# 基于变步长约瑟夫遍历和DNA动态编码的图像加密算法

牛 莹[①] 张勋才*[②]

[①](郑州轻工业大学建筑环境工程学院 郑州 450002)

[②](郑州轻工业大学电气信息工程学院 郑州 450002)

**摘 要**：数字图像传输和存储的安全问题已成为信息安全研究的热点。该文提出一种基于变步长约瑟夫遍历和DNA动态编码的图像加密方法。首先将混沌映射产生的随机序列作为约瑟夫遍历的变步长，改进约瑟夫遍历问题，并采用改进的约瑟夫遍历对图像像素位置进行置乱；其次，动态选择DNA编码规则，对图像像素进行DNA编码，并与给定的DNA序列进行碱基运算；DNA编码规则的动态选择，很好地解决了DNA编码规则少所带来的安全隐患，提高了算法的安全性。最后通过密文反馈和混沌系统迭代来进一步增强算法的混淆和扩散特性。实验和安全性分析结果表明，该算法不仅对密钥的敏感性强，而且能有效抵御统计性分析和穷举分析等攻击操作。

**关键词**：图像加密；DNA动态编码；约瑟夫遍历；置换

**中图分类号**：TP301; TN918.4 **文献标识码**：A **文章编号**：1009-5896(2020)06-1383-09

**DOI**: 10.11999/JEIT190849

# Image Encryption Algorithm of Based on Variable Step Length Josephus Traversing and DNA Dynamic Coding

NIU Ying[①] ZHANG Xuncai[②]

[①](*College of Architecture Environment Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*)

[②](*College of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*)

**Abstract**: The security of digital image transmission and storage has become a hotspot of information security research. An image encryption algorithm based on variable step length Josephus traversing and DNA dynamic coding is proposed. Firstly, through the thorough analysis of Joseph traversing, the random sequence generated by chaotic map is taken as the variable step length of Joseph traversing, and the pixel position is permutated. Secondly, according to the random sequence generated by chaotic map, the DNA coding rules of pixel points transformation are selected, and the image is dynamically encoded into DNA strand, and the DNA sequence is calculated based on the principle of complementary base pairing. Because the DNA coding rules of the pixels transformation are dynamic, the hidden danger caused by the lack of DNA coding rules is well solved, and the security of the algorithm is improved. Finally, the permutation and diffusion characteristics of the algorithm are further enhanced by ciphertext feedback and chaotic system iteration. Experiment and security analysis results show that the algorithm not only has large key space and strong sensitivity to keys, but also can effectively resist attacks such as statistical analysis and brutal analysis.

**Key words**: Image encryption; Dynamic DNA encoding; Josephus traversing; Displace

收稿日期：2019-10-31；改回日期：2020-05-03；网络出版：2020-05-19

*通信作者： 张勋才 zhangxuncai@pku.edu.cn

基金项目：国家自然科学基金(61602424, U1804262)，河南省重点研发与推广专项(202102210177, 192102210134)

Foundation Items: The National Natural Science Foundation of China (61602424, U1804262), The Key Research and Development Program of Henan Province (202102210177, 192102210134)

## 1 引言

目前，数字图像加密技术成为保护图像信息安全的重要手段[1]。由于数字图像具有数据量大、冗余度高等特点，现有的经典加密方法因其加密效率低，安全性不高等原因，已不能满足图像加密的需要。

1949年，香农[2]提出完善保密的概念，并证明一次一密密码体制具有完善保密性。但其密钥在传递和分发上存在很大困难。根据混沌系统的伪随机性、对初值敏感性以及难以预测等特点，将混沌序列作为随机密钥，可以达到与一次一密相同的加密效果，在理论上也是不可破的。因此混沌加密技术在信息安全领域，尤其是图像加密领域得到了广泛的应用[3]。Chen等人[4]提出了基于混沌系统的图像加密的混淆与扩散结构。然而，对于混沌序列，受计算机字长的限制，会导致混沌的动力学特性退化，特别是低维混沌系统[5]。这严重影响了混沌加密的安全性。为此，许多学者使用超混沌系统加密来确保混沌序列的复杂性，以提高算法的安全性。不可否认的是，单一混沌映射构成的加密算法仍无法保证所加密的图像具有较高安全性[3]。

DNA是生物体内遗传信息储存的重要载体，由于其具有超大规模并行性、超高的存储密度、超低的能耗以及独特的分子结构与分子间识别机制决定了其突出的信息存储及信息处理能力。DNA分子在信息加密、隐藏、认证等信息安全技术领域具有巨大的发展潜力[6,7]，为现代密码学的发展提供了一个新途径。1995年Boneh等人[8]用4个月的时间破解了56位的密钥，这是首次用DNA计算来破解传统的加密标准DES。随后DNA密码学的发展成为研究的一个热点。1999年，Gehani等人[9]借助DAN作为信息载体，利用生化技术在DNA分子上实现了一次一密的传统加密算法。同年，Celland等人[10]利用DNA作为信息载体实现了信息的隐藏，并把二战中著名的“June 6 invasion: Normandy”信息隐藏到DNA微点中，利用DNA的天然存储能力实现了隐写术。2013年，Goff等人[11]实现了3维(微粒阵列)加密模型，他们将DNA微粒技术与热缩片结合，把DNA聚合物固定在聚乙烯热缩片上，成功地形成了尺寸在100μm内的3维DNA水凝胶微粒阵列。2019年，我们课题组给出了基于重组DNA技术的密码方案[12]；文献[13]利用DNA折纸术构建信息加密方案。2020年，Namasudra等人[14]给出一种新的DNA密码方案，并应用于云计算环境下。这些DNA加密算法常用于加密文字信息，对于图像信息，直接加密相当困难。

近年来，学者们将DNA编码技术和混沌映射结合，提出一些新的图像加密方法[15,16]。比如，2017年Chai等人[17]结合DNA操作，给出一种基于混沌的图像加密算法。与DNA编码的结合，具有很好的加密效果。在算法中仅使用DNA编码规则，不需要复杂的生物实验，实用性强。因此，结合DNA编码与混沌特性的图像加密算法受到了众多来自不同领域的研究者的关注。但是，在当前提出的DNA编码与混沌系统的图像加密方法中，选用的DNA编码规则多是固定不变，使得算法抗穷举攻击的能力很弱，容易造成安全隐患。为此，采用DNA动态编码的方法，即不同像素点采用不同的DNA编码规则，能有效避免了简单混沌系统中存在的混沌序列容易被预测的不足，再结合约瑟夫遍历的像素置乱，进一步提高了算法的安全性。

## 2 基本理论

### 2.1 约瑟夫问题

约瑟夫问题是一个循环遍历问题，被描述为：将$S$个元素围成一个圈，按顺序循环遍历，删除第$l$个元素，并从第$l$+1个元素开始继续执行这种操作，直到从圈中选到最后一个元素[18,19]。将约瑟夫遍历用函数表达，即$f(S, l)$，这里$S$为元素数，$l$为步长。例如，函数$f(8, 3)$的解法是将1, 2, 3, 4, 5, 6, 7, 8这些元素围成一个圈，然后按顺序循环遍历并删除第3个元素，在这个约瑟夫环中依次被删除的元素分别为3, 6, 1, 5, 2, 8, 4, 7。

为对约瑟夫遍历进行扩展，即在原有规则的基础上加入起点$r$，将约瑟夫函数拓展为$f(S, l, r)$，这种方法可以选择约瑟夫环中的起点，使约瑟夫遍历更具趣味性。在此基础上，郭毅等人[19]又为约瑟夫遍历加入了循环方向和报数间隔，将约瑟夫函数拓展为$f(S, l, r, D, g)$，其中，参数$D$为循环方向；参数$g$为报数间隔。这种方法极大地增加了约瑟夫遍历的多样性。

### 2.2 DNA编码与运算

DNA分子由4种脱氧核苷酸组成，分别是腺嘌呤(A)，胞嘧啶(C)，鸟嘌呤(G)，胸腺嘧啶(T)。对于两个单链DNA分子，可以通过核苷酸之间的氢键形成一个稳定的DNA分子。碱基的化学结构确定了碱基互补配对的原则，也称为Watson-Crick碱基配对原则，即A和T之间通过2个氢键配对，G和C之间通过3个氢键配对[20]。这一天然的四进制组合，正好与半导体通断所形成的二进制类似。因此，运用碱基的排列组合可以进行信息的存储和计算。

(1) 编码规则：如果按照A→00, C→01, G→10, T→11进行对应编码。则互补数字配对00↔11

及01↔10，与碱基对的互补配对A↔T及C↔G吻合。这样共有8中编码组合满足互补配对规则。

对于灰度图像来说，每个像素的灰度值可以用8位二进制数表示，如果采用DNA编码，只需要编码4个碱基序列。转换成DNA序列后，可以将DNA序列的运算规则用到图像加密中。

(2) 碱基运算规则：根据互补配对规则。针对表1的规则1编码，给出一种碱基之间的运算规则(表2，表3，和表4)，针对其它编码，同样可以建立类似的运算规则。在碱基的加、减运算中，表3和表4刚好互拟。比如根据表3的规则：C(ADD)C=G，则根据表4的规则，G(SUB)C=C；因此，若加密采用加法运算，则解密采用减法运算。

## 3　加密算法

通过利用混沌序列、DNA序列库以及自身像素灰度值之间的变换与运算达到混淆与扩散的目的，从而实现对数字图像的加密。

表 1　8种编码规则

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| **00** | A | A | C | G | C | G | T | T |
| **01** | C | G | A | A | T | T | C | G |
| **10** | G | C | T | T | A | A | G | C |
| **11** | T | T | G | C | G | C | A | A |

表 2　异或运算规则

| XOR | A | C | G | T |
|---|---|---|---|---|
| **A** | A | C | G | T |
| **C** | C | A | T | G |
| **G** | G | T | A | C |
| **T** | T | G | C | A |

表 3　加法运算规则

| ADD | A | C | G | T |
|---|---|---|---|---|
| **A** | A | C | G | T |
| **C** | C | G | T | A |
| **G** | G | T | A | C |
| **T** | T | A | C | G |

表 4　减法运算规则

| SUB | A | C | G | T |
|---|---|---|---|---|
| **A** | A | T | G | C |
| **C** | C | A | T | G |
| **G** | G | C | A | T |
| **T** | T | G | C | A |

### 3.1　Lorenz混沌映射

Lorenz映射是混沌系统中具有代表性的混沌映射，系统的动力学方程为

$$\left.\begin{aligned}\dot{x}&=a(y-x)\\ \dot{y}&=-xz+\beta x-y\\ \dot{z}&=xy-\gamma z\end{aligned}\right\}\tag{1}$$

系统参数的典型值为$\alpha$=10, $\beta$=28, $\gamma$=8/3。在保持$\alpha$, $\gamma$不变的情况下，$\beta\geq$24.74时，系统进入混沌态。

Lorenz系统可产生单变量或多变量组合的混沌序列。使得序列的设计非常灵活。给定初值，该系统可以产生3个混沌实值序列$x$, $y$和$z$。并使用式(2)将元素的值限制给定范围内，得到随机序列$X$, $Y$和$Z$。

$$\left.\begin{aligned}X&=\mathrm{mod}\left(\left\lfloor 10^{10}(x-\lfloor x\rfloor)\right\rfloor,256\right)+1\\ Y&=\mathrm{mod}\left(\left\lfloor 10^{10}(y-\lfloor y\rfloor)\right\rfloor,256\right)+1\\ Z&=\mathrm{mod}\left(\left\lfloor 10^{10}(z-\lfloor z\rfloor)\right\rfloor,256\right)\end{aligned}\right\}\tag{2}$$

### 3.2　混沌系统的初值

采用Keccak算法对明文图像生成散列值$K$, $K$的长度为选择256 bit。将其分为32组，每组包含8个比特位，记$K=\{k_1,k_2,\cdots,k_{32}\}$。按照式(3)和式(4)计算Lorenz混沌系统的初值$x_0,y_0,z_0$。

$$h_i=((k_{j+1}\oplus k_{j+2}\oplus k_{j+3})+k_{j+4}+k_{j+5}+k_{j+6})/256\tag{3}$$

$$\left.\begin{aligned}x_0&=1+\mathrm{abs}\left(\mathrm{round}(h_1)-h_1\right)+x_0^{'}\\ y_0&=1+\mathrm{abs}\left(\mathrm{round}(h_2)-h_2\right)+y_0^{'}\\ z_0&=1+\mathrm{abs}\left(\mathrm{round}(h_3)-h_3\right)+z_0^{'}\end{aligned}\right\}\tag{4}$$

其中$j=6\,(i-1)$, $i\in\{1,2,3\}$; $x_0^{'}$, $y_0^{'}$, $z_0^{'}$为给定值。

### 3.3　DNA动态编码技术

DNA动态编码技术是根据图像矩阵$I$中待编码像素所在矩阵中的位置与给序列Z共同决定选择表1编码规则的一种，也即对像素$I_{i,j}$选择的DNA编码规则计算如式(5)。

$$\mathrm{Rule}\ R_{i,j}=(\mathrm{mod}(i-1)N+j,8)\oplus Z_{(i-1)N+1}(6:8)\tag{5}$$

这里$i\in\{1,2,\cdots,M\}$, $j\in\{1,2,\cdots,M\}$, $Z_{(i-1)N+1}(6:8)$为$Z_{(i-1)N+1}$元素$Z_{(i-1)N+1}$对应的二进制数的后3位，$M$和$N$为图像矩阵的行数和列数。

### 3.4　像素置乱

置乱是以某种特定的规则打乱像素的位置。采用约瑟夫遍历进行像素位置置乱，本文给出一种变步长的循环遍历法。该方法将约瑟夫遍历与混沌系

统像结合，把约瑟夫遍历中的步长$l$扩展成为一个序列$L(l_1,l_2,\cdots,l_s)$，在对约瑟夫圈进行遍历时，在删除第$i$个元素时使用步长$l_i$，这进一步拓展了约瑟夫遍历。

本文使用混沌映射产生的伪随机序列作为$L$序列。因此，这里的步长处于不断变化。像素位置置乱是将混沌系统产生伪随机序列作为$L$输入约瑟夫函数，分别对像素矩阵的行、列进行置乱。图1给出了采用约瑟夫置乱的效果。从图中可以看出，3种置乱都完全失去原始图像的特征。

### 3.5 像素置换和密文扩散

像素置乱破坏了相邻像素之间的相关性，但无法有效地抵抗密码学攻击，而像素置换和密文扩散能够彻底混淆明文图像和密文图像之间的关系。

(1) 像素置换：常用像素置换包括模运算和加运算，这能够使像素值与其他值关联，进而使各像素值的分布更加均为，消除置换图像的纹理特征。核酸数据库是已知核酸信息集合的一个数据资料库，序列在数据库中的ID号被称为序列代码，它具有唯一性和永久性。目前能够公开获取的DNA序列已经近2亿条，如此巨大规模数据库，相当于一个天然密码本。本文将图像像素通过编码规则转换成DNA序列，并与给定的DNA序列进行代数运算，进而达到像素替代的目的。这里的DNA序列运算可以是加、减或异或运算。

(2) 密文扩散：密文扩散使明文的微小变化可以扩散到整个密文，从而打乱明文图像与密文图像的关系，以抵抗选择明文等密码学攻击手段。结合混沌序列，利用前两个像素值来改变当前像素值，可以有效地将少量明文图像的变化传播到整个密文图像。假设图像$\boldsymbol{P}$和序列矩阵$\boldsymbol{Q}$的大小均为$M\times N$，行扩散如式(6)。

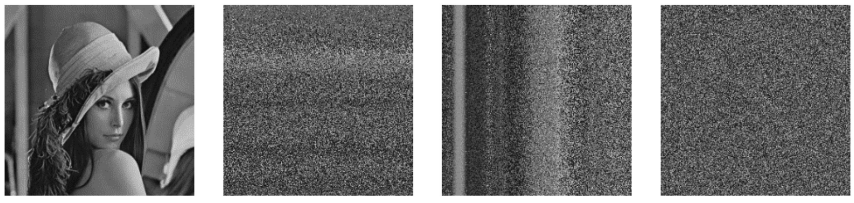
$$P'_i=\begin{cases}(P_1\oplus P_N\oplus P_{N-1}\oplus Q_1)\bmod 256, & i=1\\ (P_2\oplus P'_1\oplus P_1\oplus Q_1)\bmod 256, & i=2\\ (P_i\oplus P'_{i-1}\oplus P'_{i-2}\oplus Q_i)\bmod 256, & i\in[3,N]\end{cases} \tag{6}$$

其中$P_i$表示图像矩阵的第$i$行。同样地，也可以用式(6)对列进行扩散。

### 3.6 加密与解密方案

提出的数字图像加密算法分为两部分：第一，像素位置置乱。利用变步长的约瑟夫实现位置置乱。第二，像素变换与扩散。将原始图像的每个像素点的值转换成DNA序列，然后与DNA编码序列库中的序列运算，再通过密文反馈进行迭代置换。加密流程图如图2所示。具体步骤：

输入：灰度图像$\boldsymbol{I}$，初始参数。



(a) 明文图像 (b) 仅行置乱 (c) 仅列置乱 (d) 行列置乱

图 1 约瑟夫置乱效果

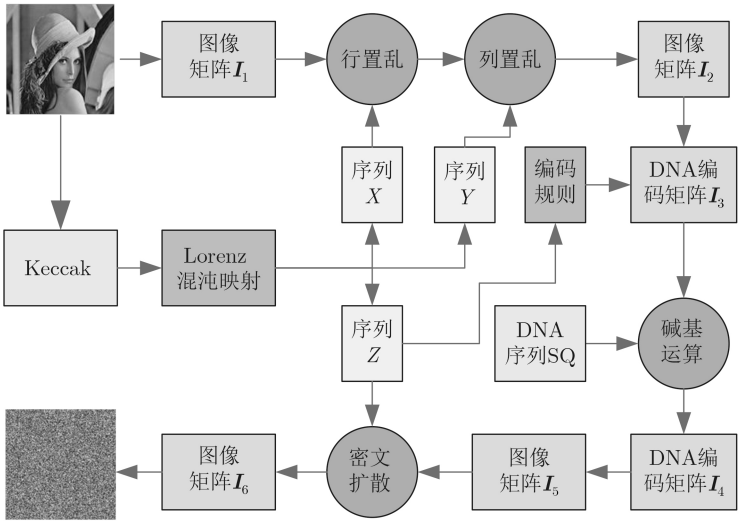



图 2 加密流程图

输出：加密图像。

(1) 将灰度图像$\boldsymbol{I}$转换成大小为$M \times N$的2维矩阵$\boldsymbol{I_1}$；

(2) 采用哈希函数计算图像矩阵$\boldsymbol{I}$的哈希值$H$，并得到混沌初始化参数$x_0$, $y_0$和$z_0$；

(3) 将Lorenz映射产生的序列$X$和$Y$以列优先的方式重组为大小为$M \times N$的矩阵；采用变步长的约瑟夫遍历对图像像素位置矩阵$\boldsymbol{I_1}$分别进行行、列置乱；得到图像像素位置矩阵$\boldsymbol{I_2}$；

(4) 采用DNA动态编码技术将每个像素编码成含有4个碱基的DNA序列，得到DNA编码矩阵$\boldsymbol{I_3}$；

(5) 从GenBank数据库中下载ID号为NZ_LOZQ01000068的DNA序列SQ。从R处截取$4\times M\times N$个碱基，根据3.5节描述的像素置换技术，对矩阵$\boldsymbol{I_3}$实现像素置换技术，这里选择异或运算。得到DNA编码序列$\boldsymbol{I_4}$。并采用编码规则1进行DNA解码，转换成图像矩阵形式，得到矩阵$\boldsymbol{I_5}$；

(6) 利用Lorenz映射产生的序列$Z$，将序列$Z$以列优先的方式重组为和原始图像大小相等的2维矩阵形式；将其转化成矩阵形式，根据3.5节描述的密文扩散技术，对图像矩阵$\boldsymbol{I_5}$实现行、列密文扩散，得到最终加密图像矩阵$\boldsymbol{I_6}$。

解密算法的实现是加密的逆过程，具体步骤如下：

输入：密文图像$\boldsymbol{I}$，初始参数和哈希值$H$。

输出：明文图像。

(1) 将密文图像$\boldsymbol{I}$转换成大小为$M\times N$的2维矩阵$\boldsymbol{I_6}$；

(2) 根据哈希值$H$和初始值$x_0^{'}$, $y_0^{'}$, $z_0^{'}$，计算混沌初始化参数$x_0$, $y_0$, 和$z_0$；

(3) 利用Lorenz映射产生的序列$Z$，将序列$Z$以列优先的方式重组为和原始图像大小相等的2维矩阵形式；按照与加密同样的过程，按列、行进行逆扩散，得到图像矩阵$\boldsymbol{I_5}$；

(4) 采用编码规则1，对图像矩阵进行编码，得到DNA序列矩阵$\boldsymbol{I_4}$，从GenBank数据库中下载ID号为NZ_LOZQ01000068的DNA序列SQ，从$R$处截取$4\times M\times N$个碱基；根据3.5节描述的像素置换技术，对矩阵$I_4$实现像素置换技术，选择异或运算。得到DNA编码序列$\boldsymbol{I_3}$；

(5) 采用DNA动态编码技术将DNA序列解码，得到图像矩阵$\boldsymbol{I_2}$；

(6) 将Lorenz映射产生的序列$X$和$Y$以列优先的方式重组为大小为$M\times N$的矩阵；采用变步长的约瑟夫遍历对图像像素位置矩阵$\boldsymbol{I_2}$列、行逆置乱，得到图像像素位置矩阵$\boldsymbol{I_1}$；即明文图像。

本文算法也适用于彩色图像的加密，只需将像素的值进行RGB分解处理即可。

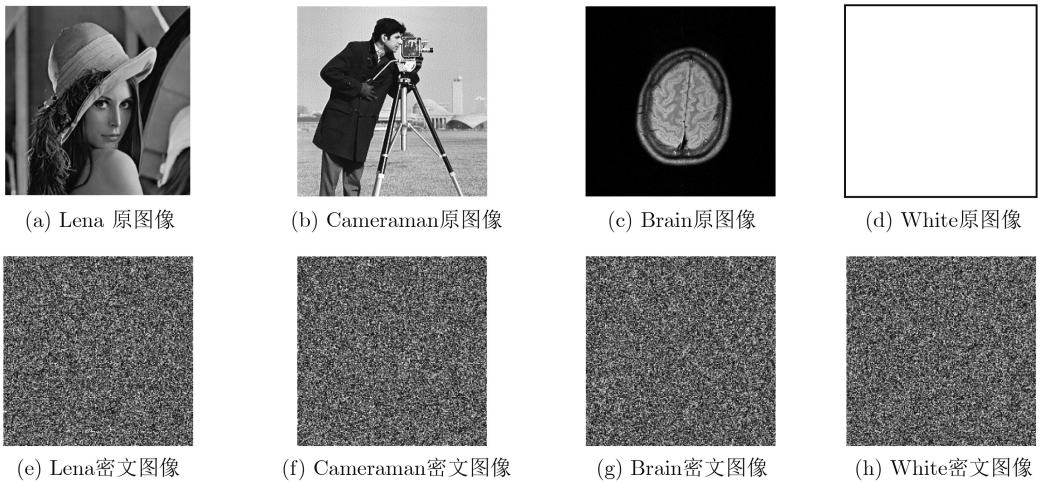
## 4　实验结果

该实验使用配置环境为Windows 7, 4.00 GB RAM, Intel(R) Core(TM) i3-4130 CPU @ 3.4 GHz的计算机在Matlab R2019a平台上进行仿真。该加密算法可以用来加密任意大小的数字图像，给定初始值$x_0^{'}=0$, $y_0^{'}=0$, $z_0^{'}=0$, DNA序列ID号NZ_LOZQ01000068，起始位置为$R$=1。使用本加密算法加密大小为256×256的原始图像和密文图像如图3所示。从图中可以看出，密文图像已经完全失去原始图像的特征，该加密算法效果良好。并且，本算法是无损的，解密图像和原始图像完全一致。

## 5　安全性分析

### 5.1　密钥空间及其敏感性分析

所采用的密钥主要用于像素置乱和扩散过程，对于Lorenz混沌映射的初值，主要是通过Hash散



(a) Lena 原图像　(b) Cameraman原图像　(c) Brain原图像　(d) White原图像

(e) Lena密文图像　(f) Cameraman密文图像　(g) Brain密文图像　(h) White密文图像

图 3 原始图像和密文图像

列值与给定的初始值计算生成。图像转换为DNA序列则采用动态编码技术，其他的DNA编码选择规则1；DNA序列ID号NZ_LOZQ01000068，起始位置为$R$=1。如果计算精度为$10^{-14}$，密钥的空间即可达到$10^{100}$，可见本算法具有足够的空间来抵抗穷举攻击。

在加密过程中，密钥的少许改变会引起密文的极大改变，这种现象成为密钥的加密敏感性。通常使用NPCR(像素改变率)和UACI(像素平均改变强度)来衡量密钥的敏感性。NPCR和UACI如式(7)所示

$$\left.\begin{aligned}\mathrm{NPCR}&=\frac{\sum_{i,j}|P_1(i,j)\oplus P_2(i,j)|}{M\times N}\times 100\%\\ \mathrm{UACI}&=\frac{\sum_{i,j}|P_1(i,j)-P_2(i,j)|}{255\times M\times N}\times 100\%\end{aligned}\right\}\tag{7}$$

NPCR和UACI的期望值为100%和33.4635%。以Lena为例，当加密密钥值增加$10^{-10}$时，其密文图像$\boldsymbol{P}_2$和原密钥加密的密文图像$\boldsymbol{P}_1$间的NPCR和UACI值如表5所示。密钥的敏感性在解密过程中体现得更为明显，当解密密钥发生微小的改变，对应的解密图像无论从像素级进行分析，还是从视觉效果上进行分析，解密图像均与原始图像差别巨大。表6所示为当解密密钥发生微小变化，解密图像和原始图像之间差异度的各项指标。这表明该算法有很好的密钥敏感性。

### 5.2 差分攻击分析

差分攻击分析是指对原始图像做微小变动后加密，继而对密文进行分析，分析其对明文的敏感程度。衡量抵御差分攻击能力的指标分别NPCR和UACI。表7中列举了明文发生1 bit改变时的密文图像与原密文图像之间的NPCR, UACI的值，表中的数据均接近于理论值，这反映出使用本加密算法加密的密文图像与原始图像之间存在着很强的关联性，即使原始图像发生1 bit的微小改变，密文图像便会发生彻底的变化。

表 5 加密密钥敏感性(%)

| 初始值 | NPCR | UACI |
|---|---|---|
| $x_0'$+$10^{-10}$ | 99.5956 | 33.5652 |
| $y_0'$+$10^{-10}$ | 99.6109 | 33.3368 |
| $z_0'$+$10^{-10}$ | 99.6261 | 33.5378 |

表 6 密钥的解密敏感性分析(%)

| 初始值 | NPCR | UACI |
|---|---|---|
| $x_0'$+$10^{-10}$ | 99.6048 | 34.6094 |
| $y_0'$+$10^{-10}$ | 99.5956 | 34.4388 |
| $x_0'$+$10^{-10}$ | 99.5529 | 34.5867 |

### 5.3 灰度直方图分析

图像的统计信息在一定程度上可以反映出原始图像灰度值的分布规律。该算法对图像像素值运算操作的目的即为抵御攻击方进行灰度统计攻击。如图4所示，从实验结果可以得出，异或处理及置换运算使所得加密图像灰度分布非常均匀，这说明该算法具有很好的抵御统计分析能力。

像素直方图的分布规律可以使用直方图的$\chi^2$分布来衡量，用$\mathrm{hist}_i(i=0,1,\cdots,255)$表示图像的直方图，则直方图$\chi^2$分布计算公式如式(8)。

$$\chi^2=\frac{1}{256}\sum_{i=0}^{255}\left(\mathrm{hist}_i-\frac{1}{256}\sum_{i=0}^{255}\mathrm{hist}_i\right)^2\tag{8}$$

直方图服从自由度为255的$\chi^2$分布。给定显著水平$\alpha$，使得$\mathrm{P}\{\chi^2\geq\chi^2_\alpha(n-1)\}=\alpha$，即$\chi^2<\chi^2_\alpha(n-1)$时接受假设。当显著水平$\alpha$=0.01, 0.05和0.1时，有$\chi^2_{0.01}(255)=310.45739$, $\chi^2_{0.05}(255)=293.24783$, $\chi^2_{0.1}(255)=274.33591$。一些图像的$\chi^2$分布如表8所示。常用的显著性水平为$\alpha$=0.05，表8中的密文图像全部通过测试。通过对比可知，该算法极大地改变了图像的直方图分布，具有良好的打破原始图像统计特征的能力。

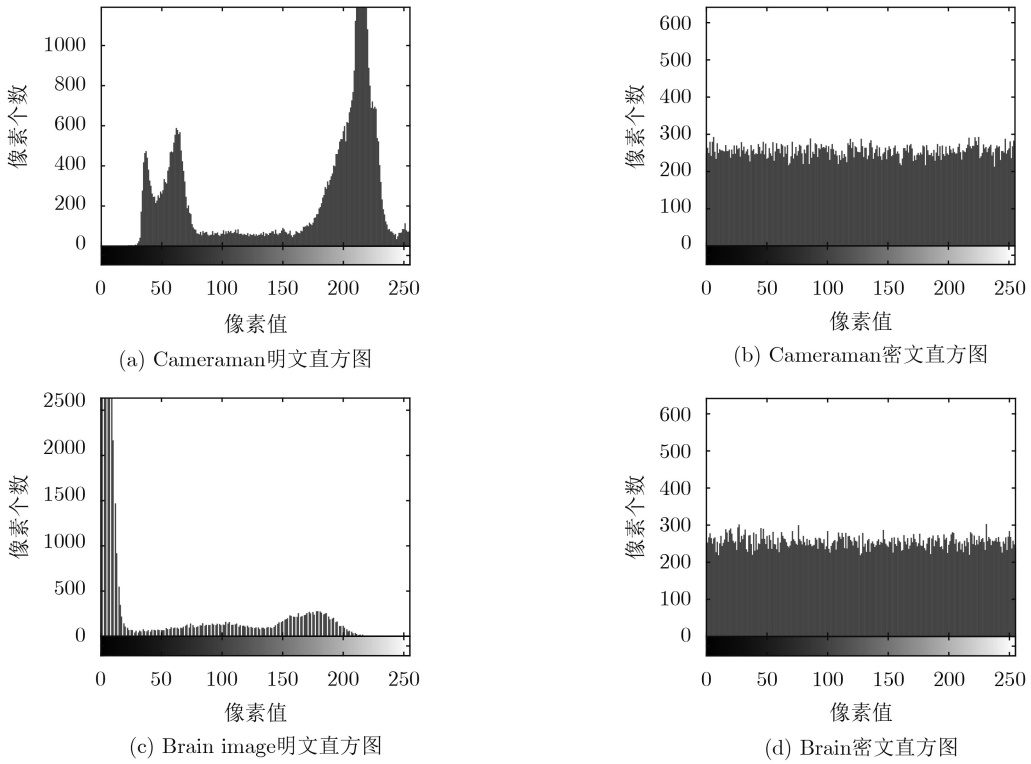
### 5.4 相关系数分析

明文图像相邻像素间的值十分接近，所以图像相邻位置间的像素值的相关性很强。而打破像素之间的强相关性，对抵抗统计分析攻击具有重大意义。相邻像素间相关系数的计算方法如式(9)。

$$\left.\begin{aligned}E(x)&=\frac{1}{N}\sum_{i=1}^{N}x_i\\ D(x)&=\frac{1}{N}\sum_{i=1}^{N}\left(\left(x_i-E(x)\right)^2\right.\\ \mathrm{cov}(x,y)&=\frac{1}{N}\sum_{i=1}^{N}\left(\left(x_i-E(x)\right)\left(y_i-E(y)\right)\right.\\ r_{xy}&=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}\end{aligned}\right\}\tag{9}$$

表 7 原始图像发生微小改变时NPCR和UACI的值(%)

| 图像 | NPCR | UACI |
|---|---|---|
| Lena | 99.5378 | 33.3080 |
| Cameraman | 99.6209 | 33.5080 |
| Brain | 99.5375 | 33.6244 |
| White | 99.6284 | 33.8780 |




(a) Cameraman明文直方图　(b) Cameraman密文直方图

(c) Brain image明文直方图　(d) Brain密文直方图

图 4 原始图像和密文图像的直方图统计

随机选取10000对像素点，对原图像和密文图像在水平方向、垂直方向和对角线方向上的相关性进行统计，结果如表9所示。可以看出，在原始图像随机选取到的像素相关性很强，而在密文图像中，像素之间的相关系数接近于0。这说明该算法可以更好地打乱像素之间的相关性。

### 5.5 信息熵分析

信息熵是一种测试不确定性的指标。计算公式如式(10)。

表 8 直方图的$\chi^2$分布统计

| | 原始图像$\chi^2$分布 | 密文图像$\chi^2$分布 | 检测结果 |
|---|---|---|---|
| Lena | 39851.3281 | 239.0847 | 通过 |
| Cameraman | 161271.875 | 212.0456 | 通过 |
| Brain | 1044635.67 | 258.3025 | 通过 |

表 9 原始图像和密文图像各方向的相关系数

| 图像 | 相关系数 | | | | | |
|---|---|---|---|---|---|---|
| | 原始图像 | | | 密文图像 | | |
| | 水平方向 | 垂直方向 | 对角线方向 | 水平方向 | 垂直方向 | 对角线方向 |
| Cameraman | 0.9540 | 0.9087 | 0.8813 | –0.0070 | 0.0083 | 0.0013 |
| Brain | 0.9965 | 0.9959 | 0.9942 | –0.0038 | 0.0051 | 0.0042 |

$$H(m)=-\sum_{k=0}^{2^N-1}p(m_i)\log_2 p(m_i) \tag{10}$$

这里，$p(m_i)$表示信息$m_i$出现的概率。对于灰度图像，信息$m$有256种状态，最小值0，最大值为255。当信息熵为8时，表明信息是完全随机的。也就是说，密文信息熵越大信息越安全。表10给出了部分使用该算法加密的图像信息熵，通过对比可知，密文图像信息熵较为接近理想值8，具有良好的随机性。

信息熵能较好地反映图像的整体随机性，而局部信息熵能较好地反映图像的微观随机性。局部信息熵是一种改进的信息熵算法，它选择图像中不重叠的区域，计算这些区域的平均信息熵。计算公式如式(11)。

$$\overline{H_{(k,T_B)}(S)}=\frac{1}{k}\sum_{i=1}^{k}H(S_i) \tag{11}$$

$H(S_i)$表示表所选区域的信息熵，$k$表示区域

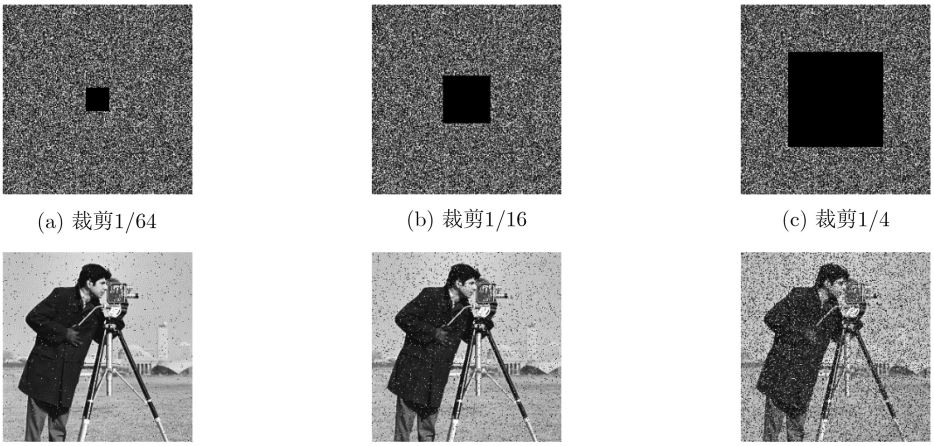
表 10 原始图像和密文图像的信息熵

| 图像 | 信息熵 | |
|---|---|---|
| | 原始图像 | 密文图像 |
| Lena | 6.8794 | 7.9873 |
| Cameraman | 6.9046 | 7.9976 |
| Brain | 5.0329 | 7.9970 |
| White | 0 | 7.9970 |

数, $T_{\mathrm{B}}$表示所选区域的像素数，$\overline{H_{(k,T_{\mathrm{B}})}(S)}$表示局部信息熵。设$k$=30, $T_{\mathrm{B}}$=1936。当显著性水平为$a$=0.05时，局部信息熵的置信区间为[7.900573, 7.904227]。Lena和Cameraman的密文图像的局部香农熵分别为7.9042和7.9032，这表明加密后的图像具有良好的局部随机性。

### 5.6 数据丢失攻击分析

数据丢失攻击是指对密文图像进行拦截并删除部分数据的攻击方式。如果解密算法的恢复能力有限，那么丢失信息后的密文图像的解密图像便不能提供足够的有效信息。图5为经过数据丢失攻击后的密文图像和对应的解密图像。为分析本图像加密算法抵抗数据丢失的能力，分析了被攻击后的解密图像和明文图像间的相关性，表11中给出了Cameraman图像遭受数据丢失攻击后的解密图像的各项指标。可以看出，本算法在遭受数据丢失攻击时具有一定的恢复能力。



(a) 裁剪1/64 (b) 裁剪1/16 (c) 裁剪1/4

(d) 裁剪1/64后的解密图像 (e) 裁剪1/16后的解密图像 (f) 裁剪1/4后的解密图像

图 5 被裁剪的密文图像和解密图像

**表 11 Cameraman图像遭受数据丢失攻击后解密图像的各项指标**

| 裁剪面积 | 相关性 | | | NPCR | UACI |
|---|---|---|---|---|---|
| | 水平 | 垂直 | 对角线 | | |
| 原图 | 0.9501 | 0.9231 | 0.9011 | 0 | 0 |
| 1/64 | 0.9145 | 0.8689 | 0.8649 | 1.7548 | 0.6277 |
| 1/16 | 0.8075 | 0.7754 | 0.7442 | 6.6223 | 2.3429 |
| 1/4 | 0.4667 | 0.4507 | 0.4352 | 25.7019 | 9.0683 |

**表 12 常用加密算法的安全性能列举**

| Cameraman | NPCR (%) | UACI(%) | 信息熵 | 相关系数 | | |
|---|---|---|---|---|---|---|
| | | | | 水平 | 垂直 | 对角线 |
| 文献[18] | 99.5986 | 33.4561 | 7.9971 | 0.0047 | –0.0066 | 0.0031 |
| 文献[21] | 99.5620 | 31.1169 | – | – | – | – |
| 文献[19] | 99.6047 | 33.5050 | 7.9963 | –0.0074 | 0.0069 | –0.0191 |
| 本文方法 | 99.6277 | 33.5715 | 7.9971 | –0.0070 | 0.0083 | 0.0013 |

### 5.7 对比分析

分析了一些参考文献中基于约瑟夫问题的数字图像加密算法的安全性分析的结果，表12给出了一些基于约瑟夫问题的加密算法的安全性分析指标，通过对比分析，说明该算法具有很好的加密性能。

### 5.8 明文攻击分析

4种经典攻击类型包括唯密文攻击、已知明文攻击、选择密文攻击和选择明文攻击，其中，选择明文攻击是最有效的方法。如果加密系统能够有效抵御选择明文攻击，则也能够抵御其他3种经典的攻击方法。

本文加密算法使用SHA-3算法将明文与密钥关联起来，当明文稍有变化时，加密密钥就会发生显著变化，加密系统中的置乱过程和扩散过程也都会发生变化，导致密码发生剧烈的变化。这个过程足以抵抗选择明文攻击。因此，该加密系统具有极高的安全性，可以有效抵御4种经典攻击分析。

## 6 结论

通过对约瑟夫遍历的分析与改进，本文提出了一种基于变步长的约瑟夫遍历和DNA动态编码的图像加密算法。该方法将超混沌系统产生的伪随机混沌序列与约瑟夫遍历结合，增加了像素位置置乱的方法；使像素点的DNA编码动态变化，有效提高了算法的安全性。并利用混沌模型的迭代将密文反馈的影响进行扩大，从而使得算法具有很好的混淆

与扩散特性，可广泛应用于图像信息的加密和传输。

## 参 考 文 献


[1] BEHNIA S, AKHSHANI A, MAHMODI H, *et al*. A novel algorithm for image encryption based on mixture of chaotic maps[J]. *Chaos, Solitons & Fractals*, 2008, 35(2): 408–419. doi: 10.1016/j.chaos.2006.05.011.

[2] SHANNON C E. Communication theory of secrecy systems[J]. *The Bell System Technical Journal*, 1949, 28(4): 656–715. doi: 10.1002/j.1538-7305.1949.tb00928.x.

[3] ÖZKAYNAK F. Brief review on application of nonlinear dynamics in image encryption[J]. *Nonlinear Dynamics*, 2018, 92(2): 305–313. doi: 10.1007/s11071-018-4056-x.

[4] CHEN G R, MAO Y B, and CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. *Chaos, Solitons & Fractals*, 2004, 21(3): 749–761. doi: 10.1016/j.chaos.2003.12.022.

[5] WANG Xinyuan, WANG Xiaojuan, ZHAO Jianfeng, *et al*. Chaotic encryption algorithm based on alternant of stream cipher and block cipher[J]. *Nonlinear Dynamics*, 2011, 63(4): 587–597. doi: 10.1007/s11071-010-9821-4.

[6] LEIER A, RICHTER C, BANZHAF W, *et al*. Cryptography with DNA binary strands[J]. *Biosystems*, 2000, 57(1): 13–22. doi: 10.1016/S0303-2647(00)00083-6.

[7] SHIMANOVSKY B, FENG J, and POTKONJAK M. Hiding Data in DNA[M]. PETITCOLAS F A P. Information Hiding. Berlin: Springer, 2008: 373–386. doi: 10.1007/3-540-36415-3_24.

[8] BONEH D, DUNWORTH C, and LIPTON R J. Breaking DES Using a Molecular Computer[M]. LIPTON R J and BAUM E B. DNA Based Computers I. Providence: American Mathematical Society, 1996: 37–65.

[9] GEHANI A, LABEAN T, and REIF J. DNA-based Cryptography[M]. JONOSKA N, PĂUN G, and ROZENBERG G. Aspects of Molecular Computing. Berlin: Springer, 2003: 233–249. doi: 10.1007/978-3-540-24635-0_12.

[10] CLELLAND C T, RISCA V, BANCROFT C. Hiding messages in DNA microdots[J]. *Nature*, 1999, 399(6736): 533–534. doi: 10.1038/21092.

[11] LE GOFF G C, BLUM L J, and MARQUETTE C A. Shrinking Hydrogel-DNA spots generates 3D microdots arrays[J]. *Macromolecular Bioscience*, 2013, 13(2): 227–233. doi: 10.1002/mabi.201200370.

[12] WANG Yanfeng, HAN Qinqin, CUI Guangzhao, *et al*. Hiding messages based on DNA sequence and recombinant DNA technique[J]. *IEEE Transactions on Nanotechnology*, 2019, 18: 299–307. doi: 10.1109/TNANO.2019.2904842.

[13] ZHANG Yinan, WANG Fei, CHAO Jie, *et al*. DNA origami cryptography for secure communication[J]. *Nature Communications*, 2019, 10: 5469. doi: 10.1038/s41467-019-13517-3.

[14] NAMASUDRA S, DEVI D, KADRY S, *et al*. Towards DNA based data security in the cloud computing environment[J]. *Computer Communications*, 2020, 151: 539–547. doi: 10.1016/j.comcom.2019.12.041.

[15] ZHANG Xuncai, ZHOU Zheng, and NIU Ying. An image encryption method based on the feistel network and dynamic DNA encoding[J]. *IEEE Photonics Journal*, 2018: 3901014. doi: 10.1109/JPHOT.2018.2859257.

[16] WANG Xingyuan, ZHANG Yingqian, and ZHAO Yuanyuan. A novel image encryption scheme based on 2-D logistic map and DNA sequence operations[J]. *Nonlinear Dynamics*, 2015, 82(3): 1269–1280. doi: 10.1007/s11071-015-2234-7.

[17] CHAI Xiuli, CHEN Yiran, and BROYDE Lucie. A novel chaos-based image encryption algorithm using DNA sequence operations[J]. *Optics and Lasers in Engineering*, 2017, 88: 197–213. doi: 10.1016/j.optlaseng.2016.08.009.

[18] WANG Xingyuan, ZHU Xiaoqiang, and ZHANG Yingqian. An image encryption algorithm based on Josephus traversing and mixed chaotic map[J]. *IEEE Access*, 2018, 6: 23733–23746. doi: 10.1109/ACCESS.2018.2805847.

[19] 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. doi: 10.3969/j.issn.1001-3695.2015.04.041.

GUO Yi, SHAO Liping, and YANG Lu. Bit-level image encryption algorithm based on Josephus and Henon chaotic map[J]. *Application Research of Computers*, 2015, 32(4): 1131–1137. doi: 10.3969/j.issn.1001-3695.2015.04.041.

[20] 梁静, 李红菊, 赵凤, 等. 一种构造GC常重量DNA码的方法[J]. 电子与信息学报, 2019, 41(10): 2423–2427. doi: 10.11999/JEIT190070.

LIANG Jing, LI Hongju, ZHAO Feng, *et al*. A method for constructing GC constant weight DNA codes[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2423–2427. doi: 10.11999/JEIT190070.

[21] CHAI Zongqian, LIANG Shili, HU Guorong, *et al*. Periodic characteristics of the Josephus ring and its application in image scrambling[J]. *EURASIP Journal on Wireless Communications and Networking*, 2018, 2018(1): 162. doi: 10.1186/s13638-018-1167-5.



牛　莹：女，1982年生，副教授，研究方向为生物信息处理与信息安全.

张勋才：男，1981年生，副教授、研究方向为智能信息处理与优化控制.