

基于 Chaos-LSTM 与混沌序列增殖的 地理信息数据加密系统

段佳^{1,2}, 胡变运^{1,2}, 肖求美³, 刘美婷³, 于文新³

¹湖南省第三测绘院, 中国长沙市, 410000

²湖南省地理信息安全与应用工程研究中心, 中国长沙市, 410000

³湖南科技大学信息与电气工程学院, 中国湘潭市, 411201

摘要: 针对传统混沌加密算法中混沌系统状态与初始状态及参数关联性强, 可能导致混沌序列存在周期性的问题, 结合混沌系统和LSTM神经网络构建了Chaos-LSTM模型。针对计算机的有限计算精度效应会使长混沌序列出现周期性, 使其不适宜对数据量大的对象进行加密的问题, 构建了混沌序列增殖(CSP)算法。结合二者, 提出了基于Chaos-LSTM与混沌序列增殖的地理信息数据加密通信系统。首先, 通过Chaos-LSTM模型输出具有较高谱熵(SE)复杂度的混沌序列; 然后, 选取较短的混沌序列, 通过CSP算法增殖出匹配加密对象的混沌加密序列, 并对增殖序列进行随机性分析与测试; 最后, 以地理图片信息为加密对象, 将混沌增殖序列与扩散算法以及置乱算法结合构成加密算法, 并将加密系统在ZYNQ平台中实现。软件测试与硬件实验表明该系统具有良好的保密性能与可拓展性, 能用于多种加密对象的保密通信, 具备良好的应用价值。

关键词: 混沌; 长短期记忆神经网络 (LSTM); 混沌序列增殖 (CSP); ZYNQ平台; 图像加密

<https://doi.org/10.1631/FITEE.2300755>