信息科学技术学术著作丛书

面向隐蔽通信的音频信息隐藏技术

杨百龙　武朋辉　郭文普　时　磊　著

科学出版社

信息科学技术学术著作丛书

面向隐蔽通信的音频信息隐藏技术

杨百龙　武朋辉　郭文普　时　磊　著

科学出版社

北京

内 容 简 介

本书围绕隐蔽通信中的音频信息隐藏预处理技术、音频信息隐藏算法等问题，深入阐述面向语音类嵌入数据的基于离散余弦变换与压缩感知的低速率编码方法和基于双一维混沌互扰系统与 m 序列的加密方法等预处理技术、小波域音频信息隐藏算法、压缩域音频信息隐藏算法、倒谱域音频信息隐藏算法、基于经验模式分解的音频信息隐藏算法、基于能量比调整的自适应音频信息隐藏算法和面向移动载密通信的音频信息隐藏算法等涉及的理论和关键技术。

本书可供计算机科学与技术、信息与通信工程、信息安全等学科专业从事隐蔽通信、信息隐藏、音频处理等相关领域的教学、科研和工程技术人员参考，也可作为高校相关专业研究生及高年级本科生的教材。

图书在版编目(CIP)数据

面向隐蔽通信的音频信息隐藏技术/杨百龙等著. —北京：科学出版社，2018. 9

（信息科学技术学术著作丛书）

ISBN 978-7-03-058885-2

Ⅰ. ①面… Ⅱ. ①杨… Ⅲ. ①音频信号处理-研究 Ⅳ. ①TN912. 3

中国版本图书馆 CIP 数据核字(2018)第 216727 号

责任编辑：魏英杰 / 责任校对：郭瑞芝

责任印制：张 伟 / 封面设计：铭轩堂

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2018 年 9 月第 一 版 开本：720×1000 B5

2018 年 9 月第一次印刷 印张：11

字数：218 000

定价：90.00 元

（如有印装质量问题，我社负责调换）

《信息科学技术学术著作丛书》序

21世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术，数据知识化和基于知识处理的未来信息服务业，低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性；体现出科学出版社“高层次、高水平、高质量”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士

原中国科学院计算技术研究所所长

前　言

基于信息隐藏的隐蔽通信技术是近年来通信安全技术中非常引人关注的研究领域。信息隐藏技术利用载体信息中具有随机特性的冗余部分，将秘密信息嵌入载体信息中，使其在通信传输过程中不被人发现，从而增强秘密信息传输安全性。如果在秘密数据嵌入之前对其进行加密预处理，则携密载体数据将具备伪装和加密的双重安全性。

信息隐藏技术的研究热点主要集中在载体信息冗余空间、秘密数据嵌入/提取方法和提高抵抗信号处理攻击能力等方面。本书在介绍国内外该方向研究进展的基础上，重点介绍作者在秘密数据预处理、音频载体中的秘密数据隐藏方法及抵抗同步攻击等方面的研究成果。

全书共8章。第1章绪论，着重介绍音频信息隐藏相关研究方向的发展历程和研究现状。第2章秘密数据预处理技术，针对音视频等数据量较大的秘密数据，提出一种基于余弦变换和压缩感知的低码率音频编解码算法，减小秘密数据嵌入量，增强载体音频的透明性，针对密级要求较高的秘密数据，提出一种基于双一维混沌互扰和 m 序列的加密算法，进一步增强秘密数据安全性。第3章小波域音频信息隐藏技术，通过设计一种大容量的小波域音频信息隐藏算法，对基于提升小波和DCT变换的音频信息隐藏算法进行研究。第4章压缩域音频信息隐藏技术，探讨以MP3文件为载体的两类音频信息隐藏算法。第5章基于经验模式分解的音频信息隐藏算法，利用现代信号处理中的经验模式分解方法，提出将秘密数据嵌入经验模式分解后的分量中，结合均匀调制技术和同步码嵌入技术，提高隐蔽通信系统的性能指标。第6章基于倒谱分析的音频信息隐藏算法，对基于倒谱分析的音频信息隐

藏算法进行改进，提高算法透明性和鲁棒性。第 7 章基于能量比调整的自适应音频信息隐藏算法，提出一种适用于 GSM 移动通信网络的音频信息隐藏算法。第 8 章基于余弦信号替代的同步算法，提出一种显式同步和隐含同步相结合的同步方法——基于余弦信号替代的同步算法。

本书是作者科研团队近年来围绕音频信息隐藏技术研究成果的总结，感谢火箭军工程大学“2110”工程项目对本书出版的资助！

限于作者水平，难免存在不妥之处，恳请读者批评指正。

作　者

目　录

第1章 绪 论

1.1 基于信息隐藏的隐蔽通信技术

保证通信数据安全是通信安全技术的永恒课题。传统的加密通信技术应用广泛，但存在致命弱点：一是随着计算机软硬件技术的发展，人类计算能力飞速提升，破解复杂加密技术的能力越来越强，尤其是基于网络实现的具有并行计算能力的破解技术日益成熟，加密算法的安全性受到严重挑战；二是加密后的数据通常以无规律的乱码形式存在，容易引起攻击者的注意和破坏欲望，即使攻击者不能破解，也可能进行拦截或予以破坏、摧毁，或以其他手段干扰通信过程的正常进行。因此，一种以隐藏秘密数据通信过程的通信安全技术——隐蔽通信技术得到高度重视和深入研究。

本书研究的隐蔽通信技术，也称隐密通信(steganographic communication)技术，是指将秘密数据隐藏在可公开的数据(包括文本、图像、音频、视频等)中以实现安全通信的技术。隐蔽通信不但可保护通信数据，而且隐蔽了秘密数据通信的存在，使非通信接收者觉察不到有秘密数据通信的发生，从而大大降低秘密数据被截取或通信过程被干扰的概率，提高秘密数据通信安全性。

隐蔽通信具有如下三个显著特点。

① 隐蔽性。隐蔽通信的最大特点是隐蔽性，将真实的秘密通信隐藏在公开数据之中，使攻击方不知道秘密通信的存在，即隐蔽秘密通信的存在性。

② 寄生性。从实现的技术手段来看，将秘密通信数据融合(或称寄生)在公开数据(载体数据)之中。

③ 欺骗性。从达到的通信目的来看，通过公开的载体数据携带秘密数据，即使通信数据被截取，与经过加密技术生成的乱码数据不同，携密载体数据具有正常的外在形式和清晰的表征意义，可极大地降低通信敏感性，尤其是在互联网等海量数据传输环境中或长期例行通信情况下，无疑具有更好的欺骗性。

隐蔽通信的关键技术是信息隐藏技术[1,2]。信息隐藏(information hiding 或 data hiding)是利用人类感觉器官的不敏感性，以及多媒体数字信号本身存在的冗余，将秘密信息隐藏于另一个称为载体(cover)的宿主信号中，得到隐蔽载体(stego cover)，而不被人的感知系统察觉或注意，且不影响宿主信号的感知效果和使用价值。

信息隐藏技术可以从不同的角度进行分类[3]。

① 按保护对象分类，主要分为版权标记技术和隐匿技术。前者主要用于保护媒体载体本身的权属，后者主要用于保密通信，保护的是秘密数据内容。

② 按密码参与程度分类，主要分为无密隐藏和含密隐藏。无密隐藏又称为纯隐写术，将秘密数据嵌入隐秘媒体载体之前，对其不做加密预处理，而且秘密数据的嵌入过程也不受密码控制，因此难以保障秘密数据的安全性。含密隐藏在秘密数据嵌入前进行加密处理，实现了“隐蔽+加密”的双重安全机制，可以增强秘密数据的安全性。根据密码体制的不同，可对含密隐藏进行分类。如果在嵌入端和提取端对秘密数据的加密解密使用的是相同的密钥，则称其为对称密码隐藏，否则为非对称密码隐藏。如果在嵌入端和提取端对秘密数据的加密解密使用的是公钥体制，则称这种隐蔽方法为公钥信息隐藏。

③ 按载体类型分类，主要包括基于文本、图形/图像、音频、视频、数据库、网络协议等对象的信息隐藏技术。文本信息隐藏是指通过在格

式化文本文件中通过调整细小的版面特性来隐藏秘密数据，比较常见的方法有特征编码法和行/字移位编码法。图形/图像信息隐藏是指在数字格式的图形/图像中，选择人类视觉系统不敏感的成分嵌入秘密数据，常见的做法是对一部分图形/图像数据本身(空域)或图形/图像的特征参数(变换域)进行修改或替换。音频信息隐藏是将秘密数据嵌入数字化音频信号中人类听觉系统无法感知的成分，常见的做法是对选定的音频数据本身(空域)或描述音频信号特征的参数(变换域)进行替换或修改。视频信息隐藏是将秘密数据嵌入数字化视频信号中的过程，视频信号由连续的多帧图像信号和音频信号按一定编码方式组成，因此视频信息隐藏的原理类似于图形/图像信息隐藏或音频信息隐藏。数据库信息隐藏是利用数据库的结构来隐藏信息，通过在数据库中加入少量不需要的节点信息来隐藏数据。网络协议信息隐藏是利用网络层协议中某些未用到的格式字段或保留字段嵌入秘密数据。

④ 按嵌入域分类，主要分为时空域信息隐藏和变换域信息隐藏。时空域信息隐藏方法是直接用待隐藏的秘密数据替换载体数据中的冗余部分。最简单常用的时空域隐藏方法就是用秘密数据代替载体数据中的一些最不重要位(least significant bit，LSB)数据。常用的变换域信息隐藏方法主要包括离散傅里叶变换(discrete Fourier transform，DFT)域信息隐藏、离散余弦变换(discrete cosine transform，DCT)域信息隐藏和离散小波变换(discrete wavelet transform，DWT)域信息隐藏。

⑤ 按提取要求分类。如果在秘密数据的提取端，不需要利用原始载体数据提取秘密数据，则称这种方法为盲隐藏方法，否则称为非盲隐藏方法。非盲隐藏算法简单且提取成功率高，然而由于原始数据在某些应用环境中(如数据监控和跟踪)的获取难度较大，而且对于大容量原始载体数据(如视频数据)，即使获得原始载体数据，但由于数据容量巨大，要使用原始载体数据也不太容易实现。因此，目前最常见的是盲隐藏技术。

信息隐藏技术在军事通信、情报传递、隐私保护及版权保护等领域均具有广阔的应用前景。

1.2 音频信息隐藏关键技术

以音频为信息隐藏载体的音频信息隐藏技术，具有以下独特潜力。

① 人类听觉系统虽然很灵敏，但还是存在时间和频率掩蔽效应，通过适当的嵌入方法，可以用来掩盖数据嵌入带来的失真。

② 音频的处理不需要大量的计算，适合实时处理，而且语音和音频的录制也比较方便。

③ 在使用有线电话或无线电通信时，少量的噪声不会引起注意和不适。

④ 在过去几年中，图像是信息隐藏偏爱的载体，然而自有报道称恐怖分子用其传递信息以后，人们对图像的信息隐藏便比较警觉。相对而言，音频还是比较安全的载体。

1.2.1 秘密数据隐藏技术

音频信息隐藏就是以音频数据为载体，且在不影响载体音频数据的听觉效果和实用价值的情况下实现各类信息隐藏。按照秘密数据嵌入域，可将音频信息隐藏技术分为时空域音频信息隐藏、变换域音频信息隐藏和压缩域音频信息隐藏。

时空域音频信息隐藏方法是直接用待隐藏的秘密数据替换载体音频数据中的冗余部分或不重要部分。最简单常用的时空域音频信息隐藏方法就是用秘密数据代替载体数据中的一些最不重要的位数据。

常用的变换域方法主要包括傅里叶变换(Fourier transform，FT)域、离散余弦变换域、离散小波变换域、奇异值分解(singular value decomposition，SVD)域和倒谱域隐藏方法。

与时空域音频信息隐藏方法相比，变换域音频信息隐藏方法的优点如下。

① 在变换域中，秘密数据嵌入引起的载体音频的能量变化，可以分布到时空域的所有载体音频采样点上。

② 在载体音频数据的变换域中，可以结合人类听觉感知系统的掩蔽特性和心理声学特征来隐藏秘密数据。

③ 变换域方法可以建立在载体数据的某些压缩过程中，因此变换域音频信息隐藏方法可以抵抗诸如压缩、剪切等常见的信号处理攻击。

压缩域音频信息隐藏方法，也称为编码域算法，是指在对音频进行编码前或编码后将秘密数据嵌入音频数据中的方法。

目前，将秘密数据隐藏到数字音频信息载体中的方法主要有 LSB 算法[4]、回声隐藏算法[5]、相位编码算法[6,7]、扩频算法[8,9]、Patchwork 算法[10,11]和量化算法[12-14]。下面简要分析这些算法的研究现状。

(1) LSB 算法

Bender[4]于 1996 年首次将 LSB 算法引入音频信息隐藏中。该算法将音频样本每个采样点的最后一位替换为秘密数据位的数据，对于 16kHz 的音频载体，秘密数据嵌入容量可达 16Kbit/s。

为了增加 LSB 算法的安全性，2002 年 Cvejic 等[15]提出基于最小误差替换的方法在每个音频载体的最后 4 个 LSB 中嵌入秘密数据，这样就可将误差引入音频载体样本的更深层次，算法安全性增加的同时，容量也得到提高，在 44.1kHz 的音频样本中，秘密数据嵌入容量可达到 176.3Kbit/s。Cvejic 等[16,17]对 LSB 算法又做了改进，在 16 位位深的音频载体采样样本中，选取第 6 个 LSB 进行秘密数据的嵌入，并对其他采样样本点进行倒置，算法的嵌入容量尽管有所降低，但嵌入误差得到了很好的控制，鲁棒性也有较大提高。

2010 年，Ahmed 等[18]提出将秘密数据嵌入第 8 位最不重要位的 LSB 算法，在嵌入数据前对音频载体进行分析，秘密数据不嵌入载体的

近似静音段中，从而提高携密音频的透明度。

2011 年，Asad 等[19]提出利用 4 个最不重要位的方法在音频载体中嵌入秘密数据。2015 年，Bazyar 等[20]对 LSB 算法作出了更进一步的改进，在 16 位位深的音频载体信号中，利用前两位最重要位(most significant bit，MSB)来决定秘密数据更替 LSB 的位深，大大提高了秘密数据的嵌入容量。

2016 年，Shahadi 等[21]利用 Xinlix 公司的 FPGA 芯片实现了改进后的 LSB 算法，算法容量可达到音频载体容量的 25%，携密音频的信噪比可达到 48dB。

LSB 算法嵌入容量高，计算复杂度低，但该方法的鲁棒性较低，由于秘密数据直接加在音频载体信号上，常规的信号处理，如滤波、幅值调整或有损压缩都有可能破坏秘密数据。

(2) 回声隐藏算法

1996 年，Gruhl 等[22]第一次提出回声隐藏的概念。回声隐藏算法是一种利用人类听觉系统的时域掩蔽特性，通过在时域中引入回声，将秘密数据嵌入载体信号中的算法。图 1.1 是人类听觉系统典型的时域掩蔽区域图，可以看出人耳对一个高能量信号前后短时间发生的少量畸变无法感知。对于人类听觉系统来说，原始音频载体信号就像是从耳机里听到的声音，没有回声，而经过回声隐藏算法处理后的携密数字音频则像是原始音频经多次反射产生的回声。

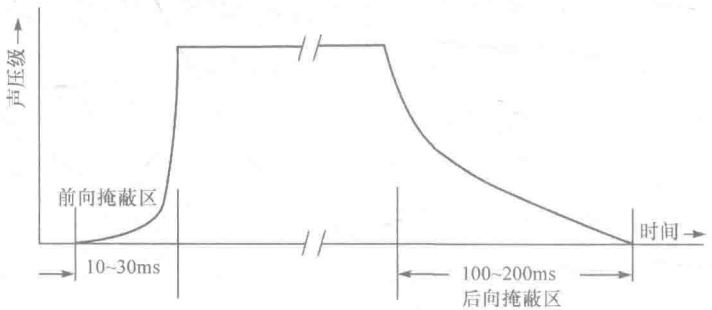

图 1.1 人耳时域掩蔽特性示意图