基于混沌和 GPS的矢量数据加密方法的研究

吴学群[1],张 凌[2]
(1.昆明理工大学 国土资源工程学院,云南 昆明 650093;
2.云南邮电规划设计院有限公司,云南 昆明 650051)

摘要: 以 shapefile为例,分析了矢量数据的格式,介绍了混沌映射理论和 GPS技术,提出了一个基于混沌和 GPS的加密 解密模型,通过所设计的加密软件进行加密,结果证明了算法的有效性.

关键词: 矢量数据;混沌映射; GPS;数据加密
中图分类号: P208 **文献标识码**: A **文章编号**: 1007 - 855X(2008)04 - 0119 - 04

Research on Vector Data Encryption Method Based on Chaotic System and GPS

WU Xue-qun[1], ZHANG Ling[2]
(1. Faculty of Land Resource Engineering, Kunming University of Science and Technology, Kunming 650093, China;
2. Yunnan Planning and Designing Institute of Posts & Telecommunications Co. Ltd., Kunming 650051, China)

Abstract: Shapefile (. shp) is taken as an example in this paper to analyze vector data format. With the introduction of the chaos theory and GPS, a new encryption/decryption model is proposed. It is shown through an experiment that the method is feasible.

Key words: vector data; chaotic map; GPS; data encryption

0 引 言

随着 GIS技术的飞速发展,地理信息系统广泛应用于包括军事、灾害防护、公共安全等有关国家安全的敏感行业在内的各个领域,特别是近几年来发展比较快的电子政务和数字城市,这些资源可能关系到国家的经济命脉、政治形式或军事姿态,是重要的战略资源.另外,空间信息覆盖面广,由不同部门分别采集、加工和提供,由于权限和付费情况不同,这些部门对空间信息拥有不同的使用权,空间信息的分布有较为分散.所以对空间信息的安全管理就显得尤其重要.

1空间数据

1.1 GIS空间数据结构

在 GIS系统中, GIS空间数据常见的内部数据结构有栅格结构和矢量结构.其中,栅格结构是最简单最直接的空间数据结构,是指将地球表面划分为大小均匀紧密相邻的网格阵列,每个网格作为一个像元或像素由行、列定义,并包含一个代码表示该像素的属性类型或量值,或仅仅包括指向其属性记录的指针.因此,栅格结构是以规则的阵列来表示空间地物或现象分布的数据组织,组织中的每个数据表示地物或现象的非几何属性特征.根据扩展名分类,常见的栅格数据格式有 BMP、GIF、JPG、TIF等.

在矢量结构中,现实世界的要素位置和范围可以采用点、线或面表达,与它们在地图上表示相似,每一个实体的位置是用它们在坐标参考系统中的空间位置 (坐标)定义.地图空间中的每一位置都有唯一的坐

收稿日期: 2008 - 03 - 12 **基金项目**:校青年基金项目资助 (项目编号: 2007 - 058).
第一作者简介:吴学群 (1975 -),男,硕士,讲师.主要研究方向:地理信息系统的开发、GPS理论研究与应用.
E - mail: wuxuequn520@163.com

标值.在一般情况下,比栅格结构精度高得多.

1.2 矢量数据

由于数据加工的格式不同,常见的矢量数据格式有 Shp(shapefile)、E00、Mif、Tab、Dxf等,为了说明矢量数据的加密,本文以 shapefile数据格式为例.

Shapefile文件是美国环境系统研究所(ESRI)研制的 GIS文件系统格式文件,是工业标准的矢量数据格式. Shapefile将空间特征表中的几何对象和属性信息存储在数据集中,特征表中的几何对象存储为以坐标点集表示的图形文件——SHP文件,它不含拓扑数据结构.一个 Shapefiles由一组文件组成,其中必要的基本文件包括坐标文件(.shp)、索引文件(.shx)和属性文件(.dbf)三个文件.坐标文件(.shp)用于记录空间坐标信息.在索引文件中,每条记录包含对应主文件记录距离主文件头开始的偏移量,dBASE表包含 SHP文件中每一个 Feature的特征属性,表中几何记录和属性数据之间的一一对应关系是基于记录数目的 ID.在 dBASE文件中的属性记录必须和主文件中的记录顺序是相同的.图形数据和属性数据通过索引号建立一一对应的关系.

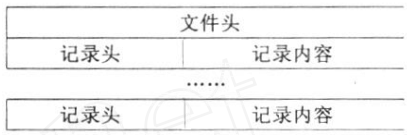

图1 坐标文件的结构

Fig.1 Structure of the coordinate file

坐标文件(.shp)由头文件和实体信息两部分构成.

坐标文件的文件头是一个长度固定(100 bytes)的记录段,一共有9个 int型和 7个 double型数据,主要记录内容见表 1.

表 1 Shapefiles头文件表

Tab.1 Table of the head file

起始位置	名称	数值	类型
0…28	…	…	…
32	几何类型	表示这个 Shapefile文件所记录的空间数据的几何类型	Integer
36…44	*X*min、*Y*min	空间数据所占空间范围的 *X*、*Y*方向最小值	Double
52…60	*X*max、*Y*max	空间数据所占空间范围的 *X*、*Y*方向最大值	Double
68*,76*	Zmin、Zmax	空间数据所占空间范围的 *Z*方向最小、最大值	Double
84*,92*	*M*min、*M*max	最小 Measure值、最大 Measure值	Double

实体信息负责记录坐标信息,它以记录段为基本单位,每一个记录段记录一个地理实体目标的坐标信息,每个记录段分为记录头和记录内容两部分.

记录头的内容包括记录号和坐标记录长度两个记录项.

记录内容包括目标的几何类型(ShapeType)和具体的坐标记录(*X*、*Y*),记录内容因要素几何类型(点状目标、线状、面状目标)的不同其具体的内容及格式都有所不同.

shapefile中的点状目标由一对 *X*、*Y*坐标构成,坐标值为双精度型(double).点状目标的记录内容如表 2.

表 2 点状目标的记录内容

Tab.2 Record content of the point object

记录项	数值	数据类型	长度	个数
几何类型	1(表示点状目标)	int	4	1
*X*方向坐标	*X*方向坐标值	double	8	1
*Y*方向坐标	*Y*方向坐标值	double	8	1

目前,对栅格数据的加密技术的研究较多,如:图像像素置乱的图像加密、基于秘密分割和秘密共享的图像加密、基于现代密码学体制的图像加密,以及基于混沌动力学体制的图像加密等.但由于行业应用的限制,矢量结构的图形数据的加密技术的研究较少.

2 混沌的定义及 Logistic映射

混沌加密是近年来兴起的一个研究课题,混沌映射具有很好的性质,即非常相近的初始条件在进行了一定次数的迭代以后会生成两个截然不同的序列;不可由序列的本身预测将产生的下一个数值;而且生成的序列具有白噪声性,即等概率地分布在值域上[1].由于这些良好的性质,它非常适合于对矢量数据的坐

标进行加密.

最基本的混沌模型是 Logistic映射[2]:

$$x_{n+1} = \mu x_n (1 - x_n) \tag{1}$$

其中 x_n为映射变量,μ为系统参数,它们的取值范围分别为:$0 \leq x_n \leq 1$, $0 < \mu \leq 4$(然而只有当 3.5699456… $\leq \mu \leq 4$时,才产生实数混沌序列). Logistic映射是一个非常简单,却又具有重要意义的非线性迭代方程,它具有确定的形式,并且系统不包含任何随机因素,但系统却能产生看似完全随机的、对参量 μ的动态变化和初值极为敏感的现象. 选定 μ=3.9有:

$$x_{n+1} = 3.9 x_n (1 - x_n),\ x_n \in (0, 1) \tag{2}$$

表 1证明了 Logistic映射对初始值的敏感性.

表 3　随机序列

Tab. 3　Random list

迭代次数	初　值	
	0.3256	0.3257
1	0.13717	0.61162
25	0.97339	0.97437
50	0.35401	0.45275
75	0.75139	0.24439
100	0.92196	0.70207

由于混沌序列随机的确定性, SchusterH. G证明混沌序列 (1)的概率分布密度函数[3]为:

$$\rho(x) = \begin{cases} \dfrac{1}{\pi \sqrt{x(1-x)}} & (0 < x < 1) \\ 0 \end{cases} \tag{3}$$

可见,$\rho(x)$不依赖初始值,它的遍历性等同于零均值白噪声,同时它还具有 δ- like型自相关函数和零的互相关函数. 作为一种非线性序列,该序列结构复杂难以分析和预测,因此可以用混沌系统迭代产生的混沌序列对矢量数据中的坐标进行加密.

3 GPS(全球定位系统)

GPS(Global positioning system)全球定位系统是美国第二代军用卫星导航系统,也是目前世界上最先进的卫星导航系统. 该系统是一种以空间卫星为基础的无线电导航和定位系统,能在全球范围内向任意多的用户全天候、实时、连续提供高精度的三维坐标、三维速度和时间基准.

4 加密算法设计

矢量数据中重要的信息是点的 XY坐标以及地理实体之间的相对位置关系. 通过对 Shapefile数据格式的分析,需要隐藏或保密的信息主要是坐标文件(. shp)里的数据内容,它包括:头文件部分的"空间数据所占空间范围的 X、Y方向最小值"、"空间数据所占空间范围的 X、Y方向最大值",实体信息部分的"X方向坐标值"、"Y方向坐标值".如果只是用同一种密码参数对坐标信息进行加密,虽然隐藏了坐标数据,但是地理实体之间的相对位置关系却仍然存在. 混沌映射的特点既可以对坐标信息进行加密,同时根据记录号的不同进行迭代,计算出不同的密码序列,对坐标数据进行加密,由于密码序列的随机性,改变了地理实体之间的相对位置关系. 同时,由于 GPS接收器模块化、小型化的实现,可以将 GPS接收器做成加密系统的软件狗,利用 GPS定位信息,空间数据的管理者将知道的数据接收方或数据存储地的地理位置信息作为一个密码参数,对空间数据进行加密,接收方只有在指定的地理位置才能解

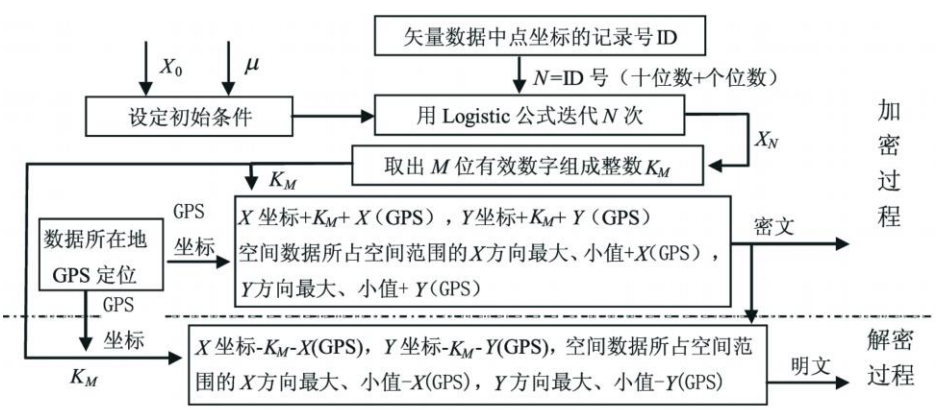

图2　加密/解密算法实现框图

Fig.2　Model of the encryption and the decryption

密信息.兼顾混沌映射、GPS定位和矢量数据的存储特点,本文设计了一个基于混沌映射和 GPS的矢量数据加密算法.

5结 语

本文利用 Delphi和 TatukGis组件开发了基于混沌和 GPS的加密实验软件,对 Shapefile坐标文件实验数据进行加密,效果如图 3.基于混沌和 GPS的加密方法隐藏了矢量数据的坐标系以及地理实体的相对位置关系,方法可行,效果良好.由于矢量数据都是海量数据,因此,混沌迭代的次数还需要考虑加载的效率,同时,混沌映射的算法目前研究较多,新的研究成果的应用有利于强化加密的效果.

图3 加密效果图

Fig.3 Result of the encryption and the decryption

参考文献:

[1] 黄润生.混沌及其应用 [M].武汉:武汉大学出版社,2000.

[2] 王丽娜.网络多媒体信息安全保密技术 [M].武汉:武汉大学出版社,2003.

[3] 王丽娜,郭迟,李鹏.信息隐藏技术试验教程 [M].武汉:武汉大学出版社,2004.

[4] 邬伦,刘瑜,张晶,等.地理信息系统 -原理、方法和应用 [M].北京:科学出版社,2004.

[5] 孙克辉,刘巍,张泰山.一种混沌加密算法的实现 [J].计算机应用,2003,23(1):15 - 17.

[6] 赵雪峰,殷国富.基于复合混沌系统的数字图像加密方法研究 [J].计算机应用,2006,26(4):827 - 829.

(上接第 100页)

3) 数据集成.物流公共信息平台的数据来源多样化,处理需求也是多样化,涉及到数据格式的统一、数据传输的实时性、数据传输的完整性和可靠性等问题.

4) 平台安全系统.根据整个平台系统安全需要,将不同业务系统划分在不同的网络安全域中,形成核心业务系统安全域、相关系统安全域、公众服务中心系统安全域和认证中心系统安全域等四个彼此隔离的网络安全域.在不同的网络安全域之间,系统的网络处于隔断状态,只有经过认可的业务数据信息才能在不同的安全域之间进行信息交换.

4结 语

基于信息交换技术的物流公共信息平台系统是一个支持多种终端接入,提供多种业务系统连接和统一管理的综合信息系统服务平台,可以较好地解决目前在物流信息化系统建设中遇到的问题,实现业务服务中点对点(用户和服务部门)、点对多点(用户和多个服务部门)的联合服务,使一站式电子物流在现代社会物流系统中的应用成为可能.

本文着重对平台的功能定位、体系结构和总架构进行研究,下一步的研究应该是更深入的需求分析、构建出相应的平台商务流程和商务模型,并对总架构的各技术层面和建设运营策略进行深入研究.

参考文献:

[1] 张锦,杨东援,关志超,等.城市现代物流公共信息平台的内涵和规划设计 [J].交通运输系统工程与信息,2005,5(4):57 - 64.

[2] 董千里,袁毅.区域综合物流信息平台的功能与构建研究 [J].交通运输系统工程与信息,2002,2(2):74 - 78.

[3] 袁毅.物流信息化发展战略研究 [D].西安:长安大学经济管理学院,2003.

[4] 何杰,李旭宏,毛海军.省级物流信息平台体系结构方案分析 [J].交通科技,2003,(6):72 - 74.

[5] 黄文成.城市物流信息公共平台的设计、实施及运营研究 [EB/OL].厦门:物流中国网,2004 - 10 - 20.

[6] 张江山,顾农,韩艺.基于 CORBA技术的 ITS综合信息平台软件设计 [J].ITS通讯,2003,(18):22 - 26.