文章编号:1671-8860(2010)09-1096-04　　文献标志码:A

面向遥感影像内容的多级安全授权方法

刘　进[1]　孙　婧[1]　徐正全[1]　姚　晔[2]

(1　武汉大学测绘遥感信息工程国家重点实验室,武汉市珞喻路 129 号,430079)
(2　UT 斯达康通讯有限公司,杭州市六和路 368 号,310053)

摘　要:针对遥感影像数据海量的特点和对安全保密的应用需求,提出了一种面向内容的遥感影像多级安全授权方法。采用选择性的多机密区域多密级的遥感影像加密算法,在保持遥感影像格式和各项应用特性不变的基础上,分发给不同用户相同处理后的影像数据和不同权限的密钥,使不同用户通过各自密钥解密获取不同信息程度的影像数据。实验结果表明,该方法具有高机密性和高计算效率,能有效解决海量遥感影像数据的安全保密难题。

关键词:遥感影像;多区域选取;多级加密;多级内容授权
中图法分类号:P237.3

目前,关于遥感影像安全问题的研究主要侧重在数字水印[1,2]、信息隐藏[3,4]和基于传统的影像加密技术[5]等方面。遥感影像的数字水印技术主要是解决遥感影像的版权保护问题,没有实现遥感影像数据本身的安全保护;信息隐藏一般是将含有机密信息的数据隐藏于非机密影像数据中,隐藏的数据量有限,而且非机密影像数据中嵌入影像机密信息后有可能会影响遥感影像的压缩、分析等应用,实用性不强;基于传统的影像加密技术由于没有考虑到遥感影像的特性和安全需求,其加密速度和加密效率不高。

关于多级安全授权的研究目前主要集中在文件信息整体多级授权,所有的文件信息都有一个密级,用户的权限不小于该文件的密级,则可以访问此文件,反之亦然[6],而针对遥感影像中不同区域的内容多级授权则鲜有研究。

本文结合遥感影像的特性,将区域多级授权思想引入到遥感影像的安全保护过程中,在保证海量遥感影像多区域机密数据快速加密的同时,不同等级的用户最终获得不同重要程度等级的遥感影像。

1　遥感影像内容的多级授权需求

1.1　加密区域的选取

遥感影像数据量巨大,如果对需要保密的影像数据不加区分地全部加密保护,必将耗费大量的时间和处理能力,并影响遥感影像的应用。在绝大多数遥感影像中,需要保密的机密区域只占整幅遥感影像很小的比例,如一帧影像包括$\{R_1,R_2,R_3,R_4,\cdots,R_n\}$区域,其中 S 为机密区域集,$/S$ 为非机密区域集。设

$$\begin{cases} S=\{R_1,R_2,R_3\} \\ /S=\{R_i \mid 3<i<n, i\in N\}=\{R_4,R_5,\cdots,R_n\} \end{cases} \tag{1}$$

S 集中的区域信息不能被普通用户获取,而影像中$/S$集信息可以被普通用户获取,因此没有必要对整幅影像数据进行加密保护。本文采用面向内容的选择性加密方法,仅加密重要区域的影像数据,如仅对影像中的 S 集数据进行保护。

1.2　多密级安全授权

遥感影像的应用不仅包含军事应用,而且还扩展到普通民用领域。设遥感影像数据的用户群为$\{U_1,U_2,U_3,U_4,\cdots,U_n\}$,其中包括军事/国防

收稿日期:2010-06-18。
项目来源:国家 863 计划重点资助项目(2007AA12020204);国家自然科学基金资助项目(40871200);测绘遥感信息工程国家重点实验室专项科研经费资助项目。

部门、政府机构、科研院所和普通民众等。U_1、U_2、U_3、U_4 等用户群具有不同的等级,设 $U_1>U_2>U_3>U_4$,分别对应着军事/国防部门、政府机构、科研院所和普通民众用户群。不同等级的用户群可以访问到的机密地物范围不同[7]。设 R_1,R_2,R_3,R_4,…,R_n 区域级别为 $R_1>R_2>R_3>R_4>\cdots>R_n$,经过对区域数据多级加密保护,不同等级的用户群经过相应权限密钥解密后,获取不同重要等级程度的信息,达到多级授权,其描述为:

$$\begin{cases}\{U_1,\text{Key\_}U_1\}\rightarrow\{R_1,R_2,R_3,R_4,\cdots,R_n\}\\ \{U_2,\text{Key\_}U_2\}\rightarrow\{R_2,R_3,R_4,\cdots,R_n\}\\ \{U_3,\text{Key\_}U_3\}\rightarrow\{R_3,R_4,\cdots,R_n\}\\ \cdots\end{cases}\tag{2}$$

1.3　基于内容的遥感影像加密

对遥感影像中部分区域进行加密的过程中,为了不影响剩余遥感影像的使用价值,需要采用基于内容的遥感影像加密方法。遥感影像格式编码都是按照统一的协议标准来组织结构的[8,9],协议采用固定的语法信息和语义信息组织影像数据结构。

语法结构信息在影像格式协议标准中起组织和指示语义信息的作用,对影像的解码识别和提取压缩码流有重要作用,加密特殊码字容易造成已知明文攻击,因此语法结构信息不能被加密保护。语义结构信息用来指示影像中的颜色、纹理、结构等内容信息,对其加密可以达到保密内容信息和降低机密区域分辨率的效果。对于此部分的数据加密,可以保证加密后的码流仍然符合标准,不产生非法码字,可以实现基于内容的加密保护[10]。

2　面向内容的多级安全授权算法

2.1　机密区域的描述、提取方法

遥感影像机密区域的描述、提取就是对遥感影像进行分割,把影像分割成各具特性的区域并提取出感兴趣目标的技术和过程[11]。由于遥感影像本身的复杂性,使得对其分割没有完全可靠的模型进行指导。

本文采用将遥感影像中地物进行分层和分类的方法,如分为点、线、面 3 层,或者分为民用建筑、飞机场、军事基地等各类地物,然后根据要加密的机密信息的空间性质和光谱特性,在相应的层或者地物类别中分析出机密信息。无论机密信息是什么形状的地物,均可用其最小外接矩形或直接采用点、线、面工具来选定,并将该包含机密地物的区域从遥感影像中分割和提取出来。

2.2　多区域多级安全加密的基本框架

为了减少加解密次数,提高系统效率,本文设计一个多级安全加密系统,实现“一次加密,多级解密”。原始遥感影像经过分割、提取后,得到 n 个机密区域影像和剩余影像。各个机密区域影像被分别指定密级,多级密钥分发系统产生其对应级别的密钥,安全加密系统利用产生的密钥加密相对应的机密区域,形成密文数据。每个机密区域影像块的密级信息、边界信息填入到机密区域描述文件中。系统将得到的处理后的影像和机密区域描述信息分发给不同权限等级的用户。不同等级的用户所获得的影像数据相同,不需要区分不同的用户给予不同的遥感影像数据,从而有效地简化了遥感影像数据的管理。

2.3　多级安全授权的密钥生成

遥感影像分发系统内的用户可以按安全权限分成不相交的用户类集合:$A=\{U_1,U_2,\cdots,U_n\}$,每个用户都有一个相应的安全级。用偏序关系“$\leqslant$”表示 A 中用户间安全级的高低,$U_i\leqslant U_j$ 就表示用户类 U_i 的安全级不高于用户类 U_j 的安全级,从而$(A,\leqslant)$构成一偏序集。

本文方法中遥感影像的用户群包括高、中、低 3 个密级的用户和普通用户,可知用户间的权限关系是一个全序集即 $U_1\leqslant U_2\leqslant\cdots\leqslant U_n$。采用密码学中单向陷门函数可以实现本方法中的多级安全。用户 U_j 仅需保存自己的密钥 K_j,当且仅当 $U_i\leqslant U_j$ 时,用户才能从 K_j 中计算出 K_i。如果 $U_i\geqslant U_j$,那么由 K_j 不能计算出 K_i[8]。

多级安全密钥产生模块使用一个随机数 Key0(需要检验其随机特性)作为初始密钥,使用 ElGamal 公开密钥密码算法(也可采用其他公钥算法)计算多级数据加密密钥。ElGamal 密钥对的私钥 SK 作为单向加密函数 E_{SK} 运算的密钥,加密密钥 SK 对初始密钥 Key0 多次使用单向加密函数 E_{SK} 分别生成由低到高的多级数据加密密钥 Key1、Key2 和 Key3。私钥 SK 由多级安全密钥产生模块产生和保存,任何等级的用户都不可能获取 SK,而公钥 PK 分发给所有等级用户。同理,在解密端,使用相应的解密函数 D_{PK} 通过公钥 PK 由高级别数据加密密钥可以生成低级别数据加密密钥,例如,高级别权限的用户可以使用自己的高级密钥 Key3 通过多次使用单向解密函数 D_{PK} 分别得到中低级密钥,计算过程为:

$$\begin{cases}\text{Key2}=D_{PK}(\text{Key3})\\ \text{Key1}=D_{PK}(\text{Key2})\end{cases}\tag{3}$$

3 实验与分析

3.1 模拟实验

采用美国地球之眼公司提供的GeoEye-1卫星图片(见图1)(500×378)测试遥感影像的多级安全授权方法,其能提供50 cm精度的影像数据。

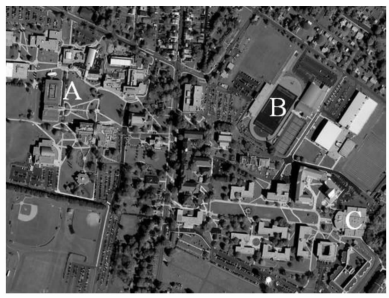

图1 实验遥感影像

Fig. 1 Remote Sensing Images for Experiment

对于多级授权方法中的机密区域的选取,本文分别采用基于外接矩形和基于点、线、面两种方式进行了实验。

1) 外接矩形的多级授权方法。对于任何形状的地物均可用其最小外接矩形近似描述其外围边界,可将影像中包含的机密地物通过最小外接矩形从遥感影像中分割和提取出来。机密区域范围较大时,一般内部区域选用较大分辨率的矩形区域类,如从图1遥感影像中提取的3个较大矩形区域影像(82×100)(见图2(a)、2(c)、2(e))。对于机密区域边界的选取一般采用类似图2(g)所示(24×24)或更小分辨率的矩形来确定。

不同等级的机密区域确定后,通过多级密钥分发管理模块产生不同等级的密钥,然后,通过不同等级的密钥采用对称加密算法,对提取的矩形区域(包括地物的内部区域和外界区域)数据进行分等级加密,之后将加密后的影像发布。图2(b)、2(d)、2(f)为图2(a)、2(c)、2(e)的不同等级加密。从效果图中可以看出,图2(b)、2(d)、2(f)影像加密强度逐渐减小,图像质量逐一提高。图2(h)、2(i)、2(j)为图2(g)的不同程度的加密,可计算它们的峰值信噪比(PSNR)以评价加密后的视觉效果,PSNR值越大,视觉效果越好,如图2(h)、2(i)、2(j)图像质量逐渐提高。

高等级用户可以用其高级别密钥通过相应的密钥计算获取机密区域各自的低级别加密密钥,然后解密图2(b)、2(d)、2(f)区域的密文影像,从而获取完整的遥感影像信息。通过相同的方法,中等级用户可以获取图2(d)、2(f)区域的加密密钥,因而获得相应区域信息,而不能获取更高等级区域图2(a)的影像信息。而普通用户不能获取到任何机密区域的密钥,只能得到图2(b)、2(d)、2(f)不清晰的遥感影像。

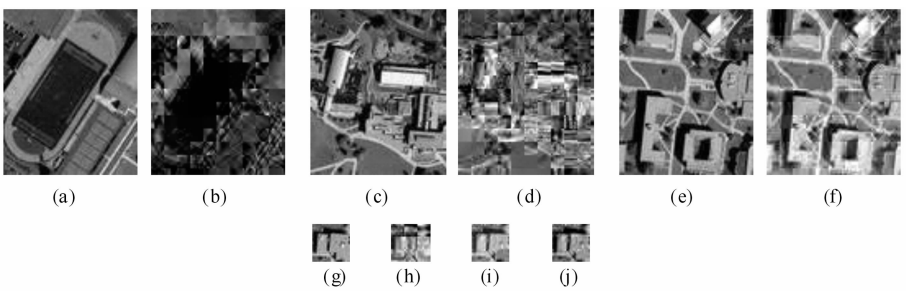

图2 区域分等级加密效果图

Fig. 2 Results of Multi-level Region Encryption Images

2) 直接采用点、线、面工具选取机密区域的多级授权方法。如图1影像中的A、B、C 3个区域,机密程度等级为$A>B>C$,采用本文提出的多级授权加密算法对3个区域进行不同等级的加密,然后将其发布。对3个区域进行加密后的影像如图3所示。

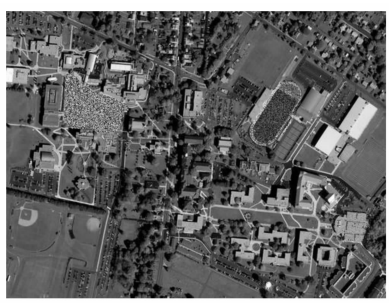

图3 基于点、线、面选取机密区域的多级加密

Fig. 3 Security Regions Multi-level Encryption Based on Point, Line and Plane Selection

从处理后的影像可以看出,A、B、C 3个区域的影像(相对于原始遥感影像)已经不同程度地被扰乱,区域A的影像完全被扰乱,不能从中获取任何信息,区域B、C影像分辨率下降,区域B比区域C下降的程度大。将处理后的相同影像

分发给不同用户,高等级用户可以用其高等级密钥计算出机密区域 A、B、C 各自的加密密钥,从而可以解密获取完整的遥感影像信息。通过相同的方法,中等级用户可以获取加密机密区域 B、C 的密钥,因而获得区域 B、C 信息,而不能获取区域 A 的影像信息。而普通用户不能获取到区域 A、B、C 的密钥,不能解密任何区域。

3.2 性能分析

本文提出的遥感影像多级授权算法的安全性主要依赖于机密区域对称加密算法和多级密钥产生模块管理的安全。其中,对称加密算法采用 AES 加密算法,多级密钥产生模块的安全性依赖于公钥加密算法 ElGamal,两者对目前所知的任何攻击都是安全的[12]。

在计算效率方面,由于只加密遥感影像中需要保密的部分影像(部分重要区域),并且对需要加密的机密区域内容采用分等级的加密保护方法,同时,采用的加密算法为对称加密算法,计算效率高,可以满足实际应用的要求。

4 结　语

本文提出了一种面向内容的遥感影像多区域多级安全授权方法,该方法首先对遥感影像的机密区域进行分割、提取,根据机密区域的机密程度采用不同级别的密钥对其进行面向内容的加密。高级别密钥通过计算可得出低级别密钥,从而可以解密采用低级别密钥加密的机密区域,反之则不行。安全测试和实验结果表明,本文提出的遥感影像多级安全授权方法计算量小,复杂度低,可靠性高,可以解决高分辨率遥感影像应用推广和安全性之间的矛盾。

参　考　文　献

[1] Barni M, Bartolini F, Cappellini V, et al. Watermarking-Based Protection of Remote Sensing Images: Requirements and Possible Solutions [C]. Mathematics of Data/Image Coding, Compression, and Enoryption, with Applications, San Diego, 2001

[2] Barni M, Bartolini F, Cappellini V, et al. Watermarking Techniques for Electronic Delivery of Remote Sensing Images [J]. Optical Engineering, 2002, 41(9): 2 111-2 119

[3] 闵连权. 基于 LSB 的遥感图像安全传输模型[J]. 测绘工程, 2005, 14(3):11-14

[4] 王贤敏,关泽群,吴沉寒. 基于遥感影像融合的不同权限信息隐藏盲算法[J]. 遥感学报, 2005,9(5): 576-582

[5] 王振朝,王芳,郑伟. 基于混沌序列的遥感图像的加密和解密[J]. 河北遥感, 2007(1):11-12

[6] 姬东耀,张福泰,王育民. 多级安全系统中访问控制新方案[J]. 计算机研究与发展, 2001,38(6): 715-720

[7] 姚晔. 基于内容的可视媒体多级授权理论与方法研究[D]. 武汉:武汉大学,2008

[8] 李飞鹏,杨志高,秦前清,等. 高分辨率遥感影像的实时压缩算法[J]. 武汉大学学报·信息科学版, 2004,29(3) :259-263

[9] 朱欣焰,陈能成,王密,等. 面向网络的海量影像空间数据在线分发技术[J]. 武汉大学学报·信息科学版,2003,28(3):288-293

[10] Wen J T, Severa M, Zeng W J, et al. A Format-compliant Configurable Encryption Framework for Access Control of Video [J]. IEEE Transactions on Circuits and Systems for Video Technology, 2002,12(6): 545-557

[11] 章毓晋. 图像分割[M]. 北京:科学出版社,2001

[12] Mollin R A. An Introduction to Cryptography[M]. Boca Raton,FL:CRC Press,2006

第一作者简介:刘进,博士生,主要从事遥感影像处理、信息安全方面的研究工作。

E-mail:honghurenmin@163.com

Content-Oriented Multi-level Security Authorization of Remote Sensing Images

LIU Jin[1]　*SUN Jing*[1]　*XU Zhengquan*[1]　*YAO Ye*[2]

(1　State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, 129 Luoyu Road, Wuhan 430079, China)

(2　UT Starcom Communication Inc, 368 Liuhe Road, Hangzhou 310053, China)

Abstract: The most confidential information of remote sensing images is related to military security and political stability , and confidential information of the regional data need to be

(下转第 1103 页)