图文信息技术

基于量子 Logistic 映射的图像加密算法研究

徐扬，黄迎久，李海荣
（内蒙古科技大学，包头 014010）

摘要：目的 提出将量子 Logistic 混沌映射与三维 Arnold 混沌映射相结合的图像加密算法，以提高图像加密的复杂度。**方法** 首先利用量子 Logistic 混沌映射生成置乱用的伪随机序列与明文进行整体置乱，再利用三维 Arnold 混沌映射生成一个整数序列，与置乱后的密文进行扩散运算。**结果** 通过仿真实验，加密图像的相关性系数接近于 0，密钥敏感性的 NPCR 和 UACI 的测试值分别约等于 99.60 和 33.4，信息熵的测试结果约等于 7.999，都非常接近于理论值。**结论** 加密算法充分体现了量子混沌映射高复杂度的非线性力学特性。通过仿真实验测试可知，加密算法具有密钥空间大、敏感性强、安全性好的特点。

关键词：图像加密；量子 logistic 映射；三维 Arnold 映射；置乱
中图分类号：TP309 **文献标识码：**A **文章编号：**1001-3563(2018)07-0180-07
DOI：10.19554/j.cnki.1001-3563.2018.07.033

Image Encryption Algorithm Based on Quantum Logistic Mapping

XU Yang, *HUANG Ying-jiu*, *LI Hai-rong*
(Inner Mongolia University of Science & Technology, Baotou 014010, China)

ABSTRACT: The work aims to propose an image encryption algorithm combining quantum Logistic chaotic mapping with 3D Arnold chaotic mapping to improve the complexity of image encryption. Firstly, the quantum Logistic chaotic mapping was used to generate the pseudo random sequence for the scrambling with the plain text as a whole, and then an integer sequence was generated with the 3D Arnold chaotic mapping. The diffusion operation was carried out with the scrambled ciphertext. Through simulation experiments, the correlation coefficient of encrypted image was close to 0, the test values of NPCR and UACI of key sensitivity were approximately equal to 99.60 and 33.4, respectively, and the test result of information entropy was approximately equal to 7.999, which were very close to the theoretical values. The encryption algorithm fully reflects the nonlinear mechanical property of high complexity of quantum chaotic mapping. Based on the simulation experiment, the encryption algorithm has such advantages as large key space, strong sensitivity and good security.

KEY WORDS: image encryption; quantum Logistic mapping; 3D Arnold mapping; scrambling

随着互联网的飞速发展，网络信息安全的问题日益突出，图像、视频等作为网络的主流信息载体，其安全性更是成为网络安全的研究热点。传统的加密算法主要应用于文本信息[1]，不适合大信息量的图像数据。1989 年，R.Matthews 首次利用广义 Logistic 映射生成大量的伪随机数应用于数据加密[2]，由此人们认识到混沌系统具有的特性非常适用于图像加密，此后学者们便研究出了各种各样的基于混沌系统的图像加密算法。L.Zhang 等提出了一种基于离散混沌映射和分段映射的图像加密算法[3]。N K Pareek 等提出了一种新的基于 Lorenz 映射的图像加密算法[4]。X Tong 和 M Cui 提出了基于组合 2 个多项式得到混沌系统应用于图像加密[5]。近 2 年来，学者们又提出了基于量子混沌的图像加密算法。Tajima 等提出了一种利用量子混沌的物理过程的加密算法[6]。Akhshani 等提出了基于量子混沌映射的图像加密算法[7]。单纯地依靠量

收稿日期：2017-09-18
基金项目：内蒙古自治区自然科学基金（2017MS0604）；内蒙古科技大学创新基金（2015XYPYL06）
作者简介：徐扬（1980—），女，硕士，内蒙古科技大学讲师，主要研究方向为计算机图像和大数据。

子混沌映射的图像加密算法在方式上仍显得单一，加密图像的安全性仍然得不到全面的保障，鉴于此，罗玉玲等提出了基于量子 Logistic 映射结合小波域的图像加密算法[8]，进一步改进了量子混沌映射在图像加密方面的应用。

基于以上学者的研究，文中提出基于量子 Logistic 混沌映射结合三维 Arnold 混沌映射的图像加密算法，该算法将成熟的混沌系统和量子混沌映射结合起来应用，既增加了图像加密的复杂度，又有效地解决了计算机精度受限的问题。

1　量子Logistic映射和三维Arnold混沌映射

1.1　量子 Logistic 映射

量子混沌系统具有经典混沌系统的各项属性[9]，同样适用于图像加密。对于一个经典混沌系统，只需改变量化标准就可得到不一样的量子混沌映射，Goggin 等利用反冲转子模型量化经典 Logistic 混沌映射，便产生了量子 Logistic 映射[10]，定义为：

$$\begin{cases} x_{n+1}=r\left(x_n-|x_n|^2\right)-ry_n \\ y_{n+1}=-y_n\,\mathrm{e}^{-2\beta}+\mathrm{e}^{-\beta}r\left[\left(2-x_n-x_n^*\right)y_n-x_nz_n^*-x_n^*z_n\right] \\ z_{n+1}=-z_n\,\mathrm{e}^{-2\beta}+\mathrm{e}^{-\beta}r\left[2\left(1-x_n^*\right)y_n-2x_ny_n-x_n\right] \end{cases} \tag{1}$$

式中：r 为可调参数；β 为耗散参数；x_n, y_n, z_n 为系统状态值；x_n^*, y_n^*, z_n^*分别为 x_n, y_n, z_n 的复共轭。通常情况下，x_n, y_n, z_n 为复数，若为实数，则有 $x_n=x_n^*$，$y_n=y_n^*$, $z_n=z_n^*$。

当 $r\in(3.74, 4.00)$，$\beta\geq3.5$，状态值 $x\in(0, 1)$，$y\in(0, 0.2461)$，$z\in(0, 0.2461)$时，系统（1）处于混沌状态。由于量子 Logistic 映射在末尾具有一个扰动量，而且扰动量在每次迭代更新时都不会消失，因此量子 Logistic 映射不但非周期性得到提高，而且随机性也得到加强[11]。

1.2　三维 Arnold 混沌映射

经典 Arnold 映射是一个混沌变换，一般形式为：

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\mathrm{mod}1) \tag{2}$$

式中：$0\leq x, y\leq1$, $0\leq x', y'\leq1$。经典 Arnold 映射的缺陷是具有周期性，为了克服其周期性，加密算法经常选用加密钥的 Arnold 映射或广义的 Arnold 映射。文中选取了三维广义的 Arnold 映射，与经典的二维 Arnold 映射相比，具有更大的密钥空间，更快的扩散速度，更广的应用范围。三维广义 Arnold 映射一般形式为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix}=\boldsymbol{A}\begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}(\mathrm{mod}N) \tag{3}$$

式中：

$$\boldsymbol{A}=\begin{bmatrix} 1+a_xa_za_y & a_z & a_y+a_xa_z+a_xa_ya_zb_y \\ a_z+a_xb_y+a_xa_zb_yb_z & 1+a_zb_z & a_ya_z+a_xa_ya_zb_z+a_xa_zb_z+a_xa_yb_y+a_x \\ a_xb_xb_y+b_y & b_x & a_xa_yb_xb_y+a_xb_x+a_yb_y+1 \end{bmatrix}。$$

设 $a_x=b_x=a_y=b_y=a_z=b_z=1$，得到三维 Arnold 映射：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix}=\begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix}\begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}(\mathrm{mod}N) \tag{4}$$

系统（4）具有 3 个 Lyapunov 指数，L_1=7.1841，L_2=0.5728，L_3=0.2430，处于混沌状态[12]。其中最大指数远大于一般的混沌系统，表明系统（4）相对于一般的混沌系统，具有更复杂的混沌特性。

2　图像加密系统

首先利用量子 Logistic 混沌映射生成一个长度为 $H\times W$ 的浮点数伪随机序列 S，将 S 中的数据放大取整后进行唯一性检索，将明文图像的像素 $A(i)$ 与 $A(S(i))$ 对应的像素进行置换；再利用三维 Arnold 映射生成一个伪随机整数序列作为中间密文，将其与置乱后的密文像素点进行扩散运算，最终生成加密图像矩阵。加密系统的流程见图 1。

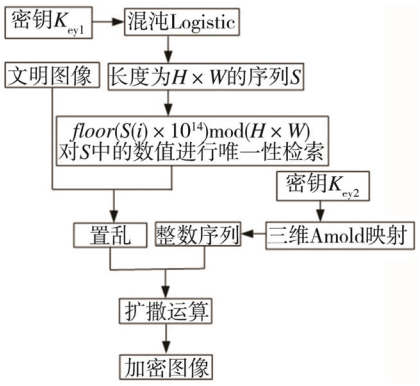


图 1　图像加密系统流程

Fig.1 Flowchart of image encryption system

2.1　置乱

图像置乱就是改变原图像像素的排列顺序，使第三方无法分辨出图像的信息，是数字图像加密常用的技术手段。

1）读取明文图像，获取图像的高和宽（$H\times W$），

并将明文图像展开为一维数组 A。

2）先将量子 Logistic 映射迭代 n（n≥200）次，消除初值影响，再迭代 $H\times W$ 次，将生成的 $H\times W$ 个浮点数存入一维数组 S 中。

3）将 S 中的数据按式（5）运算后，进行唯一性检索，去除重复值，再补充缺失的数据，使其成为长度为 $M\times N$ 的不重复的整数序列。

4）将明文像素点 $A(i)$ 与 $A(S(i))$ 进行互换，完成整体置乱。

$$S_i = floor\left(S_i \times 10^4\right) \bmod \left(H \times W\right) \tag{5}$$

2.2 扩散

扩散就是不改变图像像素的位置只改变像素灰度值的过程。单纯采取像素置乱的方法无法避免攻击者通过明文攻击的方法进行分析[13]，而灰度扩散法能使每个像素的灰度值发生变化，从而避免上述明文攻击，可进一步提高加密图像的安全性[14]。

1）将 Arnold 映射迭代 n 次(n≥200)，消除初值的影响，再迭代 $H\times W$ 次，生成一个序列 D。将 D 中的数据按下列公式计算后存入一维数组 K 中。

$$K_i = floor\left(D_i\right) \bmod 256 \tag{6}$$

2）i 为 1 ~ $H\times W$。迭代系统（1）1 次，生成 x_1, y_1, z_1 后利用下列各式进行扩散运算。

$$C_i = \left(floor\left(x_1 \times 10^4\right) \bmod 256\right) bitxor A_i bitxor K_i \tag{7}$$

$$C_i = \left(floor\left(y_1 \times 10\right) \bmod 256\right) bitxor C_i \tag{8}$$

$$x_0 = x_1 + \sin C_i \tag{9}$$

$$y_0 = y_1 + \sin C_i \tag{10}$$

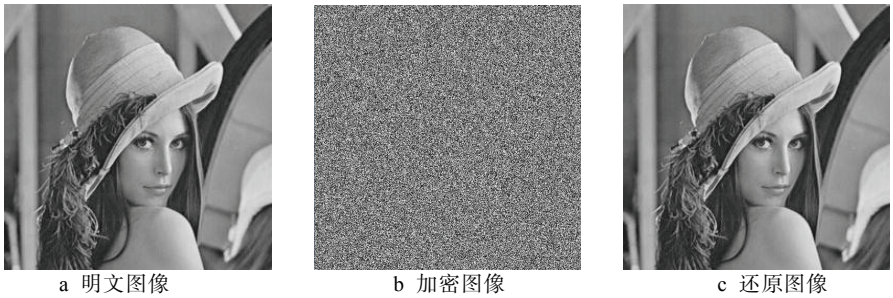
$$z_0 = z_1 + \sin C_i \tag{11}$$

$$i=i+1 \tag{12}$$

将 C 转换为 $H\times W$ 的二维矩阵，便生成密文图像矩阵。加密图像的解密过程与加密过程相反，这里不再赘述。

3 仿真实验测试

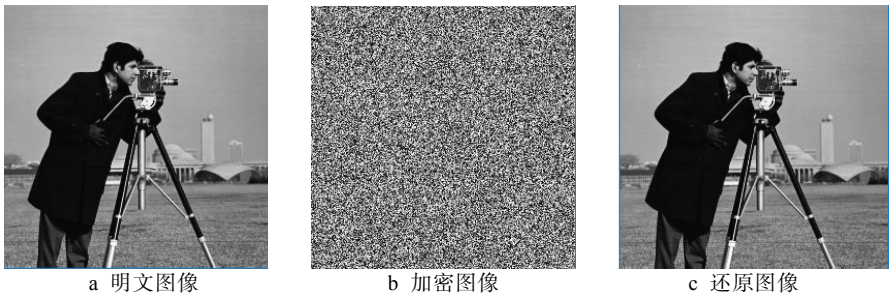
测试环境为 Win7 专业版，CPU 为 Intel I7，测试平台为 Matlab2013a。测试图像选取灰度图像 Lena, Camera 和 Peppers，加密效果见图 2—4。



a 明文图像 b 加密图像 c 还原图像

图 2 Lena 图像加密效果

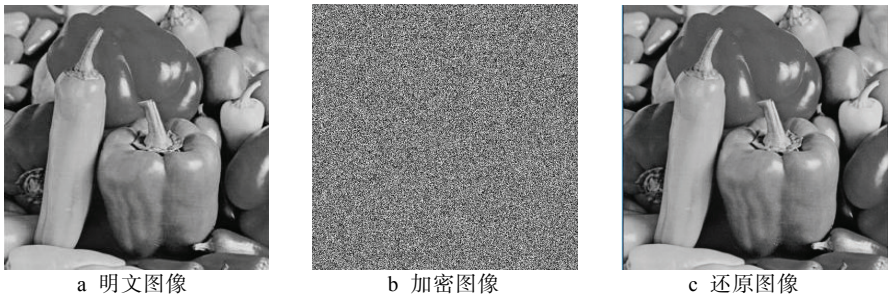
Fig.2 Lena image encryption effect



a 明文图像 b 加密图像 c 还原图像

图 3 Camera 图像加密效果

Fig.3 Camera image encryption effect



a 明文图像 b 加密图像 c 还原图像

图 4 Peppers 图像加密效果

Fig.4 Peppers image encryption effect

3.1　密钥空间

良好的加密系统必须具备足够大的密钥空间来抵抗针对密钥的暴力攻击。当密钥空间大于 2^{100} 时才能为加密系统提高安全可靠的保障[15]。密钥由系统（1）的参数{x_0, y_0, z_0, r, β}构成，其中 x_0, y_0, z_0, r, β 都是 double 型浮点数，文中的计算机为 64 位 CPU，则浮点数精度可达到 10^{-14}，因此密钥空间可达到：$10^{14}\times10^{14}\times10^{14}\times10^{14}\times10^{14}=10^{70}$ 远大于 2^{100}（$\approx1.27\times10^{30}$），可以确定加密系统具有足够大的密钥空间，完全能够抵抗针对密钥的暴力攻击。

3.2　直方图分析

通过对图像直方图的分析，可以确定图像像素点的分布状态。明文和密文的直方图见图 5—7。

由图 5—7 可知，明文的直方图跌宕起伏，而密文的直方图基本上均匀分布在一个矩形区域内。下面通过 χ^2 统计量（单边假设检验）可以对图像的直方图进行评价。对于灰度值等级为 256 的灰度图像，设图像的大小为 $H\times W$，假定直方图中每个灰度值的像素点频数 f_i 服从均匀分布，则 χ^2 统计量计算公式为：

$$\chi^2=\sum_{i=0}^{255}\frac{(f_i-g)^2}{g} \tag{13}$$

式中：$g=H\times W/256$, i=0,1,2…255。

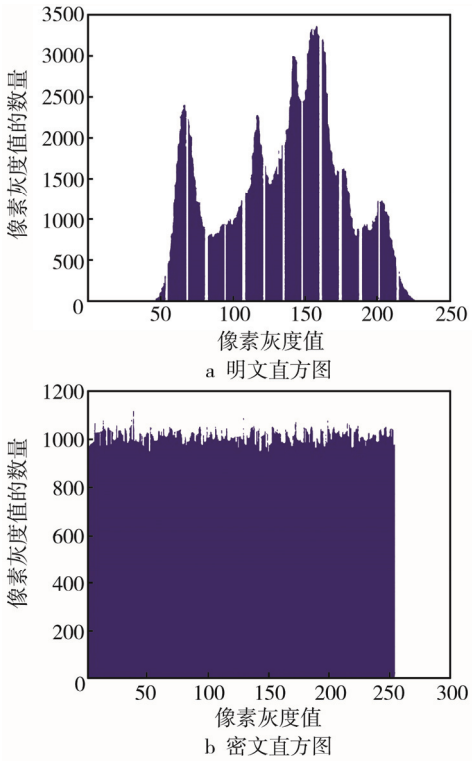


图 5　Lena 明文和密文的直方图

Fig.5 Histogram of plaintext and ciphertext in Lena

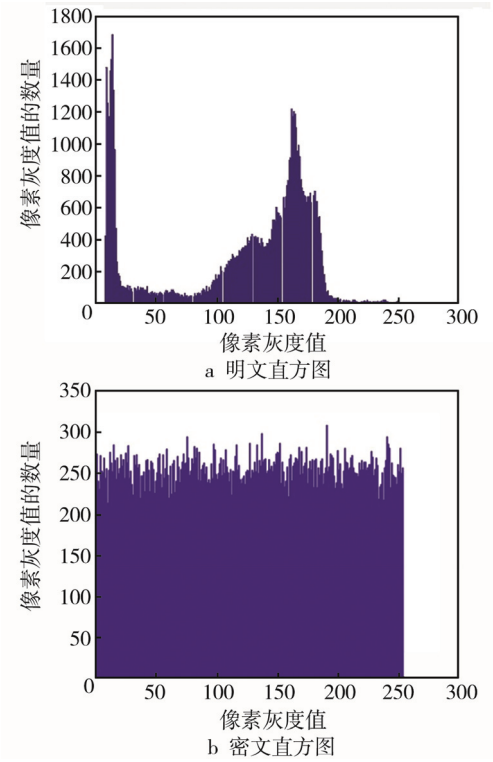


图 6　Camera 明文和密文的直方图

Fig.5 Histogram of plaintext and ciphertext in Camera

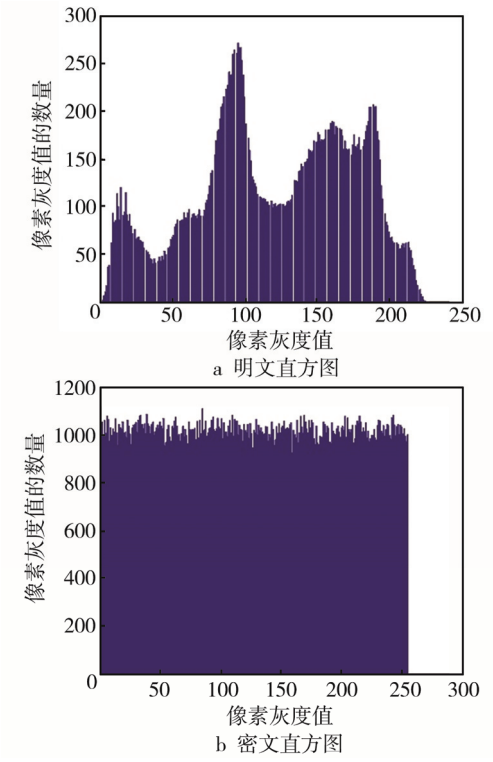


图 7　Peppers 明文和密文的直方图

Fig.7 Histogram of plaintext and ciphertext in Peppers

当显著水平 α=0.01, 0.05 和 0.1 时，有 $\chi^2_{0.01}(255)$=310.4574，$\chi^2_{0.05}(255)$=293.2478，$\chi^2_{0.1}(255)$=284.3359。这里采用 α=0.1 进行评价对比，直方图 χ^2 检验结果见表 1。

表 1 直方图 χ^2 检验结果
Tab.1 χ^2 test result of histogram

图像	明文	密文
Lena	2.42×10^5	276.8984
Camera	1.11×10^5	248.2813
Peppers	1.20×10^5	274.9941

从表 1 中看出，各测试图像的明文直方图 χ^2 检验结果均远大于 $\chi^2_{0.1}(255)$的值，而密文的直方图 χ^2 检验结果均小于 $\chi^2_{0.1}$（255）的值，可以认为密文的像素点属于均匀分布。

3.3 相关系数分析

相邻像素的相关系数可以反映出图像像素的扩散程度。相关系数越接近于 0，说明图像的像素点之间越不具备相关性，越接近于 1，则像素点之间越具有相关性。设从图像中选取 N 对相邻的像素点，其灰度值记为（u_i, v_i），i=1,2…N，u_i 的坐标为（x_i, y_i），v_i 的坐标为（x_i+1, y_i），则相关系数计算公式为：

$$r_{xy}=\frac{\mathrm{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \tag{14}$$

$$cov(u,v)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(u))(y_i-E(v)) \tag{15}$$

$$D(u)=\frac{1}{N}\sum_{i=1}^{N}\left(u_i-E(u)\right)^2 \tag{16}$$

$$E(u)=\frac{1}{N}\sum_{i=1}^{N}u_i \tag{17}$$

测试图像及其密文的相关系数测试结果见表 2。从表 2 看出，明文的相关系数都接近于 1，而加密图像的相关系数都接近于 0。Lena 相邻像素点在各方向上的相图见图 8—9。从图 8—9 看出，明文图像的相邻像素点大部分都密集聚集在直线 y=x 附近，而加密图像的相邻像素点均匀分布在一个矩形区域内。表明明文图像的相邻像素点之间具有较强的相关性，而加密图像的相邻像素点之间基本不具备相关性。

3.4 明文敏感性分析

明文敏感性是指使用同一组密钥，对 2 个差别微小的明文图像进行加密，比较得到的 2 个密文图像的差别。明文敏感性的强弱，决定着加密算法抵抗差分攻击的能力，良好的加密算法应该具有强的明文敏感性。明文敏感性可以通过 NPCR（像素改变率）和 UACI（归一化平均改变幅度）2 个指标来衡量，NPCR 反映了 2 幅加密图像对应像素灰度值的改变率，UACI 则反映了灰度值的平均改变幅度[19]。

设 P_1 和 P_2 是 2 个明文图像，并且它们仅在第（i,j）点的像素灰度值不同，设 C_1（i, j）和 C_2（i, j）为 P_1 和 P_2 的密文图像在第（i, j）点像素的灰度值，则 NPCR 和 UACI 的计算公式为：

$$\mathrm{NPCR}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)\times100\% \tag{18}$$

表 2 相关系数测试结果
Tab.2 Test results of correlation coefficient

图像	方向	密文			
		文中	文献[16]	文献[17]	文献[18]
Lena	水平	0.0019	−0.0066	0.0011	−0.0063
	垂直	0.0098	−0.0089	0.0098	−0.0109
	对角	−0.0049	0.0424	−0.0227	−0.0154
Camera	水平	−0.0085	0.0063	−0.0047	−0.0009
	垂直	0.0062	−0.0142	−0.0195	−0.0223
	对角	0.0082	0.0168	0.0279	0.0025
Peppers	水平	0.0017	0.0194	0.0071	0.0038
	垂直	−0.0098	−0.0091	−0.0065	−0.0082
	对角	0.0011	0.0123	−0.0165	0.0078

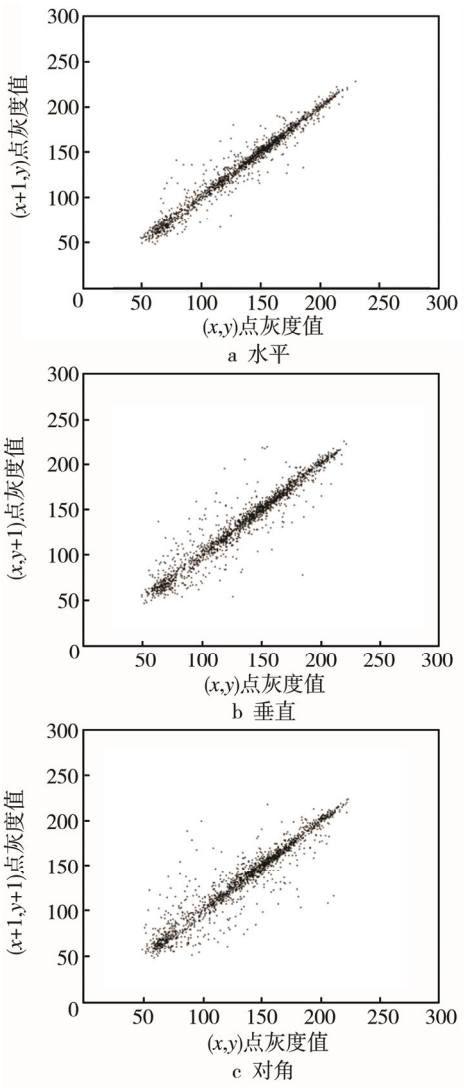


图 8 Lena 明文相邻像素点各方向相图
Fig.8 Phase diagrams of each direction of adjacent pixels in Lena plaintext

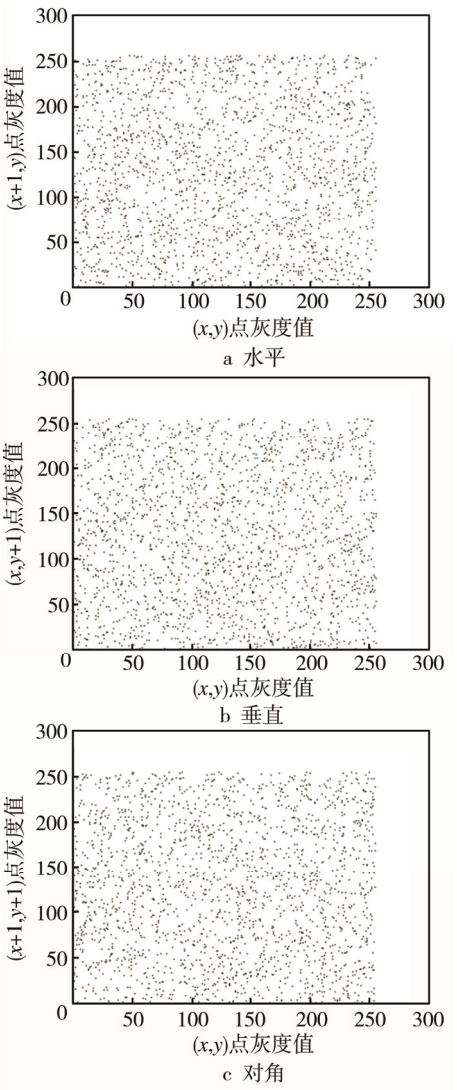


图 9　Lena 密文相邻像素点各方向相图

Fig.9 Phase diagrams of each direction of the adjacent pixels of Lena ciphertext

$$\mathrm{UACI}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \quad (19)$$

$$D(i,j)=\begin{cases}0, C_1(i,j)=C_2(i,j)\\ 1, C_1(i,j)\neq C_2(i,j)\end{cases} \quad (20)$$

式中：NPCR 和 UACI 的理论期望值分别为 99.6054%和 33.4635%。

测试过程如下所述。

1）对于明文图像 P_1，使用密钥 K_{ey} 对 P_1 进行加密，得到加密图像 C_1。

2）从 P_1 中随机选取 1 个像素点，改变该像素点的值（变化量为 1），得到另一明文图像 P_2，使用密钥 K_{ey} 对其加密，得到加密图像 C_2。

3）比较 C_1 和 C_2 的差别，计算 NPCR 和 UACI 的值。

4）重复第 2），3）步 1000 次，计算每次 NPCR 和 UACI 的值，最后计算 1000 组 NPCR 和 UACI 的平均值。

明文敏感性测试结果见表 3。从表 3 看出，文中各测试图像的 NPCR 和 UACI 的测试结果与各文献的测试结果相比，更接近于理论值，表明加密系统具有较强的明文敏感性，可以有效地“抵抗选择明文攻击”和“已知明文攻击”。

表 3　明文敏感性测试结果

Tab.3 Test results of plaintext sensitivity

图像	文中		文献[8]		文献[16]		文献[18]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.60	33.42	99.50	33.38	99.55	33.35	99.62	33.81
Camera	99.60	33.46	99.60	33.47	99.57	33.37	99.62	33.73
Peppers	99.59	33.45	99.49	33.35	99.58	33.35	99.57	33.47

3.5　密钥敏感性分析

密钥的敏感性是指初始密钥发生微小变化时而引起的加密图像的变化程度。良好的图像加密系统应该具有很强的密钥敏感性，能够有效地抵抗各种针对密钥的攻击。测试方法：选取初始密钥 $K_{\mathrm{ey}}=\{x_0, y_0, z_0, r, \beta\}$ 空间中的 1000 组值，对于每组密钥，依次选取 $\{x_0, y_0, z_0, r, \beta\}$ 中的一个量，使其微增 10^{-13}，而其他的量保持不变，加密同一明文图像，分析得到的 2 个密文图像的差异，计算它们的 NPCR 和 UACI，然后计算 1000 次测试得到的 NPCR 和 UACI 的平均值。密钥敏感性测试结果见表 4。从表 4 看出，密钥各分量的 NPCR 和 UACI 都非常接近于理论值，表明加密系统具有较强的密钥敏感性，可以有效地抵抗各种针对密钥的攻击。

表 4　密钥敏感性测试结果

Tab.4 Test results of key sensitivity

算法	图片	*x*		*y*		*z*	
		NPCR	UACI	NPCR	UACI	NPCR	UACI
文中	Lena	99.59	33.44	99.6	33.44	99.6	33.41
	Camera	99.6	33.42	99.6	33.46	99.6	33.44
	Peppers	99.6	33.44	99.6	33.45	99.6	33.43
文献[8]	Lena	99.59	33.41	99.6	33.41	99.66	33.38
	Camera	99.61	33.58	99.63	33.53	99.62	33.55
	Peppers	99.61	33.54	99.64	33.45	99.59	33.46

3.6　信息熵

信息熵可以看成是数学上离散随机事件的出现概率。一个系统越是混乱，信息熵就越高，在数字图像中，像素的灰度值分布越均匀，信息熵越大，随机性越大，安全性就越高[19]。信息熵的计算公式为：

$$H=\sum_{i=1}^{L}p(x_i)\log_2\frac{1}{p(x_i)} \quad (22)$$

式中：L 为图像的灰度等级数（通常为 256）；$p(x_i)$ 为灰度值 x_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。信息熵测试结果见表 5。从表 5 看出，测试图像信息熵的测试结果较各文献的测试结果更接近于理论值 8，表明加密系统的算法随机性良好，不确定性高，安全性好，能够有效地抵抗相关熵的攻击。

表 5 信息熵测试结果

Tab.5 Test results of information entropy

图像	文中	文献[16]	文献[17]	文献[18]
Lena	7.9991	7.9951	7.9965	7.9964
Camera	7.9973	7.9955	7.9964	7.9990
Pepeprs	7.9992	7.9965	7.9958	7.9971

4 结语

提出了一种基于量子 Logistic 混沌映射结合三维 Arnold 混沌映射的图像加密算法。加密算法首先利用量子 Logistic 映射生成伪随机序列，对明文图像进行整体置乱，再利用 Arnold 映射生成一个整数序列，与置乱后的密文进行扩散运算而得到最终加密图像。通过引入量子 Logistic 映射和高维 Arnold 映射，增强了置乱、扩散效果，提高了加密的复杂度。实验仿真证明了文中的加密算法具有密钥空间大、敏感性强、安全性高等特点。

参考文献：

[1] DIFFIE W, HELLMAN M. New Directions in Cryptography[J]. IEEE Transactions on Information Theory, 1976, 2(6): 644—654.

[2] MATTHEWS R. On the Derivation of a "Chaotic Encryption Algorithm"[J]. Cryptologin, 1989, 13(1): 29—42.

[3] ZHANG L, LIAO X, WANG X. An Image Encryption Approach Based on Chaotic Maps[J]. Chaos, Solutions and Fractals, 2005, 24(3): 759—765.

[4] PAREEK N K, PATIDAR V, SUD K K. Image Encryption Using Chaotic Logistic Map[J]. Image and Vision Computing, 2006, 24(9): 926—934.

[5] TONG X, CUI M. Image Encryption with Compound Chaotic Sequence Cipher Shifting Dynamically[J]. Image and Vision Computing, 2008, 26(6): 843—850.

[6] TAJIMA A, TANAKA A, MAEDA W, et al. Pratical Quantum Cryptosystem for Metro Area Application[J]. IEEE Journal of Selected Topics in Quantum Elextronics, 2007, 13(4): 1031—1038.

[7] AKHSHANI A, AKHAVAN A, LIM S C, et al. An Image Encryption Scheme Based on Quantum Logistic Map[J]. Communications in Nonlinear Science and Numerical Simulatyion, 2012, 17(12): 4653—4661.

[8] 罗玉玲，杜明辉. 基于量子 Logistic 映射的小波域图像加密算法[J]. 华南理工大学学报(自然科学版), 2013, 41(6): 53—62.
LUO Yu-ling, DU Ming-hui. Image Encryption Algorithm Based on Quantum Logistic Map in Wavelet Domain[J]. Journal of Sourth China University of Technology(Natrural Science Edition), 2013, 41(6): 53—62.

[9] BEERY M V, BALAZS N L, TABOR M, et al. Quantum Maps[J]. Annals of Physics, 1979, 122(1): 26—63.

[10] GOGGIN M E, SUNDARAM B, MILONNI P W. Quantum Logistic Map[J]. Physics Review A, 1990, 41 (10): 5705—5708.

[11] 谢国波，杨彬. 基于比特置乱的量子混沌图像加密算法[J]. 计算机工程, 2017, 43(7): 182—186.
XIE Guo-bo, YANG Bin. Quantum Chaos Image Encryption Algorithm Based on Bit Scrambling[J]. Computer Engineering, 2017, 43(7): 182—186.

[12] 孙燮华. 图像加密算法与实践-基于 C#语言实现[M]. 北京：科学出版社, 2013.
SUN Xie-hua. Image Encryption Algorithms and Practices with Implementtations in C#[M]. Beijing: Science Press, 2013.

[13] 刘家胜，朱灿焰，汪一鸣，等. 基于位置相关性的图像置乱效果评价方法[J]. 计算机工程，2010，36(24): 208—210.
LIU Jia-sheng, ZHU Can-yan, WANG Yi-ming, et al. Image Scrambling Effect Evaluation Method Based on Position Correlation[J]. Computer Engineering, 2010, 36(24): 208—210.

[14] 王帅，孙伟，郭一楠，等. 一种多混沌快速图像加密算法的设计与分析[J]. 计算机应用研究, 2015, 32(2): 512—515.
WANG Shuai, SUN Wei, GUO Yi-nan, et al. Design and Analysis of Fast Image Encryption Algorithm Based on Multiple Chaotic System[J]. Application Research of Computers, 2015, 32(2): 512—515.

[15] NOROUZI B, SEYEDZADEH S M, MIRZAKUCHAKI S, et al. A Novel Image Encryption Based on Row-column, Masking and Main Diffusion Processes with Hyper Chaos[J]. Multimedia Tools and Applications, 2013, 74(3): 781—811.

[16] WANG X, LIU L, ZHANG Y. A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique[J]. Opt Lasers Eng, 2015, 66: 10—8.

[17] HUA Z, ZHOU Y, PUN C M, CHEN P C L. 2D Sine Logistic Modulation Map for Image Encryption[J]. Inf Sci, 2015, 297: 80—94.

[18] WANG X Y, YANG L, LIU R, KADIR A. A Chaotic Image Encryption Algorithm Based on Perceptron Model[J]. Nonlinear Dyn, 2010, 62(3): 615—621.

[19] AZZAZ M S, TANOUGAST C, SADOUDI S, et al. Robust Chaotic Key Stream Generateor for Real-time Images Encryption[J]. Journal of Real-Time Image Processing, 2013, 8(3): 297—306.