Computer Science and Application 计算机科学与应用, 2026, 16(5), 376-391
Published Online May 2026 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2026.165191

Hans汉斯

抗差分攻击的明文关联量子图像双重加密算法

张　俊，李祯祯*，高　博，李子臣

北京印刷学院信息工程学院，北京

收稿日期：2026年4月23日；录用日期：2026年5月22日；发布日期：2026年5月29日

摘　要

近年来随着互联网的迅速发展，数字图像泄密事件频发，传统图像加密技术已经难以满足当前的安全需求，亟待升级优化。针对现有量子图像加密算法中扩散机制单一(如仅采用量子异或操作)、难以抵御差分攻击和选择明文攻击等安全缺陷，文章提出一种抗差分攻击的明文关联量子图像双重加密方案。首先，利用NEQR模型将经典图像制备为量子叠加态，并提取明文特征值作为扰动因子动态更新混沌系统的初始条件。其次，借助Logistic混沌映射驱动量子C-SWAP逻辑门构建全局量子坐标受控置换网络，彻底破坏像素间的空间拓扑相关性；最后，创新性地引入Lorenz混沌系统控制量子DNA动态逻辑门对加密图像颜色量子比特进行深度的非线性替代。经仿真与性能分析表明，该算法时间复杂度仅为O (n)，NPCR (99.6%)、UACI (33.4%)与信息熵均逼近理论极值。该方案不仅密钥空间庞大、能有效抵御各类统计攻击，还在遭受噪声干扰与数据缺失时展现卓越的鲁棒性，表明了该方案具有较高的安全性。

关键词

量子图像表示，量子图像处理，量子动态逻辑门运算

Quantum Image Dual Encryption Algorithm Resistant to Differential Attack with Plaintext Correlation

Jun Zhang, Zhenzhen Li*, Bo Gao, Zichen Li

School of Information Engineering, Beijing Institute of Graphic Communication, Beijing

Received: April 23, 2026; accepted: May 22, 2026; published: May 29, 2026

Abstract

In recent years, with the rapid development of the Internet, digital image leakage incidents have

*通讯作者。

文章引用: 张俊, 李祯祯, 高博, 李子臣. 抗差分攻击的明文关联量子图像双重加密算法[J]. 计算机科学与应用, 2026, 16(5): 376-391. DOI: 10.12677/csa.2026.165191

occurred frequently. Traditional image encryption technologies are no longer sufficient to meet current security needs and urgently require upgrading and optimization. Aiming at the security defects of existing quantum image encryption algorithms, such as a single diffusion mechanism (e.g., only adopting quantum XOR operation), difficulty in resisting differential attacks, and chosen-plaintext attacks, this paper proposes a dual quantum image encryption scheme with plaintext correlation that is resistant to differential attacks. Firstly, this paper uses the NEQR model to prepare classical images into quantum superposition states and extracts plaintext eigenvalues as disturbance factors to dynamically update the initial conditions of the chaotic system. Secondly, the Logistic chaotic map is used to drive the quantum C-SWAP logic gate to construct a global quantum coordinate-controlled permutation network, which completely destroys the spatial topological correlation between pixels. Finally, the Lorenz chaotic system is innovatively introduced to control the quantum DNA dynamic logic gate for in-depth nonlinear substitution of the color qubits of the encrypted image. Simulation and performance analysis show that the time complexity of the algorithm is only O (n), and the NPCR (99.6%), UACI (33.4%), and information entropy are all close to the theoretical extreme values. This scheme not only has a large key space and can effectively resist various statistical attacks, but also shows excellent robustness when subjected to noise interference and data loss, which indicates that the scheme has high security.

Keywords

Quantum Image Representation, Quantum Image Processing, Quantum Dynamic Logic Gate Operation

1. 引言

随着网络通信与信息技术的飞速发展，图像作为多媒体信息的重要载体，在现代互联网中扮演着不可或缺的角色。然而，图像获取途径的多样化及其固有的可编辑性导致其面临被篡改、伪造、数据泄露及损坏等严重的安全隐患。特别是在量子计算等新兴技术迅速崛起的背景下，保障数字图像在传输过程中的完整性、真实性与安全性已成为一项迫在眉睫的挑战。

Zhou 等人在 2012 年提出了基于量子图像几何变换的图像加密与解密算法[1]。该工作将经典图像几何变换思想与专用量子电路设计相结合，完成了量子图像的几何变换，是量子图像密码学领域的早期重要探索。2014 年，Yang 等人提出了基于量子傅里叶变换(QFT)和双相(随机相)编码的新型图像加密解密技术[2]，首次将双随机相位编码机制推广到量子场景，大幅提升了图像加密方案的安全性。同年，Wang 等人提出基于受限几何和颜色变换的量子图像加密方案[3]，且在不久后再次提出一种基于图像相关分解的量子图像加密算法[4]，通过图像相关性分解有效抵抗针对加密图像的蛮力攻击。2015 年，王等人提出关于 LSB (最低有效位)的量子图像隐写术算法[5]，推动了量子图像信息隐藏与隐写技术的发展。

混沌系统凭借其特有优势为图像加密提供了强大的新思路：该系统展现出高复杂度且不可预测的特性，对初始条件具有极强的依赖性和指数级的敏感性，在生成高强度加密密钥、置乱图像像素顺序以及扰动像素值等方面表现极为出色。将混沌理论与图像加密技术相结合，通过对图像数据进行深度的混淆和保护，有效突破了传统算法的安全瓶颈，这已成为近年来学术界提升图像数据安全性的重要研究趋势[6]。2018 年，Zhang 等人就提出了一种基于量子混沌映射和 DNA 编码的图像加密算法[7]，利用混沌系统生成高度随机

的序列，从而动态地进行异或(XOR)运算，这种动态可变的编码策略大幅提升了算法的可靠性和安全性。次年，Wang 等人提出了一种基于量子密钥图像的量子图像加密算法[8]；此外，Liu 等人在同年提出了一种基于量子 Arnold 变换(QAT)和量子比特随机旋转的双量子图像加密方案[9]，使用 QAT 来置乱图像的像素位置，并分别在空间域和频率域执行独立的量子比特随机旋转，最终实现对双图像的高效混淆和扩散。2020 年，Zhou 发表了一种关于 DNACNot (DNA 受控非门)的量子图像加密方法，其利用改进的 Chaos Game Representation 对扩增后的两条 DNA 序列进行修改，进而将 ICMIC 混沌映射生成的序列转换为 DNACNot [10]，极大提高了图像传输的安全性。2020 年，Deepak Vagish 等人开发出一种基于混沌映射的量子图像加密算法[11]，该方法利用量子 Hilbert 图像置乱算法(Quantum Hilbert Image Scrambling)使用量子电路将图像转换成置乱态。2022 年，Wang 等人提出基于超混沌系统与改进量子旋转门的彩色图像加密方案。该方案融合四翼超混沌系统和分段复合混沌映射[12]达到密钥空间扩大、抗攻击能力增强和计算复杂度降低。

随着科技的不断进步，许多加密方案被陆续提出。在这些学术背景的基础上，探索如何改进更加安全且置乱效果更好的加密方案具有重要意义。本文提出了一种抗差分攻击的明文关联量子图像双重加密方案。该方案基于 Logistic 混沌映射驱动量子 C-SWAP 门，构建全局量子坐标受控置换网络，再使用 Lorenz 混沌系统控制量子 DNA 动态逻辑门运算，对图像颜色和像素空间进行深度混淆，极大拓展了算法的密钥空间并且有效提升了加密的抗差分攻击能力。

2. 理论基础

2.1. 量子图像表示模型(NEQR)

量子图像表示模型(Novel Enhanced Quantum Representation, NEQR)是面向灰度数字图像的主流量子表示模型，其核心设计思路是利用量子叠加态编码图像位置信息、量子比特序列正交基态编码像素灰度信息[13]，并通过量子纠缠实现位置与灰度信息的强绑定，从而构建出可并行处理、精确测量、完整还原的量子图像编码方式，为量子图像分割、插值、置乱、加密等各类操作提供统一底层支撑。NEQR 从物理机制上解决了概率幅编码难以精确还原、无法支持复杂逻辑操作、压缩性能受限等问题，成为当前最具实用性的量子图像方案[14]。

设经典灰度图像尺寸为 $2n \times 2n$，灰度取值范围为$\left[0, 2^q - 1\right]$，则该图像对应的 NEQR 量子态可表示为式(2-1)：

$$\left|I\right\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|f\left(y,x\right)\right\rangle \otimes \left|yx\right\rangle \tag{2-1}$$

$\left|I\right\rangle$ 为量子图像最终表达形式，$1/2^n$ 为归一化系数以满足量子态概率归一性，y 和 x 分别为像素的行坐标与列坐标，$\left|yx\right\rangle$ 为像素位置量子态，$\left|f\left(y,x\right)\right\rangle$ 为像素颜色量子态。位置量子态由行坐标量子态与列坐标量子态张量积构成，如式(2-2)所示：

$$\left|yx\right\rangle = \left|y_{n-1}y_{n-2}\cdots y_0\right\rangle \otimes \left|x_{n-1}x_{n-2}\cdots x_0\right\rangle \tag{2-2}$$

共占用 $2n$ 个量子比特；

$$\left|f\left(y,x\right)\right\rangle = \left|C_{yx}^{q-1}C_{yx}^{q-2}\cdots C_{yx}^{0}\right\rangle \tag{2-3}$$

如式(2-3)所示，$C_{yx}^{k} \in \{0,1\}$ 直接对应经典灰度值的二进制位，共占用 q 个量子比特。因此，一幅尺寸为 $2^n \times 2^n$ 的图像，使用 NEQR 编码所需总量子比特数为 $q + 2n$。

以 $2^2 \times 2^2$ 的图像进行表示，如图 1 所示，每个方块内给出该像素的 8 位二进制灰度值。NEQR 的核心思想[15]是利用量子叠加态描述图像位置，并利用量子基态比特串存储像素灰度值，如式(2-4)所示。

Figure 1. NEQR
图 1. NEQR 图

$$|I\rangle=\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|f(y,x)\rangle\otimes|yx\rangle \tag{2-4}$$

$$\begin{aligned}|I\rangle&=\frac{1}{4}\sum_{y=0}^{3}\sum_{x=0}^{3}|f(y,x)\rangle\otimes|yx\rangle\\&=\frac{1}{4}\big[|00100000\rangle\otimes|0000\rangle+|01001101\rangle\otimes|0001\rangle+|01111100\rangle\otimes|0010\rangle+|10101000\rangle\otimes|0011\rangle\\&\quad+|01010011\rangle\otimes|0100\rangle+|10000111\rangle\otimes|0101\rangle+|10111101\rangle\otimes|0110\rangle+|11110000\rangle\otimes|0111\rangle\\&\quad+|01000010\rangle\otimes|1000\rangle+|01110110\rangle\otimes|1001\rangle+|10101100\rangle\otimes|1010\rangle+|11100100\rangle\otimes|1011\rangle\\&\quad+|00110011\rangle\otimes|1100\rangle+|01100110\rangle\otimes|1101\rangle+|10011001\rangle\otimes|1110\rangle+|11001100\rangle\otimes|1111\rangle\big]\end{aligned} \tag{2-5}$$

公式展开后与图像一一对应，如式(2-5)所示，完整体现 NEQR“位置叠加编码、灰度基态编码”的底层机制。

2.2. 像素空间位置置乱

2.2.1. Logistic 混沌映射

混沌系统因其对初始条件的极端敏感性、伪随机性以及遍历性(见图 2)，被广泛应用于现代密码学体系中[16]。本文选用经典的 Logistic 离散混沌映射来生成控制量子置乱网络的随机序列。Logistic 映射的动力学方程为：

$$x_{n+1}=r\cdot x_n\cdot(1-x_n) \tag{2-6}$$

式中，x_n 为第 n 次迭代的系统状态值，且满足 $x_n\in(0,1)$；r 为系统的控制参数(分岔参数)。研究表明，当 $r\in[3.5699456,4]$ 时，系统进入完全混沌状态，此时生成的序列具有高度的不可预测性[17]。

在本文的加密方案中，为了抵御选择明文攻击(CPA)，系统并未采用静态的初始密钥。相反，将明文图像的特征扰动因子 Δ 叠加至外部初始密钥 x_0，生成动态初始值 $x_0'=(x_0+\Delta)\bmod 1$。以 x_0' 为起点迭代

Logistic 方程 N 次(N 为图像总像素数)，经过降序量化处理后得到用于驱动量子逻辑门的离散寻址控制序列 $\mathrm{Seq}_{\mathrm{addr}}=\{k_N,k_{N-1},\cdots,k_2\}$。该序列中的每一个元素严格满足 $k_i\in[1,i]$，降序量化算法连续混沌→离散置换地址，输入连续混沌序列，像素总数 N 输出为离散置换地址序列：

首先进行归一化：对每个混沌值取模 1，映射到$[0,1)$ $\tilde{x}_i=|x_i|\bmod 1$。再进行从 N 到 2 逆序生成合法地址 $k_i=\lfloor \tilde{x}_i\cdot i\rfloor+1, i=N,N-1,\cdots,2$。最终输出离散置换控制序列 $\mathrm{Seq}_{\mathrm{addr}}=\{k_N,k_{N-1},\cdots,k_2\}$，确保了后续置乱操作的完备性与双射性。

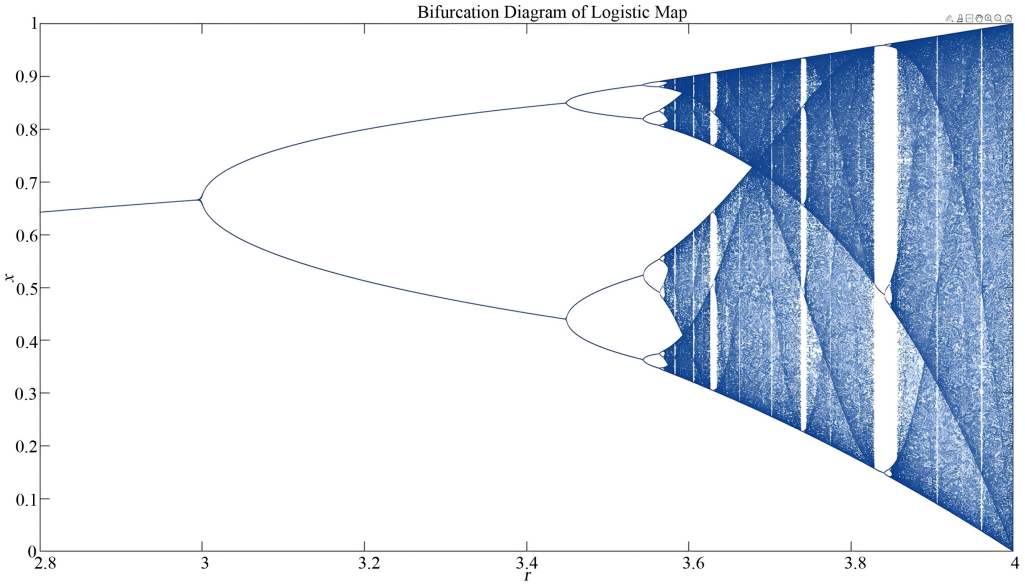

Figure 2. Logistic MAP
图 2. Logistic 映射图

2.2.2. CSWAP 量子门与坐标置换网络

在量子计算框架下，经典计算机中的数组元素对调操作必须由量子受控交换门(Controlled-SWAP Gate，又称 Fredkin 门[18])来实现。C-SWAP 门由一个控制量子比特和两个目标量子比特组成。当控制比特为|0⟩时，目标比特的状态保持不变；当控制比特为|1⟩时，两个目标比特的状态发生交换，如公式(2-7)所示：

$$\mathrm{CSWAP}|c\rangle|x\rangle|y\rangle=\begin{cases}|0\rangle|x\rangle|y\rangle, & c=0\\ |1\rangle|y\rangle|x\rangle, & c=1\end{cases} \tag{2-7}$$

当作用在 3 比特空间(控制，目标 1，目标 2) [19]则表示为仅当输入为|101⟩ (5)和|110⟩ (6)时发生交换，如式(2-8)所示：

$$\mathrm{CSWAP}=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&1&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix} \tag{2-8}$$

为了在量子线路上实现全局置乱，本文将 $N-1$ 个 C-SWAP 操作级联，构建量子坐标置换网络。对于大小为 $2^n \times 2^n$ 的量子图像 $|I\rangle$，其坐标基态可表示为 $|yx\rangle$ (等效于索引态 $|i\rangle$)。置乱过程的单步量子酉算子 U_i 定义为：受控于 Logistic 寻址序列中的 k_i，算子 U_i 将处于基态 $|i\rangle$ 的坐标量子比特与处于基态 $|k_i\rangle$ 的坐标量子比特进行全连通状态置换。

设 NEQR 量子图像系统的希尔伯特空间为 $\mathscr{H} = \mathscr{H}_{\text{pos}} \otimes \mathscr{H}_{\text{col}}$，其中 $\mathscr{H}_{\text{pos}}$ 为位置量子比特空间，$\mathscr{H}_{\text{col}}$ 为颜色量子比特空间。全局坐标置乱算子 U_1 是仅作用于位置空间的酉算子，定义为 $U_1 = I_{\text{col}} \otimes \hat{U}_{\text{scramble}}$，作用方式为 $U_1 : \mathscr{H}_{\text{pos}} \to \mathscr{H}_{\text{pos}}$。整个全局量子置乱算子 U_{scramble} 可表示为从 N 到 2 逆序级联的酉变换矩阵连乘，如式(2-9)所示：

$$U_{\text{scramble}} = \prod_{i=2}^{N} U_i = U_2 U_3 \cdots U_N \tag{2-9}$$

将算子 U_{scramble} 作用于初始态 $|I\rangle$ 的坐标寄存器上，根据量子力学的线性叠加原理，所有纠缠的像素坐标将并行完成空间重排。

2.3. 像素值非线性转变

2.3.1. Lorenz 混沌系统

Lorenz 系统是第一个经典混沌系统，由美国气象学家 Edward N. Lorenz 在 1963 年研究大气对流时提出[20]。它是一组三维自治常微分方程，是确定性非线性系统产生混沌行为的典型代表，具有对初始条件极端敏感、有界性、非周期性、拓扑混合、连续遍历以及伪随机的特性并会形成具有分形结构的 Lorenz 奇怪吸引子，因此被广泛应用于混沌保密通信、图像加密、量子混沌加密等信息安全领域。其数学建模如式(2-10)所示：

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \tag{2-10}$$

x、y、z：系统状态变量；

σ：普朗特数(Prandtl number)；

ρ：瑞利数(Rayleigh number)；

β：与物理尺度相关的参数。

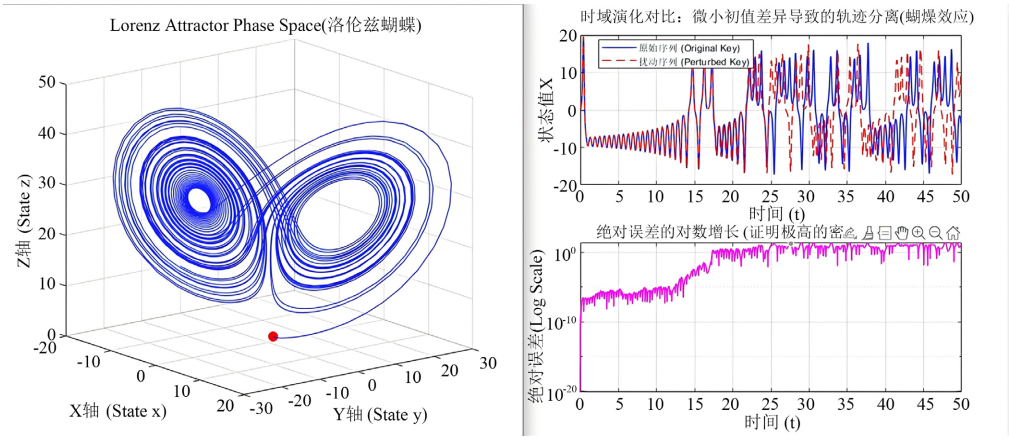

Figure 3. Lorenz model
图 3. Lorenz 模型

当系统参数取经典混沌值 $\sigma=10$ 、 $\rho=28$ 、 $\beta=8/3$ 时，Lorenz 系统呈现稳定且强混沌特性，其运动轨迹围绕两个不动点不断旋转且永不重复、永不收敛，形成典型的蝴蝶状吸引子[21]，如图 3 所示。

由于 Lorenz 系统是连续动力学系统，在实际数字加密应用中必须进行离散化求解，目前最常用、精度最高的数值求解方法为四阶龙格－库塔法(RK4)，通过设定合适的迭代步长可将连续微分方程转化为可迭代计算的离散序列，从而生成长度可控、随机性优良的混沌序列。

$$k_1 = f\left(t_n, X_n\right) \tag{2-11}$$

$$k_2 = f\left(t_n + h/2, X_n + hk_1/2\right) \tag{2-12}$$

$$k_3 = f\left(t_n + h/2, X_n + hk_2/2\right) \tag{2-13}$$

$$k_4 = f\left(t_n + h, X_n + hk_3\right) \tag{2-14}$$

$$X_{n+1} = X_n + \frac{h}{6}\left(k_1 + 2k_2 + 2k_3 + k_4\right) \tag{2-15}$$

该序列既具备随机序列的统计特性，又由确定性方程产生，便于密钥控制与算法实现。凭借结构简单、实现方便、混沌特性稳定、密钥空间大等优势，Lorenz 系统非常适合用于图像像素置乱与扩散操作，同时能够与量子门(如 CSWAP 门、CNOT 门等)有机结合，有效提升量子图像加密算法的安全性、抗攻击能力与密钥敏感性。本方案中使用 Lorenz 系统得到三维连续混沌序列 X_L、Y_L、Z_L。对 X_L 归一化、放大并取模，得到 DNA 编码规则索引 $K_{\text{rule}}(i)=\left(\left\lfloor |x_i|\times 10^{14}\right\rfloor \bmod 8\right)+1$ 满足 $K_{\text{rule}}(i)\in\{1,2,\cdots,8\}$ 。对 Y_L 放大、取整并模 256，得到扩散密钥： $K_{\text{diff}}(i)=\left(\left\lfloor |y_i|\times 10^{14}\right\rfloor \bmod 256\right)$ 满足 $K_{diff}(i)\in\{0,1,\cdots,255\}$ ，两组序列长度与图像像素数一致，分别控制量子 DNA 编码与非线性扩散。

2.3.2. 量子 DNA 动态编码

脱氧核糖核酸(DNA)凭借高信息密度、低能耗与天然并行特性，已被广泛应用于图像加密领域[22]。DNA 分子由腺嘌呤(A)、胸腺嘧啶(T)、胞嘧啶(C)和鸟嘌呤(G)四种核苷酸碱基构成。在量子计算框架下，经典图像的灰度值被转化为由 $|0\rangle$ 和 $|1\rangle$ 构成的量子比特序列。由于四种碱基恰好能容纳两位二进制信息的组合，因此可以将计算基底 $|00\rangle,|01\rangle,|10\rangle,|11\rangle$ 与四种碱基建立双射关系。

依据 Watson-Crick 互补配对原则，DNA 碱基满足 A 与 T 互补、C 与 G 互补的物理特性[23]。在二进制量子逻辑中[24]，互补意味着按位取反(即 $|00\rangle\leftrightarrow|11\rangle$ ， $|01\rangle\leftrightarrow|10\rangle$)。在理论上可能的 $4!\left[\text{cite}_s\text{tart}\right]=24$ 种代数映射中，仅有 8 种严格满足上述互补等效性。这 8 种合法的量子 DNA 映射规则定义为规则集 $\mathbb{R}=\{R_1,R_2,\cdots,R_8\}$ ，如表 1 所示。

Table 1. DNA encoding rules
表 1. DNA 编码规则

DNA	1	2	3	4	5	6	7	8
A	$\|00\rangle$	$\|00\rangle$	$\|01\rangle$	$\|01\rangle$	$\|10\rangle$	$\|10\rangle$	$\|11\rangle$	$\|11\rangle$
G	$\|01\rangle$	$\|10\rangle$	$\|00\rangle$	$\|11\rangle$	$\|00\rangle$	$\|11\rangle$	$\|01\rangle$	$\|10\rangle$
T	$\|11\rangle$	$\|11\rangle$	$\|10\rangle$	$\|10\rangle$	$\|01\rangle$	$\|01\rangle$	$\|00\rangle$	$\|00\rangle$
C	$\|10\rangle$	$\|01\rangle$	$\|11\rangle$	$\|00\rangle$	$\|11\rangle$	$\|00\rangle$	$\|10\rangle$	$\|01\rangle$

如 2.2.1 节所述，本文利用四阶龙格－库塔法(RK4)对明文关联的 Lorenz 系统进行离散化求解，生成了混沌序列 L。在动态编码阶段，该序列将被用作 DNA 规则选择的“控制流”。

假设量子中间态图像 $|I_d\rangle$ 的每个像素由 8 个颜色量子比特构成，若将其精细划分为 4 个双比特对，则一幅 $M\times N$ 大小的图像共需要 $4\times M\times N$ 个动态编码规则。提取混沌序列中的第 k 个实数值 L_k，通过

量化函数(2-16)为其生成对应的动态寻址索引：

$$CR_k = \mathrm{mod}\left(\left\lfloor |L_k| \times 10^{14} \right\rfloor, 8\right) + 1 \tag{2-16}$$

对于纠缠于特定空间坐标$|yx\rangle$的 8 位颜色量子态$\left|c_{yx}^{7}c_{yx}^{6}\cdots c_{yx}^{0}\right\rangle$，其量子 DNA 动态编码算子$\mathcal{E}_{\mathrm{DNA}}$的物理演化过程分为两步：

把 8 维希尔伯特空间中的颜色态等分为 4 个相互独立的双比特子空间，如(2-17)所示：

$$\left|c(y,x)\right\rangle \to \left|c_{yx}^{7}c_{yx}^{6}\right\rangle \otimes \left|c_{yx}^{5}c_{yx}^{4}\right\rangle \otimes \left|c_{yx}^{3}c_{yx}^{2}\right\rangle \otimes \left|c_{yx}^{1}c_{yx}^{0}\right\rangle = \bigotimes_{3}^{j=0} \left|p_j\right\rangle \tag{2-17}$$

前述生成的寻址索引序列 CR 作为控制流，对每一个双比特子空间$\left|p_j\right\rangle$施加独立的 DNA 映射操作，见(2-18)：

$$\left|\mathrm{DNA}(y,x)\right\rangle = \bigotimes_{3}^{j=0} \mathcal{E}_{\mathrm{DNA}}^{(CR_{4i+j})}\left(\left|p_j\right\rangle\right) = \left|b_3\right\rangle \otimes \left|b_2\right\rangle \otimes \left|b_1\right\rangle \otimes \left|b_0\right\rangle \tag{2-18}$$

当面临灰度值为 01111101 这样的图像信息时，首先将其拆分为 4 个双比特态(2-19)：

$$\left|01111101\right\rangle \to \left|01\right\rangle \otimes \left|11\right\rangle \otimes \left|11\right\rangle \otimes \left|01\right\rangle \tag{2-19}$$

使用 Lorenz 对这四组分别分配具体规则，例如 R3、R4、R5、R8 (假设状态)。系统分别进行独立编码，依据映射矩阵：

|01⟩查询 R3，演化为|A⟩；

|11⟩查询 R4，演化为|G⟩；

|11⟩查询 R5，演化为|C⟩；

|01⟩查询 R8，演化为|C⟩。

最终编码为一条 DNA 序列(2-20)：

$$\left|\mathrm{DNA}\right\rangle = \left|\mathrm{A}\right\rangle \otimes \left|\mathrm{G}\right\rangle \otimes \left|\mathrm{C}\right\rangle \otimes \left|\mathrm{C}\right\rangle \tag{2-20}$$

3. 量子图像加密和解密方法

3.1. 图像加密

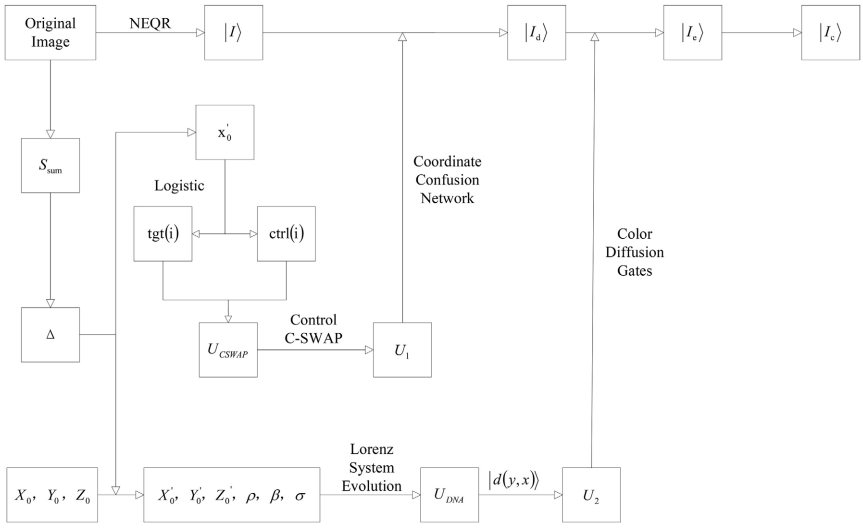

Figure 4. Encryption flow chart
图 4. 加密流程图

本加密方案是针对现有量子图像加密方案的研究短板提出的改进方案。基于 NEQR 量子图像表示模型[25]，构建“坐标置乱–颜色扩散”的双阶段混淆架构。首先利用 NEQR 将经典图像映射为量子叠加态，随后通过明文关联混沌系统驱动量子 C-SWAP 门完成空间坐标置换，最后由 Lorenz 超混沌系统控制量子 DNA 动态逻辑门实现颜色量子比特深度扩散。

其具体的流程图如图 4 所示。

步骤 1：待加密图像用 NEQR 模型表示

设原始经典图像尺寸为 $2n \times 2n$，其 NEQR 量子表示为(3-1)：

$$\begin{aligned}|I\rangle &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c(y,x)\right\rangle \otimes |yx\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c_{yx}^{7}c_{yx}^{6}\cdots c_{yx}^{0}\right\rangle \otimes \left|y_{n-1}y_{n-2}\cdots y_0\right\rangle \left|x_{n-1}x_{n-2}\cdots x_0\right\rangle\end{aligned} \tag{3-1}$$

步骤 2：量子 C-SWAP 全局坐标置乱

为破坏像素间的空间拓扑相关性，本文设计基于 Logistic 混沌驱动量子 C-SWAP 受控置换网络。利用混沌序列生成控制比特 $ctrl(i)$与目标索引 $tgt(i)$，通过量子 C-SWAP、算子 U_{SWAP} 对 NEQR 量子态的坐标与颜色关联进行全局置换。

首先计算明文图像总像素和：

$$S = \sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1} I(y,x) \tag{3-2}$$

构建明文动态偏移量：

$$\Delta = \mathrm{mod}\left(S \times 0.001234567, 1\right) \tag{3-3}$$

更新 Logistic 和 Lorenz 混沌的初始条件：

$$x_0' = \mathrm{mod}\left(x_0 + \Delta, 1\right) \tag{3-4}$$

$$\left(X_0', Y_0', Z_0'\right) = \left(X_0, Y_0, Z_0\right) + \Delta \tag{3-5}$$

生成混沌序列构建量子 C-SWAP 控制比特与目标索引：

$$x_{n+1} = r \cdot x_n \cdot \left(1 - x_n\right) \tag{3-6}$$

$$ctrl(i) = \mathrm{bitxor}\left(\mathrm{mod}\left(\left\lfloor x_i \times 10^{14} \right\rfloor, 2\right), \mathrm{mod}(i, 2)\right) \tag{3-7}$$

$$tgt(i) = x_i \tag{3-8}$$

$$U_{\mathrm{CSWAP}}|c\rangle|a\rangle|b\rangle = \begin{cases} |c\rangle|a\rangle|b\rangle, & c = 0 \\ |c\rangle|b\rangle|a\rangle, & c = 1 \end{cases} \tag{3-9}$$

最终构建全局坐标置乱算子：

$$\begin{aligned}U_1 &= \prod_{i=N}^{-1} U_{\mathrm{CSWAP}}\left(ctrl(i), \left|I(i)\right\rangle, \left|I(j)\right\rangle\right) \\ &= \prod_{i=N}^{-1} U_{\mathrm{CSWAP}}\left(ctrl(i), \left|I(i)\right\rangle, \left|I\left(\left\lfloor tgt(i)\cdot i \right\rfloor + 1\right)\right\rangle\right)\end{aligned} \tag{3-10}$$

对原始图像执行坐标置乱，其量子态演变过程如公式(3-11)所示：

$$\begin{aligned} U_1\left(\left|I\right\rangle\right) &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c\left(y,x\right)\right\rangle\otimes U_{\mathrm{CSWAP}}\left|yx\right\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|c\left(y,x\right)\right\rangle\otimes\left|y'x'\right\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|d\left(y,x\right)\right\rangle\otimes\left|yx\right\rangle \\ &= \left|I_d\right\rangle \end{aligned} \tag{3-11}$$

步骤三：Lorenz 混沌驱动量子 DNA 扩散

在完成空间置乱后，引入 Lorenz 混沌系统生成 DNA 编码规则密钥流 K_{rule} 与动态逻辑门密钥 K_{diff}。通过量子 DNA 动态逻辑门算子 U_{DNA}，对置乱后的颜色量子比特 $\left|d\left(y,x\right)\right\rangle$ 进行非线性运算，实现对颜色信息的深度混淆，其量子态演变过程如公式(3-12)所示：

$$\begin{cases} \dot{x} = \sigma\left(y-x\right) \\ \dot{y} = x\left(\rho-z\right)-y \\ \dot{z} = xy-\beta z \end{cases} \tag{3-12}$$

$$U_{\mathrm{DNA}} = G\left(K_{\mathrm{rule}},K_{\mathrm{diff}}\right) = \hat{G}\left(K_{\mathrm{rule}},K_{\mathrm{diff}}\right)\otimes I_{\mathrm{pos}} \tag{3-13}$$

$I_{\mathrm{pos}}:\mathscr{H}_{\mathrm{pos}}\to\mathscr{H}_{\mathrm{pos}}$ 为位置空间上的恒等算子，保证像素坐标不发生任何改变。

$$\begin{aligned} U_2\left(\left|I_d\right\rangle\right) &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}U_{\mathrm{DNA}}\left(Y,X\right)\left|I_d\right\rangle \\ &= \prod_{Y=0}^{2^n-1}\prod_{X=0}^{2^n-1}U_{\mathrm{DNA}}\left(Y,X\right)\left(\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left|d\left(Y,X\right)\right\rangle\left|YX\right\rangle\right) \\ &= \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}S_{YX}\left|d\left(Y,X\right)\right\rangle\left|YX\right\rangle\backslash\,\mathrm{tag22} \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|e_{yx}^{7}e_{yx}^{6}\cdots e_{yx}^{1}e_{yx}^{0}\right\rangle\left|yx\right\rangle \\ &= \left|I_e\right\rangle \end{aligned} \tag{3-14}$$

整体加密过程可表示为两次酉变换的级联：

$$\left|I_C\right\rangle = U_{\mathrm{DNA}}\cdot U_{\mathrm{CSWAP}}\cdot\left|I\right\rangle \tag{3-15}$$

将最终加密量子态 $\left|I_C\right\rangle$ 经量子测量与经典重构，得到加密图像。

3.2. 图像解密

由于量子逻辑门具有天然的可逆性(即酉算子的共轭转置等于其逆矩阵)，$U^{\dagger}=U^{-1}$，因此本方案的解密过程本质上是加密流程的逆向酉演化。接收方在获取密文图像与外部密钥后，严格按照“先逆扩散，后逆置乱”的顺序依次作用逆量子算子，最终通过量子测量坍缩回经典明文图像。整体的量子解密演化方程可表示为：

$$\left|U\right\rangle = U_{\mathrm{CSWAP}}^{\dagger}\cdot U_{\mathrm{DNA}}^{\dagger}\cdot\left|I_e\right\rangle \tag{3-16}$$

具体解密步骤如下：

步骤 1：明文关联特征值同步与密钥流重构

由于加密方案采用了抗差分攻击的明文关联机制，接收方首先需要通过安全信道获取外部初始密钥 K 以及明文特征偏移量 Δ (或明文像素总和 S)。利用这些参数严格复现加密端的 Logistic 混沌映射与 Lorenz 混沌系统演化轨迹，生成完全一致的置乱控制序列 $ctrl(i)$、$tgt(i)$以及 DNA 扩散密钥流 K_{DNA}。

步骤 2：量子 DNA 动态逻辑门逆扩散

将接收到的经典密文图像制备为量子态 $|I_e\rangle$。随后利用重构得到的 Lorenz 混沌密钥流 K_{DNA}，对颜色量子比特执行逆向 DNA 动态逻辑门运算 $U_{\mathrm{DNA}}^{\dagger}$。该过程解除了像素深度的非线性混淆，并且还原出仅带有空间坐标置乱的中间量子态 $|I_d\rangle$：

$$|I_d\rangle = U_{\mathrm{DNA}}^{\dagger}|I_e\rangle \tag{3-17}$$

步骤 3：量子 C-SWAP 网络逆置乱

在解除颜色扩散后，利用重构的 Logistic 控制序列驱动逆向全局量子 C-SWAP 网络 $U_{\mathrm{CSWAP}}^{\dagger}$。当控制比特 $ctrl(i)=1$ 时，再次触发受控交换逻辑，将之前被打乱的坐标量子态 $|y'x'\rangle$ 精准还原至原始空间位置 $|yx\rangle$：

$$|I\rangle = U_{\mathrm{CSWAP}}^{\dagger}|I_d\rangle \tag{3-18}$$

步骤 4：量子测量与经典图像重构

经过上述两次逆向酉变换，系统已完全恢复至原始明文的量子叠加态 $|I\rangle$。最后，按计算基对该量子态执行投影测(Quantum Measurement)，获取所有像素的颜色与坐标信息，并将其重构为二维经典数字图像，即完成解密。

4. 实验结果和理论分析

鉴于当前物理量子计算机的实际限制，本方案在经典计算平台(MATLAB 2022b)上完成系统的理论验证。实验通过矩阵与张量积等数学工具，精确模拟 NEQR 量子图像表示模型、量子 C-SWAP 置乱以及量子 DNA 动态扩散等全套酉变换过程。原始图像、加密图像(图 5)及解密图像(图 6)的对比结果经本文方案加密后，密文图像呈现均匀随机噪声分布。原始图像的纹理、轮廓、结构等所有视觉信息被完全隐藏无法从中获取任何明文特征，这表明加密方案具备优秀的混淆能力。在正确密钥作用下，解密图像能够恢复与原始明文图像基本一致，无信息丢失、无像素失真，充分验证了本算法在逻辑与操作上的可行性。

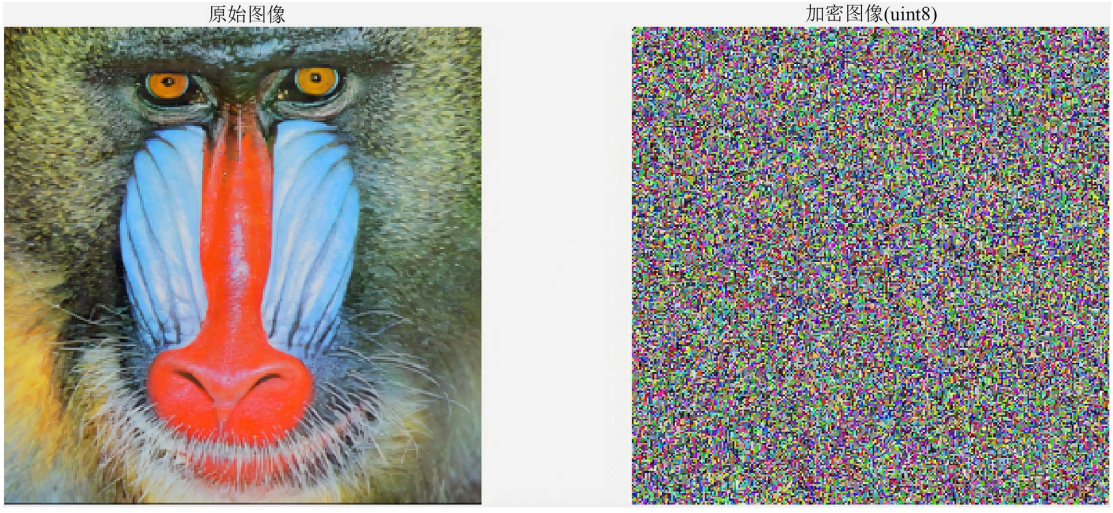

Figure 5. Encrypted image
图 5. 加密图像

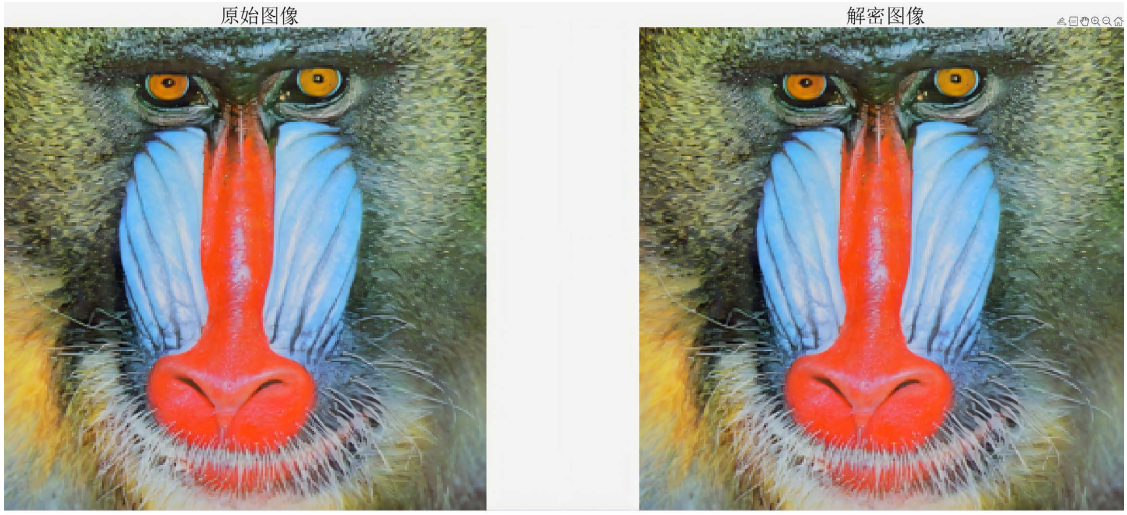

Figure 6. Decrypted image
图 6. 解密图像

4.1. 直方图结果分析

论直方图反映图像像素值的分布规律是评估加密算法消除明文统计特征能力的直接指标。对于经典图像，设图像尺寸为 $W \times H$，灰度级总数为 $L = 256$，像素值 k 出现的概率分布可表示为：

$$p_k = \frac{n_k}{W \times H}, \quad k = 0,1,\cdots,255 \tag{4-1}$$

其中，n_k 表示灰度值 k 出现的频数。

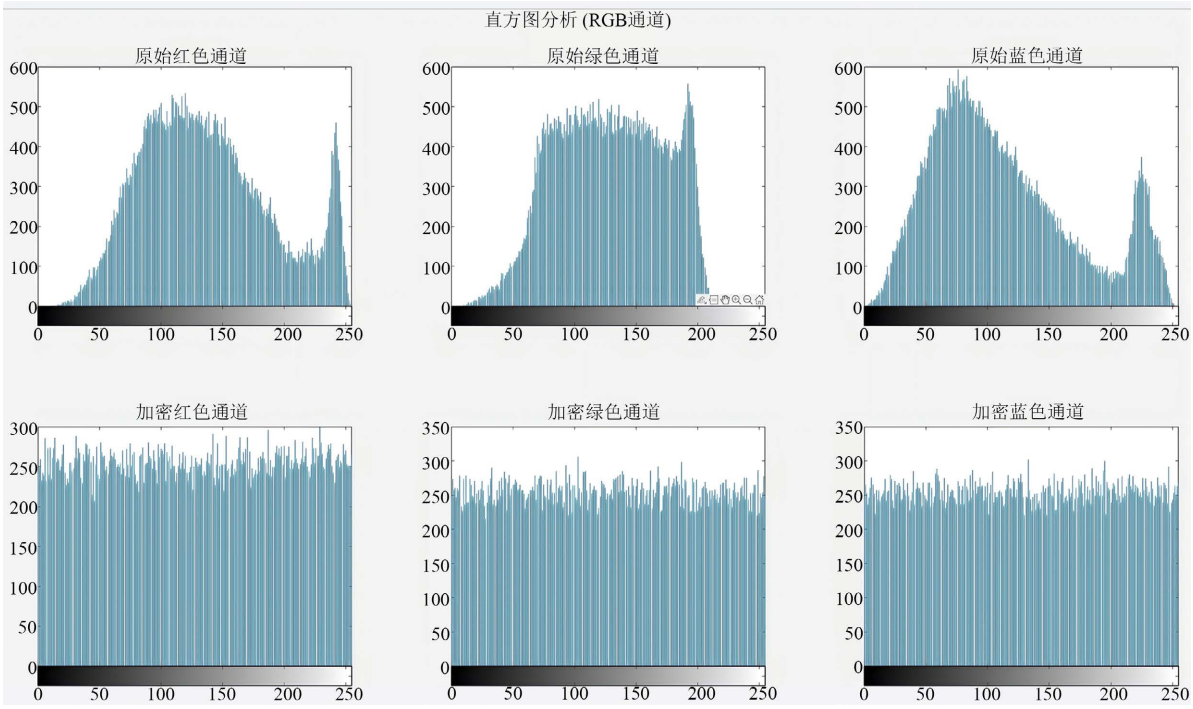

Figure 7. Histogram analysis
图 7. 直方图分析

如图 7 所示，原始图像在红、绿、蓝三个通道上的直方图均呈现明显的非均匀分布，存在尖锐的峰值且十分显著的灰度起伏，这直观反映原始图像存在的强像素相关性和纹理结构信息。经本文量子加密后的图像直方图分布均匀平坦，各灰度级概率数值均接近，且无明显峰值整体曲线平滑，像素值已彻底被混淆。这表明本方案成功消除了原始图像的统计特征，使密文图像具备较理想的随机分布。

4.2. 相邻像素相关性分析

相邻像素相关性是反映图像空间冗余信息的重要指标[26]，也是衡量加密算法混淆能力的核心标准。在自然图像中，相邻像素(水平、垂直、对角线方向)存在极强的正相关性；而理想加密图像的相邻像素应相互独立，相关系数理论上趋近于 0。

该方法随机选取图像中 3000 对相邻像素点$\left(p(i,j),p(i,j+1)\right)$、$\left(p(i,j),p(i+1,j)\right)$、$\left(p(i,j),p(i+1,j+1)\right)$，分别对应水平、垂直、对角线方向的像素相关性。其计算公式如下：

$$\bar{p}=\frac{1}{N}\sum_{k=1}^{N}p_k \tag{4-2}$$

$$Cov(p,q)=\frac{1}{N}\sum_{k=1}^{N}(p_k-\bar{p})(q_k-\bar{q}) \tag{4-3}$$

$$\rho_{p,q}=\frac{Cov(p,q)}{\sqrt{D(p)}\sqrt{D(q)}} \tag{4-4}$$

$$D(p)=\frac{1}{N}\sum_{k=1}^{N}(p_k-\bar{p})^2,\quad N=3000 \tag{4-5}$$

如图 8 所示，对比原始图像与加密图像的相关性散点图与相关系数可知，原始图像水平、垂直和对角线方向的相关系数分别为 0.9282、0.9063、0.8843，散点图呈现明显的椭圆带状分布，像素间存在着显著的线性正相关，这说明原始图像具有强烈的空间冗余性。而加密图像水平、垂直以及对角线方向的相关系数分别降至 0.0072、−0.012、−0.0142，数值均极度接近 0；散点图则均匀随机分布于整个坐标平面没有任何聚集趋势。这证明本方案消除了像素间的空间相关性，使得密文图像具备理想的随机分布特性，有效抵御基于像素相关性的统计攻击和视觉分析。

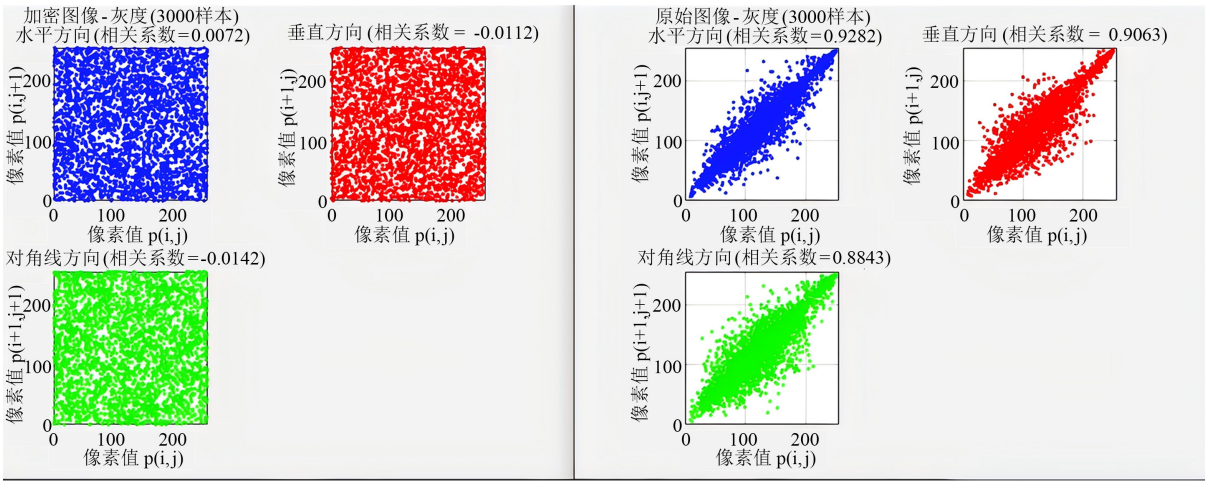

Figure 8. Correlation analysis
图 8. 相关性分析

4.3. 抗裁切攻击

在实际网络传输中，加密图像常面临数据丢失或被篡改的风险。为验证本算法的容错能力，实验对密文图像进行了裁切攻击破坏其完整性。如图 9 所示。

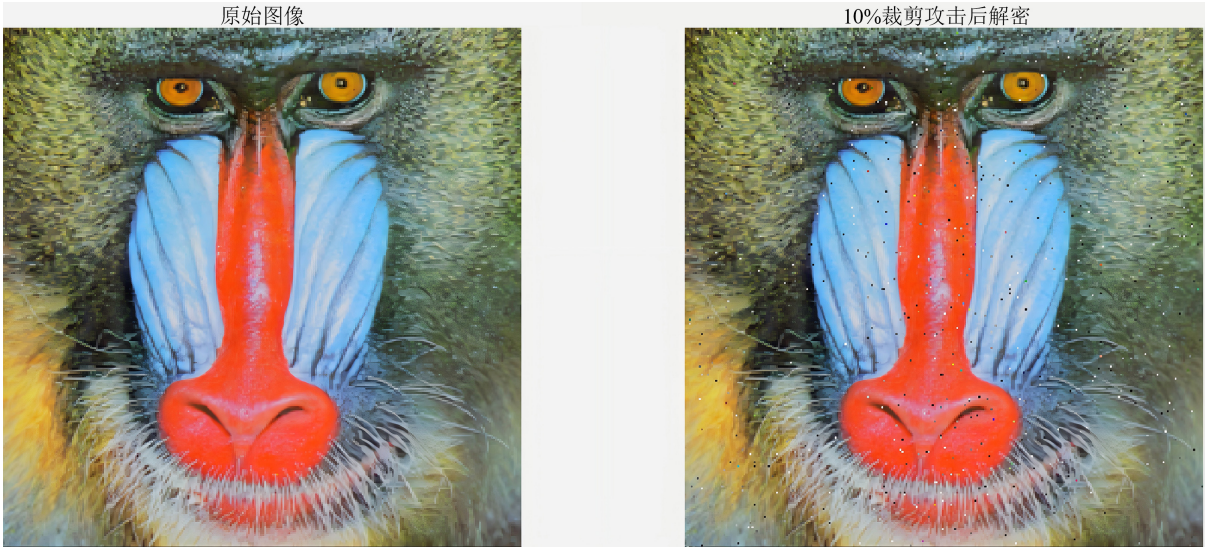

Figure 9. Cropping attacks analysis
图 9. 抗裁切攻击分析

尽管解密图像出现了一定程度的离散噪声，但仍可完整恢复面部纹理与主体结构，仅在裁剪边缘存在少量噪点，整体视觉信息清晰无失真。这种恢复效果归功于本文设计的全局受控置乱与深度扩散机制：算法将原始图像的局部特征均匀分散至全局密文空间中，使得局部的密文丢失在解密时仅表现为全局的均匀噪声而非局部盲区。

4.4. 抗噪声攻击

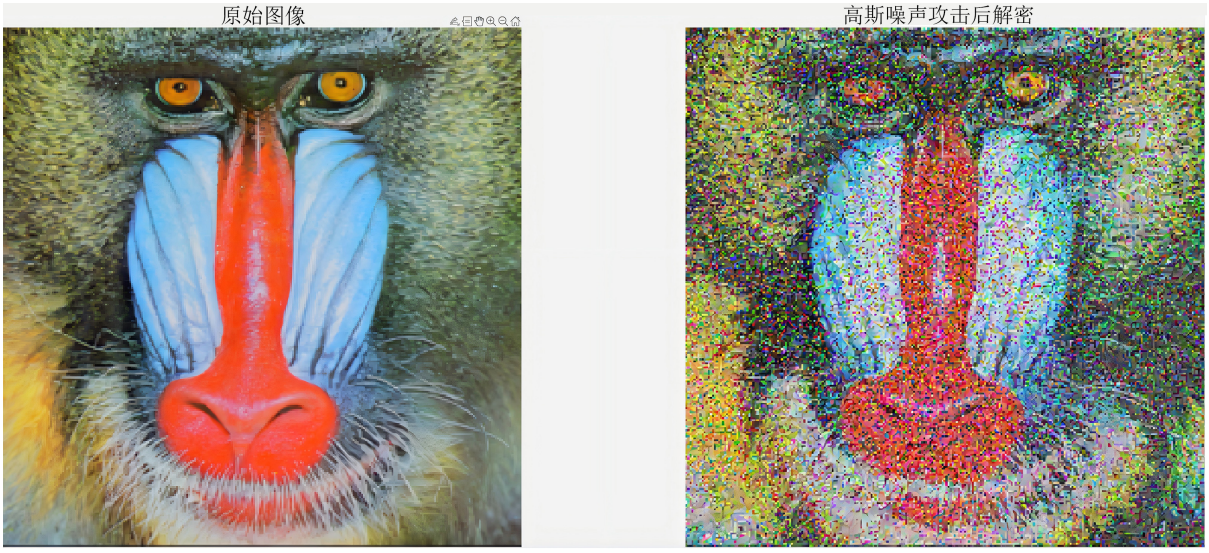

Figure 10. Noise attacks analysis
图 10. 抗噪声攻击分析

实际通信与存储场景中，图像易受信道噪声干扰，因此加密方案需具备一定的抗噪声攻击能力，以验证算法在非理想环境下的鲁棒性[27]。本实验模拟信道噪声干扰，对加密图像添加高斯噪声破坏其像素完整性，随后使用正确密钥进行解密恢复。通过对比原始图像与解密图像的视觉信息与结构可识别度(图10)，评估方案对噪声干扰的容忍度。实验结果表明，即使遭受高斯噪声干扰，解密图像仍可清晰恢复面部主体结构与核心视觉特征，仅存在全局颗粒噪点，整体信息可识别性未受显著影响。

Table 2. DNA encoding rules
表 2. 加密方法分析对比

加密方法	图像大小	NPCR (%)	UACI (%)	信息熵
本方案	256 × 256	99.61	33.42	7.9992
Wang (2022)	256 × 256	99.59	33.38	7.9997
Zhou (2023)	256 × 256	99.60	33.40	7.9998

由表 2 可知，与近年部分优秀加密方案相比，本文提出的加密方案在 NPCR、UACI、信息熵等关键指标上均体现了整体的安全性与运行效率，能有效抵御各类典型攻击。

5. 结论

本文提出了一种基于明文关联混沌驱动的量子图像双重加密方案，以 NEQR 量子图像表示为基础，通过明文特征更新混沌初始条件，构建了 Logistic 混沌驱动量子 C-SWAP 坐标置乱与 Lorenz 混沌控制量子 DNA 扩散的双阶段加密方案。实验与安全性分析表明，该方案可彻底消除明文统计特征与空间相关性，加密图像直方图均匀平坦、NPCR (99.6%)、UACI (33.4%)与信息熵均逼近理论极值，同时具备强大密钥空间、优异的抗差分攻击能力；在裁剪攻击与高斯噪声攻击下，解密图像仍能完整恢复主体结构与关键视觉信息，表现出良好的鲁棒性。该方案的时间复杂度仅为 $O_{(n)}$，不存在 O (N log N)的过程，适用于数字图像的保密传输与存储。

基金项目

国家自然科学基金资助项目(62472040、12161061、61762068)；内蒙古自治区科技计划项目(SB20210010)；北京市教育科学“十四五”规划 2025 年度一般课题(CDGB25540)；2025 年度北京市数字教育研究课题(BDEC2025619060)；北京市高等教育学会面上课题(MS2024195)；北京印刷学院青年卓越项目(Ea202411)；北京印刷学院学科建设和研究生教育专项(21090225014、21090525019)。

参考文献

[1] Zhou, R., Wu, Q., Zhang, M. and Shen, C. (2013) Quantum Image Encryption and Decryption Algorithms Based on Quantum Image Geometric Transformations. *International Journal of Theoretical Physics*, **52**, 1802-1817. https://doi.org/10.1007/s10773-012-1274-8

[2] Yang, Y., Xia, J., Jia, X. and Zhang, H. (2013) Novel Image Encryption/Decryption Based on Quantum Fourier Transform and Double Phase Encoding. *Quantum Information Processing*, **12**, 3477-3493. https://doi.org/10.1007/s11128-013-0612-y

[3] Song, X., Wang, S., Abd El-Latif, A.A. and Niu, X. (2014) Quantum Image Encryption Based on Restricted Geometric and Color Transformations. *Quantum Information Processing*, **13**, 1765-1787. https://doi.org/10.1007/s11128-014-0768-0

[4] Sang, J., Wang, S. and Niu, X. (2016) Quantum Realization of the Nearest-Neighbor Interpolation Method for FRQI and NEQR. *Quantum Information Processing*, **15**, 37-64. https://doi.org/10.1007/s11128-015-1135-5

[5] Jiang, N., Zhao, N. and Wang, L. (2016) LSB Based Quantum Image Steganography Algorithm. *International Journal*

of Theoretical Physics, **55**, 107-123. https://doi.org/10.1007/s10773-015-2640-0

[6] Hua, T., Chen, J., Pei, D., Zhang, W. and Zhou, N. (2015) Quantum Image Encryption Algorithm Based on Image Correlation Decomposition. *International Journal of Theoretical Physics*, **54**, 526-537. https://doi.org/10.1007/s10773-014-2245-z

[7] Zhang, J. and Huo, D. (2019) Image Encryption Algorithm Based on Quantum Chaotic Map and DNA Coding. *Multimedia Tools and Applications*, **78**, 15605-15621. https://doi.org/10.1007/s11042-018-6973-6

[8] Wang, J., Geng, Y., Han, L. and Liu, J. (2019) Quantum Image Encryption Algorithm Based on Quantum Key Image. *International Journal of Theoretical Physics*, **58**, 308-322. https://doi.org/10.1007/s10773-018-3932-y

[9] Liu, X., Xiao, D. and Liu, C. (2018) Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation. *Entropy*, **20**, Article 867. https://doi.org/10.3390/e20110867

[10] Zhou, S. (2020) A Quantum Image Encryption Method Based on DNACNot. *IEEE Access*, **8**, 178336-178344. https://doi.org/10.1109/access.2020.3027964

[11] Deepak Vagish, K., Rajakumaran, C. and Kavitha, R. (2020) Chaos Based Encryption of Quantum Images. *Multimedia Tools and Applications*, **79**, 23849-23860. https://doi.org/10.1007/s11042-020-09043-w

[12] Wang, X., Su, Y., Luo, C., Nian, F. and Teng, L. (2022) Color Image Encryption Algorithm Based on Hyperchaotic System and Improved Quantum Revolving Gate. *Multimedia Tools and Applications*, **81**, 13845-13865. https://doi.org/10.1007/s11042-022-12220-8

[13] Zhang, Y., Lu, K., Gao, Y. and Wang, M. (2013) NEQR: A Novel Enhanced Quantum Representation of Digital Images. *Quantum Information Processing*, **12**, 2833-2860. https://doi.org/10.1007/s11128-013-0567-z

[14] Prodan, A., Tudorache, A. and Manta, V. (2026) A New Quantum Video Processing Algorithm Based on the NEQR Technique. *Entropy*, **28**, Article 168. https://doi.org/10.3390/e28020168

[15] Zemate, A.A. and Sedra, M.B. (2026) Quantum Image Encryption Using Quantum Image Representations. *EPJ Web of Conferences*, **350**, Article ID: 01001. https://doi.org/10.1051/epjconf/202635001001

[16] 谢红梅, 夏磊, 朱孟元, 等. 基于 Logistic 混沌映射的图像加密系统及 FPGA 实现[J]. 航空兵器, 2016(2): 56-60.

[17] Naskar, P.K. and Chaudhuri, A. (2015) A Robust Image Encryption Technique Using Dual Chaotic Map. *International Journal of Electronic Security and Digital Forensics*, **7**, 358-380. https://doi.org/10.1504/ijesdf.2015.072180

[18] Chinni Prabhunath, G. and Shah, A.P. (2026) Fredkin Gate-Based Arbiter PUF Design through Challenge Obfuscation Using Garbage Outputs. *Integration*, **106**, Article ID: 102531. https://doi.org/10.1016/j.vlsi.2025.102531

[19] Morita, K. (2022) Fredkin Gates in Simple Reversible Cellular Automata. *International Journal of Parallel, Emergent and Distributed Systems*, **37**, 249-272. https://doi.org/10.1080/17445760.2022.2052871

[20] Fan, B., Zeng, X., Wang, J., Luo, M., Li, X., Liu, J., *et al*. (2026) Implementation of Hybrid Random Number Generator on FPGA: Combining Lorenz Chaotic System with Carry Chain Based Ring Oscillator. *Analog Integrated Circuits and Signal Processing*, **127**, Article No. 1. https://doi.org/10.1007/s10470-026-02572-8

[21] 杨建平, 朱平. 分析 Lorenz 系统动力学特征的新方法[J]. 计算机工程与应用, 2012, 48(23): 230-233.

[22] Chen, X., Yu, S., Wang, Q., Guyeux, C. and Wang, M. (2023) On the Cryptanalysis of an Image Encryption Algorithm with Quantum Chaotic Map and DNA Coding. *Multimedia Tools and Applications*, **82**, 42717-42737. https://doi.org/10.1007/s11042-023-15003-x

[23] Afify, Y.M., Sharkawy, N.H., Gad, W. and Badr, N. (2023) A New Dynamic DNA-Coding Model for Gray-Scale Image Encryption. *Complex & Intelligent Systems*, **10**, 745-761. https://doi.org/10.1007/s40747-023-01187-0

[24] Wang, S., Pan, J., Cui, Y., Chen, Z. and Zhan, W. (2024) Fast Color Image Encryption Algorithm Based on DNA Coding and Multi-Chaotic Systems. *Mathematics*, **12**, Article 3297. https://doi.org/10.3390/math12203297

[25] Fan, P. and Zhang, Y. (2024) Quantum Image Encryption Algorithm Based on Fisher-Yates Algorithm and Logistic Mapping. *Quantum Information Processing*, **23**, Article No. 237. https://doi.org/10.1007/s11128-024-04441-7

[26] Hua, N., Liu, H., Xiong, X., Wang, J. and Liang, J. (2023) A Dynamic Image Encryption Scheme Based on Quantum Walk and Chaos-Induced DNA. *Quantum Engineering*, **2023**, Article ID: 3431107. https://doi.org/10.1155/2023/3431107

[27] Ma, Y. and Zhou, N. (2023) Quantum Color Image Compression and Encryption Algorithm Based on Fibonacci Transform. *Quantum Information Processing*, **22**, Article No. 39. https://doi.org/10.1007/s11128-022-03749-6