基于加权直方图位混淆与分阶混沌异扩散的快速图像加密算法

石坤泉[1]，魏文国[2]，杨震伦[1]
（1.广州番禺职业技术学院 信息工程学院，广州 511483；
2.广东技术师范学院 电子与信息工程学院，广州 510665）

摘要：目的 为了解决当前图像加密技术因在置乱和扩散过程忽略了明文像素特性，导致其抗明文攻击能力较弱，并且整个像素扩散均采用相同的加密机制来实现，存在安全性不理想问题，文中设计基于加权直方图位混淆和分阶混沌异扩散的快速图像加密算法。**方法** 该算法充分利用整个明文的像素值，将其嵌入到整个置乱与扩散阶段，且在扩散过程中，利用不同的加密函数对不同的像素进行扩散。首先，联合 Logistic 与 Tent 映射，利用非线性组合思想构建新的低维混沌系统，并分析其混沌性能；考虑输入明文的像素值，建立像素加权直方图，借助外部密钥，生成复合混沌系统的初值，通过迭代输出随机序列；再将明文的每个像素在位水平上进行扩展，利用离散化的随机序列在位水平上实现明文混淆；随后，将分数阶理论嵌入 Logistic 映射中，构建分阶 Logistic 混沌映射，利用像素的加权直方图对其迭代，输出混沌数组；对混淆密文的像素进行分类，结合混沌数组，设计异扩散模型，对三类像素进行不同的加密。**结果** 测试结果显示，与当前混沌加密算法相比，所提加密机制具有更强的抗明文攻击能力，其输出密文的像素分布更为均匀。**结论** 所提加密技术兼顾了较高的安全性与效率，能够较好地保护图像在网络中安全传输。

关键词：图像加密；加权直方图；分阶 Logistic 混沌映射；位水平；异扩散模型；明文攻击
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2018)13-0199-09
DOI：10.19554/j.cnki.1001-3563.2018.13.033

Fast Image Encryption Algorithm Based on Weighted Histogram Bit Confusion and Fractional Order Chaotic Diffusion

SHI Kun-quan[1], *WEI Wen-guo*[2], *YANG Zhen-lun*[1]
(1.College of Information Engineering, Guangzhou Panyu Polytechnic, Guangzhou 511483, China; 2.College of Electronics and Information Engineering, Guangdong Polytechnic Normal University, Guangzhou 510665, China)

ABSTRACT: The work aims to design the fast image encryption algorithm based on weighted histogram bit confusion and fractional order chaotic diffusion, for the purpose of solving theses defects as low anti-plaint attack induced by ignoring the characteristics of plain pixels during the scrambling and diffusion, and low security caused by using the same encryption function during the whole pixel diffusion in current image encryption technology. The algorithm made full use of the pixel value of the entire plaintext, and embedded it into the whole scrambling and diffusion phase, and different encryption functions were used to diffuse different pixels in the diffusion process. Firstly, combined with Logistic and Tent map, a new low-dimension chaotic system was constructed by means of the nonlinear combination thought and its chaotic performances were analyzed. The pixel weighted histogram was established by taking into account the pixel

收稿日期：2017-03-27
基金项目：国家自然科学基金（61672008，61272381）；广东省科技计划（2014A010103032）；广东省自然科学基金（S2012010008639）；广州市科技计划（201605131654362）
作者简介：石坤泉（1967—），男，广州番禺职业技术学院副教授，主要研究方向为信息安全、图像处理、机器视觉。

value of the input plain, and the initial value of the composite chaotic system was generated by means of the external key. The random sequence was outputted by iteration. Then, each pixel of the plaintext was extended on the level of the plaintext, and the plaintext was confused by the discrete random sequence. Subsequently, the fractional order gistic chaotic map was constructed by embedding fractional order theory into Logistic map, and the chaotic array was outputted to iterate it with the weighted histogram of the pixel. The different diffusion model was designed by classifying the pixels of the confusion cipher and combining the chaotic array to differently encrypt three kinds of pixels. The test results showed that the proposed encryption scheme had a stronger ability to resist plaintext attacks, and the pixels of output cipher was more uniform compared with the current chaotic encryption algorithm. With higher security and efficiency, the proposed encryption technology can better protect the images during their safe transmission in the network.

KEY WORDS: image encryption; weighted histogram; fractional order Logistic chaotic map; bit level; diffusion model; plain attack

数字图像作为多媒体信息最常见的内容之一，成为当前用户互动交流的直观载体，给用户带来了巨大便利[1—2]。数字图像在网络中传输时，经常遇到外来攻击，导致信息被篡改或者窃取[3]，因此，如何确保图像在网络中安全传输，保护其信息免受攻击已经是迫在眉睫[3]。传统的数据加密技术忽略了图像的大数据容量、高冗余度的特点，难以用于图像加密[4]。近年来，随着混沌理论的出现，为图像加密提供了强有力的保障，其具有较好的伪随机性、复杂的相空间等优势，在图像加密领域被广泛研究与应用，成为当前较为主流的加密手段[4]。如柴秀丽等[5]提出了基于超混沌系统的位级自适应彩色图像加密算法，利用四维陈氏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，同时设计采用自适应加密方法，用高四位的二值图像信息去加密低四位，再用加密后的低四位信息去加密高四位，从而形成整个图像加密。虽然高维混沌系统能够提高密文的安全性，有效抗击外来攻击，但是高维混沌系统显著增加了算法的复杂，导致其加密效率低下，且对整个彩图的置乱与扩散过程均没有考虑明文像素特性，导致其抗明文攻击能力较弱。WANG 等[6]利用双复杂混沌系统来实现像素位置的置乱与像素值的扩散，根据混沌系统的输出随机序列，设计了 2D, 1D 置乱技术，混淆明文 RGB 三分量的像素位置，利用 XOR 算子，设计像素扩散机制，对图像完成加密。虽然该技术利用 2 个复杂混沌系统来增强密文安全性，且利用不同的置乱技术来降低混沌周期性，其安全度要比文献[5]更高，但是 2 个复杂混沌系统带来的计算量更大，且整个像素扩散均采用相同的加密机制来实现，导致其随机性不佳。TELEM A K 等[7]设计了基于混沌 Logistic 映射与人工神经网络的图像加密技术，利用外部密钥生成 Logistic 映射的初值条件，从而计算人工神经网络的权重与基体矩阵，再将图像进行分块，利用不同的初始条件来生成密钥流，完成图像的置乱与扩散。该技术利用了低维 Logistic 映射，并利用了人工神经网络来增强密文安全性，其加密效率要显著高于文献[5]、文献[6]技术，且具有相近水平的密文安全性，但是该技术的整个加密过程脱离了明文像素特性，导致其抗明文攻击能力较弱。

为了充分利用明文像素特性，提高其抗明文攻击性能，文中提出基于加权直方图位混淆与分阶混沌异扩散的快速图像加密算法。

1 文中快速图像加密算法

基于加权直方图位混淆与分阶混沌异扩散的快速图像加密算法过程见图 1，其加密结构为“置乱-扩散”。由图 1 可知，所提快速加密技术过程有：基于加权直方图与低维复合混沌系统的明文置乱；基于分阶 Logistic 混沌映射与异扩散的图像加密。利用明文像素值，计算加权直方图，并利用其生成低维复合混沌系统的初始条件，并将每个像素分割为 8 个子像素，每个子像素为 8 bits，实现明文在位水平上的置乱，使得整个混淆过程与明文密切相关，兼顾置乱效率与置乱度。将 2 个分数阶参数嵌入 Logistic 映射中，建立分数阶 Logistic 映射，再次利用加权直方图获取其初值条件，同时对混淆密文像素分类，通过设计异扩散函数，对 3 类不同的像素完成分段加密，降低了周期性。

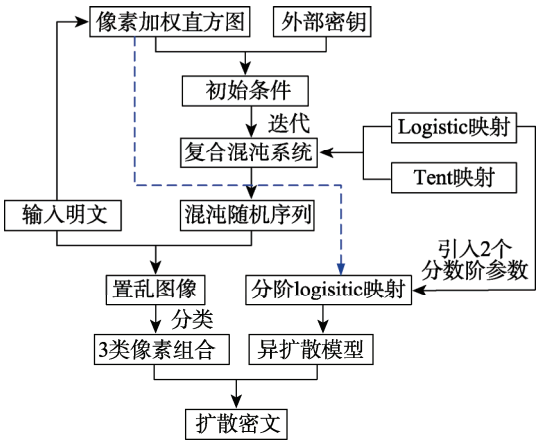


图 1 文中快速图像加密算法过程

Fig.1 Process of the proposed fast image encryption algorithm

1.1　基于加权直方图与复合混沌系统的明文置乱

1.1.1　低维复合混沌系统的构造及其混沌行为分析

为了兼顾高的安全性与低的复杂度，文中综合 Logistic 映射[8]与 Tent 映射[9]，构造了新的低维复合混沌映射。其中，Logistic 映射与 Tent 映射分别为：

$$X_{n+1}=L(r,X_n)=rX_n(1-X_n) \tag{1}$$

$$X_{n+1}=T(u,X_n)=\begin{cases}uX_n/2 & X_i<0.5\\ u(1-X_n)/2 & X_i\geqslant 0.5\end{cases} \tag{2}$$

式中：$r\in(0,4]$为 Logistic 映射的混沌参数；$u\in(0,4]$为 Tent 映射的混沌参数；X_n为第 n 个迭代输出值。

根据式（1）与式（2），基于非线性组合思想，构建了文中低维复合混沌系统，其结构见图 2。

$$X_{n+1}=L(r,X_n)+T\left[(4-r),X_n\right]\bmod l=\begin{cases}rX_n(1-X_n)+\left[(4-r),X_n/2\right]\bmod l & X_i<0.5\\ rX_n(1-X_n)+\left[(4-r),(1-X_n)/2\right]\bmod l & X_i\geqslant 0.5\end{cases} \tag{3}$$

式中：mod 为求余运算符号；l 为用户设置的常数，文中取 l=3。其余参数与式（1）相同。

由式（3）可知，该复合混沌系统混合了 Logistic 映射与 Tent 映射的混沌性能，且 mod 操作确保了该系统的输出值在[0,1]内。与单一的 Logistic 映射与 Tent 映射相比，其具有更复杂的混沌性能，见图 3。由图 3 可见，与 Logistic, Tent 映射相比，文中复合混沌系统具有更理想的 Lyapunov 指数与更大的混沌窗口，见图 3c。

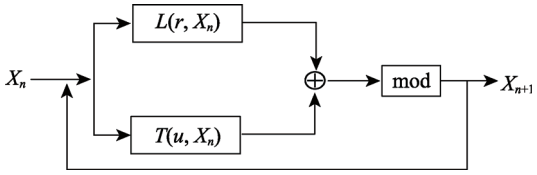


图 2　文中复合混沌系统的结构

Fig.2 The structure of the proposed composite chaotic system

1.1.2　基于加权直方图的初值生成及像素混淆

根据低维混淆系统可知，其初值条件有 r 与 X_0。为了增强整个加密算法与明文的关系，文中构建了加权直方图，并联合 256 位的外部密钥来计算 r 与 X_0。首先，将 256 位外部密钥 K 分割为 16 个 16 位子密钥 k_i：

$$K=k_1,k_2,k_3....k_{16} \tag{4}$$

则 r 与 X_0 的计算模型为：

$$r=\bmod\left(\frac{1}{256\left(k_1\oplus k_3\oplus...\oplus k_{15}\right)}+\frac{\sum_{i=1}^{16}k_i}{16},1\right) \tag{5}$$

$$X_0=\bmod\left(\frac{1}{256\left(k_2\oplus k_4\oplus...\oplus k_{16}\right)}+\frac{\sum_{i=1}^{16}k_i}{16},1\right) \tag{6}$$

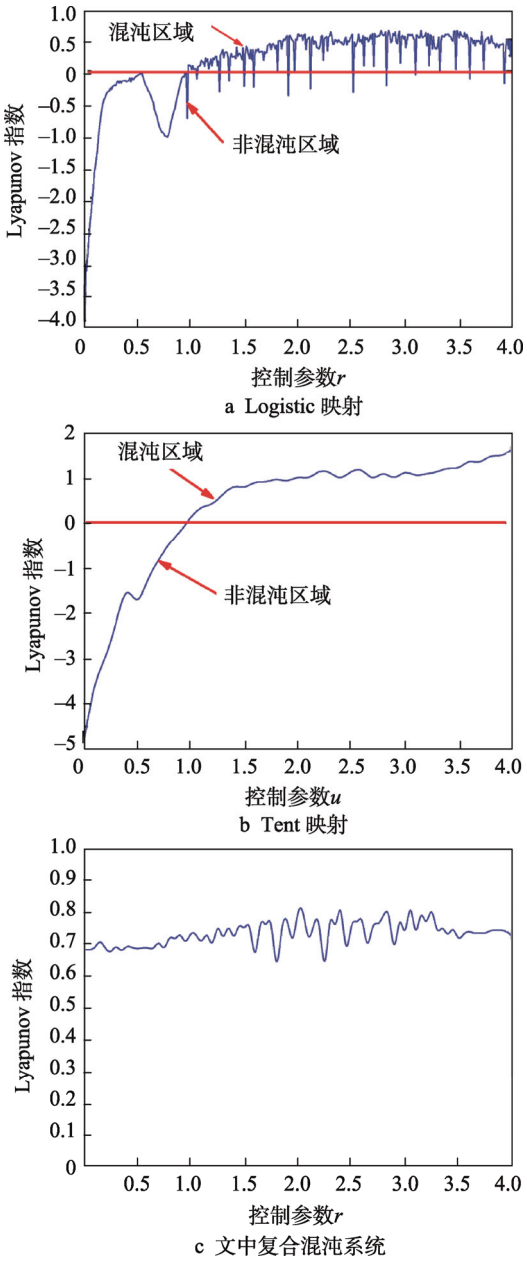


图 3　不同映射的混沌性能分析

Fig.3 Chaotic performance analysis of different maps

式中：mod 为求余运算；∑为求和运算；⊕ 为异或运算。

为了更新初值 r 与 X_0，文中利用明文像素值，以计算其加权直方图 H，该值描述了所有像素的分布：

$$H_1=\sum_{i=0}^{255}\left(\frac{h(i)}{M\times N}\right)\times h(i) \tag{7}$$

式中：M, N 分别为明文的宽度与高度；$h(i)$为一个包含了明文像素值的整数数组。

再根据式（7），计算更新后的加权直方图 H_2：

$$H_2=H_1\bmod 256 \tag{8}$$

式中：$H_2\in[0,255]$为加权直方图。

再利用十进制精度 10^{-15} 来计算明文的加权直方图 H：

$$H=\frac{H_2}{255} \tag{9}$$

利用式（9）得到的直方图 H，更新 r 与 X_0，获取新的初值 r' 与 X'_0：

$$\begin{cases} r'=r+H \\ X'_0=X_0+H \end{cases} \tag{10}$$

依据式（10）可知，其 r'，X'_0 与外部密钥、明文像素紧密相关，因此，该算法对于任何密钥或者明文的微小变化，都具备强烈的敏感性。

为了实现在像素位水平上的置乱，文中将明文中的每个像素分割成 8 个子像素，每个子像素包含 8 位；因此，明文尺寸被扩展为 $M\times N\times 8$。为了消除式（4）的瞬态效应，先利用 r 与 X_0 对其迭代 500 次，将其输出的随机序列删除；再继续对其迭代 $M\times N\times 8$ 次，输出 2 组序列 $\{X_k\},\{Y_k\}$。再对 $\{X_k\},\{Y_k\}$ 进行离散化：

$$\left\{\vec{X}_k\right\}=\{X_k\}\times 10^{15}\bmod M \tag{11}$$

$$\left\{\vec{Y}_k\right\}=\{Y_k\}\times 10^{15}\bmod(N\times 8) \tag{12}$$

对于明文中的（i,j）处的像素 $P(i,j)$，根据式（11—12），利用 $P\left(\vec{X}_i,\vec{Y}_j\right)$ 与 $P(i,j)$ 进行交换，改变其位置。式中：i=1,2…M，j=1,2…（$8N$−1）。以图 4a 为例，利用上述置乱过程，对其进行混淆，结果见图 4b。依图 4 可知，明文像素位置被高度混淆，所有明文信息均被充分掩盖，呈现 1 幅噪声干扰的图像。

为了量化所提置乱技术的像素混淆程度，根据文献[10]的方法来测试置乱图像的置乱度：

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

式中：R'为置乱图像；R 为明文；$M\times N$ 是明文尺寸；|| ||为求范数运算。

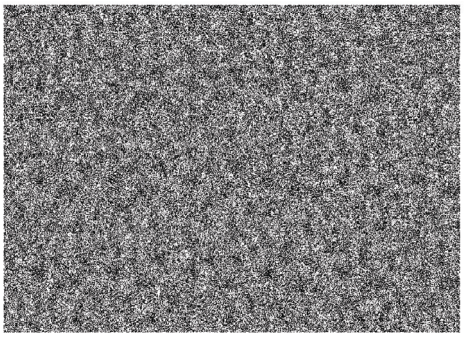
依据测试曲线可知，经过 2 轮迭代后，所提算法仅需 2 次混淆，其像素置乱度即可高达 99.83%，见图 4c。

1.2 基于分数阶 Logistic 映射与异扩散的像素加密

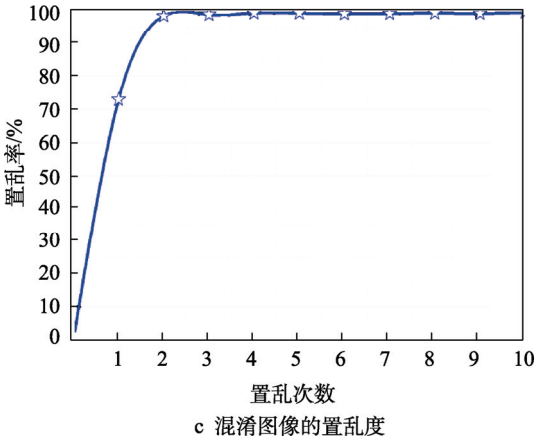
明文经过置乱操作后，其像素空间位置被充分混淆，但是其像素灰度值仍然没变[11]，因此，需要设计相应的扩散机制，改变其灰度值，增强密文的安全性。同样，为了兼顾密文安全性与加密效率，文中基于分数阶理论[12]，将 2 个分数阶参数引入到 Logistic 映射中，设计新的混沌映射。把分数阶参数 u,v 嵌入到式（1）中，形成新的混沌映射：

$$\begin{cases} \Delta_\alpha^v X_{n+1}=rX_{(n+v-1)}\left(1-X_{(n+v-1)}\right) \\ X_\alpha=X_0 \end{cases} \tag{14}$$

a 输入明文



b 置乱图像



c 混淆图像的置乱度

图 4 文中算法的置乱效果

Fig.4 Scrambling effect of the proposed algorithm

式中：α,v 均为整数；Δ 为分数阶符号。其余参数与式（1）相同。

通过利用分数阶参数 α, v，使得式（14）具备更大的混沌区域，使其输出序列的伪随机性更高，见图 5。依图可知，与图 3a 相比，式（14）的混沌区域更大，在区间(0.243, 4]内，都具有理想的混沌行为，表现出更为理想的混沌轨迹。

与置乱操作类似，为了增强像素过程与明文特性的关系，提高算法的抗明文攻击能力，文中再次利用外部密钥 K 与加权直方图，计算式（14）的初始条件 r，X_0：

$$r=\bmod\left(\frac{1}{256\left(k_1\oplus k_2\oplus\ldots\oplus k_8\right)}+\frac{\sum_{i=1}^{16}k_i}{16},1\right) \tag{15}$$

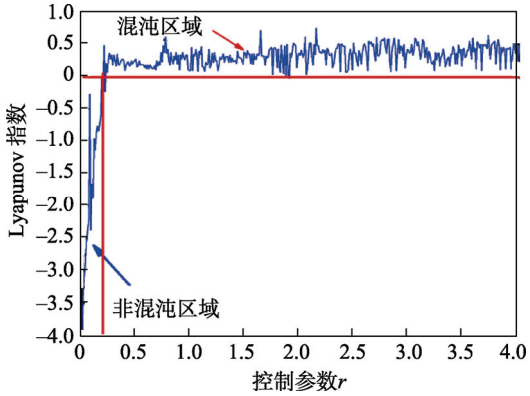


图 5　分数阶 Logistic 映射的混沌行为

Fig.5 Chaotic behavior of fractional order Logistic maps

$$X_0 = \mathrm{mod}\left(\frac{1}{256\left(k_9 \oplus k_{10} \oplus \ldots \oplus k_{16}\right)} + \frac{\sum_{i=1}^{16} k_i}{16}, 1\right) \tag{16}$$

利用式（15—16）的 r, X_0，执行式（7—10）的过程，获取 r'', X''_0。再根据用户设置的分数阶参数 u, v，对式（14）完成迭代，输出混沌序列 $\{X''_1, X''_2 \cdots X''_{M\times N}\}$。再对 $\{X''_1, X''_2 \cdots X''_{M\times N}\}$ 完成量化，获取密钥流 $\{s_1, s_2 \ldots s_{M\times N}\}$：

$$s_i = \mathrm{mod}\left(\mathrm{floor}\left(X''_i \times 10^{14}\right), 256\right) \tag{17}$$

式中：mod 为求余运算符号；floor 为向下取整运算。

为了实现对置乱密文像素的分段扩散，首先，将其像素值转化成 1D 序列 $\{P_1, P_2 \ldots P_{M\times N}\}$。然后，对其分类：第 1 个像素值 P_1，中间像素值 $\{P_2, P_3 \ldots P_{M\times N-1}\}$，以及最后 1 个像素 $P_{M\times N-1}$。

再计算像素 $\{P_2, P_3 \ldots P_{M\times N}\}$ 的综合 S_{um}：

$$S_{\mathrm{um}} = \sum_{I=2}^{M\times N} P_i \tag{18}$$

式中：$\sum$ 为求和运算。

利用式（18）的 S_{um}，计算初值 E_0：

$$E_0 = \mathrm{mod}\left(S_{\mathrm{um}}, 256\right) \tag{19}$$

联合 E_0 与密钥流 k_1，改变第一个像素 P_1 的灰度值：

$$P'_1 = E_0 \oplus P_1 \oplus k_1 \tag{20}$$

随后，利用如下扩散模型，对中间像素值 $\{P_2, P_3 \ldots P_{M\times N-1}\}$ 进行加密：

$$P'_i = P_i \oplus \left(k_i + P'_{i-1}\right) \mathrm{mod} 256 \oplus S_{\mathrm{um}} \tag{21}$$

针对最后一个像素 $P_{M\times N-1}$，利用如下扩散机制，改变其灰度值：

$$P'_{M\times N} = P_{M\times N} \oplus k_{M\times N} \oplus P_{kt_1} \tag{22}$$

$$kt_1 = \mathrm{floor}\left(\frac{\mathrm{mod}\left(\sum_{i=1}^{M\times N} P_{i-1} + k_i, 256\right)}{256\times(i-1)}\right) + 1 \tag{23}$$

根据该扩散过程可知，文中算法的像素加密操作与明文像素灰度值密切相关，且设计了 3 个不同的简单扩散机制，对不同的像素进行异扩散，与当前的扩散技术相比[5—7]，具有显著的优势。以图 4b 为对象，对其执行上述扩散过程，输出的密文见图 6。可见，经过分段扩散后，所输出的密文与置乱图像存在巨大差异，达到了双重加密的效果，显著改善了密文的抗统计攻击能力。

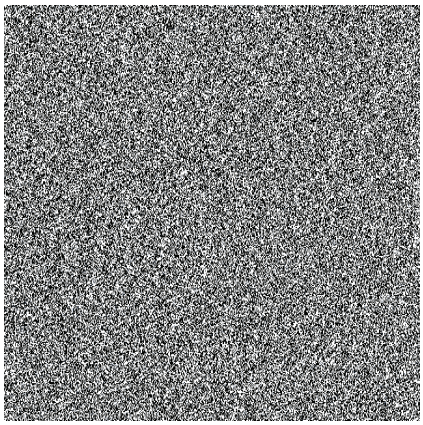


图 6　扩散密文

Fig.6 Diffusion cipher

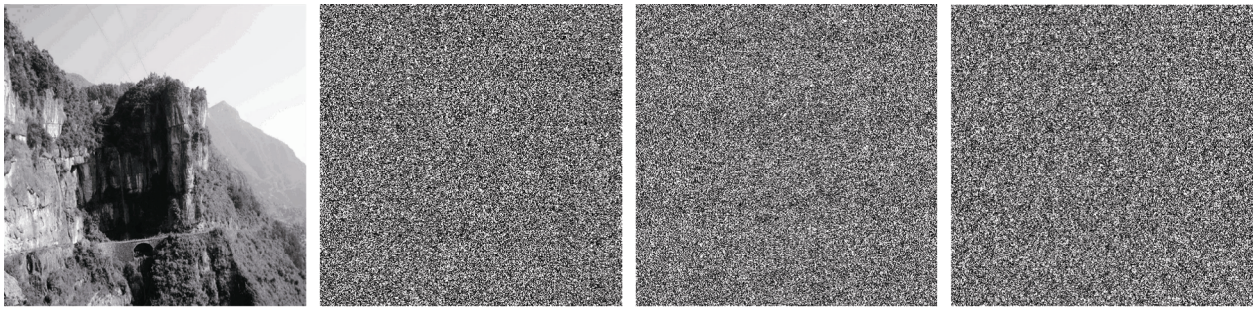
2　仿真实验与分析

利用 Matlab 平台来验证文中加密技术的安全性能与效率，同时，为了体现所提技术的优异性，把文献[7]与文献[13]作为对照组。执行加密算法的关键参数为：分数阶 α=2,v=3。

2.1　加密效果对比测试

将灰度图像视为测试对象，见图 7a，利用文中加密算法、文献[7]、文献[13]这 3 种技术对其进行处理，输出密文见图 7b—d。根据加密结果可知，3 种算法的加密视觉效果都较为理想，明文信息经过 3 种技术扩散后，其内容均被充分混淆与掩盖，没有信息泄露。另外，为了量化这 3 种加密技术的安全性差异，文中利用相似度 XSD 指标[14]来衡量密文的安全性，XSD 值越小，表明密文与明文的差异程度越大，其安全保密性越高。根据文献[14]的计算方法，得到 XSD 数据见表 1。由表 1 可知，文中加密技术输出的 XSD 值最小，为 0.286，而文献[7]、文献[13]算法的密文 XSD 值均要高于所提技术，分别为 0.392, 0.297。原因是文中通过设计复合混沌系统，扩大其混沌区域，利用外部密钥与明文自身像素值来完成提高像素位置的置乱度，并设计分数阶 Logistic 映射，利用加权直方图来设计 3 个不同的扩散机制，对置乱图像的首个像素、中间像素以及最后一个像素进行加密，实现了分段扩散，降低了混沌周期性，使得算法的安全

性更高；文献[13]主要是利用超混沌系统的序列来实现像素置乱与扩散，使其安全性较为理想，但其存在显著的周期性，使其密文 XSD 值要略大于文中技术；文献[7]则是利用传统的低维混沌映射来完成加密，虽然利用了人工神经网络来优化算法，但是低维混沌的结构简单，混沌区域较小，使其安全性最低。



a 输入明文 b 文中算法密文 c 文献[7]算法的密文 d 文献[13]算法的密文

图 7 3 种不同算法的加密效果

Fig.7 Encryption effect of three different algorithms

表 1 各算法的 XSD 测试结果

Tab.1 XSD test results of each algorithm

名称	文中算法	文献[7]	文献[13]
密文 XSD 值	0.286	0.392	0.297

2.2 相邻像素点的相关性对比测试分析

图像相邻像素之间具有强烈的相关性，而这种相关性通常被攻击者利用[15]，一般而言，图像像素分布越均匀，表明图像的抗攻击能力越高，其密文安全性越理想。故文中在图 7a—d 中取 3000 对相邻像素点来测试密文的像素相关系数 C_{xy}[15]。

$$C_{xy}=\frac{1/n\sum_{i=1}^{n}\left(x_i-E\left(x_i\right)\right)\left(y_i-E\left(y_i\right)\right)}{\sqrt{\left(1/n\sum_{i=1}^{n}\left(x_i-E\left(x_i\right)\right)^2\right)\left(1/n\sum_{i=1}^{n}\left(y_i-E\left(y_i\right)\right)^2\right)}} \tag{24}$$

3 种加密技术对应的密文相关系数 C_{xy} 测试结果见图 8。根据图 8a 可知，明文像素的分布极为不均，其相关性非常高，堆积为对角线形式；经过 3 种加密机制的置乱与扩散后，其像素分布变为均匀，这种相关性被显著降低。文中加密技术的密文像素分布最为理想，见图 8b，而文献[7]、文献[13]算法的密文像素分布均匀度要低于文中技术，出现了“空洞效应”，分别见图 8c—d。另外，明文与 3 个密文在 3 个方向的 C_{xy} 测试数据见表 2。对于任意一个方向，所提加密技术的相关系数 C_{xy} 始终是最小的，有效提高了密文的安全度。

2.3 抵御明文攻击性能分析

网络中的明文攻击对图像信息安全威胁较大，为了量化 3 种加密算法的抗明文攻击性能，引用 NPCR 与 UACI 来衡量[15]：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\mathrm{Difp}\left(I\left(i,j\right),I'\left(i,j\right)\right)}{W\times H}\times 100\% \tag{25}$$

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{ij}\frac{\left|I\left(i,j\right)-I'\left(i,j\right)\right|}{255}\right]\times 100\% \tag{26}$$

$$\mathrm{Difp}\left(I\left(i,j\right),I'\left(i,j\right)\right)=\begin{cases}0 & I\left(i,j\right)=I'\left(i,j\right)\\ 1 & I\left(i,j\right)\neq I'\left(i,j\right)\end{cases} \tag{27}$$

文中算法、文献[7]以及文献[13]这 3 种算法密文的 NPCR 与 UACI 测试结果见图 9。依据曲线数据可知，文中加密算法的抗明文攻击能力最强，密文的 NPCR 与 UACI 分别为 99.62%，34.96%，均高于文献[7]与文献[13]算法的 NPCR 与 UACI 值，见图 9a—b。其原因是所提加密技术充分利用了明文像素值，通过将其像素加权直方图作为初始条件，使得整个置乱与扩散过程均与明文密切相关，从而增强了算法的抗明文攻击能力。文献[7]与文献[13]这 2 种算法的置乱与扩散均与明文无关，仅依靠混沌系统实现像素加密，使其抗明文攻击能力较弱。

2.4 加密效率对比测试分析

优异的加密算法除了具备较高的安全性之外，加密效率也是重要的衡量指标[16]。选用尺寸为 512×512 像素的 Lena 灰度图像，仿真环境为：DELL VOSTRO1088 的 XP 系统、3.5 GHz、4 GB 的内存。利用文中算法、文献[7]、文献[13]这 3 种技术对 Lena 灰度图像完成加密，通过记录其时耗可知，文中算法的加密时间仅为 0.29 s，而文献[7]、文献[13] 2 种算法的加密时间为 0.21, 1.36 s。原因是文献[13]利用超混沌系统来完成像素的置乱与扩散，而超混沌系统的复杂度较高，导致其加密效率较低；而文献[7]的加密速度最快，主要是该技术利用 1D Logistic 映射，其解密结构简单。

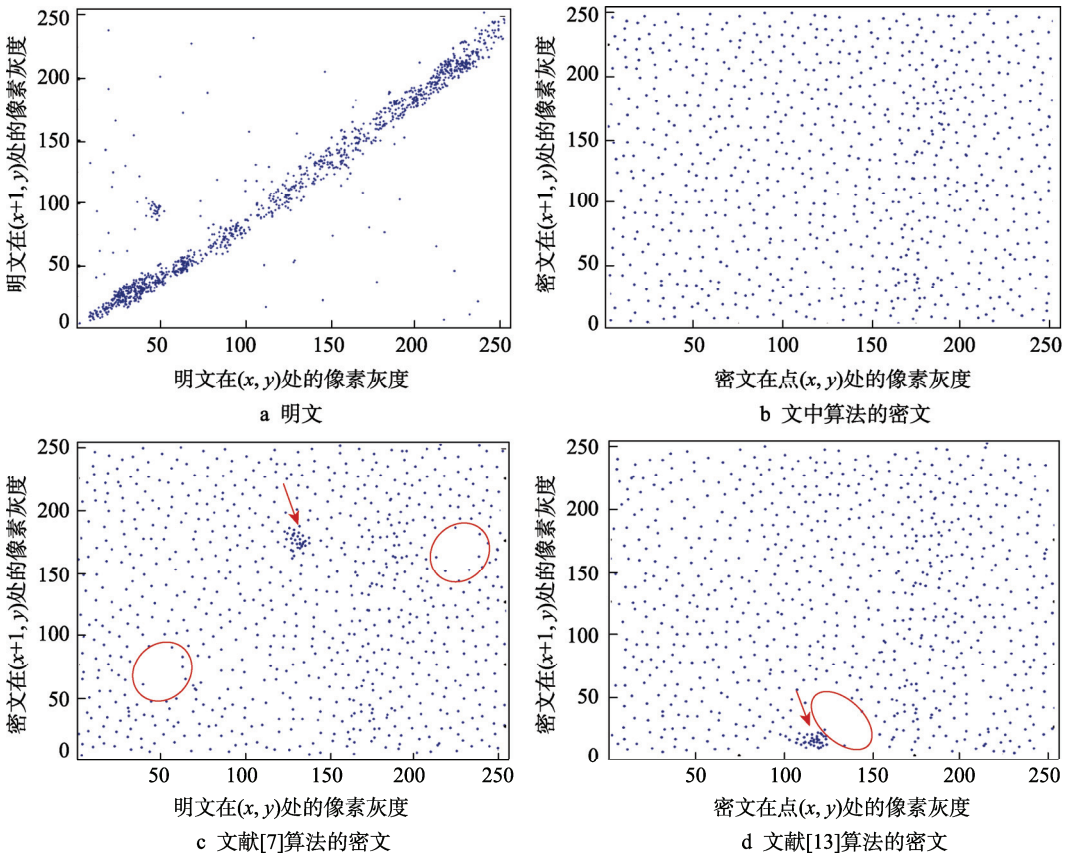


图 8　相邻像素之间的相关性测试

Fig.8 Correlation test of adjacent pixels

表 2　不同方向的相关系数测试结果

Tab.2 Test results of correlation coefficients in different directions

选取方向	文中算法密文	明文
水平	0.0027	0.9708
垂直	0.0019	0.9374
对角线	0.0036	0.095 91

文中算法虽然也是使用低维混沌映射，但是在扩散阶段采用了分段加密，增加了计算量，使其加密时耗要高于文献[7]算法。

2.5　解密效果分析

解密是加密的逆过程，为了体现所提算法的解密质量，以图 10a 为例，其初始直方图见 10b，利用所提加密技术对处理后，获取的密文见图 10c，再利用已知的密钥对其进行解密，结果见图 10e，对应的直方图见 10f。依图 10 可知，所提算法具有较好的解密质量，完整地复原了初始明文，且解密图像的直方图

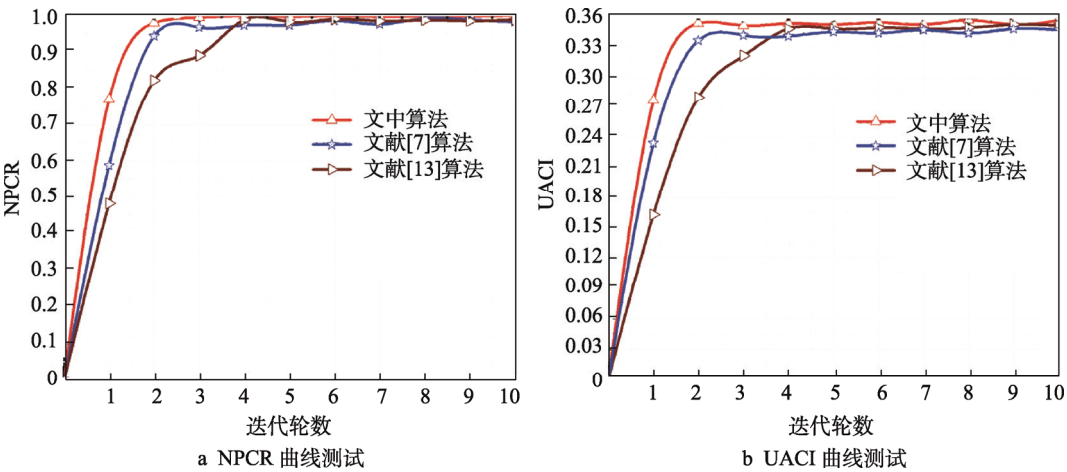


图 9　3 种算法的抗明文攻击能力测试结果

Fig.9 Test results of the three algorithms against plaintext attack

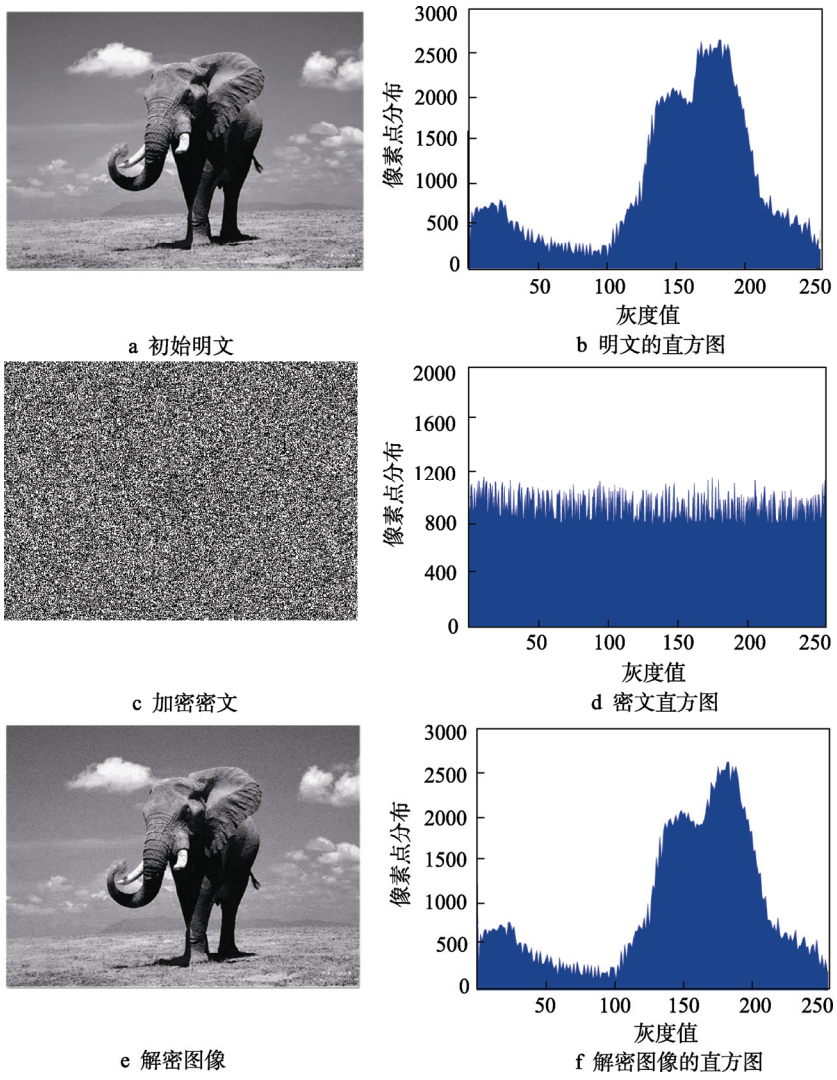


图 10　文中算法的解密效果测试

Fig.10 Decryption effect test of the proposed algorithm

特性与初始明文的直方图非常相似。这显示所提加密技术具有良好的复原效果，解密失真度很小。

3　结语

为了提高加密算法的抗明文攻击能力，提出了基于加权直方图位混淆与分阶混沌异扩散的快速图像加密算法。整个加密算法都是使用了低维混沌映射，提高了其加密效率；同时，通过设计复合混沌系统与新的 Logistic 映射，扩大算法的混沌区域，并将明文像素贯穿在整个置乱与扩散过程中，且在像素扩散期间，对像素进行分类，设计不同的加密函数实现分段扩散，从而提高密文的安全性，尤其是抗明文攻击能力。实验结果验证了所提加密技术的安全性与效率。

参考文献：

[1] CHAI X L, GAN Z H, CHEN Y R. A Visually Secure Image Encryption Scheme Based on Compressive Sensing[J]. Signal Processing, 2017, 134: 35—51.

[2] 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 Gravity Model Coupled Plaintext Pixel Cross-correlation Mechanism of Image Encryption Algorithm[J]. Packaging Engineering, 2016, 37(13): 165—172.

[3] 胡春杰, 陈晓, 陈霞. 基于改进广义 Arnold 映射的多混沌图像加密算法[J]. 包装工程, 2017, 38(3): 144—149.
HU Chun-jie, CHEN Xiao, CHEN Xia. Multi Chaotic Image Encryption Algorithm Based on Improved Generalized Arnold Map[J]. Packaging Engineering, 2017, 38(3): 144—149.

[4] 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]. 科学技术与工程, 2013, 35(13): 10523—10530.
SUN Li, HUANG Zheng-qian, FU Wei-min. Research on Image Encryption Algorithm Based on Time Delay and Hyper Chaotic Chen system[J]. Science and Technology and Engineering, 2013, 35(13): 10523—10530.

[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 New Color Image Encryption Algorithm Based on Bit Level Adaptive[J]. Computer Science, 2016, 43(4): 134—139.

[6] WANG L Y, SONG H J, LIU P. A Novel Hybrid Color Image Encryption Algorithm Using Two Complex Chaotic Systems[J]. Optics and Lasers in Engineering, 2017, 77(11): 118—125.

[7] NICOLE D, TELEM A K. A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network[J]. Advances in Multimedia, 2015, 78(7): 1120—1129.

[8] WANG X Y, BAO X M. A Wheel-switch Selective Image Encryption Scheme Using Spatiotemporal Chaotic System[J]. Zeitschrift Für Naturforschung A, 2014, 69(1/2): 61—69.

[9] YE R S, ZENG S J. A Secure and Efficient Image Encryption Scheme Based on Tent Map and Permutation-substitution Architecture[J]. International Journal of Modern Education and Computer Science, 2014, 38(7): 19—30.

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

[11] MA J M, YE R S. An Image Encryption Scheme Based on Hybrid Orbit of Hyper-chaotic Systems[J]. International Journal of Computer Network and Information Security, 2015, 7(5): 25—33.

[12] 史丽燕. 基于分数阶原始对偶模型的图像去噪方法[J]. 激光杂志, 2015, 22(12): 42—46.
SHI Li-yan. Image Denoising Method Based on Fractional Primal Dual Model[J]. Journal of Lasers, 2015, 22(12): 42—46.

[13] LI Y P, WANG C H, CHEN H. A Hyper-chaos-based Image Encryption Algorithm Using Pixel-level Permutation and Bit-level Permutation[J]. Image Encryption, 2017, 90(3): 238—246.

[14] 文昌辞, 王沁, 刘向宏. 基于仿射和复合混沌的图像加密新算法[J]. 计算机研究与发展, 2013, 50(2): 319—324.
WEN Chang-chi, WANG Qin, LIU Xiang-hong. A New Image Encryption Algorithm Based on Affine and Compound Chaos[J]. Computer Research and Development, 2013, 50(2): 319—324.

[15] 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-cellular Automata and Hash Function[J]. Computer Engineering and Design, 2017, 38(2): 470—477.

[16] 许爽, 王伟, 苏玉. 基于双向扩散机制融合伪随机数同步生成器的快速图像加密算法研究[J]. 科学技术与工程, 2014, 14(7): 45—50.
XU Shuang, WANG Wei, SU Yu. Research on Fast Image Encryption Algorithm Based on Fusion of Pseudo-random Number Generator Based on Bidirectional Diffusion Mechanism[J]. Science and Technology and Engineering, 2014, 14(7): 45—50.