计算机应用 2008 28 (02): 434-436 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

一种基于混合反馈的混沌图像加密算法

高洁[1];袁家斌[2];徐涛[2];齐艳珂[2]

郑州航空工业管理学院[1]

南京航空航天大学[2]

收稿日期 2007-9-5 修回日期 2007-11-19 网络版发布日期 2008-1-30 接受日期

摘要 针对现有基于混沌分组密码的图像加密算法中，扩散函数扩散速度慢、需要多轮迭代才能抵抗差分攻击的缺点，提出了一种新的基于密文和输出混合反馈的混沌图像加密算法。该算法利用密文扰动混沌系统的初始值，既改善了数字混沌的退化，又能使扩散函数具有非常快的扩散速度。经过实验验证，该算法只需正反两轮迭代，就能达到较高的安全性和较快的加解密速度。

Abstract Aiming at the defects of diffusion function with lower diffusing speed and needing multiple round iteration to resist differential attack in the image encryption algorithm based on chaotic block cipher, a new chaotic image encryption algorithm based on output cryptograph mixed feedback was proposed. It can improve the degradation of digital chaotic and diffusing speed of diffusion function through perturbating initial value of chaotic system with ciphertext. Experimental results show that the iterative algorithm only requires a positive iteration and an inverse iteration to achieve higher levels of security and faster encryption speed.

关键词 图像加密 混合反馈 混沌分组密码

Key words image encryption;hybrid feedback;chaotic block cipher

分类号

DOI:

通讯作者:
高洁 gjnuaa@nuaa.edu.cn;gjlw0@126.com

作者个人主页: 高洁 袁家斌 徐涛 齐艳珂