计算机工程与应用 2008 44 (4): 125-126 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

一种基于统一混沌系统的图像加密新算法

韩凤英[1, 2]

1.长沙航空职业技术学院，长沙 410124
2.中南大学信息科学与工程学院，长沙 410083

收稿日期 2007-5-28 修回日期 2007-8-13 网络版发布日期 2008-1-21 接受日期

摘要 提出了一种新的基于统一混沌系统的图像加密新算法。首先，利用统一混沌系统的二维序列排序后的位置编号置乱图像像素位置。然后引进三个辅助密钥，将统一混沌系统输出的三维混沌序列两两异或后得到的混沌密钥序列对置乱图像进行逐像素加密。实验和分析结果表明：算法具有良好的像素值混淆和扩散性能，具有抵抗强力攻击的足够大密钥空间，加密图像像素值具有类随机均匀分布特性，且相邻像素具有零相关特性。这些结果表明了所提出方案的安全性很高。

关键词 混沌 统一混沌系统 混沌排序 图像加密 混淆 扩散

分类号

New image encryption algorithm based on unified chaotic system

HAN Feng-ying[1,2]

1.Changsha Aeronautical Vocational and Technical College，Changsha 410124，China
2.School of Information Science and Engineering，Central South University，Changsha 410083，China

Abstract

A new image encryption algorithm based on unified chaotic system is proposed.Firstly，the two chaotic sequences of the unified chaotic system are used to shuffle the positions of the image pixels in the spatial-domain.The introduces into three encrptpions assisting the secret key，differect of the three chaotic sequences of the unified chaotic system are adopted to generate bykey sequences，and the shuffled image is encrypted by pixel.The experimental and theoretical results demonstrate that the algorithm has well properties of confusion and diffusion.The key space is large enough to resist the brute-force attack.For the encrypted image the distribution of grey values has a random-like behavior and the adjacent pixels satisfy zero correlation.These results indicate that the proposed scheme has high security.

Key words chaos unified chaotic system image encryption Chaos is ordered confusion diffusion

DOI:

通讯作者 韩凤英