系统工程与电子技术 2012, 34(6) 1283-1287 DOI: 10.3969/j.issn.1001-506X.2012.06.36 ISSN: 1001-506X CN: 11-2422/TN

软件、算法与仿真

JPEG彩色图像加密新算法

文昌辞[1]，王沁[1]，陈庆[2]，袁志树[3]，苗晓宁[4]

1. 北京科技大学计算机科学与技术系，北京 100083；2. 二炮692厂军代室，泸州 646605；
3. 空军京昌代表室，北京 100041；4. 空军二院283厂军代室，北京 100854

摘要：

基于复合混沌和有限整数域上的仿射变换，提出一种结合彩色图像压缩编码的加密算法。先在空域对红、绿、蓝分量以8×8大小块为基本单元统一进行位置置乱，打乱分量之间的组合关系，接着进行正常的压缩。在量化系数之后，对所有的直流系数统一进行置乱、自适应地代换和扩散，对所有的交流系数统一进行置乱、自适应地改变符号位，其中置乱操作在改变系数位置的同时根据坐标混合它的值，自适应的操作通过利用中间数据扰动复合混沌系统来实现。算法密钥空间大，敏感性强，安全性高；构造的复合混沌系统形式简单，易于并行实现；得到的密文与直接压缩的图像大小相当。

关键词： 加密 自适应 置乱 混沌 压缩

Novel encryption for JPEG color image

WEN Chang-ci[1]，WANG Qin[1]，CHEN Qing[2]，YUAN Zhi-shu[3]，MIAO Xiao-ning[4]

1. Department of Computer Science and Technology, University of Science and Technology Beijing, Beijing 100083, China〖JP〗
2. Representative of fice of Factory 692, Second Artillery of the PLA, Luzhou 646605, China;
3. Jing Chang of fice of Air Force of the PLA, Beijing 100041, China;
4. Representtative of fice of Factory 283, Air Force of the PLA, Beijing 100854, China

Abstract:

On the basis of compound chaos and affine transformation in finite integer domain, a novel encryption algorithm is proposed, which is embedded in the compression process of color images. Firstly, it scrambles the blocks of 8×8 pixels of red, green and blue components globally in space domain to disarrange the combination relationship among three components, and then proceeds with normal compression. Secondly, it scrambles, self-adaptively replaces and diffuses the frequency domain’s all direct current coefficients universally after quantization. Lastly, it scrambles alternating current coefficients’ value and changes alternating current coefficients’ signs self adaptively. The scrambling function in it mixes coefficients’ value according to corresponding coordination when changing coefficients’ position, and the self-adaptive function is implemented by introducing image data in the process to disturb the chaos system. The algorithm has huge key space, strong sensitivity and high security. The constructed compoundchaos system, which has a brief form, can be realized parallel conveniently. The ciphertext has almost the same size as original image after direct compression.

Keywords: encryption self-adaptive scramble chaos compression

收稿日期 修回日期 网络版发布日期

DOI: 10.3969/j.issn.1001-506X.2012.06.36

基金项目:

通讯作者:

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1. 何学辉，曾操，苏涛，吴顺君.基于二阶锥规划的峰值旁瓣抑制滤波器设计[J]. 系统工程与电子技术，2009,31

(11): 2567-2570
2. 谷小飞,宋建社,杨檬.基于积分方程的电磁散射优化计算[J]. 系统工程与电子技术, 2009,31(11): 2607-2609
3. 宋鸿梅1,2,王岩飞1,潘志刚1.基于FFT BAQ的SAR原始数据压缩新算法[J]. 系统工程与电子技术, 2009,31(11): 2613-2617
4. 徐湘元.反推技术及其在不确定系统中的应用[J]. 系统工程与电子技术, 2009,31(11): 2703-2709
5. 于金涛,1,2,梁廷伟2.FLAKF在无陀螺惯性测量组合中的应用[J]. 系统工程与电子技术, 2009,31(11): 2710-2713
6. 郭文成， 师五喜， 郭利进.一类不确定非线性系统的自适应模糊控制[J]. 系统工程与电子技术, 2010,32(2): 351-354
7. 王宇野, 许红珍.异结构不确定混沌系统的广义投影同步[J]. 系统工程与电子技术, 2010,32(2): 355-358
8. 甘敏，彭辉.基于带回归权重RBF-AR模型的混沌时间序列预测[J]. 系统工程与电子技术, 2010,32(4): 820-824
9. 陈阿磊，王党卫，马晓岩，粟毅.一种基于估计理论的ISAR超分辨成像方法[J]. 系统工程与电子技术, 2010,32(4): 740-744
10. 朱明哲，姬红兵，金艳.基于自适应抽取STFT的混合DS/FH扩频信号参数估计[J]. 系统工程与电子技术, 2010,32(3): 454-457
11. 王泉德, 文必洋.高频地波雷达海杂波神经网络选择集成预测[J]. 系统工程与电子技术, 2009,31(12): 2801-2805
12. 刘卫华, 何明一.基于高斯混合模型图像局部自适应去噪算法[J]. 系统工程与电子技术, 2009,31(12): 2806-2808
13. 朱圣棋，廖桂生，周争光，曲毅，刘向阳.机载双通道SAR地面慢速运动目标参数估计方法[J]. 系统工程与电子技术, 2009,31(12): 2848-2852
14. 宋立众，乔晓林，吴群.一种极化分集制导雷达及低截获概率信号设计[J]. 系统工程与电子技术, 2009,31(12): 2853-2858
15. 高志峰，姜斌.一类参数不确定的线性时变系统的故障调节[J]. 系统工程与电子技术, 2009,31(12): 2924-2928