电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (8) :2015-2018 DOI: 10.3724/SP.J.1146.2009.01071

研究简报

分组排列模式下图像加密算法的扩散性能分析与实现

周庆 胡月 廖晓峰*

重庆大学计算机学院 重庆 400044

Analysis of the Diffusion Property of Image Encryption Algorithm in Block-and-Permutation Mode and Its Implementation

Zhou Qing Hu Yue Liao Xiao-feng*

Institution of Computer Science, Chongqing University, Chongqing 400044, China

摘要 | 参考文献 | 相关文章

Download: PDF (201KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘要 该文研究了分组排列模式下图像加密的扩散性能，提出了最优扩散性与“无碰撞”排列两个概念。最优扩散性指以最少的加密轮数实现图像的全局扩散性。在分组排列模式下，当且仅当排列算法满足“无碰撞”要求时，图像加密算法具备最优扩散性。根据“无碰撞”排列的概念提出了四叉树排列算法，并证明该算法可满足最优扩散性的要求。

关键词： 图像加密 扩散 四叉树 排列

Abstract： The diffusion property of image encryption algorithms in block-and-permutation mode is investigated, where two new conceptions, the optimal diffusion and ‘collision-free’ permutation are put forward. An image encryption algorithm in block-and-permutation mode fulfills the requirement of optimal diffusion when the global diffusion is achieved within the ideally least round, which is feasible if and only if the permutation is ‘collision-free’. Further more, a permutation algorithm based on quadtree structure is proposed, which is proved to fulfill the requirement of the optimal diffusein.

Keywords： Image encryption Diffusion Quadtree Permutation

Received 2009-08-10;

本文基金:

国家自然科学基金(60703035,60873201)和重庆市自然科学基金(CSTC，2009BA2024；CSTC，2009BB2208)资助课题

通讯作者: 周庆 Email: tzhou@cqu.edu.cn

引用本文:

周庆, 胡月, 廖晓峰.分组排列模式下图像加密算法的扩散性能分析与实现[J] 电子与信息学报, 2010,V32(8): 2015-2018

Zhou Qing, Hu Yue, Liao Xiao-Feng.Analysis of the Diffusion Property of Image Encryption Algorithm in Block-and-Permutation Mode and Its Implementation [J] , 2010,V32(8): 2015-2018

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01071 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I8/2015

Service

把本文推荐给朋友

加入我的书架

加入引用管理器

Email Alert

RSS

作者相关文章

周庆

胡月

廖晓峰