



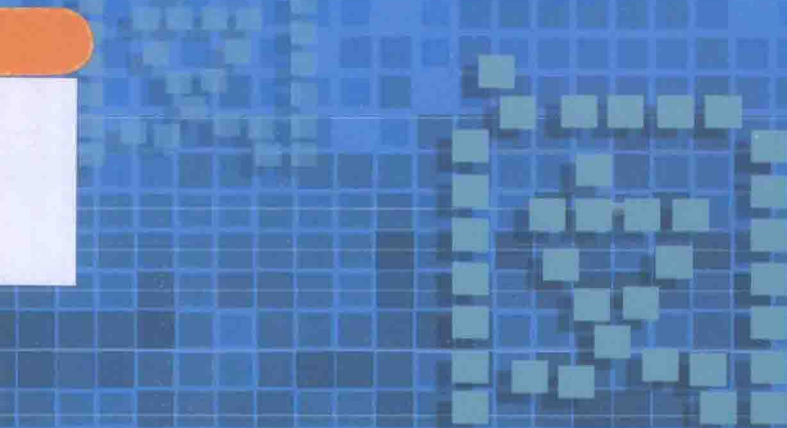
测绘地理信息科技出版资金资助
CEHUI DILI XINXI KEJI CHUBAN ZIJIN ZIZHU

高等学校统编教材

地理空间数据 隐藏与数字水印

Information Hiding and
Watermarking of Geospatial Data

闵连权 编著



测绘出版社

高等学校统编教材
测绘地理信息科技出版资金资助

地理空间数据 隐藏与数字水印

Information Hiding and Watermaking of Geospatial Data

闵连权 编著

测绘出版社

· 北京 ·

© 闵连权 2015

所有权利(含信息网络传播权)保留,未经许可,不得以任何方式使用。

内 容 简 介

地理空间数据隐藏与数字水印涉及测绘科学与技术、密码学、计算机应用技术、信号与信息处理等多学科领域。本书是在作者多年研究成果以及对国内外代表性研究成果进行系统分析的基础上撰写而成的。全书从地理空间数据的基本特征和应用实际出发,介绍了地理空间数据安全基础理论和地理空间数据加密技术,系统详细地阐述了地理空间数据隐写技术、栅格类地图数据数字水印技术、矢量地图数据空间域鲁棒数字水印技术、矢量地图数据变换域鲁棒数字水印技术、矢量地图数据脆弱数字水印技术、矢量地图数据无失真数字水印技术、矢量地图数据多重数字水印技术和矢量地图数据数字水印性能评价等内容。

本书着重理论、技术、实践相结合,重点突出,资料翔实,参考性和可操作性强,可作为高等院校测绘科学与技术、信息安全、计算机应用、信号与信息处理等相关专业的研究生或高年级本科生的教学用书,也可作为科研院所相关科研人员的参考用书。

图书在版编目(CIP)数据

地理空间数据隐藏与数字水印/闵连权编著. —北京:测绘出版社, 2015.1

ISBN 978-7-5030-3613-2

I. ①地… II. ①闵… III. ①地理信息系统—安全技术 IV. ①P208

中国版本图书馆 CIP 数据核字(2014)第 296500 号



责任编辑	贾晓林	装帧设计	李 伟	责任校对	曹 平	责任印制	喻 迅
出版发行	测绘出版社			电 话	010—83543956(发行部)		
地 址	北京市西城区三里河路 50 号				010—68531609(门市部)		
邮政编码	100045				010—68531363(编辑部)		
电子信箱	smp@sinomaps.com			网 址	www.chinasmp.com		
印 刷	三河市世纪兴源印刷有限公司			经 销	新华书店		
成品规格	184mm×260mm						
印 张	16.75			字 数	420 千字		
版 次	2015 年 1 月第 1 版			印 次	2015 年 1 月第 1 次印刷		
印 数	0001—1500			定 价	49.00 元		

书 号 ISBN 978-7-5030-3613-2/P·783

本书如有印装质量问题,请与我社联系调换。

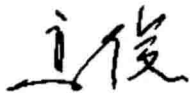
序 言

地理空间是人类生存的自然空间,也和人类的社会、经济、文化诸多环境有密切的关系。在我们接触的各种信息中,大约有 80% 是与地理环境或空间位置有关的,因此描述地理空间的地图、影像、资料与文献的数量十分巨大。当数字技术和网络技术出现之后,地理空间数据呈爆炸式增长,于是地理空间数据的安全就提到日程上了,成为大家特别关注的问题。其中,不仅有数据的拥有者、管理者,还包括更广大的数据用户。

地理空间数据是一种具有产权的资源。因为它是国家、企业或个人在资金投入、知识融合、技术研究、使用可控的条件下生产的成果,其产权受到国家法律的保护。在这个前提下,数据安全显得十分重要,涉及国家利益、知识产权、个人隐私、商业秘密等一系列法律与权益问题。在国际上,地理空间数据的占有和控制也是一场永无休止的资源争夺战,各方通过各种渠道设法获取全球或重点地区的数据,采用各种措施保护自己的数据资源不受损害。不论是在国防、经济、科技哪个范围内,也不管是在全球化、联合科学探索、经济一体化宣言哪个背景下,地理空间数据的利益本质都是一样的。

地理空间数据最早的载体是大地测量成果、航空影像、地图和地理调查资料,这些实物性信息的保管与安全措施相对简单,其使用范围与安全规定也便于落实。而当今数据来源的多样化、数据存储设备的小型化、数据传播的网络化彻底颠覆了原来的安全模式,变得十分复杂。于是出现了两个问题:一是哪些内容的数据需要列入保护的范畴,安全等级如何制定;二是采用何种技术和措施保护数据的安全。

第一个问题是专业部门的责任,是迫切要回答的一个问题。本书则是针对第二个问题,在“怎样保护”的问题上探索了一些新的技术。闵连权教授多年来从事地理空间数据安全问题的教学与科研工作,见解独到,成果颇丰。这本书可以为学生、研究者和管理人员提供有益的帮助。



2014 年 5 月

前言

地理空间数据安全是在国家信息化建设过程中,在数字技术深入各领域条件下的一个新课题,它涉及国家安全、科技协作交流和知识产权保护等各个方面,是制约我国经济、科学与技术可持续发展的重要因素之一,已经引起学术界、政府和企业的广泛关注。

地理空间数据是国家空间信息资源的核心部分,是国家信息化建设的基础,它是一切地球科学研究成果的地理定位框架,也是实施电子政务、电子商务和国防信息化建设的基础。

地理空间数据在人类的社会、经济活动中发挥着不可替代的作用,已广泛应用于社会各行业、各部门,如航空航天、环境保护、资源勘探、土地管理、城市规划、交通规划、汽车导航、工程设计、抢险救灾及观光旅游等都离不开地理空间数据的支持。随着科学和社会的发展,人们已经越来越多地认识到地理空间数据对于社会经济发展、人们生活水平提高的重要性,这也加快了人们获取和应用地理空间数据的步伐。

目前,测绘学科从理论到技术手段都发生了根本性的变化,并正在步入信息采集、数据处理和成果应用的自动化、智能化、网络化、实时化和可视化的新阶段。数字化的产品形式、网络化的保障方式已成为地理空间数据服务的主要方式。这种服务方式极大地方便了地理空间数据的交流、共享,有利于各行各业方便地使用地理空间数据,促进了各行各业的发展。但是由于数字产品复制的便捷性、复制成本的低廉性和复制品的高保真性,数据易被非法窃取、浏览、复制、篡改,数据越来越难以控制。人们在享受现代信息技术和网络技术所提供的便利的同时,安全问题也日益突出,成为信息交流的重要障碍。

当前地理空间数据共享的呼声很高,需求也很大,许多人员都在从事地理空间数据共享技术的研究,然而,与之形成巨大反差的是地理空间数据安全技术与管理还停留在传统的针对模拟产品的水平上,通过双方签订合同、保证书的形式来保障地理空间数据的安全,这种方式显然已不适应数字化的地理空间数据的安全需求。共享是以安全为前提的,没有安全保障,就不可能实现真正的共享。地理空间数据安全保密技术缺乏,严重制约了地理空间数据服务的能力和水平。可喜的是国内外已有相当多的科研人员开始从事这一领域的研究,地理空间数据隐藏与数字水印是最热门的研究方向之一,在地理空间数据的版权保护、交易跟踪、篡改提示、信息认证和安全传输等方面发挥着重要作用。为了使初学者尽快入门、少走弯路,同时也对国内外这一领域的研究成果进行系统总结,更好地梳理将来的研究思路 and 方向,给广大科技工作者以帮助,我们认为编写一本这样的书是很有必要的。

全书共分 11 章。第 1 章绪论,主要论述了地理空间数据的重要性、存在的安全问题、地理空间数据安全概念及属性、研究意义,以及国内外的研究现状;第 2 章基础理论,对地理空间数据、密码学、混沌系统、数字图像和人类视觉系统进行了介绍;第 3 章到第 10 章是本书的主体部分,着重对地理空间数据安全技术进行研究,包括地理空间数据加密技术、地理空间数据隐写技术、栅格类地图数据数字水印技术、矢量地图数据空间域鲁棒数字水印技术、矢量地图数据变换域鲁棒数字水印技术、矢量地图数据脆弱数字水印技术、矢量地图数据无失真数字水印技术和矢量地图数据多重数字水印技术;第 11 章矢量地图数据数字水印性能评价,根据矢量

地图数据的特点和实际应用,构建矢量地图数据数字水印性能评价指标体系和评价模型,为衡量不同水印算法的性能提供依据。

在书稿付梓之际,作者心中满是感激之情。感谢我国著名的地图学与地理信息工程专家、中国科学院院士高俊教授。本书的选题和写作,高院士都提出了许多前瞻性的意见,书稿完成时又得到高院士的审阅,并为本书作序,甚是感激!感谢中国工程院院士王家耀教授、南京师范大学朱长青教授、海军大连舰艇学院田震教授,与他们的交流、研讨都使我的研究工作少走了许多弯路!

本书的研究得到国家自然科学基金(41471337)资助,本书出版得到了信息工程大学地理空间信息学院教材出版专项经费资助,特致谢!

在本书的编写过程中,作者查阅了大量资料,并参考和引用了许多国内外相关书刊和文献,在此衷心感谢所有参考文献的作者。

由于作者水平所限,加上时间仓促,书中难免会出现疏漏和不足之处,敬请读者批评指正,不胜感激。

作 者

2014 年 4 月

目 录

第 1 章 绪 论	1
1.1 地理空间数据的重要性	1
1.2 地理空间数据存在的安全问题	2
1.3 地理空间数据安全	4
1.4 地理空间数据隐写与数字水印	9
第 2 章 基础理论	11
2.1 地理空间数据基础知识	11
2.2 密码学基础知识	15
2.3 混沌系统基础知识	20
2.4 数字图像基础知识	26
2.5 人类视觉系统特性	50
第 3 章 地理空间数据加密技术	53
3.1 矢量地图数据加密	53
3.2 影像地图数据加密	59
第 4 章 地理空间数据隐写技术	78
4.1 信息隐藏基础理论	78
4.2 信息隐写技术	84
4.3 LSB 替换信息隐写及其改进	88
4.4 基于遥感影像的信息隐写	96
4.5 DEM 信息隐写	101
第 5 章 栅格类地图数据数字水印技术	104
5.1 数字水印基础理论	104
5.2 基于方向性信息测度的图像水印	110
5.3 影像地图数据数字水印	120
5.4 栅格地图数据数字水印	124
5.5 DEM 数据数字水印	131
第 6 章 矢量地图数据空间域鲁棒数字水印技术	136
6.1 矢量地图数据数字水印分析	136
6.2 基于插入冗余点及定位点坐标最低有效位的数字水印	141

6.3 基于定位点坐标统计特性的数字水印	144
6.4 基于地图形态特征的数字水印	157
6.5 基于空间关系的数字水印	162
6.6 基于地理实体的数字水印	168
第7章 矢量地图数据变换域鲁棒数字水印技术	172
7.1 基于DFT的矢量地图数据数字水印	172
7.2 基于DCT的矢量地图数据数字水印	177
7.3 基于DWT的矢量地图数据数字水印	180
7.4 其他变换域矢量地图数据数字水印	186
7.5 空间域和变换域水印算法性能分析	199
第8章 矢量地图数据脆弱数字水印技术	202
8.1 脆弱数字水印	202
8.2 矢量地图数据脆弱水印	204
第9章 矢量地图数据无失真数字水印技术	209
9.1 矢量地图数据可逆数字水印	209
9.2 矢量地图数据零水印	223
第10章 矢量地图数据多重数字水印技术	229
10.1 多重数字水印概述	229
10.2 矢量地图数据互补型多重数字水印	231
10.3 矢量地图数据分级型多重数字水印	241
第11章 矢量地图数据数字水印性能评价	245
11.1 矢量地图数据数字水印性能评价指标体系	245
11.2 矢量地图数据数字水印性能评价模型	249
参考文献	251

第1章 绪论

21 世纪是一个以网络为核心的信息时代。信息技术的应用,不仅使信息的生产方式、发布渠道、传播范围、传递速度、存储介质等发生了革命性的变化,而且引起了人们的生产方式、生活方式、思想观念和行为方式的巨大变化,信息已成为人类社会必需的重要资源,信息安全已成为世界性的现实问题。在我们接触的信息中,大约有 80% 是与地理环境或空间位置有关的,地理空间数据的安全问题也越来越重要。

1.1 地理空间数据的重要性

地理空间数据是指具有空间位置属性的基础数据和专题数据,是描述关于人类赖以生存的地球的重要信息,是用来表示空间实体的位置、形状、大小及其分布特征诸多方面信息的数据,它用点、线、面及实体等基本空间数据结构来表示人们赖以生存的自然世界(闵连权,2005)。

地理空间数据在人类的社会、经济活动中发挥着不可替代的作用,已广泛应用于社会各行业、各部门,如航空航天、环境保护、资源勘探、土地管理、城市规划、交通规划、汽车导航、工程设计、抢险救灾及观光旅游等都离不开地理空间数据的支持。随着科学和社会的发展,人们已经越来越多地认识到地理空间数据对于社会经济发展、人们生活水平提高的重要性,这也加快了人们获取和应用地理空间数据的步伐。

地理空间数据是国家基础设施建设和地球科学研究的支撑性成果,是国家经济、国防建设中不可缺少的资源,对社会持续发展起着重要作用。现代社会生产力的迅速发展及社会活动的增强,使人类对环境作用的强度比以往任何时候都突出,社会和经济等重点问题的决策无不与地理空间数据相关。

地理空间数据是国家空间信息资源的核心部分,是国家信息化建设的基础,它是一切地球科学研究成果的地理定位框架,也是实施电子政务、电子商务和国防信息化建设的基础。地理空间数据是数字地球的基础信息,数字地球的绝大部分功能将以地理空间数据为基础。

地理空间数据是国家重要的资源、商品,是国家基础性、公益性设施,关系到国家在信息社会中最基本、最重要的经济命脉,是一种重要的战略资源。

地理空间数据作为一种资源应受到与物资财富、能源资源同等重要的保护,根据地理空间数据的精度、范围、用途等条件对地理空间数据的使用实行公开使用、有偿使用及限制使用等等级别(何建邦等,2000)。如有些主要用于基础性、公益性的地理空间数据可以公开使用,而有些数据则应按照商品经济的规律实行有偿使用,但地理空间数据又有自己独特的特性,有些地理空间数据关系到国家利益和社会安全,必须依法限制其公开,即地理空间数据的安全保密性,实行保密控制。对地理空间数据的某些内容实行保密也是国内外共同的政策,就连美国也不例外,如 1994 年美国签署的“国家数据基础设施”的 12906 号总统令中也明确宣布有关国家安全、国防工作等方面的地理数据不在总统令的范围。此外,属于商业秘密及个人隐私方面的地理数据也在限制公开之列。

1.2 地理空间数据存在的安全问题

传统纸质地图的信息共享是通过实物地图的复制来实现的,安全性和保密性通过严格的管理制度来保证,通过严格的申请、审批和领取制度,以及在地图的背面加盖使用单位的印记以确保责任到单位(人员)。与模拟地图相比,地理空间数据易于共享,在方便使用的同时也给数据的安全和保密带来很大隐患,数据的盗用、复制、截获方法很多,防不胜防。当前我国地理空间数据的安全形势不容乐观,十分严峻,存在着许多安全隐患,既有观念、意识上的问题,也有管理、技术上的原因。概括起来主要有以下几个方面。

1. 境外势力对我国地理空间数据的觊觎

地理空间数据是一个国家的战略资源,事关国家和军队的安全、社会的稳定和经济的发展,各个国家都力图控制本国的地理空间数据,防止被其他国家窃取,而又尽力获取其他国家的地理空间数据,从而取得信息优势,确保国家安全。中国领土内的空间基础数据的信息量(价值)是巨大的,因此,一些西方国家千方百计地获取我国的地理空间数据,甚至不惜以第三国的地理空间数据与我国交换。从这些情况可以看出,我国的地理空间数据尤其重要,必须加强安全保密意识。

2. 观念、意识上的麻痹

观念、意识上的麻痹主要表现在以下三个方面:

一是对全球化的误解。随着世界经济和技术全球化的进程,尤其是我国加入世界贸易组织(World Trade Organization, WTO)之后,经济已逐步纳入全球化体系,我国的政府工作人员、企业家、工程技术人员已涉足全球范围的活动,我国科学家已大量参与了国际性的研究与合作开发项目,因此在部分科技人员和管理人员意识中往往产生全球化的倾向,认为在和平与发展是当今时代的主题下过分强调安全保密不合时宜,认为科学、技术、基础设施等的全球化是势在必行。其实不然,科学、技术、经济都可以全球化,但是应该清醒地认识到在政治和文化多元化、世界多极化的大前提下,有关国家的基础设施等很多问题都不可能实行全球化。地理空间数据作为国家的基础设施,也绝不能实行全球化,它仍具有私有性、保密性,地理空间数据的安全关系到国家的安全和社会的稳定,这也正是为什么提倡信息共享最强烈的美国在想方设法获取别国地理空间数据的同时,却严格控制本国的地理空间数据的重要原因。

二是对获取地理空间数据的技术能力的盲信。在科学技术高度发达的今天,实时获取大范围、高精度地理空间数据的能力相当高,卫星图像可分辨出地面报纸上的大标题,全球卫星定位系统定位精度可达米级、厘米级。那么国家基础地理信息,大比例尺地形图还有什么密可保,还有没有必要采取限制性使用政策?在这方面,可能存在着技术上的误解。应当承认,现代图像技术、定位技术确实达到了极高的水平,在军事上、经济上有重大意义。但是高科技的发展,只能在条件允许的情况下,才能够更精确、更快捷地生产精密的地理信息和地形图产品,它们仅仅是获取信息的技术手段,并不代表信息产品的实体本身。首先,地形图载负的大量属性信息、地名信息,是任何卫星图像上都无法得到的。同时,卫星图像只是局部相对位置的表象,要将图像全部识别,应该有实地要素相对照。卫星图像的相对位置,要将它们变成全球统一的绝对坐标系中的地图,必须要有一定密度的精密控制点控制,这些控制点要达到地面位置、卫星图像上的位置、精确的地理坐标值的匹配一致,才能真正起到控制作图的作用。在确

定绝对地理位置方面,卫星定位系统虽能起到作用,但定位设备一定要到实地,并通过一定的操作,才能获取定位信息。所以,尽管有了高科技手段,要真正生产出他国的高精度地形图,仍然是不可能的。

保护本国的地形图,最重要的是保护了战争中可能成为对方打击目标的绝对位置。尽管在和平时期,有大量的目标已被对方锁定,但一旦进入战时,被锁定的目标可能要变迁,必然有更多的新目标产生,尽管有实时卫星图像,但如果没有绝对地理坐标的指引,也很难锁定目标。这种指引一种是靠派专门人员到实地指引;一种是靠精密的地形图,与最新的卫星图像匹配、参照,来锁定目标。

GPS(Global Positioning System,全球定位系统)接收设备,也不是万能的。不是只要有GPS,就能解决行军打仗的问题,就能长驱直入。只有GPS,仍然可能是“瞎子”,要解决行军打仗的问题,还必须要有当地的统一的大地坐标系的地图相匹配,才能解决自己在哪里,自己要到哪里,如何才能到那里的问题。这就是为什么海湾战争中,美国许多士兵都配备了GPS接收设备,但仍然无法前进。美国国防制图局不得不日夜加班,赶制作战地区的地形图,将成吨的地图运往战场,解部队机动的燃眉之急。

所以,卫星图像技术、GPS定位技术的巨大成就,并没有使地形图信息的保护失去意义。对于受侵略或受到入侵的弱者,保护精密的大比例尺地形图的内容,也是在保护自身的安全,这符合国家利益。

三是对秘密资料标准的模糊认识问题。有人认为地理空间数据的需求量大,密级定得太高使用不方便,不利于数据的共享和流通。事实上需求量的大小不是判定密级的依据,确定资料密级的唯一标准是:该资料一旦失密对国家安全造成的危害程度。数据共享与数据安全应辩证地统一起来,不能片面地强调数据共享问题而忽视数据的安全问题,数据共享必须以数据安全为前提,为了使用方便而解除保密约束,就会给国家带来危害。

3. 学术交流、科研合作等国际活动带来地理空间数据安全的隐患

在改革开放的大环境下,尤其是我国加入WTO后,在学术交流、科研(项目)合作、委托开发、技术引进与输出的力度相比以前有很大的发展,从而也带来一系列的安全问题。如有些单位在项目合作、委托开发时,将未经保密处理的大比例尺地形图和机密级重力资料擅自向外提供;有些单位在与外商项目合作中,迫于外商的压力提供精确的地理空间数据,甚至允许外商人员自己测绘获取我国的地理空间数据等。

4. 法规、管理制度的漏洞

目前,我国地理空间数据的安全管理主要依靠传统的管理方式与技术手段,基本上处于一种静态的、局部的、少数人负责的、突击式的、事后纠正式的管理方式,不是建立在安全风险评估基础上的、动态的、持续改进管理方法。保障地理空间数据的安全,技术很重要,但管理更重要,“三分技术,七分管理”,而做到有效管理的前提条件是必须有健全的法律、法规做依据,健全的地理空间数据安全的法律、法规体系是确保国家地理空间数据安全的基础,是地理空间数据安全的第一道防线。而目前我国还没有有关地理空间数据安全的专门法律、法规,主要是通过一些其他的法律、法规以及部门规章进行约束管理,如《中华人民共和国国家安全法》《中华人民共和国保守国家秘密法》《中华人民共和国计算机信息系统安全保护条例》《计算机信息系统保密管理暂行规定》《关于对外提供我国测绘资料的若干规定》《测绘管理工作国家秘密范围的规定》《重要地理信息数据审核公布管理规定》等,这与地理空间数据的安全需求不相适应。

因此,为了更好地保护地理空间数据的安全应建立专门的法规,做到有法可依。

在法律、法规和部门规章的前提下,必须加强管理,做到依法管理,违法必究,执法必严。严密的制度,严格的管理,是确保地理空间数据安全的基本保障。加强管理,首先是对涉及地理空间数据的人员的管理,加强安全教育,培养人员的安全意识,做到不泄密。其次是确保数据的存储、分发、传输和应用的安全,如存储设施的物理安全、逻辑安全,传输、分发和应用时对数据采取加密、隐藏处理等措施,防止数据被非法盗取。地理空间数据的网上泄密事件不容忽视,如有些单位是不设防的网络,有的用户在没有采取安全防范措施的情况下将涉密数据在互联网上存储、传播,有的机构对秘密信息缺乏必要的保护意识和措施。

5. 信息基础设施的安全隐患

当前,我国信息基础设施最突出的问题就是缺乏自主科技,系统安全状态脆弱,核心技术完全依赖外国(张新华,2003)。使用的 CPU 芯片、使用的操作系统和数据库、使用的网络管理软件,是制约中国计算机网络安全三个最大隐患,人们称之为“三大黑洞”。然而,这三个决定计算机安全的产品,中国厂商自己不能生产,没有自主知识产权,自然就要受制于人。目前,构成中国信息基础设施的网络、硬件、软件等产品几乎完全是建立在外国的核心技术之上的。其中,美国在网络上的垄断是全面的,它拥有世界上最大的软件公司(微软),最大的接入系统(思科),最大的互联网服务提供商(美国在线),而且全球主要的网络安全公司也在美国。我国的信息化建设尚未脱离大量依赖非专利技术的状态,整个网络系统缺乏自主技术支持,从而出现了“网域不设防”的严重局面。我国计算机网络所使用的网管设备和软件基本上是美国公司的产品,绝大部分 TCP/IP 协议、计算机芯片都是英特尔系列,软件基本上是 Windows。这些因素将使我国的计算机网络安全性能大大降低,被认为是易窃视和易打击的“玻璃网”。从根本上说,只要芯片和操作系统都是别人的,那就相当于在沙滩上建高楼,毫无安全可言。

6. 移动存储、计算设施的普及化带来空间数据的安全风险

信息技术的提高使得移动存储设备的体积越来越小,而存储量却越来越大,具有高度兼容性的移动存储设备给用户带来方便的同时也给窃贼提供了方便,不法人员利用移动存储设备可以轻易获取成百上千份涉密文件。黑客还可通过移动存储设备将病毒带到网络之中,进行破坏性攻击。

笔记本、掌上机等移动计算设施面临失窃等许多额外风险,这种由于计算设施的丢失而引起的地理空间数据的安全问题不容忽视。使用移动设施时要采取实物保护、访问控制、密码技术、备份、病毒防护及自毁等措施。

1.3 地理空间数据安全

1.3.1 信息安全概念

信息安全涉及的领域相当广泛,广义上讲,凡是涉及信息的保密性、完整性、可用性、真实性和可控性的相关理论和技术都是信息安全所要研究的领域。狭义的信息安全是指信息内容的安全性,侧重于保护信息的保密性、真实性和完整性,避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗、盗用等有损合法用户利益的行为,保护合法用户的利益和隐私(沈昌祥,2003;张世永,2003;冯登国,2003;阙喜戎等,2003)。

信息安全至少应包括以下几个方面:

(1)信息的保密性。指信息不泄露给非授权的个人和实体,或供其使用的特性,即对抗被动攻击,保证信息不被未授权者获取,这是信息安全最主要的问题。

(2)信息的完整性。指信息在存储或传输的过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性,即对抗主动攻击,保证真实的信息从真实的信源到达真实的信宿。破坏信息的完整性是对信息安全发动攻击的最终目的。

(3)信息的可用性。指信息可被合法的用户访问并能按要求顺序使用的特性,即在需要时就可以取用所需的信息,授权者可以随时使用信息和信息系统的服务。对可用性的攻击就是阻断信息的合理使用,例如破坏系统的正常运行就属于这种类型的攻击。

(4)信息的可控性。指授权机构可以随时控制信息的机密性,即信息系统的管理者可以控制管理系统和信息,能够对信息实施安全监控。

(5)信息系统的不可否认性。也称为不可抵赖性,即每个通信者具有法律生效的证据证明其是否实施过信息交换和获取的行为,所有参与者都不可能否认或抵赖曾经完成的操作和承诺,发送方不能否认已发送的信息,接收方也不能否认已接收到的信息。

1.3.2 地理空间数据安全概念及其属性

地理空间数据安全是指综合运用法律法规、管理措施和技术手段,使地理空间数据在获取、处理、存储及应用过程中免遭窃取、泄露、篡改和毁坏,确保地理空间数据的保密性、完整性、可用性、可认证性、不可抵赖性和可控性。

与一般的信息安全相比,地理空间数据具有特有的安全属性,主要表现为以下四个方面:

(1)使用者的广泛性。地理空间数据的国内用户从部门到个人,从各级各类政府机关、教学科研单位到民营公司,从政府工作人员到社会大众,人们不同程度地应用地理空间数据,并且应用环境从室内扩展到野外。随着国民素质的提高,越来越多的人应用地图等地理空间数据,并且渴望获得内容精确详细、现势性强的地理空间数据。

地理空间数据的国外用户从联合国、“全球测图”等对地图的需求和相关国际制图项目到各类公司,均不同程度地需要我国的地理空间数据。在一些大型工程项目(如石油勘探)和一些对外招标工程中也都需要高精度的大比例尺地图等地理空间数据。

(2)保密时间的长期性。地理空间数据能客观地反映地球表面显性和隐性的特征,较多的内容是地表长期存在的。因此,对大多数保密的地理空间数据而言,保密时效多为长期的。随着高新技术的发展,新的保密地理空间数据不断快速产出,保密事项不断积累,带来了较大的保密成本。长期保密特性给制定地理空间数据的保密措施和研究地理空间数据保密方法带来了难度。

(3)空间位置和内容的保密性。一般而言,地理空间数据的保密特性主要体现在两个方面:一是空间位置的保密特性,二是要素(地图)内容的保密特性。

测绘业务的主要成果是基础地理信息和地形图,利用涉及国家秘密的测绘成果开发生产的产品,其秘密等级不得低于所用测绘成果的秘密等级。

高精度的地理空间数据及大比例尺地形图既有空间位置保密特性,又有要素内容保密特性,其要素内容的保密不仅包括军事设施,也包括关乎国家命脉的民用设施(中国地理信息产业政策研究组,2007)。

(4) 数据密级与使用者身份的非正相关性。一般情况下,数据的使用者和数据的密级成正相关,如级别高的指挥员掌握着作战行动的核心机密,级别低的指挥员只掌握与本级作战有关的部分信息,一线战斗员掌握的信息更少,信息的秘密等级也最低。而对地理空间数据而言,往往使用者的身份越高,使用的地理空间数据越概略,重要程度越低,甚至是可以公开的小比例尺的地理空间数据,而师团级的战术指挥员在研究战场环境、制订作战方案,以及组织作战指挥等行动时,需要 1:5 万甚至更大尺度的地理空间数据,数据的秘密等级也较高。

从信息安全的角度来说,信息的保密与保密范围、知悉范围、保密期限三个因素有关,即保密范围越小、知悉的范围越小、保密的期限越短,信息越容易保密,否则,信息保密就很难,而地理空间数据具有保密事项多、保密范围大、使用者广、需要保密的期限长等属性,因此,地理空间数据安全保密的难度更大,更应该引起重视。

1.3.3 研究地理空间数据安全的意义

长期以来,测绘一直被各国政府视为“国之神器,不可予人”。掌握了一个国家各大关键设施的地理空间数据,对该国的国防与经济将构成重大的安全威胁。从大的方面说,关系到国家的主权和领土完整,以及国民经济政策、国防政策、外交政策的制定;从小的方面说,关系到广大人民群众的日常生活动。

地理空间数据安全是在国家信息化建设过程中,在数字技术深入各领域条件下的一个新课题,它涉及国家安全、科技协作交流和知识产权保护等各个方面,是制约我国经济、科学与技术可持续发展的重要因素之一。

随着空间技术、计算机技术、信息技术及通信技术的发展,测绘学科从理论到手段发生了根本性的变化,并正步入信息采集、数据处理和成果应用的自动化、智能化、网络化、实时化和可视化的新阶段。数字化的产品形式、网络化的保障方式已成为地理空间数据服务的主要方式。这种服务方式极大地方便了地理空间数据的交流、共享,有利于各行各业方便地使用地理空间数据,促进了各行各业的发展。但是由于数字产品复制的便捷性、复制成本的低廉性和复制品的高保真性,数据易被非法窃取、浏览、复制、篡改,数据越来越难以控制。人们在享受现代信息技术和网络技术所提供的便利的同时,安全问题也日益突出,成为信息交流的重要障碍。网络与安全是一对矛盾,共享与安全也是一对矛盾,共享是以牺牲安全为代价的,在实现地理空间数据的共享过程中,只有在可靠的安全性的前提下实现共享才有现实意义,失去安全性的共享就是失控、泄密。

以往的地理空间数据大多以地图和专题地图为载体,便于保管和有序使用,管理制度也较完善,不存在安全失控的问题。另一部分以数据记载的形式按需求提供使用,例如大地坐标成果和各学科的调查、分析数据,在安全上也有相关规定。在新的技术条件下,原有的安全标准和管理规定已不适应新形势下国家安全的需求。例如,纳入国家安全控制范围的标准是什么,传统的保密规定在很多方面已制约了科技的进步,出现了很多新的、传统方法无法控制的、涉及国家安全的、需要给予关注的的数据与信息,数据共享与数据安全的关系是什么,知识产权保护技术层面的问题等都急需从理论与方法上进行探索。

当前我国地理空间数据安全技术与管理还停留在传统的大地坐标数据、航片和地图资料保密管理的水平上,通过双方签订合同、保证书的形式来保障地理空间数据的安全,这种方式在以纸张为载体的数据存储形式下还是有一定效果的。但是,这种措施无法保障数字化的地

理空间数据的安全,相应的安全标准、手段已不适应数字化的地理空间数据的安全需求。

当前,地理空间数据安全方面存在以下问题亟待解决:

一是国家安全与社会需求的矛盾。地理空间数据是一种特殊的资源,一方面地理空间数据事关国家安全、国防安全和利益,必须根据需要设定密级,并限制其使用范围等;另一方面地理空间数据又是国家经济建设不可缺少的基础性技术资料和数据,国民经济建设和人们的日常生活越来越离不开地理空间数据的支持,国家安全与经济建设的强烈需求在这一点上构成了矛盾,不加限制的公开使用地理空间数据必然危害国家安全利益,相反对地理空间数据限制过严又会滞缓社会经济发展。

二是如何保障地理空间数据所有者的合法权益问题。地理空间数据是一种商品,地理空间数据的所有者付出了大量的人力、物力和财力生产地理空间数据,但是一些不法用户和商家非法复制、窃取、传播和破坏地理空间数据,从中牟取暴利,信息越来越难以控制,地理空间数据的所有者的合法权益得不到有效的保护。在数字条件下如何验证地理空间数据的所有者,如何证明其版权归属已经成为当前数字测绘生产中一项迫切需要解决的关键问题。

三是地理空间数据的内容认证问题。由于数字产品极易被篡改、伪造,利用被篡改的地理空间数据在军事上可能引起重大灾难,因此认证地理空间数据的真实性和完整性变得尤其重要。即数据的接收方在接收到数据后,如何确认数据的真实性和完整性?如何检测数据是否被篡改过?如果数据是被篡改过的,哪些地方被篡改了,能否恢复出原始数据?

四是内部人员的泄密问题。目前研究安全问题一般关注的是防止外部人员窃取信息,实际上,内部人员有意或无意的泄密行为是更大的安全隐患,比如移动存储设备丢失、电脑被窃,甚至于内外勾结,内部人员主动外泄等。传统的对信息进行加密的方法已不能解决这个问题,因为内部人员可以利用授权将信息解密,然后进行复制、分发、传播等非法行为;另外,采用传统的加密方式,用户每次都需要手动加密和解密文件,不仅操作烦琐,容易出现人为的疏漏,而且文件本身也存在一定时间的“风险期”,即文件在使用过程中未加密时以明文形式在硬盘中存储的阶段,这个阶段极有可能被早已潜伏在电脑中的木马或其他形式的病毒将其窃走。因此,必须加强地理空间数据的防扩散技术研究,控制地理空间数据只能在本机(或内部网络环境)使用,一旦离开本机(或内部网络环境),数据就无法使用,防止地理空间数据的非法扩散。

地理空间数据安全保密技术缺乏,严重制约了地理空间数据服务的能力和水平,为了保护地理空间数据的知识产权、维护数据所有者的合法权益、维护市场秩序,满足社会发展需要,充分发挥地理空间数据的价值,为实现地理空间数据共享等提供技术支撑,必须加强地理空间数据安全保密技术的研究。

地理空间数据存在哪些安全问题?有哪些关键技术?如何既充分利用现代技术所带来的好处,同时又保障数据的安全?如何保障地理空间数据不被非授权者获取?如何打击不良授权者通过合法手段获取数据后,再进行非法交易、篡改、伪造、发布等行为?数据的版权怎样保护?这些问题已经成为必须解决的关键问题。传统的安全手段无能为力,必须开拓新思路、研究新技术。

1.3.4 地理空间数据安全的国内外研究现状

地理空间数据安全涉及测绘科学与技术、密码学、计算机应用技术、信号与信息处理等多学科领域,这种跨学科的项目在国外也只有少数人在研究,国内才刚刚给予关注。

为保障地理空间数据的安全,我国已制定了一些专门的规定,如《关于对外提供我国测绘资料的若干规定》《测绘管理工作国家秘密范围的规定》《中华人民共和国地图编制出版管理条例》《公开地图内容表示若干规定》等,但这些规定主要是针对模拟形式的空间数据制定的。随着信息技术的发展,地理空间数据由模拟形式转变成了数字形式,而原有标准缺乏对数字化的地理空间数据的安全规范,已不适应当前我国地理空间数据的特点,地理空间数据的安全问题已逐步引起决策层和广大科研人员的重视。

国内的研究现状可以概括为三点:一是信息安全已进入国家领导层的视野,已引起了各部门的重视,但对地理空间数据这一块,尚未有足够的关注和举措;二是传统的保密安全法规已开始向数据资源延伸,有一般性的条文,但无技术保障,缺乏可行性与可监督性;三是国内研究地理空间数据共享的问题较多,各单位出于自身利益的考虑,希望通过共享来获得更多的地理空间数据资源,而对地理空间数据的安全和保密问题则重视不够,或不愿受更多的限制。因此,我们迫切需要制定出与数字化的地理空间数据相对应的安全保密标准以及法律、法规,与地理信息共享法、知识产权保护法相配套,只有这样才能做到既满足国民经济发展对地理空间数据的需求,又保障地理空间数据的安全需求,有利于地理空间数据的有序发展。

国内有关地理空间数据安全问题的研究处于分散、纯技术的阶段,仅为某些单位和某些设施的安全提供技术保障。涉及地理空间数据与国家安全的整体思路尚未形成,也缺少相应研究计划,特别是尚未引起国家、军方主管部门的重视。虽然一些科研院所等单位分别在这一领域进行了一些探索性的研究,但总体上还处于起步阶段,往往都是关于地理空间数据某一方面的某一种具体的安全措施,是一种个案研究行为,还没有一个全面、详细的安全方案。

在国外,特别是一些西方发达国家,地理空间数据安全问题先后进入了国家安全领域(李淑霞,2003)。如美国,在2001年“9·11”事件之前,政府在地理空间数据政策方面一直倡导开放和共享,主张民众对政府地理空间数据的合法访问和使用,在此期间,地理空间数据政策方面的研究主要侧重于地理空间数据共享中的技术、政策、标准、人才和成本回收等问题,但同时也对空间数据的安全问题做了一些具体规定,如作为地理空间信息政策基础的《美国法典》,以及1996年颁布的国防部关于国家影像与制图局(National Imagery and Mapping Agency, NIMA)的指示都有安全规定。但在“9·11”事件之后,美国的地理空间信息政策开始从开放转向保护,甚至趋于保守。2001年10月12日美国总检察长签署了备忘录,敦促各联邦机构严格按照《信息自由法》的要求,严加注意信息的公开。新政策取代了1993年鼓励政府信息公开的备忘录,强调在两可的情况下,不公开信息。同时,NIMA网站也停止了向公众出售大比例尺地图,禁止搜索引擎下载地图。运输部管道和危险材料安全管理局在网站上发出通知称不再开放“国家管道制图系统”,2001年10月12日,联邦书库收到来自美国地质测量局的请求,销毁含有大坝和水库及其地理位置等各种水资源信息的某种CD-ROM出版物的所有拷贝。其后,美国政府不断完善其数据保护政策。2003年5月13日颁布的国防部第5030.59号指示令中规定,任何NIMA生产或从NIMA源数据中派生的属于或受控于国防部的无密级的影像或地理空间信息和数据,满足下列条件的必须禁止其公开发布:

- (1)来源于或所包含的信息符合某项国际协议中的规定,或限定该类信息向协议方政府官员公开,或限定该类信息仅供军方或政府使用。
- (2)包含的信息已经在文件中明确,如果对其开放,将泄露过去获取地理空间数据和信息产品源数据的保密或敏感的原始资源和方法或能力。

(3)包含的信息已经在文件中明确,如果对其开放,将危害或干扰正在进行的军事或情报工作,泄露军事行动或紧急计划,或泄露、危害或危及军事或情报能力。

这些信息必须标记为“限制分发”。NIMA 局长有权决定对任何其他受控和属于国防部的地理空间信息或数据是否授权相似的保护。“9·11”事件唤起了美国对本土安全问题的重视,美国政府制定了一系列针对本土安全的信息保护政策,其中美国政府工作人员最担心的则是地理空间信息资源。为此,国家地理空间情报局(the National Geospatial-Intelligence Agency,NGA;NGA 的前身是 NIMA)加强了对地理空间信息造成的国家安全问题的重视,并专门委托兰德公司进行了评估。在此基础上,联邦地理数据委员会(Federal Geographic Data Committee,FGDC)颁布了《关于正确设置地理空间数据访问方法中的安全问题的指导办法》。该指导办法提供了确定地理空间数据集中的敏感内容的方法过程,提供了一种判定过程决策树,有助于各部门正确设置地理空间数据访问方法并且保护其敏感的信息内容,该指导办法于 2004 年发布。

总的来说,目前国内外在地理空间数据安全方面的研究还处于起步阶段,虽制定了一些安全规定和措施,但还很不完善,与地理空间数据的安全需求不相适应,可以看出这是信息技术带来的一个急需开展深入工作的新领域。

1.4 地理空间数据隐写与数字水印

密码技术是通过特殊的编码将要传送的秘密信息转变成伪随机的乱码,以对通信双方之外的第三方隐藏其通信的内容。密码技术是解决信息安全最根本的手段,是信息安全的核心,是控制信息访问的一种有效机制,在保护信息的安全方面发挥着重要作用,但是密码技术存在着天然的局限性,如信息经过加密处理后,原来有意义的明文信息变成无意义的、无法识别的、无法理解的密文信息,它在改变信息的可理解性的同时,却暴露了重要信息的存在性,从根本上造成一种不安全性。

为了克服密码技术的局限性,古老的信息隐藏技术又重新回到人们的视野,并逐渐被人们重视。当然,人们现在所研究的信息隐藏技术绝不是基于语言学或基于蜡版、化学方法等技术性的传统的信息隐藏,而是新兴的基于数字媒体的信息隐藏,即研究如何把一份重要的秘密信息隐藏在一份普通的多媒体信息中。信息隐藏技术是信息安全领域发展起来的前沿技术,它利用载体信息的冗余性,把一个有意义的信息隐藏在载体信息中得到隐秘载体,非法者不知道这个普通信息中是否隐藏了其他的信息,而且即使知道,也难以提取或去除隐藏的信息。它不仅隐藏了信息内容本身,而且隐藏了信息的“存在性”,使它们看起来与一般非机密资料没有区别,有更大的隐蔽性和安全性。信息隐藏技术是密码技术的有效补充,共同保障信息安全。

信息隐写和数字水印是信息隐藏的两个最主要的分支。它们实质上是一样的,都是将秘密信息隐藏在载体对象中,但是它们的侧重点不同。信息隐写是一种保密通信技术,它的主要目的是将重要的信息隐藏起来,以便不引人注意地传输和存储。嵌入对象是秘密信息,即通过隐写手段保护的主体,而载体对象可以是任何能够达到隐蔽传输目的的载体数据。通常情况下,选择载体对象时需要考虑隐写容量的大小和隐写结果的不可感知性这两方面因素。数字水印主要用于数字产品的版权保护及其真实性和完整性认证。载体对象是要保护的对象,而嵌入对象则只是用来保护载体对象的标记,而且这种标记通常是不可见或不可察的。