doi:10.3772/j.issn.1002-0470.2023.02.006

基于超混沌的三层量子图像加密算法研究①

刘 帅②*** 邓文博* 刘福才③***

(*燕山大学智能控制系统与智能装备教育部工程研究中心 秦皇岛 066004)

(**燕山大学极端条件下机械结构和材料科学国防重点学科实验室 秦皇岛 066004)

摘 要 具有高效运算能力的量子计算机的提出使得基于经典计算机的图像加密算法安全性大大降低,如何将图像转移到量子计算机表示并进行加密传输是一个难点。针对这一问题,设计了基于 NEQR 模型的 3 层量子图像加密算法。首先,利用希尔伯特(Hilbert)矩阵实现量子块级置乱;然后,利用超 Lorenz 混沌系统生成的随机序列,打乱量子像素中的位顺序,实现位级置乱;最后,利用量子随机图像对原始量子图像进行 CNOT 操作并进行位本身 CNOT 操作,实现位级扩散,得到最后的加密图像。实验结果表明,加密图像的相关系数较低,加密算法的密钥空间大,加密图像的像素改变率、归一化平均变化强度和熵值接近理论值,具有良好的安全性和可行性。

关键词 图像加密; 超混沌系统; 量子图像; 量子电路

0 引 言

随着网络的发展、通信手段不断更新,图像逐渐成为承载信息的主体。不仅仅是人们日常生活中产生的图像信息,军事领域、工业领域、商业领域的机密资料多数也以图像形式进行存储和传输。图像加密领域随着图像数据的增多而不断发展,从传统的加密文本数据的高级加密标准(advanced encrytion standard, AES)和数据加密标准(data encryption stantard, DES)技术,到现在的基于混沌系统和 DNA 运算的图像加密算法[1-4]、压缩感知[5]、数字水印[6]等算法,图像加密技术不断走向成熟。而量子计算机能够进行并行计算,具有比经典计算机效率更高的数据处理能力,将经典图像转换成量子图像进行加密存储以及传输能够具备更高的安全性[7]。

目前,量子图像表示模型分为 3 种:第 1 种是文献[8]提出的 FRQI(flexible representation of quantum image)量子图像表示模型,该模型通过量子比特存储位置信息,利用角度矢量存储灰度信息,由于角度矢量在转换时存在偏差,故该模型不能准确地还原图像;第 2 种是文献[9]提出的 NEQR(novel enhanced quantum representation)量子图像表示模型,将灰度信息存储到量子态基态中,将位置信息存储到另一个量子态基态中,通过 2 个纠缠的量子态基态组成一个量子叠加态,用一个量子叠加态表示图像信息,能够完整地保存像素信息与位置信息;第 3 种就是这 2 种的衍生模型 MCQI(multi-channel representation for quantum images)。

有了量子图像表示模型,基于量子图像的加密算法不断地被学者提出,文献[10]提出了基于灰度码和位平面的图像量子置乱算法。文献[11]提出了基于 Arnold 和 Fibonacci 变换实现的量子置乱算法。随后文献[12]又提出了基于希尔伯特(Hilbert)扫描矩阵的量子置乱算法。文献[13]提出了广义 Arnold 变化与量子混沌加密算法,将量子修正量加入到混沌系统中,增强混沌序列的随机性。同

① 载人航天领域预研项目(2016040301)和河北省自然科学基金(F2022203043)资助项目。

② 男,1997 年生,硕士生;研究方向:混沌量子图像加密;E-mail: 8644757784@qq.com。

③ 通信作者,E-mail: lfc@ysu.edu.cn。

(收稿日期:2022-01-10)

时,文献[14]将量子混沌与 Fourier 变换结合在一起,实现了介于空间域和频域的分数域置乱。这些方法都利用经典计算机与量子计算相结合,没有脱离经典计算机的范畴,具有经典计算机运算速度慢的缺点。近年来,一些学者基于量子图像表示模型提出了量子位平面加密的加密方法。2017 年,文献[15]提出了基于量子比特相位的量子加密算法,利用量子旋转门实现像素扩散加密。2019 年,文献[16]设计了基于 FRQI 量子图像的加密算法,利用混沌系统产生的随机序列对量子图像进行量子位平面异或以及旋转操作,达到加密效果。同时,文献[17]利用量子旋转加密实现 NEQR 旋转加密。此外,文献[18]将二维 Henon 混沌映射转换到量子计算机中生成量子混沌序列对量子图像进行加密。这些方法为量子图像加密提供了新的研究方向。

本文在量子位平面加密方法的基础上,针对目前位平面加密算法包含经典计算导致运算速度慢、效率低并且加密方式单一的问题,提出了基于超混沌的三层量子图像加密算法。首先,利用希尔伯特(Hilbert)矩阵实现量子块级置乱;然后,利用超 Lorenz 混沌系统生成的随机序列,打乱量子像素中的位顺序,实现位级置乱;最后,利用量子随机图像对原始量子图像进行受控非操作并进行位本身受控非操作,实现位级扩散,得到最后的加密图像。仿真分析结果表明,所提出的量子图像加密方法具有安全性高、可实现性强和效率高等特点。

本文的结构如下。第 1 节首先给出了加密算法选用的混沌系统、量子图像表示模型及量子 Hilbert 置乱原理,然后给出了加密算法的步骤;第 2 节给出了解密算法的步骤;第 3 节对提出的算法进行仿真实验并进行相关性、直方图和信息熵等指标对比分析,验证算法的可行性;第 4 节为结论。

1 加密算法

首先给出加密算法选用的混沌系统与量子表示模型,再给出 Hilbert 矩阵生成的算法公式,最后给出加密算法的过程。

1.1 混沌系统与模型选取

1.1.1 超 Lorenz 混沌系统

超 Lorenz 混沌系统具有初值敏感性和伪随机性等特性,其产生的混沌序列随机性较混沌系统更好,更加适合应用在图像加密领域中。超 Lorenz 混沌系统的定义如下:

$$\begin{cases}\dot{x} = a(y - x) + w\\ \dot{y} = cx - y - xz\\ \dot{z} = xy - bz\\ w = -yz + rw\end{cases} \tag{1}$$

式中,a、b、c、r 为系统参数,当 $a = 10$,$b = 8/3$,$c = 28$,$-1.52 \leqslant r \leqslant -0.06$ 时,系统处于超混沌态,用四阶龙格-库塔法进行求解可得随机序列。本文算法的超 Lorenz 混沌系统的参数为 $a = 10$,$b = 8/3$,$c = 28$,$r = -1$。

1.1.2 量子图像表达

NEQR 表示模型的量子图像能够在加密之后准确地还原图像信息,因此本文以此模型进行加密,进行的量子运算可以准确地解算。这种量子图像表示方式由 2 个量子比特分别表示灰度和位置信息。两个量子比特通过量子纠缠实现存储。

根据 NEQR 表示方法,对于大小为 $2^n \times 2^n$ 的灰度图像 I,可以表示为

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n-1}} |C_i\rangle |i\rangle$$

$$|C_i\rangle = |C_i^{q-1}\cdots C_i^1 C_i^0\rangle,\ C_i^k \in \{0,1\},\ k = q-1,\cdots,1,0$$

$$|i\rangle = |y\rangle |x\rangle = |y_{n-1}y_{n-2}\cdots y_1\rangle |x_{n-1}x_{n-2}\cdots x_1\rangle,\ y_k, x_k \in \{0,1\} \tag{2}$$

二进制量子序列 $|C_i^{q-1}\cdots C_i^1 C_i^0\rangle$ 表示图像的灰度值,最多可以表示 2^q 种颜色信息;量子比特 $|i\rangle$ 表示图像的位置信息,量子比特 $|x\rangle$ 编码水平方向的位置信息,$|y\rangle$ 编码垂直方向的位置信息。

1.2 Hilbert 矩阵

一个 $2^n \times 2^n$ 的图像可以被表征为一个矩阵,称这个矩阵为原始矩阵 $\boldsymbol{S}_n$ 并且用 $1 - 2^{2n}$ 编码它的像素位置信息。

$$\boldsymbol{S}_n = \begin{bmatrix} 1 & 2 & 3 & \cdots & 2^n \\ 2^n+1 & 2^n+2 & 2^n+3 & \cdots & 2^{n+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{2n-1}+1 & 2^{2n-1}+2 & 2^{2n-1}+3 & \cdots & 2^{2n} \end{bmatrix}$$

例如 $\boldsymbol{S}_1=\begin{bmatrix}1&2\\3&4\end{bmatrix}$,$\boldsymbol{S}_2=\begin{bmatrix}1&2&3&4\\5&6&7&8\\9&10&11&12\\13&14&15&16\end{bmatrix}$。

而希尔伯特扫描矩阵 $\boldsymbol{H}_n$ 是原始矩阵 $\boldsymbol{S}_n$ 的一种排列。例如 $\boldsymbol{H}_1=\begin{bmatrix}1&2\\4&3\end{bmatrix}$,$\boldsymbol{H}_2=\begin{bmatrix}1&2&15&16\\4&3&14&13\\5&8&9&12\\6&7&10&11\end{bmatrix}$。

量子 Hilbert 置乱就是打乱量子图像中的位置排列,将其位置信息按照 Hilbert 矩阵进行排列,填入对应的像素颜色信息,即可完成置乱操作。这里使用能直接设计量子电路的 Hilbert 矩阵生成算法[12]:

$$\boldsymbol{H}_{n+1}=\begin{cases}\begin{pmatrix}\boldsymbol{H}_n & (\boldsymbol{H}_n+4^n\boldsymbol{E}_n)^{\mathrm{T}}\\ (\boldsymbol{H}_n+3\times4^n\boldsymbol{E}_n)^{\mathrm{pp}} & (\boldsymbol{H}_n+2\times4^n\boldsymbol{E}_n)^{\mathrm{T}}\end{pmatrix} & n\text{ 为偶数}\\ \begin{pmatrix}\boldsymbol{H}_n & (4^{n+1}+1)\boldsymbol{E}_n-\boldsymbol{H}_n^{\mathrm{lr}}\\ (\boldsymbol{H}_n+4^n\boldsymbol{E}_n)^{\mathrm{T}} & (\boldsymbol{H}_n+2\times4^n\boldsymbol{E}_n)^{\mathrm{T}}\end{pmatrix} & n\text{ 为奇数}\end{cases} \tag{3}$$

其中,n 是正整数,$\boldsymbol{H}^{\mathrm{T}}$ 是矩阵的转置,$\boldsymbol{H}^{\mathrm{up}}$是矩阵的上下反转,$\boldsymbol{H}^{\mathrm{lr}}$是矩阵的左反转,$\boldsymbol{H}^{\mathrm{pp}}$是矩阵的中心反转。

1.3　三层量子图像加密算法

所提出的量子算法流程图如图 1 所示。

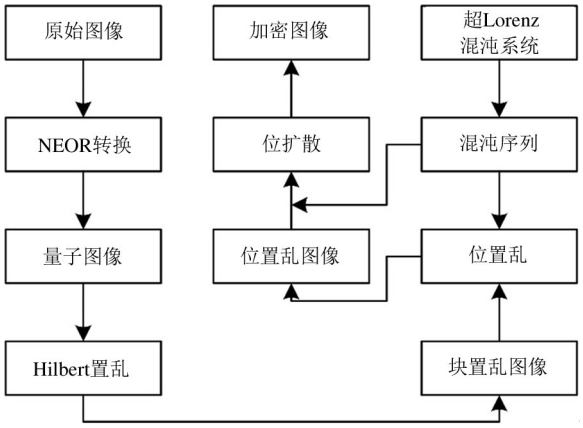


图 1　加密算法流程图

首先,将原始图像转换成 NEQR 量子图像并利用希尔伯特矩阵实现量子块级置乱;然后,利用超 Lorenz 混沌系统生成的随机序列打乱量子像素中的位顺序,实现位级置乱;最后,利用量子随机图像对原始量子图像进行 CNOT 操作并利用混沌序列实现自 CNOT 操作,得到最后的加密图像。

1.4　量子 Hilbert 块置乱

在进行量子置乱之前,先将原始图像转换成 NEQR 表示图像,如式(4)所示。

$$|I\rangle=\frac{1}{2^n}\sum_{i=0}^{2^{2n-1}}|c_i\rangle\otimes|i\rangle,|c_i\rangle=|c_i^{q-1}\cdots c_i^1c_i^0\rangle,\quad c_i^k\in\{0,1\} \tag{4}$$

量子 Hilbert 置乱分为 3 个部分。

第 1 部分:初始化 Initialization(k)。设输入图像的尺寸为 $2^n\times2^n$,将输入图像分成 $2^{n-1}\times2^{n-1}$ 个大小为 2×2 的子块。在量子电路中,就是把 x_{k+1} 与 x_{k+2} 利用量子交换门互换,相同的操作应用在 x_{k+2} 与 $x_{k+3},\cdots,x_{n-2}$ 与 x_{n-1},最后,x_{n-1} 与 y_k 进行互换。

第 2 部分:奇数运算 odd(k)。当 n 为奇数时,将上一步所得的块 $\begin{pmatrix}A&B\\C&D\end{pmatrix}$ 转换成 $\begin{pmatrix}A&D^{\mathrm{pp}}\\B^{\mathrm{T}}&C^{\mathrm{T}}\end{pmatrix}$。设计的量子电路分为 3 个步骤。

(1) 利用量子交换门交换 x_k 与 y_k,然后进行受控非门操作,其中 x_k 是控制位,y_k 是目标位。

(2) 进行控制交换门操作。其中,y_k 为控制位,当 y_k 为 1 时,y_0 与 x_0,y_1 与 x_1,…,y_{k-1} 与 x_{k-1} 进行交换。

(3) 进行 01 受控非门操作。当 y_k 为 0、x_k 为 1 时,y_0、x_0、y_1、x_1、……、y_{k-1}、x_{k-1} 取反。

第 3 部分:偶数运算 even(k)。当 n 为偶数时,将上一步所得的块 $\begin{pmatrix}A&B\\C&D\end{pmatrix}$ 转换成 $\begin{pmatrix}A&B^{\mathrm{T}}\\D^{\mathrm{pp}}&C^{\mathrm{T}}\end{pmatrix}$。设计的量子电路分为 3 个步骤。

(1) 进行受控非门操作,其中 y_k 是控制位,x_k 是目标位。

(2) 进行控制交换门操作。其中,x_k 为控制位,当 x_k 为 1 时,y_0 与 x_0,y_1 与 x_1,…,y_{k-1} 与 x_{k-1} 进行交换。

(3) 进行 0 1 受控非门操作。当 y_k 为 1、x_k 为 0 时,y_0、x_0、y_1、x_1、……、y_{k-1}、x_{k-1} 取反。

1.5　混沌量子位置乱

混沌量子位置乱分为 3 个步骤。

第 1 步：利用随机数生成超 Lorenz 混沌系统的初值，其中 $x0 \in (-40,40)$，$y0 \in (-40,40)$，$z0 \in (1,81)$，$w0 \in (-250,250)$，并将初值带入超混沌系统当中，生成随机序列 S 并转换成整数序列 X，若图像尺寸为 $M \times N$，则随机序列长度为 $M \times N \times 8$，并制备与图像尺寸等大的空白 NEQR 图像 I_1。

$$X = \mathrm{mod}(\mathrm{floor}(S \times \mathrm{pow}2^{16}),8) \tag{5}$$

第 2 步：将随机序列分成 $M \times N$ 个长度为 8 的数组，每个数组转换成无重复的 0～7 的随机数。

第 3 步：利用量子交换门按照数组的排列顺序将图像与 I_1 进行交换，经过交换后的 I_1 就是置乱后的加密图像。设初始顺序为[7,6,5,4,3,2,1,0]，若生成的随机数组为[0,2,7,6,4,1,5,3]，则置乱量子电路如图 2所示。

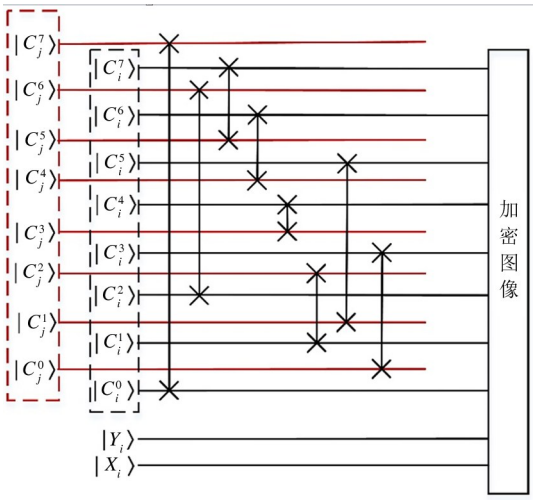


图 2　量子位平面置乱电路

1.6　混沌量子位扩散

混沌量子位扩散分为 3 个步骤，具体如下所述。

第 1 步：利用随机数生成超 Lorenz 混沌系统的初值，其中 $x0 \in (-40,40)$，$y0 \in (-40,40)$，$z0 \in (1,81)$，$w0 \in (-250,250)$。将初值带入超混沌系统当中，生成随机序列 S 并转换成整数序列 X。

$$X = \mathrm{mod}(\mathrm{floor}(S \times \mathrm{pow}2^{16}),2) \tag{6}$$

第 2 步：通过对 I_1 进行受控非操作对 I_1 进行加密，得到扩散图像 I_2。受控非门的控制位由序列 X 提供。量子电路图如图 3 所示。

第 3 步：对 I_2 进行自身受控非操作，由超 Lorenz 混沌系统生成 $M \times N + 8$ 的序列 X_1 并进行求余操作得到序列 X_2。

$$X_2 = \mathrm{mod}(\mathrm{floor}(X_1 \times \mathrm{pow}2^{16}),8) \tag{7}$$

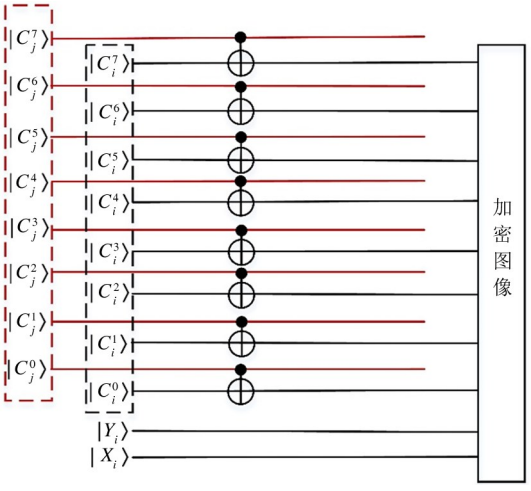


图 3　混沌量子位扩散

为增强随机性，舍弃前 $M \times N$ 个点，并对剩下的 8 个数进行无重复排列，得到整数范围为[0,7]的无重复随机数，用来表征随机扩散的顺序。设初始顺序为[7,6,5,4,3,2,1,0]，若随机序列 X_2 为[2,1,5,7,4,0,3,6]，按照默认顺序对数组顺序的量子位进行异或操作进行扩散。为了保证每一位都经历扩散操作，将序列翻转得到[6,3,0,4,7,5,1,2]，再进行一遍扩散操作，得到最终的加密图像，混沌量子位自身扩散示例图如图 4 所示。

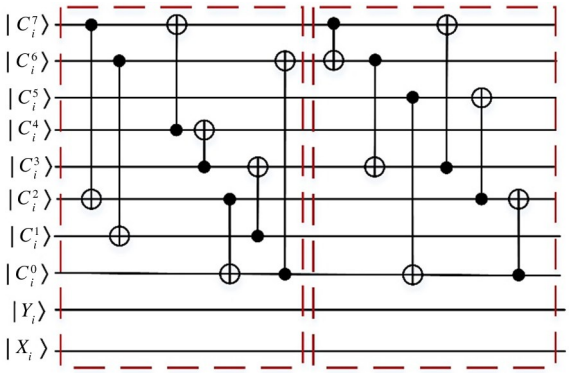


图 4　量子位平面扩散电路

2　解密算法

解密算法是加密算法的逆过程，对应加密算法

的 3 层加密,解密算法也分为 3 层。

第 1 层:位扩散解密。

将位扩散电路反方向进行即可得到位扩散解密图像。

第 2 层:将位置乱电路反方向进行即可得到位置乱解密图像。

第 3 层:按照 Hilbert 置乱的步骤反方向进行可得最终的解密图像。

解密算法流程图如图 5。

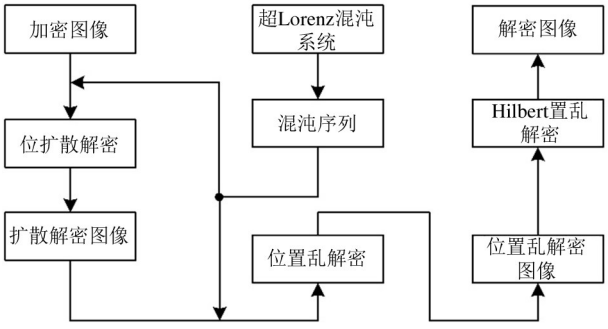


图 5　解密算法流程图

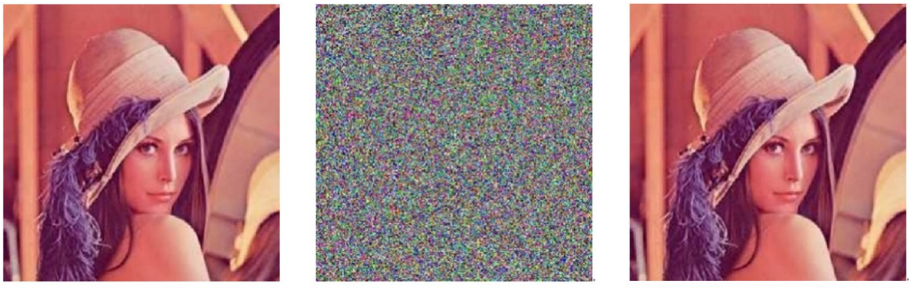
3　加密算法的仿真实验及分析

3.1　实验案例

实验采用彩色标准图像 Lena,图像大小为 256×256 像素,原图像、加密图和解密图如图 6 所示。由图 6 可知,加密算法的加密图像能够完整隐藏原始图像信息,解密出的图像能准确地还原原始图像信息,验证了该算法的可行性。

3.2　密钥空间和安全性分析

本文加密算法使用了超 Lorenz 混沌系统的初始值为密钥。即 $\boldsymbol{K}=\{x0,\ y0,\ z0,\ w0\}$, $x0\in(-40,40)$, $y0\in(-40,40)$, $z0\in(1,81)$, $w0\in(-250,\ 250)$, $x0$、$y0$ 和 $z0$ 的步长为 10^{-13}, $w0$ 的步长为 10^{-12}。因此,密钥空间的大小为 $S=2.56\times10^{59}$, 无法通过列举运算进行破解,具有安全性。



(a) 原图像　(b) 加密图像　(c) 解密图像

图 6　原图像、加密图像和解密图像

3.3　相邻像素相关性分析

相邻像素的相关性可以通过相关系数进行判断。对于加密算法来说,相关系数指的是相邻像素线性相关的程度,越接近 -1 或 1,相关性越高,反之相关性越低。原图与加密图在 3 个方向的相关系数如表 1 所示。其中,文献[15]和文献[17]是基于量子旋转的量子图像加密算法,文献[19]是基于混沌系统的量子图像加密算法,其余是混沌经典图像加密算法。

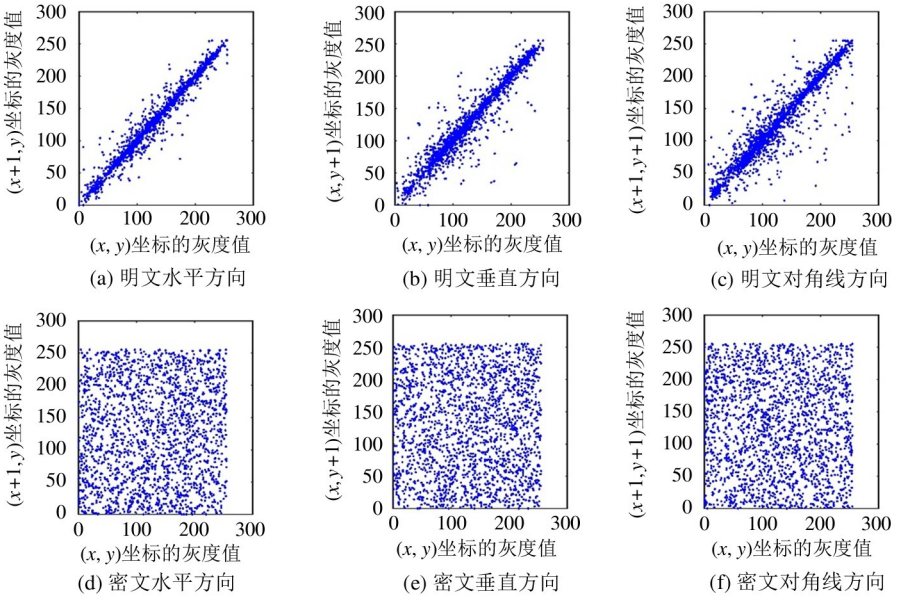
由表 1 数据可知,加密图的相关系数远远低于其余加密算法的相关系数,说明该加密算法有良好的加密效果。

表 1　Lena 图像的相关系数

图像	水平	垂直	对角线
原图	0.9819	0.9586	0.9430
加密图	-0.0001	-0.0002	-0.0006
文献[15]	0.0005	-0.0042	-0.0055
文献[17]	0.0049	0.0069	0.0013
文献[19]	0.0060	-0.0138	0.0014
文献[20]	0.0004	0.0013	-0.0023
文献[21]	0.0075	-0.0055	0.0187
文献[22]	0.0027	0.0018	0.0029

同时,这里随机选取了 Lena 图像中的 2000 对像素对,分别测试其水平、垂直和对角 3 个方向的相关性,分布图如图 7 所示。

由图 7 所知,原始图像 3 个方向像素坐标灰度值大致呈正相关分布,而加密图像 3 个方向像素坐标灰度值分布大致呈均匀分布,说明密文图像在各个方向上不具有相关性。



(a) 明文水平方向　(b) 明文垂直方向　(c) 明文对角线方向

(d) 密文水平方向　(e) 密文垂直方向　(f) 密文对角线方向

图 7　Lena 相邻像素相关性图像分布

3.4　NPCR 和 UACI 分析

比较 2 幅图像相应位置的像素点的值,记录不同的像素点个数占全部像素点的比例,这就是常用的像素改变率(number pixels change rate, NPCR),计算如式(7)所示。

$$NPCR(P_1,P_2)=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|\,\mathrm{Sign}(P_1(i,j)-P_2(i,j))\,|\times 100\% \tag{7}$$

其中,Sign(·)为符号函数,如(8)所示。

$$\mathrm{Sign}(x)=\begin{cases}1 & x>0\\ 0 & x=0\\ -1 & x<0\end{cases} \tag{8}$$

比较 2 幅图像相应位置的像素点的值,记录它们的差值,然后计算全部相应位置像素点的差值与最大差值(255)的比值的平均值,这就是归一化平均变化强度(unified averaged changed intensity, UACI),计算公式为

$$UACI(P_1,P_2)=\frac{1}{MN}\sum_{i}^{M}\sum_{j}^{N}\frac{|\,P_1(i,j)-P_2(i,j)\,|}{255-0}\times 100\% \tag{9}$$

表 2 给出了 NPCR 和 UACI 的测试结果。测试结果越接近理论值,加密图像与原始图像差异就越大。由表 2 可知,所设计的加密算法其 NPCR 与 UACI 比其余算法的加密算法更接近理想值,说明该算法有良好的加密效果以及可行性。

表 2　NPCR 和 UACI 测试结果

指标	理论值	文献[20]	文献[21]	文献[22]	本文算法
NPCR/%	99.6094	99.5900	99.0127	99.6800	99.6098
UACI/%	33.4635	33.5000	33.6872	37.0100	33.4332

3.5　直方图分析

直方图可以直接看出图像的灰度分布情况。对于加密图像来说,直方图分布越均匀,加密效果越好。Lena 图与加密图像的红绿蓝(red green blue, RGB)三通道直方图如图 8 所示。由图 8 可知,对比图像加密前后的三通道直方图可以看出,原始图像的灰度值分布不均匀,波形有明显的波动,容易被统计;加密图像的灰度值分布较为均匀,波形较平缓,分布区域集中,无法统计分析规律,能抵抗统计性攻击,具有安全性。

3.6　密钥敏感性分析

密钥敏感性分析是用来分析当加密图用密钥解密时,如果密钥发生微小变化,能否正确地解密出原

始图像。在不能解密出原始图像信息的前提下,其微小变化越低,说明加密算法的密钥敏感性越好。

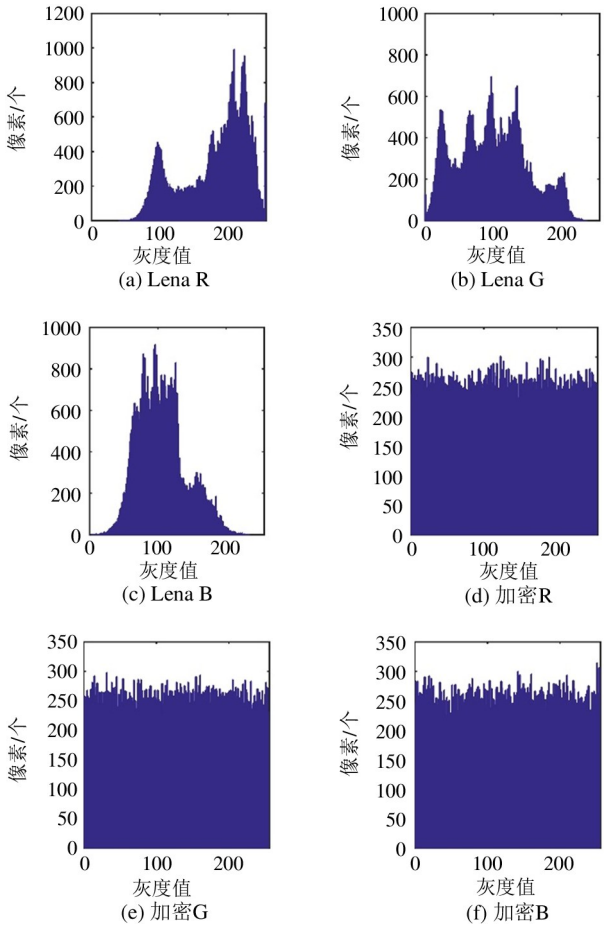


图 8　加密解密直方图

对所设计的加密算法密钥 $x0$、$y0$、$z0$ 的值上分别加上 10^{-13},在 $w0$ 的值上加上 10^{-12},对加密图像进行解密,解密图像如图 9 所示。由图 9 可知,当密钥发生微小改变低至 10^{-12},解密算法便无法解密出正确的图像,说明该算法有着良好的密钥敏感性。

3.7　信息熵分析

每一层图像像素分布的统计度量被称为信息熵。图像的信息熵可以用下面的公式来计算。

$$H = -\sum_{i=0}^{L} p(i)\log_2 p(i) \tag{10}$$

这里,L 为图像的灰度等级数,$p(i)$ 表示灰度值 i 出现的概率。

对于 $L = 256$ 的灰度随机图像,信息熵 H 的理论值为 8。表 3 展示了原图与加密图的熵值并列出了 4 种加密算法的熵值。由表 3 可知,密文的信息熵比其余的加密算法更接近理论值,说明该加密算法能较好地抵御熵攻击。

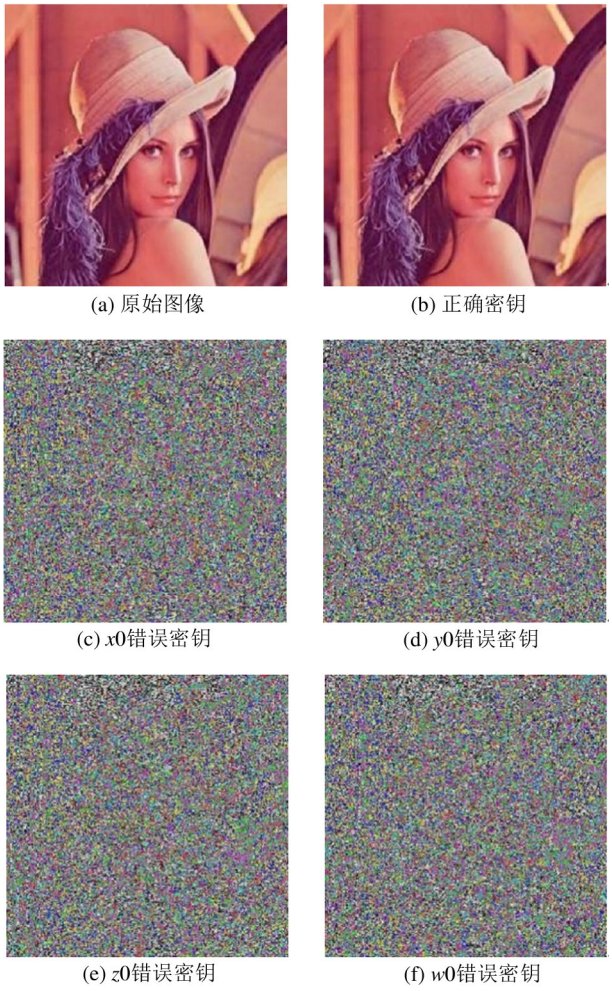


图 9　密钥敏感性分析

表 3　信息熵分析

信息熵	原图	加密图
文献[19]	7.4436	7.9983
文献[20]	无	7.9978
文献[21]	无	7.9564
文献[22]	无	7.9938
文献[23]	无	7.9941
本文算法	7.7760	7.9989

4　结　论

本文提出了一种高效的量子图像加密方法。该算法总共有 3 层加密,分别利用希尔伯特矩阵排列以及混沌序列进行块置乱、位置乱以及位扩散得到

加密图像。仿真和数值分析表明,加密图像的相关系数较低,密钥空间大,加密图像的像素改变率、归一化平均变化强度和熵值接近理论值,具有良好的安全性和可行性。且该算法完全基于量子位平面进行加密,摆脱了经典运算的局限性。但是,在进行 Hilbert 矩阵排列时会花费大量时间,且排列有固定规律,容易被破解。因此,如何设计随机性的量子块级置乱,还需进一步研究。

参考文献

[1] MIRZAEI O, YAGHOOBI M, IRANI H. A new image encryption method: parallel sub-image encryption with hyper chaos[J]. Nonlinear Dynamics, 2012, 67: 557-566.

[2] CHAI X L, CHEN Y R, BROYDE L. A novel chaos-based image encryption algorithm using DNA sequence operations[J]. Optics and Lasers in Engineering, 2017, 88: 197-213.

[3] HU T, LIU Y, GONG L H, et al. Chaotic image cryptosystem using DNA deletion and DNA insertion[J]. Signal Processing, 2017, 134: 234-243.

[4] FARAH M, GUESMI R, KACHOURI A, et al. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation[J]. Optics and Laser Technology, 2020, 121: 105777.

[5] 司菁菁,程银波. 基于方向自适应观测与 AMP 的小波域图像压缩感知[J]. 高技术通讯, 2019, 29(4): 321-328.

[6] 吴德阳,张金羽,容武艳,等. 数字图像水印技术综述[J]. 高技术通讯, 2021, 31(2): 148-162.

[7] CARAIMAN S, MANTA V. Image processing using quantum computing[C]// 2012 16th International Conference on System Theory, Control and Computing (ICSTCC). Sinaia: IEEE, 2012: 1-6.

[8] LE P Q, DONG F Y, HIROTA K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations[J]. Quantum Information Processing, 2011, 10(1): 63-84.

[9] ZHANG Y, LU K, GAO Y H, et al. NEQR: a novel enhanced quantum representation of digital images[J]. Quantum Information Processing, 2013, 12(8): 2833-2860.

[10] ZHOU R G, SUN Y J, FAN P. Quantum image gray-code and bit-plane scrambling[J]. Quantum Information Processing, 2015, 14(5): 1717-1734.

[11] JIANG N, WANG L. Analysis and improvement of the quantum Arnold image scrambling[J]. Quantum Information Processing, 2014, 13(7): 1545-1551.

[12] JIANG N, WANG L, WU W Y. Quantum Hilbert image scrambling[J]. International Journal of Theoretical Physics, 2014, 53(7): 2463-2484.

[13] 刘会,金聪. 基于量子混沌映射的高效安全的图像加密算法[J]. 计算机工程与科学, 2016, 38(11): 2227-2233.

[14] 谢国波,邓华军. 量子混沌和分数阶 Fourier 变换的图像加密算法[J]. 计算机工程与应用, 2018, 54(17): 214-220.

[15] 李盼池,曹梓崎. 基于量子比特相位的彩色图像描述方法及应用[J]. 电子与信息学报, 2017, 39(2): 489-493.

[16] 张健,霍达. 基于混沌系统的量子彩色图像加密算法[J]. 西南交通大学学报, 2019, 54(2): 421-427.

[17] 郭海儒,许权,杜娅颖. 基于像素颜色置乱的彩色量子图像加密方法[J]. 量子电子学报, 2019, 36(1): 1-5.

[18] JIANG N, DONG X, HU H, et al. Quantum image encryption based on Henon mapping[J]. International Journal of Theoretical Physics, 2019, 58(3): 979-991.

[19] DAI J Y, MA Y, ZHOU NR. Quantum multi-image compression-encryption scheme based on quantum discrete cosine transform and 4D hyper-chaotic Henonmap[J]. Quantum Information Process, 2021, 20(7): 246.

[20] WANG SC, WANG CH, XU C. An image encryption algorithm based on a hidden attractor chaos systemand the Knuth-Durstenfeld algorithm[J]. Optics and Laser Technology, 2020, 128: 105995.

[21] ALBAHRANI E A, MARYOOSH AA, LAFTA S H. Block image encryption based on modified playfair and chaotic system[J]. Journal of Information Security and Applications, 2020, 51: 102445.

[22] 袁立,谢俐,龙颖,等. 基于哈希和 DNA 编码的彩色图像混沌加密算法[J]. 重庆大学学报, 2021, 44(7): 55-63.

[23] WANG B, ZHANG B F, LIU X W. An image encryption approach on the basis of a time delay chaotic system[J]. Optik, 2021, 225: 165737.

Research on three-layer quantum image encryption algorithm based on hyperchaos

LIU Shuai[*,**], DENG Wenbo[*], LIU Fucai[*,**]

([*]Engineering Research Center of Ministry of Education for Intelligent Control System and Intelligent Equipment, Yanshan University, Qinhuangdao 066004)

([**]National Defense Key Discipline Laboratory of Mechanical Structure and Material Science under Extreme Conditions, Yanshan University, Qinhuangdao 066004)

Abstract

The proposal of a quantum computer with efficient computing power greatly reduces the security of image encryption algorithms based on classical computers. It is difficult to transfer images to quantum computers for representation and encrypted transmission. Aiming at this problem, a three-layer quantum image encryption algorithm based on the NEQR (novel enhanced quantum representation) model is designed. First, the Hilbert matrix is used to achieve quantum block-level scrambling; then, the random sequence generated by the Lorenz hyperchaotic system is used to disrupt the bit order in the quantum pixels to achieve bit-level scrambling; finally, the quantum random image is used to scramble the original quantum image to perform the CNOT operation and the bit itself CNOT operation to realize the bit-level diffusion and obtain the final encrypted image. The experimental results show that the correlation coefficient of the encrypted image is low, the key space of the encryption algorithm is large, and the pixel change rate, normalized average change intensity and entropy value of the encrypted image are very close to the theoretical values, which has good security and feasibility.

Key words: image encryption, hyperchaotic system, quantum image, quantum circuit