第27卷 第8期 计算机工程与设计 2006年4月
Vol.27 No.8 Computer Engineering and Design Apr. 2006

基于汉语拼音的鲁棒性文本水印算法

鲁 芳， 孙星明
(湖南大学 计算机与通信学院，湖南 长沙 410082)

摘 要：针对文本水印算法存在的信息量少和鲁棒性不强的特点，提出了一种新的文本水印嵌入方法。该方法提取出整个文档的汉字拼音，利用拼音的特点将文档进行分层，在各个层中通过字符水平缩放来嵌入水印。在嵌入过程中提出了一种安全的嵌入方法，将有意义的水印信息放在文本之外。实验结果表明该算法的有效载荷以及鲁棒性都得以提高。

关键词：字符缩放； 鲁棒性； 零水印； JND； 有效载荷
中图法分类号：TP391 **文献标识码**：A **文章编号**：1000-7024 (2006) 08-1330-03

Robust text watermarking algorithm based on Chinese pinyin

LU Fang, SUN Xing-ming
(School of Computer and Communication, Hunan University, Changsha 410082, China)

Abstract: A new embedding method of text watermarking is presented to solve some algorithmic deficiency, like insufficient information and bad robustness. Chinese pinyin on the whole document is distilled in order to group the document by characteristics of pinyin, the watermark is inserted by characters' extending in every group. During inserting, a secure inserting method is presented, which puts the real watermark out of the document. The result shows that effective load and robustness are improved.

Key words: characters' extending; robustness; zero watermarking; JND; effective load

0 引 言

数字水印技术是指在数字化的数字内容中嵌入不明显的记号。被嵌入的记号通常是不可见或不可察觉的，但是通过一些计算操作可以被检测或被提取。水印与原数据（如图像、文本、音频和视频数据）紧密结合并隐藏在其中，成为不可分离的一部分[1]。尽管数字水印可以应用于包括文本、声音、静止图像以及视频在内的多媒体数据中，但是目前大多数相关的研究和文献都是与静止图像、视频的保护有关的。对文本水印的研究较少，主要原因是文本没有像图像那样多的冗余信息。Brassil 和 Maxemchuk 等人提出了在 Postscript 格式中嵌入水印的 3 种方案：行间距编码、字间距编码和特征编码[2,3]。行间距编码是通过将文本的某一整行垂直移动，有很强的鲁棒性，不足是嵌入的信息量少；字间距是将文本中的某一单词进行水平移位，它没有实现盲检测，而且不适合中文；特征编码是通过改变某个单词的某一特征来插入标记的技术，例如改变 h 的垂直线的高度，但是如果有一个与它相同的但未做变化的字母与它相邻，则读者较易认出字母的变化[4]。文献[6]提出将文本当作二值图像来嵌入水印，但是文档位图化后的灰度级很少，也很难适用于一般的水印算法。Purdue 大学的 Atallah 教授提出一种鲁棒性很好的文本水印算法——基于计算机自然语言处理技术的文本数字水印技术[5]，但是目前计算机对于自然语言的理解仍然是一个研究中的课题，分词、句法分析、改写技术和词义消歧等自然语言处理技术还不成熟，而且使用这种技术嵌入水印后的载体文本容易发生语义改变的情况，且中文的表达比英文丰富很多，稍微进行一下语义或句法的修改会让人难以理解或者让人感觉很别扭，所以这种方法对于中文来说不太适合。

Cox 提出水印的几个主要特性：嵌入有效性，保真度，数据有效载荷，鲁棒性，盲检测或含辅助信息检测。其中以数据的有效载荷和鲁棒性为研究的重点。本文针对文本水印算法存在的有效载荷小、鲁棒性不强的特点，提出一种新的文本水印算法。文章的第 1 章对数字水印的通用算法进行了描述；第 2 章详述了基于汉语拼音的鲁棒性水印算法，包括嵌入算法和检测算法两个部分；第 3 章给出了算法的实验结果及其对算法的性能进行了分析。

1 数字水印通用算法的框架

通用水印算法框架（GWF）可用六元组(X,W,K,G,ξ,D)表示，其中：

收稿日期：2005-01-17。
基金项目：国家自然科学基金项目 (60373062)；湖南省自然科学基金项目 (04JJ3052)；教育部科研重点基金项目 (03092)；湖南省杰出中青年基金项目 (02JJYB012)。
作者简介：鲁芳 (1979－)，湖南浏阳人，硕士研究生，研究方向为文本数字水印； 孙星明 (1963－)，湖南益阳人，博士，教授，博士生导师，研究方向为网络信息安全和自然语言处理。

(1)X表示要被保护的数字产品的集合；

(2)W是水印信号的集合；

(3)K是水印密钥空间；

(4)G是水印生成算法：$G: X\times K\rightarrow W$ $W=G(X,K)$；

(5)ξ是在数字产品X_0中加入水印的水印嵌入算法

$$\xi: X\times W\times K\rightarrow X'$$

$$X'=\xi(X_0,W)$$

(6)D是水印检测算法

$$D(X'\times K)\rightarrow\{0,1\}\text{或者}D(X',W,K)=\begin{cases}1 & \text{相似度>=阈值 } T\\ 0 & \text{其它}\end{cases}$$

整个数字水印系统由水印信息的生成、水印信息的嵌入、水印信息检测等几个算法模块组成。首先引入密钥K，利用水印信息的生成算法G构造水印信息；通过嵌入算法ξ将水印信息嵌入到数字产品中；最后通过水印信息的检测算法D提取水印信息检验是否与原始水印信息相符，来判断数字产品中是否存在有数字水印，以达到产权保护的目的。

2 基于汉语拼音的文本水印算法

2.1 算法的几个基本思想

在文本中嵌入水印的前提是最好不要修改文本的任何内容，因此最好对文本的行、字和词在页面上做不易被识别地轻微改变，本文提出的是将字符进行水平缩放来嵌入水印，在嵌入时将零水印思想与传统的文本水印思想结合起来，将有意义的水印信息嵌在文本之外。

在提取汉语拼音时，是基于国标码 GB2312-80 的，GB 2312-80 编码中的汉字按其使用频率、组词能力以及用途大小分成一级汉字和二级汉字。一级汉字按拼音字母顺序排列，如遇同音字，则按起笔的笔形顺序排列。这样可利用 GB2312-80 一级汉字的特点来提取出整个文档这中一级汉字的汉语拼音。

为了增强算法的鲁棒性，统计汉语拼音首字母出现的频率，将文档分成几层 group[0],group[1],……在各个层中冗余嵌入水印。提取水印时首先分别提取各个层中的水印，然后对各个层中的水印进行相互校验，从而得到最终提取的水印。

2.2 嵌入算法

传统的文本水印算法都是将有意义的水印信息或者一串伪随机序列通过加密嵌入到文档里，这样攻击者可以分析文档的字面信息，解密后就可以得到所嵌入的水印。为此有人提出一种新的嵌入方法——零水印：不将水印信息嵌入到宿主信息里。零水印一般是指提取出图像的特征来构造一个水印，将这些图像特征进行一定处理后进行保存和管理，它不修改宿主信息，解决了鲁棒性和不可见性的矛盾[7]。由于它不嵌到宿主信息里去，那么任何人都可以根据图像特征来构造零水印，这不利于零水印来证明版权。因此我们将零水印的思想与传统数字水印的思想相结合，将实际的水印信息不嵌到文本里面去。嵌入算法描述如下：

s1: 将有意义的水印W转换成二进制序列$\{s_i\}$ (i=1,2,…,n)；

s2: 利用两个密钥($K1$, $K2$)确定相同长度的x_i序列和y_i序列；

$$\text{s3: }\{d_i\}=\begin{cases}1 & x_i>y_i\\ 0 & x_i<=y_i\end{cases}$$

$$\text{s4: }\{u_i\}=\{s_i\}\oplus\{d_i\}$$

s5: $\{w_j\}=\text{MD5}(\{u_i\})$, j=1,2,…, m(m<=文本长度L，也即文本长度得要大于 128)；

s6: 提取出整个文档的汉字拼音，按照拼音首字母出现的频率从大到小进行统计 arr[1],arr[2],…,arr[26]，如果 arr[1]>=m，则 group[0]为 arr[1]对应的拼音首字母，否则 group[0]为 arr[1]和 arr[2]对应的拼音首字母，直到 group[0]> = m。其余的分组依次类推；

s7: 对整个文档X通过字符缩放在各个层（本实验的层数是 3 层）中嵌入水印$\{w_j\}$；

Insert()：

$$w_j=\begin{cases}1 & \text{水平拉伸}\lambda\text{倍(实践证明，当}\lambda<=1.05\text{ 时都低于临界差异 JND(just noticeable difference)的值)}\\ 0 & \text{字符保持不变}\end{cases}$$

分层嵌入水印的方法如下

```
for i:=1 to L(文本长度) do
//汉字拼音首字母在group[0]中从头到尾进行水印的嵌入
if THzSpellPyHeadOfHz(word(i)) in group[0]
Insert (wj)
//汉字拼音首字母在group[2]中从尾到头进行水印的嵌入
if THzPyHeadOfHz(word(L－i+1)) in group[2]
Insert(wj)
//汉字拼音首字母在group[1]中从中间向两端进行水印的嵌入
if THzPyHeadOfHz(word(L/2± i)) in group[1]
Insert(wj)
```

其中：THzSpellPyHeadOfHz()为提取汉字的拼音首字母的函数。

这种嵌入方法的优点是：①因为MD5后的水印长度固定，因此很适合长水印嵌入到短文本中，解决了水印信息量与隐蔽性之间的矛盾；②满足 Kerchhoff 原则，算法可公开，依赖密钥（$K1$,$K2$）来保证安全性。这是因为即使第 3 方可通过分析字面特征得到所嵌入的水印，它得到的是$\{w_j\}$，无论如何解密也不可能得到真正的水印信息W，因为真正的水印信息没有嵌到文本里面去；③将文档进行分层处理的话，这样一旦有攻击现象的话，不同层之间的水印可进行相互校验，从而得到提取的水印。

2.3 检测算法

(1) 前 6 步与嵌入算法相同；

(2) 在各个层中提取出水印，对提取出的各个层的水印进行相互校验，得到最终提取出的水印信息 Watermark；

(3) 检测出的水印信息与第 5 步（即嵌入算法的s5）的$\{w_j\}$进行相似度比较

$$D(X',W,K)=\begin{cases}1 & \text{compare}(\{w_j'\},\{w_j\})>=\text{阈值 } T\\ 0 & \text{其它情况}\end{cases}$$

compare()函数是比较提取出的水印信息$\{w_j'\}$与原始嵌入的水印信息$\{w_j\}$做相似度比较，如果compare()大于阈值T的话表示存在这个有意义的水印 W。实验中阈值T的值为 45 %。

3 实验结果及性能分析

本实验对一篇 word 文档嵌入水印信息“湖南大学计算机与通信学院”，嵌入前后的部分 word 文档如图 1、图 2 所示。

对两篇已嵌入水印的文档进行攻击后的检测情况：

目前很多文本水印算法在嵌入有效性，保真度，以及直接测上达到了理想的效果，但是在数据有效载荷和鲁棒性上存在较多的问题，还没有一个比较理想的算法。对鲁棒性的研究主要是针对嵌入水印的方法，一旦攻击者知道了你所用的嵌入方法，那么这种方法的鲁棒性也就随即消失。Kerchhoff 原则即体制的安全性不依赖于算法的保密，只依赖于密钥的保密，对于数字水印算法也是同样适用的。尽管加密可以在一定程度上解决一定的问题，但是加密后数据的少量损坏就有可能导致解密后数据的大量破损。所以抗攻击的水印算法还是数字水印的一个薄弱环节。

图 1　原始文档

目前很多文本水印算法在嵌入有效性，保真度，以及直接测上达到了理想的效果，但是在数据有效载荷和鲁棒性上存在较多的问题，还没有一个比较理想的算法。对鲁棒性的研究主要是针对嵌入水印的方法，一旦攻击者知道了你所用的嵌入方法，那么这种方法的鲁棒性也就随即消失。Kerchhoff 原则即体制的安全性不依赖于算法的保密，只依赖于密钥的保密，对于数字水印算法也是同样适用的。尽管加密可以在一定程度上解决一定的问题，但是加密后数据的少量损坏就有可能导致解密后数据的大量破损。所以抗攻击的水印算法还是数字水印的一个薄弱环节。

图 2　嵌入水印后的文档

水印信息：湖南大学计算机与通信学院；

攻击方法：随机攻击。

性能分析：①本算法可对每个字符嵌入一个水印信息，比 Brassil 提出的几种方法的有效载荷量都得以提高；②在 Brassil 提出的几种方法中，行间距算法的鲁棒性最好，但是行间距算法只要随机删除几行就很难检测到原来的水印信息了。此实验采用的算法在检测水印时，删除已嵌水印文档的几行或者增加几行，都没有破坏嵌入的水印。多次的实验表明，当破坏率达到文档的 43 %以上时，相似度值才低于阈值 T，如图 3 所示。这是因为：(a)水印进行了各层的冗余嵌入，而且嵌入方向不同，因此不同层之间的水印可进行相互的校验，从而保证了较好的鲁棒性；(b)本算法是基于整个文档的汉语拼音的统计规律进行水印的嵌入，要损坏这些水印信息，除非攻击者破坏了每一层汉语拼音的统计规律，而这需要较大的破坏量。

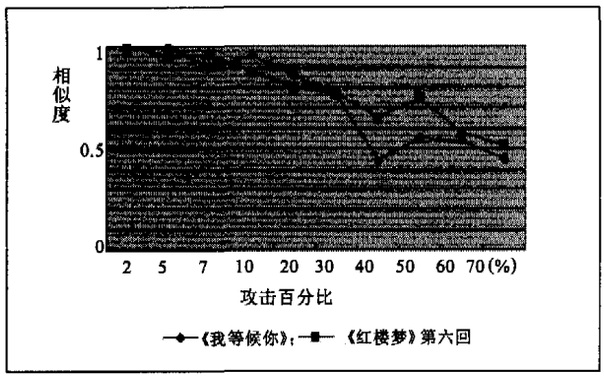

图 3　可靠性

4　结束语

本文提出的算法较好地解决了以往水印算法中数据有效载荷和鲁棒性之间的矛盾，经过大量的实验表明，该算法有较强的鲁棒性。不过如果重新录入整个文档，本算法仍是脆弱的。

参考文献：

[1] Ingemar J Cox, Matthew L Miller, Jeffrey A Bloom. Digital watermarking[M]. 北京:电子工业出版社, 2003.17-25.

[2] Brassil J T, Low S, Maxemchuk N F. Copyright protection for the electronic distribution of text documents[J]. *Proceedings of the IEEE*, 1999,87(7):1181-1196.

[3] Brassil J, Low S, Maxemchuk N F, et al. Electronic marking and identification techniques to discourage document copying [J]. *IEEE Journal on Sel Areas in Commun*,1995, 13(8):1495-1504.

[4] Low S H, Maxemchunk N F. Performance comparison of two text marking methods [J]. *IEEE Journal on Selected Areas in Communications*, 1998,16(4):561-572.

[5] Atallah M J, Raskin V. Natural language watermarking and tamper proofing [EB/OL]. 2004-4-20.*www.cerias.purdue.edu/homes/wmnlt/semdemo.html*.

[6] 张小华,刘芳,焦李成. 一种有效的文档水印技术[J]. 通信学报, 2003,24(5):21-28.

[7] 杨树国,李春霞,孙枫,等. 小波域内图像零水印技术的研究[J]. 中国图像图形学报, 2003, 8(6):554-669.

[8] 袁占亭,张秋余,陈宁.数字水印的鲁棒性分析与研究[J].计算机工程与设计, 2005,26(3):617-618.

(上接第 1329 页)

of Knowledge Discovery and Data Mining[C]. 1998-8.16-22.

[3] Huhtala Y, Kärkkäinen J, Toivoen H. Mining for similarities in aligned time series using wavelets[C]. *Orlando, Florida: Data Mining and Knowledge Discovery: Theory, Tools, and Technology*, 1999.150-160.

[4] Fu T C, Chung F L, Luk R, et al. Pattern discovery from stock time series using self-organizing maps[C]. *San Francisco: Workshop Notes of KDD2001 Workshop on Temporal Data Mining*, 2001.27-37.

[5] Keogh E, Lonardi S, Chiu B. Finding surprising patterns in a time series database in linear time and space[C].*Edmonton, Canada: SIGKDD*, 2002.550-556.

[6] Mannila H, Toivonen H, Verkamo A I. Efficient algorithms for discovery associateion rules [C]. *Seattle: AAAI*'94 *Workshop Knowledge Discovery in Database(KDD* 94), 1994.181-192.

[7] Mannila H, Toivonen H, Verkamo A I. Discovering frequent episodes in sequences [C]. *Montreal, Canada: Proc of KDD*, 1995-8.210-215.

[8] Agrawal R, Imielinski T, Swami A. Mining association rules sets of items in large databases[C].*Washington DC:Proceedings of the ACM SIGMOD International Conference on Management of Data*, 1993.207-216.

[9] 曾海泉,刘永丹,宋扬,等. 基于互关联后继树的多时间序列关联模式挖掘[J].计算机研究与发展, 2003,40(7):934-940.

[10] 曾海泉,宋扬,申展,等. 基于互关联后继树的时间序列相似性查询[J].计算机研究与发展, 2004,41(2):325-332.

[11] 胡运发. 互关联后继树——一种新型全文数据库数学模型[R]. 上海:复旦大学计算机与信息技术系 CIT-02-3, 2002.