网络、通信与安全

基于混沌系统广义同步定理的信息隐藏方案

朱 玮[1]，闵乐泉[1]，尹 萍[2]，赵 耿[3]

1.北京科技大学 应用科学学院，北京 100083
2.北京科技大学 信息工程学院，北京 100083
3.北京电子科技学院 计算机系，北京 100070

摘要　　利用混沌系统广义同步定理，基于蔡电路系统构造了一个新的混沌系统，基于该系统设计了一个文本复合加密隐藏方案。该方案首先用复合系统产生的混沌码对明文加密，然后将密文隐藏到语音信号中。方案能够实现无失真解密。数值模拟显示新加密方案产生的混沌流具有良好的伪随机性。该方案对混沌系统的参数及初始条件极为敏感，表明该方案具有较高的安全性。数值模拟显示该方案能够有效地应用于网络通讯。

关键词　　广义同步定理　加密隐藏方案　混沌码伪随机性　网络通讯

分类号

Encryption scheme and hiding technology of voice based on generalized synchronization theorem for chaos system

ZHU Wei[1]，MIN Le-quan[1]，YIN Ping[2]，ZHAO Geng[3]

1.School of Applied Science，University of Science and Technology Beijing，Beijing 100083，China
2.School of Information Engineering，University of Science and Technology Beijing，Beijing 100083，China
3.Department of Computer Science and Technology，Beijing Electrical Science and Technology Institute，Beijing 100070，China

Abstract

　A new chaos system is established based on the theorem of generalized synchronization and Chua system.The chaos sequences generated via this system and Lorenz system has better pseudo-random properties.A message encryption and hiding scheme is also established on the system and Lorenz system.The scheme is successful to encrypt and decrypt message.Ciphertexts are sensitive to the parameters and initial conditions of the chaos system.It shows that this scheme has good security.Numerical simulations show that our scheme is effective to be used in network communication.

Key words　generalized synchronization theorem　encryption and hiding scheme　pseudo-random properties of chaos sequence　network secure communication

DOI:

通讯作者　朱 玮 E-mail：kitty5966@163.com

扩展功能

本文信息

▶ Supporting info
▶ PDF(1349KB)
▶ [HTML全文](0KB)
▶ 参考文献

服务与反馈

▶ 把本文推荐给朋友
▶ 加入我的书架
▶ 加入引用管理器
▶ 复制索引
▶ Email Alert
▶ 文章反馈
▶ 浏览反馈信息

相关信息

▶ 本刊中 包含"广义同步定理"的相关文章
▶本文作者相关文章

· 朱 玮
· 闵乐泉
· 尹 萍
· 赵 耿