

# 一种基于离散分数阶混沌系统和 DNA 序列运算的新型彩色图像加密算法

陈立平<sup>1</sup>, 尹昊<sup>1</sup>, 袁利国<sup>2</sup>, António M. LOPES<sup>3</sup>,

J. A. Tenreiro MACHADO<sup>4</sup>, 吴然超<sup>5</sup>

<sup>1</sup>合肥工业大学电气与自动化工程学院, 中国合肥市, 230009

<sup>2</sup>华南农业大学数学与信息学院, 中国广州市, 510642

<sup>3</sup>波尔图大学工程学院, 葡萄牙波尔图市, 4200-465

<sup>4</sup>波尔图理工学院电气工程系, 葡萄牙波尔图市, 4249-015

<sup>5</sup>安徽大学数学科学学院, 中国合肥市, 230601

**摘要:** 提出一种基于动态DNA编码和混沌的新型彩色图像加密算法。将一个三神经元分数阶离散Hopfield神经网络作为伪随机混沌序列发生器。其初值由外部输入的五位密钥以及明文图像的哈希值计算得来。外部密钥包含分数阶离散Hopfield神经网络的离散步长和阶次。哈希值由SHA-2函数计算得到。在保证较大密钥空间的同时, 提高了算法对明文图像的敏感性。在此基础上, 提出一种新型三维投影置乱方法, 置乱图像红、绿、蓝信号通道中像素位置。DNA编码以及扩散被用于扩散图像信息。使用离散分数阶Hopfield神经网络生成的伪随机数序列确定每个像素的编码规则, 用以保证编码方式的多样性。最后, 运用置乱 $\Pi$ 和XOR提升算法的安全性。实验结果和安全性分析表明, 该算法具有较好安全性, 能够抵御多种典型攻击。

**关键词:** 分数阶离散系统; 神经网络; DNA加密; 彩色图像加密

<https://doi.org/10.1631/FITEE.1900709>