计算机工程　2007 33 (20): 165-166,169　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

CH混沌序列图像加密算法分析

张 斌，金晨辉

(信息工程大学电子技术学院，郑州 450004)

收稿日期　修回日期　网络版发布日期 2007-10-11　接受日期

摘要　分析了一个基于混沌序列的图像加密算法的安全性，发现该加密算法本质上是一个移位密码且密钥空间太小，利用古典密码中对移位密码的分析方法得到混沌序列，进而给出了穷举参数求解其密钥的已知明文攻击方法。对于大小为M×N的明文图像，该攻击方法的计算复杂性为O(M+N)。理论分析和实验结果均表明该图像加密算法是不安全的。

关键词　混沌密码；图像加密；密码分析；已知明文攻击

分类号　TN918

DOI:

对应的英文版文章：072059b

通讯作者:

作者个人主页: 张 斌;金晨辉