DOI: 10.13718/j.cnki.xdzk.2018.04.019

基于 8 方向折叠与自更新置乱的图像加密算法①

徐嵩松[1]，　蒲　斌[2]

1. 成都工业职业技术学院 信息工程学院，成都 610208；2. 西华师范大学 计算机学院，四川 南充 637009

摘要：当前的图像加密算法主要是在一个方向上对像素进行扩散，且在整个加密过程中，都是利用相同的扩散、混淆函数来改变像素位置与灰度值，导致算法的随机度与安全性不佳，因此本文提出了一种基于 8 方向折叠机制与自更新的图像加密算法. 首先，联合 Lucas、Fibonacci 序列，通过二维 Arnold 变换设计一种像素自更新置乱算法，对输入明文进行混淆操作，充分提高像素位置的置乱度；引入 Logistic 映射，利用明文像素来生成其初始值，根据其随机序列的量化密钥流来设计 8 方向折叠机制，从 8 个方向对置乱图像进行高度加密，对于每一个方向的像素扩散，利用不同的加密函数来改变其像素值，显著降低了置乱、扩散的周期性. 测试数据显示：与当前的图像加密机制相比，本文所提算法具有更高的安全性与用户响应值，其密文像素分布更为均匀.

关　键　词：图像加密；8 方向折叠机制；自更新置乱技术；Lucas 序列；Fibonacci 序列；用户响应

中图分类号：TP391　　**文献标志码**：A　　**文章编号**：1673-9868(2018)04-0139-12

数字图像具有丰富的用户信息与直观的表达能力，是多媒体技术中常用的介质，给用户的生活带来了极大的方便[1-2]. 但是，图像信息主要是借助开放的网络来传输，在传输过程中易遭遇攻击，导致信息泄露、篡改，给用户带来极大的安全隐患，因此如何避免图像受到网络攻击，使其安全传输至接收端，已经是当前各国学者研究的热点[3-4]. 较为主流的加密技术是采用置乱-扩散的加密结构，如 Liu 等人[5]提出了一种基于超混沌系统与动态 S 盒的图像加密技术，其加密密文能够有效抵御统计攻击. Ye 等人[6]提出了一种基于波线置换和块扩散的混沌图像加密算法，实验数据验证了其算法的合理性与优异性. 李凯佳等人[7]提出了一种基于 DNA-记忆元胞自动机与 Hash 函数的图像加密算法，实验结果验证了其算法的实用性. 但是，此类加密技术主要是在一个方向上对像素进行扩散，且在每一轮加密期间，都是利用相同的扩散函数来改变像素值，使其密文存在周期性，导致算法的安全性不够高.

为了在消除周期性的同时提高算法的安全性与抗攻击能力，本文提出了一种基于 8 方向折叠机制与像素自更新置乱技术的图像加密算法. 首先，基于像素自更新置乱技术来高度置乱图像像素位置，兼顾其置乱度与抗明文攻击能力；然后，借助明文尺寸来生成 Logistic 映射的初始条件，通过迭代该映射的输出序列来设计 8 方向折叠机制，从 8 个方向对置乱图像进行加密，并利用不同的扩散函数来改变其像素值，充分消除密文的周期性；最后，测试所提加密算法的安全性与用户响应值.

1　本文图像加密算法设计

基于 8 方向折叠机制与像素自更新置乱技术的图像加密算法过程见图 1，它是利用不同的扩散函数从不同的方向对明文进行像素加密，避免了周期性，提高了混沌序列的随机性与密文的安全性. 其主要有 2 个步骤：① 基于像素自更新置乱技术的明文混淆；② 基于 8 方向折叠机制的像素加密.

① 收稿日期：2017-06-05
基金项目：国家自然科学基金项目(61379019)；四川省科技厅支撑项目(2014SZ0104)；四川省教育厅项目(16ZB0174).
作者简介：徐嵩松(1981-)，男，四川成都人，讲师，主要从事图像处理、网络信息安全、信息工程等方面的研究.

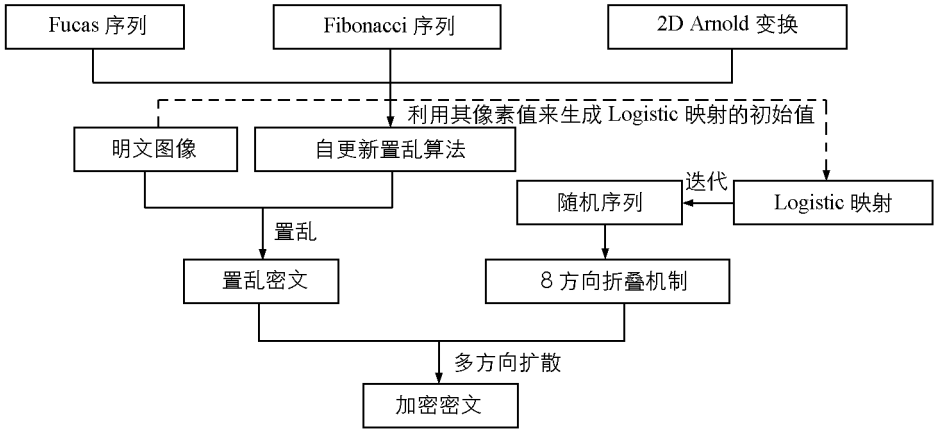


图 1 本文图像加密算法过程

1.1 基于像素自更新置乱算法的明文混淆

当前的图像加密思路是先变换像素位置，再改变像素值，从而实现明文的双重加密. 但是，当前的加密技术所采用的像素置乱方法为周期性置乱，在多轮置乱过程中，始终使用同一个置乱操作来混淆，使其密文存在显著的周期性，降低了密文的安全性[8]. 对此，本文利用 Fibonacci 序列[9]与 Lucas 序列[10]，构建一种自更新置乱算法，完成像素的动态混淆，充分提高明文的置乱度. 标准的 Fibonacci 序列的初始种子仅有[(0，1)，(1，1)]. 它是通过选择合适的种子[(0，1)，(1，1)]，根据循环次数的变化来实时更新其输出的整数序列，其函数分别为[9]

$$F_n=\begin{cases}0 & n=1\\ 1 & n=2\\ F_{n-1}+F_{n-2} & n\geqslant 3\end{cases} \tag{1}$$

$$F_n=\begin{cases}1 & n=1\\ 1 & n=2\\ F_{n-1}+F_{n-2} & n\geqslant 3\end{cases} \tag{2}$$

综合式(1)、(2)可知，在确定好种子后，随着 n 的变化，其对应的 F_n 值是截然不同的.

标准的 Lucas 序列和 Fibonacci 序列具有同样的性质，其初始种子为(2，1)，相应的函数为[10]

$$L_n=\begin{cases}2 & n=1\\ 1 & n=2\\ L_{n-1}+L_{n-2} & n\geqslant 3\end{cases} \tag{3}$$

随着 n 的变化，其对应的 L_n 值也相应地变化.

依据 Fibonacci、Lucas 序列的动态特性，使其满足加密技术的动态性与随机性[11]. 本文充分结合 Fibonacci，Lucas 序列，利用 2D Arnold 变换[12]，设计了像素自更新置乱算法：

$$\begin{bmatrix}x'\\ y'\end{bmatrix}=\begin{bmatrix}F_n & F_{n+1}\\ L_n & L_{n+1}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}\bmod N \tag{4}$$

其中，$(x，y)$为初始明文的像素位置；$(x'，y')$是处理后的像素坐标；F_n，L_n 分别代表 Fibonacci，Lucas 序列值；N 为图像宽度.

通过对比式(2)、式(3)，可以发现 Lucas 序列与种子(1，1)的 Fibonacci 序列之间有如下关系：

$$L_n=F_n+F_{n-2}\qquad n\geqslant 3 \tag{5}$$

根据标准的 Lucas 序列与 Fibonacci 序列的性质，为了满足式(5)，提高所提算法的随机性与安全性，本文取 Fibonacci 序列的种子为(1，1)，Lucas 序列的种子为(2，1).

因此，式(4)可变换为

$$\begin{bmatrix}x'\\ y'\end{bmatrix}=\begin{bmatrix}F_n & F_{n+1}\\ F_n+F_{n-2} & F_{n+1}+F_{n-1}\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}\bmod N \tag{6}$$

由式(6)可知，在对明文进行多轮混淆时，随着混淆次数 n 的增加，使得 F_n，F_{n+1}，F_{n-1}，F_{n+2} 的值出现巨

大差异，导致变换核 $\begin{bmatrix} F_n & F_{n+1} \\ F_n+F_{n-2} & F_{n+1}+F_{n-1} \end{bmatrix}$ 随着 n 的不同而变化. 也就是在对明文进行多轮置乱时，本文像素自更新置乱算法是利用不同的混淆函数来实现像素置乱，显著改善了置乱度.

为了测试所提的像素自更新置乱算法的优异性，本文以图 2(a)为样本，利用式(6)对其进行 4 次混淆，所获取的置乱密文见图 2(b)～2(e). 根据输出的结果可知，每一轮置乱所获取的密文是不同的，也就是相邻两次混淆之间的相关性较低，避免了周期性，明文的像素被充分置乱.

为了量化其置乱度，选择文献[3]、文献[5]作为对照组，利用这 3 种算法的置乱技术对图 2(a)完成混淆，并基于文献[13]的方法来计算像素置乱度，

$$Q=\frac{\| R'_{M\times N} \| - \| R_{M\times N} \|}{M\times N - \| R_{M\times N} \|} \tag{7}$$

其中，R'为置乱图像；R 为明文；$M\times N$ 为明文尺寸.

3 种技术对图 2(a)的置乱度见图 2(f). 由测试结果可知，本文像素自更新置乱算法的置乱度最高，经过 3 轮混淆后，其置乱度达到稳定值，为 99.37%，这表明明文像素被高度置乱，而文献[3]、文献[5]算法的置乱度都要小于本文所提算法，分别为 95.19%、98.26%. 原因是本文像素自更新置乱算法充分结合了 Fibonacci 序列、Lucas 序列的动态特点，对于不同的迭代次数，其置乱核是不同的，有效地削弱了置乱周期性，继而改善了像素置乱度，而文献[3]、文献[5]算法是采用相同的置乱方法来进行每一轮像素混淆，使得相邻 2 次置乱密文之间存在一定的联系，周期性明显，降低了像素的置乱度.

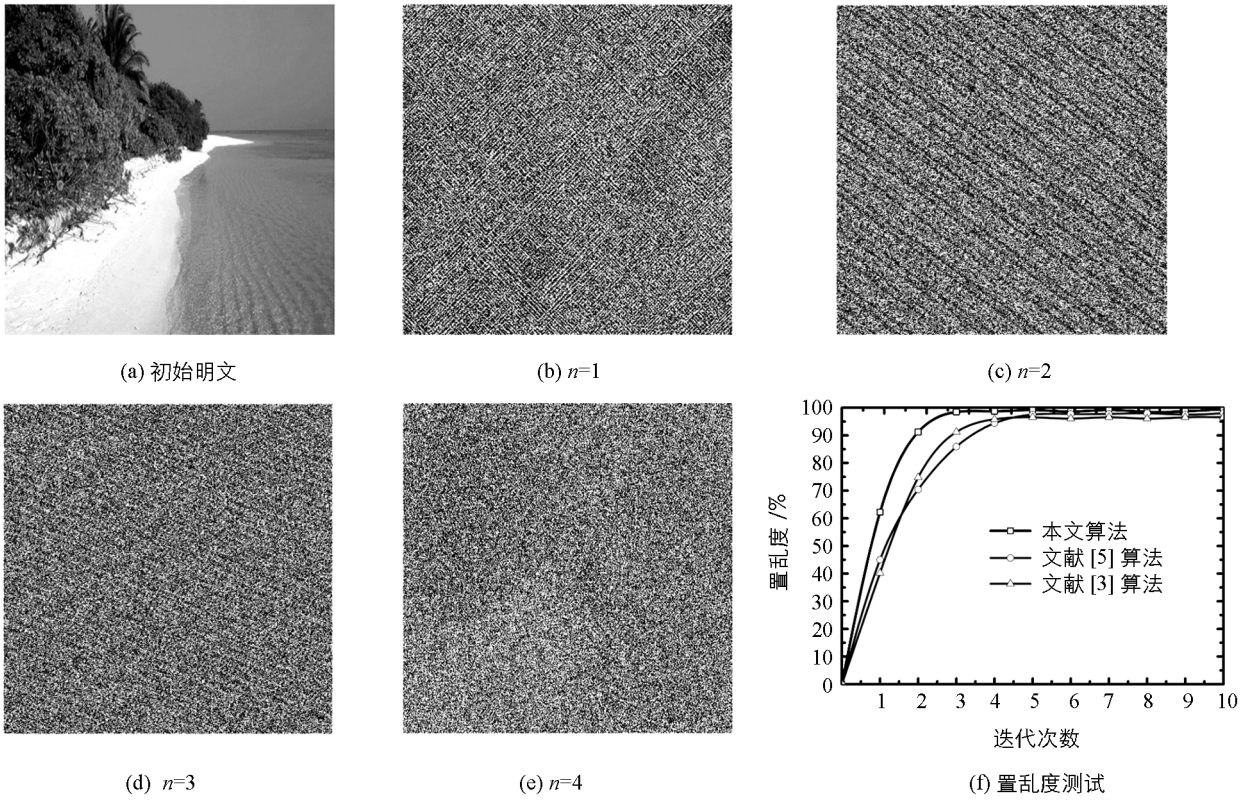


图 2　3 种像素置乱算法的输出结果

1.2　基于 8 方向折叠机制的像素扩散

明文经过像素置乱后，虽然其信息得到了隐藏，但是像素值并未变化，导致其安全性较低[2]. 为此，本文设计了一种基于 8 方向折叠机制的像素扩散算法，从不同的方向、利用不同的扩散函数来实现加密. 首先，引入 Logistic 映射来获取随机序列，其模型为[14]

$$x_{k+1}=\lambda x_k(1-x_k) \tag{8}$$

其中，$\lambda\in[0,4]$是混沌性能的控制参数；x_i 是系统变量.

为了增强加密算法与明文之间的联系，提高其抗明文攻击能力，本文利用明文像素与外部密钥来设置

式(8)的初始值 x_0. 先将128位外部密钥 K 分割为8位子密钥 k_i，则

$$K=k_1k_2\cdots k_{16} \tag{9}$$

依据式(9)与明文像素，则初始值 x_0 为

$$x_0=\left[(k_2\oplus k_4\oplus k_6\oplus k_8)+\frac{\sum_{i=1}^{16}k_i \bmod 2^8}{255}+\left(\frac{\sigma}{255}+t\right)\bmod 1\right]\bmod 1 \tag{10}$$

其中，σ 为明文像素均值；t 为用户设置的常量；

再选择λ，结合 x_0，对式(8)进行 $M\times N$ 次迭代，输出混沌序列 $x=\{x_1, x_2, \cdots, x_{M\times N}\}$. 利用 $\{x_i\}$ 来建立量化机制，获取密钥流 $\{k_i\}$，则

$$k_i=\bmod\ (floor\,(x_i\times 10^{14}),\ 256) \tag{11}$$

随后，根据密钥流 $\{k_i\}$，设计基于8方向折叠机制的扩散算法，具体步骤如下所示：

① 将尺寸为 $M\times N$ 的置乱密文 I' 的像素用矩阵 $\boldsymbol{R}$ 表示；同时，把密钥流 $\{k_i\}$ 用矩阵 $\boldsymbol{Q}$ 表示. 对于第1个方向的像素扩散，其过程见图3(a)，扩散函数为

$$\begin{cases}T_h'(i,j)=T_h(i,j)\oplus Q_h(i,j)\\ B_h'(N-i+1,j)=B_h(N-i+1,j)\oplus T_h'(i,j)\end{cases} \tag{12}$$

其中，$T_h(i,j)$、$B_h(N-i+1,j)$分别是矩阵 $\boldsymbol{R}$ 上半部分中(i,j)、下半部分中$(N-i+1,j)$对应的像素值；$Q_h(i,j)$是矩阵 $\boldsymbol{Q}$ 上半部分中(i,j)对应的密钥流；$T'_h(i,j)$、$B'_h(N-i+1,j)$分别是 $T_h(i,j)$、$B_h(N-i+1,j)$扩散后的像素值.

② 经过步骤①的扩散后，输出第一个密文 I_1'；再根据密文 I_1'，进行第2个方向的像素加密，其过程见图3(b)，扩散函数为

$$\begin{cases}T_r'(i,j)=T_r(i,j)\oplus Q_{tr}(i,j)\\ B_l'(j,i)=B_l(j,i)\oplus T_r'(i,j)\end{cases} \tag{13}$$

其中，$T_r(i,j)$是密文 I_1'右上半部分中(i,j)对应的像素值；$B_l(j,i)$是密文 I'左下部分与(i,j)关于对角线对称位置的像素值；$Q_{tr}(i,j)$是矩阵 $\boldsymbol{Q}$ 右上部分中(i,j)对应的密钥流；$T'_r(i,j)$、$B'_l(j,i)$分别是 $T_h(i,j)$、$B_h(j,i)$扩散后的像素值.

③ 经过步骤②的扩散后，输出第2个密文 I_2'；再根据密文 I_2'，进行第3个方向的像素加密，其过程见图3(c)，扩散函数为

$$\begin{cases}R_h'(i,j)=R_h(i,j)\oplus Q_{rh}(i,j)\\ L_h'(i,N-j+1)=L_h(i,j)\oplus R_h'(i,N-j+1)\end{cases} \tag{14}$$

其中，$R_h(i,N-j+1)$、$L_h(i,j)$分别是密文 I_2'右半部分中$(i,N-j+1)$、左半部分中(i,j)对应的像素值；$Q_{tr}(i,j)$是矩阵 $\boldsymbol{Q}$ 右半部分中(i,j)对应的密钥流；$R'_h(i,N-j+1)$、$L'_h(i,j)$分别是 $R_h(i,N-j+1)$、$L_h(i,j)$扩散后的像素值.

④ 经过步骤③的扩散后，输出第3个密文 I_3'；再根据密文 I_3'，进行第4个方向的像素加密，其过程见图3(d)，扩散函数为

$$\begin{cases}R_b'(i,j)=R_b(i,j)\oplus Q_{rb}(i,j)\\ L_t'(i-1,j-1)=R_b'(i,j)\oplus L_t(i-1,j-1)\end{cases} \tag{15}$$

其中，$R_b(i,j)$是密文 I_3'右下部分中(i,j)对应的像素值；$L_t(i-1,j-1)$是密文 I'_3 左上部分中$(i-1,j-1)$对应的像素值；$Q_{rb}(i,j)$是矩阵 $\boldsymbol{Q}$ 右下半部分中(i,j)对应的密钥流；$R'_b(i,j)$、$L'_t(i-1,j-1)$分别是 $R_b(i,j)$、$L_t(i-1,j-1)$扩散后的像素值.

⑤ 经过步骤④的扩散后，输出第4个密文 I_4'；再根据密文 I_4'，进行第5个方向的像素加密，其过程见图3(e)，扩散函数为

$$\begin{cases}B_m'(i,j)=B_m(i,j)\oplus Q_{bh}(i,j)\\ T_m'(N-i+1,j)=T_m(N-i+1,j)\oplus B_m'(i,j)\end{cases} \tag{16}$$

其中，$B_m(i,j)$是密文 I_4'下半部分中(i,j)对应的像素值；$T_m(N-i+1,j)$是密文 I'_4 上半部分中$(N-i+1,j)$对应的像素值；$Q_{bh}(i,j)$是矩阵 $\boldsymbol{Q}$ 下半部分中(i,j)对应的密钥流；$B'_m(i,j)$、$T'_m(N-i+1,$

j)分别是 $B_m(i,j)$、$T_m(N-i+1,j)$扩散后的像素值.

⑥ 经过步骤⑤的扩散后，输出第 5 个密文 I_5'；再根据密文 I_5'，进行第 6 个方向的像素加密，其过程见图 3(f)，扩散函数为

$$\begin{cases} B_n'(i,j)=B_n(i,j)\oplus Q_{bl}(i,j) \\ T_s'(j,i)=T_s(j,i)\oplus B_n'(i,j) \end{cases} \tag{17}$$

其中，$B_n(i,j)$是密文 I_5'左下部分中(i,j)对应的像素值；$T_s(j,i)$是密文 I'_5 右上部分与(i,j)关于对角线对称位置的像素值；$Q_{bl}(i,j)$是矩阵 $\boldsymbol{Q}$ 左下部分中(i,j)对应的密钥流；$B'_n(i,j)$、$T'_s(j,i)$分别是 $B_n(i,j)$、$T_s(j,i)$扩散后的像素值.

⑦ 经过步骤⑥的扩散后，输出第 6 个密文 I_6'；再根据密文 I_6'，进行第 7 个方向的像素加密，其过程见图 3(g)，扩散函数为

$$\begin{cases} L_o'(i,j)=L_o(i,j)\oplus Q_{lh}(i,j) \\ R_o'(i,N-j+1)=R_o(i,N-j+1)\oplus L_o'(i,j) \end{cases} \tag{18}$$

其中，$L_o(i,j)$是密文 I_6'左半部分中(i,j)对应的像素值；$R_o(i,N-j+1)$是密文 I'_6 右半部分中$(i,N-j+1)$对应的像素值；$Q_{lh}(i,j)$是矩阵 $\boldsymbol{Q}$ 左半部分中(i,j)对应的密钥流；$L'_o(i,j)$、$R'_o(i,N-j+1)$分别是 $L_o(i,j)$、$R_o(i,N-j+1)$扩散后的像素值.

⑧ 经过步骤⑦的扩散后，输出第 7 个密文 I_7'；再根据密文 I_7'，进行第 8 个方向的像素加密，其过程见图 3(h)，扩散函数为

$$\begin{cases} L_b'(i,j)=L_b(i,j)\oplus Q_{lt}(i,j) \\ R_t'(i+1,j+1)=R_t(i+1,j+1)\oplus L_b'(i,j) \end{cases} \tag{19}$$

其中，$L_b(i,j)$是密文 I_7'左上部分中(i,j)对应的像素值；$R_t(i+1,j+1)$是密文 I'_7 右下部分中$(i+1,j+1)$对应的像素值；$Q_{lt}(i,j)$是矩阵 $\boldsymbol{Q}$ 左上部分中(i,j)对应的密钥流；$L'_b(i,j)$、$R'_t(i+1,j+1)$分别是 $L_b(i,j)$、$R_t(i+1,j+1)$扩散后的像素值.

经过第 8 个方向的扩散处理后，输出最终的密文 I_8'. 以图 2(d)为目标，利用本文设计的 8 方向折叠机制对其进行扩散加密，输出的密文见图 4. 依图可知，经过 8 个方向的像素扩散后，每个方向的输出密文均与置乱图像是截然不同的，图像信息的隐密度进一步提高，抗攻击能力更强.

本文引入信息熵值[7]来量化每个方向输出密文的安全性能，它是衡量图像信息不确定性的理想指标. 因图像数据量大，且其像素间的相关性较高，因此，未经加密的图像其熵值较小，而经过加密后的图像其熵值很大. 当值越靠近 8 时，显示其不确定性越高，密文安全性也就越高[15]. 信息熵值计算函数为[15]

$$H=-\sum_{i=1}^{L}P(x_i)\log_2 P(x_i) \tag{20}$$

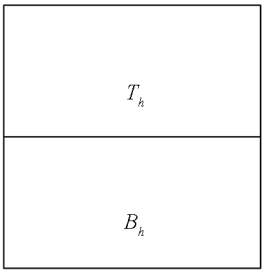
其中，x_i 是图像中第 i 个像素的灰度值；$L\in[0,256]$为图像灰度等级；$P(x_i)$为第 i 个像素的灰度值在整个图像中所占的比例，且

$$\sum_{i=1}^{L}P(x_i)=1$$

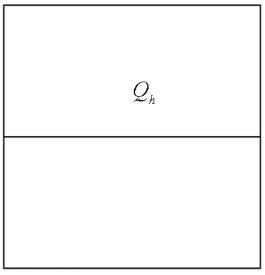
依据式(20)，利用文献[15]的计算过程，得到图 8(a)～8(b)的熵值见表 1，由表可知，随着方向个数的增加，其扩散效果越来越好. 经过第 8 次扩散后，其密文熵值约为 7.997 6，与理论值 8 非常接近. 这表明对明文进行多个方向扩散，能够显著提高密文的安全性. 为此，本文将方向数量设置为 8 进行加密实验.

表 1　每个方向的扩散密文对应的熵值

名　　称	密文熵值	名　　称	密文熵值
图 4(a)	7.801 3	图 4(e)	7.920 7
图 4(b)	7.847 1	图 4(f)	7.945 2
图 4(c)	7.879 3	图 4(g)	7.979 4
图 4(d)	7.896 4	图 4(h)	7.997 6

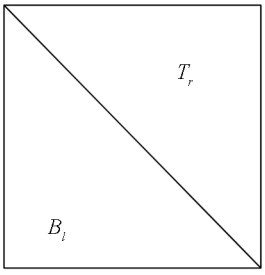


置乱图像

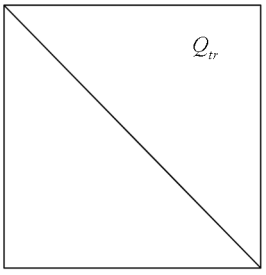


密钥流矩阵

(a) 第1次折叠(从上到下)

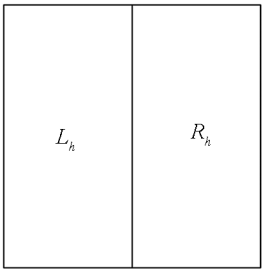


第1次扩散后的密文

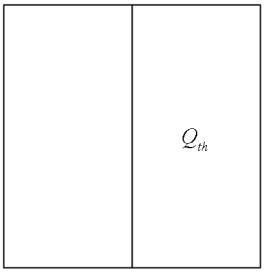


密钥流矩阵

(b) 第2次折叠(从右上到左下)

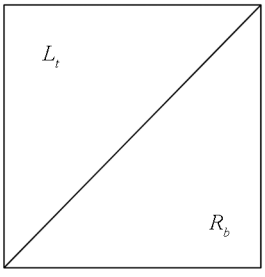


第2次扩散后的密文

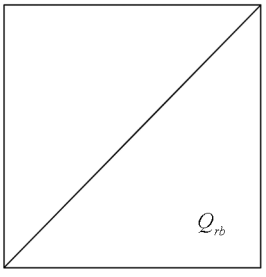


密钥流矩阵

(c) 第3次折叠(从右到左)

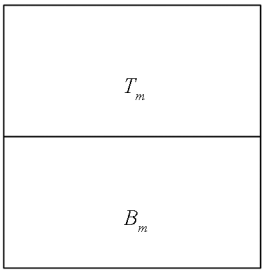


第3次扩散后的密文

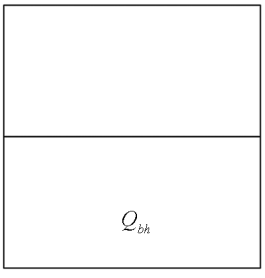


密钥流矩阵

(d) 第4次折叠(从右下到左上)

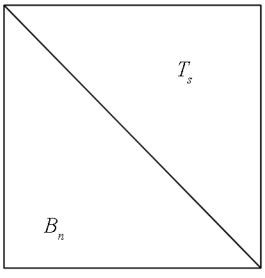


第4次扩散后的密文

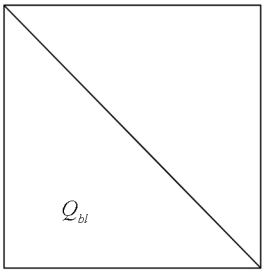


密钥流矩阵

(e) 第5次折叠(从下到上)

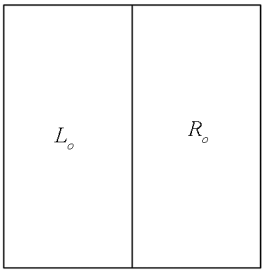


第5次扩散后的密文

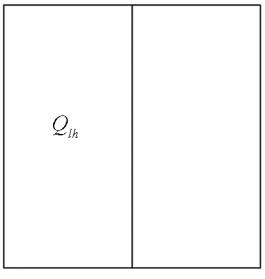


密钥流矩阵

(f) 第6次折叠(从左下到右上)

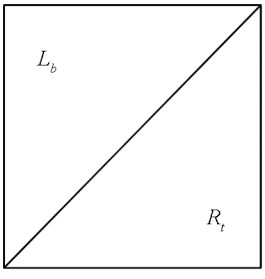


第6次扩散后的密文

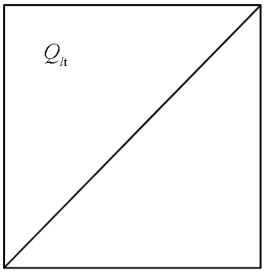


密钥流矩阵

(g) 第7次折叠(从左上到右下)



第7次扩散后的密文



密钥流矩阵

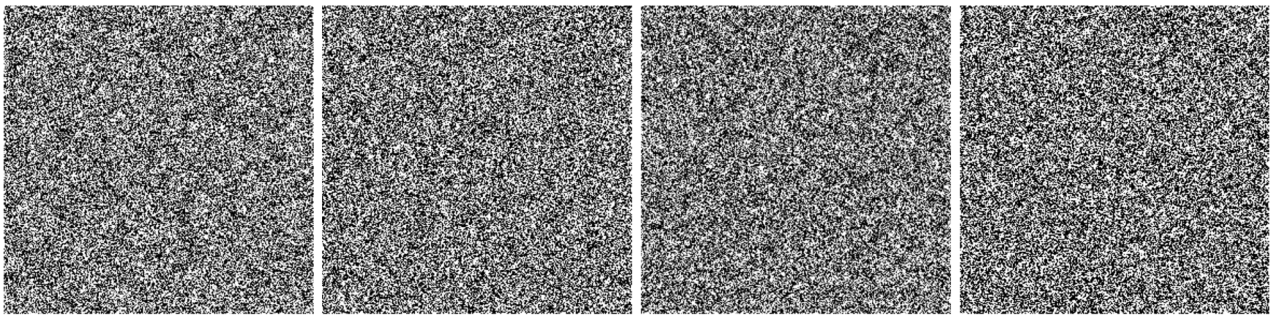
(h) 第8次折叠(从顶左到底右)

图3 8个方向的像素扩散

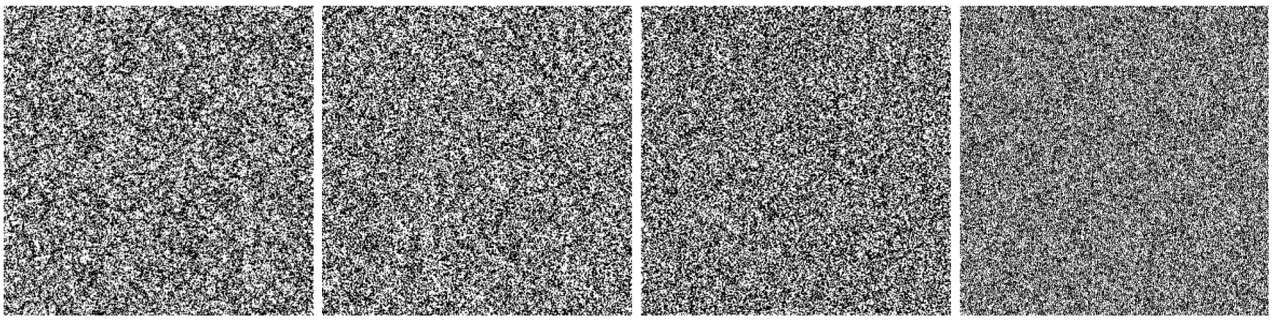
2 实验结果与分析

为了验证所提加密算法的安全性与抗攻击能力，本文在Matlab平台上进行测试，另外，将当前安全度较高的加密技术作为对照组：文献[18]、文献[5]、文献[7]. 其中，文献[18]为光学加密技术，通过利用不同的混沌映射来生成所需要的随机模板来实现图像加密. 而文献[5]、文献[7]则是采用了置乱-扩散的混沌

加密结构. 算法关键参数为：初始种子为(1，1)，$\lambda=3.35$，外部密钥 $K=$10yhg65ewmaz91bx，$t=2$.



(a) 第 1 个方向　(b) 第 2 个方向　(c) 第 3 个方向　(d) 第 4 个方向



(e) 第 5 个方向　(f) 第 6 个方向　(g) 第 7 个方向　(h) 第 8 个方向

图 4　8 方向折叠机制的扩散结果

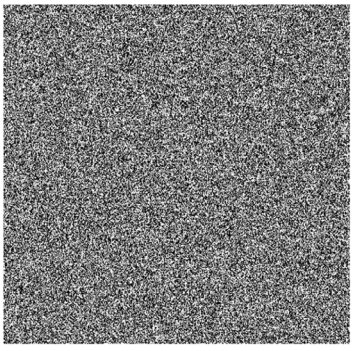
2.1　加密质量对比分析

把图 5(a)作为加密实验的样本，4 种加密算法结果分别见图 5(b)～5(e). 由测试结果可知，本文算法与文献[18]、文献[5]、文献[7]算法的加密效果都较为理想，初始图像的信息均被充分隐藏，明文内容被高度混淆，没有视觉信息泄露. 为了区分 4 种加密算法的安全性，本文再次利用信息熵值[7]来量化，得到的熵值见表 2. 由表 2 可知，本文算法的密文熵值最大，达到了 7.998 4，与理论值 8 的偏差非常小，这显示其安全性最高，而文献[5]、文献[7]、文献[18]算法的密文熵值均要低于所提算法，分别为 7.992 6，7.989 5，7.981 4，这表明三者的安全性不佳. 尤其是文献[18]，虽然该算法能够充分隐藏明文信息，但是存在一定的轮廓效应，见图 5(e). 原因是本文加密机制充分结合了 Lucas、Fibonacci 序列的动态性，采用了像素自更新技术，在每一轮像素置乱过程中，利用不同的置乱核来混淆像素位置，有效降低了置乱周期性，同时，利用明文像素与外部密钥来生成密钥流，采用了 8 方向折叠机制，从 8 个方向利用 8 个不同的扩散函数来改变像素值，避免了像素扩散的周期性，显著提高了密文的安全性与抗攻击能力；而文献[5]虽然采用了高维混沌系统，通过牺牲算法的效率来提高密文安全性，而且通过设计动态 S 盒来充分改变像素值，提高了算法的动态性与随机性，但是该算法在置乱与扩散过程中，都是采用相同的加密操作来获取密文，导致其密文存在显著的周期性特点，继而削弱了算法的安全性，且整个加密机制忽略了明文自身特性，使其抗明文攻击能力较弱；文献[7]通过将时间延迟思想引入低维混沌映射中，降低序列的自相关性，而且利用记忆元胞自动机来实现像素扩散，但是此算法是从一个方向来实现像素扩散，且在每一轮加密过程中，都是采用相同的置乱与扩散机制来改变像素位置与像素值，使得明文内容的混淆程度不佳，从而导致密文的安全性较弱. 文献[18]虽然结合了混沌理论与光学技术来快速加密图像，其实质为光学干涉加密，明文通过光学加密装置后，将明文的所有信息集中在一个纯相位掩码中，使其存在轮廓显现问题，导致密文安全性不理想.

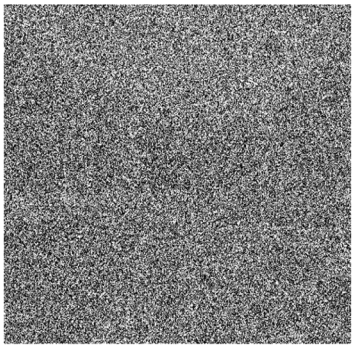
表 2　各算法对应的密文熵值测试果

名　　称	本文算法	文献[5]	文献[7]	文献[18]
密文熵值	7.998 4	7.992 6	7.989 5	7.981 4

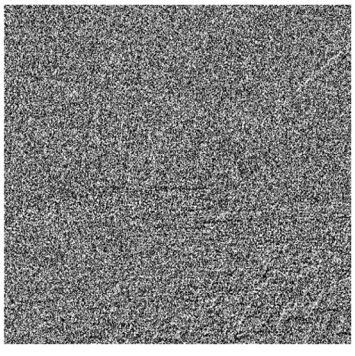
(a) 输入明文



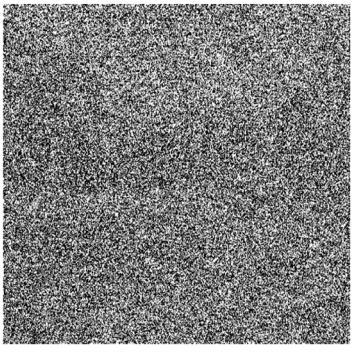
(b) 本文算法的输出密文



(c) 文献[7]算法的输出密文



(d) 文献[5]算法的输出密文



(e) 文献[18]算法的输出密文

图5 输入明文与4种加密算法的输出密文

2.2 密文相邻像素间的相关性测试

图像相邻两像素之间的相关性对密文安全性有较大威胁，攻击者通常利用像素间的相关性破译密文，故数字图像加密技术应该要最大程度地降低这种相关性[3]. 为了测试输出密文的相关性，本文从图5(b)～5(e) 4幅密文中选择2 500对相邻像素点来验证其相关性，相关性用相关系数C_{xy}来表示，C_{xy}值越大相关性越大，其模型为[7]

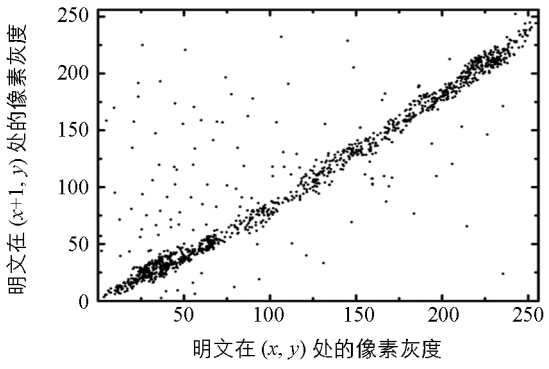
$$C_{xy}=\frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-E(x_i))(y_i-E(y_i))}{\sqrt{\left(\frac{1}{n}\sum_{i=1}^{n}(x_i-E(x_i))^2\right)\left(\frac{1}{n}\sum_{i=1}^{n}(y_i-E(y_i))^2\right)}} \tag{21}$$

各算法的密文在X方向上的相关性测试结果见图6. 由图6(a)可知，初始图像的像素相关系数很高，像素分布极为不均，其C_{xy}值约为0.961 8；然而，初始明文被4种算法加密后，明文的相关性被显著降低，输出密文的像素分布变得均匀，其C_{xy}值分别为0.003 1,0.006 8,0.004 9,0.007 5. 本文所提算法输出密文的像素分布均匀性最好，没有堆积现象，其分布均匀性要优于其他3种算法，见图6(b)～6(e).

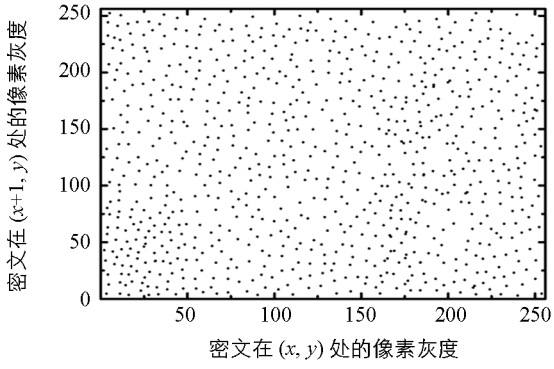
各密文在另外2个方向上的C_{xy}计算数据如表3所示. 由表3可知，初始图像的C_{xy}值是最大的，表明其相关性最大. 但是，明文经过4种加密算法处理后，图像的C_{xy}值被显著降低，且本文所提算法的C_{xy}值是最小的，要远低于其他3种加密算法.

表3 不同方向的相关系数测试结果

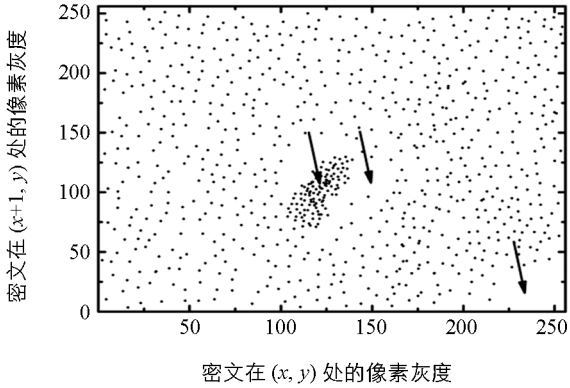
方 向	图5(a)	图5(b)	图5(c)	图5(d)	图5(e)
X轴	0.961 8	0.003 1	0.006 8	0.004 9	0.007 5
Y轴	0.942 7	0.002 5	0.005 7	0.003 6	0.006 2
对角线	0.909 3	0.001 1	0.003 9	−0.002 3	−0.004 6



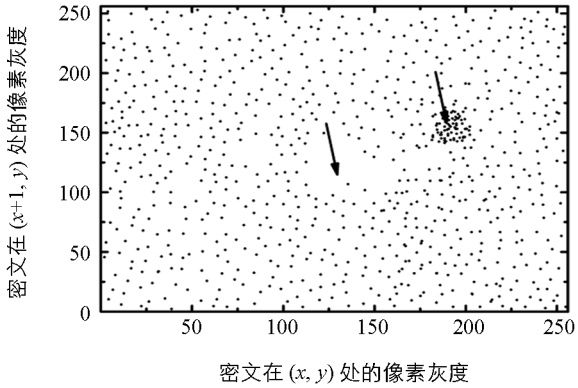
(a) 初始图像的相关性



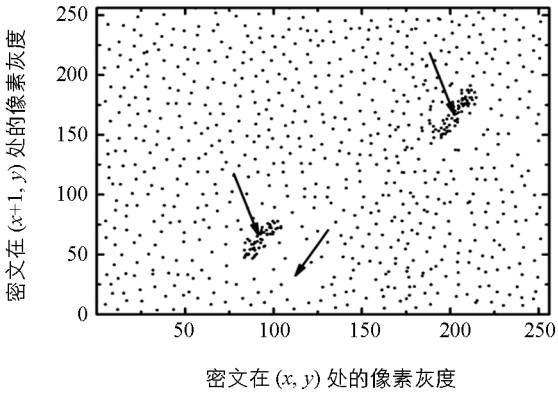
(b) 本文算法对应密文的相关性



(c) 文献 [7] 算法对应密文的相关性



(d) 文献 [5] 算法对应密文的相关性



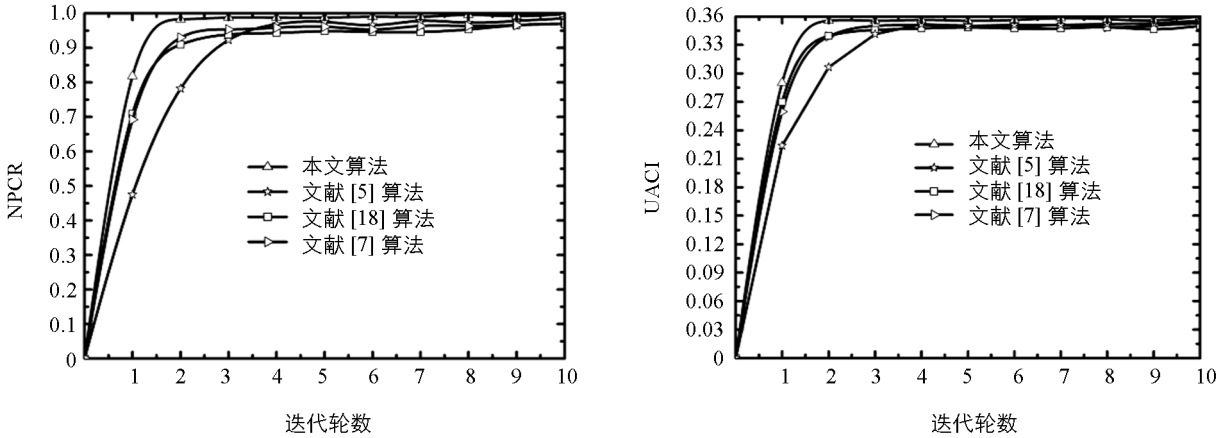
(e) 文献 [18] 算法对应密文的相关性

图 6　加密前后的密文像素之间的相关性测试

2.3　抗明文攻击能力对比测试

在国内外研究中，NPCR 与 UACI 曲线是衡量加密算法抗明文攻击能力的有效指标[15]. 故本文基于文献[16]的方法，验证 4 种算法的 NPCR 与 UACI 曲线，结果见图 7. 在这 4 种加密方案中，本文所提加密算法具有更高的 NPCR 与 UACI 均值，分别为 99.79%，34.52%，而文献[5]、文献[7]、文献[18]的 NPCR 与 UACI 均值都要略小于本文算法，尤其是文献[18]，其 NPCR 与 UACI 均值最小. 这表明本文加密算法的抗明文攻击能力最好，原因是所提加密机制利用明文像素来生成一组密钥流，并以此设计了 8 方向折叠机制来改变像素值，使得在 8 个不同方向的像素扩散中，均考虑了明文像素，从而增强了抗明文攻击的能力. 文献[5]利用高维混沌系统来加密明文，在一定程度上提高了密文的安全性，但是其置乱与扩散过程均与明文无关，导致其抗明文攻击能力要低于本文所提算法；文献[7]与本文算法一样，借助低维混沌映射来置乱与扩散，虽然利用了 DNA 编码技术，但 DNA 编码技术也是脱离了明文，从而导致其抗明文攻击能力

较弱. 文献[18]虽然采用了光学装置来实现加密，但是它将明文的所有信息集中在一个纯相位掩码中，存在轮廓显现问题，且其加密过程忽视了明文特性，从而使其安全性最低，导致其抗明文攻击能力不理想.

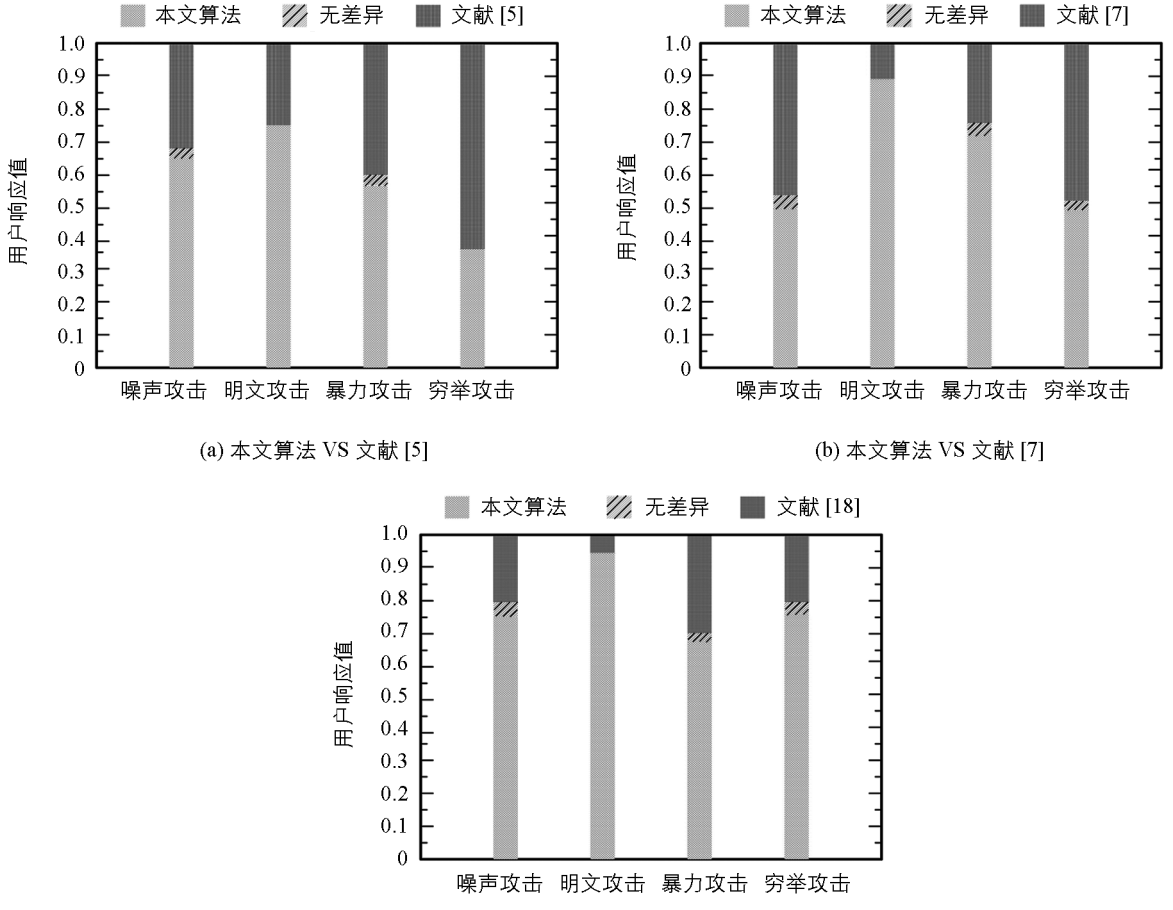


(a) NPCR 测试　　(b) UACI 测试

图 7　不同加密算法的抗明文攻击能力测试结果

2.4　用户响应对比测试

用户响应是评估加密算法在市场上受欢迎程度的重要参考指标，故本文利用 Amazon Mechanical Turk[17]来验证这 4 种算法的用户响应值. 根据图像在网络中常遇到的攻击类型，将噪声、明文、暴力与穷举攻击[7]作为本次实验的对象，不同攻击类型下各算法的响应值见图 8.



(a) 本文算法 VS 文献 [5]　　(b) 本文算法 VS 文献 [7]

(c) 本文算法 VS 文献 [18]

图 8　不同加密算法的用户响应结果

根据响应结果可知，面对噪声、暴力以及明文攻击时，所提算法的用户响应程度更高，但是，在面对穷举攻击时，文献[5]的算法使用了高维混沌系统与动态 S 盒来实现加密，显著增大了算法的密钥空间，使其响应度最高.

3　结　论

为了从多个方向对明文进行扩散，且能有效消除周期性，本文提出了一种基于 8 方向折叠机制与自更新置乱的图像加密算法. 利用 Lucas、Fibonacci 序列设计了一种像素自更新置乱算法，有效地降低了混淆周期性，进一步提高了明文像素的置乱度；利用明文与外部密钥来生成 Logistic 映射初值，利用量化机制来获取密钥流，从而设计了 8 方向折叠机制，从 8 个方向对置乱图像进行高度加密. 实验结果验证了所提算法的安全性与抗攻击能力.

参考文献：

[1] 郑洪英，彭钟贤，肖　迪. 加密医学图像中的视觉无损信息隐藏算法 [J]. 西南大学学报(自然科学版)，2014，36(12)：157－161.

[2] 马庆禄，魏悦川，潘晓中. 基于单通道 RGB 分量的彩色图像加密算法 [J]. 西南师范大学学报(自然科学版)，2014，39(11)：81－89.

[3] 杨贵宝，高　霞. 基于分数阶 logistic 映射与随机变换的双图像加密算法 [J]. 内蒙古大学学报(自然科学版)，2017，48(2)：189－195.

[4] WANG X Y，LIU C M. A Novel and Effective Image Encryption Algorithm Based on Chaos and DNA Encoding [J]. Multimedia Tools and Applications，2016，76(5)：6229－6245.

[5] LIU Y，TONG X J，MA J. Image Encryption Algorithm Based on Hyper-Chaotic System and Dynamic S-Box [J]. Multimedia Tools and Applications，2016，75(13)：7739－7759.

[6] YE G D，ZHAO H Q，CHAI H J. Chaotic Image Encryption Algorithm Using Wave-Line Permutation and Block Diffusion [J]. Nonlinear Dynamics，2016，83(4)：2067－2077.

[7] 李凯佳，俞锐刚，袁凌云. 基于 DNA -记忆元胞自动机与 Hash 函数的图像加密算法 [J]. 计算机工程与设计，2017，38(2)：470－477.

[8] BENYAMIN N，SATTAR M. Breaking an Image Encryption Algorithm Based on the New Substitution Stage with Chaotic Functions [J]. Optik-International Journal for Light and Electron Optics，2016，127(14)：5695－5701.

[9] CODARA P，D'ANTONA O M. Generalized Fibonacci and Lucas Cubes Arising from Powers of Paths and Cycles [J]. Discrete Mathematics，2016，339(3)：241－251.

[10] 邓　勇. 基于广义 Fibonacci 和 Lucas 数的准循环矩阵研究 [J]. 重庆师范大学学报(自然科学版)，2015，51(6)：72－76.

[11] 李智慧. 基于 Lucas 序列的公钥密码体制的研究 [D]. 北京：北京邮电大学，2012：23－27.

[12] SAHA B J，KABI K K. A New Approach on Color Image Encryption Using Arnold 4D Cat Map [J]. Computational Intelligence in Data Mining，2016，1：131－136.

[13] 吴　丽，余文春. 快速置乱耦合 3D 混沌映射的图像加密算法研究 [J]. 电视技术，2014，38(19)：51－56.

[14] LIU L F，MIAO S X. A New Image Encryption Algorithm Based on Logistic Chaotic Map with Varying Parameter [J]. Springer Plus，2016，5(1)：1－12.

[15] 王迤冉，朱维军，詹新生. 基于图像加密的置乱性能分析研究 [J]. 计算机工程与设计，2006，27(24)：4729－4731.

[16] 李长齐，王　菡. 基于无序分割投影策略与重力模型的图像加密算法 [J]. 包装工程，2017，38(7)：191－196.

[17] WEI X P, WANG B, ZHANG Q, et al. Image Encryption based on Chaotic Map and Reversible Integer Wavelet Transform [J]. Journal of Electrical Engineering, 2014, 65(2): 90－96.

[18] 朱 薇, 杨 庚, 陈 蕾, 等. 基于混沌的改进双随机相位编码图像加密算法 [J]. 光学学报, 2014, 34(6): 58－68.

An Image Encryption Algorithm Based on the Eight-Direction Folding and Self-Update Scrambling Technique

XU Song-song[1], PU Bin[2]

1. *School of Information Engineering, Chengdu Industry Career Technical College, Chengdu 610208, China;*
2. *School of Automation, China West Normal University, Nanchong Sichuan 637009, China*

Abstract: The current image encryption algorithm suffers from the defects of low randomness and security, for it diffuses the pixels in one direction and uses the same diffusion function to change the pixel value in the whole encryption process. In order to solve this problem, a new image encryption algorithm based on the eight-direction folding mechanism and the quantum complex chaotic system is proposed in this paper. Firstly, a pixel self-update scrambling technique is designed by jointing the Lucas and the Fibonacci sequences and using the 2D Arnold transformation to scramble the image. Then, an 8-direction folding mechanism is designed based on the stochastic sequence of the logistic map to encrypt the highly scrambled images from 8 directions, so that different encryption functions are used to change their pixel values for significantly reducing the periodicity of scrambling and diffusion. The test data show that compared with the current image encryption algorithm, this new algorithm has higher security and user response, and more uniform distribution of cipher pixels.

Key words: image encryption; eight-direction folding mechanism; self-update scrambling technique; Lucas sequence; Fibonacci sequence; user response

责任编辑 崔玉洁