通 信 学 报
Journal on Communications

邓晓衡,廖春龙,朱从旭,陈志刚.像素位置与比特双重置乱的图像混沌加密算法[J].通信学报,2014,(3):216~222

像素位置与比特双重置乱的图像混沌加密算法

Image encryption algorithms based on chaos throughdual scrambling of pix

投稿时间： 2012-07-24

DOI：10.3969/j.issn.1000-436x.2014.3.025

中文关键词：图像加密 混沌系统 像素置乱 比特置乱

英文关键词:image encryption chaotic system pixels scrambling bit scrambling

基金项目:国家自然科学基金资助项目(61379058, 61379057,61350011, 60903058)；湖南省自然科学基金资助项目(10JJ6093)

作者	单位
邓晓衡，廖春龙，朱从旭，陈志刚	中南大学 信息科学与工程学院，湖南 长沙 410083

中文摘要:

针对当前流行的一类具有置乱—扩散结构的混沌图像加密算法存在的安全缺陷问题，提出了一种能抵抗选择明(密)文攻击的图像加密算法根据明文像素值的特征和输入的密钥，分别产生混沌系统的参数和预迭代次数。首先，利用混沌序列实现图像像素位置的全局置乱；其次，像素值中0 bit、1 bit的置乱。实现了混沌映射产生的序列与图像本身内容的关联，从而实现了中间密钥随明文自适应变化，能有效抵抗选择明以往算法不能抵抗选择明(密)文攻击的缺陷，同时具有加密算法简单、密钥空间大等加密性能，并能较好地抵抗统计特性分析、差分分析攻击

英文摘要:

As the current popular chaos-based image encryption algorithms with the permutation－diffusion structure have security flaws of no immunity to att proposed based on the analysis of current algorithms, which can well resist the chosen-plaintext and the chosen-ciphertext attacks. The algorithm uses K produces the parameters of the chaotic system and the iteration times according to the characteristics of plaintext pixels and input key. Firstly, the positi chaotic se-quence. Secondly, the 0 and 1 bit positions of image pixels were scrambled by using another chaotic sequence generated by the input key. The cannot only resist the chosen plaintext attack and chosen ciphertext attack but also achieve better cryptographic properties,such as key space, statistical

查看全文 查看/发表评论 下载PDF阅读器

关闭