

基于改进的复合混沌系统的图像加密算法

魏 慧, 李国东, 许向亮

(新疆财经大学 统计与数据科学学院, 新疆 乌鲁木齐 830012)

摘 要: 针对单一混沌系统加密不足的问题: 主要提出的算法是基于改进的 LCL 复合混沌系统和 DFT 变化的图像加密算法. 首先对图像 DFT 变换, 应用高维 Lorenz 系统产生的混沌序列进行随机组合排列, 将得到的一组索引序列结合改进的 Cat 系统对明文图像进行置乱; 其次, 采用超 Lorenz 混沌系统设计得到 Logistic 映射的伪随机序列, 将其进行异或处理得到密文图像; 为了达到加密效果更优良的目的, 重复以上步骤进行循环加密处理. 仿真结果表明本文设计算法具有优良的加密效果, 密钥空间大、明密文敏感性强、能有效抵抗统计攻击等.

关键词: 二维离散傅里叶变换; 混沌映射; 信息熵; 图像加密

Image encryption algorithm based on improved complex chaotic system

WEI Hui, LI Guo-dong, XU Xiang-liang

(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

Abstract: Aiming at the problem of insufficient encryption of a single chaotic system, the main proposed algorithm is an image encryption algorithm based on improved LCL composite chaotic system and DFT variation. Firstly, DFT transformation of images is carried out, chaotic sequences generated by high-dimensional Lorenz system are randomly combined and arranged, and a group of obtained index sequences are combined with an improved Cat system to scramble plaintext images; Secondly, the pseudo-random sequence of Logistic map is designed by using hyper-Lorenz chaotic system, and the encrypted image is obtained by XOR processing. In order to achieve better encryption effect, repeat the above steps for cyclic encryption. The simulation results show that the algorithm designed in this paper has excellent encryption effect, large key space, strong sensitivity to plaintext, and can effectively resist statistical attacks.

Key words: 2-D discrete Fourier transform; Chaotic mapping; Information entropy; Image encryption

作者简介:

魏 慧 女, (1996-), 硕士研究生. 研究方向为数字分析与图像处理.

李国东 (通讯作者) 男, (1976-), 博士, 教授. 研究方向为数字分析与图像处理. E-mail: lgdzhzy@126.com.