第 25 卷 第 1 期
2010 年 2 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol.25 No. 1
Feb. 2010

针对版权保护的图形图像数字水印算法

顾 翀
（天津科技大学包装与印刷工程学院，天津 300222）

摘 要：针对矢量图形数据和栅格图像数据的差异，围绕着数字水印算法的鲁棒性和透明性进行研究，提出了基于坐标漂移的图形数据水印算法和基于 DCT 的图像水印算法，并利用软件实现了数字水印的嵌入和提取. 实验表明，这两种算法不仅满足数字水印透明性的要求，而且对于常规的数据攻击均具有很强的抵抗能力.

关键词：数字水印；矢量；栅格；离散余弦变换；鲁棒性
中图分类号：TS801 **文献标志码**：A **文章编号**：1672-6510(2010)01-0062-04

Digital Watermarking System of Graphic and Image for Copyright Protection

GU Chong
(College of Packaging and Printing Engineering, Tianjin University of Science & Technology, Tianjin 300222, China)

Abstract: The issues about the difference between vector graphic data and raster image data were discussed; and the robustness and invisible ability were researched focus on these two kinds of data. Then a vector watermarking algorithm based on coordinate drifting and a DCT raster image watermarking algorithm were proposed, the ultimate digital watermark embedding and extraction were realized with software. Experiments show that both algorithms are not only transparent but also have strong resistance against the common attracts.

Keywords: digital watermarking; vector; raster; DCT; robustness

数字水印技术作为信息隐藏领域的分支，已日益成为数字作品版权保护的一种有效手段. 其基本思想是利用数字作品中存在的冗余数据和随机性，将版权标识等数字信息作为水印信号，嵌入到图像、文本、视频、音频等数字作品中，从而起到保护产品版权的作用[1].

针对图形数据的水印算法中，比较著名的是由日本山梨大学提出的 MQUAD 水印算法[2]，这种基于四叉树的方法虽然有效但抗剪切能力很不理想，因此很多改进算法被陆续提出[3-4]，虽然抗击剪切的能力增强，但在抵抗缩放攻击上仍有可改进之处. 针对这一问题，本文从图形数据的描述方法出发，提出了坐标点漂移的水印算法，可以完全抵抗平移、缩放等攻击，同时对剪切也具有很强的鲁棒性.

在对印前数字图像的版权保护研究中，大部分算法采用的水印信息多为无意义的序列号[5]或简单的符号[6]，容量有限. 本文提出的基于 DCT 变换域的水印算法将复杂的二值版权图像作为水印信息嵌入到图像中，不仅可以抗击印刷扫描的模数转换，而且提出的水印能作为有效的版权证明.

1 图形与图像水印算法的要求

在印前数字文件中，通常把组成印刷页面的图文信息元素分为图像、图形和文字. 其中，文字可以看做具有语义的图形. 这样，图文信息元素可以分成图像和图形两大类，而它们的描述方法和组成是截然不同的. 在计算机中，图形为矢量数据，用某种数学函

收稿日期：2009-09-01；**修回日期**：2009-11-01
基金项目：天津科技大学科学研究基金资助项目(20070219)
作者简介：顾 翀（1981—），女，天津人，讲师，guchong@tust.edu.cn.

数表示，并通过记录坐标的方式表现各种几何实体，与分辨率无关. 常见的图形文件为数字地图. 图像为栅格数据，它是由像素构成，每个像素都有一个明确的位置和颜色值，并且受到分辨率的限制. 各种数码照片、影像等均属于图像类. 对图像和图形进行版权保护时，由于它们本质上的区别，决定了所采用的数字水印算法是完全不同的.

成功的数字水印算法都需要遵循如下原则：

透明性原则：要求水印嵌入后不会引起矢量数据在不同平台上的可察觉性. 对图像数据而言，其显示质量不应当由于水印信号的嵌入有明显降低；对图形数据而言，则要求不能明显改变形体的外观，甚至保持形体的形状不变[7].

鲁棒性原则：嵌入水印的数字作品在经过某些常规的信号处理后，嵌入到其中的水印仍能够被检测出来.

可证明性原则：水印算法应该能够为版权保护的信息产品的归属提供完全及可靠的证明.

2　矢量数据水印算法的设计与实现

2.1　水印的嵌入

在矢量图形中，几乎所有实体的定义中都包含关于坐标的属性，因此可以通过顶点坐标来嵌入水印. 由于点、线条等对象通常遍布矢量图形，因此嵌入的水印信息在空间上是分散隐藏的，减少了集中嵌入局部位置可能引起的不稳定.

水印的嵌入是通过对原有实体顶点的坐标漂移并增加新属性的方法实现的. 首先寻找原有实体顶点并进行坐标漂移，然后给这些漂移坐标增加一个属性，此属性可以写入水印信息. 实验中，用于测试的原始图形文件采用 DXF 文件格式的数字地图.

在水印的嵌入过程中，首先遍历整个文件结构，找到储存坐标的位置，如 DXF 文件是以组码和组值来存放坐标的. 接着读取 x,y 坐标(由于这里研究的对象是二维的矢量格式，几何实体的 z 坐标数据永远是 0)，在允许的精度范围内对其进行修改，将点的位置进行重置. 然后将重置后的点写入文件结构中，并通过 VC++程序对重置后的点添加水印版权信息. 同时，将漂移点设定为“不可见”，避免视觉上对图形文件产生影响. 水印嵌入过程如图 1 所示.

嵌入水印的信息量是随着图形中含有的矢量实体数的增加而递增的，这一点可以从表 1 中看出. 实体数越多，可嵌入水印信息的位置就越多，水印信息的分散性就越好. 这样，恶意的篡改或攻击对水印的破坏力就越小.

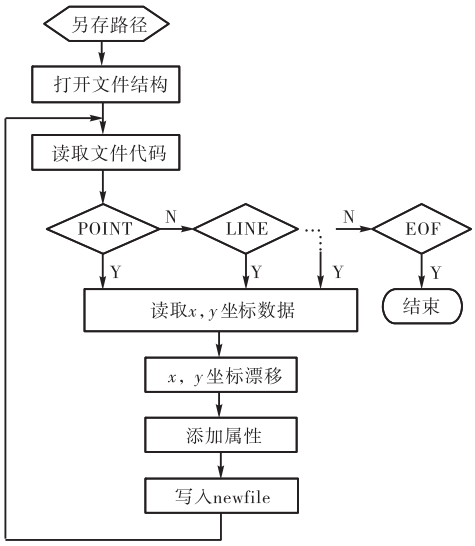

图 1　水印嵌入流程图

Fig.1　Flow of watermark embedding

表 1　水印的嵌入信息量

Tab.1　Information quantity of watermark embedding

实体总数	可嵌入水印的数据量/坐标数	水印容量/bit
372	310	57
682	596	57
1463	1 237	87
2 541	2 074	101
4 095	3 296	240
6 482	5 309	360
8 543	7 018	480
10 605	8 980	540

2.2　水印的检测

水印的检测是在程序打开文件时进行的，这一过程是通过 VC++程序实现. 打开图形文件时，程序会逐行读取图形文件的数据结构，如果发现文件中嵌有本算法特有的水印信息，说明这是已经进行加密的文件，则需要用户输入密码，若密码正确可以显示版权信息；若密码错误则无法打开文件.

水印系统实现流程如图 2 所示.

2.3　算法评价

2.3.1　透明性评价

由于加入的水印标识的坐标偏移点被人为地添加了“不可见”属性，因此，本算法水印信息完全透明，在 AutoCAD、Illustrator、CorelDraw 等常用的图形软件中打开时均不会影响图形的视觉质量.

2.3.2　鲁棒性评价

水印的嵌入是在建立在点坐标基础上的，所以平

移、缩放不会对水印造成任何影响. 鲁棒性评价是分别对嵌入水印后的图形文件进行各种攻击,然后利用编写的 VC++程序进行测试的. 表 2 给出了算法在不同攻击下的误读率,其中剪切实验是将嵌入水印的图形按面积分别剪切至原图的 1/16 ~ 1/2,每种剪切比例采用两种剪切方式,表格中给出的是两种剪切方式下误读率的平均值.

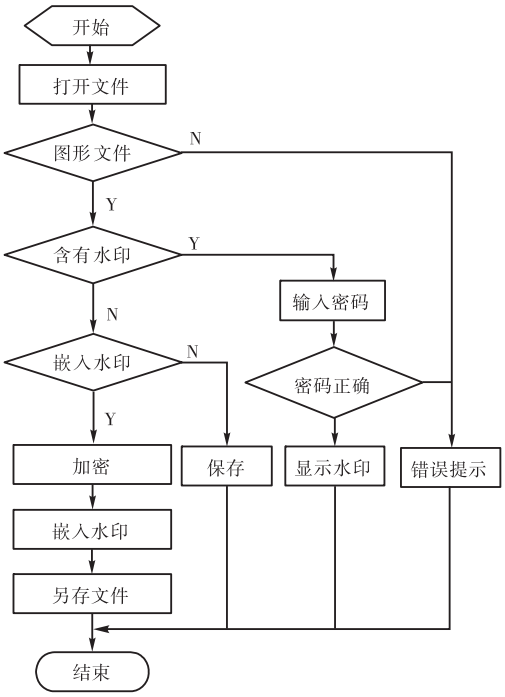

图 2　水印系统实现的流程图

Fig.2　Flow of realization of watermark system

表 2　各种攻击下算法的误读率

Tab.2　False negative rates of various attacks

攻击模式	误读率/%
平移	0
缩放	0
扭曲变形	0
迭加随机噪声 α=50	0.1
迭加随机噪声 α=80	4.9
剪切 1/16	9.1
剪切 1/8	6.4
剪切 1/4	5.7
剪切 1/2	0

从实验结果可以看出,此算法可以抵抗平移、不同比例的缩放、扭曲等攻击. 受随机噪声的攻击时,当 α=50 时,本算法的错误率接近于 0,当 α=80 时,算法的错误率在 5%之内,在剪切模式攻击下,模式准确率也在可以接受的范围内. 可见,如果进行漂移重置的点到达一定数量时,对于剪切也有较强的鲁棒性.

3　栅格数据水印算法的设计与实现

栅格图像将空间分割成有规则的网格,网格中的每个小格是一个像素,线由彼此连接的像素构成. 当像素足够小,它们之间的距离足够短时,人眼便就不能将它们分辨出来. 这样,可以利用人眼视觉的冗余来嵌入水印,或者说将水印嵌入到图像中人眼不易被察觉的位置. 本文所采用的算法是基于变换域算法中的离散余弦变换(DCT)方法.

实验中,原始图像选择了两幅格式为 TIFF 的 480 像素×480 像素灰度图(如图 3(a)和 3(b)),水印图像是天津科技大学校徽的二值图像,格式为 BMP.

(a)原图 1　(b)原图 2　(c)水印

图 3　原始图像和水印

Fig.3　Host image and watermark

3.1　水印的嵌入

根据对人类视觉系统的研究,人眼对低频部分的噪声相对敏感,而高频部分又容易受到攻击而丢失水印信息,影响水印的鲁棒性. 因此应将水印信息嵌入到原始载体图像的中频部分[8]. 具体步骤如下:

(1)原始图像的分块 DCT 变换. 为了与国际压缩标准兼容,以便算法可以在压缩域中实现,将原始图像分割为互不覆盖的 8×8 个子块,再对每个子块进行 DCT 变换.

(2)基于纹理掩蔽特性进行块分类. 计算子块的平均灰度 m 和方差 δ^2:

$$m=\frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}x(i,j)$$

$$\delta^2=\frac{1}{n^2}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}[x(i,j)-m]^2$$

方差值 δ^2 的大小反映了块的平滑程度,水印图像应当被嵌入到方差值较大的纹理复杂区域.

(3)依据系统密钥在 DCT 中频嵌入随机序列,最后通过子块的 DCT 逆变换生成含水印的图像.

3.2　水印的提取

水印提取为加载水印算法的逆运算,过程如下:

(1)将原始图像和待测图像在 DCT 域进行求差运算,比较相关性.

(2) 根据图像块的方差值的大小确定纹理块，从而确定水印的嵌入位置.

(3) 与嵌入时的步骤相似，根据序列以及纹理块复杂度的次序形成一维水印序列.

(4) 将水印序列重新组成二维水印恢复图像，并据此进行图像的版权认证.

3.3 算法评价

3.3.1 透明性评估

对水印的透明性进行评估，一般采用的度量标准是峰值信噪比 *PSNR*，计算公式为

$$PSNR = 10\lg\left[\frac{MNa_{\max}{}^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{n-1}[f(i,j)-g(i,j)]^2}\right]$$

通过计算，原始图像 1、原始图像 2 与水印图像之间的 *PSNR* 值分别为 44.603 2 和 44.687 2，该算法具有较好的不可见性.

3.3.2 鲁棒性评估

水印系统的鲁棒性评估是以水印图像在经历各种攻击后是否能够检测出水印为依据. 本次实验选择了几种常见的攻击，如剪切、污损、涂改、格式修改等，然后对水印进行提取操作，并通过相似度来判断提取的水印与嵌入的原始水印进行比较得到的相似程度. 相似度的计算可以通过调用 coor2 函数完成. 通常认为当相似度 $s \geqslant 0.7 \sim 0.8$ 时，可以认定成功地检测出了水印信息. 对图 3 中的原始图像和水印，采用不同的攻击方法攻击嵌入水印的图像后，求其相似度，结果见表 3.

表 3　不同攻击时的相似度

Tab.3　Similarity of various attacks

攻击与篡改	原图 1 水印	原图 2 水印
未篡改	0.927 5	0.912 8
7%的涂改	0.848 7	0.848 7
12%的剪切	0.820 6	0.836 2
9%的污损	0.809 6	0.795 7
格式修改	0.902 1	0.890 6
印刷扫描后	0.801 7	0.799 4

根据表 3，未篡改水印图像时提取的水印信息与原始水印相似度分别为 0.927 5 和 0.912 8，提取的水印图像与原始水印非常接近. 误差产生的原因是，在水印的嵌入过程中产生 3 600 个随机位置时，这些位置可能出现重复，导致水印像素的嵌入产生覆盖现象，造成误差.

对图像 1 提取的水印受到攻击时的相似度均超过了 0.8，水印图像 2 虽然在污损和抗击印刷扫描方面稍差，但相似度也接近 0.8，这说明从提取的水印信息中可以识别出版权归属.

4 结　语

本文通过对图形和图像的数据形式分析，从数据本身特性出发挖掘出其可修改属性，并结合特殊要求设计相应的水印方法，找到了两种数据的视觉冗余位置或信息，提出了针对图形和图像的两套截然不同的水印算法，并用实验和分析验证了两种算法的可行性，为进一步的研究奠定了基础.

参考文献：

[1] Ingemar J Cox，Matthew L Miller，Jeffrey A Bloom. 数字水印[M]. 王颖，黄志蓓，译. 北京：电子工业出版社，2003.

[2] Ohbuchi R，Ueda H，Endoh S. Robust watermarking of vector digital maps[C]//Proceedings of IEEE Conference on Multimedia and Expo 2002(ICME). Piscataway：IEEE，2002：577–580.

[3] 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：自然科学版，2004(5)：719–723.

[4] 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(10)：1377–1381.

[5] 周季峰，庞明勇，李黎，等. 一种印刷品数字水印防伪方法[J]. 计算机工程与应用，2007(5)：189–192.

[6] 张丽强. 印刷图像数字水印技术研究[D]. 长沙：国防科学技术大学，2005.

[7] 向辉. 图形数据数字水印技术[J]. 系统仿真学报，2002(12)：1649–1651.

[8] Samuel S，Penzhorn W T. Digital watermarking for copyright protection[C]//Proceedings of 7th AFRICON Conference in Africa. Piscataway：IEEE，2004：953–957.