高等学校电子信息类专业
“十三五”规划教材

ELECTRONIC
INFORMATION SPECIALTY

编码理论

（第三版）

田丽华　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息类专业“十三五”规划教材

编 码 理 论

（第三版）

田丽华 编著

西安电子科技大学出版社

内 容 简 介

本书系统地介绍了信源压缩编码、信道纠错编码、密码编码及组合编码等的基本原理及应用，同时简单介绍了学习本书所需的信息理论、数论及近代代数的相关知识。主要内容有信息传输系统研究的对象、目的和内容，信源及其信息度量，信道及其信道容量，信源压缩编码原理及编码方法，信道纠错编码的基本原理和编码方法，密码编码的基本原理和编码方法，消息认证的相关知识，组合编码原理及编码方法。

本书叙述通俗易懂，内容由浅入深、循序渐进，重点突出，对物理概念和编码的基本原理的阐述清晰明了，实用性强，可作为电子信息类、信息工程类、计算机类等专业本科生和研究生的教材或参考书，也可供相关专业的科技人员参考。

图书在版编目(CIP)数据

编码理论/田丽华编著. —3 版. —西安：西安电子科技大学出版社，2016.12
高等学校电子信息类专业“十三五”规划教材
ISBN 978-7-5606-4081-5

Ⅰ. ① 编… Ⅱ. ① 田… Ⅲ. ① 编码理论—高等学校—教材 Ⅳ. ① O157.4

中国版本图书馆 CIP 数据核字(2016)第 290796 号

策　　划　云立实
责任编辑　买永莲
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西华沐印刷科技有限责任公司
版　　次　2016 年 12 月第 3 版　2016 年 12 月第 7 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 23
字　　数　548 千字
印　　数　23001～26000 册
定　　价　40.00 元
ISBN 978-7-5606-4081-5/O
XDUP　4373003-7

前　言

编码理论既是一门工程科学，又是一门应用科学，同时又是一门不断发展的学科。信源压缩编码、信道纠错编码及密码编码是信息编码的三大核心内容。本书试图用有限的篇幅将信源压缩编码、信道纠错编码、密码编码以及组合编码等所有重要基本原理及方法有机结合起来，使之具有知识性、可研究性、实用性、先进性、综合性，使之结构严谨、合理而系统，使之物理概念清晰、通俗易懂、由浅入深、循序渐进，使之具有较强的应用性。书中突出了编码理论在信息传输系统中的应用，有助于读者了解理论产生的实际背景，从而有利于提高读者解决实际问题的能力，提高工科学生的学习兴趣。此外，本书的示例丰富，可方便读者学习。

学习本书所要求的数学基础知识是初等的，只需具备概率论、随机过程、线性代数等知识即可。同时，本书对所要求的数学基础中的数论、离散数学及近代代数中的初等知识，做了必要的介绍，供读者学习时参考。

全书共16章，系统地介绍了信源的压缩编码、信道的纠错编码、密码编码学及组合编码等的基本原理及应用，同时简单介绍了学习本书需要的数论及近代代数的相关知识。书中除了第10.5节的“秩距离码”以外的内容都适合于本科教学，其中第6章可以不讲，供学习相关内容时参考。书中有些较深的内容，对本科生讲授时，可作适当取舍，或只讲授基本内容，如BCH码、Goppa码、秩距离码、AES算法、IDEA算法、EIGamal算法、椭圆曲线加密算法、Turbo码及TCM码等。

本书是作者在多年教学经验和实践经验的基础上编写而成的，其中，蔡东杰编写了第12章、第14章和第15章的内容，田立军编写了第6章、第8章及第10章的内容，李金峰编写了第11章、第13章及第16章的内容，其余章节的内容均由田丽华编写，书中的所有图形均由蔡东杰设计并绘制。

近几十年来，国内外有不少信息编码方面的优秀教科书和专著，本书的编写得益于作者以前对于这些著作的学习。此外，在编写过程中还参阅了许多文献、资料，在此对这些著作的作者深表谢意。

同时，感谢吉林大学提供的良好的教学及科研环境；感谢信息系的领导及同事提出的宝贵意见及提供的帮助；感谢西安电子科技大学出版社的信任与支持，以及工作

人员的辛勤劳动；感谢教过的几届学生，他们的反馈为本书改进提供了很好的帮助；感谢我的家人，没有他们的支持与理解，本书是不可能完成的；感谢在本书编写过程中所有给予过热情帮助的前辈、同行及学生们：王新梅、康键、云立实、杨晓萍、王国鸿、张巍、周文慧等。

限于作者的水平，书中不妥之处在所难免，欢迎读者将发现的错误、遗漏以及其他的建议发至邮箱 tlh85@sina.com。

作　者

2016 年 3 月

目 录

第1章 绪 论

美国数学家香农(C. E. Shannon)在1948年发表的著名论文《通信的数学理论》，开创了一门在现代科学技术中具有重大意义的崭新的学科——信息论。信源压缩编码、信道纠错编码、密码编码构成了信息论的核心内容。目前，编码方法繁多，发展也相当迅速，随着根据不同应用目的而制定的压缩编码的国际标准的相继推出，再加上数学、工程技术以及计算机本身体系结构软、硬件性能的深入发展和提高，编码的理论和技术得到了前所未有的发展和应用。

1.1 信息传输系统

1.1.1 信息传输的目标

研究通信系统的目的就是要找到信息传输过程的共同规律，以提高信息传输的可靠性、有效性、保密性和认证性，从而使信息传输系统最优化。所谓的高可靠性，就是要使信源发出的消息经过信道传输以后，尽可能准确、不失真地再现在接收端。而所谓的高有效性，就是经济效果好，即用尽可能短的时间和尽可能少的设备来传送一定数量的信息。提高可靠性和提高有效性常常会发生矛盾，需要统筹兼顾。例如，为了兼顾有效性(考虑经济效果)，有时不一定要求绝对准确地在接收端再现原来的消息，而是可以允许一定的误差或一定的失真，或者说允许近似地再现原来的消息。所谓的保密性，就是隐蔽和保护通信系统中传送的消息，使它只能被授权接收者获取，而不能被未授权者接收和理解。所谓的认证性，是指接收者能正确判断所接收消息的正确性，验证消息的完整性，确认消息不是伪造的和被篡改的。上述可靠性、有效性、保密性、认证性，加上经济性构成了现代通信系统对信息传输的全面要求。

1.1.2 信息传输系统模型

各种现代数字通信系统，如电报、电话、无线电、电视、广播、因特网、遥测、遥控、雷达和导航等，虽然形式和用途各不相同，但本质是相同的，都是信息的传输系统。为了便于研究信息传输和处理的共同规律，将各种通信系统中具有共同特性的部分抽取出来，概括成一个统一的理论模型，如图1-1所示，通常称它为信息传输系统模型。

图1-1所示的信息传输系统模型也适用于其他的信息流通系统，如生物有机体的遗传系统，人体、动物的神经网络系统和视觉系统等，甚至人类社会的管理系统都可用这个模型来概括。人们通过系统中消息的传输和处理来研究信息传输和处理的共同规律。信息传输或通信的目的，是要把收方不知道的信息及时、可靠、完整、安全而又经济地传送给指定

的收方。该模型按功能可分为信源、编码器、信道、译码器、信宿五个部分。

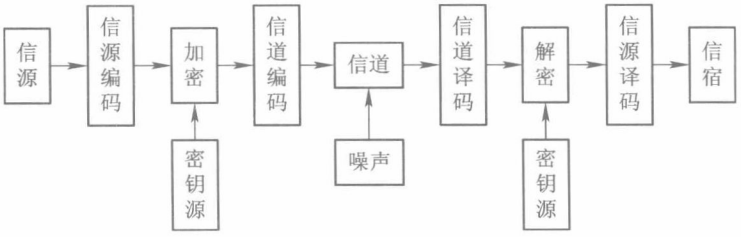

图 1-1　信息传输系统模型

1. 信源

信源是产生消息和消息序列的源，可以是人、生物、机器或其他事物，它是事物各种运动状态或存在状态的集合。信源发出的消息有语音、信源、文字等，人的大脑思维活动也是一种信源。信源的输出是消息，消息是具体的，但它不是信息本身。另外，信源输出的消息是随机的、不确定的，但又有一定的规律性。信源输出的消息有多种形式，可以是离散的或连续的、平稳的或非平稳的、无记忆的或有记忆的。

2. 编码器

编码器可分为信源编码器、信道编码器和保密编码器三种。信源编码器对信源输出的消息进行适当的变换和处理，可提高信息传输的效率。为了使传输更为经济、有效，还要去掉一些与被传输信息无关的多余度。信道编码器可提高信息传输的可靠性，保密编码器可保证信息的安全性。由于传输信息的媒质如电波、有线等总是存在各种人为或天然的干扰和噪声，因此，为了提高整个通信系统信息传输的可靠性，就需要对加密器输出的信息进行一次纠错编码，人为地增加一些多余信息，使信息传输系统具有自动检错或纠错功能。当然，对于各种实际的通信系统，编码器还应包括换能、调制、发射等各种变换处理功能。

3. 信道

信道是信息传输和存储的媒介，是通信系统把载荷消息的信号从甲地传输到乙地的媒介。在狭义的通信系统中，实际信道有明线、电缆、波导、光纤、无线电波传播空间等，这些都属于传输电磁波能量的信道。当然，对于广义的通信系统来说，信道还可以是其他的传输媒介。信道除了传输信号以外，还有存储信号的作用。在信道中还存在噪声和干扰，为了分析方便起见，把在系统其他部分产生的干扰和噪声都等效地折合成信道干扰，看成由一个噪声源产生的，它将作用于所传输的信号上。这样，信道输出的已是叠加了干扰的信号。由于干扰或噪声往往具有随机性，所以信道的特性也可以用概率空间来描述。

4. 译码器

译码器就是编码器的反变换。一般认为这种变换是可逆的。译码器也可分成信源译码器、信道译码器和保密译码器三种。

5. 信宿

信宿是消息传送的对象，即接收消息的人或机器。

图 1-1 给出的模型只适用于收发两端单向通信的情况。它只有一个信源和一个信宿，信息传输也是单向的。更一般的情况是信源和信宿各有若干个，即信道有多个输入和多个

输出。另外，信息传输也可以双向进行。例如，广播通信是一个输入、多个输出的单向传输通信，因特网是多个输入、多个输出的多向传输通信，卫星通信网也是多个输入、多个输出的多向传输通信。

1.2 信息编码的发展

1.2.1 信源压缩编码的发展

1948年，香农在《通信的数学理论》一文中，用概率测度和数理统计的方法系统地讨论了通信的基本问题，得出了几个重要而带有普遍意义的结论。香农理论的核心是：在通信系统中采用适当的编码后能够实现高效率和高可靠性的信息传输，并得出了信源编码定理和信道编码定理。从数学观点看，这些定理是最优编码的存在定理。但从工程观点看，这些定理不是结构性的，不能从定理的结果直接得出实现最优编码的具体途径。然而，它们给出了编码的性能极限，在理论上阐明了通信系统中各种因素的相互关系，为人们寻找最佳通信系统提供了重要的理论依据。

从无失真信源编码定理出发，1948年，香农在论文中提出并给出了简单的编码方法(香农编码)。1952年，费诺(Fano)提出了费诺编码；同年，霍夫曼(D. A. Huffman)构造了霍夫曼编码，并证明了它是最佳码。霍夫曼编码是有限长度的块码中最好的码，亦即它是代码总长度最短的码。1949年，克拉夫特(L. G. Kraft)提出了克拉夫特不等式，指出了即时码的码长必须满足的条件。后来，麦克米伦(B. McMillan)在1956年证明唯一可译码也满足此不等式。1961年，卡拉什(J. Karush)简化了B. McMillan的证明方法。

霍夫曼编码在实际中已有所应用，但它仍存在一些块码及变长码所具有的缺点。例如，概率特性必须精确地测定，它若略有变化，还需更换码表；而二元信源常需多个符号合起来编码，才能取得好的效果等。因此，霍夫曼编码在实用中常需作一些改进，同时也就有研究非块码的必要性。算术编码就是一种非块码，它是从整个序列的概率匹配的角度来进行编码的。其实，此概念也是由香农首先提出来的，后经许多学者改进，已逐渐进入实用阶段。1968年前后，埃利斯(P. Elias)发展了香农-费诺码，提出了算术编码的初步思路。1976年，里斯桑内(J. Rissanen)给出和发展了算术编码，并于1982年和兰登(G. G. Langdon)一起将算术编码系统化，省去了乘法运算，使其更为简化，易于实现。

若对概率特性未知或不确知的信源进行有效的编码，上述方法已无能为力。对有些信源，要确知信源的统计特性相当困难，尤其是高阶条件概率，何况有时信源的概率特性根本无法测定，或是否存在也不知道。例如，地震波信号就是如此，因为无法取得大量实验数据。当信源序列非平稳时，其概率特性随时间而变更，要测定这种信源的概率特性也近乎不可能。因此总希望能有一种编码方法，通用于各类概率特性的信源。通用编码就是在信源统计特性未知时，对信源进行编码，且编码效率很高的一种码。

20世纪70年代末，以色列学者兰佩尔(A. Lempel)和奇费(J. Ziv)提出一种语法解析码(简称LZ码)。1977年，他们首先提出这种基于字典的方法，1978年又提出了改进算法，分别称为LZ77算法和LZ78算法。1984年，韦尔奇(T. A. Welch)以LZ码中的LZ78算法为基础修改成一种实用的算法，后定名为LZW算法。LZW算法保留了LZ78算法的自

适应性能，压缩效果也大致相同，但 LZW 算法的显著特点是逻辑性强，易于硬件实现，且价格低廉，运算速度快。LZW 算法已经作为一种通用压缩方法，广泛应用于二元数据的压缩。

前面介绍的无失真信源编码只适用于离散信源或数字信号，不适用于连续信源或模拟信号，如语音、图像等信号的数字处理。因为连续信源的每个样值所能载荷的信息量是无限大的，而数字信号的值则是有限的，所以对连续信源不引入失真是不可能的。并且连续信号所对应的信宿一般是人，当失真在某一限度以下时是不易被人感觉到的，因此是容许的。连续信源编成代码后就无法无失真地恢复原来的连续值，此时只能根据率失真理论进行限失真编码。限失真信源编码的研究较信道编码和无失真信源编码落后约十年左右。1948 年，香农在其论文中已体现出了关于率失真函数的思想，1959 年他发表了《保真度准则下的离散信源编码定理》一文，首先提出了率失真函数及率失真信源编码定理。率失真信源编码理论是信源编码的核心问题，是频带压缩及数据压缩的理论基础，直到今天，它仍是信息论研究的课题。

以上简述了根据香农信源编码定理发展起来的各种信源编码方法，这些方法都是从概率论形成的信息出发，通过去掉冗余而达到压缩码率的目的。

现在，编码理论与技术不仅在通信、计算机以及自动控制等电子学领域中得到了直接的应用，而且还广泛地渗透到生物学、医学、生理学、语言学、社会学和经济学等各领域。在编码理论与自动控制、系统工程、人工智能、仿生学、电子计算机等学科互相渗透、互相结合的基础上，形成了一些综合性的新兴学科。尤其是随着数学理论(如小波变换、分形几何理论、数学形态学等)以及相关学科(如模式识别、人工智能、神经网络、感知生理心理学等)的深入发展，世界范围内的有关专家一直在追求并寻找现有压缩编码的快速算法，同时，又在不断探索新的科学技术在压缩编码上的应用，因此，新颖、高效的现代压缩方法相继产生。

1.2.2 信道纠错编码的发展

在研究信源编码的同时，信道编码(纠错码)的研究工作也在进行着，并已经形成了一门独立的分支——纠错码理论。1950 年，汉明(R. W. Hamming)发表的论文《检错码与纠错码》是开拓编码理论研究的第一篇论文。这篇论文主要考虑在大型计算机中如何纠正编码中所出现的单个错误。1952 年，费诺(R. M. Fano)给出并证明了费诺不等式，同时，给出了关于香农信道编码逆定理的证明；1957 年，沃尔夫维兹采用类似典型序列的方法证明了信道编码强逆定理；1961 年，费诺又描述了分组码中码率、码长和错误概率的关系，并提供了香农信道编码定理的充要性证明；1965 年，格拉格尔(R. G. Gallager)发展了费诺的证明结论，并提供了一种简明的证明方法；1972 年，阿莫托(S. Arimoto)和布莱哈特(R. Blahut)分别发展了信道容量的迭代算法。1948 年，香农首先分析并研究了高斯信道问题；1964 年，霍尔辛格(J. L. Holsinger)发展了有色高斯噪声信道容量的研究；1969 年，平斯克尔(M. S. Pinsker)提出了具有反馈的非白噪声高斯信道容量问题；1989 年，科弗尔(T. M. Cover)对平斯克尔的结论给出了简洁的证明。从能够纠正单个错误的汉明码到能够纠正多个错误的 BCH 码，经历了整整 10 年的时间。因此，可以说 20 世纪 60 年代是代数编码理论发展的鼎盛时期。20 世纪 70 年代出现的 Goppa(高帕)码，又把编码理论推向了

一个新的高峰。到了 20 世纪 80 年代，茨伐斯曼(Tsfasman)等人运用代数几何的方法推广了 Goppa 码的思想，指出存在 GF(m)上的一列码。这一令人吃惊的结果给编码理论的进一步发展带来了新的希望。

汉明码出现后，人们把代数方法引入到纠错码的研究中，形成了代数编码理论。由此找到了大量可纠正多个错误的码，而且提出了可实现的编译码方法。但代数编码的渐近性能很差，不能实现香农信道编码定理所指出的结果，因此，1960 年左右，有人提出了卷积码的概率译码，并逐步形成了一系列概率译码理论，尤其是以维特比(Viterbi)译码为代表的译码方法被美国卫星通信系统所采用，使香农理论成为真正具有实用意义的科学理论。香农于 1961 年发表的论文《双路通信信道》开拓了网络信息论的研究。1970 年以来，随着卫星通信、计算机通信网的迅速发展，网络信息理论的研究异常活跃，成为当前信息论的中心研究课题之一。一方面，艾斯惠特(R. Ahlswede，1971 年)和廖(H. Liao，1972 年)找出了多元接入信道的信道容量区，在 1973 年，沃尔夫(J. K. Wolf)和斯莱平(D. Slepian)将它推广到具有公共信息的多元接入信道中，科弗尔和艾斯惠特也于 1983 年分别发表文章讨论相关信源在多元接入信道中的传输问题。另一方面，在 1972 年，科弗尔提出了广播信道的研究，伯格曼斯(P. Bergmans，1973 年)、格拉格尔(1974 年)、科弗尔(1975 年)、马登(K. Marton，1979 年)、伊·盖马尔(A. ElGamal，1979 年)和范·德·缪伦(E. C. Van der Meulen，1979 年)等人也先后分别研究了广播信道的容量区问题。多年来，这一领域的活跃研究使得网络信息论的存在理论日趋完善。

1.2.3　密码编码的发展

1949 年，香农的奠基性论文《保密系统的通信理论》(The Communication Theory Of Secrecy Systems)在《贝尔系统技术杂志》上发表，奠定了密码学理论基础。香农在论文中，首先用信息论的观点对信息保密问题作了全面的论述。由于保密问题的特殊性，直至 1976 年 Diffe 和 Hellman 发表了《密码学的新方向》一文，提出了公开密钥密码体制，保密通信问题才得到广泛研究。今天，信息的安全和保密问题更加突出和重要，人们通过把线性代数、初等数论、矩阵等知识引入保密问题的研究，形成了独树一帜的分支——密码学理论。

密码是一个古老的话题。早在四千多年前，古埃及人就开始使用密码来保密传递的消息。作为保密信息的手段，密码技术本身也处于秘密状态，基本上仅限于军事目的，只为少数人掌握和控制，所以，它的发展受到了限制。

在第一次世界大战之前，密码技术的进展很少见诸于世，直到 1918 年弗里德曼(F. Friedman)的论文《重合指数及其在密码学中的应用》(The Index Of Coincidence and Its Applications in Cryptography)发表时，情况才有所好转。此后，直到 1967 年，密码学文献几乎空白。1967 年，戴维·卡恩(David Kahn)收集整理了第一次世界大战和第二次世界大战的大量史料，创作出版了《破译者》(The Codebreakers)，为密码技术的公开化、大众化拉开了序幕。此后，密码学的文献大量涌现。

20 世纪 70 年代是密码学发展的重要时期，其间有两件重大事件发生。其一，美国国家标准局(NBS，即现在的美国国家标准与技术研究院(NIST))开始数据加密标准(Data EncryptionStandard)的征集工作。1975 年 3 月 17 日，NBS 在 Federal Register 上公布了一个候选算法；1976 年 11 月 23 日，该算法被正式确认为联邦标准 DES，并授权在政府通信

中使用；此后，DES被多个部门和标准化机构采纳，甚至成为事实上的国际标准，直到1998年该标准才正式退役。其二，1976年11月，Diffie与Hellman的革命性论文《密码学的新方向》(New Directions In Crypotography)发表，开辟了公开密钥密码学的新领域，成为现代密码学的一个里程碑。1978年，里维斯特(R. L. Rivest)、沙米尔(A. Shamir)和阿德尔曼(L. Adleman)实现了RSA公钥密码体制，它成为了公钥密码的杰出代表和事实标准。

1969年，哥伦比亚大学的威斯纳(Stephen Wiesner)首次提出"共轭编码(Conjugate Coding)"的概念。1984年，本奈特(Charles Bennett)等人在威斯纳思想的启发下，首次提出了基于量子理论的(现称为)BB84协议，从此量子密码理论宣告诞生。量子密码不同于以前的密码技术，是一种可以发现窃听行为，且安全性基于量子定律的密码技术，可以抗击具有无限计算能力的攻击。有人甚至认为，在量子计算机诞生之后，量子密码技术可能成为唯一的真正安全的密码技术。1985年，科布利茨(N. Koblitz)和米勒(V. Miller)把椭圆曲线理论应用到公钥密码技术中，使公钥密码技术取得了重大进展，成为公钥密码技术研究的新方向。

密码技术的另一个重要方向——流密码(也称序列密码)理论也取得了重要的进展。1989年，马修斯(R. Mathews)、惠勒(D. Wheeler)、皮科拉(L. M. Pecora)和卡罗尔(Carroll)等人把混沌理论引入到流密码及保密通信理论中，为序列密码理论开辟了一条新的途径。

1997年9月12日，美国国家标准与技术研究院(NIST)开始征集新一代数据加密标准来接任即将退役的DES；2000年10月2日，由比利时密码学家Joan Daemen和Vincent Rijmen提交的Rijndael算法被确定为AES算法。

2000年1月，欧盟启动了新欧洲数据加密、数字签名、数据完整性计划，旨在提出一套强壮的包括分组密码、流密码、散列函数、消息认证码(MAC)、数字签名和公钥加密的密码标准，使欧洲工业界保持密码学研究领域的领先地位，2002年底最后确定了各类标准算法。

经典的密码学是关于加密和解密的理论，主要用于通信保密。今天，密码学已得到了更加深入、广泛的发展，其内容已不再是单一的加、解密技术，已被有效、系统地用于电子数据的保密性、完整性、真实性和不可否认性等各个方面。这里所说的保密性就是对数据进行加密，使非法用户无法读懂数据信息，而合法用户可以应用密钥读取信息；完整性是对数据完整性的鉴别，以确定数据是否被非法篡改，保证合法用户得到正确、完整的数据；真实性是指数据来源和数据本身真实性的鉴别，保证合法用户不被欺骗；不可否认性是真实性的另一个方面，有时，不但要确定数据来自何方，而且还要求数据源不可否认发送的数据。

现代密码技术的应用已深入到信息安全的各个环节和对象，主要技术有数据加密、密码分析、数字签名、信息鉴别、零知识认证及秘密共享等。密码学的数学工具也更加丰富，如概率统计、数论、组合、代数、混沌、椭圆曲线等，现代数学的许多领域都有密码学的足迹。

另一个值得一提的就是近年来发展迅速的信息隐藏技术。这是一种将需要保密的信息隐藏在公开信息中传输的技术，可以称为秘密的信息嵌入技术，它主要基于不在意信息传

输的思想。相对而言，密码技术是一种公开的信息嵌入、刻意传输技术。如果把密钥视为秘密隐藏信息的秘密，那么，广义地说，密码技术也是一种信息隐藏技术。这种信息隐藏的秘密由密钥控制。狭义上隐藏信息的秘密由算法控制，如果算法暴露或公开，那么信息也就无法隐藏了，所以，信息隐藏技术的另一个重要环节是不在意传输，即将信息隐藏在一般的经常性的公开信息(如广播、电视、图片等)中进行传输，使窃密者无从下手，以此达到逃避信息窥测的目的。数字水印及数字指纹等技术是信息隐藏技术的典型方法，已被广泛地应用于数字产品的产权保护上。

1.3 信息编码的研究目标

有效性、可靠性、保密性、认证性和经济性构成了现代通信系统对信息传输的全面要求，其中前 4 项正是本书要研究的主要内容。如果研究信息传输的有效性，则可只考虑信源与信宿之间的信源编(译)码，将其他部分都看成一个无干扰信道。如果研究信息传输的可靠性，则可将信源、信源编码和密码编码都等效成一个信源，而将信宿、信源译码和解密译码都等效成一个信宿。如果考虑信息传输的保密性和认证性，则可将信源和信源编码等效成一个信源，将信道编码、信道、噪声源和信道译码等效成一个无干扰信道，而将信源译码和信宿等效成信宿。

1.3.1 信源压缩编码的目标

信源压缩编码的主要目标是压缩每个信源符号的平均比特数或信源的码率。信源编码可分为经典信源编码和现代信源编码两大类。经典信源编码又可分为无失真信源编码和限失真信源编码。

从经典信源编码理论出发，不难得到信源编码的两种基本途径：其一是设法改变信源的概率分布，使其尽可能地非均匀，再用最佳编码方法使平均码长逼近信息熵；其二是联合信源的冗余度寓于信源间的相关性之中，去除它们之间的相关性，使之成为或差不多成为不相关信源。基于基本途径一的编码方法有霍夫曼编码、算术编码、游程编码等，其压缩效率都以其熵为极限值；基于基本途径二的编码方法有预测编码、变换编码、混合编码、矢量量化等，同时也大都受信息熵的约束。虽然经典方法依据了信源本身固有的统计特性和利用人视觉系统的某些特性进行压缩编码，但是利用得还不够充分，且伴随着感知生理以及心理学的发展，人们越来越清楚地认识到，人的视觉感知特点与统计意义上的信息分布并不一致，即统计上需要更多的信息量才能表征特征，对视觉感知可能并不重要。从感知角度来讲，无需详细表征这部分特征。这时，编码技术的研究就突破了传统香农理论的框架，注重对感知特性的利用，使得编码压缩效率得以极大提高，因此称其为现代压缩编码方法。

1.3.2 信道纠错编码的目标

信道纠错编码的主要目标是提高信息传输的可靠性。信道中的干扰常使通信质量下降，也可说使信息传输不可靠。对于模拟信号，表现为收到的信号的信扰比下降；对于数字信号，则表现为误码率增大。信道编码的主要方法是增大码率或频带，也就是增大所需的

信道容量。这恰与信源编码相反，例如为了提高模拟信号的信扰比，可采用大频偏的调频方式，这类信号的频带远大于一般的调幅或单边带信号，需要更大容量的信道。对于数字信号，尤其是二进制信号，通常可在信息位之后，按一定的规律附加一些监督位。这样就可在接收端检出错误并要求重发，或直接纠正某些差错。采用了检错或纠错措施后，显然可降低误码率，也就是提高了信息传输的可靠性。同时，由于增加了监督位，码率将有所扩展，因而将占用较大的信道容量。也有一些信道编码方法并不要求增大容量来提高可靠性，例如在数字调制技术中，相干解调的误码率可低于非相干解调，采用部分相应技术也有此等作用。格状码调制(TCM)技术把多电平调制和纠错码结合起来，在保持一定有效性的条件下，可较大地提高可靠性。用这些方法提高可靠性的代价是使设备复杂化。信道编码的理论基础是信息论中的信道编码定理。该定理指出，当传送的信息率低于信道容量时，误码可接近零。这就是说，理想的信道编码器应能在码率接近信道容量时，保证可靠通信，而现有技术还远不能达到这一目标。

复用技术也可认为是信道编码。从理论基础来说，这是另一类问题：它并不是为了提高可靠性，而是为了充分利用信道。这种技术在通信中有重要意义。新的复用方式尚在发展中，除了传统的频分复用及时分复用外，还有码分复用、统计复用、多址接入复用等，所以也是一个值得注意的问题。

1.3.3 密码编码的目标

密码编码的主要目标是保证信息传输的保密性、完整性、真实性和不可否认性等。在信息传输或处理过程中，除了指定的接收者外，非指定或非授权的用户也可以接收到，其中的恶意者会通过各种技术手段窃取机密信息。因此，有必要研究信息传输的安全性问题。

通信系统中的传输媒质有电缆、明线、光纤和无线电波等，信号通过这些媒质时，除了存在各种天然的干扰使被传输信号产生错误外，还有一些人为干扰，如非指定的用户或敌人通过各种方法(如搭线、电磁波接收及声音接收等)对所传输的信号进行侦听(称被动攻击)，更有甚者，采用删除、更改、增添、重放、伪造等手段，向系统注入信号或破坏被传输的信号，以达到欺骗别人、利于自己的目的，这种攻击称为主动攻击。为了保证被传输信息的安全，除了必须对信源的输出进行加密，用编码方法对信息进行隐藏外，还要求信息传递过程中不被伪造和篡改。对于这些攻击行为，虽然相应的法律已逐步建立，但是由于犯罪形式的特殊性，对它的监督和量刑都是很困难的。因而，除了不断完善相应的法律和监督措施外，更需要自我保护。理论和事实都说明，密码技术是一种经济、实用而有效的方法。这也是密码技术得到快速发展和广泛应用的原因。

1.3.4 组合编码的目标

近年来，以计算机为核心的大规模信息网络，尤其是互联网的建立和发展，对信息传输的质量要求较高。传统的方法通常是对系统的各个部分单独设计，以使各部分的性能达到最佳，从而使整个系统最佳。但自 20 世纪 70 年代中期以来，人们开始把通信系统的几个部件看成一个整体进行设计，以使系统达到最佳。如信源编码与纠错编码相结合的设计，特别是纠错编码与调制相结合的 TCM 技术的出现，使系统获得了多个分贝的增益，取得了显著的经济效益。针对不同信道、不同调制方式的各种 TCM 技术，目前已普遍应用在各