基于变参混沌的异位异或图像加密算法

吕冬梅，李国东，王丽娟
（新疆财经大学 统计与数据科学学院，乌鲁木齐 830012）

摘要：目的 解决混沌序列的混沌性能退化，加密算法不能较好地抵御选择明文攻击等问题。**方法** 提出一种基于变参混沌系统，采用密文反馈的方式，对明文块依次加密的图像加密算法，并在扩散部分摒弃常规的按位异或扩散方式，提出一种按块异位异或算法。**结果** 对算法进行仿真的结果表明，文中算法对密钥敏感，测试对象的 NPCR 值分别为 99.59%，99.61%，99.61%，UACI 值分别为 33. 44%，33.46%，33.45%，信息熵分别为 7.9872，7.9989，7.9977，相较于其他类似算法，文中算法的综合效果更好，密钥空间为 $(10^{16})^6+10^{14}\times9$。**结论** 密文对明文敏感，能抵抗选择明文攻击，该算法不仅有效解决了问题，还具有较高的安全性能。

关键词：变参混沌系统；密文反馈；异位异或；图像加密
中图分类号：TP391 **文献标识码：**A **文章编号：**1001-3563(2019)17-0227-08
DOI：10.19554/j.cnki.1001-3563.2019.17.033

Ectopic XOR Image Encryption Algorithm Based on Variable Parameter Chaos

LYU Dong-mei, *LI Guo-dong*, *WANG Li-juan*
(School of Statistics and Data Science, Xinjiang University of Finance & Economics, Urumqi 830012, China)

ABSTRACT: The work aims to solve the problem of chaotic performance degradation of chaotic sequences as encryption algorithm cannot better resist the attacks of chosen plaintext. An image encryption algorithm based on variable parameters was proposed. The proposed algorithm used cipher feedback mode to encrypt the plaintext block sequentially. In the diffusion part, a conventional bitwise XOR diffusion method was abandoned, and a block-by-block ectopic XOR algorithm was proposed. The simulation results showed that, the proposed algorithm was sensitive to the key, and the NPCR values of the test subjects were respectively 99.59%, 99.61%, and 99.61%. UACI values were respectively 33.44%, 33.46% and 33.45%, and the information entropies were 7.9872, 7.9989 and 7.9977, respectively. Compared with other similar algorithms, the proposed algorithm had better comprehensive effects. The key space was $(10^{16})^6+10^{14}\times9$. The ciphertext is sensitive to plaintext, and can resist the chosen plaintext attacks. The proposed algorithm not only solves the problem effectively, but also has high security performance.

KEY WORDS: variable parameter chaotic system; ciphertext feedback; ectopic XOR; image encryption

随着互联网技术的迅猛发展，探索高效、安全的图像加密算法成为了研究的热点。近年来，应用混沌对图像进行加密的算法成为了学者们重点学习的课题之一，越来越多的混沌图像加密算法问世[1—6]，从大量文献[7—13]中总结出大部分算法会出现的几个缺陷分别是：混沌单一性使得破解难度降低，计算机有

收稿日期：2019-04-06
基金项目：国家自然科学基金（11461063）；自治区自然科学基金（2017D01A24）
作者简介：吕冬梅（1995—），女，新疆财经大学硕士生，主攻数据挖掘与图像处理。
通信作者：李国东（1972—），男，新疆财经大学教授，主要研究方向为数据挖掘与图像处理。

限数字精度的限制导致混沌序列的混沌性能退化；加密算法不能抵抗噪声、剪切及压缩的攻击；加密算法对明文的敏感度不高；加密算法不能抵御选择明文攻击等。对上述问题，学者们又设计了解决办法。徐潇、马峻等[14]提出了一种基于计算全息、Arnold 变换和混沌映射的三维信息分级加密方案，实现了三维信息的加密。程东升、谭旭等[15]基于四维超混沌系统，提出了一种位级图像加密算法，该算法对图像位平面进行行列循环移位置乱，并将置乱后的位面与 4 个混沌矩阵执行按位异或运算。但是在上述算法中，混沌单一性、混沌性能退化等问题均没有得到有效和针对性的解决，使得算法较容易被破解。沈超、王威威[16]设计了一个基于明文相关的超混沌图像加密算法，选取 Lorenz 超混沌和 Chen 超混沌系统产生密码序列，再将序列用于图像的置乱和扩散。汪乐乐、李国东[17]提出了一种改进的 H-L(Henon-Logistic)混沌图像加密算法，以游程性序列为基础，将改进的 H-L 系统产生的混沌序列应用于图像加密。上述算法有效解决了混沌单一性和加密算法对明文的敏感度不高的问题。程宁、王茜娟[18]为了解决当前光学图像加密技术没有考虑明文自身特性，抗明文攻击能力较低的问题，设计了基于混沌 Gyrator 变换与矩阵分解的非对称彩色图像加密算法，该算法在序列混沌性能退化等问题上没有给出改善措施。

对于混沌单一性问题，文中构建由广义 Henon 映射控制的新型三维变参超混沌系统，该系统每次迭代时使用的控制参数都由 Henon 映射所更新，不存在一个固定的混沌系统进行长期迭代的情况，如此便有效解决了计算机有限数字精度导致混沌性能退化这一问题。对于加密算法不能抵抗噪声、剪切及压缩攻击的问题，在加密算法中加入像素位置置乱算法便可有效解决这一问题。针对加密算法对明文的敏感度不高的问题，在算法中加入明文关联因素，使混沌系统产生序列的初始条件与明文图像相关。针对算法不能抵御选择明文攻击这一缺点，对明文进行分块，采用密文反馈的方式依次按块加密。在大量混沌图像加密算法中，对像素扩散部分采用按位异或方法，文中设计一种自定义分块异位异或的数值扩散算法。

1 基于变参混沌和异位异或算法的加密系统

1.1 变参混沌的设计

采用广义 Henon 映射更新三维离散混沌系统的参数，最终形成三维变参混沌系统。

广义 Henon 映射如下所示：

$$\begin{cases} x_1(i+1)=a_1-x_2(i)\cdot x_2(i)-b_1\cdot x_3(i) \\ x_2(i+1)=x_1(i) \\ x_3(i+1)=x_2(i) \end{cases} \tag{1}$$

式中，当 $0.54<a_1<2, 0<|b_1|<1$ 时，系统处于超混沌状态，具有 2 个正的李雅普诺夫指数，作为混沌系统一，对混沌系统二进行参数扰动。

新型三维离散混沌系统如下所示：

$$\begin{cases} y_1(i+1)=\sin\left(y_1(i)\right)\cdot\sin\left(y_2(i)\right)-a_2\sin\left(y_3(i)\right) \\ y_2(i+1)=b_2\sin\left(y_1(i)\right)\cdot\cos\left(y_2(i)\right)-y_1(i) \\ y_3(i+1)=c_2\cdot y_2(i)+\sin\left(y_3(i)\right) \end{cases} \tag{2}$$

当式中的参数 $a_2=4, b_2=2, c_2=1$ 时，此系统产生的是混沌序列。式（2）为混沌系统二，对式（2）进行 Matlab 仿真模拟，选择初始值 $y_1(0)=-2$, $y_2(0)=0.5, y_3(0)=1.3$，其相图见图 1。

用系统一来扰动系统二，构建三维变参混沌系统：

$$\begin{cases} y_1(i+1)=\sin\left(y_1(i)\right)\cdot\sin\left(y_2(i)\right)- \\ \qquad\left(a_2+d\cdot x_1(i)\right)\cdot\sin\left(y_3(i)\right) \\ y_2(i+1)=\left(b_2+d\cdot x_2(i)\right)\cdot\sin\left(y_1(i)\right)\cdot\cos\left(y_2(i)\right) \\ y_3(i+1)=\left(c_2+d\cdot x_3(i)\right)\cdot y_2(i) \end{cases} \tag{3}$$

式中：$-0.09\leqslant d\leqslant 0.09$。

选择初始值 $x_1(0)=0.2, x_2(0)=0.3, x_3(0)=0.5$，$y_1(0)=-2, y_2(0)=0.5, y_3(0)=1.3$，对变参混沌系统进行 Matlab 仿真模拟，其相图见图 2。

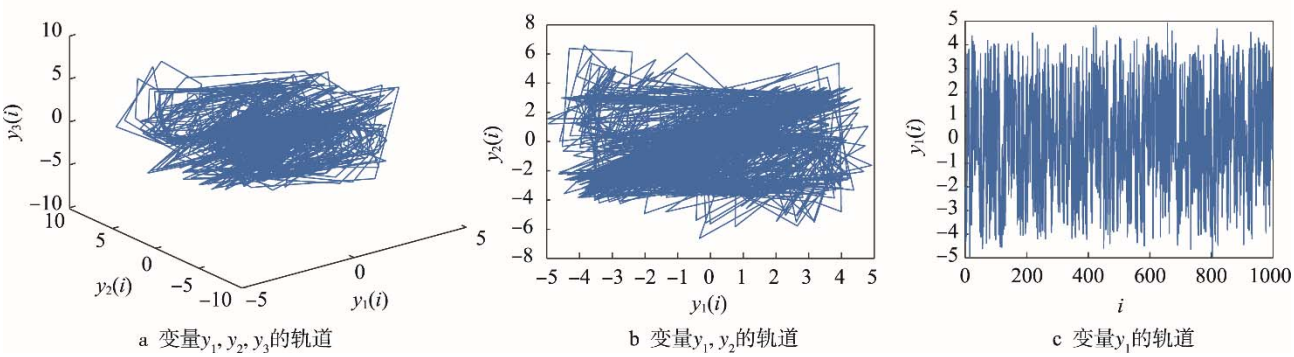


图 1 三维映射的混沌解轨道

Fig.1 Chaotic solution orbit of three-dimensional mapping

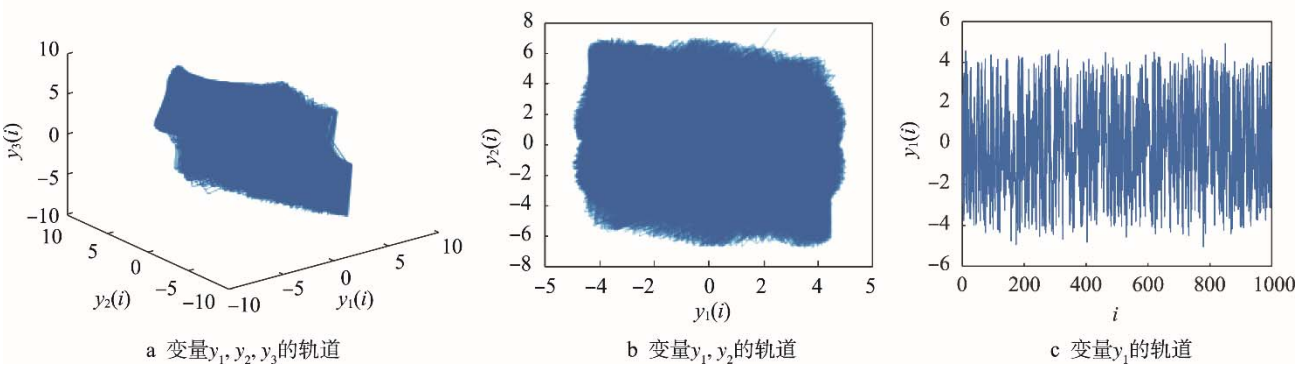


图 2　变参数映射的混沌解轨道

Fig.2 Chaotic solution orbit of variable parameter mapping

1.2　异位异或数值扩散算法的设计

摒弃一般的比特按位异或扩散算法，设计了一种自定义分块异位异或扩散算法：

$$\begin{cases} F_i(j,r)=C_i(j,r)\oplus E_i(j,l,k,q) \\ r=1,l=r-0,k=r-0,q=r+0 \\ r=2,l=r-1,k=r-1,q=r+1 \\ r=3,l=r-1,k=r-2,q=r+1 \\ r=4,l=r-2,k=r-3,q=r+3 \\ r=5,l=r-3,k=r-3,q=r-3 \\ r=6,l=r-3,k=r-3,q=r-1 \\ r=7,l=r-6,k=r-5,q=r-1 \\ r=8,l=r-7,k=r-6,q=r+0 \end{cases} \tag{4}$$

式中：$i=1,\cdots,\dfrac{mn}{64}$，$j=1,\cdots,64$，$r=1,\cdots,8$，$l,k,q$ 的取值随 r 值变化，其中 m 和 n 为图像尺寸；$C_i(j,r)$ 为 C_i 矩阵中第 j 个数的第 r 位；$E_i(j,l,k,q)$：锁定 E_i 矩阵组中第 j 个矩阵，第 l 行第 k 列个数的第 r 位。

1.3　加密算法

设计一个基于变参混沌系统、明文关联、密文反馈的图像加密算法，整体流程见图 3。

Step1：分块。

对尺寸为 $m\times n$ 的明文图像 A，依据从左到右、从上到下顺序进行分块，每个明文块尺寸为 8×8，明文块数量为 $(m/8)\times(n/8)$，将明文块转化为一维矩阵，并分别记为矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_{(m\times n/64)}$。

Step2：对矩阵 $\boldsymbol{A}_1$ 加密。

1）设计密钥矩阵。

设生成混沌序列的初始条件为：

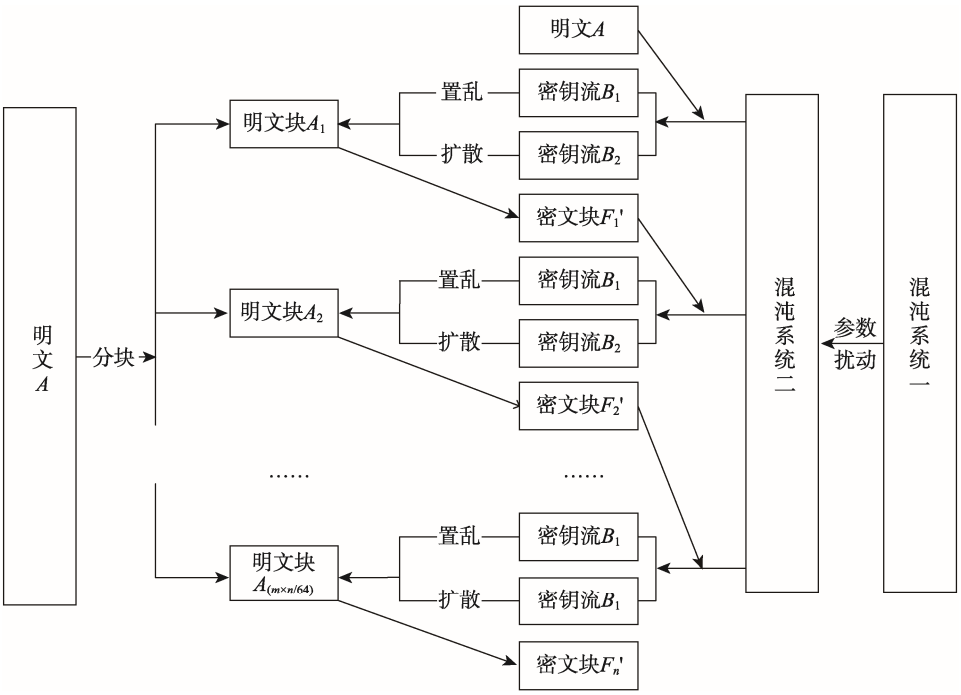


图 3　算法整体流程

Fig.3 Whole process of the algorithm

$$\boldsymbol{D}=[d,X(0),Y(0),N_1+64,N_2+256]$$

其中：d 为变参混沌系统中的控制参数；$X(0)$ 和 $Y(0)$ 为式（1）和（3）中变量初始值；N_1+64 和 N_2+256 为 2 组迭代次数（$X(0)$，$Y(0)$，N_1，N_2 均为密钥）。

为了使密文矩阵具有明文关联性，令：

$$d=\left(\mathrm{mod}(T,256)/256\right)/100+p_1 \tag{5}$$

其中：

$$T=\mathrm{sum}(\mathrm{sum}(A)) \tag{6}$$

p_1=0.03（p_1取值范围为$[-0.08,0.08]$，在文中作为一个密钥）。

将初始条件 $\boldsymbol{D}$ 与变参混沌系统相结合，对变参混沌系统迭代 N_1+64 次，舍弃前 N_1 项，取剩余序列存入数组 b_1，b_2，b_3。

由式（7）将三维数组 b_1，b_2，b_3 转化为长度为 64 的一维数组 B_1：

$$B_1=k_1b_1+k_2b_2b_3 \tag{7}$$

式中：

$$k_1=\sqrt{x_1(0)+x_2(0)+x_3(0)} \tag{8}$$

$$k_2=\sqrt{y_1(0)+p_2+y_3(0)} \tag{9}$$

其中，$p_2=\sqrt{5}$（p_2 可取任意正数，在文中作为一个密钥）。

对变参混沌系统迭代 N_2+256 次，舍弃前 N_2 项，取剩余序列存入数组 b_4，b_5，b_6。

由式（10）将三维数组 b_4，b_5，b_6 转化为长度为 256 的一维数组 B_2，并且其数值大小为 $[0,255]$ 上的整数：

$$B_2=\mathrm{mod}\left(\lceil k_3\times b_4\times b_5\times b_6\rceil\times 10^{14},256\right) \tag{10}$$

式中：$\lceil\bullet\rceil$ 表示去整运算，即保留小数点后的数。

$$k_3=\sqrt{x_1(0)+y_2(0)+y_3(0)} \tag{11}$$

2）矩阵 $\boldsymbol{A}_1$——像素置乱。

对 B_1 按降序排序，得其索引序列 S_1，依据序列 S_1 对 $\boldsymbol{A}_1$ 矩阵进行像素位置置乱，置乱结果记为 $\boldsymbol{C}_1$。即：

$$\boldsymbol{C}_1(j)=\boldsymbol{A}_1(S_1(j)),j=1,2,3,...,64 \tag{12}$$

3）矩阵 $\boldsymbol{C}_1$——像素扩散。

依据式（13）将 B_2 转化为尺寸为 2×128 的矩阵 $\boldsymbol{E}_1$：

$$\boldsymbol{E}_1=\mathrm{reshape}(B_2,2,128) \tag{13}$$

依据从左到右每 2 列组成一个矩阵块的规则，将 $\boldsymbol{E}_1$ 分成 64 块尺寸为 2×2 的块矩阵，即：

$$\boldsymbol{E}_1=\{\boldsymbol{E}_1(j),j=1,2,\cdots,64\}$$

对矩阵 $\boldsymbol{C}_1$ 根据按块异位异或扩散算法进行扩散，结果存入 $\boldsymbol{F}_1$ 中，按块异位异或示意见图 4。

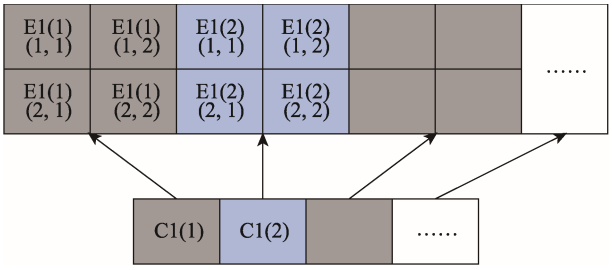


图 4 按块异位异或示意

Fig.4 Schematic diagram of block-by-block ectopic XOR

4）矩阵 $\boldsymbol{F}_1$——像素扩散。

将 $\boldsymbol{F}_1$ 中的每个数值根据不同的循环因子根据式（14）进行比特左循环移位，结果存入 $\boldsymbol{F}_1'$ 中。

$$\boldsymbol{F}_1'(j)=\mathrm{circshift}(F_1(j),q(j)) \tag{14}$$

循环因子：

$$q(j)=\mathrm{mod}(E_1(j),7)+1 \tag{15}$$

Step3：对矩阵 $\boldsymbol{A}_2,\cdots,\boldsymbol{A}_{(m\times n/64)}$ 加密。

利用密文反馈的方式对生成混沌序列的初始条件 $\boldsymbol{D}=[d,X(0),Y(0),N_1+64,N_2+256]$ 进行更新，即：

$$\begin{cases}T=\mathrm{sum}(\mathrm{sum}(F_1'))\\ d=\left(\mathrm{mod}(T,256)/256\right)/100+0.03,\\ x_1(0)=\mathrm{mod}(T,m)/m\\ x_2(0)=\mathrm{mod}(T,n)/n,\\ x_3(0)=\mathrm{mod}(T,256)/256\\ y_1(0)=\mathrm{rem}(-T,m)/m+2.5\\ y_2(0)=\mathrm{rem}(-T,n)/n+7.5\\ y_3(0)=\mathrm{rem}(T,256)/256\\ N_1=\mathrm{floor}(T/255)\\ N_2=\mathrm{ceil}(T/256)\end{cases} \tag{16}$$

根据 Step2 对矩阵 $\boldsymbol{A}_2$ 进行加密。

对 $\boldsymbol{A}_3$ 加密时，利用密文块矩阵 $\boldsymbol{F}_2'$ 更新初始条件 $\boldsymbol{D}$，并依次对剩余所有明文块矩阵进行加密。

Step4：合并。

将所有密文块矩阵重组为尺寸为 8×8 的矩阵，依据从左到右、从上到下拼接的方式拼接起来，得到最终加密矩阵 $\boldsymbol{W}$。

1.4 解密算法

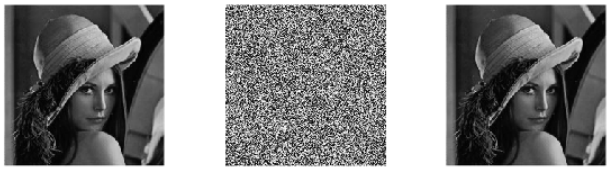
密文接收者首先将密文矩阵 $\boldsymbol{W}$ 按 8×8 大小分块，由式（16）可知密钥矩阵的产生条件 $\boldsymbol{D}$，得到密钥矩阵后依据加密的逆过程解密即可。

2 实验仿真

对算法进行仿真，测试对象为灰度图像 lena、飞机、电路板（分块时，若矩阵不能整分，可添 0 处理），加密的初始密钥集为：

$$\begin{cases} p_1=0.03,\ p_2=\sqrt{5},\ x_1(0)=0.0550,\ x_2(0)=0.0551 \\ x_3(0)=0.5117,\ y_1(0)=2.4451,\ y_2(0)=7.4452 \\ y_3(0)=0.5017,\ N_1=11224,\ N_2=12181 \end{cases}$$

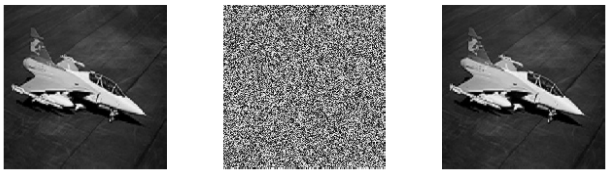
加密效果见图 5—7。



a 明文图像　b 密文图像　c 正确解密图像

图 5　lena 图像加密效果

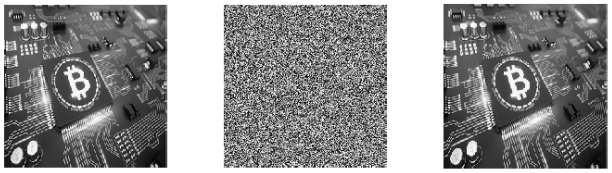
Fig.5 Lena image encryption effect



a 明文图像　b 密文图像　c 正确解密图像

图 6　飞机图像加密效果

Fig.6 Jet image encryption effect



a 明文图像　b 密文图像　c 正确解密图像

图 7　电路板图像加密效果

Fig.7 Circuit board image encryption effect

3　安全性分析

3.1　直方图分析

像素直方图可以表示像素点灰度值的分布状况。明、密文图像对应的像素直方图见图 8—10。由图 8—10 中 b 可知，已经无法从视觉上获得任何明文信息，加过加密后，像素值在 0~255 区间上均匀分布。

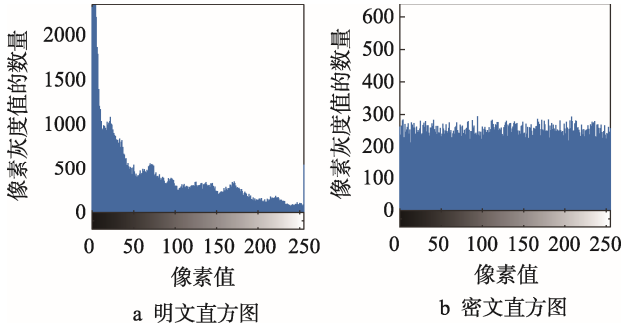


图 8　Lena 图像明-密文直方图

Fig.8 Histogram of plaintext-ciphertext in Lena image

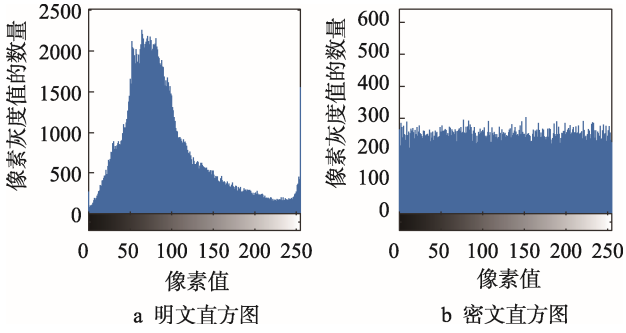


图 9　飞机图像明-密文直方图

Fig.9 Histogram of plaintext-ciphertext in aircraft image

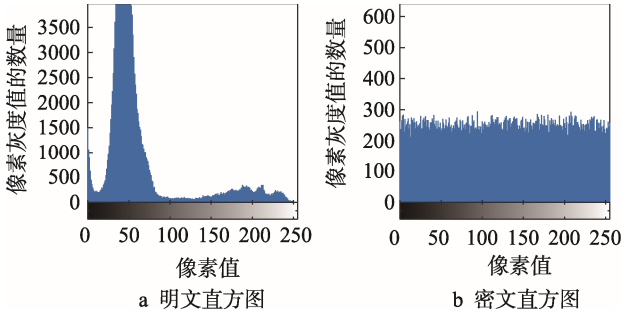


图 10　电路板图像明-密文直方图

Fig.10 Histogram of plaintext-ciphertext in circuit board image

3.2　相邻像素相关性

相邻像素相关性反映图像相邻位置像素值的相关程度。好的图像加密算法能够使相邻像素尽量达到零相关。从 Lena 明、密文图像中随机抽取 2000 对相邻的像素点，对比 Lena 明、密文图像在水平、垂直、对角线方向上的相邻像素相关性，见图 11。通过式（17）计算测试图像相邻像素间的相关系数，文献[16—18]的加密算法应用于测试图像后的相关系数测试结果见表 1。

$$\begin{cases} E(x)=\dfrac{1}{N}\sum_{i=1}^{N}x_i \\ D(x)=\dfrac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \\ \operatorname{cov}(x,y)=\dfrac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \\ \gamma_{xy}=\dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}} \end{cases} \tag{17}$$

从图 11a—c 可以看出，明文图像的像素点在 3 个方向上均分布集中在直线 $y=x$ 附近，相邻像素点间具有极高的相关性。从图 11d—f 可以看出，加密后图像像素点分布均匀，密文图像相邻像素间的相关性降低。

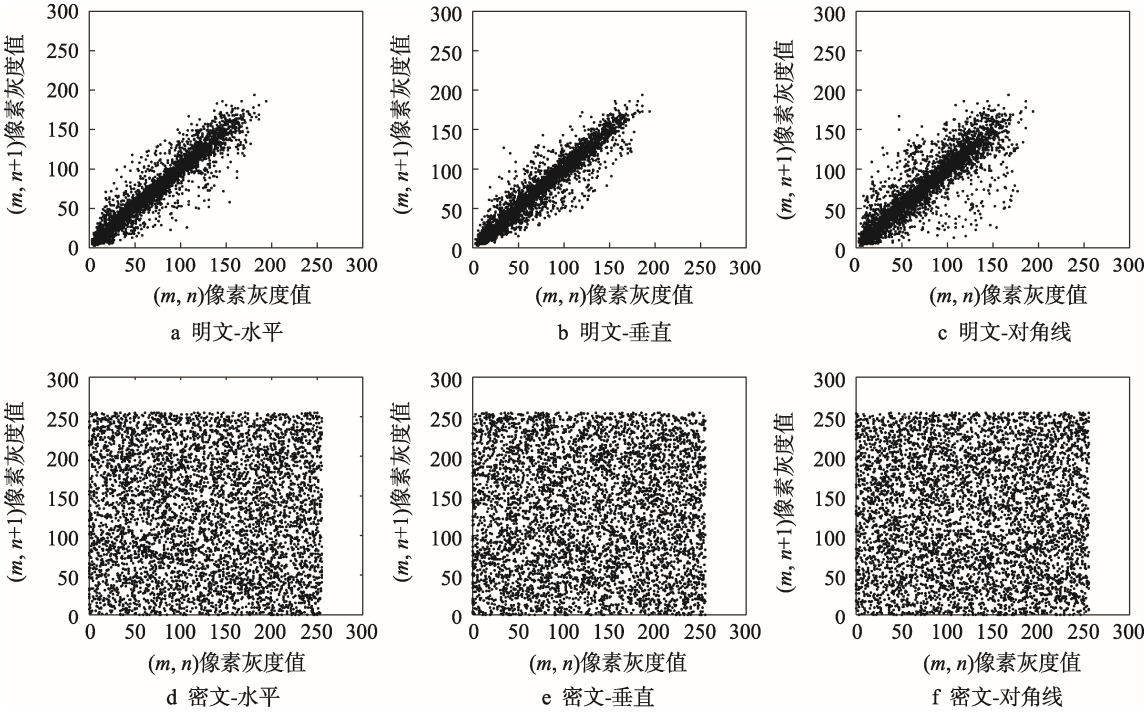


图 11　Lena 明-密文图像像素点相关性

Fig.11 Correlation of pixel points in Lena plaintext-ciphertext image

表 1　相邻像素相关系数测试结果

Tab.1 Test results of correlation coefficient of adjacent pixels

图像	方向	密文			
		文中	文献[16]	文献[17]	文献[18]
Lena	水平	0.0193	− 0.0243	0.0207	− 0.0170
	垂直	0.0197	− 0.0212	0.0225	− 0.0237
	对角	0.0025	0.0114	− 0.0170	0.0155
Jet	水平	− 0.0106	− 0.0418	0.0194	− 0.0031
	垂直	− 0.0023	0.0217	− 0.0106	− 0.0124
	对角	0.0018	− 0.0107	0.0203	0.0202
Circut Board	水平	0.0045	− 0.0064	− 0.0153	− 0.0143
	垂直	− 0.0107	0.0211	− 0.0118	− 0.0191
	对角	− 0.0031	0.0162	0.0171	0.0049

3.3　抗剪切攻击

置乱算法可达到抗剪切攻击的效果。如图 12 所示，对 Lena 图像进行 1/4 的剪切，若加密算法中不包含像素位置置乱，则解密效果见图 12b，剪切部分彻底消失。对经过文中加密算法加密后的 Lena 图像进行 1/4 的剪切，解密效果如图 12d，可以大致看出图像整体结构。

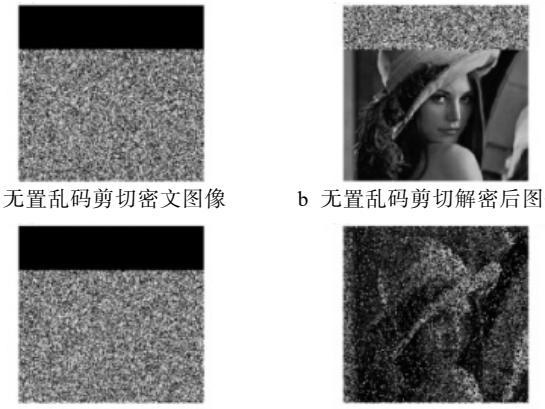
3.4　抗差分攻击分析

差分攻击的思路：对明文图像进行很小的改变，然后对改动前后的明文图像用同一个加密算法进行加密，对加密后结果进行对比，进而对算法进行破解。一般使用 NPCR（像素变化率）、UACI（平均改变强度）来评价算法抗差分攻击的性能。计算结果见表 2。其中 NPCR，UACI 计算公式分别为：

$$\mathrm{NPCR}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D_{ij}}{M\times N}\times 100\%,\quad D_{ij}=\begin{cases}1, x(i,j)\neq x'(i,j)\\ 0, x(i,j)=x'(i,j)\end{cases} \tag{18}$$

$$\mathrm{UACI}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{x(i,j)-x'(i,j)}{255}\right)}{M\times N}\times 100\% \tag{19}$$

对于一幅 256 级的图像，NPCR 和 UACI 的理想值为 99.6054%，33.4635%[17]。由表 2 可以看出，文中的测试结果与其他文献中的测试结果相比，更接近理论值，表明文中算法可以有效抵抗差分攻击。



a 无置乱码剪切密文图像　b 无置乱码剪切解密后图像

c 有置乱码剪切密文图像　d 有置乱码剪切解密后图像

图 12　有无置乱算法解密效果对比

Fig.12 Comparison of the decryption effect with/without the scrambling algorithm

3.5　信息熵分析

信息熵是对某一件事件的发生结果所含信息量的期望值。对于一个好的加密算法，密文图像的信息熵越接近 8 越好。常使用式（20）计算信息熵：

$$H=-\sum_{i=0}^{255}p(i)\log_2 p(i) \tag{20}$$

式中：$p(i)$表示灰度值 i 出现的概率。文中算法的信息熵计算结果见表 3。

从表 3 可以看出，密文图像的信息熵较其它文献相比，更接近理论值 8。可以认为文中算法能够有效改善像素点的随机性，并且能够抵抗信息熵攻击。

3.6　密钥空间

一个好的加密算法应该是有一个足够大的密钥空间，以抵抗穷举攻击。在文中加密算法中，初始密钥包 $x_1, x_2, x_3, y_1, y_2, y_3$ 的初始值，N_1，N_2，p_1，p_2，其中 p_1 的取值区间为 $[-0.08, 0.08]$，p_2 为任意正数，N_1，N_2 为正整数，当数据精度为 10^{16} 时，密钥空间可达到 $\left(10^{16}\right)^6+10^{14}\times 9$，远大于 2^{100} 次，足以抵抗穷举攻击。

表 2　明文敏感性测试结果

Tab.2 Test results of plaintext sensitivity

图片	文中		文献[16]		文献[17]		文献[18]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Lena	99.59	33.44	99.57	33.54	99.56	33.47	99.63	33.51
Jet	99.61	33.46	99.56	33.49	99.60	33.44	99.58	33.49
Circuit Board	99.61	33.45	99.60	33.45	99.59	33.49	99.62	33.46

表 3　信息熵测试结果

Tab.3 Test results of information entropy

图像	文中	文献[16]	文献[17]	文献[18]
Lena	7.9872	7.9864	7.9798	7.9773
Jet	7.9989	7.9966	7.9957	7.9821
Circuit Board	7.9977	7.9893	7.9874	7.9958

3.7　抵抗选择明文攻击

选择明文攻击指攻击者可以加密一定数量的明文，并得到相应的密文，以破解加密算法。在文中算法中，加密对象和加密系统所产生的置乱阶段的密钥流和扩散阶段的密钥流都有相关性，所以加密一些特殊的图像并不能得到目标密文的密钥流，因而文中的加密算法能抵抗选择明文攻击。

4　结语

文中算法有 2 个特点：设计了由 2 个混沌系统组成的变参混沌系统，对分块后的明文图像逐一用密文反馈的方式对所有明文块进行置乱和扩散加密，有效解决了基于混沌对图像进行加密的五大常见问题；在扩散部分，设计了一种按块异位异或算法。对多幅图像进行算法的实验仿真后，结果和安全性分析表明，该算法不仅有效解决了问题，还具有比其他优秀算法更高的安全性能。

参考文献：

[1] LI S, ZHENG X. Cryptanalysis of a Chaotic Image Encryption Method[C]//IEEE International Symposium on Circuits and Systems, 2002CISCAS'2002), EEE, 2002: 708—711.

[2] WANG Y, WONG K W, LIAO X, et al. A New Chaos-Based Fast Image Encryption Algorithm[J]. Applied Soft Computing, 2011, 11(1): 514—522.

[3] 刘泉, 李佩朗, 章明朝, 等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报, 2014, 36(6): 1271—1277.
LIU Quan, LI Pei-lang, ZHANG Ming-chao, et al. Image Encryption Algorithm Based on Markov Segmentation Chaotic System[J]. Journal of Electronics &

Information Technology, 2014, 36(6): 1271—1277.

[4] 文小爽, 朱凯歌. 基于置乱与扩散的彩色图像加密算法[J]. 软件导刊, 2018, 17(10): 81—84.
WEN Xiao-shuang, ZHU Kai-ge. Color Image Encryption Algorithm Based on Scrambling and Diffusion[J]. Software Guide, 2018, 17(10): 81—84.

[5] 张顺, 高铁杠. 基于类 DNA 编码分组与替换的加密方案[J]. 电子与信息学报, 2015, 37(1): 150—157.
ZHANG Shun, GAO Tie-gang. Encryption Scheme Based on Class of DNA Encoding Grouping and Substitution[J]. Journal of Electronics & Information Technology, 2015, 37(1): 150—157.

[6] 文昌辞, 王沁, 黄付敏, 等. 基于仿射和复合混沌的图像自适应加密算法[J]. 通信学报, 2012, 33(11): 119—127.
WEN Chang-ci, WANG Qin, HUANG Fu-min, et al. Image Adaptive Encryption Algorithm Based on Affine and Compound Chaos[J]. Journal of Communications, 2012, 33(11): 119—127.

[7] 李树钧. 数字化混沌密码的分析与设计[D]. 西安: 西安交通大学, 2003.
LI Shu-jun. Analysis and Design of Digital Chaotic Ciphers[D]. Xi'an: Xi'an Jiaotong University, 2003.

[8] 朱淑芹, 李俊青. 参数扰动下的混沌的图像加密方案[J]. 计算机科学, 2017, 44(S1): 356—360.
ZHU Shu-qin, LI Jun-qing. Image Encryption Scheme of Chaos under Parameter Disturbance[J]. Computer Science, 2017, 44(S1): 356—360.

[9] 汪乐乐, 李国东. 基于分数阶 Fourier 的双混沌加密算法[J]. 计算机科学, 2018, 45(S2): 393—397.
WANG Le-le, LI Guo-dong. Double Chaotic Encryption Algorithm Based on Fractional Fourier[J]. Computer Science, 2018, 45(S2): 393—397.

[10] 王鲜芳, 王晓雷, 王俊美, 等. 一种动态猫映射混沌图像加密算法[J]. 河南师范大学学报(自然科学版), 2018, 46(5): 110—117.
WANG Xian-fang, WANG Xiao-lei, WANG Jun-mei, et al. A Dynamic Cat Mapping Chaotic Image Encryption Algorithm[J]. Journal of Henan Normal University(Natural Science), 2018, 46(5): 110—117.

[11] 马婷, 高大鹏, 王欣. 基于 Logistic 混沌加密的 NSCT-SVD 抖动调制盲水印算法[J]. 包装工程, 2016, 37(5): 156—160.
MA Ting, GAO Da-peng, WANG Xin. Jitter Modulation Blind Watermarking Algorithm Based on Logistic Chaotic Encryption NSCT-SVD[J]. Packaging Engineering, 2016, 37(5): 156—160.

[12] 郭静博. 基于物理随机位生成器与混沌像素交叉互换的图像加密算法[J]. 包装工程, 2018, 39(13): 222—232.
GUO Jing-bo. Image Encryption Algorithm Based on Cross-Interchange of Physical Random Bit Generator and Chaotic Pixels[J]. Packaging Engineering, 2018, 39(13): 222—232.

[13] 石坤泉, 魏文国, 杨震伦. 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[J]. 包装工程, 2018, 39(13): 199—207.
SHI Kun-quan, WEI Wen-guo, YANG Zhen-lun. Fast Image Encryption Algorithm Based on Weighted Histogram Bit Confusion and Stepped Chaotic Heterodiffusion[J]. Packaging Engineering, 2018, 39(13): 199—207.

[14] 徐潇, 马峻, 莫凡珣, 等. 基于计算全息和 Arnold-混沌技术的三维信息分级加密[J]. 激光杂志, 2018, 39(11): 66—70.
XU Xiao, MA Jun, MO Fan-xun, et al. Three-dimensional Information Hierarchical Encryption Based on Computational Holography and Arnold-chaos Technology[J]. Laser Journal, 2018, 39(11): 66—70.

[15] 程东升, 谭旭, 许志良, 等. 结合四维超混沌系统和位分解的图像加密算法研究[J]. 电子科技大学学报, 2018, 47(6): 906—912.
CHENG Dong-sheng, TAN Xu, XU Zhi-liang, et al. Study on Image Encryption Algorithm Combined with Four-Dimensional Hyperchaotic System and Bit Decomposition[J]. Journal of University of Electronic Science and Technology of China, 2018, 47(6): 906—912.

[16] 沈超, 王威威. 一种基于明文关联的超混沌图像加密算法的设计[J]. 现代计算机(专业版), 2018(36): 55—57.
SHEN Chao, WANG Wei-wei. Design of a Hyperchaotic Image Encryption Algorithm Based on Plaintext Correlation[J]. Modern Computer (Professional Edition), 2018(36): 55—57.

[17] 汪乐乐, 李国东. 基于游程性序列的双重混沌的图像加密算法[J]. 计算机科学, 2018, 45(S2): 361—366.
WANG Le-le, LI Guo-dong. Image Encryption Algorithm Based on Double Sequence Chaos of Run-length Sequences[J]. Computer Science, 2018, 45(S2): 361—366.

[18] 程宁, 王茜娟. 基于混沌 Gyrator 变换与矩阵分解的光学图像加密算法[J]. 电子测量与仪器学报, 2019, 33(1): 191—202.
CHENG Ning, WANG Xi-juan. Optical Image Encryption Algorithm Based on Chaotic Gyrator Transform and Matrix Decomposition[J]. Journal of Electronic Measurement and Instrument, 2019, 33(1): 191—202.