Computer Science and Application 计算机科学与应用, 2023, 13(11), 2097-2108
Published Online November 2023 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2023.1311209

Hans汉斯

基于祖冲之序列的量子图像加密算法

李亚晴，王骞卉，张　朝，李祯祯*

北京印刷学院信息工程学院，北京

收稿日期：2023年10月17日；录用日期：2023年11月16日；发布日期：2023年11月23日

摘　要

近年来，数字图像信息泄露事件时有发生，因此，确保数字图像信息传输的安全性日益凸显。为提高图像的加密强度，首先，本文利用祖冲之序列密码算法，设计分组链接模式对彩色图像进行加密。接着，使用量子Arnold置乱算法对祖冲之序列加密算法生成的密文图像进行进一步的置乱处理。最后，得到最终的密文图像。实验结果表明，经过这一系列的加密步骤后，图像中相邻像素之间的相关性被明显减弱，说明该方法显著增强了图像的置乱效果，大幅度地改变了像素灰度的统计特性。此外，本文进行了经典计算机仿真模拟，验证了所提方案的有效性；通过分析直方图和信息熵，表明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，量子图像置乱

Quantum Image Encryption Algorithm Based on ZUC

Yajing Li, Qianhui Wang, Zhao Zhang, Zhenzhen Li*

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

Received: Oct. 17th, 2023; accepted: Nov. 16th, 2023; published: Nov. 23rd, 2023

Abstract

In recent years, the leakage of digital image information has occurred frequently, therefore, ensuring the security of digital image information transmission has become increasingly prominent. In order to improve the encryption strength of images, firstly, this article uses the ZUC sequence cipher algorithm to design a group link mode for encrypting color images. Next, the cipher text image generated by ZUC sequence encryption algorithm is further scrambled using quantum Arnold scrambling algorithm. Finally, the final cipher text image is obtained. The experimental re-

*通讯作者。

文章引用: 李亚晴, 王骞卉, 张朝, 李祯祯. 基于祖冲之序列的量子图像加密算法[J]. 计算机科学与应用, 2023, 13(11): 2097-2108. DOI: 10.12677/csa.2023.1311209

sults show that after a series of encryption steps, the correlation between neighboring pixels in the image is significantly weakened, indicating that this method significantly enhances the scrambling effect of the image and significantly changes the statistical characteristics of pixel grayscale. In addition, this article conducted classic computer simulation to verify the effectiveness of the proposed scheme; by analyzing the histogram and information entropy, it is shown that this scheme has high security.

Keywords

Quantum Image Representation, Quantum Image Processing, Quantum Image Scrambling

1. 引言

随着网络技术的飞速发展，以及信息通讯技术的飞速发展，多媒体数据的传输已成为现代社会不可或缺的一部分。图像作为一种重要信息载体具有很多优点[1]，但也存在一些缺点。图像的可编辑性和真实性都可能导致其被篡改，伪造或者失真，降低了图像的可靠性；其次，图像中可以隐藏消息或数据，这可能导致潜在的安全隐患和隐私问题。因此，人们在使用图像作为信息载体时需要注意信息的完整性、真实性和安全性[2]。所以，随着量子计算和量子计算机等领域的迅速进展，确保数字图像信息传输的安全性日益凸显。近年来，量子图像处理技术持续不断地深入研究，保障量子图像的安全性成为一个不可避免的挑战。

2012 年，Zhou 等人提出了基于量子图像几何变换的加解密算法[3]。结合经典图像的几何变换，通过设计量子电路实现了量子图像的几何变换，并完成了量子灰度图像的加解密算法。该算法属于量子图像几何变换的应用，是量子图像密码学研究的新探索。2013 年，Yang 等提出的基于量子傅里叶变换(QFT)和双相位编码(DRPE)的灰度图像加解密方案[4]。该方案首次将双随机相位编码技术推广到量子场景，利用两个随机相位编码作为密钥，提高了方案的安全性。2014 年，Song Xian-Hua 等于 2014 年提出了基于受限几何和颜色变换的量子图像加密方案[5]，该方案主要是通过限制几何变换对像素位置编码进行置换该阶段的加密密钥由两个敏感混沌映射生成，具有高效的置乱效果。与之类似，2014 年 Wang Shen 等提出了基于 QWT 变换与双扩散的量子图像加密方案[6]，其加密密钥是由敏感的混沌逻辑图生成。Hua 等在 2015 年提出一种基于图像相关分解的量子图像加密算法[7]，该加密算法具有较大的密钥空间，能够抵抗蛮力攻击，同年，王申等人提出量子图像的最小有效量子位信息隐藏算法[8]，该算法设计了相应的幺正变换，以实现将秘密信息嵌入到代表量子覆盖图像颜色的最低有效量子位上。2016 年，姜楠等在王申的基础上提出基于 LSB 的量子图像隐写算法[9]，推动了将秘密信息隐藏在量子图像等量子覆盖物中的技术的发展。

随着不断涌现出各种量子图像加密算法，多个量子置乱算法也已陆续被提出。在学术研究和理论的基础上，针对这些量子置乱算法，探索如何设计出处理速度更快，且置乱效果更好的方案是一个有价值的问题。量子图像置乱方案的改进对于量子图像水印、量子图像隐写等量子图像安全应用具有重要意义，这些改进的置乱方案可以显著增强图像的安全性，从而提高其保密性。图像置乱是图像加密的基本操作，通过改变图像的像素排列顺序来降低相邻像素值的相关性，使得图像呈现为一幅不具有明显意义的噪声

图像。目前有两种主要的图像置乱方法。第一种是基于位置空间的置乱算法，其基本思想是通过改变图像的像素位置来破坏原始图像的信息。常见的置乱算法包括 Arnold 置乱算法，Fibonacci 置乱算法以及正交拉丁方置乱算法等。第二种方法则是基于像素颜色的置乱，特别适用于量子图像加密。该方法的基本思想是破坏原始量子图像的颜色信息的统计特性，使直方图平滑，不再反映原始图像的信息，从而达到置乱的效果。目前这类置乱算法包括灰度编码置乱算法，通过位平面变换的置乱算法等。

量子 Arnold 置乱方法由于其较好的置乱效应而被广泛应用于量子图像加密，但是由于其自身的周期特性，经过多次迭代后，所得到的加密信息仍会被破解。因此，本文采用量子 Arnold 置乱与祖冲之序列加密相结合的方法，对量子图像置乱效果进行有效增强，提高其加密强度与安全性。基于量子 Arnold 置乱算法，祖冲之序列加密算法的知识，本文设计了基于祖冲之序列的量子图像加密算法，并对其算法复杂度进行分析，最后通过仿真实验展示和分析加密的效果。

2. 理论基础

2.1. 量子图像表示模型(FRQI)

2010 年由 Le 等人首次提出了名为 FRQI 的表达式，它具有捕捉图像中每个像素点的颜色信息和对应位置信息的能力，借助量子叠加态来表示图像的信息，使其处于归一化的量子状态。公式(2.1)为 FRQI 整合为量子态形式，即

$$|I\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle \tag{2.1}$$

式中，

$$|c_i\rangle=\cos\theta_i|0\rangle+\sin\theta_i|1\rangle \tag{2.2}$$

FRQI 表达式使用$|i\rangle$来表示原始图像的位置信息，且$|i\rangle$包含了图像的横纵坐标信息[10]；公式(2.2)中，$|0\rangle$与$|1\rangle$表示为二维量子基态；$\theta=\left(\theta_0,\theta_1,\cdots,\theta_{2^{2n}-1}\right)$为对应颜色信息的角度向量，$\theta_i\in[0,\pi/2]$。总而言之，FRQI 表达式则涵盖了编码图像的颜色信息$|c_i\rangle$和位置信息$|i\rangle$这两个关键部分。

$$|i\rangle=|y\rangle|x\rangle=|y_{n-1}y_{n-2}\cdots y_0\rangle|x_{n-1}x_{n-2}\cdots x_0\rangle \tag{2.3}$$

公式(2.3)中，前 n 个量子比特 $y_{n-1}y_{n-2}\cdots y_0$ 编译图像纵坐标的位置信息，后 n 个量子比特 $x_{n-1}x_{n-2}\cdots x_0$ 编译图像横坐标的位置信息。

假设 FRQI 图像大小为 2 × 2，如图 1 所示，那么其对应的 FRQI 量子态表达式为[11]：

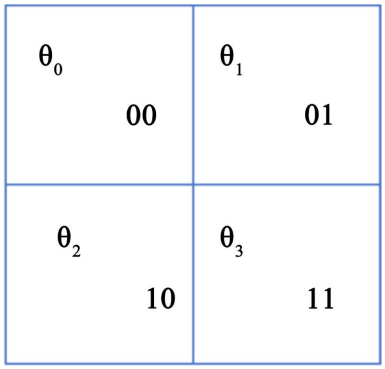

Figure 1. FRQI image
图 1. FRQI 图像

$$|I\rangle=\frac{1}{2}\left[\left(\cos\theta_0|0\rangle+\sin\theta_0|1\rangle\right)\otimes|00\rangle+\left(\cos\theta_1|0\rangle+\sin\theta_1|1\rangle\right)\otimes|01\rangle\right.$$
$$\left.+\left(\cos\theta_2|0\rangle+\sin\theta_2|1\rangle\right)\otimes|10\rangle+\left(\cos\theta_3|0\rangle+\sin\theta_3|1\rangle\right)\otimes|11\rangle\right]$$

在进行量子图像编译时，在量子计算领域，首要步骤是将计算设备初始化为所需的预备状态。这一初始过程是为了确保量子计算能够顺利进行。本文是通过使用 Le 等提出的 PPT 定理，将量子计算设备从初始状态演变为所需的图像表达式状态。

量子计算机从初始状态$|0\rangle^{\otimes 2n+1}$转化为公式(2.1)所示的 FRQI 状态，其中关键步骤是通过酉变换完成的。具体的酉变换步骤如下：

1) 多项式数个 Hadamard 变换

使用 Hardamard 门将初始状态$|0\rangle^{\otimes 2n+1}$转换为$|H\rangle$，具体计算过程为

二维单位矩阵 I 和二维 Hardamard 矩阵表示为

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \tag{2.4}$$

将 $2n$ 个 Hadamard 矩阵的张量积表示为$|H\rangle^{\otimes 2n}$，在$|0\rangle^{\otimes 2n+1}$上应用变换 $\mathrm{H}=I\otimes H^{\otimes 2n}$ 来产生状态$|H\rangle$，即

$$\mathrm{H}\left(|0\rangle^{\otimes 2n+1}\right)=\frac{1}{2^n}\otimes\sum_{i=0}^{2^{2n}-1}|i\rangle=|H\rangle \tag{2.5}$$

2) 利用受控旋转门，将量子计算机从初始化状态转换为 FRQI 状态

用旋转矩阵 $R_y(2\theta_i)$ 将量子计算机从初始化状态$|0\rangle^{\otimes 2n+1}$转换为 FRQI 状态$|I\rangle$。

已知旋转矩阵 $R_y(2\theta_i)$ 是沿 y 轴进行 $2\theta_i$ 角度旋转和受控旋转矩阵 R_i 得到的，其表达式如下：

$$R_y(2\theta_i)=\begin{pmatrix}\cos\theta_i&-\sin\theta_i\\\sin\theta_i&\cos\theta_i\end{pmatrix} \tag{2.6}$$

$$R_i=\left(I\otimes\sum_{j=0,j\neq 1}^{2^{2n}-1}|j\rangle\langle j|\right)+R_y(2\theta_i)\otimes|i\rangle\langle i| \tag{2.7}$$

将 R_k 和 R_lR_k 应用于$|H\rangle$，其表达式如下：

$$R_lR_k|H\rangle=\frac{1}{2^n}\left[|0\rangle\otimes\left(\sum_{i=0,i\neq k,l}^{2^{2n}-1}|i\rangle\langle i|\right)+\left(\cos\theta_k|0\rangle+\sin\theta_k|1\rangle\right)\otimes|k\rangle+\left(\cos\theta_l|0\rangle+\sin\theta_l|1\rangle\right)\otimes|l\rangle\right] \tag{2.8}$$

$$\mathrm{R}=R_lR_k \tag{2.9}$$

因此，从上式可以得到，

$$R_lR_k|H\rangle=\mathrm{R}|H\rangle=\left(\prod_{i=0}^{2^{2n}-1}R_i\right)|H\rangle=|I(n)\rangle \tag{2.10}$$

2.2. 量子图像置乱

图像置乱是指通过调整像素的位置，将图像呈现为不可读的形式，同时保持像素数量不变。在 2014 年，姜楠等研究人员首次提出并成功实施了基于量子图像的 Arnold 置乱、Fibonacci 置乱以及 Hilbert 置乱技术[12]，以及它们的逆变换，这一突破代表了在图像处理领域的一项重要研究成果。前两者主要是基于量子加法器实现，后者是通过逐步迭代的方式实现。

量子 Arnold 置乱

Arnold 置乱是建立在 Arnold 的遍历理论研究的基础之上的，作为其发展而来的一个重要理论成果。1992 年，Dyson 等研究人员将 Arnold 置乱方法成功应用于图像置乱领域。

(x,y) 表示原始图像 $I(x,y)$ 像素的位置坐标，$x,y=0,1,\cdots,N$，这里假设图像大小为 $N\times N$，那么一个二维的 Arnold 置乱表示方法如下所示[13]：

$$\begin{pmatrix} x_A \\ y_A \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, N) \tag{2.11}$$

则

$$x_A = (x+y) \bmod N \tag{2.12}$$

$$y_A = (x+2y) \bmod N \tag{2.13}$$

公式(2.10)中，(x_A, y_A) 是 Arnold 置乱后图像的横纵坐标信息。其中，$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ 为置乱矩阵。Arnold 置乱的逆变换如下所示：

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_A \\ y_A \end{pmatrix} (\mathrm{mod}\, N) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_A \\ y_A \end{pmatrix} (\mathrm{mod}\, N) \tag{2.14}$$

即

$$x = (2x_A - y_A) \bmod N \tag{2.15}$$

$$y = (-x_A + y_A) \bmod N \tag{2.16}$$

本文采用 FRQI 表示方法来描述图像，而量子 Arnold 置乱算法仅处理图像的位置信息，因此仅需在 FRQI 表达方式中改变坐标信息 $|i\rangle$ 即可。在这里，我们定义了 Arnold 图像置乱操作为 A，原始量子图像为 I，$|I_A\rangle$ 表示置乱后的量子图像，已知原始量子图像大小为 $2n\times 2n$，则

$$|I_A\rangle = A|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes A|i\rangle \tag{2.17}$$

其中，

$$A|i\rangle = A|y\rangle A|x\rangle \tag{2.18}$$

2.3. 祖冲之序列加密算法

祖冲之序列加密算法的结构可划分为三个主要组成部分。顶层是线性反馈移位寄存器(LFSR) [14]，LFSR 是一个寄存器序列，其根据预定义的反馈多项式进行位移操作。LFSR 的作用是生成加密算法所需的伪随机序列，用于对原始数据进行扩散和混淆。第二部分是比特重组单元，是通过对 LFSR 输出序列进行重新排列和组合来进一步增加序列的复杂性和扩散效果。在第三部分，是对第二部分的比特数据进行非线性交换，主要采用 S 盒和高扩散特性的线性变换 L，这一步骤旨在增强加密算法的输出，增加与密钥之间的复杂关系，从而提高安全性。

2.3.1. 线性反馈移位寄存器(LFSR)

LFSR 主要包括两种模式，详细流程如下[15]：

初始化模式下，将 31 比特数据流 u 作为输入，$u=(W\oplus X_3)\gg 1$，其中，W 是非线性函数 F 的输出，F 与 X_3 异或，得到的结果往右移一位，操作过程如下：

$$v=2^{15}s_{15}+2^{17}s_{13}+2^{21}s_4+\left(1+2^8\right)s_0 \bmod\left(2^{31}-1\right);$$

$$s_{16}=\left(v+u\right)\bmod\left(2^{31}-1\right);$$

if $s_{16}=0$, then set $s_{16}=2^{31}-1$;

$$\left(s_1,s_2,\cdots,s_{15},s_{16}\right)\rightarrow\left(s_0,s_1,\cdots,s_{14},s_{15}\right);$$

在工作模式下，LFSR 停止接收任何输入信号，其操作方式具体描述如下：

$$s_{16}=2^{15}s_{15}+2^{17}s_{13}+2^{21}s_4+2^{20}s_4\left(1+2^8\right)s_0 \bmod\left(2^{31}-1\right);$$

if $s_{16}=0$, then set $s_{16}=2^{31}-1$;

$$\left(s_1,s_2,\cdots,s_{15},s_{16}\right)\rightarrow\left(s_0,s_1,\cdots,s_{14},s_{15}\right)。$$

2.3.2. 比特重组

比特重组是通过采用不同的置换函数或混淆操作，对 LFSR 序列的比特进行重新排列，具体是从以下的 8 个单元$\left(s_0,s_2,s_5,s_7,s_9,s_{11},s_{14},s_{15}\right)$进行重新组合，最终输出 4 个 32 位的字 X_0,X_1,X_2,X_3，具体流程如下：

$$X_0=S_{15H}\|S_{14L}$$

$$X_1=S_{11L}\|S_{9H}$$

$$X_2=S_{7L}\|S_{5H}$$

$$X_3=S_{2L}\|S_{0H}$$

2.3.3. 非线性函数

W 是一个 32 字的输出，通过非线性函数 $w=F\left(X_0,X_1,X_2\right)$ 计算得出，其中，X_0,X_1,X_2 是非线性函数 F 的输入，详细步骤如下：

$$W=\left(\left(X_0\oplus R_1\right)+R_2\right)\bmod 2^{32}$$

$$W_1=\left(R_1+X_1\right)\bmod 2^{32}$$

$$W_2=R_2\oplus X_2$$

$$R_1=S\left[L_1\left(W_{1L}\|W_{2H}\right)\right]$$

$$R_2=S\left[L_2\left(W_{2L}\|W_{1H}\right)\right]$$

1) S 盒

在非线性函数 F 中，S 盒实现了非线性函数的作用。S 盒是由 4 个 8*8 的 S 盒组成，即 $S=\left(S_0,S_1,S_2,S_3\right)$，令 $S_0=S_1,S_2=S_3$。

2) 线性变换函数 L_1 和 L_2

在非线性函数 F 中 L_1 和 L_2 为两个线性变换函数：

$$L_1\left(X\right)=X\oplus\left(X<<<2\right)\oplus\left(X<<<10\right)\oplus\left(X<<<18\right)\oplus\left(X<<<24\right)$$

$$L_2\left(X\right)=X\oplus\left(X<<<8\right)\oplus\left(X<<<14\right)\oplus\left(X<<<22\right)\oplus\left(X<<<30\right)$$

3) 密钥扩展

密钥扩展的过程通常包括将初始密钥进行扩展和变换，以生成更长的密钥序列。

这里，初始密钥 k 和初始向量 iv 的长度均为 128 位，然而 LFSR 的初始状态是每 31 位 16 个单元，因此需要对密钥和初始向量进行扩展。$k=k_0\|k_1\|k_2\|\cdots\|k_{15}$，$iv=iv_0\|iv_1\|iv_2\|\cdots\|iv_{15}$。$D$ 是常量，将 D 分为 16 组 15 比特的常量，则 $D=d_0\|d_1\|d_2\|\cdots\|d_{15}$，将 k_i 和 iv_i 组合，得到 LFSR 的初值 $s_i=k_i\|d_i\|iv_i$，$0\le s_i\le 15$。

3. 量子图像加密和解密方法

3.1. 量子图像加密

量子图像加密方法包括两个主要步骤。首先，以明文图像为输入，通过对其与以祖冲之序列生成的密钥序列进行加密分组链接模式的异或操作，获得相应的图像。其次，利用量子 Arnold 置乱方法对图像进行置乱，得到最终的密文图像。

3.1.1. 祖冲之序列加密算法

使用传统的祖冲之序列加密算法进行加密时，每个时序周期可以生成一个 32 比特的密钥，然后将这个密钥序列与明文图像数据信息进行按位异或操作。解密算法是将产生的密文图像与上述加密过程相同的密钥按位异或，从而还原出原始的明文图像信息。

为了提高图像的加密强度，本文采用加密分组链接模式进行加密。首先，对明文图像的数据信息进行分组，每 32 比特为 1 组。然后，引入初始化向量，并将第一组明文 M1 与初始化向量进行异或运算。接着，通过祖冲之序列加密算法生成的 32 比特密钥与异或结果进行加密，得到第一组密文 C1。从第 2 组开始，将前一组的密文 C1 与当前明文 M2 进行异或，然后在进行加密得到密文 C2 [16] [17] [18] [19]。以此类推，直至加密完最后一组明文。图 2 展示了加密分组链接模式的加密过程。

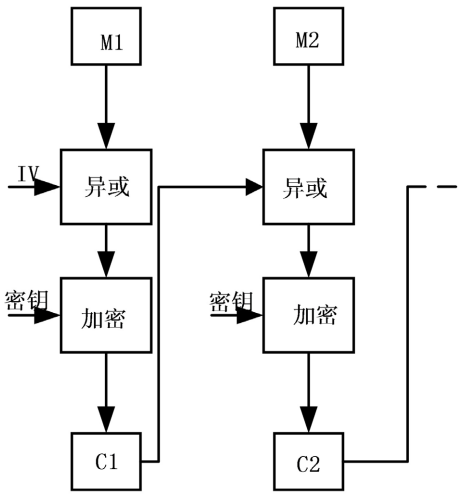

Figure 2. Encryption group link mode encryption process
图 2. 加密分组链接模式加密过程

3.1.2. 量子 Arnold 置乱算法

采用量子 Arnold 算法对之前所述的祖冲之序列加密算法生成的加密图像进行置乱。首先，对图像进行预处理，分别提取图像的红色(R)、绿色(G)和蓝色(B)通道的像素值。然后，使用不同的密钥对每个通道进行独立的加密操作。最后，将三个通道分别加密后的图像合并，形成最终的密文图像。

根据(2.14)和(2.15)得 Arnold 图像置乱的量子表示方式，

$$|x_A\rangle = A|x\rangle = |x+y\rangle \bmod 2^n \tag{3.1}$$

$$|y_A\rangle = A|y\rangle = |x+2y\rangle \bmod 2^n \tag{3.2}$$

即

$$|I_A\rangle = A|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle \otimes |x+y\rangle \bmod 2^n |x+2y\rangle \bmod 2^n \tag{3.3}$$

3.2. 量子图像解密

Arnold 算法在加密过程中是可逆的。祖冲之序列加密算法被归类为对称密码算法。因此，该算法的解密过程就是其加密过程的逆过程。下面是解密的详细步骤：将密文像素的位置信息$|i_A\rangle$经过 Arnold 的逆置乱后得到$|i\rangle$。

根据(2.14) (2.15)所示的 Arnold 逆置乱原理，可得

$$|x\rangle = |2x_A - y_A\rangle \bmod 2^n \tag{3.4}$$

$$|y\rangle = |-x_A + y_A\rangle \bmod 2^n \tag{3.5}$$

对第一组密文 C1 使用分组密码进行解密，然后将结果与初始向量 IV 执行按位异或操作，以获得明文 M1。接着，再次使用分组密码对密文 C2 进行解密，随后与第一组密文 C1 执行按位异或操作，得到明文信息 M2。这一过程可以连续进行，依次获得后续的明文 M3、M4，一直延续到第 n 个明文 Mn。如图 3 所示，这描述了加密分组链接模式的解密过程[20]。

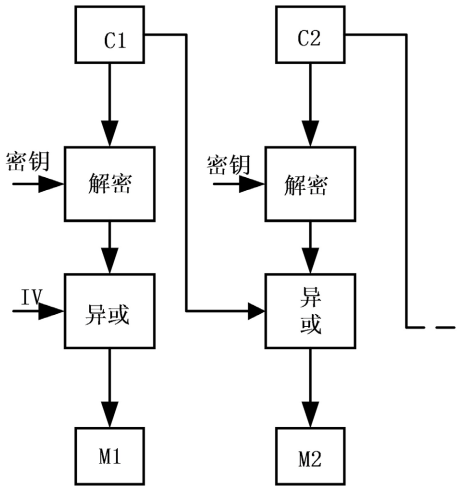

Figure 3. Encrypted group link mode decryption process
图 3. 加密分组链接模式解密流程

4. 实验结果和理论分析

本节基于学术研究和理论，对上述加密方案进行了在经典计算机上的仿真实验，所有实验均采用 Matlab R2022b 进行实现[21]，实验用到的数据是经典图像 Lena，图 4 展示了 512 × 512 大小的原始图像 Lena，图 5 展示了加密后的图像，图 6 是解密后的图像。本文将从下面两方面来分析图像加密算法的效果。具体如下图所示。

Figure 4. Original image lena
图 4. 原始图像 Lena

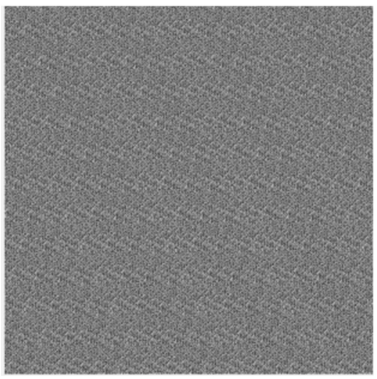

Figure 5. Encrypted image
图 5. 加密后图像

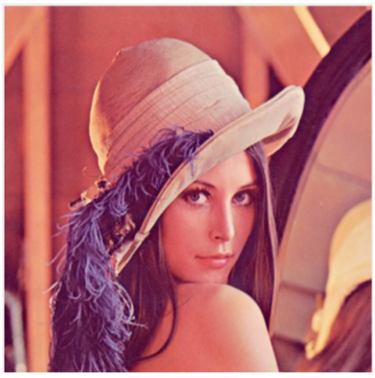

Figure 6. Decrypted image
图 6. 解密后图像

4.1. 直方图分析

图像直方图描述了一幅图像像素值的分布状况[22]。图像在经过理想的加密算法后，密文图像的像素值会发生随机变化，使得原始图像的特征无法被直接观察到。密文图像的直方图分布越均匀，信号变得越随机，密文图像中明文图像的统计信息明显降低，加密后的图像越安全，从而可以抵御统计分析。下图 7 对比了原始图像和经过加密处理后的图像的直方图分布情况。研究结果表明，加密图像的直方图显

示出了均匀的分布特征，波动在一定数值范围内[23]。这表明通过本文提出的加密方法后的图像抵御了直方图分析。

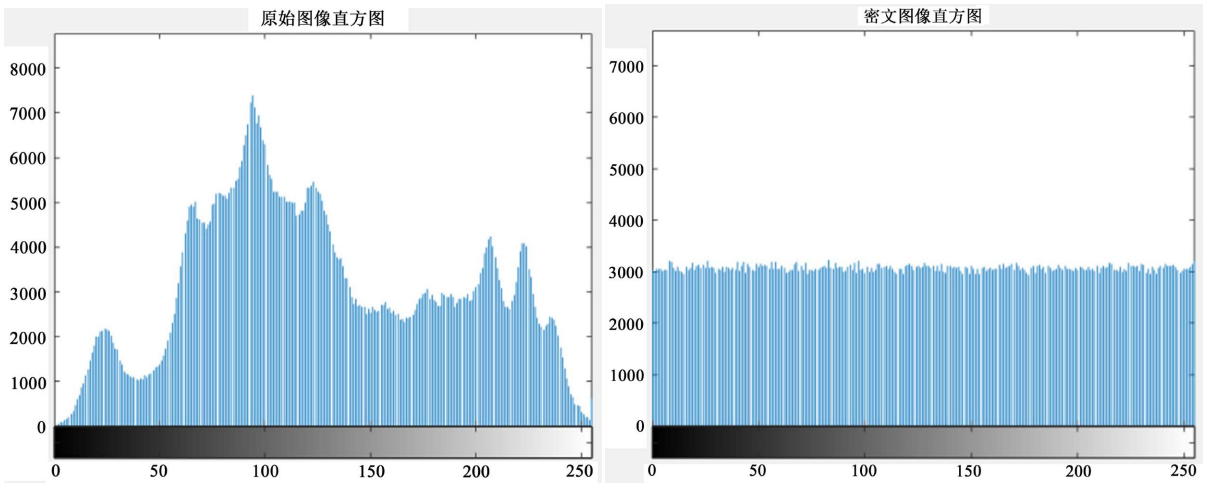

Figure 7. Comparison of histograms between original image and cipher text image
图 7. 原始图像和密文图像直方图对比图

4.2. 信息熵

信息熵是评估图像混乱程度的重要度量标准，其的数学表达式为[24]

$$H(m)=-\sum_{i=0}^{2^n-1}p(a_i)\log_2 p(a_i) \tag{4.1}$$

公式(4.1)中，a_i 表示图像中的第 i 个像素位置；而 $p(a_i)$ 则表示该像素点在整个图像中的出现概率，且 $\sum_{i=0}^{2^n-1}p(a_i)=1$。对于图像而言，理想的信息熵值应为 8 位，即每个像素点的分布应均匀[25]。从表 1 中可以看出，密文图像的 R，G，B 三个通道的信息熵分别为 7.993，7.992 和 7.993，说明加密后图像的混乱程度大，表明通过采用该加密方案，图中的实验证据显示出其具备较高的安全性，并能够有效地抵御信息熵攻击。

Table 1. Comparison of information entropy of each channel in images before and after encryption
表 1. 加密前后图像各通道信息熵对比

各通道信息熵	原始图像	加密图像
R 通道信息熵	7.2682	7.9993
G 通道信息熵	7.5901	7.9992
B 通道信息熵	6.9951	7.9993

5. 结论

本文设计了一种基于祖冲之序列的量子图像加密算法，充分利用了祖冲之算法的高度安全性以及加解密操作的简便性[26]，提出了一种安全性高且高效的图像加密方法。其主要优点有两点：1) 祖冲之序列的快速性与资源节省性：该算法运行速度快，资源消耗较少，有效地提高了图像加密的速度。此外，

它产生流式密钥时的快速实时性也大大增加了图像加密的效率。2) 分组链接模式的增强复杂性与随机性：在祖冲之序列加密过程中，采用了分组链接模式，通过按位异或操作，极大地提高了加密算法的复杂性和随机性[27]。通过进行仿真实验，结果表明本文提出的加密算法有效地减少了相邻像素之间的相关性。加密后的图像能够抵御直方图分析攻击，而且密文图像的信息熵接近 8，表明具有高度的安全性，并且能够抵抗信息熵攻击。

基金项目

北京市教委科研计划项目(KM202010015009)；北京印刷学院网络空间安全(数字版权保护技术)培育学科建设项目(21090123010)；北京印刷学院青年卓越项目(Ea202411)。

参考文献

[1] 黄林荃, 刘会, 张牧. 改进 Arnold 变换与量子混沌的图像加密系统[J]. 小型微型计算机系统, 2019, 40(9): 1897-1902.

[2] 李玥. 图像块自适应均衡水印算法[D]: [硕士学位论文]. 阜新: 辽宁工程技术大学, 2019.

[3] Zhou, R.G., Wu, Q., Zhang, M.Q. and Shen, C.Y. (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

[4] Yang, Y.G., 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

[5] Song, X.H., Wang, S., Abd El-Latif, A.A. and Niu, X.M. (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

[6] Wang, S., Song, X. and Niu, X. (2014) A Novel Encryption Algorithm for Quantum Images Based on Quantum Wavelet Transform and Diffusion. In: Pan, J.S., Snasel, V., Corchado, E., Abraham, A. and Wang, S.L., Eds., *Intelligent Data Analysis and Its Applications*, Volume II, Springer, Cham, 243-250. https://doi.org/10.1007/978-3-319-07773-4_24

[7] Hua, T., Chen, J., Pei, D., Zhang, W.Q. and Zhou, N.R. (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

[8] Wang, S., Sang, J., Song, X. and Niu, X.M. (2015) Least Significant Qubit (LSQb) Information Hiding Algorithm for Quantum Image. *Measurement*, **73**, 352-359. https://doi.org/10.1016/j.measurement.2015.05.038

[9] 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

[10] 曹梓崎. 量子图像加密及水印策略研究[D]: [硕士学位论文]. 大庆: 东北石油大学, 2019.

[11] 桑建芝. 量子彩色图像安全保护关键问题研究[D]: [博士学位论文]. 哈尔滨: 哈尔滨工业大学, 2019.

[12] 陶梦霞. 量子图像置乱和水印算法研究[D]: [硕士学位论文]. 南京: 东南大学, 2019.

[13] 王玲玲. 基于块分类技术的自适应数字图像水印算法研究[D]: [硕士学位论文]. 合肥: 合肥工业大学, 2011.

[14] 易鸿. 基于 FPGA 的图像硬件加密算法设计[J]. 河南科学, 2016, 34(12): 1976-1981.

[15] 杜红红, 张文英. 祖冲之算法的安全分析[J]. 计算机技术与发展, 2012, 22(6): 151-155.

[16] Kumar, A. and Li, B. (2010) On Implementing Motion-Based Region of Interest Detection on Multi-Core CELL. *Computer Vision and Image Understanding*, **114**, 1139-1151. https://doi.org/10.1016/j.cviu.2010.03.013

[17] Hung, S.H., Tu, C.H. and Yang, W.L. (2011) A Portable, Efficient Inter-Core Communication Scheme for Embedded Multicore Platforms. *Journal of Systems Architecture*, **57**, 193-205. https://doi.org/10.1016/j.sysarc.2010.11.003

[18] Kim, W., Suh, S., Hwang, W. and Han, J.J. (2014) SVD Face: Illumination-Invariant Face Representation. *IEEE Signal Processing Letters*, **21**, 1336-1340. https://doi.org/10.1109/LSP.2014.2334656

[19] Wang, Y. and Jiang, Z.W. (2011) Face Detection Based on Skin and Improved ICA. *Advanced Materials Research*, **219-220**, 1486-1490. https://doi.org/10.4028/www.scientific.net/AMR.219-220.1486

[20] 牛莹, 张勋才. 基于填充曲线和相邻像素比特置乱的图像加密方法[J]. 电子与信息学报, 2022, 44(3): 1137-1146.

[21] 蒋东华, 刘立东, 陈颖频, 等. 基于分数阶 Chen 超混沌系统和压缩感知的可视化图像加密算法[J]. 小型微型计算机系统, 2022, 43(11): 2387-2393. https://doi.org/10.20009/j.cnki.21-1106/TP.2021-0231

[22] 代高乐, 葛斌. 基于 DHIM 映射和分块置乱的彩色图像加密算法[J]. 赤峰学院学报(自然科学版), 2022, 38(8): 24-28. https://doi.org/10.13398/j.cnki.issn1673-260x.2022.08.011

[23] 李红凯, 裘国永. 基于超混沌理论的小波域分块图像加密算法[J]. 郑州轻工业学院学报(自然科学版), 2014, 29(6): 67-72.

[24] 李雪倩. 基于混沌系统的图像密码系统设计[D]: [硕士学位论文]. 南昌: 江西财经大学, 2020.

[25] 汤鹏志, 李彪, 李晓雄. 基于多线性映射的无证书代理盲签名方案[J]. 合肥工业大学学报(自然科学版), 2012, 35(5): 613-616, 707.

[26] 韩娣. 序列密码 Grain-128 和祖冲之算法的安全性研究[D]: [硕士学位论文]. 焦作: 河南理工大学, 2017.

[27] 欧阳春娟, 杨群生, 刘昌鑫. 基于粒子群优化的 DCT 域盲水印算法[J]. 井冈山大学学报(自然科学版), 2011, 32(2): 63-66.