



OPEN Quantum color image encryption using a novel 4D hyperchaotic Lorenz system and Fibonacci transform

Saba Inam¹✉, Shamsa Kanwal¹, Rehana Amir¹, Amel Ksibi² & Irum Matloob³

Satellite images are critical for ecological monitoring and national security; thus, protecting its integrity is imperative. Nonetheless, existing encryption methods struggle to balance robustness and efficiency. This paper proposes a novel quantum chaos-based image encryption scheme (QCIES) combining a 4D hyperchaotic Lorenz system (4D-HLS) and quantum Fibonacci transform (QFT) addressing these limitations. During the encryption process, we first used The Generalized Quantum Image Representation (GQIR) technique to transform a conventional color image into quantum data. Then, 4D-HLS generates complex, unpredictable keys through bifurcation and sensitivity to initial conditions. 4D-HLS complex dynamics coupled with quantum pixel reorganization provide unprecedented resistance against statistical and brute-force attacks. Additionally, QFT with a quantum adder randomly encrypts pixel locations, producing the final encrypted image. Performance evaluation was conducted using Python to analyze key metrics including histogram distribution, information entropy, and adjacent pixel correlation. Extensive security testing revealed QCIES robust performance, achieving near-ideal correlation coefficients (< 0.004), information entropy (> 7.999), NPCR (99.64%), UACI (33.56%) and massive key space $10^{140} \gg 2^{128}$. The achieved 10^{140} key space notably exceeds the 2^{128} NIST standard, while maintaining computational efficiency through optimized quantum circuit design. These innovations establish a new benchmark for satellite image transmission in critical infrastructure applications.

Keywords Quantum image encryption, Chaotic systems, Quantum circuits, Quantum adders, Fibonacci transformation, Security analysis

A multidisciplinary discipline of quantum mechanics and informatics, quantum information and computing has grown rapidly and produced amazing advancements in a number of fields, including quantum computers, quantum communication, and quantum cryptography¹. A subfield of quantum information called "quantum image processing" is focused on developing quantum protocols and methods for storing, extending, and recapturing visual data. Despite being in its upbringing, the discipline has so far made substantial advances to the processing of images, such as quantum image steganography and disambiguation², quantum image encryption³⁻⁵, and quantum image watermarking^{6,7}.

Image encryption is commonly used to conceal image data and carry out initial or post processing for safe storage and transportation. Its major purpose is to disrupt an organized real life image, which may drastically enhance image preservation. To address the dual challenges of encryption efficiency and security, researchers have developed diverse cryptographic approaches leveraging both classical and emerging paradigms. Chaotic systems remain a cornerstone of this field due to their inherent unpredictability^{8,9}, with recent advancements introducing memristor-based chaotic neurons^{10,11}. Complementary techniques such as DNA sequence operations^{12,13} and compressed sensing¹⁴ offer additional layers of security, while neural network-based methods^{11,15} demonstrate adaptive encryption capabilities. The field has also seen growing integration of quantum principles^{16,17} and hybrid approaches.

¹Department of Mathematical Sciences, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan.

²Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. ³Department of Software Engineering, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan. ✉email: saba.inam@fjwu.edu.pk

Cryptography, on the one hand, is a continuous process. Since demonstrating their disruptive predominance, quantum computers made an enormous mark on present time cryptosystems. One method for reducing the ultimatum caused by quantum computers is that they use Shannon's one-time password (OTP)¹⁸ encryption, which is scientifically unreservedly strong, indicating that there is no way to rupture it. An OTP's encryption and decryption are quite simple. A set of keys is shared between the encryption and decryption processes prior to encryption. Because each bit of the key can only be used once and the key length must match the message length, the encryption challenge becomes one of giving the sender and the recipient the shared secret in order to guarantee the OTP's unconditional security. Although, in person key exchange is a powerful technique, but that frequently falls short of user requirements, such as temporary and remote encryption operations. An isolated, immediate, and potentially unbreakable secure mechanism for sharing key is provided by quantum key distribution (QKD). Bennett and Brassard devised the first QKD protocol in 1984, which became known as the BB84 protocol¹⁹. Many researchers proceeded further to verify its theoretical safety^{20–23}.

Yin et al.²⁴ suggested an effective quantum digital signature method using quantum keys that are asymmetric acquired by a general hash and secret sharing. Furthermore, the author develops the first quantum security network that consolidates digital signatures, safe transmission and secret sharing. Through tests, author illustrates the advantages of this signature efficiency.

Chaos is a great encryption technique for uncertainty and dissemination because of its accessibility and productivity, high susceptibility to starting conditions, auto correlating rapid decrease, unpredictability and disorderly like properties., creating a revolutionary encryption technique. According to the theory, hyper-chaos is more likely to occur in chaotic high-dimensional systems.

Rossler²⁵ established the concept of hyper-chaos and put forth the hyperchaotic Rossler system. Because a hyperchaotic system²⁶ has more Lyapunov exponents and its dynamic behavior is harder to anticipate, it is more beneficial in safe communication as opposed to an all around chaotic system.

The field of chaos-based image encryption has evolved considerably in recent years, with numerous innovative algorithms emerging that exploit the unique advantages of chaotic systems for secure data protection^{27–32}.

Image encryption makes extensive use of the efficient scrambling effect of the Fibonacci transformation³³. It has a fatal fault, though, in that it is readily cracked after many attempts. The preparation techniques for various quantum image representations may vary. Numerous quantum image representation schemes had been suggested by researchers^{34,35}. In 2011, Le et al.³⁶ introduced the Flexible Representation of Quantum Images (FRQI) model. Zhang et al.³⁷ presented the A Novel Enhanced Quantum Representation (NEQR) model in 2013. Both methods combined color and location data into quantum superposed phases to represent visual data by utilizing the characteristics of quantum entanglement. In 2015, Jiang et al.³⁸ introduced Generalized Quantum Image Representation (GQIR) model, which overcame the limitation of previous models that could only represent images of fixed sizes and color depths, enabling the representation of images with any depth of color and size.

She-Xiang Jiang et al.³⁹ introduced a novel double quantum image representation (DNEQR) model capable of encoding two digital images simultaneously within a single quantum superposition state. In addition, they developed a new two-dimensional hyperchaotic system derived from sine and logistic maps, which demonstrates improved chaotic properties and a broader parameter range compared to conventional models.

El Latif AAA et al.⁴⁰ made major improvements to key space and algorithm enactment the same year. Even though several encryption algorithms, such as Fibonacci, Arnold and Hilbert scrambling⁴¹, are quite simple,^{42,43} used them on quantum circuits.

Jilong Cui et al.⁴⁴ proposed a quantum watermarking scheme that utilizes a novel enhanced quantum representation (NEQR) of images. Their method incorporates a space geometric transformation alongside Fibonacci scrambling to enhance the robustness and security of watermark embedding in the quantum domain.

Recently, Yan et al.⁴⁵ proposed quantum color image compression and encryption algorithm based on Fibonacci transform.

Using several effective encryption columns, Guohao Cui et al.⁴⁶ have proven adept at ciphering intricate quantum data. The calculation becomes more challenging due to the discrete Fourier transform and quantum walk. Despite that, these systems have drawbacks, including processing constraints and lack of long-term cryptanalysis due to their novelty. Being relatively new, quantum walk-based ciphers may have unexamined vulnerabilities (e.g., attacks exploiting symmetry in walks, or quantum backtracking).

To overcome the limitations of existing encryption methods such as insufficient robustness against quantum attacks and suboptimal efficiency for high-dimensional data, we propose a Quantum Chaos-Based Image Encryption Scheme (QCIES). QCIES utilizes a chaotic system for image encryption^{18,26,45}. The incorporation of chaos-based encryption offers several advantages, such as improved security, the capacity to decrease pixel correlation, and non-deterministic image production, thereby increasing resilience to various types of attacks. This marks a significant advancement developing quantum image encryption methods that are more reliable and secure.

For the first time, image encryption is achieved using a key set derived from the 4D-HLS⁴⁷, which is applied to both the intertwined color and correlate information. By merging quantum Fibonacci transform along an additional key for encryption generated by 4D-HLS, an operator for encryption is attained. The final encryption is then completed by applying this operator on the image that was encrypted in initial phase. Furthermore, image preparing steps such as Fibonacci perturbing and encryption of color values can be implemented using quantum circuits, indicating this method holds significant potential for practical implementation on quantum devices.

Cryptanalysis is essential for evaluating the robustness and practicality of image encryption schemes, as evidenced by recent studies exposing vulnerabilities in even advanced cryptographic systems. For instance, quantum chaotic maps combined with DNA coding were cryptanalyzed through chosen-plaintext attacks, revealing weak diffusion properties⁴⁸. In medical image encryption, high-speed scrambling and pixel-adaptive

diffusion methods were found susceptible to statistical attacks due to inadequate entropy preservation⁴⁹. Even structured approaches like Feistel networks with dynamic DNA encoding have been compromised when chaotic systems lack ergodicity⁵⁰, while 2D logistic-adjusted-sine maps were shown to degrade security under chosen-ciphertext attacks⁵¹. These findings underscore the necessity of rigorous cryptanalysis not only to identify weaknesses but also to guide the design of resilient systems. In this work, we validate the proposed QCES against these attack vectors, ensuring its resistance to known statistical, differential, and chosen-text attacks through formal security analysis, chaos-based key sensitivity tests, and comparative benchmarking with prior cryptanalyzed schemes.

The key contributions of this paper are summarized as follows:

- We propose the Quantum Chaos-Based Image Encryption Scheme (QCIES), integrating a 4D hyperchaotic Lorenz system (4D-HLS) with quantum Fibonacci transform (QFT). This combination enhances both security and computational efficiency, addressing limitations in existing quantum-chaotic encryption methods.
- Unlike conventional chaotic systems, our 4D-HLS generates highly unpredictable keystreams with improved Lyapunov exponents and entropy, significantly expanding the key space and resisting brute-force attacks.
- We introduce a two-phase encryption process that combines:

A hyperchaos-driven pixel permutation technique that completely disrupts spatial correlations in the image, eliminating structural patterns vulnerable to correlation analysis.

The Quantum Fibonacci Transform (QFT) applies nonlinear, quantum-inspired operations to alter pixel values at the bit-level, ensuring robust confusion properties.

- We prove that QCIES reduces computational complexity in quantum image encryption compared to classical methods

This article is structured as follows. 4D-HLS, quantum adder, quantum Fibonacci scrambling, and the improved quantum color image representation technique are all introduced in section “[Related work](#)”. The encryption and decryption process for images is described in section “[Workflow of encryption and decryption process](#)”. The suggested GQIR color image encryption scheme, which is based on the multidimensional chaotic system and an experimental analysis is presented in section “[Simulation experiment and analysis](#)”. A succinct conclusion is presented in section “[Conclusion](#)”.

Related work

Herein, we first present the 4D hyperchaotic Lorenz system (4D-HLS) that serves as the chaotic foundation of QCIES. We then introduce the generalized quantum image representation (GQIR) framework for encoding color images, followed by the quantum Fibonacci transform (QFT) and its quantum adder implementation for secure pixel diffusion.

4D-HLS

Chaotic phenomena are deterministic but display stochastic-like behavior in nonlinear dynamical structures, which are very sensitive to initial circumstances, acyclic, and non-convergent. 4D-HLS, which adds a fourth dimension while maintaining the chaotic dynamics, is based on the 3D Lorenz system⁴⁷. The system is specified by the following Eq. (1)

$$\begin{cases} \frac{dx}{dt} = \alpha(-x + y) + w, \\ \frac{dy}{dt} = \alpha(-x + y) + w, \\ \frac{dz}{dt} = xy - \beta z, \\ \frac{dw}{dt} = rw - yz, \end{cases} \quad (1)$$

At least two positive Lyapunov exponents and at least one four-dimensional phase space are requirements for hyperchaotic systems^{52,53}. Wang’s method⁵⁴ states that when starting parameters are set to $\alpha = 10, \beta = 8/3, \gamma = 28$, and $-1.52 \leq r < -0.06$ (the control parameters are defined in Eq. 1), the system behaves in a hyperchaotic manner. Additionally, there is complete flexibility in the beginning values for x, y, z , and w . Figure 1 illustrates the Runge–Kutta method and Python software used to discretize 4D-HLS. The control parameter is $r = -1$. The system’s Lyapunov exponents are $\lambda_1 = 0.3381, \lambda_2 = 0.1586, \lambda_3 = 0$, and $\lambda_4 = -15.1752$, proving hyperchaos.

Quantum color image representation of GQIR

Quantum image processing leverages fundamental quantum principles such as quantum parallelism and quantum entanglement to optimize image storage, improve processing speed, enhance the security of information transmission and the efficiency of computing resources. As an improvement over the Novel Enhanced Quantum Representation (NEQR) model, we use Jiang Nan’s Generalized Quantum Image Representation (GQIR) technique in this work, which enables more efficient quantum image representation by utilizing entangled quantum sequences. GQIR allows for the scaling of image size from $2^n \times 2^n$ to arbitrary dimensions of $H \times W$, where H represents the image’s height and W its width. For an image of size $H \times W$, each color channel has a value of $[0, 2^{d-1}]$, where d is the RGB’s channel color depth, the quantum state representation of GQIR image is defined accordingly:

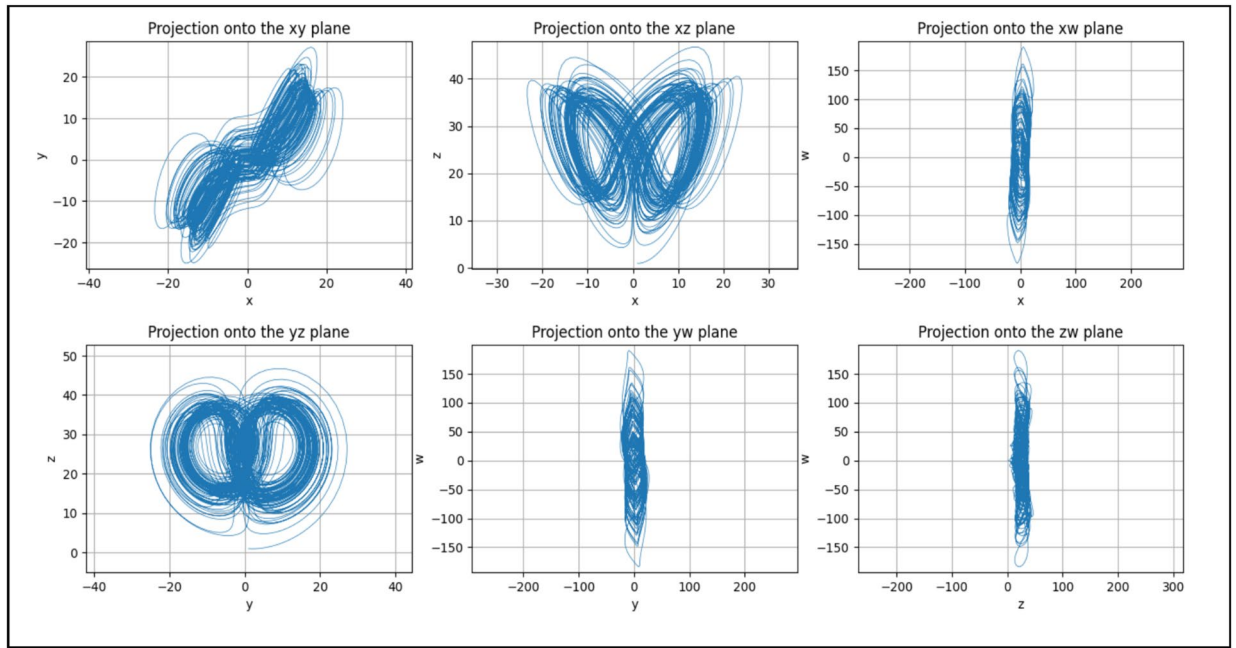


Fig. 1. Lorenz attractor projection with the parameter set to $r = -1$. **(a)** $x - y$ plane. **(b)** $x - z$ plane. **(c)** $x - w$ plane. **(d)** $y - z$ plane. **(e)** $y - w$ plane. **(f)** $z - w$ plane.

$$|\psi\rangle = \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |C_{YX}^j\rangle |YX\rangle. \tag{2}$$

where $|YX\rangle$ demonstrates coordinate information and $|C_{YX}^j\rangle$ demonstrates color information. The bits of $|C_{YX}^j\rangle$ are equally divided into three parts: $|R\rangle |G\rangle |B\rangle$, representing the R, G, and B channels of the quantum color image, respectively. $|YX\rangle$ and $|C_{YX}^j\rangle$ are shown in Eq. (3).

$$\begin{aligned} |YX\rangle &= |Y\rangle |X\rangle = |y_0 y_1 y_2 \dots y_{h-1}\rangle |x_0 x_1 x_2 \dots x_{w-1}\rangle, \\ |C_{YX}^j\rangle &= |R_{YX}^0 \dots R_{YX}^{d-1}\rangle |G_{YX}^0 \dots G_{YX}^{d-1}\rangle |B_{YX}^0 \dots B_{YX}^{d-1}\rangle. \end{aligned} \tag{3}$$

where $j = 0, 1, \dots, d - 1$ & $y_j, x_j \in \{0, 1\}$. Equation (4) can be used to formulate the values of h and w .

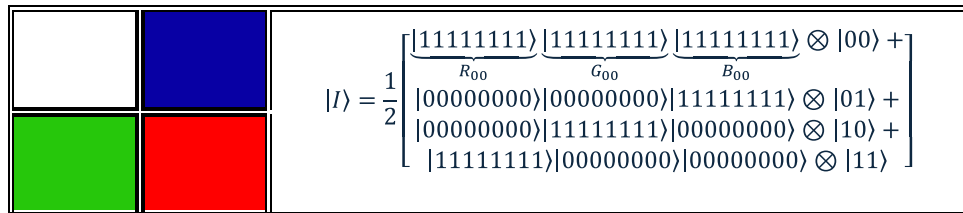
$$\begin{aligned} h &= \begin{cases} \lceil \log_2 H \rceil, & H > 1 \\ 1, & H = 1 \end{cases} \\ w &= \begin{cases} \lceil \log_2 W \rceil, & W > 1 \\ 1, & W = 1 \end{cases} \end{aligned} \tag{4}$$

Quantum representation can drastically cut down on the amount of storage space needed for color images as compared to traditional techniques. For a color image of size $2^n \times 2^n$, the classical image representation requires $8 \times 2^n \times 2^n + n^2$ bits. In contrast, quantum image representation requires $2n + 3d$ quantum bits where d is the quantity of bits required for each channel representation, so image's color depth is represented by $d + d + d$ quantum bits, and coordinate data Y and X of image stored with $2n$ quantum bits consecutively. Then, $\log_2 H + \log_2 W + d$ qubits are finally required for an image in quantum state of a GQIR's color model. GQIR's color imitation and its associated quantum representation with the range size $[0, 2^{8-1}]$, $n = 1$ and $q = 8$ are used to illustrate a 2×2 image in Fig. 2.

With quantum mechanical measurement theory³⁶, using measurement operator \hat{L} we may find the image in the quantum state $|\psi\rangle$. \hat{L} represents the position of the measurement operator in a quantum state as shown in Eq. (5).

$$\hat{L} = \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |YX\rangle \langle YX| I^{\otimes q}. \tag{5}$$

where q is the identity matrix used for color data on each pixel and $I^{\otimes q}$ is the tensor product of identity matrix. The color information measurement operator \hat{C} is shown in Eq. (6).



$$|I\rangle = \frac{1}{2} \left[\begin{array}{l} \underbrace{|1111111\rangle}_{R_{00}} \underbrace{|1111111\rangle}_{G_{00}} \underbrace{|1111111\rangle}_{B_{00}} \otimes |00\rangle + \\ |0000000\rangle |0000000\rangle |1111111\rangle \otimes |01\rangle + \\ |0000000\rangle |1111111\rangle |0000000\rangle \otimes |10\rangle + \\ |1111111\rangle |0000000\rangle |0000000\rangle \otimes |11\rangle \end{array} \right]$$

Fig. 2. A quantum representation of 2×2 size of GQIR color image.

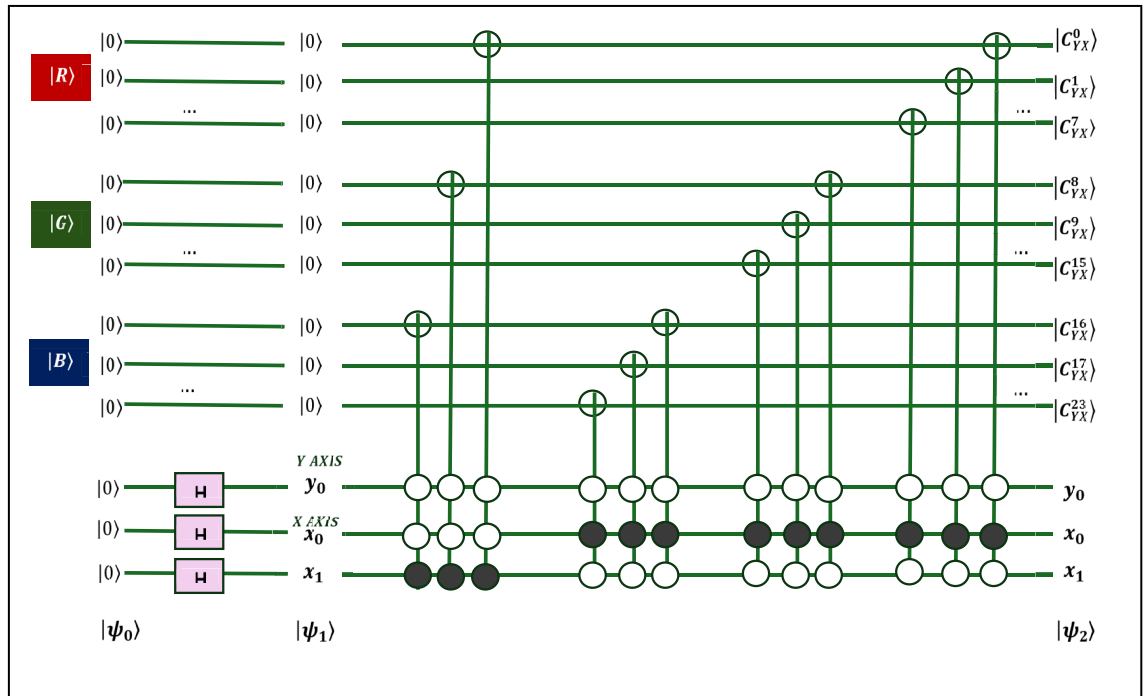


Fig. 3. Quantum circuit of 2×2 size of GQIR color image.

$$\hat{C} = \sum_{c'=0}^{2^q-1} C |c'\rangle \langle c'|. \tag{6}$$

The eigenvalues of C are denoted by c' . Accurate observation of the image’s information is possible once the operator has been applied to the quantum image. The GQIR color image’s quantum circuit is shown in Fig. 3.

Fibonacci transformation (FT)

The Fibonacci Transform (FT) scrambles image pixels depending on Fibonacci sequence. The image uses Fibonacci matrix to disorder its own pixel coordinates’ position ordering in order to finish the shuffling process. The image that will be encrypted is labeled as $I(x, y)$, and its dimensions are $2^n \times 2^n$. Equation (7) provides a definition of the FT.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{2^n}, \quad x, y = 0, 1, \dots, 2^n. \tag{7}$$

The generalized form of FT is shown in Eq. (8).

$$\begin{cases} x' = (x + ay) \pmod{2^n}, \\ y' = (bx) \pmod{2^n}, \end{cases} \tag{8}$$

The output (x', y') represents the scrambled coordinates of x and y . The inverse FT is generated by reversing the FT. The inverse of classical FT is shown in Eq. (9).

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & a \\ b & -1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ mod } 2^n, \quad x, y = 0, 1, \dots, 2^n. \tag{9}$$

The inverse of generalized FT is shown in Eq. (10).

$$\begin{cases} x = (ay') \text{ mod } 2^n, \\ y = (bx' - y') \text{ mod } 2^n, \end{cases} \tag{10}$$

Quantum adder

Quantum circuits’ reversibility¹⁷ enables the implementation of complex computations. The quantum ADDER, that combines the data kept in 2 quantum registers, is one of them. Equation (11) illustrates how the quantum ADDER functions if the 2 quantum registers are $|x\rangle$ and $|y\rangle$.

$$|x, y\rangle \rightarrow |x, x + y\rangle. \tag{11}$$

The calculated sum of two additive values x and y are reserved in the original y location. When adding negative values, it’s appropriate to use same ADDER because binary negative figures are represented in an additive manner. The image becomes non-rectangular and goes beyond the scope after passing the adder. With a particular implementation technique, the adder network depicted in Fig. 4 should be used to create the quantum modular N ¹⁷ adder. Equation (12) is used to determine the quantum ADDER with modulus N .

$$|x, y\rangle \rightarrow |x, (x + y) \text{ mod } N\rangle. \tag{12}$$

Quantum fibonacci transform (QFT)

We require a quantum adder-mod 2^n module in order to transform FT to the Quantum Fibonacci transform (QFT) and work with quantum images. QFT and its inverse are shown in Eqs. (13) and (14).

$$\begin{cases} |x'\rangle = |(x + ay) \text{ mod } 2^n\rangle, \\ |y'\rangle = |(x + ay) \text{ mod } 2^n\rangle, \end{cases} \tag{13}$$

$$\begin{cases} |x\rangle = |(ay') \text{ mod } 2^n\rangle, \\ |y\rangle = |(bx' - y') \text{ mod } 2^n\rangle, \end{cases} \tag{14}$$

A quantum adder is being utilized in methodology of QFT of image position data. The FT used for pixel shuffling of image. Table 1 provides definitions for the classical, generalized and quantum form of FT, and the inverse forms that correspond to it. The components $x, y, x', y' \in 0, 1, \dots, 2^n$, (x, y) represents the pixel position of the original image, while x', y' corresponds to the scrambled one, a and b are two positive integers, and $2^n \times 2^n$ is the size of the original image.

Workflow of encryption and decryption process

This work presents QCIES, an advanced multi-image encryption algorithm that synergistically combines the robust chaotic behavior of 4D-HLS with quantum-inspired Fibonacci transformations to achieve superior security and performance characteristics. To protect images, the recommended QCIES consists of several key stages. A plain image is first converted to a quantum image. 4D-HLS is then used to create the keys. In order to do diffusion, the received information from the quantum image and the color operator created using two of the generating keys are subjected to an XOR operation. An intermediate cipher image is created concurrently. Secret keys are also used in the quantum Fibonacci transform to increase security. An encrypted image with a robust resistance against unauthorized access is produced by the exacting process. Figure 5 illustrates the workflow of

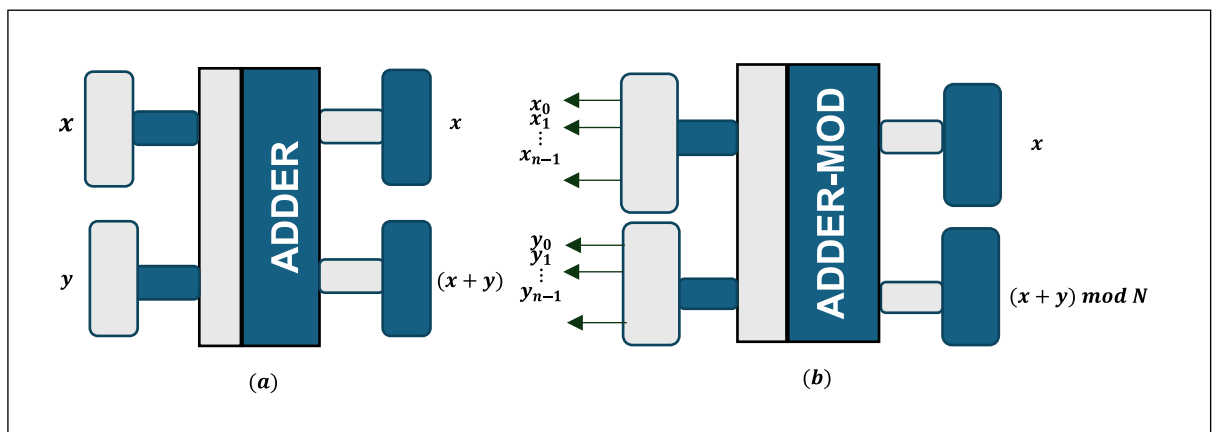


Fig. 4. (a) Quantum ADDER. (b) Quantum ADDER-MOD.

Classical FT	Classical inverse FT
$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{2^n}$	$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & a \\ b & -1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \pmod{2^n}$
Generalized FT	Generalized Inverse FT
$x' = (x + ay) \pmod{2^n}$ $y' = (bx) \pmod{2^n}$	$x = (ay') \pmod{2^n}$ $y = (bx' - y') \pmod{2^n}$
QFT	Inverse QFT
$ x'\rangle = (x + ay) \pmod{2^n}\rangle$ $ y'\rangle = (bx) \pmod{2^n}\rangle$	$ x\rangle = (ay') \pmod{2^n}\rangle$ $ y\rangle = (bx' - y') \pmod{2^n}\rangle$

Table 1. Classical Generalized and QFT.

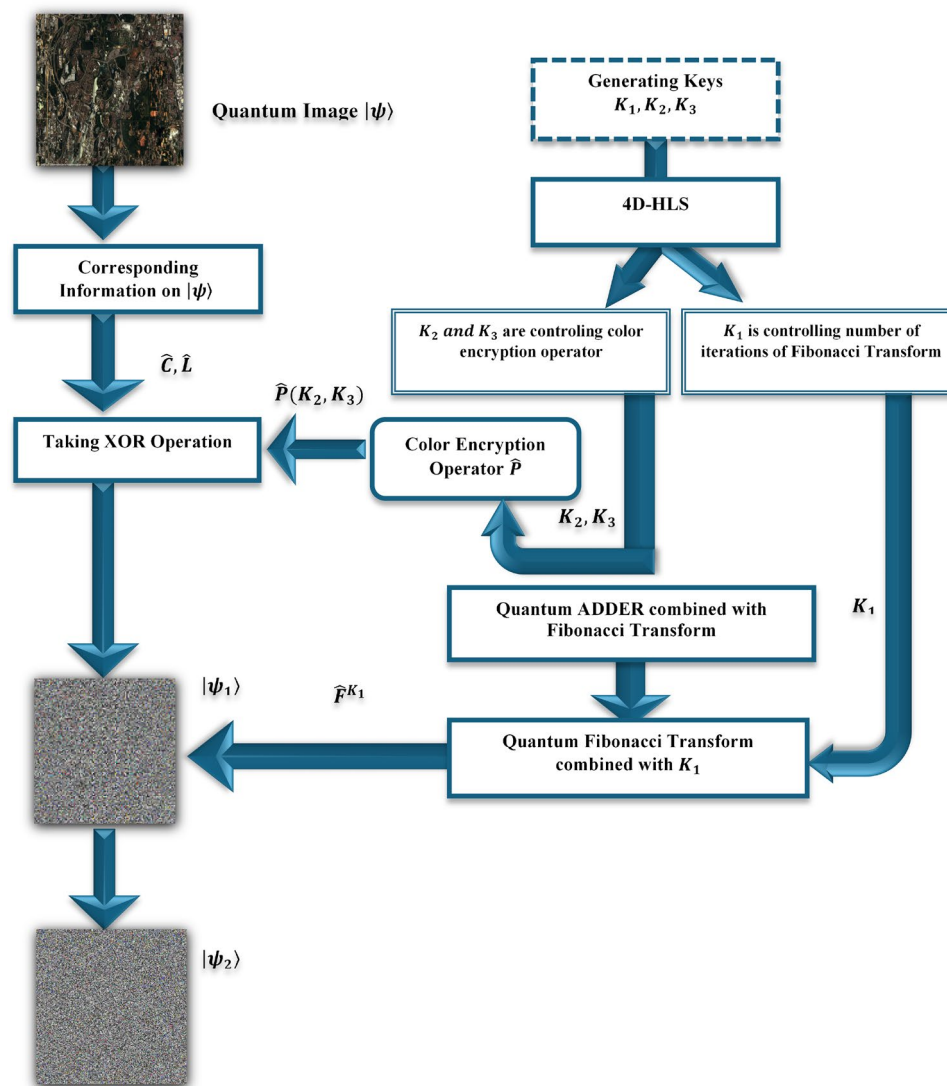


Fig. 5. Encryption process of quantum color image.

our recommended QCIES. The decryption procedure of QCIES is shown in Fig. 6, which outlines the process to reverse the encryption to recover the original satellite image.

Encryption procedure

This section explains the encryption process of 4D-HLS based QCIES. The proposed encryption algorithm consists of four main stages: quantum image conversion, extracting parameters, diffusion, and scrambling. The following is a list of the measures that were taken in this investigation.

1. A plain RGB image of dimensions $H \times W$ is selected, where H and W denotes height and width of image respectively.

2. Encryption Stage 1: Convert to Quantum State

The first phase in retaining the global dimensional properties of the original image is to turn it into a quantum image using the GQIR method. The quantum representation of color image using GQIR could be defined accordingly:

$$|\psi\rangle = \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^0 \dots R_{YX}^{d-1}\rangle |G_{YX}^0 \dots G_{YX}^{d-1}\rangle |B_{YX}^0 \dots B_{YX}^{d-1}\rangle |YX\rangle. \quad (15)$$

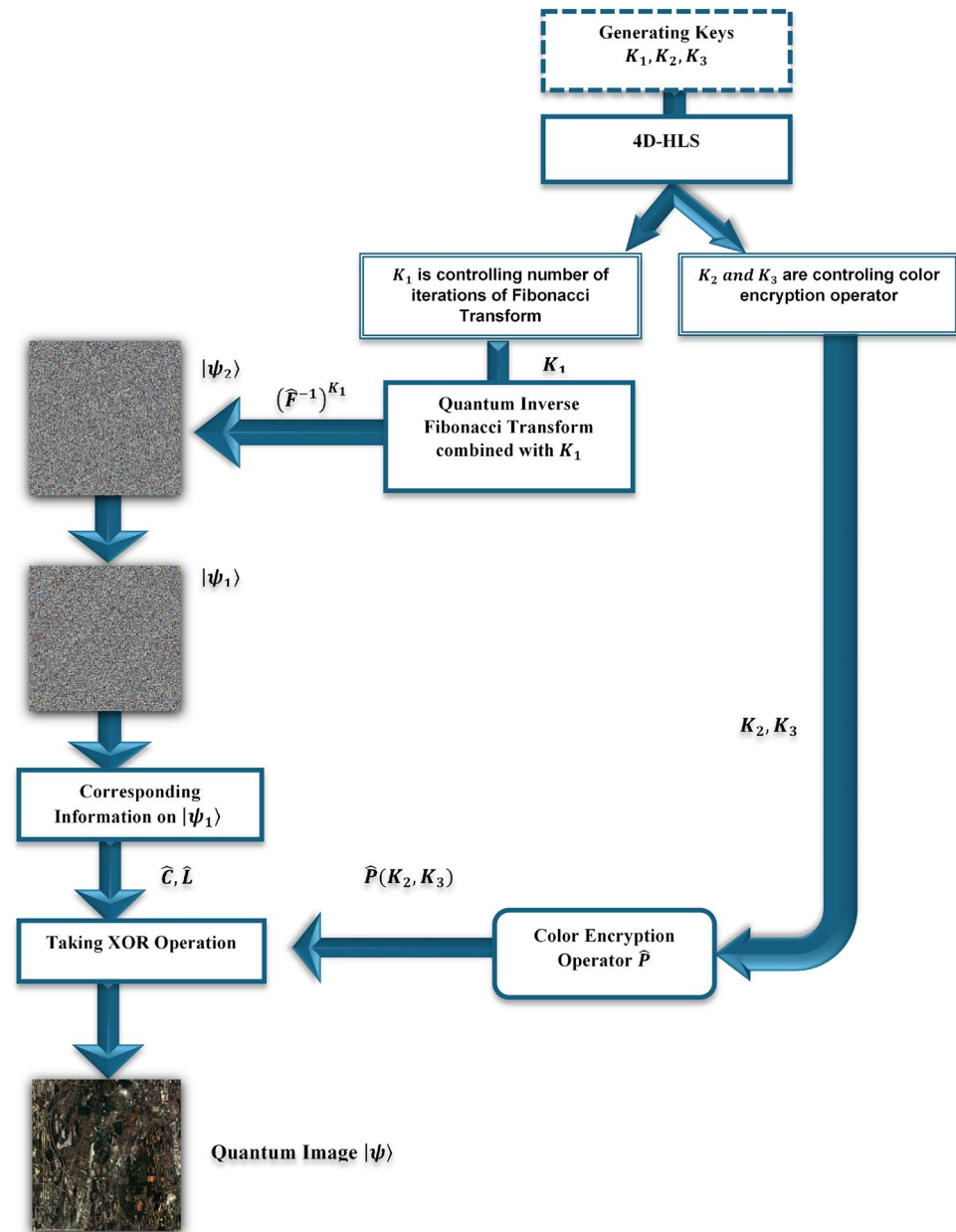


Fig. 6. Decryption process of quantum color image.

where $|YX\rangle$ demonstrates coordinate information and $|C_{YX}^j\rangle$ demonstrates color information. The bits of $|C_{YX}^j\rangle$ are equally divided into three parts: $|R\rangle |G\rangle |B\rangle$, representing the R, G, and B channels of the quantum color image, respectively. $|YX\rangle$ and $|C_{YX}^j\rangle$ are shown in Eq. (16).

$$\begin{aligned} |YX\rangle &= |Y\rangle |X\rangle = |y_0y_1y_2 \dots y_{h-1}\rangle |x_0x_1x_2 \dots x_{w-1}\rangle, y_j, x_j \in \{0, 1\} \\ |C_{YX}^j\rangle &= |R_{YX}^0 \dots R_{YX}^{d-1}\rangle |G_{YX}^0 \dots G_{YX}^{d-1}\rangle |B_{YX}^0 \dots B_{YX}^{d-1}\rangle. \end{aligned} \tag{16}$$

where $j = 0, 1, \dots, d - 1$.

3. Encryption Stage 2: Reading Parameter \widehat{L}

Using measurement operator \widehat{L} , it is possible to retrieve the corresponding information about the image in quantum state using Eq. (17).

$$\widehat{L} = \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} |YX\rangle \langle YX| I^{\otimes q}. \tag{17}$$

where q is the identity matrix utilized for each pixel's color information and $I^{\otimes q}$ is tensor product of identity matrix. The color information measurement operator \widehat{C} can be obtained using Eq. (18).

$$\widehat{C} = \sum_{c'=0}^{2^q-1} C |c'\rangle \langle c'|. \tag{18}$$

4. Encryption stage 3: diffusion phase

Using two keys K_2 and K_3 , the random color encryption operator generated to performs a modular operation $P_n(Y, X)$. An XOR operation is then applied between $P_n(Y, X)$ and the correspondent information of quantum image to conceal its information. Finally, the quantum state containing the RGB data is regularized to produce the first encrypted image $|\psi_1\rangle$ as described in Eq. (19).

$$\begin{aligned} P_n(Y, X) &= \text{floor} \left\{ \frac{K_{n_2} + 1}{K_{n_2} + K_{n_1} + 2} \times 10^{14} \right\} \text{mod } 256. \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}^{h+w}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^i\rangle |G_{YX}^i\rangle |B_{YX}^i\rangle |YX\rangle, \\ |R_{YX}^i G_{YX}^i B_{YX}^i\rangle &= |R_{YX}^0 \dots R_{YX}^{255}\rangle |G_{YX}^0 \dots G_{YX}^{255}\rangle |B_{YX}^0 \dots B_{YX}^{255}\rangle, \in \{0, 1\} \\ |R_{YX}^{n-1} G_{YX}^{n-1} B_{YX}^{n-1}\rangle &= \left| \frac{r_{YX}^{n-1} g_{YX}^{n-1} b_{YX}^{n-1} + P_{n-1}(Y, X)}{512} \right\rangle, r_{YX}^{n-1} g_{YX}^{n-1} b_{YX}^{n-1} \in \{0, 1, 2, \dots, 255\}. \end{aligned} \tag{19}$$

The keys utilized in this phase are obtained using 4D-HLS and Algorithm 1 demonstrates how they are obtained.

Input:

1. Control parameters

$$\alpha = 10, \beta = \frac{8}{3}, \gamma = 28 \text{ and } r = -1;$$

2. Initial Conditions

Initial state vector $[\mathbf{x}(0), \mathbf{y}(0), \mathbf{z}(0), \mathbf{w}(0)]$;

3. Time vector

A time array \mathbf{t} representing the time steps for solving the system

e.g., $\mathbf{t} = \text{np.linspace}(0, 100, 100000)$;

4. As the non-linear controller, we select the \mathbf{w} variable from Equation (1) and set initial value of $\mathbf{w}(t_0)$ at random. Next, we give each pixel in the original image a discrete time t_n . Consequently, the three chaotic signals are shown as follows:

$$\mathbf{K}_1 = \mathbf{x}(t_n), \mathbf{K}_2 = \mathbf{y}(t_n), \mathbf{K}_3 = \mathbf{z}(t_n).$$

Output:

- Key 1 (\mathbf{K}_1): corresponding to $\mathbf{x}(t)$
 - Key 2 (\mathbf{K}_2): corresponding to $\mathbf{y}(t)$
 - Key 3 (\mathbf{K}_3): corresponding to $\mathbf{z}(t)$
- Byte range of Keys [0, 255].

Algorithm 1. Generation of keys

5. Encryption stage 4: scrambled stage

The QFT operator \widehat{F}^{K_1} containing key K_1 is applied to first encrypted image $|\psi_1\rangle$ obtained in diffusion phase to generated final encrypted image $|\psi_2\rangle$. Equation (20) describes the specific computation technique.

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^i\rangle |G_{YX}^i\rangle |B_{YX}^i\rangle \widehat{F}^{K_1} |YX\rangle, \\ &= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^{\prime i}\rangle |G_{YX}^{\prime i}\rangle |B_{YX}^{\prime i}\rangle |Y'X'\rangle. \end{aligned} \quad (20)$$

Here, the encrypted image $|\psi_1\rangle$ is altered using the generalized FT operator \widehat{F}^{K_1} . The encryption process is made more secure by this operation. The generated image $|\psi_2\rangle$ is extremely secure and appropriate for safe transmission or storage since it captures the hidden color data.

Decryption procedure

The decryption procedure reverses the encryption process. The phases are as follows:

1. Decryption stage 1: generation of keys

Getting the required system control settings and initial values is the first step. During this stage, decryption keys are created.

2. Decryption stage 2: scrambled stage

This phase involves the use of FT operator's inverse (\widehat{F}^{-1}) to the operator (\widehat{F}^{K_1}) and inverse operation of the key. Using the final encrypted image $|\psi_2\rangle$ this procedure is performed. Equation (21) produces the image $|\psi_1\rangle$.

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^{\prime i}\rangle |G_{YX}^{\prime i}\rangle |B_{YX}^{\prime i}\rangle \left(\widehat{F}^{-1}\right)^{K_1} |Y'X'\rangle, \\ &= \frac{1}{\sqrt{2^{h+w}}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{j=0}^{d-1} |R_{YX}^i\rangle |G_{YX}^i\rangle |B_{YX}^i\rangle |YX\rangle. \end{aligned} \quad (21)$$

3. Decryption stage 3: diffusion phase

To recover the color data of image $|\psi_1\rangle$ and acquire original image $|\psi\rangle$ prior to encryption, the color encryption operator $P_n(Y, X)$ produced by the keys is utilized. This may be computed using Eq. (22).

$$\left| R_{YX}^{n-1} G_{YX}^{n-1} B_{YX}^{n-1} \right\rangle = \left\lfloor \frac{512 \times R_{YX}^{n-1} G_{YX}^{n-1} B_{YX}^{n-1} - P_{n-1}(Y, X) - 1}{256} \right\rfloor, \quad (22)$$

$$R_{YX}^{n-1} G_{YX}^{n-1} B_{YX}^{n-1} \in \{0, 1, 2, \dots, 255\}.$$

By simply reversing the color encryption operator method, this phase makes it possible to get the original image $|\psi\rangle$ prior to encryption.

The efficacy and efficiency of the suggested satellite image encryption method will be assessed in the next section utilizing a range of performance measures and tests.

Simulation experiment and analysis

This section focuses on thoroughly evaluating the performance of the suggested image cryptosystem. Tests will be conducted to ensure QCIES is secure against various attacks. The satellite images for this study are obtained from Airbus Defense and Space Limited 2024⁵⁵ and benchmark images (Ape and Jet plane) are obtained from GitHub⁵⁶.

To simulate QCIES, all experimental trials utilized randomly generated cryptographic keys. Since satellite images are the main focus of our proposed system, we extended our testing to include popular benchmark images such as Ape and Jet plane in order to guarantee the stability and versatility of the recommended encryption method. These images are frequently used as benchmarks in image processing and cryptography. The test images used are five images. Many widely used performance evaluation metrics entropy, histogram, correlation, and key sensitivity, among other perspectives, are used in this work based on current research^{42,46,56}. The experimental setup specifications, including both hardware and software environments, are detailed in Table 2.

Visual effect

A robust image encryption scheme must transform plaintext images into ciphertext outputs exhibiting visual indistinguishability from random noise. In this subsection, two benchmark images (Ape and Jet Plane) and three satellite images (Malaysia, Waterloo and Rainforest) go through encryption and subsequent decryption processes utilizing our QCIES algorithm. QCIES performance on two conventional images and three satellite images are shown in Fig. 7 to show that it works well not just with satellite images but also with other common types of images used in research. All images are of different sizes selected as test objects.

Information entropy analysis

In encrypted communications, information entropy³¹ serves as a crucial standard. For images, entropy is calculated by analyzing the pixel distribution across different gray levels in each color channel. A more uniform distribution of pixels leads to higher entropy, indicating greater randomness and complexity in the image. Specifically, for the RGB channels of a color image, an absolute entropy's value 8 signifies that pixel values are evenly distributed, making the image more resistant to analytical attacks. The capacity of image to resist such attacks is strengthened by the higher the entropy, the more equally the pixels are distributed. As a result, an encryption technique's security and resilience can be assessed using entropy's information. The formula for calculating information entropy is given in Eq. (23).

$$H(z) = - \sum_{i=0}^{255} P(z_i) \log_2 P(z_i). \quad (23)$$

where $H(z)$ represents the value of information entropy, z_i represents the gray value of first pixel, and $P(z_i)$ represents the probability of the gray level. The results reveal a significant difference in entropy between the original and encrypted images. The original images' entropy is far from 8, whereas the encrypted images show entropy's value approaching 8, indicating that the QCIES effectively resists attacks based on entropy analysis. This reinforces the security of the algorithm.

To more thoroughly assess the randomness of cipher images, a metric known as Local Shannon Entropy (LSE) has been introduced³¹. This measure has gained widespread adoption for evaluating the randomness in encrypted images. The mathematical definition of LSE is given as follows:

Component	Specification
Processor	Intel (R) Core (TM) i3-2350 M CPU 2.30 GHz
Memory	8 GB DDR3 RAM
Operating system	Windows 10 Pro (64-bit)
Simulation software	Python 3.13.0 and MATLAB R2016a

Table 2. Software and hardware configurations.

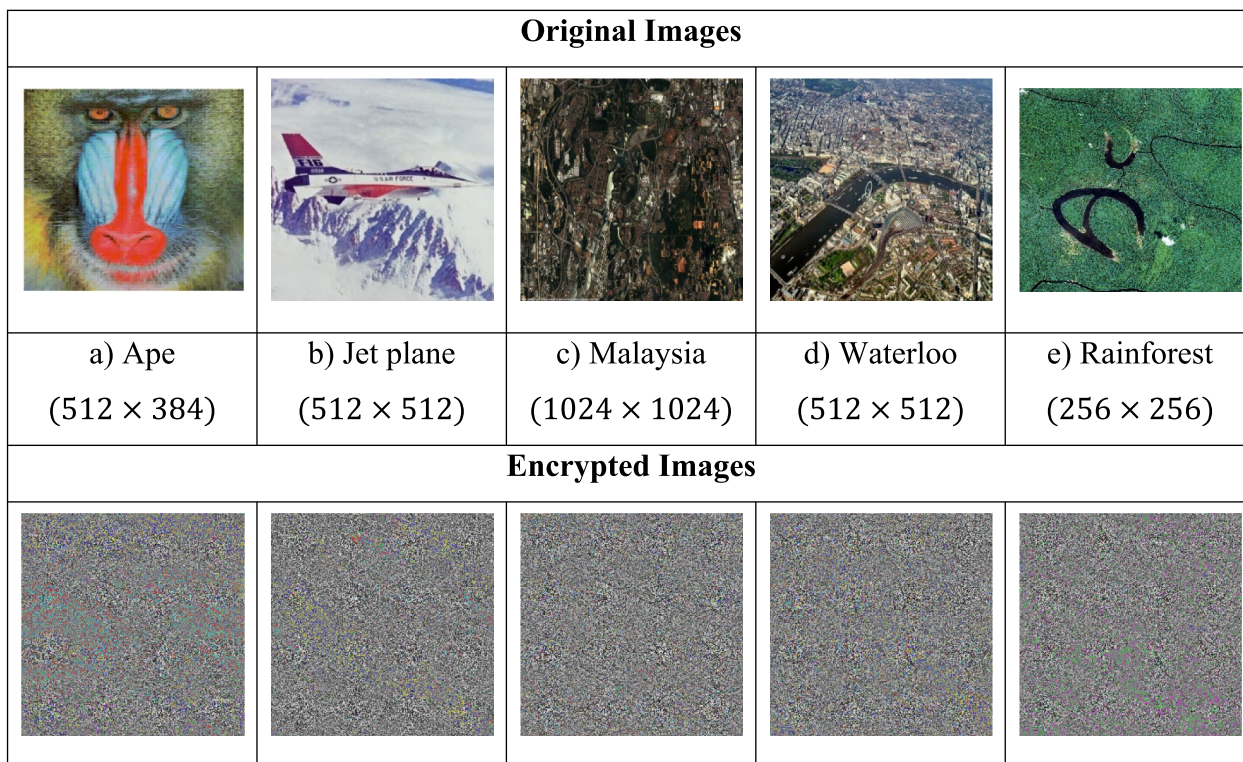


Fig. 7. Evaluation of suggested encryption and decryption analysis. Images in plaintext are displayed in the second row. Images that have been encrypted are shown in fifth row, while Images that have been encrypted their names and sizes are shown in the third row.

Images	QCIES		
	Original	Encrypted	
	Global	Local	
Ape	7.6565	7.9993	7.9023
Jet Plane	6.6801	7.9994	7.8883
Malaysia satellite	6.9801	7.9992	7.2324
Rainforest satellite	6.1015	7.9994	7.6881
Waterloo	7.0112	7.9993	7.8891

Table 3. Information Entropy.

Images	QCIES			Ref ⁶⁶	Ref ⁶⁷
	Original	Encrypted		Encrypted	Encrypted
	Global	Local		Global	Global
Ape	7.6565	7.9993	7.9023	7.9993	7.9994
Jet Plane	6.6801	7.9994	7.8883	7.9993	7.9993

Table 4. Comparison of global entropy levels.

$$L_{q,p}(s) = - \sum_{i=1}^q \frac{P(s_i) \log_2 P(s_i)}{q} \tag{24}$$

where $P_w(z_i)$ is the probability of intensity i in the local window, p is the number of pixels in each block. Table 3 shows global and local entropy of original and encrypted images and Table 4 shows comparison of global entropy levels for several encryption techniques.

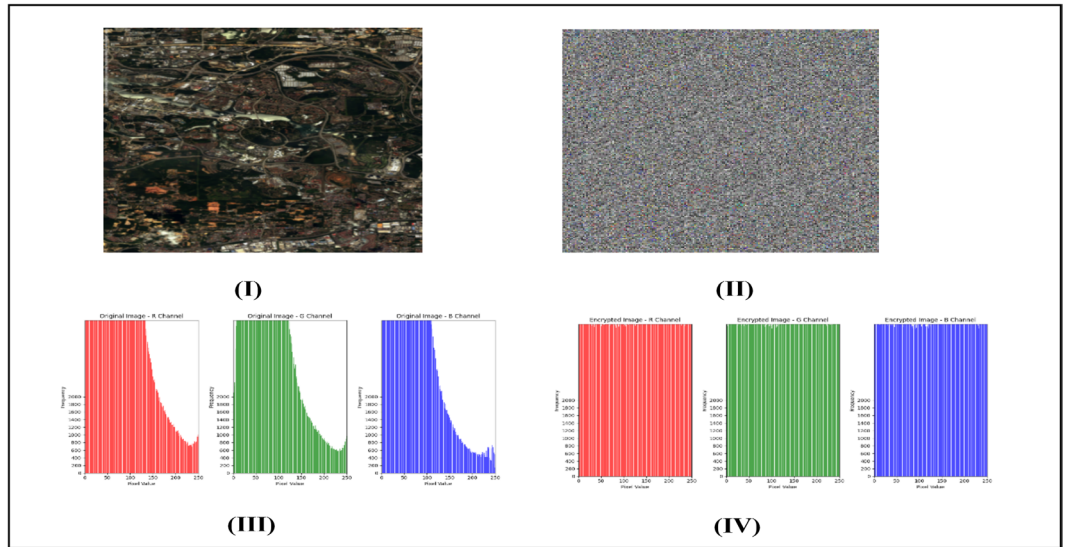


Fig. 8. Comparison of Malaysia satellite image (1024 × 1024) and its histogram before & after encryption (I) Malaysia satellite image (II) Malaysia satellite encrypted image (III) Malaysia satellite image’s histogram (IV) Malaysia satellite encrypted image’s histogram.

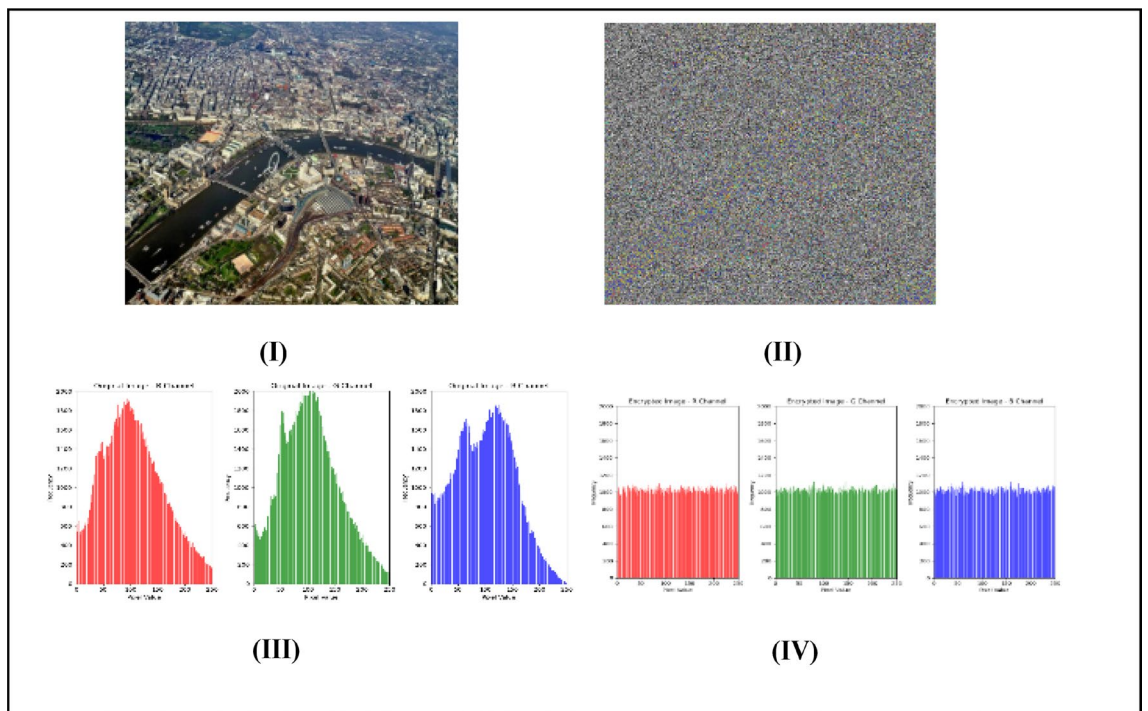


Fig. 9. Comparison of Waterloo image and its histogram before & after encryption (I) Waterloo image (II) Waterloo encrypted image (III) Waterloo image’s histogram (IV) Waterloo encrypted image’s histogram.

Histogram analysis

A key method for evaluating the image cryptosystem’s efficacy to compare an encrypted image with its original version is the use of the human visual system (HVS). The image’s histogram provides a clear representation of how pixel values are spread throughout the image⁵⁵. Figures 8, 9 and 10 display various original images alongside their encrypted versions, along with corresponding histograms. The encrypted images’ histograms show almost identical consistent distributions, while the original images’ histograms exhibit distinct analytical features, making it difficult to determine the source of the encrypted images. Statistical analysis on the encrypted image yields no meaningful information, indicating that the encryption system is robust against histogram-based attacks.

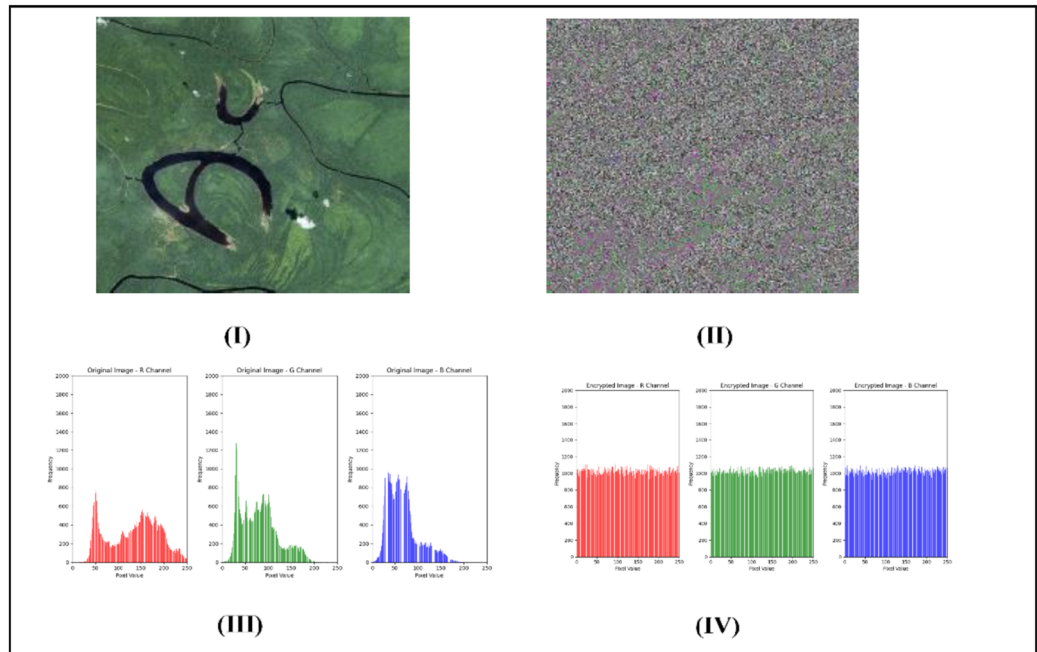


Fig. 10. Comparison of Rainforest image (256 × 256) and its histogram before & after encryption (I) Rainforest image (II) Rainforest encrypted image (III) Rainforest image’s histogram (IV) Rainforest encrypted image’s histogram.

Metrics	Jet plane image	Malaysia satellite image	Waterloo satellite image	Ape image	Rainforest satellite image
χ^2 value	250.4641	272.5501	254.1352	256.1210	242.7215
<i>p</i> -value	0.5629	0.2284	0.5123	0.3223	0.5523
Uniformity	Yes	Yes	Yes	Yes	Yes

Table 5. Chi-square test results for evaluating histogram uniformity.

Assessment of histogram uniformity using chi-square test

The uniformity of pixel distribution in encrypted images was rigorously evaluated using the chi-square (χ^2) test⁵⁸, a statistical measure that quantifies the discrepancy between observed and expected pixel frequencies. The test statistic is computed as shown in Eq. (25).

$$\chi^2 = \sum_{i=1}^{256} \frac{(O_i - E_i)^2}{E_i} \tag{25}$$

where O_i represents the observed frequency of pixel intensity in the encrypted image, and E_i denotes the expected frequency under a perfectly uniform distribution. For RGB images, the final χ^2 value was obtained by averaging the results across the R, G, and B channels to ensure comprehensive assessment.

As presented in Table 5, the proposed encryption algorithm consistently accepted the null hypothesis ($p > 0.05$ at a 5% significance level) for all tested cipher images. This indicates that the encrypted histograms exhibit no statistically significant deviation from uniformity, effectively concealing the redundancy present in the original images. The high *p*-values confirm that the algorithm successfully eliminates discernible patterns in the pixel distribution, thereby enhancing resistance against statistical attacks. These findings demonstrate the robustness of the encryption scheme in maintaining security against frequency-based cryptanalysis.

Correlation analysis

Correlation analysis⁵⁸ is a method used to evaluate the strength and direction of the relationship between two variables. The correlation coefficient, which ranges from -1 to $+1$, indicates how strongly the two variables are related and the nature of their relationship. A correlation coefficient closer to 0 suggests a weaker relationship, while $+1$ represents a perfect positive correlation and -1 signifies a perfect negative correlation. For an effective encryption algorithm, the correlation in the ciphertext between adjacent pixels should be near to zero. The adjacent pixels’ correlation values in the original and encrypted images are assessed in the diagonal, vertical,

and horizontal directions. Therefore, pixel correlation serves as a useful criterion for evaluating the image encryption's efficacy. The calculation method for the adjacent pixels' correlation is given by Eq. (26).

$$\rho_{NM} = \frac{cov(N, M)}{\sqrt{\sigma(N)}\sqrt{\sigma(M)}} \tag{26}$$

where $cov(N, M) = \frac{1}{X} \sum_{i=1}^X (N_i - \mu(N))(M_i - \mu(M))$, $\sigma(N) = \frac{1}{X} \sum_{i=1}^X (N_i - \mu(N))^2$, $\sigma(M) = \frac{1}{X} \sum_{i=1}^X (M_i - \mu(M))^2$ and $\mu(N) = \frac{1}{X} \sum_{i=1}^X (N_i)$. X is the total pixel pairs, and N_i, M_i denote the pixel values of two adjacent pixels. To assess the correlation, ten thousand pairs of neighboring pixels are chosen at random from the image and evaluated in horizontal, vertical, and diagonal directions. Figures 11 illustrate the pixel correlation in the row, column, and diagonal directions for both the original and encrypted Malaysia satellite images. Figure 12 displays the combined 3D RGB channel correlations for all investigated images, with all color channels visualized in a unified plot to demonstrate their inter-channel relationships. Table 6 presents the values of correlation between neighboring pixels in original and encrypted Malaysia satellite images for each color channel (R, G, and B). Table 7 presents the values of correlation between neighboring pixels in original and encrypted Rainforest satellite, Waterloo satellite and Jet Plane images. The average values of the R, G, and B channels of the Malaysia satellite image are used to compute the correlation values.

From the data in Tables 6 and 7, it is evident that the plaintext image has a high pixel correlation (close to 1), indicating a strong relationship between adjacent pixels. The ciphertext image's pixel distribution becomes more consistent and the correlation is greatly reduced once QCIES is applied. This indicates that the QCIES effectively disrupts the pixel correlation. Combining chaos-controlled parameters with the quantum image Fibonacci transform, after implementing an XOR operation on adjacent pixels, effectively reduces the correlation between adjacent pixels in the encrypted image.

Tables 6 and 7 further demonstrates that images are susceptible to a number of attacks before encryption. However, pixel correlation in ciphertext is markedly weakened, increasing resistance to pixel-level correlation

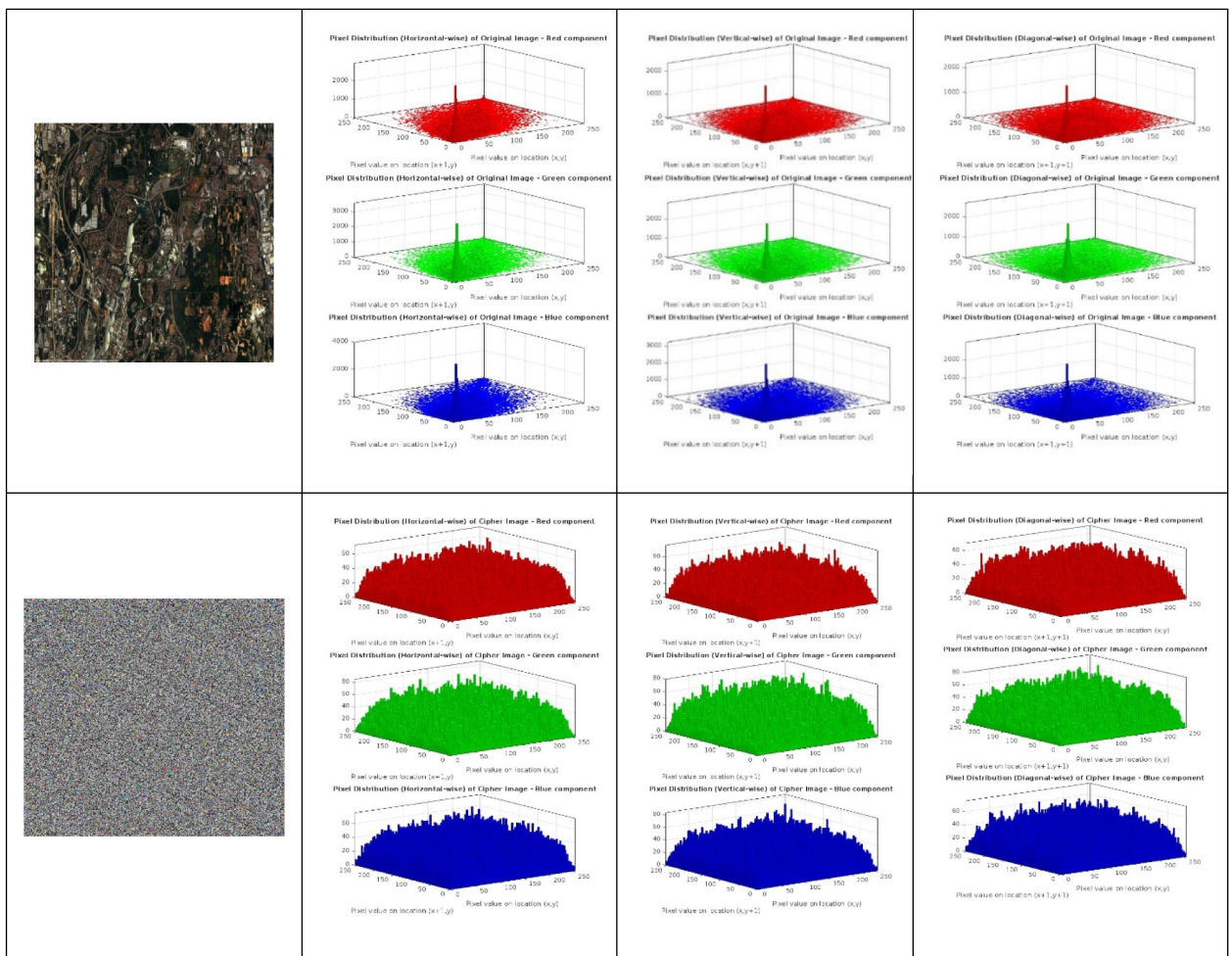


Fig. 11. Pixel's correlation in row, column and diagonal direction for both original in first row and encrypted in second row for Malaysia satellite image.

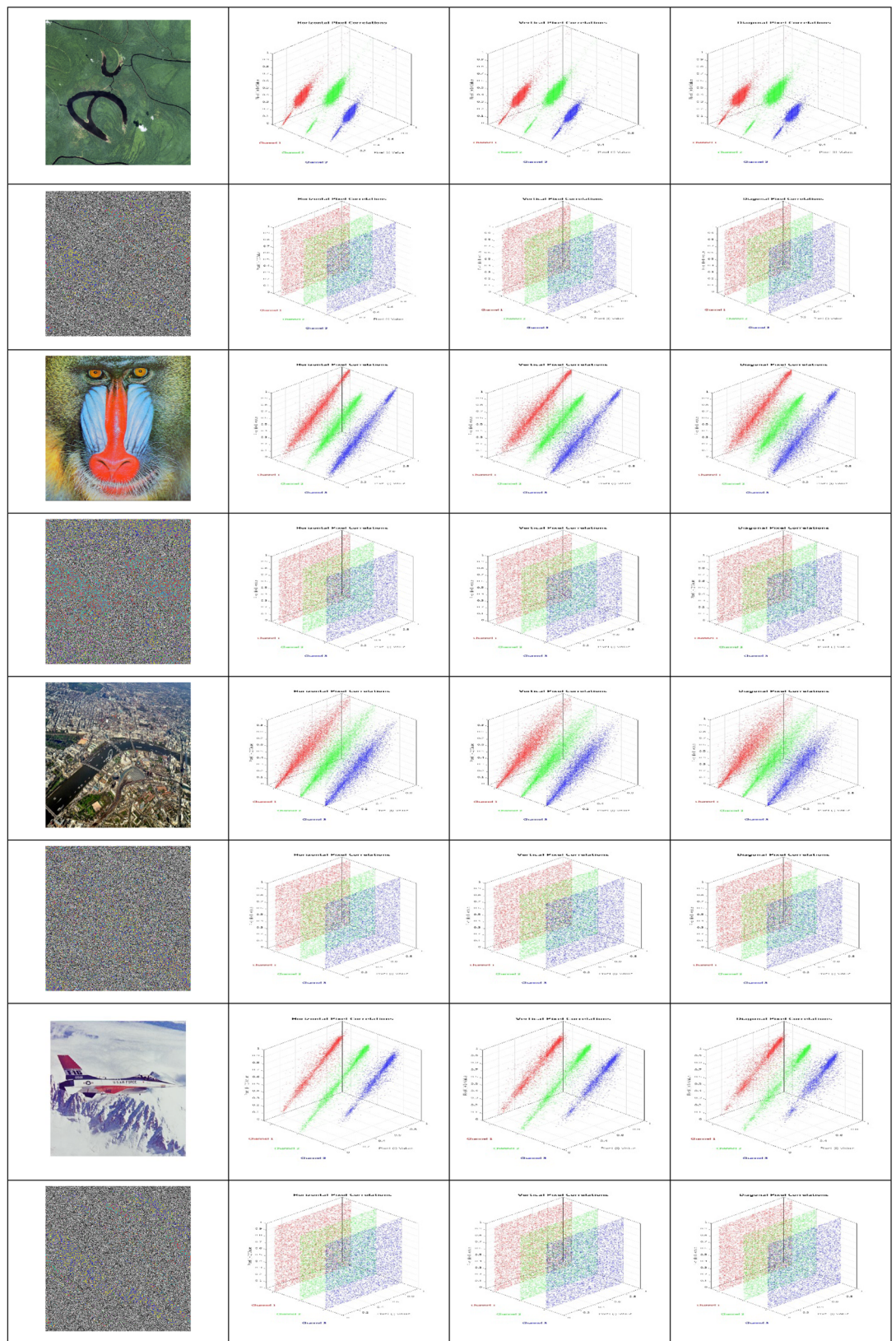


Fig. 12. Combined 3D visualization of RGB channel correlations across all spatial directions for all investigated images.

Direction	Red		Green		Blue	
	Original	Encrypted	Original	Encrypted	Original	Encrypted
Vertical	0.7412	0.0033	0.7402	0.0048	0.7490	0.0016
Horizontal	0.8613	0.0028	0.8571	0.0032	0.8547	0.0022
Diagonal	0.6804	0.0010	0.6791	0.0012	0.6875	0.0037

Table 6. Correlation coefficient values for original and encrypted Malaysia satellite image.

Images	Original			Encrypted		
	V	H	D	V	H	D
Waterloo	0.8234	0.8488	0.7520	0.0047	-0.0013	0.0046
Rainforest	0.8238	0.8301	0.7629	0.0043	0.0029	0.0025
Jet Plane	0.9302	0.9249	0.8758	0.0025	0.0009	-0.0003

Table 7. Correlation coefficient values for original and encrypted Investigated images.

Algorithm	Original			Encrypted		
	V	H	D	V	H	D
Proposed	0.9218	0.8555	0.8295	0.0026	0.0009	0.0011
Ref ⁴⁶	0.8349	0.9000	0.8069	0.0103	0.0143	0.0103
Ref ⁵⁸	0.8169	0.7509	0.7460	0.0074	0.0003	0.0002

Table 8. Comparability of correlation coefficients values of Ape's image.

attacks after encryption. This improvement in robustness is a critical feature of QCIES security. The use of chaos-based parameters in combination with the quantum image Fibonacci transform makes QCIES more complex, adding a layer of resistance to attacks that depend on predictable patterns. Table 8 presents the comparison of correlation coefficient values of Ape's image.

Beyond pixel correlation, the strategy is made to resist a variety of attacks, including brute-force efforts and differential cryptanalysis. It has shown resilience against common attacks, such as differential and frequency analysis. Additionally, the QCIES robustness extends to its ability to maintain security even against potential quantum computing-based attacks.

Differential attack analysis

The effectiveness of image encryption techniques is often assessed through differential attacks¹. Differential attack analysis is a cryptanalytic technique that looks at how specific changes made to the input plaintext inside the encryption methods affect the ciphertext that is produced in the end.

Plaintext sensitivity analysis

For an image encryption algorithm to be resilient against such threats, it must exhibit very strong plaintext sensitivity²⁹. This means that even a slight modification such as a single bit change in any pixel of the input image should produce significant and unpredictable differences in the resulting ciphertext. To evaluate the plaintext sensitivity of QCIES, we intentionally altered two pixel bits in a 512×512 test image: one located at the top-left corner and the other at the bottom-right. The modified images, shown in the second and third columns of the first row in Fig. 13, are visually indistinguishable from the original image. We then encrypted all three images using the QCIES method and computed the differences between the resulting ciphertexts. As illustrated in Fig. 13, the encrypted outputs and their respective difference images appear completely noise-like. This visual evidence confirms that even minimal changes in the plaintext lead to extensive, seemingly random transformations in the ciphertext, demonstrating that QCIES achieves a high level of plaintext sensitivity.

This sensitivity is typically linked to the susceptibility of its control parameters and the initial state of the chaotic mapping, both of which affect the plaintext sensitivity in chaotic cryptography. The literature suggests two tests to meet these requirements: Unified Average Changing Intensity (UACI) to determine the mean difference and Number of Pixel Change Rate (NPCR) for contrasting independent pixels. Higher UACI encryption is seen to be more advantageous. A good image encryption technique requires a large valued NPCR.

When the plaintext image's pixel is altered, corresponding encrypted image should preferably reflect an ordinary change to resist differential attacks. The standard values for NPCR and UACI are 99.6094% and 33.4635%, respectively, and these can be calculated using Eq. (27).

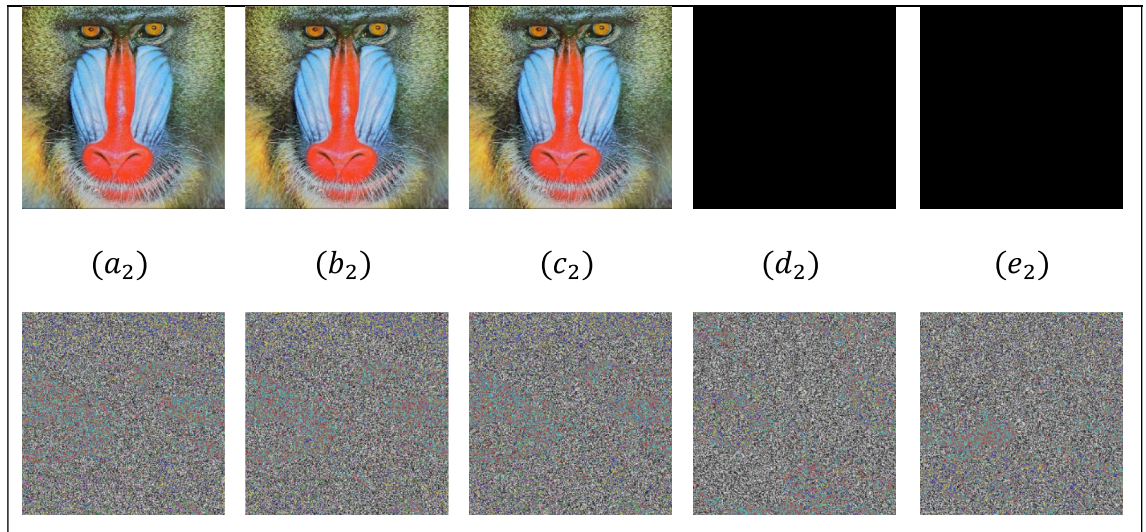


Fig. 13. Visual demonstration of plaintext sensitivity in QCIES : (a_1) Original test image; (b_1) Modified image with the least significant bit of the first blue channel pixel inverted; (c_1) Modified image with the least significant bit of the last red channel pixel inverted; (d_1) Pixel-wise difference between (a_1) and (b_1); (e_1) Pixel-wise difference between (a_1) and (c_1); (a_2) Encrypted output corresponding to (a_1); (b_2) Encrypted output corresponding to (b_1); (c_2) Encrypted output corresponding to (c_1); (d_2) Difference between ciphertexts (a_2) and (b_2); (e_2) Difference between ciphertexts (a_2) and (c_2).

QCIES images	RGB average NPCR	RGB average UACI
Ape	99.64	33.59
Jet plane	99.64	33.55
Malaysia Satellite	99.62	33.53
Rainforest Satellite	99.63	33.57
Waterloo satellite	99.64	33.54

Table 9. RGB average NPCR & UACI data

Algorithm	Average NPCR	Average UACI
Proposed	99.64	33.56
Ref. ³¹	99.60	33.43
Ref. ⁴⁰	99.61	33.42
Ref. ⁴⁶	99.60	33.49

Table 10. Comparison of NPCR & UACI values of different algorithms.

$$\begin{aligned}
 NPCR : N(\mu_1, \mu_2) &= \frac{\sum_{i,j} C(i, j)}{W \times H} \times 100\%, \\
 UACI : U(\mu_1, \mu_2) &= \frac{1}{W \times H} \sum_{i,j} \frac{|\mu_1(i, j) - \mu_2(i, j)|}{255} \times 100\%.
 \end{aligned}
 \tag{27}$$

where W and H are the width and height of the images, and $C(i, j)$ is defined in Eq. (28).

$$C(i, j) = \begin{cases} 0, & \mu_1(i, j) = \mu_2(i, j), \\ 1, & \mu_1(i, j) \neq \mu_2(i, j), \end{cases}
 \tag{28}$$

Here, $\mu_1(i, j), \mu_2(i, j)$ represent the pixel values at point (i, j) in the two ciphertexts. By changing a single bit in the key K , for a same plaintext image two distinct ciphertext images can be generated.

Table 9 shows the NPCR and UACI values of proposed scheme. Experimental results indicate that the NPCR and UACI values of the proposed scheme are close to the ideal values. Table 10 shows a comparison between the

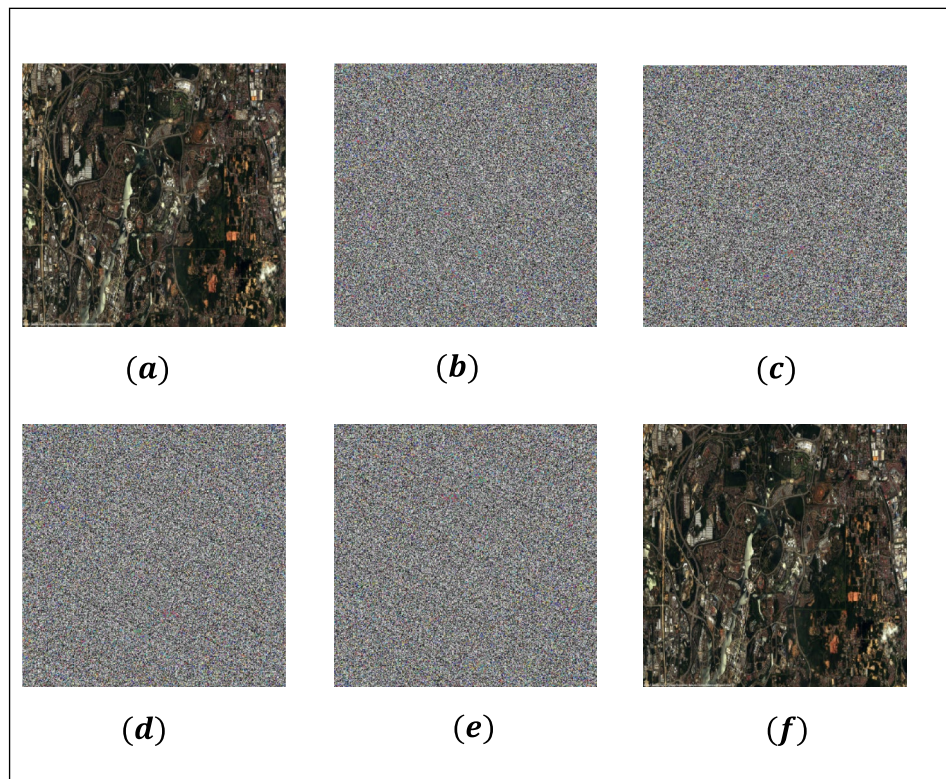


Fig. 14. Key susceptibility analysis.

Key variation	NPCR (%)	UACI (%)
Original vs K_1	99.62	33.51
Original vs K_2	99.59	33.48

Table 11. Quantitative key sensitive tests.

NPCR and UACI results obtained from QCIES and those from related studies. When determining the NPCR and UACI values for the images, the average of the R, G, and B channels is taken into account.

Key space and sensitivity research

Key susceptibility is the property of an absolute multimedia encryption system, which signifies that change in a single bit of key should result in drastically divergent encryption output. QCIES utilized in this study is based on a quantum 4D-HLS, which is highly susceptible to the starting values. We conducted sensitivity analysis on related keys. The results, depicted in Fig. 14, highlight the technique's high sensitivity. Even a slight deviation in the key prevents successful decryption of the original image, further emphasizing the system's robustness. Figure 14a shows the original image. At first, original image is encrypted using the correct keys as shown in Fig. 14b. Then encrypted image is decrypted using three different sets of keys. We derived three different set of keys K_1, K_2, K_3 by applying slight modifications of $\varepsilon = 10^{-15}$ to individual components of the original key K as $x'_0 = x_0 + \varepsilon, y'_0 = y_0 + \varepsilon$ and $z'_0 = z_0 + \varepsilon$ and the results are obtained as in Fig. 14c–e. Figure 14f shows the image decrypted with correct set of keys.

Correct set of Keys $K = (x_0, y_0, z_0, w_0, \alpha, \beta, \gamma, r)$

Incorrect Key $K_1 = (x'_0, y_0, z_0, w_0, \alpha, \beta, \gamma, r)$

Incorrect Key $K_2 = (x_0, y'_0, z_0, w_0, \alpha, \beta, \gamma, r)$

Incorrect Key $K_3 = (x_0, y_0, z'_0, w_0, \alpha, \beta, \gamma, r)$

Table 11 presents the quantitative key sensitivity analysis using NPCR and UACI metrics, demonstrating that slight variations in the encryption key lead to significant changes in the encrypted image.

A robust encryption approach must have an adequately large key space to make it infeasible for an attacker to discover the correct key within a reasonable timeframe. To withstand advanced attacks, the key space should ideally exceed 2^{128} . In this study, the chaotic system parameters' precision can be achieved to a level of 10^{-16} . In QCIES, the key space reaches 10^{140} , which is far greater than 2^{128} . This demonstrates that QCIES has a key space large enough to effectively resist brute-force attacks. Table 12 demonstrates the comparison of QCIES key space with other studies.

	Proposed	Ref ¹⁶	Ref ¹⁶
Key space size	10^{140}	10^{128}	10^{83}

Table 12. Comparison of key space.

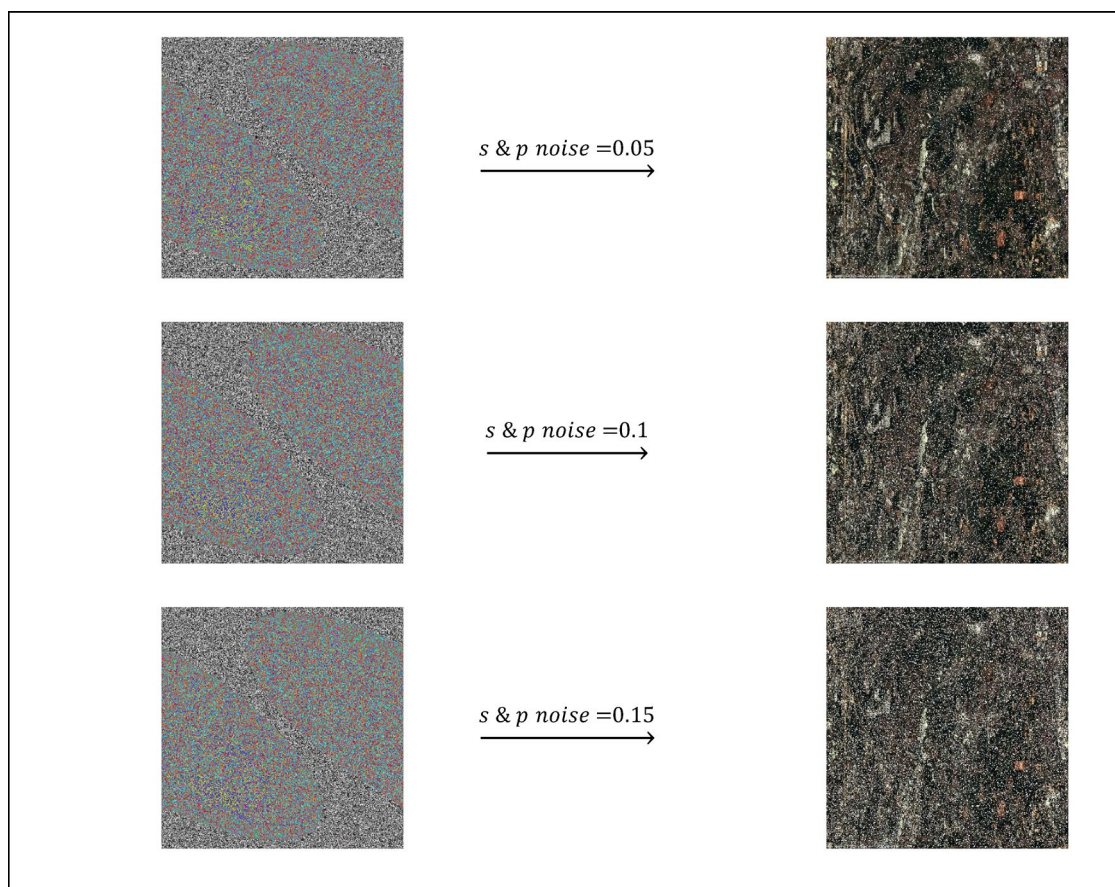


Fig. 15. The transformation effect of “Malaysia satellite” image subjected to various salt and pepper s&p variations.

Robustness against transmission noise

During digital transmission, encrypted images frequently encounter channel-induced distortions including additive noise, signal degradation, and data corruption. Such disturbances may compromise decryption fidelity, necessitating robust cryptographic designs capable of withstanding real-world noise interference. Standard evaluation protocols simulate these conditions by applying controlled noise perturbations⁵⁸ (e.g., Gaussian, salt-and-pepper, occlusion attack) to ciphertext images prior to decryption, with structural similarity metrics quantifying recovery quality.

To evaluate robustness, salt-and-pepper noise (0.05–0.15 density) and Gaussian noise (0.10–0.20 variance) were introduced to encrypted versions of the satellite images, respectively. Figure 15 and 16, shows successful decryption despite these perturbations, proving the algorithm’s noise resistance.

Occlusion attack resistance analysis

Robust encryption schemes must maintain data integrity when facing partial data loss, whether from network disruptions or malicious interference. We evaluate our algorithm’s resilience by simulating progressive occlusion attacks (25%, 50%, and 75% data loss) on cipher images. As demonstrated in Fig. 17, the decrypted images retain sufficient visual coherence and recover critical information even under severe occlusion (75% data loss).

Assessment of encryption effectiveness using PSNR and SSIM

To initiate the statistical analysis, the Peak Signal-to-Noise Ratio (PSNR)⁵⁹ is computed to assess the quality of the encrypted image and ensure that the original image is effectively transformed by the encryption algorithm. PSNR measures the difference between the original and encrypted images, where a lower PSNR value indicates a

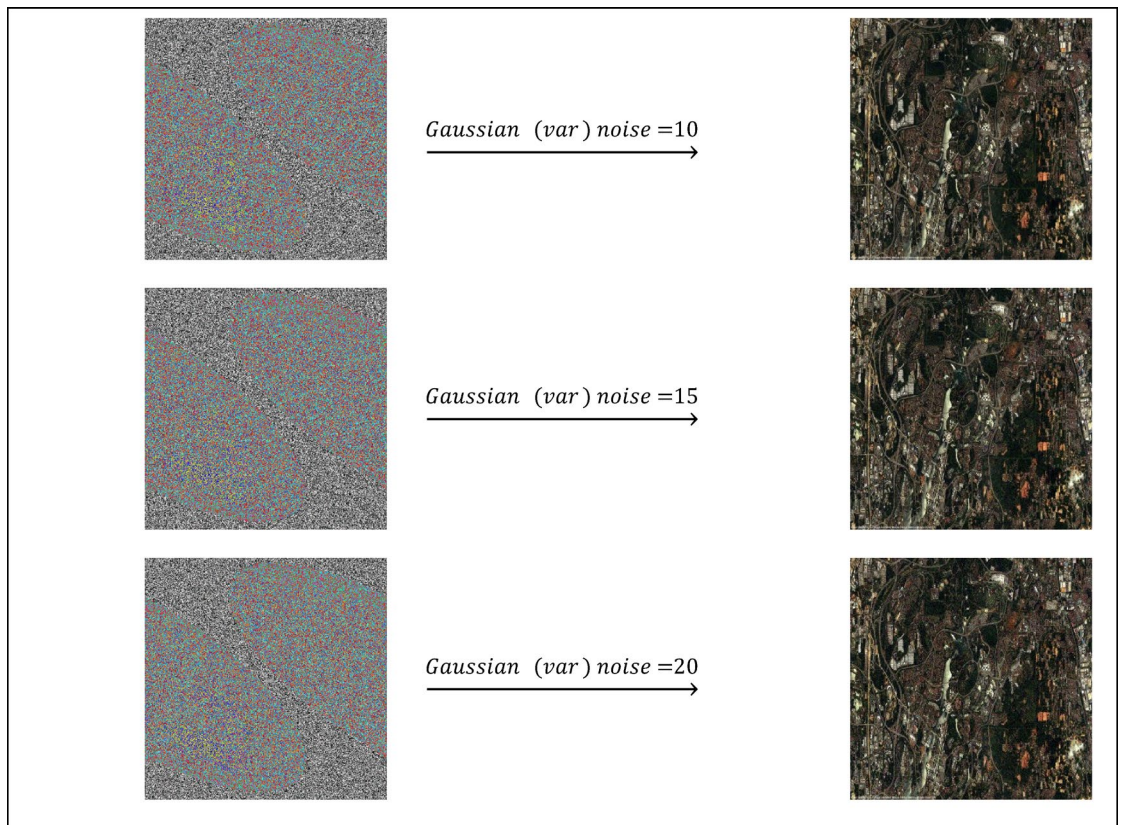


Fig. 16. The transformation effect of “Retina” image subjected to various Gaussian variations.

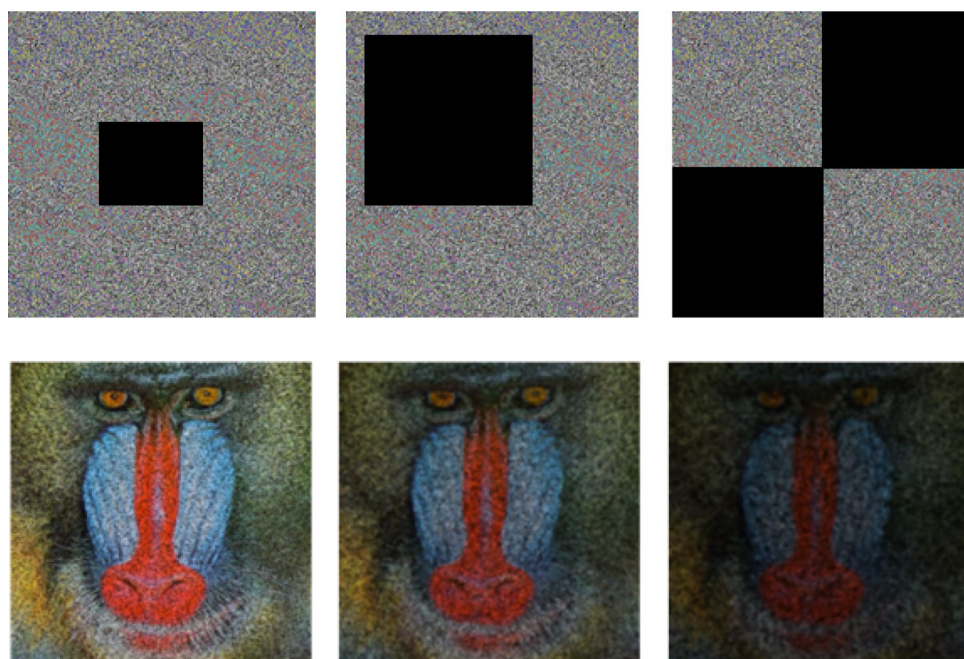


Fig. 17. Top row: Encrypted ‘Ape’ image with clipping. Bottom row: Corresponding decrypted image.

Images	PSNR	SSIM
Ape	8.0039	0.000109
Jet plane	8.7626	0.000212
Malaysia satellite	8.7880	0.008793

Table 13. PSNR & SSIM values for images.

QCIES	Time (in s)
Ape (512 × 384)	9.3894
Jet plane (256 × 256)	3.8206
Malaysia satellite (1024 × 1024)	48.4120

Table 14. Evaluation of execution time (in s).

Algorithm	Time (in s)
QCIES	48.4120
Ref ²⁹	60.1052
Ref ⁵⁹	64.1120

Table 15. Comparison of execution time (in seconds) for (1024 × 1024) size.

significant distinction between the plaintext and encrypted images. The formula for calculating PSNR is shown in Eq. (29).

$$\log \frac{255 \times 255}{\sqrt{\sum_{i=1}^n \sum_{j=1}^m \frac{[P(i,j) - E(i,j)]^2}{m \times n \times 3}}} \quad (29)$$

where $P(i, j)$ represents plain image's while $E(i, j)$ represents the encrypted image's pixel values.

Beyond pixel-by-pixel variations captured by traditional metrics such as PSNR, the Structural Similarity Index Measure (SSIM) is employed to evaluate the similarity between two images in terms of structure, texture, and pixel intensity. Higher SSIM values, which range from 0 to 1, indicate less distortion, whereas an ideal encryption result should yield an SSIM value near zero, signifying that the encrypted image is structurally very different from the original. The formula for calculating SSIM is shown in Eq. (30).

$$= \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (30)$$

where x and y are corresponding image patches. μ_x & μ_y mean intensities, σ_x^2 & σ_y^2 variance, σ_{xy} means covariance of x and y . C_1 & C_2 are small constants to stabilize the division.

Table 13 demonstrates the PSNR and SSIM values for three encrypted images. It should be noted that the PSNR and SSIM values for the Ape image are calculated by averaging the results across the R, G, and B color channels.

Efficiency analysis

While security remains paramount, computational efficiency is equally critical for practical deployment of image encryption. Computational complexity analysis focuses on time and spatial complexity. QCIES achieves significant performance gains through three key optimizations. The 4D-HLS generates all keystreams in advance, eliminates iterative chaotic computations during pixel processing. The Quantum Fibonacci Transform (QFT) operates on 8 × 8 pixel blocks (64-bit vectors) instead of individual pixels. All operations (chaotic shuffling, QFT) use relative coordinates, avoiding padding overhead for non-square images.

Time complexity analysis

To thoroughly validate the efficiency advantages of our proposed QCIES algorithm, we conduct timing test under strictly controlled conditions. Table 14 presents computational time measurements for images of varying sizes (256 × 256, 512 × 384, and 1024 × 1024). Table 15 compares the computation time from relevant literature in this article by taking average of all image's values.

Tests	Algorithms		
	Ref ⁴⁶	Ref ⁵⁷	Proposed QCIES
Entropy	7.9993	7.9994	7.9993
NPCR	99.60	99.60	99.64
UACI	33.43	33.49	33.56
PSNR	8.7626	7.3068	8.7827
SSIM	0.0075	0.01000	0.00012
Key space	Ref ⁴⁶	Ref ¹⁶	Proposed QCIES
	10^{128}	10^{83}	10^{140}

Table 16. Performance analysis phase.

Spatial complexity analysis

The quantum XOR operation and quantum Fibonacci transformation have an impact on the intricacy of QCIES. A color image of dimensions $2^n \times 2^n$ requires $2n + 24$ qubits and contains 3×2^{2n} pixels to be converted into image in quantum state. $2n$ quantum exchange gates, which can all be broken down into 3 *CNOT* gates and an adder module operation are involved in the quantum Fibonacci transformation. The *ADDER – MOD 2^n* operation contains $28n - 12$ simple gates⁵³, with total $x_1^* \bmod n$ iterations. Consequently, the total number of basic gates required is $((28n - 12) + 2n \times 3) \times (x_1^* \bmod n)$. The number of shifts is $x_3^* \bmod n + 1$ and 23 switching gates are essential for the operation of cycle shift. Therefore, $23 \times 3 \times (x_3^* \bmod n + 1)$ basic gates involved in the quantum bit level shift function. In terms of quantum resemblance, the XOR function on quantum images needs $2n - \text{CNOT}$ gates. Each $n - \text{CNOT}$ gate can be broken down into $(4n - 8)$ Toffoli gates, with each Toffoli gate consisting of 6 CNOT gates¹⁷. This results in a total of $(4n - 8) \times 2 \times 3 \times 6$ basic gates (Table 16).

To summarize, the quantum Fibonacci transformation has a complexity of $O(n^2)$, while XOR operation have a complexity of $O(n)$. Therefore, the GQIR based QCIES has an overall complexity of $O(n^2)$. The traditional image encryption technique, on the other hand, has an overall complexity of $O(2^{2n})$. Therefore, QCIES has a lessened computational complexity compared to the classical encryption algorithm.

Conclusion

This study introduces a novel encryption method designed to enhance the security of sensitive digital evidence, such as satellite images, and represents a significant advancement in the field of digital forensics. Protecting information from unauthorized access is a critical challenge in the practical use of satellite images. With the continuous evolution of cyber threats from malicious actors, researchers are under constant pressure to develop new algorithms that can better secure essential satellite data. By utilizing chaotic systems to maintain transmission confidentiality, this paper seeks to contribute to the field of encrypted satellite images. QCIES provides a valuable tool for forensic applications, ensuring both the confidentiality and integrity of sensitive data.

QCIES begins by utilizing a quantum Fibonacci transform with a key to determine the coordinates of the jumbled values of the pixels during the encryption step. It then uses a quantum chaotic sequence to apply a linear transformation to the pixel data. All pixels are processed to create the ciphertext images after the displacement procedure is complete. When this displacement is paired with pixel gray value encryption utilizing a key, QCIES intricacy and unpredictability are greatly increased. Information entropy, histogram analysis, correlation, and key susceptibility were among the metrics used to evaluate QCIES performance. The outcomes of the experiment were deemed to be quite satisfactory. To enhance the decrypted image's quality even more, all image encryption operations are performed using reversible quantum logic gates⁴⁵. QCIES enables the exact restoration of the original image, provided the key is correct.

QCIES is prone to disastrous attacks and produces shuffled images with stronger enhanced security. QCIES overcomes the issues of common encryption techniques, such as recurrence, key space limitations, and exposure to statistical evaluation, and offers dependable and efficient encryption system. QCIES utilizes the properties of Quantum Fibonacci transformation permutation, periodicity, and unpredictability of the 4D-HLS, using the larger key. The Lorenz system provides space in 4 dimensions.

However, it should be noted that quantum image compression faces challenges because real quantum computers aren't powerful enough to handle large, real-world images. One possible solution is to use classical methods for early steps like feature extraction, and then apply quantum techniques for actual compression. This hybrid approach could be more practical with today's technology. However, building quantum computers that can scale and work reliably is still a big challenge. Using many quantum gates increases errors due to noise and instability. So, it's still difficult to apply these algorithms on real quantum hardware. To enhance the image representation and lower computational demands, we plan to investigate an equitably optimized quantum circuit in our future work. This will result in a more effective and adaptable image encryption method.

Data availability

Data is provided within the manuscript.

Received: 24 December 2024; Accepted: 24 October 2025

Published online: 21 November 2025

References

- Liu, X.-D. et al. Quantum image encryption algorithm based on four-dimensional chaos. *Front. Phys.* **12**, 1230294. <https://doi.org/10.3389/fphy.2024.1230294> (2024).
- Dong, Y. & Yan, R. A new integrated steganography scheme for quantum color images. *J. Supercomput.* **80**, 24758–24780. <https://doi.org/10.1007/s11227-024-06332-1> (2024).
- Mou, D. & Dong, Y. Color image encryption algorithm based on quantum random walk and multiple reset scrambling. *Phys. Scr.* **99**(3), 035106. <https://doi.org/10.1088/1402-4896/ad22c2> (2024).
- Zhu, H.-H., Chen, Z.-G. & Leng, T. Random permutation-based mixed-double scrambling technique for encrypting MQIR image. *J. Appl. Phys.* **135**(1), 014401. <https://doi.org/10.1063/5.0177920> (2024).
- Hu, M., Li, J. & Di, X. Quantum image encryption scheme based on 2D Sine2-Logistic chaotic map. *Nonlinear Dyn.* **111**, 2815–2839. <https://doi.org/10.1007/s11071-022-07942-1> (2023).
- Xing, Z., Lam, C.-T., Yuan, X., Im, S.-K. & Machado, P. MMQW: Multi-modal quantum watermarking scheme. *IEEE Trans. Inf. Forensics Secur.* **19**, 5181–5195. <https://doi.org/10.1109/TIFS.2024.3394768> (2024).
- Gorle, R. & Guttavelli, A. A novel dynamic image watermarking technique with features inspired by quantum computing principles. *AIP Adv.* **14**, 045024. <https://doi.org/10.1063/5.0209417> (2024).
- Shi, L., Li, X., Jin, B. & Li, Y. A chaos-based encryption algorithm to protect the security of digital artwork images. *Mathematics* **12**(21), 3162 (2024).
- Lai, Q. & Liu, Y. A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map. *Expert Syst. Appl.* **223**, 119923. <https://doi.org/10.1016/j.eswa.2023.119923> (2023).
- Deng, Q., Wang, C., Sun, Y., Deng, Z. & Yang, G. Memristive Tabu learning neuron generated multi-wing attractor with FPGA implementation and application in encryption. *IEEE Trans. Circuits Syst. I Regul. Pap.* **72**(1), 300–311. <https://doi.org/10.1109/TC SI.2024.3439869> (2024).
- Lai, Q., Lai, C., Zhang, H. & Li, C. Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption. *Chaos Solitons Fractals* **158**, 112017. <https://doi.org/10.1016/j.chaos.2022.112017> (2022).
- Zhu, S., Deng, X., Zhang, W. & Zhu, C. Image encryption scheme based on newly designed chaotic map and parallel DNA coding. *Mathematics* **11**, 231. <https://doi.org/10.3390/math11010231> (2023).
- Alawida, M., Teh, J. S. & Alshoura, W. H. A new image encryption algorithm based on DNA state machine for UAV data encryption. *Drones* **7**, 38. <https://doi.org/10.3390/drones7020038> (2023).
- Li, Y., Li, C., Li, Y., Moroz, I. & Yang, Y. A joint image encryption based on a memristive Rulkov neuron with controllable multistability and compressive sensing. *Chaos Solitons Fractals* **182**, 114800. <https://doi.org/10.1016/j.chaos.2023.114800> (2024).
- Kong, X. et al. Memristor-induced hyperchaos, multiscroll and extreme multistability in fractional-order HNN: Image encryption and FPGA implementation. *Neural Netw.* **171**, 85–103. <https://doi.org/10.1016/j.neunet.2024.01.006> (2024).
- Verma, V. & Kumar, S. Quantum image encryption algorithm based on 3D-BNM chaotic map. *Nonlinear Dyn.* **113**, 3829–3855. <https://doi.org/10.1007/s11071-024-10403-6> (2025).
- Feng, W. et al. Exploiting newly designed fractional-order 3D lorenz chaotic system and 2D discrete polynomial hyper-chaotic map for high-performance multi-image encryption. *Fractal Fract.* **7**(12), 887 (2023).
- Shannon, C. E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**(4), 656–715. <https://doi.org/10.1002/j.1538-7305.1949.tb00928.x> (1949).
- Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoret. Comput. Sci.* **560**, 7–11. <https://doi.org/10.1016/j.tcs.2014.05.025> (2014).
- Saiyed, A. I. Optimizing quantum key distribution (QKD) protocols for secure communication in noisy quantum networks. *Ann. Appl. Sci.* **6**(1) (2025). Retrieved from <http://annalsofappliedsciences.com/index.php/aas/article/view/14>
- Xie, Y.-M. et al. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **3**, 020315. <https://doi.org/10.1103/prxquantum.3.020315> (2022).
- Zahidy, M. et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nat. Commun.* **15**, 1651. <https://doi.org/10.1038/s41467-024-45876-x> (2024).
- Zapatero, V., Navarrete, Á. & Curry, M. Implementation security in quantum key distribution. *Adv. Quantum Technol.* <https://doi.org/10.1002/qute.202300380> (2024).
- Yin, H.-L. et al. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **9**(4), nwac228. <https://doi.org/10.1093/nsr/nwac228> (2022).
- Rössler, O. E. An equation for hyperchaos. *Phys. Lett. A* **71**(2), 155–157. [https://doi.org/10.1016/0375-9601\(79\)90150-6](https://doi.org/10.1016/0375-9601(79)90150-6) (1979).
- Wang, X.-Y. & Wang, M.-J. A hyperchaos generated from Lorenz system. *Physica A* **387**(14), 3751–3758. <https://doi.org/10.1016/j.physa.2008.02.020> (2008).
- Feng, W. et al. Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform. *Mathematics* **10**(15), 2751. <https://doi.org/10.3390/math10152751> (2022).
- Chen, Y., Huang, H. & Tang, C. A novel adaptive image privacy protection method based on Latin square. *Nonlinear Dyn.* **112**, 10485–10508. <https://doi.org/10.1007/s11071-024-09580-1> (2024).
- Feng, W. et al. A novel multi-channel image encryption algorithm leveraging pixel reorganization and hyperchaotic maps. *Mathematics* **12**(24), 3917. <https://doi.org/10.3390/math12243917> (2024).
- Ma, X., Wang, Z. & Wang, C. An image encryption algorithm based on tabu search and hyperchaos. *Int. J. Bifurc. Chaos* **34**(14), 2450170. <https://doi.org/10.1142/S0218127424501700> (2024).
- Feng, W. et al. Exploiting robust quadratic polynomial hyperchaotic map and pixel fusion strategy for efficient image encryption. *Expert Syst. Appl.* **246**, 123190. <https://doi.org/10.1016/j.eswa.2024.123190> (2024).
- Feng, W., Zhang, J. & Qin, Z. A secure and efficient image transmission scheme based on two chaotic maps. *Secur. Commun. Netw.* **2021**, 1898998. <https://doi.org/10.1155/2021/1898998> (2021).
- Hosny, K. M., Kamal, S. T., Darwish, M. M. & Papakostas, G. A. New image encryption algorithm using hyperchaotic system and fibonacci Q-matrix. *Electronics* **10**(9), 1066. <https://doi.org/10.3390/electronics10091066> (2021).
- Chen, G. L. et al. QIRHSI: Novel quantum image representation based on HSI color space model. *Quantum Inf. Process.* **21**, 5. <https://doi.org/10.1007/s11128-021-03337-0> (2022).
- Senokosov, A., Sedykh, A., Sagingaliev, A., Kyriacou, B. & Melnikov, A. Quantum machine learning for image classification. *Mach. Learn. Sci. Technol.* **5**(1), 015040. <https://doi.org/10.1088/2632-2153/ad2aef> (2024).
- Le, P. Q., Dong, F. & Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Inf. Process.* **10**, 63–84. <https://doi.org/10.1007/s11128-010-0194-0> (2011).

37. Zhang, Y., Lu, K., Gao, Y. & Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **12**, 2833–2860. <https://doi.org/10.1007/s11128-013-0645-1> (2013).
38. Jiang, N., Wang, J. & Mu, Y. Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio. *Quantum Inf. Process.* **14**, 4001–4026. <https://doi.org/10.1007/s11128-015-0975-4> (2015).
39. Jiang, S.-X., Li, Y., Shi, J. & Zhang, R. Double quantum images encryption scheme based on chaotic system. *Chin. Phys. B* **33**(4), 040306. <https://doi.org/10.1088/1674-1056/ad1174> (2024).
40. El-Latif, A. A. A., Li, L., Wang, N., Han, Q. & Niu, X.-M. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **93**, 2986–3000. <https://doi.org/10.1016/j.sigpro.2013.03.031> (2023).
41. Aldin, S. S. A. B., Aykaç, M. & Aldin, N. B. Quad-color image encryption based on chaos and Fibonacci Q-matrix. *Multimedia Tools Appl.* **83**, 7827–7846. <https://doi.org/10.1007/s11042-023-15958-x> (2024).
42. Jiang, S. X. et al. Quantum block image encryption based on Arnold transform and improved zigzag transform. *Quantum Inf. Process.* **24**, 123. <https://doi.org/10.1007/s11128-025-04735-4> (2025).
43. Sari, C. A., Abdussalam, A., Rachmawanto, E. H. & Islam, H. M. M. Hybrid quantum representation and Hilbert scrambling for robust image watermarking. *Sci. J. Inform.* **11**(4), 873–880. <https://doi.org/10.15294/sji.v11i4.10140> (2024).
44. Cui, J., Li, W., Qiu, Y., Wei, Z. & Li, T. Quantum watermarking scheme based on a novel geometric transformation and Fibonacci scrambling. *Opt. Express* **33**, 17355–17377 (2025).
45. Ma, Y. & Zhou, N.-R. Quantum color image compression and encryption algorithm based on Fibonacci transform. *Quantum Inf. Process.* **22**, 39. <https://doi.org/10.1007/s11128-022-03749-6> (2023).
46. Cui, G. et al. Optical color image encryption algorithm based on two-dimensional quantum walking. *Electronics* **13**(11), 2026. <https://doi.org/10.3390/electronics13112026> (2024).
47. Agarwal, S., ByramDharmika, M., Dhathri, S., Thanikaiselvan, V., Subashanthini, S., & Amirtharajan, R. 4D-Rössler hyperchaotic system for image encryption and decryption with high security. In: *2024 10th International Conference on Communication and Signal Processing (ICCSP)* pp. 1016–1020. IEEE (2024). <https://doi.org/10.1109/ICCSP60870.2024.10544009>
48. Zhao, Y., Shi, Q. & Ding, Q. Cryptanalysis of an Image Encryption Algorithm Using DNA Coding and Chaos. *Entropy* **27**(1), 40. <https://doi.org/10.3390/e27010040> (2025).
49. Chen, Y., Tang, C. & Ye, R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **167**, 107286. <https://doi.org/10.1016/j.sigpro.2019.107286> (2019).
50. Feng, W., Qin, Z., Zhang, J. & Ahmad, M. Cryptanalysis and improvement of the image encryption scheme based on Feistel network and dynamic DNA encoding. *IEEE Access* **9**, 145459–145470. <https://doi.org/10.1109/ACCESS.2021.3123571> (2021).
51. Feng, W., He, Y., Li, H. & Li, C. Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. *IEEE Access* **7**, 12584–12597. <https://doi.org/10.1109/ACCESS.2019.2893760> (2019).
52. Lin, R. & Li, S. An image encryption scheme based on Lorenz hyperchaotic system and RSA algorithm. *Secur. Commun. Netw.* **2021**(1), 5586959. <https://doi.org/10.1155/2021/5586959> (2021).
53. Shi, J.-J., Chen, T., Chen, S.-H., Li, Q. & Shi, R.-H. Quantum image chaotic cryptography scheme based on Arnold transforms. *J. Electron. Inf. Technol.* **44**(9), 4284–4293. <https://doi.org/10.11999/JEIT211143> (2022).
54. Chen, S.-S., Hu, J., Wang, C.-P. & Lü, J.-H. Adaptive synchronization of uncertain Rössler hyperchaotic system based on parameter identification. *Phys. Lett. A* **321**(1), 50–55. <https://doi.org/10.1016/j.physleta.2003.12.011> (2004).
55. Airbus DS. Vision 1 Putrajaya Roundabout. Airbus Space Solutions (2021). <https://space-solutions.airbus.com/newsroom/satellite-e-image-gallery/various/vision-1-putrajaya-roundabout/>
56. SciJS. baboon-image. GitHub (2016). <https://github.com/scijs/baboon-image/blob/master/baboon.png>
57. Gao, J., Wang, Y., Song, Z. & Wang, S. Quantum image encryption based on quantum DNA codec and pixel-level scrambling. *Entropy* **25**(6), 865. <https://doi.org/10.3390/e25060865> (2023).
58. Kanwal, S. et al. A robust approach to satellite image encryption using chaotic map and circulant matrices. *Eng. Rep.* **6**, e13010. <https://doi.org/10.1002/eng2.1301> (2024).
59. Olvera-Martinez, L. et al. Symmetric grayscale image encryption based on quantum operators with dynamic matrices. *Mathematics* **13**(6), 982. <https://doi.org/10.3390/math13060982> (2025).

Acknowledgements

This research was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R759), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author contributions

1. Conceptualization, Methodology, Formal Analysis, Validation, Supervision: Saba Inam 2. Formal Analysis, Visualization, Validation: Shamsa Kanwal 3. Programming, Writing original Draft: Rehana Amir 4. Visualization, Review and editing Draft: Amel Ksibi 5. Additional experimental results, Review and editing Draft: Irum Matloob.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.I.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2025