

## 摘 要

多输入多输出 (MIMO) 技术在通信系统的频谱利用率和信道容量方面性能卓越, 并有效地对抗无线信道衰落的影响, 将成为第四代移动通信系统的关键技术之一。MIMO 技术的采用促进了数字音频、数字图像、数字影像等多媒体产品在无线通信领域的应用。与此同时, 传输中的各种多媒体信息的版权问题面临着严峻的考验。如何使 MIMO 无线通信信道中多媒体信息安全地传输, 已成为非常紧迫的问题, 也是本文的主要研究内容。

本文将数字水印技术应用于 MIMO 无线通信系统中, 以实现多媒体作品版权的保护。仿真实验结果得出这是一个可行并且有效地安全保护无线信道中多媒体作品的方法。

本文首先对数字水印技术进行研究, 采用混沌置乱和 Turbo 编码的水印预处理技术使数字水印具有自我检错能力, 增强其鲁棒性; 而采用小波变换低频域的均值量化嵌入算法能使接收端实现数字水印的盲提取。然后对 MIMO 系统的几种关键技术进行分析: 信道容量方面, 比较不同收发天线数目的通信系统的信道增益, 结果显示多天线技术是信道容量增加的关键; 无线信道衰落方面, 对瑞利衰落信道、莱斯衰落信道和天线相关信道分别进行分析, 这三个信道都对信道的增益产生了负面的影响; 重点研究空时编码技术, 并仿真比较三种空时编码技术对抗各种衰落的性能, 结果表明空时格型码技术在三种信道中均是性能最佳的空时编码, 得出多媒体产品在采用空时格型码编译码的 MIMO 系统中传输能更好的保证信息的安全。最后将数字水印技术应用于 MIMO 系统, 整个系统采用以上分析提出的方式, 即水印采用 Turbo 编码与均值量化嵌入相结合的嵌入算法, MIMO 系统的建立采用空时格型码技术, 通过 MATLAB 平台的仿真实验, 在不同的无线信道中以及各种攻击下, 均可以得到不可见性和鲁棒性兼备的数字水印, 并且实现了接收端的盲提取。

文章采取的方案使在 MIMO 无线信道中传输的多媒体产品嵌有的版权信息具有高鲁棒性, 同时兼顾了该版权信息的不可见性和提取的方便性, 能够适用于第四代移动通信这样开放的环境中对多媒体信息进行安全保护。

**关键词:** 数字水印, Turbo 码, MIMO, 无线衰落信道, 空时格型码

## Abstract

Multiple-Input Multiple-Output (MIMO) system achieves high performance in the area of frequency spectrum usage and channel capacity, and it effectively against the effect of wireless fading channel. MIMO system has become the most superior and important technology in the 4th generation of mobile communication system. By using MIMO technology, the digital audios, images and other multi-media products can be transferred in wider application range. Meanwhile, copyright or patent of those multi-media information during the transaction is facing challenges. This paper is drawn to evaluate and analyze the security issue transmitted by MIMO system which has been paid a great attention in modern society.

This article focuses on the application of digital watermarking technology in MIMO system, so as to achieve the copyright protection of multi-media works. The simulation results prove that this is an achievement method and effectively secure the multi-media in the wireless channel.

This paper firstly concentrate on the study of digital watermarking technology, making use of the good performance of the chaos and Turbo coding technology with self-testing ability of digital watermarking so as to increase the robustness. In this algorithm, mean quantization of low frequency range by DWT is used to detect the digital watermark without original host image. Then study on the key technique of MIMO system: channel capacity, by comparing with the channel gain in different numbers of antenna system, the results show that MIMO system is the key to increase information capability; in the fading of wireless channel, analysis is drawn at Rayleigh Fading Channel, Rice fading channel and coherent antenna channel, each fading channel has increase the side effects of channel gain; much attention has been paid on STC, and the simulation compare three space coding technology to against the fade of wireless channel. The results shows that STTC works the best among all of them, and by using the STTC encoding and decoding during the transmission of MIMO is enhance the information security system. Finally by using the digital watermarking technology into the MIMO system, the system according to the above analysis which is embedding digital watermarking by Turbo code and mean

quantization, MIMO system uses STTC. Through MATLAB platform, the simulation results show that digital watermarking which has transmitted in wireless channel is well invisibility and strong robustness so as to achieve the blind detection in the receiver under different wireless channels and attacks.

The algorithm has pointed out the high robustness of copyright information which embedded in multi-media products while transmitting in MIMO channel, and enhanced the invisibility of watermarking and extracting convenience, can be used in the 4th generation of mobile communication in the open environment so as to protect the multi-media information.

**Key word:** Digital watermarking, Turbo code, MIMO, Wireless fading channel, STTC

## 独创性声明

本人声明，所呈交的论文是本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得武汉理工大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

签名：罗静 日期：2009.12.7

## 关于论文使用授权的说明

本人完全了解武汉理工大学有关保留、使用学位论文的规定，即学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权武汉理工大学可以将本学位论文的全部内容编入有关数据库进行检索，可以采用影印、缩印或其他复制手段保存或汇编本学位论文。同时授权经武汉理工大学认可的国家有关机构或论文数据库使用或收录本学位论文，并向社会公众提供信息服务。

(保密的论文在解密后应遵守此规定)

研究生(签名)：罗静 导师(签名)：和志 日期 2009.12.7

# 第 1 章 绪论

## 1.1 课题研究背景和意义

现今，第三代移动通信（3rd Generation, 3G）系统已经被广泛应用于大带宽高速度的无线通信领域。3G 手机能同电脑一样接入网络浏览网页、下载文件、玩网络游戏、甚至视频聊天等等网上业务。紧接着将会出现的下一代移动通信技术 4G（4th Generation）将是一种传输速率更快、业务类型更全的无线通信技术。阿尔卡特朗讯公司的 CTO 奥利弗表示，3G 会给用户带来几兆的带宽，而 4G 能带来 100 兆以上的带宽，可以享受高清视频电视和各种多媒体应用，是移动通信业的一场革命。

MIMO（Multiple-Input Multiple-Output, 多输入多输出）技术被视为第四代移动通信技术的重要组成部分，已经受到通信界的强烈关注。它能充分利用空间资源，在不增加系统带宽和天线总发射功率的情况下，有效对抗无线信道衰落的影响，大大提高系统的频带利用率和信道容量<sup>[1]</sup>。日本 NTTDoCoMo 公司已经通过 4×4 和 12×12 多天线 MIMO 技术在 100MHz 带宽下分别验证了 1Gbit/s（室外试验）和 5Gbit/s 的峰值传输速率<sup>[2]</sup>。在如此大带宽和传输速率的信道上，数字多媒体产品（如数字图像、数字音频、数字视频等）能更快捷地传输，因此，4G 时代将是数字多媒体信息与无线移动通信相结合飞速发展的时代。同时，它也带来了十分严重的问题——多媒体版权安全的问题。

一些不法分子恶意拷贝并且传播有版权的数字产品，或者攻击并篡改信息传输中有意义的数据等等都给产品所有者带来了经济上的巨大损失。据美国唱片行业协会估计，全世界每年因盗版而造成的直接经济损失高达 50 亿美元；美国电影行业协会的统计估计，盗版使美国电影业的年收入减少了 25 亿美元<sup>[3]</sup>。因此，如何有效地保护数字多媒体产品版权和维护作者的合法权益是产业界十分关注的问题。

数字水印技术将数字产品的版权信息嵌入产品文件中，但不会引起原始产品文件的完整性和视觉上的改变。它与传统的密码技术相比，优势在于它不仅能在信息从发送者到接收者的传输过程中进行数据的加密保护，

还能帮助产品所有者跟踪监视合法接收者如何处理能够使用的数据，这样，产品的合法用户只能使用产品，而不能拷贝产品和传播副本。用水印技术保护数字产品的版权及维护其真实性和追踪盗版具有良好的应用前景。

本课题将数字水印技术应用于 MIMO 无线通信系统中，保护数字多媒体产品的版权，提高数字产品在无线传输过程中的安全性。

## 1.2 MIMO 技术的研究现状

1985 年 Salz 对加性噪声 MIMO 信道中存在耦合问题的改进<sup>[4]</sup>以及 1996 年 Foschini 的贝尔实验室分层空时(Bell Layered Space-Time, BLAST)编码结构的建立<sup>[5]</sup>，为 MIMO 无线通信技术的信息奠定了坚实的理论基础；而 Wolniansky 等人在 Foschini 理论的基础上对垂直-贝尔实验室分层空时(V-BLAST)编码进行的试验结果表明多个天线的通信结构不占用额外频谱带宽也能够有效地提高信道容量<sup>[6]</sup>，这一研究成果引发了无线通信领域对 MIMO 技术研究的热潮。而由于 MIMO 系统是一个时变、非平稳系统，对其基本理论、关键技术目前尚有大量问题需要研究，主要集中在发送分集和空时编码方面的研究。

空时编码(Space-Time Codes, STC)技术已经突破了智能天线技术的自适应信号处理方式，使 MIMO 无线通信系统在不损失带宽的前提下获得优良的性能增益<sup>[7]</sup>，是国内外无线通信研究机构和学者们研究的热点。紧随着 Foschini 提出贝尔实验室分层空时码之后，Tarokh 等人将网格编码调制(TCM)技术结合发送分集提出了空时网格码(STTC)<sup>[8]</sup>，Alamouti 为了解决空时网格码复杂的译码过程提出了一种简单的双路分集发射方案<sup>[9]</sup>，并被演化为基于正交概念的空时分组码(STBC)。大多数研究都建立在非频率选择衰落的信道上，而实际上并非如此。最近几年，学者们纷纷将眼光投向频率域上的编码，将正交频分复用(Orthogonal Frequency Divided Modulation, OFDM)技术在抗频率选择性衰落上的优势与 MIMO 相结合形成空-时-频(STF)编码技术<sup>[10]</sup>，能够使 MIMO-OFDM 系统在频率选择性衰落中获得最大的分集增益，其值等于收发天线数目及可分离多径数目三者的乘积<sup>[11]</sup>。

科研机构中朗讯科技的贝尔实验室分层的空时技术是移动通信方面

领先的 MIMO 应用技术。2002 年 10 月，世界上第一颗 BLAST 芯片在朗讯公司贝尔实验室问世，贝尔实验室研究设计小组宣布推出了业内第一款结合了贝尔实验室空时分层 MIMO 技术的芯片，这一芯片支持最高 4×4 的天线布局，可处理的最高数据速率达到 19.2Mbps。该技术用于移动通信，BLAST 芯片使终端能够在 3G 移动网络中接收每秒 19.2 兆比特的数据，现在，朗讯科技已经开始将此 BLAST 芯片应用到其 Flexent OneBTS 家族的系列基站中，同时还计划授权终端制造商使用该 BLAST 芯片，以提高无线 3G 数据终端支持高速数据接入的能力。

MIMO 技术已成为未来无线通信系统的框架技术，以它能充分利用空间资源获得高且可靠的频谱利用率的优点，具有巨大的发展潜力。

### 1.3 数字水印技术的研究现状

1996 年在英国剑桥召开的数字水印领域的第一次学术研讨会标志着数字水印技术作为一门新的学科诞生了。如今，数字水印技术作为知识产权保护的有效手段，得到了广泛的关注和应用。

最早开始的研究是以图像为对象的水印技术，也是各个对象水印技术的基础。现在，无论是 Word 文档、CD 唱片、电视电影视频，还是电子邮件或是网络上的资源，都能借助水印技术标记它版权的信息。国外已有许多研究机构和企业加入数字水印的研究，如朗讯公司的贝尔实验室、微软公司的剑桥研究院、荷兰飞利浦公司、SONY 公司等等。国内学术界也于 1999 年举办了第一次信息隐藏技术研讨会，国家 863 计划智能计算机专家组会同北京邮电大学信息中心<sup>[12]</sup>在 2000 年召开了专门的“数字水印学术研讨会”，促进了中国学者在数字水印技术领域的交流。

数字水印技术现已开始运用于商业并服务于相关行业。日本电信电话通信公司研发的最新技术即是把数字水印嵌入照片中，处理后的照片与原始照片用人眼看不出差别，只有通过专用的扫描仪才能检测出其中的水印，采用这种技术可以迅速无误地确认证件的真伪<sup>[13]</sup>。我国爱国者公司也将数字水印技术应用于数码相机中，爱国者数字水印相机 AIGO WM 01 已经实现 800 万像素隐藏水印的添加时间仅为 5 秒钟，从而为数字水印技术在国内能够真正的由理论转化为生产力提供了强大支持。这两项技术可以应用于公安、司法、保险、金融和医学等实用领域<sup>[14]</sup>。

尽管数字水印在不长的发展过程中已经涌现出很多的研究成果，但水印技术仍然是一个不完全的研究领域。要使水印技术在更大范围应用值得我们更深入的研究，如在原始载体的保真度和水印的鲁棒性之间权衡寻找最佳的嵌入算法、对于大尺度变换会破坏水印的情况需要找到抵抗攻击鲁棒性强的水印、盲检测器的几何和时间失真问题等等。

## 1.4 本文的主要研究与内容安排

本文围绕 MIMO 无线传输系统中的信息安全问题进行了探讨，为了提高数字产品版权保护的力度，做了以下工作：

1) 将 Turbo 编码技术应用于数字水印中，采用添加监督码和迭代译码的方式，以增强数字水印的抗攻击的能力。

2) 采用小波变换低频域的均值量化算法嵌入水印，使在接收端能实现水印的盲检测。

3) 研究无线通信信道的衰落特性，采用瑞利衰落、莱斯衰落和天线相关三个方面建立 MIMO 系统信道，以适应不同信号传输地区的信道。

4) 重点研究 MIMO 的关键技术——空时编码。对需要确切知道信道状态信息的三种常用的空时编码：分层空时编码、空时格型编码和空时分组编码进行分析和比较。分别采用不同的编码技术设计 MIMO 发射/接收系统，并结合各种衰落信道对其进行实验仿真，分析三种传输系统的性能，得出采用空时格型编码技术最适合作为数字水印的 MIMO 系统的传输方式。

5) 将数字水印技术应用于 MIMO 系统，将嵌入水印的图像一维化处理后送入空时格型码编码器进行传输，接收端利用 Viterbi 译码方式得到接收的图像，再用与 Turbo 编码水印相逆的方式提取出水印。

论文共包括五章，各章具体安排如下：

第 1 章主要研究了论文选题的研究背景及意义，分别对 MIMO 技术和数字水印技术的国内外研究现状和发展趋势进行简要的叙述。并介绍了论文的研究内容和章节安排。

第 2 章对数字水印技术进行论述。由通信系统模型引入数字水印的嵌入和提取模型，并提出 Turbo 码水印算法，用实验仿真证明 Turbo 码水印具有优良的不可见性和鲁棒性。

第 3 章对 MIMO 系统各个关键技术进行分析和研究。首先论述 MIMO 系统的简单模型，分析出多天线技术对信道容量的增加有显著作用，通过对无线信道特性的仿真模拟验证无线信道的衰落对信道容量也有影响。最后对三种空时编码技术进行重点分析。

第 4 章将数字水印技术应用于 MIMO 系统中并对其仿真，实验是建立在瑞利衰落、莱斯衰落和天线相关三种信道上的 MIMO 系统的嵌有水印信号的图像的传输，分析了水印在各种攻击下的鲁棒性和不可见性。

第 5 章是全文的总结部分，总结本文研究的成果及不足，并对以后工作方向进行展望。

## 第 2 章 Turbo 码数字水印技术

### 2.1 基于通信理论的数字水印模型

数字水印处理系统可以等价于数字通信系统，即在水印的嵌入端和提取端之间传递已嵌入水印的载体信息。水印系统包括嵌入、传输和检测三个部分，水印的嵌入是对水印信息进行编码并采用某种方法将水印嵌入载体信息中，这相当于通信系统中的发送端；水印的检测是对接收到的信息进行水印的提取，这相当于通信系统中的接收端；数字水印在传输的过程中可能会受到各种攻击或噪声的影响，这与通信系统中的信道传输过程相类似，因此，可以将数字水印系统归结为图 2-1 所示的通信系统模型。

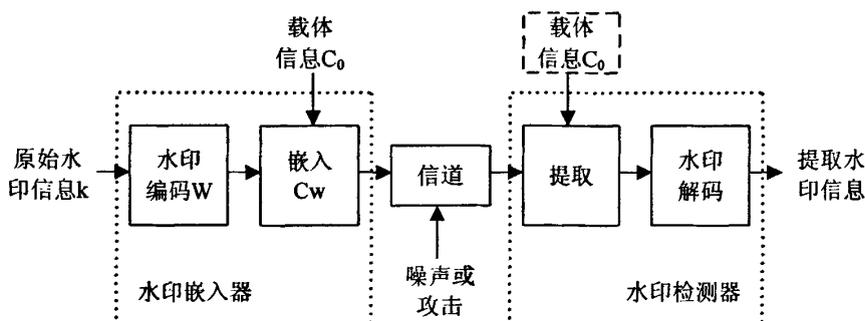


图 2-1 基于通信理论的数字水印系统模型

水印的嵌入过程分为水印的编码和嵌入两个步骤。首先，将原始水印信息  $k$  进行编码，形成编码后信息  $W$ 。然后对  $W$  采用类似于式 2-1 的方式嵌入载体信息中。

$$C_w = C_0 + \alpha W \quad (2-1)$$

式中， $C_0$  为原始载体信息， $\alpha$  为嵌入强度，通过加权后相加，得到已嵌入水印的作品信息  $C_w$ 。

水印的提取过程可分为有原始载体信息参与的提取和没有原始载体信息参与的提取，即非盲水印检测和盲水印检测。非盲水印检测就直接从接收到的作品信息  $\hat{C}_w$  中减去原始载体信息  $C_0$ ，得到含噪声的水印编码信息  $\hat{W}$ ，

再对  $\hat{W}$  进行解码得到提取的水印信息  $\hat{k}$ 。盲水印检测过程则全部由水印的解码器来完成，它先进行信道解码恢复正确序列，再进行信源解码恢复水印  $\hat{k}$ 。

对于一些有鲁棒性要求的应用，如操作跟踪、拷贝控制和所有者鉴别等，可以将通信中纠错编码技术应用于水印的编码和解码中，以提高数字水印在信道中传输的可靠性和抗攻击的能力。

## 2.2 Turbo 码数字水印的基本原理

Turbo 码数字水印即是将数字水印信息嵌入载体图像之前，采用混沌置乱算法和 Turbo 编码对水印信息进行预处理。这样利用混沌序列的加密功能和纠错编码的自我检错性能增强了水印信息的鲁棒性，使传输在多径时变的无线信道中的多媒体产品的版权信息更加安全可靠且不易被破坏。

### 2.2.1 Turbo 码原理

为了能判断接收的信息是否有误，可以由发送端的编码器在信息序列中增加一些监督码元，这些监督码元和信息序列有一定的关系，使接收端可以利用这种关系由译码器来发现或纠正可能存在的错码<sup>[15]</sup>，这就是纠错编码的基本原理。随着数字通信技术的发展，人们研究开发了各种纠错编码算法，各自建立在不同的数字模型基础上。由于信道传输中发生的错误大多是突然发生的一串差错的，或是突发差错和随机独立的错误并存的，针对这一类信道，法国不列颠通信大学的两位教授 C. Berrou、A. Glaienux 与缅甸籍博士 P. Thitimajshima 提出了一种新的纠错码——Turbo 编码<sup>[16]</sup>。

Turbo 码的核心思想是子编码器的级联和迭代译码算法。C. Berrou 教授等人在计算机仿真中，采用编码效率为 1/2 的编码单元和长度为 65536 的伪随机交织器，在信噪比大于 0.7dB 的高斯白噪声信道中传输，接收端经过了 18 次迭代译码后，误比特率小于  $10^{-5}$ ，与 Shannon 理论极限性能仅相差 0.7dB，称为最接近 Shannon 极限的纠错编码。它很好地应用了 Shannon 信道编码定理中的随机性编/译码条件，在抵御加性高斯噪声方面性能优越，而且具有很强的抗衰落和攻击的能力<sup>[17]</sup>，这也是本文选用 Turbo 码作为 MIMO 无线通信信道传输中水印的编码的原因。其编码器和译码器的结构框图如图 2-2<sup>[18]</sup>。

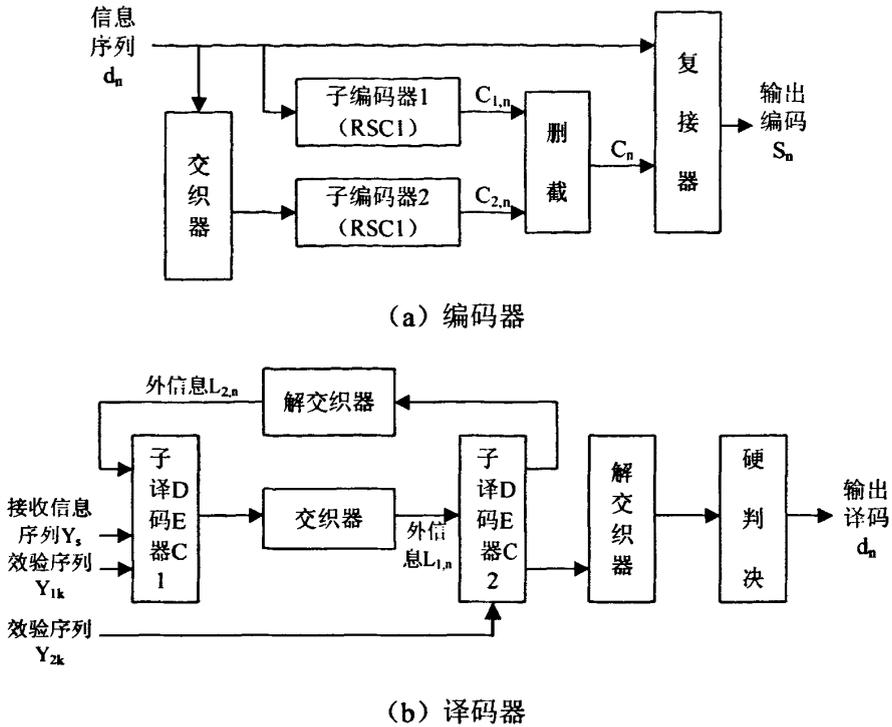


图 2-2 Turbo 码编码器的结构框图

图 2-2 (a) 中, Turbo 编码器由两个子编码器 (RSC1、RSC2) 通过交织器并行级联, 再经过删截和复接器得到输出的编码数据流  $S_n$ 。编码单元由两个完全相同的递归系统卷积码 (RSC) 组成, 信息序列在进入编码器之前被分为多组长度为  $n$  的比特流, 每一组比特流记为  $D = (d_1, d_2, d_3 \dots d_n)$ , 一部分输入到第一个子编码器 RSC1 进行编码, 另一部分通过交织器后进入第二个子编码器 RSC2 进行编码。每个 RSC 有两路效验位 ( $C_{1,n}$ 、 $C_{2,n}$ ) 输出, 两个效验序列经过删截控制编码码率得到  $C_n = (C_{1,1}, C_{2,2}, C_{1,3}, C_{2,4} \dots)$ , 再通过复接器得到 Turbo 码  $S_n = (S_1, S_2, S_3 \dots S_n)$ , 其中  $S_i = (d_i, C_i)$ ,  $d_i, C_i \in \{0,1\}$ 。子编码器是整个 Turbo 码编码器的核心, RSC 能使各子编码器中的信息更好地互相利用, 总的码重更接近于平均码重附近<sup>[19]</sup>, 这样更适合于低信噪比的信道。

图 2-2 (b) 中, 译码器由两个子译码器 (DEC1、DEC2)、交织器、解交织器级联组成。每个子译码器都采用软输入软输出 (SISO) 的译码算法, 在进行译码判决的同时还给出每一位信息的可靠估值, 即为译码器的外信息。一部分外信息  $L_{1,n}$  直接经过交织器, 另一部分外信息  $L_{2,n}$  经过解交织器作为另外一个子

译码器的先验信息，协助其译码。这种迭代的方式能使每个输出码元得到接收的信息序列中所有码元的信息，从而，Turbo 码译码器的性能远远优于其它类型的译码器。

交织器是影响 Turbo 码性能的一个重要因素。在编码器中，它可以增加码字的自由距离、改善码字的距离谱特性，降低重量偏重或偏轻的码字数量的输出，使得码字距离谱窄化；在译码器中，它可以降低外信息的相关性<sup>[17]</sup>。交织器的设计应尽可能的置乱原来的数据排列顺序；尽量提高最小码重码字的重量和减小低码重码字的数量；还要尽量避免与同一信息位直接相关的两个分量编码器中的效验位被误删<sup>[20]</sup>。本文采用基于 3GPP 标准的交织器，可以降低译码中的误码性能，而且译码性能也比较稳定。

SISO 译码算法应考虑两方面的问题：如何引入外信息和如何充分利用所有码元信息而防止正反馈的形成。标准 MAP (Maximum A Posterior Probability) 算法通过除以先验分布来消除正反馈的形成，但计算量为每比特  $6 \times 3^m$  次乘法和  $5 \times 2^m$  次加法 ( $m$  为约束长度)<sup>[21]</sup>，运算量庞大，不易实现。MAX-LOG-MAP 算法是在对数中实现，将乘法运算变成了加法运算，并将对数域中似然值加法表示式中的对数分量忽略，省去了大部分的加法运算，降低了运算复杂度，但并不是最优的算法。LOG-MAP 算法是对 MAX-LOG-MAP 算法的修正，多了查表和加法运算，复杂度仅仅多了一点，而性能却有提高 (如图 2-3)。定义为：

$$\begin{aligned} \ln(e^{x_1} + e^{x_2}) &= \max(x_1, x_2) + \ln(1 + e^{-|x_1 - x_2|}) \\ &= \max(x_1, x_2) + f_c(x_1 - x_2) \end{aligned} \quad (2-2)$$

式中， $x_1, x_2$  为译码出来的符号， $f_c(x)$  为修正函数。软输出 Viterbi 算法 (Soft Output Viterbi Algorithm, SOVA) 是利用最优留存路径和被删路径的度量差做修正，以保留必要的信息，比 LOG-MAP 算法损失近 1dB。

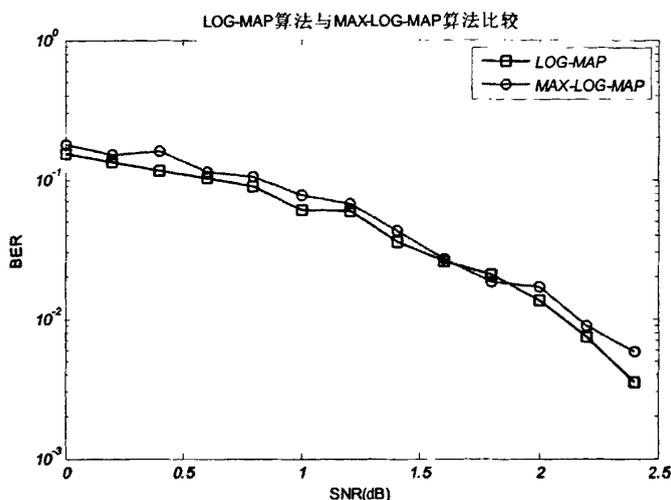


图 2-3 LOG-MAP 算法与 MAX-LOG-MAP 算法比较

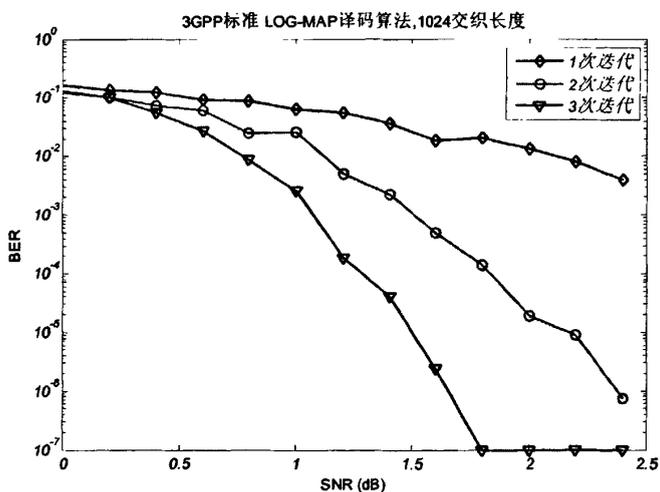


图 2-4 不同迭代次数下 LOG-MAP 译码误码率曲线

Turbo 译码是迭代的。图 2-4 所示为不同迭代次数下，交织长度为 1024、码率为 1/3 的 LOG-MAP 译码的误码率 (BER) 与信噪比 (SNR) 的关系曲线。可以看出迭代次数越大，译码性能越高。但同时也带来了译码的延时，对数据量大的信息来说尤为明显。从图中也可以看出迭代次数增加到一定程度，对译码的性能的改善趋于稳定，因此设计中应考虑译码延时，寻找最佳的迭代次数。本文实验根据信道易受攻击的特性，选择译码迭代次数为 15 次。

## 2.2.2 混沌置乱算法

基于保密通信的安全性需求高的考虑, 本文对水印图像进行 Turbo 编码之前首先应对其进行混沌置乱, 将水印图像加密。采用混沌序列是因为它对初值的敏感性很高, 安全性强, 它的低通特性可以有效的抵抗低通滤波和 JPEG 压缩攻击<sup>[22]</sup>。用于数字水印预处理的混沌方法主要有四种: Logistic 映射、Chebshev 映射、Reny 映射和花托自同构。

Logistic 映射以它的遍历性和对初值高度敏感性而备受关注, 在保密通信领域的应用十分广泛。本文就采用 Logistic 映射方法, 从数学形式上来看它是一个非常简单的混沌映射, 它定义为<sup>[23]</sup>

$$s_{i+1} = \mu s_i (1 - s_i) \quad \mu \in [1, 4] \quad i = 0, 1, 2, \dots \quad (2-3)$$

此式为 Logistic 混沌置乱的密钥。式中,  $\mu$  为控制参数, 通常选为接近 4 的实数, 本文采用的值为 3.9;  $0 < s_i < 1$ , 使序列  $s$  的取值范围是单极性的, 本文采用的值为 0.7。再将生成的混沌序列  $s$  从小到大排序, 形成新的序列  $ss_j$ , 并记录每一位序列  $s_i$  的初始位置值, 再将新的序列  $ss_j$  映射到一维化的待置乱的水印信息  $M_i$  中, 即  $ss_1 = M_1$ 、 $ss_2 = M_2 \dots$  直到把水印像素点放完为止, 再将映射了水印像素点的序列  $ss_j$  按其初始的位置值排列, 如此进行伪随机排序以生成最终的混沌水印。水印置乱效果如图 2-5。

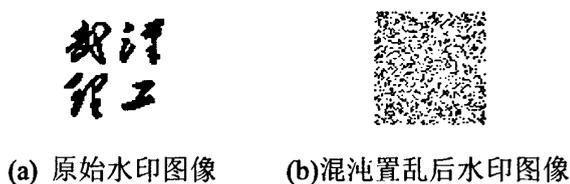


图 2-5 水印混沌置乱

## 2.3 数字水印系统的实现

### 2.3.1 数字水印系统的总体框图

本文的数字水印系统的总体框图如图 2-6。

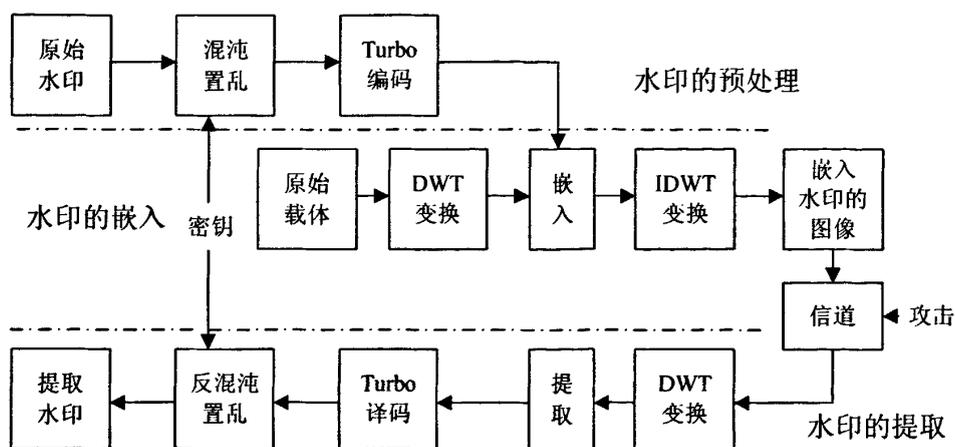


图 2-6 数字水印系统总体框图

本系统分为水印的预处理、水印的嵌入和水印的提取三个部分。

### 2.3.2 水印的预处理

本文选择有实际意义的水印信息如图 2-5 (a)，因为有意义的水印与无意义的水印序列相比更能反映出多媒体产品的版权信息。

首先对水印图像进行 Logistic 映射混沌置乱，对水印信息产生一道密钥。再将置乱后的水印信息转为一维的比特序列，通过 Turbo 编码器，为水印信息加上监督码元，最后将一维的信息序列二维化，生成待嵌入的水印信息。

### 2.3.3 水印的嵌入

离散小波变换 (Discrete Wavelet Transform, DWT) 是目前数字水印技术经常用到的嵌入方法。小波变换把原始图像分解成多频段的图像，能适应人眼的视觉特性且使得水印的嵌入和检测可分多个层次进行。为了增加水印对 JPEG 压缩攻击的鲁棒性，并实现盲检测的目的，本文采用了一种均值量化嵌入算法<sup>[24]</sup>。

首先，对原始载体图像进行三级小波分解，如图 2-7 所示，L 表示低通滤波器，H 表示高通滤波器。

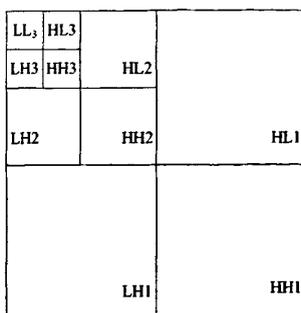


图 2-7 三级小波分解

其次，从 LL<sub>1</sub> 子带（包括 HH<sub>2</sub>, HL<sub>2</sub>, LH<sub>2</sub>, LH<sub>3</sub>, HL<sub>3</sub>, LL<sub>3</sub> 子块）选取  $n$  个系数  $X_{iu}$ ,  $u=0,1,\dots,n-1$ , 计算它们的均值。

$$\overline{X}_i = \frac{1}{n} \sum_{u=0}^{n-1} X_{iu} \quad (2-4)$$

然后，选取 3 个相邻的子块  $D_1, D_2, D_3$ , 比较它们均值之间的大小。若  $D_1, D_2, D_3$  均不相等，则将水印信息转成二进制比特序列，按图 2-8 所示<sup>[24]</sup>，当水印信号为 ‘0’ 时，将均值  $\overline{X}_i$  量化到最近的虚线值；当水印信号为 ‘1’ 时，将均值  $\overline{X}_i$  量化到最近的实线值，计算出均值  $\overline{X}_i$  的修改量为  $\Delta$ ，即为均值  $\overline{X}_i$  的量化步长，计算得到修改后的均值为  $X'_{iu} = X_{iu} + \Delta$ ,  $u=0,1,\dots,n-1$ ；若  $D_1, D_2, D_3$  中有两个相等，则按式 (2-5) 来计算量化步长。

$$\Delta = \frac{D_3 - D_1}{Q} \quad (2-5)$$

其中  $D_1$  与  $D_3$  为不相等的子块均值，将  $D_2$  修改为  $D_2 + \Delta$ ，再按三个子块均值不相等的方法计算；若  $D_1, D_2, D_3$  均相等，则将  $D_1$  修改为  $D_1 - 2\Delta$ ,  $D_2$  修改为  $D_2 + 2\Delta$ ，再按三个子块均值不相等的方法计算。

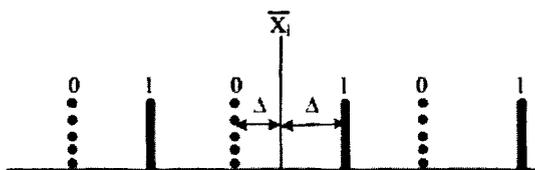


图 2-8 均值量化嵌入原理

最后对经系数调整后的子块进行离散小波反变换，得到嵌入水印的图像。

### 2.3.4 水印的提取

水印的提取是嵌入的逆过程。由于水印的嵌入过程中采用了小波变换域的均值量化的方法，检测时无需原始载体图像的参与，达到水印信息的盲提取。具体步骤如下：

1) 对待检测的图像先进行三级 DWT 变换，计算  $LL_1$  子带中  $n$  个系数的均值，对 3 个相邻的细节子块计算均值，若三个子块均值都不相等，则按式 (2-5) 计算量化步长，将均值之间分段，若中间值的均值接近实线，则提取水印信号为 ‘1’，若中间值的均值接近虚线，则提取水印信号为 ‘0’；若三个子块均值中有两个相等，则提取的水印信号为 ‘0’；若三个子块均值都相等，则提取的水印信号为 ‘1’；

2) 将提取的水印信息通过 Turbo 译码器进行 LOG\_MPA 算法迭代译码；

3) 将译码后的水印信息用混沌密钥进行反置乱，得到提取的水印信息。

### 2.3.5 图像水印系统的评价方法

数字水印系统的评价不能仅从人的感觉上去主观的判断提取水印的好坏，因为人对事物的感觉会因为光照程度、环境影响等客观因素和个人喜好、心情等主观因素不同而有很大的区别，因此应该有一些客观的标准来评判。

原始载体图像的保真度是评价水印算法的一个重要指标，需要考虑人类视觉系统的图像失真度量准则，峰值信噪比 (Peak Signal to Noise Ratio, PSNR) 是较好的判断嵌入水印后图像与原始载体图像像素亮度值之间差异的度量准则，其定义如下<sup>[25]</sup>：

$$PSNR = \frac{M \times N \times \max_{i,j}(I_{i,j}^2)}{\sum_{i,j} (I_{i,j} - I'_{i,j})^2} \quad (2-6)$$

式中， $M \times N$  为图像的尺寸， $I_{i,j}$  为原始水印矩阵在坐标  $(i, j)$  处的值， $I'_{i,j}$  为提取水印矩阵在坐标  $(i, j)$  处的值。PSNR 的值越高，图像间的相似程度越高，也就表示嵌入水印后的图像有较高的不可见性。

为了评价提取水印与原始水印的相似度，采用归一化互相关系数 (NC) 来表征它们之间的差别，NC 的值越接近 1，提取的水印与原始水印的相似程度越大，表明水印的鲁棒性能越好。其定义为<sup>[25]</sup>：

$$NC = \frac{\sum_{i,j} I_{i,j} \times I'_{i,j}}{\sum_{i,j} I_{i,j}^2} \quad (2-7)$$

## 2.4 数字水印仿真实验

实验的仿真平台是 MATLAB7.7, 原始载体图像为 lena.bmp (512×512) 标准灰度图像, 待嵌入的原始水印图像是大小为 64×64 有意义的二值位图图像, Turbo 码的码率为 1/2, 交织器为 3GPP 标准的交织器, 采用性能好且复杂度较低的 LOG\_MAP 译码, 译码迭代次数为 15 次。

图 2-9 所示为无任何攻击时, Turbo 水印嵌入后提取的效果, 此时提取的水印图像与原始水印图像的归一化互相关系数 NC 的值为 1, 即提取的水印信息与原始水印信息完全相同。



(a)原始载体图像 (b)原始水印图像 (c)嵌入水印后图像 (d)提取水印图像

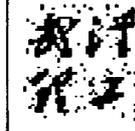
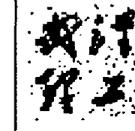
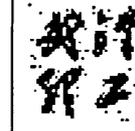
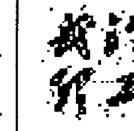
图 2-9 无攻击时 Turbo 水印的提取

对水印的抗攻击性能测试, 实验分别采用了高斯白噪声攻击、椒盐噪声攻击、剪切攻击、JPEG 压缩攻击以及中值滤波攻击五种攻击方式。并且为了验证采用 Turbo 编码的数字水印的抗攻击能力优于采用其他纠错编码的数字水印, 实验同时也对采取 (31, 16) BCH 编码、(31, 16) RS 编码、(7, 4) 汉明编码和编码效率为 1/2 的卷积编码预处理过水印的嵌入与提取过程进行了仿真。文献[26]提到做不同纠错码水印比较时, 应保证嵌入水印的容量和水印的嵌入强度一致, 因为在水印信道中受水印不可察觉性的限制, 纠错编码带来的信息冗余会导致水印嵌入强度的降低, 换言之, 纠错编码码率会影响水印嵌入强度。因此本文实验采取的纠错码的码率均接近于 1/2。

1) 高斯白噪声攻击

高斯白噪声是服从正态分布的加性噪声，是无线信道中最常见的噪声。实验对已嵌入水印的图像中加入高斯噪声，各种纠错编码数字水印算法的水印提取的效果如表 2-1。

表 2-1 水印抗高斯白噪声攻击性能比较

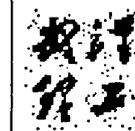
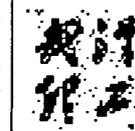
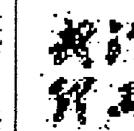
	无纠错码	BCH 编码	RS 编码	汉明码	卷积编码	Turbo 编码
PSNR	20.1092	20.1025	20.1000	20.0949	20.1096	20.0893
NC	0.88083	0.96892	0.96044	0.96993	0.97107	0.97110
提取水印图像						

实验结果可以看出，在高斯白噪声的攻击下，RS 编码的纠错效果最不尽人意，其余的纠错码水印的提取效果都较好，卷积编码水印的提取效果与 Turbo 编码水印的提取效果相差无几。Turbo 编码水印算法的抗高斯白噪声的能力是这几种纠错码水印算法中最好的。

2) 椒盐噪声攻击

椒盐噪声是由图像传感器，传输信道，解码处理等产生的黑白相间的亮暗点噪声。实验在已嵌入水印的图像中加入椒盐噪声，各种纠错码水印算法提取水印效果如表 2-2。

表 2-2 水印抗椒盐噪声攻击性能比较

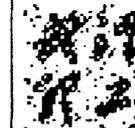
	无纠错码	BCH 编码	RS 编码	汉明码	卷积编码	Turbo 编码
PSNR	18.3753	18.3395	18.3101	18.3993	18.4070	18.4147
NC	0.87877	0.96778	0.96174	0.96211	0.96184	0.96577
提取水印图像						

实验结果表明,椒盐噪声对水印的攻击作用比高斯噪声影响大,此时 Turbo 编码水印算法的提取效果略低于 BCH 编码水印算法的提取效果,但比 RS 编码水印、汉明码水印和卷积编码水印的提取效果好。

### 3) 剪切攻击

多媒体产品在信道传输过程中有可能会遭到拦截,并且恶意修改产品信息,如剪切、压缩等。实验模拟剪切攻击,对图像的(128~256,256~384)像素区域进行剪切。各种纠错码水印算法提取水印的效果如表2-3。

表 2-3 水印抗剪切攻击性能比较

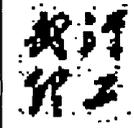
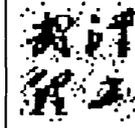
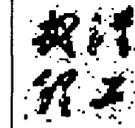
	无纠错码	BCH 编码	RS 编码	汉明码	卷积编码	Turbo 编码
PSNR	19.0560	19.0560	19.0560	19.0560	19.0560	19.0560
NC	0.90068	0.93682	0.93231	0.93311	0.93193	0.93970
提取水印图像						

实验结果可以看出,剪切攻击对水印的影响很大,造成了提取的水印信息都有较明显的噪点。各种纠错编码预处理过的水印提取效果相差并不明显。相对而言, Turbo 编码水印算法抗剪切攻击的能力是这几种纠错码水印算法中最好的。

### 4) JPEG 压缩攻击

JPEG 压缩为有损压缩,即不可逆的压缩算法。压缩的品质因数可选范围为 0~100,品质因数越大,压缩比越小,图像质量越好。实验选用的品质因数为 80,各种纠错码水印提取水印效果如表 2-4。

表 2-4 水印抗 JPEG 压缩攻击性能比较

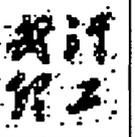
	无纠错码	BCH 编码	RS 编码	汉明码	卷积编码	Turbo 编码
PSNR	25.1286	25.1286	25.1286	25.1286	25.1286	25.1286
NC	0.90581	0.98252	0.95739	0.97429	0.97290	0.98341
提取水印图像						

实验结果表明，纠错码水印算法抗品质因数为 80 的 JPEG 压缩的攻击是非常有效的，只是 RS 编码水印的纠错效果略低。Turbo 编码水印算法的抗 JPEG 压缩攻击的能力是纠错码水印算法中最好的。

### 5) 中值滤波攻击

中值滤波法是一种非线性平滑滤波，它将每一像素点的灰度值设置为该点某邻域窗口内的所有像素点灰度值的中值，因此给原始图像的灰度值造成了失真。实验对已嵌入水印的图像中进行 5×5 的中值滤波，各种纠错码水印提取水印效果如表 2-5。

表 2-5 水印抗 5×5 中值滤波攻击性能比较

	无纠错码	BCH 编码	RS 编码	汉明码	卷积编码	Turbo 编码
PSNR	24.9084	24.9084	24.9084	24.9084	24.9084	24.9084
NC	0.95675	0.96740	0.97594	0.97461	0.97394	0.97815
提取水印图像						

实验结果表明，纠错码水印算法抗 5×5 中值滤波攻击也是非常有效的，其中，Turbo 编码水印算法的抗 5×5 中值滤波攻击的能力是纠错码水印算法中最好的。

由以上五组实验可以看出：在水印的不可见性上，Turbo 编码数字水印算法与其他纠错码数字水印相差不大，甚至有些情况（如噪声攻击）还优于某些纠错编码的数字水印算法；在水印的鲁棒性上，Turbo 编码数字水印算法除了抗椒盐噪声的能力稍有不如下 BCH 编码预处理过的数字水印，其余的抗攻击能力都明显强于其他纠错编码水印，可见 Turbo 编码数字水印算法能有效地抵抗无线信道传输过程中的大部分攻击，特别在对抗高斯噪声、JPEG 压缩、中值滤波等攻击上具有较高鲁棒性的优势。并且采用均值量化嵌入的方法可以实现了水印的盲提取。

## 2.5 本章小结

本章由通信系统理论引入数字水印的系统的模型,并将通信理论中的 Turbo 编码技术应用于数字水印系统,而采用小波变换域的均值量化嵌入算法使提取水印时不需要原始载体图像的参与。最后,为了验证 Turbo 编码的数字水印技术是优于其他纠错编码的水印技术,通过仿真实验的结果,证明 Turbo 编码数字水印算法的确是一种兼顾水印的不可见性和鲁棒性的算法。

## 第3章 MIMO 无线通信系统中关键技术

### 3.1 MIMO 技术基本原理

MIMO, 顾名思义, 就是多发送多接收天线系统。图 3-1 是一个简单的 MIMO 线性天线阵列, 发送端有  $N_t$  副天线, 接收端有  $N_r$  副天线。

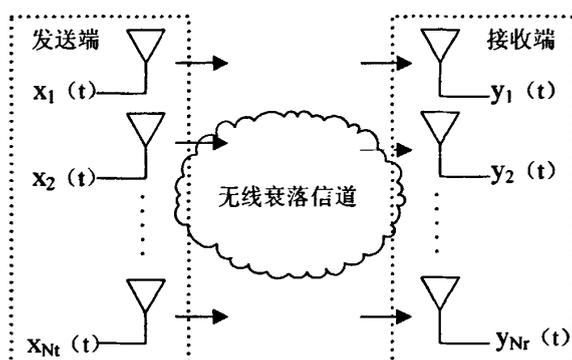


图 3-1 简单的 MIMO 物理模型

信息序列以二进制形式进入一个信息模块, 被映射为  $N_t$  路互相独立的比特流, 每路比特流通过发送端其中一个天线发送出去。经过无线信道, 在接收端通过  $N_r$  个天线接收, 并进入信息模块合并为一串信息序列<sup>[27]</sup>。接收端第  $j$  个天线上接收信号  $y_j(t)$  可以定义为:

$$y_j(t) = \sum_{i=1}^{n_t} h_{j,i} x_i(t) + \eta_j(t) \quad (3-1)$$

式中,  $x_i(t)$  为发射端第  $i$  个天线发送信号,  $h_{j,i}$  为发送天线  $i$  到接收天线  $j$  上的信道衰落,  $\eta_j(t)$  为加性噪声。

### 3.2 MIMO 系统的信道容量

对于  $N_t$  副发送天线和  $N_r$  副接收天线的 MIMO 信道, 在发送端不知道传输信道状态的条件下, 只需根据信道衰落系数的概率密度函数统计特性对其进行

积分运算，即可得到信道平均容量：

$$C = E\{\log_2[\det(I_{N_r} + \frac{E_s}{N_t N_0} Q)]\} \quad (3-2)$$

其中， $E\{\bullet\}$  表示相对信道矩阵求数学期望， $\det(\bullet)$  为矩阵行列式，矩阵  $Q$  的定义如下：

$$Q = \begin{cases} H^H H, N_t < N_r \\ H H^H, N_t > N_r \end{cases} \quad (3-3)$$

一般来说， $H^H H$  和  $H H^H$  都满足  $\chi^2$  分布随机变量的统计特征。

当发送天线和接收天线数目逐渐增大，信道容量的计算式 (3-2) 变得很复杂，需借助 Laguerre 多项式进行估计<sup>[28]</sup>：

$$C = \int_0^\infty \log_2(1 + \frac{E_s}{N_t N_0} \lambda) \sum_{k=0}^{m-1} \frac{k!}{(k+n+m)!} [L_k^{(n-m)}(\lambda)]^2 \lambda^{n-m} e^{-\lambda} d\lambda \quad (3-4)$$

式中， $m = \min(N_t, N_r)$ ， $n = \max(N_t, N_r)$ ， $L_k^{(n-m)}(\lambda)$  为  $k$  次 Laguerre 多项式。

令  $m = n = N_t = N_r$ ，可简化为：

$$\lim_{n \rightarrow \infty} C/n \geq 1/(\pi) \int_0^1 \log_2(1 + \frac{E_s}{N_0} \nu) \sqrt{(1/\nu - 1/4)} d\nu \geq \log_2 \frac{E_s}{N_0} - 1 \quad (3-5)$$

(3-5) 式表明，MIMO 信道容量与天线数  $n$  成线性的正比关系，与信噪比  $E_s/N_0$  成对数的正比关系。因此，MIMO 系统的多天线输入输出比单天线的输入输出系统的容量要大得多。为了验证 MIMO 的信道容量的优势，实验对 SISO、MISO、SIMO、MIMO 信道进行了仿真，分别选取  $1 \times 1$ 、 $1 \times 2$ 、 $2 \times 1$ 、 $2 \times 2$  等 4 种天线数，信道为瑞利衰落信道，得到信道容量与信噪比之间的关系如图 3-2。

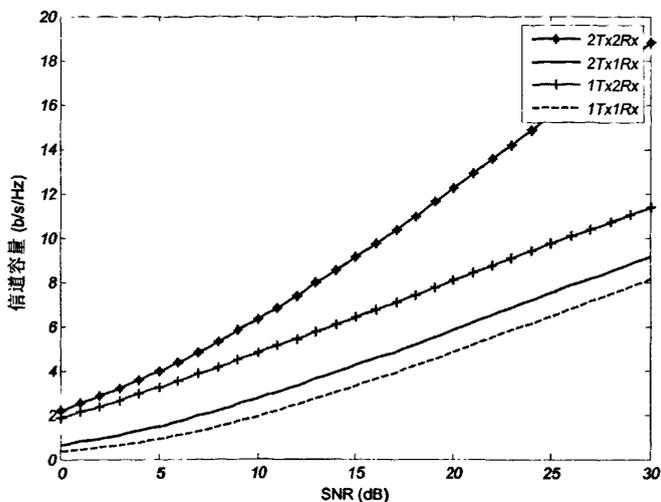


图 3-2 不同收发天线数系统信道容量

从图 3-1 中可以看出，随着天线数目的增加，信道容量成倍地增加，而且信道信噪比每增加 5dB，SISO 系统、SIMO 系统和 MISO 系统的信道容量增加大约 2bit/s/Hz，而 MIMO 系统的信道容量增加 4 bit/s/Hz，特别在高信噪比的信道中，MIMO 系统的信道容量远远大于 SISO 系统、SIMO 系统和 MISO 系统的信道容量。由此可知，MIMO 技术在改善系统信道平均容量方面有着显著的优势。

### 3.3 MIMO 无线系统的衰落信道

一切无线通信在自由空间中传播时都会受到各种障碍物阻碍，经过若干次反射、折射、散射和衍射，产生了阴影效应、多径效应和多普勒效应，使到达接收端的信号与发送信号相比发生了变化。MIMO 系统也是如此，无线信道给 MIMO 传输信号带来的影响主要是衰落和扩展。在传统的无线信道中，常用瑞利分布和莱斯分布作为近似信道特征的模型。当发射端和接收端之间障碍物密集不存在直接传播路径时，采用瑞利分布来描述信道的特征；而当发射端和接收端之间存在直接传播路径时，则用莱斯分布模型来描述信道的特征<sup>[29]</sup>。因此，瑞利衰落信道适用于描述建筑物密集的城镇中心地带的无线信道，莱斯衰落信道适用于描述空旷的郊区的无线信道。

### 3.3.1 瑞利 (Rayleigh) 衰落信道

瑞利衰落是由于障碍物的阻挡使信号被分为了多条路径传播, 接收端接收到的信号来自不同的传播路径, 各条路径的延时也不相同, 而各个方向的分量互相叠加, 又产生了驻波场强, 从而形成信号的快衰落。此时接收信号是由大量的平面波复合而成的, 可以将接收信号近似为方差为  $\sigma$  的独立同分布的零均值高斯随机过程。

用  $(a, \varphi)$  来表示瑞利衰落信道模型, 其中,  $a$  表示衰落幅度,  $\varphi$  表示衰落相位, 这两个变量分别服从瑞利分布和均匀分布<sup>[30]</sup>:

$$f_a(a) = \int_0^{2\pi} f_{a,\varphi}(a, \varphi) d\varphi = \int_0^{2\pi} \frac{a}{2\pi\sigma^2} \exp\left(-\frac{a^2}{2\sigma^2}\right) d\varphi = \frac{a}{\sigma^2} \exp\left(-\frac{a^2}{2\sigma^2}\right) \quad (3-6)$$

$$f_\varphi(\varphi) = \int_0^\infty f_{a,\varphi}(a, \varphi) da = \int_0^\infty \frac{a}{2\pi\sigma^2} \exp\left(-\frac{a^2}{2\sigma^2}\right) da = \frac{1}{2\pi} \quad (3-7)$$

### 3.3.2 莱斯 (Rice) 衰落信道

当障碍物不是很密集, 接收到的信号具有衍射分量的同时具有直接抵达的分量时, 莱斯衰落信道矩阵可以用式 (3-8) 来表示:

$$H = AH_{LOS} + H_{Ray} \quad (3-8)$$

式中,  $H_{LOS}$  表示无散射、仅有直射路径的信道分量,  $H_{Ray}$  表示无直射、仅有散射路径的信道分量。

可以将接收信号近似为方差为  $\sigma$  的非零均值复高斯随机过程。此时衰落幅度的边缘概率密度为<sup>[31]</sup>:

$$f_a(a) = \frac{a}{\sigma^2} \exp\left(-\frac{a^2 + \rho^2}{2\sigma^2}\right) I_0\left(\frac{a\rho}{\sigma^2}\right) \quad (3-9)$$

直射分量和散射分量的功率之比为莱斯分布的主要参数——莱斯因子  $K$ :

$$K = \frac{A^2}{2\sigma^2} \quad (3-10)$$

为了分析  $K$  因子对 MIMO 信道容量的影响, 对  $2 \times 2$  的 MIMO 信道进行仿真,  $K$  因子分别取 1、10、100、1000 四种情况, 如图 3-3。

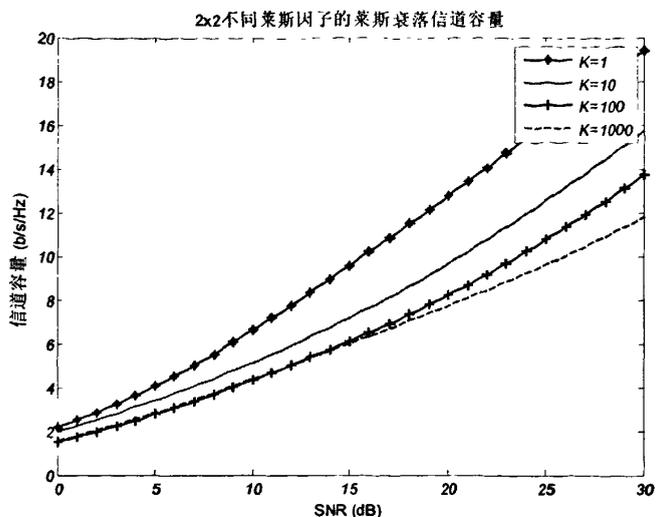


图 3-3 不同莱斯因子 2x2 MIMO 系统信道容量

从仿真结果可以看出，信道容量会因  $K$  因子的增加而减小，并且对于  $K$  因子较大时，随着信噪比的增大，对信道容量的影响就越大。不过，当  $K$  因子大到一定的程度时，对信道容量的影响区别已不太明显。

### 3.3.3 天线相关信道

一般来说，MIMO 各个天线发射的信号序列是互相独立非相关的信号。但是在散射物并不是很多或者在室内环境中，MIMO 信道的非相关的特性将消失，取而代之的是天线上信号之间的相关和互相重叠。相关的信号固然会引起接收信号的变化，造成衰落。

对于接收天线相关的 MIMO 信道，信道矩阵可以表示为<sup>[32]</sup>：

$$H = R_r^{1/2} H_0 \quad (3-11)$$

式中， $H_0$  为理想状态的独立同分布 MIMO 信道矩阵， $R_r$  为  $N_r \times N_r$  维接收相关矩阵。

对于发射天线相关的 MIMO 信道，信道矩阵则表示为：

$$H = H_0 R_t^{1/2} \quad (3-12)$$

式中， $R_t$  为  $N_t \times N_t$  维发射相关矩阵。

以  $2 \times 2$  的 MIMO 信道为例,  $R_r = R_t = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}$ ,  $\rho$  为相关系数, 定义为<sup>[33]</sup>:

$$\rho = \frac{E[(r_1 - \bar{r}_1)(r_2 - \bar{r}_2)]}{\sqrt{E|r_1 - \bar{r}_1|^2 \cdot E|r_2 - \bar{r}_2|^2}} \quad (3-13)$$

式中,  $r_1$  和  $r_2$  分别为两个接收天线接收到的瞬时归一化信号包络值,  $\bar{r}_1$  和  $\bar{r}_2$  为接收天线接收信号的均值。

为了分析相关系数  $\rho$  对 MIMO 信道容量的影响, 对  $2 \times 2$  的 MIMO 信道进行了仿真,  $\rho$  分别取 0.1、0.3、0.6 和 0.95, 如图 3-4。

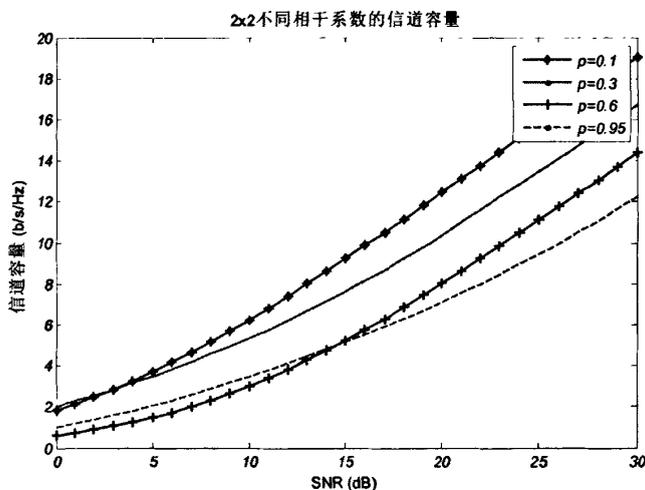


图 3-4 不同相关系数  $2 \times 2$  MIMO 系统信道容量

由仿真结果可以得到, 天线相关系数越大, 对信道的容量的影响越大, 而且信噪比越大, 容量的损失就越大。

### 3.4 空时编码技术

前面已经分析 MIMO 系统与单天线系统相比, 在信道容量上有显著的提高, 信道容量上的增大就会使信息传输速率提高和利用增加信息冗余使传输可靠性增加。为 MIMO 系统带来如此好处的原因就是它采用了空时编码 (STC) 技术。该技术将天线阵列与分集接收相结合, 在不同天线所发送的信号中引入时间和空间的相关性, 从而不用牺牲带宽而获得分集增益和编码增益。

### 3.4.1 空时编码基本模型

一个具有  $N_t$  副发送天线和  $N_r$  副接收天线的 MIMO 系统模型如图 3-5。

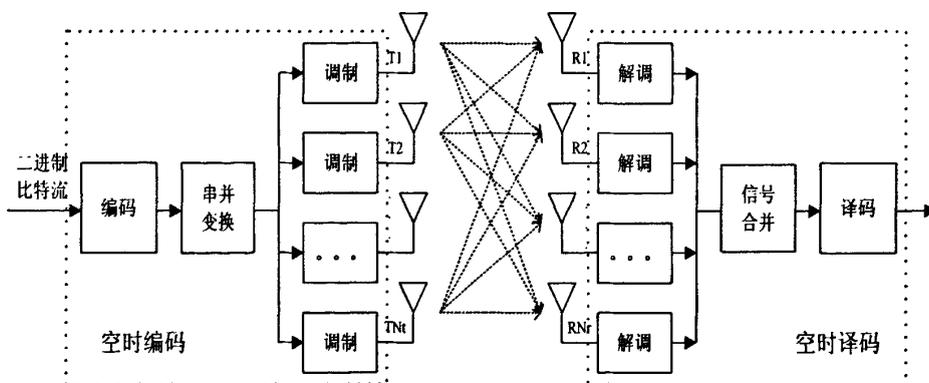


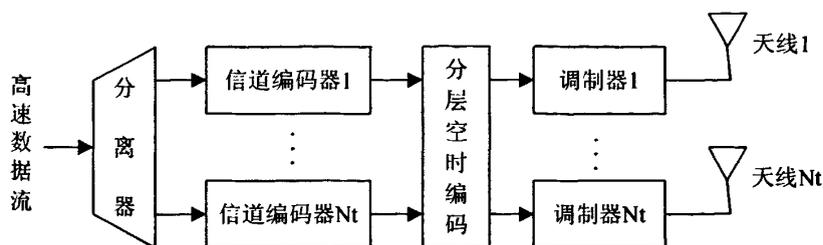
图 3-5 空时编码基本模型

二进制信息序列进入空时编码器后，进行串并变换形成能从  $N_t$  副天线同时发送出去的多路信号。发射天线阵同时发射出去的信号称为空时码元<sup>[34]</sup>。在接收端对接收到的信号进行与发送端相反的处理，合并各天线接收到的信号，译码处理后输出原始信息。

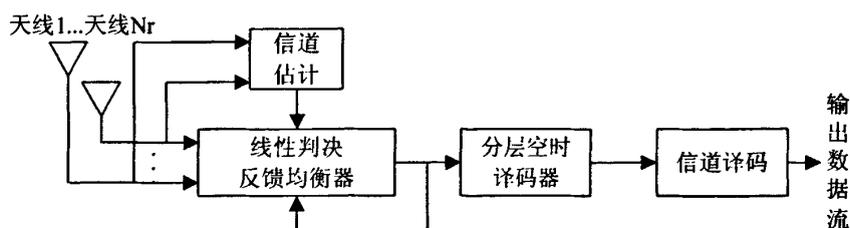
目前研究的最多的空时编码有分层空时码（LSTC）、空时格型码（STTC）、空时分组码（STBC）。它们在解码时都需要确切地知道信道状态信息（CSI）。

### 3.4.2 分层空时码

分层空时码（LSTC）最早是由美国 Bell 实验室的 Foschini 等人于 1996 年提出的。在发送端，将高速度、高信噪比的数据流转化为多路低速率、低信噪比的子数据流进行传输，各子数据流独立地进行编码、调制后用多个天线发送，从而实现发送分集；在接收端，由于分层空时码的译码需要用到信道的传输特性，因此需要进行信道估计，并由线性判决反馈均衡器分层反馈实现对信道干扰的过滤，然后进入分层空时译码器，得到输出的信号序列。分层空时码的发射和接收模型如图 3-6。



(a) 发送端模型



(b) 接收端模型

图 3-6 分层空时码模型

分层空时码的编码过程首先将信号经过分离器将输入信号序列分成  $N_t$  个长度相同的低速数据流，分别输入  $N_t$  个编码器独立地进行信道编码，再将已编码的比特流经调制映射到对应的发射天线上同步发送出去。依据分层后的数据流与天线映射方式的不同，从  $N_t$  个并行信道编码器输出的信号有三种分层空时编码：水平分层空时码（Horizontally-BLAST）、垂直分层空时码（Vertical-BLAST）和对角分层空时码（Diagonally-BLAST）<sup>[35]</sup>。其中，V-BLAST 因其检测的简单而在这三种空时编码中最受关注。

空时分层码的译码器由于要进行信道估计，则可以采用最佳的矢量译码方式——最大似然译码（ML）算法，它从所有可能发送信号的集合中找出一个信号，使其满足<sup>[36]</sup>：

$$\hat{c} = \arg \min \| \bar{r} - \bar{H}c \|^2 \quad (3-14)$$

作为发送信号的估值。ML 算法是在所有接收码字矩阵上遍历求得的估值，因此它的性能是最优的，并且能达到最大的分集度  $N_t$ 。

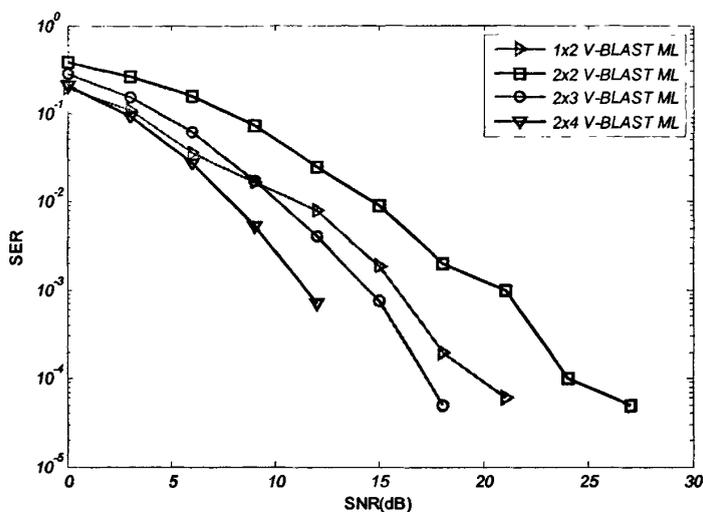


图 3-7 不同天线数的 ML 译码算法性能比较

由图 3-7 可知不同数目的发射天线（如 1×2 和 2×2）系统发射天线越少 ML 译码性能越好，因为发射天线数目越多，空间干扰越大；对于相同数目的发射天线（如 2×2、2×3 和 2×4）系统接收天线越多 ML 译码性能越好，这是因为接收增益增大的原因，因此，LSTC 系统的信道增益只与接收天线的数目有关。

但是 ML 算法的运算量随发射天线的个数增加而呈指数增加，对于多发射天线的系统译码非常复杂。于是学者提出了复杂度较低的 ZF（迫零）算法和 MMSE 算法。ZF 算法引入广义逆矩阵简化了算法，还抑制了发射天线发送信号时产生的干扰<sup>[37]</sup>。而 MMSE 算法是对 ZF 算法准确性的提高，考虑了信道噪声的影响。图 3-8 和图 3-9 分别为 ZF 译码算法和 MMSE 译码算法在不同天线数系统中的性能比较。

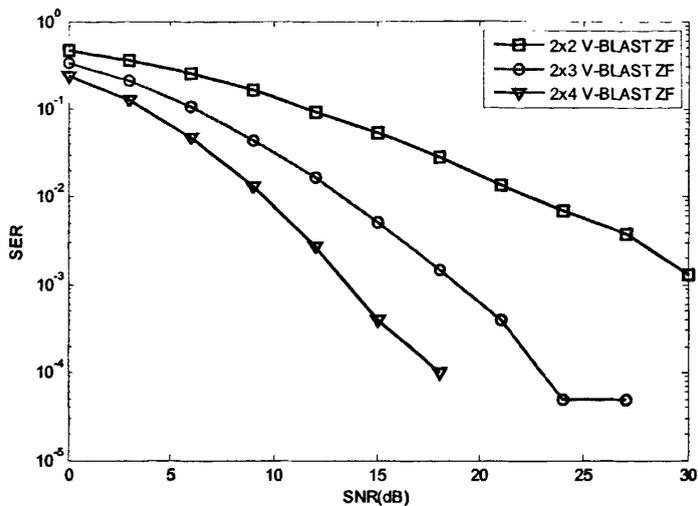


图 3-8 不同天线数的 ZF 译码算法性能比较

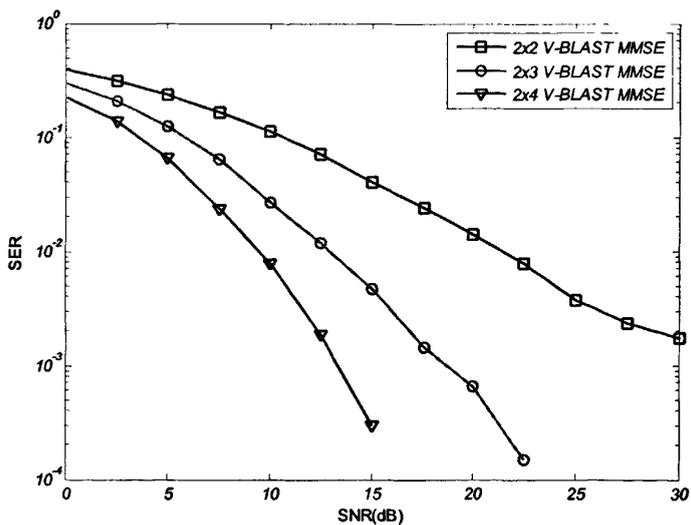


图 3-9 不同天线数的 MMSE 译码算法性能比较

鉴于 V-BLAST 不是基于发送分集的，图 3-8 和图 3-9 只给出了接收天线数目不同的性能比较。ZF 译码算法和 MMSE 译码算法在相同的发射天线而接收天线不同的性能与 ML 译码算法近似，信道增益都是随接收天线的数目增加而增加。

### 3.4.3 空时格型码

空时格型码 (STTC) 最早是 1998 年由 Tarokh 将发送分集技术与网格编码调制 (TCM) 技术相结合提出的<sup>[38]</sup>。它是能达到编译码性能和频带利用率折中的最佳编码方式。

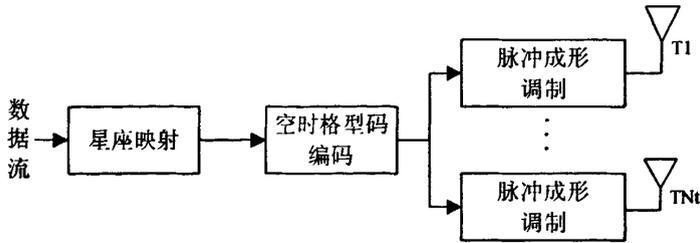


图 3-10 空时格型码编码模型

图 3-10 所示空时格型码的编码过程分为星座映射和空时格型码编码两部分。星座映射一般采用 M-PSK 或 M-QAM 调制<sup>[39]</sup>。以 4-PSK 为例，图 3-11 为 4 状态的网格结构。信息序列进入空时格型编码器后，每 2bit 分为一组，每组被映射为 4 个星座点的圆形星座图 (图 3-11 (a))。空时格型编码的映射如图 3-11 (b)，比如在初始状态为 1，输入比特位为 00 01 10 11 时，编码被映射到 10, 11, 12, 13，则在天线 1 上发送的数据为 (1, 1, 1, 1)，天线 2 上发射的数据为 (0, 1, 2, 3)。

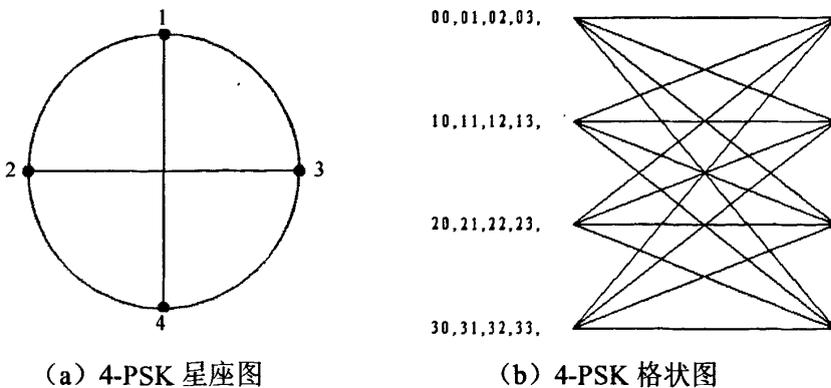


图 3-11 4-PSK 4 状态空时编码网格图

空时格形码的译码采用 Viterbi 算法来实现，它是通过选择最小累计路径来达到译码输出的，它的路径距离采用欧氏距离算法：

$$\sum_{j=1}^{N_r} \left| y_j^t - \sum_{i=1}^{N_t} h_{j,i} q_i^t \right|^2 \quad (3-15)$$

式中， $h_{j,i}$  为发射天线  $i$  到接收天线  $j$  的信道状态信息， $y_j^t$  为接收天线  $j$  在  $t$  时刻接收到的信号。Viterbi 算法可以简单概括为“相加-比较-保留”，具体算法为：根据接收符号  $y_j^t$  从初始状态 0 出发，逐个向右进行扩展，并与接收数字原来的分支进行比较，计算它们之间的欧式距离，将计算所得距离加到被延伸路径的累积距离值中。对到达每个状态的各条路径的距离累积值进行比较，保留距离值最小的一条路径，称为幸存路径<sup>[40]</sup>。图 3-12 所示 4-PSK 在初始状态为 0 时译码路径，图中标出了到达各级节点的幸存路径的距离累积值。

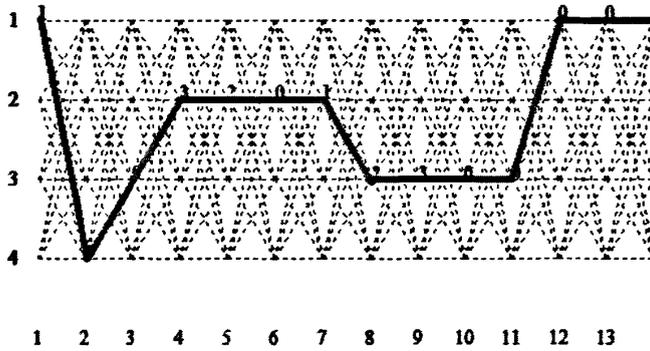


图 3-12 Viterbi 译码的最佳路径

图 3-13 给出了 4-PSK 星座调制，2bit/Hz 空时编码不同状态下的性能曲线，同一信噪比上，随着状态数的增加空时格型编码的误符号率降低，说明可以通过增加状态数改善信道性能。

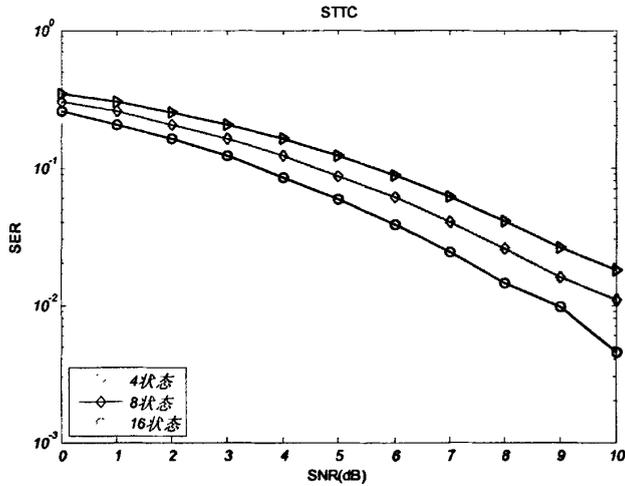


图 3-13 4-PSK 调制不同状态下的 STTC 系统性能比较

Viterbi 算法虽然能保证最小的译码错误率，但是它的计算复杂度与天线分集的程度和传输的速率成指数增长，因此需要找到更简单的译码方式，于是人们提出了空时分组码。

### 3.4.4 空时分组码

空时分组码 (STBC) 是 1998 年由 Alamouti<sup>[9]</sup> 首先提出，Tarokh<sup>[8]</sup> 在他的基础上结合正交编码形成的空时编码技术。由于正交编码技术的应用，在接收端可以采用最大似然译码，完全采用线性处理技术，则大大降低了译码的复杂度，解决了空时格型码译码复杂的问题。而且在性能上与空时格型码相比，虽然有一点损失，也能得到最大的发送分集。

空时分组码的编码同样首先采用星座映射，与空时格型码不同的是编码部分。将信息序列分组，每组  $km$  个比特，通过  $2^m$  个点组成的星座，映射出的  $k$  个调制信号  $x_1, x_2, \dots, x_k$ ，对这些  $k$  采用列正交编码矩阵 (3-16) 进行编码<sup>[37]</sup>。

$$G = \begin{bmatrix} c_1^1 & \cdots & c_1^{N_t} \\ \vdots & & \vdots \\ c_p^1 & \cdots & c_p^{N_t} \end{bmatrix} \quad (3-16)$$

其中  $p$  表示第  $p$  时刻。得到各天线上的发送信号序列互相正交。以 2 发 2 收天线为例， $X_1$ 、 $X_2$  分别表示天线 1 和天线 2 上的发射序列。

$$X_1 = [x_1, -x_2^*] \quad X_2 = [x_2, x_1^*] \quad (3-17)$$

两发射序列满足正交性，即： $X_1 \bullet X_2 = 0$ 。

经过信道衰落，接收到的信号分别  $y_1$  和  $y_2$

$$y_1 = h_1 x_1 + h_2 x_2 + n_1 \quad y_2 = -h_1 x_2^* + h_2 x_1^* + n_2 \quad (3-18)$$

其中  $h_1, h_2$  为衰落系数， $n_1, n_2$  为信道中的加性噪声。

将两路接收信号合并

$$[y_1, y_2^*]^T = \begin{pmatrix} h_{11}^* & h_{12} \\ h_{12}^* & -h_{11} \end{pmatrix} [x_1, x_2]^T + [n_1, n_2]^T \quad (3-19)$$

最后对合并的信号进行最大似然检测判决，即对所有接收的码字采用式 [36]

$$\sum_{j=1}^m \left( |y_1^j - h_{1,j} x_2 - h_{2,j} x_1|^2 + |y_2^j - h_{1,j} x_2^* - h_{2,j} x_1^*|^2 \right) \quad (3-20)$$

找出使式 (3-19) 最小的  $x_1$  和  $x_2$ ，即为译码后的接收信号。

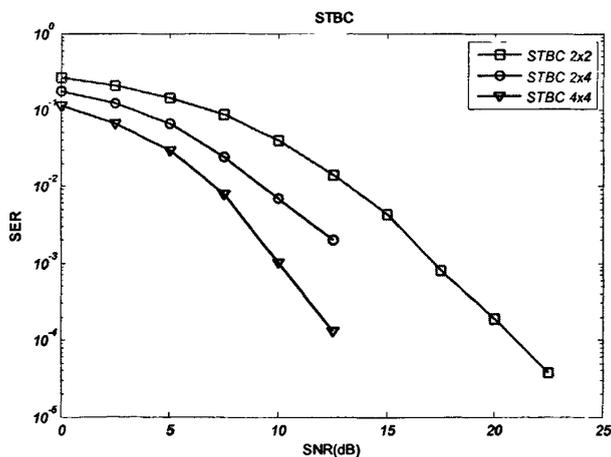


图 3-14 不同天线数的 STBC 系统性能比

图 3-14 为不同收发天线数目在 4-PSK 星座映射调制时 STBC 系统性能比较的仿真曲线。当误符号率为  $10^{-3}$  时，同样发送天线数目下，多接收天线（如 2×4）系统的信噪比比少接收天线（如 2×2）系统少大约 5dB，而对于相同接收天线数目下，多发送天线（如 4×4）系统的信噪比比少发送天线（如 2×4）系统只少大约 2dB。接收天线的增加对系统的增益的增加是剧烈的，而随着发送天线的增加，发送分集增益增加的趋势将变缓。

### 3.4.5 三种空时编码的比较

对分层空时码、空时格型码、空时分组码三种空时编码方法分别在瑞利衰落信道、莱斯衰落信道和天线相关信道进行仿真，比较三种空时编码对抗无线信道衰落的能力。天线数均为 2 发 2 收，其中分层空时码采用 V-BLAST 编码，译码采用了 MMSE、ZF 两种译码方式，空时格型码和空时分组码调制均采用 4 状态的 4-PSK 调制。

图 3-15 为静态平坦瑞利衰落信道下的仿真，接收天线上的噪声为高斯白噪声。

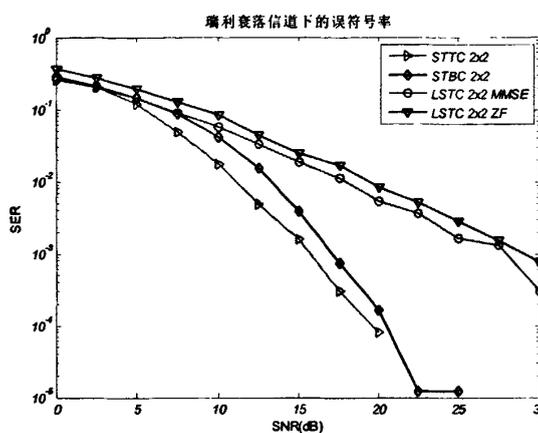


图 3-15 瑞利衰落信道下各空时编码性能比较

图 3-16 为莱斯衰落信道，莱斯因子取 10。

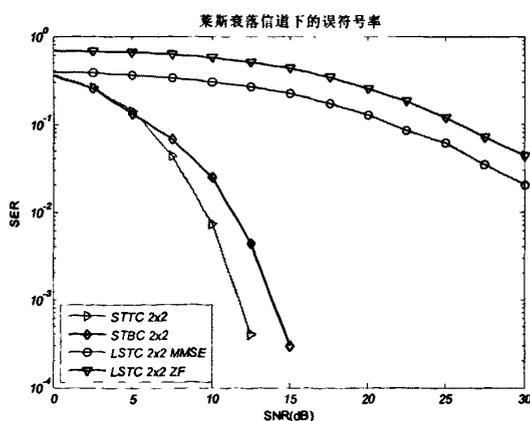


图 3-16 莱斯衰落信道下各空时编码性能比较

图 3-17 为天线相关信道，相关系数取 0.5。

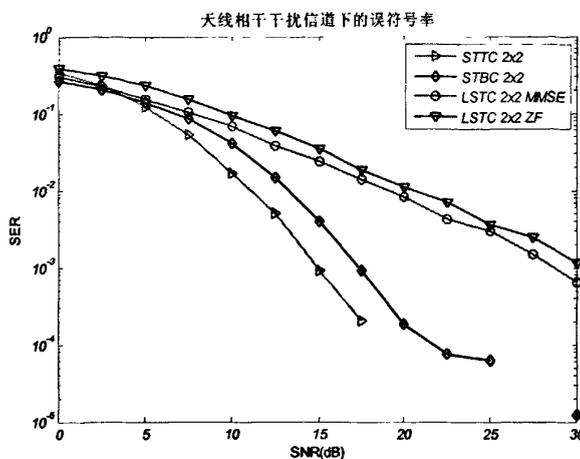


图 3-17 天线相干衰落信道下各空时编码性能比较

由仿真结果可以看出，分层空时码系统中 MMSE、ZF 译码系统的性能相差不多，MMSE 译码系统比 ZF 译码系统的性能稍好一点，区别不大。而空时分组码系统和空时格型码系统的性能明显强于分层空时码系统的性能，而且随着信噪比的增大，优势更加明显，特别在莱斯衰落信道中，分层空时码系统的误码率极其大，无论多大的信噪比，都对误码的改善甚微，而此时空时分组码和空时格型码表现出较好的信道增益效果。但是无论是瑞利衰落信道，还是莱斯衰落信道，或是天线相关信道，空时格型码系统相对于空时分组码都表现出较低的误码率，可见空时格型码的性能略高于空时分组码的性能。因此，为了使多媒体产品在 MIMO 信道上传输更加安全可靠，本课题选用空时格型码作为 MIMO 系统的编译码方式。

### 3.5 本章小结

本章讨论了 MIMO 系统的几个关键技术，首先介绍 MIMO 系统的信道容量，并对单天线信道和多天线信道容量进行了仿真，得出多天线对信道容量的增加有明显的的作用；然后讨论了 MIMO 信道的特性——衰落，并对不同莱斯因子和不同相关系数的衰落对信道容量的影响作了仿真；最后重点研究了空时编码技术，并结合 MIMO 信道衰落的特性，得出空时格型码的抗衰落性能在三种空时编码中最佳。

## 第 4 章 基于 MIMO 系统的数字水印技术的应用

无线信道是采用电磁波在空间自由的传播来实现信息的传输，因此由于天气原因、环境影响或人为的因素造成的不确定有很多，因此在像 MIMO 系统这样高速率大带宽的无线信道里采用将多媒体信息中加入数字水印来保护产品版权是十分具有现实意义的措施。

本章将数字水印技术应用于 MIMO 系统的无线传输信道上以实现多媒体信息的安全传输。

### 4.1 系统的总体设计方案

多媒体产品应用数字水印技术作为版权保护的方式，是因为数字水印具有重要的两个特性，即不可见性和鲁棒性。根据前面几章的分析，为了提高数字水印的抗攻击能力和自我检错的能力，采用经过 Turbo 编码预处理过的水印信息，而且为了抵抗 MIMO 无线传输信道上的各种衰落，应采用性能最好的空时格型码技术。

#### 4.1.1 系统发送端设计

将已嵌入 Turbo 水印的图像，转化为一维的比特流送入 MIMO 系统的空时格型码编码器进行无线信道的传输，其过程如图 4-1。

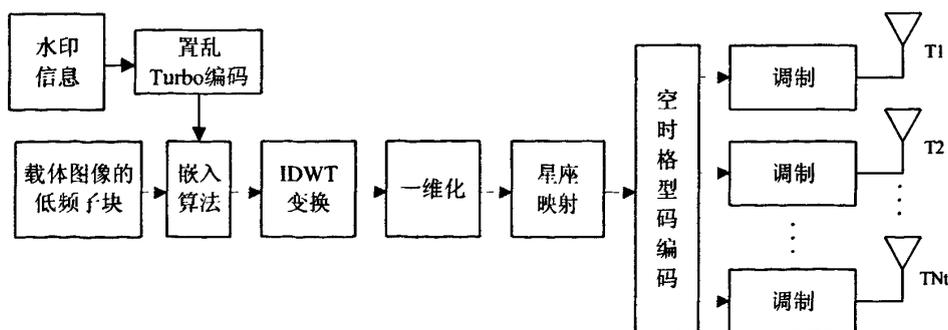


图 4-1 MIMO 系统发送端原理图

发送端系统分为数字水印的嵌入和信号的发送，具体步骤如下：

1) 水印信息采用有特殊意义的图像，它代表需嵌入水印的载体图像的版权信息。数字水印的图像的生成和嵌入算法采用 2.3 节所描述的方法，即将混沌置乱和 Turbo 编码后的数字水印采用小波变换域均值量化算法嵌入载体图像中。

2) 在产生已嵌入水印信息的图像后，需将其转为一维的序列，并且将图像各像素点的灰度值用 8 位二进制数表示，产生一维的比特序列。

3) 然后将一维序列送入空时编码器，通过星座映射和空时格型码的编码器，在某一时刻被平均分为  $N_t$  段相同长度的数据符号，分别对应  $N_t$  个发射天线，再对每段数据符号分别进行脉冲成形调制，将调制信号通过天线发送出去。

#### 4.1.2 系统接收端设计

天线接收到的数据符号通过空时格型码译码器，得到嵌有水印信息的图像，对该图像采用 Turbo 水印提取算法提取水印信息，其过程如图 4-2。

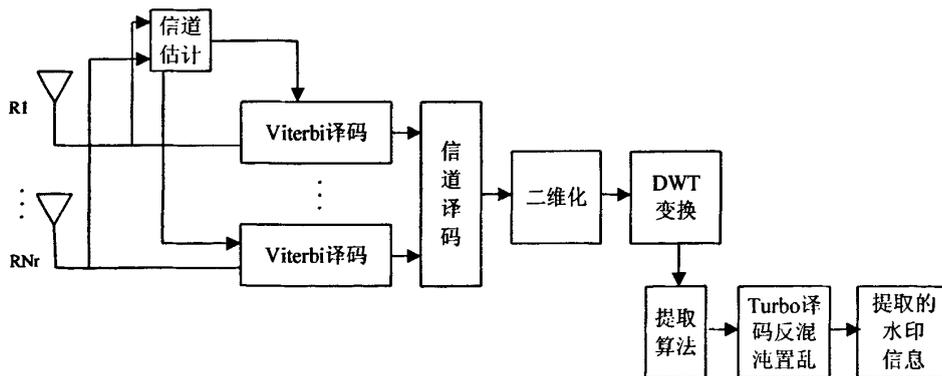


图 4-2 MIMO 系统接收端原理图

信号序列从发送天线到接收天线，经过了无线衰落信道，抵达接收端被天线接收，接收端对信号处理得到需要的信息。接收端系统分为信号的接收和水印的提取，具体步骤如下：

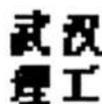
1) 由于 MIMO 编码器采用的是空时格型码，因此在接收端解码时需要知道信道的状态信息，需首先对天线接收到的信息进行信道估计，得到信道的增益信息进入译码器，对每一时刻每一根天线上接收的信号分别进行 Viterbi 译码，保证误码的概率最小。

2) 输出的译码信息为一维的比特序列, 在进行水印提取前, 需将其做二维化处理。

3) 数字水印的提取采用 2.3 节所述的算法, 提取水印信息。

## 4.2 实验结果与分析

对  $2 \times 2$  的 MIMO 系统进行嵌入数字水印的图像的传输。MIMO 系统采用空时格型编码方式, 编码器为 4 状态的 4-PSK 星座映射, 译码器采用 Viterbi 译码算法。数字水印嵌入采用 Turbo 码与小波变换域均值量化结合的嵌入算法, 实现水印的盲检测。原始载体图像为  $256 \times 256$  标准的 lena.bmp 灰度图像如图 4-3 (a), 待嵌入的水印信息为  $22 \times 22$  的写有“武汉理工”字样的二值位图图像如图 4-3 (b)。



(a) 原始载体图像

(b) 原始水印图像

图 4-3 载体图像和待嵌入的水印图像

由于在无线信道中一般都会有信号的衰落, 因此仿真实验的信道也加入了衰落的成分, 分别对瑞利衰落信道、莱斯衰落信道和天线相关信道都进行了嵌入水印图像的传输。仿真平台为 MATLAB7.7。

### 4.2.1 瑞利衰落信道上的信息传输

瑞利衰落信道适用于城镇地区, 衰落幅度服从瑞利分布, 接收端天线上的噪声为信噪比 (SNR) 取 10dB 的高斯白噪声。其嵌入与传输的效果如图 4-4。



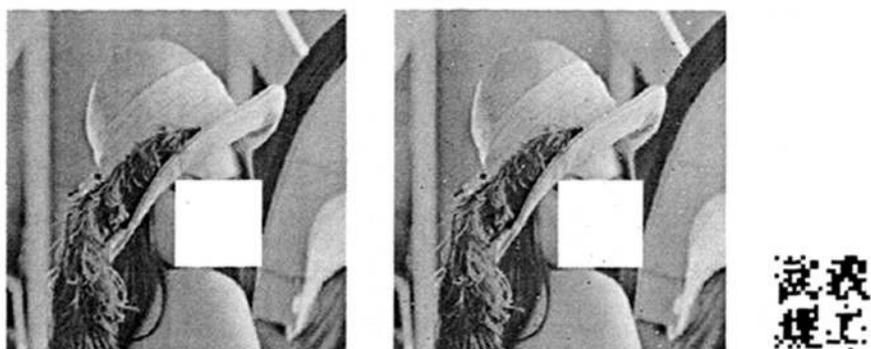
(a) 发送端已嵌入水印的图像 (b) 接收端输出图像 (c) 接收端提取水印图像  
图 4-4 瑞利衰落信道下仿真实验效果

已嵌入水印的图像与原始图像的峰值信噪比  $PSNR=305.7166$ ，高的峰值信噪比说明水印嵌入算法具有良好的不可见性。图 4-4 (b) 中 lena 图像与发送端的图像相比多了一些不均匀的黑白噪点，这是由于图像通过瑞利衰落信道造成的，此时它与原始载体图像的归一化相关系数  $NC=0.9993$ ，表明信息在无线通信的瑞利衰落信道上传输有一定的损失，但损失不大。提取的水印图像与原始水印图像间的  $NC=0.9682$ ，即提取的水印质量较好，水印抗瑞利衰落的鲁棒性较强。

信息在传输的过程中可能被人为的篡改，比如剪切、JPEG 压缩、旋转等等，这种盗版侵权的现象屡有发生，致使接收到的信息并不是原来发送端发送的信息，此时能提取接收信号的水印信息，将是对盗版现象的一个有力的打击。因此实验对各种攻击后的图像在瑞利衰落信道上传输进行仿真。

#### 1) 剪切攻击

不法分子经常对一幅图像最重要的部分进行剪切，如图 4-5 (a) 对 lena 图像的人物脸部剪切，在同样参数的瑞利衰落信道上传输，水印提取效果如图 4-5。



(a) 剪切后的图像 (b) 接收端输出图像 (c) 接收端提取水印图像

图 4-5 瑞利衰落信道下剪切攻击后仿真实验效果

### 2) JPEG 压缩攻击

对嵌入水印的图像进行 JPEG 压缩，压缩因子的值取 80，水印提取效果如图 4-6。



(a) JPEG 压缩后的图像 (b) 接收端输出图像 (c) 接收端提取水印图像

图 4-6 瑞利衰落信道下 JPEG 压缩攻击后仿真实验效果

### 3) 旋转攻击

将嵌入水印的图像向左旋转  $5^\circ$ ，水印提取效果如图 4-7。



图 4-7 瑞利衰落信道下旋转攻击后仿真实验效果

表 4-1 瑞利衰落信道实验数据

	攻击后图像 PSNR	接收端图像 NC	提取水印 NC
无攻击	—	0.9993	0.9682
剪切攻击	16.0823	0.9694	0.8916
JPEG 压缩攻击	38.2609	0.9990	0.9634
旋转攻击	16.1169	0.9638	0.8603

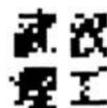
由图 4-5、4-6、4-7 以及表 4-1 可以看出，当嵌入了水印的图像受到攻击后，通过传输都有不同程度的被破坏，其中压缩因子为 80 的 JPEG 有损压缩对图像的影响最小，提取的水印图像几乎接近于不受攻击时的提取图像效果，而旋转攻击对图像的影响较明显，但提取出的水印图像均能较好的反映原始产品的版权信息。

#### 4.2.2 莱斯衰落信道上的信息传输

莱斯衰落信道适用于郊区，取莱斯因子为 100，同样接收端噪声为信噪比取 10dB 的高斯白噪声，水印嵌入载体图像后经 MIMO 无线衰落信道传输提取的效果如图 4-8。



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-8 莱斯衰落信道下仿真实验效果

接收端输出的图像与原始载体图像的归一化相关系数  $NC = 0.9977$ ，比瑞利衰落信道下接收的图像质量略差，表明莱斯因子为 100 的莱斯衰落信道比瑞利衰落信道对信号的影响更大，这是因为莱斯衰落信道由无散射仅有直射路径信道与只有散射而无直射路径信道两部分组成，它包含了瑞利衰落信道的部分特性。提取水印的效果比瑞利信道上的提取效果略差，此时归一化相关系数  $NC = 0.9646$ ，但从人眼来看几乎没有差别。

同样对莱斯衰落信道上的图像信息进行剪切、JPEG 压缩、旋转攻击进行仿真。仿真效果如图 4-9、4-10 和 4-11，表 4-2 则描述各攻击后输出图像与原始载体图像的归一化相关系数值和提取的水印图像与原始水印图像之间的归一化相关系数值。



(a) 接收端输出图像

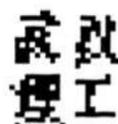


(b) 接收端提取水印图像

图 4-9 莱斯衰落信道下剪切攻击后仿真实验效果



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-10 莱斯衰落信道下 JPEG 压缩攻击后仿真实验效果



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-11 莱斯衰落信道下旋转攻击后仿真实验效果

表 4-2 莱斯衰落信道实验数据

	接收端图像 NC	提取水印 NC
无攻击	0.9977	0.9646
剪切攻击	0.9679	0.8862
JPEG 压缩攻击	0.9946	0.9420
旋转攻击	0.9605	0.8577

由图 4-9、4-10、4-11 和表 4-2 可以看出，在莱斯衰落信道上传输攻击后的图像受到的影响比在瑞利衰落信道上传输更加明显，虽然 JPEG 压缩攻击在这三种攻击中还是影响最小的，但与瑞利衰落信道相比较，莱斯信道对 JPEG 压缩攻击后的图像影响更大，衰减更多。

### 4.2.3 天线相关信道上的信息传输

天线相关信道既适用于郊区也适用于室内的环境，它是在瑞利衰落信道基础上增加了天线的相关特性的信道。取相关系数为 0.5，同样接收端噪声为信噪比取 10dB 的高斯白噪声，其嵌入与传输的效果如图 4-12。



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-12 天线相关衰落信道下仿真实验效果

接收端输出的图像与原始载体图像的归一化相关系数  $NC=0.9973$ ，比瑞利衰落信道下接收的图像质量差，这是因为天线相干信道是在瑞利衰落信道的基础上增加的相干天线的影响，衰落程度比瑞利衰落信道深。提取的水印的效果也比瑞利信道上的提取效果稍差。而与莱斯衰落信道的接收图像的效果相差不多。此时水印的归一化相关系数  $NC=0.9601$ 。

同样对天线相干信道上的图像信息进行剪切、JPEG 压缩、旋转攻击进行仿真。仿真效果如图 4-13、4-14 和 4-15，表 4-3 则描述了各攻击后输出图像与原始载体图像的归一化相关系数值和提取的水印图像与原始水印图像之间的归一化相关系数值。



(a) 接收端输出图像

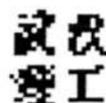


(b) 接收端提取水印图像

图 4-13 天线相关衰落信道下剪切攻击后仿真实验效果



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-14 天线相关衰落信道下 JPEG 压缩攻击后仿真实验效果



(a) 接收端输出图像



(b) 接收端提取水印图像

图 4-15 天线相关衰落信道下旋转攻击后仿真实验效果

表 4-3 天线相关信道实验数据

	接收端图像 NC	提取水印 NC
无攻击	0.9973	0.9601
剪切攻击	0.9581	0.8906
JPEG 压缩攻击	0.9971	0.9564
旋转攻击	0.9548	0.8538

由图 4-13、4-14、4-15 和表 4-3 可以看出, 相关信道对攻击后的图像的影响都比瑞利衰落信道对攻击后的图像的影响大, 与莱斯因子为 100 的莱斯衰落信道相比, 无攻击和剪切攻击时提取的水印信息效果不如莱斯衰落信道, 而 JPEG 压缩、攻击和旋转攻击时的提取效果则比莱斯衰落信道好。

三种衰落信道中, 都能实现水印的盲检测, 并且得到水印的较好提取效果, 其中, 瑞利衰落信道对提取水印的影响最小, 相干系数为 0.5 的天线相干衰落信道对水印的提取影响较大, 而相干衰落信道对水印提取的效果与莱斯信道相比差距不大。对于攻击后图像的传输, 数字水印最能抵抗 JPEG 压缩的攻击, 对旋转攻击的抵抗能力稍差, 提取的水印信息均能很好的反映多媒体产品的版权。

### 4.3 本章小结

本章将数字水印技术应用于 MIMO 系统中, 水印的嵌入与提取算法采用能抵抗多种攻击的 Turbo 算法和能实现水印盲检测的小波域均值量化嵌入算法, MIMO 系统采用对抗无线信道衰落最有效的空时格型码。最后对建立起的系统在各种衰落信道以及不同攻击方式下进行仿真, 得到提取效果较佳的水印图像, 并实现了接收端的盲检测。

## 第 5 章 总结与展望

在笔者攻读研究生的几年中，有幸亲临 3G 通信时代给神州大地带来翻天覆地的变化。2008 年 8 月，北京奥运会在通信行业的代名词几乎就是 3G；2009 年 5 月，各大运营商开始向民众推广 3G 业务；如今 3G 以较便宜的价格、新鲜的业务、广泛的服务被越来越多各行业人士所接受。与此同时，我们期待着速度更快、信息量更大、传输更可靠的 4G 通信时代的来临。

以 MIMO 技术为核心的 4G 无线通信系统，应用多天线阵列技术得到大容量的信道，可以满足人们进行流畅的视频通话、高速的文件传输等需求。同时也带来了严重的多媒体产品盗版侵权危害。因此，本文将不影响原始多媒体信息视觉效果的数字水印技术引入 MIMO 系统的无线传输中，实现多媒体产品的版权保护。

### 5.1 本文的主要工作

本文主要对数字水印在 MIMO 系统信道中传输的应用进行了研究，所涉及的内容有：

1) 对数字水印技术的研究现状作了概述，研究了使用纠错编码进行数字水印信息的预处理可以提高水印的鲁棒性。通过实验验证 Turbo 编码预处理过的水印的抗攻击性能在所有纠错编码水印中是最优的。并采用小波变换后低频域的均值量化嵌入算法，实现了检测端不需要原始载体图像参与的水印盲提取；

2) 研究了 MIMO 系统的几个关键技术和 MIMO 系统在无线信道传输中会产生各种衰落和影响。从分析信道容量中得出传输使用的天线数目越多，信道增益就越大。而实现多天线传输的技术是空时编码，也是 MIMO 系统中最重要的技术。

通过对三种空时编码技术的分析和比较，得出空时格型码在任何衰落信道中的低误符号率性能是其他空时编码不可比拟的。因此本文选用空时格型码作为 MIMO 空时码的关键技术对多媒体产品进行分集发送和合并接收，能有效地抵抗无线传输中的衰落和噪声。

3) 将 Turbo 码数字水印技术应用于 MIMO 系统中。针对无线信道的衰落

特性和各种人为的攻击，对算法的鲁棒性和不可见性进行分析。此算法对各种衰落和攻击具有良好的鲁棒性，而且在接收端进行水印提取时不需要原始载体图像的参与，具有极强的实用性。

## 5.2 未来工作的展望

结合本文的研究工作和多媒体信息传播的发展趋势，在以下几个方面，需要在后续的工作中进一步完善。

1) 本文采用的 Turbo 算法数字水印并不是在所有的攻击情况下都是最佳的算法，比如在椒盐噪声的影响下，Turbo 算法提取的水印效果不如 BCH 编码预处理过水印的提取效果。因此，在抗攻击性能上，数字水印的算法还需进一步完善。

2) 数字水印技术由于采用了小波变换域的均值量化技术，嵌入容量不高，再由于 Turbo 编码对水印进行了增加校验位的处理，更使嵌入容量降低，嵌入水印的容量问题尚待解决。

3) 空时格型码的性能的确优于其他空时编码，但是译码复杂度是一个非常明显的问题，特别在更多天线的信道和传输信息量大时，接收端的译码过程需要经过很长时间才能完成。今后的工作可以运用性能略低于空时格型码但运算简单的空时分组码作为 MIMO 编译码技术。

## 致 谢

本论文的写作伴随着众多老师同学和亲友的支持与帮助而完成的，借此机会，谨向曾经帮助我的老师同学和亲朋好友表达我最诚挚的感谢。

首先衷心感谢我的导师杨杰教授，在我研究生学习的过程中，处处得到导师的关怀和帮助。学习上，无论是进校时的课程选择、项目指导，还是研究课题的确立、技术上的帮助、论文精心的审阅，杨老师都为此倾注了汗水；生活上，杨老师也对我们关怀备至并给与了极大的帮助。杨老师正直的品格、严谨的治学态度、渊博的学识、缜密的学术思维对我有着潜移默化的影响，终身受益。

特别感谢信号与信息处理专业的王虹老师、阙大顺老师、杨春金老师、胡君萍老师、沈维聪老师等等在硕士期间对我的培养和教诲，赋予我知识，开阔了我眼界，使我在两年半的学习中能顺利完成学业。你们科学的学习方法和求实的学习态度深深感染了我，让我在以后的学习道路中严于律己求实求新。

同时感谢实验室里一起奋斗过的范亚琼、金克琼、李亚南、简雄军、马海、王舸、陈寅和周慧博士以及所有 07 级信号与信息处理专业的同学。他们营造了浓厚的学习氛围和融洽的工作环境，给与了我很多的帮助，使我度过了快乐的研究生生涯。

最后感谢父母及亲友对我的理解和支持，让我毫无负担的完成学业。

再次感谢所有支持和帮助我的人！

## 参考文献

- [1] 黄韬,袁超伟,杨睿哲,刘鸣. MIMO 相关技术与应用[M]. 北京: 机械工业出版社, 2007
- [2] 中国联通网站.B3G 无线通信技术的发展趋势 [EB/OL] .[2009-7]  
[http://www.xzra.gov.cn/news\\_con.aspx?id=367](http://www.xzra.gov.cn/news_con.aspx?id=367)
- [3] 王颖,肖俊,王蕴红. 数字水印原理与技术[M]. 北京: 科学出版社, 2007.3
- [4] Guangze Zhao Loyka, S. Impact of Multipath Clustering on the Performance of MIMO systems[J]. Wireless Communications and Networking Conference, IEEE, 2004: 1056~1061
- [5] 俞晓帆, 王建国. 垂直分层空时码系统 (V-BLAST) 及其检测算法研究[J]. 电力系统通信, 2005, 第 26 卷: 76~80
- [6] Valenzuela, Golden, G D R A Wolniansky. Detection algorithm and initial laboratory results using V-BLAST space-time communication architecture[J]. Electronics Letters, 1999,35 (1) : 14~16
- [7] D. Gesbert, M. Shafi, D. Shiu, P. J. Smith. From Theory to Practice: An Overview of MIMO Space-Time Coded Wireless Systems[J]. IEEE Journal on Selected Areas in Communications. 2003,Vol.21: 281~287
- [8] V. Tarokh, N. Seshadri, A. R. Calgerbank. Space-time codes for high data rate wireless communication: Performance criterion and code construction[J]. IEEE Trans Info Theory, 1998, 44(3): 744~765
- [9] Georgios B, Zhiqiang Liu, Xiaoli Ma 著, 王钢 译. 宽带无线通信中的空时编码 (Space Time Coding for Broadband Wireless Communications) [M]. 北京: 机械工业出版社, 2009
- [10] L. Shao, S. Roy. Rate-one space-frequency block codes with maximum diversity for MIMO-OFDM[J]. IEEE Trans, Wireless Communication. 2005, Vol. 4, no. 4, pp: 1674~1687
- [11] L. Gordon, R. John. Broadband MIMO-OFDM Wireless Communications[J]. Proceedings of the IEEE. 2004, Vol.92, no.2, pp: 2232~2236
- [12] 王洪婷. 基于纠错编码的图像数字水印技术研究[D]. 华北电力大学硕士学位论文, 2008.
- [13] 搜狐网.钱铮. 日本电信公司开发出数字水印, 防伪技术更加高明[EB/OL]. [2008-11-2]  
<http://it.sohu.com/20081102/n260386570.shtml>
- [14] 中关村在线. 陈亮. 保护知识产权, 爱国者发布数字水印相机 [EB/OL] . [2009-4-22]  
<http://dcdv.zol.com.cn/130/1304980.html>.
- [15] 樊昌信, 张甫翊,徐炳祥,吴成柯. 通信原理(第 6 版)[M]. 北京: 国防工业出版社, 2006

- [16] C. Berrou, A. Glaienux, P. Thitimajshima. Near Shannon Limit Error-correcting Coding and Decoding: Turbo-Codes[J]. Proc ICC'93, 1993: 1064~1070
- [17] 杨素敏,王嘉祯,张政保等. 基于 Turbo 和小波分形的数字水印算法[J]. 机械工程学院学报, 2006: 48~51
- [18] 孙圣和,陆哲明,牛夏牧. 数字水印技术及应用[M]. 北京: 科学出版社, 2004
- [19] 胡艳维. 基于 TURBO 码的鲁棒性数字水印算法[D]. 湖南大学硕士学位论文, 2006
- [20] 王军选,张晓燕,张燕燕. 无线通信调制与编码[M]. 北京: 人民邮电出版社,2008
- [21] 文睿. Turbo 码的研究及在 DS/CDMA 系统中的应用[D]. 哈尔滨工程大学硕士学位论文, 2007
- [22] Yen Jui Cheng, Guo Jiun In. A new chaotic key-based design for image encryption and decryption[J]. Proc IEEE Int Systems, 2007: 49~52
- [23] T. Kohda T and A. Tsuneda. Pseudo noise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties[J]. IEICE Transactions on Communications. 1993, E76-B(8): 855~862
- [24] L. H. Chen and J. J. Lin. Mean Quantization Based Image Watermarking. Image and Vision Computing[J], 2003,21:717~727
- [25] 朱冰莲,陈禧. 基于卷积码和量化的盲数字水印算法[J]. 光电子激光, 2007:617~620
- [26] M. Kutter and F. A. P. Petitcolas. A Fair Benchmark for Image Watermarking Systems[J]. Proceedings of SPIE. 1999: 36~57
- [27] 陈丽萍. 基于纠错码的水印技术研究[D]. 福建师范大学硕士学位论文, 2005
- [28] 伍欲江,聂在平. MIMO 无线通信系统的统一建模[J]. 系统仿真学报, 2008: 1036~1040
- [29] 魏崇毓. 无线通信基础及应用[M]. 西安: 西安电子科技大学出版社, 2009
- [30] 李光球. 相关衰落信道上 MIMO 系统中组合 SC/MRC 的性能分析[J]. 电波科学学报, 2009, 第 24 卷: 103~107
- [31] 赖国庭, 尹俊勋, 喻华文. 空间相关莱斯快衰落信道下的 MIMO 系统性能[J]. 华南理工大学学报(自然科学版), 2006: 34~36
- [32] 吴伟陵. 移动通信中的关键技术[M]. 北京: 北京邮电大学出版社, 2003
- [33] I. E. Telatar. Capacity of Multi-Antenna Gaussian Channels[J]. European Transactions on Telecommunications. 1999,10(6): 585~595
- [34] 杨曦. MIMO 空时编码技术比较研究[J]. 信息技术, 2006: 103~105
- [35] R. Kalbasi, D. D. Falconer, A. H. Banihashemi. Optimum Power Allocation for a V-BLAST System with Two Antennas at the Transmitter[J]. IEEE Communications Letters. 2005, vol.9, No.9, pp: 826~828
- [36] 邓自立. 最优估计理论及应用[M]. 哈尔滨: 哈尔滨工业大学出版社, 2005

- [37] 李可. MIMO 空时码技术研究[D]. 电子科技大学硕士学位论文, 2006
- [38] V. Tarokh, H. Jafarkhani, A. R. Calderbank. Space-time Block Coding for Wireless Communications: Performance Results[J]. IEEE Journal on selected areas in communications, 1999, 17(3): 451~460
- [39] L. Xian, H. Liu. Optimal Rotation Angles for Quasi-orthogonal Space-time Codes with PSK Modulation[J]. IEEE Communications Letters. 2005, vol.9, No.8, pp: 676~678,
- [40] 江藤良纯. 纠错码及其应用[M]. 北京: 科学出版社, 2004
- [41] 吴虹, 丁勇, 赵迎新等. 一种 MIMO-OFDM 无线通信系统的设计与仿真[J]. 电讯技术, 2008: 30~33
- [42] 陈逸. MIMO-OFDM 系统信道估计方法研究[D]. 东南大学硕士学位论文, 2006
- [43] 李丽娟. 基于 OFDM 的无线传输中数字水印的应用研究[D]. 武汉理工大学硕士学位论文, 2007
- [44] 邓华. MATLAB 通信仿真及应用实例详解[M]. 北京: 人民邮电出版社, 2003
- [45] 孙屹, 李妍. MATLAB 通信仿真开发手册[M]. 北京: 国防工业出版社, 2005
- [46] 韦刚, 季飞, 傅娟. 通信系统建模与仿真[M]. 北京: 电子工业出版社, 2007

## 攻读硕士学位期间发表的论文情况

1. 罗静,杨杰. 基于 MIMO 无线通信系统的数字水印应用的研究. 中国科技论文在线, 2009.09
2. 罗静,杨杰. 基于 Turbo 码和小波变换的盲数字水印算法. 中国科技论文在线, 2009.10