基于量子长短期记忆网络的量子图像混沌加密方案*

王伟杰 姜美美 王淑梅 曲英杰 马鸿洋 邱田会†

(青岛理工大学理学院, 青岛 266520)

(2023 年 2 月 20 日收到; 2023 年 4 月 11 日收到修改稿)

近年来, 图像信息的传输安全性已经成为互联网领域的重要研究方向. 本文提出了一种基于量子长短期记忆 (quantum long-short term memory, QLSTM) 网络的量子图像混沌加密方案. 结果发现, 因为 QLSTM 网络具有复杂的结构和较多的参数, 应用 QLSTM 网络对 Lorenz 混沌序列进行改进, 其最大 Lyapunov 指数比原序列提高 2.5465%, 比经典长短期记忆 (long-short term memory, LSTM) 网络改进的序列提高 0.2844%, 同时在 0—1 测试中结果更接近 1 且更稳定, 因此 QLSTM 网络改进的序列具备更优异的混沌性能, 更难以被预测, 提高了单一混沌系统加密的安全性. 运用 NCQI (novel quantum representation of color digital images) 量子图像表示模型, 将原始图像存储为量子态形式, 利用 QLSTM 网络改进的序列分别控制三级径向扩散、量子广义 Arnold 变换和量子 W 变换, 改变量子图像的灰度值与像素位置, 生成最终的加密图像. 本文提出的加密方案在统计学特性测试中, 实现了 RGB 三通道平均信息熵均大于 7.999, 像素数改变率的平均值达 99.6047%, 统一平均变化强度的平均值为 33.4613%, 平均相关性为 0.0038 等, 比其他一些传统方法具有更高的安全性, 能够抵抗常见的攻击方式.

关键词: 量子图像加密, 量子长短期记忆网络, 混沌系统

PACS: 03.65.–w, 03.67.Ac, 05.45.Gg **DOI:** 10.7498/aps.72.20230242

1 引 言

随着计算机网络的快速发展, 在人们的日常信息交流中, 图像作为信息载体起着越来越大的作用, 如何保证图像信息的安全性是目前面临的重要问题之一. 图像加密 [1–7] 是一种信息保护的手段, 通过加密可以最大程度地确保图像信息不被窃密者获取, 从而确保信息的安全性. 由于量子力学中叠加态的存在, 量子计算机的效率远远高于经典计算机. 并且, 量子态的非克隆性确保了量子图像加密的安全性. 因此, 有关量子图像加密的研究方向 [8–16] 受到了极大的关注.

20 世纪 70 年代发展起来的混沌理论为加密算法提供了新的方向, 混沌系统的初值与参数极端敏感性、非周期性和长期演化轨道的不可预测性 [17–19] 与图像加密系统的密钥敏感性、密文呈噪声特性和明文敏感性等特性相对应, 因此基于混沌系统的图像加密方案受到了极大关注. 2019 年, Jiang 等 [20] 提出一种基于 GQIR (generalized qquantum image representation) 量子图像表示方法和 Henon 混沌映射的量子图像加密方案. 2020 年, Ge 和 Luo[21] 提出了一种结合混沌序列和量子密钥的图像加密方案. 2022 年, Hu 和 Dong[22] 提出了一种基于新型

* 山东省自然科学基金 (批准号: ZR2021MF049)、山东省自然科学基金联合项目 (批准号: ZR2022LLZ012, ZR2021LLZ001)、山东省大学生创新创业训练计划 (批准号: S202210429001) 和青岛理工大学大学生科技创新项目 (批准号: KJCXXM141) 资助的课题.

† 通信作者. E-mail: qiutianhui@qut.edu.cn

三维混沌系统的量子彩色图像加密方案. 2022 年, 刘瀚扬等[23] 提出了一种基于量子随机行走和涉及 Lorenz 和 Rossler 多维混沌的三维图像加密方案.

随着机器学习研究的深入, 已经有学者将机器学习运用到混沌时间序列的预测中. 2018 年, Faqih 等[24] 利用极端学习机制对径向基函数神经网络进行改进, 提升了预测混沌时间序列的精确性. 2020 年, Qu 等[25] 提出了一种深度卷积神经网络, 降低了卷积神经网络在预测混沌时间序列时的误差. 2021 年, Yang 等[26] 提出了一种基于干扰补偿的复合多层神经网络自适应控制算法用以预测混沌时间序列. 2022 年, Li 等[27] 提出了一种基于新型回声状态网络模型, 用来预测混沌时间序列. 同时, 量子信息与神经网络模型优势相结合的量子神经网络正蓬勃发展, 在图像分类[28–30]、图像识别[31] 等方向被广泛应用.

本文利用量子长短期记忆 (quantum long-short term memory, QLSTM) 网络将超混沌 Lorenz 序列进行改进, 通过改进后的序列分别控制三级径向扩散改变灰度值与量子广义 Arnold 变换和量子 W 变换共同改变像素位置, 达到图像加密的效果. 另外, 在 QLSTM 网络线路中添加了线性层, 减少了量子位的数量要求, 实现了任意大的外部状态. 利用 QLSTM 网络改进的序列, 混沌性能更好, 预测难度更大, 因此加密的安全性更高. 经过仿真与理论分析, 本文所提方案不仅具有优良的加密效果, 而且具有较强的安全性, 能够抵抗常见的攻击方式.

本文第 2 节介绍 QLSTM 网络的基本知识, 第 3 节和第 4 节分别介绍具体的加密方案和解密方案, 第 5 介绍对 QLSTM 网络改进的序列的动力系统分析和本文针对检测加密方案效果的仿真与理论分析, 第 6 节是对本文工作的总结, 同时也对后续工作进行了展望.

2 相关工作

2.1 长短期记忆网络

为了改善循环神经网络受梯度消失或爆炸造成的长程依赖问题, 长短期记忆 (long-short term memory, LSTM) 网络被提出[32]. 引入门控机制控制 LSTM 网络中信息的传递路径, 实现信息的遗忘或保留. 通过输入门 I_t、输出门 O_t 和遗忘门 F_t, 结合候选状态 $\tilde{C}_t$, 将内部状态 C_t 的信息传输到外部状态 H_t.

$$\begin{cases} F_t = \sigma(X_t W_{x\mathrm{f}} + H_{t-1} W_{h\mathrm{f}} + b_{\mathrm{f}}), \\ I_t = \sigma(X_t W_{x\mathrm{i}} + H_{t-1} W_{h\mathrm{i}} + b_{\mathrm{i}}), \\ \tilde{C}_t = \tanh(X_t W_{x\mathrm{c}} + H_{t-1} W_{h\mathrm{c}} + b_{\mathrm{c}}), \\ C_t = F_t C_{t-1} + I_t \tilde{C}_t, \\ O_t = \sigma(X_t W_{x\mathrm{o}} + H_{t-1} W_{h\mathrm{o}} + b_{\mathrm{o}}), \\ H_t = O_t \tanh(C_t), \end{cases} \tag{1}$$

其中, X_t 是当前时刻的输入, W 是各个门的权重向量, b 是偏置向量, σ 是 Logistic 函数.

2.2 QLSTM 网络

变分量子线路 (variational quantum circuits, VQC) 是混合量子经典的方法之一, 它利用量子和经典计算的优势, 对噪声具有鲁棒性[33,34], 在深度强化学习[35]、数据分类[36–38] 等各个领域已经被广泛使用. 本文采用 VQC 替换 LSTM 网络循环单元中的门, 代替权重矩阵, 称为 QLSTM 网络, 起到了特征提取和数据压缩的作用, 能够以更少的参数达到比经典更好的效果. VQC 主要由三部分组成, 包括数据编码层、变分层和量子测量层, 通用架构如图 1 所示.

数据编码层由 H 门、R_y 和 R_z 门组成, 主要目的为状态准备. H 门对初始状态进行转化, 通过对每个元素 x_i 取 $\theta_{i,1} = \arctan(x_i)$ 和 $\theta_{i,2} = \arctan(x_i^2)$, $\theta_{i,1}$ 应用于 R_y 门控制 y 轴旋转, $\theta_{i,2}$ 应用于 R_z 门控制 z 轴旋转, 能够将经典数据编码为量子态, 加载到量子线路中.

变分层由多个 CNOT 门和 R 门组成, 主要目的为学习优化. CNOT 门应用于每对具有固定相邻关系的量子位, 得到多量子位纠缠. R 门的 3 个参数为沿 x, y, z 轴的 3 个旋转角 α, β, γ, 最初 3 个参数均无确定的值, 而是通过梯度下降的方法, 不断迭代进行优化. 变分层可以重复叠加, 增加 VQC 的深度, 从而增加变分参数的数量.

VQC 的末端是量子测量层, 主要目的为输出量子态, 测量每个量子比特的期望值.

另外, 本文在线路中引入线性层[39], 能够将任意长度的张量转换成固定长度的张量, 缩短 Q-张量的长度, 使长 Q-张量变为短 Q-张量, 以此压缩输入信息和外部状态数据, 大大减少在 VQC 中所需量子位的数量.

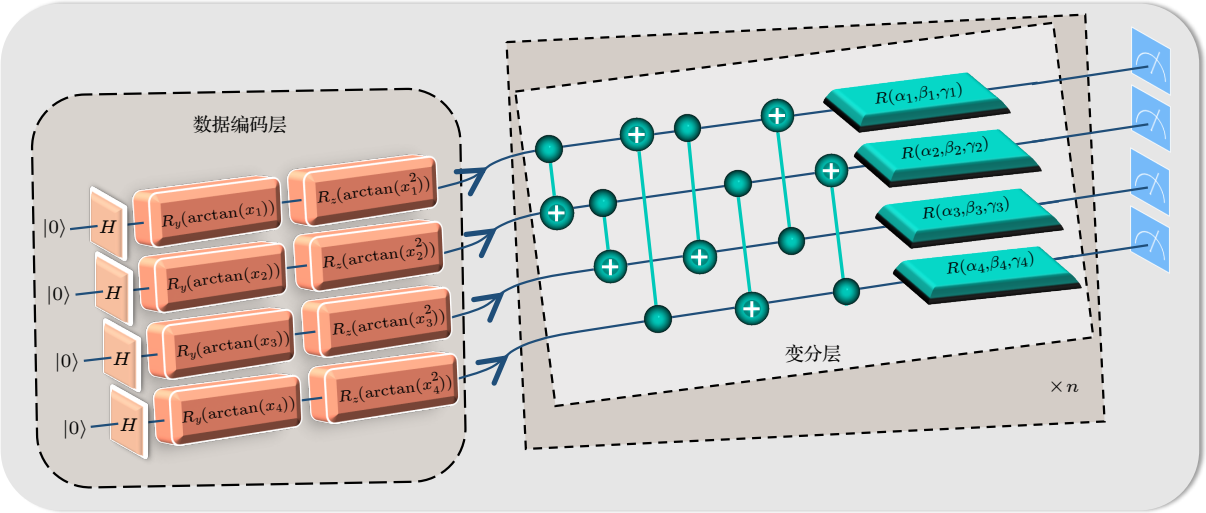

图 1 VQC 的通用架构

Fig. 1. General architecture of VQC.

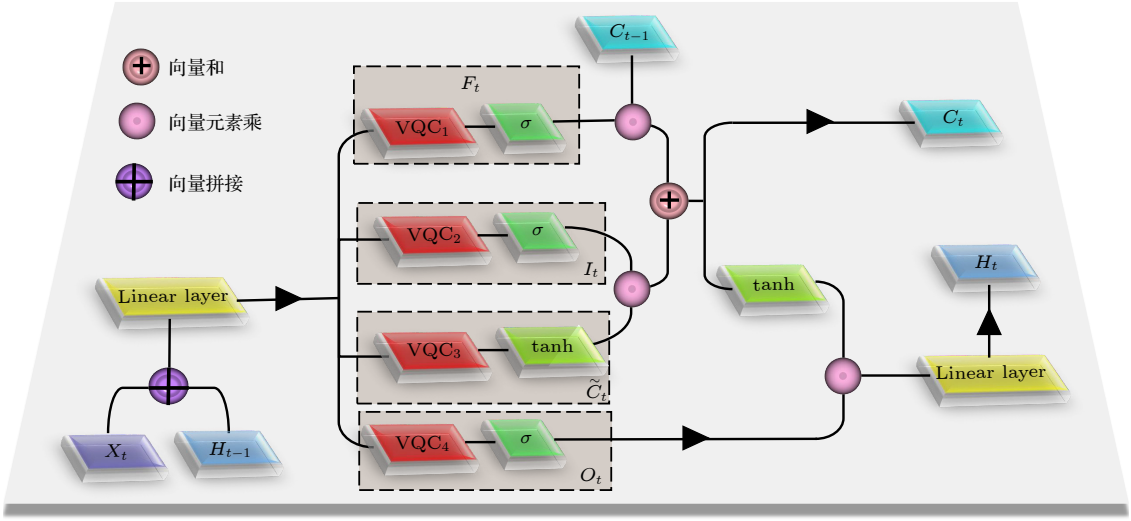

图 2 QLSTM 网络的循环单元结构

Fig. 2. Cyclic cell structure of QLSTM network.

$$\begin{cases} F_t = \sigma(\mathrm{VQC}_1(X_t + H_{t-1})), \\ I_t = \sigma(\mathrm{VQC}_2(X_t + H_{t-1})), \\ \tilde{C}_t = \tanh(\mathrm{VQC}_3(X_t + H_{t-1})), \\ C_t = F_t C_{t-1} + I_t \tilde{C}_t, \\ O_t = \sigma(\mathrm{VQC}_4(X_t + H_{t-1})), \\ H_t = O_t \tanh(C_t). \end{cases} \tag{2}$$

QLSTM 网络的循环单元结构如图 2 所示. 4 个 VQC 的输入均为 X_t 和 H_{t-1}. 根据目的, QLSTM 网络循环单元主要分为 3 个层. 忘记层: 确定遗忘还是保留内部状态的信息. 输出值 F_t 范围为 $[0, 1]$, 1 表示信息被完全保留, 0 表示信息被完全遗忘. 通常情况下, 输出值介于 0 和 1 之间, 表示遗忘部分信息, 并保留部分信息. 输入层和更新层: 确定添加到内部状态的新信息, 对内部状态进行更新. 输出层块: 确定最终输出的信息, 并将内部状态信息传递给外部状态.

3 加密方案

步骤 1 通过 NCQI (novel quantum representation of color digital images) 表示模型, 将原始图像加载为量子图像.

NCQI 模型能够准确获取图像 RGB 通道信息, 将整个彩色图像存储为归一化的量子叠加态[40]. 设大小为 $2^n \times 2^n$ 的彩色图像, NCQI 模型下, 量子

图像$|M\rangle$可以表示为

$$|M\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|C_{\mathrm{RGB}_{yx}}\right\rangle \otimes |yx\rangle, \tag{3}$$

其中, $|yx\rangle = |y\rangle|x\rangle$代表位置信息, $\left|C_{\mathrm{RGB}_{yx}}\right\rangle$代表颜色信息, 每个颜色通道的灰度值为$[0, 2^{m-1}]$, m为颜色通道的颜色深度, 本文所提出的加密方案中$m = 8$.

$$\begin{aligned}&\left|C_{\mathrm{RGB}_{yx}}\right\rangle = |R_{yx}\rangle|G_{yx}\rangle|B_{yx}\rangle\\ =&\left|R_{yx}^{m-1}\cdots R_{yx}^{0}\right\rangle\left|G_{yx}^{m-1}\cdots G_{yx}^{0}\right\rangle\left|B_{yx}^{m-1}\cdots B_{yx}^{0}\right\rangle\\ =&\left|R_{yx}^{7}\cdots R_{yx}^{0}\right\rangle\left|G_{yx}^{7}\cdots G_{yx}^{0}\right\rangle\left|B_{yx}^{7}\cdots B_{yx}^{0}\right\rangle,\end{aligned} \tag{4}$$

其中, $|R_{yx}\rangle$, $|G_{yx}\rangle$和$|B_{yx}\rangle$分别代表红色、绿色和蓝色通道的灰度值.

步骤 2 利用 QLSTM 网络改进混沌序列.

Step1 超混沌 Lorenz 系统是从经典 Lorenz 混沌系统改进并优化而来的, 在原本系统的基础上附加了新的状态变量, 具有更复杂的动态行为和更高的随机性, 能够进一步增强图像加密系统的安全性.

超混沌 Lorenz 系统可表示为

$$\begin{cases}\dot{x} = a(y-x) + w,\\ \dot{y} = cx - y - xz,\\ \dot{z} = xy - bz,\\ \dot{w} = -yz + rw,\end{cases} \tag{5}$$

其中, x, y, z和w为系统的状态变量; a, b, c和r为系统参数.

Step2 设置超混沌 Lorenz 系统的参数与初值, 得到 4 个伪随机序列, 记为$\{l_i\}, i = 1, 2, 3, 4$.

Step3 利用 QLSTM 网络对$\{l_i\}, i = 1, 2, 3, 4$进行改进, 得到新的序列$\{l_i'\}, i = 1, 2, 3, 4$. 本文中 VQC 的变分层数量$n = 4$.

步骤 3 用下列等式, 分别将 4 个序列$\{l_i'\}$, $i = 1, 2, 3, 4$转换成 4 个整数序列$\{L_i\}, i = 1, 2, 3, 4$.

$$\{L_i\} = \mathrm{mod}((l_i' - \mathrm{floor}(l_i')) \times 10^{14}, 256), i = 1, 2, 3, 4, \tag{6}$$

其中, mod 是求余函数, floor 是取整函数.

步骤 4 对量子图像$|M\rangle$进行三级径向扩散, 对灰度值进行变化, 得到量子图像$|M^1\rangle$.

径向扩散是具有径向结构的位级扩散, 共有 3 种类型: 二位扩散、四位扩散和八位扩散, 如图 3 所示. 其中每一层都有八位节点, 将这 3 种类型根据不同的排列顺序, 相互组合, 共能得到 6 种情况.

量子图像中三个通道的像素值均可以使用 8 个量子位表示, 即$|C_{yx}^7C_{yx}^6C_{yx}^5C_{yx}^4C_{yx}^3C_{yx}^2C_{yx}^1C_{yx}^0\rangle$; 同时, 序列中的每个元素也能以八位的形式表示, 即$a_7a_6a_5a_4a_3a_2a_1a_0$. 因此, 将每个像素的值与序列的元素依次进行异或运算, 并交换结果的位置, 得到新的值, 从而改变量子图像的像素值.

以二位、四位和八位径向扩散的规则为例, 三级径向扩散的详细描述如下:

$$\begin{cases}F_{\mathrm{RGB}}^7 = [(C_{\mathrm{RGB}}^2 \oplus L_{1_{i_2}}) \oplus L_{2_{i_3}}] \oplus L_{3_{i_0}},\\ F_{\mathrm{RGB}}^6 = [(C_{\mathrm{RGB}}^3 \oplus L_{1_{i_3}}) \oplus L_{2_{i_2}}] \oplus L_{3_{i_1}},\\ F_{\mathrm{RGB}}^5 = [(C_{\mathrm{RGB}}^0 \oplus L_{1_{i_0}}) \oplus L_{2_{i_1}}] \oplus L_{3_{i_2}},\\ F_{\mathrm{RGB}}^4 = [(C_{\mathrm{RGB}}^1 \oplus L_{1_{i_1}}) \oplus L_{2_{i_0}}] \oplus L_{3_{i_3}},\\ F_{\mathrm{RGB}}^3 = [(C_{\mathrm{RGB}}^6 \oplus L_{1_{i_6}}) \oplus L_{2_{i_7}}] \oplus L_{3_{i_4}},\\ F_{\mathrm{RGB}}^2 = [(C_{\mathrm{RGB}}^7 \oplus L_{1_{i_7}}) \oplus L_{2_{i_6}}] \oplus L_{3_{i_5}},\\ F_{\mathrm{RGB}}^1 = [(C_{\mathrm{RGB}}^4 \oplus L_{1_{i_4}}) \oplus L_{2_{i_5}}] \oplus L_{3_{i_6}},\\ F_{\mathrm{RGB}}^0 = [(C_{\mathrm{RGB}}^5 \oplus L_{1_{i_5}}) \oplus L_{2_{i_4}}] \oplus L_{3_{i_7}},\end{cases} \tag{7}$$

其中, $L_{1_{i_j}}, L_{2_{i_j}}, L_{3_{i_j}}$ $(j = 7, 6, \cdots, 0)$表示序列$\{L_1\}$, $\{L_2\}$, $\{L_3\}$的第i个数的第j位.

序列$\{L_1\}$, $\{L_2\}$, $\{L_3\}$作为异或运算中的元素, $\{L_4\}$决定排列顺序. 径向扩散包括 3 种不同的类型, 根据不同的排列顺序, 将二位、四位、八位径向扩散相互组合, 共有 6 种情况, 由序列$\{L_4\}$决定三级径向扩散的规则, 规则如下:

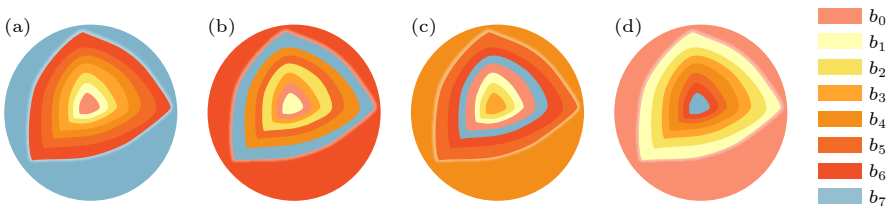

图 3 径向扩散 (a) 原序列; (b) 二位径向扩散; (c) 四位径向扩散; (d) 八位径向扩散

Fig. 3. Radial diffusion: (a) Original sequence; (b) two-position radial diffusion; (c) four-position radial diffusion; (d) eight-position radial diffusion.

1) 如果 $L_{4_i} \bmod 6 = 0$, 第一、第二和第三级分别是二位、四位和八位径向扩散; 2) 如果 $L_{4_i} \bmod 6 = 1$, 第一、第二和第三级分别是二位、八位和四位径向扩散; 3) 如果 $L_{4_i} \bmod 6 = 2$, 第一、第二和第三级分别是四位、二位和八位径向扩散; 4) 如果 $L_{4_i} \bmod 6 = 3$, 第一、第二和第三级分别是四位、八位和二位径向扩散; 5) 如果 $L_{4_i} \bmod 6 = 4$, 第一、第二和第三级分别是八位、二位和四位径向扩散; 6) 如果 $L_{4_i} \bmod 6 = 5$, 第一、第二和第三级分别是八位、四位和二位径向扩散. 其中, L_{4_i}是第 4 个序列$\{L_4\}$的第 i 个数.

经过三级径向扩散后的量子图像$|M^1\rangle$为

$$|M^1\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle \otimes |yx\rangle. \tag{8}$$

步骤 5 对$|M^1\rangle$进行量子广义 Arnold 变换或量子 W 变换, 改变像素位置, 得到最终的加密图像$|M^2\rangle$.

量子广义 Arnold 变换的公式为

$$\begin{cases} |x'\rangle = |(x+my) \bmod 2^n\rangle, \\ |y'\rangle = |[ux+(mu+1)y] \bmod 2^n\rangle, \end{cases} \tag{9}$$

其中, (x,y)是原始图像的坐标位置; (x',y')是变换后图像的坐标位置; m,u是变换系数.

量子 W 变换[41] 的公式为

$$\begin{cases} |x'\rangle = |(2x+y+e) \bmod 2^n\rangle, \\ |y'\rangle = |(3x+y+f) \bmod 2^n\rangle, \end{cases} \tag{10}$$

其中, e,f是平移系数.

序列$\{L_1\}$控制变换的方式, $\{L_2\},\{L_3\}$决定量子 Arnold 变换系数m,u或量子 W 变换平移系数e,f, $\{L_4\}$控制变换的迭代次数.

由序列$\{L_1\}$决定使用像素位置的变换方式, 规则如下: 1) 如果 $L_{1_i} \bmod 2 = 0$, 对$|M^1\rangle$进行量子广义 Arnold 变换; 2) 如果 $L_{1_i} \bmod 2 = 1$, 对$|M^1\rangle$进行量子 W 变换. 其中, L_{1_i}是第一个序列$\{L_1\}$的第 i 个数.

量子广义 Arnold 变换的详细描述如下:

$$\begin{aligned} A^{L_4}|M^1\rangle &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle A^{L_4}|yx\rangle \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle \prod_{j\in Z}A^{L_{4_j}}|y\rangle \prod_{j\in Z}A^{L_{4_j}}|x\rangle \\ &= \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle |y'x'\rangle = |M^2\rangle. \end{aligned} \tag{11}$$

量子 W 变换的详细描述如下:

$$\begin{aligned} W^{L_4}|M^1\rangle &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle W^{L_4}|yx\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle \prod_{j\in Z}W^{L_{4_j}}|y\rangle \prod_{j\in Z}W^{L_{4_j}}|x\rangle \\ &= \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle |y'x'\rangle = |M^2\rangle. \end{aligned} \tag{12}$$

4 解密方案

解密过程是加密过程的逆操作, 具体步骤如下:

步骤 1 根据上述加密方案, 得到 4 个整数序列$\{L_i\}, i=1,2,3,4$.

步骤 2 对加密图像$|M^2\rangle$进行量子广义 Arnold逆变换或量子 W 逆变换, 得到$|M^1\rangle$. 序列$\{L_1\}$控制变换的方式, 与加密方案中规则相同, $\{L_2\},\{L_3\}$决定相关系数, $\{L_4\}$控制迭代次数.

量子广义 Arnold 逆变换的详细描述如下:

$$\begin{aligned} A^{-L_4}|M^2\rangle &= \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle A^{-L_4}|y'x'\rangle = \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle \prod_{j\in Z}A^{L_{4_j}}|y'\rangle \prod_{j\in Z}A^{L_{4_j}}|x'\rangle \\ &= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|F_{\mathrm{RGB}_{yx}}\rangle |yx\rangle = |M^1\rangle, \end{aligned} \tag{13}$$

其中, $|x\rangle = |[(mu+1)x' - my'] \bmod 2^n\rangle$, 以及 $|y\rangle = |(-ux'+y') \bmod 2^n\rangle$.

量子 W 逆变换的详细描述如下:

$$W^{-L_4}\left|M^2\right\rangle = \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle W^{-L_4}\left|y'x'\right\rangle$$

$$= \frac{1}{2^n}\sum_{y'=0}^{2^n-1}\sum_{x'=0}^{2^n-1}\left|F_{\mathrm{RGB}_{y'x'}}\right\rangle \prod_{j\in Z} W^{-L_{4_j}}\left|y'\right\rangle \prod_{j\in Z} W^{-L_{4_j}}\left|x'\right\rangle$$

$$= \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left|F_{\mathrm{RGB}_{yx}}\right\rangle\left|yx\right\rangle = \left|M^1\right\rangle, \tag{14}$$

其中, $|x\rangle = |[(e-x')+(y'-f)] \bmod 2^n\rangle$, $|y\rangle = |[3(x'-e) \bmod 2^n + 2(f-y') \bmod 2^n] \bmod 2^n\rangle$.

步骤 3 对$|M^2\rangle$进行三级逆径向扩散, 得到原图$|M\rangle$.

首先由$\{L_4\}$决定三级逆径向扩散的规则, 其与加密方案中规则相反, 具体如下:

1) 如果 $L_{4_i} \bmod 6 = 0$, 第一、第二和第三级分别是八位、四位和二位径向扩散; 2) 如果 $L_{4_i} \bmod 6 = 1$, 第一、第二和第三级分别是四位、八位和二位径向扩散; 3) 如果 $L_{4_i} \bmod 6 = 2$, 第一、第二和第三级分别是八位、二位和四位径向扩散; 4) 如果 $L_{4_i} \bmod 6 = 3$, 第一、第二和第三级分别是二位、八位和四位径向扩散; 5) 如果 $L_{4_i} \bmod 6 = 4$, 第一、第二和第三级分别是四位、二位和八位径向扩散; 6) 如果 $L_{4_i} \bmod 6 = 5$, 第一、第二和第三级分别是二位、四位和八位径向扩散.

$\{L_3\}, \{L_2\}, \{L_1\}$作为异或运算中的元素参与解密, 以八位、四位和二位径向扩散的规则为例, 三级逆径向扩散的详细描述如下:

$$\begin{cases} C^7_{\mathrm{RGB}} = [(F^2_{\mathrm{RGB}} \oplus L_{3_{i_2}}) \oplus L_{2_{i_5}}] \oplus L_{1_{i_6}}, \\ C^6_{\mathrm{RGB}} = [(F^3_{\mathrm{RGB}} \oplus L_{3_{i_3}}) \oplus L_{2_{i_4}}] \oplus L_{1_{i_7}}, \\ C^5_{\mathrm{RGB}} = [(F^0_{\mathrm{RGB}} \oplus L_{3_{i_0}}) \oplus L_{2_{i_7}}] \oplus L_{1_{i_4}}, \\ C^4_{\mathrm{RGB}} = [(F^1_{\mathrm{RGB}} \oplus L_{3_{i_1}}) \oplus L_{2_{i_6}}] \oplus L_{1_{i_5}}, \\ C^3_{\mathrm{RGB}} = [(F^6_{\mathrm{RGB}} \oplus L_{3_{i_6}}) \oplus L_{2_{i_1}}] \oplus L_{1_{i_2}}, \\ C^2_{\mathrm{RGB}} = [(F^7_{\mathrm{RGB}} \oplus L_{3_{i_7}}) \oplus L_{2_{i_0}}] \oplus L_{1_{i_3}}, \\ C^1_{\mathrm{RGB}} = [(F^4_{\mathrm{RGB}} \oplus L_{3_{i_4}}) \oplus L_{2_{i_3}}] \oplus L_{1_{i_0}}, \\ C^0_{\mathrm{RGB}} = [(F^5_{\mathrm{RGB}} \oplus L_{3_{i_5}}) \oplus L_{2_{i_2}}] \oplus L_{1_{i_1}}. \end{cases} \tag{15}$$

5 实验仿真

由于缺乏量子计算机, 我们在配备经典计算机的 MATLAB 和 Python 环境中进行模拟实验. 数值处理中, 不考虑量子版本中退相干和误差的影响.

5.1 动力系统分析

5.1.1 最大 Lyapunov 指数分析

Lyapunov 指数可以反映系统的动态行为, 并分析动态系统是否是混沌系统. 当系统处于混沌状态时, Lyapunov 指数大于 0, 指数越大, 混沌特征越显著. 最大 Lyapunov 指数 (largest lyapunov exponent, LLE) 是判断和描述时间序列是否具有混沌特性的重要参数之一[42].

设序列$\{S(k)\}$的 d 维相空间为

$$S(k) = \{S(k), S(k+t), \cdots, S(k+(d-1)t)\}, \tag{16}$$

其中, t 为延迟时间.

选取 $S(k_0)$, $S(k_0)$与最近邻点 $s(k_0)$的距离为 $D(k_0)$, 从 k_0时刻到 k_1时刻, 直到两点之间距离大于规定值ε $(\varepsilon > 0)$:

$$D'(k_1) = |S(k_1) - s(k_1)| > \varepsilon. \tag{17}$$

寻找 $S(k_1)$的最近邻点 $s(k_0)$, 使

$$D(k_1) = |S(k_1) - s(k_1)| < \varepsilon. \tag{18}$$

$D'(k_1)$与$D(k_1)$之间的夹角最小时, 重复 (17) 式和 (18) 式, 直到包含所有点, 则 LLE 为

$$\lambda = \frac{1}{k_N - k_0}\sum_{i=1}^{N}\log_2\frac{D'(k_i)}{D(k_{i-1})}, \tag{19}$$

其中, N 为迭代次数.

为了检验 QLSTM 网络改进的序列是否具有混沌特性, 计算得到序列的 LLE. 实验仿真结果如图 4 所示, 具体数据见表 1. 序列的 LLE 均大于 0, 且超过原序列与 LSTM网络改进的序列, 因此 QLSTM 网络改进的序列混沌性能更好.

表 1 LLE 数据对比

Table 1. Comparison of LLE data.

序列来源	LLE
Henon映射	0.4192
超混沌Lorenz系统	0.3381
LSTM网络改进的序列[43]	2.6002
QLSTM网络改进的序列	2.8846

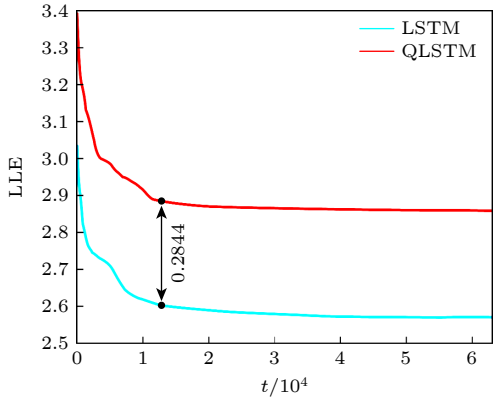

图 4 LSTM 网络和 QLSTM 网络改进的序列的 LLE 曲线

Fig. 4. Largest Lyapunov exponent curves for sequences improved by LSTM network or QLSTM network.

5.1.2 0—1 测试

0—1 测试是一种二进制检测方法, 用于验证时间序列是否混沌[44]. 对于 $\{S(k), k=1,2,\cdots,N\}$, 定义函数 $p(n)$ 和 $q(n)$:

$$\begin{cases} p(n)=\sum\limits_{i=1}^{n} S(k)\cos(\mu(k)), \\ q(n)=\sum\limits_{i=1}^{n} S(k)\sin(\mu(k)), \end{cases} \quad k=1,2,\cdots,N, \tag{20}$$

其中, $\mu(k)=kr, k=1,2,\cdots,n, r\in[0,\pi]$.

$p(n)$ 和 $q(n)$ 的均方位移 $M(n)$ 为

$$M(n)=M_r(n)-E^2\frac{1-\cos(nr)}{1-\cos r}, \tag{21}$$

其中, $M_r(n)=\lim\limits_{n\to\infty}\sum\limits_{i=1}^{N}\left[(p(k+n)-p(k))^2+(q(k+n)-q(k))^2\right]$, $E=\lim\limits_{N\to\infty}\dfrac{1}{N}\sum\limits_{i=1}^{N}S(k)$.

均方位移 $M(n)$ 的渐进线性增长率 $K_{\rm r}$ 为

$$K_{\rm r}=\lim_{n\to\infty}\lg M(n)/\lg n. \tag{22}$$

当 $K_{\rm r}\approx 0$ 时, 序列是非混沌的; 当 $K_{\rm r}\approx 1$ 时, 序列具有混沌性.

表 2 0—1 测试的数据对比

Table 2. Comparison of from 0–1 test data.

序列来源	0—1测试
Henon映射[45]	0.6173
超混沌Lorenz系统	0.7937
LSTM网络改进的序列[43]	0.9218
QLSTM网络改进的序列	0.9572

图 5 给出了 QLSTM 网络改进的序列的 0—1 测试结果, 具体数据见表 2, 与 Lorenz 混沌序列和 LSTM 网络改进的序列比较, QLSTM 网络改进的序列的 0—1测试的结果更接近 1, 且更稳定. 因此, QLSTM 网络改进的序列混沌性能更好.

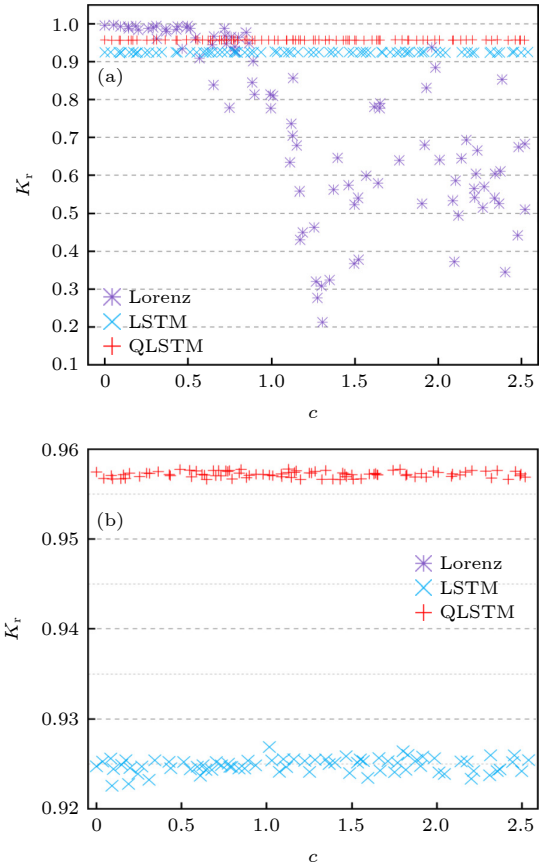

图 5 Lorenz 混沌序列、LSTM 网络和 QLSTM 网络改进的序列的 0—1 测试图

Fig. 5. 0–1 test images for Lorenz chaotic sequences and sequences improved by LSTM network or QLSTM network.

5.2 安全性分析

本节以像素大小为 512×512 的 3 幅彩色图像作为原始图像对加密数据进行分析. 加密和解密的仿真结果如图 6 所示.

5.2.1 相邻像素的相关性分析

相邻像素包括水平相邻像素、垂直相邻像素和对角相邻像素. 相邻像素的相关性是判断加密方案优劣的重要依据之一. 原图的相邻像素的相关性很强, 而经过加密方案后, 加密图像的相邻像素的相关性应趋近于 0. A 和 B 分别表示相邻像素的值, 其协方差和方差为

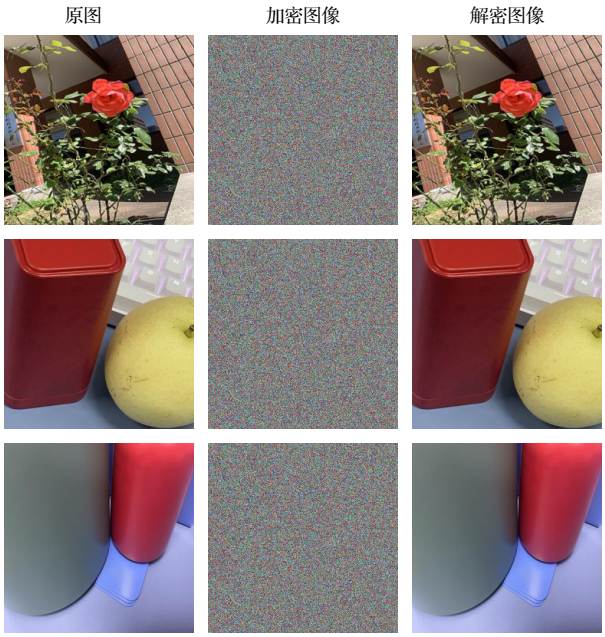

图 6 加密和解密的效果图

Fig. 6. Effect of encryption and decryption.

$$\begin{cases} \mathrm{cov}(A,B)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}(A_i-E(A))(B_i-E(B)), \\ V(A)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(A_i-\dfrac{1}{N}\sum_{i=1}^{N}A_i\right)^2, \\ V(B)=\dfrac{1}{N}\displaystyle\sum_{i=1}^{N}\left(B_i-\dfrac{1}{N}\sum_{i=1}^{N}B_i\right)^2. \end{cases} \tag{23}$$

相邻像素的相关性[46]为

$$r=\frac{\mathrm{cov}(A,B)}{\sqrt{V(A)}\sqrt{V(B)}}. \tag{24}$$

结果如图 7 所示, 具体数据见表 3. 在 3 个方向上原图的相关性都很高, 经过本文算法加密后, 加密图像的 3 个方向上相关性都接近于 0. 因此该算法能够抵抗统计攻击, 攻击者难以得到加密图像的分布特性.

表 3 加密图像的相关性分析

Table 3. Pixel correlation analysis of encrypted images.

图像	通道	水平	垂直	对角
1	R	0.0074	0.0031	0.0064
	G	0.0039	0.0021	0.0019
	B	0.0044	0.0013	0.0058
2	R	0.0006	0.0067	0.0026
	G	0.0017	0.0049	0.0047
	B	0.0057	0.0006	0.0069
3	R	0.0003	0.0052	0.0013
	G	0.0035	0.0005	0.0042
	B	0.0090	0.0029	0.0045

5.2.2 直方图分析

直方图反映的是像素的统计信息和分布情况. 原图的直方图具有一定的规律, 易受到统计分析攻击. 因此, 加密图像的直方图应是均匀的, 直方图越均匀, 加密方案的安全性越高, 抵抗统计分析攻击的能力越强[47].

图 8 给出了原图与加密图像的 RGB 通道直方图. 明显能够发现, 原图中直方图分布不均匀, 经过本文的加密算法后, 加密图像的直方图分布变得均匀. 因此该算法具有很好的抵抗统计攻击的能力, 攻击者无法通过分析密文图像, 得到规律破解算法.

5.2.3 信息熵

熵表示事物的混乱程度, 信息熵是衡量密文图像分布的随机性的度量方式. 信息熵的值越接近 8, 图像的像素值越混乱, 抵抗统计攻击能力越强[48]. 信息熵的定义式为

$$H(o)=\sum_{i=0}^{N-1}p(o_i)\log_2\frac{1}{p(o_i)}, \tag{25}$$

其中, $p(o_i)$表示 o_i 发生的概率. 具体结果如表 4 所列, RGB 三通道的平均信息熵均接近 8, 表示加密图像的像素分布均匀, 攻击者不能从密文中找到有效信息, 因此本文提出的算法具有很好的安全性.

5.2.4 秘钥敏感性分析

秘钥敏感性是在秘钥有微小变化的情况下, 经加密方案后, 加密图像会产生巨大的变化. 像素数改变率 (number of pixels change rate, NPCR) 和统一平均变化强度 (unified average changing intensity, UACI) 的理想值分别为 99.6094% 和 33.4635%. 数值越接近理想值, 密钥敏感性越强, 抵抗差分攻击的能力越强, 加密算法的安全性越高.

本文算法加密后的 NPCR 和 UACI 数据如表 5 所列, NPCR 与 UACI 均接近理想值, 因此本文提出的加密算法具有很好的抵抗差分攻击的能力.

将本文所提加密方案与文献 [43] 中的加密方案从平均 NPCR 和 UACI 的角度进行对比分析, 得到的数据见表 6.

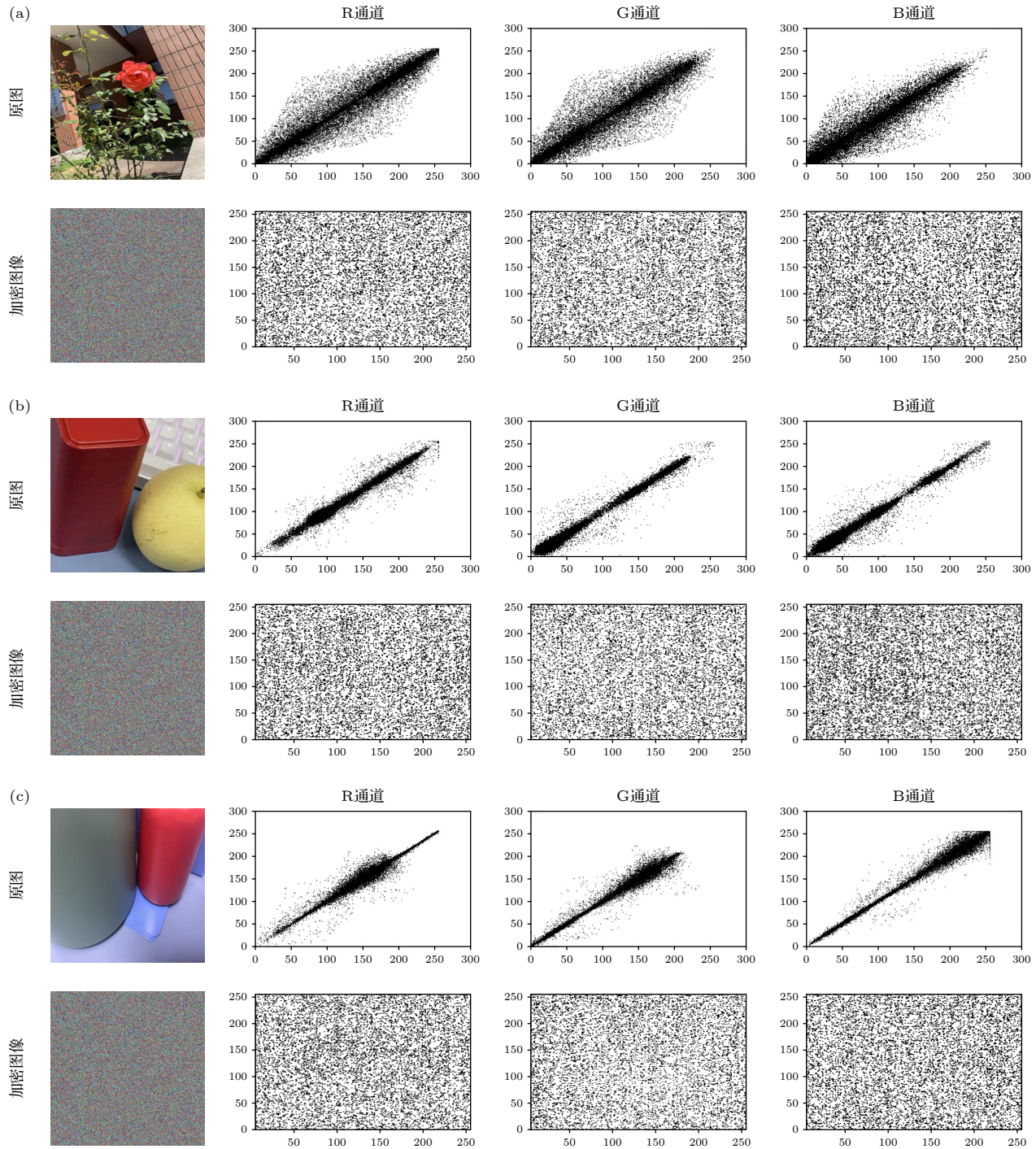

图 7 加密前后相关性分析对比图

Fig. 7. Comparison of pixel correlation analysis before and after encryption.

表 4 加密图像的信息熵

Table 4. Information entropy of encrypted images.

图像	R	G	B
1	7.99928	7.99973	7.99951
2	7.99935	7.99908	7.99975
3	7.99912	7.99949	7.99921

表 5 加密图像的 NPCR 与 UACI

Table 5. NPCR and UACI of encrypted images.

图像	NPCR	UACI
1	99.6048%	33.4604%
2	99.6063%	33.4609%
3	99.6029%	33.4627%

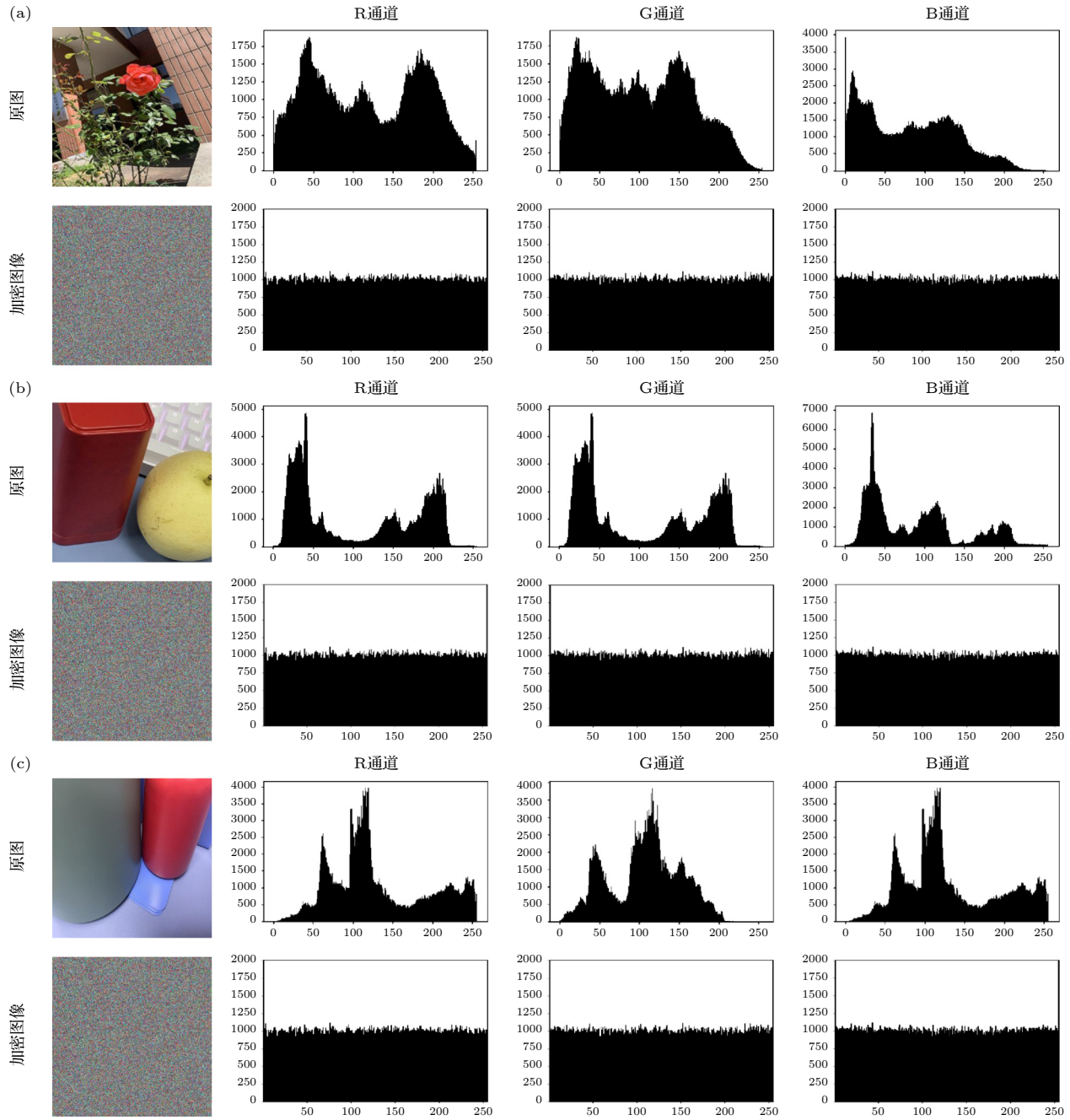

图 8 加密前后直方图分析对比图

Fig. 8. Comparison of histogram analysis before and after encryption.

表 6 NPCR 与 UACI 的对比分析

Table 6. Comparison of NPCR and UACI.

算法	平均NPCR	平均UACI
本文	99.6047%	33.4613%
文献[43]	99.604%	33.46%

6 结 论

本文提出了一种基于 QLSTM 网络的量子图像混沌加密方案, 利用 QLSTM 网络改进超混沌 Lorenz 系统产生的序列, 通过改进后的序列控制三级径向扩散、广义 Arnold 变换和量子 W 变换, 生成加密图像, 达到加密效果. QLSTM 网络具有复杂的结构和较多的参数, 并且通过 QLSTM 网络改进的序列具有更好的混沌性, 这给破解带来了很大的难度, 提高了算法安全性. 在 QLSTM 网络循环单元中添加线性层, 减少了量子位的数量要求, 提高效率. 利用复杂度低的 NCQI 表示模型, 将原始图像编码为量子图像, 使得后续的量子操作更加

准确. 三级径向扩散改变灰度值, 其每级结果与前一级有关, 同时量子广义 Arnold 变换和量子 W 变换共同改变像素位置, 增大了破译难度. 结合理论分析和仿真表明, 平均 NPCR = 99.6047%, 平均 UACI = 33.4613%, 平均相关性为 0.0038, 平均信息熵大于 7.999, 因此本文的方案是可行的, 具有更好的安全性, 能抵抗常见的攻击. 并且本文表明了将量子机器学习算法应用到量子图像加密领域的前景十分广阔, 在之后的研究工作中希望将其优势更好地发挥与利用.

参考文献

[1] Shakir H R, Mehdi S A A, Hattab A A 2022 *Bull. Electr. Eng. Inform.* **11** 2645

[2] Wang Y N, Song Z Y, Ma Y L, Hua N, Ma H Y 2021 *Acta Phys. Sin.* **70** 230302 (in Chinese) [王一诺, 宋昭阳, 马玉林, 华南, 马鸿洋 2021 物理学报 **70** 230302]

[3] Liu G Z, Li W, Fan X K, Li Z, Wang Y X, Ma H Y 2022 *Entropy* **24** 608

[4] Zhao J B, Zhang T, Jiang J W, Fang T, Ma H Y 2022 *Sci. Rep.* **12** 14253

[5] Li C Q, Lin D D, Lu J H 2017 *IEEE MultiMedia* **24** 64

[6] Li C M, Yang X Z 2022 *Optik* **260** 169042

[7] Xian Y J, Wang X Y 2021 *Inf. Sci.* **547** 1154

[8] Zhou N R, Hu Y Q, Gong L H, Li G Y 2017 *Quantum Inf. Process.* **16** 164

[9] Liu H, Zhao B, Huang L Q 2019 *Entropy* **21** 343

[10] Song X H, Wang S, Abd El-Latif A A, Niu X M 2014 *Quantum Inf. Process.* **13** 1765

[11] Akhshani A, Akhavan A, Lim S C, Hassan Z 2012 *Commun. Nonlinear Sci. Numer. Simul.* **17** 4653

[12] Zhou N R, Huang L X, Gong L H, Zeng Q W 2020 *Quantum Inf. Process.* **19** 284

[13] Wang X Y, Su Y I, Luo C, Nian F Z, Teng L 2022 *Multimedea Tools Appl.* **81** 13845

[14] Gao Y J, Xie H W, Zhang J, Zhang H 2022 *Physia A* **598** 127334

[15] Liu X B, Xiao D, Liu C 2021 *Quantum Inf. Process.* **20** 23

[16] Jiang J W, Zhang T, Li W, Wang S M 2023 *Quantum Eng.* **2023** 3746357

[17] Zhao J F, Wang S Y, Chang Y X, Li X F 2015 *Nonlinear Dyn.* **80** 1721

[18] Chai X L, Fu J Y, Zhang J T, Han D J, Gan Z H 2021 *Neural. Comput. Appl.* **33** 10371

[19] Chai X L, Gan Z H, Yuan K, Lu Y, Chen Y R 2017 *Chin. Phys. B* **26** 020504

[20] Jiang N, Dong X, Hu H, Ji Z X, Zhang W Y 2019 *Int. J. Theor. Phys.* **58** 979

[21] Ge B, Luo H B 2020 *Int. J. Autom. Comput.* **17** 123

[22] Hu W B, Dong Y M 2022 *J. Appl. Phys.* **131** 114402

[23] Liu H Y, Hua N, Wang Y N, Liang J Q, Ma H Y 2022 *Acta Phys. Sin.* **71** 170303 (in Chinese) [刘瀚扬, 华南, 王一诺, 梁俊卿, 马鸿洋 2022 物理学报 **71** 170303]

[24] Faqih A, Kamanditya B, Kusumoputro B 2018 *International Conference on Computer, Information and Telecommunication Systems* (Alsace: IEEE) p1

[25] Qu J Y, Zhao T, Ye M, Li J Y, Liu C 2020 *Neural Process. Lett.* **52** 1461

[26] Yang G C, Zhu T, Wang H, Yang F B 2021 *IEEE Trans. Circuits Syst. Express Briefs* **69** 1487

[27] Li Y T, Li Y 2022 *Neurocomputing* **491** 321

[28] Li W, Chu P C, Liu G Z, Tian Y B, Qiu T H, Wang S M 2022 *Quantum Eng.* **2022** 5701479

[29] Chen G M, Long S, Yuan Z D, Li W Y, Peng J F 2023 *Quantum Eng.* **2023** 2842217

[30] Zhang Y, Ni Q 2021 *Quantum Eng.* **3** e75

[31] Wei S J, Chen Y H, Zhou Z R, Long G L 2022 *AAPPS Bulletin* **32** 2

[32] Hochreiter S, Schmidhuber J 1997 *Neural Comput.* **9** 1735

[33] Kandala A, Mezzacapo A, Temme K, Takita M, Brink M, Chow J M, Gambetta J M 2017 *Nature* **549** 242

[34] McClean J R, Romero J, Babbush R, Aspuru-Guzik A 2016 *New J. Phys.* **18** 023023

[35] Chen S Y C, Yang C H H, Qi J, Chen P Y, Ma X L, Goan H S 2020 *IEEE Access* **8** 141007

[36] Schuld M, Bocharov A, Svore K M, Wiebe N 2020 *Phys. Rev. A* **101** 032308

[37] Benedetti M, Lloyd E, Sack S, Fiorentini M 2019 *Quantum Sci. Technol.* **4** 043001

[38] Havlicek V, Corcoles A D, Temme K, Harrow A W, Kandala A, Chow J M, Gambetta J M 2019 *Nature* **567** 209

[39] Di Sipio R, Huang J H, Chen S Y C, Mangini S, Worring M 2022 *ICASSP 2022–2022 IEEE International Conference on Acoustics, Speech and Signal Processing* (Singapore: IEEE) p8612

[40] Sang J Z, Wang S, Li Q 2017 *Quantum Inf. Process.* **16** 42

[41] Wu Y L 2008 *Electron. Sci.* **21** 69

[42] Wolf A, Swift J B, Swinney H L, Vastano J A 1985 *Phys. D: Nonlinear Phenomena* **16** 285

[43] Zhao Z P, Zhou S, Wang X Y 2021 *Acta Phys. Sin.* **70** 230502 (in Chinese) [赵智鹏, 周双, 王兴元 2021 物理学报 **70** 230502]

[44] Gottwald G A, Melbourne I 2004 *Proc. R. Soc. London, Ser. A* **460** 603

[45] Sun K H, Liu X, Zhu C X 2010 *Chin. Phys. B* **19** 110510

[46] Boriga R, Dascalescu A C, Priescu I 2014 *Signal Process. Image Commun.* **29** 887

[47] Raja S S, Mohan V 2014 *Int. J. Adv. Eng. Res.* **8** 1

[48] Yang Y G, Tian J, Lei H, Zhou Y H, Shi W M 2016 *Inf. Sci.* **345** 257

Quantum image chaos encryption scheme based on quantum long-short term memory network*

Wang Wei-Jie Jiang Mei-Mei Wang Shu-Mei
Qu Ying-Jie Ma Hong-Yang Qiu Tian-Hui †

(*School of Science*, *Qingdao University of Technology*, *Qingdao* 266520, *China*)

(Received 20 February 2023; revised manuscript received 11 April 2023)

Abstract

In recent years, the transmission security of image information has become an important research direction in the internet field. In this work, we propose a quantum image chaos encryption scheme based on quantum long-short term memory (QLSTM) network. We find that because the QLSTM network has a complex structure and more parameters, when the QLSTM network is used to improve the Lorenz chaotic sequence, its largest Lyapunov exponent is 2.5465% higher than that of the original sequence and 0.2844% higher than that the sequence improved by the classical long-short term memory (LSTM) network, while its result is closer to 1 and more stable in the 0–1 test. The improved sequence of QLSTM network has better chaotic performance and is predicted more difficultly, which improves the security of single chaotic system encryption. The original image is stored in the form of quantum states by using the NCQI quantum image representation model, and the improved sequence of QLSTM network is used to control the three-level radial diffusion, quantum generalized Arnold transform and quantum W-transform respectively, so that the gray value and pixel position of the quantum image are changed and the final encrypted image is obtained. The encryption scheme proposed in this work obtains the average information entropy of all three channels of RGB of greater than 7.999, the average value of pixel number change rate of 99.6047%, the average value of uniform average change intensity of 33.4613%, the average correlation of 0.0038, etc. In the test of statistical properties, the encryption scheme has higher security than some other traditional methods and can resist the common attacks.

Keywords: quantum image encryption, quantum long-short term memory network, chaotic systems

PACS: 03.65.–w, 03.67.Ac, 05.45.Gg **DOI:** 10.7498/aps.72.20230242

* Project supported by the Natural Science Foundation of Shandong Province, China (Grant No. ZR2021MF049), the Joint Fund of Natural Science Foundation of Shandong Province, China (Grant Nos. ZR2022LLZ012, ZR2021LLZ001), the Innovation and Entrepreneurship Training Program for College Students of Shandong Province, China (Grant No. S202210429001), and the Scientific and Technological Innovation Project for College Students of Qingdao University of Technology, China (Grant No. KJCXXM141).

† Corresponding author. E-mail: qiutianhui@qut.edu.cn

物理学报 Acta Physica Sinica

Chinese Physical Society

Institute of Physics, CAS

基于量子长短期记忆网络的量子图像混沌加密方案

王伟杰 姜美美 王淑梅 曲英杰 马鸿洋 邱田会

Quantum image chaos encryption scheme based on quantum long-short term memory network

Wang Wei-Jie Jiang Mei-Mei Wang Shu-Mei Qu Ying-Jie Ma Hong-Yang Qiu Tian-Hui

引用信息 Citation: Acta Physica Sinica, 72, 120301 (2023) DOI: 10.7498/aps.72.20230242

在线阅读 View online: https://doi.org/10.7498/aps.72.20230242

当期内容 View table of contents: http://wulixb.iphy.ac.cn
