第 32 卷 第 15 期 计 算 机 工 程 2006 年 8 月
Vol.32 № 15 Computer Engineering August 2006
·安全技术· 文章编号：1000—3428(2006)15—0146—03 文献标识码：A 中图分类号：TP309

英文文本多重数字水印算法设计与实现

袁树雄[1]，孙星明[2]
(1. 湖南大学软件学院，长沙 410082；2. 湖南大学计算机与通信学院，长沙 410082)

摘 要：针对现有英文文本数字水印方法存在的不足，提出并实现了一种基于字符属性及单词内容的多重文本数字水印算法。该方法可以实现较大的水印容量且水印的隐蔽性好，同时针对攻击者对文本内容或水印的破坏，该算法具有较好的检测和纠错提取性能。攻击实验数据证明水印的鲁棒性较强。

关键词：文本数字水印；水印容量；完整性

Design and Implementation of a Multiple Watermarking Algorithm for English Texts

YUAN Shuxiong[1], SUN Xingming[2]
(1. College of Software, Hunan University, Changsha 410082; 2. College of Computer and Communication, Hunan University, Changsha 410082)

【Abstract】 For the deficiency of current digital watermarking methods for English texts, the paper proposes a multiple text watermarking method which is based on the characters' attribute and the words' content. This method can make a huge contain of the watermarking, on the other hand, the watermarking can be hided effectively. Moreover, it has a strong ability of testing and correcting the watermarking after the demolishing made to the text content or the watermarking by attackers. Attacking experiments have shown that the watermarking has a good ability of robustness.

【Key words】 Text digital watermarking; Contain of watermarking; Integrality

1 概述

数字水印(digital watermarking)技术作为信息安全的一个较新的研究领域，是指嵌入到多媒体数据中的信息，可以是数字、序列号、文字、图像标志等各类信息，以起到版权保护、标志产品、秘密通信、证实数据归属权、鉴别数据真伪等作用[1]。数字水印可以应用于包括文本、声音、软件、数据库、静止图像以及视频在内的多媒体数据中[1～5]，但目前更多的相关研究和文献都是与静止图像的保护有关，对文本水印的研究相对较少，主要原因是文本没有像图像那样多的冗余信息。

讨论文本水印算法时，常将文本分为 2 类：非格式化文本，如 ASCII 文本文件和计算机源码文件；格式化文本，如 WORD、PDF、PostScript、RTF 等这些高级形式的文档。

对于非格式化文本常采用在行末加空格来加载秘密信息，这种方法稳健性较差。故对文本水印主要集中于格式化文本水印的研究。Brassil和Maxemchuk等提出了在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[6,7]。行间距编码是通过将文本的某一整行垂直移动，有较强的鲁棒性，但嵌入的信息量少；字间距是将文本中的单词进行水平移位，它需要原始文本，没有实现盲检测；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作变化的字母与它相邻，则读者较易认出字母的变化。国外还提出了几种能同时运用到格式化文本和非格式化文本的水印算法。例如对文本中特定的单词进行同义词替换的方法，但是能够完全等价的同义词很少。Purdue大学的Atallah教授提出一种基于计算机自然语言处理技术的文本水印技术[8]。但是目前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文本容易发生语义改变和难以理解的情况。

对于格式化英文文本，如 WORD、PDF、PostScript、RTF 等文档，考虑到 WORD 文档应用最为广泛，本文旨在提出和实现一种在英文 WORD 文档中多重嵌入数字水印，实现水印检测、恢复和提取的算法，并使之达到比较好的隐蔽性、鲁棒性和稳健性。

2 英文文本多重水印算法

2.1 水印嵌入模型

水印嵌入模型如图 1 所示。

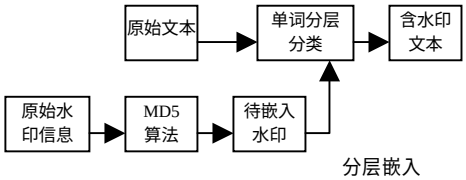

图 1 水印嵌入模型

2.2 水印的生成

为增强水印的鲁棒性，基于英文 WORD 文档的特点我们提出多重水印的嵌入方法。然而水印的多重嵌入增大了文本的水印容量之要求，当嵌入的水印信息量稍大时，将对文本长度有更高的要求。基于降低文本长度限制和原始水印信息

基金项目：国家自然科学基金资助项目(60373062，60573045)；高校博士点基金资助项目(20050532007)
作者简介：袁树雄(1968—)，男，硕士生，主研方向：信息安全，数字水印；孙星明，博士、教授、博导
收稿日期：2006-01-23 **E-mail：**ssxxyy0301@yahoo.com.cn

量尽量不受限制的考虑，选择一种安全可靠的 HASH 函数(MD5 算法)求得原始水印信息的摘要(长度为 128 位)作为最终加载的水印数据，一方面对原始水印起到了加密的效果，另一方面原始水印信息的长度可以不受限制。相应地以待加载的水印数据与原始水印信息为表的记录建立数据库表，用于提取水印后获取原始水印信息。

2.3 多重水印的嵌入方式

(1)基于 WORD 中的 range 对象(如字符等)的 NoProofing 属性默认值保持不变而编程方可修改此值的特点，对单词的第 2 字符或第 3 字符利用其 NoProofing 属性嵌入水印数据。此方法不通过编程不能发现、添加和修改水印特征，WORD 文件的菜单操作也不能清除此水印特征，具备较强的隐蔽性和抗攻击性。

(2)利用单词中字符的东亚语言类别即 LanguageIDFarEast 属性(需要时可将 LanguageIDFarEast 的默认值改为 wdTraditionalChinese 或 wdChineseSingapore 等，此属性具有隐蔽性强的特点)嵌入水印数据。

(3)基于文档中字符颜色适当修改后人的视觉对此难于觉察和辨别的特点，修改单词中字符的颜色(Color 属性)为 wdColorGray95 或 wdColorGray90，以嵌入水印数据。

2.4 水印嵌入的实现

2.4.1 嵌入的基本思想

按照英文 WORD 文本的单词(2 字符及以上)内容将单词划分为 3 种，从而全文 2 字符以上的单词构成 3 个集合，每个集合中的单词就构成了一个层。分层后的文本成为一个多层的稳定的立体，每层按一种水印嵌入方式嵌入 2 组(次)水印，用于文本遭到各种攻击与破坏时提取出完整水印以及水印的相互校验和纠错等水印恢复的实现。水印嵌入时以文本中的单词为对象，将每层的所有单词划分为 2 类，对单词嵌入水印位的时候根据其类别的不同以不同方法嵌入，使水印的嵌入与单词内容相关，以利于水印检测时能够发现某些情况下攻击者有意或无意地保留水印而对文本内容进行刻意篡改(如单词中字符的逐个替换，此时因 WORD 本身的继承性，替换后字符的属性即水印特征不变)或者直接修改水印特征的行为，从而较大程度上增强了文本完整性检测的性能；而同一层的第 1 组和第 2 组水印嵌入的规则又相区别，以利于文本受到删除等破坏时提取水印时分离 2 个组的水印信息。

2.4.2 文本的分层和单词分类

(1)将全文所有 2 字符及以上的单词按如下算法予以分层(分 3 层)：每个单词根据其中字母的 ASCII 码作如下运算：w_ceng = Int(asc_all / N + 0.85) Mod 3，其中 asc_all 为此单词所有字符 ASCII 码的和，N 是此单词字符个数。分层或分类依据是使各层或各类单词数比较均衡。

规则 1 分层依据

此单词属于第 1/2/3 层：如果 w_ceng=0/1/2。

(2)将每层所有单词分为 2 类，先计算 asc_ave =Int(asc_all/ N)。

规则 2 分类依据

此单词属于第 1 类：如果 asc_ave > 105 And asc_ave < 112；

此单词属于第 2 类：如果 asc_ave≤105 Or asc_ave≥112。

2.4.3 水印嵌入规则

令最终加载的水印码序列W=$w_1w_2…w_n$。

规则 3 第 1 层单词的水印嵌入规则

(1)单词字符数有 3 个或以上

1)对第 1 组中的单词如属于第 1 类或对第 2 组的单词如属于第 2 类：

- 单词的第 2 和第 3 字符嵌入 10：如果w_i=1；
- 单词的第 2 和第 3 字符嵌入 01：如果w_i=0。

2)对第 1 组的单词如属于第 2 类或对第 2 组的单词如属于第 1 类：

- 单词的第 2 字符嵌入 1’：如果 wi=1；
- 单词的第 2 字符和第 3 字符嵌入 11：如果 wi=0。

(2)第 1 组或第 2 组的单词字符数为 2 时

- 单词的第 2 字符嵌入 1’：如果 wi=1；
- 单词的第 2 字符嵌入 1：如果 wi=0。

注：如第 2 和第 3 字符嵌入 10：代表第 2 字符的 NoProofing=True，第 3 字符的 NoProofing 值保持默认值(false)不变。第 2 字符嵌入 1’：代表此字符的 LanguageIDFarEast = wdChineseSingapore 。

规则 4 第 2 层单词的水印嵌入规则

(1)第 1 组(或第 2 组)的单词属于第 1 类：

- 单词的第 1 字符嵌入 1(或 1p)：如果 wi=1；
- 单词的第 1 字符嵌入 1’(或 1p’)：如果 wi=0。

第 1 组(或第 2 组)的单词属于第 2 类

- 单词的第 2 字符嵌入 1(或 1p)：如果 wi=1；
- 单词的第 2 字符嵌入 1’ (或 1p’)：如果 wi=0。

注：如第 1 字符或第 2 字符嵌入 1/1’：代表此字符的 LanguageIDFarEast = wdTraditionalChinese/wdChineseSingapore ; 嵌入 1p/1p’：代表此字符的 LanguageIDFarEast = wdChineseHongKong / wdChineseMacao

规则 5 第 3 层单词的水印嵌入规则

(1)单词字符数有 3 个或以上

1)对第 1 组的单词如属于第 1 类或对第 2 组的单词如属于第 2 类：

- 单词的第 2 字符和第 3 字符嵌入 10：如果 wi=1；
- 单词的第 2 字符和第 3 字符嵌入 01：如果 wi=0。

2)对第 1 组的单词如属于第 2 类或对第 2 组的单词如属于第 1 类：

- 单词的第 2 字符和第 3 字符嵌入 00：如果 wi=1；
- 单词的第 2 字符和第 3 字符嵌入 11：如果 wi=0。

(2) 第 1 组或第 2 组的单词字符数为 2

- 单词的第 2 字符嵌入 0：如果 wi=1；
- 单词的第 2 字符嵌入 1：如果 wi=0。

注：如第 2 字符和第 3 字符嵌入 10：代表第 2 字符的 Color = wdColorGray95，第 3 字符的 Color = wdColorGray90。

规则 6 第 1 层或第 2 层的第 1 组水印结束单词后(第 2 组开始单词之前)的连续 4 个词嵌入几个水印标志，以方便区分第 1 组或第 2 组水印结束或开始，而层中第 2 组水印之后 2 个单词嵌入结束标志；类似地，第 3 层的中间 3 个单词嵌入几个水印标志，以方便区分第 1 组或第 2 组水印，而第 1 组或第 2 组水印之后 2 个单词嵌入结束标志。

2.4.4 水印嵌入算法

Step 1 输入原始水印内容和待处理文本；

Step 2 用 MD5 算法求得原始水印数据的摘要作为最终加载的水印数据；

Step 3 将全文所有 2 字符及以上的单词按规则 1 分层，将每层所有单词按规则 2 分类；

Step 4 对第 1 层单词按照从前往后的顺序依规则 3 嵌入 2 组水印；

Step 5 对第 2 层单词按照从后往前的顺序依规则 4 嵌入 2 组水印；

Step 6 对第 3 层单词按照从中间往两边的顺序依规则 5 嵌入 2 组水印。

2.5 水印的检测、纠错和提取

(1)水印的检测

1)水印检测模型

水印检测模型如图 2 所示。

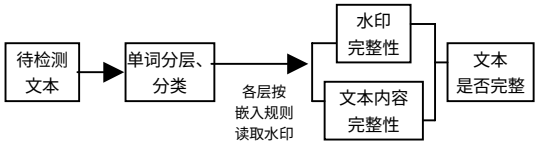

图 2 水印检测模型

2) 执行步骤

Step 1 将待检测文本的所有 2 字符及以上的单词按规则 1 分层，将每层所有单词按规则 2 分类。

Step 2 对各层的单词按顺序并按嵌入规则读取水印数据，并保存各单词的状态(分为已读取正常水印值 1/0、无水印、水印值与单词内容矛盾等几种状态值)，从而得到 6 组水印。

Step 3 当 6 组水印一致并匹配数据库一条记录，同时没有水印与单词内容矛盾的情况而水印组中也没有多余单词(无水印的单词)时，表明所有水印完全正常，文件无被破坏迹象，即文本的完整性没有遭到破坏，水印提取完全正常、程序结束。否则，转(2)。

(2)水印的纠错与提取

1)水印的纠错与提取模型(图 3)

水印的纠错与提取模型如图 3 所示。

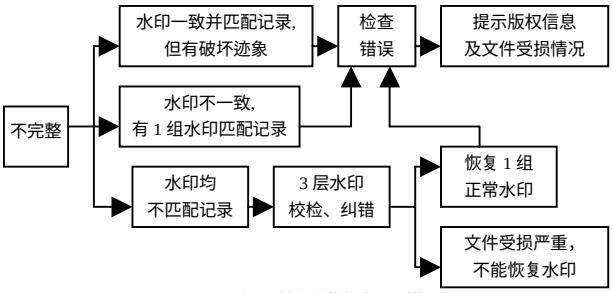

图 3 水印的纠错与提取模型

2)执行步骤

Step 1 当 6 组水印一致并匹配数据库一条记录时，如发生水印与单词内容矛盾的情况或水印组中有多余的无水印单词(内容增加)，提示提取的版权信息及文件完整性受损情况。否则，转 Step 2。

Step 2 6 组水印不一致但至少 1 组水印匹配数据库一条记录时，提示提取的版权信息并根据发现的错误类型提示文件完整性受损情况。否则，转 Step 3。

Step 3 6 组水印均不匹配数据库记录，遭到不同程度破坏，针对文本内容添加删除或水印删除攻击，利用 6 组水印相互补充、校检和纠错，恢复 1 组完整水印，提示提取的版权信息及文件完整性受损情况。否则，转 Step 4。

Step 4 文件破坏程度大，提示文件受损严重，不能恢复水印。

3 水印实验与性能分析

3.1 水印嵌入实验

对一英文 WORD 文本进行水印嵌入实验，嵌入水印前后的部分文本如图 4、图 5 所示。

> How can a trial and the final outcome that is so important to the success of this fledgling democracy i IRAQ continue to be delayed and stalled? I believe it harms our efforts by instilling fear in those who have been repressed and it emboldens those who seek to regain power. Finally, how can a former US

图 4 原文本

> How can a trial and the final outcome that is so important to the success of this fledgling democracy i IRAQ continue to be delayed and stalled? I believe it harms our efforts by instilling fear in those who have been repressed and it emboldens those who seek to regain power. Finally, how can a former US

图 5 嵌入水印后的文本

3.2 水印检测、纠错和提取实验及分析

(1)部分实验结果示意

对某个正常水印文件的提取结果见图 6。

图 6 正常水印文件的水印提取结果

对某个单词数为 970 的水印文件，删除中间约 48%时的提取结果见图 7。

图 7 遭删除攻击后含水印文件的水印提取结果

对某个单词数为 1715 的水印文件删除前后 3 处共占单词数 52%的内容，且在几处地方增加内容时的提取见图 8。

图 8 水印文件遭到较大攻击时纠错恢复 1 组水印的结果

(2)实验总结与分析

实验前期曾考虑对水印予以实施重复编码或奇偶校验码等差错控制码，但因攻击行为往往针对文本连续的若干单词(段落)，这样差错控制码的纠错功能就很有限，所以没有采用差错控制码，而是用层内分组的方式，使水印多重冗余嵌入以利于校检和纠错。

水印检测、纠错和提取算法的预期效果和实验结果相吻合，如表 1 所示。

表 1 水印文本经受各种攻击的水印可恢复性能

攻击方式	水印可提取/水印可恢复条件
全文清除 3 个水印特征之 1 或 2 个	不纠错即可提取水印
针对部分单词的水印清除攻击	通过 3 层水印的相互纠错一般均可恢复 1 组完整水印
增加内容的攻击	水印照常提取
删除攻击	允许被删除单词数占比的最大值少则 45%，多则 90%以上

4 小结

本文提出并实现了一种基于字符属性及单词内容的多重文本数字水印算法。该算法具有以下特点：

(下转第 154 页)