一种基于语句主谓语编码的文本水印技术

李桂森 陈建平 马海英 杨方兴
(南通大学计算机科学与技术学院 南通 226019)

摘 要 文本水印通过在文本中嵌入版权标识信息(水印)来保护文本作品的知识产权。提出一种对文本中语句的主谓语进行编码来嵌入水印的方法。将水印信息转换成十六进制的Unicode码串,借助哈尔滨工业大学的语言技术平台(LTP),对文本中的语句进行一系列处理获取其中的主谓语,用上述Unicode码串中的一段对每一个主谓语进行编码表示,以此实现水印的嵌入。提取水印时,从被检测的文本中获取语句的主谓语,对照嵌入水印时形成的码本,对每个主谓语进行比较和译码,取出各主谓语所对应的Unicode码段,将它们按正确顺序拼接起来,转换成对应的字符,得到嵌入的水印信息。所提算法具有很好的隐蔽性,能有效抵抗各种常见的攻击。

关键词 数字水印,文本水印,主谓语编码,LTP
中图法分类号 TP309.2 **文献标识码** A

Method for Text Watermarking Based on Subject-verb Encoding

LI Gui-sen CHEN Jian-ping MA Hai-ying YANG Fang-xing
(School of Computer Science and Technology, Nantong University, Nantong 226019, China)

Abstract Text watermarking protects the copyrights of text works by embedding copyright information(watermark) into a text. This paper proposed a text watermarking technique, in which the watermark is embedded by encoding the subject-verbs of the sentences in a text. A watermark message is converted into a string of the hexadecimal Unicode code. With the help of the language technology platform(LTP) of Harbin Institute of Technology, a series of processes are applied to the text to obtain the subject-verbs in the text. Each of the subject-verbs is encoded with one piece of the Unicode string, which achieves the embedding of the watermark. When extracting the watermark, the subject-verbs are obtained from the detected text and decoded according to the codebook generated in the watermark embedding. The corresponding pieces of the Unicode string are taken out from the codebook and put together in correct order. They are then converted back into the original characters to obtain the embedded watermark message. The proposed algorithm has a good nature of concealment and can resist various watermark attacks.

Keywords Digital watermarking, Text watermarking, Subject-verb encoding, LTP

1 引言

互联网和信息技术的普及应用促进了电子出版、电子商务、电子政务、数字图书馆、网络音频和视频服务等行业的快速发展,越来越多的多媒体信息以电子版的方式在网络上传播,使得人们获取信息更加方便快捷。与此同时,这也给盗版和盗用行为提供了方便,数字作品的知识产权侵犯问题日益严重,受到业界的广泛关注。为解决这一问题,一方面需要建立相应的法律法规,另一方面需要采取有效的技术手段。文本数字水印是近年来出现的保护数字文字作品知识产权的一项技术,它将代表著作权人身份的特定信息(即数字水印)以某种方式嵌入数字文字作品中。在产生版权纠纷时,通过合法的发行者、运营者相应的算法提取出该数字水印,从而验证版权的归属,确定侵权和盗用[1,3]。除了文字作品的版权保护外,文本水印技术还可以用于在文本文件中隐藏和传递秘密信息。

关于文本水印技术,目前研究得较多的主要有基于文本格式的文本水印和基于自然语言的文本水印。基于文本格式的水印技术利用轻微改变文本格式不易被察觉的特点嵌入水印信息,如调整行间距[4]、调整字间距[5]、修改字符颜色[6]、调整字形结构[7],以及附加空格的方法[8]等等。这类基于文本格式的水印技术编码简单、实现便捷,但对文本进行格式变换就有可能使嵌入的水印遭到破坏,抗攻击性不强、鲁棒性较差。为了解决这一问题,美国普渡大学的Atallah等人提出了自然语言文本水印技术[9],它可以利用文本内容的语法语义进行编码来嵌入水印信息[10,11],目前实现得较多的是通过同义词替换和句法变换对水印信息进行编码[12,13]。与基于文本格式的水印相比,自然语言文本水印具有更好的隐蔽性和鲁棒性,格式变换不会对水印产生影响。由于中文语言的复杂性,上述基于同义词替换和句法变换的水印算法会有产生歧义或改变语义的问题,同时它也不适用于文本内容不宜改

本文受国家自然科学基金项目(61402244),南通市应用研究计划项目(BK2011026)资助。
李桂森(1989—),男,硕士生,主要研究方向为文本水印;陈建平(1960—),男,教授,主要研究方向为信息安全,E-mail:chen.jp@ntu.edu.cn(通信作者);马海英(1977—),女,讲师,主要研究方向为信息安全;杨方兴(1990—),男,硕士生,主要研究方向为文本水印。

变的情形。基于此，有人提出了零水印技术[14]，即不改变载体信息而实现水印的嵌入，如对文本内容进行分词，然后统计每个分词的词频或各类词性的频次来嵌入水印[15,16]。该方法需要第三方认证，实现起来比较复杂。本文结合自然语言文本水印技术和零水印的思想，提出一种通过提取文本中语句的主谓语进行编码来嵌入水印信息的方法。所提算法不对文本格式与内容做任何改变，具有良好的隐蔽性和抗攻击性，同时算法构造简单、易于实现。下文介绍水印算法的基本原理，给出算法的具体实现步骤和应用系统实例。

2 水印算法的基本原理

一个实际的文本通常都是由句子组成的。完整的语句一般都有主谓语，如果将一个文本中所有语句的主谓语提取出来作为一个集合，那么这个集合是唯一的。可以用这些主谓语对所需嵌入的水印信息进行编码，以此完成水印信息的嵌入。当需要提取水印时，对照码本对这些主谓语进行译码，便得到嵌入的水印信息。主谓语的提取可以借助哈尔滨工业大学的语言技术平台，经过一系列处理得到。

2.1 主谓语的提取

语言技术平台(Language Technology Platform，LTP)是哈工大社会计算与信息检索研究中心历时 10 年研制的一整套开放式在线中文自然语言处理系统[17]，囊括了词法分析(包括分词、词性标注和命名实体识别)、句法分析(依存句法分析)、语义分析(词义消歧和语义角色标注)3 方面共 6 项语言处理基础技术。该平台对外开放，使用方便。它提供一个应用程序接口(API)，用户只需根据 API 参数集构造 HTTP 请求，即可在线获得分析结果。

本文主要用到 LTP 的依存句法分析功能，将待分析的文本提交给平台，经平台处理得到文本中语句各成分之间的依存关系。然后根据依存关系，经过进一步处理得到语句的主谓语。其基本过程如下。

将待分析的文本转换为字符串，将该字符串和其它一系列 API 参数(包括用户注册获得的 api_key，指定的分析模式 dp，指定的结果格式类型 xml 等)在线提交给 LTP 平台进行分析处理。

获取 LTP 平台的处理结果，得到一个包含文本中句子成分依存关系的 xml 格式的文本。该文本包含了 para(段落)、sent(句子)、word(词)等节点。每个词节点(word)有以下属性：id，词在句子中的序号；cont，分词内容；parent，依存句法分析的父节点的 id 号；relate，相对应的关系。为找出文本中的所有主谓语，循环遍历文本中的每一段、每一句、每一个分词。当循环遍历到 word 节点时，如果属性 relate＝“HED”(HED 表示核心关系)，则 word 节点的 cont 值即为本句谓语，然后查找本句是否存在这样的 word 节点，节点的 relate 属性值为 SBV(SBV 表示主谓关系)，并且其 parent 属性值与谓语节点的 id 号相等。如果存在，该 word 节点的 cont 值就是本句的主语。将本句的主语和谓语提取出来，保存到一个集合中。

2.2 水印的嵌入

用集合中的主谓语对水印信息进行编码。将水印信息的每个字符用其十六进制的 UTF-16 编码表示(采用 UTF-16 编码可以兼顾水印信息中含有的中文、英文或其它标点符号)，每个字符为 2 个字节，4 位十六进制数，形成一个十六进制的 Unicode 码串。将这一 Unicode 码串分成若干段，每一个主谓语用其中的一段来编码表示。考虑到针对文本水印的改变句子顺序的攻击可能会使水印信息不能正确提取，对每一个主谓语对应的 Unicode 码段给定一个编号，用于后期提取水印时进行 Unicode 码串的拼接。如果文本中的主谓语数量多于水印信息的位数，则可以选取部分主谓语进行编码。编码完成即实现了水印的嵌入。

下面给出一个编码的实例。假设需要保护的文本中含有 5 个主谓语，主谓语分别为 *sbv*1、*sbv*2、*sbv*3、*sbv*4、*sbv*5。需要嵌入的水印信息为“南通大学 Copyright © 2014”(共 18 个字符)。将水印信息用 UTF-16 编码表示，每个字符为 4 位十六进制数(如“南”的 UTF-16 编码为 5357)，得到一个 72 位的 Unicode 码串。将这一 Unicode 码串分成 5 段，前 4 段每段 14 位，最后一段 16 位，形成的码本如表 1 所列。

表 1 对水印信息进行编码的码本

主谓语	编码	编号
sbv1	5357901a59275b	1
sbv2	660043006f0070	2
sbv3	00790072006900	3
sbv4	670068007400a9	4
sbv5	0032003000310034	5

2.3 水印的提取

水印的提取是对文本中的主谓语进行译码的过程。当需要提取水印时，借助哈工大的 LTP 从需要检测水印的文本中解析出所含的主谓语。对照嵌入水印时形成的码本，对这些主谓语逐一进行译码。具体来讲，就是将解析出的每个主谓语与码本中的主谓语逐个进行比对，两者一致时，就取出该主谓语对应的 Unicode 码段及其编号。将这些 Unicode 码段按其编号顺序拼接起来，就得到代表水印信息的 Unicode 码串。然后按照所用的 UTF-16 编码规则，每 4 位转换为一个字符就得到嵌入的水印信息，从而实现了水印的提取。

3 水印算法的具体实现

3.1 水印的嵌入

第一步　将需要嵌入的水印信息每个字符用其十六进制 UTF-16 编码表示，每个字符占 4 位，最终得到一个代表水印信息的 Unicode 码串。设需要嵌入的字符数为 k，则生成的 Unicode 码串的位数为 $m=4k$。

第二步　根据上一节介绍的过程，借助哈工大的 LTP 平台提取出需要嵌入水印的文本中的主谓语，去除其中的重复项(防止提取水印时发生错误)，将主谓语置于一个集合中。

第三步　将主谓语集合中的每个主谓语用一段代表水印信息的 Unicode 码段来进行编码。设主谓语的个数为 n，m 整除 n 的结果为 p。对前 $n-1$ 个主谓语，依次从第一步生成的 Unicode 码串中取出 p 位分配给每一个主谓语，最后剩下的 Unicode 码分配给最后一个主谓语。对每一个主谓语对应的 Unicode 码段分配一个编号。每一行的主谓语、Unicode 码段及其编号之间分别用空格隔开，最终形成的码本文件如下所示：

sbv1 5357901a59275b 1

sbv2 660043006f0070 2

sbv3 00790072006900 3

sbv4 670068007400a9 4

sbv5 0032003000310034 5

将上述码本内容写入到一个文件保存起来，以备提取水印时使用。至此，水印信息的嵌入完成。

3.2 水印的提取

第一步　运用哈工大的 LTP 解析出需要检测水印的文本中的主谓语，把获取的主谓语存放于一个集合中。该过程与上面嵌入水印时相同。

第二步　打开嵌入水印时形成的码本文件，对照码本，对上述主谓语集合中的每一个主谓语进行译码，即如果码本中存在该主谓语，就取出该主谓语对应的 Unicode 码段。具体做法为，将码本文件的每一行读入到一个字符串数组，根据第一个空格符分割出每一行的主谓语，将其与主谓语集合中的主谓语逐一进行比较。若有一致者，则取出这一行的 Unicode 码段及其编号。然后，再根据 Unicode 码段与其编号之间的空格将各 Unicode 码段与其编号分割开来。最后，根据编号顺序将各 Unicode 码段拼接起来，就得到代表水印信息的 Unicode 码串。

第三步　将提取出的代表水印信息的十六进制 Unicode 码串转换为对应的字符，最终得到嵌入的水印信息。

4 算法性能分析

上述基于主谓语编码的文本水印算法对所保护的文本不作任何改动，具有绝对的隐蔽性，不会被察觉和发现。

该算法嵌入和提取水印的过程除文本中的主谓语外不涉及任何具体的文本格式、语法或语义结构，可以抵抗多种常见的针对文本水印的攻击[18]，包括针对行移编码攻击、字移编码攻击、特征编码攻击、变换句子顺序的攻击等。对文本调换句子顺序有可能会改变文本中某些主谓语的先后顺序，对于这一点，已在编码设计中采取了措施，即为每个主谓语对应的编码给定一个编号，提取水印时按照编号顺序来拼接 Unicode 码串，不受获取的主谓语顺序的影响。因此，调换句子顺序攻击对本方法也不起作用。

5 应用系统实例

根据本文提出的方法，设计开发出一个对文本文件进行水印嵌入与提取的应用系统。

系统主界面如图 1 所示。

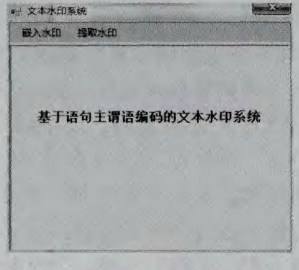

图 1　水印系统主界面

点击“嵌入水印”选项，出现图 2 所示界面。

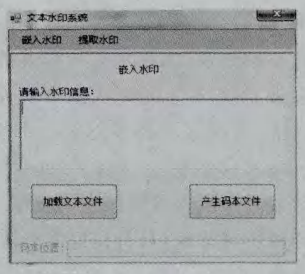

图 2　嵌入水印界面

在图 2 所示文本框内输入欲嵌入的水印信息，如“南通大学 Copyright © 2014”；然后点击“加载文本文件”按钮，选定需要嵌入水印的文本文件；点击“产生码本文件”按钮，系统完成水印信息的嵌入，输出生成的码本文件，如图 3 所示。用户保存好码本文件，以供日后提取水印所用。

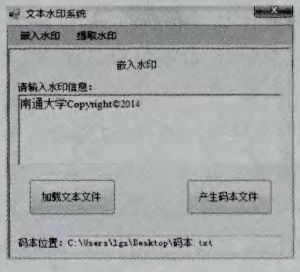

图 3　完成水印嵌入界面

当需要提取水印时，点击图 1 所示主界面的“提取水印”选项，出现图 4 所示界面。

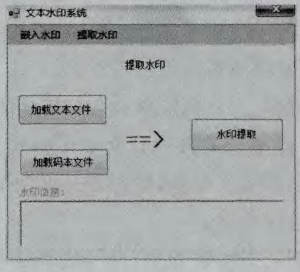

图 4　提取水印界面

点击“加载文本文件”按钮，选定需要检测水印的文本文件；然后点击“加载码本文件”按钮，载入嵌入水印时得到的码本文件；点击“水印提取”按钮，系统完成水印信息的提取，输出提取出的水印信息，结果如图 5 所示。

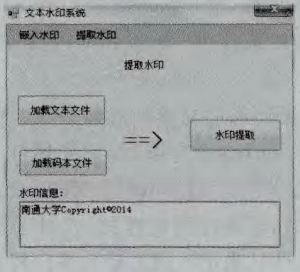

图 5　完成水印提取界面

如果被检测的文本文件不是我们嵌入水印信息的文件（即不含有参与编码的那些主谓语），系统则会提示未检测出水印。

结束语　本文提出一种基于语句主谓语编码的自然语言

文本水印技术，该技术在不对文本做任何改变的情况下实现水印信息的嵌入和提取，具有很好的隐蔽性，可以抵抗多种常见的针对文本水印的攻击。算法构造简单、易于实现，可据此设计出具有实用意义的文本水印嵌入与提取系统。

参 考 文 献

[1] Atallah M, McDonough C, Nirenburg S, et al. Natural Language Processing for Information Assurance and Security: An Overview and Implementations[C]// Proceedings of the 9th ACM/SIGSAC New Security Paradigms Workshop. Ireland, 2000: 51-65

[2] 刘晏昊，孙堡垒，郭云彪，等. 文本数字水印技术研究综述[J]. 东南大学学报(自然科学版)，2007，37(z1)：225-230

[3] 黄华，齐春，李俊，等. 文本数字水印[J]. 中文信息学报，2001，15(5)：52-57

[4] 梁旭，远志永，黄明. 基于行间距编码的文本数字水印算法[J]. 信息技术，2008，32(3)：38-41

[5] 于晨斐. 基于二次余数的 Word 文档数字水印[J]. 计算机仿真，2007，24(11)：324-326

[6] 蔡菲菲，刘洋，尹香兰. 一种基于 word 文档的文本水印技术研究[J]. 计算机科学，2012，39(z3)：39-40

[7] 陈翔. 一种基于中文字符编码的文本水印算法研究[J]. 计算机技术与发展，2013(2)：237-240

[8] Maxemchuk N F. Electronic Document Distribution[J]. AT&T Bell Laboratories Technical Journal, 1994, 73(5): 73-80

[9] Atallah M J, Raskin V, Meta C. Natural language watermarking: design, analysis, and a proof-of-concept implementation[C]// Proc. of Information Hiding-Fourth International Workshop. Berlin: Springer, 2001: 185-200

[10] 张宇，刘挺，陈毅恒，等. 自然语言文本水印[J]. 中文信息学报，2005，19(1)：56-62

[11] 杨超，李仁发，蒋斌，等. 基于语义的自然语言文本数字水印研究[J]. 计算机工程与设计，2005，26(6)：1428-1430

[12] 甘灿，孙星明，刘玉玲，等. 一种改进的基于同义词替换的中文文本信息隐藏方法[J]. 东南大学学报，2007，37(z1)：137-140

[13] Jalil Z, Mirza A M. A Review of Digital Watermarking Techniques for Text Documents[C]// International Conference on Information and Multimedia Technology. Jeju Island, 2009: 230-234

[14] 温泉，孙锬锋，王树勋. 零水印的概念与应用[J]. 电子学报，2003，31(2)：214-216

[15] 斯琴，张力，廉德亮. 基于文本特征的文本水印算法[J]. 计算机应用，2009，29(9)：2348-2350

[16] 舒娟娟，刘玉玲. 基于词性频率的中文文本零水印算法[J]. 计算机应用，2011，31(z2)：103-105

[17] Che Wan-xiang, Li Zheng-hua, Liu Ting. LTP: A Chinese Language Technology Platform[C]// Proc. of the Coling 2010: Demonstrations. Beijing, 2010: 13-16

(上接第 356 页)

根据《随机性检测规范》的原理，对多个样本进行随机性检测，统计得到的 P-value 值应当均匀分布在闭区间[0,1]内，其均值约为 0.5。对表 1 进行数据分析可以看出，LEX 和 DLEX 两种算法产生样本的 P-value 值的期望值均在 0.5 左右的一定区间内分布，并且两者的 P-value 值的期望值和方差都非常接近，符合统计规律，说明了 DLEX 算法与 LEX 算法产生的随机序列其随机性的统计特性相当。

结束语 LEX 算法以分组密码 AES 作为密钥流生成的核心部件，架起了分组密码与流密码之间的桥梁。但是由于其按奇偶数轮固定位置提取 4 个字节轮密钥加 ARK 的结果作为密钥流，导致其对于差分故障攻击存在安全隐患。本文分析了针对 LEX 算法的差分故障攻击，采取将一个随机序列与每组轮密钥异或的结果作为新的轮密钥的方法对 LEX 进行了改进，并用一个实例仿真来验证了改进算法的密钥流随机性。结果表明，改进的 LEX 抗差分故障攻击的能力得到了增强，且具有与原算法相当并符合国家规范的密钥流随机性，增强了 LEX 算法的密码性能。

参 考 文 献

[1] 刘依依. eSTREAM 和流密码分析现状[J]. 信息安全与通信保密，2009，31(12)：47-49

[2] Alex B. A new 128 bit key stream cipher LEX[EB/OL]. [2005-06-13]. http://www.ecrypt.eu.org/stream/ciphers/lex/lex.pdf

[3] National Institute of Standards and Technology (NIST). Announcing the Advanced Encryption Standard(AES) [EB/OL]. (2001-11-26). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] 邓元庆，龚晶，石会. 密码学简明教程[M]. 北京：清华大学出版社，2011：71-93

[5] Henricksen M. Flexible Block Ciphers: Modifying LEX [C]// Proceedings of ICCSIT2010. Chengdu, 2010

[6] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults[M]// Advances in Cryptology—EUROCRYPT'97. 1997: 37-51

[7] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems[M]// Advances in Crytpology—CRYPTO'97. 1997: 37-51

[8] Huang J, Susilo W, Seberry J. Differential fault analysis of LEX [C]// Proceedings of SCN 2010. Amalfi, Italy, 2010

[9] Skorobogatov S, Anderson R. Optical fault induction attacks [M]// Cryptographic Hardware and Embedded System-CHES 2002. 2003: 2-12

[10] Giraud C. DFA on AES[M]// Advanced Encryption Stardard-AES. 2005: 27-41

[11] 张中亚，关杰. 对流密码算法 LEX 的差分故障攻击[J]. 上海交通大学学报，2012，40(6)：865-869

[12] 王秋燕，金晨辉. LEX 算法的输出位置分析[J]. 计算机应用与软件，2014，31(10)：309-313

[13] 随机性检测规范：GM/T 0005-2012[S]. 北京：中国标准出版社，2012