

# 改进的引力模型耦合明文像素相关交叉机制的图像加密算法

郭静博，孙琼琼  
(平顶山教育学院，平顶山 467000)

**摘要：**目的 解决当前图像加密技术严重依赖混沌系统，使其通用性较差，难以直接加密非方形图像，且因混沌系统的周期性，算法的安全性不足的问题。**方法** 提出了改进的引力模型耦合明文像素相关交叉算子的图像加密算法。首先，利用多个一维混沌映射，定义联合混沌变换模型，输出密钥流；随后，基于明文像素位置，设计像素相关交叉机制，联合密钥流，对明文进行高效置乱；构造质量动态变化函数，用其替代传统引力模型中的恒定粒子质量，增强算法的敏感性，并用改进的引力模型对置乱图像完成扩散，彻底改变像素值；最后，构建密文增强模型，对输出密文进行二次扩散，扩大密文的 NPCR(Number of pixel change rate)与 UACI(Unified average changed intensity)值。**结果** 实验结果表明：与当前图像加密机制相比，所提加密算法不但可以扩散方形图像，而且能够对非方形目标直接加密，具有更高的通用性与安全性，以及更强的抗差分攻击能力。**结论** 所提出的算法能够加密非方形尺寸的图像，具有较强的通用性与安全性。

**关键词：**图像加密；引力模型；像素相关交叉机制；联合混沌变换模型；密文增强；质量动态变化函数  
**中图分类号：**TS853<sup>+</sup>.6   **文献标识码：**A   **文章编号：**1001-3563(2016)13-0165-08

## Image Encryption Algorithm Based on Improved Gravity Model Coupled with Plain Pixel Correlation Crossing Mechanism

GUO Jing-bo, SUN Qiong-qiong  
(Pingdingshan Institute of Education, Pingdingshan 467000, China )

**ABSTRACT:** In order to solve the problems such as bad versatility of image encryption and difficulty in directly encrypting non-square images which were caused by severe dependence on chaotic system, and also insufficient algorithm security because of the periodicity of the chaotic system, an improved encryption algorithm was put forward based on improved gravity model coupled with plain pixel correlation crossing mechanism. Firstly, this algorithm defined the combined chaotic transformation model by multiple 1D chaotic maps and output the key stream; and then, it designed pixel correlation crossing operator based on the location of plain pixels, and efficiently scrambled the plain image by combining the key stream; built dynamic variation function of mass to substitute the constant particle mass in the traditional gravity model and increase the sensitivity of the algorithm; and then diffused the permutation image with the improved gravity model to completely change the pixel value; finally it built an enhanced model to have secondary diffusion for the output cryptograph and increase its NPCR (number of pixels change rate) and UACI (unified averaged changed intensity). Compared with the current image encryption algorithm, the proposal could not only diffuse square images but also directly encrypt non-square objects, and it had higher versatility and security and stronger ability to resist differential attacks. The algorithm proposed can encrypt non-square images and have better versatility and security.

**KEY WORDS:** image encryption; gravity model; pixel correlation intersection mechanism; combined chaotic transformation model; cipher enhancement; dynamic variation function of mass

收稿日期：2015-12-25

基金项目：河南省科技计划重点项目（102102210416）

作者简介：郭静博（1982—），女，河南平顶山人，硕士，平顶山学院讲师，主要研究方向为图像处理、信息安全。

图像作为当今信息交流的重要介质之一,其含有丰富的内容信息,是人们日常信息交流中最为直观的载体,带给各领域、各国人们极大的生活便利<sup>[1-2]</sup>。然而,因为图像在开放的网络条件下发送,易遇到各种外来攻击,导致图像信息外泄,造成巨大隐患与经济损失<sup>[3]</sup>,因此,对图像进行加密保护,防止信息被窃取,就显得非常重要<sup>[4-5]</sup>。近年来,随着混沌系统理论的日益完善,为图像加密提供了一种新的有效保护手段,如Yong Zhang等人<sup>[6]</sup>为了保护彩色图像安全传输,提出了基于Choquet模糊积分和超混沌Lorenz系统的彩图加密算法,提高算法的抗明文攻击与暴力攻击能力,实验结果验证了其算法的有效性。Zhang等人<sup>[7]</sup>为了提高加密算法的安全性,设计了基于整体扰乱与双向扩散的数字图像加密技术,利用混沌系统生成混度序列,对明文完成置乱,并设计了双向扩散机制,对置乱图像完成正反方向的像素扩散,仿真数据显示其算法拥有较高的安全性。姜晓洁等人<sup>[8]</sup>为了扩大普通混沌系统加密算法的密钥空间,设计了超混沌系统的光学图像加密算法,采用Logistic混沌序列对光学图像像素位置矩阵进行置乱操作,然后采用超混沌Chen系统对置乱后像素的灰度值进行扩散处理,并对其算法进行了实验验证。

然而,基于混沌系统的加密技术严重依赖混沌系统参数,当明文发生微小变化时,不能有效影响其置乱过程,缺乏大尺度传播效应,无法直接加密非方形图像,使其通用性较差,且因混沌系统的周期性,其算法安全性仍有待提高。为此,文中提出了改进的引力模型耦合明文像素相关交叉算子的图像加密算法,介绍了其设计原理,并测试了算法的安全性。

## 1 文中加密算法设计

提出的改进的引力模型耦合明文像素相关交叉算子的图像加密算法,是依赖密文像素来完成像素置乱与扩散的,降低了其对混沌参数的依赖程度,其加密过程见图1。由图1可知,该算法包含4个部分:联合混沌变换模型的定义,输出伪随机特性较强的密钥流;基于明文像素位置的像素相关交叉机制的设计,对明文进行高效率置乱,显著提高像素位置的像素置乱率;通过引入自适应引力系数,改进了引力模型,完成像素的扩散;密文增强模型的构建,增大密文的NPCR与UACI值,提高算法的抗差分攻击能力。

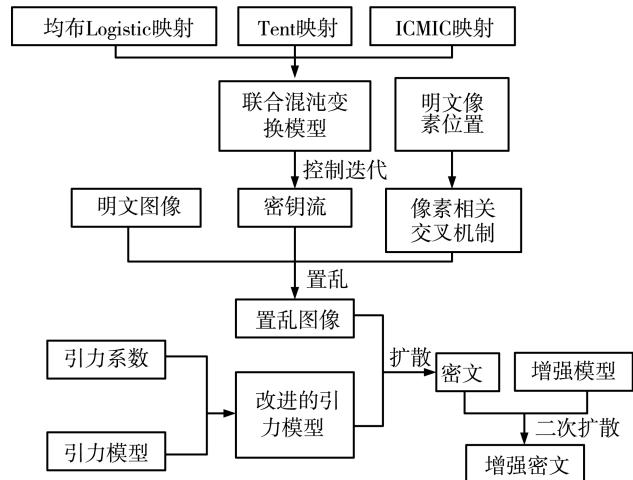


图1 改进加密算法的流程  
Fig.1 Improved encryption algorithm flow diagram

### 1.1 联合混沌变换模型

若初始明文大小为  $M \times N$ ,为了提高算法的敏感性,耦合多个简单一维(1D: one Dimension)混沌映射,设计联合混沌变换模型,见图2。所设计的联合混沌变换模型是依据一致分布Logistic系统迭代值来确定最终的密钥流输出,通过迭代值,确定密钥流的生成器,使得最终的密钥流为混合序列,使其具备较高的伪随机特性。

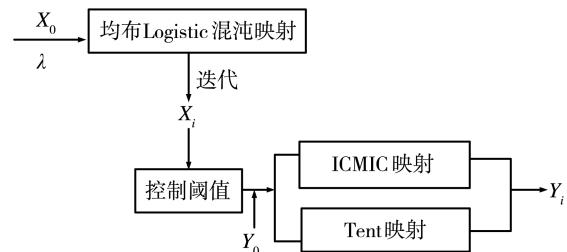


图2 联合混沌变换模型  
Fig.2 Combined chaotic transformation model

依据图2所示,通过迭代一致分布Logistic系统,将其输出值与其他2个1D映射的触发阈值进行比较,继而形成了联合混沌变换模:

$$Y_{i+1} = \begin{cases} I(Y_i) & X_i \geq 1 \\ T(Y_i) & 0.5 < X_i < 1 \end{cases} \quad (1)$$

其中: $Y_{i+1}$ 代表所提联合混沌变换模的输出值; $T(\cdot)$ 代表Tent映射; $I(\cdot)$ 代表ICMC映射。

$$X_{k+1} = \frac{4\lambda^2 X_k (1 - X_k)}{1 + (4\lambda^2 - 1) X_k (1 - X_k)} \quad (2)$$

$$T(L_i) = \begin{cases} \beta L_i & L_i < 0.5 \\ \beta(1 - L_i) & 0.5 \leq L_i < 1 \end{cases} \quad (3)$$

$$I(X_i) = \sin\left(\frac{a}{X_i}\right), a \in [0, \infty] \quad (4)$$

其中： $X_{i+1}$ ， $X_i$  分别是模型(2)的第( $i+1$ )和 $i$ 个迭代值； $L_i$  是 Tent 映射的变量参数； $I(\cdot)$  是 ICMC 映射[9]； $T(\cdot)$  是 Tent 映射； $i=1, 2, \dots, M \times N$ ，为迭代数量； $\lambda$  为控制参数，当  $-4 \leq \lambda \leq 4$  时，Logistic 系统是混沌的； $\gamma \in [0, 2]$ ，为控制参数； $X_i \in [0, 1]$ ，为系统变量。

依据图 1 可知，变换模型是耦合了 3 个一维简单混沌映射，故该变换模型仍然属于一维系统，因此，对于模型(2)的迭代输出值  $X_i$ ，变换模型可在 Tent, ICMC 映射之间交叉迭代，继而输出混合密钥流。其控制机制为：若  $\lambda \in [0, 2]$ ，且  $0 \leq X_i < 1$ ，则该变换模型的输出密钥流由 Tent 映射控制；如果  $\lambda \in [2, 3]$ ，且  $X_i \geq 1$ ，则该变换模型的输出密钥流由 ICMC 映射控制；如果  $\lambda \in [3, 4]$ ，且  $0 \leq X_i < 1$ ，则该变换模型的输出密钥流由 Tent 与 ICMC 映射共同控制。

通过模型(1)–(4)，最终输出密钥流  $S_C(R)$ 。

设置  $X_0 (X_0 = 0.6)$  和  $Y_0 = 0.25$ ，迭代模型(1)与其他 3 个 1D 映射，以验证本模型输出的密钥流的随机特性，故用测试信息熵[10]  $H(m)$  来衡量这些混沌映射的混沌行为：

$$H(m) = \sum_{i=0}^{L-1} p(m_i) \log_2 [p(m_i)] \quad (5)$$

式中： $L$  为图像灰度级别； $p(m_i)$  代表像素  $m_i$  出现的几率。

随后，依据文献[10]提供的技术，测试模型 1–4 所迭代输出混沌序列的熵值，数据见表 1。从表 1 可知，文中联合混沌变换模型具备更强的混沌轨迹，其输出序列的  $H(m)$  值，始终大于其他 3 个系统的序列熵值。

表 1  $H(m)$  测试结果 ( $L=256$ )

Tab.1  $H(m)$  test results

控制参数			模型 1	模型 2	模型 3	模型 4
$\lambda$	$\beta$	a				
3.1	1.1	1.5	7.5381	7.4713	6.9571	6.7815
3.3	1.4	2	7.6022	7.5702	7.2780	6.9679
3.5	1.7	3.5	7.7319	7.6134	7.3936	7.4728
3.7	1.9	4	7.8933	7.6927	7.5804	7.5187
4	2	4.2	7.9216	7.8406	7.6671	7.5594

## 1.2 基于明文像素相关交叉机制的置乱

为了避免传统置乱策略需要经过多轮扰乱像素位置方可提高其安全度，通过迭代联合混沌变换模型，输出密钥流，再基于明文像素位置，设计像素相关交叉机制，完成对明文的高效置乱。将尺寸为  $M \times N$  的明文以及置乱后的密文，按照从左到右、从上到下的顺序，转化为一维数组，则其像素可分别表示为： $P = \{P(0), P(1), \dots, P(M \times N - 1)\}$ ， $C = \{C(0), C(1), \dots, C(M \times N - 1)\}$ 。令  $R$  代表当前像素位置， $R'$  为交叉像素位置，则  $R'$  的计算模型为：

$$R' = R + [S_C(R) + C(R-1)] \bmod (M \times N - R) \quad (6)$$

其中： $S_C(R)$  代表联合混沌变换模型的输出密钥； $C(R-1)$  代表前一个混淆像素的灰度值。

依据模型(6)，设计像素交叉机制：

$$\begin{aligned} C(R) &= P(R') = \\ &P(R + (S_C(R) + C(R-1)) \bmod (M \times N - R)) \end{aligned} \quad (7)$$

$$P(R') = P(R) \quad (8)$$

为了清晰阐述所设计的基于明文像素相关交叉机制，从明文图像中随机选取 9 个像素，分别见图 3 与图 4。假设像素 A 前面的像素都是被混淆的，

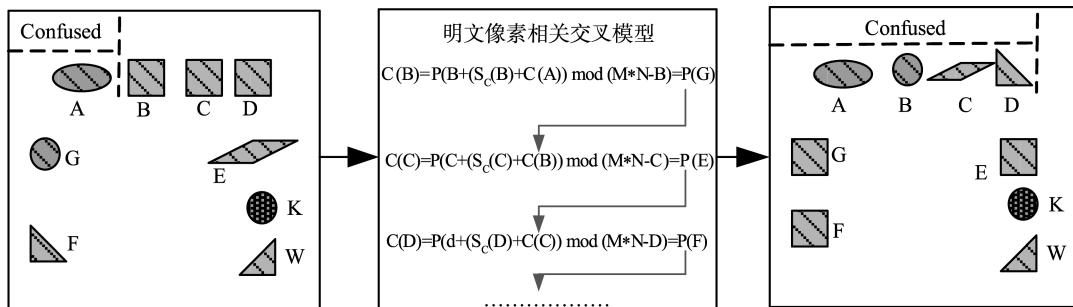


图 3 明文像素交叉机制  
Fig.3 Plain pixel crosses mechanism

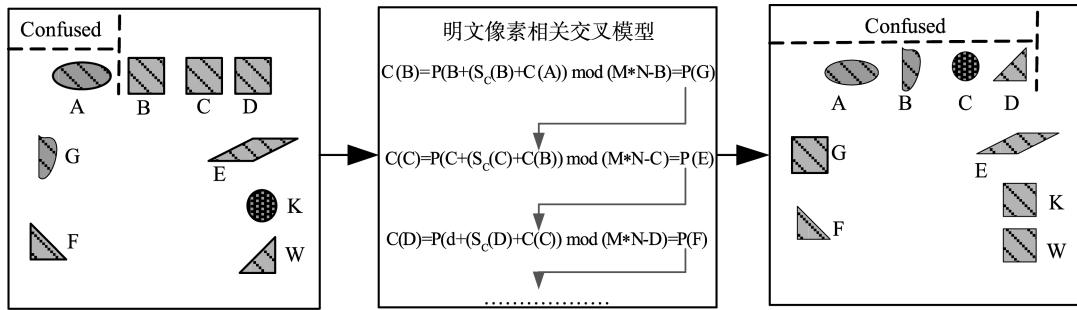


图4 改变像素G的明文像素交叉机制  
Fig.4 Plain pixel cross mechanism with improved pixel

G即像素B,C,D是需要交叉置乱的目标,见图3;而像素E,F,G则是根据模型(6)和(7),利用像素B,C,D来互换其位置。假设2个明文图像中像素G存在轻微差异,其灰度值分别为 $P(G),P(G')$ ,依据模型(5)可知,这种差异会影响像素C的交叉。如图4所示,像素 $P(C)$ 被交叉成 $P(W)$ ,其他像素的交叉处理以此类推。通过将这种差异对图像剩下的像素进行扩散,从而形成一幅与明文彻底不同的图像,其像素被高度置乱。

为了量化明文像素相关交叉机制的置乱度,将文献[11]视为对照组,利用置乱度[11]作为评估指标,以衡量算法的置乱性能:

$$Q = \frac{\|R'_{M \times N}\| - \|R_{M \times N}\|}{M \times N - \|R_{M \times N}\|} \quad (9)$$

首先,以图5a为例,利用明文像素相关交叉机制与文献[11]的置乱技术对其完成混淆,输出密文见图5b,c,e,f,并依据文献[11]的方法,测量了2种算法的置乱性能,见图5g。从人眼视觉上看,2种置乱技术都具备较强的通用性与混淆性能,对于不同尺寸的图像,都可彻底混淆像素位置,然而,从图5g可知,文中算法的置乱度与效率要略高于文献[11]。

### 1.3 基于改进的引力模型的像素扩散

若明文图像 $I=\{0 \leq f(i,j) \leq 256; i=1,2,\dots,M, j=1,\dots,N\}$ 的尺寸 $M \times N$ ,将其所有像素视为空间内同一平面内的粒子,若任意像素的质量 $m_{ij}$ 不为0,且有一个粒子E在空间的另外一个平面。则粒子E与像素存在引力,故可利用引力来改变图像像素值。文献[12]验证了利用引力模型来完成像素扩散,具有良好的保密性能:

$$B'_{ij} = \left[ \frac{G \times m(x,y,z) \times m_{ij}(i,j)}{(x-i)^2 + (y-j)^2 + z^2} \right] \bmod 256 \oplus B_{ij} \quad (10)$$

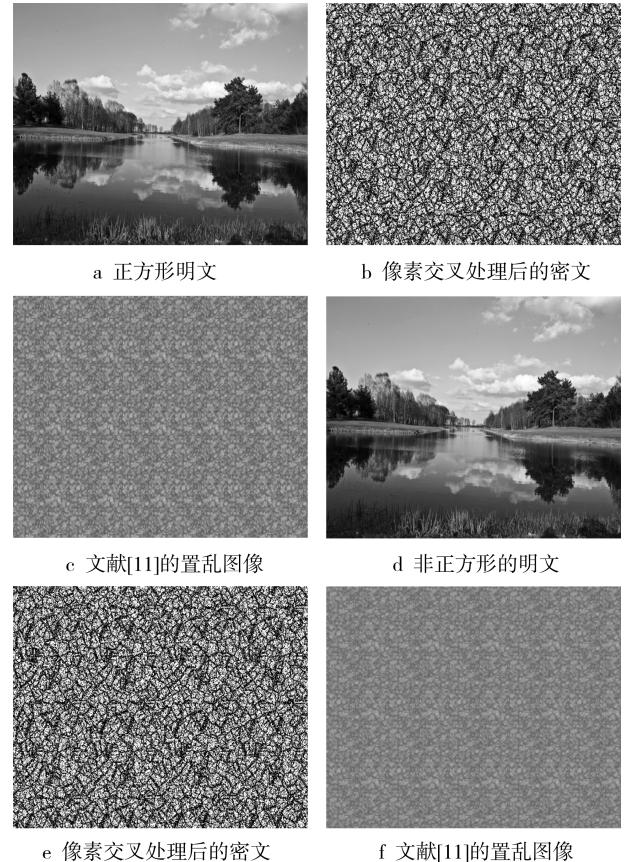


图5 2种算法的置乱性能  
Fig.5 Permutation performance of two algorithms

$$\begin{aligned} m(x, y, z) &= 1 \\ m(i, j) &= 21i^2 + j^3 + 5 \end{aligned} \quad (11)$$

其中:  $G$  代表自适应引力系数;  $m(x, y, z)$  代表粒子  $E$  的质量;  $(x, y, z)$  代表粒子  $E$  的坐标;  $m(i, j)$  为像素质量;  $B_{ij}$  为置乱像素值;  $B'_{ij}$  是式(10)加密后的密文像素值。为了确保式(10)分母不为 0, 规定  $z \neq 0$ 。

然而, 式(10)是将  $m(x, y, z)$  视为恒定值, 取其值为 1, 使其算法的密钥敏感性不佳; 故构造质量动态变化函数, 用其替代传统引力模型中的恒定粒子质量, 对其进行改进:

$$B'_{ij} = \left[ \frac{G \times m_0(x, y, z) \times m_{ij}(i, j)}{(x-i)^2 + (y-j)^2 + z^2} \right] \bmod 256 \oplus B_{ij} \quad (12)$$

$$m(x, y, z) = 1500 \times \bmod[(11 \times x^2 + y^3), 256] \quad (13)$$

所提算法就是利用式(12)完成置乱图像的加密。为了展示改进的引力模型的加密性能, 将文献[12]视为对照组, 以图 6a 为测试目标, 依据文献[12]的实验思路, 设置  $x=150$ ,  $y=300$ ,  $z=150$ ,  $G=3 \times 10^8$ , 利用改进的引力模型与文献[12]的引力模型对其完成加密, 结果见图 6b, c, 从图 6 中可知, 通过嵌入质量动态变化函数, 改善了密文的信息隐藏程度, 使其加密质量要优于文献[12]。

#### 1.4 密文增强模型的构建

为了提高密文的抗差分攻击能力, 构建了密文增强模型, 以进一步提高密文的 NPCR 与 UACI 值:

$$\begin{cases} B''_0 = \text{floor}\left(\frac{\text{SUM}}{M \times N}\right) \\ B''_i = B''_{i-1} \oplus B'_i \bmod [x_i \times 10^{10}, 256] \end{cases} \quad (14)$$

其中:  $\text{SUM}$  代表密文像素总量;  $M \times N$  为密文尺寸;  $B''_i$  是增强后的密文像素值;  $B'_i$  为利用改进引力模型扩散后输出密文的像素值。

利用式(14)对图 6b 进行增强, 输出结果见图 6d。为了体现增强模型的优势, 以图 6a 为例, 根据文献[13]所提供的方法, 测量了图 6b 与 d 两密文的 NPCR 与 UACI 值, 分别为 98.26% 与 99.77%, 33.18% 与 33.49%, 可见, 密文增强前后, 其 NPCR 与 UACI 值存在较大差距, 对密文进行深度增强, 可以进一步提升加密算法的安全性能。

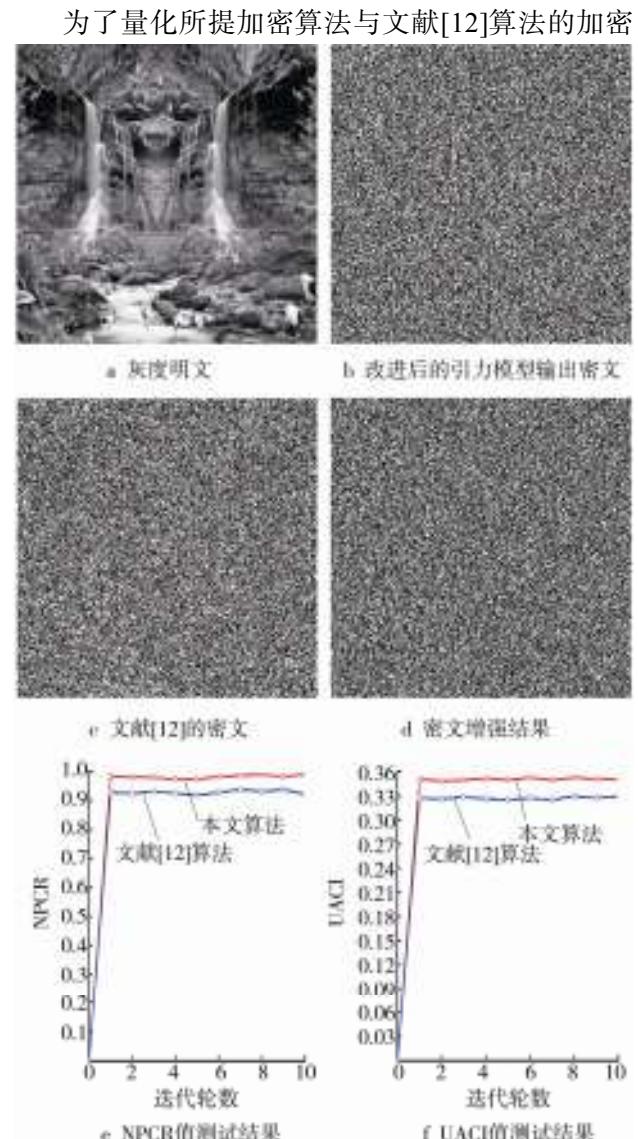


图 6 引力模型改进前后的加密性能及 2 种算法的安全性  
能测试

Fig.6 The encryption performance before and after improvement of gravity model, and security performance test of two algorithms

性能, 利用 NPCR 与 UACI 值来评估 2 种算法的优异, 以图 6c 与图 6d 为目标, 2 种算法的测试结果见图 6e 与图 6f。依图 6 可知, 2 种算法都具有较高的加密效率, 但是本文算法的加密质量要优于文献[12], 其 NPCR 与 UACI 值更高, 见图 6e。原因是本算法利用了明文像素相关交叉机制, 彻底扰乱明文像素, 再通过嵌入质量动态变化函数, 改进了引力模型, 增强了算法的鲁棒性, 并定义了密文增强模型, 对明文实现了二次扩散, 使算法的加密质量更高; 而文献[12]采用的引力模型是固定  $m(x, y, z)$  值, 导致其敏感性较低, 属于简单的一次扩散加密技术, 使算法安全性不佳。

## 2 实验结果与分析

在 Matlab 平台上验证所提加密算法的可靠性。为了反映出所提算法的优势, 将当前加密性能较好的算法视为对照组: 文献[14]与文献[15]。依据式(1) — (4) 的混沌行为, 在各参数变量的取值范围内, 将算法的部分关键变量设置为:  $k=3.8$ ,  $\beta=2$ ,  $a=5$ ,  $X_0=0.5$ 。

### 2.1 加密效果对比分析

首先, 对算法的通用性完成验证, 以方形明文图 7a、矩形明文图 7c 为目标, 利用所提算法对其进行加密, 结果分别见图 7b 与图 7d。依图 7 可知, 算法不但能够对正方形图像进行加密, 而且能对非方形图像完成扩散, 可见算法具备良好的通用性。

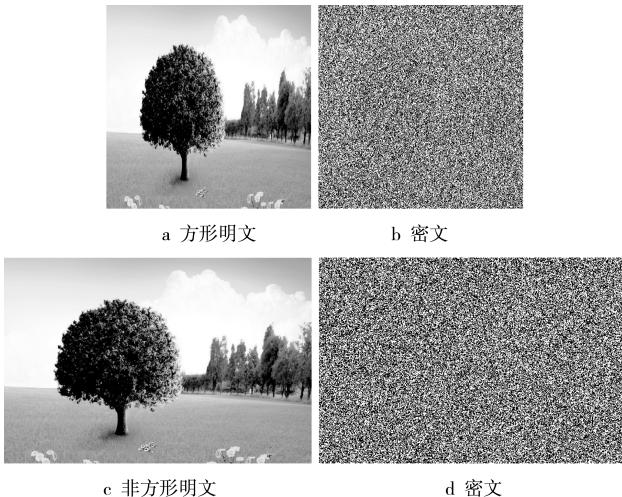


图 7 改进算法的通用性测试  
Fig.7 Versatility test of this algorithm

由于文献[14]与文献[15]都是利用混沌系统, 使其只能对方形图像加密, 为了使得实验具备对比性, 以图 8a 为对象, 利用本文算法与文献[14]、文献[15]对其加密, 结果见图 8b—d。从人眼角度看, 3 种算法确实没有区别, 都具有良好的保密可靠度。为了量化这些算法的差异, 体现所提技术的优势, 利用信息熵<sup>[10]</sup>  $H(m)$  来衡量, 得到 3 种算法的  $H(m)$  值分别为 7.9217 (本算法)、7.8552 (文献[14])、7.8931 (文献[15])。文中算法的密文具备更大的  $H(m)$  值, 均大于其他 2 种技术的  $H(m)$  值。原因是文中算法利用联合混沌变换模型与像素相关交叉机制, 对明文进行高效率乱, 并利用改进的引力模型与增强模型, 对输出密文进行了二次增强, 降低算法对混沌系统的依赖, 以及避免了因混沌系

统的周期性而降低算法安全度; 而文献[14]、文献[15]均是基于混沌系统的加密技术, 对混沌参数依赖程度非常大, 与明文无关, 故其敏感性不佳。

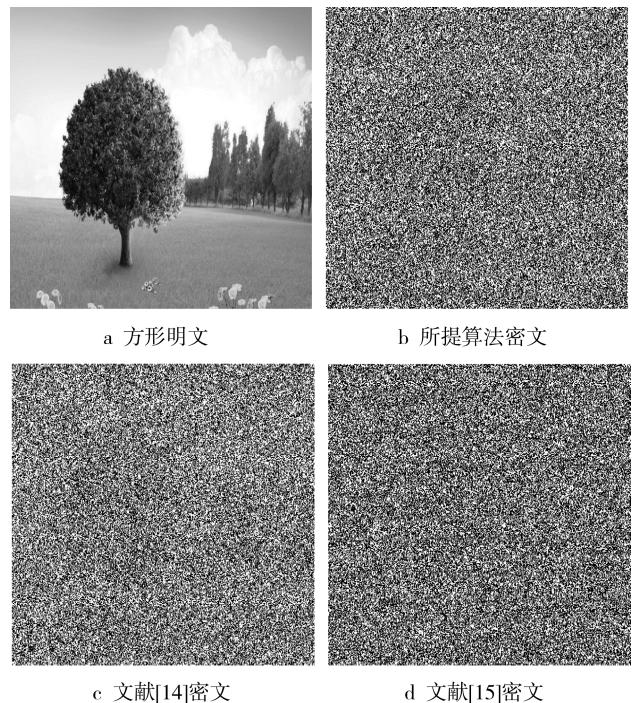


图 8 3 种算法的加密效果  
Fig.8 Encryption effect of the three algorithms

### 2.2 相邻 2 个像素点的相关性分析

若图像相邻像素之间的相关性较强, 容易被攻击者破译, 从而降低了算法的安全性, 因此, 可靠的加密技术需要降低这种相关性, 以确保抵抗统计攻击<sup>[16]</sup>, 故在图 8a 与图 8b 中随机择取 2000 对相邻像素点, 计算其相关系数  $Q_{xy}$ :

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

图 9 是图 8a 与图 8b 中水平方向上的  $Q_{xy}$  测试结果。依图 9a, 图 8a 中的像素呈现对角线形式, 表明其具有较高的相关性,  $Q_{xy}$  达到 0.9602; 经本文技术加密后, 有效降低了像素间的相关性, 从而改善了算法的抗统计攻击能力, 见图 9b,  $Q_{xy}$  约为 0.0018。对角线方向, 图 8a 与图 8b 的  $Q_{xy}$  分别为 0.0979, 0.0041,  $y$  轴方向分别为 0.9215, 0.0026。数据说明, 文中所提加密技术显著降低了相邻像素间的相关系数。

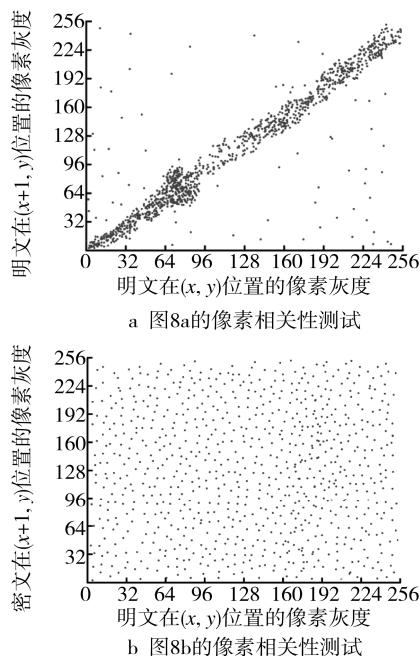


图9 加密前后图像像素之间的相关性测试

Fig.9 Correlation test between image pixels before and after encryption

### 2.3 抗差分攻击性能分析

安全可靠的图像加密技术应该能有效抗击外界攻击,具备较强的抗差分攻击性能<sup>[17]</sup>,而NPCR与UACI是衡量算法该性能的主要依据,故利用NPCR与UACI曲线来评估算法,其计算模型见式(15)–(17)。3种算法的输出密文的NPCR与UACI曲线见图10,从图10可知,文中算法由于构造了

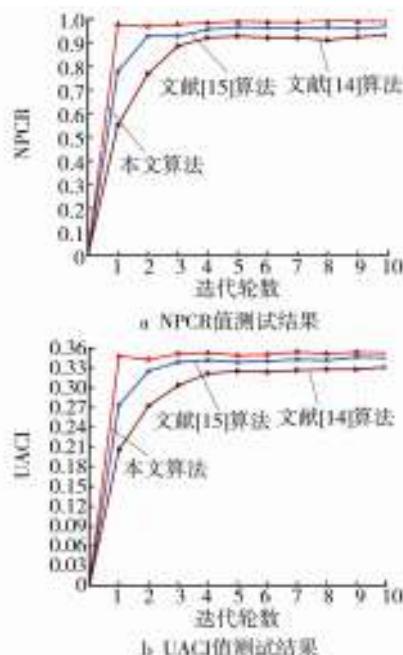


图10 算法抗差分攻击性能测试

Fig.10 Performance test of the algorithm against differential attack

质量动态变化函数,改进了引力模型,从而增强了算法的敏感性,且对初始密文进行了增强处理,使得算法的密文具有更高的NPCR与UACI值;而另2种算法因依赖混沌系统的程度较高,其迭代周期性降低了算法的安全性与敏感性,使其抗差分攻击能力不佳。

### 3 结语

为了改善当前算法的安全性与通用性,设计了改进的引力模型耦合明文像素相关交叉算子的图像加密算法。通过耦合多个1D混沌映射,定义联合混沌变换模型,输出伪随机特性较强的密钥流;并利用明文像素位置,设计像素相关交叉机制,联合密钥流,对明文进行高效置乱,降低算法对混沌系统参数的过度依赖,提高算法的扩散效应;随后利用改进的引力模型对置乱图像完成扩散,最后构建密文增强模型,对输出密文进行二次扩散,扩大密文的NPCR与UACI值。实验结果表明,与当前图像加密机制相比,所提加密算法具有更高的安全性与适应性,能加密非正方形的明文,具有更强的抗差分攻击能力。

### 参考文献:

- [1] ZHU Cong-xu, XU Si-yuan, HU Yu-ping. Breaking a Novel Image Encryption Scheme Based on Brownian Motion and PWLCM Chaotic System[J]. Nonlinear Dynamics, 2015, 79 (2):1511—1518.
- [2] 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.
- [3] MAJID B. A Novel Text and Image Encryption Method Based on Chaos Theory and DNA Computing[J]. Natural Computing, 2013, 12(1):101—107.
- [4] IQTADAR H, TARIQ S, MUHAMMAD A G. A Novel Image Encryption Algorithm Based on Chaotic Maps and GF(28) Exponent Transformation[J]. Nonlinear Dynamics, 2013, 72 (1):399—406.
- [5] 芮坤坤. 基于离散傅里叶变换融合双混沌映射的图像加密算法研究[J]. 计算机应用与软件, 2014, 29(4): 321—324.
- [6] BING Kun-kun. Research on Image Encryption Algorithm Based on Discrete Fu Liye Transform and Fusion of Double Chaotic Maps[J]. Computer Applications and Software, 2014, 29(4):321—324.
- [7] ZHANG Yong. Comments on Color Image Encryption Using Choquet Fuzzy Integral and Hyper Chaotic Sys-

- tem[J]. Optik-International Journal for Light and Electron Optics, 2014, 125(19):5560—5565.
- [7] ZHANG Xuan-ping, ZHAO Zhong-meng. Chaos-based Image Encryption with Total Shuffling and Bidirectional Diffusion[J]. Nonlinear Dynamics, 2014, 75(1-2): 319—330.
- [8] 姜晓洁, 谢永超. 基于超混沌系统的光学图像加密算法[J]. 激光杂志, 2015, 36(6):68—71.
- JIANG Xiao-jie, XIE Yong-chao. Optical image Encryption Algorithm Based on Hyper Chaotic System[J]. Laser Journal, 2015, 36(6):68—71.
- [9] 赵欣. 不同一维混沌映射的优化性能比较研究[J]. 计算机应用研究, 2012, 29(3):913—916.
- ZHAO Xin. A Comparative Study on the Optimal Performance of Different One-dimensional Chaotic Maps[J]. Computer Application Research, 2012, 29(3): 913—916.
- [10] ZHEN W, HUANG X, LI Y X, et al. A Novel Image Encryption Algorithm Based on the Fractional-Order Hyperchaotic Lorenz System[J]. Chinese Physics B, 2013, 22(1):010504-1-010504-7.
- [11] 吴丽. 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.
- WU Li. Research on Image Encryption Algorithm Based on 3D Chaotic Map[J]. Video Technology, 2014, 38(19):51—56.
- [12] 孙玉峰, 陈建华. 一种基于万有引力模型的图像置乱新方法[J]. 福州大学学报, 2006, 34(1):48—50.
- SUN Yu-feng, CHEN Jian-hua. A New Image Scrambling Method Based on Universal Gravitation Model[J]. Journal of Fuzhou University, 2006, 34(1):48—50.
- [13] HUANG Xiao-ling. Image Encryption Algorithm UsinG Chaotic Chebyshev Generator[J]. Nonlinear Dynamics, 2012, 67 (4):2411—2417.
- [14] 朱从旭, 胡玉平, 孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报, 2012, 4(7):1735—1743.
- ZHU Cong-xu, HU Yu-ping, SUN Ke-hui. New Image Encryption Algorithm Based on Hyper Chaotic System and Cipher Text[J]. Journal of Electronics and Information, 2012, 4(7):1735—1743.
- [15] YE Guo-dong. A Block Image Encryption Algorithm Based on Wave Transmission and Chaotic Systems[J]. Nonlinear Dynamics, 2014, 75(3):417—427.
- [16] ZHU He-gui, ZHAO Cheng, ZHANG Xiang-de. A Novel Image Encryption-compression Scheme Using Hyper-chaos and Chinese Remainder Theorem[J]. Signal Processing: Image Communication, 2013, 28(6): 670—680.
- [17] RASUL E, ABDUL H A. Chaos-based Image Encryption Using a Hybrid Genetic Algorithm and a DNA Sequence[J]. Optics and Lasers in Engineering, 2013, 56(4):83—93.