文章编号 1004-924X(2017)03-0749-07

量子混沌与折叠算法的图像加密系统

金 聪*,刘 会
(华中师范大学 计算机学院,湖北 武汉 430079)

摘要:本文提出一种量子混沌与折叠算法相结合的图像加密系统。该系统的主要思想是通过量子混沌映射和二维 Logistic 映射分别进行 Arnold 变换,得到两个由伪随机数组成的与灰度图像大小相等的矩阵 ***Q***、***E***,然后利用这两个矩阵对图像分别进行以下操作:一是利用矩阵 ***Q*** 对图像从 4 个方向进行"折叠操作",二是使用前一个像素值与当前像素值进行异或,然后将异或得到的值加上 ***E*** 对应的值,以对当前像素值进行修改,从而达到图像扩散的效果,增加差分攻击的难度。利用 MATLAB 对测试图像进行模拟仿真分析,结果显示,经该加密系统加密后的图像,其水平、竖直和对角线方向像素值的相关性分别为 0.001 006、0.000 152、0.000 789,信息熵 $H(s)=7.997\ 3$。一系列的实验结果表明该加密系统具有很高的安全性和随机性。

关 键 词:量子混沌映射;Logistic 映射;Arnold 变换;折叠操作;差分攻击
中图分类号:TP391 **文献标识码**:A **doi**:10.3788/OPE.20172503.0749

An image encryption scheme based on quantum chaos and folding algorithm

JIN Cong*, LIU Hui

(*School of Computer, Central China Normal University, Wuhan* 430079, *China*)
* *Corresponding author, E-mail: jinc26@aliyun.com*

Abstract: An image encryption system combining quantum chaos with folding algorithm was proposed. The main idea of the proposed algorithm is to make Arnold transform through quantum chaos map and 2D Logistic map respectively, to generate the matrix ***Q*** and the matrix ***E***, and the two matrices were made of pseudo random numbers and identical to grayscale image. Then, such matrices were used for two operations on the image and to achieve image encryption, as follows: one was to achieve "folding operation" on image at four directions by application of matrix ***Q*** and another was to execute nonequivalence of the former pixel value and present pixel value, plus the values after nonequivalence with ***E*** corresponding value, so the modification of present pixel value was obtained and the effect of image diffusion was realized and the difficulty of the differential attack was increased. Simulation analysis on tested image was conducted by application of MATLAB and the results show that for images encrypted by such encryption system, the correlations of pixel value at horizontal, vertical and diagonal directions are 0.001 006, 0.000 152 and 0.000 789 respectively, with entropy $H(s)=7.997\ 3$. The results of a series of tests show that the proposed encryption system has highly security and randomness.

Key words: quantum chaotic map; logistic map; Arnold transform; folding operation; differential attack

收稿日期:2016-12-21;**修订日期**:2017-01-15.
基金项目:华中师范大学中央高校基本科研业务费项目资助(No. CCNU15GF007)

1 引　言

由于图像数据信息量非常庞大，而且相邻两像素间具有较强的相关性，因此一些传统加密算法，比如 RSA(Rivers Shamir Adleman)[1]不适合对图像加密。混沌映射[2]因能以很小的时间代价达到很高的加密标准而深受信息安全研究者的青睐，其中量子混沌[3]的优势尤为明显。为了使量子混沌映射得到的伪随机序列的随机性更强，本文通过采用广义的二维 Arnold 变换[4-5]，同时为其添加了一对密钥以扩大该加密系统的密钥空间，从而提高加密系统的复杂度。

Akhshani A 等[6]证明了基于量子混沌映射的伪随机数发生器所产生的伪随机序列具有极弱的相关性和极强的遍历性。图像加密通常采用置乱加密方式，置乱加密的方式有很多种，其中包括 RGB 平移置乱加密[7]、SCAN 模式加密[8]等。在本文的置乱过程中，采用了一种新的加密方法：折叠算法。另外，为了提高混沌系统对初始条件的敏感性，本文将量子混沌映射和二维 Logistic 映射[9-10]代入到最邻近耦合映像格子(Nearest-neighboring Coupled-map Lattices，NCML)中[11-12]。本文的主要贡献有：(1)提出了一种新的加密算法：折叠算法，并通过试验证明该算法具有良好的混乱性能；(2)将二维 Logistic 映射引入到置乱算法中，大大降低了相邻两像素的相关性，获得了良好的扩散效果。

2 系统理论基础

2.1 量子混沌映射

耗散量子系统[6]与谐振子路径耦合会产生带有量子修正的量子 logistic 映射：

$$\begin{aligned}\varphi_1(x'_n)&=r(x'_n-|x'_n|^2)-ry'_n,\\ \varphi_1(y'_n)&=-y'_n\mathrm{e}^{-2\beta}+\\ &\mathrm{e}^{-\beta}r[(2-x'_n-x'^{*}_n)y'_n-x'_nz'^{*}_n-x'^{*}_nz'_n],\\ \varphi_1(z'_n)&=-z'_n\mathrm{e}^{-2\beta}+\\ &\mathrm{e}^{-\beta}r[2(1-x'^{*}_n)z'_n-2x'_ny'_n-x'_n].\end{aligned}\tag{1}$$

式中：$x'=\langle\alpha\rangle$，$y'=\langle\delta\alpha^{\dagger}\delta\alpha\rangle$，$z'=\langle\delta\alpha\ \delta\alpha\rangle$，$\beta$ 是耗散参数，r 是控制参数。通常情况下 x'_n，y'_n，z'_n 和 y 都为复数，x'^{*}_n 和 z'^{*}_n 分别是 x'_n 和 z'_n 的共轭复数。如果设该混沌系统中的初始值为实数，那么系统接下来所产生的混沌序列则都为实数，并且有 $x'^{*}_n=x'_n$，$z'^{*}_n=z'_n$。这些参数的取值分别为：$x'_n\in[0,1]$，$y'_n\in[0,0.1]$，$z'_n\in[0,0.2]$，$\beta\in[6,+\infty]$，$r\in[0,4]$。Akhshani A[6]等人已经证明了当 $r=3.99$，$\beta\geqslant6$ 时该混沌映射的随机性最好。

2.2 二维 Logistic 映射

Logistic 映射具有表达式简单、性能优良等优点，是最常用的混沌映射之一。二维 Logistic 映射[9-10]的定义如下：

$$\begin{aligned}\varphi_2(x_n)&=\mu_1x_n(1-x_n)+\gamma_1y_n^2,\\ \varphi_2(y_n)&=\mu_2y_n(1-y_n)+\gamma_2(x_n^2+x_ny_n).\end{aligned}\tag{2}$$

当参数满足：$\mu_1\in(2.75,3.4]$，$\mu_2\in(2.75,3.45]$，$\gamma_1\in(0.15,0.21]$，$\gamma_2\in(0.13,0.15]$时上述映射成为混沌映射，其中 x_n，$y_n\in(0,1)$。

2.3 带有密钥的广义 Arnold 变换

设明文图像中某像素点所在位置的坐标为 (x,y)，经过 Arnold 变换后该点的坐标为 (x',y')。根据文献[4-5]可知，广义 Arnold 变换定义如下：

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\mathbf{A}\begin{bmatrix}x\\y\end{bmatrix}(\mathrm{mod}\ \mathrm{N}),\mathbf{A}=\begin{bmatrix}1&a\\b&ab+1\end{bmatrix},\tag{3}$$

式(3)中 $\mathrm{N}=256$。为了提高该加密系统的安全性，本文将参数 a，b 都设为密钥，同时添加矩阵 $(ku,kv)^{\mathrm{T}}$ 作为密钥。由此给出了带有密钥的广义 Arnold 变换的定义：

$$\begin{bmatrix}x'\\y'\end{bmatrix}=\mathbf{A}^n\begin{bmatrix}x\\y\end{bmatrix}+\begin{bmatrix}ku\\kv\end{bmatrix}(\mathrm{mod}\ \mathrm{N}),\mathbf{A}=\begin{bmatrix}1&a\\b&ab+1\end{bmatrix},\tag{4}$$

式中 n 表示迭代次数。

2.4 最邻近耦合映像格子

最邻近耦合映像格子(NCML)的定义如下：

$$z_{n+1}(j)=(1-\varepsilon)\varphi(z_n(j+1))+\varepsilon\varphi(z_n(j+1)),\tag{5}$$

式中 $n=0,1,\cdots,L-1$，表示迭代次数；L 表示明文图像的长度；φ 代表混沌映射；$\varepsilon\in(0,1)$是耦合参数。当参数 $\varepsilon=0.001$ 时该等式具有良好的混沌特性[12]。根据周期性，本文将 $z_n(j+T)=z_n(j)$ 代入到该系统中进行计算。

将等式(1)代入到等式(5)中：

$$\begin{aligned}x'_{n+1}&=(1-\varepsilon)\varphi(x'_{n+1})+\varphi(y'_{n+1}),\\ y'_{n+1}&=(1-\varepsilon)\varphi(y'_{n+1})+\varphi(z'_{n+1}),\\ z'_{n+1}&=(1-\varepsilon)\varphi(z'_{n+1})+\varphi(x'_{n+1}).\end{aligned}\tag{6}$$

同样，将等式(2)代入到等式(5)中，有：

$$x_{n+1}=(1-\varepsilon)\varphi(x_n)+\varepsilon\varphi(y_n),$$
$$y_{n+1}=(1-\varepsilon)\varphi(y_n)+\varepsilon\varphi(x_n). \quad (7)$$

迭代等式(6)、(7)即得到所需要的伪随机序列。

3　加密过程

本文的加密过程包括 3 个阶段：密钥发生器、混乱阶段和扩散阶段。

密钥发生器：

该加密系统采用了 128 位外部密钥 K，将 K 分成 16 个 8 位的二进制分段密钥 $k_i(i=1,2,\cdots,16)$，即：

$$K=k_1,k_2,\cdots,k_{16}. \quad (8)$$

将分段密钥 $k_i(i=1,2,\cdots,16)$分别进行以下操作得到相应参数：

$\mu_1=0.75+\mathrm{mod}(k_1/N,0.06)$，$\mu_2=2.75+\mathrm{mod}(k_2/N,0.7)$；$\gamma_1=0.15+\mathrm{mod}(k_3/N,0.06)$，$\gamma_2=0.13+\mathrm{mod}(k_4/N,0.02)$；$x_0=k_5/N$，$y_0=k_6/N$；$x_0'=k_7/N$，$y_0'=\mathrm{mod}(k_8/N,0.2)$，$z_0'=\mathrm{mod}(k_9/N,0.1)$；$a=k_{10}$，$b=k_{11}$，$ku=k_{12}$，$kv=k_{13}$；$n_0=k_{14}$，$m_1=k_{15}$，$m_2=k_{16}$。

将公式(6)、(7)分别迭代 m_1+L 和 m_2+L 次，为了消除混沌序列前若干项的干扰，本文分别丢弃混沌序列的前 m_1 项和 m_2 项。将剩下的 L 项按照一定的规则进行排列，组成混沌矩阵 $\boldsymbol{Q}$、$\boldsymbol{E}$。

代入初始参数(x_0,y_0,z_0)和 m_1，对于量子混沌映射，其排列规则如下：

$$\boldsymbol{Q}(3i-2)=(x_{i+m_1}\times N\times N\times 10^3)\bmod 256,$$
$$\boldsymbol{Q}(3i-1)=(y_{i+m_1}\times N\times N\times 10^3)\bmod 256,$$
$$\boldsymbol{Q}(3i)=(z_{i+m_1}\times N\times N\times 10^3)\bmod 256. \quad (9)$$

代入初始参数(x_0',y_0')和 m_2，对于量子混沌映射，则其排列规则如下：

$$\boldsymbol{E}(2i-1)=(x'_{i+m_2}\times N\times N\times 10^3)\bmod 256,$$
$$\boldsymbol{E}(2i)=(x'_{i+m_2}\times N\times N\times 10^3)\bmod 256, \quad (10)$$

其中 $i=1,2,\cdots,L$。

代入初始参数 a,b 和(ku,kv)，本文对得到的混沌矩阵 $\boldsymbol{Q}$ 和 $\boldsymbol{E}$ 按照公式(4)进行带有密钥的广义 Arnold 变换，得到矩阵 $\boldsymbol{Q}'$、$\boldsymbol{E}'$。

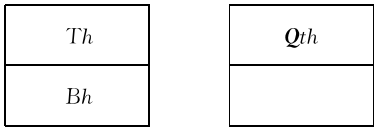
混乱阶段：

混乱阶段是利用矩阵 $\boldsymbol{Q}'$从 4 个方向对图像进行折叠加密，具体的加密过程如下。

(1)将明文图像 P 的上半部分 Th 与矩阵 $\boldsymbol{Q}'$ 的上半部分 $\boldsymbol{Q}th$ 异或并赋值给 Th，然后将结果与明文图像的下半部分 Bh 异或，得到从上到下进行折叠操作后的密文图像 P_1：

$$Th(i,j)=Th(i,j)\oplus\boldsymbol{Q}th(i,j),$$
$$Bh(N-i+1,j)=Bh(N-i+1,j)\oplus Th(i,j), \quad (11)$$

其中 i,j 分别代表像素值的行下标和列下标，$i=1,2,\cdots,N/2$；$j=1,2,\cdots,N$。



(a)明文图像 P　(b)混沌矩阵 $\boldsymbol{Q}'$
(a)Plain-image P　(b)Chaotic matrix $\boldsymbol{Q}'$

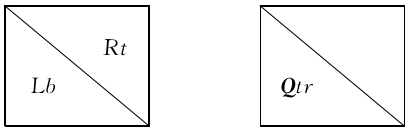
图 1　从上往下折叠

Fig. 1　Folding from top to bottom

(2)将密文图像 P_1 的右上半部分 Rt 与矩阵 $\boldsymbol{Q}'$的右上半部分 $\boldsymbol{Q}rt$ 异或并赋值给 Rt，然后将结果与密文图像 P_1 的下半部分 Lb 异或，得到从右上到左下进行折叠操作后的密文图像 P_2：

$$Rt(i,j)=Rt(i,j)\oplus\boldsymbol{Q}rt(i,j),$$
$$Lb(j,i)=Lb(j,i)\oplus Rt(i,j), \quad (12)$$

其中 i,j 分别代表像素值的行下标和列下标，$i=1,2,\cdots,N$；$j=i+1,i+2,\cdots,N$。



(a)密文图像 P_1　(b)混沌矩阵 $\boldsymbol{Q}'$
(a)Encrypted-image P_1　(b)Chaotic matrix $\boldsymbol{Q}'$

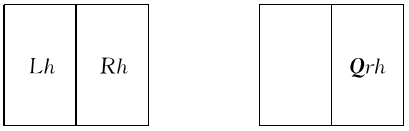
图 2　从右上往左下折叠

Fig. 2　Folding from top right to bottom left

(3)将密文图像 P_2 的右半部分 Rh 与矩阵 $\boldsymbol{Q}'$ 的右半部分 $\boldsymbol{Q}rh$ 异或并赋值给 Rh，然后将结果与密文图像 P_2 的左半部分 Lh 异或，得到从右到左进行折叠操作后的密文图像 P_3：

$$Rh(i,j)=Rh(i,j)\oplus\boldsymbol{Q}rh(i,j),$$
$$Lh(i,N-j+1)=Lh(i,j)\oplus Rh(i,N-j+1), \quad (13)$$

其中 i,j 分别代表像素值的行下标和列下标，$i=1,2,\cdots,N$；$j=N/2+1,N/2+2,\cdots,N$。



(a)密文图像 P_2　(b)混沌矩阵 $\boldsymbol{Q}'$

(a)Encrypted-image P_2　(b)Chaotic matrix $\boldsymbol{Q}'$

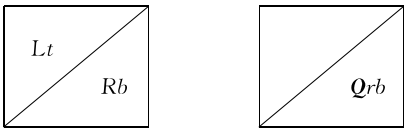
图 3　从右往左折叠

Fig. 3　Folding from right to left

(4)将密文图像 P_3 的右下半部分 Rb 与矩阵 $\boldsymbol{Q}'$ 的右半部分 $\boldsymbol{Q}rb$ 异或并赋值给 Rb，然后将结果与密文图像 P_3 的左上半部分 Lt 异或，得到从右下到左上进行折叠操作后的密文图像 P_4：

$$Rb(i,j)=Rb(i,j)\oplus\boldsymbol{Q}rb(i,j),$$
$$Lt(i,j)=Rb(j,i)\oplus Lt(i,j),\quad(14)$$

其中 i,j 分别代表像素值的行下标和列下标，$i=1,2,\cdots,N;j=N-i+2,N-i+3,\cdots,N$。



(a)密文图像 P_3　(b)混沌矩阵 $\boldsymbol{Q}'$

(a)Encrypted-image P_3　(b)Chaotic matrix $\boldsymbol{Q}'$

图 4　从右下往左上折叠

Fig. 4　Folding from bottom right to top left

扩散阶段：

扩散的意义是当改变原图的一个比特时，其加密图像将以不可预测的方式完全改变，从而可以抵抗差分攻击。将经过折叠加密得到的密文图像 P_4 和混沌矩阵 $\boldsymbol{E}'$ 分别转换成长度为 L 的向量 $\boldsymbol{C}$ 和 $\boldsymbol{I}$。本文提供的扩散公式如下：

$$\boldsymbol{C}_1'=(n_0\oplus\boldsymbol{C}_1+\boldsymbol{I}_1)\bmod 256,$$
$$\boldsymbol{C}_i'=(\boldsymbol{C}_{i-1}\oplus\boldsymbol{C}_i+\boldsymbol{I}_i)\bmod 256,\quad(15)$$

其中 $i=2,3,\cdots,L$。将得到的向量 $\boldsymbol{C}'$ 重新转换成二维矩阵 $\boldsymbol{P}'$，$\boldsymbol{P}'$ 即为最终的加密图像。至此，图像加密过程完成。

4　解密过程

按照混乱阶段和扩散阶段的逆过程，可以对密文图像实现解密。具体的实现步骤如下：

(1)将相同的密钥 K 代入密钥发生器中，得到初始值与混沌矩阵 $\boldsymbol{Q}'$、$\boldsymbol{E}'$。

(2)同样，将混沌矩阵 $\boldsymbol{E}'$ 和 $\boldsymbol{P}'$ 转换成长度为 $L=N\times N$ 的向量 $\boldsymbol{I}$ 和 $\boldsymbol{C}'$，经过如下解密算法可实现对加密图像 $\boldsymbol{P}'$ 的初步解密：

$$\boldsymbol{C}_i=[(\boldsymbol{C}_i'-\boldsymbol{I}_i+256)\bmod 256]\oplus\boldsymbol{C}_{i-1}',$$
$$\boldsymbol{C}_1=[(\boldsymbol{C}_1'-\boldsymbol{I}_1+256)\bmod 256]\oplus n_0,\quad(16)$$

其中 $i=L,L-1,\cdots,2$ 是矩阵的下标，$\boldsymbol{C}$ 为对扩散阶段解密后得到的向量。

(3)将向量 $\boldsymbol{C}$ 转换为相应的二维矩阵 $\boldsymbol{P}_4$，实现对折叠加密的解密，如下：

$$Lt(i,j)=Rb(j,i)\oplus Lt(i,j),$$
$$Rb(i,j)=Rb(i,j)\oplus\boldsymbol{Q}rb(i,j),\quad(17)$$

其中 $i=1,2,\cdots,N;j=N-i+2,N-i+3,\cdots,N$。这样就实现了对折叠加密的第一轮解密，得到矩阵 $\boldsymbol{P}_3$。

$$Lh(i,N-j+1)=Lh(i,j)\oplus Rh(i,N-j+1),$$
$$Rh(i,j)=Rh(i,j)\oplus\boldsymbol{Q}rh(i,j),\quad(18)$$

其中 $i=1,2,\cdots,N;j=N/2+1,N/2+2,\cdots,N$。这样就实现了折叠加密的第二轮解密，得到矩阵 $\boldsymbol{P}_2$。

$$Lb(j,i)=Lb(j,i)\oplus Rt(i,j),$$
$$Rt(i,j)=Rt(i,j)\oplus\boldsymbol{Q}rt(i,j),\quad(19)$$

其中 $i=1,2,\cdots,N;j=i+1,i+2,\cdots,N$。这样就实现了折叠加密的第三轮解密，得到矩阵 $\boldsymbol{P}_1$。

$$Bh(N-i+1,j)=Bh(N-i+1,j)\oplus Th(i,j),$$
$$Th(i,j)=Th(i,j)\oplus\boldsymbol{Q}th(i,j),\quad(20)$$

其中 $i=1,2,\cdots,N/2;j=1,2,\cdots,N$。此时得到的矩阵 $\boldsymbol{P}$ 即为明文图像。至此，解密完成。

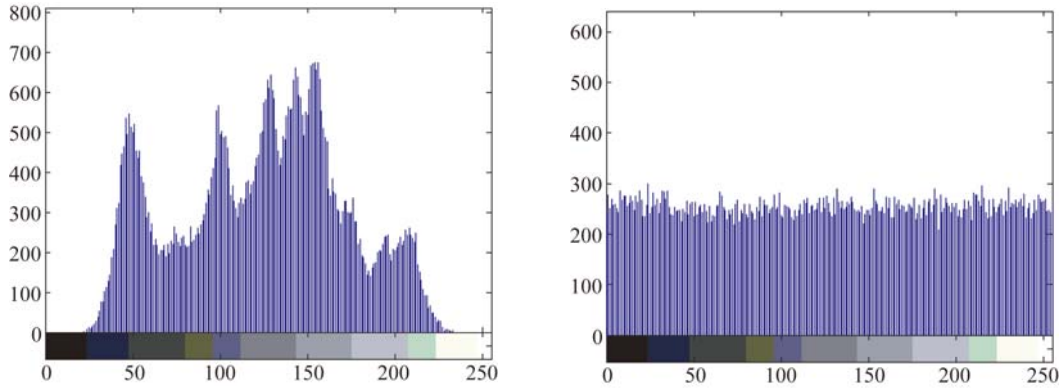
5　性能分析

本文选取大小为 256×256 的 Lena 图像作为测试对象，分别从统计分析，扩散性测试，密钥空间分析和信息熵测试等多个角度对图像的加密效果进行分析。

5.1　统计分析

5.1.1　直方图分析

图 5 为利用本文方法加密 Lena 图像的直方图。理想加密算法所加密图像的像素值应该有均匀的频率分布，直方图可以准确地反应图像各个像素值的频率分布。图 5 所示的密文图像的直方图不依赖于明文图像，且分布均匀。这说明本文算法不会提供任何有价值的统计信息，可以有效地防止统计攻击。



(a) Lena 明文图像直方图
(a) Histogram of Lena plain-image

(b) Lena 密文图像直方图
(b) Histogram of Lena encrypted-image

图 5　加密前后 Lena 图像直方图对比

Fig. 5　Comparison of histograms for Lena image before and after encryting

5.1.2　相关性分析

图像的相关性测试是指对图像从水平、竖直、对角线 3 个方向随机选取若干组样本进行相关性计算，相关性越低，表示加密效果越理想。具体的相关性计算方法如下：

$$E=\frac{1}{N}\sum_{i=1}^{N}x_i,$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2,$$

$$Cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)),$$

$$r_{xy}=\frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{21}$$

式中：x、y 分别代表相邻两像素的灰度值，所得到的 r_{xy} 值可反应两相邻像素灰度值的相关性。图 6 给出了经本文算法处理后，明文图像和密文图像在水平方向、竖直方向和对角线方向上相邻两像素点的相关性。定量结果见表 1。

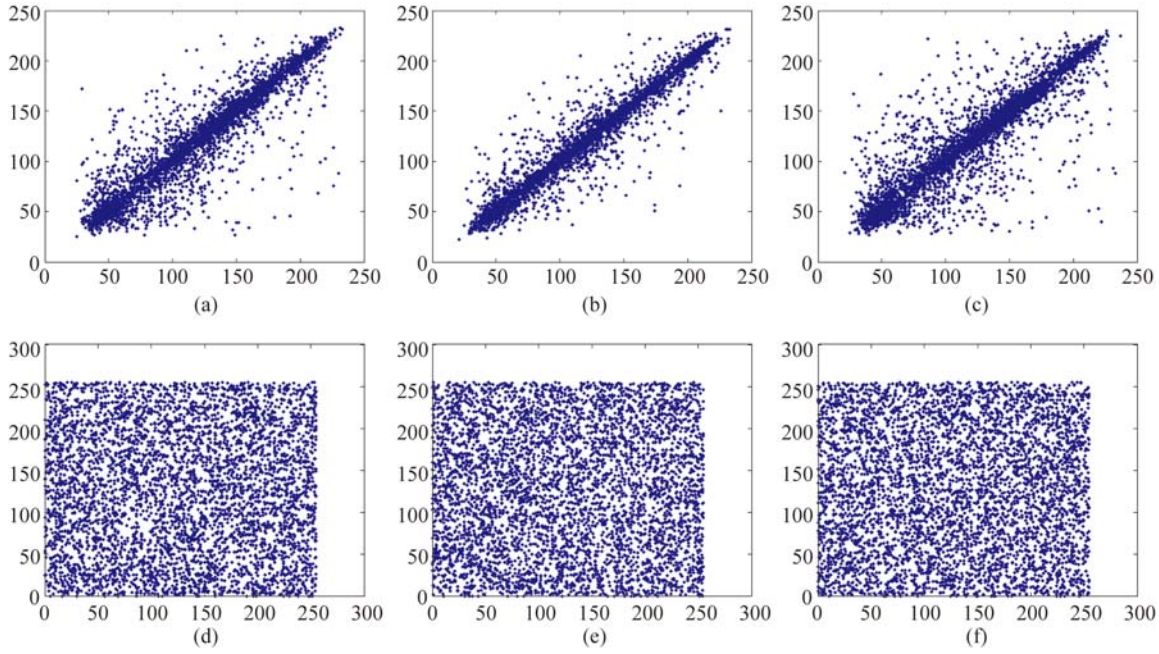


图 6　(a)、(b)、(c)依次表示明文图像水平、竖直、对角线方向相邻的像素分布情况；(d)、(e)、(f)依次表示密文图像水平、竖直、对角线方向相邻的像素分布情况

Fig. 6　(a)、(b)、(c) are pixel distributions for plain-image in horizontal, vertical and diagonal direction respectively; (d)、(e)、(f) are pixel distributions for encrypted-image in horizontal, vertical and diagonal direction respectively

由表 1 可知，密文图像相邻两像素的相关性明显比明文图像相邻两像素的相关性弱。

表 1　明文图像和密文图像相邻像素值的相关性

Tab. 1　Correlation coefficients between plain-image and encrypted-image

扫描方向	Lena				
	明文图	本文	文献[6]	文献[10]	文献[11]
水平	0.932 740	0.001 006	0.000 32	0.001 019	0.014 8
竖直	0.966 433	0.000 152	0.002 74	0.021 391	0.003 7
对角线	0.908 226	0.000 789	0.001 47	0.004 985	0.023 5

5.2　密钥空间分析

理想的加密系统必须具备足够大的密钥空间，以抵抗对密钥空间的暴力破解攻击。根据[13]可以知道，只有当密钥空间大于 2^{100} 时，才能为加密系统的安全性提供良好保障。本文中的密钥流长度为 128 位，密钥空间大小为 2^{128}，足以抵御任何暴力破解攻击。

5.3　信息熵测试

信息熵是研究随机性事件的最重要参数之一[14]。信息熵越大，说明加密效果越好，信息熵的定义如下：

$$H(s)=-\sum_{i=0}^{T-1}p(s_i)\log_2 p(s_i),\ \sum_{i=0}^{T-1}p(s_i)=1,\quad(22)$$

式中：$p(s_i)$ 表示 s_i 出现的概率，$T=256$。理想情况下 $H(s)=8$。通过表 2 可以发现，本文加密算法的信息熵大于其他加密系统。

表 2　信息熵结果

Tab. 2　Results of information entropy

算法	信息熵
本文算法	7.997 3
文献[9]	7.985 6
文献[10]	7.997 1
文献[15]	7.996 5

6　结　论

本文提出的加密算法主要包括两个部分：混乱阶段和扩散阶段。在混乱阶段中，本文采用了一种新的、效果良好的加密算法：折叠算法。该算法旨在通过量子混沌序列对明文图像从 4 个方向进行折叠异或，形成加密。在扩散阶段，本文将水平相邻的两像素同时与 Logistic 混沌序列关联起来，使加密系统具有良好的扩散性。为了使整个加密系统获得更大的密钥空间、更好的随机性，本文将量子混沌序列和 Logistic 序列进行了 Arnold 变换。

参考文献：

[1] IRFAN P, PRAYUDI Y, RIADI I. Image encryption using combination of chaotic system and rivers shamir adleman (RSA) [J]. *International Journal of Computer Applications*, 2015, 123 (6): 975-8887.

[2] 贺锋涛，张敏，白可，等. 基于激光散斑和 Henon 映射的图像加密方法[J]. 红外与激光工程，2016，45(4)：268-272.
HE F T, ZHANG M, BAI K, *et al.*. Image encryption method based on laser speckle and Henon mapping [J]. *Infrared & Laser Engineering*, 2016, 45(4): 268-272. (in Chinese)

[3] CAO G, ZHOU J, ZHANG Y. Quantum chaotic image encryption with one time running key [J]. *International Journal of Security & Its Applications*, 2014, 8(4): 77-88.

[4] 孙燮华. 图像加密算法与实践[M]. 北京：科学出版社，2013.
SUN X H. *Image Encryption Algorithms and Practices* [M]. Beijing: Science Press, 2013. (in Chinese)

[5] JIN C, TU Z. A *Novel Color Image Encryption Algorithm Using Chaotic Map and Improved* RC4 [M]. Automation Control Theory Perspectives in Intelligent Systems, Springer, 2016: 3-14.

[6] AKHSHANI A, AKHAVAN A, MOBARAKI A. Pseudo random number generator based on quantum chaotic map [J]. *Communications in Nonlinear Science & Numerical Simulation*, 2014, 19 (1): 101-111.

[7] GOEL A, CHANDRA N. A technique for image encryption based on explosive $n*n$ block displacement followed by inter-pixel displacement of RGB attribute of a pixel [C]. 2012 *International Con-*

ference on Communication Systems and Network Technologies (CSNT), *IEEE*, 2012: 884-888.

[8] SIVAKUMAR T, VENKATESAN R. A novel image encryption using calligraphy based scan method and random number [J]. *KSII Transactions on Internet & Information Systems*, 2015, 9(6): 2317-2337.

[9] 张永红，张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究，2015，32(6)：1770-1773.
ZHANG Y H, ZHANG B. Algorithm of image encrypting based on Logistic chaotic system [J]. *Application Research of Computers*, 2015, 32(6): 1770-1773. (in Chinese)

[10] WANG X Y, ZHANG Y Q, ZHAO Y Y. A novel image encryption scheme based on 2-D logistic map and DNA sequence operations [J]. *Nonlinear Dynamics*, 2015, 82(3): 1269-1280.

[11] 底晓强，毋一宁，李锦青，等. 一种基于 TLM 超混沌细胞神经网络图像加密新算法[J]. 红外与激光工程，2014，43(12)：4170-4176.
DI X Q, MU Y N, LI J Q, *et al.*. Novel image encryption algorithm based TLM hyperchaotic cellular neural network [J]. *Infrared & Laser Engineering*, 2014, 43(12): 4170-4176. (in Chinese)

[12] WANG Y, LIAO X, XIAO D. One-way hash function construction based on 2D coupled map lattices [J]. *Information Sciences*, 2008, 178(5): 1391-1406.

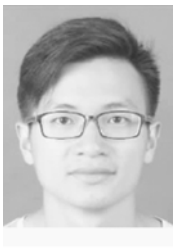
[13] SCHNEIER B. Applied cryptography: protocols, algorithms, and source code in C [J]. *Government Information Quarterly*, 2015, 13(3): 336.

[14] SEYEDZADEH S M, MIRZAKUCHAKI S. A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map [J]. *Signal Processing*, 2012, 92(5): 1202-1215.

[15] WANG X, TENG L, QIN X. A novel colour image encryption algorithm based on chaos [J]. *Signal Processing*, 2012, 92(4): 1101-1108.

作者简介：

金　聪(1960－)，女，上海人，博士，教授，博士生导师，2006 年于华中科技大学图像识别与人工智能研究所获得工学博士学位，主要从事数字图像处理、机器学习、软件质量预测、计算机病毒检测与控制等方面的研究。E-mail：jinc26@aliyun.com



刘　会(1992－)，男，湖北监利人，硕士研究生，2015 年于荆楚理工学院获得学士学位，主要从事数字图像加密、信息安全等方面的研究。E-mail：1126193462@qq.com