基于无序分割投影策略与重力模型的图像加密算法

李长齐，王菡
（保山学院，保山 678000）

摘要：目的 解决当前图像算法因其像素置乱和扩散操作与明文无关，导致其抗明文攻击能力较弱，且其置乱过程存在周期性，使其安全性不佳等问题。**方法** 提出基于无序分割投影策略与重力模型的图像加密算法。首先对输入明文进行无序分割，获取重叠子块，并构建每个子块的位置坐标计算模型，输出图像子块的位置；根据明文像素量计算 Kent 映射的初值，通过迭代 Kent 映射获取随机序列组；定义位置置乱机制，对重叠子块进行混淆；再引入分割投影策略，互换每个置乱子块中的像素位置，再对其重组，输出置乱密文；通过设计像素质量变化函数替换重力模型的固定质量，改进重力模型，对置乱密文完成像素加密。**结果** 实验结果显示与当前图像加密技术相比，文中算法具有更高的安全性，输出密文中的相邻两像素间的关联度最低，具有更强的抗明文攻击与剪切攻击性能。**结论** 所提加密算法能够较好地用于图像信息安全传输，具有较好的应用价值。

关键词：图像加密；无序分割；投影策略；重力模型；Kent 映射；位置置乱机制
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2017)07-0191-06

Image Encryption Algorithm Based on Chaotic Segmentation Projection Strategy and Gravity Model

LI Chang-qi, *WANG Han*
(Baoshan University, Baoshan 678000, China)

ABSTRACT: The work aims to solve these defects, such as low anti-plaintext attack ability induced because the pixel scrambling and diffusion of the current image algorithm are not related to the plaintext, and the poor security caused by periodicity in the scrambling process. The image encryption algorithm based on chaotic segmentation projection strategy and gravity model was proposed. Firstly, the overlapping sub-blocks were obtained by chaotic segmentation of the input plaintext, and the calculation model for the position coordinates of each sub-block was built to output the positions of image sub-blocks. Then, the initial value of Kent mapping was calculated according to the quantity of plaintext pixels, and the random sequence set was obtained by iterative Kent mapping. Overlapping sub-blocks were confused by defining the position scrambling mechanism. The pixel positions in each scrambled sub-block were interchanged by introducing the segmentation project strategy and the scrambled cipher was outputted by reorganizing theses sub-blocks. Finally, the gravity model was improved by designing the quality change function of the pixel to substitute the fixed quality for pixel encryption of the scrambled cipher. The experimental results showed that, compared to the current image encryption technique, the proposed algorithm had greater security, and the correlation of two adjacent pixels in the outputted cipher was the minimum, with stronger anti-plaintext and anti-shear attack performances. The proposed encryption algorithm can be better used for the safe transmission of image information and has better application value.

KEY WORDS: image encryption; chaotic segmentation; projection strategy; gravity model; Kent mapping; position scrambling mechanism

收稿日期：2016-10-20
基金项目：云南省教育厅指导性项目（2016ZDX139）
作者简介：李长齐（1981—），男，硕士，保山学院讲师，主要研究方向为教育技术学、计算机技术。

二维码图像在物流、包装、印刷等领域应用广泛，然而，图像通常是在未知授权的网络环境中传输，易遭遇到黑客攻击，使得图像信息被窃取，导致信息面临巨大威胁，当前，图像信息安全已成为当今各国的研究重点[1−2]。传统的数据加密机制没有考虑到图像的大数据容量与高冗余度等特征，无法确保图像安全传输[3]，因此，对数字图像的加密算法研究较多[4]，较为主流的算法就是基于混沌理论来完成图像加密。如柴秀丽等人[5]设计了基于超混沌系统的位级自适应彩色图像加密新算法，通过迭代 Chen 超混沌系统产生的混沌序列对原始彩色图像的 R，G，B 分量图像进行置乱和扩散，并在位级完成像素扩散。然而，利用四维混沌系统对其完成图像置乱，使得算法复杂度较高，且通过迭代混沌系统产生的随机序列存在明显的周期性，易给攻击者留下破绽，降低算法的安全性。贾嫣等[6]提出了基于改进混沌映射的图像加密算法，通过迭代雅克比椭圆映射，输出密钥，并采用位置集合置乱方法对该密钥进行处理，获取位置集合，从而完成明文像素加密。雅克比椭圆映射为 1D 映射，且该技术只有置乱过程，无法改变像素值，加上迭代混沌映射的周期性，使得算法的安全性不高。Wang 等[7]提出了基于迭代混沌映射结构的彩色图像加密算法，先将彩图 RGB 三分量转换成矩阵，再利用 1DLogistic、2DLogistic 混沌映射生成置乱矩阵，对彩图明文完成置乱，并引入 XOR 算子对明文矩阵进行扩散，完成彩色图像加密，但是，利用迭代低维混沌映射产生的矩阵对其完成混淆，存在周期性，且其加密过程脱离了明文，使其安全性有待提高。

对此，为了削弱迭代混沌系统的周期性，使加密过程与明文紧密相关，继而提高抗明文攻击能力，文中提出了基于无序分割投影策略与重力模型的图像加密算法。通过明文完成无序分割，获取重叠子块，并根据子块位置坐标计算模型，输出图像子块的位置；利用明文像素量来计算 Kent 映射的初值，通过迭代该映射，输出随机序列组；定义位置置乱机制，对重叠子块进行混淆；再引入分割投影策略，互换每个置乱子块中的像素位置，再对其重组，输出置乱密文；最后，利用改进的重力模型改变置乱密文的像素值。并测试了文中算法的加密性能与抗明文攻击能力。

1 文中图像加密算法设计

为了使得加密算法与明文紧密相连，消除混沌的周期性，文中提出了基于无序分割投影策略与重力模型的图像加密算法，其置乱-扩散过程见图 1，包括：基于位置置乱机制与分割投影策略的明文置乱；基于改进的重力模型的置乱密文像素扩散。通过将明文分割为重叠块，定义位置置乱机制，改变每个子块的像素位置，并引入分割投影策略，提取投影线，对每个重叠块内的像素完成细混淆，提高明文的置乱度。为了增强算法的敏感性，构建像素质量变化函数，从而改进了重力模型，对混淆密文进行扩散。

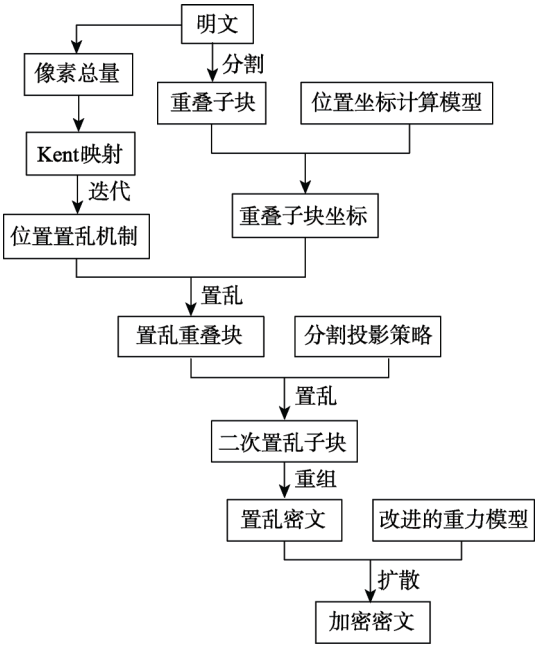


图 1 文中加密算法过程

Fig.1 Encryption algorithm process

1.1 基于位置置乱机制与分割投影策略的明文置乱

为了增强算法的安全性，文中将输入明文分割重叠块，增加子块可用数量。假设输入明文为 I，其大小为 $M\times N$，将其无序分割为 $a\times a$ 的重叠子块。首先，根据明文，建立 2D 坐标，令 $L\in[1,a]$是图像在 x 与 y 2 个方向上相邻重叠子块间的重叠尺寸；而 n_x，n_y 分别是 x, y 方向上的子块数量，则对于 $M\times N$ 的明文 I，子块总数 $n_{\text{total}}=n_x\times n_y$。其中，$n_x, n_y$ 的计算函数为：

$$n_x=\begin{cases}\dfrac{N-L}{a-L} & \text{Mod}(N-L,a-L)=0\\ \left\lceil\dfrac{N-L}{a-L}\right\rceil+1 & \text{else}\end{cases} \tag{1}$$

$$n_y=\begin{cases}\dfrac{M-L}{a-L} & \text{Mod}(M-L,a-L)=0\\ \left\lceil\dfrac{M-L}{a-L}\right\rceil+1 & \text{else}\end{cases} \tag{2}$$

式中：⌈ ⌉是向上取整运算。

为了对重叠子块实现初步置乱，文中首先确定每个重叠子块的坐标 X_i, Y_i，其位置坐标计算模型为：

$$X_i=(i-1)(a-L),\ i=1,2\cdots n_x-1 \tag{3}$$

$$Y_i=(j-1)(a-L),\ j=1,2\cdots n_x-1 \tag{4}$$

$$X(n_x)=\begin{cases}(i-1)(a-L) & \text{mod}(N-L,a-L)=0\\ N-L+1 & \text{else}\end{cases} \tag{5}$$

$$X\left(n_y\right)=\begin{cases}(i-1)(a-L) & \bmod(M-L,a-L)=0\\ M-L+1 & \text{else}\end{cases} \tag{6}$$

依据式(3)—(6)，可以得到任意重叠子块的坐标为(X_{ni}, Y_{ni})。随后，依据明文像素总量，引入 Kent 映射，生成随机数组，从而构建位置置乱机制。其中，Kent 映射模型[8]为：

$$F(x)=\begin{cases}x/p & x\in(x,p]\\ (1-x)/(1-p) & x\in(p,1)\end{cases} \tag{7}$$

式中：p 为 Kent 映射的混沌调节参数。

当 $x\in(0,1)$, $p\in(0,1)$时，式(7)是混沌的。在初始条件 x_0, p 2 个初值条件下，Kent 映射输出的数字是非周期性的。同时，为了使得加密算法与明文紧密相关，文中利用明文像素总量来生成控制参数 p 与预迭代次数 K：

$$\begin{cases}p=T/10^8\\ K=\bmod(T,1000)\end{cases} \tag{8}$$

式中：T 为明文像素总量。

通过设置好初值 x_0，结合式(8)的 p, K，迭代 Tent 映射，将前 K 次输出的结果删除，以消除瞬态效应，最终得到随机数组 $F=(f_K, f_{K+1}, f_{K+2}\cdots f_{M\times N})$。再将 $F=(f_K, f_{K+1}, f_{K+2}\cdots f_{M\times N})$按照递增顺序，对其重排，形成新的数组 $F'=(f'_1, f'_2, f'_3\cdots f'_{M\times N-K})$。然后再数组 $F=(f_K, f_{K+1}, f_{K+2}\cdots f_{M\times N})$中确定 $F'=(f_1, f_2, f_3\cdots f_{M\times N-K})$的位置，得到位置序列 $S=(s_1, s_2\cdots s_n)$：

$$f'_i=f_{s_i} \tag{9}$$

利用位置序列 $S=(s_1, s_2\cdots s_n)$对重叠子块完成初步置乱，改变这些重叠子块在明文中的位置。虽然位置置乱能够改变重叠子块的位置，但是子块内的像素伪造却没有变，使得明文的置乱度不高，因此，文中引入分割投影策略[9]，通过提取投影线的像素，交换重叠子块中的像素位置，其互换过程见图 2。

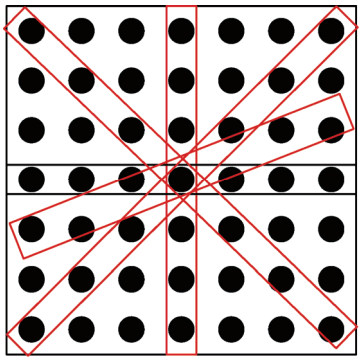


图 2　分割图像的投影线

Fig.2 Projection line for split image

为了利用非重叠子块的投影线来改变其内部像素的位置，需要提取每个子块的投影线。若子块的 B_i 的大小为 $a\times a$，其中心像素位置为(x_c, y_c)，则有 $x_c=m/2$, $y_c=m/2$。令 $u_{i,\theta}$为第 i 个子块在角度 $\theta\in[0, 179]$线上的全部像素集合，则 $u_{i,\theta}$就是采集到的投影线。则 $u_{i,\theta}$内的像素满足：

$$-\frac{1}{2}\leqslant(x-x_c)\cos\theta+(y-y_c)\sin\theta\leqslant\frac{1}{2} \tag{10}$$

图像子块 B_i 可表征为 $U_i=\{u_{i,0}, u_{i,1}\cdots u_{i,179}\}$，故对每个子块内像素的位置进行置乱时，只需对其投影线进行混淆。例如，对于子块 B_j 与 B_i，通过互换二者的投影线 $u_{j,\theta}$与 $u_{i,\theta}$，则子块 B_j与 B_i内所有像素被改变。对于文中加密算法，由于不同的 θ，对应的投影线是不同的。而在对投影线 $u_{j,\theta}$ 与 $u_{i,\theta}$ 进行交换时，必须确保 B_j, B_i无交叉部分，故文中定义了图像子块重叠识别准则：

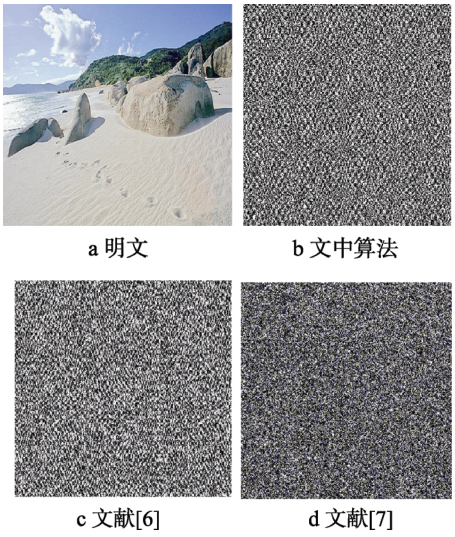
$$\left|X[u_i]-X[u_j]\right|<a \tag{11}$$

$$\left|Y[v_i]-Y[v_j]\right|<a \tag{12}$$

式中：$\left(X_{u_i}, Y_{v_i}\right)$，$\left(X_{u_j}, Y_{v_j}\right)$分别为 B_i与 B_j的坐标。

当子块 B_i 与 B_j同时满足式(11)与式(12)，则二者存在重叠部分；否则，二者无交叉部分。经过分割投影策略混淆后，对这些子块进行重组，输出置乱密文 I'。以图 3a 为样本，利用文中置乱技术、文献[6]与文献[7]对其进行混淆，结果见图 3。由人眼视觉系统可知，3 种算法的置乱技术都较为理想，较好地将图像信息隐藏起来。为了量化这 3 种置乱技术的优异差距，文中引入置乱度[10]来评估：

$$Q=\frac{\left\|R'_{M\times N}\right\|-\left\|R_{M\times N}\right\|}{M\times N-\left\|R_{M\times N}\right\|} \tag{13}$$



a 明文　　b 文中算法

c 文献[6]　　d 文献[7]

图 3　各算法的置乱质量

Fig.3 Scrambling quality of each algorithm

式中：R'为置乱密文；R 为明文；$M\times N$ 为明文尺寸。

根据文献[10]的方法，测试图 3b—d 3 个密文的置乱度，结果见图 4。由图可知，文中算法的置乱效果最高，明文像素的置乱度约为 98.14%，文献[6]与

文献[7]的置乱密文的置乱度均低于文中技术。原因是文中构建了位置置乱机制，对明文子块进行粗混淆，并引入分割投影策略，通过提取每个子块的投影线，对 2 个不重叠的子块进行互换，显著避开了混沌周期性，有效增加了动态性，从而提高了算法的置乱度；文献[6]、文献[7] 2 种技术都是依赖混沌系统来改变明文像素位置，难以消除周期性，使其置乱效果不佳。

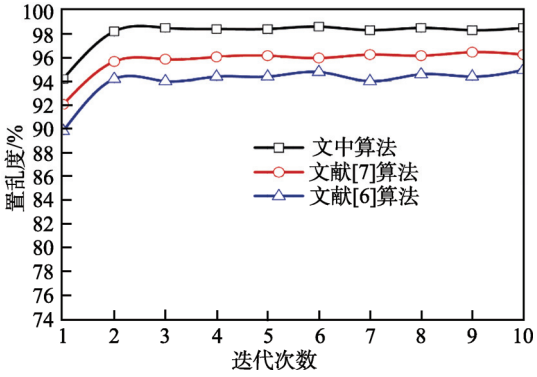


图 4 置乱度测试结果

Fig.4 Results of scrambling degree test

1.2 基于改进的重力模型的置乱密文像素扩散

虽然位置置乱机制与分割投影策略能够彻底改变明文像素位置，但其仍然不能改变像素值，因此，文中基于重力模型[11]，构建像素扩散结构，完成加密。令置乱密文为 $I'=\{f(i,j)\leqslant 256;\ i=1,2\cdots M,\ j=1,2\cdots N\}$，将其每个像素都视为一个粒子，随机择期粒子 P，则 P 与密文 I'的空间关系见图 4[11]。依据重力的概念，粒子 P 与密文 I'中的每个像素间都存引力，故文中利用该特性来改变像素值。文献[11]已利用重力模型，实现了图像加密的目的，并验证了其有效性：

$$B'_{ij}=\left[\frac{G\times m(x,y,z)\times m_{ij}(i,j)}{(x-i)^2+(y-j)^2+z^2}\right]\bmod\left(256\oplus B_{ij}\right) \quad (14)$$

$$\begin{aligned} m(x,y,z)&=1\\ m(i,j)&=21i^2+j^3+5\end{aligned} \quad (15)$$

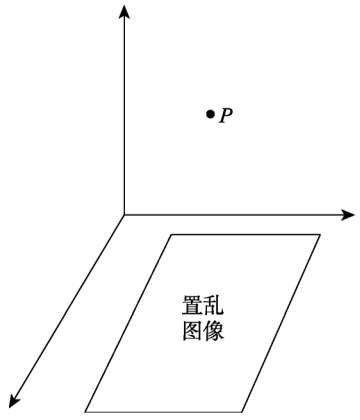


图 5 置乱密文在空间内的平面映射[11]

Fig.5 Plane mapping in the space of scrambling cipher text

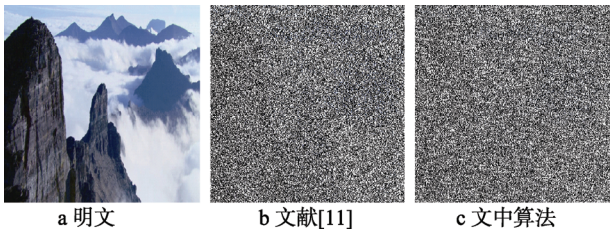
式中：G 为重力系数；$m(x,y,z)$为粒子质量；(x,y,z)为粒子空间位置；$m(i,j)$为像素质量；B_{ij} 为置乱密文的像素值；B'_{ij} 为扩散像素值；$\oplus$ 为异或和运算。为确保式(14)的分母不为 0，设置 $z\neq 0$。

依据式(15)可知，传统的重力模型所定义的像素质量 $m(x,y,z)$是固定，使得算法的随机性较低，故文中构建像素质量变化函数，以替换文献[11]中的 $m(x,y,z)=1$：

$$B'_{ij}=\left[\frac{G\times m_0(x,y,z)\times m_{ij}(i,j)}{(x-i)^2+(y-j)^2+z^2}\right]\bmod 256\oplus B_{ij} \quad (16)$$

$$m(x,y,z)=3000\times\bmod\left[\left(12\times x^2+\sqrt{(x+y)^3}\right),256\right] \quad (17)$$

依据式(17)可知，文中像素质量变化函数与置乱密文的像素位置紧密相关，不同的像素，其位置不同，从而增加了算法的随机特性，改善算法敏感性。为了验证改进前后的重力模型像素扩散效果，将文献[11]视为对照组，以图 6a 视为样本，沿用文献[11]的参数 x=150, y=300, z=150, $G=3\times 10^8$，利用式(14)与式(16)对其完成扩散，结果见图 6b—c，依图可知，利用式(14)对图像像素进行扩散，能够取得更好的加密质量，见图 6b。



a 明文　b 文献[11]　c 文中算法

图 6 改进前后的重力模型扩散效果

Fig.6 Diffusion effect of gravity model before and after improvement

2 实验结果与分析

为了测试所提算法的有效性，在 Matlab 工具中进行加密实验，同时，为了体现该算法的优势，将当前加密性能较高的算法视为对照组：文献[7]与文献[12]。算法参数设置为：x_0=0.5, x=150, y=300, z=150, $G=3\times 10^8$。

2.1 加密质量对比分析

以图 7a 为目标，用文中加密算法、文献[7]、文献[12]对其像素进行置乱-扩散处理，对应的密文见图 7b—d。根据输出密文可知，文中算法与对照组都能够较好地将图像信息隐藏，均无明显的信息外泄。为了反映出本文算法的加密优势，引入信息熵值[13]来评估 3 种算法对应的密文安全性，文中算法的密文熵值为 7.9913、文献[12]的为 7.9814、文献[7]的

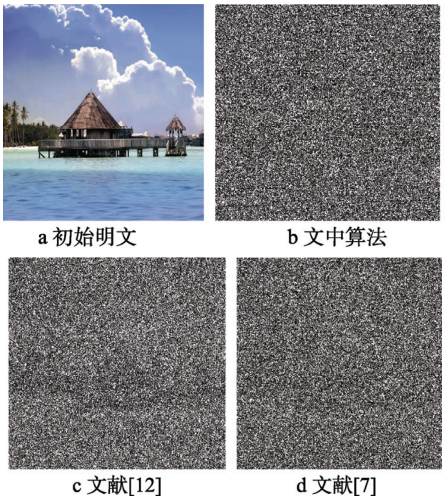


图 7　3 种算法的加密质量

Fig.7 Encryption quality of the three algorithms

为 7.9862。由表可知，所提算法对应的输出密文的熵值最大，为 7.9913，而文献[12]、文献[7] 2 种加密技术的密文的熵值分别为 7.9814, 7.9862。原因定义了位置置乱机制，对重叠子块的像素位置进行混淆，再引入分割投影策略，对非重叠块中的像素位置进行互换，实现了子块间、子块内的双重置乱，有效避免了混沌周期性，且利用改进的重力模型对置乱密文像素进行扩散，有效提高了密文安全性；而文献[12]、文献[7] 2 种技术都是严重依赖混沌系统，利用其输出随机序列完成置乱与扩散，而混沌周期性会降低算法安全性。

2.2　相邻像素的相关性测试

相邻像素间的强烈相关性易被攻击者利用，从而导致密文被破译，对图像信息安全造成严重威胁，因此，理想的加密算法应能有效降低这种紧密度，以提高抗击统计攻击[14]，在图 7a, b 中随机选取 2000 对相邻像素点，计算其相关系数[14]Q_{xy}：

$$Q_{xy}=\frac{1/n\sum_{i=1}^{n}\left(x_i-E(x_i)\right)\left(y_i-E(y_i)\right)}{\sqrt{\left(1/n\sum_{i=1}^{n}\left(x_i-E(x_i)\right)^2\right)\left(1/n\sum_{i=1}^{n}\left(y_i-E(y_i)\right)^2\right)}} \tag{18}$$

图 8 显示的是图 7a, b 在水平方向上的 Q_{xy} 结果，根据图 8a 中的像素分布状况，图 7a 的相邻像素间紧密度非常强烈，表现为对角线，其值为 0.9422；利用文中加密机制对其扩散后，图 7b 中的相邻像素间的紧密度被有效降低，从而增强算法的安全性，见 8b，其 Q_{xy} 值为 0.0015。

另外，图 7a 在垂直方向 Q_{xy} 值为 0.8947、对角线方向的 Q_{xy} 值为 0.9257；图 7b 在垂直方向 Q_{xy} 值为 0.0039、对角线方向的 Q_{xy} 值为 0.0033 测试数据见表 2。可见，明文经过所提算法的置乱与扩散后，这种强烈的紧密度被有效削弱。

2.3　抗明文攻击性能测试

选择明文攻击是威胁图像安全传输的常见攻击手段之一，也是衡量加密算法的优异性的重要指标[15]，为此，文中引用像素变化率（NPCR）与平均变化强度（UACI）2 个指标[16]来量化。以图 7a 为目标，利用文献[15]的计算方法，形成 3 个密文对应的 NPCR 与 UACI 曲线，见图 9。依图可知，文中算法定义的位置置乱机制与明文密切相关，且消除了混沌周期

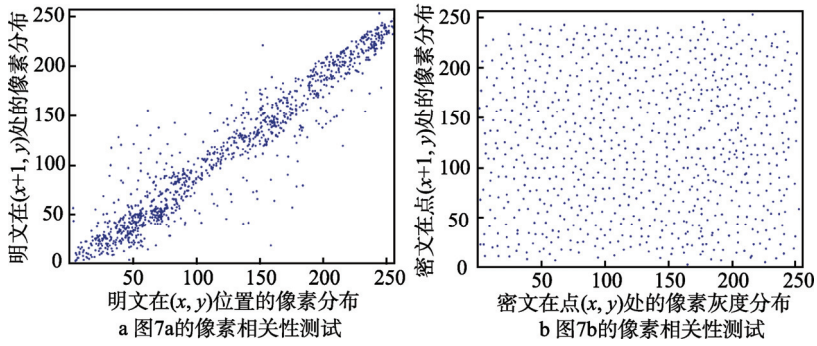


图 8　明文与密文像素间的相关性测试

Fig.8 Correlation test between the text and the pixels of the encrypted text

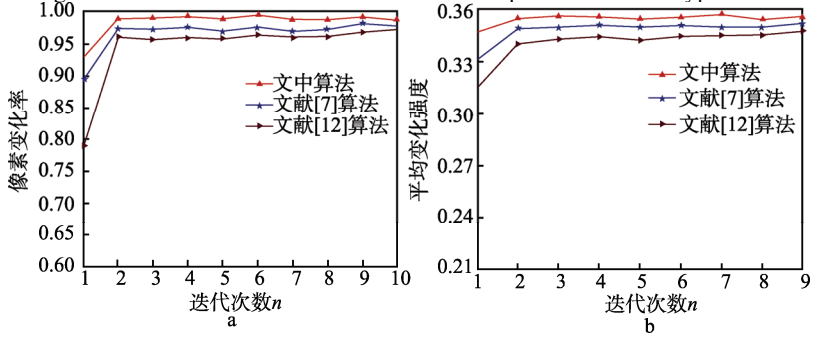


图 9　3 种算法抗明文攻击测试

Fig.9 Three algorithms against plain text attack test

性，使得所提算法的抗明文攻击能力最强，导致文中算法输出密文的 NPCR 与 UACI 值更高；而文献[7]、文献[12] 2 种算法的像素置乱与扩散操作与明文无关，使其抗明文攻击能力不佳。

3 结语

为了提高加密算法的抗明文攻击能力，并有效降低混沌周期性的干扰，文中提出了基于无序分割投影策略与重力模型的图像加密算法。通过对输入明文进行无序分割，并计算每个子块的位置坐标；再根据明文像素量，计算 Kent 映射的初值，通过迭代 Kent 映射，获取随机序列组；利用该随机数组，定义位置置乱机制，改变重叠子块的位置；再利用分割投影策略，提取其对应的投影线，对 2 个非重叠子块内的像素进行混淆，再对其重组，输出置乱密文；最后，利用改进了重力模型，对置乱密文完成像素加密。实验结果显示：与当前基于混沌理论的图像加密技术相比，文中算法的安全性更高，具有更强的抗明文攻击与剪切攻击性能。

参考文献：

[1] LIANG Ya-ru, LIU Guo-ping, ZHOU Nan-run. Image Encryption Combining Multiple Generating Sequences Controlled Fractional DCT with Dependent Scrambling and Diffusion[J]. Journal of Modern Optics, 2015, 62(4): 251—264.

[2] LOKESHWARI G, SUSARLA S, KUMAR S U. A Modified Technique for Reliable Image Encryption Method Using Merkle-Hellman Cryptosystem and Rsa Algorithm[J]. Journal of Discrete Mathematical Sciences and Cryptography, 2015, 18(3): 293—300.

[3] 海洁, 杜海龙, 邓小鸿. 基于快速混沌置乱的鲁棒型医学图像加密算法[J]. 计算机应用, 2015, 35(2): 430—434.
HAI Jie, DU Hai-long, DENG Xiao-hong. Robust Medical Image Encryption Algorithm Based on Fast Chaotic Scrambling[J]. application, 2015, 35(2): 430—434.

[4] XU Lu, LI Zhi, LI Jian. A Novel Bit-Level Image Encryption Algorithm Based on Chaotic Maps[J]. Optics and Lasers in Engineering, 2016, 78(12): 102—109.

[5] 柴秀丽, 甘志华. 基于超混沌系统的位级自适应彩色图像加密新算法[J]. 计算机科学, 2016, 43(4): 134—139.
CHAI Xiu-li, GAN Zhi-hua. A Novel Bit Level Adaptive Color Image Encryption Algorithm Based on Hyper Chaotic System[J]. Computer Science, 2016, 43(4): 134—139.

[6] 贾嫣, 张萍, 陈蕾. 基于改进混沌映射的图像加密算法[J]. 计算机工程与设计, 2015, 33(5): 1187—1191.
JIA Yan, ZHANG Ping, CHEN Lei. Image Encryption Algorithm Based on Improved Chaotic Map[J]. Computer Engineering and Design, 2015, 33 (5): 1187—1191.

[7] WANG Xing-yuan, ZHAO Yuan-yuan, ZHANG Hui-li. A Novel Color Image Encryption Scheme Using Alternate Chaotic Mapping Structure[J]. Optics and Lasers in Engineering, 2015, 82(7): 79—86.

[8] 刘建军, 石定元, 武国宁. 基于 Kent 映射的混合混沌优化算法[J]. 计算机工程与设计, 2015, 33(6): 1498—1503.
LIU Jian-jun, SHI Ding-yuan, WU Guo-ning. Hybrid Chaos Optimization Algorithm Based on Kent mapping[J]. Computer Engineering and Design, 2015, 33(6): 1498—1503.

[9] 王飞. 基于随机投影分割和中国剩余定理的图像加密算法[D]. 广西: 广西师范大学, 2015.
WANG Fei. Image Encryption Algorithm Based on Random Projection Segmentation and Chinese Remainder Theorem[D]. Guangxi: Guangxi Normal University, 2015.

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

[11] 赵建峰, 王淑英, 李险峰, 等. 基于假分数阶激光混沌的数字图像加密研究[J]. 四川大学学报(自然科学版), 2016, 53(1): 79—86.
ZHAO Jian-feng, WANG Shu-ying, LI Xian-feng, et al. Research on Encryption of Digital Image Based on Improper Fractional-Order Laser Chaos[J]. Journal of Sichuan University(Natural Science Edition), 2016, 53(1): 79—86.

[12] 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.
XIE Guo-bo, DING Yu-ming. The Variable Logistic Map Image Scrambling Encryption Algorithm[J]. Parameter Based on Microelectronics and Computer, 2015, 12(4): 111—115.

[13] LIU Ling-feng, MIAO Suo-xia. A New Image Encryption Algorithm Based on Logistic Chaotic Map with Varying Parameter[J]. Springer Plus, 2016, 5(1): 1—12.

[14] HUSSAIN I, SHAH T. A Novel Image Encryption Algorithm Based on Chaotic Maps and GF Exponent Transformation[J]. Nonlinear Dynamics, 2013, 72(1): 399—406.

[15] WANG Xing-yuan, GUO Kang. A New Image Alternate Encryption Algorithm Based on Chaotic Map[J]. Nonlinear Dynamics, 2014, 76(4): 1943—1950.

[16] 郭毅, 邵利平, 杨璐. 基于约瑟夫和 Henon 映射的比特位图像加密算法[J]. 计算机应用研究, 2015, 32(4): 1131—1137.
GUO Yi, SHAO Li-ping, YANG Lu. A Bit Image Encryption Algorithm Based on Joseph and Henon Mapping[J]. Computer Application Research, 2015, 32(4): 1131—1137.