一种基于新型耦合映像格子系统和 DNA 运算的图像压缩加密方案

李媛媛[1]，游晓庆[2]，卢剑权[3]，楼俊钢[4,5]
[1]南京林业大学理学院应用数学系，中国南京市，210037
[2]东南大学网络空间安全学院，中国南京市，210096
[3]东南大学数学学院系统科学系，中国南京市，210096
[4]湖州师范学院长三角（湖州）智慧交通研究院，中国湖州市，313000
[5]浙江师范大学计算机科学与技术学院，中国金华市，321004

摘要：本文提出一种基于混合线性-非线性耦合逻辑映像格子（NMLNCML）系统和 DNA 运算的有效图像加密方案。所提出的 NMLNCML 系统增强了系统的混沌特性，适用于图像加密。该加密系统具有大量的密钥空间；对密钥的敏感性高；对选择明文攻击、统计学攻击和差分攻击具有很强的抵抗能力；并且对一定程度的噪声和数据丢失有很好的鲁棒性。提出的图像密码系统采用置乱—压缩—扩散的架构。首先，通过离散小波变换将普通图像变换为稀疏系数矩阵，并对系数矩阵执行与明文相关的 Arnold 置乱。然后，采用半张量积（STP）压缩感知对系数矩阵进行压缩和加密。最后，通过 DNA 随机编码、DNA 加法，和位 XOR 运算来扩散压缩系数矩阵。NMLNCML 系统用于在压缩传感的 STP 测量矩阵和 DNA 操作中的伪随机序列中生成混沌元素。SHA-384 函数用于产生明文密钥，从而使所提出的加密算法对原始图像高度敏感。仿真结果和性能分析验证了该方案的安全性和有效性。

关键词：压缩感知；耦合映像格子（CML）；DNA运算；半张量积
https://doi.org/10.1631/FITEE.2200645