数字水印与信息安全技术研究

王俊杰 著

Research of Digital Watermarking and Information Security Technology

知识产权出版社
全国百佳图书出版单位

北京工商大学学术专著项目
[ZZCB2014-13]资助出版

数字水印与信息安全技术研究

王俊杰 著

SHUZI SHUIYIN YU
XINXI ANQUAN JISHU
YANJIU

知识产权出版社

图书在版编目（CIP）数据

数字水印与信息安全技术研究/王俊杰著.—北京 ：知识产权出版社, 2014.7
ISBN 978-7-5130-2841-7
Ⅰ.①数… Ⅱ.①王… Ⅲ.①电子计算机－密码术－研究
②信息安全－安全技术－研究 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2014)第 154481 号

内容提要

数字水印技术是近年来学术界研究的一个热点领域，它与信息安全、信息隐藏、数据加密等技术有密切的关系。全书共分 10 章，分别介绍了数字水印的基础知识、量化置乱与攻击、基于 DCT 变换的水印、基于 DWT 变换的水印、DCT 与 DWT 相结合的水印、基于矩阵奇异值分解的水印、基于 LSB 的鲁棒音频水印、脆弱水印、半脆弱水印、数字水印系统的应用等。本书取材广泛，内容新颖，充分反映了近几年来数字水印与信息安全领域最新的研究成果，具有很强的理论性与指导性。它既可以作为高等院校计算机、密码学、信息安全等专业本科生和研究生的教材和毕业设计指导书，又可以作为信息安全与保密通信、多媒体数字产品保护和电子商务安全等领域技术人员的参考书。

责任编辑：张 珑　　责任出版：谷 洋

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

数字水印与信息安全技术研究

王俊杰 著

出版发行：知识产权出版社有限责任公司　　网　址：http://www.ipph.cn;
http://www.laichushu.com
电　话：010-82004826　　社　址：北京市海淀区马甸南村 1 号
邮　编：100088
责编电话：010-28000860 转 8540　　责编邮箱：riantjade@sina.com
发行电话：010-82000860 转 8101/8029　　发行传真：010-82000893/82003279
印　刷：北京中献拓方科技发展有限公司　　经　销：各大网上书店、新华书店及相关专业书店
开　本：720mm×1000 mm　1/16　　印　张：13.5
版　次：2014 年 8 月第 1 版　　印　次：2014 年 8 月第 1 次印刷
字　数：240 千字　　定　价：50.00 元
ISBN 978-7-5130-2841-7

出版权专有　侵权必究

如有印装质量问题，　本社负责调换。

前　言

互联网和计算机技术的高速发展，加速了数字时代的到来，这使得文本、图像、音频和视频等数字媒体的存储与传播变得越来越容易，给人们的生活带来了极大的便利。但随之而来的盗版侵权、网络攻击等行为也越来越猖獗，严重侵犯了版权所有者的合法利益。因此，如何有效地保护数字媒体文件的真实性、完整性及版权信息的原始性已经成为当前形势下我们不得不面临的严峻问题。

以数据加密技术为代表的传统技术能够用于数字产品的内容保护。它将多媒体数据加密成密文后传送，能大大减小加密信息在传输时被截获的可能性，但它并不能完全解决问题。这是因为需要保密的信息经过加密后会成为一堆乱码，这非常容易引起攻击者的好奇心，从而加大被破解的可能性。而且数据只有在解密后才能正常使用，随着数据的解密，其保护作用也就随之消失。因此，加密技术已经不能从根本上解决多媒体信息的保密问题和版权保护问题。

数字水印技术就是在此背景下产生，它作为信息隐藏技术研究领域的重要分支，是实现版权保护的有效办法，受到了国内外学术界的高度关注，日渐成为信息安全领域的热点。数字水印技术是在被保护的数字多媒体信息中嵌入秘密水印信息来证明版权归属或跟踪侵权行为。嵌入的秘密水印信息既不能影响原有内容的价值和使用，也不能被人的听觉和视觉系统察觉，并且数字水印必须难以被清除和篡改。这表明数字水印技术必须具有较强的透明性、鲁棒性和安全性，必须能够经受常规的无意和恶意攻击。嵌入到载体中的水印信息可分为两种：一种是有意义水印，它可以是作者的签名、图像、公司图像、图标、特殊意义的文本、视频信号或生物特征等；另外一种是无意义水印，它的数据量小，实际应用价值不大。一般情况下，水印算法应该既能隐藏大量数据，又可以抵抗多种信道噪声、剪切等恶意攻击。但这两个指标是相互矛盾的，很难同时实现，在实际应用中，往往需要在它们之间寻找一个平衡点。

目前，世界上很多著名科研机构和高校都很重视数字水印技术的研究。哥伦比亚大学的ADVENT实验室、普渡大学图像和视频处理实验室下的多媒体安全研究组、日内瓦大学的数字水印研究组、代尔夫特大学的信息和通信理论组、MIT和Princeton大学等研究机构在数字水印领域都有深入的研究。除此之外，世界一些知名的企业也相继投入到数字水印技术的研究中来，如Philips、Macrovision、IBM、NEC、Digimarc、Sony等公司相继成立了水印技术研究组。当下流行的图像处理软件，如Auto CAD、Photoshop和Illustrator等都具备添加水印信息的功能。总的来说，国外数字水印技术的研究主导着数字水印技术的发展方向，具有

一定的研究深度和很强的现实意义。

我国科学界对数字水印技术也十分关注，国家对此方向的研究也越来越重视，当前许多研究机构和大学也参与到该领域的研究中。全国信息隐藏学术研讨会是对数字水印的研究活动中最具代表性的一个，它是我国信息安全领域很重要的一个学术交流会议，极大地促进了我国信息隐藏技术的应用与研究。自从第一届全国信息隐藏学术研讨会于1999年在北京电子技术应用研究所召开之后，时至今日该会已经举办了十一次。其中，2013年10月在西安举办的第十一届大会出现了很多优秀的文章，并取得了很多研究成果，得到了学术界的肯定。

国内一些研究单位对此前沿领域也倾注了极大的热情，有些还得到了国家相关基金项目，如“973计划”“863计划”、国家自然科学等基金项目的大力支持。一些商业化的数字水印产品也推向了市场，如上海阿须数码技术有限公司是国内专门从事数字水印研究与开发的公司，目前已申请了多项国际、国内数字水印方面的技术专利。由于我国对数字水印技术的研究起步相对比较晚，与国外的研究相比，仍然有一定差距。因此，在数字水印技术的相关领域上，我们仍有许多研究需要深入下去。

本书共分10章。第1章是绪论，简要地介绍了数字水印的研究背景，研究历史、现状、将来的发展趋势，基于水印技术的保密通信意义，水印的特征与分类，系统的性能评估以及数字水印研究需要解决的主要问题。第2章主要介绍了数字水印的基础知识，包括人类听觉系统模型（HAS），采用量化方法嵌入水印信息的原理，水印的置乱技术，攻击方法等。第3、4、5章分别研究了基于DCT变换的水印算法，基于DWT域的音频水印算法和一种DWT与DCT相结合的水印算法，并对这3种算法的性能进行了比较。第6章研究了基于矩阵奇异值分解的水印。第7章研究了基于LSB的鲁棒音频水印算法。第8、9章分别研究了用于完整性认证的脆弱水印、用于内容认证的半脆弱水印。第10章研究了数字水印系统在保密通信和电子印章系统中的应用。

编写本书的目的是向广大读者介绍数字水印的各项关键技术，以及一些经典的水印算法与应用，使读者对数字水印有一个全面、系统的认识，为以后的学习和研究工作打下一定的基础。

本书的研究撰写和出版得到了北京工商大学网络中心的支持，得到了很多朋友、同仁的帮助，得到了知识产权出版社编辑们的帮助，在此深表感谢。

由于时间仓促、作者的水平有限，书中难免会有不足之处，敬请读者朋友们批评指正。

作者

2014年4月于北京

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第1章 绪 论

1.1 研究的背景

近年来，随着网络通信和多媒体技术的飞速发展，人们的学习和生活越来越方便，但与此同时，网络环境下的信息安全问题也日益显露出来。因此，世界上主要的发达国家都在积极地研究实用性强、安全性高、功能完善的保密通信系统，一些著名的情报部门和机构更是积极应用隐密通信以确保国家政治、军事和经济等信息安全可靠地传输和共享。在我国，许多大学和研究机构也在积极地进行这方面的研究和探索。目前，常用的保密通信方法主要有两种。

第一种方法：数字水印技术。

数字水印技术是指将秘密水印信息嵌入到公开的载体信息中（包括图像、声音、视频等信号），使其不易被攻击者发现，从而实现文件的真伪鉴别、版权保护、保密通信等。嵌入的秘密水印信息隐藏于公开的载体文件中，不会影响其完整性，也不会影响原始载体文件的视觉与听觉效果。因此，它不易引起攻击者的注意，从而达到保密通信的目的。由于具有冗余特性的载体非常丰富，这在客观上增强了数字水印技术的隐蔽性和可行性。嵌入的秘密水印信息一般是证明版权归属或跟踪侵权行为的信息，如公司的图标，作者的签章或序列号、有意义的文本等。

第二种方法：数字加密技术。

数字加密技术就是按确定的加密变换方法（加密算法），对需要保护的数据（即明文）作出一定的处理，使它变换为难以识读的数据（即密文）。加密的基本功能包括：防止不速之客查看机密的数据文件；防止特权用户（如系统管理员）查看私人数据文件；防止机密数据被泄露或篡改；使入侵者不能轻易地查找一个系统文件。

为了使加密算法能被多人共用，在加密过程中又引入了一个可变量——加密密钥。这样，不改变加密算法，只要按照需要改变密钥也能将相同的明文加密成不同的密文，但是没有密钥的攻击者就不能正确理解通信的内容信息。

由于信息加密后通常是一堆乱码，这非常容易引起攻击者的怀疑和破解欲望，即使攻击者不能破解加密后的信息，也能成功地拦截加密后的信息或干扰通信的正常进行。因此，数据加密在防止他人从中得到信息的同时，也暴露了秘密水印信息存在这一根本事实。在实际的应用中，在能用水印技术进行保密通信的情况下，应该尽量少用数字加密技术。

Simmons等提出的“囚犯问题”（图1-1）就是基于水印技术的保密通信的原型[1, 2]。由于两个囚犯Bob和Alice分别被关押在监狱的不同牢房，他们之间希望通过一种隐蔽的方式交换信息，但交换信息必须要通过看守Wendy的严密检查。因此，他们要想办法在不引起看守者Wendy怀疑的情况下，在看似正常的信息中，传递他们之间的秘密信息。如果他们采用加密方法进行通信容易引起Wendy的怀疑，因为加密信息是乱码。

一个有用的方法是将秘密的水印信息隐藏在看似普通正常的公开载体信息中。这就如同自然界中，生物利用保护色巧妙地将自己隐藏于周围环境中，使自己不会被天敌发现和攻击一样[3, 4]。这是传统的加密通信技术不具备的优势，也是本研究最根本的出发点。如果嵌入前对秘密的水印信息进行加密，然后将加密后的水印信息嵌入到公开的载体信息中，这无形中增加了攻击者截取秘密信息的难度，嵌有秘密水印信息的公开载体信息将具备更强的抗攻击能力[5]，从而为基于数字水印技术的保密通信提供了一个崭新的方法。

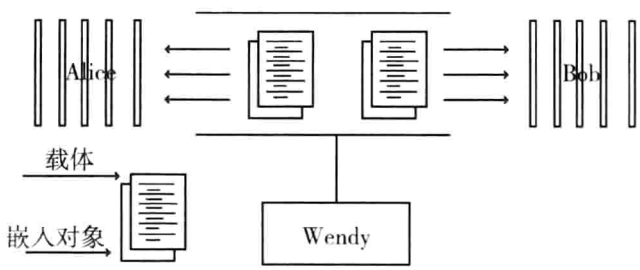

图1-1　囚犯问题

从使用的角度出发，应用于保密通信的数字水印技术应从以下两个方面来考虑：

第一，在没有遭受攻击的前提下，隐藏于公开载体信息中的秘密水印信息不会使公开载体信息在视觉或者听觉上存在明显的失真，且在受到攻击以后，攻击者仍然无法感觉到隐藏于公开载体信息中的秘密水印信息的存在。

第二，对提取出来的秘密水印信息来说，在经历了各种有意或者恶意的攻击以后，仍然能从视觉上或者听觉上分辨出它的含义[6, 7]。

1.2 数字水印研究的历史与现状

早在13世纪，意大利的Fabriano镇就出现了纸水印，这些纸水印是通过在纸模中加细线模板制造出来的，在存在细线的区域纸就会略微薄一些，也会更透明一些。到了18世纪，在欧美国家中，纸水印已经变得相当实用了。由于纸水印的存在既不影响正常使用，也不影响美观。因此它的应用越来越广泛。造纸是中国古代的四大发明之一，同时中国也是世界上最早使用纸币的国家。宋真宗在位时，四川民间就发明了交子，发行于北宋前期（1023年）的成都。交子的正面都有票人的印记，有密码画押，票面金额在使用时填写，可以兑换和自由流通，交子上的印文信息既包含了水印技术也包含了消隐技术。

数字水印技术的研究可以追溯到20世纪50年代。当时Muzac公司的埃米利·希姆布鲁克（Emil Hembrooke）为带有水印的音乐作品填写了一份题为“声音和相似信号的辨别”的专利，此发明使得原创音乐的辨认成为可能，从而建立一套阻止盗版的方法。

目前，世界上很多国家都非常重视数字水印技术的研究工作，许多知名的研究机构或者知名的公司，如日本的NEC公司、Sony公司、美国麻省理工学院的多媒体实验室、伊利诺伊大学、美国空军研究院、朗讯公司贝尔实验室、荷兰飞利浦公司等都在从事这一领域的相关研究工作，也提出了很多先进的算法。为了保证鲁棒性和更好的HVS特性，Gao等利用广义的统计直方图，构建了基于直方图的无损水印算法框架，该算法对于JPEG（Joint Photographic Experts Group，联合图像专家组的缩写，文件后辍名为“.jpg”或“.jpeg”）压缩等攻击表现出很好的性能[8]。Hazem等人在像素水印模型的基础上，提出了一种选择性算法，并将其推广至彩色图像。实验结果表明，该算法在视觉效果上具有较好的不可感知性，定量计算得到的PSNR也较高，而且该算法还具有很好的安全性[9]。Bas等提出的基于内容的图像水印算法利用了不变点的内容，将水印嵌入至Delaunay三角形内，算法对几何攻击具有很好的鲁棒性[10]。

国内也有不少研究机构、高等院校、公司等正在从事水印方面的研究。从目前的情况来看，我国在该领域的研究也取得了一定的成果，有自己独特的思路。尺度不变特征转换（Scale-Invariant Feature Transform，SIFT），是用于图像处理领域的一种描述子，用来侦测与描述影像中的局部性特征。这种描述具有尺度不变性，可在图像中检测出关键点，并提取出其位置、尺度、旋转不变量。李雷达等在空域内结合尺度不变特征转换生成了圆形的鲁棒区域，可以有

效抵抗几何攻击及滤波、压缩等信号处理攻击[11]。景丽等则结合SIFT算法，将秘密水印信息嵌入到离散小波变换的低频系数中，利用SIFT算子的不变特性，进行了仿射变换的校正和估计，他们提出来的算法可以有效抵抗仿射变换等攻击[12]。张翼等对图像进行归一化处理，取得了水印的同步信息，因而算法对常见的几何攻击非常有效[13]。

国内也有一些商业化的数字水印产品推向市场，如上海阿须数码技术有限公司，它是国内专门从事数字水印研究与开发的公司，目前已申请了多项国际、国内数字水印方面的技术专利。2000年6月成立的成都宇飞信息工程有限责任公司，是一家专门从事以基于内容的计算机信息安全软件技术产品研发、生产和推广应用的高科技企业。该公司的数字水印技术的研究、开发及商业化应用已经处于国际领先水平。在成功开发出音频、视频、图像及文本数字水印技术平台的基础上，率先开发出了国内外第一个印刷打印数字水印软件，制定了数字水印第一个企业标准，承担了印刷数字水印技术国家标准的起草，第一个获得了国家科技创新基金对数字水印商业化应用项目的资助，第一个将数字水印在信息安全、防伪溯源、版权保护、电子商务和电子政务等领域投入了商业化应用。目前，该公司独立开发、具有完全自主知识产权的“宇飞数字水印”已广泛用于烟、酒、药品、食品、音像制品等名优产品的商标、包装和各种证书、证照，税务发票、邮票及重要文体场馆门票等印刷品的防伪及版权保护。基于数字水印的电子政务、电子商务和电子图书馆等计算机信息的防篡改、防拷贝及来源认证、身份认证系统也获得广大需求商的普遍认同，并且取得了良好的社会效益和经济效益。

南京师范大学朱长青教授研发的“吉印”地理空间数据数字水印系统，能够自动生成图片、文字等水印信息，支持多种数据类型及海量数据，能够实现多用户、多文件、多图层批量处理。该产品在军队和地方的测绘、地理信息、国土资源、规划、导航、地质、水利、城市管理、公安、宣传、出版及GIS软件生产商等多个领域。

该系统是基于4项地理信息安全方面的国家级项目成果和20项专利及软件著作权研发出来的，拥有完全的自主知识产权，具有如下特点。

（1）该系统适用于矢量数据、影像数据、栅格地图数据、数字高程模型数据、三维模型数据、PDF数据、视频数据等地理信息的水印嵌入和检测，也适用于普通的数字化照片等。

（2）该系统能够嵌入版权信息、用户信息等水印信息，水印信息量没有限制。

此为试读，需要完整PDF请访问：www.ertongbook.com

（3）水印系统能够嵌入包括用户信息和版权信息的水印信息，且不易被用户发现或删除。

（4）数据嵌入水印信息时能够进行批量处理，对批量数据的文件数没有限制。

“吉印”地理空间信息数字水印系统的性能指标如下：

（1）采用盲水印算法，水印检测时不需要原始数据，检测虚警概率不超过0.1‰；

（2）矢量的小数据量（大于等于50个点）的数据图层可以正确的嵌入和检测水印信息；

（3）嵌入水印信息的数字产品能够保持好的数据精度，保证嵌入水印后数据的精度能满足各种应用的需求，矢量数据图上误差不超过0.2mm；

（4）系统能有效地抵抗数据的格式转换、裁剪、噪声、压缩、删除、增加、平移、旋转、重采样等攻击；

（5）系统嵌入和检测的效率在目前主流配置下不低于10M/s。

这些水印产品的出现标志着我国的数字水印技术的研究已经取得了一定的成果，与国外先进水平的差距正在缩小。这些走上商业化和实用化的产品，在一定程度上推动了国内数字水印技术的蓬勃发展。

1.3 重要概念与术语

载体信号：它充当数字水印信息的载体，即：数字水印信息会嵌入到里面，它可以是受保护的数字媒体产品，也可以是在公开信道中传输的多媒体数据（包括数字图像、音频、视频等数字产品）。

水印信息：是指嵌入到原始的载体信息中，真正要传输的信息。水印信息可以用来认证数字产品来源的真实性，确定版权所有者，提供关于数字产品的其他附加信息，确认所有权认证和跟踪侵权行为。如今，数字水印在数据的分级访问、数字产品的鉴定篡改、数据检测与跟踪、商业和视频广播、数字媒体的服务付费、电子商务认证鉴定等方面的应用非常广泛。

密钥（key）：在秘密水印信息嵌入到公开载体信号，以及从公开载体信号提取秘密水印信息时，都需要用到一些额外的参数，其目的是保护秘密水印信息的安全。这些额外的参数就是密钥。它是在明文转换为密文和随后的密文转换为明文的算法中输入的一组数据。密钥分为对称密钥与非对称密钥

两种类型。

对称密钥加密：又称私钥加密或会话密钥加密算法，是指发送方和接收方使用同一个密钥去加密和解密数据。其优点是加密和解密的速度快，适合于对大量的数据进行加密；缺点是密钥管理困难。

非对称密钥加密：又称公钥密钥加密。它需要使用不同的密钥来分别完成加密和解密操作。其中，公开密钥可以公开发布，私用密钥则由用户自己保存，需要严格保密。信息发送时，发送方用公开密钥加密，在接收方接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度要比对称密钥加密慢很多。

综合考虑对称密钥加密和非对称密钥加密的优点和缺点，在实际的应用中，人们通常是将两者结合在一起使用。例如：对称密钥加密系统用于加密大量的数据信息，而非对称密钥（公开密钥）加密系统则用于加密密钥，这是因为加密密钥的数据量很小。

信号的嵌入：利用水印的嵌入算法，将秘密的水印信息加载到公开的载体信号中的过程。

信道噪声：网络在传输嵌入了秘密水印的混合载体时，可能会遇到各种复杂的情况，如信号降质，失真，压缩或其他攻击等。把这种针对信号的各种失真和攻击称之为信道噪声。信道噪声能够干扰通信效果，降低通信的可靠性。

1.4 数字水印研究的常见方法

根据嵌入秘密水印信息时，对公开载体信号处理的差异，可将数字水印技术分为空间域（时域）水印技术和变换域（频域）水印技术。

空间域（时域）水印技术：直接修改公开载体信号的值（如修改公开载体信号的最低位），以完成秘密水印信息的嵌入。该类方法对压缩和滤波有较好的鲁棒性，但嵌入的水印信息不能太多，否则影响感官质量[14]。

变换域（频域）水印技术：它首先对公开载体信号的采样数据进行适当的变换，该变换既可以全局进行，也可以分段进行；然后将秘密水印信息嵌入到频域选定的系数上，即：通过修改原始载体信号的频域系数来达到嵌入秘密水印信息的目的；嵌入秘密水印信息以后，在对载体信号进行相应的反变换，即可生成含有秘密水印信息的公开载体信息。提取水印时，需要先对含有水印的公开载体信号进行相应的变换，然后才能提取出秘密的水印信息。

1.4.1 时域方法

时域方法本身简单易实现，它通过对水印数据和嵌入过程进行加密，安全性可以得到保证，而且水印嵌入和提取算法简单，速度快。但它对信道的干扰及数据操作的抵抗能力很差。到目前为止，比较成熟的音频水印技术有四种：最不重要位法、相位编码方法（Phase Coding）、回声隐藏方法和扩展频谱方法。

1.扩频方法

扩频水印是Cox发明的一种鲁棒数字水印技术，其基本思想是借鉴扩频通信以高传输带宽换取低传输信噪比的思想，将1bit的水印信息隐藏在多个载体系数中，从而达到扩频和降低传输信噪比的目的。

扩频通信方式有很多，常用的有直接序列扩频编码方法（Direct Sequence Spread Spectrum Encoding，DSSS）。所谓直接序列扩频，就是在发送端直接用具有高码率的扩频码序列对信息比特流进行调制，从而扩展信号的频谱；在接收端，用与发送端相同的扩频码序列进行相关解扩，把展宽的扩频信号恢复成原始信息。一种直接序列扩频技术是使用异或运算将数字信息流与扩展码位流结合起来。例如：在扩频通信系统的发送端，如果要发送的信息是“1”，那么就用“1010010011”代替；如果要发送的信息是“0”，那么就用“0100101100”代替，从而实现了扩频。在扩频通信系统的接收端，如果收到的信息是“1010010011”，就恢复成“1”，如果收到的信息是“0100101100”，就恢复成“0”，从而完成解扩。这样信源速率就被提高了10倍，同时处理增益也达到了10dB以上，从而有效地提高了信噪比（图1-2，图1-3）。

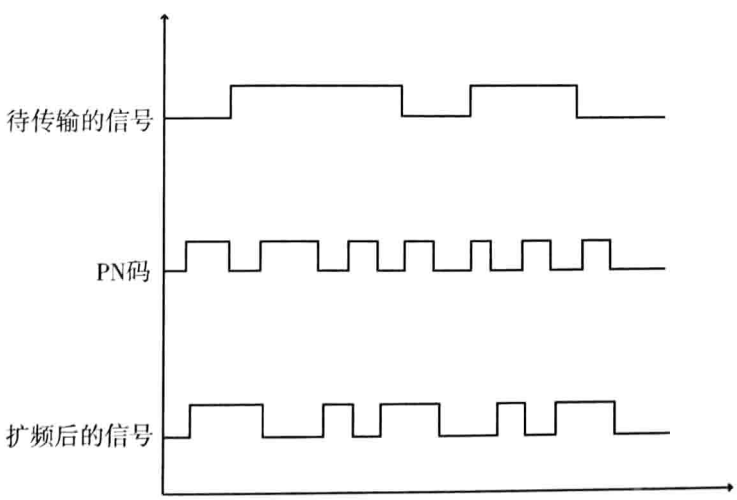

图1-2 直接序列扩频通信的原理图(发送端)

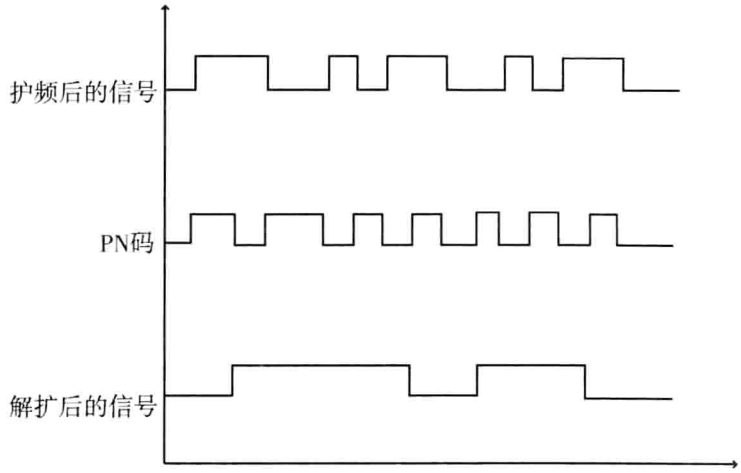

图1-3　直接序列扩频通信的原理图(接收端)

直接序列扩频通信中功率密度和频谱密度的变化如图1-4~图1-7所示。原始信号的功率密度和频谱宽度如图1-4所示，它是有用的信号，也是等待传输的信号。图1-5是扩频之后的信号，从图中可以看出，扩频以后信号的功率密度下降了。

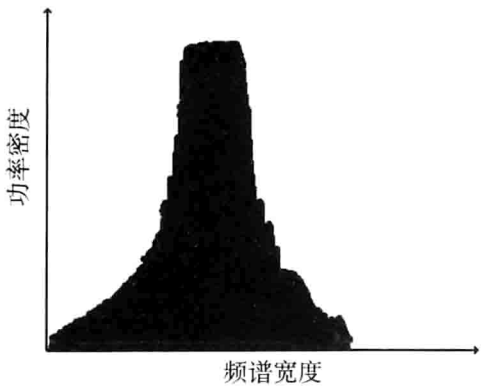

图1-4　原始信号

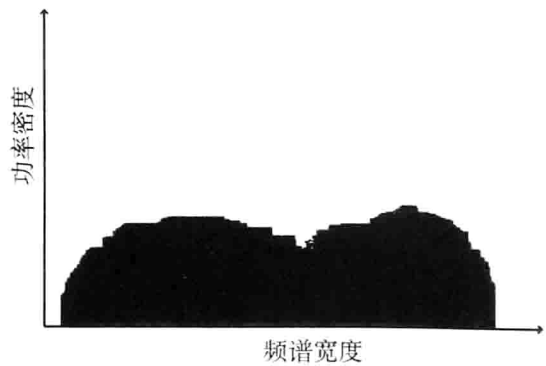

图1-5　扩频后的信号

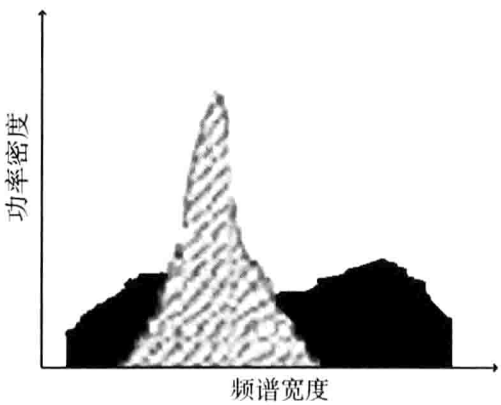

图1-6　传输中受到噪声干扰的信号

图1-7　解调后的信号

图1-6表示扩频以后的信号在传输过程中受到了噪声信号的干扰。从图1-7可以看出，解调以后噪声信号的功率密度下降，有用信号的功率密度上升，原始信号被恢复。

直接序列扩频之所以应用很广泛，主要是因为它具有很多优点，具体如下。

（1）隐蔽性好。因为信号在很宽的频带上被扩展，单位带宽上的功率很小，即信号功率谱密度很低，信号淹没在白噪声之中，令人难以发现信号的存在，加之不知扩频编码，很难拾取有用信号，而极低的功率谱密度，也很少对于其他电讯设备构成干扰。

（2）抗多径干扰。无线通信中抗多径干扰一直是难以解决的问题，利用扩频编码之间的相关特性，在接收端可以用相关技术从多径信号中提取分离出最强的有用信号，也可把多个路径来的同一码序列的波形相加使之得到加强，从而达到有效的抗多径干扰。

（3）抗干扰性强。抗干扰是扩频通信主要特性之一，如信号扩频宽度为100倍，窄带干扰基本上不起作用，而宽带干扰的强度降低为1/100，如要保持原干扰强度，则需加大100倍总功率，这实质上是难以实现的。因信号接收需要扩频编码进行相关解扩处理才能得到，所以即使以同类型信号进行干扰，在不知道信号的扩频码的情况下，由于不同扩频编码之间的不同的相关性，干扰也不起作用。正因为扩频技术抗干扰性强，美国军方在海湾战争等场合广泛采用扩频技术的无线网桥来连接分布在不同区域的计算机网络。

（4）直扩通信速率高。直扩通信速率可达2Mbps、8Mbps、11Mbps，无需申请频率资源，建网简单，网络性能好。在802.15.4通信标准中，要求的无线通信的速度是250kbps，所以，CC2430高频部分也是使用这个通信速度。

（5）易于实现码分多址（Code Division Multiple Access，CDMA）。直扩通信占用宽带频谱资源通信，改善了抗干扰能力，是否浪费了频段？事实正好相反，扩频通信提高了频带的利用率。正是由于直扩通信要用扩频编码进行扩频调制发送，而信号接收需要用相同的扩频编码作相关解扩才能得到，这就为频率复用和多址通信提供了基础。充分利用不同码型的扩频编码之间的相关特性，分配给不同用户不同的扩频编码，就可以区别不同用户的信号，众多用户只要配对使用自己的扩频编码，就可以互不干扰地同时使用同一频率通信，从而实现了频率复用，使拥挤的频谱得到充分利用。发送者可用不同的扩频编码，分别向不同的接收者发送数据；同样，接收者用不同的扩频编码，就可以收到不同的发送者送来的数据，实现了多址通信。美国国家航天管理局（NASA）的技术报告指出：采

用扩频通信提高了频谱利用率。另外，扩频码分多址还易于解决随时增加新用户的问题。

Boney等提出了一种适用于音频水印的扩频方法[15]。他们选用的是一个伪随机序列，且为了利用HAS的长期或短期掩蔽效应，对该序列进行若干级的滤波。为利用HAS的长期掩蔽效应，对每个512点采样的重叠块，计算出它的掩蔽阈值，并近似地采用一个10阶的全极点滤波器，对PN序列进行滤波。利用短期掩蔽效应，即根据信号相应的时变能量，对滤波后的PN序列做加权处理。这样在音频信号能量低的地方可削弱水印。另外，水印还要经过低通滤波，即用完全音频压缩和解压实现低通滤波，以保证水印可抵御音频压缩。嵌入水印的高频部分，可使水印更好地从未经压缩的音频片段中检测出来，但压缩过程会将它去除掉。作者用“低频水印”和“误码水印”来表示水印的两个空间成分。利用原始信息和PN序列，采用相关性方法，则可通过假设检验将水印提取出来。实验结果显示了该方法对MP3音频编码、粗糙的PCM量化和附加噪声的鲁棒性。

2.最低有效位法

最低有效位（Least Significant Bit，LSB）法是一种最简单的数据嵌入方法。任何的秘密数据都可以看作是一串二进制位流，而音频文件的每一个采样数据也是用二进制数来表示。这样，就可以将每一个采样值的最不重要位，多数情况下为最低位，用代表秘密数据的二进制位替换，以达到在音频信号中编码进秘密数据的目的。

为了加大对秘密数据攻击的难度，可以用一段伪随机序列来控制嵌入秘密二进制位的位置[16]。伪随机信号可以由伪随机序列发生器的初始值来产生。这样在收发双方只需要秘密地传送一个初始值（作为密钥），而不需要传送整个伪随机序列值。只要能保证合法用户才能得到该密钥，则根据Kerchoff法则可知系统是安全的。任何不知道密钥的第三方都不能正确的提取出秘密信息。

最低有效位方法本身简单易实现；音频信号里可编码的数据量大；采用流加密方式分别对数据本身和嵌入过程进行加密，其安全性完全依赖于密钥；信息嵌入和提取算法简单，速度快。但它主要的也是最致命的缺点是对信道干扰及数据操作的抵抗力很差。事实上，信道干扰、数据压缩、滤波、重采样等都会破坏编码信息。

为了提高鲁棒性，可将秘密数据位嵌入到载体数据的较高位。但这样带来的结果是大大降低了数据隐藏的隐蔽性（因为人耳对低频信号更敏感）。为了改善这一点，可以在嵌入过程中根据音频的能量进行数据嵌入位选择的自适应，当然

此为试读，需要完整PDF请访问：www.ertongbook.com