DOI:10.13718/j.cnki.xsxb.2018.05.018

基于黄金分割-Lucas 动态置乱与异扩散的图像加密算法①

王 瑶[1], 徐 洋[2]

1. 重庆城市职业学院 信息工程系, 重庆 永川 402160;
2. 贵州师范大学 计算机科学与工程学院, 重庆 400050

摘要: 当前图像加密算法的每一轮像素位置置乱过程都是相同的, 且扩散操作是有序的, 降低了算法的动态性与随机程度, 使得算法安全性不佳. 为了解决这一问题, 本文提出了黄金分割-Lucas 动态置乱与异扩散的图像加密算法. 首先, 引入黄金分割序列与 Lucas 序列, 基于 2D Arnold 映射变换思想, 设计了动态置乱机制, 根据不同的迭代次数, 动态改变其置乱变换核, 使得每一次像素置乱操作都是不同的, 有效提高明文像素置乱度; 联合 Cosine 映射、sine 映射与 Logistic 映射, 设计复合串联混沌映射, 利用置乱密文的像素总量来生成复合映射的初始条件, 输出伪随机序列, 并构造量化函数, 对其进行量化, 获取一组密钥流; 最后, 对置乱图像像素进行分组, 并结合密钥流, 设计两个加密引擎函数, 通过构造像素加密模型, 分别对图像第一个像素、中间像素以及最后一个像素进行异扩散, 完成图像的加密. 实验结果表明, 与当前混沌加密技术相比, 所提算法具有更高的安全性与用户响应, 具备更强的抗明文与抗噪声攻击能力.

关 键 词: 图像加密; 黄金分割-Lucas 置乱; 串联混沌映射; 量化函数; 加密引擎函数; 异扩散; 用户响应

中图分类号: TP391 **文献标志码:** A **文章编号:** 1000-5471(2018)05-0106-10

数字图像在未知授权的网络中传输, 容易导致图像内容遭遇攻击, 使得图像信息面临巨大威胁, 因此, 如何确保图像在网络中安全传输, 已成为当前研究重点与热点[1-3]. 为此, 各国学者提出了相应的数字图像加密算法来提高图像在网络传输中的抗攻击能力[4-7].

虽然采用了置乱-扩散加密结构的算法, 不但改变了像素位置, 而且改变了图像像素值, 具有较高的安全性[6], 但是在图像像素置乱过程中, 每一轮置乱都是相同的操作, 使其动态敏感性不佳, 且扩散过程与明文无关, 均是进行有序扩散, 导致加密算法的安全性仍然不理想.

为了增强图像像素置乱操作的动态随机性, 提高算法的抗明文攻击能力, 本文提出了黄金分割-Lucas 动态置乱与异扩散的图像加密算法. 首先, 联合黄金分割变换与 Lucas 序列, 在每一轮置乱过程中, 不断变换其置乱变换核, 从而提高像素位置的置乱度; 其次综合 3 个低维映射, 设计复合串联混沌映射, 通过构造量化函数, 从而建立两个加密引擎函数, 对像素进行异扩散; 最后, 验证了所提加密算法的安全性与用户响应.

① 收稿日期: 2017-02-25
基金项目: 国家重点基础研究发展计划项目(2014CB340600); 国家自然科学基金重点项目(61332019); 贵州省科技合作计划重点项目(黔科合 LH 字[2015]7763 号).
作者简介: 王 瑶(1979-), 女, 重庆永川人, 讲师, 主要从事人工智能、信息安全、图像处理.

1　黄金分割-Lucas 动态置乱与异扩散的图像加密算法

黄金分割-Lucas 动态置乱与异扩散的图像加密算法流程见图 1，主要包含：①基于黄金分割-Lucas 机制的图像置乱；②基于复合串联混沌映射的密钥流生成；③基于加密引擎函数的像素异扩散.

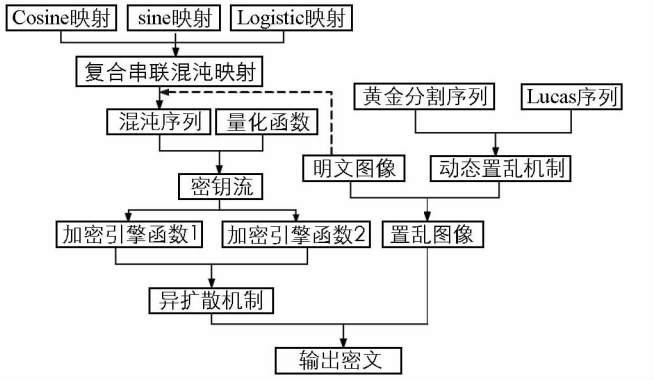


图 1　本文图像加密算法过程

1.1　基于黄金分割-Lucas 机制的图像置乱

加密算法通常都是采用先置乱后扩散的结构，首先利用置乱技术来改变图像的像素位置，实现像素预混淆[8]. 为此，为了克服当前置乱技术的不足，本文联合黄金分割序列[9] 与 Lucas 序列[10]，设计了动态置乱机制. 黄金分割序列是一种循环关系的整数序列，根据不同的种子[(0，1)，(1，1)]，产生不同的序列，其模型为[9]：

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

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

根据式(1)，(2) 可知，根据 n 的递进关系与初始种子，能够输出两个分割整数数组 0,1,1,2,3,5,8,13,21,34…，以及 1,1,2,3,5,8,13,21,34,55….

而 Lucas 序列与黄金分割序列类似，也是一种循环累加关系，其模型为[10]：

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

同样地，根据 n 的递进关系与初始种子，可获得一组序列 2,1,3,4,7,11,18,29,47…. 为此，本文联合黄金分割序列与 Lucas 序列，基于 2D Arnold 映射[11] 的原理，设计了动态置乱模型：

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

其中：$(x，y)$ 是输入明文的像素位置；$(x'，y')$ 是经过动态置乱后的像素坐标；F_n，L_n 分别是黄金分割序列、Lucas 序列；N 是图像宽度；mod 是求余运算.

根据式(2) 与式(3) 可知，Lucas 序列与初始种子[1，1] 的黄金分割序列存在如下关系：

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

则式(4) 可演变为：

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

依据式(6) 可知，当置乱轮数 n 动态更新时，导致 F_n，F_{n+1}，F_{n-1}，F_{n+2} 序列值也不断更新，使得式(6) 中的变换核 $\begin{bmatrix}F_n & F_{n+1}\\ F_n+F_{n+2} & F_{n+1}+F_{n-1}\end{bmatrix}$ 动态变化. 每轮置乱之间都会形成不同的置乱操作.

为了验证所提的黄金分割-Lucas动态置乱机制的优异性，本文以Lena图像为目标，见图2(a)，利用式(6)对其进行混淆4次，结果见图2(b)－2(e). 由图2可知，不同迭代次数所形成的置乱结果是截然不同的，降低了相关性，图像信息被有效打乱. 同时为了量化本文动态置乱机制的置乱度，将文献[5]、文献[7]视为对照技术，利用这3种技术对图2(a)进行多轮置乱，并根据文献[11]的方法来测试置乱图像的置乱度，其模型为：

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

其中：R' 为置乱图像；R 是明文；$M\times N$ 是明文尺寸；$\| \ \|$ 代表求范数运算.

图2(a)经过3种算法多轮置乱后，其输出图像的置乱度见图2(f). 由图2(f)可知，本文动态置乱机制的输出密文具有更高的置乱度，明文像素位置混淆更彻底，其置乱度约为99.52%，而文献[5]、文献[7]两种技术的置乱度均要低于本文算法，分别为98.49%,98.17%. 主要是本文设计的黄金分割-Lucas动态置乱技术能够根据迭代次数实时改变置乱变换核，避免了循环置乱周期性，显著提高了像素置乱度，而文献[5]、文献[7]两种技术的每一轮置乱都是相同的，周期性明显，使得这种重复性像素混淆的置乱度有待进一步提高. 另外，根据图2(f)可知，本文算法与文献[5]技术需要经过3轮置乱后，才能达到理想的置乱度.

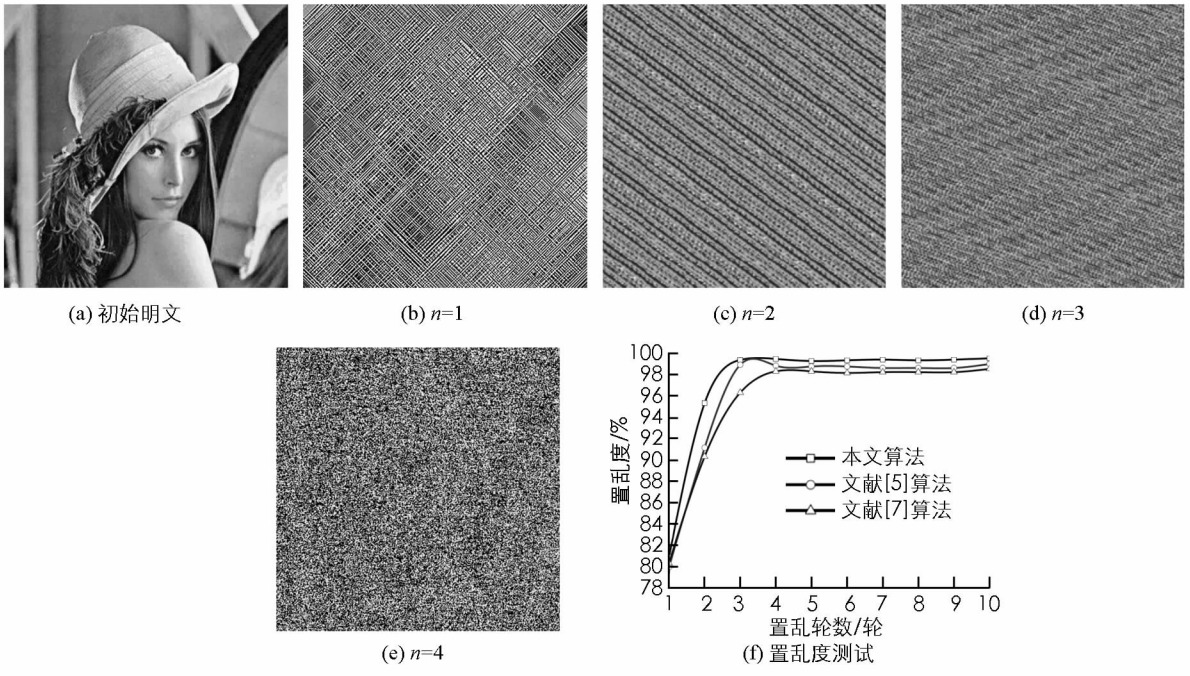


图2 动态置乱技术的混淆结果

1.2 基于复合串联混沌映射的密钥流生成

高维混沌系统(维数不低于3)的加密安全度高，但是计算复杂度太高，而低维混沌系统(维数不高于2)结构简单，加密效率高，但是其安全性不佳[12]. 为此，本文联合cos映射[13]、sin映射[14]与Logistic映射[15]这3个一维映射，设计复合串联混沌映射，以兼顾安全性与扩散效率. 3个一维映射模型如下：

$$x_{n+1} = b\cos\left(\pi\frac{x_n}{2}\right) \tag{8}$$

$$X_{n+1} = \gamma X_n(1 - X_n) \tag{9}$$

$$Y_{n+1} = a\sin(\pi Y_n) \tag{10}$$

其中：x_n, X_n, Y_n 分别是cos,Logistic以及sin混沌映射；$b \in (0, 1]$，$\gamma \in (0, 4]$，$a \in (0, 1]$ 是混沌控制参数.

根据(8)－(9)式，设计了复合串联混沌映射：

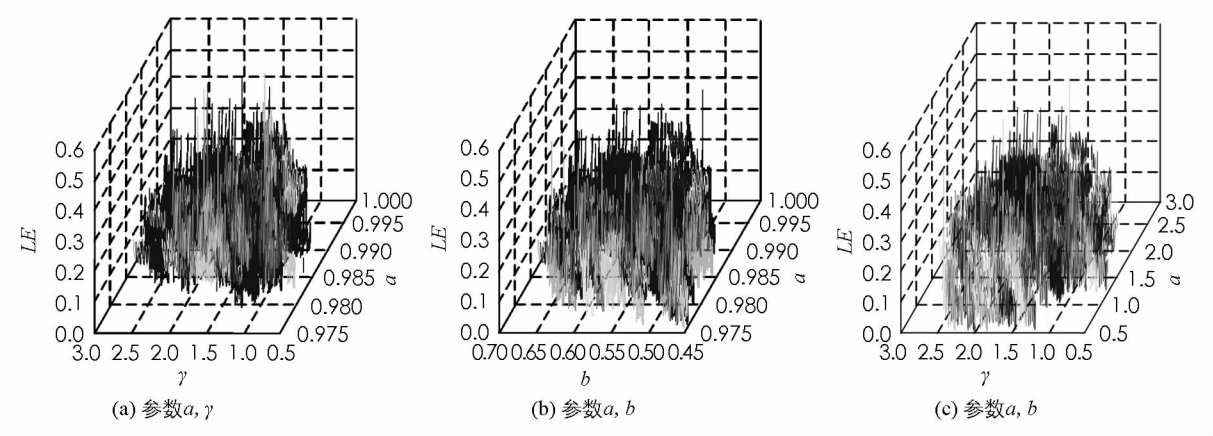
$$x_{n+1} = \mathrm{mod}\left[a\ \sin\left(b\pi\cos\left(\frac{\pi x_n}{2}\right)+\gamma b\cos\left(\frac{\pi x_n}{2}\right)\left(1-b\pi\cos\left(\frac{\pi x_n}{2}\right)\right),\ 1\right)\right] \tag{11}$$

为了测试式(11)的动力特性，本文进行了大量仿真，结果表明式(11)基本融合了式(8)－(10)的混沌窗口优势，虽然该复合映射无法在整个控制参数区间内得到理想的混沌轨迹，但是式(11)在较大区间内仍然可保持理想的混沌行为. 故本文测试了参数 $b \in [0.45,\ 0.7]$，$\gamma \in [0.5,\ 3.0]$，$a \in (0.975,\ 1]$ 的 Lyapunov 指数，结果见图 3. 依据图 3 可知，式(11)的 Lyapunov 指数在整个控制参数内均大于零.

随后，利用 Zigzag 扫描技术将置乱密文变为像素序列$\{S_i\}$，$i = 1,2,3,\cdots,M\times N$. 并输入初始条件$(x_0,\ a,\ \gamma,\ b)$对复合串联混沌映射进行迭代. 为了使得扩散过程与明文密切相关，本文利用输入图像的像素总量来产生初值 x_0：

$$x_0 = \frac{T}{10^6} \tag{12}$$

其中 T 是输入明文的像素总数.



(a) 参数a, γ　　(b) 参数a, b　　(c) 参数a, b

图 3　本文复合串联混沌映射的混沌特性测试

联合式(12)的 x_0 与控制参数$(a,\ \gamma,\ b)$，生成随机序列$\{x_i\}$，$i = 1,2,\cdots,M\times N$；并构造量化函数来处理$\{x_i\}$，获取密钥流$\{k_i\}$：

$$k_i = \mathrm{mod}(\mathrm{floor}(x_i \times 10^{14}),\ 256) \tag{13}$$

其中 floor() 为向下取整运算.

1.3　基于加密引擎函数的像素异扩散

为了提高算法的安全性，还需改变其像素值. 然而，当前加密技术均是利用同一个扩散模型，按照从第一个像素开始到最后一个像素进行加密，虽然这种扩散技术有着较高的动态性，但是有序扩散难以抵御统计攻击[16]. 为此，本文对置乱图像像素进行分组，利用密钥流，设计两个加密引擎函数，实现异扩散. 首先，将置乱像素序列$\{S_i\}$中的第一个像素 S_1 剔除，计算其余像素值的总和：

$$sum = \sum_{i=2}^{M\times N} S(i) \tag{14}$$

其中 $\sum$ 为求和运算.

再根据式(14)的总和 sum，估算初值 E_0：

$$E_0 = \mathrm{mod}(sum,\ 256) \tag{15}$$

根据 E_0，利用密钥流$\{k_i\}$，对第一个元素 S_1 进行扩散：

$$S'(1) = E_0 \oplus S(1) \oplus k(1) \tag{16}$$

其中⊕为异或运算.

由式(16)可知，图像中首个像素加密值与置乱像素总和有关，也就是对于不同的输入图像，其首个像素扩散值是截然不同的，显著增强了算法的随机特性.

对于图像中的剩余像素，设计两个加密引擎函数 kt_1,kt_2：

$$kt_1 = \mathrm{floor}\left(\frac{\mathrm{mod}(S(i-1)+k(i),\ 256)}{256\times(i-1)}\right)+1 \tag{17}$$

$$kt_2 = \mathrm{floor}\left(\frac{\mathrm{mod}(S(i-1)+k(i),\ 256)}{256\times(M\times N-i-1)}\right)+i+1 \tag{18}$$

其中：$kt_1\in[1,\ i-1]$，$kt_2\in[i+1,\ M\times N]$ 都是动态引擎.

联合 kt_1,kt_2 设计加密函数，对像素 S_i 进行扩散：

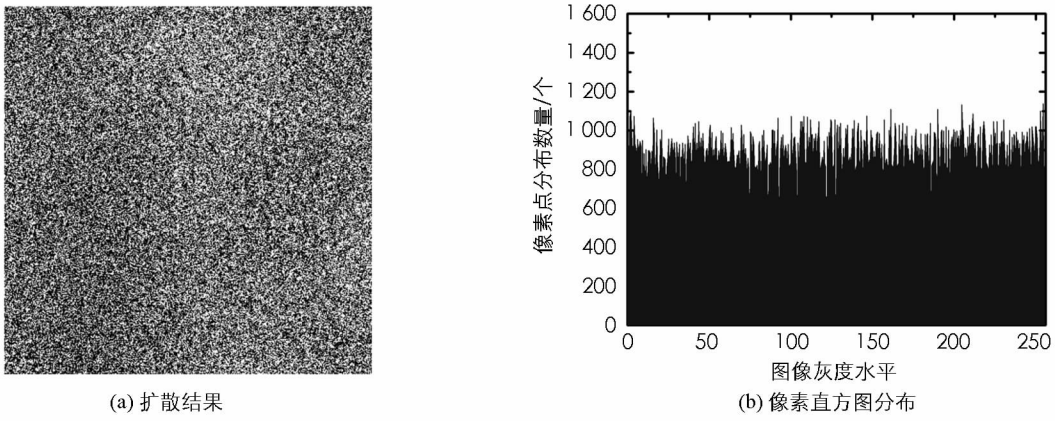
$$S'(i) = S(i)\oplus k(i)\oplus S(kt_1)\oplus S(kt_2) \tag{19}$$

其中 $S'(i)$ 是扩散像素.

重复上述过程，直到 $i=M\times N-1$. 最后，利用加密引擎 kt_1，对图像中的最后一个像素 $S(M\times N)$ 完成扩散：

$$S'(M\times N) = S(M\times N)\oplus k(M\times N)\oplus S(kt_1) \tag{20}$$

本文的异扩散将整个图像像素分为3个不同的组，利用两个加密引擎函数与密钥流进行不同的加密操作，相对于当前的扩散技术而言，有着一定的优势. 利用本文异扩散机制对图2(d)进行扩散后，结果见图4. 根据扩散结果可知，初始明文信息高度混淆，得到了一幅与置乱密文截然不同的图像，且输出密文的像素分布较为均匀，有效提高算法的抗统计攻击能力.



(a) 扩散结果 (b) 像素直方图分布

图4 本文算法的加密结果

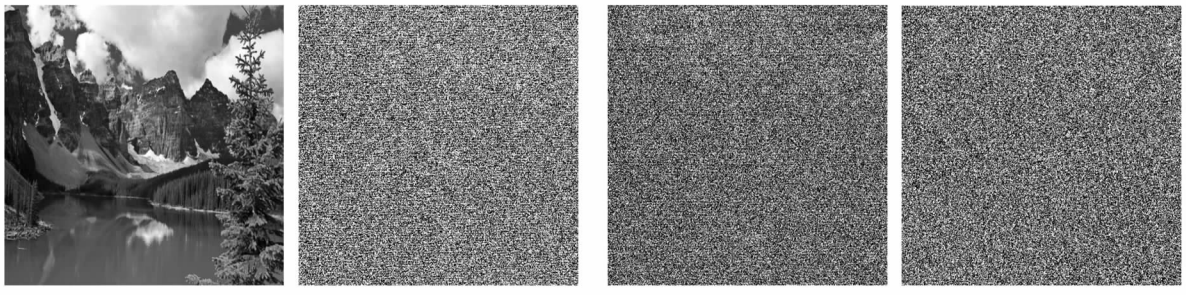
2 仿真实验与分析

借助 Matlab 工具对所提图像加密算法进行测试，同时，为了体现本文技术的优异性，将当前图像加密性能较好的算法视为对照组，并将文献[17]与文献[6]视为对照组. 在 $b\in[0.45,\ 0.7]$，$\gamma\in[0.5,\ 3.0]$，$a\in(0.975,\ 1]$ 范围内，通过对参数 b,γ,a 与 Lyapunov 指数的关系进行优化，得到一组较优的参数组合为：$\gamma=2.5$，$a=0.98$，$b=0.65$.

2.1 加密质量对比分析

以灰度明文图5(a)作为测试目标，利用本文算法、文献[17]、文献[6]对其进行加密，3种技术对应的输出密文分别见图5(b)－5(d). 根据加密结果可知，本文算法与文献[17]、文献[6]3种技术均有较好的加密质量，视觉上无差异，明文像素信息得到了高度混淆，有效地隐藏了图像内容，无信息泄露. 同时，为了体现本文加密算法与文献[17]、文献[6]两种机制的性能差异，利用信息熵值[5]来量化3者的加密安全性，各算法的密文熵值见表1. 由测试数据可知本文算法的安全性最佳，其对应的密文熵值最大，为7.996 3，

非常接近理论值 8，而文献[17]、文献[6]两种算法的密文熵值分别为 7.988 5，7.983 1. 主要是本文算法彻底避免了周期性置乱过程，通过联合黄金分割-Lucas 序列，形成动态置乱，在多轮迭代期间，使用不同的置乱变换核来实现像素混淆，且利用复合串联混沌映射与量化函数得到的密钥流构建了两个动态引擎加密函数，结合明文像素对置乱密文进行 3 部分扩散，实现了图像异扩散，从而整体上提高了算法的随机度与动态性，使得算法具有更高的安全性；而文献[17]、文献[6]算法的置乱过程均是重复性的，在每轮置乱期间，都是采用相同的置乱操作来改变像素位置，存在明显的周期性，且其扩散过程与明文无关，实质是有序扩散，使得二者的安全性要低于本文算法.



(a) 输入明文　(b) 本文算法密文　(c) 输入明[17]的密文　(d) 文献[6]的密文

图 5　3 种算法的加密质量测试

表 1　熵值测试结果

名称	本文算法	文献[17]	文献[6]
密文熵值	7.996 3	7.988 5	7. 983 1

2.2　密文相邻像素间的相关性测试

图像中相邻两像素之间的相关性对加密算法具有较大威胁，容易给攻击者留下线索，导致密文被破译，故优异的加密算法应能消除或者大幅度降低这种负面影响[17]. 为此，本文在图 5(b)、图 5(c) 、图 5(d) 中随意选择 2000 对相邻像素点来测试算法的安全性，相邻像素之间的相关性系数 C_{xy} 计算函数为[17]：

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

其中 E 代表期望值.

3 种加密技术对应的密文像素在水平方向上的分布情况见图 6. 由图 6(a) 可见，输入明文相邻像素间的相关性非常高，像素分布不均匀，聚集于对角线，其 C_{xy} 值达到为 0.937 2；但是明文经过本文算法、文献[17]、文献[6]3 种技术处理后，这种强烈的相关性得到了大幅降低，扩散后的密文像素分布都比较均匀，其相关性系数分别为 0.001 8，0.003 5，0.005 1，然而，本文算法的密文像素分布最为均匀，无“像素聚堆”现象，其均匀程度要高于文献[17]、文献[6].

3 种算法对应的密文在其他两个方向上的 C_{xy} 测试数据见表 2. 根据表 2 中数据可知，不管是哪个方向，明文中相邻像素的 C_{xy} 值始终是最高的，而利用 3 种加密技术对其置乱-扩散后，3 个方向上的相关系数值均大幅下降，且本文算法的相关系数 C_{xy} 值最小. 原因是所提算法通过设计黄金分割-Lucas 动态置乱技术，通过实时改变每一轮置乱的变化核，降低了置乱周期性，显著提高了算法的随机度，且通过异扩散将图像分为 3 部分进行加密，改善了算法的动态性；而文献[17]与文献[6]则是通过周期性置乱与有序扩散，使其随机度不佳，导致相邻像素的相关性要高于所提算法.

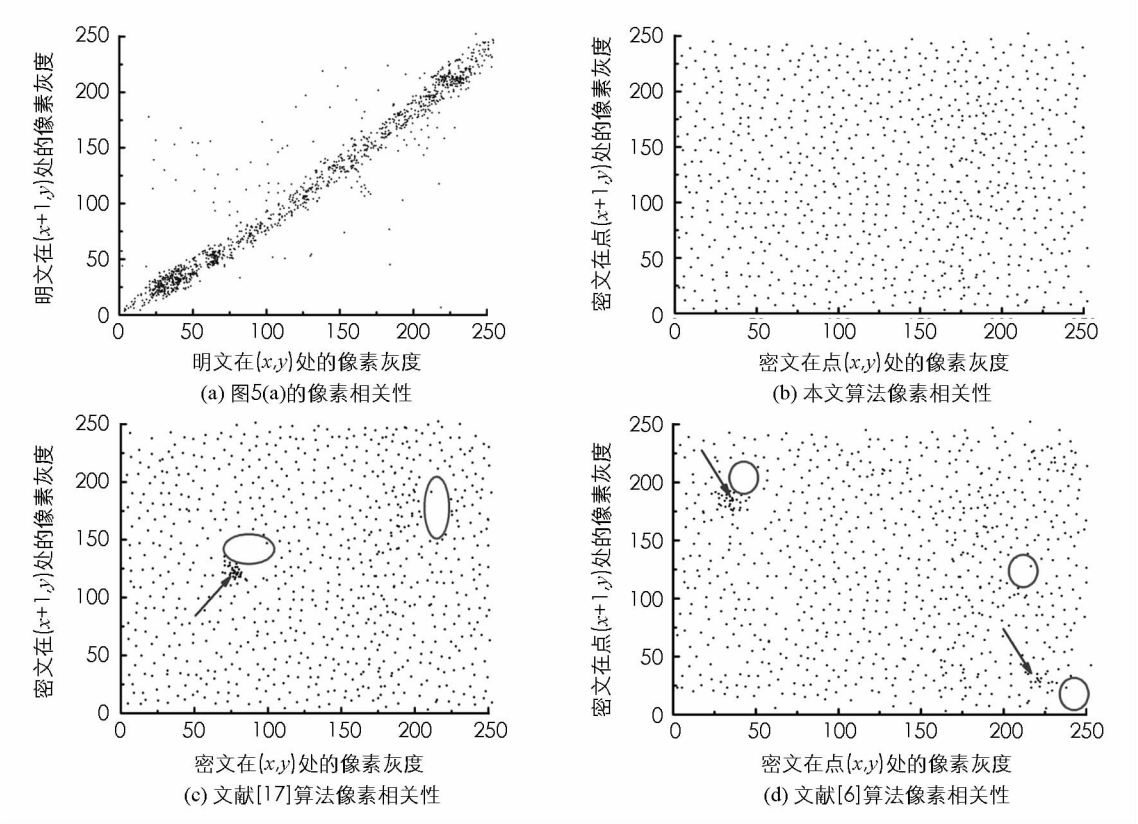


图 6 明文与各算法对应的密文像素之间的相关性测试

表 2 不同方向的相关系数测试结果

选取方向	相关系数			
	明文	本文算法	文献[17]	文献[6]
水 平	0.937 2	0.001 8	0.003 5	0.005 1
垂 直	0.953 9	0.002 5	0.006 1	0.007 3
对角线	0.916 4	−0.001 4	0.004 3	−0.002 9

2.3 抗明文攻击与抗噪声攻击性能分析

明文攻击是加密算法中常遇到的攻击手段，对图像安全传输造成较大的威胁，因此，良好的加密算法应有较强的抗明文攻击性能[3]. 当前，常用 UACI(unified averaged changed intensity) 曲线来量化抗明文攻击能力，其计算模型分别为[5]：

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} Difp(I(i,j), I'(i,j))}{W \times H} \times 100\% \tag{22}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{ij} \frac{|I(i,j) - I'(i,j)|}{255}\right] \times 100\% \tag{23}$$

$$Difp(I(i,j), I'(i,j)) = \begin{cases} 0 & I(i,j) = I'(i,j) \\ 1 & I(i,j) \neq I'(i,j) \end{cases} \tag{24}$$

利用文献[5]的方法，计算3种算法的NPCR与UACI曲线(图7). 由测试结果可知，经过多轮置乱与扩散后，3种加密技术都呈现出良好的抗明文攻击能力，但是本文算法扩散操作与明文密切相关，且对明文3个不同部位的像素进行同扩散，使得所提算法的抗明文攻击能力最强，其对应的NPCR与UACI值都是最大，分别为99.53%,34.39%，而[17]、文献[6]两种算法主要是凭借高维混沌系统的复杂轨迹来改善算法的安全性，其扩散过程忽略了明文，而且周期性置乱操作也削弱了算法的安全性，导致二者的抗明文攻

击能力不佳，其 NPCR 与 UACI 值均要低于本文算法.

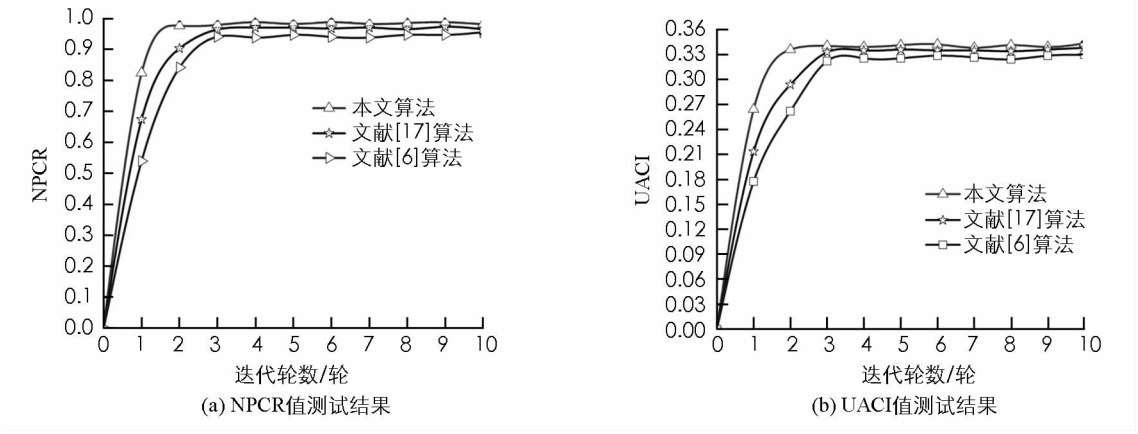


图 7　三种算法的抗差分攻击性能测试

同时，在图像处理和传输过程中都会有噪声的影响，故良好的加密机制是具有理想的抗噪声攻击能力[18]. 为此，本文将方差为 0.3 的高斯噪声嵌入在图 5(b)－(d) 中，输出相应的噪声密文：

$$E' = E(1 + KN) \tag{25}$$

其中：E' 是噪声密文；k 代表噪声强度系数；N 是高斯噪声.

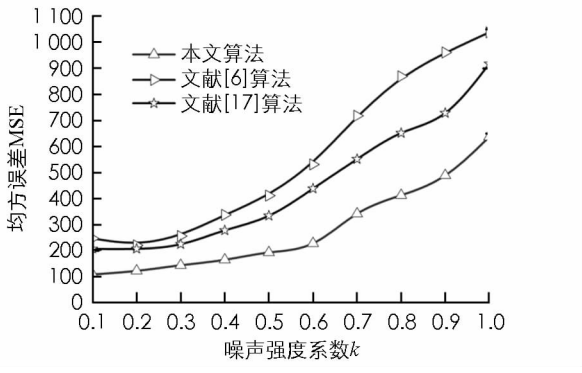


图 8　3 种算法的抗噪声攻击能力测试

3 种算法在噪声干扰下的复原结果见图 8 与表 3. 根据 MSE 曲线与表 3 可知，各算法的复原图像的 MSE 值与 k 值成正比. 文献[17]、文献[6] 与本文算法均有较好的抗噪声攻击能力，但是所提算法的抗噪攻击能力最强. 当 $k = 1$ 时，本文算法的复原图像的 MSE 值要低于文献[17]、文献[6]，3 者分别为 654，902，1 043，均远低于解密阈值 3 000. 这显示本文动态加密技术具有更强的抗噪攻击性能.

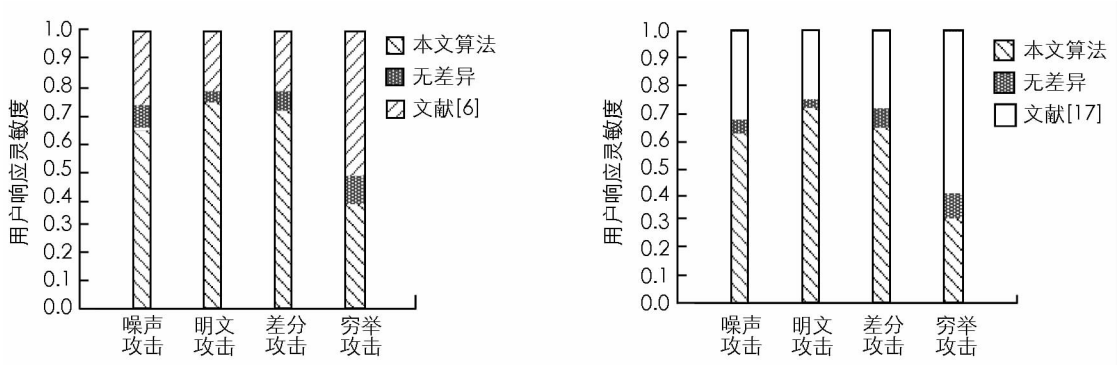
表 3　不同算法的抗噪声攻击能力测试结果

噪声系数 k	均方误差 MSE		
	本文算法	文献[17]	文献[6]
0.1	109	207	248
0.2	123	208	221
0.3	145	226	257
0.4	166	278	338
0.5	194	335	412
0.6	229	438	531
0.7	342	552	718
0.8	413	652	869
0.9	489	729	961
1.0	654	902	1 043

2.4　算法用户响应分析

用户响应是衡量加密算法实用性的常用指标，为此，本文利用 Amazon Mechanical Turk[19] 来测试本文算法与文献[17]、文献[6]3 种算法的用户响应. 选择明文攻击、差分攻击、噪声攻击以及穷举攻击[5] 为样本进行测试，响应结果见图 9. 据图 9 可知，在网络中遇到噪声攻击、差分攻击以及明文攻击时，本文加密技术具备更高的用户响应，而文献[17]、文献[6]的受欢迎度不佳. 但是面对穷举攻击时，由于文献[17]、

文献[6]使用了高维混沌系统，增大了算法的密钥空间，导致二者的抗穷举攻击能力要高于本文算法，从而使得两种算法的用户响应要略高于本文加密技术.



(a) 本文算法与文献[6]算法比较 (b) 本文算法与文献[17]算法比较

图9 3种算法的用户响应测试

3 结 论

为了避免图像像素置乱采用周期性操作与有序扩散而导致算法的安全性不佳的问题，本文提出了黄金分割-Lucas动态置乱与异扩散的图像加密算法. 结合黄金分割与Lucas序列，设计动态置乱技术，改变每一轮置乱的变换核，降低周期性，显著提高了像素置乱度. 并设计了复合串联混沌映射与量化函数，利用其输出的密钥流来设计异扩散机制，分别对相应的第一个像素、最后一个像素以及中间像素进行独立加密，从而提高算法的安全性与随机性. 测试结果表明所提算法拥有更高的抗攻击能力与用户响应.

参考文献：

[1] 王 永，雷 鹏. 一种基于Baker映射与时空混沌的图像加密算法[J]. 重庆邮电大学(自然科学版)，2015，27(4)：556－562.

[2] 张文娟，王大羽，余梅生. 基于两种独立混沌函数的图像加密算法[J]. 重庆邮电大学学报(自然科学版)，2017，29(2)：232－239.

[3] 孙 力，黄正谦，傅为民. 时间延迟与超混沌Chen系统相融合的图像加密算法研究[J]. 科学技术与过程，2014，12(35)：10523－10530.

[4] ÇAVUŞOGLU ÜNAL，KAÇAR SEZGIN. Secure Image Encryption Algorithm Design Using a Novel Chaos Based S-Box [J]. Chaos Solitons & Fractals，2017，95(18)：92－101.

[5] 李凯佳，俞锐刚，袁凌云. 基于DNA-记忆元胞自动机与Hash函数的低延迟图像加密认证算法[J]. 计算机工程与设计，2017，38(2)：470－477.

[6] WU X，WANG D，KURTHS J. A Novel Lossless Color Image Encryption Scheme Using 2D DWT and 6D Hyperchao [J]. Information Sciences，2016，38(7)：502－512.

[7] 谢国波，丁煜明. 基于Logistic映射的可变置乱参数的图像加密算法[J]. 微电子学与计算机，2015，12(4)：111－115.

[8] 赵 锋，吴成茂. 自编码和超混沌映射相结合的图像加密算法[J]. 计算机辅助设计与图形学学报，2016，28(1)：119－128.

[9] CODARA P，D'ANTONA O M. Generalized Fibonacci and Lucas Cubes Arising from Powers of Paths and Cycles [J]. Discrete Mathematics，2014，339(3)：241－251.

[10] 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.

[11] LI L，EL-LATIF A，NIU X. Elliptic Curve El-Gamal Based Homomorphism Image Encryption Scheme for Sharing Secret Images [J]. Signal Process，2012，38(92)：1069－1078.

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

[13] 朱竹青，冯少彤. 基于离散余弦变换的复值加密图像隐藏技术 [J]. 中国激光，2009，36(1)：177－181

[14] 张同锋. 基于一维复合混沌映射的数字图像加密算法研究 [D]. 兰州：兰州大学，2016，34－38.

[15] WANG X, WANG Q, ZHANG Y. A Fast Image Algorithm Based on Rows and Columns Switch [J]. Nonlinear Dynamics, 2015, 79 (2): 1141－1149.

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

[17] LI Y, WANG C, CHEN H. A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation [J]. Optics and Lasers in Engineering, 2016, 38(7): 117－126.

[18] WANG Y, QUAN C, TAY C J. Asymmetric Optical Image Encryption Based on an Improved Amplitude-Phase Retrieval Algorithm [J]. Optics and Lasers in Engineering, 2016, 78(5): 8－16.

[19] SIMCOX T, FIEZ J A. Collecting Response Times Using Amazon Mechanism Turk and Adobe Flash [J]. Behavior Research Method, 2014, 48(1): 95－111.

On Image Encryption Algorithm Based on Gold Segmentation-Lucas Dynamic Scrambling and Different Diffusion

WANG　Yao[1]，　XU　Yang[2]

1. Department of Information Engineering, Chongqing City Vocational College, Chognqing 402160, China;

2. College of Computer Science and Engineering, Guizhou Normal University, Guiyang 550001, China

Abstract: In order to solve the defect such as low dynamic and random degree resulting in low security caused by same pixel location scrambling process with each round, and the orderly diffusion operation, the image encryption algorithm based on gold segmentation-Lucas dynamic scrambling and different diffusion has been proposed in this paper. Firstly, the plaint pixel scrambling degree was effectively improved by introducing the gold segmentation-Lucas transform mechanism to dynamic transform the permutation changing kernel according to the iteration number so that the pixel scrambling operation is different during each round. Then the complex tandem chaotic mapping was designed based on Cosine map, sine map and Logistic map to produce its initial conditions according to the pixels number of cipher for outputting the random sequence, and a quantization function was constructed to quantifies the sequence to obtain the key-streams. Finally, the block image is grouped, and the two encryption engine functions are designed combination with the key stream. By constructing the pixel encryption model, the first pixel, middle pixels and the last pixel of the image is diffused to finish the image encryption. The experimental results show that this proposed algorithm has higher security and user response with stronger anti-shear, anti-plaintext attack capability compared with the current chaotic encryption technology.

Key words: image encryption; gold segmentation-Lucas scrambling; composite tandem chaotic mapping; quantization function; encryption engine function; heterogeneous diffusion; user response

责任编辑　张　枸