文章编号：1001-3806(2017)06-0897-07

一种基于混沌映射的快速图像加密算法优化

乔建平，邓联文*，贺 君，廖聪维
（中南大学 物理与电子学院 超微结构与超快过程湖南省重点实验室，长沙 410083）

摘要：为了解决现有图像加密算法存在随图像尺寸变大导致加密时间迅速增加的问题，采用基于 logistic 和 Arnold 映射的改进加密算法实现了快速图像加密算法的优化。该算法基于两种混沌映射对原文图像进行像素置乱和灰度值替代，像素置乱是按图像大小选择以 H 个相邻像素为单位进行，通过适当调整 H 的取值实现加密时间优化；灰度值替代是利用 Arnold 映射产生混沌序列对置乱图像进行操作而得到密文图像。结果表明，对于 256×256 的 Lena 标准图像，加密时间降低到 0.0817s。该算法具有密钥空间大和加密速度快等优点，能有效抵抗穷举、统计和差分等方式的攻击。

关键词：图像处理；图像加密；混沌映射；Lena 图像
中图分类号：TP309.7 **文献标志码**：A **doi**：10.7510/jgjs.issn.1001-3806.2017.06.026

Optimization of fast image encryption algorithm based on chaotic mapping

QIAO Jianping, *DENG Lianwen*, *HE Jun*, *LIAO Congwei*
(Hunan Key Laboratory for Super-microstructure and Ultrafast Process, School of Physics and Electronics, Central South University, Changsha 410083, China)

Abstract: In order to solve the rapid increase of the encryption time because of the increasing image size in the existing image encryption algorithm, the optimized encryption algorithm based on logistic and Arnold mapping was used to achieve the optimization of the fast image encryption algorithm. The algorithm was based on two kinds of chaotic maps to the original image, pixel scrambling and gray value substitution. Pixel scrambling was to select the H adjacent pixels according to the image size, appropriately adjust the H value and realize the encryption time optimization. Gray value substitution is to generate chaotic sequences by Arnold mapping, operate the scrambling image and get the cipher image. The results show that, for 256×256 Lena standard images, the encryption time is reduced to 0.0817s. The algorithm has advantages of large key space and fast encryption speed, and can effectively resist the attack of exhaustive, statistical, and differential means.

Key words: image processing; image encryption; chaotic mapping; Lena image

引 言

近年来，随着互联网、多媒体以及通信技术的快速发展和普及，信息的安全传输显得尤为重要。由于图像具有信息数据量大、相关性强等特点，传统加密技术，比如数据加密标准(data encryption standard, DES)和高级加密标准(advanced encryption standard, AES)，都难以满足图像信息实时加密的需求。混沌系统具有的初值敏感性、遍历性、参量可控性以及伪随机性等特征，为数字图像加密算法的研究提供新的思路，因而基于混沌的图像加密算法成为了研究热点[1-4]。

现有的混沌图像加密算法一般基于置乱和替代模型[5-7]。LI 等人[8]提出了基于 Hash 函数和多混沌系统的图像加密算法，该算法的安全性相对较强，但加密效率并不高。ZHENG[9]等人提出了基于时空混沌系统的图像分组加密算法，该算法安全系数较高，但对于尺寸大于 256×256 的图像，加密效率难以满足实时通信要求。WANG 等人[10]提出基于分块置乱与扩散的分数阶混沌彩色图像加密算法，加密效率相对较高，但当原文图像尺寸变大时，加密时间呈快速增加趋势。因此，迫切需要设计一种实现过程简单、加密效率高、灵活性高，又能有效抵御统计分析等多种攻击方式的图像加密算法。本文中提出一种基于 logistic 映射和 Arnold 映射的快速图像加密算法，通过采用分组置乱方法解决以往算法存在随图像尺寸变大而使加密时间快速增加的问题。

1 算法设计

logistic 映射[11]定义为：

基金项目：湖南省科技计划资助项目(2015JC3041)
作者简介：乔建平(1992-)，男，硕士研究生，主要研究方向为图像加密算法的研究。
*通讯联系人。E-mail：dlw626@163.com
收稿日期：2016-12-12；收到修改稿日期：2017-02-17

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

式中，μ 是系统参量，且 $\mu \in (0, 4]$，当 $\mu \in (3.5699456, 4]$ 时，logistic 系统处于混沌态，具有非常复杂的动力学行为。

经典的 Arnold 映射[12]定义为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \tag{2}$$

式中，(x_n, y_n) 表示系统的状态变量，mod 表示取余运算。

为了能更好地运用到实际应用中，Arnold 映射扩展为更加普遍的形式[13]，其数学表达式为：

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod M \tag{3}$$

式中，p 和 q 为系统参量，M 表示图像大小，本文中取 $M = 256$。

本文中加密算法的基本原理流程图如图 1 所示，加密过程包括像素置乱和灰度值替代两部分。

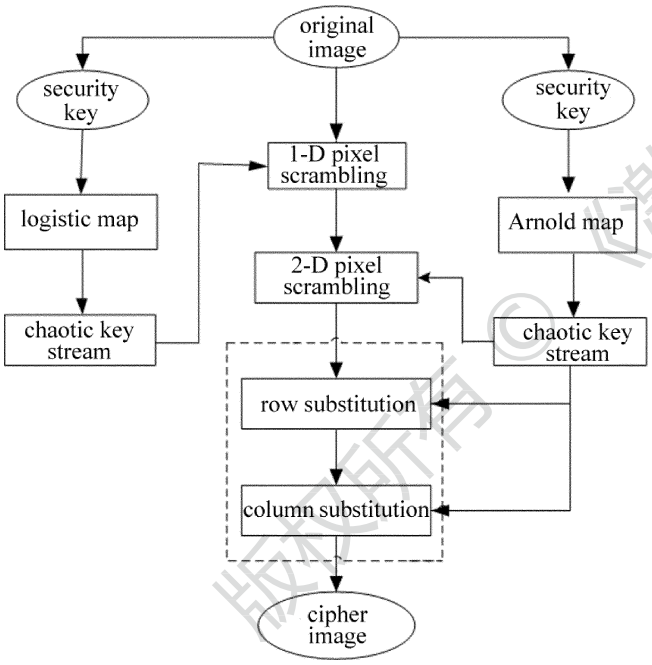

Fig. 1 Flowchart of the proposed algorithm

1.1 像素置乱

假定原始图像为 $\boldsymbol{A}$，大小为 $M \times N$，将 $\boldsymbol{A}$ 转换成长度为 $L = M \times N$ 的 1 维序列 $\boldsymbol{P} = \{p_1, p_2, p_3, \cdots, p_L\}$；再将 $\boldsymbol{P}$ 平均分割成 4 段序列，每段长度都为 $L/4$，分别表示 $\boldsymbol{D}_1, \boldsymbol{D}_2, \boldsymbol{D}_3, \boldsymbol{D}_4$，在这 4 段中，以每 H 个相邻元素（像素）为一个单位，将每个单位看成一个小块，每段有 m 个包含 H 个相邻元素的小块，m 的个数由原始图像的大小决定，假设 $L = M \times N$，则 $m = L/(4H)$。转换分割过程如图 2 所示。

设置 logistic 映射的系统参量 μ 和初值 x_0，预迭代 1000 次，以消除暂态效应，从第 1001 项取值，通过下式产生 4 个长度为 m 的随机序列 $\boldsymbol{R}_1, \boldsymbol{R}_2, \boldsymbol{R}_3, \boldsymbol{R}_4$：

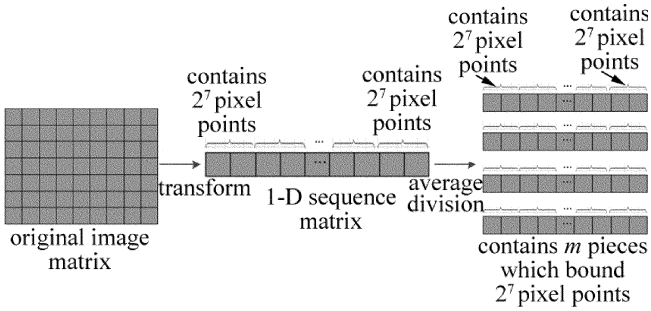

Fig. 2 Schematic diagram of conversion segmentation process

$$\begin{cases} R_1(i) = \text{floor}(x(i) \cdot S \cdot 10^4 \bmod 256) \\ R_2(i) = \text{floor}(x(i) \cdot S \cdot 10^7 \bmod 256) \\ R_3(i) = \text{floor}(x(i) \cdot S \cdot 10^{10} \bmod 256) \\ R_4(i) = \text{floor}(x(i) \cdot S \cdot 10^{13} \bmod 256) \end{cases} \tag{4}$$

式中，$x(i)$ 为 logistic 映射迭代 1000 次后的状态值，S 是原始图像所有像素值之和，floor(x) 表示取不大于 x 的最大整数。

由小到大重新排列序列 $\boldsymbol{R}_1, \boldsymbol{R}_2, \boldsymbol{R}_3, \boldsymbol{R}_4$，得到新的有序序列 $\boldsymbol{R}_{11}, \boldsymbol{R}_{12}, \boldsymbol{R}_{13}, \boldsymbol{R}_{14}$。例如，对序列 $\boldsymbol{R}_1 = \{r_1, r_2, r_3, \cdots, r_m\}$ 按升序由小到大排序，得到新的有序序列 $\boldsymbol{R}_{11} = \{r_{11}, r_{12}, r_{13}, \cdots, r_{1m}\}$，同时生成用于记录序列 $\boldsymbol{R}_{11}$ 中各个元素在原序列 $\boldsymbol{R}_1$ 中的位置的新序列 $\boldsymbol{S}_1 = \{s_1, s_2, s_3, \cdots, s_m\}$。同理，以同样的方式重新排列序列 $\boldsymbol{R}_2$，$\boldsymbol{R}_3$ 和 $\boldsymbol{R}_4$ 得到 $\boldsymbol{S}_2, \boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$。分别用序列 $\boldsymbol{S}_1, \boldsymbol{S}_2, \boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$ 去置乱如图 2 所示得到的序列 $\boldsymbol{D}_1, \boldsymbol{D}_2, \boldsymbol{D}_3$ 和 $\boldsymbol{D}_4$。为了方便分析，以第 1 段 $\boldsymbol{D}_1$ 为例，在 $\boldsymbol{D}_1$ 中，以 H 个相邻元素为一个单位，每个单位看成一个小块，那么 $\boldsymbol{D}_1$ 可看成只包含 m 个小块的序列，则 $\boldsymbol{D}_1 = \{d_1, d_2, d_3, \cdots, d_m\}$，然后通过序列 $\boldsymbol{S}_1$ 置乱 $\boldsymbol{D}_1$，得到置乱的 $\boldsymbol{D}_{11} = \{d_{11}, d_{12}, d_{13}, \cdots, d_{1m}\}$，置乱原理见下：

$$d_{ij} = d_{s_i}, (i, j = 1, 2, 3, \cdots, m) \tag{5}$$

同理，分别用 $\boldsymbol{S}_2, \boldsymbol{S}_3$ 和 $\boldsymbol{S}_4$ 置乱 $\boldsymbol{D}_2, \boldsymbol{D}_3$ 和 $\boldsymbol{D}_4$ 得到 $\boldsymbol{D}_{12}, \boldsymbol{D}_{13}$ 和 $\boldsymbol{D}_{14}$。

上述置乱效果仍不够理想，原因在于 $\boldsymbol{D}_{11}, \boldsymbol{D}_{12}, \boldsymbol{D}_{13}$ 和 $\boldsymbol{D}_{14}$ 中以 H 个相邻元素为单位的小块内部包含的像素仍处于相邻状态并没有置乱。为达到更好的置乱效果，分别从 $\boldsymbol{D}_{11}, \boldsymbol{D}_{12}, \boldsymbol{D}_{13}, \boldsymbol{D}_{14}$ 中分别同时取出第 1 个包含 H 个相邻像素为单位的小块，组成 4 行 H 列的 2 维矩阵 $\boldsymbol{W}_{4 \times H}$。通过设置 Arnold 映射初值 x_1 和 y_1，以及控制参量 p 和 q，并迭代产生两个混沌序列，通过下式产生密钥序列 k_1 和 k_2，长度分别为 4 和 H：

$$\begin{cases} k_1(i) = \text{round}(x[i + 1000] \cdot L \cdot 10^8) \bmod 256 \\ k_2(i) = \text{round}(y[i + 1000] \cdot L \cdot 10^{12}) \bmod 256 \end{cases} \tag{6}$$

式中，$x(i)$ 和 $y(i)$ 是由 Arnold 映射迭代产生的两个混

沌序列，round(x)表示取最接近于 x 的整数。

按升序重新排列密钥序列 k_1 和 k_2，用序列 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 分别记录 k_1 和 k_2 升序排列之前的元素位置，然后将 2 维矩阵 $\boldsymbol{W}_{4\times H}$的每一行按照序列 $\boldsymbol{T}_1$ 对应的元素进行行移位置乱操作；同理，将 $\boldsymbol{W}_{4\times H}$的每一列按照序列 $\boldsymbol{T}_2$ 对应的元素进行列移位置乱操作，得到 $\boldsymbol{W}_{1,4\times H}$，操作过程如图 3 所示。

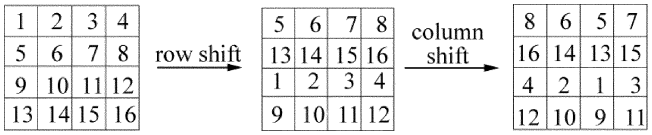

Fig. 3 The shifting process

从 $\boldsymbol{D}_{11}$，$\boldsymbol{D}_{12}$，$\boldsymbol{D}_{13}$和 $\boldsymbol{D}_{14}$中分别取出第 2 个以 H 个相邻像素为单位的小块，再以上述方式实现置乱操作，得到 $\boldsymbol{W}_{2,4\times H}$，并依次循环执行下去，剩余小块同样以相同方式置乱，从而得到 $\boldsymbol{W}_{3,4\times H}$，$\boldsymbol{W}_{4,4\times H}$，$\cdots$，$\boldsymbol{W}_{m,4\times H}$，最后将 $\boldsymbol{W}_{1,4\times H}$，$\boldsymbol{W}_{2,4\times H}$，$\cdots$，$\boldsymbol{W}_{m,4\times H}$转换成 1 维矩阵，并连接成长度为 $L=M\times N$ 的 1 维序列 $\boldsymbol{C}_L$，最后将 $\boldsymbol{C}_L$ 转变成 2 维矩阵 $\boldsymbol{C}$，即得到置乱图像 $\boldsymbol{C}$。

1.2 灰度值替代

像素置乱过程只改变原始图像像素位置的分布，并未改变像素灰度值的统计特性，为了提高加密算法的安全性，还必须对置乱图像进行灰度值替代。由 Arnold 映射迭代产生两个混沌序列，为消除暂态效应，舍弃前 1000 次的迭代值。从第 1001 项取，通过下式产生长度分别为 M 和 N 的密钥流 k_3 和 k_4：

$$\begin{cases} k_3(j)=\text{floor}(x(i)\cdot 10^7)\bmod 256 \\ k_4(i)=\text{floor}(y(i)\cdot 10^{11})\bmod 256 \end{cases} \tag{7}$$

假设置乱图像表示为像素矩阵 $\boldsymbol{C}(i,j)$，具体的灰度值替代操作包括行替代和列替代。

1.2.1 *行替代* 对置乱图像 $\boldsymbol{C}$ 的第 1 行像素 $\boldsymbol{C}(1,j)$ 按照下式进行替代加密，得到加密像素 $\boldsymbol{C}'(1,j)$，$j=\{1,2,3,\cdots,N\}$。

$$\boldsymbol{C}'(1,j)=k_3(j)\oplus\boldsymbol{C}(1,j) \tag{8}$$

从第 2 行至最后一行，按照下式执行行替代加密，直至每一行所有的灰度值都进行了行替代异或操作：

$$\boldsymbol{C}'(i,j)=\boldsymbol{C}'(i-1,j)\oplus\boldsymbol{C}(i,j)\oplus k_3(j) \tag{9}$$

式中，i 表示行数，$i=\{2,3,4,\cdots,M\}$；j 表示列数，$j=\{1,2,3,4,\cdots,N\}$。

1.2.2 *列替代* 对行替代操作后的图像 $\boldsymbol{C}'$的第 1 列像素 $\boldsymbol{C}'(i,1)$按照下式进行替代加密，得到加密像素 $\boldsymbol{E}(i,1)$，$i=\{1,2,3,\cdots,M\}$：

$$\boldsymbol{E}(i,1)=k_4(i)\oplus\boldsymbol{C}'(i,1) \tag{10}$$

从第 2 列至最后一列，按照下式执行列替代加密，直至每一列所有的灰度值都进行了列替代异或操作：

$$\boldsymbol{E}(i,j)=\boldsymbol{E}(i,j-1)\oplus\boldsymbol{C}'(i,j)\oplus k_4(i) \tag{11}$$

式中，i 表示行数，j 表示列数，$i=\{1,2,3,4,\cdots,M\}$，$j=\{2,3,4,\cdots,N\}$。最终得到加密图像 $\boldsymbol{E}$，结合加密图像和正确密钥，经逆向运算操作可解密得到原始图像 $\boldsymbol{A}$。

2 结果与分析

在 MATLAB R2013a 平台进行仿真验证，选取 256 × 256 的 Lena 照片图像为对象，设定 logistic 的系统参量 $\mu=3.99198012$ 和初值 $x_0=0.19910127$，Arnold 映射参量 $p=20$，$q=4$，初值为 $x_1=0.39920328$，$y_1=8.91953206$，在置乱过程可令 $H=2^l$，$l=\{2,3,4,5,6,7,8,9,10,\cdots\}$，如此取 l 值，H 跨度较大，当然 H 也可按其它方式取值。为方便分析，先设 $l=7$，即 $H=2^7=128$，按步骤对图像进行加解密操作，如图 4b 所示，从密文图像看不到任何有效信息；如图 4c 所示，对加密图像进行有效解密获得的图像与原始图像几乎一致。当密钥初值有微小误差：$x_0=0.19910127+10^{-12}$，其它密钥都正确的情况下，对加密图像进行解密，得到的图像效果如图 4d 所示，可见，因密钥初值的细微误差可导致解密图像的严重变化和完全失真，验证了本算法具有很强的密钥敏感性。

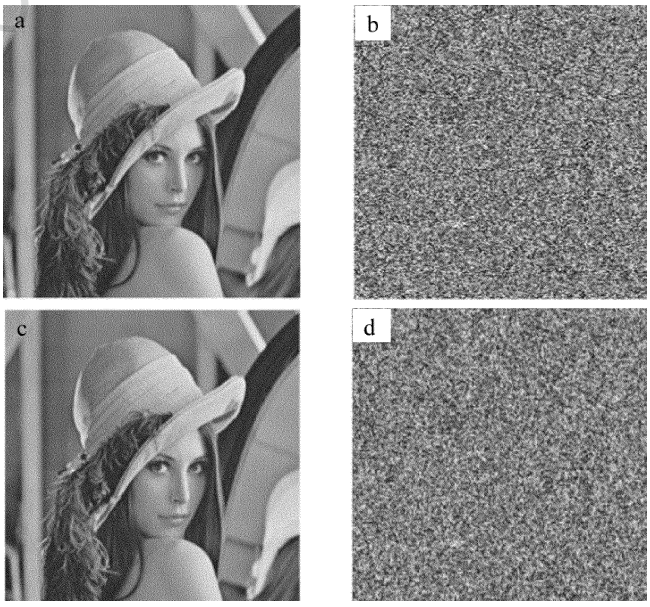

Fig. 4 Encryption and decryption results

a—original image b—cipher image c—decryption image d—the decryption image by the wrong key with x_0+10^{-12}

2.1 密钥空间分析

密钥空间的大小可以反映一种加密算法的安全性高低，密钥空间须足够大才能有效抵御穷举攻击。在本算法中，系统的密钥包括 logistic 系统的初值 x_0 和参量 μ，Arnold 映射的参量 p 和 q，以及初值 x_1 和 y_1，当数据精度达到 10^{-15} 时，算法的密钥空间将达到 $10^{90}\approx$

2^{298},拥有如此大的密钥空间,因而足以抵御穷举攻击。

2.2 统计特性分析

2.2.1 信息熵分析 信息熵可以度量图像灰度值分布,即信息熵越大,图像的灰度值分布越均匀。信息熵[14]数学表达式定义为:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} \tag{12}$$

式中,m_i 表示像素值,$p(m_i)$ 表示图像像素值 m_i 出现的概率,N 表示像素值的总数,对于具有 256 个灰度级的图像,其信息熵的理想理论值是 $H(m)=8$。选取 3 个 256×256 的图像进行实验,根据(12)式计算其密文图像的信息熵,如表 1 所示,均非常接近理论值 8,表明经本算法加密后发生图像信息泄露的概率极低。

Table 1 Information entropy of different images

	Lena. tiff	Baboon. tiff	Peppers. tiff
original image	7.4451	7.3583	7.5937
cipher image	7.9973	7.9972	7.9973

2.2.2 直方图分析 图像灰度直方图在图像分析中有重要作用,一种优秀的图像加密算法应具有强大抵御统计分析攻击的能力。图 5 中分别给出了 Lena 原始图像及其加密图像的直方图。明显可见,加密图像的直方图灰度值分布非常均匀,与原始图像的直方图差异明显,表明该算法能使统计分析攻击难以起作用。

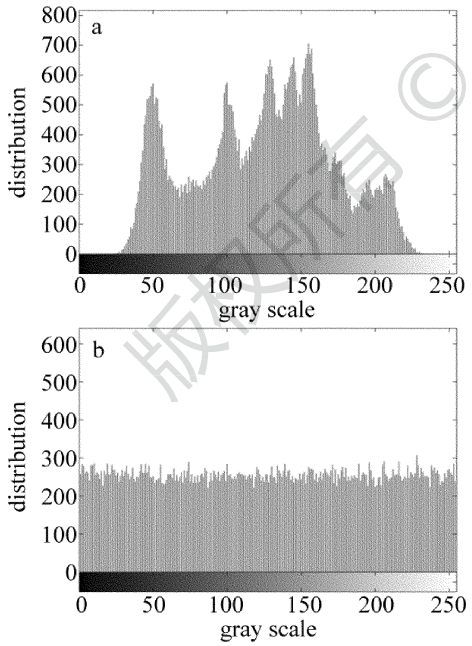

Fig. 5 Histogram analysis

a—the original Lena image b—the encrypted image

2.2.3 抗差分攻击能力分析 像素数目变化率(number of pixels change rate, NPCR)和归一化平均变化强度(unified average change intensity, UACI)是权衡算法抵御差分攻击的一个重要指标。NPCR 指随机改变某一个明文图像像素值后,密文图像像素值数目的变化率;UACI 表示明文图像中某个像素点灰度值发生改变后,加密图像像素值数目的变化程度,NPCR 和 UACI 的计算公式[15]如下:

$$N_{\mathrm{NPCR}} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\boldsymbol{D}(i,j)\times 100\% \tag{13}$$

$$U_{\mathrm{UACI}} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|\boldsymbol{C}_1(i,j)-\boldsymbol{C}_2(i,j)|}{255}\times 100\% \tag{14}$$

式中,$M\times N$ 为图像大小,假设两个明文图像中仅有一个像素点不同时,经加密后两者的密文图像中第(i,j)点的像素值分别是 $\boldsymbol{C}_1(i,j)$ 和 $\boldsymbol{C}_2(i,j)$,如果 $\boldsymbol{C}_1(i,j)=\boldsymbol{C}_2(i,j)$,则 $\boldsymbol{D}(i,j)=0$;如果 $\boldsymbol{C}_1(i,j)\neq\boldsymbol{C}_2(i,j)$,则 $\boldsymbol{D}(i,j)=1$,用数学公式表达为:

$$\boldsymbol{D}(i,j) = \begin{cases} 0, (\boldsymbol{C}_1(i,j) = \boldsymbol{C}_2(i,j)) \\ 1, (\boldsymbol{C}_1(i,j) \neq \boldsymbol{C}_2(i,j)) \end{cases} \tag{15}$$

NPCR 和 UACI 的理想期望值[16]分别为 99.609% 和 33.463%。选取 50 组 Lena 图像来测试,每组两张图像,一张为原始图像,另一张为原始图像随机选取一个像素并令其值加 1,对两幅图像分别加密,计算出 50 组的 NPCR 和 UACI 值,如图 6 所示,NPCR 和 UACI 的平均值高于理想期望值。另外,还对几个不同图像进行加密,并计算 50 组的 NPCR 和 UACI 的平均值,如表 2 所示,平均值均大于或接近理想期望值,表明本算法具有良好的抗差分攻击性能。

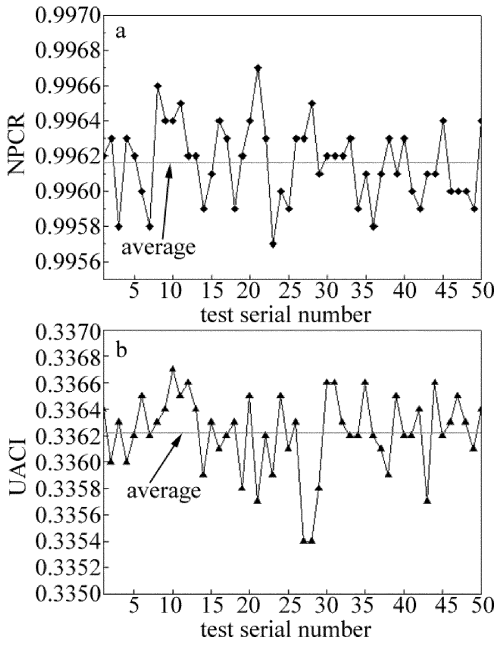

Fig. 6 a—NPCR b—UACI

Table 2 Average value of NPCR and UACI in different encrypted images

	Lena. tiff	Baboon. tiff	Peppers. tiff	Airplane. tiff
$\overline{N_{\mathrm{NPCR}}}$	0.9962	0.9961	0.9960	0.9961
$\overline{U_{\mathrm{UACI}}}$	0.3362	0.3349	0.3357	0.3351

2.2.4 相关性分析 在原始图像中,相邻像素相关系数很高,而加密图像相关系数应显著降低。为了检验原始图像和加密图像相邻像素间的相关性,选取若干图像进行测试,并分别从明文图像和密文图像的水平、垂直和对角 3 个方向中随机选取 $N=5000$ 个的相邻像素,根据以下几个式子计算:

期望值:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{16}$$

方差:

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)]^2 \tag{17}$$

协方差:

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x)][(y_i-E(y)] \tag{18}$$

相关系数:

$$\rho_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\cdot\sqrt{D(y)}} \tag{19}$$

式中,x 和 y 分别表示图像中两个相邻像素的灰度值,ρ_{xy}即为 2 个相邻像素的相关系数。图 7 是 Lena 原始图像与加密图像在 3 个方向的相关性图。可见该算法能使原始图像的统计特性很好地扩散到密文图像中。表 3 中列出了本算法和其它算法[17-18]对 Lena 图像仿真得到的相关系数值,经比较发现,本算法的密文图像相邻像素相关系数更小,即本算法在降低相邻像素间

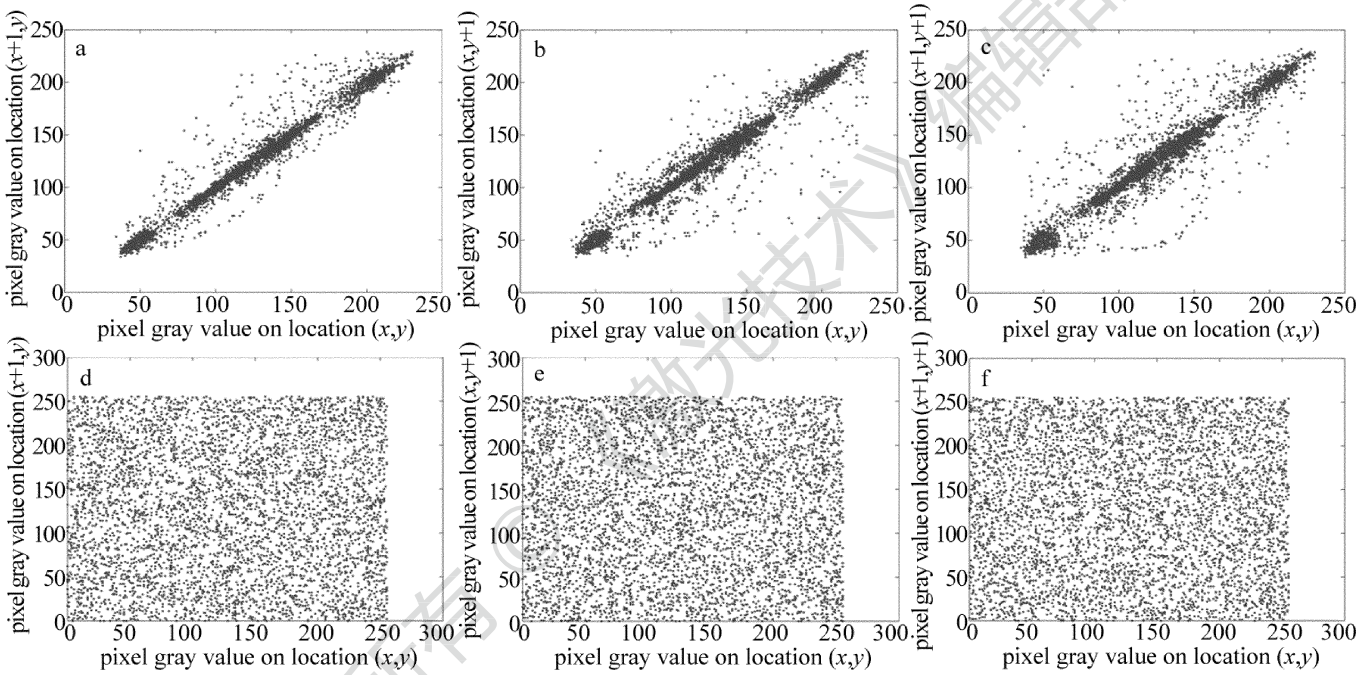

Fig. 7 Correlation between adjacent pixels of the original and encrypted image

a—horizontal of original image b—horizontal of encrypted image c—vertical of original image d—vertical of encrypted image e—diagonal direction of original image f—diagonal direction of encrypted image

Table 3 Comparison of the correlation coefficients between the algorithm with the adjacent pixels and the other algorithms

direction	original image	proposed algorithm	reference[17]	reference[18]
horizontal	0.9456	0.0054	0.0096	0.0192
vertical	0.9717	−0.0028	0.0172	−0.0108
diagonal	0.9318	-4.4027×10^{-4}	−0.0128	0.0056

相关性方面也具有一定优势,安全性更高。

2.2.5 抗裁剪攻击 在实际应用中,数字图像由于信号传输环境不理想而造成数据丢失。攻击者截获到密文图像后,可能会采取剪切、加噪等恶意攻击来破坏图像,因此探究密文图像在数据丢失后解密图像的效果有一定现实意义。为了模拟数字图像数据丢失的情景,本文中设计了抗裁剪攻击实验。以 256×256 标准图像为实验对象,图 8a 和图 8b 所示分别为对密文图像裁剪 0.39% 和 1.56%,图 8c 和图 8d 分别为对应的解密图像。可见,在不同比例的裁剪攻击下,本算法仍能还原出原图像的绝大部分信息,因此其具备一定的抗裁剪攻击性。

2.2.6 加密速度分析 优秀的图像加密算法需要有较高的加密效率以满足实时应用,比较本文中算法和近期几种算法对 256×256 的 Lena 图像的加密速度。本文中使用 MATLAB R2013a 软件平台来运行加密算法程序,计算机采用 Microsoft Windows 7 操作系统,实验硬件环境设备为 2.4GHz Intel(R) Core(TM) i3 CPU,2.0 RAM 和 300G 硬盘的笔记本电脑,采用本文中算法和算法分别对不同尺寸的 Lena 标准图像进行加密,各算法对不同尺寸图像的加密时间如表 4 所示。可见本算法在图像尺寸变大的情况下加密时间增加幅

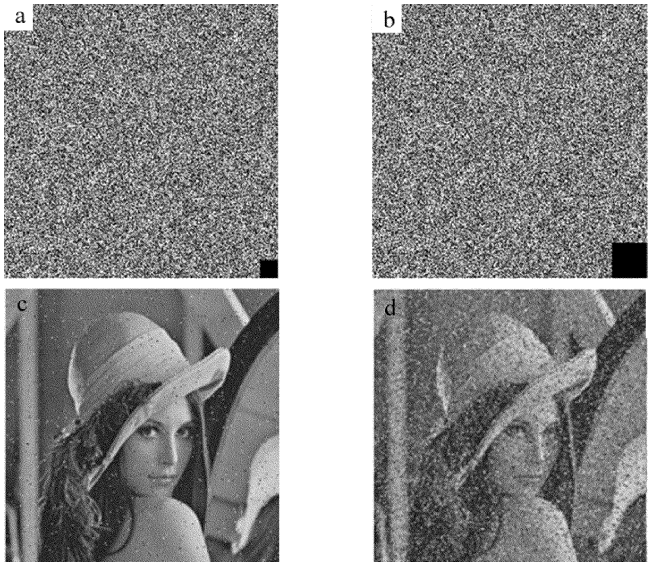

Fig. 8 Test of image cropping attacks

a—encrypted Lena image by 0.39% data cut b—encrypted Lena image by 1.56% data cut c—decrypted Lena image from Fig. 8a d—decrypted Lena image from Fig. 8b

Table 4 Comparison of the encryption time of different algorithms

image size	time/s		
	proposed	reference[17]	reference[19]
128×128	0.0423	0.2593	0.1835
128×256	0.0619	0.3271	0.2587
256×256	0.0817	0.6825	0.5256
512×512	0.1380	0.8527	0.7813

度最小,足见其具有加密效率更高的优势,符合实时加密要求,有效地解决了随图像尺寸变大而导致的加密时间迅速增加问题。

在置乱步骤中,令 $H=2^l$,当 l 取不同值时,用该算法分别对 256×256 和 512×512 的 Lena 图像执行一轮加密,图 9a 和图 9b 分别表示其加密时间随 l 的变

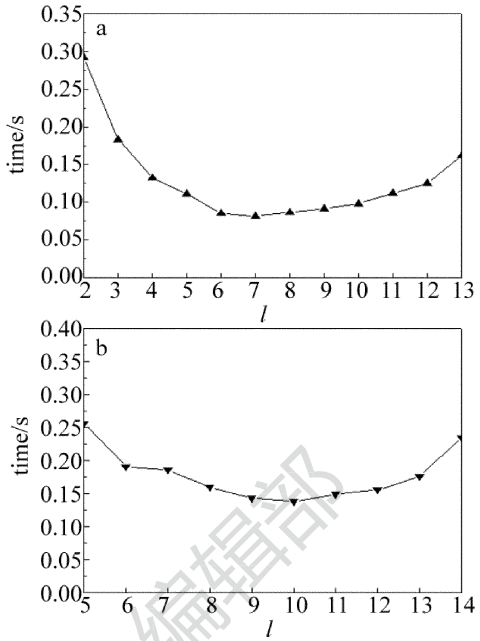

Fig. 9 Encryption time of two kinds of image

a—256×256 b—512×512

化,可见对两幅图像都有各自的加密时间最低点。图 9a 显示 $l=7$ 时,加密时间最短为 0.0817s;图 9b 显示 $l=10$ 时,加密时间最短为 0.1380s。经实验验证,该算法亦可运用于长宽不相等的图像,并获得良好效果。表 5 中列出了 l 取不同值时,该算法对 256×256 的 Lena 图像进行加密的各项参量,综合各项参量分析并且考虑快速加密的要求,$l=7$ 可达到最理想状态,即选取 $l=7$ 进行试验最为合适。本文中算法的一大优势在于加密者可根据图像大小,在像素置乱步骤适当选择 l 值,以 2^l 相邻像素为单位进行置乱,对不同 l 值加密完成后的加密图像参量进行综合分析,可确定最符合要求的加密时间,反映该算法也具有良好灵活性。

Table 5 Performance parameters for different l values

l	information entropy	NPCR	UACI	vertical	horizontal	diagonal	encryption speeds/s
2	7.9975	0.9962	0.3345	−0.0027	0.0050	8.9480×10^{-4}	0.2979
3	7.9975	0.9960	0.3344	0.0021	0.0013	0.0045	0.1964
4	7.9973	0.9965	0.3350	-0.9782×10^{-4}	0.0025	0.0026	0.1318
5	7.9973	0.9961	0.3342	−0.0048	−0.0023	−0.0027	0.1127
6	7.9968	0.9961	0.3351	0.0052	-9.5974×10^{-4}	0.0042	0.0828
7	7.9973	0.9962	0.3362	−0.0028	0.0054	-4.4027×10^{-4}	0.0817
8	7.9975	0.9962	0.3346	−0.0020	0.0037	1.3699×10^{-4}	0.0832
9	7.9970	09961	0.3345	1.9570×10^{-4}	0.0088	0.0048	0.0843
10	7.9964	0.9961	0.3342	0.0013	0.0028	−0.0040	0.0896
11	7.9970	0.9962	0.3353	5.3722×10^{-4}	−0.0079	0.0046	0.1097
12	7.9972	0.9962	0.3355	−0.0044	−0.0010	8.4257×10^{-4}	0.1295
13	7.9972	0.9963	0.3353	−0.0025	6.8750×10^{-4}	-9.7786×10^{-4}	0.1591

3 结 论

基于混沌映射和像素置乱与灰度值替代加密技术提出的快速图像加密算法,能有效解决随图像尺寸变大而导致的加密时间迅速增加问题。同时,运用 logistic 和 Arnold 映射的该图像加密算法具有灵活性高、加

密速度快、密钥敏感性强,且能有效抵抗差分攻击和统计攻击等特点。

参 考 文 献

[1] XU G X, XU Sh Q, GUO X J, *et al*. Image compression-encryption algorithm combined DCT transform with DNA operation[J]. Laser Technology, 2015,39(6):806-810 (in Chinese).

[2] ZHU C X, SUN K H. Encryption algorithm for a class of hyper chaotic image encryption algorithm and its improvement[J]. Acta Physica Sinica, 2012, 61(12):120503(in Chinese).

[3] WANG X Y, LIU L T, ZHANG Y Q. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics & Lasers in Engineering, 2015, 66(66):10-18.

[4] ZHANG W, YU H, ZHAO Z L, *et al*. Image encryption based on three-dimensional bit matrix permutation[J]. Signal Processing, 2016, 118(3): 36-50.

[5] ZHOU Y C, BAO L, CHEN P C L. A new 1-D chaotic system for image encryption[J]. Signal Processing, 2014, 97(7): 172-182.

[6] REN X K, MA Ch. Improvement and implementation of 3D color image encryption[J]. Microellectronics & Computer, 2015, 32(1): 96-99(in Chinese).

[7] 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, 2016, 77(15): 118-125.

[8] LI F Y, XU J F. Image encryption algorithm based on Hash function and multi chaotic system[J]. Computer Engineering and Design, 2010, 31(1): 141-144(in Chinese).

[9] ZHENG H Y, LI W J, XIAO D. Novel image blocking encryption algorithm based on spatiotemporal chaos system[J]. Journal of Computer Application, 2011, 31(11): 3053-3055(in Chinese).

[10] WANG Ch L, WU X J. Fractional order chaotic color image encryption algorithm based on block scrambling and diffusion[J]. Journal of Henan University(Natural Science Edition), 2014, 44(6): 715-724(in Chinese).

[11] LIU P, YAN Ch, HUANG X G. Improved generation method of chaotic spread spectrum sequence based on Logistic map[J]. Journal of Communication, 2007, 28(2):134-140(in Chinese).

[12] GU G S, LING J. A fast image encryption method by using chaotic 3-D cat maps[J]. Optik—International Journal for Light and Electron Optics, 2014, 124(17):4700-4705.

[13] WANG X Y, LIU L T, ZHANG Y Q. A novel chaotic block image encryption algorithm based on dynamic random growth technique[J]. Optics & Lasers in Engineering, 2015, 66(3):10-18.

[14] ZHAO J F, WANG S Y, CHANG Y X, *et al*. A novel image encryption scheme based on an improper fractional-order chaotic system[J]. Nonlinear Dynamics, 2015, 80(4):1721-1729.

[15] WU Y. NPCR and UACI randomness tests for image encryption[J]. Cyber Journals: Journal of Selected Areas in Telecommunications, 2011,4(1):1-8.

[16] PATIDAR V, PAREEK N K, SUD K K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2009,14 (7): 3056-3075.

[17] WANG X Y, WANG Q. A novel image encryption algorithm based on dynamic S-boxes constructed by chaos[J]. Nonlinear Dynamics, 2014, 75(3):567-576.

[18] LI L, WANG W N, LI J J. Security improvement for image encryption algorithm based on hyper-chaotic system[J]. Application Research of Computer, 2011, 28(11): 4335-4337(in Chinese).

[19] YE R S. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism [J]. Optics Communications, 2011, 284(22): 5290-5298.