frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 18 October 2022
DOI 10.3389/fphy.2022.1028630

OPEN ACCESS

EDITED BY
Tianyu Ye,
Zhejiang Gongshang University, China

REVIEWED BY
Guodong Ye,
Guangdong Ocean University, China
Xingbin Liu,
Southwest University, China

*CORRESPONDENCE
Wei-Ping Zou,
zwp@ncu.edu.cn

SPECIALTY SECTION
This article was submitted to Quantum Engineering and Technology, a section of the journal Frontiers in Physics

RECEIVED 26 August 2022
ACCEPTED 23 September 2022
PUBLISHED 18 October 2022

CITATION
Ma Y, Yu F-F, Gong L-H and Zou W-P (2022), Fast quantum image encryption scheme based on multilayer short memory fractional order Lotka-Volterra system and dual-scale triangular map. *Front. Phys.* 10:1028630. doi: 10.3389/fphy.2022.1028630

Fast quantum image encryption scheme based on multilayer short memory fractional order Lotka-Volterra system and dual-scale triangular map

Yan Ma[1], Fang-Fang Yu[2], Li-Hua Gong[2] and Wei-Ping Zou[1]*

[1]Department of Computer Science and Technology, Nanchang University, Nanchang, China, [2]Department of Electronic Information Engineering, Nanchang University, Nanchang, China

The Caputo fractional order Lotka-Volterra system is time-consuming in practical applications, since its starting point is fixed. To tackle this problem, a short memory fractional order Lotka-Volterra system (SMFrLVS) is proposed, where the chaotic attractor of the short memory fractional order Lotka-Volterra system is achieved by the predictor-corrector method. Then, a multilayer fractional order Lotka-Volterra system with short memory (MSMFrLVS) is introduced, whose chaotic behaviors are explored *via* Poincare sections and frequency power spectra. A quantum image encryption algorithm is proposed by combining MSMFrLVS with quantum dual-scale triangular map. A quantum circuit of the dual-scale triangular map is designed with ADDER-MOD2^n. At the permutation stage, the plaintext image is transformed into quantum form with the generalized quantum image representation model. The resulting quantum image is divided into sub-blocks and scrambled by the quantum dual-scale triangular map. Subsequently, the intra and the inter permutation operations on bit-planes are realized by sorting pseudo-random sequence and by quantum Gray code, respectively. At the diffusion stage, the initial values of the MSMFrLVS are generated with a plaintext correlation mechanism. The ciphertext image can be acquired by carrying out three-level diffusion operations. It is demonstrated that the proposed quantum image encryption algorithm performs better than some typical image encryption algorithm in terms of security, robustness, computational complexity and encryption speed.

KEYWORDS

quantum image encryption, fractional order differential equation, Lotka-Volterra system, predictor-corrector method, quantum dual-scale triangular map

1 Introduction

Lots of efficient quantum image encryption algorithms have been developed [1–5]. Since chaotic systems have good dynamic characteristics, they are very suitable for quantum image encryption [6–8]. Dai et al. presented an image encryption and compression algorithm based on 4D hyper-chaotic Henon map [9]. Zhou et al.

designed a secure quantum image encryption algorithm based on 5D hyper-chaotic system [10]. Ye et al. explored a fast image encryption scheme based on public key cryptosystem, quantum logistic map and the substitution-permutation network [11]. Khan et al. proposed a fast quantum image encryption scheme based on affine transform and fractional order Lorenz-like chaotic dynamical system [12]. Signing et al. provided an image encryption algorithm by combining a chameleon chaotic system with dynamic DNA coding [13]. Wang et al. researched a color image encryption scheme by combining hyper-chaotic system with improved quantum revolving gate [14]. Li et al. proposed an image encryption scheme by combining quantum chaos with discrete fractional wavelet transform [15]. Wu et al. designed a quantum image encryption based on 2D logistic map and quantum Baker map [16]. Hu et al. presented an efficient quantum color image encryption scheme using a new 3D chaotic system [17]. Kamran et al. proposed a secure image encryption algorithm based on quantum walk and chaos [18].

There have been numerous proposals for quantum image encryption algorithms with image scrambling methods [19–21]. Hu et al. proposed a quantum image encryption algorithm based on Arnold transform and wavelet transform, where the wavelet coefficients are scrambled by the Arnold transform [22]. Liu et al. designed a quantum image encryption algorithm by combining general Arnold transform with substitution tables (S-box) scrambling [23]. Liu et al. developed a quantum block image encryption algorithm with quantum Arnold transform based on the superposition property of quantum states [24]. Zhou et al. suggested a multi-image encryption scheme based on quantum 3D Arnold transform [25]. However, these methods have some limitations and cannot be used to scramble the rectangle image. For any rectangle image, it should be expanded into the square image or divided into many square images before scrambling, which will add extra space and increase computational complexity.

A fast quantum image encryption scheme for a rectangle image based on the MSMFrLVS and quantum dual-scale triangular map is proposed. During the encryption process, the plaintext image is represented with the generalized quantum image representation (GQIR) model, the image sub-blocks are shuffled with quantum dual-scale triangular map. Subsequently, the bit-level permutation is performed by the random sequence generated by the MSMFrLVS and quantum Gray code, respectively. Then, the three-level diffusion operations among the pixel values, binary bits and pixel bits are implemented by the chaotic sequences originated by the MSMFrLVS. Simulation analyses show the proposed quantum image encryption algorithm has good encryption performance and can resist any key sensitivity attacks and any brute-force attacks.

The rest of this paper is organized as follows: The basic knowledge of the GQIR for images, the MSMFrLVS and the Gray code are introduced in Section 2. The quantum circuits of dual-scale triangular map are designed in Section 3. The proposed quantum image encryption scheme is shown in Section 4. Numerical simulation analyses are described in Section 5. Finally, a conclusion is given in Section 6.

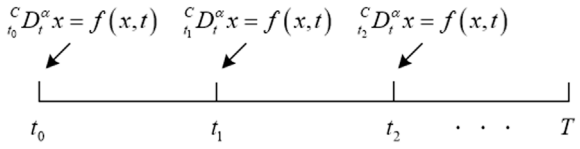

FIGURE 1
Short memory fractional order system.

2 Preliminaries

2.1 Generalized quantum image representation

In Ref. [26], the generalized quantum image representation (GQIR) can store arbitrary integer numbers $H \times W$ quantum images with $\lceil \log_2 H \rceil + \lceil \log_2 W \rceil + q$ qubits, where q is the image color depth, $\lceil \log_2 H \rceil$ and $\lceil \log_2 W \rceil$ remarked as h and ω are the sizes of the Y-axis coordinate information and the X-axis coordinate information, respectively. Hence, an $H \times W$ quantum image $|I\rangle$ with GQIR can be expressed as

$$\begin{aligned} |I\rangle &= \frac{1}{(\sqrt{2})^{h+\omega}} \left(\sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \otimes_{i=0}^{q-1} |C_{YX}^{i}\rangle |YX\rangle \right) \\ |YX\rangle &= |y_0 y_1 \cdots y_{h-1}\rangle |x_0 x_1 \cdots x_{\omega-1}\rangle, y_i, x_i \in \{0,1\}, \\ |C_{YX}\rangle &= |C_{YX}^{0} C_{YX}^{1} \cdots C_{YX}^{q-1}\rangle, C_{YX}^{i} \in \{0,1\} \end{aligned} \tag{1}$$

where $|YX\rangle$ and $|C_{YX}\rangle$ are the location information and the color information, respectively.

2.2 Multilayer short memory fractional order Lotka-Volterra system

2.2.1 Short memory fractional order system

The α order Caputo fractional derivative of function $f(t)$ is defined as [27]

$${}_{t_0}^{C}D_t^{\alpha} f(t) = \frac{1}{\Gamma(1-\alpha)} \int_{t_0}^{t} \frac{f(s)}{(t-s)^{\alpha}} \mathrm{d}s, \quad 0 < \alpha < 1, \tag{2}$$

where $\Gamma(\cdot)$ is the Gamma function. The standard Caputo fractional order system is illustrated as

$$ {}_{t_0}^{C}D_t^{\alpha}x(t) = f(t, x(t)), \quad x(t) = x_0, \tag{3} $$

where t_0 is the fixed starting point of the fractional order system.

The standard fractional order system Eq. 3 stores memory from $t = t_0$. Wu et al. proposed a short memory fractional order system which holds memory from $t\star = t_k$ and provides more freedom in the real-world applications [28], as shown in Figure 1. Let the interval $[t_0, T]$ be divided into m_1 subintervals of length $n_1 h_1$ such that $[t_0, T] = [t_0, t_1] \cup [t_1, t_2] \cup \cdots \cup [t_{m_1-1}, t_{m_1}]$, n_1 is an integer and $h_1 = (T - t_0)/N_1$. The short memory fractional order system is given as

$$ \begin{cases} {}_{t_*}^{C}D_t^{\alpha}x(t) = f(x,t), \quad x(t_0) = x_0 \\ t_* = t_k, \quad t \in [t_k, t_{k+1}], k = 0, \ldots, m_1 - 1 \end{cases}. \tag{4} $$

2.2.2 Short memory fractional order Lotka-Volterra system

The fractional order Lotka-Volterra chaotic system is defined as [29].

$$ \begin{aligned} {}_{t_0}^{C}D_t^{\alpha_1}x &= \gamma x + ex^2 - \varpi xy - \lambda zx^2 \\ {}_{t_0}^{C}D_t^{\alpha_2}y &= -\mu y + \tau xy \\ {}_{t_0}^{C}D_t^{\alpha_3}z &= -\xi z + \sigma zx^2 \end{aligned}, \tag{5} $$

where $\alpha_i\,(i = 1, 2, 3)$ represents the fractional order of the system Eq. 5, γ denotes the intrapopulation natural growth rate of the prey, ϖ denotes the effect of the predator on the prey, μ is the intrapopulation natural growth rate of the predator, τ is the positive effect of the prey on the predator, the parameters $\gamma, \varpi, \mu, \tau$, and the constants e, ξ, σ are positive.

We define the SMFrLVS as

$$ \begin{aligned} {}_{t_*}^{C}D_t^{\alpha_1}x &= \gamma x + ex^2 - \varpi xy - \lambda zx^2 \\ {}_{t_*}^{C}D_t^{\alpha_2}y &= -\mu y + \tau xy \\ {}_{t_*}^{C}D_t^{\alpha_3}z &= -\xi z + \sigma zx^2 \end{aligned}. \tag{6} $$

In Eq. 6, the starting point of the SMFrLVS is the variable point $t\star$ rather than a fixed point t_0 such that the SMFrLVS improves the speed of the numerical computation.

2.2.3 Predictor-corrector method for the SMFrLVS

The predictor-corrector method is one of the most widely methods used in the chaotic analysis of the fractional order system, which explains the approximate solution of the nonlinear fractional order differential equations. The SMFrLVS is solved by the predictor-corrector method as follows.

For the interval $[t_0, t_1]$, the predicted values are given as

$$ \begin{aligned} x_1^p &= x_0 + \frac{h_1^{\alpha_1}}{\alpha_1\Gamma(\alpha_1)}\left(\gamma x_0 + ex_0^2 - \varpi x_0 y_0 - \lambda z_0 x_0^2\right) \\ y_1^p &= y_0 + \frac{h_1^{\alpha_2}}{\alpha_2\Gamma(\alpha_2)}\left(-\mu y_0 + \tau x_0 y_0\right) \\ z_1^p &= z_0 + \frac{h_1^{\alpha_3}}{\alpha_3\Gamma(\alpha_3)}\left(-\xi z_0 + \sigma z_0 x_0^2\right) \end{aligned}. \tag{7} $$

The numerical solutions are determined by

$$ \begin{aligned} x_1 &= x_0 + \frac{h_1^{\alpha_1}}{\Gamma(\alpha_1+2)}\left[(1+\alpha_1)\left(\gamma x_0 + ex_0^2 - \varpi x_0 y_0 - \lambda z_0 x_0^2\right) + \gamma x_1^p + ex_1^p 2 - \varpi x_1^p y_1^p - \lambda z_1^p x_1^{p2}\right] \\ y_1 &= y_0 + \frac{h_1^{\alpha_2}}{\Gamma(\alpha_2+2)}\left[(1+\alpha_2)\left(-\mu y_0 + \tau x_0 y_0\right) + \tau x_1^p y_1^p - \mu y_1^p\right] \\ z_1 &= z_0 + \frac{h_1^{\alpha_3}}{\Gamma(\alpha_3+2)}\left[(1+\alpha_3)\left(-\xi z_0 + \sigma z_0 x_0^2\right) + \sigma z_1^p x_1^{p2} - \xi z_1^p\right] \end{aligned}. \tag{8} $$

For $t \in [t_k, t_{k+1}]$, $1 \le k \le m_1 - 1$, and $m_1 \ge 2$, the predicted values are defined as

$$ \begin{aligned} x_{k+i+1}^p &= x_k + \frac{h_1^{\alpha_1}}{\Gamma(\alpha_1)}\sum_{j=0}^{i} b_{j,i+1}\left(\gamma x_k + ex_k^2 - \varpi x_k y_k - \lambda z_k x_k^2\right) \\ y_{k+i+1}^p &= y_k + \frac{h_1^{\alpha_2}}{\Gamma(\alpha_2)}\sum_{j=0}^{i} b_{j,i+1}\left(-\mu y_k + \tau x_k y_k\right) \\ z_{k+i+1}^p &= z_k + \frac{h_1^{\alpha_3}}{\Gamma(\alpha_3)}\sum_{j=0}^{i} b_{j,i+1}\left(-\xi z_k + \sigma z_k x_k^2\right) \end{aligned}, \tag{9} $$

where the coefficient $b_{j,i+1}$ is expressed as

$$ b_{j,i+1} = \frac{1}{\alpha}\left[(i+1-j)^{\alpha} - (i-j)^{\alpha}\right]. \tag{10} $$

The numerical solutions are defined as

$$ \begin{aligned} x_{k+i+1} &= x_k + \frac{h_1^{\alpha_1}}{\Gamma(\alpha_1+2)}\left(\sum_{j=0}^{i} a_{j,i+1}\left(\gamma x_{k+j} + ex_{k+j}^2 - \varpi x_{k+j} y_{k+j} - \lambda z_{k+j} x_{k+j}^2\right)\right. \\ &\quad \left. + \gamma x_{k+i+1}^p + ex_{k+i+1}^{p2} - \varpi x_{k+i+1}^p y_{k+i+1}^p - \lambda z_{k+i+1}^p x_{k+i+1}^{p2}\right) \\ y_{k+i+1} &= y_k + \frac{h_1^{\alpha_2}}{\Gamma(\alpha_2+2)}\left[\sum_{j=0}^{i} a_{j,i+1}\left(-\mu y_{k+j} + \tau x_{k+j} y_{k+j}\right) + \tau x_{k+i+1}^p y_{k+i+1}^p - \mu y_{k+i+1}^p\right], \\ z_{k+i+1} &= z_k + \frac{h_1^{\alpha_3}}{\Gamma(\alpha_3+2)}\left[\sum_{j=0}^{i} a_{j,i+1}\left(-\xi z_{k+j} + \sigma z_{k+j} x_{k+j}^2\right) + \sigma z_{k+i+1}^p x_{k+i+1}^{p2} - \xi z_{k+i+1}^p\right] \end{aligned} \tag{11} $$

where the coefficient $a_{j,i+1}$ is given as

$$ a_{j,i+1} = \begin{cases} i^{\alpha+1} - (i-\alpha)(i+1)^{\alpha}, & j = 1; \\ (i-j+2)^{\alpha+1} + (i-j)^{\alpha+1} - 2(i-j+1)^{\alpha+1}, & 1 < j \le i; \\ 1, & j = i+1. \end{cases} \tag{12} $$

The parameters are set as $\gamma = 1$, $\varpi = 1$, $\mu = 1$, $\tau = 1$, $e = 2$, $\xi = 3$, $\sigma = 2.7$, $h_1 = 0.01$, $N_1 = 5000$, and the initial values are taken as $[1, 1.4, 1]$. When $\alpha_i\,(i = 1, 2, 3) = 0.8$, the chaotic attractors of the SMFrLVS with phase portraits are plotted in Figure 2. When $\alpha_i\,(i = 1, 2, 3) = 0.95$, the chaotic attractors of the SMFrLVS with phase portraits are described in Figure 3. The SMFrLVS can significantly save time and is more suitable for practical applications than the fractional order Lotka-Volterra system, since the SMFrLVS starts from $t\star$, as shown in Table 1.

2.2.4 Multilayer short memory fractional order Lotka-Volterra system

We propose the MSMFrLVS as follows

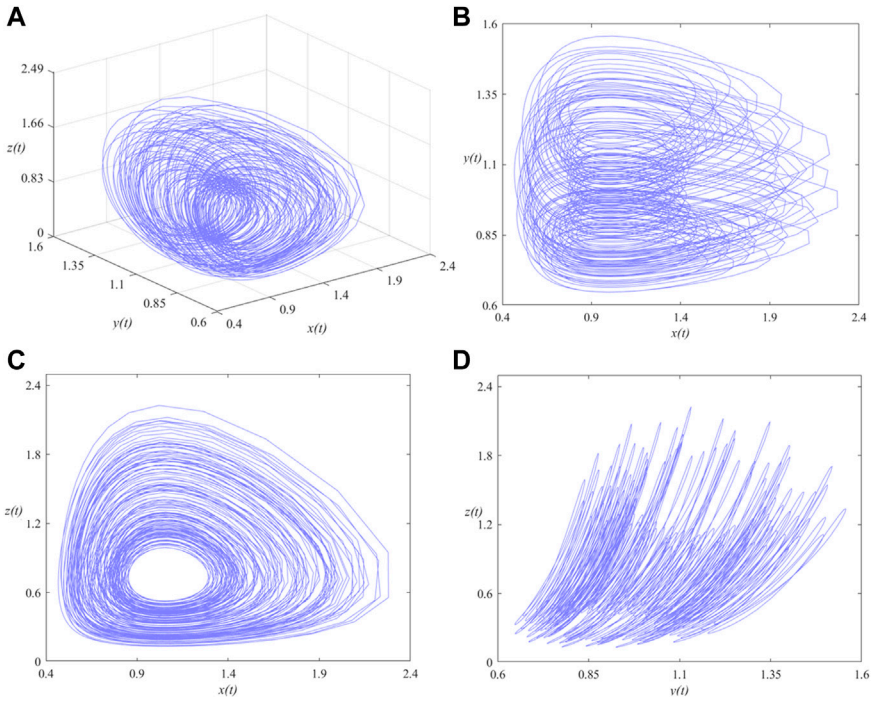

FIGURE 2
Phase portraits of the SMFrLVS when α_i (i = 1, 2, 3) = 0.8 in: **(A)** x-y-z space, **(B)** x-y, **(C)** x-z, **(D)** y-z planes.

$$\begin{cases} {}_{t_*}^{C}D_t^{\alpha_1'}x = \gamma x + ex^2 - \varpi xy - \lambda zx^2 \\ {}_{t_*}^{C}D_t^{\alpha_2'}y = -\mu y + \tau xy \\ {}_{t_*}^{C}D_t^{\alpha_3'}z = -\xi z + \sigma zx^2 \\ {}_{t_*}^{C}D_t^{\alpha_4'}w = (vx^2 - 1)\tanh(w) \end{cases}, \tag{13}$$

where the parameters $\gamma, \varpi, \mu, \tau$, and the constants $e, \xi, \sigma, v$are positive, $\alpha_i'(i = 1, 2, 3, 4)$ represent the fractional order of the MSMFrLVS, the starting point of the MSMFrLVS is t_*. The numerical solutions of the MSMFrLVS are acquired with the predictor-corrector method, the chaotic attractors of the MSMFrLVS with phase portraits are depicted in Figure 4, when $\alpha_i'(i = 1, 2, 3, 4) = 0.95$ and N_1 takes 2000, 3000, 4000, 5000, the values of other parameters remain unchanged, it is illustrated that the number of layers of the MSMFrLVS increases with the increase of N_1. When $N_1 = 5000$ and $\alpha_i'(i = 1, 2, 3, 4) = 0.7, 0.8, 0.85, 0.9$, the values of other parameters remain unchanged, the chaotic attractors of the MSMFrLVS with phase portraits are displayed in Figure 5, it is shown that the number of layers of the MSMFrLVS decreases as the increase of the fractional order.

It is difficult to describe the orbits of a chaotic system concisely due to the disorder of the orbits. One of the ideas is to reduce the dimension of description and simplify the trajectory of the space into a series of discrete points, thus the Poincare section is observed. A large number of points observed at the intersection of the phase space trajectory and the Poincare section are a feature of the chaotic motion, as shown in Figure 6. In addition, the continuous frequency power spectrum is generally regarded as an indicator of chaos, the frequency power spectra of the MSMFrLVS are plotted in Figure 7.

2.3 Gray code

Gray code is a signal coding method and generally used in the digital conversions [30]. Gray code can be expressed as

$$\begin{cases} \phi_i = \delta_i \oplus \delta_{i+1}, i = 0, 1, \ldots, q-1 \\ \phi_q = \delta_q \end{cases}, \tag{14}$$

where δ is a positive integer with binary code $\delta = \delta_q\delta_{q-1}\cdots\delta_1\delta_0$.

3 Quantum realization of the dual-scale triangular map

3.1 Quantum representation of the dual-scale triangular map

Li et al. [31] proposed 2D dual-scale triangular map which can be utilized to scramble a rectangle image directly. For a given

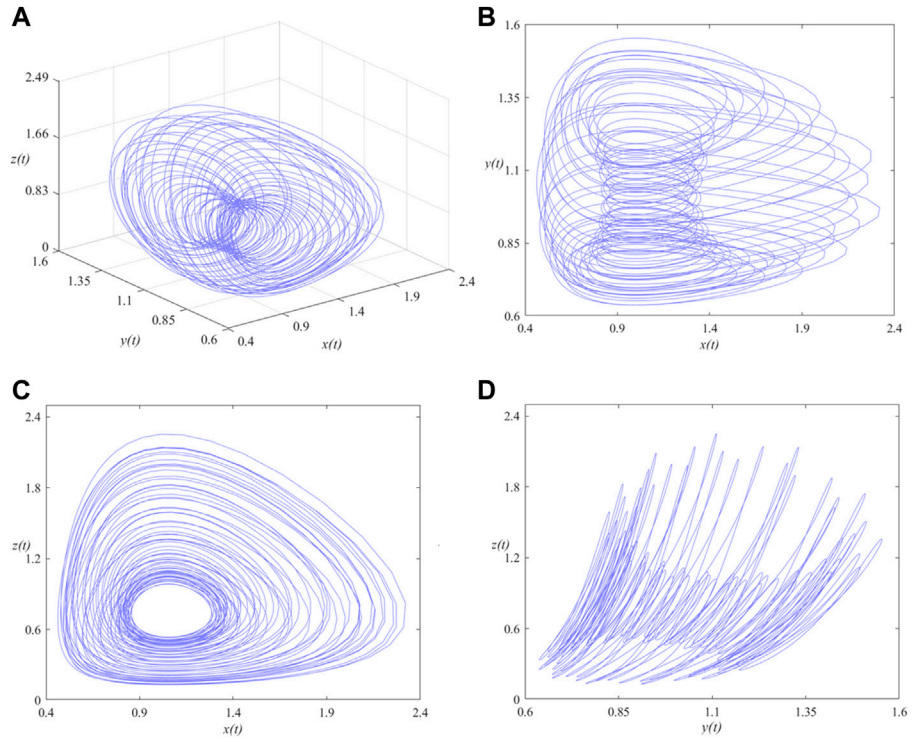

FIGURE 3
Phase portraits of the SMFrLVS when α_i (i = 1, 2, 3) = 0.95 in: **(A)** x-y-z space, **(B)** x-y, **(C)** x-z, **(D)** y-z planes.

$M \times N$ matrix, (x, y) represent the pixel coordinates and (x', y') corresponding to the changed pixel coordinates. 2D dual-scale triangular map is defined as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix}, \tag{15}$$

where a, c and d are non-negative integers. Note that a and M should be co-prime, so should d and N.

The inverse dual-scale triangular map is

$$\begin{cases} x = \left(a^{-1}x'\right) \bmod M \\ y = \left(d^{-1}y' - px + s\right) \bmod N \end{cases}, \tag{16}$$

where $p = d^{-1}c$ and $s = \text{ceil}(cM/N) \cdot N \cdot d^{-1}$, ceil (x) denotes that each element of x is rounded to the nearest integer greater than or equal to that element. $(a^{-1}a) \bmod M = 1$ and $(d^{-1}d) \bmod N = 1$.

According to the classical dual-scale triangular map, the quantum representation of the dual-scale triangular map can be expressed as

$$\begin{cases} |x'\rangle = |ax \bmod 2^m\rangle \\ |y'\rangle = |(cx + dy) \bmod 2^n\rangle \end{cases}. \tag{17}$$

Correspondingly, the quantum representation of the inverse dual-scale triangular map can be defined as

$$\begin{cases} |x\rangle = |a^{-1}x' \bmod 2^m\rangle \\ |y\rangle = \left|\left(d^{-1}y' - px + s\right) \bmod 2^n\right\rangle \end{cases}. \tag{18}$$

3.2 Quantum circuits for the dual-scale triangular map and the inverse dual-scale triangular map

3.2.1 Quantum circuits for the dual-scale triangular map

According to Eq. 17, the states $|x'\rangle$ and $|y'\rangle$ are independent of each other. Therefore, the quantum circuits of $|x'\rangle$ and $|y'\rangle$ can be designed.

(1) Quantum circuit $|x'\rangle$. According to Eq. 17, $|x'\rangle$ can be achieved with a steps.

$$|x, x\rangle \rightarrow |x, 2x \bmod 2^m\rangle \rightarrow \cdots \rightarrow |x, ax \bmod 2^m\rangle. \tag{19}$$

$ax \bmod 2^m$ from the first step to the last step can be acquired with the ADDER-MOD2^m network [32], as shown in Figure 8A.

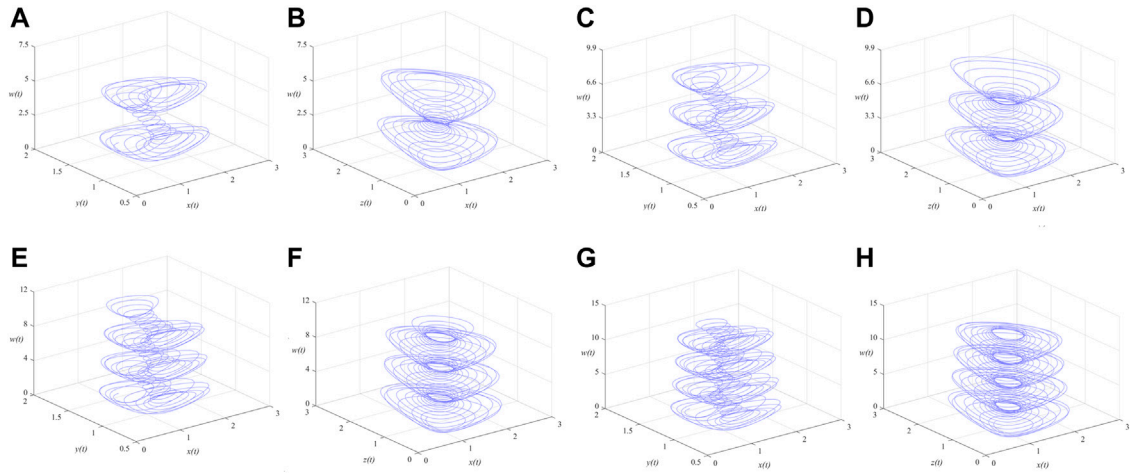

FIGURE 4
Phase portraits of the MSMFrLVS in x-y-w space and x-z-w space: **(A,B)**: $N_1 = 2000$, **(C,D)**: $N_1 = 3000$, **(E,F)**: $N_1 = 4000$, **(G,H)**: $N_1 = 5000$.

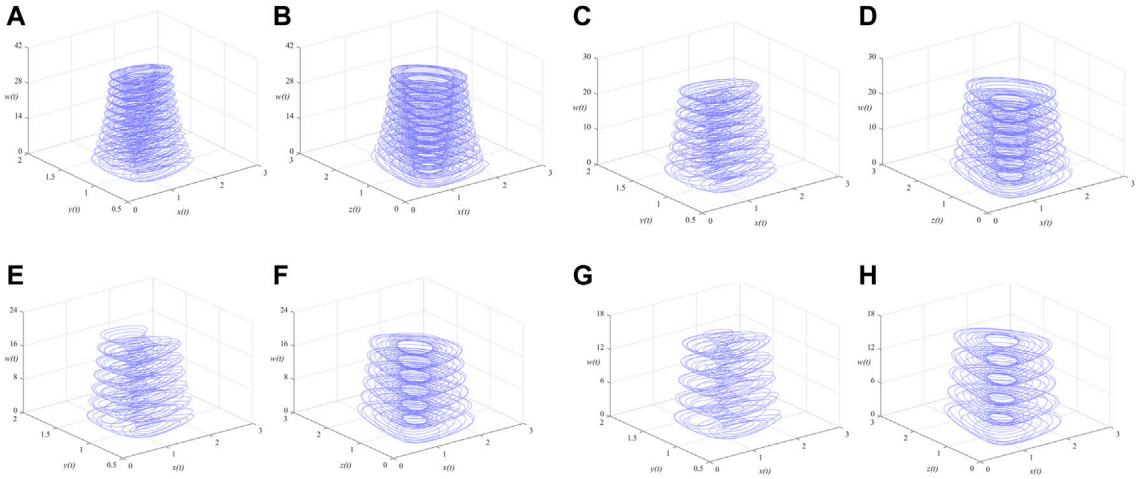

FIGURE 5
Phase portraits of the MSMFrLVS in x-y-w space and x-z-w space: **(A,B)**: $\alpha_i' = 0.7$, **(C,D)**: $\alpha_i' = 0.8$, **(E,F)**: $\alpha_i' = 0.85$, **(G,H)**: $\alpha_i' = 0.9$

TABLE 1 Time comparison between the SMFrLVS and the fractional order Lotka-Volterra system.

N_1	The SMFrLVS (s)	Fractional order Lotka-Volterra system (s)
4,000	0.863	14.575
8,000	0.992	66.054
16,000	1.077	226.386
30,000	1.272	1306.923
40,000	1.437	1802.287
50,000	1.624	3,256.137

(2) Quantum circuit $|y'\rangle$. According to Eq. 17, $|y'\rangle$ can be realized with $c + d + 1$ steps.

$$|x, x\rangle \rightarrow |x, 2x \bmod 2^n\rangle \rightarrow \cdots \rightarrow |x, cx \bmod 2^n\rangle \rightarrow |y, cx \bmod 2^n\rangle \rightarrow |y, (cx + y) \bmod 2^n\rangle \rightarrow \cdots \rightarrow |y, (cx + dy) \bmod 2^n\rangle. \tag{20}$$

It shows that $cx \bmod 2^n$ from the first step to the c-th step can be obtained with the ADDER-MOD2^n network. In the $(c + 1)$-th step, x is substituted for y. $(cx + dy) \bmod 2^n$ from the $(c + 2)$-th step to the last step can be constructed with the ADDER-MOD2^n network. The quantum circuit $|y'\rangle$ is depicted in Figure 8B.

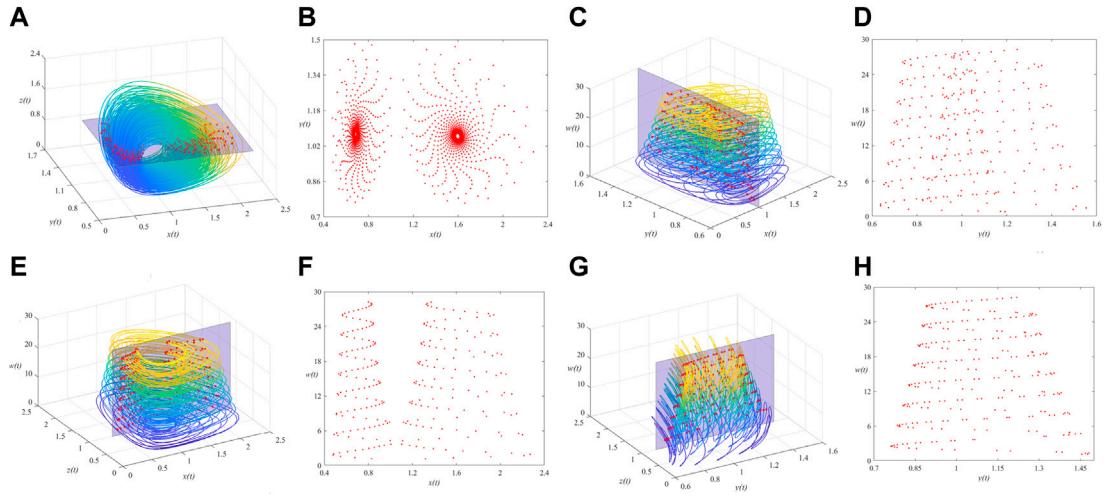

FIGURE 6
3D view of the MSMFrLVS and the Poincare section in: **(A,B)**: *x-y-z* space, **(C,D)**: *x-y-w* space, **(E,F)**: *x-z-w* space, **(G,H)**: *y-z-w* space.

3.2.2 Quantum circuits for the inverse dual-scale triangular map

To recover the plaintext image from the scrambled image, the quantum circuits of $|x\rangle$ and $|y\rangle$ should be involved. From Eq. 18, the inverse transform uses subtraction operation. A theorem stated in [32] provides a solution to realizing the subtraction operation.

$$(x - y)\bmod 2^n = (x + (\bar{y} + 1))\bmod 2^n, \tag{21}$$

where $\bar{y} = \overline{y_{n-1}y_{n-2}}\ldots\overline{y_0}$, $\overline{y_i} = 1 - y_i$, $i = n-1, n-2, \ldots, 0$.

(1) Quantum circuit $|x\rangle$. From Eq. 18, it requires a^{-1} steps to realize $|x\rangle$, as illustrated in Figure 9A. $|x\rangle$ can be constructed as

$$|x', x'\rangle \rightarrow\cdots\rightarrow |x', a^{-1}x'\bmod 2^m\rangle. \tag{22}$$

$a^{-1}x'\bmod 2^m$ from the first step to the last step can be created with the ADDER-MOD2^m network.

(2) Quantum circuit $|y\rangle$. By recalling Eq. 18, $|y\rangle$ can be implemented with $p + d^{-1} + 6$ steps, as depicted in Figure 9B.

$$\begin{aligned}&|\bar{x}, \bar{x}\rangle \rightarrow\cdots\rightarrow |\bar{x}, p\bar{x}\bmod 2^n\rangle \rightarrow |p, p\bar{x}\bmod 2^n\rangle \rightarrow |p, p(\bar{x}+1)\bmod 2^n\rangle\\ &\rightarrow |y', p(\bar{x}+1)\bmod 2^n\rangle \rightarrow\cdots\rightarrow |y', (p(\bar{x}+1) + d^{-1}y')\bmod 2^n\rangle\\ &\rightarrow |s, (p(\bar{x}+1) + d^{-1}y')\bmod 2^n\rangle \rightarrow |s, (p(\bar{x}+1) + d^{-1}y' + s)\bmod 2^n\rangle.\end{aligned} \tag{23}$$

It demonstrates that $p\bar{x}\bmod 2^n$from the first step to the p-th step can be obtained with the ADDER-MOD2^n network. $\bar{x}$ is superseded by p in the $(p+1)$-th step. In the $(p+2)$-th step, $p(\bar{x}+1)\bmod 2^n$ is acquired with the help of the ADDER-MOD2^n operation. In the $(p+3)$-th step, p is replaced by y'. From the $(p+4)$-th step to the $(p + d^{-1} + 4)$-th step, $(p(\bar{x}+1) + d^{-1}y')\bmod 2^n$ is generated with the ADDER-MOD2^n network. In the $(p + d^{-1} + 5)$-th step, y' is substituted for s. In the last step, $(p(\bar{x}+1) + d^{-1}y' + s)\bmod 2^n$ is accomplished by the ADDER-MOD2^n network.

4 Quantum image encryption and decryption algorithm

4.1 Quantum image encryption algorithm

The proposed quantum image encryption scheme based on the MSMFrLVS and quantum dual-scale triangular map is shown in Figure 10. The plaintext image is represented with the GQIR model. During the permutation stage, the position information of the quantum image is shuffled by the block-level permutation and the intra and the inter bit-level permutation operations, while the color information of the quantum image remains unchanged. In the diffusion stage, three-level diffusion operations including pixel values, binary bits and pixel bits are accomplished for the scrambled image.

Assume the plaintext image of size $N \times M$ with a color depth q to be encrypted is expressed as $|I\rangle$ and its GQIR representation can be written as

$$|I\rangle = \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle|YX\rangle. \tag{24}$$

The specific encryption algorithm involves the following steps.

Step 1: Block-level scrambling is performed. To effectively realize the block-level arrangement, the plaintext image

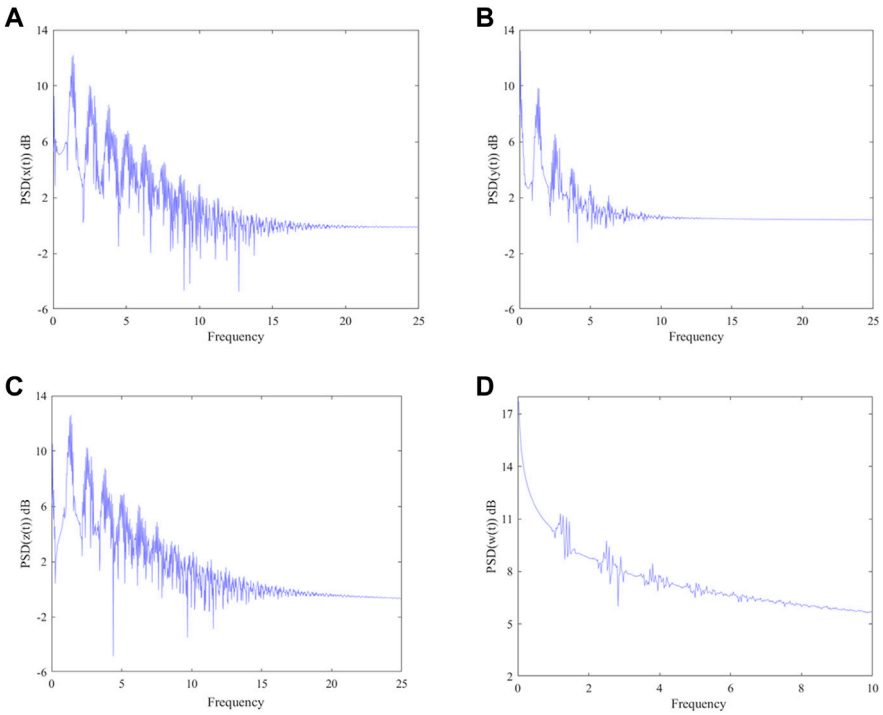

FIGURE 7
Frequency power spectra of the MSMFrLVS in: **(A)** x, **(B)** y, **(C)** z, **(D)** w planes.

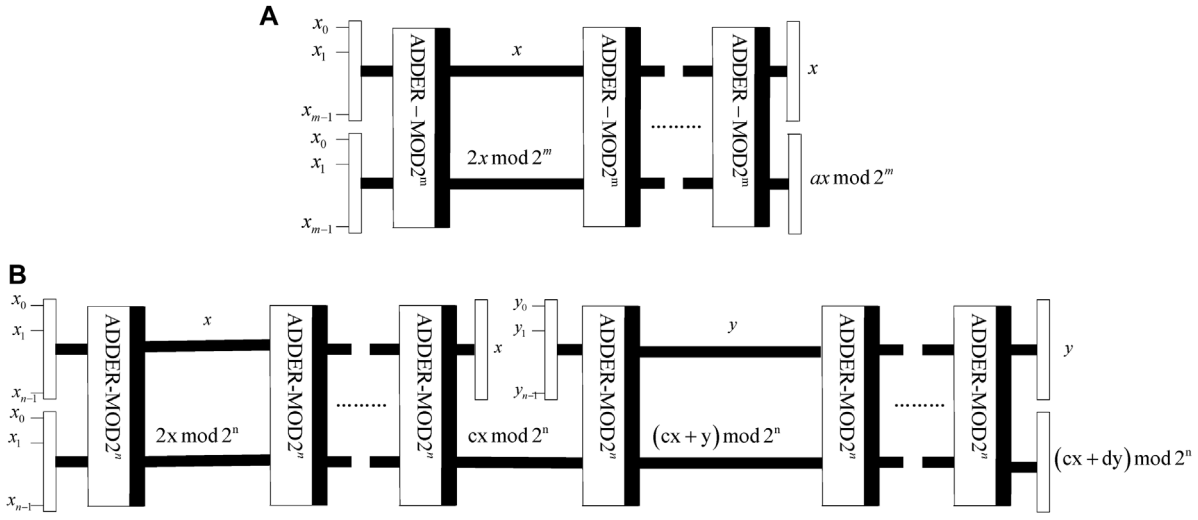

FIGURE 8
Quantum circuits:**(A)** $|x'\rangle$, **(B)** $|y'\rangle$.

should be decomposed into sub-blocks. If the block size is $2^{w_1} \times 2^{w_1}$, then the number of blocks is $2^{n-w_1} \times 2^{m-w_1}$ after division. Assume that Q_{dst} represents the quantum dual-scale triangular map which is applied on the $n - w_1$ and $m - w_1$ qubits and the scrambled block image $|I_b\rangle$ can be acquired.

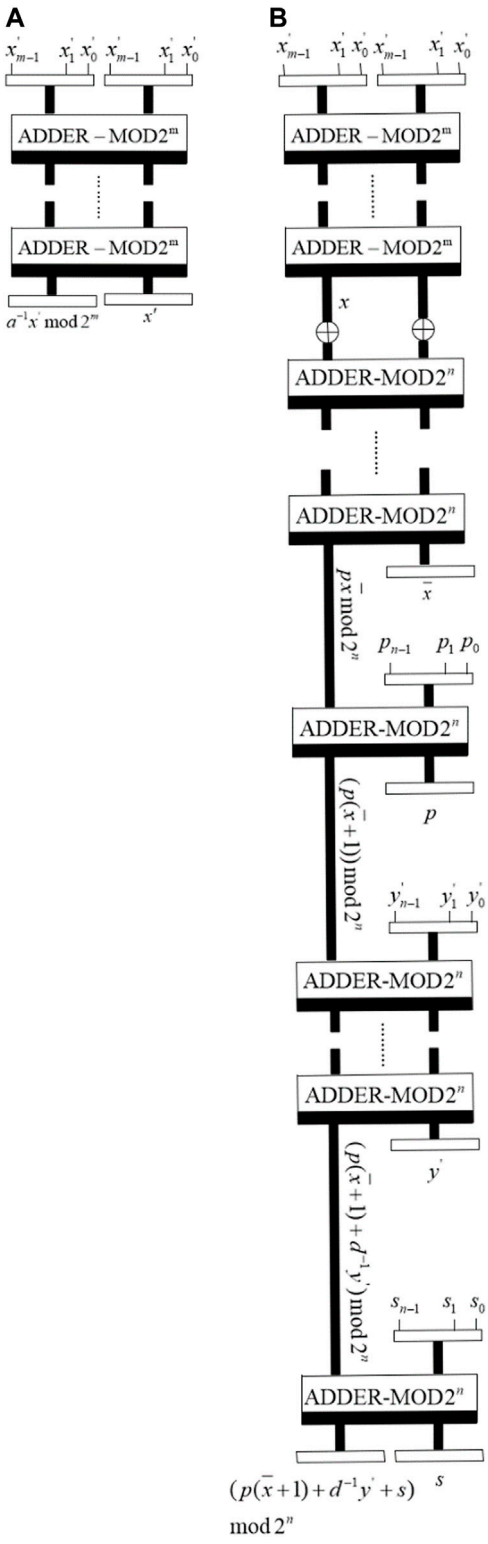

FIGURE 9
Quantum circuit **(A)** $|x\rangle$, **(B)** $|y\rangle$.

$$
\begin{aligned}
|I_b\rangle &= Q_{\mathrm{dst}}|I\rangle = \frac{1}{(\sqrt{2})^{n+m}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} \bigotimes_{j=0}^{q-1} |C_{YX}^j\rangle Q_{\mathrm{dst}}|YX\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} \bigotimes_{j=0}^{q-1} |C_{YX}^j\rangle Q_{\mathrm{dst}}\left(\left|y_{n-1}y_{n-2}\cdots y_0\right\rangle |x_{m-1}x_{m-2}\cdots x_0\rangle\right) \\
&= \frac{1}{(\sqrt{2})^{n+m}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} \bigotimes_{j=0}^{q-1} |C_{YX}^j\rangle Q_{\mathrm{dst}}\left(\left|y_{n-1}y_{n-2}\cdots y_{w_1}\right\rangle\right)\left|y_{w_1-1}\cdots y_0\right\rangle \\
&\quad Q_{\mathrm{dst}}\left(|x_{m-1}x_{m-2}\cdots x_{w_1}\rangle\right)|x_{w_1-1}\cdots x_0\rangle \\
&= \frac{1}{(\sqrt{2})^{n+m}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} \bigotimes_{j=0}^{q-1} |C_{YX}^j\rangle \left|y'_{n-1}\ y'_{n-2}\cdots y'_{w_1}\ y_{w_1-1}\cdots y_0\right\rangle \left|x'_{m-1}\ x'_{m-2}\cdots x'_{w_1}\ x_{w_1}\cdots x_0\right\rangle.
\end{aligned}
\tag{25}
$$

According to Eq. 17, the scrambled position qubits $|y'_{n-1}\ y'_{n-2}\cdots y'_{w_1}\rangle$ and $|x'_{m-1}\ x'_{m-2}\cdots x'_{w_1}\rangle$ can be obtained as

$$
\begin{cases}
\left|y'_{n-1}\ y'_{n-2}\cdots y'_{w_1}\right\rangle = Q_{\mathrm{dst}}\left(y_{n-1}y_{n-2}\cdots y_{w_1}\right) \\
\qquad\qquad = \left(c|x_{n-1}x_{n-2}\cdots x_{w_1}\rangle + d\left|y_{n-1}y_{n-2}\cdots y_{w_1}\right\rangle\right) \bmod 2^{n-w_1} \\
\left|x'_{m-1}\ x'_{m-2}\cdots x'_{w_1}\right\rangle = Q_{\mathrm{dst}}\left(x_{m-1}x_{m-2}\cdots x_{w_1}\right) = \left(a|x_{m-1}x_{m-2}\cdots x_{w_1}\rangle\right) \bmod 2^{m-w_1}
\end{cases}.
\tag{26}
$$

The circuit of image block-level permutation based on Q_{dst} is depicted in Figure 11.

Step 2. : To improve the security of the system, a plaintext correlation mechanism is employed to obtain the initial values of the MSMFrLVS. The method is expressed as

$$
\begin{cases}
x'(0) = x(0) + \sum_{i=1}^{8} h_i \times 10^{-6} + \dfrac{h_9 \oplus h_{10} \oplus \cdots h_{16}}{10^{10}} \\
y'(0) = y(0) + \sum_{i=17}^{24} h_i \times 10^{-6} + \dfrac{h_{25} \oplus h_{26} \oplus \cdots h_{32}}{10^{10}} \\
z'(0) = z(0) + \sum_{i=33}^{40} h_i \times 10^{-6} + \dfrac{h_{41} \oplus h_{42} \oplus \cdots h_{48}}{10^{10}} \\
w'(0) = w(0) + \sum_{i=49}^{56} h_i \times 10^{-6} + \dfrac{h_{57} \oplus h_{58} \oplus \cdots h_{64}}{10^{10}}
\end{cases},
\tag{27}
$$

where $x(0)$, $y(0)$, $z(0)$ and $w(0)$ are the initial values of Eq. 13, h_i is a 256-bit hash value, $x'(0)$, $y'(0)$, $z'(0)$ and $w'(0)$ are the updated initial values of Eq. 13. Obviously, the new initial values are related to the plaintext image.

Step 3: The initial values $x'(0)$, $y'(0)$, $z'(0)$ and $w'(0)$ are iterated with Eq. 13 $m' + 2^n \times 2^m$ times, m' is set to 100. To avoid the harmful effect of transient procedure, a new chaotic sequence $\{\Upsilon_i | i = 1, 2, \ldots, 2^n \times 2^m\}$ is obtained after abandoning the former m' elements, where $\Upsilon \in \{x, y, z, w\}$.

Step 4: The new chaotic sequence is transformed into integer sequence, $\{\Upsilon_i^* | i = 1, 2, \cdots, 2^n \times 2^m\}$,

$$
\Upsilon_i^* = \left|\left\lfloor \left(\Upsilon_i - \lfloor \Upsilon_i \rfloor\right) \times 10^{14} \right\rfloor\right| \bmod 256,
\tag{28}
$$

where $\lfloor \Upsilon \rfloor$ rounds Υ to the nearest integer towards zero.

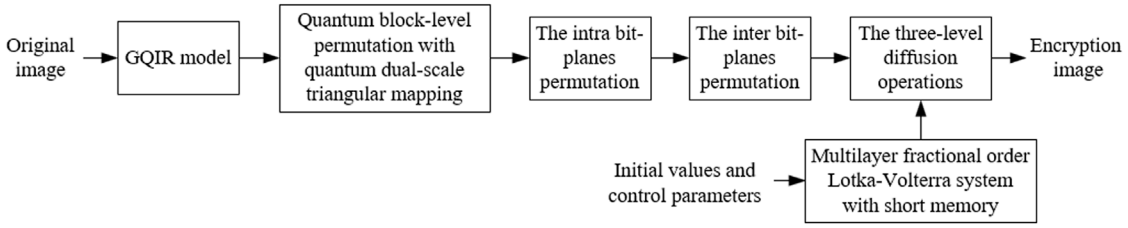

FIGURE 10
Flowchart of image encryption algorithm.

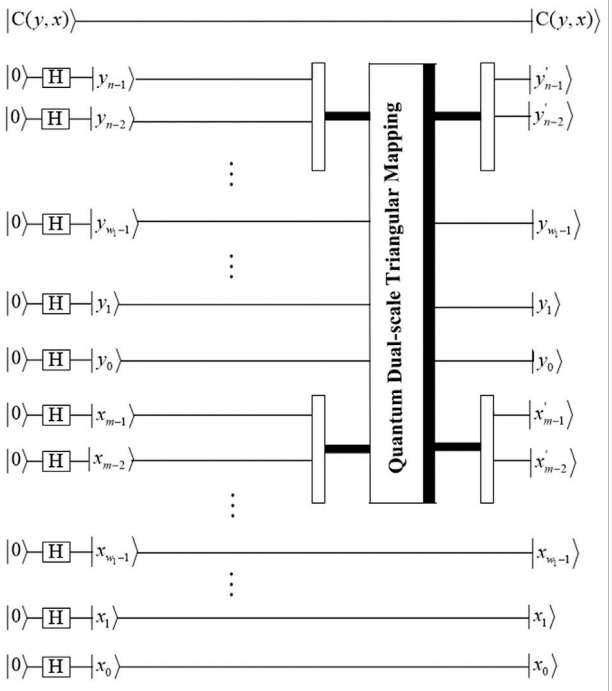

FIGURE 11
Quantum circuit for the block-level permutation based on Q_{dst}.

Step 5. : Bit-level permutation includes the intra bit-planes permutation and the inter bit-planes permutation. The intra bit-planes permutation is accomplished by sorting the sequence $\{x_i^*|i = 1, 2, \cdots, 8\}$ in ascending order. The corresponding quantum circuit is shown in Figure 12, where the exchange of bit-planes is implemented with quantum swap gate.

For pixel (Y, X), a quantum sub-operation φ_{YX} can be constructed as

$$\varphi_{YX} = I \otimes \sum_{y=0}^{2^n-1} \sum_{x=0, YX \neq yx}^{2^m-1} |yx\rangle\langle yx| + G_{YX} \otimes |YX\rangle\langle YX|. \quad (29)$$

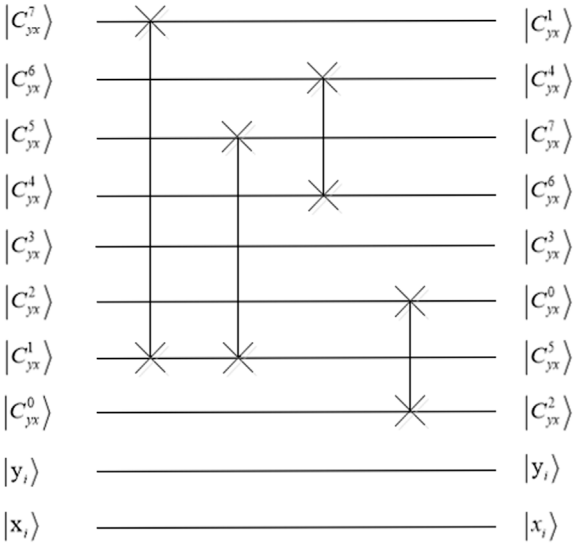

FIGURE 12
Quantum circuit of the intra bit-planes permutation.

where G_{YX} to realize bit-planes permutation operation is defined as

$$\begin{aligned} G_{YX}|C(y,x)\rangle &= G_{YX}\left|c_{yx}^7 c_{yx}^6 c_{yx}^5 c_{yx}^4 c_{yx}^3 c_{yx}^2 c_{yx}^1 c_{yx}^0\right\rangle \\ &= \left|c_{yx}^1 c_{yx}^4 c_{yx}^7 c_{yx}^6 c_{yx}^3 c_{yx}^0 c_{yx}^5 c_{yx}^2\right\rangle \end{aligned}, \quad (30)$$

By applying the quantum sub-operation φ_{YX} on the block-level permutation image $|I_b\rangle$, the bit-planes of pixel (Y, X) are scrambled.

$$\begin{aligned} \varphi_{YX}|I_b\rangle &= \frac{1}{(\sqrt{2})^{n+m}}\varphi_{YX}\left(\sum_{y=0}^{2^n-1}\sum_{x=0, YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + |C(Y,X)\rangle|YX\rangle\right) \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0, YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + \varphi_{YX}\left(\left|c_{yx}^7 c_{yx}^6 c_{yx}^5 c_{yx}^4 c_{yx}^3 c_{yx}^2 c_{yx}^1 c_{yx}^0\right\rangle|YX\rangle\right) \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0, YX\neq yx}^{2^m-1}|C(y,x)\rangle|yx\rangle + \left|c_{yx}^1 c_{yx}^4 c_{yx}^7 c_{yx}^6 c_{yx}^3 c_{yx}^0 c_{yx}^5 c_{yx}^2\right\rangle|YX\rangle. \end{aligned} \quad (31)$$

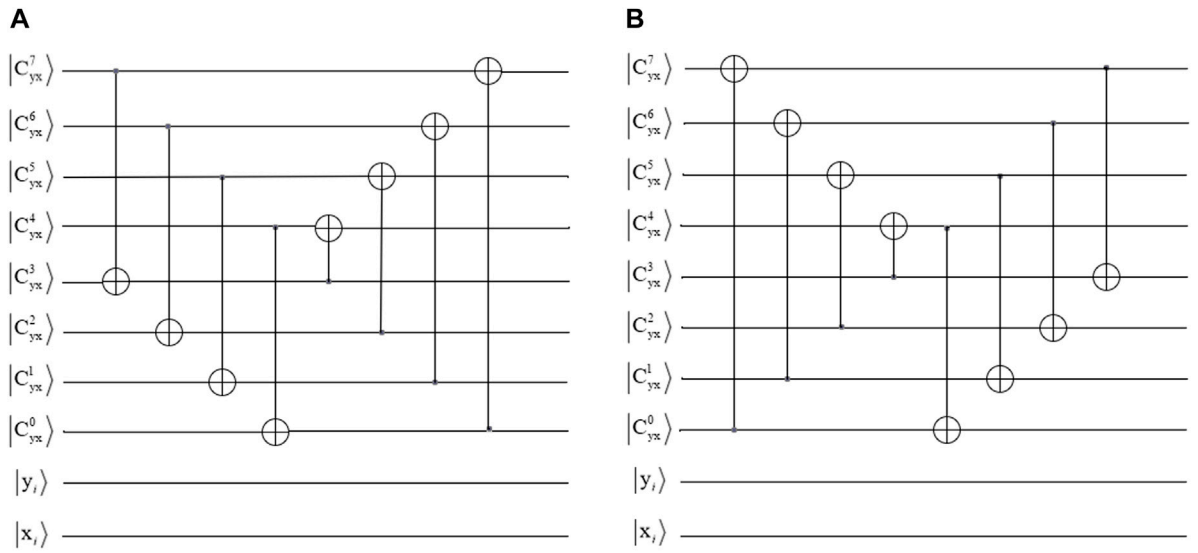

FIGURE 13
Circuits **(A)** Quantum Gray code, **(B)** Inverse quantum Gray code.

To complete bit-planes scrambling of all the pixels, a quantum operation S is defined,

$$\begin{aligned}|I_k\rangle &= S|I_b\rangle = \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^m-1}\varphi_{YX}|I_b\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\left|c^1_{yx}c^4_{yx}c^7_{yx}c^6_{yx}c^3_{yx}c^0_{yx}c^5_{yx}c^2_{yx}\right\rangle|YX\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^m-1}|C'(y,x)\rangle|yx\rangle.\end{aligned} \tag{32}$$

Step 6. : The inter bit-planes permutation is accomplished with quantum Gray code. By scrambling quantum image $|I_k\rangle$ with quantum Gray code, the scrambled quantum image $|I_s\rangle$ is obtained. The circuit of quantum Gray code is shown in Figure 13A.

Step 7. : The sequence $\{w_i'|i = 1, 2, \cdots, 2^n \times 2^m\}$ is given by

$$w_i' = w_i^* \bmod 3. \tag{33}$$

The scrambled quantum image $|I_s\rangle$ is chosen to perform diffusion operations among pixel values, binary bits and pixel bits according to the sequence $\{w_i'|i = 1, 2, \cdots, 2^n \times 2^m\}$.

Step 8. : If $w_i' = 0$, then the pixel values diffusion operation is performed.

$$\begin{cases} \text{aa} = \text{floor}\left(\frac{1}{2}\times 10^4 \sin\left(4\sin y^*(i)+1\right)\right)\bmod 256 \\ \text{bb} = \text{floor}\left(0.9\cos 3.9\pi z^*(i)\times\left(1-z^*(i)\right)\times 10^4\right)\bmod 256 \\ I_e(i) = \left(I_s(i)+\text{aa}\oplus\text{bb}\right)\bmod 256 \end{cases}. \tag{34}$$

If $w_i' = 1$, then the binary bits diffusion operation is performed.

$$I_e(i) = I_s(i)\oplus y^*(i)\oplus z^*(i). \tag{35}$$

If $w_i' = 2$, then the pixel bits diffusion operation is performed.

$$\begin{cases} a_1 = \text{floor}\left(\frac{y^*(i)}{100}\right) \\ b_1 = \text{floor}\left(\frac{y^*(i)-100a_1}{10}\right) \\ c_1 = \text{floor}\left(y^*(i)-100a_1-10b_1\right) \end{cases}, \tag{36}$$

$$\begin{cases} a_{11} = \left[a_1+\text{floor}\left(0.99\sin 0.99\times 10^4\pi a_1\right)\bmod 100\right]\bmod 10 \\ b_{11} = \left[b_1+\text{floor}\left(0.99\sin 0.99\times 10^4\pi b_1\right)\bmod 100\right]\bmod 10 \\ c_{11} = \left[c_1+\text{floor}\left(0.99\sin 0.99\times 10^4\pi c_1\right)\bmod 100\right]\bmod 10 \end{cases}, \tag{37}$$

$$\text{abc} = \left(100a_{11}+10b_{11}+c_{11}\right)\bmod 256, \tag{38}$$

$$I_e(i) = \left[\text{abc}+\text{floor}\left(0.99\sin 2\pi 10^4 z^*(i)\right)+I_s(i)\right]\bmod 256. \tag{39}$$

According to Eq. 36, the hundreds place a_1, tens place b_1, and one place c_1. They were then entered into Eq. 37 to obtain a_{11}, b_{11}, and c_{11}. They are then substituted in Eq. 38 and combined to

yield *abc*. Finally, the quantum ciphertext image $|I_e\rangle$ can be generated by substituting them into Eq. 39.

4.2 Quantum image decryption algorithm

The decryption process is the reverse process of the encryption process, the specific image decryption process is as follows.

Step 1: The encryption quantum image $|I_e\rangle$ performs three-level diffusion operations with the integer sequences $\{y_i^*|i = 1, 2, \ldots 2^n \times 2^m\}$ and $\{z_i^*|i = 1, 2, \ldots 2^n \times 2^m\}$, the scrambled quantum image $|I_s\rangle$ is retrieved.

Step 2. : The quantum image $|I_k\rangle$ is retrieved by the inverse quantum Gray code on the scrambled quantum image $|I_s\rangle$, the circuit of the inverse quantum Gray code is depicted in Figure 13B.

Step 3: The quantum image $|I_b\rangle$ is obtained by the inverse bit-planes exchange operation S^{-1} on the quantum image $|I_k\rangle$.

$$\begin{aligned}|I_b\rangle &= S^{-1}|I_k\rangle = \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^m-1}\varphi_{YX}^{-1}|I_k\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}G_{YX}^{-1}\left|c_{YX}^1c_{YX}^4c_{YX}^7c_{YX}^6c_{YX}^3c_{YX}^0c_{YX}^5c_{YX}^2\right\rangle \otimes |YX\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\left|c_{YX}^7c_{YX}^6c_{YX}^5c_{YX}^4c_{YX}^3c_{YX}^2c_{YX}^1c_{YX}^0\right\rangle \otimes |YX\rangle.\end{aligned} \tag{40}$$

Step 4: The plaintext image can be recovered by performing inverse Q_{dst} on the quantum image $|I_b\rangle$.

$$\begin{aligned}&|I\rangle = Q_{\mathrm{dst}}^{-1}|I_b\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{dst}^{-1}\left(\left|y'_{n-1}\ y'_{n-2}\cdots y'_{w_1}\ y_{w_1-1}\cdots y_0\right\rangle\left|x'_{m-1}\ x'_{m-2}\cdots x'_{w_1}\ x_{w_1}\cdots x_0\right\rangle\right) \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle Q_{dst}^{-1}\left|y'_{n-1}\ y'_{n-2}\cdots y'_{w_1}\right\rangle\left|y_{w_1-1}\cdots y_0\right\rangle Q_{dst}^{-1}\left|x'_{m-1}\ x'_{m-2}\cdots x'_{w_1}\right\rangle\left|x_{w_1-1}\cdots x_0\right\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle|y_{n-1}y_{n-2}\cdots y_0\rangle|x_{m-1}x_{m-2}\cdots x_0\rangle \\ &= \frac{1}{(\sqrt{2})^{n+m}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^m-1}\bigotimes_{j=0}^{q-1}|C_{YX}^j\rangle|YX\rangle.\end{aligned} \tag{41}$$

5 Numerical simulation and discussion

The numerical simulations are run on a MATLAB R2019b platform due to a lack of equipment. To test the effectiveness and reliability of the proposed quantum image encryption algorithm, the plaintext images in Figures 14A–C are image "Barbara" of size 580 × 720, image "Arnav" of size 248 × 300, and color image "Girls" of size 321 × 481 × 3 [33–35]. The block size w_1 has been set to four. The simulation parameters are as follows: $a = 1, c = 2, d = 1, \gamma = 1, \varpi = 1, \mu = 1, \tau = 1, e = 2, \xi = 3, \sigma = 2.7, h_1 = 0.01, N_1 = 5000, x(0) = 1, y(0) = 1.4, z(0) = 1$ and $w(0) = 1$. The relevant ciphertext images are shown in Figures 14D–F. Because all ciphertext images are encrypted and exhibit chaotic behavior, attacks will have an enormously difficult time extracting the original plaintext images. When decrypted with the correct keys, Figures 14G–I show the corresponding decrypted images. There is no discernible difference between the original plaintext image and the decrypted image, indicating that the proposed fast quantum image encryption scheme based on a multilayer short memory fractional order Lotka-Volterra system and a dual-scale triangular map is effective.

The proposed algorithm was evaluated using three types of statistical property analyses, comprising histogram, correlation of adjacent pixels, and information entropy. The histogram assures that plaintext images and ciphertext images are different from each other. The association between two neighboring pixels was shown by the correlation of adjacent pixels. The information entropy looks at the encryption effect of the ciphertext images. In order to verify the proposed algorithm's resistance to various attacks, differential attack analysis, noise attack analysis, and shear attack analysis were also carried out. To show the space and sensitivity of the keys, key space analysis and key sensitivity analysis are then done. The proposed algorithm's computational complexity was then described. Last but not least, tests and comparisons of the encryption and decryption times in seconds were performed. All of the preceding analyses will guarantee that proposed algorithms would both be technically proficient and efficient.

5.1 Statistical property analysis

5.1.1 Histogram

The histograms of the color images "Girls," "Sailboat," and "Goldhill" are shown in Figures 15A–C, and the histograms of the corresponding ciphertext images are shown in Figures 15D–F. It is demonstrated that the histograms of ciphertext images differ noticeably from those of plaintext images. The pixel values of ciphertext images are evenly distributed and completely different from those of plaintext images. It demonstrates that the proposed quantum image encryption scheme can withstand the histogram attack.

Furthermore, the chi-square test is used to precisely measure the difference between the ciphertext image and the plaintext image.

$$\chi^2 = \sum_{L=0}^{255}\frac{(o_L - e_L)^2}{e_L}, \tag{42}$$

where o_L is the observed number of the L-th gray level and e_L is the expected number of the L-th gray level. Table 2 displays the results of the chi-square test on ciphertext and plaintext images. Table 2 shows that the chi-square values of ciphertext images are

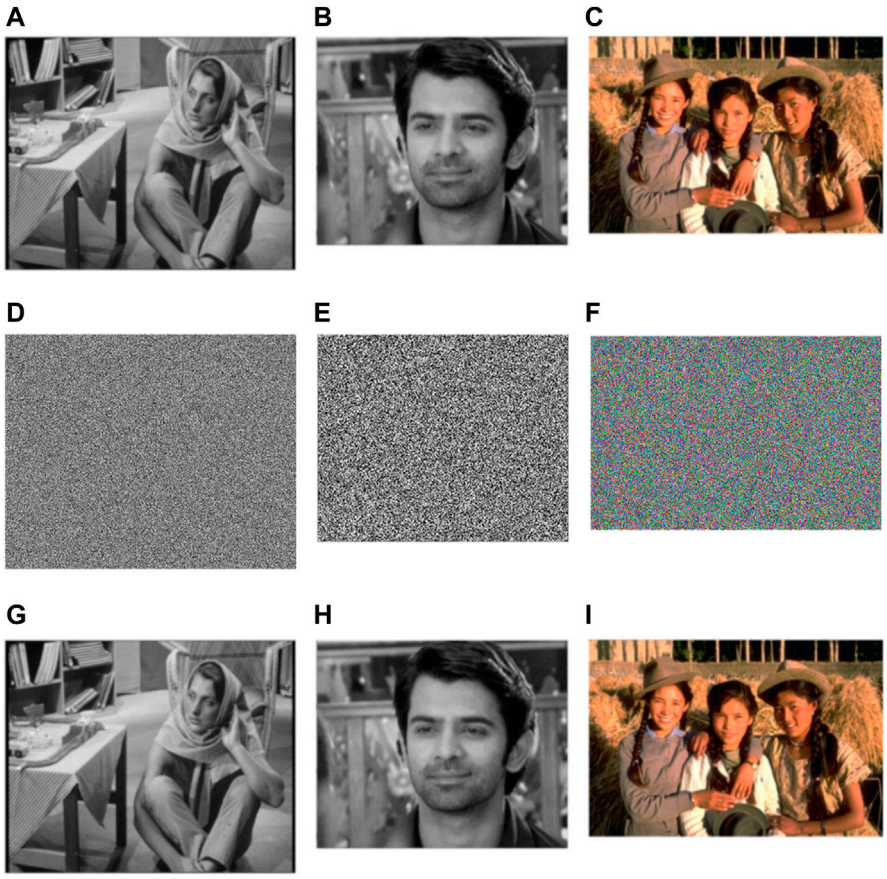

FIGURE 14
Plaintext images, ciphertext images and decryption images: **(A)** "Barbara," **(B)** "Arnav," **(C)** "Girls," **(D)** "Barbara," **(E)** "Arnav," **(F)** "Girls," **(G)** "Barbara," **(H)** "Arnav," **(I)** "Girls." ("Barbara" is from the University of Southern California's signal and image process institute image dataset, "Arnav" is from the IMDB-WIKI 500k dataset, "Girls" is from the Berkeley segmentation dataset (BSD) 500 dataset.).

less than 5% of the significance level, demonstrating that the proposed encryption scheme can withstand the histogram attack.

5.1.2 Correlation of adjacent pixels

Assume that N pairs of adjacent pixels need to be randomly selected from the image to be investigated, and the gray values are recorded as (x, y), the correlation coefficient between two vectors is defined as

$$C_{XY} = \frac{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)}{\sqrt{\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N}x_i\right)^2\sum_{i=1}^{N}\left(y_i - \frac{1}{N}\sum_{i=1}^{N}y_i\right)^2}}. \tag{43}$$

The correlation distribution of plaintext image "Girls" and ciphertext image "Girls" in horizontal, vertical and diagonal directions are depicted in Figure 16. The correlation coefficients of plaintext images and ciphertext images are edited in Table 3. As can be seen from Figure 16 and Table 3, the correlations between the adjacent pixels of plaintext images are extremely strong, while the correlations between the adjacent pixels of ciphertext images are close to 0, which are almost no correlations. Compared with [10, 24], the proposed image encryption scheme has stronger capacity to resist the correlation analysis attack.

5.1.3 Information entropy

The information entropy $H(x)$ calculation formula is written as

$$H(x) = -\sum_{i=0}^{255} p(x_i)\log_2 p(x_i), \tag{44}$$

where $p(x_i)$ represents the probability of the gray value i. The theoretical value of information entropy for a gray-scale random image with level 256 is 8 bits. The information entropy of

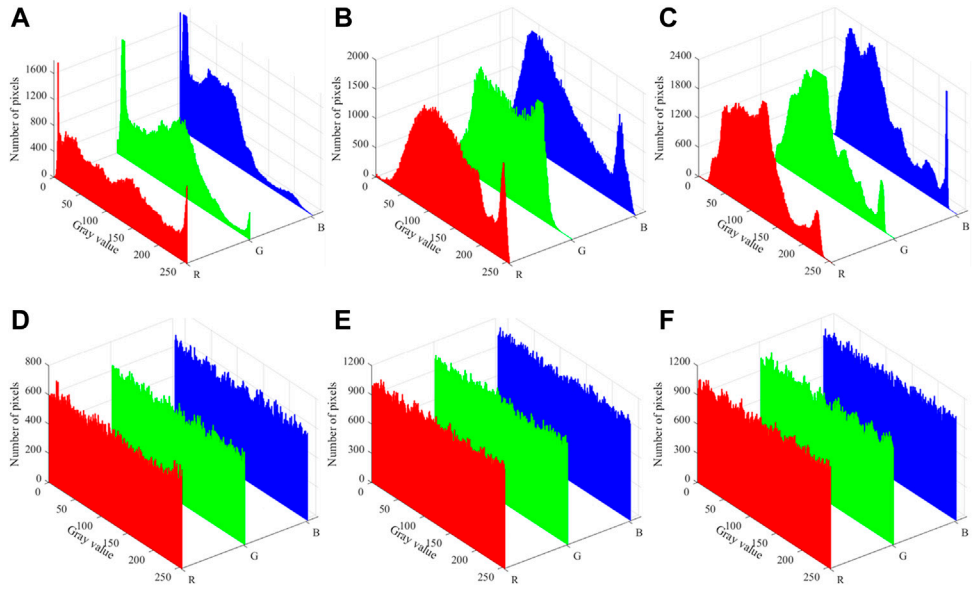

FIGURE 15
Histograms of plaintext images and ciphertext images: **(A)** "Girls," **(B)** "Sailboat," **(C)** "Goldhill," **(D)** "Girls," **(E)** "Sailboat," **(F)** "Goldhill."

TABLE 2 Chi-square test.

Image		Plaintext image	Ciphertext image
Barbara		1.6314e+05	235.6696
Arnav		4.0976e+04	278.3243
Bridge		1.5584e+05	265.5647
Lake		1.5144e+05	259.4658
Baboon		1.4652e+04	265.2458
	R channel	1.4164e+05	236.4007
Girls	G channel	1.1872e+05	206.2859
	B channel	1.6640e+05	234.2054
	R channel	1.6543e+05	256.5642
Sailboat	G channel	1.2564e+05	286.2656
	B channel	1.3654e+05	266.6462
	R channel	1.5621e+05	269.5354
Goldhill	G channel	1.4365e+05	275.3564
	B channel	1.6543e+05	265.3564
Critical value (5%)		293.2478	293.2478

plaintext images and ciphertext images is listed in Table 4. It is demonstrated that the information entropy of each ciphertext image approaches the theoretical value, whereas the information entropy of each plaintext image deviates significantly from the theoretical value, and the image encryption effect outperforms [10, 24].

5.2 Differential attack analysis

To quantitatively measure the difference between two images of the same size, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) can be performed.

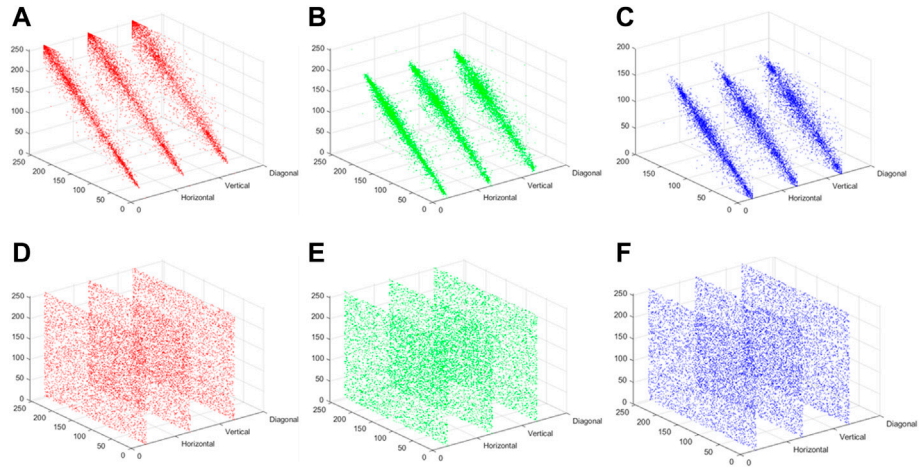

FIGURE 16
Correlation distribution of two adjacent horizontal, vertical and diagonal pixels of "Girls": **(A)** R channel, **(B)** G channel, **(C)** B channel; Correlation distribution of two adjacent horizontal, vertical and diagonal pixels of encryption "Girls": **(D)** R channel, **(E)** G channel, **(F)** B channel.

$$\begin{cases} \text{NPCR} = \sum_{j=1}^{N}\sum_{i=1}^{M}\frac{D(i,j)}{M\times N}\times 100\% \\ \text{UACI} = \sum_{j=1}^{N}\sum_{i=1}^{M}\frac{\left|c_1(i,j)-c_2(i,j)\right|}{M\times N\times 255}\times 100\% \end{cases}. \tag{45}$$

Besides NPCR and UACI, Block Average Changing Intensity (BACI) can also measure the difference between two random images.

$$\text{BACI} = \frac{1}{(M-1)(N-1)}\sum_{i=1}^{(M-1)(N-1)}\frac{m_i}{255}. \tag{46}$$

If the NPCR of the two images is 100%, and the UACI is close to the theoretical value, but the visual effects of the two images are similar, it indicates that NPCR and UACI are still insufficient in describing the differences between the two images, and BACI makes up for this deficiency. The theoretical value of BACI is 26.7712%. From Table 5, NPCR, UACI and BACI are all close to the theoretical values. Therefore, the proposed encryption scheme is very sensitive to any small changes of the pixel of plaintext image.

5.3 Key space analysis

The key space of the image cryptosystem should be large enough to resist brute force attack effectively. The key space should be at least 2^{128}. In the proposed scheme, the key space contains the parameters of quantum dual-scale triangular map, the initial values of the MSMFrLVS and the hash value of plaintext image. The key space of quantum dual-scale triangular map is estimated to be 10^8. The precision of the initial values of the MSMFrLVS is 10^{15}, the total key space is $10^8 + 10^{15\times4} + 2^{256}$. Therefore, the key space of the proposed algorithm is large enough to resist the brute-force attack.

5.4 Key sensitivity analysis

A good image encryption system should have strong key sensitivity. To be more precise, the key sensitivity of the system is evaluated by the mean-squared error (MSE).

$$\text{MSE} = \frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left[D(x,y)-I(x,y)\right]^2, \tag{47}$$

where $M\times N$ denotes the image size, $D(x,y)$ and $I(x,y)$ represents the pixel values of decryption image and plaintext image at the position (x,y), respectively. Figures 17B–E show the MSE curves with wrong keys x_0+10^{-14}, y_0+10^{-14}, z_0+10^{-14} and w_0+10^{-14}, respectively. As can be seen from Figure 17, the ciphertext images obtained under the condition of minor changes of the keys are quite different. Since the keys are randomly selected from the key space, it can be explained that each key in the key space is valid and sensitive.

5.5 Shear attack analysis

In addition to the noise attack, the ciphertext image is also susceptible to malicious cutting by the attacker during the process of transmission and processing, therefore it is necessary to analyze the anti-clipping ability of the proposed algorithm. Figure 18 shows the ciphertext images of different

TABLE 3 Correlation coefficients of adjacent pixels.

Correlation coefficient		Horizontal	Vertical	Diagonal
Plaintext Barbara		0.9803	0.9806	0.9591
Ciphertext Barbara		0.0079	−0.0087	−0.0035
Plaintext Arnav		0.9844	0.9837	0.9730
Ciphertext Arnav		0.0097	0.0100	−0.0138
Plaintext Baboon		0.9763	0.9356	0.9435
Ciphertext Baboon		0.0053	0.0059	0.0043
Plaintext Bridge		0.9786	0.9442	0.9624
Ciphertext Bridge		0.0023	0.0045	0.0026
	R channel	0.9678	0.9494	0.9304
Plaintext Girls	G channel	0.9456	0.9247	0.8827
	B channel	0.9162	0.8944	0.8352
	R channel	−0.0093	−0.0303	−0.0049
Ciphertext Girls	G channel	−0.0177	−0.0203	0.0057
	B channel	−0.0155	0.0052	−0.0117
Plaintext Sailboat	R channel	0.9356	0.9869	0.9364
	G channel	0.9468	0.9576	0.9567
	B channel	0.9256	0.9564	0.8967
	R channel	−0.0053	0.0134	0.0036
Ciphertext Sailboat	G channel	0.0054	−0.0023	0.0054
	B channel	−0.0034	0.0098	−0.0068
Reference [10]		−0.0423	0.0202	−0.0212
Reference [24]		0.0295	0.0187	0.0393

TABLE 4 Information entropy.

Images		Plaintext image (bit)	Ciphertext image (bit)
Barbara		7.6578	7.9996
Arnav		7.4914	7.9973
Baboon		7.4465	7.9985
Bridge		7.2645	7.9976
Lake		7.6548	7.9992
	R channel	7.7771	7.9975
Girls	G channel	7.5523	7.9981
	B channel	7.2687	7.9975
	R channel	7.6782	7.9968
Sailboat	G channel	7.6485	7.9978
	B channel	7.4356	7.9986
	R channel	7.6897	7.9991
Goldhill	G channel	7.8562	7.9981
	B channel	7.7568	7.9985
Reference [10]		7.1273	7.9970
Reference [24]		7.0097	7.9970

clipping regions and their corresponding decryption images. From Figure 18, the resolution of decryption images varies with the cutting degree of ciphertext images, but the crucial information of the decryption images can still be identified. Therefore, the proposed encryption algorithm has a certain ability to resist the shear attack.

TABLE 5 NPCR, UACI and BACI.

Image		NPCR%	UACI%	BACI%
Barbara		99.6090	33.4476	26.7930
Arnav		99.5820	33.3371	26.6211
Baboon		99.6032	33.4562	26.7568
Bridge		99.5962	33.3685	26.6238
Lake		99.5658	33.3456	26.8664
	R channel	99.6237	33.4665	26.8179
Girls	G channel	99.6538	33.3546	26.7534
	B channel	99.5456	33.1562	26.6481
	R channel	99.6023	33.4356	26.5562
Sailboat	G channel	99.6548	33.3346	26.7652
	B channel	99.5964	33.3450	26.6724
	R channel	99.6432	33.3315	26.6482
Goldhill	G channel	99.6023	33.3725	26.7315
	B channel	99.6130	33.4456	26.6856

5.6 Computational complexity

Assume that I is an $M \times N$ image, and N is greater than M. The computational complexity of the proposed quantum image encryption algorithm primarily depends on quantum dual-scale triangular map, the intra bit-planes permutation and quantum XOR operation. In the block-level permutation stage, the basic gates of ADDER-MOD2^n are $28n - 12$ and the complexity of the ADDER-MOD2^n is about $140n$ [1]. Hence, the computational complexity of quantum dual-scale triangular map is $O(n)$. In addition, the intra bit-planes permutation involves four quantum swap gates, and each swap gate is achieved by three C-NOT gates, thus the intra bit-planes permutation is realized by $12n$ basic gates, the computational complexity of the intra bit-planes permutation is $O(n)$. What's more, the quantum XOR operation needs $8n - 16$ Toffoli gates [36], and each Toffoli gate is composed of six C-NOT gates, thus the quantum XOR operation involves $384n - 768$ basic gates, and the computational complexity of the quantum XOR operation is $O(n)$. Consequently, the computational complexity of the proposed quantum algorithm is $O(n)$, while the computational complexity of the corresponding classical image encryption scheme is $O(2^{2n})$. Obviously, the proposed quantum image encryption algorithm is better than its classical counterparts in terms of computational complexity.

5.7 Noise attack analysis

Assume that the ciphertext image "Arnav" is added with the Gaussian noise.

$$C' = C + kG, \tag{48}$$

where C' and C are the noisy ciphertext images and the noise-free ciphertext images, k represents noise intensity, G is the Gaussian noise with zero mean and unit standard deviation. Figure 19A shows

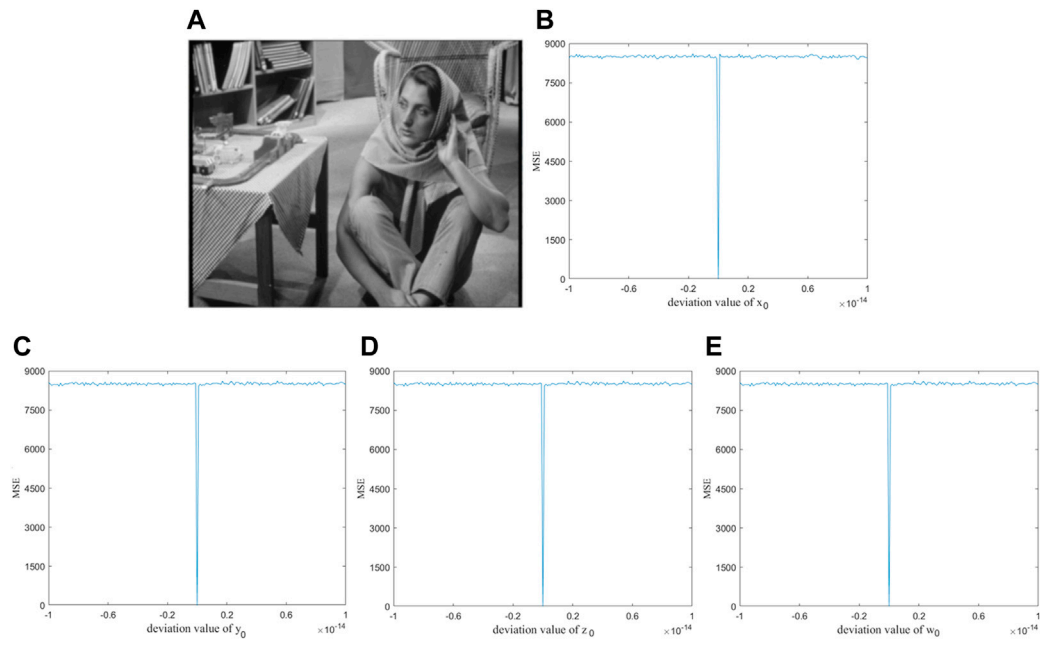

FIGURE 17
(A) Plaintext image, MSE curves: **(B)** x_0, **(C)** y_0, **(D)** z_0, **(E)** w_0.

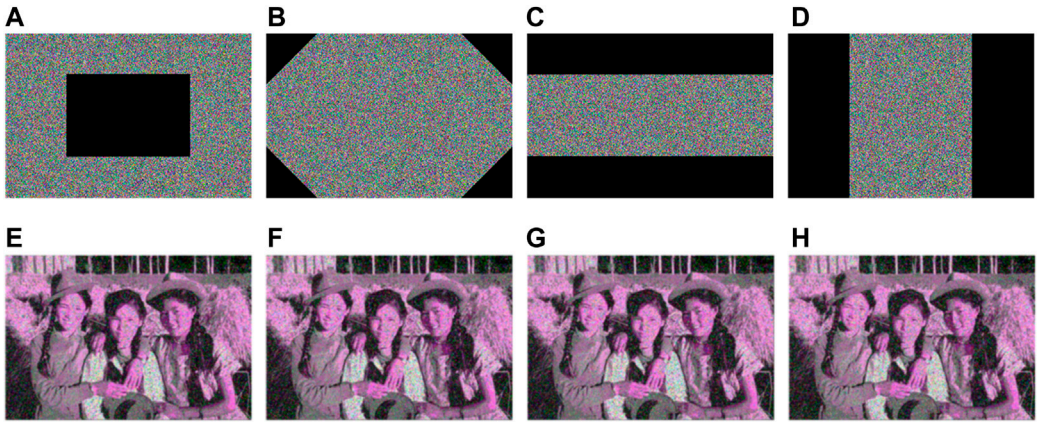

FIGURE 18
Sheared images in different position: **(A–D)**, the corresponding decryption images: **(E–H)**.

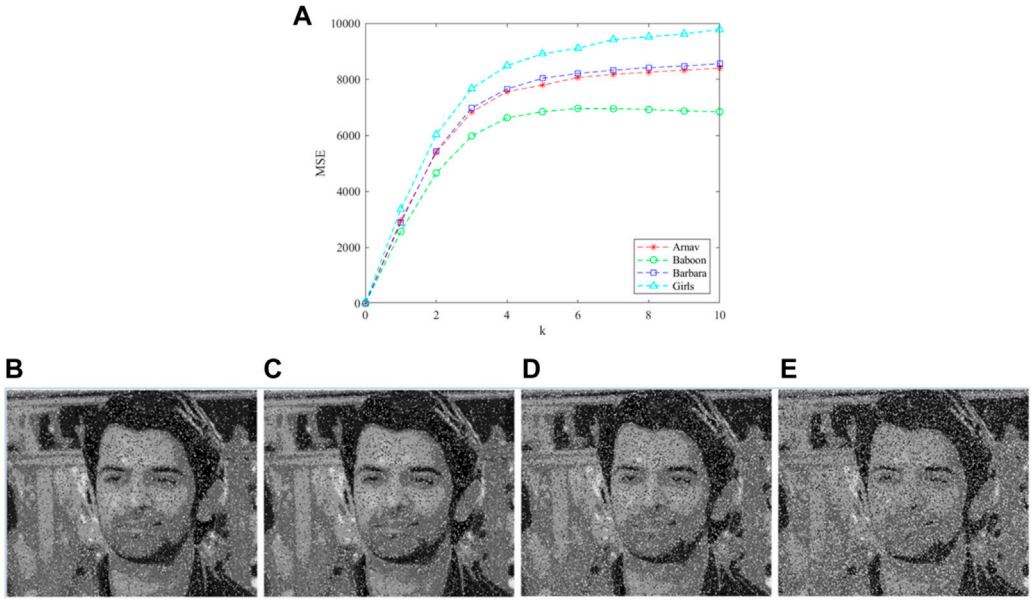

FIGURE 19
Results of noise attack: **(A)** MSE curve, noise intensities: **(B)** $k = 2$, **(C)** $k = 4$, **(D)** $k = 6$, **(E)** $k = 8$.

the MSE curves with different noise intensities, Figures 19B–E give the decryption images with noise intensities 2, 4, 6 and 8. From Figure 19, with the increase of noise intensity, decryption images become more and more blurred, but the outline of decryption images can still be seen clearly, the proposed image encryption scheme can resist the noise attack to some degree.

5.8 Encryption time analysis

The length of the execution time is an index to evaluate the quality of an encryption algorithm. The execution time of the proposed algorithm and Refs. [9, 12, 16, 17] are listed in Table 6. In [9, 16, 17], the pseudo-random sequences are originated by iterating the 4D hyper-chaotic Henon map, 2D logistic map and 3D chaotic system, respectively, which take too much time. In [12], the encryption process is time-consuming owing to the

TABLE 6 Encryption and decryption time in second.

Time(s)	Proposed scheme	[9]	[12]	[16]	[17]
Encryption time	0.9235	1.2540	1.2230	1.9450	1.9123
Decryption time	0.9582	2.3540	1.1958	2.2895	2.0012

fractional-order Lorenz-like chaotic system. In our algorithm, the initial point of the MSMFrLVS is variable such that the algorithm can save the encryption time greatly, thus the proposed image encryption algorithm can be developed for fast image encryption.

6 Conclusion

The quantum image encryption scheme is proposed by combining the MSMFrLVS with the quantum dual-scale triangular map. The block-level permutation, intra and inter bit-plane permutations, and three-level diffusion operations are used to implement the encryption process. The independent parameters of quantum dual-scale triangular map, the initial values and the control parameters of the MSMFrLVS and the hash value of plaintext image consist of the keys of the proposed quantum image encryption algorithm. As a result, the encryption system's key space is sufficiently large. Numerical simulation analyses demonstrate the proposed algorithm's reliability and effectiveness, and it requires less computation time. Furthermore, the proposed image encryption algorithm has lower computational complexity than its conventional counterparts. In the future, we will focus on combining quantum image encryption with semi-quantum cryptography protocols [37] in order to propose an algorithm with improved security and quantum communication capacity.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

YM: Conceptualization, methodology, investigation; F-FY: Formal analysis, writing—original draft; L-HG: Validation, writing- reviewing and editing; W-PZ: Conceptualization, funding acquisition, resources, supervision, writing—review and editing.

Funding

This work is supported by the National Natural Science Foundation of China (Grant No. 61861029), the Top Double 1000 Talent Programme of Jiangxi Province (Grant No. JXSQ2019201055).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Zhou NR, Hua TX, Gong LH, Pei DJ, Liao QH. Quantum image encryption based on generalized Arnold transform and double random-phase encoding. *Quan Inf Process* (2015) 14(4):1193–213. doi:10.1007/s11128-015-0926-z

2. Malik A, Dhall S, Gupta S. An improved bit plane image encryption technique using RC4 and quantum chaotic demeanour. *Multimed Tools Appl* (2020) 80(5): 7911–37. doi:10.1007/s11042-020-09973-5

3. Zhu HH, Chen XB, Yang YX. A multimode quantum image representation and its encryption scheme. *Quan Inf Process* (2021) 20(9):315. doi:10.1007/s11128-021-03255-1

4. Zhang JL, Huang ZJ, Li X, Wu MQ, Wang XY, Dong YM. Quantum image encryption based on quantum image decomposition. *Int J Theor Phys (Dordr)* (2021) 60(8):2930–42. doi:10.1007/s10773-021-04862-5

5. Wang L, Ran QW, Ma J. Double quantum color images encryption scheme based on DQRCI. *Multimed Tools Appl* (2020) 79(9-10):6661–87. doi:10.1007/s11042-019-08514-z

6. Vagish KD, Rajakumaran C, Kavitha R. Chaos based encryption of quantum images. *Multimed Tools Appl* (2020) 79(33-34):23849–60. doi:10.1007/s11042-020-09043-w

7. Zhou NR, Huang LX, Gong LH, Zeng QW. Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map. *Quan Inf Process* (2020) 19(9):284. doi:10.1007/s11128-020-02794-3

8. Wang Y, Chen LQ, Yu KL, Gao Y, Ma Y. An image encryption scheme based on logistic quantum chaos. *Entropy* (2022) 24(2):251. doi:10.3390/e24020251

9. Dai JY, Ma Y, Zhou NR. Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henon map. *Quan Inf Process* (2021) 20(7):246. doi:10.1007/s11128-021-03187-w

10. Zhou NR, Chen WW, Yan XY, Wang YQ. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quan Inf Process* (2018) 17(6):137. doi:10.1007/s11128-018-1902-1

11. Ye GD, Jiao KX, Huang XL, Goi BM, Yap WS. An image encryption scheme based on public key cryptosystem and quantum logistic map. *Sci Rep* (2020) 10(1): 21044. doi:10.1038/s41598-020-78127-2

12. Khan M, Rasheed A. A fast quantum image encryption algorithm based on affine transform and fractional-order Lorenz-like chaotic dynamical system. *Quan Inf Process* (2022) 21(4):134. doi:10.1007/s11128-022-03474-0

13. Signing VRF, Tegue GAG, Kountchou M, Njitacke ZT, Tsafack N, Nkapkop JDD, et al. A cryptosystem based on a chameleon chaotic system and dynamic DNA coding. *Chaos Solitons Fractals* (2022) 155:111777. doi:10.1016/j.chaos.2021.111777

14. Wang XY, Su YN, Luo C, Nian FZ, Teng L. Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. *Multimed Tools Appl* (2022) 81(10):13845–65. doi:10.1007/s11042-022-12220-8

15. Li CM, Yang XZ. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. *Optik* (2022) 260:169042. doi:10.1016/j.ijleo.2022.169042

16. Wu WQ, Wang Q. Quantum image encryption based on Baker map and 2D logistic map. *Int J Theor Phys (Dordr)* (2022) 61(3):64. doi:10.1007/s10773-022-04979-1

17. Hu WB, Dong YM. Quantum color image encryption based on a novel 3D chaotic system. *J Appl Phys* (2022) 131(11):114402. doi:10.1063/5.0084611

18. Kamran MI, Khan MA, Alsuhibany SA, Ghadi YY, Arshad AJ, Ahmad J, et al. A highly secured image encryption scheme using quantum walk and chaos. *Comput Mater Contin* (2022) 73(1):657–72. doi:10.32604/cmc.2022.028876

19. Alhumyani H, El-Banby GM, El-Sayed HS, El-Samie F, Faragallah OS. Efficient generation of cancelable face templates based on quantum image Hilbert permutation. *Electronics* (2022) 11(7):1040. doi:10.3390/electronics11071040

20. Zhong HY, Li GD. Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. *Multimed Tools Appl* (2022) 81:24757–76. doi:10.1007/s11042-022-12479-x

21. Chen C, Zhang HY, Wu B. Image encryption based on arnod transform and fractional chaotic. *Symmetry (Basel)* (2022) 14(1):174. doi:10.3390/sym14010174

22. Hu WW, Zhou RG, Luo J, Jiang SX, Luo GF. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quan Inf Process* (2020) 19(3):82. doi:10.1007/s11128-020-2579-9

23. Liu H, Zhao B, Huang L. Quantum image encryption scheme using Arnold transform and S-box scrambling. *Entropy* (2019) 21(4):343. doi:10.3390/e21040343

24. Liu XB, Xiao D, Huang W, Liu C. Quantum block image encryption based on Arnold transform and sine chaotification model. *IEEE Access* (2019) 7:57188–99. doi:10.1109/ACCESS.2019.2914184

25. Zhou NR, Yan XY, Liang HR, Tao XY, Li GY. Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. *Quan Inf Process* (2018) 17(12):338. doi:10.1007/s11128-018-2104-6

26. Zhou RG, Liu X, Luo J. Quantum circuit realization of the bilinear interpolation method for GQIR. *Int J Theor Phys (Dordr)* (2017) 56(9):2966–80. doi:10.1007/s10773-017-3463-y

27. Li Y, Chen YQ, Podlubny I. Stability of fractional-order nonlinear dynamic systems: Lyapunov direct method and generalized Mittag-Leffler stability. *Comput Math Appl* (2010) 59(5):1810–21. doi:10.1016/j.camwa.2009.08.019

28. Wu GC, Deng ZG, Baleanu D, Zeng DQ. New variable-order fractional chaotic systems for fast image encryption. *Chaos* (2019) 29(8):083103. doi:10.1063/1.5096645

29. Agrawal SK, Srivastava M, Das S. Synchronization between fractional-order ravinovich-fabrikant and lotka-volterra systems. *Nonlinear Dyn* (2012) 69(4):2277–88. doi:10.1007/s11071-012-0426-y

30. El-Latif AAA, Abd-El-Atty B, Talha M. Robust encryption of quantum medical images. *IEEE Access* (2018) 6:1073–81. doi:10.1109/ACCESS.2017.2777869

31. Li PS, Zheng Q, Hong JG, Xing CH. 2D triangular mappings and their applications in scrambling rectangle image. *Inf Tech J* (2008) 7(1):40–7. doi:10.3923/itj.2008.40.47

32. Jiang N, Wang L. Analysis and improvement of the quantum Arnold image scrambling. *Quan Inf Process* (2014) 13(7):1545–51. doi:10.1007/s11128-014-0749-3

33. University of Southern California. Signal and Image Processing Institute. USC-SIPI Image Database (1997) Available at: http://sipi.usc.edu/database (Online Accessed March 15, 2021).

34. Rothe R, Timofte R, Gool LV. Deep expectation of real and apparent age from a single image without facial landmarks. *Int J Comput Vis* (2018) 126(2):144–57. doi:10.1007/s11263-016-0940-3

35. Arbelaez P, Maire M, Fowlkes C, Malik J. Contour detection and hierarchical image segmentation. *IEEE Trans Pattern Anal Mach Intell* (2011) 33(5):898–916. doi:10.1109/TPAMI.2010161

36. Ralph TC, Resch KJ, Gilchrist A. Efficient Toffoli gates using qudits. *Phys Rev A (Coll Park)* (2007) 75(2):022313. doi:10.1103/PhysRevA.75.022313

37. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. *Quan Inf Process* (2021) 21(4):123. doi:10.1007/s11128-022-03457-1