

QE-CCHM: A Quantum-Walk-Enhanced Cross-Coupled Hyperchaotic Map with Broad Parameter-Domain Exploration and Its Application to Image Encryption

De Rosal Ignatius Moses Setiadi ^{1,*}, Supriadi Rustad ¹, T. Sutojo ¹, Muhamad Akrom ¹, Wise Herowati ¹, Pulung Nurtantio Andono ², Minh T. Nguyen ³, Deshinta Arrova Dewi ⁴, Danang ⁵, and Siti Umami Masrurroh ⁶

¹ Research Group for Quantum Computing and Materials Informatics, Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Semarang 50131, Indonesia; e-mail : moses@dsn.dinus.ac.id; srustad@dsn.dinus.ac.id; sutojo@dsn.dinus.ac.id; m.akrom@dsn.dinus.ac.id; wise@dsn.dinus.ac.id.

² Faculty of Intelligent Technology, Universitas Dian Nuswantoro, Semarang 50131, Indonesia; e-mail : pulung@dsn.dinus.ac.id

³ Thai Nguyen University of Technology, Thai Nguyen University, Thai Nguyen, 240000, Vietnam; e-mail : nguyentuanminh@tnut.edu.vn

⁴ Faculty of Data Science and Information Technology, INTI International University, Persiaran Perdana BBN, Putra Nilai, 71800 Nilai, Negeri Sembilan, Malaysia; e-mail : deshinta.ad@newinti.edu.my

⁵ Faculty of Academic Studies, Universitas Sains dan Teknologi Komputer, Semarang, Central Java 50192, Indonesia; e-mail : danang2@stekom.ac.id

⁶ Department of Informatics Engineering, Faculty of Science and Technology, Universitas Islam Negeri (UIN) Syarif Hidayatullah Jakarta, South Tangerang, Banten 15412, Indonesia; e-mail : ummi.masrurroh@uinjkt.ac.id

* Corresponding Author : De Rosal Ignatius Moses Setiadi 

Abstract: Chaotic and hyperchaotic systems have been widely investigated for pseudorandom sequence generation and image encryption, but many existing approaches remain limited by relatively narrow parameter regions and predominantly classical dynamics. This study proposes a Quantum-Walk-Enhanced Cross-Coupled Hyperchaotic Map (QE-CCHM), a hybrid classical–quantum dynamical framework that introduces process innovation by integrating nonlinear cross-coupled classical states with two discrete-time quantum walks (DTQWs) through bidirectional measurement feedback. The quantum observables dynamically influence the classical states and the coin angles of the coupled DTQW subsystems, making quantum evolution an integral component of the dynamical process. The proposed system is evaluated using phase-space trajectories, bifurcation diagrams, Lyapunov exponents (LE), and broad parameter-domain exploration. In the investigated region $3.5 \leq \xi \leq 50$, both leading LEs remain positive across all 100 evaluated parameter values, increasing from 6.2501 and 5.3408 at $\xi=3.5$ to 9.5432 and 8.6661 at $\xi=50$. A global exploration further investigates ξ from 10^{-2} to approximately 10^{308} , including 10,033 evaluations across the extended positive-parameter domain. The resulting sequences exhibit high normalized entropy and low lag-1 autocorrelation across widely separated parameter scales. For application validation, the generated sequences are applied to a reversible image-encryption scheme combining pixel permutation and modular substitution. Across six grayscale images, entropy exceeds 7.998 bits/pixel, adjacent-pixel correlations approach zero, and NPCR and UACI range from 99.59% to 99.63% and 33.09% to 33.69%, respectively, demonstrating the potential of QE-CCHM for pseudorandom sequence generation and image encryption.

Keywords: Chaotic image encryption; Cross-coupled hyperchaotic map; Discrete-time quantum walk; Image encryption; Lyapunov exponent; Pseudorandom sequence; Quantum computing; Quantum-enhanced dynamics.

Received: August, 8th 2026

Revised: October, 10th 2026

Accepted: October, 17th 2026

Published: October, 18th 2026



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) licenses (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

The rapid development of digital communication, the Internet of Things (IoT), cloud computing, and multimedia applications has increased the need for data-protection

mechanisms that can preserve confidentiality and withstand statistical analysis [1]–[5]. Digital images require particular attention because of their relatively large size, high redundancy, and strong correlations between neighboring pixels. These characteristics make the generation of pseudorandom sequences with high complexity, sensitivity to initial conditions, and favorable statistical properties an important component of image-oriented security systems [6]–[8].

Chaotic maps have been widely investigated as sources of pseudorandom sequences for security applications because of their deterministic, nonlinear, and initial-condition-sensitive behavior [6], [9]–[11]. Classical chaotic maps, such as the logistic, sine, and tent maps, have been employed to generate sequences for confusion and diffusion processes. However, low-dimensional systems generally exhibit relatively simple dynamical structures and limited parameter regions. Moreover, the presence of chaotic behavior in a particular parameter region does not necessarily imply that the resulting sequences possess statistical characteristics suitable for security applications. These issues motivate the development of dynamical systems with greater complexity and more flexible operating characteristics.

One approach to increasing dynamical complexity is the use of hyperchaotic systems. Unlike conventional chaotic systems, which typically exhibit one positive Lyapunov exponent, hyperchaotic systems are characterized by at least two positive Lyapunov exponents, indicating expansion along multiple directions in the phase space [12]–[14]. This property can generate more complex trajectories and provide greater diversity for pseudorandom sequence generation [15], [16]. Nevertheless, increasing the complexity or dimensionality of a classical system alone does not necessarily guarantee improved sequence characteristics. Hyperchaotic systems may still exhibit restricted operating regions, specific orbit structures, or sensitivity to parameter and numerical configurations. Therefore, alternative mechanisms that can enrich nonlinear dynamics beyond purely classical evolution remain of interest.

Quantum computing provides an opportunity to combine quantum dynamics with nonlinear classical systems [17]. Among quantum computational models, the discrete-time quantum walk (DTQW) is particularly attractive because of its superposition, interference, and unitary evolution. Unlike a classical random walk, a DTQW evolves a quantum state through interactions between coin and position spaces, producing state distributions through quantum interference. These characteristics have motivated the use of quantum walks in sequence generation and cryptographic applications [18], [19]. However, existing quantum-walk-based approaches commonly employ quantum walks as key-generation, keystream, or transformation components, rather than integrating quantum evolution directly into the dynamics of a classical chaotic system. Such integration requires an explicit coupling mechanism that preserves deterministic and reproducible system evolution.

Another issue concerns the evaluation of chaotic systems over broad parameter domains. Many studies focus on selected parameter intervals to identify chaotic regions and then choose several operating points for subsequent applications. Although such analysis is useful for characterizing local dynamical behavior, it provides limited information about whether desirable dynamical and sequence characteristics persist across widely separated parameter scales [20]–[22]. A systematic parameter exploration can therefore provide a broader view of the robustness and flexibility of a proposed dynamical system and support more informed selection of operating configurations.

Motivated by these considerations, this study proposes the Quantum-Walk-Enhanced Cross-Coupled Hyperchaotic Map (QE-CCHM), a hybrid classical–quantum dynamical framework that integrates nonlinear cross-coupled classical states with two discrete-time quantum walks. The proposed framework employs a bidirectional quantum–classical feedback mechanism in which the evolving classical states and quantum observables jointly influence the quantum-walk evolution, while the resulting quantum observables are fed back into the classical dynamics. Consequently, the quantum subsystem becomes an integral component of the iterative dynamical process rather than an auxiliary randomization or post-processing module.

The proposed system is investigated through dynamical analysis and large-scale parameter exploration to characterize its behavior and identify configurations suitable for pseudorandom sequence generation. The generated sequences are subsequently evaluated statistically and applied to image encryption to examine their practical applicability in a security-oriented task. The encryption framework is designed as a reversible permutation–substitution scheme, allowing the properties of the generated sequences to be assessed directly through established image-security indicators. The main contributions of this study are as follows:

- A Quantum-Walk-Enhanced Cross-Coupled Hyperchaotic Map (QE-CCHM) is developed by integrating nonlinear classical dynamics with two coupled DTQW subsystems through bidirectional quantum–classical feedback.
- The dynamical characteristics and parameter robustness of QE-CCHM are systematically investigated using phase-space analysis, bifurcation analysis, Lyapunov spectra, and large-scale parameter exploration.
- The generated sequences are evaluated using statistical and temporal characteristics and applied to a reversible image-encryption scheme to assess their practical applicability.

The remainder of this paper is organized as follows. Section 2 reviews related studies on chaotic and hyperchaotic systems and quantum walks for sequence generation and cryptographic applications. Section 3 presents the proposed QE-CCHM, including its classical formulation, DTQW subsystems, quantum–classical coupling mechanism, and iterative algorithm. Section 4 analyzes the dynamical properties and sequence characteristics of the proposed system. Section 5 presents the image-encryption application and its security analysis. Finally, Section 6 concludes the paper and discusses its limitations and directions for future work.

2. Related Work and Theoretical Background

2.1. Classical chaotic and hyperchaotic systems

Chaotic systems have long been employed in information security, particularly for generating pseudorandom sequences in applications such as image encryption. Low-dimensional chaotic maps, including the Logistic, Sine, Tent, and Hénon maps, have been widely used because of their simple iterative structures and low computational cost [23]. However, the quality of a chaotic map is not determined solely by the presence of chaotic behavior, but also by the size of its chaotic parameter region, sensitivity, state distribution, and robustness to finite-precision effects. Limited parameter regions may reduce the effective key space and increase the possibility of parameter-estimation-based attacks [24]. Subsequent developments have focused on hybrid, coupled, and multidimensional chaotic systems that combine multiple nonlinear mechanisms to achieve more complex dynamics. For example, the Logistic–Tent–Sine (LTS) map combines Logistic, Sine, and Tent nonlinearities and has been reported to provide an expanded chaotic region, enhanced sensitivity and ergodicity, and sequences suitable for cryptographic applications [24]. Coupled maps have also been employed to strengthen nonlinear interactions and feedback mechanisms. Wang et al. [25] developed a 3DSHCM based on Sine and Hénon dynamics, which was reported to exhibit a wider continuous chaotic range, larger Lyapunov exponents, and a more uniform phase-space distribution than several low-dimensional chaotic maps.

In addition to coupling, the complexity of dynamical systems has been enhanced through hyperchaotic systems, which are generally characterized by at least two positive Lyapunov exponents. This characteristic provides multiple expanding directions and additional degrees of freedom in the phase space, making hyperchaotic systems attractive for sequence generation as well as the construction of permutation, diffusion, and encryption parameters [12], [26]. Various four-dimensional and higher-dimensional hyperchaotic systems have been applied to image encryption, including combinations with DNA coding, domain transformations, and confusion-diffusion mechanisms [27]. Other studies have explored fractional-order dynamics, state-dependent parameters, coupling, and combinations of multiple nonlinear maps to obtain more flexible dynamical behavior [28], [29]. Among these approaches, state-dependent variable fractional-order hyperchaotic dynamics and coupling-enhanced cubic hyperchaotic maps have been employed for image protection [30], while other hyperchaotic approaches have been combined with additional cryptographic mechanisms [27], [31], [32]. Nevertheless, increasing the dimensionality or complexity of a dynamical system does not automatically guarantee cryptographic security. The characteristics of the chaotic source still need to be validated through analyses such as phase-space trajectories, bifurcation diagrams, Lyapunov exponents, entropy, sensitivity, and randomness testing. For example, in 3DSHCM, parameter analysis and Lyapunov exponents were combined with entropy and NIST testing, whereas the LTS study associated the expansion of the chaotic region with an increase in effective key space and improved resistance to parameter inference [24].

Furthermore, cryptanalysis has shown that the security of chaos-based schemes also depends on the overall algorithmic design, including key structure, diffusion mechanisms, and interactions between encryption stages. Several chaotic schemes have been reported to exhibit issues such as equivalent keys, fixed keystreams, inadequate diffusion, and vulnerability to chosen-plaintext attacks [33], [34]. Therefore, chaotic or hyperchaotic systems should be regarded as one component of a cryptographic design rather than as a guarantee of security by themselves [35]. Based on these developments, there is a clear progression from simple chaotic maps toward hybrid and hyperchaotic systems with richer dynamics and broader parameter domains. However, most existing studies still focus on relatively limited parameter regions and selected operating points. Exploring whether a dynamical system can maintain favorable chaotic characteristics across an extremely broad parameter domain therefore remains an interesting direction for further investigation.

2.2. Quantum walks for random sequence generation and cryptography

Discrete-time quantum walk (DTQW) extends the concept of a classical random walk into the framework of quantum mechanics. Unlike a classical random walk, which uses transition probabilities between positions, a DTQW represents the state as a quantum superposition that evolves through a combination of operations in the coin space and position space [36], [37]. This evolution enables the system to produce state distributions resulting from quantum interference and unitary evolution.

The superposition and interference properties of quantum walks have motivated their use in various areas of quantum computing, including quantum search, quantum simulation, random sequence generation, and cryptographic applications. In the context of information security, several studies have explored quantum walks as sources of keystreams, transformation mechanisms, or components of image-encryption systems [38], [39]. These approaches indicate that the measurement outcomes of quantum walks can be utilized to generate values with characteristics that differ from conventional deterministic chaotic sequences. Quantum-walk-based image encryption has also developed through various strategies, including the use of probability distributions obtained from quantum walks to construct keys or keystreams and their integration with classical cryptographic algorithms [40]–[42].

These hybrid approaches demonstrate the potential of quantum walks to increase the complexity of data-transformation processes. However, in the approaches reported so far, quantum walks are generally employed as processing components, key-generation mechanisms, or keystreams within encryption systems, whereas their integration as an intrinsic part of a dynamical map coupled with classical chaotic dynamics remains relatively limited. The use of a quantum walk in cryptography does not, by itself, produce a chaotic or hyperchaotic system; an explicit coupling mechanism is required to connect the evolution of classical and quantum states. From this perspective, DTQW provides an attractive mechanism for establishing such an interaction, for example, by mapping quantum observables back to the classical domain as states or control parameters. Such an approach allows the quantum component to participate directly in the formation of the system dynamics rather than serving merely as an additional source of randomness.

2.3. Research Gap and Motivation

Although various chaotic and hyperchaotic systems have been developed for pseudorandom sequence generation and information security, there remains room for systems that integrate the complexity of classical dynamics with quantum evolution mechanisms in a more intrinsic manner. DTQW-based research has demonstrated the potential of quantum superposition, interference, and measurement outcomes for sequence generation and cryptographic applications [36]–[42]. However, in the approaches discussed above, quantum walks generally serve as components for key generation, keystream construction, or transformation within an encryption algorithm rather than being directly coupled with the evolution of classical chaotic states.

On the other hand, research on hybrid, coupled, and hyperchaotic systems has shown that increased nonlinear interactions can produce more complex dynamics and broaden chaotic operating regions [12], [24]–[32]. However, such increases in complexity are generally constructed entirely within the classical domain. This creates an opportunity to explore a hybrid dynamical system that integrates classical nonlinear evolution with quantum-walk

dynamics through a unified deterministic coupling and feedback mechanism. Another aspect that remains relatively underexplored is the breadth of the parameter domain. Most analyses of chaotic systems are conducted over specific parameter ranges to identify chaotic regions, followed by the selection of several operating points. Such an approach is important for validating local dynamical behavior, but it does not directly demonstrate whether a system can maintain characteristics suitable for sequence generation when its parameters are explored across an extremely broad domain. The breadth of the parameter region that produces favorable sequences may be important for system configuration flexibility and the formation of the effective key space.

Motivated by these gaps, this study develops the Quantum-Enhanced Cross-Coupled Hyperchaotic Map (QE-CCHM) as a classical–quantum dynamical framework that integrates classical nonlinear dynamics and DTQW through coupling and measurement feedback mechanisms. Unlike approaches that use quantum walks merely as additional components of cryptographic algorithms, QE-CCHM places quantum evolution directly within the process that forms the system dynamics. The study therefore not only evaluates the presence of hyperchaotic behavior at selected parameter values, but also explores the system characteristics across an extremely broad ξ domain before determining suitable operating regions for pseudorandom sequence generation and image-encryption applications.

3. Proposed QE-CCHM

3.1. Classical coupled-map formulation

The classical component of the proposed Quantum-Embedded Cross-Coupled Hyperchaotic Map (QE-CCHM) consists of two nonlinear state variables x_n and y_n , which are mutually coupled through nonlinear trigonometric terms. The classical dynamics are further influenced by quantum feedback obtained from two discrete-time quantum walks (DTQW-X and DTQW-Y). For a given control parameter ξ , the intermediate nonlinear functions are defined as:

$$F_x(x_n, y_n, \xi) = \pi \xi x_n (1 - x_n) + \pi \sin\left(\frac{\xi(1 - \xi)}{y_n^*}\right) + e, \quad (1)$$

and

$$F_y(x_n, y_n, \xi) = \pi(1 - \xi)y_n(1 - y_n) + \pi \sin\left(\frac{x_n}{\xi}\right) + e, \quad (2)$$

where y_n^* denotes a numerically regularized value of y_n . Specifically,

$$y_n^* = \begin{cases} \delta, & |y_n| < \delta, y_n \geq 0, \\ -\delta, & |y_n| < \delta, y_n < 0, \\ y_n, & |y_n| \geq \delta, \end{cases} \quad (3)$$

where δ prevents numerical instability caused by the denominator approaching zero. This regularization is explicitly implemented in the QE-CCHM map used for the global parameter exploration. The classical states are then updated using the quantum feedback terms:

$$x_{n+1} = \sin[F_x(x_n, y_n, \xi) + \kappa q_{y,n}], \quad (4)$$

$$y_{n+1} = \sin[F_y(x_n, y_n, \xi) + \kappa q_{x,n}], \quad (5)$$

where $q_{x,n}$ and $q_{y,n}$ are quantum observables generated by DTQW-X and DTQW-Y, respectively, and κ controls the strength of quantum feedback. Importantly, the feedback is cross-coupled: the observable generated by the Y -walk affects the X -state, while the observable generated by the X -walk affects the Y -state. This structure is directly implemented in the classical–quantum map.

3.2. Quantum Discrete-Time Quantum Walk formulation

The quantum component of QE-CCHM consists of two coupled DTQW subsystems, denoted DTQW-X and DTQW-Y. Each DTQW uses one coin qubit and two position qubits,

resulting in $N_{\text{qubits}} = 3$ and $N_{\text{qubits}} = 2^2 = 4$. Consequently, each quantum walk operates in an eight-dimensional Hilbert space. The notebook explicitly defines one coin qubit and two position qubits for this construction. For a coin angle θ , the quantum coin operation is represented by an $R_Y(\theta)$ rotation,

$$R_Y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \quad (6)$$

The coin operator is extended to the complete coin-position Hilbert space as $C(\theta) = R_Y(\theta) \otimes I_4$. The conditional shift operator S moves the quantum walker according to the state of the coin. When the coin state is 0, the position is shifted one step in the negative direction, whereas coin state 1 shifts the position one step in the positive direction. The position space is periodic, such that the four positions form a cycle. The corresponding DTQW unitary is therefore:

$$U_{\text{DTQW}}(\theta) = SC(\theta) = S[R_Y(\theta) \otimes I_4] \quad (7)$$

For a quantum state $|\psi_n\rangle$, one DTQW evolution step is

$$|\psi_{n+1}\rangle = U_{\text{DTQW}}(\theta_n)|\psi_n\rangle \quad (8)$$

This evolution is implemented directly in the notebook through the matrix product $U = SC$.

The corresponding quantum-circuit representations of the two DTQW subsystems are illustrated in Figure 1. Both circuits employ one coin qubit and two position qubits and realize the coin operation followed by the conditional position-shift mechanism. The DTQW-X and DTQW-Y subsystems share the same overall walk structure, while their quantum operations are associated with the respective x - and y -components of the proposed map.

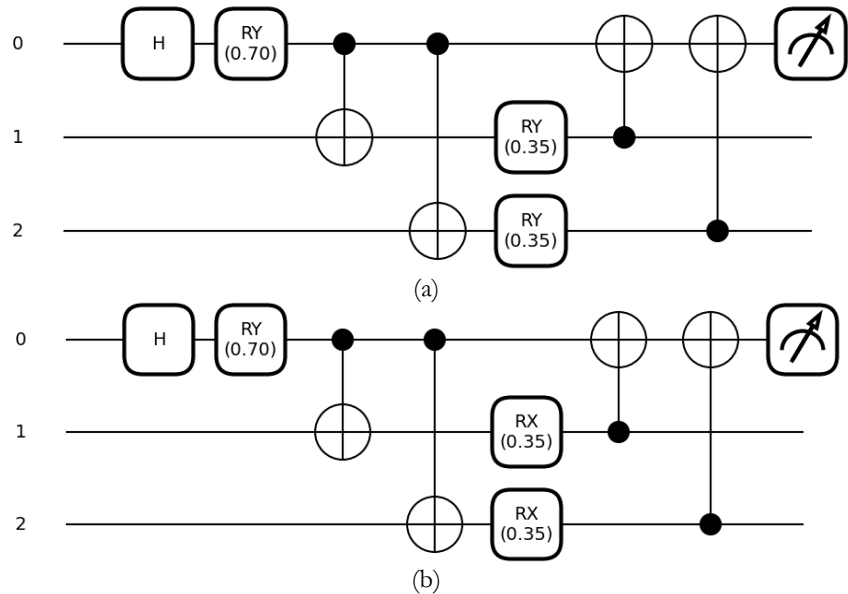


Figure 1. Quantum circuits employed in the two DTQW subsystems: (a) DTQW-X; and (b) DTQW-Y.

The two DTQW subsystems employ the same three-qubit architecture, consisting of one coin qubit and two position qubits. As shown in Fig. 1(a), DTQW-X applies an R_Y rotation to the coin qubit and R_Y rotations to the position qubits. In contrast, DTQW-Y uses the same R_Y coin operation but applies R_X rotations to the position qubits, as shown in Fig. 1(b). Both circuits incorporate controlled shift operations and Z-basis measurement of the coin qubit to obtain the quantum observables used in the subsequent feedback mechanism.

The rotation values displayed in Figure 1, namely 0.70 and 0.35, are used only for circuit visualization and should not be interpreted as fixed QE-CCHM parameters. In the proposed algorithm, the effective coin angles are dynamically determined during the iterative evolution.

Thus, the circuit figures are intended to illustrate the gate structure and information flow of the DTQW subsystems rather than specify a particular operating parameter.

Each DTQW is initialized from the computational basis state $|\psi_0\rangle = |000\rangle$, corresponding to an eight-dimensional state vector whose first amplitude is one and all remaining amplitudes are zero. The same initialization is used for both DTQW-X and DTQW-Y. The quantum observable used to provide feedback to the classical system is the expectation value of the coin Z observable. For each quantum state, the probabilities associated with coin states 0 and 1 are obtained by summing the probabilities over the four position states,

$$p_0 = \sum_{j=0}^3 |\psi_j|^2, \quad p_1 = \sum_{j=0}^3 |\psi_{4+j}|^2 \quad (9)$$

The resulting observable is,

$$q_n = p_0 - p_1 = \langle \psi_n | Z \otimes I_4 | \psi_n \rangle \quad (10)$$

The same procedure is applied independently to DTQW-X and DTQW-Y to obtain $q_{x,n}$ and $q_{y,n}$.

3.3. Classical–quantum coupling mechanism

The main characteristic of QE-CCHM is that the DTQW coin parameters are dynamically determined by the classical states and the observable produced by the opposite quantum subsystem. For DTQW-X, the coin angle is in Equation (11) while DTQW-Y uses Equation (12).

$$\theta_{x,n} = \pi \left(\frac{x_n + 1}{2} \right) + \kappa \pi q_{y,n}^{(old)} \quad (11)$$

$$\theta_{y,n} = \pi \left(\frac{y_n + 1}{2} \right) + \kappa \pi q_{x,n}^{(old)} \quad (12)$$

Here, $q_{x,n}^{(old)}$ and $q_{y,n}^{(old)}$ denote the observables extracted from the current quantum states before the next DTQW step. The functions $\theta_{x,n}$ and $\theta_{y,n}$ determine the coin rotation angles for DTQW-X and DTQW-Y, respectively, based on the corresponding classical variables and the observable from the other quantum subsystem. Thus, the quantum walk is not driven solely by the classical variables; instead, the coin rotation angles are dynamically influenced by both classical states and cross-coupled quantum observables, establishing an interaction between the two DTQW subsystems and the classical dynamics. Instead,

$$x_n \rightarrow \theta_{x,n}, \quad q_{y,n}^{(old)} \rightarrow \theta_{x,n}, \quad (13)$$

and

$$y_n \rightarrow \theta_{y,n}, \quad q_{x,n}^{(old)} \rightarrow \theta_{y,n}, \quad (14)$$

After the corresponding DTQW evolutions, new observables $q_{x,n}^{(new)}$ and $q_{y,n}^{(new)}$ are extracted and fed back into the classical map:

$$x_{n+1} = \sin[F_x(x_n, y_n, \xi) + \kappa q_{y,n}^{(new)}] \quad (15)$$

$$y_{n+1} = \sin[F_y(x_n, y_n, \xi) + \kappa q_{x,n}^{(new)}] \quad (16)$$

Therefore, the coupling is bidirectional and cross-dependent:

$$x_n \rightarrow DTQW - X \rightarrow q_{x,n} \rightarrow y_n + 1, \quad (13)$$

while

$$y_n \rightarrow DTQW - Y \rightarrow q_{y,n} \rightarrow x_n + 1 \quad (14)$$

At the same time, the previous quantum observables affect the opposite DTQW coin angles. The implementation follows this ordering explicitly: current q_x, q_y are first obtained, then θ_x, θ_y are calculated, each DTQW is evolved, new observables are extracted, and only then are the classical states updated. This feedback architecture is the key mechanism through which the classical nonlinear dynamics and quantum walk dynamics become an integrated dynamical system rather than two independent processes.

3.4. Complete QE-CCHM algorithm

Based on the classical coupled-map formulation and the two DTQW subsystems described above, QE-CCHM operates through an iterative classical–quantum feedback loop. The complete computational workflow is illustrated in Figure 2, where the classical states x_n and y_n determine the quantum coin angles, while the quantum observables obtained from the DTQW subsystems are fed back into the classical map.

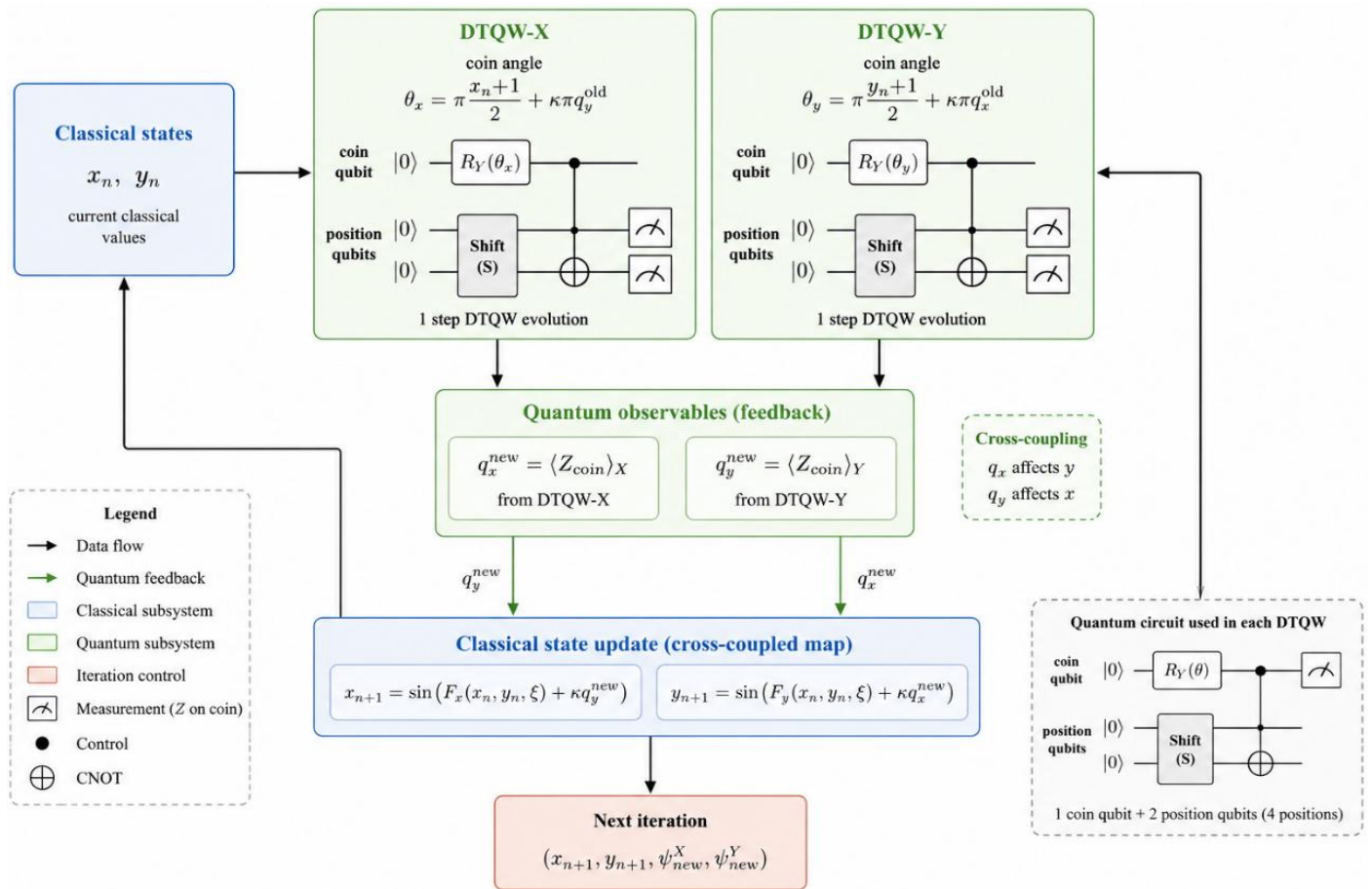


Figure 2. Complete computational workflow of the proposed QE-CCHM, showing the bidirectional classical–quantum feedback between the cross-coupled classical map and the two DTQW subsystems.

At the beginning of the iteration, the system is initialized with the classical states x_n and y_n together with the corresponding quantum states of the DTQW-X and DTQW-Y subsystems. The current quantum observables are first obtained from the respective quantum states. These observables are then combined with the current classical states to determine the dynamically varying coin angles θ_x and θ_y . Thus, the quantum evolution is not driven by a fixed coin parameter, but is dynamically modulated by the evolving classical system.

The two DTQW subsystems subsequently perform one quantum-walk evolution using the $R_Y(\theta)$ coin operation followed by the conditional shift operation. The quantum states are then measured through the Z -observable of the coin qubit to obtain the updated feedback values $q_x^{(\text{new})}$ and $q_y^{(\text{new})}$. As shown in Fig. 2, these quantum observables are cross-

coupled into the classical subsystem: $q_y^{(new)}$ contributes to the update of x , whereas $q_x^{(new)}$ contributes to the update of y .

The resulting classical states are therefore determined jointly by the nonlinear classical interaction and the quantum feedback: $(x_n, y_n, q_x^{(new)}, q_y^{(new)}) \rightarrow (x_{n+1}, y_{n+1})$. The newly obtained classical states are then used to determine the coin angles of the next DTQW evolution, closing the classical–quantum feedback loop. Consequently, each iteration consists of classical-state evolution, quantum-walk evolution, quantum observation, and cross-coupled classical feedback rather than independent execution of a classical map and a quantum circuit. The complete iterative process can therefore be summarized as:

$$(x_n, y_n, q_{x,n}^{(old)}, q_{y,n}^{(old)}) \rightarrow (\theta_x, \theta_y) \rightarrow \text{DTQW} - X, \text{DTQW} - Y \rightarrow (q_{x,n}^{(new)}, q_{y,n}^{(new)}) \rightarrow (x_{n+1}, y_{n+1}) \quad (19)$$

which is repeated for the required number of iterations. This architecture makes the quantum subsystem an integral component of the dynamical evolution rather than an external post-processing or randomization module.

The latter was indeed too generic and did not reflect the actual two-DTQW feedback loop in the notebook. More specifically, the complete steps are:

- Step 1 — Initialization: Set the classical initial states, for example $x_0 = 0.37$, $y_0 = 0.61$, and initialize two quantum states, $|\psi_{x,0}\rangle = |000\rangle$ and $|\psi_{y,0}\rangle = |000\rangle$. The global exploration code uses these same initial conditions.
- Step 2 — Extract current quantum observables: Calculate $q_{x,n}^{(old)} = \langle \psi_{x,n} | Z_c | \psi_{x,n} \rangle$ and $q_{y,n}^{(old)} = \langle \psi_{y,n} | Z_c | \psi_{y,n} \rangle$
- Step 3 — Generate dynamically coupled coin angles: Calculate $\theta_{x,n} = \pi \frac{x_{n+1}}{2} + \kappa \pi q_{y,n}^{(old)}$ and $\theta_{y,n} = \pi \frac{y_{n+1}}{2} + \kappa \pi q_{x,n}^{(old)}$
- Step 4 — Perform DTQW evolution: For each subsystem, $|\psi_{x,n+1}\rangle = S[R_Y(\theta_{x,n}) \otimes I_4] |\psi_{x,n}\rangle$ and $|\psi_{y,n+1}\rangle = S[R_Y(\theta_{y,n}) \otimes I_4] |\psi_{y,n}\rangle$. The notebook implements the DTQW step exactly as $|\psi'\rangle = U(\theta)|\psi\rangle$, $U(\theta) = S[R_Y(\theta) \otimes I_4]$.
- Step 5 — Obtain new quantum feedback: Calculate $q_{x,n}^{(new)} = \langle \psi_{x,n+1} | Z_c | \psi_{x,n+1} \rangle$ and $q_{y,n}^{(new)} = \langle \psi_{y,n+1} | Z_c | \psi_{y,n+1} \rangle$.
- Step 6 — Update classical states: calculate $F_x = \pi \xi x_n (1 - x_n) + \pi \sin\left(\frac{\xi(1-\xi)}{y_n^*}\right) + e$ and $F_y = \pi \xi y_n (1 - y_n) + \pi \sin\left(\frac{x_n}{\xi}\right) + e$. Then apply quantum feedback: $x_{n+1} = \sin\left[F_x + \kappa q_{y,n}^{(new)}\right]$ and $y_{n+1} = \sin\left[F_y + \kappa q_{x,n}^{(new)}\right]$. This is precisely the update implemented in `cqhc_map()` in the DTQW-based version.
- Step 7 — Repeat: The resulting $(x_{n+1}, y_{n+1}, \psi_{x,n+1}, \psi_{y,n+1})$ becomes the state for the next iteration.

4. Dynamical Properties and Chaotic Sequence Evaluation

To evaluate the dynamical characteristics of QE-CCHM, a series of experiments was conducted, including phase-space trajectory analysis, bifurcation analysis, Lyapunov spectrum analysis, and exploration of the ξ parameter domain. The primary objective was to assess whether the interactions between the cross-coupled classical dynamics and the two DTQW subsystems produce complex dynamical behavior that persists across a broad range of parameter values. Unless otherwise stated, the initial conditions were set to $x_0 = 0.37$ and $y_0 = 0.61$, while the coupling parameters were fixed at $\kappa = 0.10$, $\alpha = 0.10$, $\gamma = 0.05$, and $\delta = 0.001$. Parameter ξ was used as the primary control parameter.

4.1. Phase-space trajectories

The phase-space behavior of QE-CCHM was first examined to visualize the evolution of the coupled classical states under representative values of the control parameter ξ . Figure 3 shows the resulting trajectories for $\xi = 4, 10, 20$, and 50.

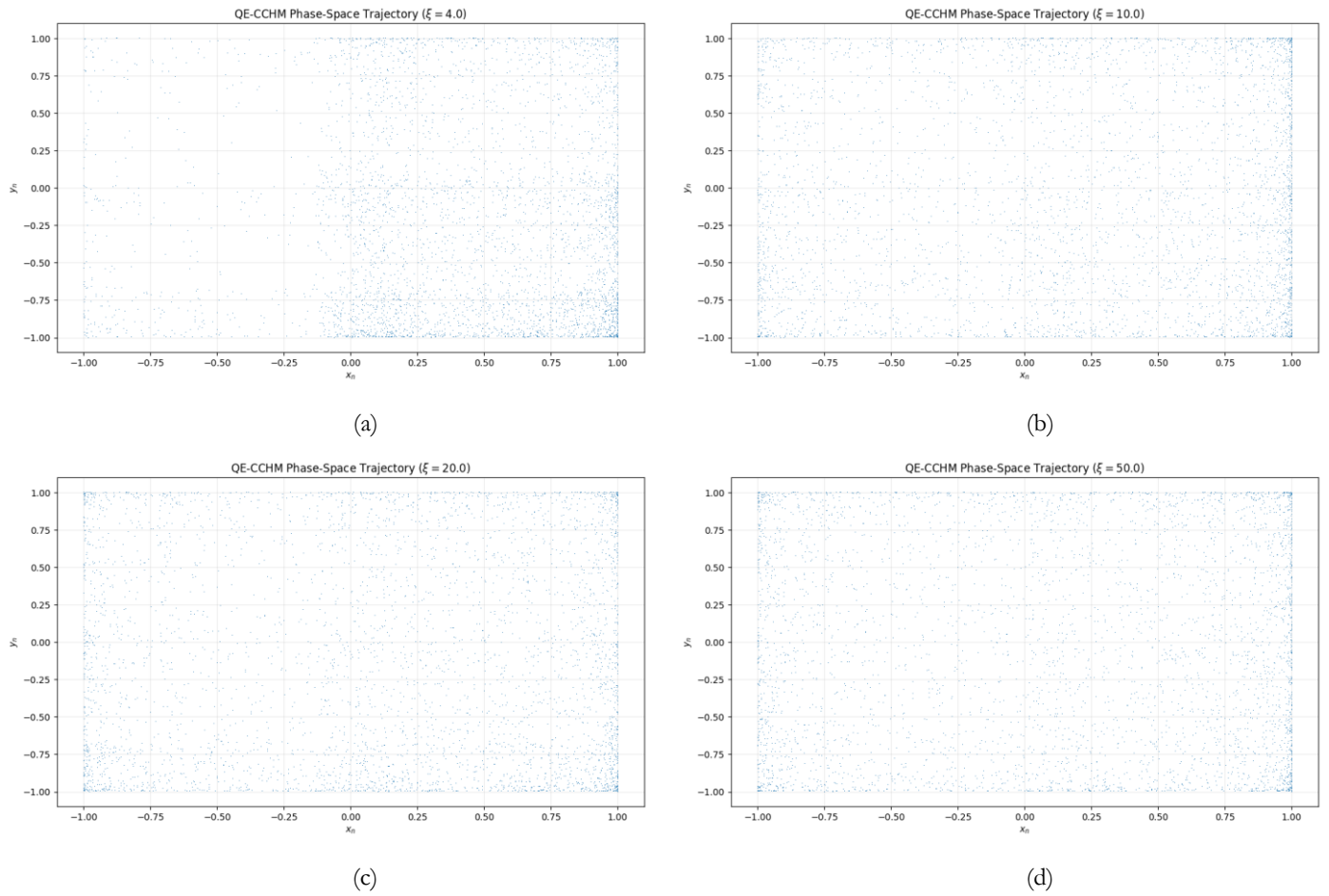


Figure 3. Phase-space trajectories of QE-CCHM for representative values of the control parameter ξ : (a) $\xi=4$; (b) $\xi=10$; (c) $\xi=20$; and (d) $\xi=50$.

At $\xi=4$, the trajectory already covers a relatively broad region of the x , y phase space, although several areas remain sparsely populated. As ξ increases to 10, 20, and 50, the trajectories become increasingly dispersed and occupy a larger portion of the state space. The trajectories remain bounded within the effective state range while exhibiting no visually apparent convergence toward a fixed point or a small periodic orbit. These results provide an initial indication that the control parameter ξ strongly influences the dynamical structure of QE-CCHM. In particular, the increasingly widespread phase-space occupation suggests richer state evolution at larger ξ . Nevertheless, phase-space visualization alone cannot establish chaotic or hyperchaotic behavior; quantitative confirmation is therefore provided through the bifurcation and Lyapunov analyses in the following subsections.

4.2. Bifurcation analysis

Bifurcation analysis was conducted to investigate how the long-term dynamics of QE-CCHM evolve as the control parameter ξ varies. The resulting bifurcation diagrams of the two classical state variables, x_n and y_n , are shown in Fig. 4(a) and Fig. 4(b), respectively, while the corresponding quantum observables q_x and q_y are presented in Fig. 4(c).

As shown in Fig. 4(a), the x_n trajectories become increasingly dispersed as ξ increases, with the state values occupying a broad region of the accessible state space. A similar pattern is observed for y_n in Fig. 4(b), where the trajectories remain widely distributed over the investigated parameter range. The absence of a dominant set of discrete branches indicates that the system does not remain confined to a simple periodic orbit as the control parameter varies. The quantum observables in Fig. 4(c) also exhibit irregular and broadly distributed behavior across the ξ -domain. Both q_x and q_y cover a substantial range of values and vary continuously with the control parameter. This behavior is consistent with the role of the quantum

subsystem in QE-CCHM, where the quantum observables are generated from the evolving quantum states and subsequently incorporated as feedback into the classical cross-coupled map.

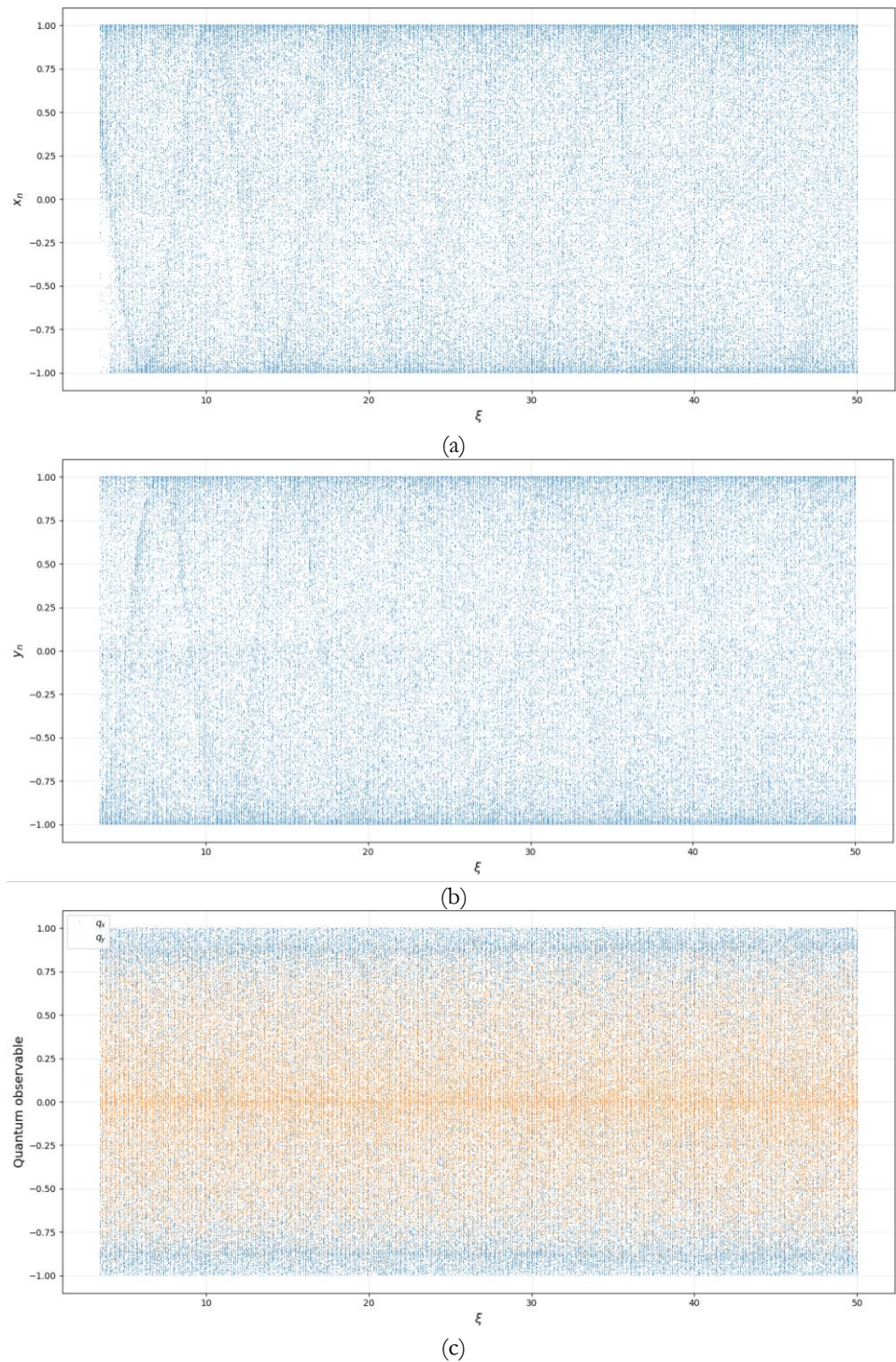


Figure 4. Bifurcation diagrams of QE-CCHM over the investigated ξ -range: (a) classical state x_n ; (b) classical state y_n ; and (c) quantum observables q_x and q_y .

At the lower end of the investigated parameter range, particularly around $\xi = 4$, the distribution of x_n is somewhat less dense in the central region than that observed at larger values of ξ . This observation is consistent with the phase-space trajectories discussed in Section 4.1, where the state-space coverage at $\xi = 4$ was also less uniform. Nevertheless, the trajectories do not collapse into a fixed point or a clearly dominant periodic structure. As ξ

increases, the distributions become progressively denser and more broadly dispersed. Overall, the bifurcation diagrams demonstrate that QE-CCHM exhibits rich parameter-dependent dynamics over a wide ξ -range. However, bifurcation structure alone is not sufficient to establish hyperchaotic behavior; therefore, the dynamical nature of these regions is further quantified using the Lyapunov spectrum in Section 4.3.

4.3. Lyapunov spectrum

To quantitatively characterize the dynamical behavior indicated by the phase-space and bifurcation analyses, the Lyapunov spectrum of QE-CCHM was evaluated over the investigated control-parameter range. The resulting first and second Lyapunov exponents, λ_1 and λ_2 , are shown in Fig. 5. Both exponents remain positive throughout the entire investigated range of ξ . At the lower boundary, $\xi = 3.5$, the obtained values are $\lambda_1 = 6.2501$ and $\lambda_2 = 5.3408$. The two exponents generally increase as ξ increases, although moderate fluctuations are observed along the parameter sweep. At $\xi = 50$, the corresponding values are $\lambda_1 = 9.5432$ and $\lambda_2 = 8.6661$. Among the 100 evaluated parameter values, the minimum values of λ_1 and λ_2 are 6.2501 and 5.3408, respectively, while the maximum values reach approximately 9.60 and 8.84.

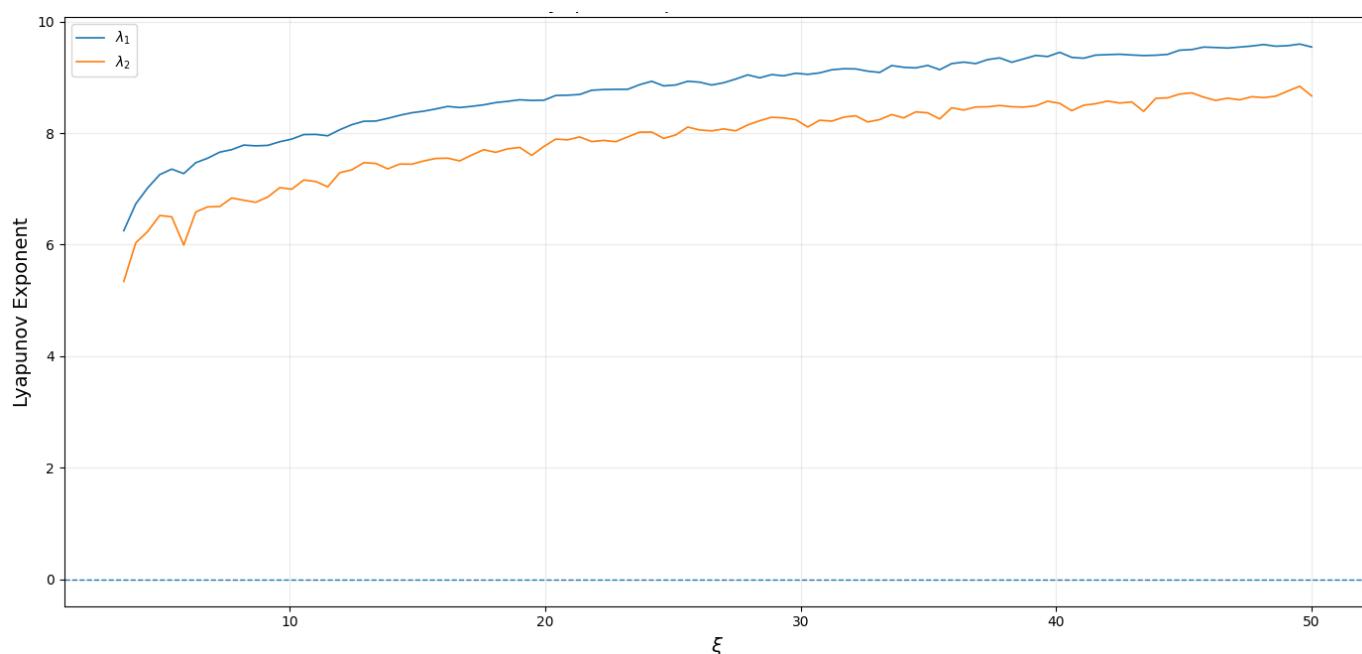


Figure 5. Lyapunov spectrum of QE-CCHM over the investigated control-parameter range $\xi \in [3.5, 50]$, showing the first Lyapunov exponent λ_1 and second Lyapunov exponent λ_2 .

An important observation concerns the lower- ξ region. As discussed in Sections 4.1 and 4.2, the phase-space and bifurcation diagrams around $\xi = 4$ exhibit relatively lower state-space density and less uniform coverage than those observed at larger values of ξ . Nevertheless, the Lyapunov exponents at this region remain strongly positive. In particular, the values at $\xi = 3.5$ are substantially above the zero boundary, demonstrating that the comparatively less dense visual distribution does not correspond to a loss of chaotic divergence. This distinction is important because state-space coverage and Lyapunov divergence characterize different aspects of the dynamics.

The simultaneous positivity of λ_1 and λ_2 provides quantitative evidence of hyperchaotic behavior in the effective two-dimensional classical dynamics of QE-CCHM. More importantly, this condition is maintained at all 100 sampled values of ξ between 3.5 and 50. Thus, the hyperchaotic behavior observed in the bifurcation analysis is not confined to isolated parameter values or a narrow operating interval. The generally increasing trend of both exponents toward larger ξ further suggests stronger divergence of nearby trajectories in this region. This Lyapunov analysis complements the visual observations from the phase-space

and bifurcation diagrams. While the lower- ξ region shows somewhat weaker state-space coverage, it nevertheless retains strong hyperchaotic divergence. At larger ξ , both the visual distribution and Lyapunov exponents indicate increasingly pronounced dynamical complexity. These results establish a broad hyperchaotic region within the investigated parameter range, while the subsequent parameter-domain exploration is used to identify the region that provides the most suitable overall dynamical characteristics.

4.4. Parameter-domain exploration

To investigate the robustness of the proposed QE-CCHM beyond the parameter region used in the preceding experiments, a global exploration of the positive- ξ domain was performed. The exploration considered an extremely wide range, $51 \leq \xi \leq 10^{308}$, which extends the parameter scale by more than 306 orders of magnitude. Because a uniform sampling of ξ would strongly bias the exploration toward the largest numerical values, ξ was sampled approximately uniformly in the logarithmic domain. In total, 10,000 random samples were generated and supplemented with 33 predefined reference values, resulting in 10,033 parameter evaluations. Each candidate was iterated for 300 iterations, with the first 150 iterations discarded as transient behavior. All trajectories passed the numerical validity screening without non-finite state values. These settings and the resulting screening data are recorded in the computational output.

The two largest Lyapunov exponents were first evaluated at representative values distributed across the global domain. As shown in Figure 6, both exponents remain positive throughout the examined range. Starting from $\lambda_1=4.8405$ and $\lambda_2=3.9159$ at the lower boundary $\xi=51$, both exponents increase rapidly in the lower and intermediate regions before approaching a relatively stable regime at large ξ . For example, at $\xi=106$, the exponents reach 14.2617 and 14.1127, respectively, while they remain around 14.7 at much larger parameter values. This behavior indicates that increasing ξ beyond the intermediate regime does not continuously increase the measured instability; instead, the system enters a broad high-expansion regime in which the two leading exponents fluctuate around a relatively stable level.

The global screening was further complemented by distributional and temporal indicators. For each candidate, normalized histogram entropy was calculated independently for the x - and y -sequences using 64 bins, while the absolute lag-1 autocorrelation was used as a simple measure of short-term temporal dependence. The screening procedure treats high entropy as desirable and low autocorrelation as desirable. A preliminary score was consequently defined as:

$$S = \frac{H_x + H_y}{2} - \frac{|AC_x(1)| + |AC_y(1)|}{2} \quad (20)$$

This score is used only to rank candidate parameter values and is not intended to serve as an independent definition or proof of chaotic or cryptographically random behavior.

The resulting screening landscape exhibits generally high normalized entropy across the explored domain, with several candidates simultaneously showing weak lag-1 temporal dependence. Table 1 summarizes selected reference values together with representative high-scoring candidates. The high-scoring values are distributed over widely separated logarithmic scales, indicating that the desirable combination of state-space distribution and weak short-term dependence is not confined to a narrow parameter interval. The highest preliminary score is obtained at $\xi=4.1351 \times 10^{267}$, with $S=0.9244$, while other high-scoring candidates occur at substantially different scales.

To provide an additional global consistency check, a denser bifurcation analysis was subsequently performed using 2,000 logarithmically distributed ξ values from 51 to 10^{308} . For each parameter value, 500 iterations were performed, with the first 300 discarded as transient and 200 subsequent points retained for the bifurcation representation. As shown in Figure 7, both x and y exhibit densely populated regions across the explored logarithmic domain rather than a single isolated chaotic window. This behavior is consistent with the positive Lyapunov exponents and supports the persistence of complex dynamics over a broad parameter range.

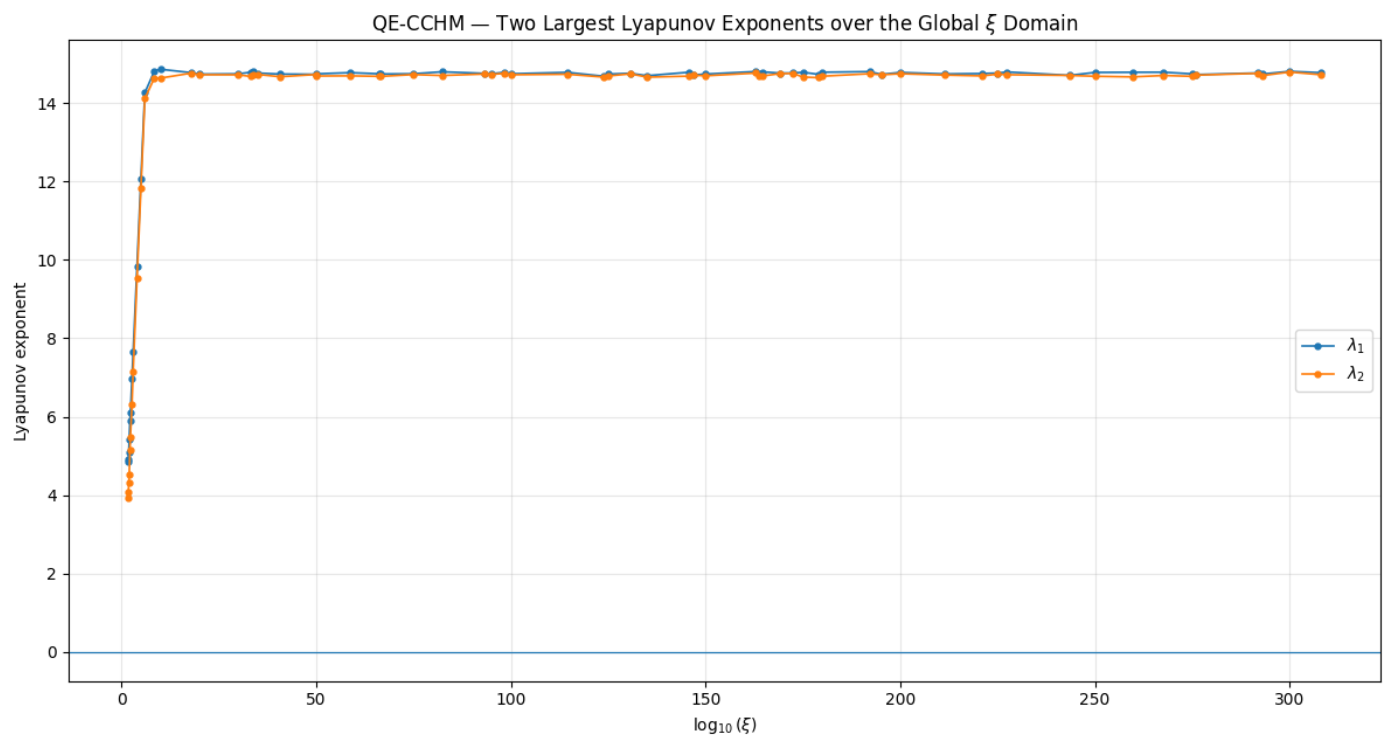


Figure 6. Two largest Lyapunov exponents of QE-CCHM for representative ξ values spanning the global positive- ξ domain. Both exponents remain positive across the explored range, while their values approach a relatively stable regime around 14.7 at very large ξ .

Table 1. Representative and high-scoring ξ values from the global parameter-domain screening

ξ	$\log_{10} \xi$	H_x	H_y	$ AC_x(1) $	$ AC_y(1) $
51	1.708	0.9027	0.8946	0.0596	0.0764
10^3	3.000	0.8668	0.9102	0.0862	0.0278
10^6	6.000	0.9338	0.9206	0.1571	0.0485
2.8868×10^8	8.460	0.9006	0.9264	0.0025	0.0019
10^{20}	20.000	0.9150	0.8936	0.0799	0.0264
10^{30}	30.000	0.9075	0.8922	0.0068	0.0104
1.2972×10^{95}	95.113	0.9122	0.9203	0.0018	0.0041
1.0305×10^{135}	135.013	0.9181	0.9154	0.0012	0.0008
2.3918×10^{172}	172.379	0.9394	0.9165	0.0045	0.0092
1.2321×10^{221}	221.091	0.9349	0.8976	0.0010	0.0022
4.1351×10^{267}	267.616	0.9240	0.9385	0.0119	0.0019
10^{308}	308.000	0.8830	0.8963	0.0019	0.0272

Note: H_x and H_y denote normalized histogram entropy; $|AC(1)|$ denotes absolute lag-1 autocorrelation; S is the preliminary screening score defined by the average entropy minus the average lag-1 autocorrelation. The table is intended for parameter screening, not as a substitute for independent chaos or statistical-randomness validation.

This global exploration indicates that QE-CCHM does not rely on a narrowly tuned value of ξ to generate complex dynamics. Positive leading Lyapunov exponents, high normalized entropy, and low short-term temporal correlation are observed across widely separated regions of the explored domain. Nevertheless, these results should be interpreted primarily as evidence of parameter robustness and candidate selection. The screening score alone does not establish cryptographic randomness; therefore, selected parameter settings require the more stringent statistical and application-specific evaluations presented in the subsequent sections.

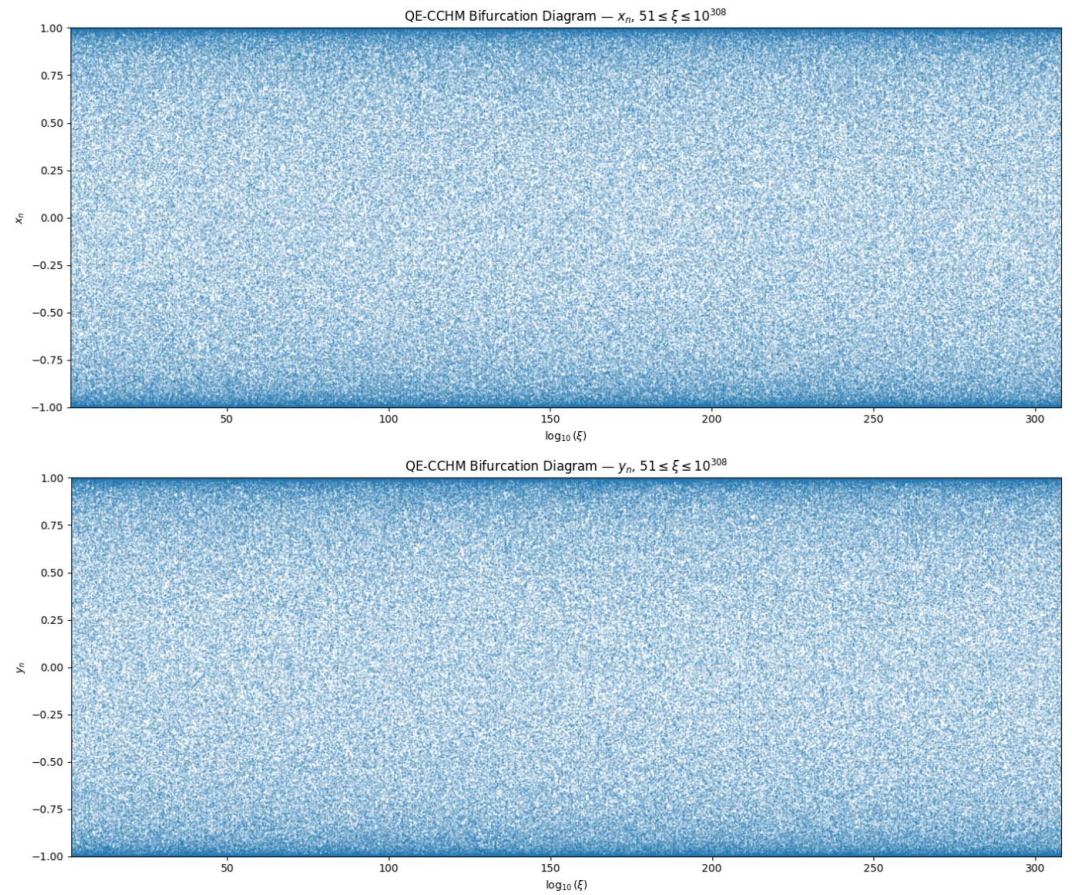


Figure 7. Global bifurcation diagrams of QE-CCHM for $51 \leq \xi \leq 10^{308}$. The dense distributions of x_n (top) and y_n (bottom) over the explored logarithmic parameter range indicate persistent complex dynamics across the global domain.

4.5. Key-Space and Parameter-Range Analysis

The parameterization of QE-CCHM provides a broad space for generating distinct dynamical trajectories through variations in the initial classical states and the control parameter. In the proposed framework, the principal key-related quantities are the initial classical states x_0 and y_0 , together with the control parameter ξ . The remaining parameters define the fixed structure of the hybrid quantum-classical system and are kept constant throughout the experiments.

The parameter space of QE-CCHM is determined by the initial classical states, the control parameter ξ , and the fixed parameters governing the quantum–classical coupling. Table 2 summarizes the principal parameters, their domains or values, and their roles in the proposed system. The global exploration considered an exceptionally broad range of the control parameter, from 10^{-2} to 10^{308} , while the previously investigated region $3.5 \leq \xi \leq 50$ was explicitly represented by predefined reference values. The parameter values were sampled approximately uniformly in the logarithmic domain to provide coverage across widely separated scales. This broad exploration demonstrates that the dynamical behavior of QE-CCHM is not restricted to a narrow operating interval.

The initial conditions x_0 and y_0 also influence the generated trajectories and are defined within the valid classical-state interval. In addition, the quantum subsystem contributes persistent feedback through the DTQW states and the observables q_x and q_y . The fixed parameters, including $\kappa=0.10$, $\Delta=10^{-8}$, the three-qubit DTQW configuration, the four-position state space, and the initial quantum state $|000\rangle$ define the system configuration and are therefore not treated as independently varied parameters in the global exploration.

It is important to distinguish the parameter domain from a cryptographic key space. The range $10^{-2} \leq \xi \leq 10^{308}$ describes the numerical domain investigated for the dynamical system and does not represent 10308 independent parameter values or cryptographic keys. is

represented using finite-precision floating-point arithmetic, the explored parameter domain should be interpreted as a numerical parameter space rather than as an arbitrary set of real numbers. In the IEEE-754 double-precision representation used in the numerical implementation, each value is represented with approximately 15–17 significant decimal digits. Consequently, the absolute spacing between representable values increases with the magnitude of ξ . For example, values such as 3.5, 3.500001, and 3.5000001 are distinct representable parameter settings, whereas sufficiently small differences cannot be distinguished once ξ becomes extremely large. The logarithmic sampling is therefore appropriate for examining the dynamical behavior across widely separated orders of magnitude. Overall, the analysis demonstrates that QE-CCHM can be investigated over an exceptionally broad numerical parameter range, extending from the sub-unit regime to approximately 10308, while the observed dynamical properties remain present across widely separated parameter scales.

Table 2. Principal QE-CCHM parameters, domains, and roles.

Parameter	Value / Domain	Role in QE-CCHM
x_0	$0 < x_0 < 1$ for encryption initialization	Key-derived initial classical state
y_0	$0 < y_0 < 1$ for encryption initialization	Key-derived initial classical state
ξ	10^{-2} to 10^{308} explored globally	Main nonlinear control parameter
ξ for global positive- ξ validation	51 to 10^{308}	Extended parameter-domain validation
κ	0.10	Quantum-classical coupling strength
Δ	10^{-8}	Regularization threshold
Coin qubits	1	DTQW coin subsystem
Position qubits	2	DTQW position subsystem
Total qubits	3	Quantum subsystem
Quantum state dimension	$2^3=8$	State-vector dimension
Initial quantum state	$ 000\rangle$	Quantum-state initialization
Coin operation	$R_Y(\theta)$	Dynamically controlled coin
Position states	4	DTQW position space
Quantum feedback	q_x, q_y	Feedback to classical dynamics

5. Image Encryption Application and Security Analysis

To demonstrate the applicability of the proposed QE-CCHM dynamical system, an image encryption scheme is developed by exploiting the classical sequences generated through the hybrid quantum-classical dynamics. A deliberately simple encryption construction is adopted, combining only pixel permutation and modular substitution, so that the cryptographic behavior can be evaluated primarily from the properties of the proposed QE-CCHM sequences rather than from additional complex encryption mechanisms. This design provides a direct application-level assessment of whether the proposed hyperchaotic dynamics can generate sequences with properties suitable for disrupting spatial and intensity patterns in digital images.

For an $M \times N$ grayscale image, the encryption process produces a ciphertext with the same dimensions as the plaintext while retaining exact reversibility when the correct secret key is provided. The architecture, encryption procedure, and corresponding decryption procedure are described in Section 5.1. The security characteristics of the resulting ciphertext are subsequently evaluated in terms of histogram distribution, information entropy, chi-square statistics, adjacent-pixel correlation, NPCR, and UACI.

5.1. Image encryption architecture

The overall architecture of the proposed image encryption scheme is presented in Fig. 8. The scheme consists of four principal stages: secret-key processing, QE-CCHM sequence generation, image encryption, and image decryption. Let $I \in \{0, 1, \dots, 255\}^{M \times N}$ denote an 8-bit grayscale image, where M and N represent the image height and width, respectively.

The total number of pixels is $L = M \times N$. The image is first converted into a one-dimensional pixel sequence, $\mathbf{p} = [p_0, p_1, \dots, p_{L-1}]$.

A secret key K is processed using SHA-256 to produce a 256-bit digest. The digest is mapped to the initial classical states x_0 , y_0 , and the control parameter ξ . These parameters initialize the QE-CCHM system, which subsequently generates the classical sequences $\mathbf{X} = \{x_n\}_{n=1}^{L-1}$, $\mathbf{Y} = \{y_n\}_{n=1}^{L-1}$, as well as the quantum observables $\mathbf{Q}_X = \{q_{x,n}\}_{n=1}^{L-1}$, $\mathbf{Q}_Y = \{q_{y,n}\}_{n=1}^{L-1}$. As shown in Fig. 8, the X sequence is employed to determine the pixel permutation, whereas the Y sequence is transformed into an 8-bit integer sequence for modular substitution. The quantum observables do not directly operate on the image pixels; instead, they participate in the QE-CCHM feedback mechanism and thereby influence the generated classical sequences. The encryption therefore follows the general structure $K \rightarrow (x_0, y_0, \xi) \rightarrow QE-CCHM \rightarrow (\mathbf{X}, \mathbf{Y}, \mathbf{Q}_X, \mathbf{Q}_Y) \rightarrow \text{Permutation} \rightarrow \text{Substitution} \rightarrow I_C$. The detailed encryption and decryption procedures are given below.

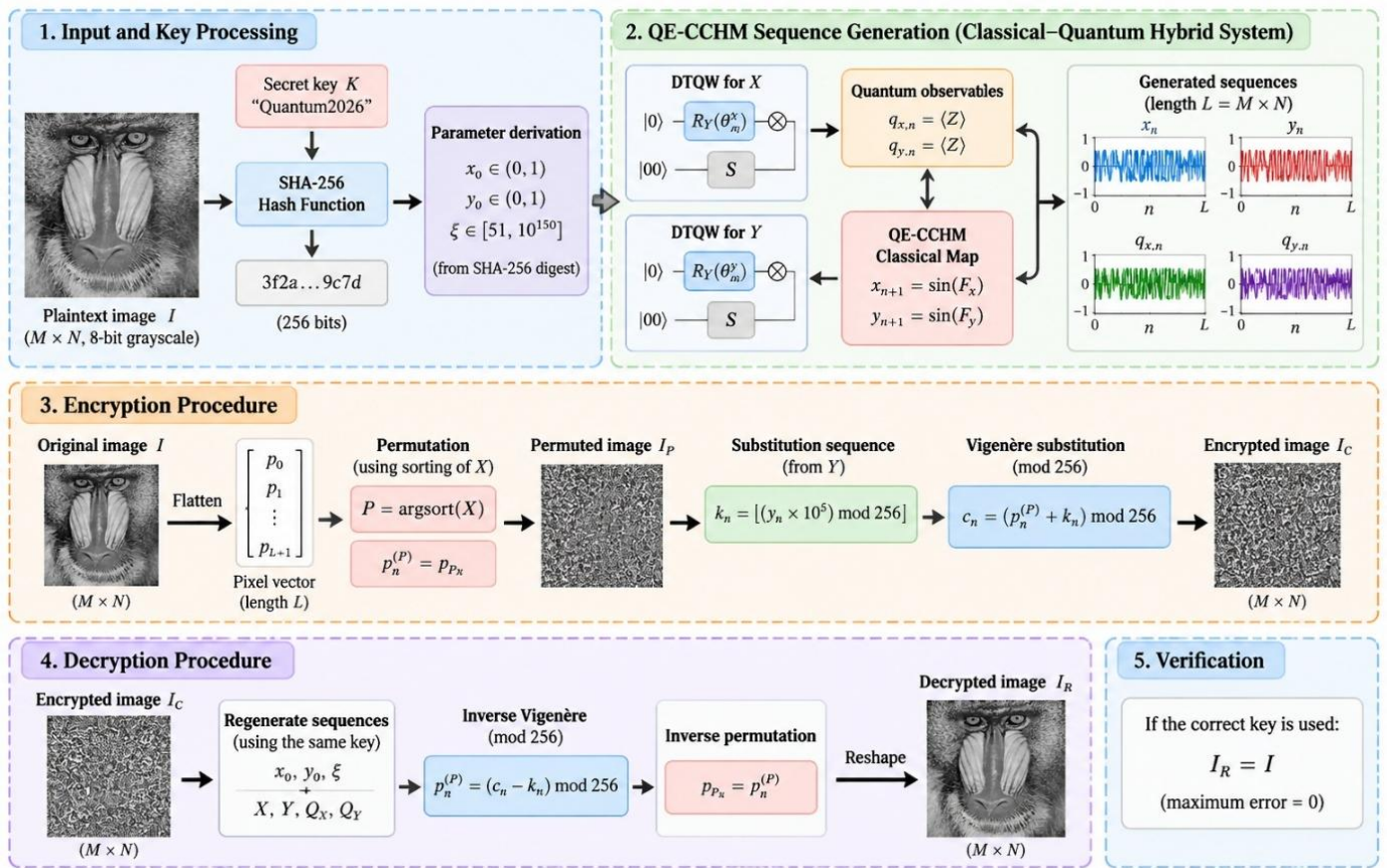


Figure 8. Overview of proposed image encryption.

5.1.1. Encryption procedure

Step 1: Image preprocessing: The input grayscale image I is represented using 8-bit unsigned integers. Its dimensions are $M \times N$, giving a total of $L = MN$ pixels. The two-dimensional image is flattened into $\mathbf{p} = [p_0, p_1, \dots, p_{L-1}]$ where $p_n \in [0, 255]$.

Step 2: Secret-key processing: The secret key K is converted into a byte representation and processed using SHA-256 ($H_K = \text{SHA256}(K)$). The resulting 256-bit digest is divided into segments and mapped to the QE-CCHM parameters x_0 , y_0 , and ξ . The initial classical states satisfy $0 \leq x_0 \leq 1$, $0 \leq y_0 \leq 1$. For the image-encryption implementation, ξ is selected within the numerically stable application range established for the QE-CCHM system.

Step 3: The QE-CCHM sequences are generated by iterating the two-DTQW feedback mechanism described in Section 3.4. At each iteration, the persistent quantum states are evolved according to the dynamically coupled coin angles, and the resulting quantum

observables are fed back into the classical states. After the transient iterations, the system is iterated for $L = MN$ steps to generate the sequences $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Q}_X$, and $\mathbf{Q}_Y$. The X sequence is used for pixel permutation, while the Y sequence is used to construct the substitution sequence.

Step 4: Pixel permutation: The X sequence is used to determine the permutation order by sorting its elements: $P = \text{argsort}(\mathbf{X})$. The resulting vector P contains the pixel indices in ascending order of the corresponding X -sequence values. The permuted pixel sequence is therefore defined as $p_n^{(P)} = p_{P_n}$, $n = 0, 1, \dots, L - 1$. The resulting sequence is reshaped into an $M \times N$ image to obtain the permuted image I_P . This operation changes the spatial positions of the pixels while preserving their intensity values.

Step 5: Integer substitution sequence generation: The Y sequence is transformed into an integer-valued sequence in the range $[0, \dots, 255]$ according to $k_n = \lfloor (y_n \times 10^6) \bmod 256 \rfloor$. Hence $k_n \in \{0, 1, \dots, 255\}$. The resulting sequence $\mathbf{K}_S = [k_0, k_1, \dots, k_{L-1}]$ serves as the substitution sequence for the pixel values.

Step 6: Modular Vigenère substitution: The permuted pixel sequence is combined with the generated integer sequence using modular addition: $c_n = (p_n^{(P)} + k_n) \bmod 256$. The resulting sequence $\mathbf{c} = [c_0, c_1, \dots, c_{L-1}]$ is reshaped into the original $M \times N$ dimensions to produce the encrypted image I_C .

Therefore, the complete encryption process can be summarized as $\mathbf{p} \xrightarrow{\text{argsort}(\mathbf{X})} \mathbf{p}^{(P)} \xrightarrow{\mathbf{K}_S, \bmod 256} \mathbf{c}$, where the permutation is controlled by the X sequence, and the substitution is controlled by the Y sequence.

5.1.2. Decryption procedures

The decryption procedure reverses the encryption operations in the opposite order. Given the ciphertext I_C and the correct secret key K , the receiver can regenerate the same QE-CCHM parameters and sequences used during encryption.

Step 1: Secret-key reconstruction: The receiver provides the same secret key K . SHA-256 is applied to obtain $H_K = \text{SHA256}(K)$. The digest is processed using the same parameter-mapping procedure to reconstruct x_0 , y_0 , and ξ . Because the key-processing procedure is deterministic, the same parameters are obtained when the correct key is supplied.

Step 2: QE-CCHM sequence regeneration: The QE-CCHM system is initialized using the reconstructed x_0 , y_0 , and ξ , together with the same initial DTQW states and transient length used during encryption. The system is then iterated to regenerate $\mathbf{X}$, $\mathbf{Y}$, $\mathbf{Q}_X$, and $\mathbf{Q}_Y$. The regenerated X sequence is used for pixel permutation index $P = \text{argsort}(\mathbf{X})$, while the regenerated Y sequence produces the same integer substitution sequence: $k_n = \lfloor (y_n \times 10^6) \bmod 256 \rfloor$.

Step 3: Inverse modular substitution: The ciphertext sequence is first subjected to the inverse Vigenère operation. For each ciphertext pixel c_n , $p_n^{(P)} = (c_n - k_n) \bmod 256$. This recovers the pixel sequence after the permutation stage.

Step 4: Inverse permutation: The permutation is then reversed using the regenerated index vector P . Since encryption produced $p_n^{(P)} = p_{P_n}$, the original pixel sequence is recovered by assigning $p_{P_n} = p_n^{(P)}$. The recovered one-dimensional sequence is subsequently reshaped into its original $M \times N$ dimensions to obtain the decrypted image I_R .

The complete decryption process can therefore be expressed as $I_C \xrightarrow{\text{inverse Vigenère}} I_P \xrightarrow{\text{inverse Permutation}} I_R$. For the correct secret key and deterministic QE-CCHM evolution, the decrypted image should satisfy $I_R = I$. Exact recovery is verified by comparing every pixel of the original and decrypted images. In the implementation, successful recovery is indicated by zero maximum pixel error, $\max_n |p_n - p_n^{(R)}| = 0$, and an identical SHA-256 digest of the original and recovered image data.

5.2. Experimental setup

The image encryption experiment was conducted using a 512×512 8-bit standard gray-scale image (see Figure 9), resulting in $L=262,144$ pixels. The proposed QE-CCHM was

implemented in Python using NumPy and PIL, and the quantum-walk component was simulated using a state-vector representation. The experiment was executed in the Google Colab environment with the input image accessed through Google Drive. The secret key was processed using SHA-256 to deterministically derive the initial classical states x_0 , y_0 , and the control parameter ξ . The values of x_0 and y_0 were mapped to (0,1), whereas ξ was logarithmically mapped to the numerically stable encryption domain $51 \leq \xi \leq 10^{150}$. The quantum-classical coupling parameter was set to $\kappa=0.10$, and the regularization parameter was set to $\Delta=10^{-8}$. The quantum subsystem consisted of three qubits, comprising one coin qubit and two position qubits, corresponding to four position states and an eight-dimensional state vector. The initial quantum states were set to $|0_{\text{coin}}, 00_{\text{position}}\rangle$. A transient of 1,000 iterations was discarded before sequence generation. Subsequently, $L=262,144$ iterations were performed to generate the X , Y , Q_X , and Q_Y sequences.

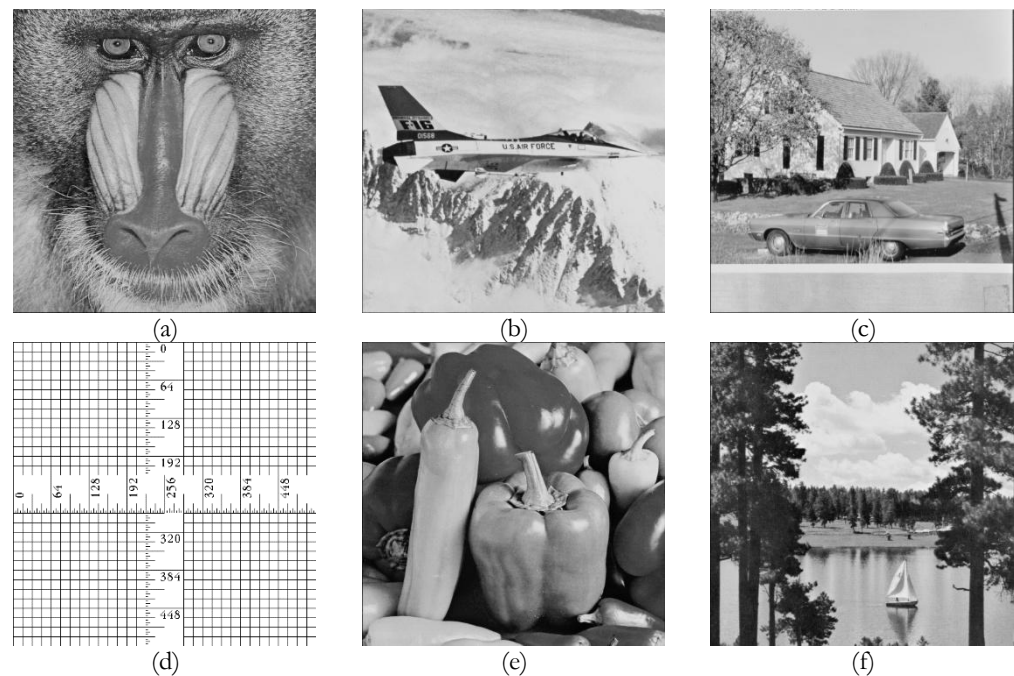


Figure 9. Image used for proposed image encryption (a) Baboon; (b) F16; (c) House; (d) Ruler; (e)Peppers; (f) Sailboat

5.3. Statistical security analysis

5.3.1. Histogram and Chi-square Analysis

Histogram analysis was first performed to examine the distribution of pixel intensities before and after encryption. An effective image encryption process is expected to produce a ciphertext whose intensity distribution is substantially more uniform than that of the plaintext, thereby reducing statistical information that may reveal characteristics of the original image.

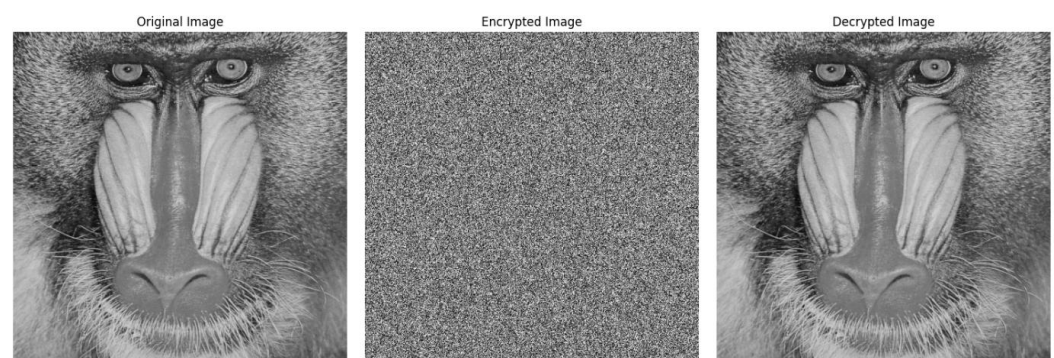


Figure 10. Original, encrypted, and decrypted Baboon images

Figure 10 shows the original, encrypted, and decrypted Baboon images. The original image contains clearly recognizable visual structures, whereas these structures are effectively obscured after encryption. The encrypted image exhibits a noise-like appearance with no visually distinguishable content from the plaintext. In contrast, the decrypted image recovers the visual content of the original image, confirming the reversibility of the proposed encryption and decryption procedures.

Figure 11 further compares the pixel-intensity histograms of the original and encrypted images. The histogram of the original Baboon image is highly non-uniform, with several intensity ranges having substantially higher frequencies than others. This distribution reflects the spatial structures, textures, and intensity characteristics of the plaintext image. After encryption, the histogram becomes considerably flatter, with the 256 grayscale levels distributed much more uniformly. This indicates that the encryption process effectively suppresses the dominant intensity patterns present in the original image.

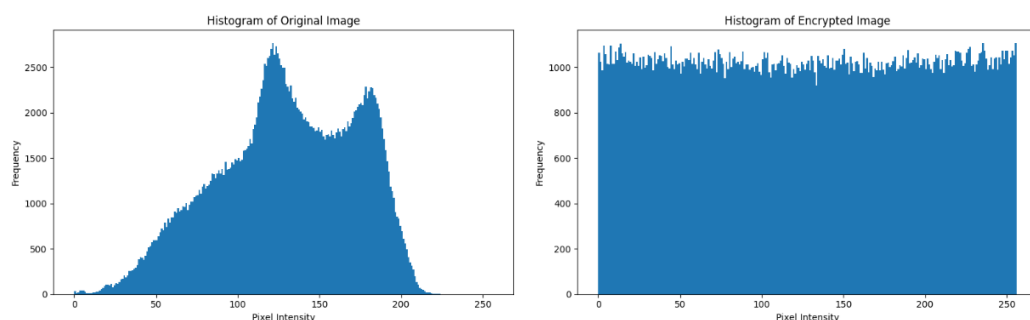


Figure 11. Pixel-intensity histograms of original (left) and encrypted Baboon images (right).

To provide a quantitative assessment of histogram uniformity, the chi-square statistic was calculated as $\chi^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i}$, where O_i is the observed frequency of grayscale level i , and E_i is the expected frequency under a uniform distribution. For an 8-bit grayscale image, the number of intensity levels is 256, resulting in 255 degrees of freedom. At a significance level of $\alpha=0.05$, the critical value is 293.2478. Thus, an encrypted image with $\chi^2 < 293.2478$ does not provide sufficient statistical evidence to reject the null hypothesis of a uniform intensity distribution.

Table 3 presents the chi-square statistics obtained for the original and encrypted versions of six test images. The original images exhibit very large chi-square values, ranging from 120,179.507812 for Peppers to 53,702,747.132812 for Ruler. These values clearly exceed the critical value, indicating highly non-uniform intensity distributions in the plaintext images.

Table 3. Chi-square statistics of the original and encrypted images.

Image	Original	Encrypted
Baboon	187366.248047	253.326172
F16	717781.802734	289.636719
House	336947.824219	286.378906
Ruler	53702747.132812	292.722656
Peppers	120179.507812	280.859375
Sailboat	179871.339844	265.947266

In contrast, all encrypted images produce chi-square values below the critical value of 293.2478. For the Baboon image, the chi-square statistic decreases from 187,366.248047 in the original image to 253.326172 after encryption. Similarly, the values for F16, House, Ruler, Peppers, and Sailboat decrease to 289.636719, 286.378906, 292.722656, 280.859375, and 265.947266, respectively. The highest encrypted value is obtained for Ruler (292.722656), which nevertheless remains below the critical threshold.

5.3.2. Information Entropy Analysis

Information entropy was used to quantify the randomness of the pixel-intensity distribution. For an 8-bit grayscale image, the entropy is defined as $H = -\sum_{i=0}^{255} p_i \log_2(p_i)$,

where p_i is the probability of occurrence of intensity level i . The theoretical maximum is 8 bits/pixel, corresponding to a uniform distribution. The results demonstrate a substantial and consistent increase in entropy after encryption. All six encrypted images achieve entropy values above 7.998 bits/pixel, despite their substantially different plaintext distributions. Baboon increases from 7.358320 to 7.999303 bits/pixel, while F16 and House reach 7.999202 and 7.999211, respectively. The most pronounced improvement is observed for Ruler, whose entropy increases from only 0.500033 to 7.998185 bits/pixel, an improvement of approximately 7.498 bits/pixel. This shows that the encryption process can transform even a highly non-uniform plaintext distribution into a near-maximal-entropy ciphertext. Peppers and Sailboat also achieve 7.999171 and 7.999271 bits/pixel, respectively. The difference between the highest and lowest encrypted entropy values is only 0.001118 bits/pixel, demonstrating highly consistent entropy behavior across the six test images.

Table 4. Information entropy of the original and encrypted images.

Image	Original	Encrypted
Baboon	7.358320	7.999303
F16	6.702451	7.999202
House	7.233404	7.999211
Ruler	0.500033	7.998185
Peppers	7.593603	7.999171
Sailboat	7.484263	7.999271

5.3.3. Correlation Coefficient Analysis

The correlation coefficient analysis was conducted to evaluate the degree of linear dependency between adjacent pixels in the original and encrypted images. For a grayscale image, the correlation coefficient between two adjacent pixel sequences x and y is calculated as $r_{xy} = \frac{\sum_{i=1}^N (x_i - \bar{x}) \sum_{i=1}^N (y_i - \bar{y})}{\sqrt{\sum_{i=1}^N (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^N (y_i - \bar{y})^2}}$, where x_i and y_i represent adjacent pixel values and $\bar{x}$ and $\bar{y}$ are their corresponding means. The analysis was performed in the horizontal, vertical, and diagonal directions.

Table 5. Correlation coefficients of adjacent pixels in the original and encrypted images.

Image	Direction	Original	Encrypted
Baboon	Horizontal	0.866544	-0.000452
	Vertical	0.758732	-0.002052
	Diagonal	0.726189	-0.000586
F16	Horizontal	0.966317	0.001393
	Vertical	0.964127	-0.002226
	Diagonal	0.937025	-0.001421
House	Horizontal	0.948470	-0.002371
	Vertical	0.957764	0.001108
	Diagonal	0.913522	-0.000837
Ruler	Horizontal	0.454197	0.002302
	Vertical	0.464804	-0.001683
	Diagonal	-0.028994	0.001205
Peppers	Horizontal	0.976771	-0.000193
	Vertical	0.979206	0.002329
	Diagonal	0.963935	-0.000372
Sailboat	Horizontal	0.975099	-0.001487
	Vertical	0.971538	-0.000969
	Diagonal	0.957770	-0.000335

The results are presented in Table 5. For the original images, relatively strong positive correlations are observed for most test images, particularly in the horizontal and vertical directions. For example, the Peppers image exhibits correlation coefficients of 0.976771, 0.979206, and 0.963935 in the horizontal, vertical, and diagonal directions, respectively. Similarly, the F16, House, and Sailboat images exhibit strong positive correlations, reflecting the spatial continuity and structural characteristics naturally present in neighboring pixels.

A substantial reduction in adjacent-pixel correlation is observed after encryption for all six test images and in all three directions. The encrypted-image coefficients remain very close to zero, ranging from approximately -0.002371 to 0.002329. This indicates that neighboring pixels in the ciphertext exhibit almost no linear statistical dependency.

The effect is particularly evident for images with highly correlated neighboring pixels. For example, the horizontal correlation of Peppers decreases from 0.976771 to -0.000193, while its vertical correlation decreases from 0.979206 to 0.002329. The corresponding diagonal correlation decreases from 0.963935 to -0.000372. Similar behavior is observed for F16, House, and Sailboat. Thus, the encryption process effectively disrupts the spatial relationships present in the plaintext images.

For the Baboon image used as the representative example, the horizontal, vertical, and diagonal correlations decrease from 0.866544, 0.758732, and 0.726189 to -0.000452, -0.002052, and -0.000586, respectively. The corresponding scatter plots are shown in Fig. 12. In the original image, the pixel pairs form concentrated diagonal patterns, demonstrating strong spatial dependency between neighboring pixels. After encryption, the distribution becomes substantially more dispersed across the intensity range, with no visually dominant linear pattern. This visual observation is consistent with the numerical correlation coefficients approaching zero.

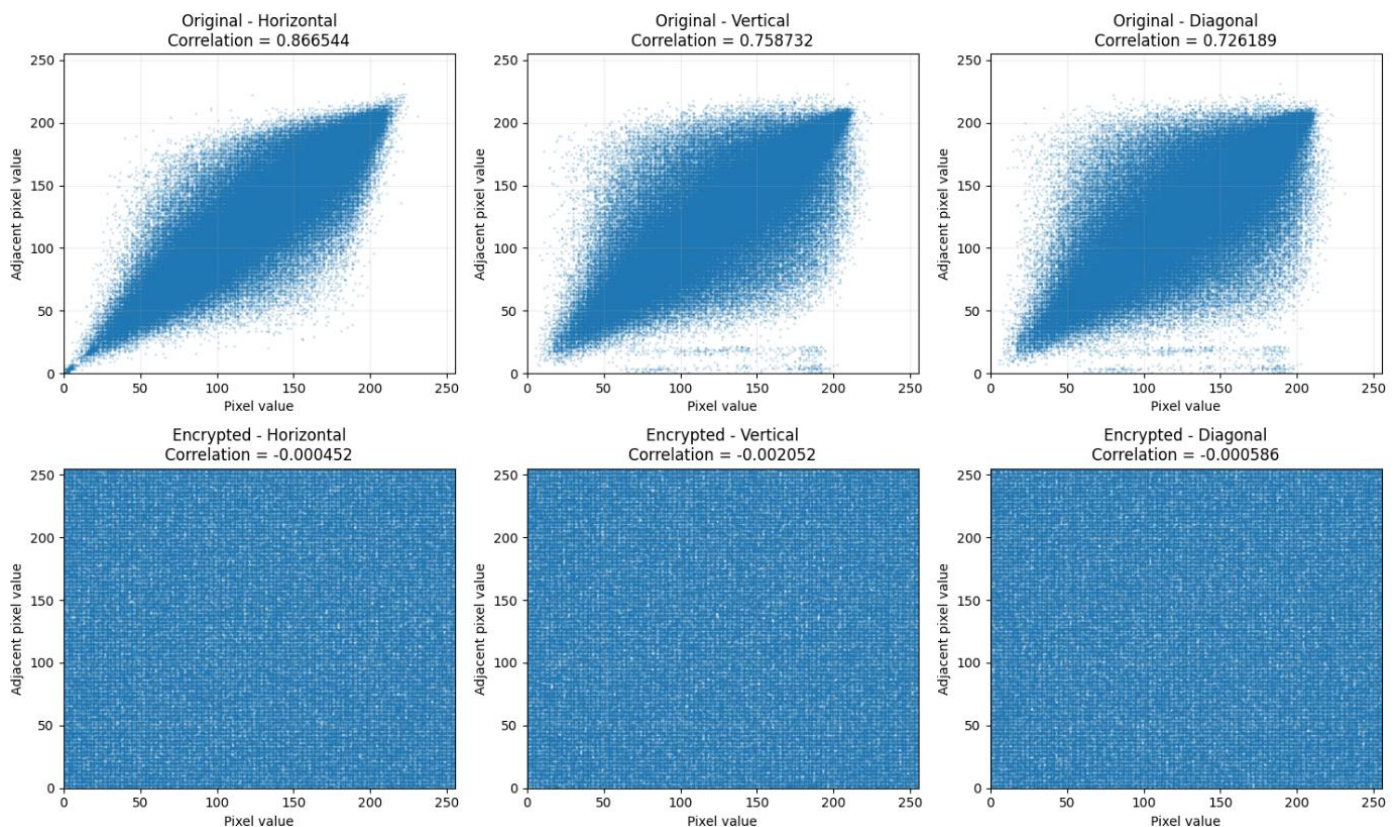


Figure 12. Adjacent-pixel correlation plots of the Baboon image before and after encryption in the horizontal, vertical, and diagonal directions.

5.3.4. NPCR dan UACI Analysis

The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) were employed to evaluate the sensitivity of the encryption scheme to a small modification in the plaintext image. These measures are particularly important for image

encryption because a desirable encryption algorithm should propagate a very small plaintext modification to a large portion of the ciphertext. For this experiment, only one pixel of each plaintext image was modified, while all other pixels were kept unchanged. Specifically, a copy of the original image was created, and the intensity value of one selected pixel was changed by one gray-level unit. For an 8-bit grayscale image, if the selected pixel has value p , the modified image uses $p' = (p + 1) \bmod 256$. Thus, the two plaintext images differ by exactly one pixel, while their dimensions and all other pixel values remain identical.

The two images were then independently encrypted using the same secret key and the same encryption procedure. Because the QE-CCHM parameters are derived from the secret key rather than from the plaintext image, the same key generates the same initial conditions and control parameter for both encryptions. The resulting ciphertexts can therefore be compared directly to measure the propagation of the one-pixel modification. For 8-bit grayscale images, values close to approximately 99.6% for NPCR and 33.5% for UACI are commonly used as reference points for assessing strong differential behavior. These values should be interpreted as statistical reference values rather than strict acceptance thresholds.

Table 6. NPCR and UACI results obtained from one-pixel plaintext modification.

Image	NPCR	UACI
Baboon	99.620056%	33.698648%
F16	99.635696%	33.497555%
House	99.624634%	33.457508%
Ruler	99.596786%	33.097002%
Peppers	99.593353%	33.598008%
Sailboat	99.613571%	33.535994%

The results in Table 6 show that changing only one plaintext pixel produces changes in more than 99.59% of the ciphertext pixels for all six test images. The NPCR values range from 99.593353% to 99.635696%, indicating a very strong propagation of the plaintext modification throughout the ciphertext. For the Baboon image, for instance, a single-pixel modification produces an NPCR of 99.620056%, meaning that nearly the entire ciphertext is altered. Comparable behavior is observed for F16 and House, which achieve NPCR values of 99.635696% and 99.624634%, respectively. Even the lowest NPCR, obtained for Peppers (99.593353%), indicates that the effect of the one-pixel modification is propagated to almost the complete ciphertext. The relatively narrow range of NPCR values across the six images also suggests that this propagation behavior is not strongly dependent on the particular spatial characteristics of the plaintext.

The UACI values range from 33.097002% to 33.698648%. Baboon produces the highest UACI value of 33.698648%, while Ruler produces the lowest value of 33.097002%. The remaining images yield values between 33.46% and 33.60%. Thus, despite the plaintext modification being restricted to a single pixel, the resulting ciphertexts exhibit substantial changes in pixel intensity across the image. The Ruler result is worth noting. Although its UACI (33.097002%) is lower than those of the other test images, its NPCR remains high at 99.596786%. This indicates that the one-pixel modification still propagates spatially to almost the entire ciphertext, even though the average magnitude of the resulting intensity changes is somewhat lower. This difference illustrates why NPCR and UACI provide complementary information: NPCR measures how many ciphertext pixels change, whereas UACI measures how strongly their intensity values change on average.

5.3.5. Decryption and Key Sensitivity Analysis

The reversibility of the proposed encryption scheme and its sensitivity to a small key perturbation were evaluated in a decryption experiment. First, the ciphertext was decrypted using the correct secret key to verify that the proposed permutation and modular substitution operations are exactly reversible. The decrypted image was compared pixel-by-pixel with the original plaintext image. For the key-sensitivity experiment, the original secret key $K = \text{QE-CCHM-Image-Encryption-2026}$ was modified by changing only one character, resulting in $K' = \text{QE-CCHM-Image-Encryption-2026}$.

The change from “n” to “m” corresponds to a one-bit difference in their ASCII representations. No other characters in the key were changed. The ciphertext generated using the

original key was then decrypted using K' , while all other encryption/decryption settings remained unchanged. Figure 13 illustrates the resulting images. The correct-key decryption reconstructs the original Baboon image, demonstrating the reversibility of the proposed encryption scheme. In contrast, decrypting the same ciphertext using the minimally modified key produces an image that is visually indistinguishable from random noise and contains no recognizable structure of the original image.

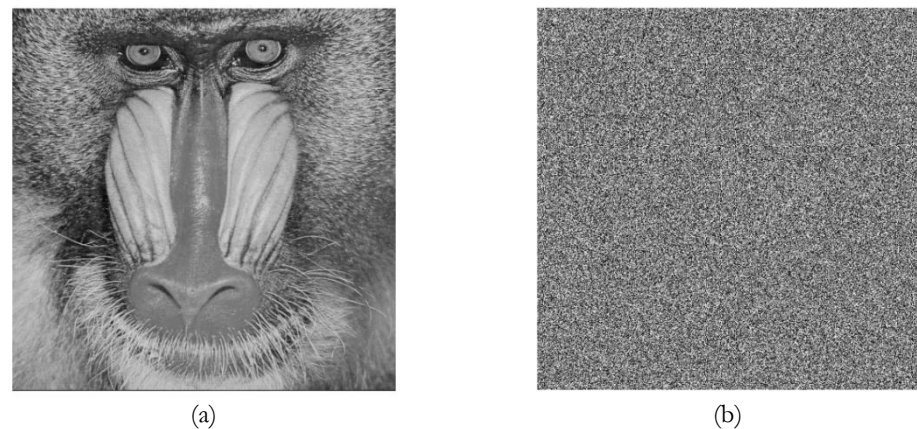


Figure 13. Decryption results of the Baboon image using (a) the correct key and (b) a key differing by one bit.

The big difference between the two decryption outcomes demonstrates the high sensitivity of the proposed scheme to the secret key. Although the two keys differ by only one bit, the modified key produces different SHA-256 output and consequently different initial values x_0 , y_0 , and the control parameter ξ . These altered initial conditions cause the subsequent QE-CCHM trajectories and generated encryption sequences to diverge from those produced by the correct key. As a result, the permutation order and substitution sequence reconstructed during decryption no longer correspond to those used during encryption.

5.3.6. Comparison with state-of-the-art

Table 7 compares the encryption performance of QE-CCHM with those of Ref. [40] and Ref. [42] using the grayscale Baboon image. Overall, the proposed method achieves competitive statistical results. Its encrypted-image entropy is 7.9993, comparable to Ref. [42], while its horizontal correlation coefficient of -0.00045 is slightly closer to zero than that of Ref. [42]. The proposed method also achieves the highest NPCR (99.620056%) and UACI (33.698648%) among the three methods. However, Ref. [42] produces a lower vertical correlation coefficient and a lower chi-square value than QE-CCHM. These results indicate that the proposed method is competitive in terms of statistical encryption performance, although no single method is superior across all evaluated metrics.

Table 7. Comparison with existing image-encryption methods using the grayscale Baboon image.

Measurements	Ref [40]	Ref [42]	Ours
Chi-square	-	247.50195	253.32617
Entropy	7.9990	7.9993	7.9993
Correlation Coefficient (H)	0.0026	-0.00030	-0.00045
Correlation Coefficient (V)	-0.0043	-0.00006	-0.00205
Correlation Coefficient (D)	0.0034	-0.00050	-0.00058
NPCR	99.59340%	99.61662%	99.620056%
UACI	33.45510%	33.42832%	33.698648%

Beyond the image-encryption results, QE-CCHM offers a distinct advantage in its underlying dynamical architecture. Both leading Lyapunov exponents remain positive across all 100 evaluated parameter values in the investigated region $3.5 \leq \xi \leq 50$, supporting the presence of hyperchaotic behavior in this region. Furthermore, the global exploration covers an

exceptionally broad parameter domain, from 10^{-2} to approximately 10^{308} , demonstrating the potential to investigate complex dynamics across widely separated parameter scales. This parameter range represents a numerical exploration domain rather than a cryptographic key space, and the image-encryption experiments use a more conservative operating range because of numerical stability considerations.

QE-CCHM also employs two DTQW subsystems, each consisting of three qubits, integrated with two classical state variables through bidirectional quantum–classical feedback. This compact quantum-walk configuration provides a relatively lightweight architectural choice for incorporating quantum dynamics into a low-dimensional classical system. Unlike approaches that use quantum walks primarily as auxiliary keystream or transformation components, QE-CCHM integrates quantum observables directly into the iterative evolution of the coupled system. Therefore, its main contribution lies not in uniformly outperforming existing methods on every image-encryption metric, but in combining competitive encryption results with a cross-coupled classical–quantum architecture and an exceptionally broad investigated parameter domain. The computational efficiency of this architecture, however, requires further benchmarking before a quantitative efficiency advantage can be established.

6. Conclusions

This study proposed QE-CCHM, a hybrid classical–quantum dynamical framework that integrates nonlinear cross-coupled classical states with two discrete-time quantum walks (DTQWs) through bidirectional quantum–classical feedback. The main contribution is the integration of quantum observables directly into the iterative evolution of the coupled system, rather than using quantum walks solely as auxiliary keystream generators or transformation components. The dynamical analyses indicate that hyperchaotic behavior is maintained throughout the investigated parameter interval, while the global exploration identifies parameter configurations with favorable distributional and short-term temporal characteristics across widely separated numerical scales.

The application of QE-CCHM to image encryption demonstrates its potential for generating sequences that support pixel permutation and modular substitution. The experiments show that the resulting ciphertexts have near-maximal intensity entropy, low adjacent-pixel correlations, and strong responses to one-pixel plaintext modifications. Exact image recovery with the correct secret key and substantial degradation under a one-bit key perturbation further demonstrate the reversibility and key sensitivity of the implemented scheme. These findings support the feasibility of QE-CCHM as a hybrid dynamical framework for image-encryption research, but they do not by themselves establish resistance to comprehensive cryptanalytic attacks or superiority over existing encryption methods.

Several limitations remain. The broad parameter-domain exploration should be distinguished from the narrower operating range used in the encryption experiments, which was selected with numerical stability in mind. In addition, the global screening indicators are not a substitute for standardized randomness testing and systematic cryptanalysis. The DTQW components were evaluated through classical state-vector simulation, so the results do not establish performance on physical quantum hardware or demonstrate a computational-efficiency advantage. Future work should therefore prioritize comprehensive randomness and security testing, further investigation of numerical precision and stability, and evaluation of the coupled system under alternative simulation settings and, where feasible, quantum-hardware constraints.

Author Contributions: Conceptualization: D.R.I.M.S., S.R., T.S., and M.A.; Methodology: D.R.I.M.S.; Software: D.R.I.M.S.; Validation: D.R.I.M.S., S.R., T.S., and M.A.; Formal analysis: D.R.I.M.S., S.R., T.S., and M.A.; Investigation: D.R.I.M.S., S.R., and T.S.; Resources: D.R.I.M.S., D.A.D, D., and S.U.M.; Writing—original draft preparation: D.R.I.M.S.; Writing—review and editing: D.R.I.M.S., P.N.A, M.T.N; Visualization: M.A. and W.H.; Supervision: D.R.I.M.S.; Project administration: W.H.; Funding acquisition: n/a. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Kementerian Pendidikan Tinggi, Sains, dan Teknologi (Kemdiktisaintek), Indonesia, grant numbers 133/C3/DT.05.00/PL-MULTITAHUN

LANJUTAN/2026; 16/LL6/AL.04.03/PL-MULTITAHUN LANJUTAN/2026; and 131/F.09/UDN-09/III/2026.

Data Availability Statement: No additional data were created or analyzed in this study. All results are presented within the article.

Acknowledgments: 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. Generative AI tools were used to assist with language refinement and grammatical editing. The authors reviewed and verified the content and take full responsibility for the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

- [1] H. Wen *et al.*, “A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication,” *IEEE Access*, vol. 9, pp. 20481–20492, 2021, doi: 10.1109/ACCESS.2021.3054952.
- [2] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, “Image encryption scheme by combining the hyper-chaotic system with quantum coding,” *Opt. Lasers Eng.*, vol. 124, no. August 2019, p. 105836, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105836.
- [3] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, “A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size,” in *2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Oct. 2017, pp. 16–21. doi: 10.1109/ISEMANTIC.2017.8251836.
- [4] H. Huang, Z. Liu, Z. Wang, and F. Yan, “A secure image encryption mechanism using biased Fourier quantum walk and addition-crossover structure in the Internet of Things,” *Internet of Things*, vol. 31, no. February, p. 101559, May 2025, doi: 10.1016/j.iot.2025.101559.
- [5] B. S. W. Poetro, K. Adi, and A. P. Widodo, “Block-wise Authenticated DNA-based Image Encryption with Tamper Localization using HKDF-Derived Keys,” *J. Comput. Theor. Appl.*, vol. 4, no. 1, pp. 230–250, Jul. 2026, doi: 10.62411/jcta.16605.
- [6] B. Zhang and L. Liu, “Chaos-Based Image Encryption: Review, Application, and Challenges,” *Mathematics*, vol. 11, no. 11, 2023, doi: 10.3390/math11112585.
- [7] T. W. Broto, S. Rustad, A. Z. Fanani, S. Winarno, and D. R. I. M. Setiadi, “Pseudo-Random Number Generation Based on Quantum Kicked Rotor Dynamics,” in *2025 IEEE 2nd International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, Oct. 2025, pp. 1–7. doi: 10.1109/ICoCICs68032.2025.11384053.
- [8] M. N. M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and S. Astuti, “An improved secure image hiding technique using PN-sequence based on DCT-OTP,” in *2017 1st International Conference on Informatics and Computational Sciences (ICICOS)*, Nov. 2017, pp. 47–52. doi: 10.1109/ICICOS.2017.8276336.
- [9] M. Alawida, “Enhancing logistic chaotic map for improved cryptographic security in random number generation,” *J. Inf. Secur. Appl.*, vol. 80, p. 103685, Feb. 2024, doi: 10.1016/j.jisa.2023.103685.
- [10] M. Nazish, M. Javid, and M. T. Bandy, “Enhanced logistic map with infinite chaos and its applicability in lightweight and high-speed pseudo-random bit generation,” *Cybersecurity*, vol. 8, no. 1, p. 24, Apr. 2025, doi: 10.1186/s42400-024-00319-4.
- [11] A. Abba, N. Ahmed, and H. A. Sulaimon, “Experimental Evaluation of Various Chaos-based Image Encryption Schemes,” *J. Comput. Theor. Appl.*, vol. 3, no. 1, pp. 91–103, Aug. 2025, doi: 10.62411/jcta.13483.
- [12] S. Zhu, X. Deng, W. Zhang, and C. Zhu, “Construction of a New 2D Hyperchaotic Map with Application in Efficient Pseudo-Random Number Generator Design and Color Image Encryption,” *Mathematics*, vol. 11, no. 14, p. 3171, Jul. 2023, doi: 10.3390/math11143171.
- [13] D. R. I. M. Setiadi *et al.*, “Hyperchaotic cross-coupled quantum 2D maps with interdependent rotational asymmetry for secure image encryption,” *Opt. Commun.*, vol. 600, no. September 2025, p. 132699, Mar. 2026, doi: 10.1016/j.optcom.2025.132699.
- [14] M. Elbadri *et al.*, “Study of the Variable-Order Fractional Arncodo System: Bifurcation, Chaos, and Dynamic Behavior,” *Fractal Fract.*, vol. 10, no. 5, p. 296, Apr. 2026, doi: 10.3390/fractalfract10050296.
- [15] A. M. M. El Den, K. H. Moussa, A. Zaki, and M. E. Khedr, “An Enhanced Pseudorandom Number Generator Based on 5D-Memrestive Hyperchaotic Map,” in *2025 International Telecommunications Conference (ITC-Egypt)*, Jul. 2025, pp. 213–218. doi: 10.1109/ITC-Egypt66095.2025.11186646.
- [16] D. Murillo-Escobar, M. Á. Murillo-Escobar, C. Cruz-Hernández, A. Arellano-Delgado, and R. M. López-Gutiérrez, “Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation,” *Nonlinear Dyn.*, vol. 111, no. 7, pp. 6773–6789, Apr. 2023, doi: 10.1007/s11071-022-08101-2.
- [17] D. R. I. M. Setiadi *et al.*, “Single Qubit Quantum Logistic-Sine XYZ-Rotation Maps: An Ultra-Wide Range Dynamics for Image Encryption,” *Comput. Mater. Contin.*, vol. 83, no. 2, pp. 2161–2188, 2025, doi: 10.32604/cmc.2025.063729.
- [18] J. P. Mendonça, F. A. B. F. de Moura, M. L. Lyra, and G. M. A. Almeida, “Emergent nonlinear phenomena in discrete-time quantum walks,” *Phys. Rev. A*, vol. 101, no. 6, p. 062335, Jun. 2020, doi: 10.1103/PhysRevA.101.062335.
- [19] S. Omanakuttan and A. Lakshminarayan, “Quantum walks with quantum chaotic coins: Loschmidt echo, classical limit, and thermalization,” *Phys. Rev. E*, vol. 103, no. 1, p. 012207, Jan. 2021, doi: 10.1103/PhysRevE.103.012207.
- [20] Y. Li, Z. Allen-Zhao, W. Song, and S. Liu, “Robust Parameter Interval Identification for a Logistic-Type Fractional Difference System,” *Fractal Fract.*, vol. 10, no. 1, p. 29, Jan. 2026, doi: 10.3390/fractalfract10010029.

- [21] M. S. Hasan, A. Dhungel, P. S. Paul, M. Sadia, and M. R. Hossain, "Normalized Linearly-Combined Chaotic System: Design, Analysis, Implementation, and Application," *IEEE Open J. Ind. Electron. Soc.*, vol. 4, pp. 486–505, 2023, doi: 10.1109/OJIES.2023.3328497.
- [22] V. C. Iheanacho *et al.*, "Operating-Map Analysis of a Memristive Diode-Bridge Circuit Using Numerical Continuation," *Electronics*, vol. 15, no. 16, p. 3638, Aug. 2026, doi: 10.3390/electronics15163638.
- [23] M. K. Khairullah, A. A. Alkahtani, M. Z. Bin Baharuddin, and A. M. Al-Jubari, "Designing 1D Chaotic Maps for Fast Chaotic Image Encryption," *Electronics*, vol. 10, no. 17, p. 2116, Aug. 2021, doi: 10.3390/electronics10172116.
- [24] A. S. Alali, M. K. Jamil, R. Ali, R. Alotaibi, and W. Albalawi, "Design and evaluation of a novel chaotic logistic-tent-sine map for S-box construction in image encryption," *Chaos, Solitons & Fractals*, vol. 211, no. P2, p. 118733, Oct. 2026, doi: 10.1016/j.chaos.2026.118733.
- [25] X. Wang, B. Yang, and X. Xie, "A multi-image encryption scheme based on 3DSHCM chaotic map and eight-base DNA coding with bit-plane information," *Digit. Signal Process.*, vol. 184, no. July, p. 106374, Nov. 2026, doi: 10.1016/j.dsp.2026.106374.
- [26] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn.*, vol. 105, no. 2, pp. 1859–1876, Jul. 2021, doi: 10.1007/s11071-021-06663-1.
- [27] Z. A. N. Fauzyah, A. Sambas, P. W. Adi, and D. R. I. M. Setiadi, "Quantum Key Distribution-Assisted Image Encryption Using 7D and 2D Hyperchaotic Systems," *J. Futur. Artif. Intell. Technol.*, vol. 2, no. 1, pp. 47–62, Apr. 2025, doi: 10.62411/faith.3048-3719-93.
- [28] W. Feng *et al.*, "State-Dependent Variable Fractional-Order Hyperchaotic Dynamics in a Coupled Quadratic Map: A Novel System for High-Performance Image Protection," *Fractal Fract.*, vol. 9, no. 12, p. 792, Dec. 2025, doi: 10.3390/fractalfract9120792.
- [29] M. Wang, M. An, S. He, X. Zhang, H. Ho-Ching Iu, and Z. Li, "Two-dimensional memristive hyperchaotic maps with different coupling frames and its hardware implementation," *Chaos An Interdiscip. J. Nonlinear Sci.*, vol. 33, no. 7, Jul. 2023, doi: 10.1063/5.0154516.
- [30] W. Ali, Z. Zuping, M. Hussain, A. Hussain, and S. Ullah, "A secure image encryption scheme using a 2D chaotic map integrated with sequential permutation and nucleotide-level diffusion," *Comput. Stand. Interfaces*, vol. 99, no. August 2026, p. 104193, Jan. 2027, doi: 10.1016/j.csi.2026.104193.
- [31] K. Nugroho, D. R. I. M. Setiadi, E. Zuliarso, A. Sambas, and O. Farooq, "FeistelX network-based image encryption leveraging hyperchaotic fusion and extended DNA coding," *Egypt. Informatics J.*, vol. 31, no. June, p. 100716, Sep. 2025, doi: 10.1016/j.eij.2025.100716.
- [32] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Integrated dual hyperchaotic and Josephus traversing based 3D confusion-diffusion pattern for image encryption," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 9, p. 101790, Oct. 2023, doi: 10.1016/j.jksuci.2023.101790.
- [33] Y. Lin *et al.*, "Cryptanalysis and Improvement of a Video Cryptosystem via Chaos and S-Box," *ACM Trans. Multimed. Comput. Commun. Appl.*, vol. 22, no. 6, pp. 1–28, Jun. 2026, doi: 10.1145/3808699.
- [34] A. Abba, J. Sen Teh, and M. Alawida, "Towards accurate keyspace analysis of chaos-based image ciphers," *Multimed. Tools Appl.*, vol. 83, no. 33, pp. 79047–79066, Mar. 2024, doi: 10.1007/s11042-024-18628-8.
- [35] L. Shi-yi, S. Jing-yu, and Z. Hao, "FPGA implementation of 4D-CSHA chaotic system with hidden attractors and its application in lightweight image encryption," *Integration*, vol. 111, p. 102858, Nov. 2026, doi: 10.1016/j.vlsi.2026.102858.
- [36] V. Mittal and Y.-P. Huang, "Quantum magic in discrete-time quantum walk," *Phys. Rev. Res.*, vol. 8, no. 1, p. 013124, Feb. 2026, doi: 10.1103/7rwg-lhqv.
- [37] A. Saha, D. Saha, and A. Chakrabarti, "Discrete-time quantum walks in qudit systems," *Eur. Phys. J. Plus*, vol. 139, no. 11, p. 971, Nov. 2024, doi: 10.1140/epjp/s13360-024-05751-6.
- [38] X. Qiang, S. Ma, and H. Song, "Quantum Walk Computing: Theory, Implementation, and Application," *Intell. Comput.*, vol. 3, Jan. 2024, doi: 10.34133/icomputing.0097.
- [39] M. Islam Kamran *et al.*, "A Highly Secured Image Encryption Scheme using Quantum Walk and Chaos," *Comput. Mater. Contin.*, vol. 73, no. 1, pp. 657–672, 2022, doi: 10.32604/cmc.2022.028876.
- [40] G. Liu, W. Li, X. Fan, Z. Li, Y. Wang, and H. Ma, "An Image Encryption Algorithm Based on Discrete-Time Alternating Quantum Walk and Advanced Encryption Standard," *Entropy*, vol. 24, no. 5, p. 608, Apr. 2022, doi: 10.3390/e24050608.
- [41] G. Cui, X. Zhou, H. Wang, W. Hao, A. Zhou, and J. Ma, "Optical Color Image Encryption Algorithm Based on Two-Dimensional Quantum Walking," *Electronics*, vol. 13, no. 11, p. 2026, May 2024, doi: 10.3390/electronics13112026.
- [42] A. A. Abd El-Latif, M. Almousa, and B. Abd-El-Atty, "A Robust Image Encryption Scheme Based on Quantum Walks and Dynamic DNA for Secure Cloud Applications," *IEEE Access*, vol. 13, pp. 119110–119130, 2025, doi: 10.1109/ACCESS.2025.3582705.