一种新的基于比特置乱的超混沌图像加密算法

谢国波，王　添

（广东工业大学 计算机学院 ，广东 广州 510006）

摘　要： 提出了一种新的基于超混沌和比特替换的图像加密算法.算法所采用的混沌系统为 Hyperhenon 映射和 Kent 映射，而且在加密过程中引入了与图像本身特性密切相关的参数.首先是利用 Kent 映射所产生的一组混沌序列来对明文图像位置进行置乱；再通过 Hyperhenon 映射产生的混沌序列，结合该混沌序列的特性来对每个像素进行内部比特置乱和像素扩散，从而使明文图像达到更好地加密效果.实验仿真结果显示，新的加密算法既能较好地抵抗统计特性分析和差分攻击，又能有效抵抗选择明文（密文）攻击，还具有密钥空间大、加密效果好等优点.

关键词： 混沌系统；图像加密；比特；Kent 映射；Hyperhenon 映射

A Novel Hyperchaotic Image Encryption Algorithm Based on Bit Scrambling

XIE Guo-bo ,WANG Tian

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510006，China)

Abstract： We propose a new chaotic image encryption algorithm based on hyperchaotic and bit substitution .The algorithm uses Hyperhenon map and Kent map , and makes the encryption process be related closely with the plaintext image’s self characteristics. First, A chaotic sequence generated by Kent map is used to make image position global scrambling ;Then ,use Hyperhenon map to generate a chaotic sequence,and by using properties of the chaotic sequence to scramble internal bit of each pixel and pixel diffusion so that plain image information can be well hidden.The simulation results show that the algorithm can better resist statistical characterization, differential attack, and can effectively resist chosen plaintext (ciphertext) attacks, and have big key space, good encryption effect.

Key words： chaotic systems；image encryption；bit;Kent map；Hyperhenon map

作者简介：

谢国波　男，(1977-)，博士，教授.研究方向为嵌入式系统.

E-mail:guoboxie@163.com

王　添　男，(1990-)，硕士研究生.研究方向为嵌入式系统、混沌保密通讯.