矢量地图数字水印研究综述

孙建国[1] 门朝光[1] 俞兰芳[2] 曹刘娟[1]

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1] (哈尔滨市职工医学院 哈尔滨 150001)[2]

摘 要 矢量地图广泛应用于地理信息系统、军事测绘等领域。矢量地图数字水印为数字地图提供版权保护及防伪认证等功能,近几年其研究取得了较大的进展。为使人们对该领域研究现状有概要了解,首先论述了矢量地图水印的特性及评价准则;然后重点分析了空域、频域、零水印以及多重水印算法,并通过实验比较了几类算法的优缺点;最后提出了矢量地图数字水印的发展方向和研究目标。

关键词 信息隐藏,数字水印,矢量地图,评价

中图法分类号 TP391 **文献标识码** A

Survey of Digital Watermarking for the Vector Maps

SUN Jian-guo[1] MEN Chao-guang[1] YU Lan-fang[2] CAO Liu-juan[1]

(School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]

(Harbin Staff Medical College, Harbin 150001, China)[2]

Abstract Vector maps are widely used in the geographic information systems (GIS), military surveying and mapping and so on. Watermarking techniques for vector maps are widely used for protecting the copyright of digital maps, preventing from illegal forgery and authentication. They have been well developed recently. Firstly the characters and appraisement criteria of watermarking for vector maps were given. Then the analysis of spatial domain, frequency domain, zero-watermark and multi watermark were discussed. The comparisons showed the advantages and disadvantages of these algorithms. Finally the development direction and possible research targets were pointed out.

Keywords Data hiding, Digital watermarking, Vector map, Appraisement

数字地图是一种重要的有价值的信息资源。作为地理信息系统、智能交通系统、Web地图服务等技术的核心组成部分,数字地图面临着严峻的数据安全问题。数字水印技术为数字地图提供了版权认证及内容完整性保护的服务。

2维数字地图分为两类:栅格结构和矢量结构[1]。前者通常表示为图像像素的2维序列,很多图像数字水印技术均适用于该类数字地图的版权保护。矢量地图由于精度高,数据冗余量小及高压缩率使得水印技术的应用较为困难[2]。

本文总结了当前国内外矢量地图数字水印技术的研究情况,结合仿真实验分析了研究路线和存在的主要问题,并对该领域未来可能的研究方向和重点进行了讨论。

1 矢量地图数字水印基本情况介绍

1.1 矢量地图的基本特性

矢量数字地图一般由3部分组成:地理(geometric)信息、属性(attribute)信息和拓扑(topological)信息。地理信息主要包括矢量空间内实体的位置信息、定位信息,如点的坐标;属性信息主要描述空间实体特征,如名称,类型等;拓扑信息则主要记录空间实体间的拓扑关系。目前大多数研究方法都将地理信息与拓扑信息结合起来,称为空间数据(几何数据)信息。信息按类型的分层管理是数字矢量地图的数据处理技术之一。在我国,通常将矢量地图中各种信息要素分为14层。

矢量数字地图(见图1d)的表示由点、线、区域3类基础图层复合而成。点图层(见图1a)元素使用空间坐标形式(x, y)表示;线图层(见图1b)元素表示为序列$\langle(x_1, y_1), (x_2, y_2), \cdots, (x_i, y_i)\rangle$,其中$(x_1, y_1)$代表线的起点,$(x_i, y_i)$代表线的终点;区域(图1c)则表示为环$\langle(x_0, y_0), (x_2, y_2), \cdots, (x_i, y_i), \cdots, (x_0, y_0)\rangle$,从点$(x_0, y_0)$开始沿固定方向环绕,最终回到$(x_0, y_0)$处。通常,经过点、线和区域图层的叠加就能够表示具有矢量结构的数字地图。

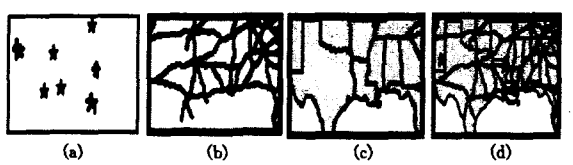

图1 矢量数字地图的组成

1.2 矢量地图数字水印的基本特性

根据矢量地图数据特点,其数字水印应具有如下要求:

1)不可感知性:数字水印的嵌入要求不会引起矢量地图数据的明显改变。所谓"明显"是导致地图的视觉失真和测量

到稿日期:2008-11-03 返修日期:2009-01-04 本文受国家自然科学基金(60873138)资助。

孙建国(1981-),男,讲师,CCF会员,主要研究方向为信息隐藏与数字水印等,E-mail:sunjianguo@hrbeu.edu.cn;门朝光(1963-),男,教授,博士生导师,CCF高级会员,主要研究方向为可信计算、数字水印等;俞兰芳 女,副教授,主要研究方向为智能信息处理等;曹刘娟 女,博士研究生,主要研究方向为无损数字水印及信息隐藏等。

失真。

2)不可抵赖性:对水印信息的解释具有唯一性,即算法所描述的嵌入及提取过程无歧异,对相同的信息输入应具有水印信息的重现特征。

3)容量:对于水印所选择的嵌入方式,要保证载体有足够的嵌入空间,过少的嵌入量会降低水印的安全性能。

4)高精度:矢量地图在军事、测绘、导航等领域获得广泛的基础在于其高精度特性,尤其是定位精度,水印的嵌入应以不破坏地图使用及精度为前提。

5)安全性:包含两个方面,非法用户不能感知水印信息存在,合法用户在未授权情况下无法提取或检测到水印。

6)鲁棒性:当矢量地图遇到几何变换、数据压缩、存储格式转换等操作时,要求水印信息能够保证其完整性及抗攻击能力。

1.3 矢量地图数字水印性能的评价准则

矢量地图数字水印不仅要求嵌入的水印信息不被发现,同时要确保矢量地图在经过某种变换操作(如变换、压缩、简化、恶意攻击等)后,仍能正确地提取到水印信息。其中,衡量水印技术可行性及有效性评价指标包括8类,如表1所列。

表1 矢量地图数字水印指标说明

序号	指标	说明
1	不可见性	保证矢量地图水印的感官检测率较低
2	鲁棒性	对于地图修改变换操作,水印具有抵抗能力
3	不可抵赖性	水印能够唯一确定嵌入的矢量地图,无歧义
4	精度无损	保证矢量地图的高精度,特别是定位精度
5	效率	水印嵌入提取过程改动和读取的信息量
6	水印容量	保证容纳的数字水印编码规模
7	误码率	提取的数字水印编码被错误编译的比例
8	抗数据压缩	保证矢量压缩过程中对水印的影响尽可能小

1—6号指标可以归纳为矢量地图数字水印的隐藏性分析和隐藏性攻击[3]。隐藏分析通常包括视觉检测和工具检测两方面内容;视觉攻击通常采用基于统计的方式。常用的工具检测方法主要包括LSB(最不重要位)法[4]、特征检测法[5]、统计学检测法[6]等。隐藏性攻击主要借助于水印攻击软件,目的是将水印从被嵌入对象中强行移除。

误码率通常用于横向比较几种水印算法的实用性和可靠性,在水印信息的同等嵌入率下,评价误码率低的水印算法是最优的。

抗矢量数据压缩是衡量矢量地图数字水印性能的重要指标。由于矢量地图资源庞大,动辄几十个G的空间占有率,因此,在地图使用和传播过程中,往往需要进行复杂的矢量数据压缩。数据压缩使得嵌入地图的水印信息存在被轻易去除或改变的风险,因此,能够抵抗矢量数据压缩是考核水印可行性的必备要素之一。

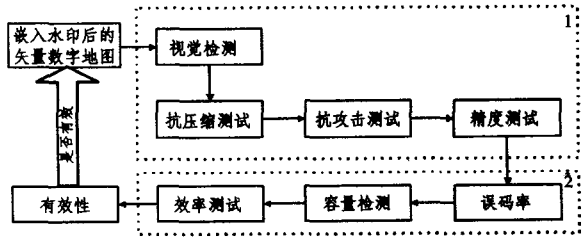

图2 矢量地图数字水印有效性验证流程

对于矢量地图数字水印有效性的检测通常经过以下过程(见图2):其中区域1过程主要验证水印算法的可行性和正确性;区域2过程主要验证算法的性能和实用性。对应各环节的主要结论为性能评价指标。

2 矢量地图数字水印技术研究现状

矢量地图数字水印的研究起步较晚,国内外可检索到的文献仅有百余篇[7],国内有关该领域的数字水印发明专利申请仅有两项。结合目前公开的文献,将矢量地图数字水印算法主要分为空域数字水印、频域数字水印、零水印、多重水印。

2.1 空域水印算法

文献[8]中最早提出了空域数字水印思想,同时它也是最早公开发表的有关矢量地图数字水印的文献,其思路是选取矢量地图上的结点位置坐标,将水印信息按照比特单位独立地嵌入坐标值内,嵌入操作彼此独立;该算法为矢量地图空域水印研究提供了理论基础,但由于嵌入方式对地图精度扰动过大,且难以抵抗简单的几何攻击,因此,尽管算法效率较高,易于实现,但在矢量地图版权保护方面不具有现实的可行性。

Tirkel等人提出将最不重要位(LSB)替换和位平面工具应用于空域算法,以提高空域算法的鲁棒性。最低有效位(LSB,Least Significant Bit)是一种典型的空间域数据隐藏方法,其理论基础在于矢量地图图像的每个像素点都由多比特方式构成,根据像素点对图像能量的贡献程度不同,把整个图像分解为8个位平面,即从最低有效位0到最高有效位7。由于低位所代表的能量很少,改变低位对图像的质量没有太大的影响,因此Tirkel提出利用最低有效位隐藏水印信息。该方法早期仅用于图像数字水印。文献[9]提出将LSB方法与矢量地图的拓扑信息相结合的算法,并对水印信息预加密,算法在一定程度上提高了空域水印对于剪切、扭曲等几何攻击的抵抗能力。

随着理论研究的深入,近年来,空域水印主要朝两类研究方向发展:

1.以提高抗攻击能力及鲁棒性为主的空域水印。文献[10]提出网格划分思想,通过双重网格将水印信息分散隐藏到顶点坐标最低有效位上,以此抵抗常规的顶点编辑和地图剪切攻击;文献[11]提出一种基于四叉树划分的矢量地图空域水印算法,在保证任意矩形网格所包含顶点数均等的前提下,把地图划分为矩形子块,并在不同子块中重复多次嵌入水印信息,以此提高水印算法在全局范围内的鲁棒性;文献[12]则对文献[11]中的四叉树划分算法进行了扩展,提出了一种双重嵌入的矢量地图水印算法。该算法按地图对象特征把矢量地图分为两层,对不同的图层采用不同算法调制水印信息嵌入到各顶点,并分别计算两个图层中代表水印信息的位移量,在阈值的控制下,选择有效的顶点并计算坐标平均值,即得到水印信息位序列。该水印算法特别对随机噪声、扭曲变形和各种剪切攻击具有很强的鲁棒性。

2.以减少对矢量地图精度损伤为目标的空域水印。文献[13]在差值扩大思想基础上,提出一种无损数据隐藏算法。通过修改地图中相邻顶点坐标间的差值来嵌入水印信息,在较强坐标相关性的地图中具有较高的嵌入容量。文献[14]将矢量图层所含多边形特征分解,对分解后的矢量多边形进行分析。选择合适的多边形的线段,在其顶点处嵌入水印。该方法对于坐标变换、平移、旋转、缩放,以及图形剪切均具有较

强的鲁棒性。

此外，文献[15]提出了一种抗矢量数据压缩的空域水印算法，即在嵌入水印信息之前对数据进行道格拉斯-普克法压缩，然后在特征点中嵌入水印信息。随着矢量地图数字水印的逐步应用，提高抗数据压缩性能以及精度无损的空域水印将成为研究重点。

2.2 频域水印算法

与空域方法相比，矢量地图频域水印算法的鲁棒性更强、安全性更高、可研究空间和内容更大。频域水印算法主要包括离散傅立叶变换(DFT)、离散余弦变换(DCT)和离散小波变换(DWT)[16]水印算法。

2.2.1 频域方法介绍

离散傅立叶变换(DFT)是连续傅里叶变换在时域和频域上都离散的形式，将时域信号的采样变换为在离散时间傅里叶变换(DTFT)频域的采样。

基于DFT的水印算法思路是：通过对矢量地图结点信息的提取，形成一个顶点坐标序列(X_n,Y_n)，表示为一个复数序列$u(n)$，如式(1)：

$$u(n)=x_n+iy_n(n=0,1,2,\cdots,N-1) \tag{1}$$

式中，N为序列中所有顶点的个数。通过离散傅立叶变换产生频域序列$a(k)$，如式(2)：

$$a(k)=\sum_{n=0}^{N-1}u(n)e^{-2\pi ikn/N}\quad k=0,1,2,\cdots,N-1 \tag{2}$$

逆离散傅立叶变换如式(3)：

$$u(n)=\frac{1}{N}\sum_{k=0}^{N-1}a(k)e^{2\pi ikn/n}\quad n=0,1,2,\cdots,N-1 \tag{3}$$

调整频域系数嵌入水印信息。

离散余弦变换(DCT)相当于只使用实数的DTF变换，是数字图像处理以及信号处理常用的一种正交变换，具有压缩比高、误码率小、信息集中能力强和计算复杂性综合效果较好等优点。目前普遍采用8×8的DCT变换，变换公式如下：

$$F(u,v)=\frac{1}{4}c(u)c(v)\sum_{i=0}^{7}\sum_{j=0}^{7}f(i,j)\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16} \tag{4}$$

$$f(i,j)=\frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}c(u)c(v)F(u,v)\cos\frac{(2i+1)u\pi}{16}\cos\frac{(2j+1)v\pi}{16} \tag{5}$$

式(5)中，$f(i,j)$代表图像像素矩阵(i,j)点处的像素值，$F(u,v)$代表DCT变换系数矩阵(u,v)点处的值，系数$c(u)$如下：

$$c(u)=\begin{cases}\sqrt{1/2} & u=0\\ 1 & 1\leqslant u\leqslant 7\end{cases} \tag{6}$$

同DFT一样，水印信息将嵌入到调整后的分量系数中。

Cox[17]等提出用小波变换的方法描述图像信号，并将图像信号分解成一组多尺度子带图像，即{LL，LH，HL，HH}，小波分析的多分辨率特点，使其具有对信号的自适应性，经过小波变换后能量主要集中在低频LL子带，具有较高的频率分辨率；高频子带主要是垂直LH、水平HL及对角线HH的边缘信息，含有的能量较低，具有较高的时间分辨率。

小波分解的空间频率特性是小波变换区别于DFT和DCT的一个重要方面。根据该特性可以将高强度的水印嵌入到HVS不太敏感的区域，这样在保证不影响图像视觉质量的前提下可以最大限度地增加嵌入水印的强度。图3为4级小波分解示意图。

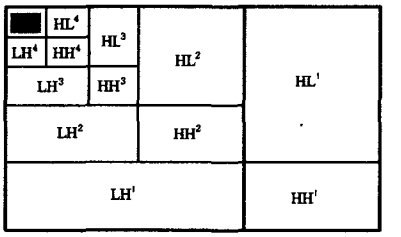

图3 小波变换示意图

2.2.2 水印算法介绍

文献[18]在空域水印算法基础之上，提出将水印信息嵌入DFT变换的中频系数内，实现空域到频域的转化，增强了水印的鲁棒性；文献[19]提出利用矢量地图多边形变换嵌入水印的理论构想，文献[20]继承并改进了该算法，对多边形集合的顶点序列中各个坐标点$V_k(x_k,y_k)$按照$a_k=x_k+iy_k$的规则，构成复数序列a_k，并对a_k进行DFT变换，使得算法的鲁棒性较空域水印均有大幅提高，能够抵抗多种几何变换攻击。

Michael Voigt[21]等人提出一种基于DCT的矢量地图水印算法，通过改变地图数据的整数DCT系数来隐含水印信息，将水印嵌入AC分量中。文献[22]选择在DCT的低频域上加载水印数据，嵌入前对原始水印和分块水印都进行扰乱处理。该算法具有较好的隐藏效果和抗剪切、抗压缩功能。

文献[23]提出基于DWT变换的盲水印算法。该方法将矢量图形中图元的顶点坐标有顺序地排成一维序列，通过离散小波变换将序列分解成不同空间和频率上的复值系数，并根据水印的大小与小波系数之间的关系把水印嵌入到小波系数的幅值中，系数的相位不变。为了保持小波系数邻域平均值的不变性，将水印隔点嵌入到系数中，最后进行小波反变换，去掉延拓的顶点，得到嵌入水印的矢量图。该算法可以抵抗复杂的几何攻击，但对于数据压缩攻击不稳健。

随着多种数学模型的引入及对频域方法的掌握，基于多种频域方法组合使用的水印算法将成为该领域的研究方向。

2.3 零水印算法

矢量地图是属性信息描述下，通过拓扑关系约束，以图形图像为表现形式的数字产品。为解决矢量地图所遭受的侵权、篡改等数据安全问题，已提出许多基于空域和频域水印的算法。上述算法通过修改地图的空域或频域系数嵌入水印标识，但算法对地图精度均存在不同程度的损失，特别是对于复杂的矢量数据压缩，实用性较差。为此，提出了对载体内容不进行任何修改的水印技术，即“零水印”[24]。

零水印算法主要包括两类：改进的频域零水印算法以及多技术融合的零水印算法。前者通过对频域算法的改进来获取水印载体的重要特征信息，通过对特征信息进行二次加密和重新构造的方式构造零水印序列或图像，由于特征点选取上存在不确定性以及频域算法本身的局限性，该类零水印易陷入局部鲁棒最优性，复杂的矢量数据压缩攻击及几何变换易导致水印失效。多技术融合的零水印算法主要结合视觉检测、图像分形计算等技术，获得水印载体对人最敏感部分的特征信息及地图的特征数据，以图像方式完成水印制作。该类算法安全性略差，当数字载体被篡改时，水印对载体的可证明性较差，难以抵抗解释攻击。

零水印算法的特点在于：1. 保持地图的完整性，使地图精度无任何损失；2. 抗矢量数据压缩能力突出，地图的使用无法脱离关键信息，而零水印是通过提取地图的关键特征形成的，与地图联系较为紧密；3. 易受到解释攻击，对于零水印的多版权申明攻击，抵抗能力较弱。

目前，有关矢量地图零水印的研究内容较少，但从面向应用的角度来看，对于零水印的第三方版权认证模式的研究也可能会成为未来的研究热点。

2.4 多重水印算法

在鲁棒性方面，单一水印具有较明显的靶向性，易被攻击者掌握或破坏。多重水印克服了单一数字水印的不足，算法将多个水印标识嵌入到载体中，并且每个水印标志都有不同的特征维度，从不同方面为矢量地图提供版权支持。多重数字水印技术可用来解决矢量地图在销售及流通领域的认证问题。多水印标识提高了水印的鲁棒性和安全性。

关于矢量地图多重水印的文献目前较少，多重水印大致分为两类：静态水印及动态水印。

静态水印是指在嵌入前，将水印标识制作完成。静态水印包括独立、组合两种嵌入方式。

独立静态水印是指根据载体特征信息，将多种数字水印标识彼此独立地嵌入。由于水印容量和载体承载水印信息能力无法预知，因此超负荷嵌入操作会导致水印的互攻击情况发生。为保证独立水印的不可见性和鲁棒性、多水印标识的嵌入顺序是该类算法的研究重点。

组合静态水印通常是在水印信息嵌入前，利用空域或频域水印算法，将多种水印标识复合生成为单一的水印标识，将该水印标识嵌入载体中。从某种意义上，该类方法可以理解为对单一水印的鲁棒性及不可见性的强化。

动态水印是在水印嵌入过程中，结合载体实际情况将多种水印标识嵌入矢量地图。该类水印更具有实时性，能够根据捕获到的载体特征信息，随时调整水印容量及嵌入强度。

对于多重水印来说，由于水印标识的嵌入和提取操作互不相关，如何保证后嵌入水印标识不对已嵌入水印造成损坏或失效是其研究难点。同时，解释攻击（或称 IBM 攻击）[25] 将是多重水印算法的瓶颈。多重水印同零水印一样，在矢量地图领域研究较少。

2.5 其它类型水印算法

除以上介绍的几类典型算法外，还包括一些其它类型的矢量地图数字水印算法。

文献[26]提出一种基于数据统计特征的水印算法，该算法以地图曲线特征点提取为基础，在控制水印嵌入扰动的前提下，尽量保持地图元素的形状特征，并对简化、乱序以及加性噪声等几种威胁较大的攻击方法进行了特殊设计，使算法获得了有针对性的鲁棒性能。但该算法对变形扭曲的攻击鲁棒性较差，同时，未对抗数据压缩性能加以讨论。

文献[27]根据矢量地图各要素层的数据规模，设计了两种不同的数据分类规则，实现了嵌入不同大小水印的算法。对数据量较小的要素层，数据分类的类型少，嵌入的水印信息小；而对数据量丰富的要素层，数据分类的类型多，嵌入的水印信息大。水印检测不需要原始矢量地图的参与，是一种盲水印算法。该算法对地图精度影响较小，对常见的水印攻击具有很好的鲁棒性，但抗矢量数据压缩性能较差。

文献[28]根据矢量数据的奇异性，将水印信息嵌入到间隔的特征点中。在水印嵌入过程中，综合分析特征点在整个数据链中的奇异性，然后在奇异性较强的特征点中嵌入水印信息，并使嵌入水印的特征点的奇异性得到增强。该算法具有很好的抵抗几何变换等攻击的鲁棒性。

以上 3 种算法均未对水印在抵抗矢量数据压缩攻击方面的性能进行深入实验和讨论，这是由于复杂的矢量数据压缩会去除大量地图实体和信息，且不同的压缩算法其压缩对象也有所不同，使得水印算法在应对复杂压缩攻击时鲁棒性较弱。目前为止，还无法获得较理想的实验结果。

3 算法仿真实验对比

在基于 MapX 插件的 VC. NET 环境下，对几类典型算法分别加以实现，并在确保相同嵌入率的情况下，对算法的鲁棒性、抗数据压缩性能以及精度损失进行了实验验证。最终的衡量指标为误码率。选择的代表性算法包括：文献[15]中的空域水印算法；文献[20]和文献[23]中的频域水印算法以及文献[26]描述的算法。

误码率是指在水印的提取过程中信息位发生错误的概率。若为 $p(0<p<\frac{1}{2})$，则正确提取的概率为 $1-p$，即水印编码前后不相同的概率是 p，则 p 称为误码率。

水印攻击方式选取了几何变换和矢量数据压缩攻击。几何变换为图 4 所示的 8 种剪切方式以及基于 X 轴、Y 轴的拼贴；矢量数据压缩选取经典的道格拉斯-普克压缩算法（DP 算法），压缩比例分别选定为 5%，15%和 30%。

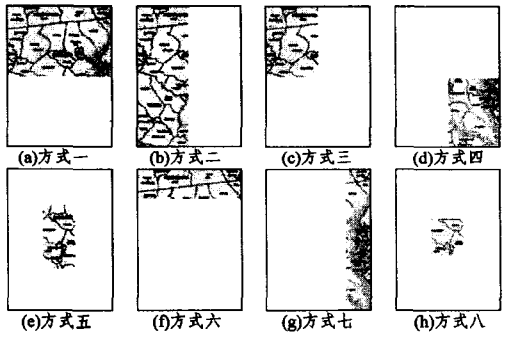

图 4 8 种剪切模式

对 4 种算法的仿真实验结果如表 2，表 3 所列。表 2 为几何攻击下各算法的误码率。由于分层嵌入以及嵌入强度的自适应调整，使得文献[26]所提出的算法在应对几何变换攻击中性能较突出。

表 2 几何变换攻击下各算法的误码率

攻击类型		误码率(%)			
拼贴	X 轴	5.25	6.7	3.15	7.09
	Y 轴	16.03	10.02	4.03	10.25
剪切	方式 1	10.84	4.18	6.17	3.84
	方式 2	18.95	8.93	11.86	6.95
	方式 3	22.46	14.14	17.1	11.46
	方式 4	28.13	18.89	23.53	13.13

表 3 为数据压缩攻击下各算法的误码率。从实验数据来看，4 种算法对矢量数据压缩攻击的鲁棒性均较差，这主要是由于水印算法过分侧重运用地图地理信息，水印算法未结合地图属性信息及拓扑关系，导致大量携带水印编码的结点或

实体被去除，水印信息被破坏甚至失效。

表 3　数据压缩攻击下的算法误码率(%)

压缩率	文献[15]	文献[20]	文献[23]	文献[26]
5%	19.86	14.48	12.29	10.55
15%	30.77	18.17	17.61	16.74
30%	37.91	29.76	25.49	19.15

整体实验结果说明：目前的矢量地图水印算法能够保证抵抗复杂几何攻击的鲁棒性能，对于如何确保地图精度零损失以及抵抗复杂的矢量数据压缩将是研究重点。

结束语　随着矢量地图数字水印由理论研究到系统应用的逐渐转变，作者认为未来的研究重点或将主要集中于以下几个方面：

1. 数据压缩攻击算法

目前，对于水印的数据压缩鲁棒性能测试，多选择已有的矢量地图数据压缩算法，但这些算法更注重于地图数据压缩的实效性，缺少有针对性的水印攻击内容，不能准确有效地评价水印性能。因此，有必要针对空域、频域等多类水印算法，提出一些用于测试水印性能的数据压缩攻击算法。

2. 精度无损

高精度是矢量地图得到广泛应用的技术基础，水印向矢量地图内容的嵌入不可避免地对地图精度产生影响，使得地图应用效果降低。已提出的无损数字水印[13]也仅是采取缩小调整幅度的方式来实现无损效果。地图精度零损失的解决思想是将水印标识嵌入矢量地图的属性空间。

3. 解释攻击

是对载有水印信息的地图不断追加其它水印标记的过程，使得地图出现版权多申明。解释攻击被认为是数字水印技术应用面临的难点之一，由于时间戳等方案同样存在被修改及缺乏第三方证明的问题，使得数字版权被轻易篡改。目前，有关应对该类攻击的水印算法较少，其研究重点将集中于将时间属性与水印信息完全绑定以及对水印信息的时效性进行证明。

4. 水印版权注册及认证

水印为矢量地图版权认证及内容完整性保护提供了技术支持，但只有公认、权威的水印认证模式，才能使水印为版权拥有者提供服务。基于第三方认证模式将成为该领域的研究热点，即版权申明方将矢量地图内容及必要的水印信息提交给第三方认证，由第三方对其进行审核和说明。一旦发生版权纠纷，第三方只需根据数字产品，查询其版权注册信息即可做出判定，该模式非常适用于网络数字产品的传播、复制及发放。

5. 性能整体评价

一直以来对数字水印性能的评价，主要包括鲁棒性、不可见性、水印容量等指标。在面向实用性的评价过程中，考虑到的因素有多种，如安全性、可行性等。为此，需要提出一种整体评价方案，赋予指标不同的权重，对每种指标的测量给出测试标准，最终以权值的方式体现水印算法的综合性能。

参 考 文 献

[1] Ohbuchi R, Ueda H, Endoh S. Robust watermarking of vector digital maps[C]// Proceedings of IEEE International Conference on Multimedia and Expo (ICME'02). Lausanne, Switzerland, 2002:577-580

[2] Voigt M, Busch C. Feature-based watermarking of 2d-vector data[C] // Proceedings of SPIE, Security and watermarking of Multimedia Content. Santa Clara, USA, 2003:359-366

[3] 王道顺，梁敬弘，戴一奇，等. 图像水印系统有效性的评价框架[J]. 计算机学报，2003，26(7)：779-788

[4] 刘红翼，王继军，韦月琼，等. 一种基于 LSB 的数字图像信息隐藏算法[J]. 计算机科学，2008，35(1)：100-102，125

[5] Avcibas I, Memon N, Sankur B. Steganalysis of watermarking techniques using image quality metrics [C] // Proceedings of SPIE—The International Society for Optical Engineering. San Jose, CA, USA, 2001, 4314:523-531

[6] Maiorana E, Campisi P, Neri A. Multi-level signature based biometric authentication using watermarking[C] // Proceedings of the SPIE-The International Society for Optical Engineering. 2007, 27:1-12

[7] Xu D H, Zhu C Q, Wang Q S. A survey of the research on digital watermark for the vector digital map [J]. Geomatics World, 2007, 12(6):42-48

[8] Cox G S, de Jager G. A survey of point pattern matching techniques and a new approach to point pattern recognition [C]// Proceedings of Symposium on Communication and Signal Processing. Lesotho, 1993:243-248

[9] 贾培宏，马劲松，史照良，等. GIS 空间数据水印信息隐藏与加密技术方法研究[J]. 武汉大学学报：信息科学版，2004，29(8)：747-751

[10] Deng Shujun, Lu Liang, Che Sen. Research on a Digital Watermarking Algorithm Suitable to Vector Map [C]// Proceedings of the IEEE international Conference on Automation and Logistics. jinan, china, August 2007:1236-1240

[11] Ohbuchi R, Ueda H, Endoh S. Robust watermarking of vector digital maps[C] // Proceeding of the IEEE International Conference on Multimedia and Expo. Lausanne, Switzerland, 2002:577-580

[12] 王勋，林海，鲍虎军. 一种鲁棒的矢量地图数字水印算法[J]. 计算机辅助设计与图形学报，2004，16(10)：1377-1381

[13] 邵承永，王孝通，徐晓刚，等. 矢量地图的无损数据隐藏算法研究[J]. 中国图像图形学报，2007，12(2)：206-211

[14] 王伟，李岩. 一种鲁棒性的 2D 矢量图形水印算法[C]// 第十三届全国图像图形学术会议. 南京，2006：191-196

[15] 朱长青，杨成松，李中原. 一种抗数据压缩的矢量地图数据数字水印算法[J]. 测绘科学技术学报，2006，23(4)：281-283

[16] Ntalianisks, Doulamisnd, Doulamisad, et a1. Automatic stereoscopic video object-based watermarking using qualified significant wavelet trees[C]// IEEE 2002 International Conference on Image Proces-sing. 2002(18):188-189

[17] Cox I J, Kilian J, Leighton F J, et al. Secure spread specnum watermarking for multimedia[C]. IEEE Trans on Image Processing, 1997, 6(12):1673-1686

[18] 钟尚平. 双重嵌入 MQUAD 水印算法分析与改进[J]. 计算机研究与发展，2005，42(增刊)：142-149

[19] Solachidis V, Nikolaidis N, Pitas I. Watermarking polygonal lines using fourier descriptors[C]// IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'2000). Istanbul, Turkey, 2000:1955-1958

[20] Kitamura I, Kanai S, Kishinami T. Copyright protection of vec-

tor map using digital watermarking method based on discrete Fourier transform[C]// International Geoscience and Remote Sensing Symposium (IGARSS). 2001(3):1191-1193

[21] Voigt M, Yang B, Busch C. Reversible watermarking of 2D-vector data[C]// Proceedings of the 2004 ACM Internation Workshop on Multimedia and security. Germany, Magdeburg, 2004: 160-165

[22] 姚惠明,周冠玲,杨义先,等. 一种基于矢量共享方案的 DCT 域上数字水印分存算法[J]. 计算机学报,2004,27(7):998-1003

[23] 李媛媛,许录平. 矢量图形中基于小波变换的盲水印算法[J]. 光子学报,2004,33(1):97-100

[24] Wen Q, Sun T F, Wang S X. Concept and application of zero watermark[J]. ACTA Electronica Sinica, 2003, 31(2): 214-216

[25] 李庆诚,窦毅. 数字水印的解释攻击与关联性特征[J]. 计算机应用研究,2005(5):115-117

[26] 邵承永,汪海龙,牛夏牧. 基于统计特征的二维矢量地图鲁棒水印算法[J]. 电子学报,2005,33(12):2312-2316

[27] 闵连权. 一种鲁棒的矢量地图数据的数字水印[J]. 测绘学报,2008,37(2):262-267

[28] 王忠军,王玉海,王豪. 一种鲁棒的矢量地图数字水印算法[J]. 测绘科学,2008,33(4):148-150

(上接第 6 页)

仅可以发挥其实际效用,还可以对其功能进行验证,以便进一步对其进行修正,使其更完善合理。

(5)模型构建方法研究。可以进一步结合计算机科学其它分支(如人工智能、机器学习)和其它学科或技术手段构建更有效、更合理、更实用的信任模型。

参 考 文 献

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management[C]// Dale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996: 164-173

[2] Jøsang A, Tran N. Trust Management for E-Commerce. 2000

[3] Koutrouli E, Tsalgatidou A. Reputation-based trust systems for P2P applications: design issues and comparison framework[C]// LNCS 4083. 2006: 152-161

[4] Weeks S. Understanding trust management systems[C]// Proc. of the 2001 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2001: 94-105

[5] RFC 1422. Privacy Enhancement for Internet Electronic Mail, Part 2: Certificate-based Key Management

[6] Gambetta D. Can We Trust Trust [C]// Gambetta D, ed. Trust: Making and Breaking Cooperative Relations. Basil Blackwell, Oxford, 1990: 213-238

[7] The Gnutella Protocol Spec. v0.6, Intelligent Club Management in Peer-to-Peer Networks[C]// Proceedings of Workshop on Economics of P2P Systems (P2PECON '03). Berkeley, CA, 2003

[8] KaZaA file sharing network[EB/OL]. http://www.kazaa.com/, 2002

[9] Resnick P, Zeckhauser R. Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system[C]// NBER Workshop on Empirical Studies of Electronic Commerce. California, 2000

[10] Rindova V P, Kotha S. Building reputation on the Internet: Lessons from amazon.com and its competitors. 2006-03-27

[11] McKnight D H, Chervany N L. The Meaning of Trust[R]. MISRC Working Paper Series 96-04. Management Information Systems Research Center, University of Minnesota, 1996

[12] Jøsang A, Ismail R, Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision[J]. Decision Support Systems, 2005

[13] Kamvar S D, Schlosser M T, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks[C]// Proceedings of the 12th International World Wide Web Conference. Budapest, Hungary: ACM Press, 2003: 640-651

[14] Bonachi P. Eigenvector-like Measures of Centrality for Asymmetric Relations[J]. Social Networks, 2001, 23(4): 191-201

[15] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities[J]. IEEE Transactions on Data and Knowledge Engineering (Special Issue on Peer-to-Peer Based Data Management), 2004, 16(7): 843-857

[16] Oram A. Peer-to-Peer: Harnessing the Power of Disruptive Technologies[M]. O'Reilly and Associates, 2001

[17] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Network[C]// Proceedings of the European Symposium on Research in Security. 1994

[18] Jøsang A. The right type of trust for distributed systems[C]// Meadows C, ed. Proceedings of the 1996 New Security Paradigms Workshop. Lake Arrowhead, CA: ACM Press, 1996

[19] Jøsang A. A model for trust in security systems[C]// Proceedings of the 2nd Nordic Workshop on Secure Computer Systems. 1997

[20] Kaelbling L P, Littman M L, Moore A W. Reinforcement learning: A survey[J]. Journal of Artificial Intelligence Research, 1996, 4: 237-285

[21] Kinateder M, Baschny E, Rothermel K. Towards a generic trust model—Comparison of various trust update algorithms[C]// Proc. of the iTrust 2005. LNCS 3477. 2005: 177-192

[22] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks[C]// Moro G, ed. Proc. of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004: 23-34

[23] Khambatti M, Dasgupta P, Ryu K D. A role-based trust model for Peer to Peer communities and dynamic coalitions[C]// The Second IEEE International Information Assurance Workshop. New York: IEEE Press, 2004: 141-154

[24] Nefti S, Meziane F, Kasiranl K. A fuzzy trust model for e-commerce [C]// The 7th IEEE Int'l Confon E-Commerce Technology (CEC'05). Edinburgh, UK, 2005

[25] Wright T. A simple algorithm for tighter exact upper confidence bounds with rare attributes in finite universes [J]. Statistics & Probability Letters, 1997, 36(1): 59-67

[26] Golle P, Leyton-Brown K, Mironov I. Incentives for sharing in peer-to-peer networks [C]// Wellman M P, Shoham Y, eds. Proc. of the 3rd ACM Conf. on Electronic Commerce. New York: ACM Press, 2001: 264-267