基于L-R混沌系统和双重扩散的图像加密算法*

费 敏，李国东†
(新疆财经大学 统计与数据科学学院，新疆 乌鲁木齐 830021)

摘 要： 为解决加密算法中的密码只受密钥控制、与明文无关，并且加密使用的混沌系统较为单一而容易被攻击破解、安全性差等问题，提出一种密钥与明文紧密相关联的双重扩散图像加密方案. 将密钥分为两级，初始密钥代入超Lorenz混沌系统迭代生成混沌序列，运用混沌序列从明文图像中选像素点；为了提升加密效率，对已有的运算规则进行改进，将改进后的运算方式生成第二级密钥，代入Rossler混沌映射生成混沌序列用于加密，对明文按照“正向扩散-动态约瑟夫置乱-逆向扩散”的顺序实现加密. 通过实验仿真，可以证明该算法具有抗统计和差分攻击能力，密钥空间足够的大，加密效率和安全性都很高，能够相当好的将图像信息隐藏，在信息安全方面有非常大的实际意义和应用价值.

关键词： 双向扩散；超Lorenz混沌；Rossler混沌；明文；约瑟夫置乱
DOI： 10.13568/j.cnki.651094.651316. 2020.12.09.0001
中图分类号： TP309 **文献标识码：** A **文章编号：** 2096-7675(2021)03-0290-010
引文格式： 费敏, 李国东. 基于L-R混沌系统和双重扩散的图像加密算法[J]. 新疆大学学报(自然科学版)(中英文), 2021, 38(3): 290-299+333.
英文引文格式： FEI M, LI G D. Image encryption algorithm based on L-R chaotic system and double diffusion[J]. Journal of Xinjiang University(Natural Science Edition in Chinese and English), 2021, 38(3): 290-299+333.

Image Encryption Algorithm based on L-R Chaotic System and Double Diffusion

FEI Min, LI Guodong

(*College of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi Xinjiang 830021 China*)

Abstract： In order to solve the problems that the cipher in the encryption algorithm is only controlled by the key and has nothing to do with the plaintext and the chaotic system used in encryption is relatively simple, so it is easy to be attacked and cracked and the security is poor, a double diffusion image encryption scheme with key and plaintext is proposed. The key is divided into two levels. The initial key is substituted into the super Lorenz chaotic system to generate the chaotic sequence iteratively. The chaotic sequence is used to select the pixels from the plaintext image. In order to improve the encryption efficiency, the existing operation rules are improved. The second level key is generated by the improved operation method, which is substituted into the Rossler chaotic map to generate the chaotic sequence for encryption. The encryption is realized in the order of ”dynamic scrambling reverse diffusion”. Through the experimental simulation, it can be proved that the algorithm has the ability to resist statistical and differential attacks, the key space is large enough, the encryption efficiency and security are very high, it can well hide the image information, and has great practical significance and application value in information security.

Key words： bidirectional diffusion; hyperchaos; chaos; plaintext; Josephus scrambling

0 引 言

图像中包含的数据跟文本信息有很大区别，主要在于包含的数据量较为丰富且冗余度高. 现如今，海量的文本、图片、音频以及视频在网络上传送，这些文件隐秘安全的传送引起学者们的重视. 设计既安全又高效的加密算法是一项具有重大现实意义的研究课题，这关系到国家信息安全和人们隐私的安全. 混沌因其具有很强

* **收稿日期：** 2020-12-09
基金项目： 国家自然科学基金项目（11461063）；新疆维吾尔自治区自然科学基金项目（2017D01A24）；新疆财经大学基金项目（2019XTD002）.
作者简介： 费敏（1995-），女，硕士生，主要从事混沌图像加密的研究，E-mail: 1522478017@qq.com.
† **通讯作者：** 李国东（1976-），男，博士，教授，主要从事混沌保密通讯的研究.

的初值敏感性、有界和拓扑传递性、分岔和长期不可预测性、分数维特性以及内在随机性等特点，常用于图像加密.

马聪等[1]利用两个以上的混沌系统对明文做两次置乱扩散达到加密的目的，创新点在于对位级和像素级图像都进行了加密，加密步骤紧密相关，还加入了Hilbert置乱，该算法解决了加密时选用混沌系统结构单一的问题，能非常好地隐藏明文图像信息. 王瑶等[2]为了解决当前加密方案使用单向扩散导致抗破译性能较弱的问题，将非线性S盒与双向扩散相结合设计一种密钥与明文相关的图像加密算法，不仅可以将图像内容高度隐藏，而且高效安全. 牛莹等[3]运用改进的约瑟夫对图像置乱，运用DNA动态编码对图像扩散，还加入了密文反馈机制完成图像无损加密，算法创新点在于密钥、加密算法与明文紧密关联，能够抗数据丢失攻击，在密文信息被拦截攻击破坏时具有恢复能力，有效提高了算法的安全性，但是算法使用的混沌系统结构较为单一.

本文针对混沌系统结构相对单一，密钥、部分加密算法与明文无关，使用单向扩散导致加密算法安全性不高等问题，给出一种“双向扩散置乱”加密结构、密钥与明文关联的图像加密方案. 其大致框架：首先，对超Lorenz混沌系统迭代生成混沌序列并对其预处理，从明文中选择部分像素点，并与选出的部分明文像素点运算共同产生第二级密钥；其次，利用三维Rossler混沌和第二级密钥生成加密需要的密码；最后，使用密码和三维Rossler映射对图像进行正-逆向扩散和置乱. 仿真实验表明该算法在保证具有更高安全性的同时提升了加密效率.

1　混沌理论和约瑟夫问题

1.1　超Lorenz混沌[4]

超Lorenz混沌的动力学方程为

$$\begin{cases} \dot{x}=a(y-x)+w \\ \dot{y}=cx-y-xz \\ \dot{z}=xy-bz \\ \dot{w}=-yz+rw \end{cases} \tag{1}$$

当参数$a=10, b=\frac{8}{3}, c=28, -1.52\leq r\leq -0.06$时，式（1）是超混沌的. 当$r=-1$时，混沌系统的4个李雅普诺夫指数分别为：$\lambda_1=0.338\ 1, \lambda_2=0.158\ 6, \lambda_3=0, \lambda_4=-15.175\ 2$，系统状态初始值$\{x_0, y_0, z_0, w_0\}$的取值范围分别是：$x_0\in(-40,40), y_0\in(-40,40), z_0\in(1,81), w_0\in(-250,250)$. 根据式（1），图1展示了进行20 000次迭代的混沌吸引子[5,7].

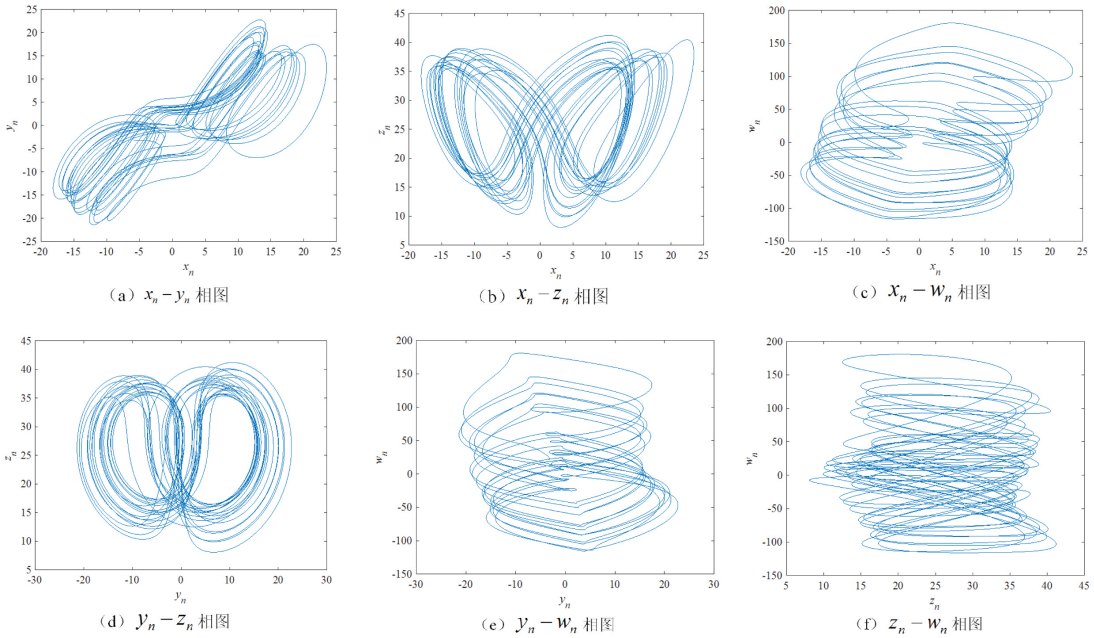


图 1　超混沌Lorenz系统相图

Fig 1　Phase diagram of hyperchaotic system

1.2 Rossler混沌

Rossler混沌系统最早在1976年被挖掘[8−13]，将Rossler映射用在图像加密中. Rossler混沌方程组为

$$\begin{cases} \dot{x}=-(y+z) \\ \dot{y}=x+ay \\ \dot{z}=b+z(x-c) \end{cases} \tag{2}$$

式（2）中：x,y,z为系统变量，a,b,c为系统参数；当$a=0.2,b=0.2,c=5.7$时，系统是混沌的，系统的复杂程度与参数a的取值呈正比. 对超Lorenz混沌系统迭代生成序列，做预处理后作为方程组（2）的初始值，图2展示了迭代系统200 000次产生的混沌吸引子.

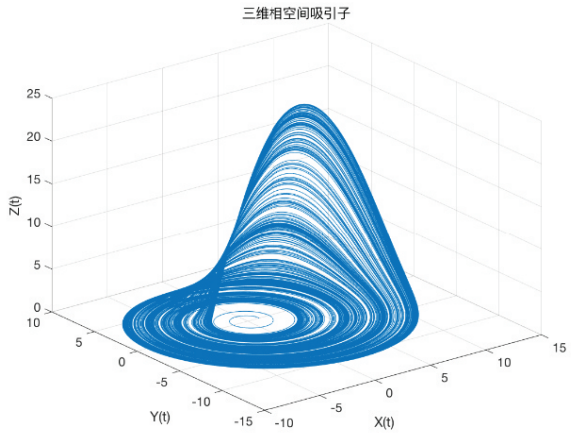


图 2 L-R混沌系统奇异吸引子

Fig 2 Singular attractor of L-R chaotic system

1.3 约瑟夫环问题的基本描述

这是一个循环遍历问题，编号为$1,2,\cdots,n$的人按照顺时针方向围着一张圆桌坐在其周围，给定一个长度m，从编号为1的报数，到m的那个出局；从它的下一个继续从1报数，到m的那个继续出局；按照这个过程开始循环，循环到最后一个出局[12]. 将这一过程用函数表达，即$f(n,m)$. 其中：n为元素总数，m为步长. 具体的例子，函数$f(9,3)$的解法是将$1,2,3,4,5,6,7,8,9$这些元素围成圈，按顺时针方向循环遍历并且删除第3个元素，被删除的元素顺序为$3,6,9,4,8,5,2,7,1$. 郭毅等[12]将约瑟夫函数拓展为$f(n,m,r,D,g)$，其中：参数r为起点，D为循环方向，g为间隔[13].

2 L-R双混沌系统的图像加密算法

2.1 加密流程

加密方案主要分成3个步骤：（1）正向扩散；（2）动态约瑟夫置乱；（3）逆向扩散. 图3给出了加密流程.

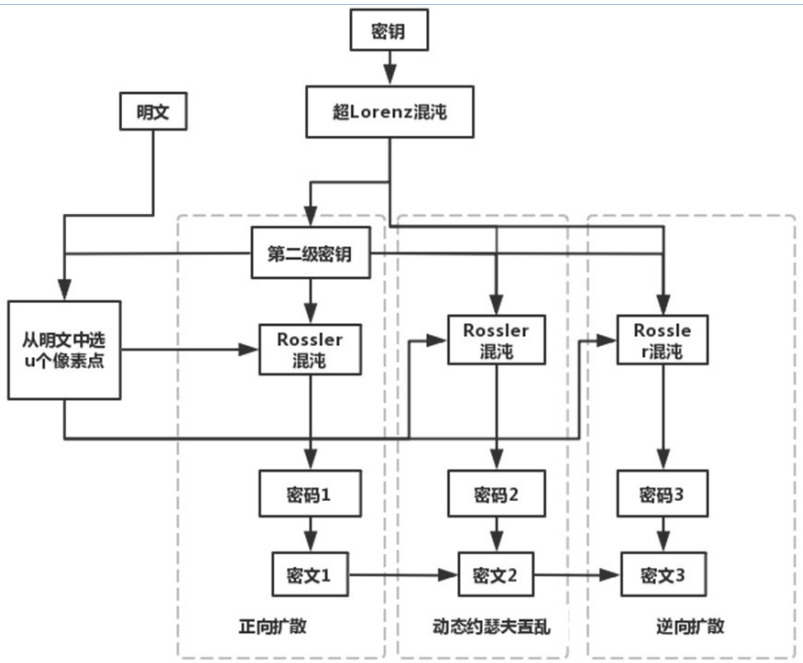


图 3 图像加密流程

Fig 3 Image encryption process

2.2　加密具体步骤

首先，通过初始密钥K来迭代超Lorenz混沌，运用产生的混沌序列通过给定的筛选规则从明文选出一部分像素点，用数学归纳法对前人的运算规则进行改进，运用改进后的运算规则和部分像素值运算，可得4条序列，将这4条序列做简单运算作为第二级密钥$\{x_0,y_0,z_0\}$；代入三维Rossler映射迭代得到3个混沌序列，其次按设定好的运算规则将其转化为整数序列，用来达到“双扩散-置乱”加密的目的，详细步骤如下：

步骤1 首先读图，将大小记为$m=M\times N$，其次，按从左到右再从上至下的扫描顺序扫描明文图像展开为一维向量，记做$I=\{I_i\,|i=1,2,\cdots,m\}$.

步骤2 将初始密钥$K=\{xL_0,yL_0,zL_0,wL_0\}$和系统参数值$\{a=10,b=8/3,c=28,r=-1\}$作为超混沌Lorenz映射的初始值和参数. 使用四阶龙格库-塔法进行迭代式（1）$r_1+r_2+2\ 000$次跳过映射的过渡态；再迭代u次，得到4个序列，记为$ua,ub,uc,ud,\{ua_i,ub_i,uc_i,ud_i\,|i=1,2,\cdots,u\}$，其次通过式（3）将序列$ua,ub,uc,ud$整数化，得到4个一维向量，记做$ux,uy,uz,uw$，即$ux,uy,uz,uw,\{ux_i,uy_i,uz_i,uw_i\,|i=1,2,\cdots,u\}$. 最后，继续迭代$M\times N$次，得到4个序列，记做$sx,sy,sz,sw,\{sx_i,sy_i,sz_i,sw_i\,|i=1,2,\cdots,M\times N\}$.

$$\begin{aligned}
ux_i&=floor((ua_i\times 100-floor(ua_i\times 100))\times 10^{10})\bmod (M\times N/4)\\
uy_i&=floor((ub_i\times 100-floor(ub_i\times 100))\times 10^{9})\bmod (M\times N/4)\\
uz_i&=floor((uc_i\times 100-floor(uc_i\times 100))\times 10^{8})\bmod (M\times N/4)\\
uw_i&=floor((ud_i\times 100-floor(ud_i\times 100))\times 10^{7})\bmod (M\times N/4)
\end{aligned}\tag{3}$$

步骤3 运用序列ux,uy,uz,uw和式（4）的运算规则从向量I中选择部分像素点放在PU中，即PU是一个$1\times u$的向量.

$$PU(1,i)=I(1,ux(i)+uy(i)+uz(i)+uw(i)),\ i=1,2,\cdots,u\tag{4}$$

如果一维向量PU与混沌序列sx,sy,sz,sw用文献[6]“逐次相加取模运算”的计算规则，会增加加密所需要的时间；以序列sx和矩阵PU为例，其过程如图4所示.

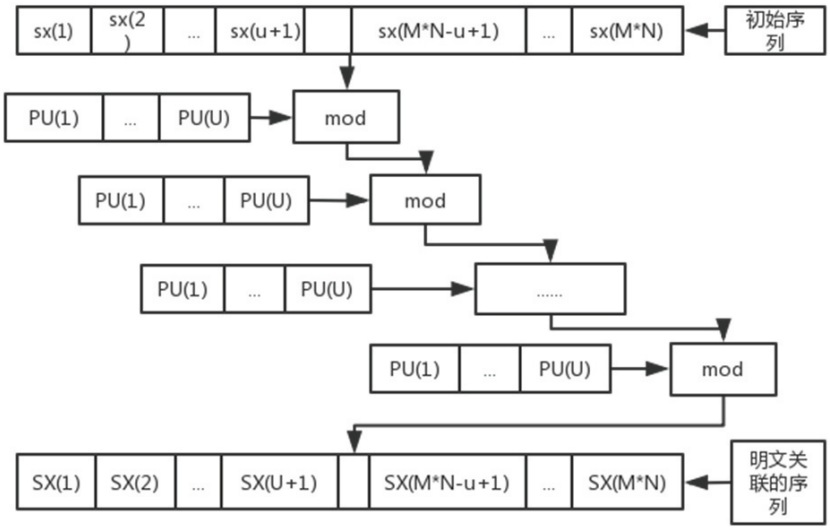


图 4　所筛选像素与原始序列运算规则

Fig 4　Operation rules of filtered pixels and original sequence

现对文献[6]中规则进行改进，先详细分析运算规则可得结论：因PU的大小已固定且小于序列sx的大小，则$i\in[1,u-1]$，序列中第i个元素与PU的前i个元素集合对应；在$i\in[u,M\times N-u+1]$，序列中第i个元素与PU的u个元素集合对应；在$i\in[M\times N-u+2,M\times N]$，序列中第$i$个元素与$PU$的后$M\times N-i+1$个元素集合对应，图5为详细过程. 具体改进方法如下：先算原始混沌序列中每一元素对应的明文像素点的值的总和，得到一条长为$M\times N$的序列，具体过程由图6给出；其次对该序列和原始混沌序列做加法和取模运算得到新混沌序列. 改进后能提升加密效率.

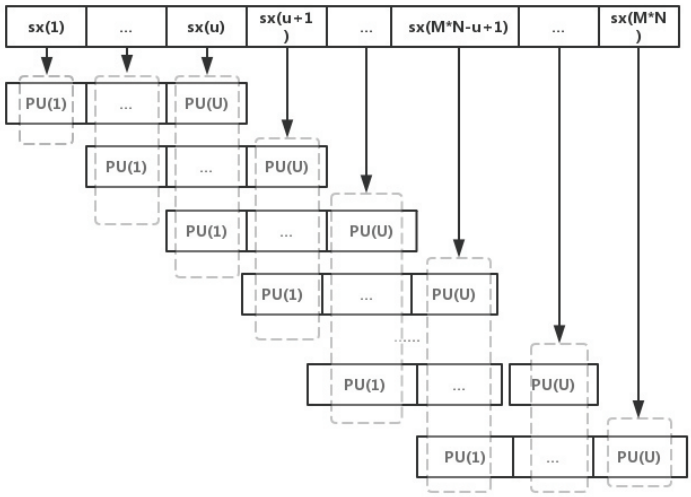


图 5 筛选像素与混沌序列的对应规则

Fig 5 Corresponding rules of filtering pixels and chaotic sequences

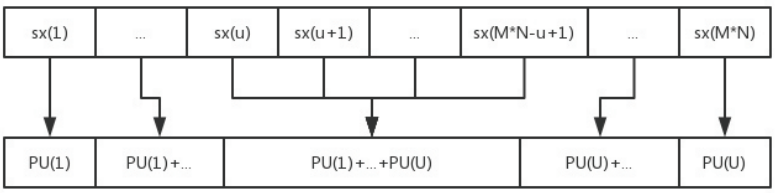


图 6 混沌序列与筛选像素和的对应规则

Fig 6 Corresponding rules of chaotic sequence and filtered pixel sum

步骤4 借助式(5)分别计算序列sx每一个元素对应明文像素点集合的和值，得到$M\times N$的一维向量，记为$px, px=\{px_i\,|i=1,2,\cdots,M\times N\}$.

$$\begin{aligned} px_i &= \mathrm{sum}(PU(1,1toi)), i\in[1,u-1] \\ px_i &= \mathrm{sum}(PU(1,1toi)), i\in[u,M\times N-u+1] \\ px_i &= \mathrm{sum}(PU(1,u-(M\times N-i+1)+1tou)), i\in[M\times N-u+2,M\times N] \end{aligned} \tag{5}$$

步骤5 重复步骤4三次，计算出序列sy,sz,sw对应的一维向量py,pz,pw.

步骤6 借助式(6)将序列sx,sy,sz,sw和px,py,pz,pw进行加法和取模运算，得到跟明文有关的序列，记做psx, $psy,psz,psw,\{psx_i\ ,psy_i,psz_i,psw_i,|i=1,2,\cdots,M\times N\}$，将其进行简单相加运算得到三条序列$\{psx_i,+psy_i\ psy_i+psz_i,psz_i+psw_i\,|i=1,\cdots,M\times N\}$作为三维Rossler混沌的初始值.

$$\begin{aligned} psx_i &= (px_i+sx_i)\bmod 1 \\ psy_i &= (py_i+sy_i)\bmod 1 \\ psz_i &= (pz_i+sz_i)\bmod 1 \\ psw_i &= (pw_i+sw_i)\bmod 1 \end{aligned} \tag{6}$$

步骤7 将三维Rossler映射初始值和系统参数$a=0.2,b=0.2,c=5.7$代入式(2)，迭代步长为0.002，迭代次数为$M\times N$，得到3个一维向量，记做$x_i,y_i,z_i,\{x_i,y_i,z_i\,|i=1,2,\cdots,M\times N\}$. 其次通过式(7)将三条序列整数化，生成三条序列，记为$X,Y,Z,\{X_i,Y_i,Z_i\,|i=1,2,\cdots,M\times N\}$.

$$X(i,j)=(floor(((x_{(i-1)\times N+j}+500)\bmod 1)\times 10^{13})\bmod M)+1Y(i,j)=(floor(((y_{(i-1)\times N+j}+500)\bmod 1)\times 10^{13})$$
$$\bmod M)+1Z(i,j)=(floor(((z_{(i-1)\times N+j}+500)\bmod 1)\times 10^{13})\bmod N)+1 \tag{7}$$

其中：$i=1,2,\cdots,M,j=1,2,\cdots,N$.

步骤8 将序列X作为加密向量，运用式(8)和式(9)对I向量进行正向扩散，加密后的向量记为$C_1=\{C_{1,j},j=1,\cdots,M\times N\}$.

$$C_{1,1}=\bmod(I_1+X_1+r_1,256) \tag{8}$$

$$C_{1,j}=\bmod(I_j+X_j+C_{1,j-1},256),j=2,\cdots,M\times N \tag{9}$$

步骤9 将C_1转换为矩阵形式，用动态约瑟夫对C_1图像置乱，将约瑟夫遍历与混沌系统结合，把约瑟夫遍历中的步长m拓展成为一个序列$M(m_1,m_2,\cdots,m_s)$，在对约瑟夫圈进行遍历时，删除第i个元素时使用步长m_i. 为使步长不断变化，让混沌序列Y替代M序列，输入到约瑟夫函数中，对C_1图像每行像素的位置按照约瑟夫遍历的顺序调整，再对C_1图像中每列像素的位置按照约瑟夫遍历的顺序调整，得到的密文图像记为C_2.

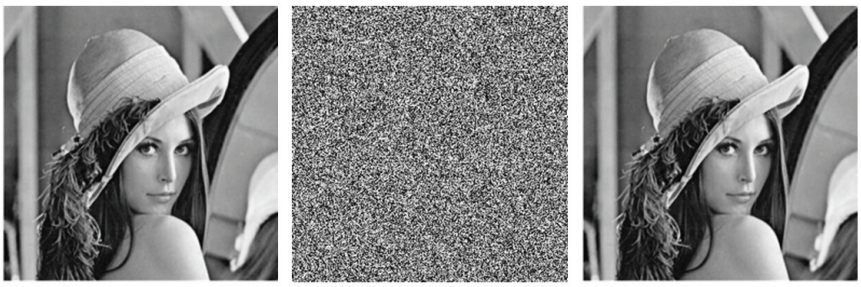
步骤10 将序列Z作为加密向量，运用式(10)和式(11)对C_2向量进行逆向扩散，加密后的向量记为$C_3=\{C_{3,j},j=1,\cdots,M\times N\}$，将其转化为矩阵形式，记为最终密文图像$D$.

$$C_{3,M\times N}=\bmod((C_{2,M\times N}+Z_{M\times N}+r_2),256) \tag{10}$$

$$C_{3,j}=\bmod(C_{2,j}+Z_j+C_{3,j+1},256),j=M\times N-1,M\times N-2,\cdots,2 \tag{11}$$

3　仿 真

选用Lena图像进行实验仿真，所使用的计算机配置为4G内存，Windows7操作系统，1.90 GHz处理器，Lena图像的分辨率为256×256，大小为192 KB[14−17]. 算法在Matlab R2018a 环境下进行仿真，其中，超Lorenz混沌的参数设置为$\{a=10,b=8/3,c=28,r=-1\}$，超Lorenz混沌初始密钥为$K=\{xL_0,yL_0,zL_0,wL_0,r_1,r_2,u\}$，数值为$\{xL_0=3.313\ 3,yL_0=12.054\ 6,zL_0=40.887\ 9,wL_0=-34.567\ 7,r_1=89,r_2=118,u=16\}$, Rossler混沌参数是$\{a=0.2,\ b=0.2,c=5.7\}$，图7给出仿真结果.



（a）明文　　（b）密文　　（c）解密图

图 7　实验结果

Fig 7　Experimental results

4　加密算法安全性分析

4.1　速度测试

以灰度图像Lena例，大小为256×256，按照本文给出的算法加解密200次，计算平均加解密时间分别为0.755 8, 0.763 4，由表1可知，与文献[8]相比，本文设计的算法拥有更快的加密速度.

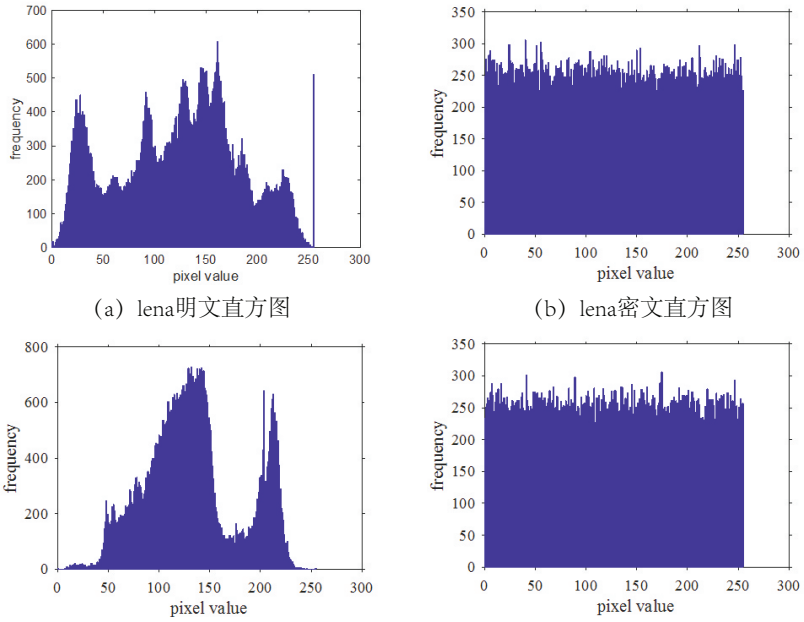
表 1　本文与文献[8]的加解密时间

Tab 1　Encryption and decryption time of this paper and reference [8]

算法	加密时间	解密时间
本文算法	0.755 8	0.763 4
文献[8]	0.764 1	0.769 8

4.2 直方图分析

图8给出直方图分析结果，从图8可以看出加密得到的密文像素值频率分布是非常均匀的，在一定程度上说明加密算法有将图像的统计特性隐藏的足够好的能力，说明算法具有抗统计攻击能力[18−20].



（a）lena明文直方图 （b）lena密文直方图

（a）Peppers明文直方图 （a）Peppers密文直方图

图 8 明密文直方图

Fig 8 Histogram of ciphertext

4.3 密钥空间及敏感性分析

衡量加密算法的好坏要计算它的密钥空间[21]. 密钥空间足够大才能抗穷举攻击. 加密效率高的加密算法的密钥长度至少为2^{128}，才有抵抗暴力破解的能力. 加密方案初始的7个密钥分别是：$\{xL_0, yL_0, zL_0, wL_0, r_1, r_2, u\}$，其中，$xL_0 \in (-40,40), yL_0 \in (-40,40), zL_0 \in (1,81), wL_0 \in (-250,250), r_1 \in [0,255], r_2 \in [0,255], u \in [1,256]$；其中，$xL_0, yL_0, zL_0, wL_0$是浮点数，精度达到了$10^{-15}$，而$r_1, r_2, u$则是整数，步长为1. 即算法密钥空间具体是：$2\times40\times2\times40\times81\times2\times250\times(10^{15})^4\times256\times256\times256\approx4\times10^{75}$远远大于$2^{128}$，因为$2^{10}\approx10^3$，所以密钥空间$4\times10^{75}\approx2^{252}$，从表2可知，与文献[1]相比，给出的算法密钥空间更大，有抗穷举攻击的能力.

表 2 本文与文献[1]的密钥空间

Tab 2 2 Key space of this paper and reference [1]

算法	密钥空间
本文算法	2^{252}
文献[1]	2^{200}

（a）错误解 （b）正确解密

图 9 密钥敏感性测试

Fig 9 Key sensitivity test

对超Lorenz混沌系统的初值进行2×10^{-14}的微小扰动，当$xL_0=3.313\ 3+2\times10^{-14}$时，图9（a）为解密得到的图像，说明给出的加密方案有很强的密钥敏感性，给密钥做肉眼看不到的微小改变都无法获得正确解密图.

4.4　明文敏感性分析

像素变化比率（简称$NPCR$）表示明文一个像素值变化密文像素值变化的比率，$NPCR$越接近100%，加密效果越好[22]. D_1表示密文，D_2表示明文，公式为：

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times100\% \tag{12}$$

归一化平均改变强度（简称$UACI$）指两图全部对应位置像素点差值和最大差值比值的均值. $UACI$越接近33.4635%越好，公式为：

$$UACI=\frac{1}{M\times N}\times[\sum_{i}\sum_{j}\frac{D_1(i,j)-D_2(i,j)}{256}]\times100\% \tag{13}$$

对明文中任意一点像素值进行非常微小的变动，通过计算，此时$NPCR$和$UACI$分别为99.83%和33.43%，均非常接近理想值，对比文献[1]，结果如表3所示.

表 3　明文敏感性分析

Tab 3　Plaintext sensitivity analysis

指标	本文算法	文献[1]
$NPCR$	0.998 3	0.997 8
$UACI$	0.334 3	0.333 7

4.5　相邻像素相关性分析

根据式(14)，截取2 000对像素点(x,y)进行分析，计算结果如表4和图10. 由表4、图10可知，明文图像相邻像素点相关性高，相关系数在1附近，密文图各方向像素间相关系数都在0附近，说明本文加密算法达到了理想效果. 同文献[1]比较，本文给出的算法加密得到的密文相关性系数值更小，有抗基于相关特性攻击的能力.

$$r_{x,y}=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{14}$$

式中:

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

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

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

表 4　明文和密文相邻像素间相关系数

Tab 4　Correlation coefficients between adjacent pixels of plaintext and ciphertext

方向	原图	密文	文献[1]
水平	0.973 9	0.006 4	-0.020 8
垂直	0.943 6	-0.036 8	0.042 4
对角线	0.917 3	0.014 0	0.021 2

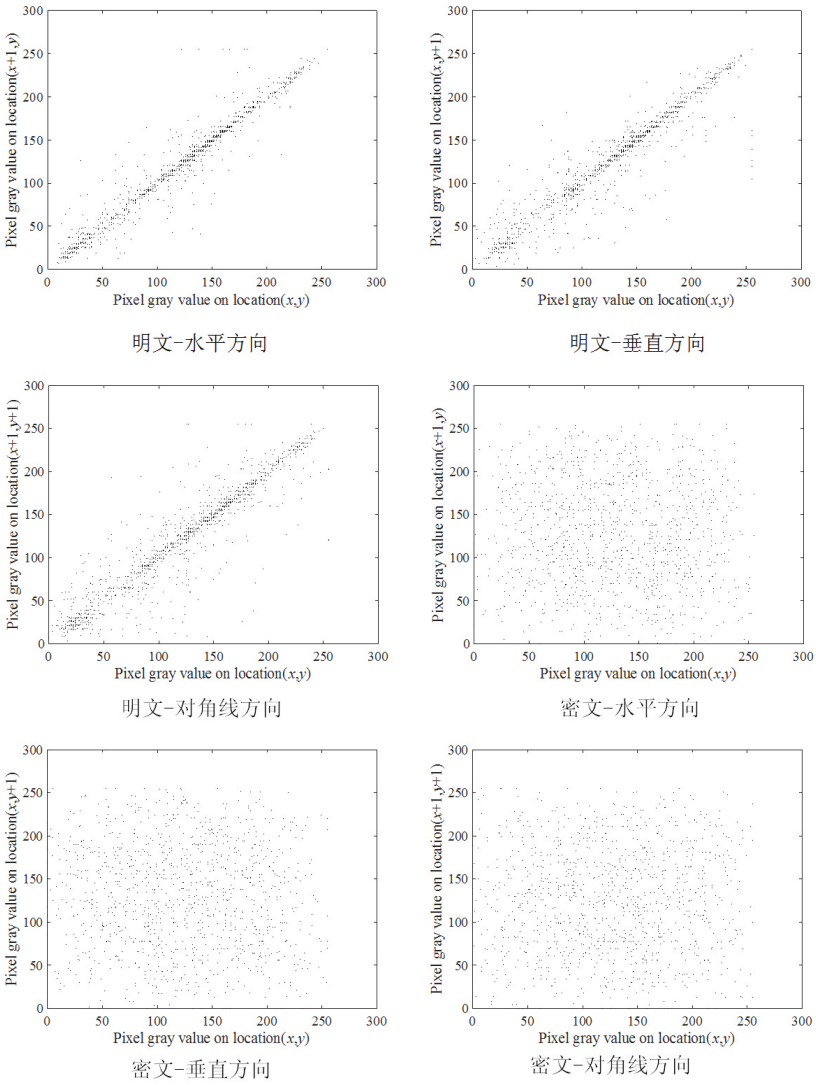


图 10 明密文各方向相邻像素相关性

Fig 10 10 Correlation of adjacent pixels in each direction of ciphertext

4.6 信息熵

根据Shannon定理，信息熵反映了一个序列的随机性[23]. 对256个灰度级的灰度图像而言，信息熵越靠近8越好. 为体现加密方案较为优秀，对Lena图像的明文与密文信息熵进行对比，根据式(15)计算信息熵的结果见表5，式中$m(i)$指的是灰度值i出现的概率. 由表5可知，与使用文献[1]中给出的加密算法生成的密文的信息熵相比，使用本文所给出的加密算法生成的密文信息熵更加接近理想值8，表明本文算法加密效果更好.

$$H(m)=-\sum_{i=1}^{255}p(m_i)\log_2 p(m_i) \tag{15}$$

表 5 信息熵结果

Tab 5 Information entropy results

图像	明文信息熵	密文信息熵
Lena	7.445 0	7.997 4
文献[1]	7.445 0	7.997 0

5 结 论

本文给出的基于L-R混沌和双重扩散的图像加密算法的密钥与明文图像相关联，也就是给定相同的密钥但

是不同的明文图像都会对应不同的密码. 设定两级密钥和更加高效的运算规则来产生混沌序列. 此外，该算法运用约瑟夫遍历与混沌系统相结合，使约瑟夫遍历中步长不断发生变化的方法来置乱图像. 加密体系结构为“正向扩散-动态约瑟夫置乱-逆向扩散”. 通过Matlab实验分析说明算法具有高的加密效率与高的安全性，密文直方图呈现均匀分布，具有很强的抗统计、差分和穷举攻击能力，安全性高，并且该算法解决了混沌加密系统结构单一以及与明文无关的问题.

参考文献：

[1] 马聪, 李国东. 基于L-K双混沌系统的彩色位级图像加密算法[J]. 计算机应用与软件, 2020, 37(3): 321-326.
MA C, LI G D. Color image encryption algorithm based on L-K double chaotic system[J]. Computer Applications and Software, 2020, 37(3): 321-326. (in Chinese)

[2] 王瑶, 韩亚军. 基于双向相关扩散与非线性混沌S盒的图像加密算法[J]. 包装工程, 2019, 40(15): 243-251.
WANG Y, HAN Y J. Image encryption algorithm based on bidirectional correlation diffusion and nonlinear chaotic S-box[J]. Packaging Engineering, 2019, 40(15): 243-251. (in Chinese)

[3] 牛莹, 张勋才. 基于变步长约瑟夫遍历和DNA动态编码的图像加密算法[J]. 电子与信息学报, 2020, 42(6): 1383-1391.
NIU Y, ZHANG X C. Image encryption algorithm based on variable step size Joseph traversal and DNA dynamic coding[J]. Acta Electronica Sinica, 2020, 42(6): 1383-1391. (in Chinese)

[4] 王兴元, 王明军. 超混沌Lorenz系统[J]. 物理学报, 2007, 56(9): 5136-5141.
WANG X Y, WANG M J. Hyperchaotic Lorenz system[J]. Acta Physica Sinica, 2007, 56(9): 5136-5141. (in Chinese)

[5] ZHANG Y. Plain text related image encryption scheme using chaotic map[J]. Telkomnika Indonesian Journal of Electrical Enginering, 2014, 12(1): 635-643.

[6] ZHANG Y. Two-level secret key image encryption method based on piecewise linear map and logistic map[J]. Applied Mechanics & Materials, 2013, 241/244: 2728-2731.

[7] 张勇. 混沌数字图像加密[M]. 北京: 清华大学出版社，2016.
ZHANG Y. Chaotic digital image encryption[M]. Beijing: Tsinghua University Press, 2016. (in Chinese)

[8] 谢国波, 高兆曦. 明文关联的多混沌彩色图像加密算法[J]. 计算机工程与设计, 2019, 40(4): 920-930.
XIE G B, GAO Z X. Multi chaotic color image encryption algorithm based on plaintext correlation[J]. Computer Engineering and Design, 2019, 40(4): 920-930. (in Chinese)

[9] 陈士华, 谢进, 陆君. Rossler混沌系统的追踪控制与同步[J]. 物理学报, 2002, 4(4): 749-752.
CHEN S H, XIE J, LU J. Tracking control and synchronization of Rossler chaotic system[J]. Acta Physica Sinica, 2002, 4(4): 749-752. (in Chinese)

[10] 陈炜, 郭媛, 敬世伟. 基于深度学习压缩感知与复合混沌系统的通用图像加密算法[J]. 物理学报, 2020, 69(24): 99-111.
CHEN W, GUO Y, JING S W. General image encryption algorithm based on deep learning compressed sensing and composite chaotic system[J]. Acta Physica Sinica, 2020, 69(24): 99-111. (in Chinese)

[11] 赵国敏, 李国东. 基于广义Henon映射以及CNN超混沌系统图像加密方案[J]. 信阳师范学院学报（自然科学版）, 2015, 28(1): 141-145.
ZHAO G M, LI G D. Image encryption scheme based on generalized Henon mapping and CNN hyperchaotic system[J]. Journal of Xinyang Normal University(Nat Sci), 2015, 28(1): 141-145. (in Chinese)

[12] 郭毅, 邵利平, 杨璐. 基于约瑟夫和Henon映射的比特位图像加密算法[J]. 计算机应用研究, 2015, 32(4): 1131-1137.
GUO Y, SHAO L P, YANG L. Bit image encryption algorithm based on Joseph and Henon mapping[J]. Computer Application Research, 2015, 32(4): 1131-1137. (in Chinese)

[13] ROSSLER O E. An equation for continuous chaos[J]. Phys Lett A，1996(57): 397-400.

[14] 班多晗, 吕鑫, 王鑫元. 基于一维混沌映射的高效图像加密算法[J]. 计算机科学, 2020, 47(4): 278-284.
BAN D H, LYU X, WANG X Y. Efficient image encryption algorithm based on one dimensional chaotic map[J]. Computer Science, 2020, 47(4): 278-284. (in Chinese)

[15] 宋金林, 张绍武. 整合ChaCha20哈希运算的分块扩散自适应图像加密算法[J]. 中国图象图形学报, 2016, 21(6): 698-710.
SONG J L, ZHANG S W. Block diffusion adaptive image encryption algorithm integrating chacha20 hash operation[J]. Chinese Journal of Image Graphics, 2016, 21(6): 698-710. (in Chinese)

（下转第 333 页）

[48] 张博文, 展新忠, 陈川, 等. 西天山喇嘛苏外围铜矿床岩石地球化学及成矿背景研究[J]. 新疆大学学报(自然科学版), 2018, 35(1): 86-95.
ZHANG B W, ZHANG X Z, CHEN C, et al. Study on petrogeochemistry and metallogenic background of Lamasuwaiwei copper deposit in Western Tianshan Orogenic[J]. Journal of Xinjiang University (Natural Science Edition), 2018, 35(1): 86-95. (in Chinese)
[49] 韩秉峻, 弓小平, 刘祥, 等. 新疆冰草沟地区铀矿地球化学及成矿特征[J]. 新疆大学学报(自然科学版), 2018, 35(4): 513-521.
HAN B J, GONG X P, LIU X, et al. Geochemical and metallogenic characteristics of uranium deposit in Bingcaogou region, Xinjiang[J]. Journal of Xinjiang University (Natural Science Edition), 2018, 35(4): 513-521. (in Chinese)
[50] OHMOTO H. Systematics of sulfur and carbon isotopes in hydrothermal ore deposits[J]. Economic Geology, 1972, 67: 551-578.
[51] ZARTMAN R E, DOE B R. Plumbotectonics–the Model[J]. Tectonophysics, 1981, 75: 135-162.
[52] LI Q L, CHEN F, YANG J H, et al. Single grain pyrite Rb–Sr dating of the Linglong gold deposit, eastern China[J]. Ore Geology Reviews, 2008, 34: 263-270.
[53] HU F F, FAN H R, JIANG X H, et al. Fluid inclusions at different depths in the Sanshandao gold deposit, Jiaodong Peninsula, China[J]. Geofluids, 2013, 13: 528-541.
[54] ZHANG L C, LIU T B, SHEN Y C, et al. Structure, isotopes and $^{40}Ar/^{39}Ar$ dating of the Pengjiakuang gold deposit, Mesozoic Jiaolai basin, eastern China[J]. International Geology Review, 2003, 45: 691-711.
[55] MAO J W, XIE G Q, ZHANG Z H, et al. Mesozoic large–scale metallogenic pulses in North China and Corresponding geodynamic setting[J]. Acta Petrologica Sinica, 2005, 21: 169-188.
[56] MAO J W, PIRINO F, COOK N. Mesozoic metallogeny in East China and corresponding geodynamic settings–An introduction to the special issue[J]. Ore Geology Reviews, 2011, 43: 1-7.

责任编辑：赵新科

(**上接第** 299 **页**)

[16] 黄胡晏, 饶从军. 一种新型混沌图像加密算法[J]. 华中师范大学学报(自然科学版), 2017, 51(4): 441-448.
HUANG H Y, RAO C J. A new chaotic image encryption algorithm[J]. Journal of Central China Normal University (Nat Sci), 2017, 51(4): 441-448. (in Chinese)
[17] 庄志本, 李军, 刘静漪, 等. 基于新的五维多环多翼超混沌系统的图像加密算法[J]. 物理学报, 2020, 69(4): 50-63.
ZHUANG Z B, LI J, LIU J Y, et al. Image encryption algorithm based on new five dimensional multi ring multi wing hyperchaotic system[J]. Acta Physica Sinica, 2020, 69(4): 50-63. (in Chinese)
[18] 刘志军, 刘丹. 基于耦合混沌和循环移位的彩色图像加密算法[J]. 新疆大学学报(自然科学版), 2017, 34(4): 440-445.
LIU Z J, LIU D. Color image encryption algorithm based on coupled chaos and cyclic shift[J]. Journal of Xinjiang University(Nat Sci), 2017, 34(4): 440-445. (in Chinese)
[19] 余萍, 闻恺. 基于混沌交换控制表与关联动态引擎的图像加密算法[J]. 新疆大学学报(自然科学版), 2017, 34(4): 459-466.
YU P, WEN K. Image encryption algorithm based on chaos exchange control table and correlation dynamic engine[J]. Journal of Xinjiang University(Nat Sci), 2017, 34(4): 459-466. (in Chinese)
[20] 古丽孜拉, 王兴元. 基于多个一维混沌映射系统的多重加密算法[J]. 新疆大学学报(自然科学版), 2008, 26(2): 228-234.
Gulizila, WANG X Y. Multiple encryption algorithm based on multiple one-dimensional chaotic mapping systems[J]. Journal of Xinjiang University(Nat Sci), 2008, 36(2): 228-234. (in Chinese)
[21] 杨帆, 臧睿. 基于伪中心可逆矩阵的图像加密[J]. 数学的实践与认识, 2020, 50(19): 253-260.
YANG F, ZANG R. Image encryption based on pseudo central invertible matrix[J]. Practice and Understanding of Mathematics, 2020, 50(19): 253-260. (in Chinese)
[22] 黄林茎, 刘会, 王志颖, 等. 结合混沌映射与DNA计算的自适应图像加密算法[J]. 小型微型计算机系统, 2020, 41(9): 1959-1965.
HUANG L Q, LIU H, WANG Z Y, et al. Adaptive image encryption algorithm based on chaotic mapping and DNA computing[J]. Minicomputer System, 2020, 41(9): 1959-1965. (in Chinese)
[23] 梁颖, 张绍武. 位级同步置乱扩散和像素级环形扩散图像加密算法[J]. 中国图象图形学报, 2018, 23(6): 814-826.
LIANG Y, ZHANG S W. Bit level synchronous scrambling diffusion and pixel level ring diffusion image encryption algorithm[J]. Chinese Journal of Image Graphics, 2018, 23(6): 814-826. (in Chinese)

责任编辑：赵新科