计算机应用 2009, 29(10) 2681-2683 DOI: ISSN: 1001-9081 CN: 51-1307/TP

图形图像处理

基于Logistic混沌序列和位交换的图像置乱算法

袁玲[1],康宝生[2]

1. 西北大学信息科学与技术学院新疆喀什师范学院信息工程技术系
2. 西北大学信息科学与技术学院

摘要： 在分析传统迭代型图像置乱方法不足的基础上，提出一种新的基于混沌序列和位交换的图像置乱算法。算法根据各像素点的位置，采用不同的Logistic混沌序列和像素值的二进制序列进行异或操作改变图像像素值，并利用图像本身的自相关性进行加密，不需迭代，经过一次运算即可得到加密图像。仿真实验结果表明，该算法可有效地实现灰度和彩色图像置乱，并能较好地抵抗椒盐和裁剪攻击，在效率上也优于迭代型置乱方法。

关键词： 图像置乱 位交换 混沌序列 密钥 迭代

Image scrambling algorithm based on Logistic chaotic sequence and bit exchange

Abstract: Based on the analysis of the defect of the traditional iterated image scrambling, a new image scrambling algorithm was proposed based on chaotic sequence and bit exchange. According to the pixel location, the algorithm changed the image pixel values by using XOR operation in different Logistic chaotic sequence and the binary sequences of pixel value. Without iteration, the algorithm used the self-relativity of image to encrypt image. Experimental data and results show that the algorithm can achieve more effective image scrambling compared with the traditional algorithm. The algorithm has good performance in resisting the salt pepper and cutting attack. Compared with the iterative type s scrambling methods, it has higher efficiency too.

Keywords: image scrambling bit exchange chaotic sequence secret key iteration

收稿日期 2009-04-01 修回日期 2009-05-24 网络版发布日期 2009-10-28

DOI:

基金项目:

无

通讯作者: 袁玲

作者简介:

作者Email: julyyuan@163.com

参考文献：

本刊中的类似文章

1．孙卫平; 尹霞; 施新刚.密钥交换协议性能测试研究[J]. 计算机应用, 2006,26(4): 824-826

2．雷明 杨丹 雷明 罗建禄.基于二代小波和图像置乱的数字图像盲水印算法[J]. 计算机应用, 2007,27(2): 295-298

3．王梦 金文标 .基于函数迭代系统的3-D分形插值算法[J]. 计算机应用, 2006,26(11): 2701-2703

4．杨涛;刘锦德;谭浩.Web服务安全基础设施的研究[J]. 计算机应用, 2006,26(6): 1248-1250

5．叶永飞 余梅生.基于簇结构的Ad Hoc网络安全密钥管理方案[J]. 计算机应用, 2007,27(3): 611-613

6. 李志军 耿技 王佳昊 秦志光 .传感器网络的多重单向散列随机密钥预分配协议[J]. 计算机应用, 2006,26(8): 1802-1806
7. 叶文珺; 郑骞; 耿新民.基于遗传算法的异构分布式并行分形图像压缩算法[J]. 计算机应用, 2006,26(4): 793-796
8. 唐斌兵 陈团强 王正明.基于小波变换的图像配准方法[J]. 计算机应用, 2007,27(9): 2103-2105
9. 刘良 邓亚平 李钦 王江波 .一种基于ID的传感器网络密钥管理方案[J]. 计算机应用, 2006,26(10): 2347-2350
10. 陈妮 姚剑波 文光俊.无线传感器网络中一种改进的密钥管理方案[J]. 计算机应用, 2008,28(10): 2478-2480
11. 毕方明 张虹 闫大顺 .一种对等信任模型的研究与实现[J]. 计算机应用, 2006,26(10): 2315-2317
12. 石峰 戴冠中 刘航 苗胜 李美峰 .基于门限方案的智能卡密钥管理系统的设计与实现[J]. 计算机应用, 2006,26(9): 2156-2159
13. 李伟 方江涛 郝林 .同余方程加密方案的研究[J]. 计算机应用, 2006,26(9): 2114-2115
14. 陈卓 金豪 张正文 .一种无线局域网多安全域间的密钥共识协议[J]. 计算机应用, 2006,26(9): 2121-2123
15. 杨建强 .基于Java ME的点到点短信加密应用[J]. 计算机应用, 2006,26(8): 1813-1816
16. 章静; 许 力; 林志伟.自组网中基于簇的混合密钥管理策略[J]. 计算机应用, 2006,26(6): 1328-1330
17. 宣文霞.一种适合大型动态多播的密钥管理方案[J]. 计算机应用, 2006,26(6): 1334-1336
18. 董亮卫;汪文勇;黄鹂声.支持单点登录的统一资源管理体系研究[J]. 计算机应用, 2006,26(5): 1146-1147
19. 闫鸿滨; 袁丁.基于单向函数的动态密钥托管方案[J]. 计算机应用, 2006,26(5): 1093-1095
20. 江沸菠 王玲 董莉.一种新的移动Ad Hoc网络的按需同步码分多址协议[J]. 计算机应用, 2007,27(4): 818-820
21. 刘文艳.基于GDH的协商式虚拟动态子群组密钥管理方案[J]. 计算机应用, 2007,27(4): 849-851
22. 马文静 陈辉 田宏阳.线性拟合联合参数法在图像配准中的应用[J]. 计算机应用, 2007,27(4): 976-978
23. 余昭平 康斌.基于ECC的高效可认证组密钥协商协议[J]. 计算机应用, 2007,27(5): 1033-1034
24. 商建伟 李锋 张燕燕.一种入侵容忍的广播通讯KDC方案[J]. 计算机应用, 2007,27(5): 1038-1040
25. 王晓华 赵明.一种XP项目迭代周期估计方法[J]. 计算机应用, 2007,27(5): 1248-1250
26. 谭利平 李方伟.移动通信系统中的认证与密钥协商协议[J]. 计算机应用, 2007,27(6): 1343-1344
27. 何毅俊 李杰 徐楠.提供向前保密性的无线密钥交换和双向认证协议[J]. 计算机应用, 2007,27(7): 1603-1605
28. 杨曦 侯整风.一种可定期更新的多秘密共享方案[J]. 计算机应用, 2007,27(7): 1609-1610
29. 田捷 张新访 宋翊灵 程明.手持设备上可变运动矢量的多媒体版权方案[J]. 计算机应用, 2007,27(7): 1611-1612
30. 张楠 张建华 陈建英 谈文蓉 赵国.无线传感器网络中基于混沌的密钥预分配方案[J]. 计算机应用, 2007,27(8): 1901-1903
31. 张建民 刘贤德 徐海峰.基于Hash函数的无线传感器网络密钥预分配方案[J]. 计算机应用, 2007,27(8): 1904-1906
32. 张慧档 贺昱曜.基于混沌序列的SVM参数选择及其在笔迹鉴别中的应用[J]. 计算机应用, 2007,27(8): 1961-1963
33. 张艳硕 刘卓军 .有门限可认证的多重秘密密钥协商方案[J]. 计算机应用, 2007,27(10): 2450-2452
34. 周翔翔 尹忠海 刘守义 韩毅娜 .一种基于密钥的水印嵌入位置置乱算法[J]. 计算机应用, 2007,27(10): 2473-2474
35. 李平 吴佳英.传感器网络中对偶密钥建立协议研究[J]. 计算机应用, 2008,28(1): 62-64
36. 向文 陶良升 王同洋.一种高效的WTLS握手协议[J]. 计算机应用, 2008,28(11): 2798-2800
37. 沈金波 许力 陈建伟.无线传感器网络中一种安全高效的共享密钥发现协议[J]. 计算机应用, 2008,28(11): 2817-2819
38. 杨斌 熊选东 苏克军.基于仲裁者的身份加密方案研究[J]. 计算机应用, 2008,28(11): 2835-2836
39. 宋华 刘江.一种基于二次误差测度的三维累进网格生成算法[J]. 计算机应用, 2008,28(12): 3160-3162
40. 向新银.可认证的无证书密钥协商协议[J]. 计算机应用, 2008,28(12): 3165-3167
41. 张学峰 姜皇普 王永栓.基于矩阵格的传感器网络密钥预配置方案[J]. 计算机应用, 2008,28(1): 85-87
42. 张政 张小虎 傅丹.一种高精度鲁棒的基于直线对应的位姿估计迭代算法[J]. 计算机应用, 2008,28(2): 326-329,
43. 周耀伟 邱卫东 温蜜.一种带认证的ＬＵ密钥预分配方案[J]. 计算机应用, 2009,29(1): 161-164
44. 胡宏银 姚峰 何成万.一种基于文件过滤驱动的Windows文件安全保护方案[J]. 计算机应用, 2009,29(1): 168-171

45. 曾玮妮 林亚平 卢秋英.无线传感器网络中基于簇协作的分布式组密钥管理方案[J]. 计算机应用, 2009,29(3): 638-842
46. 史安生 吕东辉 张海燕 杨云峰.足部标记图像中标尺提取与像素测量[J]. 计算机应用, 2009,29(2): 468-469
47. 李洁 吴振强 于璐 孙鹏 程瑶.一种改进的直接匿名认证方案[J]. 计算机应用, 2009,29(2): 364-366
48. 谢松 郭忠文 曲海鹏 吕广鹏.基于多密钥空间的无线传感器网络密钥管理方案[J]. 计算机应用, 2009,29(4): 932-934,
49. 程东升 叶瑞松.基于四维混沌系统生成二值序列的方法及其加密应用[J]. 计算机应用, 2008,28(3): 677-679
50. 朱建新 李成华 张新访.对一种基于身份的强密钥绝缘签名方案的改进[J]. 计算机应用, 2008,28(5): 1128-1129
51. 王丽美 费金龙 祝跃飞.防御蓝牙PIN码攻击的研究与实现[J]. 计算机应用, 2009,29(4): 941-943,
52. 郝晓弘 段晓燕 李恒杰.基于BP神经网络的迭代学习初始控制策略研究[J]. 计算机应用, 2009,29(4): 1025-1027
53. 吴书凯 都思丹 李华.基于半规则网格的视差估计算法[J]. 计算机应用, 2008,28(4): 957-959
54. 黄河 王亚弟 韩继红 栗帅.一种基于令牌环的密钥元更新方案[J]. 计算机应用, 2008,28(5): 1158-1160
55. 章志明 王祖俭 彭雅丽 余敏.一种无线传感器网络的密钥管理方案[J]. 计算机应用, 2008,28(5): 1164-1166
56. 田丰 王交峰 王传云 潘琢金 孙小平.无线传感器网络随机密钥预分配改进方案[J]. 计算机应用, 2008,28(6): 1388-1391
57. 罗捷 严飞 余发江 张焕国.可信计算平台模块密码机制研究[J]. 计算机应用, 2008,28(8): 1907-0911
58. 陈宇环 易称福.基于时空混沌序列的视频加密设计与实现[J]. 计算机应用, 2008,28(8): 1936-1939
59. quietloner.高效的动态安全组播密钥协商方案[J]. 计算机应用, 2008,28(8): 1943-1945
60. 刘瑞华 鲍政.基于Gibbs分布的盲图像修复[J]. 计算机应用, 2008,28(9): 2281-2284
61. 吴成茂 田小平 谭铁牛.基于差分互信息距离的图像置乱效果评价法 [J]. 计算机应用, 2009,29(05): 1293-1300
62. 叶晓彤 彭奘 简清明.基于无可信第三方IBS的XML数字签名 [J]. 计算机应用, 2009,29(05): 1297-1300
63. 徐巧娟 郑燕飞 陈克非 朱博.基于LU矩阵空间的随机对密钥预分配方案[J]. 计算机应用, 2009,29(07): 1816-1819
64. 张建民 李建 刘贤德.无线传感器网络中基于区组设计的密钥预分配方案 [J]. 计算机应用, 2009,29(06): 1622-1624
65. 万武南 索望 陈运.基于公钥的3G认证和密钥分配协议 [J]. 计算机应用, 2009,29(06): 1625-1661
66. 张辉 渠瀛 海丹 李勇 陈龙伟.基于聚类匹配的移动机器人地图实时创建算法 [J]. 计算机应用, 2009,29(08): 2116-2119
67. 胡国政 洪帆.一个无证书代理签名方案的安全性分析 [J]. 计算机应用, 2009,29(08): 2204-2206
68. 常郝 周国祥.基于书写力与字形信息的生物特征密钥生成 [J]. 计算机应用, 2009,29(08): 2207-2209
69. 张小彬 韩继红 王亚弟 刘敏.基于分簇的Ad Hoc网络组密钥建立方案 [J]. 计算机应用, 2009,29(08): 2213-2217
70. 谢颂华 陈黎 陈建勋 聂晖.迭代分水岭和脊检测的图像分割[J]. 计算机应用, 2009,29(10): 2668-2670
71. 赵冠华.基于二次Renyi熵的非迭代最小二乘支持向量机预测模型[J]. 计算机应用, 2009,29(10): 2751-2754
72. 傅迎华 陈玮 付东翔.二值分解压缩和Consensus算法 [J]. 计算机应用, 2009,29(10): 2703-2705
73. 邓亚平 付红 谢显中 张玉成 石晶林.基于公钥体制的3GPP认证与密钥协商协议[J]. 计算机应用, 2009,29(11): 2936-2938
74. 刘金梅 丘水生.几类混沌伪随机序列复杂度的稳定性[J]. 计算机应用, 2009,29(11): 2946-2947
