

基于混沌系统与多方向扩散的图像加密算法

王瑶¹, 徐洋²

(1.重庆城市职业学院, 重庆 402160; 2.贵州师范大学, 贵阳 550001)

摘要: **目的** 为了避免只从单一方向来扩散图像像素, 并提高加密密文的安全性, 设计了混沌系统与多方向连续扩散的图像加密算法。**方法** 综合 Tent, sine 映射, 联合改进的 Logistic 映射, 设计混合混沌机制, 将 Logistic 模型的输出值作为触发器, 获取一组随机性较强的混沌序列, 对初始明文进行交叉置乱, 高度混淆其像素位置, 有效降低置乱周期性; 构建量化机制对混沌序列进行处理, 获取密钥流, 从而设计多方向连续扩散机制, 从 4 个不同的方向, 利用不同的扩散模型来改变像素值, 显著降低扩散周期性。**结果** 实验结果显示, 与当前混沌加密机制相比, 所提算法具有更高的安全性与敏感性。**结论** 所提加密算法能够确保图像在网络中安全传输, 在包装信息防伪等领域具有较好的应用价值。

关键词: 图像加密; 混沌系统; Logistic 映射; 量化机制; 多方向连续扩散; 混沌序列

中图分类号: TP391 **文献标识码:** A **文章编号:** 1001-3563(2017)23-0217-06

Image Encryption Algorithm Based on Chaotic System and Multi-direction Diffusion

WANG Yao¹, XU Yang²

(1.Chongqing City Vocational College, Chongqing 402160, China;

2.Guizhou Normal University, Guiyang 550001, China)

ABSTRACT: The work aims to design an image encryption algorithm based on chaotic system and multi-direction continuous diffusion for the purpose of preventing the diffusion of image pixel in a single direction and improving the security of encrypted cipher. Firstly, with the output value of Logistic model as the trigger, the mixed chaotic mechanism was designed in combination with Tent map, Sine map and improved Logistic mapping to obtain a set of chaotic sequences with strong randomness for scrambling the initial plaintext to highly confuse the pixel position and effectively reduce the scrambling periodicity. Then, the quantization mechanism was constructed to deal with chaotic sequences for obtaining the key-stream; and the multi-direction continuous diffusion mechanism was designed to change the pixel values from 4 different directions with different diffusion models, thus reducing the diffusion periodicity remarkably. The experimental results showed that the proposed algorithm had higher security and sensitivity compared with the current chaotic encryption mechanism. The proposed encryption algorithm can ensure the secure transmission of images in the network, and has better application value in packaging information anti-counterfeiting and other fields.

KEY WORDS: image encryption; chaotic system; Logistic mapping; quantization mechanism; multi-direction continuous diffusion; chaotic sequence

随着多媒体技术与计算机科学的不断发展与完善, 图像作为人们常用表达信息的重要介质, 在数字交流和网络中具有重要意义^[1]。因图像或视频所包含的信息非常多, 涉及到私人秘密、国家机密等, 加上当前免费开放的网络环境, 对图像信息进行保密性带来了严重的挑战^[2], 因此, 如何防止图像内容在开放网络中进行存储和传输期间受到外来攻击具有重要

意义^[3]。虽然过去一段时间, 有学者提出采用数据加密技术来提高图像的抗攻击能力, 如 DES 与 RSA 等方法, 但是, 这些数据加密方案都忽略图像的大数据容量与高冗余度等性质, 导致其难以用于数字图像加密^[4]。对此, 学者们开始设计相应的数字图像加密技术, 当前较为主流的手段是利用混沌理论的复杂相空间与混沌轨迹来实施图像加密, 大都采用了置乱-扩

收稿日期: 2017-06-12

基金项目: 国家重点基础研究发展计划 (2014CB340600); 国家自然科学基金 (61332019); 贵州省科技合作计划 (黔科合 LH 字[2015]7763 号)

作者简介: 王瑶 (1979—), 女, 硕士, 重庆城市职业学院讲师, 主要研究方向为人工智能、信息安全、图像处理。

散的双重加密结构,如李凯佳等^[5]为了提高加密算法的安全性,融合 DNA 与元胞自动机,设计了一种带有 Hash 认证功能的图像加密技术,利用迭代 Logistic 混沌映射的输出序列来构建位置集合混淆技术,提高明文像素的置乱度,同时,依据混沌序列,建立 DNA 规则,结合改进的元胞自动机,设计像素扩散机制,改变像素值,实验结果验证了其算法的实用性与优异性。Wang 等^[6]为了增强密文的抗攻击能力,设计了基于 DNA 编码与混沌系统的图像加密方案,利用分段线性映射与 Logistic 映射来生成一个密钥图像,再利用 Logistic 映射来设计相应的 DNA 规则,对密钥图像完成编码处理,最后,利用编码后密文来构建 DNA 操作,完成图像的加密,实验结果显示其算法具有理想的安全性与抗明文攻击能力。Liu 等^[7]为了进一步提高加密密文的安全性,使其能够有效抵御网络中的外来攻击,设计了一种基于量子混沌序列的图像加密算法,联合 Logistic 映射、量子映射以及耦合映射格子,设计一种量子复合混沌系统,利用其输出的复合随机序列来置乱像素,同时,根据 Logistic 映射的输出序列来设计一种折叠算法,对置乱密文完成扩散,实验结果验证了其算法具有较高的安全性与密钥敏感性。

虽然基于混沌理论的双重加密算法具有良好的安全性,能够有效保护图像在网络中安全传输,且具有较好的使用价值,但是这些算法都是利用同一个扩散函数、从单一方向来改变像素值,使其加密密文存在明显的周期性,导致其安全性不理想。为此,为了降低这种周期性,文中设计混沌系统与多方向连续扩散的图像加密算法,并测试所提加密算法的安全性与抗攻击能力。

1 设计图像加密算法

所提基于混沌系统与多方向连续扩散的图像加密算法过程见图 1。由图 1 可知,所提算法同样采用了置乱-扩散的加密结构,主要分为 2 个阶段:基于混合混沌系统的明文置乱和基于多方向连续扩散的图像加密。

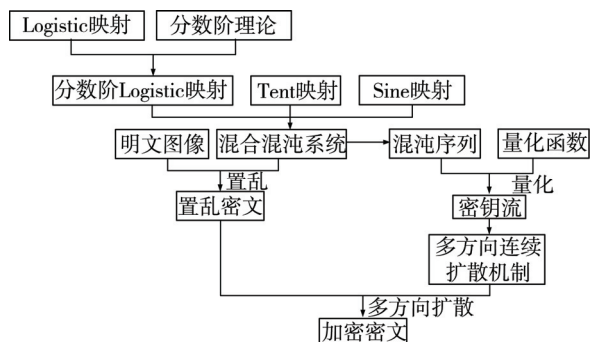


图 1 文中多方向图像加密算法过程

Fig.1 The process of multi-direction image encryption algorithm

1.1 基于混合混沌系统的明文置乱

低维混沌映射具有结构简单、加密效率高的优点,被广泛用于数字图像加密,但是其输出安全性不高^[8]。为此,文中联合 Tent, sine 映射^[9-10],通过将改进的 Logistic 映射作为触发器来构建一个混合混沌系统,兼顾其安全性与加密效率,其过程见图 2。由图 2 可知,Logistic 映射是一个选择参数,根据其来决定随机序列是由 Tent 或 sine 映射来形成。

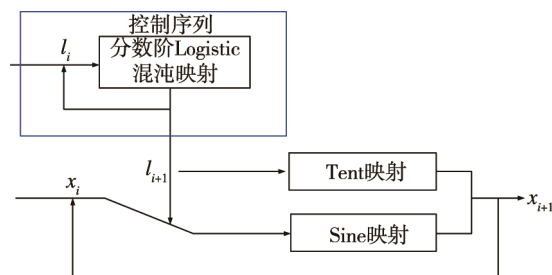


图 2 混合混沌系统

Fig.2 Mixed chaotic system

Tent, sine 映射函数分别为^[9-10]:

$$T(\eta, x_n) = x_{n+1} = \begin{cases} \eta x_n & 0 \leq x_n \leq 0.5 \\ \eta(1 - x_n) & 0.5 < x_n \leq 1 \end{cases} \quad (1)$$

$$Y_{n+1} = a \sin(\pi Y_n) \quad (2)$$

式中: π 、 η 分别为 Tent, sine 以映射; $\eta \in (0, 2]$, $b \in (0, 1]$ 均为混沌参数。

为了改善算法的安全性,文中利用分数阶理论^[11]来改进 Logistic 映射^[3]。传统的 Logistic 映射为^[3]:

$$L(\lambda, x_n) x_{n+1} = \lambda x_n (1 - x_n) \quad (3)$$

式中: $\lambda \in (0, 2]$ 为混沌变量; x_n 为系统变量。

再基于分数阶理论^[11],引入 2 个分数阶参数 α, v , 对式 (3) 进行改进:

$$\begin{cases} \Delta_{\alpha}^v x_{n+1} = \lambda x_{(n+v-1)} (1 - x_{(n+v-1)}) \\ x_{\alpha} = x_0 \end{cases} \quad (4)$$

式中: α, v 均为整数。

根据图 2 的设计思想,形成混合混沌系统为:

$$x_{n+1} = \begin{cases} S(x_n) & L_i \geq 0.5 \\ T(x_n) & L_i < 0.5 \end{cases} \quad (5)$$

依据式 (5) 可知,文中混合机制充分融合了 Tent, sine 以及 Logistic 映射。其最终的输出序列是由 Tent, sine 交叉组合形成的:若 $\lambda \in [0, 2]$, $0 \leq L_i < 0.5$, 则式 (5) 的随机序列值由 Tent 映射决定;若 $\lambda \in [2, 3]$, $0 \leq L_i < 0.5$, 则式 (5) 的随机序列值由 sine 映射决定;若 $\lambda \in [3, 4]$ 且 $0 \leq L_i < 1$, 则式 (5) 的随机序列由 Tent, sine 映射共同构成。

如明文尺寸为 $M \times N$, 通过设置好参数 η, b 值, 以及 λ 与 x_0 , 对式 (5) 迭代 $M \times N$ 次, 可获取混合随机序列 $\{x_1, x_2, x_3, \dots, x_{M \times N}\}$ 。再对 $\{x_1, x_2, x_3, \dots, x_{M \times N}\}$ 进行升

序排列, 形成新的序列 $\{y_1, y_2, y_3 \dots y_{M \times N}\}$ 。然后在 $\{x_1, x_2, x_3 \dots x_{M \times N}\}$ 中确定出 $\{y_1, y_2, y_3 \dots y_{M \times N}\}$ 对应序列值的位置, 从而构建了置乱序列 $\{z_1, z_2, z_3 \dots z_{M \times N}\}$:

$$y_i = x_{z_i} \quad (6)$$

随后, 利用置乱序列 $\{z_1, z_2, z_3 \dots z_{M \times N}\}$ 对明文 I 进行混淆, 即可得到置乱图像 I' 。以图 3a 为例, 令 $\eta=0.5$, $b=0.37$, $\lambda=3.5$ 且 $x_0=0.52$, 对式 (5) 完成迭代后, 利用置乱序列对图 3a 实施混淆, 结果见图 3b。依图 3 可知, 明文经过置乱后, 其信息被充分打乱与隐蔽, 无任何信息泄露。

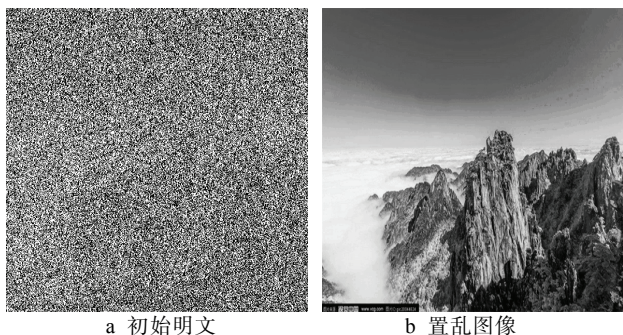


图 3 明文置乱效果

Fig.3 Plaintext scrambling effect

1.2 基于多方向连续扩散的图像加密

由于图像置乱仅改变了像素位置, 其像素值没有任何变动^[1], 因此, 文中设计了多方向连续扩散机制来改变其像素值, 从不同的方向、利用不同的扩散函数来实现加密。首先, 对式 (3) 迭代 $M \times N$ 次, 获取随机序列 $\{x_1, x_2, x_3 \dots x_{M \times N}\}$, 再构造量化机制, 对 $\{x_1, x_2, x_3 \dots x_{M \times N}\}$ 完成量化, 获取一组密钥流 $\{k_i\}$ 。

$$k_i = \text{mod}(\text{floor}(x_n \times 10^{14}), 256) \quad (7)$$

再利用密钥流 $\{k_i\}$, 建立了 4 方向连续扩散机制, 充分改变像素值。具体如下所述。

1) 把大小为 $M \times N$ 的图像 I' 中的所有像素形成一个矩阵 R ; 另外, 把密钥流 $\{k_i\}$ 也变成一个矩阵 Q 。首先, 对 I' 进行上下对折, 形成第 1 个方向, 见图 4a。此时, 其相应的扩散机制为:

$$\begin{cases} T'_h(i, j) = T_h(i, j) \oplus Q_h(i, j) \\ B'_h(N-i+1, j) = B_h(N-i+1, j) \oplus T'_h(i, j) \end{cases} \quad (8)$$

式中: $T_h(i, j)$, $B_h(i, j)$ 为 R 的上、下部分中在 (i, j) 处的像素值; $Q_h(i, j)$ 为 Q 上半部分在 (i, j) 处的密钥流; $T'_h(i, j)$, $B'_h(i, j)$ 为 $T_h(i, j)$, $B_h(i, j)$ 对应的加密像素值。

2) 置乱图像被式 (8) 处理后, 可获取第 1 个方向的加密结果 I'_1 , 再把 I'_1 按照图 4b 所示的过程进行折叠, 其扩散机制为:

$$\begin{cases} T'_r(i, j) = T_r(i, j) \oplus Q_r(i, j) \\ B'_l(j, i) = B_l(j, i) \oplus T'_r(i, j) \end{cases} \quad (9)$$

式中: $T_r(i, j)$, $B_l(i, j)$ 为 I'_1 右上、左下部分在 (i, j) 处的像素值; $Q_r(i, j)$ 为 Q 右上部分在 (i, j) 处的密钥流; $T'_r(i, j)$, $B'_l(i, j)$ 为 $T_r(i, j)$, $B_l(i, j)$ 对应的加密像素值。

3) 密文 I'_1 被式 (9) 处理后, 可获取第 2 个方向的加密结果 I'_2 , 再把 I'_2 按照图 4c 所示的过程进行折叠, 其扩散机制为:

$$\begin{cases} R'_h(i, j) = R_h(i, j) \oplus Q_{rh}(i, j) \\ L'_h(i, N-j+1) = L_h(i, j) \oplus R'_h(i, N-j+1) \end{cases} \quad (10)$$

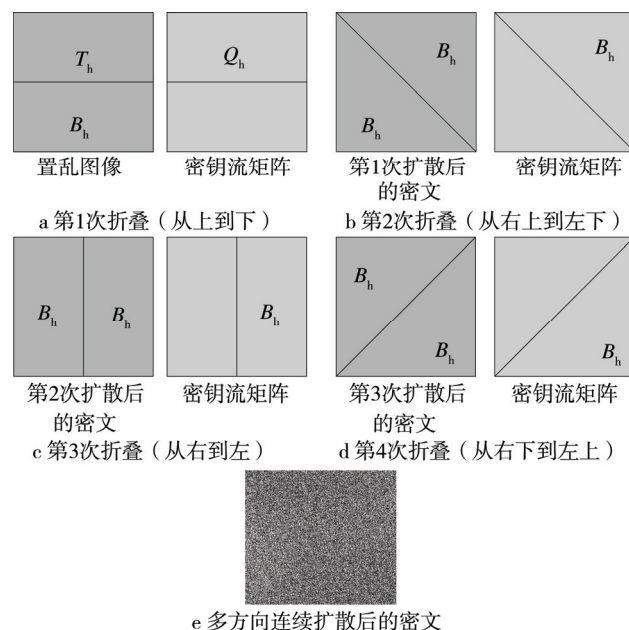
式中: $R_h(i, j)$, $L_h(i, j)$ 为 I'_2 右、左半部分在 (i, j) 处的像素值; $Q_{rh}(i, j)$ 为 Q 右半部分在 (i, j) 处的密钥流; $R'_h(i, j)$, $L'_h(i, j)$ 为 $R_h(i, j)$, $L_h(i, j)$ 对应的加密像素值。

4) 经密文 I'_1 被式 (10) 处理后, 可获取第 2 个方向的加密结果 I'_3 , 再把 I'_3 按照图 4d 所示的过程进行折叠, 其扩散机制为:

$$\begin{cases} R'_b(i, j) = R_b(i, j) \oplus Q_{rb}(i, j) \\ L'_t(i, j) = R_b(i, j) \oplus L_t(i, j) \end{cases} \quad (11)$$

式中: $R_b(i, j)$, $L_t(i, j)$ 为 I'_3 左上、右下部分在 (i, j) 处的像素值; $Q_{rb}(i, j)$ 为 Q 右下半部分中位于 (i, j) 对应的密钥流; $R'_b(i, j)$, $L'_t(i, j)$ 为 $R_b(i, j)$, $L_t(i, j)$ 对应的加密像素值。

置乱图像 I' 被上述 4 个方向加密后, 可获取一个理想的加密结果 I'_4 。将图 3b 视为样本, 根据 6 方向连续扩散机制来对其完成加密, 结果见图 4e。由图 4 可知, 图像经过式 (8—11) 的连续加密后, 所输出的加密结果与置乱密文存在较大差异, 其信息隐秘度被显著提高, 为一幅严重噪声干扰图。



e 多方向连续扩散后的密文

图 4 多方向连续扩散

Fig.4 Multi-direction continuous diffusion

2 实验结果与分析

利用 Matlab 平台来测试所提加密技术的安全性与实用性。同时,为了突出所提加密技术的优越性,将当前安全性较高的技术作为对照组,分别是文献[5]和文献[6]。实验环境为:戴尔 3.5 Hz 双核 CPU,内存为 8 GB;系统为 XP。执行参数为 $\eta=1.52$, $b=2.35$, $\lambda=3.6$ 且 $x_0=0.55$ 。

2.1 加密效果对比测试

将大小为 256×256 的灰度图像视为目标,利用文中算法、文献[5]、文献[6]等 3 种技术对其进行加密,结果见图 5b—d。根据加密效果可知,从视觉上看,3 种技术都有良好的信息隐蔽性能,明文所有的信息均被混淆,攻击者是无法从中获取任何线索。

为了从客观上量化这 3 种技术的差异,文中引入密文熵值^[12]来量化,依据文献[12]的方法,得到图 5b—d 相应的熵值,根据计算数据可知,所提技术的安全性更高,其熵值最大,为 7.9986,与理论值 1^[13]非常靠近。文献[5]、文献[6]这 2 种技术的安全性均要低于所提技术,分别为 7.9852, 7.9974。原因是所提算法融合了 3 个低维混沌映射来输出一个混合序列,显著提高了其随机性,降低其周期性,而且设计了一种多方向连续扩散机制,从 4 个不同方向,以及不同的扩散机制来充分加密图像,消除了扩散周期性,使其密文安全性最高。文献[5]、文献[6]这 2 种技术则是从单一方向来实现像素加密,利用相同的扩散函数来改变像素值,存在显著的周期性,从而降低了二者对应密文的安全性。

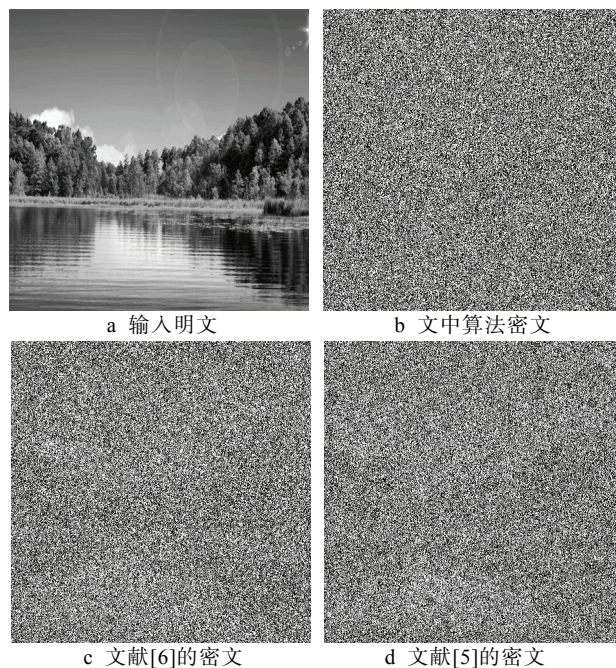


图 5 不同算法的加密效果

Fig.5 Encryption effects of different algorithms

2.2 密钥敏感性测试

密钥敏感性使衡量加密算法安全性的重要指标,当密钥发生微小变化时,攻击者仍然无法获取准确的解密结果^[2]。为了测试所提技术的敏感性,选择密钥 $\lambda=3.6$ (其余密钥不变)进行实验。利用偏差值 $\delta=10^{-14}$ 来篡改密钥 λ ,获取 2 个错误的密钥值 $\lambda_1=3.6+10^{-14}$, $\lambda_2=3.6-10^{-14}$ 。利用这 3 组密钥对图 5b 进行解密,结果见图 6。根据复原结果可知,只有利用正确的密钥

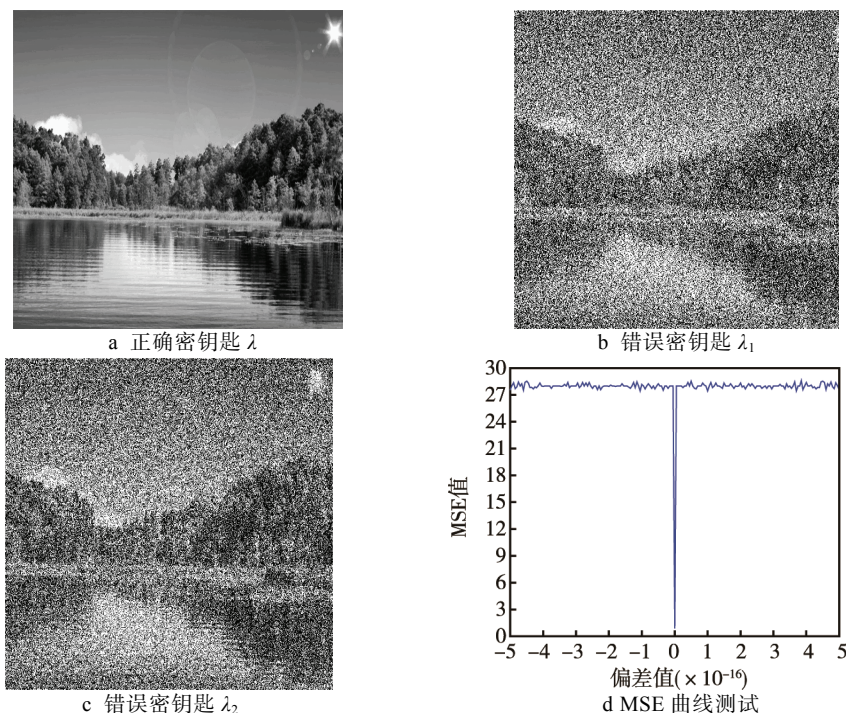


图 6 文中算法的密钥敏感性测试

Fig.6 Key sensitivity test of the proposed algorithm

当 $\lambda=3.6$ 方能对密文完成精确复原, 见图 6a。当密钥发生了 10^{-14} 这样的微小偏差, 攻击者仍然无法得到初始信息, 而且输出 2 个噪声图像见图 6b—c。这显示所提加密技术具备理想的雪崩效应。另外, 根据图 6d 显示的 MSE 曲线可知, 仅当偏差值为 0 时, 其 MSE 值为 0, 哪怕偏差值有一点误差, 其 MSE 都出现巨变。

2.3 相邻像素的相关性测试

图像相邻像素之间的相关性异常强烈, 容易被攻击者利用, 从而破译密文, 对算法的安全性威胁较大^[14], 因此, 文中从图 5b, c 中分别选择 2000 对像素点来测试, 利用相关系数 C_{xy} 来量化这种相关性^[15]:

$$C_{xy} = \frac{\frac{1}{n} \sum_{i=1}^n (x_i - E(x_i))(y_i - E(y_i))}{\sqrt{\left(\frac{1}{n} \sum_{i=1}^n (x_i - E(x_i))^2\right) \left(\frac{1}{n} \sum_{i=1}^n (y_i - E(y_i))^2\right)}} \tag{12}$$

3 种算法对应密文在水平方向上的 C_{xy} 测试结果见图 7。其余方向的 C_{xy} 值见表 1。由图 7 可知, 初始图像的像素分布特别不均, 聚集在一起, 其 C_{xy} 值最大, 为 0.9743, 这显示其像素间的相关性异常强烈, 但是, 经过文中算法、文献[5]、文献[6]等 3 种技术处理后, 像素分布较为均匀。其中, 所提算法的密文像素分布均匀最佳, 无空洞效应, 见图 7b, 其 C_{xy} 值为 0.0019。同时, 根据表 1 可知, 不管是哪个方向, 初始图像的相关性最强, 而所提加密技术大幅降低了这种不利因素。

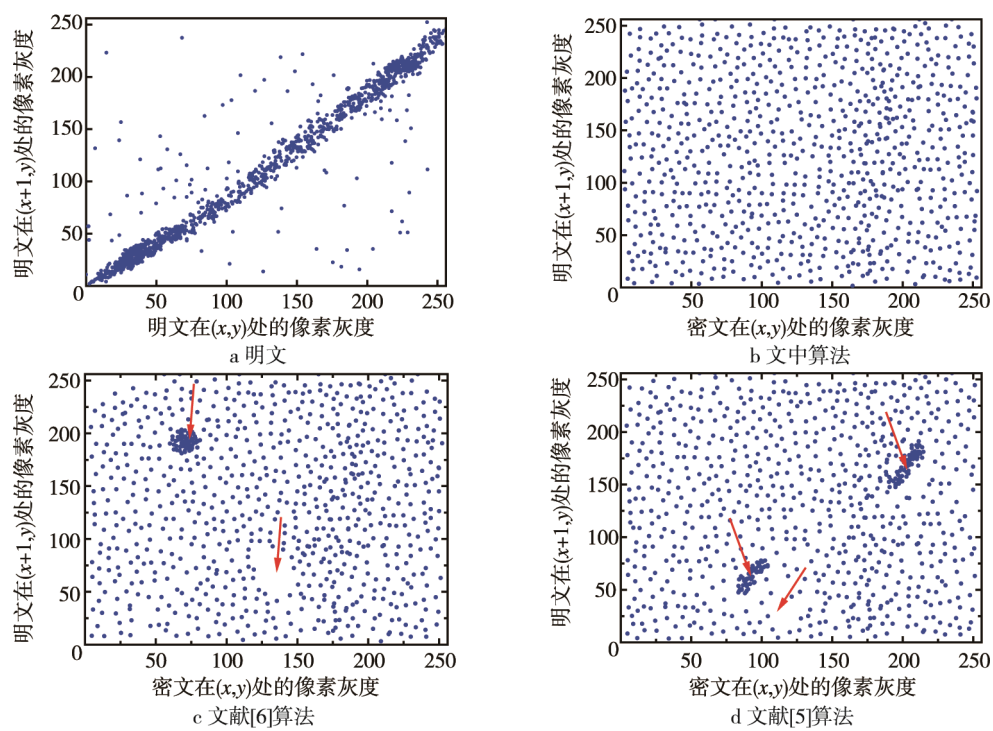


图 7 算法的相关性测试
Fig.7 Correlation test of each algorithm

表 1 不同方向的相关系数测试结果

Tab.1 Test results of correlation coefficients in different directions

选取方向	图5a	图5b	图5c	图5d
水平(x轴)	0.9743	0.0019	0.0034	0.0073
垂直(y轴)	0.9501	0.0031	0.0049	0.0051
对角线	0.9182	0.0004	0.0017	-0.0028

3 结语

为了从多个方向来实现图像加密, 并降低迭代周期性, 设计了混沌系统与多方向连续扩散的图像加密

算法。通过设计混合混沌机制来获取随机性较高的混沌序列, 充分融合了 3 个 1D 混沌映射的优点, 兼顾安全性与效率, 利用量化机制的输出密钥流来构建 4 方向连续扩散机制, 从 4 个不同的方向, 利用不同的扩散模型来改变像素值, 显著提高密文安全性。实验数据验证了所提算法的安全性与优越性, 显示所提技术的输出密文的像素分布更为均匀并且有较强的敏感性。

参考文献:

[1] 李长齐, 王茜. 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.
LI Chang-qi, WANG Han. Image Encryption Algorithm Based on Unordered Segmentation Projection Strategy and Gravity Model [J]. Packaging Engineering, 2017, 38(7): 191—196.
- [2] 索昱. 基于参数转换混沌耦合系统及其一维、二维变换规则的图像加密算法[J]. 科学技术与工程, 2014, 32(11): 37—43.
SUO Yu. Image Encryption Algorithm Based on Parameter Transformation, Chaotic Coupling System and Its One-dimensional and Two-dimensional Transformation Rules[J]. Science Technology and Engineering, 2014, 32(11): 37—43.
- [3] CHAI Xiu-li. An Image Encryption Algorithm Based on Bit Level Brownian Motion and New Chaotic Systems[J]. Multimedia Tools and Applications, 2017, 76(1): 1159—1175.
- [4] MA M E. A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos[J]. Signal Processing, 2015, 109(12): 119—131.
- [5] 李凯佳, 俞锐刚, 袁凌云. 基于 DNA-记忆元胞自动机与 Hash 函数的图像加密算法[J]. 计算机工程与设计, 2017, 38(2): 470—477.
LI Kai-jia, YU Rui-gang, YUAN Ling-yun. Image Encryption Algorithm Based on DNA-memory Cellular Automata and Hash Function[J]. Computer Engineering and Design, 2017, 38(2): 470—477.
- [6] WANG Xing-yuan, LIU Chuan-ming. A Novel and Effective Image Encryption Algorithm Based on Chaos and DNA Encoding[J]. Multimedia Tools and Applications, 2017, 76(5): 6229—6245.
- [7] LIU Hui, JIN Cong. A Novel Color Image Encryption Algorithm Based on Quantum Chaos Sequence[J]. 3D Research, 2017, 8(1): 1—6.
- [8] 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, 3(2): 189—195.
YANG Gui-bao, GAO Xia. Double Image Encryption Algorithm Based on Fractional Logistic Mapping and Random Transform[J]. Journal of Inner Mongolia University (Natural Science Edition), 2017, 3(2): 189—195.
- [9] 刘志军. 基于复合混沌与仿射变换的彩色图像加密算法[J]. 山东大学学报(工学版), 2016, 46(4): 1—8.
LIU Zhi-jun. Color Image Encryption Algorithm Based on Complex Chaos and Affine Transformation [J]. Journal of Shandong University(Engineering Science), 2016, 46(4): 1—8.
- [10] 徐亚, 张绍武. 基于 Arnold 映射的分块双层自适应扩散图像加密算法[J]. 中国图象图形学报, 2015, 20(6): 740—748.
XU Ya, ZHANG Shao-wu. A Block Double Layer Adaptive Diffusion Image Encryption Algorithm Based on Arnold Mapping[J]. Journal of Chinese Image and Graphics, 2015, 20(6): 740—748.
- [11] 潘光, 魏静. 一种分数阶混沌系统同步的自适应滑模控制器设计[J]. 物理学报, 2015, 64(4): 41—47.
PAN Guang, WEI Jing. An Adaptive Sliding Mode Controller Design for Synchronization of Fractional Order Chaotic Systems[J]. Journal of Physics, 2015, 64(4): 41—47.
- [12] YE Guo-dong, ZHAO Hai-qing, CHAI Hua-jin. Chaotic Image Encryption Algorithm Using Wave-line Permutation and Block Diffusion[J]. Nonlinear Dynamics, 2016, 83(4): 2067—2077.
- [13] ZHANG Qiang, LIU Li-li, DU Xiao-peng. Improved Algorithm for Image Encryption Based on DNA Encoding and Multi-chaotic Maps[J]. AEU-International Journal of Electronics and Communications, 2014, 68(3): 186—192.
- [14] 郭祖华, 徐立新, 张晓. 并行图像耦合超混沌系统的图像加密算法[J]. 计算机工程与设计, 2015, 32(5): 1170—1175.
GUO Zu-hua, XU Li-xin, ZHANG Xiao. Image Encryption Algorithm for Parallel Image Coupled Hyperchaotic Systems[J]. Computer Engineering and Design, 2015, 32(5): 1170—1175.
- [15] 郭静博, 孙琼琼. 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[J]. 包装工程, 2016, 37(13): 165—172.
GUO Jing-bo, SUN Qiong-qiong. Improved Model of Gravity Coupled Image Encryption Algorithm for Plaintext Cross Correlation Mechanism[J]. Packaging Engineering, 2016, 37(13): 165—172.