

矢量图形脆弱水印研究与实现^{*}

郑良斌, 冯柳平, 陈如琪, 程晓锦

(北京印刷学院, 北京 102600)

摘 要: 分析了矢量图形内容完整性认证的常用方法及矢量图形数字水印研究现状。针对线状实体组成的矢量图形, 提出将矢量图形中线状实体分成不同的组, 以组为计算单位将水印信息嵌入在矢量图形数据中, 不仅能验证矢量图形的完整性, 还能将篡改的定位能力精确到组, 嵌入了水印信息的矢量图形仍有使用价值; 在对数据精度要求极高的情况下, 可以通过数据完整性验证提取出原始矢量图形数据, 更好地满足一些特殊应用的需求。

关键词: 矢量图形; 脆弱数字水印; 完整性验证

中图分类号: TP391

文献标志码: A

文章编号: 1001-3695(2011)10-3820-03

doi:10.3969/j.issn.1001-3695.2011.10.058

Research and implementation of fragile watermark for vector graphics

ZHENG Liang-bin, FENG Liu-ping, CHEN Ru-qi, CHENG Xiao-jin

(Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: This paper described the methods of integrity authentication for vector graphics firstly, and then introduced digital watermarking for vector graphics. For vector graphics composed by linear entities, it proposed a fragile watermark algorithm, which was based on that the linear entities of vector graphics were divided into different groups, and watermark information was embedded in these groups. The extraction procedure not only verified the integrity of the watermarked vector graphics, but also located modification. The watermarked vector graphics can be used for its data is modified slightly, and the original vector graphics can be restored by extraction procedure for special application.

Key words: vector graphics; fragile digital watermark; integrity authentication

0 引言

矢量图形用一组指令集合来描述图形的内容, 这些指令用来描述构成图形的所有图元的位置、维数和形状等属性。在屏幕上显示矢量图形要有专门软件将描述图形的指令转换成在屏幕上显示的形状和颜色, 即根据矢量数据结构不同和算法不同画出这个图形。用于产生和编辑矢量图形的程序可以产生和操作矢量图形的各个成分, 并对矢量图形进行移动、缩放、旋转和扭曲等变换。

矢量图形广泛用于计算机辅助设计、地理信息系统(GIS)、艺术设计、动画制作等, 绝大多数 GIS、CAD 和 3D 造型软件使用矢量图形作为基本的图形存储格式。矢量图形具有高精度、处理自动化以及无损缩放等优点, 并且易于存储、易于发布。然而, 数字化存储的数据极易被编辑篡改, 并造成严重的后果, 如用于军事目的的地图显然不容篡改。因此, 在很多场合, 需要对矢量图形的完整性(也称真实性)进行验证, 明确地知道矢量图形是否被修改过, 甚至还希望知道矢量图形数据的哪些部分被篡改了。

数据完整性是指数据本身的真实性, 即数据是否被篡改。目前, 数字媒体内容完整性认证方案主要有两种: a) 通过传统的密码学认证方法; b) 利用数字水印技术。

传统的密码学认证方法用来验证数据的完整性已经发展得非常成熟。它把所有的数据当做二进制比特流, 计算该比特流的哈希散列值并产生消息认证码, 或者用非对称加密算法加密哈希值产生数字签名, 最后把它附加在原来消息的末尾。在传输过程中, 任何比特的改变都可能导致认证失败。传统的密码学认证方法安全性较高, 但它无法确定篡改的位置和程度。另外, 消息认证码或数字签名与原始数字媒体捆绑在一起存储或传输, 由于消息认证码或数字签名独立于数字媒体数据而存在, 因此其很容易被删除。

所谓数字水印技术就是在数字媒体中嵌入一些特定的信息, 以达到确认内容创建者、购买者, 或认证内容是否真实完整的目的。就用途而言, 数字水印一般可分为用于版权保护的鲁棒数字水印和用于防篡改的脆弱数字水印。鲁棒数字水印必须很难去掉, 能抵抗普通数据处理或恶意篡改; 而脆弱数字水印则具有对数字媒体少许的改动就会导致提取的水印与原始水印不同的特性, 利用这一特性可以鉴定数字媒体是否被篡改, 从而辨别真伪。因此, 脆弱数字水印可被用于数字媒体的认证和完整性保护。脆弱数字水印用于认证和完整性保护, 其优点是不需要在原始数字媒体后额外地附加认证信息, 水印可以离散地分布到数字媒体的各个部分, 提高了攻击难度, 增加了安全性。另外, 脆弱数字水印技术还能指出具体的篡改位置和程度, 甚至完成对已篡改数据的恢复, 克服了传统的密码学

收稿日期: 2011-03-03; **修回日期:** 2011-04-14 **基金项目:** 北京市教委科技发展计划面上项目(KM201010015003); 北京市属高校人才强教资助项目(PHR201108349)

作者简介: 郑良斌(1972-), 男, 安徽人, 博士研究生, 主要研究方向为网络信息安全、数字内容版权保护(zlb@bige.edu.cn); 冯柳平, 女, 副教授, 博士; 陈如琪, 男, 副教授; 程晓锦, 男, 副教授。

认证方法的缺点。

不同于数字图像,矢量图形的使用价值主要取决于图形数据的精度而不是视觉质量,因此在矢量图形中嵌入水印必须遵循相应的独特准则。首先,水印嵌入带来的扰动不能超过图形数据所能允许的精度误差范围。矢量图形主要由属性数据和空间坐标数据组成,由于属性数据通常不允许改动,因此数字水印一般嵌入到空间坐标数据中,并且必须保证水印嵌入幅度控制在空间坐标允许的误差范围之内。其次,对水印系统隐蔽性和图形数据质量的评价也必须考虑空间坐标的误差容限,而不能过多地依赖人的视觉感官。再次,矢量图形水印面临的主要攻击方式也不同于普通图像,必须考虑针对矢量图形的特定攻击方式,如坐标变化等。

相对于对图像、视频及音频数字水印技术的受关注,专门针对矢量图形数据的数字水印技术研究相对较少。在现有的矢量图形数字水印技术中,根据嵌入技术的不同主要有以下几种:空间域算法^[1~11],主要思想是在精度允许的范围内,通过改变矢量图形坐标值达到嵌入水印的目的;变换域算法^[12~18],主要是将矢量图形坐标值进行某种变换,通过改变变换后的系数达到嵌入水印的目的;基于图像数字水印算法^[19~21],主要思想是将矢量图形通过一定的数据预处理过程,转换为包含一定矢量图形数据信息的栅格图像,然后利用图像数字水印技术对栅格图像进行水印嵌入,再转换为矢量数据,达到水印嵌入的目的。文献[2~21]都是在讨论用于版权保护的鲁棒数字水印,研究用于矢量图形完整性认证的文献较少。脆弱水印能够验证矢量图形的完整性,验证矢量图形哪些部分被篡改,甚至恢复被篡改的部分,有非常广泛的应用前景。对此,文献[1]提出一种用于防篡改的脆弱数字水印,该算法的主要缺陷在于矢量图形顶点的增加和删除会破坏算法的篡改定位能力。文献[22]基于差值扩大的思想,通过修改矢量地图中相邻顶点坐标值的差值嵌入水印信息,提出了一种应用于矢量地图的无损数据隐藏算法,该算法的缺陷是地图顶点的扰动方向没有考虑原始地图的形状特性,因此在充分放大的地图中,这些扰动使地图具有不自然的外形特征。

1 矢量图形脆弱数字水印算法设计与实现

矢量图形通常由不同的实体组成,本文以具有代表性的由线性实体构成的矢量图形为例进行水印信息的嵌入。将矢量图形中的线状实体分成不同的组;针对每个线状实体组,提取坐标数据可以被修改的位组成数据序列;将提取到的数据序列先进行压缩,再将压缩后的数据序列与原始坐标数据的数字摘要连接成一个新的数据序列;用新的数据序列替换原始数据中提取的数据序列实现水印的嵌入。

1.1 矢量图形分组

设每个线状实体组至少含 m 个坐标点,变量 count 初始值为 0,矢量图形按如下方法分组:

a) 依次统计矢量图形中线状实体坐标点的个数,并将坐标点的个数累加到 count 中,直到 count 中的值大于 m 或统计完矢量图形中的线状实体。

b) 当 count 中的值大于 m 时,将统计的线状实体记为一个分组;当 count 中的值小于 m ,但矢量图形中线状实体已统计

完,则将统计的线状实体作为最后一个分组的一部分,分组操作结束。

c) 将 count 的值置为 0,依次统计矢量图形中剩余的线性实体坐标点的个数,并将坐标点的个数累加到 count 中,直到 count 中的值大于 m 或统计完矢量图形中的线状实体。

d) 重复步骤 b) ~ c)。

矢量图形分组操作的结果为将矢量图形划分成一系列线状实体组,每个线状实体组含有的坐标点数大于等于 m 。

1.2 水印信息的生成

为处理方便,将矢量图形分组中所有的浮点坐标转换成整数坐标,然后转换成二进制序列,记为 $P_n = \{x_i, y_i \mid i = 1, 2, \dots, m\}$ 。其中: n 为组的标号; x_i 和 y_i 分别是组内顶点横、纵坐标转换成的二进制整数, i 是组内顶点的标号; m 是组内顶点的个数。对于每个组进行如下操作:

a) 根据矢量图形的精度容限,提取坐标数据可以被修改的位组成数据序列。本文采用的原始矢量图形是 `shapefile` 格式的河流图,在坐标误差容限允许的范围内,对组中的每个顶点的横、纵坐标,提取其低 4 位数据,按顺序连接成一个二进制序列,记为 $O_n = \{z_k \in \{0, 1\} \mid k = m \times 4 \times 2\}$,其中 m 是组内顶点的个数。

b) 采用无损压缩算法压缩 O_n ,得到缩短的比特序列 S_n 。

c) 采用哈希算法计算原始坐标序列 P_n 的哈希值,得到数据 P_n 的唯一数字摘要,记为 $H_n = \text{hash}(P_n)$ 。

d) 将压缩后的比特序列 S_n 和数字摘要 H_n 连接成一个新的序列 $C_n = S_n + H_n$,然后在 C_n 的末尾补上序列“1000...”,控制“0”的个数,使 C_n 序列与原序列 O_n 具有相同的长度, C_n 序列即为最后生成的水印信息。

哈希算法对任意长度的输入比特流产生固定长度的数字摘要。为了给数字摘要提供足够的存放空间,在一个组内,压缩数据序列 S_n 的长度至少要比原序列 O_n 缩短数字摘要占用的长度。由于矢量图形元素的连续性和光滑性,图形顶点的坐标数据具有一定的相关性,只要组内有足够的坐标点,压缩结果能够满足要求。

1.3 水印信息的嵌入

为了得到篡改定位能力,水印信息的嵌入以组为单位进行。对每个组,用水印信息 C_n 数据序列替换原始数据中所选的数据序列 O_n ,即可得到含水印数据 P_{un} 。此时原始数据 P_n 已经被水印系统保护起来。由于数据序列 O_n 的选择考虑了图形的误差容限,这个数据替换过程不会破坏图形的使用价值。

1.4 水印信息的提取

水印信息的提取过程实际上是矢量图形数据完整性验证过程。对于待检测的矢量图形,先用同样的方法将其划分成一系列分组数据 P'_{un} ,在每个组内分别完成数据的恢复和认证。

a) 原始矢量图形的恢复。提取组中每个顶点横、纵坐标的低 4 位组成数据序列 C'_n ,接着从 C'_n 中分离出数字摘要 H'_n 和压缩序列 S'_n ,并将 S'_n 解压得到数据序列 O'_n 。用解压后的序列 O'_n 替换 P'_{un} 中对应的数据序列 C'_n ,得到恢复的原始矢量图形数据 P'_n 。

b) 数据完整性验证。对于恢复的数据 P'_n ,计算其哈希值 $H''_n = \text{hash}(P'_n)$,并与提取的数据摘要 H'_n 进行比较。由哈希

函数的性质可知,如果 $H''_n = H'_n$,则嵌入水印后的数据没有经过任何篡改,也意味着 $P'_n = P_n$,即原始数据得到了准确无误的恢复;否则,即便是 P'_{un} 经历了很微小的改动,也会导致提取的哈希值不匹配,即 $H''_n \neq H'_n$ 。

2 实验结果

在 Windows XP 平台上用 Visual C++ .NET 实现了本文算法。实验中采用了 MD5 哈希算法计算数字摘要,对任意长度的输入比特流产生固定长度为 128 bit 的数字摘要,用 LZW 编码方法进行数据的无损压缩。实验所用矢量图形是 shapefile 格式的河流图,含有 2 438 个坐标点,每个组至少含 500 个坐标点。图 1 为实验结果,其中,(a) 为原始矢量图形,(b) 为对应的嵌入水印后的矢量图形,两幅图之间的差异被严格控制在误差容限以内。只要含水印图形没有经过任何篡改,那么原始图形数据能够被准确无误地恢复出来。为了检验算法的检测及定位篡改位置的能力,对含水印图形的特定区域进行人为的改动(更改一些坐标点的坐标值、增加一些坐标点、删除一些坐标点),图 1(c) 显示了检测结果,对于没有改动的数据,原始数据仍被准确恢复,对于存在任何改动的数据,算法能够准确地检测出来,并用虚线标志出可能被修改的部分。

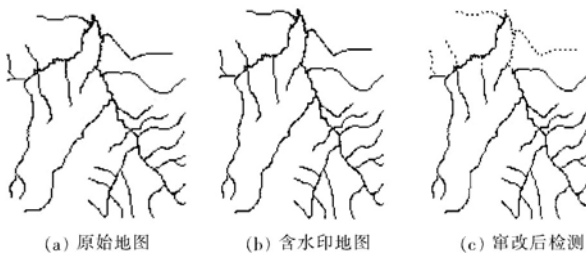


图1 水印嵌入与检测实验结果

3 结束语

数字水印技术是近几年发展起来的新兴研究领域,针对矢量图形数据的数字水印技术研究相对较少。本文针对线状实体组成的矢量图形,提出将矢量图形中的线状实体分成不同的组,以组为计算单位将水印信息嵌入在矢量图形中,不仅能验证矢量图形的完整性,还能将篡改的定位能力精确到相应的分组,有效地克服了传统密码学认证方法的缺点。另外,水印信息的嵌入考虑了图形的误差容限,嵌入了水印信息的矢量图形仍有使用价值,在对数据精度要求极高的情况下,可以通过数据完整性验证提取出原始矢量图形数据,更好地满足了一些特殊应用的需求。

参考文献:

- [1] 邵承永,王孝通. 矢量地图的安全问题与一种可逆数字水印认证方案[C]//全国博士学术论坛论文集. 2005:326-331.
- [2] OHBUCHI R, UEDA H, ENDOH S. Robust watermarking of vector digital maps[C]//Proc of IEEE International Conference on Multimedia and Expo. 2002:577-580.
- [3] SONNET H, ISENBERG T, DITTMANN J, et al. Illustration watermarks for vector graphic[C]//Proc of the 11th Pacific Conference on Computer Graphics and Applications. 2003:73-82.
- [4] VOIGT M, BUSCH C. Watermarking 2D-vector data for geographical information system[C]//Proc of IS&T/SPIE Electron Imaging. 2002:621-628.
- [5] VOIGT M, BUSCH C. Feature-based watermarking of 2D-vector data[C]//Proc of SPIE. 2003:359-366.
- [6] SCHULZ G, VOIGT M. A high capacity watermarking system for digital maps[C]//Proc of ACM Multimedia and Security Workshop. New York:ACM Press, 2004:180-186.
- [7] 闵连权. 矢量地图数据的数字水印技术[J]. 测绘通报, 2007(1):43-46.
- [8] 李媛媛,许录平. 用于矢量地图版权保护的数字水印[J]. 西安电子科技大学学报, 2004, 31(5):719-723.
- [9] 马桃林,顾静,张良培,等. 基于二维矢量数字地图的水印算法研究[J]. 武汉大学学报, 2006, 31(9):792-794.
- [10] 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学报, 2004, 16(10):1377-1381.
- [11] 朱长青,杨成松. 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.
- [12] SOLACHIDIS V, NIKOLAIDIS N, PITAS I. Fourier descriptors watermarking of vector graphics images[C]//Proc of International Conference on Image Processing. 2000:9-12.
- [13] KITAMURA I, KANAI S, KISHINAMI T. Copyright protection of vector map using digital watermarking method based on discrete fourier transform[C]//Proc of IEEE International Geoscience and Remote Sensing. 2001:191-193.
- [14] VOIGT M, YANG B, BUSCH C. Reversible watermarking of 2D-vector data[C]//Proc of ACM Multimedia and Security Workshop. New York:ACM Press, 2004:160-165.
- [15] VOIGT M, YANG B, BUSCH C. High-capacity reversible watermarking for 2D-vector data[C]//Proc of the SPIE. 2005:409-417.
- [16] 钟尚平,高庆狮. 矢量地图水印归一化相关检测的可行性分析与改进[J]. 中国图象图形学报, 2006, 11(3):401-409.
- [17] 杨成松,朱长青. 基于小波变换的矢量地理空间数据数字水印算法[J]. 测绘科学技术学报, 2007, 24(1):37-39.
- [18] 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.
- [19] KITAMURA I, KANAI S, KISHINAMI T. Watermarking vector digital map using wavelet transformation[C]//Proc of Annual Conference of Geographical Information Systems Association. 2000:417-421.
- [20] 闵连权,喻其宏. 基于离散余弦变换的数字地图水印算法[J]. 计算机应用与软件, 2007, 24(1):146-148.
- [21] 梅蓓蓓. 数字地图版权保护[D]. 西安:西安电子科技大学, 2002.
- [22] 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]. 中国图象图形学报, 2007, 12(2):206-211.
- [6] 王会歌,王彩芬,易玮,等. 高效的无证书可公开验证签名方案[J]. 计算机工程, 2009, 35(5):147-149.
- [7] LIU Zhen-hua, HU Yu-pu, ZHANG Xiang-son, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(1):452-464.
- [8] SHACHAM H. New paradigms in signature schemes[D]. Stanford: Stanford University, 2005.

(上接第3802页)

- [4] YU Yong, YANG Bo, SUN Ying, et al. Identity based signcryption scheme without random oracles[J]. Computer Standard & Interfaces, 2009, 31(1):56-62.
- [5] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology, vol 2894. Berlin: Springer-Verlag, 2003:452-473.