网络首发时间：2021-12-06 14:08:18
网络首发地址：https://kns.cnki.net/kcms/detail/11.4494.tn.20211201.1011.002.html

基于指数-余弦离散混沌映射的图像加密算法研究

刘思聪[①②] 李春彪*[③] 李泳新[③]

[①](电子科技大学生命科学学院 成都 611731)

[②](江苏经贸职业技术学院智能工程学院 南京 210045)

[③](南京信息工程大学人工智能学院 南京 210044)

摘 要：为了增强图像数据传输的安全性，该文提出一种新型的2维指数-余弦离散混沌映射系统。该系统通过向1维余弦混沌系统中引入指数和高次幂非线性项来构造新型混沌映射。引入的非线性项对1维余弦混沌系统的迭代过程进行扰动得到更饱满的混沌相轨。利用Lyapunov指数谱、系统分岔图等对该系统的混沌动力学性质进行了验证。基于此混沌映射，该文提出一种新型的混沌图像加密算法。该算法通过“置乱-扩散-置乱”等加密环节，使得加密后的数据具有很好的数据安全性。加密图像数据的安全性分析也表明2维指数-余弦混沌映射具有较强的算法鲁棒性以及加密安全性。

关键词：2维离散混沌映射；图像加密；算法鲁棒性；加密安全性检验

中图分类号：TN911.7 **文献标识码**：A **文章编号**：1009-5896(2021)00-0001-10

DOI: 10.11999/JEIT210270

A Novel Image Encryption Algorithm Based on Exponent-cosine Chaotic Mapping

LIU Sicong[①②] LI Chunbiao[③] LI Yongxin[③]

[①](*School of Life Science, University of Electronic Science and Technology of China, Chengdu* 611731, *China*)

[②](*School of Artificial Intelligence and Engineering, Jiangsu Vocational Institute of Commerce, Nanjing* 210045, *China*)

[③](*School of Artificial Intelligence, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*)

Abstract: In order to enhance the security of image data transmission, a novel two-dimensional exponent - cosine chaotic map is proposed. In this system, a new chaotic map is constructed by introducing exponent and high-power nonlinear terms into one dimensional cosine chaotic system. The nonlinear term is introduced to perturb the iterative process of one-dimensional cosine chaotic system to obtain fuller chaotic phase orbits. Lyapunov exponential spectrum and system bifurcation diagram are used to verify the features of chaotic system. Based on the chaotic map, a novel image encryption algorithm is proposed. The encrypted data has good encryption security by following a “scrambling-diffusion-scrambling” strategy. Security analysis of encrypted image data also shows that the two-dimensional exponential - cosine chaotic map has strong robustness and encryption security.

Key words: Two-dimensional chaotic map; Image encryption; Algorithm robustness; Encryption security checking

1 引言

伴随5G时代与后疫情时代的到来，越来越多的人际交流迁移到了线上。出于对个人隐私的保护及确保信息安全，人们对于图像加密的需求也越来越大。目前的图像加密算法普遍存在加密过程复杂，耗时较长等缺点。对一些要求能够进行实时加密传输的场合，现有加密算法并不能满足要求。随着Matthews等人[1]将混沌系统应用于信息加密领域，混沌加密算法引起了研究人员的注意，已有多种1维混沌系统被应用于信息加密[2–4]。1维混沌系统多数具有迭代速度快、实现方法简单等特点，但是由于1维混沌系统的系统控制参数较少，相空间轨道分布较为单薄，极易受到相空间重构等方法的

收稿日期：2021-04-02；

*通信作者： 李春彪 chunbiaolee@nuist.edu.cn; goontry@126.com

攻击，从而导致密文被恶意破解。研究者为了克服1维混沌系统的缺点，提出了一系列的改进方案。例如：有研究者将一维混沌系统的多个控制参数间进行耦合操作，使得整个系统的混沌性质变得更加复杂。也有研究者将多个1维混沌映射整合为1个系统，整个加密过程中在不同混沌系统间进行切换或级联操作[5–7]。上述方法可使1维混沌系统具有更好的迭代效率和不可预测性。与此同时，也有研究者尝试通过构建复数域上的1维混沌系统来对信息进行加密，以期获得更好的混沌特性与加密效果[8]。上述手段提高了1维混沌系统的信息加密强度，但受限于1维混沌系统自身的结构与参数特点，其信息加密强度仍然有待提高。目前，研究者将焦点聚集于高维混沌系统以及混沌系统的加密应用上，部分高维混沌系统具有更高的参数维度，其相空间的轨道分布更加复杂，初值敏感性更强，整个系统的混沌映射结构也更加复杂。通过对高维混沌系统的研究，可以获得更好的加密效果[9]。

Gan等人[10]基于3维Chen混沌映射系统，提出了一种3维比特平面重排列的彩色图像加密算法。利用该算法加密后的图像，可以有效降低彩色图像(红，黄，蓝 , Red Green Blue)3通道间的像素相关性，并且整个加密过程具有更大的算法特异性。Qi等人[11]在4阶超混沌系统的基础上，利用广度优先搜索策略，构建了一种新的图像加密算法。该算法提高了加密的安全性和灵敏度。Luo等人[12]在baker映射及Logistic映射的基础上提出了一种新的混沌图像加密算法，该算法通过2维baker映射来控制Logistic映射的参数空间选择，从而使得Logistic映射的混沌行为更加的复杂。通过使用一次置乱-扩散策略，该算法能够有效的提高图像加密的有效性与抗攻击能力。Khan等人[13]通过整合多个混沌映射系统，构造出了一个新型的图像加密算法，该算法构建了一个图像加密流，首先通过2维Henon映射来对原始图像的像素点进行空间置乱操作，之后再利用1维圆映射来进行混沌扩散操作。经过上述加密步骤后，得到了加密图像数据，通过对加密图像数据进行有效性分析，表明该算法具有较好的加密性能和抗攻击能力。Ye等人[14]利用2维正弦映射构造了一个混沌参数空间，并采用置乱-重写-扩散的加密策略，提出了一种新的混沌加密算法。该算法对传统加密算法中彼此分离的两个加密步骤：置乱与扩散过程进行了整合，从而提高了算法的抗攻击能力。同时该算法在像素位置变换与对应像素点灰度值变换之间建立起了联系，从而增强了算法的加密效果。Liu等人[15]基于正弦混沌映射，提出了同步置乱-扩散加密算法，该算法通过生成动态密钥流和索引的方法，将图像的置乱与扩散过程整合在一起，提高了图像加密效率的同时也加强了算法的敏感性。

但是上述研究中所提混沌映射系统，其动力学特性较为单一，在面对基于深度神经网络的新型攻击算法时，极易遭到攻击，从而导致加密失败。基于此，为了提高混沌映射系统的动力学复杂度，本文通过向1维余弦混沌映射系统中引入非线性指数项和高次幂项来对1维混沌系统进行维度提升。被引入的非线性指数项和高次幂项作为混沌扰动源来对余弦混沌映射的迭代过程进行扰动。通过上述方法，构建出了一个新的2维指数-余弦混沌系统。对本系统的混沌特性进行研究，发现本系统具有更加复杂的混沌特性，相空间轨道分布复杂。在本系统的基础上，提出了图像加密算法。理论分析与仿真实验，发现该算法具有较强的鲁棒性和较好的加密效果。

2 2维混沌映射模型及基本动力学分析

2.1 系统方程

1维cosine混沌映射作为一种经典的混沌映射系统，具有控制参数少，易于实现等优点[9]，尽管1维cosine系统具有混沌特性，但是该系统混沌映射构造相对简单，序列迭代排序方式较易被预测。为了提高系统的混沌映射结构复杂度，可以通过向低维混沌系统中引入非线性扰动源的方式来对系统的映射维度进行提升。维度提升后的混沌系统具有更多的控制参数，更复杂的混沌映射结构，序列迭代排序方式变得更加难以预测。本文提出一种新的2维离散混沌映射，该映射的数学模型为

$$\left.\begin{aligned} x_{n+1} &= 1 - a\cos(\pi x_n)(1+x_n) - e^{cy_n} \\ y_{n+1} &= be^{x_n}(x_n - x_n^2) \end{aligned}\right\} \tag{1}$$

其中，a, b, c为控制参数，且$a \neq 0$, $b \neq 0$, $c \neq 0$。

2.2 不动点分析

非线性迭代方程的不动点作为刻画系统动力学演变过程的有力工具。系统式(1)存在不动点，满足$F=(x^*,y^*)$方程为

$$\left.\begin{aligned} x^* &= 1 - a\cos(\pi x^*)(1+x^*) - e^{cy^*} \\ y^* &= be^{x^*}(x^* - {x^*}^2) \end{aligned}\right\} \tag{2}$$

$$\boldsymbol{J} = \begin{bmatrix} a\pi\sin(\pi x)(1+x) - a\boldsymbol{cos}(\pi x) & -ce^{cy} \\ be^x(x-x^2) + be^x(1-2x) & 0 \end{bmatrix} \tag{3}$$

$$det(\lambda \boldsymbol{E} - J) = \lambda^2 - \mathrm{tr}(J)\lambda + det(J) = 0 \tag{4}$$

其中，det为解线性方程组产生的一个算式，取值为标量。$\boldsymbol{J}$为雅可比矩阵，$\boldsymbol{E}$为单位矩阵，tr为矩

阵的迹。系统式(1)在固定参数$a=0.4$, $b=1.75$, $c=0.85$，不同初始值对应的特征值分布，如图1所示。其中图1(a)中起振点，在[1,1.5]范围内变化。图1(b)中起挣点，在[0, 0.2]范围内变化。其中绿色代表特征值λ_1，梅红色代表特征值λ_2，系统式(1)部分特征值分布在单位圆外，这说明系统式(1)是不稳定的。

2.3 基本分岔行为分析

固定初始值$(x_0,y_0)=(0.74,1.38)$，设定参数$a=0.4,c=0.85$，当参数b取值范围在[1, 2]之间，随着参数b的增大，系统依次出现周期，混沌等不同动力学振荡行为。如图2所示，当b在[1, 1.5]内系统捕获到周期解，当b在[1.624, 1.965]内系统具有混沌动力学行为，当b在[1.966, 1.979]有一处周期窗清晰可见。选取动力学系统部分典型相轨展示在图3中，系统存在多种振荡行为如表1所示。

如图3所示，对比图3(a)～图3(c)可知参数b可有效修正系统遍历性，伴随着参数b的增加，动力学系统遍历性增强。图(d)对应上述系统处于周期窗时吸引子运动轨迹。系统式(1)锁定控制参数为$a=0.4,c=0.85$，$(x_0,y_0)=(0.74,1.38)$，当b当取不同参数时动力学系统典型相轨展示。其中参数b的变化均在图中标注。 其中(a)(b)(c)处于混沌状态，(d)处于离散周期点。

3 指数-余弦离散混沌图像加密算法

3.1 加密算法框架设计

为了能够利用指数-余弦离散混沌(Exponent-cosine Chaotic Mapping, 2D-ECs)系统对图像信息进行混沌加密操作，首先对图像数据进行RGB多通道提取，接着对抽取出的单通道图像数据进行混沌加密，之后再将加密后的单通道图像数据重写回图像当中，进而完成对图像数据的加密。在对图像数据进行混沌加密时，采用了“置乱-扩散-置乱”的加密策略。

3.2 第1轮置乱加密

步骤1　在对图像数据进行置乱操作时，首先利用2D-ECs混沌系统生成离散数据序列(x_n,y_n)，设置初始值$(x_0,y_0)=(0.74,1.38)$，控制参数$(a,b,c)=(0.4,1.75,0.85)$。迭代轮次为$M\cdot N+10000$，其中M,N为图像的宽、高值。为了避免混沌序列在迭代早期存在的单值性与周期性，因此将序列中前8000点数据废弃不用。在完成上述操作后，对生成的离散数据序列(x_n,y_n)进行去重处理，将去重后的x_n序列作为图像置乱的行坐标，y_n序列作为图像置乱的列坐标，对原始图像进行空间置乱操作。具体置乱操作，如式(5)所示

$$p(x_i,y_j)=p'(x_{ni},y_{mj}) \tag{5}$$

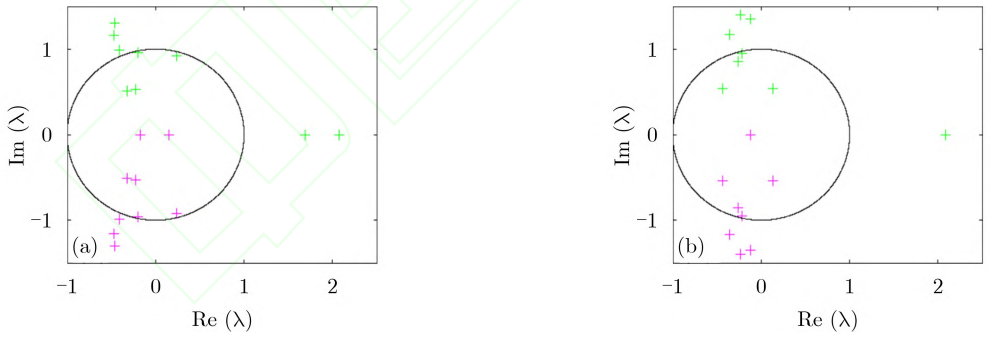

图 1 动力学系统在不同初始值下特征值分布图。

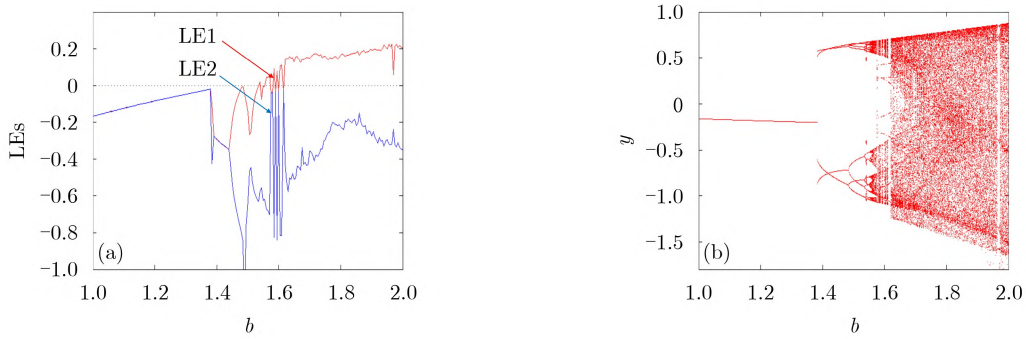

图 2 (a)李雅普诺夫指数谱；(b)分岔图

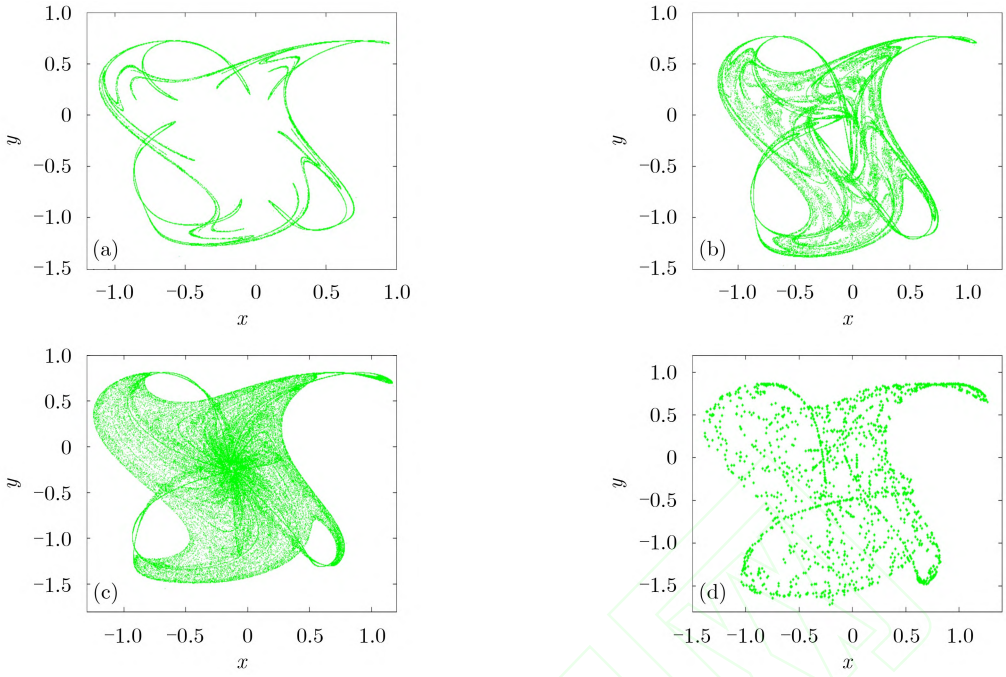

图 3 系统动力学系统典型相轨图

表 1 不同参数b对应的李雅普诺夫指数谱及吸引子类型

b	李雅普诺夫指数谱	吸引子类型
1.65	0.1301, –0.4619	混沌吸引子
1.75	0.1580, –0.2573	混沌吸引子
1.85	0.1781, –0.2180	混沌吸引子
1.97	–0.1155, –0.1155	离散周期点

步骤2 在完成上述操作后，将从步骤1中获得的置乱后图像数据沿列方向展开为1维序列数据。再利用由初始值$(x_0, y_0) = (0.15, 1.7)$与控制参数$(a, b, c) = (0.4, 1.75, 0.85)$构成的2D-ECs混沌系统生成的用于第1轮加密的离散加密序列，来对空间置乱数据进行加密。2D-ECs系统生成的离散加密序列长度为$M \cdot N + 10000$。为了避免混沌序列在迭代早期存在的单值性与周期性，因此将序列中前8000点数据废弃不用。

步骤3 将步骤2中获得的离散加密序列(x_n, y_n)与坐标置乱后的图像数据(Q)进行双螺旋加密。具体加密步骤，如式(6)所示

$$Q' = Q \oplus x_n^{-1} \oplus y_n \oplus x_n \oplus y_n^{-1} \tag{6}$$

其中，x_n^{-1}, y_n^{-1}由离散序列x_n, y_n逆序排列得到，Q'为加密后的图像。通过上述步骤，即可完成第1轮的置乱加密操作。

3.3 扩散加密

为了使加密后的数据具有较好的抵抗选择明文攻击的能力，需要对置乱加密后的密文数据进行扩散加密操作。通过该操作，可以使加密系统对于明文图像极微小的变化变得非常敏感。即使只更改明文图像中一个像素的数据值，也会使得整个加密数据发生较大的变化。具体操作步骤如下所示：

步骤1 首先计算待加密明文图像的平均像素值M，再对该平均值进行归一化操作，使其处于0~1的取值范围内。再将该归一化后的像素均值M'作为2D-ECs混沌系统的x_0初始值，并设Ky_0初始值为1.5，此时控制参数$(a, b, c) = (0.4, 1.75, 0.85)$。经过$M$ x N+10000轮迭代后，抛弃前8000个数据点，获得扩散序列Kx_n, Ky_n。

步骤2 将经过置乱加密后的图像数据(Q')沿列方向展开为1维序列数据。再与步骤1中所获得的扩散序列进行双螺旋扩散加密操作。具体扩散加密公式如式(7)所示

$$G = Q' \oplus x_n^{-1} \oplus y_n \oplus x_n \oplus y_n^{-1} \tag{7}$$

其中，x_n^{-1}, y_n^{-1}由离散序列Kx_n, Ky_n逆序排列得到。G为扩散后的密文数据。通过上述步骤，即可完成对加密数据的扩散操作。

3.4 第2轮置乱加密

为了使图像的加密效果更佳，在完成了上述置乱与扩散操作后，再对加密后的数据进行第2轮空间置乱操作。

步骤1 在对图像数据进行置乱操作时，首先利用2D-ECs混沌系统生成离散数据序列(x_n, y_n)，设置初始值(x_0, y_0)=$(0.74, 1.38)$，控制参数(a, b, c)=$(0.4, 1.75, 0.85)$。迭代轮次为M x N+10000，其中M, N为图像的宽、高值。为了避免混沌序列在迭

代早期存在的单值性与周期性，同时为了增强算法空间的随机性，因而将序列中前9000点数据废弃不用。在完成上述操作后，对生成的离散数据序列(x_n, y_n)进行去重处理，将去重后的x_n序列作为图像置乱的行坐标，y_n序列作为图像置乱的列坐标，来对原始图像进行空间置乱操作。具体置乱操作如式(5)所示。通过上述步骤，即可完成第2轮空间置乱加密操作。本文系统的加密算法流图，如图4所示。

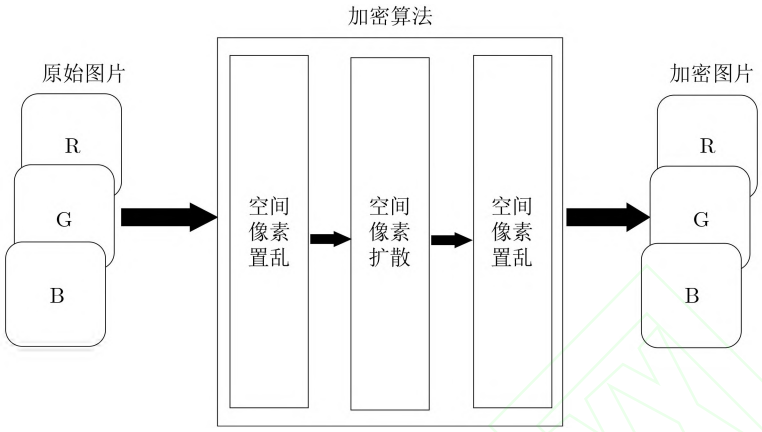

图 4 2D-ECs混沌加密系统加密算法流图

3.5 算法时间复杂度分析

图像加密算法的时间复杂度是衡量加密算法性能的重要指标之一。通过对算法的时间复杂度进行分析，可以从理论上说明图像加密算法的加密效率。一个好的加密算法应该尽可能地花费较少的时间成本来完成对数据的加密。根据上文所述算法流程，可知文中算法不存在循环嵌套等复杂程序运算过程，因此时间复杂度为$O\ (n)$。而目前已有的一些混沌加密算法[11–13]，因存在较为复杂的循环嵌套，因此算法时间复杂度远大于$O(n)$。具体时间复杂度计算结果，如表2所示。

从表2可知，本文所提加密算法具有更小的时间复杂度，其算法计算效率更高。

4　仿真结果与安全性分析

为了验证本文提出的2D-ECs混沌系统加密算法的加密有效性、鲁棒性与安全性，从密钥空间大小，差分攻击分析，自相关性分析，信息熵，算法鲁棒性等方面进行了实验仿真，并对仿真结果进行了分析。上述所有分析均在如下计算平台上完成，平台具体配置为：CPU AMD R7 3700, 16 G内存，GPU Nvdia RTX 2060 6 G，操作系统为Windows 10专业版。所有程序均由Python语言编写。

表 2　算法时间复杂度分析

算法名称	时间复杂度
2D-ECs	$O(n)$
文献[11]	$O(n^2)$
文献[12]	$O(n\log n)$
文献[13]	$O(n^2)$

4.1 仿真结果

利用2D-ECs混沌加密算法对如下标准灰度图像进行加密操作：(1)cameraman图像；(2)lena图像；(3)boat图像。上述图像尺寸均为200×200像素。加密结果如图5所示。

由图5可知，经过2D-ECs混沌系统加密算法加密后的图像像素之间相关性几乎消除，密文图像像素值分布均匀，密码破译难度较大。

4.2 密钥空间分析

密钥空间大小对于加密算法的加密安全性具有较大的影响。密钥空间越大，密码破译所花时间越长。当密钥空间足够大时，密文破译所需时间将呈指数级增长。

本文所设计的2D-ECs混沌系统加密算法采用随机密钥生成方式。加密算法所需的密钥为$\mathrm{Key}=\{x_0, y_0, a, b, c, \mathrm{Ky}_0, \mathrm{Ka}, \mathrm{Kb}, \mathrm{Kc}, \mathrm{StartPosition}$, $\mathrm{StartPositoin2}\}$。其中$x_0, y_0$为第1轮置乱时所用的系统初始值，$a, b, c$为系统控制参数，$\mathrm{Ky}_0$为扩散加密时所用初始值，$\mathrm{Ka}, \mathrm{Kb}, \mathrm{Kc}$为扩散时所用系统控制参数，$\mathrm{StartPosition}, \mathrm{StartPositoin2}$ 为两轮置乱操作时参数序列的起始值。x_0, y_0, Ky_0取值由式(8)计算得到

$$\left.\begin{aligned} x_0 &= \frac{\left(\sum_{i=1}^{128} \mathrm{Random}\cdot 2^{i-1}\right)}{2^{128}} \\ y_0 &= \frac{\left(\sum_{i=1}^{128} \mathrm{Random}\cdot 2^{i-1}\right)}{2^{128}} \\ \mathrm{Ky}_0 &= \frac{\left(\sum_{i=1}^{128} \mathrm{Random}\cdot 2^{i-1}\right)}{2^{128}} \end{aligned}\right\} \tag{8}$$

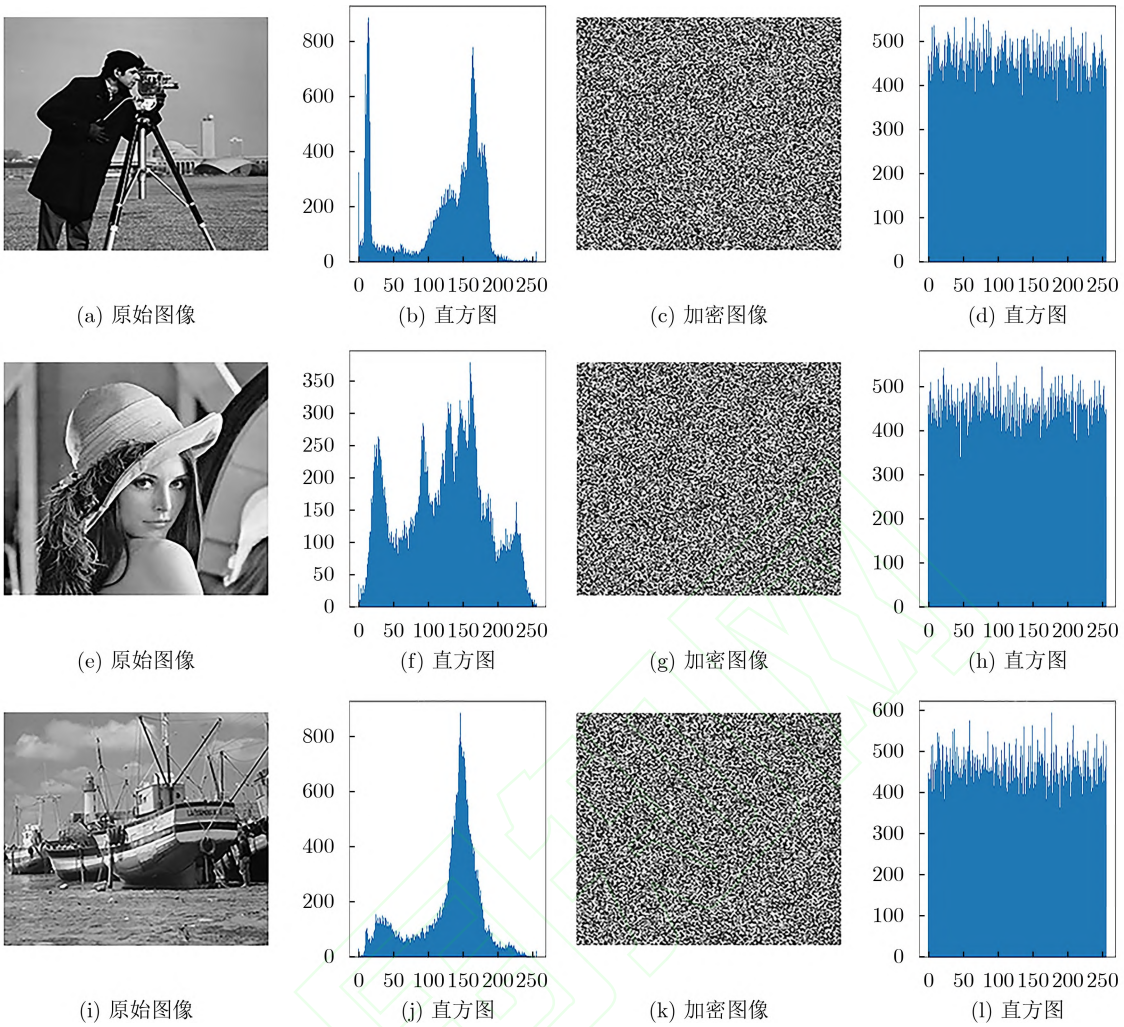

图 5 2D-ECs混沌加密图像及直方图信息

控制参数a,b,Ka,Kb采用随机取值的方式从$a,Ka\in[0,\ 0.4]$,$b,Kb\in[0,1.7]$, $c,Kc\in[0.6,0.9]$随机抽取。随机取值间隔为0.01。StartPosition, StartPositoin2取值采用随机取值的方式，从[3000, 12000]之间随机抽取。综上所述，可知该算法具有较大的密钥空间，可以有效抵御穷举式破译攻击。

4.3 差分攻击分析

差分攻击是通过分析明文细微差异所导致的密文改变程度，来对加密算法进行攻击的一种破译方法。为了分析2D-ECs混沌系统加密算法对于差分攻击的抵抗能力，本文通过改变明文图像中任意一点像素值的方式来观察两次加密后的密文图像间的差异程度。如果差异程度较大，则说明该算法能够有效的抵御差分攻击。本文采用计算像素数变化率(Number of Pixels Change Rate, NPCR)以及统一平均变化强度(Unified Average Changing Intensity, UACI)的方式来衡量密文图像之间差异程度的大小。设I_1,I_2为只具有一像素值差异的两幅待加密明文图像，这两幅图像之间的NPCR值与UACI值，可通过式(9)进行计算

$$\left.\begin{aligned}&\mathrm{NPCR}=\frac{1}{MN}\sum_i^M\sum_j^N D(i,j)\cdot 100\%\\&D(i,j)=\begin{cases}1, I_1(i,j)\neq I_2(i,j)\\0, I_1(i,j)=I_2(i,j)\end{cases}\\&\mathrm{UACI}=\frac{1}{MN}\sum_i^M\sum_j^N\frac{|I_1(i,j)-I_2(i,j)|}{255}\cdot 100\%\end{aligned}\right\}\tag{9}$$

对于任意NPCR值而言，其理想值为(255/256)×100%=99.6094%，对任意UACI值而言，其理想值约为33.4635%[11] 。本文算法对不同灰度图像分别计算NPCR与UACI值，计算结果如表3所示。

通过表3可知，同文献[12–14]相比，本文提出的2D-ECs混沌系统加密算法的NPCR值与UACI值更加接近理想值，故本文所提加密算法对于明文图像像素值的变化非常敏感，可以有效地抵御差分攻击。

4.4 自相关分析

加密效果良好的图像加密算法应当使加密后的

表 3　NPCR,UACI参数值(%)

灰度图像	2D-ECs		文献[12]		文献[13]		文献[14]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
cameraman	99.610	33.464	–	–	–	–	99.72	33.36
lena	99.611	33.466	–	–	99.66	33.520	–	–
boat	99.615	33.467	99.190	33.400	–	–	–	–

密文图像具有白噪音的特点，这样可以使密码破译者无法从加密图像中截获有用的信息。自相关系数是用来衡量图像像素点间相关性的一个重要指标。自相关系数越大，说明像素点间关联程度越大，反之，则表明像素点间关联程度越小。本文分别对(1)cameraman图像；(2)lena图像；(3)boat图像及其加密后的密文图像计算了自相关系数。

从上述图像中随机选取N对相邻像素点，并记其灰度值为(u,v)，则这N对相邻像素点间的相关系数，可以通过式(10)来进行计算。具体计算公式为

$$\left.\begin{aligned} r_{xy} &= \frac{\boldsymbol{cov}(u,v)}{\sqrt{D(u)}\sqrt{D(v)}} \\ \boldsymbol{cov}(u,v) &= \frac{1}{N}\sum_{i=1}^{N}(x_i - E(u))(y_i - E(v)) \\ D(u) &= \frac{1}{N}\sum_{i=1}^{N}(u_i - E(u))^2 \\ E(u) &= \frac{1}{N}\sum_{i=1}^{N}u_i \end{aligned}\right\} \tag{10}$$

不同图像的自相关系数计算结果，如表4所示。

从表4可知，不同明文图像，其6邻域方向均具有较强的自相关性，而通过本文算法加密后，各方向上的自相关性很弱，说明本文加密算法可以很好的隐藏明文中的图像信息。

4.5　信息熵分析

信息熵是衡量信息中不确定性大小的一个重要指标。信息熵越大，说明信息的不确定程度越高，信息的加密效果越好。理想信息熵的值为8[14]，越接近该值，说明图像的加密效果越好。信息熵计算公式，如式(11)所示

$$H(m) = \sum_{i=1}^{2^N-1} p(m_i)\log_2\frac{1}{p(m_i)} \tag{11}$$

其中，m_i表示第i位的像素的值，$p(m_i)$表示像素值为m_i的概率，N表示在密文图像中所有的像素个数。

本文中所用灰度图像的信息熵计算结果，如表5所示。

4.6　算法鲁棒性分析

为了破坏正常的图像加密传输过程，恶意密码破译者可能会对截获到的密文数据进行数据篡改或向密文中添加干扰信息，从而导致加密图像无法被正常解密。因此，对于加密算法而言，应当对密文数据的缺损具有一定的容忍度，当密文数据出现一定程度的缺失或损坏后，也能正常的进行解密操作。这种能力被称为算法鲁棒性。

为了验证本文所提算法的鲁棒性，对加密后的灰度图像数据随机进行像素点移除，并观察是否

表 4　自相关系数

图像	方位角	原始值	加密后
boat	左	0.87986	–0.0029753
	右	0.87578	0.00099645
	上	0.89982	–0.00026347
	下	0.89718	–0.00096155
	左上	0.81343	–0.00034887
	左下	0.82413	–0.00022197
	右上	0.83087	0.00025217
	右下	0.80362	–2.4882e-05
cameraman	左	0.91761	0.0006906
	右	0.92347	0.00017951
	上	0.95272	–0.00039079
	下	0.95336	0.00040691
	左上	0.88771	–0.00042397
	左下	0.90207	3.8675e-05
	右上	0.90196	0.00051293
	右下	0.88703	0.00053786
lena	左	0.94044	–0.00029284
	右	0.93955	–0.00011737
	上	0.96882	0.00014822
	下	0.97068	–0.00053991
	左上	0.91482	–0.00088227
	左下	0.94011	0.00059065
	右上	0.93857	–0.00044307
	右下	0.91636	1.7261e-05

表 5　图像信息熵

图像	信息熵
boat	7.9958
cameraman	7.9944
lena	7.9951

能够正常的进行解密操作。实验仿真结果，如图6所示。

通过图6可知，在密文数据损失10%,30%时，本文算法仍然能够正常的进行解密操作，并且明文数据的有效信息并未严重丢失。当密文数据损失达到50%时，解密后的数据仍然保留的一定程度的有效信息。说明本文所提算法具有较好的算法鲁棒性。

4.7 彩色图像加密

由于本文所提算法主要针对图像像素值进行加密，因此该算法也可对彩色图像进行加密。在对彩色图像进行加密时，首先需要将图像分离为R, G, B 3通道值，之后分别针对各通道数据进行混沌加密，加密完成后，再将加密后的R, G, B通道值进行整合，进而生成加密图像。加解密图像的处理结果，如图7所示。

5 结论

本文通过向1维cosine混沌映射系统中引入指数及高次幂项的方式，构造出了一个具有混沌特性的2D-ECs 2维混沌系统。通过对该系统利用Lyapunov指数计算，分岔图及空间相图绘制等方法进行研究后，发现该系统具有复杂的相空间结构，说明该系统具有非常复杂的混沌行为。在此基础上，本文设计一种基于2D-ECs混沌系统的图像加密算法。本算法具有密钥空间大，加密效果好等特点。仿真实验表明，该算法可以有效的抵御穷举式以及差分式攻击。同时该算法可以有效的消除明文图像中的像素相关性，并且对于明文中像素间的微小变化异常敏感，极微小的变化也可以使加密后的数据完全改变。综上所述，本文所提基于2D-ECs混沌系统

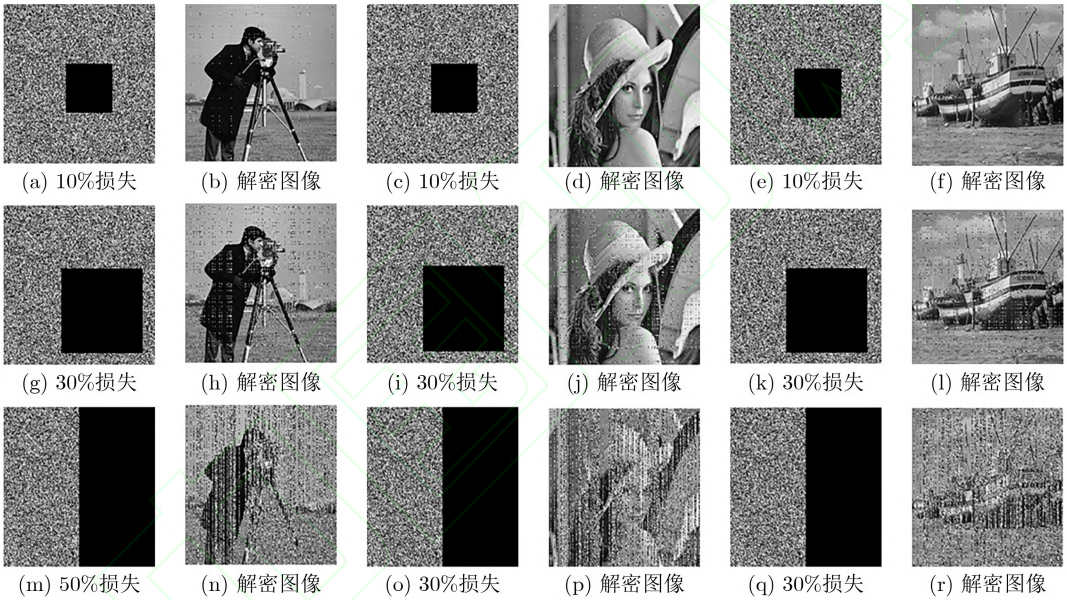

图 6 随机像素点移除

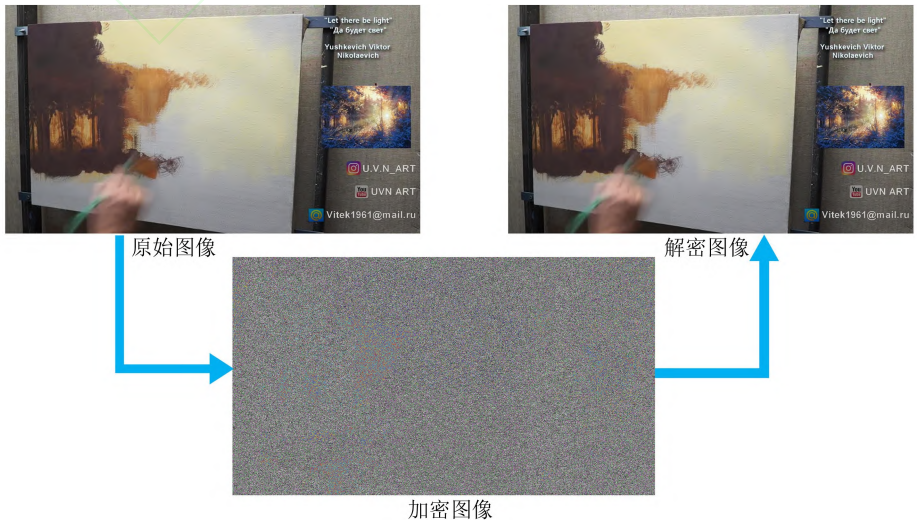

图 7 彩色图像加解密效果图

的图像加密算法具有较高的密码安全性和较好的实际应用前景。

参 考 文 献

[1] MATTHEWS R. On the derivation of a “Chaotic” encryption algorithm[J]. *Cryptologia*, 1989, 13(1): 29–42. doi: 10.1080/0161-118991863745.

[2] STOYANOV B and KORDOV K. Image encryption using Chebyshev map and rotation equation[J]. *Entropy*, 2015, 17(4): 2117–2139. doi: 10.3390/e17042117.

[3] HUANG Xiaoling. Image encryption algorithm using chaotic chebyshev generator[J]. *Nonlinear Dynamics*, 2012, 67(4): 2411–2417. doi: 10.1007/s11071-011-0155-7.

[4] MURILLO-ESCOBAR M A, CRUZ-HERNÁNDEZ C, ABUNDIZ-PÉREZ F, *et al*. A RGB image encryption algorithm based on total plain image characteristics and chaos[J]. *Signal Processing*, 2015, 109: 119–131. doi: 10.1016/j.sigpro.2014.10.033.

[5] 吕群, 薛伟. 结合混沌系统和动态S-盒的图像加密算法[J]. 小型微型计算机系统, 2018, 39(3): 607–613. doi: 10.3969/j.issn.1000-1220.2018.03.038.

LV Qun and XUE Wei. Image encryption algorithm combining chaotic system and dynamic S-boxes[J]. *Journal of Chinese Computer Systems*, 2018, 39(3): 607–613. doi: 10.3969/j.issn.1000-1220.2018.03.038.

[6] HUA Zhongyun and ZHOU Yicong. One-dimensional nonlinear model for producing chaos[J]. *IEEE Transactions on Circuits and Systems I:Regular Papers*, 2018, 65(1): 235–246. doi: 10.1109/TCSI.2017.2717943.

[7] ZHOU Yicong, BAO Long, and CHEN C L P. Image encryption using a new parametric switching chaotic system[J]. *Signal Processing*, 2013, 93(11): 3039–3052. doi: 10.1016/j.sigpro.2013.04.021.

[8] LIU Yang, TONG Xiaojun, and HU Shicheng. A family of new complex number chaotic maps based image encryption algorithm[J]. *Signal Processing:Image Communication*, 2013, 28(10): 1548–1559. doi: 10.1016/j.image.2013.07.009.

[9] HUA Zhongyun and ZHOU Yicong. Image encryption using 2D logistic-adjusted-sine map[J]. *Information Sciences*, 2016, 339: 237–253. doi: 10.1016/j.ins.2016.01.017.

[10] GAN Zhihua, CHAI Xiuli, HAN Daojun, *et al*. A chaotic image encryption algorithm based on 3-D bit-plane permutation[J]. *Neural Computing and Applications*, 2019, 31(11): 7111–7130. doi: 10.1007/s00521-018-3541-y.

[11] YIN Qi and WANG Chunhua. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion[J]. *International Journal of Bifurcation and Chaos*, 2018, 28(4): 1850047. doi: 10.1142/S0218127418500475.

[12] LUO Yuqin, YU Jin, LAI Wenrui, *et al*. A novel chaotic image encryption algorithm based on improved baker map and logistic map[J]. *Multimedia Tools and Applications*, 2019, 78(15): 22023–22043. doi: 10.1007/s11042-019-7453-3.

[13] KHAN M and MASOOD F. A novel chaotic image encryption technique based on multiple discrete dynamical maps[J]. *Multimedia Tools and Applications*, 2019, 78(18): 26203–26222. doi: 10.1007/s11042-019-07818-4.

[14] YE Guodong, PAN Chen, HUANG Xiaoling, *et al*. An efficient pixel-level chaotic image encryption algorithm[J]. *Nonlinear Dynamics*, 2018, 94(1): 745–756. doi: 10.1007/s11071-018-4391-y.

[15] LIU Lidong, LEI Yuhang, and WANG Dan. A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation[J]. *IEEE Access*, 2020, 8: 27361–27374. doi: 10.1109/ACCESS.2020.2971759.

[16] 李春彪, 赵云楠, 李雅宁, 等. 基于正弦反馈Logistic混沌映射的图像加密算法及其FPGA实现[J]. 电子与信息学报, 2022. doi: 10.11999/JEIT200575..

LI Chunbiao, ZHAO Yunnan, LI Yaning, *et al*. . An image encryption algorithm based on logistic chaotic mapping with sinusoidal feedback and its FPGA implementation[J]. *Journal of Electronics & Information Technology*, 2022. doi: 10.11999/JEIT200575..

[17] HUA Zhongyun, ZHOU Yicong, PUN C M, *et al*. 2D sine logistic modulation map for image encryption[J]. *Information Sciences*, 2015, 297: 80–94. doi: 10.1016/j.ins.2014.11.018.

[18] 摆玉龙, 杨阳, 唐丽红. 一个新多涡卷混沌系统的设计及在图像加密中的应用[J]. 电子与信息学报, 2021, 43(2): 436–444. doi: 10.11999/JEIT191002.

BAI Yulong, YANG Yang, and TANG Lihong. Design of a multi-scroll chaotic system and its application to image encryption[J]. *Journal of Electronics & Information Technology*, 2021, 43(2): 436–444. doi: 10.11999/JEIT191002.

[19] 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. doi: 10.11999/JEIT190849.

NIU Ying and ZHANG Xuncai. Image encryption algorithm of based on variable step length Josephus traversing and DNA dynamic coding[J]. *Journal of Electronics & Information Technology*, 2020, 42(6): 1383–1391. doi: 10.11999/JEIT190849.

[20] 李付鹏, 刘敬彪, 王光义, 等. 基于混沌集的图像加密算法[J]. 电子与信息学报, 2020, 42(4): 981–987. doi: 10.11999/JEIT190344.

LI Fupeng, LIU Jingbiao, WANG Guangyi, *et al*. An image encryption algorithm based on chaos set[J]. *Journal of Electronics & Information Technology*, 2020, 42(4):

981–987. doi: 10.11999/JEIT190344.

[21] 陈艳浩, 刘中艳, 周丽宴. 基于差异混合掩码与混沌Gyrator变换的光学图像加密算法[J]. 电子与信息学报, 2019, 41(4): 888–895. doi: 10.11999/JEIT180456.
CHEN Yanhao, LIU Zhongyan, and ZHOU Liyan. Optical image encryption algorithm based on differential mixed mask and chaotic Gyrator transform[J]. *Journal of Electronics & Information Technology*, 2019, 41(4): 888–895. doi: 10.11999/JEIT180456.

[22] YANG Yuguang, WANG Baopu, YANG Yongli, *et al*. Visually meaningful image encryption based on universal embedding model[J]. *Information Sciences*, 2021, 562: 304–324. doi: 10.1016/j.ins.2021.01.041.

[23] MANSOURI A and WANG Xingyuan. A novel one-dimensional chaotic map generator and its application in a new index representation-based image encryption scheme[J]. *Information Sciences*, 2021, 563: 91–110. doi: 10.1016/j.ins.2021.02.022.

[24] 马啸宇, 张金生, 李婷. 基于蔡氏电路和压缩感知的图像压缩加密方法[J]. 系统工程与电子技术, 2021, 43(9): 2407–2412. doi: 10.12305/j.issn.1001-506X.2021.09.05.
MA Xiaoyu, ZHANG Jinsheng, and LI Ting. Image compress and encryption method based on Chua's circuit and compressed sensing[J]. *Systems Engineering and Electronics*, 2021, 43(9): 2407–2412. doi: 10.12305/j.issn.1001-506X.2021.09.05.

[25] 田佳鹭, 邓立国. 基于五阶CNN超混沌系统的图像加密方法[J]. 西华大学学报:自然科学版, 2021, 40(2): 63–70,81. doi: 10.12198/j.issn.1673-159X.3855.
TIAN Jialu and DENG Liguo. Image encryption method based on fifth order CNN hyperchaotic system[J]. *Journal of Xihua University:Natural Science Edition*, 2021, 40(2): 63–70,81. doi: 10.12198/j.issn.1673-159X.3855.

[26] JIANG Xiao, XIAO Ying, XIE Yiyuan, *et al*. Exploiting optical chaos for double images encryption with compressive sensing and double random phase encoding[J]. *Optics Communications*, 2021, 484: 126683. doi: 10.1016/j.optcom.2020.126683.

[27] RAZAQ A, IQRA, AHMAD M, *et al*. A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption[J]. *Multimedia Tools and Applications*, 2021, 80(13): 20191–20215. doi: 10.1007/s11042-021-10587-8.

[28] ZHU Hegui, DAI Lewen, LIU Yating, *et al*. A three-dimensional bit-level image encryption algorithm with Rubik's cube method[J]. *Mathematics and Computers in Simulation*, 2021, 185: 754–770. doi: 10.1016/j.matcom.2021.02.009.

[29] ABBASI A A, MAZINANI M, and HOSSEINI R. Evolutionary-based image encryption using biomolecules and non-coupled map lattice[J]. *Optics & Laser Technology*, 2021, 140: 106974. doi: 10.1016/j.optlastec.2021.106974.

[30] WANG Xingyuan, CHEN Shengnan, and ZHANG Yingqian. A chaotic image encryption algorithm based on random dynamic mixing[J]. *Optics & Laser Technology*, 2021, 138: 106837. doi: 10.1016/j.optlastec.2020.106837.

[31] SU Yonggang, XU Wenjun, LI Tianlun, *et al*. Optical color image encryption based on fingerprint key and phase-shifting digital holography[J]. *Optics and Lasers in Engineering*, 2021, 140: 106550. doi: 10.1016/j.optlaseng.2021.106550.

[32] CHEN Hang, LIU Zhengjun, TANOUGAST C, *et al*. Comment on "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation"[J]. *Optics & Laser Technology*, 2021, 138: 106901. doi: 10.1016/j.optlastec.2020.106901.

刘思聪：男，1986年出生，讲师，研究方向为离散混沌系统与信息安全、神经网络与智能信息处理.

李春彪：男，1971年出生，教授，研究方向为混沌系统、忆阻神经形态电路与网络及其应用.

李泳新：男，1997年出生，硕士生，研究方向为离散混沌系统、忆阻神经网络与应用.

责任编辑：余 蓉