YINPING XINXI YINCANG YU
SHUZI SHUIYIN

音频信息隐藏与数字水印

杨 榆 雷 敏 编著

北京邮电大学出版社
www.buptpress.com

音频信息隐藏与数字水印

杨 榆 雷 敏 编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书共分为三个部分，第一部分介绍了音频信息隐藏和数字水印的基本概念、音频的基本知识、音频隐藏算法的性能研究等内容，信息隐藏和数字水印算法分为正向和反向研究；第二部分介绍了回声隐藏、基于 DWT 和 DCT 域的各种隐藏算法、零水印算法和半脆弱水印算法，属于正向研究；第三部分介绍了隐写分析、基于 DCT 的音频隐写和基于回声隐藏的隐写分析算法，属于反向研究。

本书可作为专业课程参考书，可作为课程设计和毕业设计指导书，也可作为音频信息隐藏与数字水印研究人员参考书。

图书在版编目(CIP)数据

音频信息隐藏与数字水印 / 杨榆，雷敏编著. -- 北京：北京邮电大学出版社，2015.10
ISBN 978-7-5635-4521-6

Ⅰ. ①音… Ⅱ. ①杨…②雷… Ⅲ. ①数字音频技术—密码术—应用—信息安全 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2015)第 219207 号

书　　名：音频信息隐藏与数字水印
责任著作者：杨　榆　雷　敏
责 任 编 辑：艾莉莎
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京九州迅驰传媒文化有限公司
开　　本：720 mm×1 000 mm　1/16
印　　张：9.5
字　　数：189 千字
版　　次：2015 年 10 月第 1 版　2015 年 10 月第 1 次印刷

ISBN 978-7-5635-4521-6　　定价：22.00 元

·如有印装质量问题，请与北京邮电大学出版社发行部联系·

目　录

第 1 章　概论 …… 1

1.1　基本概念 …… 1

1.1.1　什么是信息隐藏 …… 1

1.1.2　信息隐藏的历史 …… 2

1.1.3　信息隐藏算法性能指标 …… 4

1.1.4　音频信息隐藏研究内容 …… 5

1.2　音频数字水印 …… 9

1.2.1　普通水印 …… 9

1.2.2　强鲁棒性水印 …… 10

1.2.3　半脆弱水印 …… 11

1.3　音频水印的具体应用 …… 11

参考文献 …… 13

第 2 章　音频基础 …… 18

2.1　音频信息隐藏的生理学基础 …… 18

2.1.1　等响曲线 …… 18

2.1.2　时域掩蔽 …… 19

2.1.3　频域掩蔽 …… 20

2.2　离散音频信号处理基础 …… 22

2.2.1　短时加窗处理 …… 23

2.2.2　短时平均能量和跨零数 …… 24

2.2.3　短时自相关函数和短时平均幅度差函数 …… 25

2.2.4　短时傅里叶变换 …… 26

2.2.5 同态分析…… 27
2.2.6 语谱分析…… 27
2.2.7 音频信号的线性预测分析…… 28
2.3 音频信号的统计特性…… 28
2.4 音频信号处理基础…… 31
2.4.1 音频波形编码…… 31
2.4.2 语音短时特性…… 33
2.4.3 线性预测分析…… 34
参考文献 …… 35

第 3 章 音频信息隐藏算法性能研究 …… 37

3.1 透明性…… 37
3.1.1 透明性现有算法评价方法…… 38
3.1.2 压缩算法音质客观评价算法…… 40
3.1.3 评价…… 42
3.2 水印容量…… 43
3.3 鲁棒性…… 43
3.3.1 误码率…… 43
3.3.2 归一化系数…… 44
3.4 本章结语…… 44
参考文献 …… 45

第 4 章 回声隐藏研究 …… 46

4.1 引言…… 46
4.1.1 隐藏原理…… 46
4.1.2 隐藏算法…… 48
4.1.3 提取算法…… 48
4.2 复倒谱…… 49
4.2.1 短时复倒谱分析…… 49
4.2.2 微分法…… 51
4.2.3 最小相位…… 51

此为试读,需要完整PDF请访问: www.ertongbook.com

4.2.4　递归法 …… 52
4.2.5　模 2π 相位展开器 …… 53
4.2.6　离散复倒谱中的误差 …… 53
4.3　回声隐藏经典算法 …… 54
4.3.1　多回声算法 …… 54
4.3.2　前后向算法 …… 55
4.3.3　PN 算法 …… 56
4.3.4　自适应算法 …… 57
4.3.5　ABS 算法 …… 58
4.3.6　评价 …… 58
4.4　多位置隐藏 …… 58
4.5　性能分析 …… 59
4.5.1　秘密信息恢复率分析 …… 60
4.5.2　噪声攻击后恢复率分析 …… 60
4.5.3　*A* 律压缩后恢复率分析 …… 61
4.5.4　*mu* 律压缩后恢复率分析 …… 61
4.5.5　重采样后恢复率分析 …… 62
4.5.6　低通滤波后的恢复率分析 …… 63
4.5.7　分段信噪比分析 …… 63
4.5.8　分段自相关分析 …… 64
4.5.9　载体分析 …… 65
4.5.10　小结 …… 66
4.6　本章结语 …… 67
参考文献 …… 67

第 5 章　基于 DWT、DCT 和 SVD 的音频水印 …… 69

5.1　引言 …… 69
5.1.1　离散小波变换(DWT) …… 70
5.1.2　离散余弦变换(DCT) …… 71
5.1.3　奇异值分解变换(SVD) …… 71
5.2　基于 DWT-DCT-SVD 的音频盲水印算法 …… 74

5.2.1 水印嵌入算法…… 74
5.2.2 水印提取算法…… 76
5.3 实验与性能分析…… 77
5.3.1 透明性…… 77
5.3.2 算法容量 …… 80
5.3.3 鲁棒性 …… 80
5.3.4 与其他算法的比较 …… 82
5.4 本章结语…… 83
参考文献 …… 83

第 6 章 基于 DWT、DCT 和 *QR* 的音频盲水印算法 …… 85

6.1 引言…… 85
6.2 音频盲水印算法…… 85
6.2.1 水印嵌入算法…… 86
6.2.2 水印提取算法…… 87
6.3 仿真实验与性能分析…… 87
6.3.1 透明性和鲁棒性…… 88
6.3.2 健壮性…… 89
6.4 本章结语…… 91
参考文献 …… 91

第 7 章 基于 DWT 和 DCT 组合的零水印算法 …… 93

7.1 概述…… 93
7.2 算法描述…… 94
7.2.1 水印嵌入算法…… 94
7.2.2 水印提取算法…… 94
7.3 实验仿真…… 95
7.4 本章结语…… 96
参考文献 …… 97

第 8 章 DWT 域半脆弱音频水印算法 …… 99

8.1 引言…… 99

8.1.1　半脆弱水印系统 …… 100
8.1.2　音频半脆弱水印的基本框架 …… 101
8.2　DWT 域半脆弱音频水印算法 …… 102
8.2.1　水印预处理 …… 102
8.2.2　水印嵌入 …… 103
8.2.3　水印提取 …… 104
8.3　实验与性能分析 …… 106
8.3.1　透明性 …… 106
8.3.2　容忍常见音频信号处理能力 …… 106
8.3.3　恶意篡改定位能力 …… 108
8.4　本章结语 …… 113
参考文献 …… 113

第 9 章　音频隐写分析 …… 115

9.1　隐写分析概述 …… 115
9.2　隐写分析分类 …… 116
9.2.1　根据适用性 …… 116
9.2.2　根据已知消息 …… 117
9.2.3　根据采用的分析方法 …… 117
9.3　隐写分析评价指标 …… 117
9.3.1　准确性 …… 118
9.3.2　适用性 …… 118
9.3.3　实用性 …… 118
9.3.4　复杂度 …… 118
参考文献 …… 119

第 10 章　DCT 域音频隐写分析算法 …… 120

10.1　引言 …… 120
10.2　DCT 域音频水印算法 …… 122
10.3　音频 DCT 域隐写分析算法 …… 123
10.3.1　差值比例隐写分析算法 …… 123

10.3.2 实验与性能分析…… 124
10.4 本章结语…… 126
参考文献…… 127

第 11 章 基于回声隐藏的隐写分析算法 …… 129

11.1 引言 …… 129
11.1.1 回声隐藏算法简介…… 129
11.1.2 回声隐藏的嵌入算法…… 130
11.1.3 回声隐藏提取算法…… 131
11.2 回声隐藏分析算法…… 132
11.2.1 原理 …… 133
11.2.2 一种新的隐写分析算法…… 135
11.2.3 测试音频文件的选择…… 137
11.3 实验和性能分析…… 139
11.4 本章结语…… 141
参考文献…… 142

第1章 概 论

1.1 基本概念

随着计算机技术和网络技术的发展，越来越多的数字化多媒体内容信息（图像、视频、音频等）纷纷以各种形式在网络上快速地交流和传播。在开放的网络环境下，如何对数字化多媒体内容进行有效的管理和保护，成为信息安全领域的研究热点。对于上述问题，人们最初的想法是求助于传统的密码学。但是传统的加密手段在对数字内容管理和保护上存在着一定的缺陷。为此，人们开始寻找新的解决办法来作为对传统密码系统的补充。多媒体数字内容在网络上的传递、发布和扩散带来了一系列问题和应用需求，从总体上来说可以分为两大部分：多媒体数字内容的版权保护问题和伪装式保密通信，这两个研究问题都属于信息隐藏[1-3]研究的范畴。

1.1.1 什么是信息隐藏

在很多文献中，对信息隐藏、数字水印、隐写术和隐写分析的描述经常混淆，甚至很多文献将信息隐藏等同于隐写术。本书采用以下约定：

（1）信息隐藏（Inforamtion Hiding）：信息隐藏通过对载体进行难以被感知的改动，从而嵌入信息。

（2）隐写术（Steganography）：隐写术是通过对载体进行难以被感知的改动，从而嵌入秘密信息的技术。Steganography 单词来自于希腊词根：steganos 和 graphie。Steganos 指有遮盖物的；graphie 指写。因此，Steganography 的字面意思即为隐写。

（3）数字水印（Digital Watermarking）：数字水印是通过对载体进行难以被感知的改动，从而嵌入与载体有关的信息，嵌入的信息不一定是秘密的，也可能是可见。

（4）隐写分析（Steganalysis）：隐写分析是检测、提取、破坏隐写载体中秘密信

息的技术。

信息隐藏的载体可以是文本、图像、音频、视频、网络协议和各类数据等。在不同的载体中，信息隐藏的方法有所不同，需要根据载体的特征选择合适的信息隐藏算法。比如图像、视频、音频中的信息隐藏，大部分都是利用了人类感观对于这些载体信号的冗余来隐藏信息。

隐写术与数字水印是信息隐藏的两个重要研究分支，采用的原理都是将一定量的秘密信息嵌入到载体数据中，但由于应用环境和应用场合的不同，对具体的性能要求不同。隐写术主要用在相互信任的点对点之间进行通信，隐写主要是保护嵌入到载体中的秘密信息。隐写术注重的是信息的不可觉察性和不可检测性，同时要求具有相当的隐藏容量以提高通信的效率，隐写术一般不考虑鲁棒性。而数字水印要保护的对象是隐藏信息的载体，数字水印要求的主要性能指标是鲁棒性（脆弱水印除外），对容量要求不高，数字水印有一些是可见的，有一些是不可见的。可见水印和不可见水印应用场合不同。

信息隐藏不同于传统的数据加密[4]，数据加密隐藏信息的内容，让第三方看不懂；信息隐藏不但隐藏了信息的内容，而且隐藏了信息的存在性，让第三方看不见。传统的密码技术与信息隐藏技术并不矛盾，也不互相竞争，而是有益的相互补充。它们可用在不同场合，而且这两种技术对算法要求不同，在实际应用中也可相互配合。

1.1.2 信息隐藏的历史

类似于密码学，信息隐藏自古就有。本章根据一些文献上记载的重要历史事件来了解人们是如何利用隐写术的。古代的隐写术从应用上可以分为这样几个方面：技术性的隐写术、语言学中的隐写术和应用于版权保护的隐写术。

（1）技术性的隐写术

最早的隐写术例子可以追溯到远古时代。用头发掩盖信息：在大约公元前440年，为了鼓动奴隶们起来反抗，Histiaus给他最信任的奴隶剃头，并将消息刺在头上，等到头发长出来后，消息被遮盖，这样消息可以在各个部落中传递[5]。

使用书记板隐藏信息：在波斯朝廷的一个希腊人Demeratus，他要警告斯巴达将有一场由波斯国王薛西斯一世发动的入侵，他首先去掉书记板上的腊，然后将消息写在木板上，再用腊覆盖，这样处理后的书记板看起来是一个完全空白的。事实上，它几乎欺骗了检查的士兵和接收信息的人[5]。

将信函隐藏在信使的鞋底、衣服的皱褶中，妇女的头饰和首饰中等[6]。

在一篇信函中，通过改变其中某些字母笔划的高度，或者在某些字母上面或下面挖出非常小的孔，以标识某些特殊的字母，这些特殊的字母组成秘密信息。

Wilkins(1614—1672)对上述方法进行了改进，采用无形的墨水在特定字母上

此为试读，需要完整PDF请访问：www.ertongbook.com

制作非常小的斑点[7]。这种方法在两次世界大战中又被德国间谍重新使用起来[8]。

在1857年,Brewster[9]提出将秘密消息隐藏"在大小不超过一个句号或小墨水点的空间里"的设想。到1860年,制作微小图像的难题被一个叫Dragon的法国摄影师解决了,很多消息就可以放在微缩胶片中。如在1870—1871年弗朗格-普鲁士战争期间,巴黎被围困时,印制在微缩胶片中的消息就是通过信鸽传递的[10]。

Brewster的设想在第一次世界大战期间终于付诸实现,其作法是:先将间谍之间要传送的消息经过若干照相缩影后缩小到微粒状,然后粘贴在无关紧要的杂志等文字材料中的句号或逗号上[11]。

使用化学方法的隐写术。如中国魔术中采用的一些隐写方法,用笔蘸淀粉水在白纸上写字,然后喷上碘水,则淀粉和碘起化学反应后显出棕色字体。化学的进步促使人们开发更加先进的墨水和显影剂。但是,随着"万用显影剂"的发明,则不可见墨水的隐写方法就无效了。"万用显影剂"的原理是,根据纸张纤维的变化情况,来确定纸张的哪些部位被水打湿过,这样,所有采用墨水的隐写方法,在"万用显影剂"下都无效了。

(2) 语言学中的隐写术

语言学中的隐写术,其最广泛使用的方法是藏头诗。国外最著名的例子可能要算Giovanni Boccaccio(1313—1375)的诗作Amorosa visione,据说是"世界上最宏伟的藏头诗"作品[12]。他先创作了三首十四行诗,总共包含大约1 500个字母,然后创作另一首诗,使连续三行押韵诗句的第一个字母恰好对应十四行诗的各字母。

到了16世纪和17世纪,已经出现了大量的关于伪装术的文献,其中许多方法依赖于信息编码手段。Gaspar Schott(1608—1666)在他的著作*Schola Steganographica*中,扩展了由Trithemius在书*Polygraphia*中提出的"福哉马利亚(Ave Maria)"编码方法,其中*Polygraphia*和*Steganographia*是密码学和隐藏学领域所知道的最早出现的两部专著。扩展的编码使用40个表,其中每个表包含24个用四种语言(拉丁语、德语、意大利语和法语)表示的条目,每个条目对应于字母表中的一个字母。每个字母用出现在对应表的条目中的词或短语替代,得到的密文看起来像一段祷告、一封简单的信函、或一段有魔力的咒语。

Gaspar Schott还提出可以在音乐乐谱中隐藏消息。用每一个音符对应一个字母,可以得到一个乐谱。当然,这种乐谱演奏出来就可能被怀疑。

中国古代也有很多藏头诗(也称嵌字诗),并且这种诗词格式也流传到现在。如一年中秋节,绍兴才子徐文长在杭州西湖赏月时,做了一首七言绝句:

平湖一色万顷秋,
湖光渺渺水长流。

秋月圆圆世间少，
月好四时最宜秋。

其中前面四个字连起来读，正是“平湖秋月”。

中国古代信息隐藏方法中，发送者和接收者各持一张完全相同的、带有许多小孔的纸，这些孔的位置是被随机选定的。发送者将这张带有孔的纸覆盖在一张纸上，将秘密信息写在小孔的位置上，然后移去上面的纸，根据下面的纸上留下的字和空余位置，编写一段普通的文章。接收者只要把带孔的纸覆盖在这段普通文字上，就可以读出留在小孔中的秘密信息。在16世纪早期，意大利数学家Cardan(1501—1576)也发明了这种方法，这种方法现在被称作卡登格子法。

(3) 用于版权保护的隐写术

版权保护和侵权的斗争从古至今一直在持续着。根据Samuelson的记载[13]，第一部“版权法”是“圣安妮的法令”，由英国国会于1710年制定。

Lorrain(1600—1682)是17世纪一个很有名的风景画家，当时出现了很多对他画的模仿和冒充，由于当时还没有相关的版权保护法律，他就使用了一种方法来保护他画的版权。他自己创作了一本称为 *Liber Veritatis* 的书，这是一本写生形式的素描集，它的页面是交替出现的，四页蓝色后紧接着四页白色，不断重复着，它大约包含195幅素描。他创作这本书的目的是为了保护自己的画免遭伪造。事实上，只要在素描和油画作品之间进行一些比较就会发现，前者是专门设计用来作为后者的“核对校验图”，并且任何一个细心的观察者根据这本书仔细对照后就能判定一幅给定的油画是不是赝品。

类似的技术在目前仍然使用着。如，一种图像保护系统ImageLock[14]是这样工作的：系统中对每一个图像保存一个图像摘要，构成一个图像摘要中心数据库，并且定期到网络上搜寻具有相同摘要的图像。它可以找到任何未被授权使用的图像，或者任何仿造的图像，通过对比图像摘要的办法来指证盗版。

1.1.3 信息隐藏算法性能指标

经过几十年的研究和发展，信息隐藏技术不同的应用使它形成不同的特点，但是，所有的信息隐藏算法共有一些基本的特点。对信息隐藏某一种算法进行评价时，经常会考虑到这个算法的三个最重要性能指标：透明性、鲁棒性和隐藏容量。Goljan Miroslav[15]将信息隐藏的性能指标描述成几何三角关系，如图1-1所示。

(1) 透明性(imperceptibility)

信息隐藏的首要特性是透明性，也称为不可感知性。是指嵌入的秘密信息导致隐写载体信号质量变化的程度。即在被保护信息中嵌入数字水印后应不引起原宿主媒体质量的显著下降和视听觉效果的明显变化，不能影响隐写载体的正常使用。也就是说，隐写载体如果仅通过人类听觉或视觉系统很难察觉有异常。

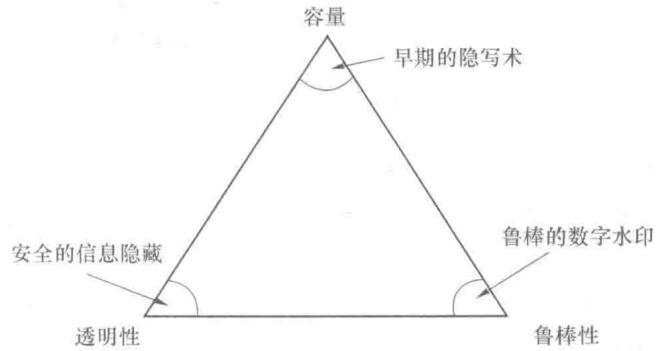

图 1-1 信息隐藏三种特征之间的关系

(2) 鲁棒性(robustness)

鲁棒性也称稳健性,是指隐藏的秘密信息抵抗各种信号处理和攻击的能力,鲁棒性水印通常不会因常见的信号处理和攻击而丢失隐藏的水印信息。

(3) 隐藏容量(capacity)

隐藏秘密信息的容量指在单位时间或一幅作品中能嵌入水印的比特数。对于一幅图片而言,数据容量是指嵌入在此幅图像中的所有比特数。对于音频而言,数据容量即指一秒传输过程中所嵌入秘密信息的比特数。对于视频而言,数据容量既可指每一帧中嵌入的比特数,也可指每一秒内嵌入的比特数。

信息隐藏算法这三个性能指标之间相互制约,没有一种算法能让这三个性能指标达到最优。当某一种算法透明性较好时,说明原始载体与隐藏秘密信息的载体之间从人类视听觉效果上几乎无法区分,嵌入这些秘密信息的时候对原始载体的改动就不能太大,这种算法鲁棒性往往比较差。当某一种算法鲁棒性较好的时候,一般是修改了载体比较重要的位置,也就是说隐藏的信息与载体的某些重要特征结合在一起,这样才能抵抗各种信号处理和攻击,但是修改载体比较重要位置的隐藏算法就会改变载体的某些特征,隐藏秘密信息后载体的透明性就比较差。而且信息隐藏容量和透明性也相互矛盾,当隐藏的信息容量比较大时,隐藏后隐写载体的透明性就比较差。

1.1.4 音频信息隐藏研究内容

信息隐藏的载体很多,如图像、音频、视频、文本,甚至还可以是网络协议。本书介绍的主要内容是音频信息隐藏,本书中所使用的载体是音频。

音频信息隐藏技术就是在不影响原始音频质量的条件下嵌入信息。嵌入的秘密信息与原始音频数据紧密结合并隐藏在音频载体中,人耳听觉系统感觉不到隐写音频文件的异常。

音频信息隐藏根据隐藏信息的目的可以分为数字水印和隐写术两个分支。为了区分数字水印和隐写术，对本书中使用的术语进行如下约定：

- 自然音频是指用于隐写算法中嵌入秘密信息之前的音频；
- 隐写音频是指嵌入秘密信息之后的音频；
- 原始音频是指数字水印算法中嵌入水印信息之前的音频；
- 含水印音频是指嵌入水印信息之后的音频；
- 待检测音频是指隐写分析算法检测的对象。

音频水印嵌入的信息可以是音频版权保护信息、作品序列号、艺术家和歌曲名字等，用于音频的版权保护、盗版追踪和拥有者识别等。

音频数字水印的研究分为正向研究和逆向研究两个方面。正向研究是研究在音频载体中嵌入和提取水印信息的算法，这些算法在音频中嵌入水印时不能引起音频质量的明显下降，同时含水印音频在传输的过程可能会受到各种音频信号处理的攻击，音频水印算法对这些处理和攻击具有较强的鲁棒性，经过信号处理和攻击后水印提取端还能提取水印信息；音频水印攻击的目标是阻碍水印信息的顺利提取，主要研究各种攻击方法。

音频隐写主要是为利用信息隐藏技术把需要传递的秘密信息隐藏在看似正常的音频载体中，隐藏秘密信息的存在性，用于保密通信，第三方无法感知正常的通信过程中隐藏了秘密信息。音频隐写术主要应用在需要安全保密通信的部门。

音频信息隐藏中隐写术的研究分为正反两个方面。其中正向研究是研究各种隐藏算法，反向研究是研究各种隐写分析算法。音频信息隐藏是研究在音频载体中隐藏秘密信息的算法，这些算法尽量在不引起监听者察觉变化的基础上还能隐藏尽量多秘密信息，以提高隐蔽通信的效率。隐写分析目的就是要对听觉上正常的音频载体进行分析，判断待检测载体是否为隐写载体，甚至只是怀疑该载体为隐写载体，从而达到拦截和破坏秘密信息隐蔽传递的目标。

音频信息隐藏根据研究的内容分为：数字水印、水印攻击、隐写术和隐写分析。如图 1-2 所示。

音频水印可以根据水印抵抗各种音频信号处理的鲁棒性分为普通水印、强鲁棒性水印和半脆弱水印。普通水印能够抵抗常见音频信号处理，如加噪、MP3 压缩、重量化、低通滤波和重采样等。普通水印根据水印嵌入的位置分为时域和变换域两种。

强鲁棒性水印不但能抵抗常见的音频信号处理，还对大部分音频信号处理有一定的抵抗能力。强鲁棒性水印根据信号处理的类型，可分为抗格式转换、抗 A/D 与 D/A 转换和抗同步转换三种。抗格式转换主要是音频在传输过程中可能会进行一些编码格式上的转换，水印算法能抵抗这些格式转换；抗 A/D 与 D/A 转换是指音频在传输过程中可能要经过 D/A 和 D/A 转换，水印能抵抗此种转换。同

步转换是指在传输过程中对音频进行裁剪、随机删除、增加样本、抖动和 TSM 转换等，抗同步转换的水印算法能抵抗此种类型的转换。

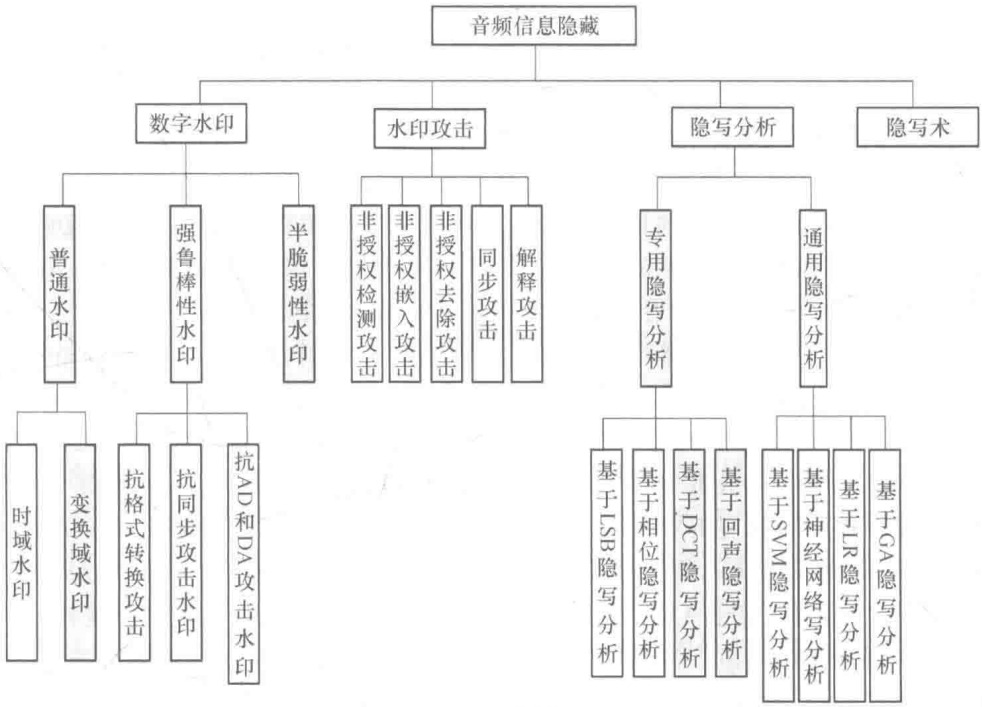

图 1-2　音频信息隐藏研究内容

半脆弱水印主要用于音频内容完整性保护，可以检测音频内容是否被恶意篡改。当以图像为载体时，与半脆弱水印相对的还有图像全脆弱水印。图像的全脆弱水印要求图像在传输过程中不能被修改，否则无法通过认证。但是音频的全脆弱水印研究较少，现有的文献中提到的全脆弱水印也是采用传统的密码学技术来实现[16]，并不是真正意义上的水印方案。音频半脆弱水印能容忍一定程度的常规音频信号处理操作，同时能检测和定位对音频内容的恶意篡改。

虽然目前已经提出很多种数字水印算法，但是几乎所有的算法都有安全漏洞。针对现有水印算法的漏洞，研究者提出多种攻击方法。研究水印攻击方法，一方面可以分析、评估现有水印系统的安全性，找出现有系统的安全漏洞；另一方面根据找到的安全漏洞可以设计更加安全的水印系统，以提高水印系统的性能。

水印攻击的目标是妨碍水印信息的顺利提取。总的来说，主要可以分为非授权检测攻击、非授权嵌入攻击、非授权去除攻击和系统攻击[17-22]。非授权检测攻击是指未经授权就试图检测载体是否存在水印或解码水印信息。非授权嵌入攻击是指攻击者在未取得他人授权的情况下在含水印作品中嵌入自己的信息或将他人

合法的水印嵌入到另外的载体中。非授权去除攻击的目标是试图去除水印或者让检测器检测不到水印信息。系统攻击是指攻击者不仅仅攻击水印嵌入和检测算法，而且攻击水印协议、水印算法的软硬件环境等等。

音频隐写术主要是为了利用信息隐藏技术把需要传递的秘密信息隐藏在看似正常的音频载体中，隐藏秘密信息的存在性从而用于保密通信，使第三方无法感知正常的通信过程中隐藏了秘密信息。隐写术需要保护的对象是隐藏在音频中的秘密信息，音频隐写术主要应用在需要安全保密通信的部门。

隐写术研究各种算法的目标是提高算法的透明性和隐藏容量。提高透明性的目标是为更好隐藏秘密信息的存在性，提高秘密信息的隐藏容量是为了提高音频隐写的效率，在单位时间的音频中隐藏更多秘密信息以提高音频隐写效率。

早期的音频隐写方法基本上都是采用时域的 LSB 算法(Least Significant Bit，最低有效位)来隐藏信息[23]，但是该算法的隐藏容量有限，有研究者[24]改进传统的 LSB 算法以提高算法的透明性和隐藏容量。随着 PSTN 网络(Public Switched Telephone Network，公共交换电话网络)和移动通信网络的发展，各种语音保密系统不断被提出。陈亮等在文献[25]中将保密语音通过 MELP 编码(Mixed Excitation Linear Predictive，混合激励线形预测)，形成秘密信息，然后根据人耳听觉的掩蔽效应，在公开语音 DCT 域(Discrete Cosine Transform，离散余弦变换)的中频系数中嵌入秘密信息。测试结果表明，在隐藏信息后，信道中传输的公开语音保持一定的透明性，并在受到压缩、滤波等攻击时具有较高的鲁棒性，但该算法提取秘密信息时需原始音频，属于非盲水印方法，因此实用性较差。钮心忻等[26]利用合成分析法(ABS)，结合 GSM 语音编码算法(Global System for Mobile Communication，全球移动通信系统)特点，提出一种隐藏容量大、隐藏效果较好的保密语音隐藏算法，并借助公共电话网初步实现了一个伪装式数字化语音保密传输系统。杨伟等[27-29]提出一种伪装式数字化语音保密通信系统。该系统将需要传输的秘密音频信息利用 MELP 算法编码后，使用 ABS 算法隐藏到一段 GSM 编码的明文语音中传输。这样窃听者听到的是一段正常的明文音频信息，不易引起窃听者怀疑，从而达到安全传输密文信息的目标。白剑等[30]提出一种新的适用于 GSM 移动通信中的语音隐藏算法，它利用 GSM 移动系统中的语音压缩编码 RPE-LTP 的特性：编码前后语音相邻段落之间的能量比改变不大。这种方法可以在 GSM 移动终端的声码器前端进行信息隐藏，因此可以兼容各种 GSM 移动终端，具有良好的实用性。

音频隐写分析是隐写术的对立技术，可以分析判断待检测载体是否为隐写载体。隐写分析分为专用隐写分析和通用隐写分析。专用隐写分析主要是针对某一种隐写算法提出的隐写分析方法，算法的准确率较高。通用隐写分析算法是针对所有隐写算法都适用的分析算法。通用隐写分析算法通过分类器对待检测的音频

此为试读，需要完整PDF请访问：www.ertongbook.com