the degrees of freedom are 255 and the significance level is 0.05, then the critical chi-square value is around 293.25. If the calculated chi-square value is smaller than this critical value, then the intensity distribution can be considered statistically uniform.

The chi-square calculation results in Table 2 show that all are below the critical value. This indicates that the pixel intensity has been distributed evenly, approaching the characteristics of a uniform distribution. In other words, the encryption algorithm has successfully hidden the original pattern of the image, ensuring security against statistical analysis.

Table 2: Chi-square results

Image	Red	Green	Blue	Average
4.2.03 Baboon	246.537	243.332	245.545	245.1380
4.2.05 Airplane	252.978	241.822	208.972	234.5906
4.2.07 Peppers	255.381	241.449	232.048	242.9593

4.2.2 Entropy Analysis

Entropy is an important metric to measure the randomness of the pixel intensity distribution in an encrypted image. The maximum entropy for an 8-bit digital image is calculated using Shannon information theory and is expressed in Eq. (17).

$$H(X) = -\sum_{i=0}^{255} p_i \log_2 (p_i) \tag{17}$$

where p_i is the probability of occurrence of the i-th intensity. The entropy value approaches the theoretical maximum value of 8 bits for an image with a uniform pixel distribution. The closer the entropy value is to 8, the more random the pixel distribution is, which reflects the effectiveness of the encryption algorithm in hiding the original image pattern.

The entropy values for global entropy calculations are presented in Table 3. The average entropy values across all color channels show high consistency, ranging from 7.9993 to 7.9994, which signifies a nearly ideal randomness level.

Table 3: Global entropy results

Image	Red	Green	Blue	Average
4.2.03 Baboon	7.9993	7.9993	7.9994	7.99933
4.2.05 Airplane	7.9993	7.9994	7.9994	7.99937
4.2.07 Peppers	7.9994	7.9993	7.9993	7.99933

The results in Table 3 indicate that the global entropy values approach the theoretical maximum, meaning that the pixel intensity distribution is highly randomized, making it challenging to extract any meaningful patterns.

To further assess the randomness across different image regions, a local Shannon entropy test was conducted using 120 randomly selected blocks, each containing 1936 pixels. This configuration was carefully adjusted based on the methodology outlined in [39]. The local entropy was computed for each block, and the min, max, and mean local entropy values were reported to evaluate localized randomness within the encrypted images comprehensively.

The local entropy values presented in Table 4 confirm a high level of randomness across different regions of the encrypted images. The mean entropy values for the red, green, and blue channels consistently range between 7.9014 and 7.9038, indicating a nearly uniform pixel intensity distribution across different color channels. The minimum entropy values exhibit slight variations, with the lowest recorded entropy being 7.8771 (Red-Airplane), while the maximum entropy values remain within a narrow range, peaking at 7.9295 (Blue-Airplane). These variations demonstrate localized differences in randomness, which are inherent in encryption processes but remain within an acceptable range. The consistency of minimum and maximum entropy values across different channels reinforces the robustness of the encryption scheme, ensuring that no discernible pattern exists within the encrypted images. This study provides a more detailed randomness assessment by complementing global entropy analysis with local entropy evaluation, further validating the encryption method's resilience against statistical attacks.

Table 4: Local entropy results

Image	Red			Green			Blue		
	Mean	Min	Max	Mean	Min	Max	Mean	Min	Max
4.2.03 Baboon	7.9022	7.8843	7.9241	7.9029	7.8823	7.9252	7.9038	7.8846	7.9268

(Continued)

Table 4 (continued)

Image	Red			Green			Blue		
	Mean	Min	Max	Mean	Min	Max	Mean	Min	Max
4.2.05 Airplane	7.9014	7.8771	7.9299	7.9035	7.8851	7.9211	7.9027	7.8759	7.9295
4.2.07 Peppers	7.9036	7.8876	7.9205	7.9038	7.8768	7.9287	7.9018	7.8780	7.9162

4.2.3 Correlation of Adjacent Pixel Analysis

Adjacent pixel correlation analysis is one of the important methods to evaluate the efficiency of encryption algorithms in eliminating the relationship between neighboring pixels. In the original image, adjacent pixels, either horizontally, vertically, or diagonally, tend to correlate highly due to consistent visual patterns. However, the correlation should be close to zero in an ideal encrypted image, indicating that the relationship between pixels has been wholly randomized [40]. The calculation of the correlation coefficient is done by randomly selecting 100,000 pairs of adjacent pixels from the image in three directions: horizontal (H), vertical (V), and diagonal (D). The correlation coefficient is calculated using Eq. (18).

$$\rho = \frac{cov\left(X, Y\right)}{\sqrt{var(X) \cdot var(Y)}} \tag{18}$$

where X and Y are the intensities of adjacent pixels; $cov\left(X, Y\right)$ is the covariance between X and Y; $var(X)$ and $var(Y)$ are the variances of X and Y, respectively. It is important to note that ρ values close to zero indicate a weak or no correlation, while values close to 1 or −1 indicate a strong correlation.

In the encrypted image, the correlation values in all three directions (H, V, and D) for each color channel are very close to zero, as shown in Table 5. The pixel correlation in the original image, shown in Fig. 12, appears to have a high value because it has a diagonal pattern of pixel intensity distribution. In contrast, the results in Fig. 13 for the encrypted image show an almost random intensity distribution without any clear pattern because all points are evenly distributed. These results highlight the algorithm's efficiency in creating a random intensity distribution, where the original visual relationships are entirely randomized, making them unrecognizable.

4.2.4 Differential Analysis

Differential analysis, including the measurement of the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI), is used to assess the sensitivity of the encryption algorithm to small changes in the original image, such as modifying a single pixel. NPCR on a grayscale image can be calculated by Eq. (19), while UACI is calculated by Eq. (20).

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D\left(i, j\right)}{M \times N} \times 100\% \tag{19}$$

$$\text{UACI} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1\left(i, j\right) - C_2\left(i, j\right)\right|}{255} \times 100\% \tag{20}$$

where $D\left(i, j\right)$ is a binary matrix defined as $D\left(i, j\right) = \begin{cases} 1 & \text{if } C_1\left(i, j\right) \neq C_2\left(i, j\right) \\ 0 & \text{if } C_1\left(i, j\right) = C_2\left(i, j\right) \end{cases}$; M and N is the image dimension; $C_1\left(i, j\right)$ and $C_2\left(i, j\right)$ is the pixel intensity at the position $\left(i, j\right)$, for the encrypted image before and after a 1-bit change of a pixel.

Table 5: Correlation of adjacent pixel analysis results

Image	Direction	Red	Green	Blue
4.2.03 Baboon	D	0.00127	−0.00284	0.00296
	H	0.00347	0.00130	0.00001
	V	−0.00293	0.00023	0.00075
4.2.05 Airplane	D	0.00354	−0.00165	−0.00393
	H	0.00168	0.00191	−0.00201
	V	−0.00289	−0.00651	−0.00198
4.2.07 Peppers	D	0.00223	0.00315	−0.00003
	H	0.00052	0.00112	0.00005
	V	−0.00359	0.00302	0.00155

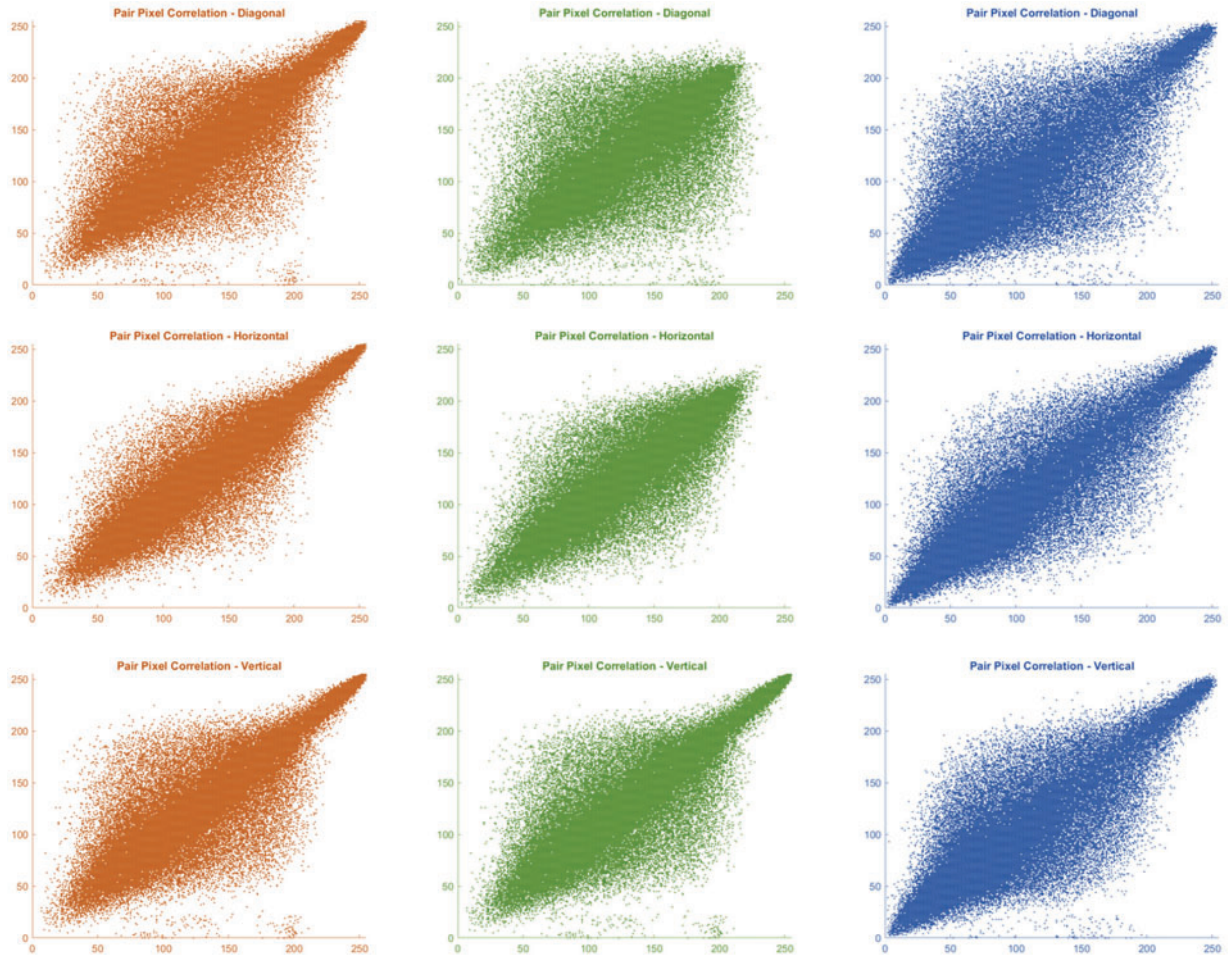

Figure 12: Plot of correlation analysis of original baboon image (column 1) red channel; (column 2) green channel; (column 3) blue channel

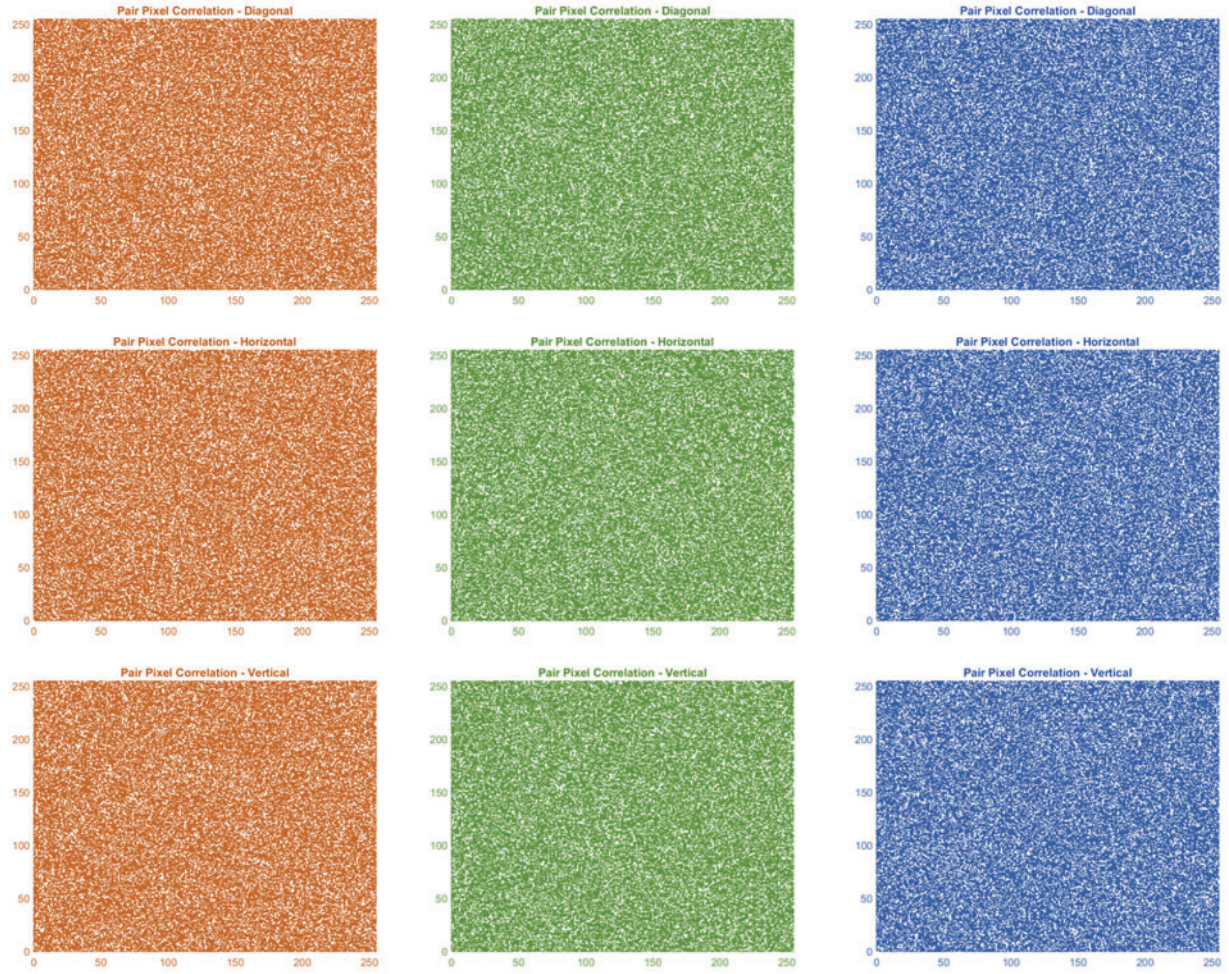

Figure 13: Plot of correlation analysis of encrypted baboon image (column 1) red channel; (column 2) green channel; (column 3) blue channel

The ideal value for NPCR comes from the assumption of a uniform random distribution, calculated from the probability that a pixel value changes after a slight change in the original image, which is $\approx 1 - \frac{1}{2^8} \approx$ 99.61%. The standard deviation of NPCR is usually tiny because the large total pixels reduce the influence of statistical noise. For an image with a size of 512 × 512 with a deviation of ±0.05%, the ideal NPCR range is 99.56% ≤ NPCR ≤ 99.66%. While the ideal UACI is ≈ 33.3% with an ideal deviation of ±0.5%, the ideal range of UACI is 32.8% ≤ UACI ≤ 33.8%.

The differential analysis results in Table 6 show that the NPCR values for all test images are within the ideal range. This confirms that the algorithm is susceptible to small changes in the original image, such as one-pixel modification, so the original pattern is difficult to recognize after encryption. Table 7 also shows the UACI results for all test images, with average values ranging from 33.2250% to 33.5503%. This value is within the ideal range of 32.8%–33.8%, indicating that the change in pixel intensity between two encrypted images due to slight modifications to the original image is close to a perfectly random distribution.

Table 6: NPCR results

Image	Red	Green	Blue	Average
4.2.03 Baboon	99.567	99.582	99.653	99.6007
4.2.05 Airplane	99.658	99.653	99.594	99.6350
4.2.07 Peppers	99.603	99.625	99.565	99.5977

Table 7: UACI results

Image	Red	Green	Blue	Average
4.2.03 Baboon	33.425	33.579	33.647	33.5503
4.2.05 Airplane	33.443	33.506	33.494	33.4810
4.2.07 Peppers	33.214	33.424	33.037	33.2250

4.2.5 Keyspace Analysis

A key space assessment is an important factor in determining the security provision of an encryption algorithm when subjected to brute force attacks. The larger key space guarantees that the algorithm will have a high level of resistance to exhaustive key-guessing attacks. In the proposed encryption algorithm, SQQLSR is used to produce chaotic sequences that assist in the key generation together with some key parameters that considerably broaden the key space as follows:

1. The initial seed is obtained from hashing the original image using the SHA-512 method. The hashing process produces a numerical vector of 512 bits (h) with 2^{512} possible combinations. Subsequently, x_0 s is calculated as the standard deviation of the hash values ($\sigma(h)$)and normalized to ensure $x_0 < 1$ through iteration (Eq. (5)). This process guarantees the uniqueness of the seed for each image and maintains system stability.
2. The adjustment parameter is calculated using Eq. (6), which introduces an additional layer of randomness based on the value of <1. Since the original image directly influences <1, k_i ensures each image generates a different key, enhancing security against correlation attacks.
3. The control parameter r varies between 0 and 10^{24}, providing broad flexibility in the chaotic dynamics. This ultra-wide range significantly expands the key space compared to classical chaotic maps, which typically have much narrower parameter ranges, such as [0, 4] or [0, 10].
4. The chaotic sequence SQQLSR generated by SQQLSR is normalized to produce S_2 (Eq. (7)). This normalization ensures that the chaotic values are distributed within a stable range. Subsequently, S_1 and S_2 are converted into integer forms using a modulo operation (Eq. (8)), adding a layer of randomness essential for substitution processes in encryption.

In conclusion, the estimated key space of the proposed algorithm incorporates contributions from several factors. First, the SHA-512 function provides a key space of 2^{512}. Second, the control parameter r, with a value range between 0 and 10^{24} and floating-point precision (10^{16}), offers a key space of approximately 10^{40}, providing additional flexibility. By combining all these factors, the total key space of the proposed algorithm reaches $2^{512} \times 10^{40}$.

4.2.6 Robustness Test

The robustness test is important in estimating the strength of cryptographic schemes against the totality of data attacks such as cropping/loss, noise addition, and compression. These tests imitate practical situations where the encrypted data is incomplete or is of lower quality than the intended one due to the loss sustained during transmission or storage. In this case, some areas of the encrypted image have been cut or masked to zero, emulating data loss. Following this, the strength of the decryption technique has been examined by inspecting the image built from the decryption process. As depicted in Fig. 14, two trimming forms were evaluated, namely, 200 × 200 and 400 × 400 cropping losses. The resilience being displayed connotes an extensive retention mechanism, and the algorithm can disperse the key information across the whole area of the image so that losing some data locally will not be detrimental to the utilization of the image. Noticeable degradation occurred with larger cropping sizes, demonstrating the limitations of extreme data loss. However, the object's shape in the image can still be recognized visually.

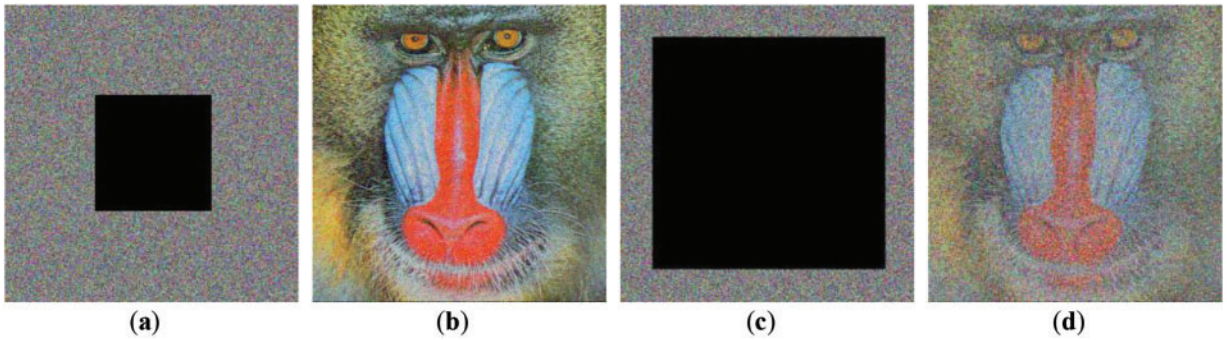

Figure 14: Robustness test under crop/loss attack (**a**) Encrypted image with loss 200 × 200 pixels; (**b**) Decrypted image after loss 200 × 200 pixels; (**c**) Encrypted image with loss 400 × 400 pixels; (**d**) Decrypted image after loss 400 × 400 pixels

In this case, the second robustness measure introduced salt and pepper noises of intensity equal to 0.05 and 0.1 to the already encrypted image. This form of noise model roughly simulates pixel errors that might happen to a pixel during its transmission or storage. The results, shown in Fig. 15, prove that the algorithm under consideration can properly process noisy data. The encryption algorithm has good noise immunity and can handle severe random damage. This strength also comes from the algorithm's parametrization, which is highly sensitive, and the use of non-linear chaotic mapping, which guarantees that the encryption does not depend on neighborhood pixel values.

Lastly, JPEG compression with quality settings of Q = 75 and Q = 50 were used in assessing the algorithm's performance concerning lossy compression. These values are intended to imitate actual situations in which images must be compressed to minimize the use of space in storage or bandwidth. As shown in Fig. 16, the algorithm performs well with lossy compression such as JPEG. The uninformation diffusion seems to be aided by the chaotic mapping within the image, which enables successful decryption even after a considerable amount of quality has been sacrificed.

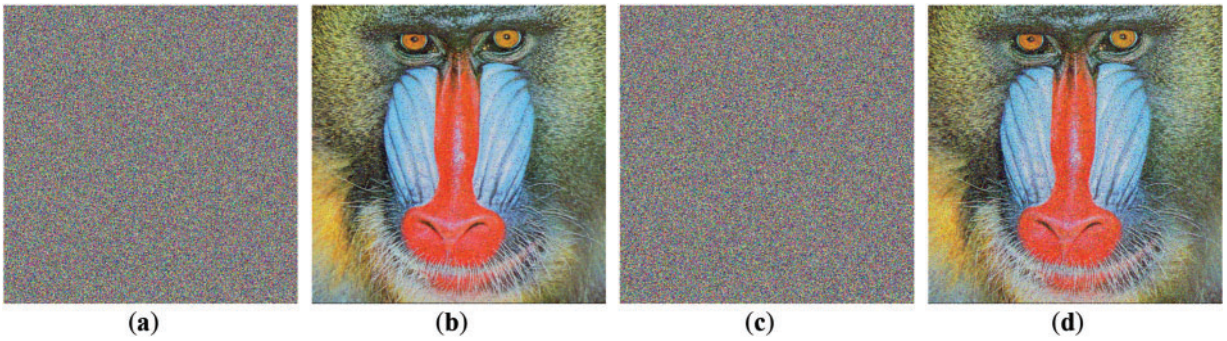

Figure 15: Robustness test under noise additional attack (**a**) Encrypted image under salt & pepper 0.05; (**b**) Decrypted image after salt & pepper 0.05; (**c**) Encrypted image under salt & pepper 0.1; (**d**) Decrypted image after loss salt & pepper 0.1

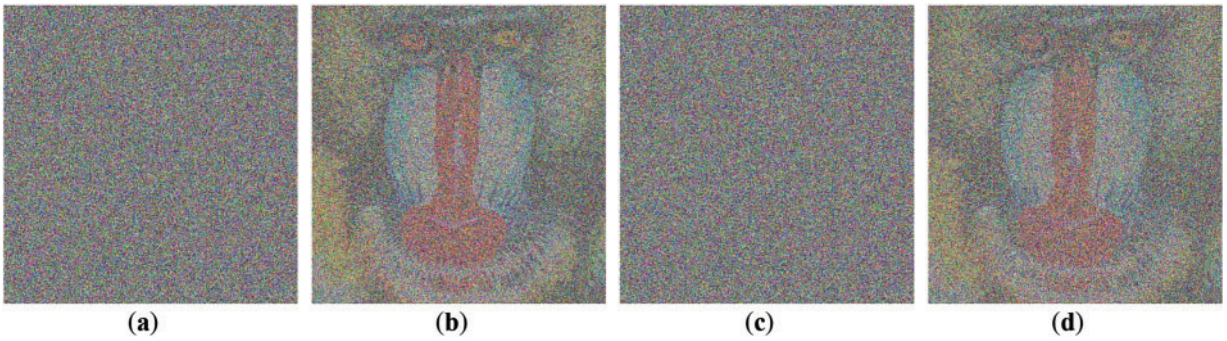

Figure 16: Robustness test under JPEG compression attack (**a**) Compressed using Q = 75; (**b**) Decrypted image after JPEG compression Q = 75; (**c**) Compressed using Q = 50; (**d**) Decrypted image after JPEG compression Q = 50

4.2.7 Decryption and Key Sensitivity Analysis

The ability of an encryption algorithm to perfectly decrypt an image is a key indicator of the reliability of the method used. Key sensitivity analysis is also important to evaluate the algorithm's security against small changes in the key or initial parameters. Fig. 17 shows that decryption with the correct key (Fig. 17b) results in a fully recovered image, while a tiny change in the initial seed (−0.00000001) results in an unrecognizable image (Fig. 17a). This confirms the high sensitivity of the algorithm to the key, thus preventing brute-force attacks or correlation-based key guessing. The decryption process with the correct key shows the peak signal-to-noise ratio (PSNR) value reaching infinity, proving that data integrity is maintained without any information loss. Thus, the SQQLSR algorithm offers high security through key sensitivity and guarantees perfect decryption when the correct key is used, making it highly reliable for image encryption applications.

4.2.8 Comparison with Related Work

Performance comparisons are performed using the same dataset as published papers. This allows for a fair and direct comparison of the effectiveness of the proposed encryption methods. In this study, the encryption method is designed with a simple approach so that the performance of SQQLSR can be seen more dominantly. This approach is deliberately carried out to focus on evaluating the randomness and complexity produced by SQQLSR so that in the future, this method is still open to further development that is more integrated with complex encryption systems. In Table 8, the comparison results using Peppers images show

that the NPCR value for the proposed method is very competitive with existing methods, even higher for some color channels, such as the green channel (99.625%). The UACI value of this method is slightly lower than some references but is still within the ideal range (32.8%–33.8%), indicating adequate sensitivity to small changes in the original image. Meanwhile, the proposed method appears relatively superior based on entropy and pixel correlation analysis.

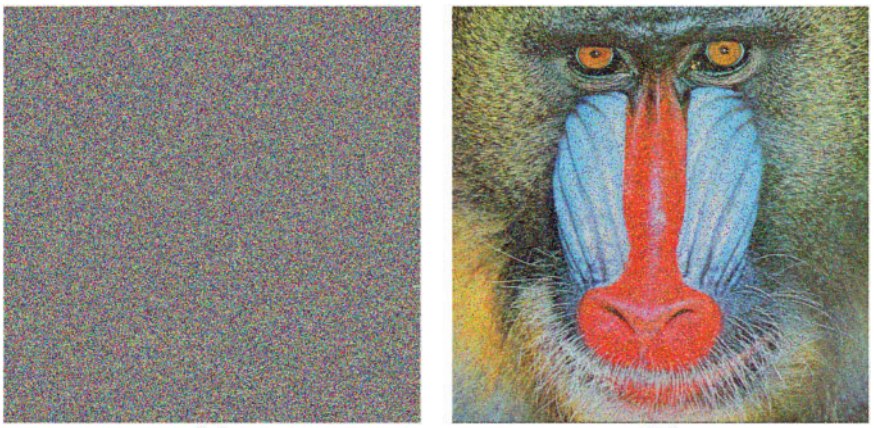

Figure 17: Decryption result (**a**) using a slight modification of initial seed (−0.00000001); (**b**) using the correct key

Table 8: Comparison of peppers image

Image	Ch	NPCR	UACI	Entropy	Correlation direction		
					Horizontal	Vertical	Diagonal
Ref. [41]	R	99.6090	33.4641	7.9993	−0.0323	0.0025	−0.0051
	G	99.6102	33.4580	7.9993	0.0408	−0.0020	−0.0001
	B	99.6093	33.4833	7.9993	0.0742	0.0772	0.0737
Ref. [42]	R	99.6043	33.4037	7.9971	−0.0052	−0.0001	−0.0013
	G	99.6022	33.4538	7.9973	−0.0045	0.0008	−0.0015
	B	99.6123	33.3678	7.9967	−0.0028	−0.0019	0.0001
Proposed	R	99.6030	33.214	7.9994	0.0005	−0.0036	0.0022
	G	99.6250	33.424	7.9993	0.0011	0.0030	0.0031
	B	99.5650	33.037	7.9993	0.0000	0.0015	−0.0000

In Table 9, we re-encrypt the baboon image and convert it to a grayscale image. The proposed method shows the highest NPCR result (99.621%), surpassing most other methods. The UACI value is also very competitive (33.434%), indicating that this method successfully produces significant intensity changes between pixels in the encrypted image. The entropy of the encrypted image also shows the most superior value. While the adjacent correlation also has outstanding results, competing with Ref. [32].

Table 9: Comparison of grayscale baboon image

Image	NPCR	UACI	Entropy	Correlation direction		
				Horizontal	Vertical	Diagonal
Ref. [43]	98.341	31.505	7.9849	–	–	–
Ref. [27]	99.702	33.134	7.9982	0.0055	−0.0317	0.0017
Ref. [29]	99.674	33.536	7.9991	–	–	–
Ref. [32]	99.614	–	7.9973	−0.0050	0.0001	0.0006
Proposed	99.621	33.434	7.9993	0.0034	−0.0000	−0.0020

Although the encryption method is relatively simple, the results are very competitive compared to previous methods. The proposed method performs better in some aspects, such as NPCR and entropy. This shows that SQQLSR has great potential for further development, not only as a randomness generator but also as a core part of more complex encryption methods in the future.

5 Conclusions

The proposed SQQLSR significantly advances 1D chaotic systems by integrating quantum principles such as superposition using Hadamard and quantum rotations. This study highlights how SQQLSR achieves ultra-wide chaotic dynamics, characterized by a broad bifurcation range without periodic windows, exceptional Lyapunov Exponent values reaching up to ≈55.265, and a significantly expanded keyspace. The ultra-wide range of the r control parameter alone provides a key space of up to 10^{40}, which is an incredible achievement in a chaotic system. These properties collectively ensure enhanced randomness, sensitivity to initial conditions, and resistance against brute-force attacks, making SQQLSR a robust and versatile chaotic map.

While the study includes image encryption as a proof-of-concept, the encryption method was deliberately kept simple to focus on showcasing SQQLSR's core capabilities. The evaluations, including metrics like NPCR, UACI, entropy, and robustness, demonstrate that even with this simplified approach, the system delivers competitive and, in some cases, superior performance compared to existing methods. These results affirm SQQLSR's potential as a foundational component for advanced cryptographic and security applications.

Although this study primarily focuses on image encryption, SQQLSR holds strong potential for broader cryptographic applications, particularly in lightweight encryption for IoT devices, secure communication protocols, and real-time key generation for quantum-based security frameworks. The ability of SQQLSR to operate on a single qubit while maintaining strong chaotic properties makes it an attractive choice for resource-constrained environments where computational efficiency is a critical factor. Additionally, the inherent unpredictability of SQQLSR's chaotic dynamics can be leveraged for key expansion techniques, secure authentication mechanisms, and random number generation, making it a viable candidate for next-generation security frameworks.

Given that our study uses Pennylane quantum simulators, we acknowledge that practical implementation on real quantum hardware presents additional challenges, such as gate fidelity, decoherence, and execution time constraints. Addressing these challenges will be a key focus of future research, where we plan to evaluate SQQLSR's performance on actual quantum processors and explore optimizations for hardware-specific noise resilience and efficient gate decompositions. Moreover, in-depth cryptanalysis is necessary to

assess SQQLSR's resistance to quantum attacks and side-channel vulnerabilities, ensuring its robustness in real-world cryptographic implementations.

In conclusion, SQQLSR lays the groundwork for future research into integrating quantum chaotic systems with more sophisticated cryptographic frameworks. Its adaptability and strong performance make it a promising tool for enhancing security in various domains, paving the way for further innovations in quantum and chaos-based technologies.

Acknowledgement: This research was supported by the Ministry of Higher Education, Science, and Technology (Kemdiktisaintek), Indonesia. The authors also express gratitude to those who provided administrative and technical assistance.

Funding Statement: This research was funded by Kementerian Pendidikan Tinggi, Sains, dan Teknologi (Kemdiktisaintek), Indonesia, grant numbers 108/E5/PG.02.00.PL/2024; 027/LL6/PB/AL.04/2024; and 061/A.38-04/UDN-09/VI/2024.

Author Contributions: Conceptualization: De Rosal Ignatius Moses Setiadi; Data curation: T. Sutojo; Formal analysis: Supriadi Rustad, Sudipta Kr Ghosal, and Minh T. Nguyen; Investigation: De Rosal Ignatius Moses Setiadi, Minh T. Nguyen, and Arnold Adimabua Ojugo; Methodology: De Rosal Ignatius Moses Setiadi; Project administration: Supriadi Rustad; Resources: Muhamad Akrom and T. Sutojo; Software: T. Sutojo and Muhamad Akrom; Supervision: De Rosal Ignatius Moses Setiadi; Validation: De Rosal Ignatius Moses Setiadi, Supriadi Rustad, and Muhamad Akrom; Visualization: T. Sutojo; Writing—original draft: De Rosal Ignatius Moses Setiadi; Writing—review & editing: De Rosal Ignatius Moses Setiadi, Supriadi Rustad, Minh T. Nguyen, and Arnold Adimabua Ojugo. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

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

References

1. Malik SK. Secure framework for cyber data. In: 2023 International Conference on Artificial Intelligence and Smart Communication (AISC); 2023 Jan 27–29; Greater Noida, India. p. 124–7.
2. Çetin A, Öztürk S. Comprehensive exploration of ensemble machine learning techniques for IoT cybersecurity across multi-class and binary classification tasks. J Future Artif Intell Technol. 2025;1(4):371–84. doi:10.62411/faith.3048-3719-51.
3. Kallapu B, Dodmane R, Krishnaraj Rao NS, Thota S, Sahu AK. Enhancing cloud communication security: a blockchain-powered framework with attribute-aware encryption. Electronics. 2023;12(18):3890. doi:10.3390/electronics12183890.
4. Alawida M, Sen TJ, Samsudin A, Alshoura WH. An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Process. 2019;164(1):249–66. doi:10.1016/j.sigpro.2019.06.013.
5. Liu Y, Qin Z, Liao X, Wu J. A chaotic image encryption scheme based on Hénon-Chebyshev modulation map and genetic operations. Int J Bifurc Chaos. 2020;30(6):2050090. doi:10.1142/S021812742050090X.
6. Teng L, Wang X, Xian Y. Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Inf Sci. 2022;605(6):71–85. doi:10.1016/j.ins.2022.05.032.
7. Winarno E, Nugroho K, Adi PW, Setiadi DRIM. Combined interleaved pattern to improve confusion-diffusion image encryption based on hyperchaotic system. IEEE Access. 2023;11:69005–21. doi:10.1109/ACCESS.2023.3285481.
8. Setiadi DRIM, Rijati N. An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations. Computation. 2023;11(9):178. doi:10.3390/computation11090178.

9. Setiadi DRIM, Robet R, Pribadi O, Widiono S, Sarker MK. Image encryption using half-inverted cascading chaos cipheration. J Comput Theor Appl. 2023;1(2):61–77. doi:10.33633/jcta.v1i2.9388.
10. Raghunandan KR, Dodmane R, Bhavya K, Rao NSK, Sahu AK. Chaotic-map based encryption for 3D point and 3D mesh fog data in edge computing. IEEE Access. 2023;11(10):3545–54. doi:10.1109/ACCESS.2022.3232461.
11. Tong XJ, Wang Z, Zhang M, Liu Y, Xu H, Ma J. An image encryption algorithm based on the perturbed high-dimensional chaotic map. Nonlinear Dyn. 2015;80(3):1493–508. doi:10.1007/s11071-015-1957-9.
12. 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.
13. Talhaoui MZ, Wang X. A new fractional one dimensional chaotic map and its application in high-speed image encryption. Inf Sci. 2021;550(2):13–26. doi:10.1016/j.ins.2020.10.048.
14. 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.
15. Han C. An image encryption algorithm based on modified logistic chaotic map. Optik. 2019;181(4):779–85. doi:10.1016/j.ijleo.2018.12.178.
16. Mansouri A, Wang X. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf Sci. 2020;520:46–62. doi:10.1016/j.ins.2020.02.008.
17. Hu Y, Wang X, Zhang L. 1D sine-map-coupling-logistic-map for 3D model encryption. Front Phys. 2022;10:1–15. doi:10.3389/fphy.2022.1006324.
18. 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.
19. Setiadi DRIM, Rijati N, Muslikh AR, Indriyono BV, Sambas A. Secure image communication using galois field, hyper 3D logistic map, and B92 quantum protocol. Comput Mater Contin. 2024;81(3):4435–63. doi:10.32604/cmc.2024.058478.
20. Morissa VSG, Setiadi DRIMS. Implementation of a mixed triple logistic map and the BB84 quantum key distribution for secure image communication. In: 2024 International Seminar on Application for Technology of Information and Communication; 2024 Sep 21–22; Semarang, Indonesia.
21. Kamran MI, Khan MA, Alsuhibany SA, Ghadi YY, Arshad A, Arif J, et al. A highly secured image encryption scheme using quantum walk and chaos. Comput Mater Contin. 2022;73(1):657–72. doi:10.32604/cmc.2022.028876.
22. Ho WW, Choi S. Exact emergent quantum state designs from quantum chaotic dynamics. Phys Rev Lett. 2022;128(6):060601. doi:10.1103/PhysRevLett.128.060601.
23. Choi J, Shaw AL, Madjarov IS, Xie X, Finkelstein R, Covey JP, et al. Preparing random states and benchmarking with many-body quantum chaos. Nature. 2023;613(7944):468–73. doi:10.1038/s41586-022-05442-1.
24. Yuan X, Zhou H, Cao Z, Ma X. Intrinsic randomness as a measure of quantum coherence. Phys Rev A. 2015;92(2):022124. doi:10.1103/PhysRevA.92.022124.
25. Mendoza BD, Lara DA, López-Aparicio J, Armendáriz G, López-Hernández L, Velázquez V, et al. Quantum chaos in time series of single photons as a superposition of wave and particle states. Photonics. 2021;8(8):326. doi:10.3390/photonics8080326.
26. Zhang J, Huo D. Image encryption algorithm based on quantum chaotic map and DNA coding. Multimed Tools Appl. 2019;78(11):15605–21. doi:10.1007/s11042-018-6973-6.
27. Wang Y, Chen L, Yu K, Gao Y, Ma Y. An image encryption scheme based on logistic quantum chaos. Entropy. 2022;24(2):1–22. doi:10.3390/e24020251.
28. Anitha R, Vijayalakshmi B. Image encryption using multi-scroll attractor and chaotic logistic map. Comput Mater Contin. 2022;72(2):3447–63. doi:10.32604/cmc.2022.021519.
29. Rehman MU. Quantum-enhanced chaotic image encryption: strengthening digital data security with 1-D sine-based chaotic maps and quantum coding. J King Saud Univ-Comput Inf Sci. 2024;36(3):101980. doi:10.1016/j.jksuci.2024.101980.
30. Wang S. Fast adaptive synchronization of discrete quantum chaotic maps. Results Phys. 2023;52(7):106833. doi:10.1016/j.rinp.2023.106833.

31. Rajan AA, Vetrian V. QMedShield: a novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud. J Mod Opt. 2024;71(13–15):524–42. doi:10.1080/09500340.2024.2436521.
32. Abd El-Latif AA, Abd-El-Atty B, Amin M, Iliyasu AM. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci Rep. 2020;10(1):1930. doi:10.1038/s41598-020-58636-w.
33. Alnajim AM, Abou-Bakr E, Alruwisan SS, Khan S, Elmanfaloty RA. Hybrid chaotic-based PRNG for secure cryptography applications. Appl Sci. 2023;13(13):7768. doi:10.3390/app13137768.
34. Ullah F, Faheem M, Hashmi MA, Bashir R, Khan AR. A Novel 1-dimensional cosine chaotic equation and digital image encryption technique. IEEE Access. 2024;12(4):118857–74. doi:10.1109/ACCESS.2024.3447889.
35. Akhshani A, Akhavan A, Mobaraki A, Lim SC, Hassan Z. Pseudo random number generator based on quantum chaotic map. Commun Nonlinear Sci Numer Simul. 2014;19(1):101–11. doi:10.1016/j.cnsns.2013.06.017.
36. Auzzi R, Baiguera S, De Luca GB, Legramandi A, Nardelli G, Zenoni N. Geometry of quantum complexity. Phys Rev D. 2021;103(10):106021. doi:10.1103/PhysRevD.103.106021.
37. Dalzell AM, Harrow AW, Koh DE, La Placa RL. How many qubits are needed for quantum computational supremacy? Quantum. 2020;4:264. doi:10.22331/q-2020-05-11-264.
38. USC Viterbi School of Engineering. SIPI Image Database [Internet]. [cited 2019 Mar 27]. Available from: http://sipi.usc.edu/database/.
39. Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan JP, Natarajan P. Local Shannon entropy measure with statistical tests for image randomness. Inf Sci. 2013;222:323–42. doi:10.1016/j.ins.2012.07.049.
40. Andono PN, Setiadi DRIM. Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption. IEEE Access. 2022;10:115143–56. doi:10.1109/ACCESS.2022.3218886.
41. Wen H, Zhang C, Chen P, Chen R, Xu J, Liao Y, et al. A quantum chaotic image cryptosystem and its application in IoT secure communication. IEEE Access. 2021;9:20481–92. doi:10.1109/ACCESS.2021.3054952.
42. AbdElHaleem SH, Abd-El-Hafiz SK, Radwan AG. A generalized framework for elliptic curves based PRNG and its utilization in image encryption. Sci Rep. 2022;12(1):1–16. doi:10.1038/s41598-022-17045-x.
43. Cheng G, Wang C, Xu C. A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing. Multimed Tools Appl. 2020;79(39–40):29243–63. doi:10.1007/s11042-020-09542-w.