普通高等教育信息安全类国家级特色专业系列规划教材

多媒体信息安全

孔祥维　郭艳卿　王波　编著

科学出版社

普通高等教育信息安全类国家级特色专业系列规划教材

多媒体信息安全

孔祥维　郭艳卿　王　波　编著

科学出版社
北京

内 容 简 介

多媒体信息安全涉及多媒体产生、传输、分发和应用过程的安全保障问题。本书力求涵盖与多媒体相关的信息安全的主流研究内容，包括多媒体的数据特性、隐密技术和隐密分析技术、数字水印、数字媒体取证、生物认证和生物模版安全等内容，最后给出典型算法的 Matlab 程序。

本书可作为高等院校的电子工程专业、信息安全专业、计算机应用专业、通信工程专业的高年级本科生或研究生的教材，也可作为科研院所相关专业科技工作者的研究参考。

图书在版编目(CIP)数据

多媒体信息安全/孔祥维，郭艳卿，王波编著. —北京：科学出版社，2014.3
普通高等教育信息安全类国家级特色专业系列规划教材
ISBN 978-7-03-039818-5

Ⅰ.①多… Ⅱ.①孔… ②郭… ③王… Ⅲ.①多媒体-信息安全-安全技术-高等学校-教学 Ⅳ.①G203

中国版本图书馆 CIP 数据核字(2014)第 031396 号

责任编辑：潘斯斯 张丽花 / 责任校对：蒋 萍
责任印制：闫 磊 / 封面设计：迷底书装

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

新科印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2014 年 3 月第 一 版 开本：787×1092 1/16
2014 年 3 月第一次印刷 印张：17
字数：446 000

定价：40.00 元

(如有印装质量问题，我社负责调换)

前　言

随着人类社会进入数字时代，数字内容的信息安全、保护和取证成为一个崭新的挑战课题。一方面，通过计算机和网络来进行的犯罪活动已经占据了越来越大的比例，对计算机、网络等数字设备和数字化的多媒体信息进行技术层面的司法取证和鉴定，特别是近年来数字化信息篡改频繁引发的政治、经济、社会、司法等方面的纠纷争端，使得数字取证成为学术界的前沿课题；另一方面，如何确保多媒体信息在通信和传播中的安全，一直是人类面临的重要研究课题。随着网络及多媒体技术的飞速发展，信息隐藏和信息隐藏分析、数字水印和生物模板保护为代表的数字媒体保护和认证技术，已成为近年来信息领域关注的热点问题。

本书是在参考目前国内外同类教材和文献的基础上，力求反映本学科基本概念和最新发展编写而成的。本书在内容组织上注重基础性、系统性和实用性，包括基本概念及对实用需求问题解决方法的阐述；在文字表达上力求简洁、清晰、流畅、易读，同时每章配有概念性和实际应用方面的习题和程序。

本书参考学时为32学时，共分7章。第1章为绪论；第2章介绍与多媒体安全相关的多媒体数据特性；第3章介绍隐密技术；第4章介绍隐密分析技术；第5章介绍数字水印；第6章介绍数字媒体取证；第7章介绍生物认证和生物模板安全。这些章节构成了本书的体系结构。

本书由大连理工大学孔祥维教授主编，同时组织2位长期在多媒体信息安全技术领域工作、具有丰富教学和应用经验的教师共同编写完成。其中，第1、5、7章由孔祥维教授编写；第3、4章由郭艳卿副教授编写；第2、6章由王波博士编写。

由于编者水平有限，书中不当之处在所难免，殷切希望广大读者批评指正。

编　者

2013年9月

目　录

第1章 绪 论

1.1 多媒体信息安全的重要意义

信息时代的到来，从多方面影响着国家利益的构成和内涵，信息本身已成为国家利益的一个重要组成部分，同时也是社会发展的重要战略资源之一，对信息的开发、控制和利用已成为当前各发达国家为国家利益争夺的重要内容。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，致使信息的控制保障和安全上升为世界性的问题，成为维护国家安全和社会稳定的一个焦点，同时也是亟待解决、影响国家大局和长远利益的重大关键问题。

当今数字信息的发展也给人们的社会和日常生活带来了深刻的革命性变化，由于计算机网络和信息化的普及，人类越来越依靠网络和信息，数字多媒体和互联网的普及，给人们带来欣赏和愉悦的同时也提出了许多挑战性的问题。新技术的双刃剑带来了新的安全威胁，互联网主要信息载体的信息内容安全问题变得日益突出。

“9·11”事件对信息技术产生了巨大的影响，使得世界范围内的信息安全形势发生了巨大变化，从而使信息安全保障和反恐上升为世界性的国家问题。由于从保护国家和个人的利益出发，各国政府无不重视信息安全，特别是各发达国家均大力加强信息安全的研究和督导。

信息安全的内涵随着信息技术的发展与应用的不断深入也在不断延伸。人们传统地把信息安全理解为对信息的机密性、完整性和可用性的保护，但这仅是面向个人用户的信息数据保密。后来发展到信息的完整性、可用性、可控性和不可否认性，进而又发展到“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。在当今时代，分布式计算、物联网 、云计算的应用、互连互通的无缝传播，信息安全强调面向用户的安全是鉴别、授权、访问控制、抗否认性和可服务性，以及隐私、知识产权保护等。

当今大数据在成为竞争新焦点的同时，亦成为网络攻击和安全的显著目标，带来了新的安全风险。大量社交网络、邮件、微博、电子商务、电话和家庭住址等信息，使黑客的攻击更加精准，攻击一次就能获得相当多的数据。虽然数据大集中可将复杂多样的数据存储在一起，但大量数据的汇集增加了用户隐私泄露的风险。

综上所述，信息安全的内涵已从最初的信息保密提升到信息安全保障能力，逐渐发展并形成一个综合性交叉学科领域，它广泛涉及数学、密码学、信息、网络、通信、控制、人工智能、安全管理工程、系统工程领域等诸多学科，近几年迅速成为国际上的热点学科领域，是当前世界各国正在奋力谋求的制高点。

目前我国信息与网络安全的防护能力处于发展的初级阶段，许多应用系统处于不设防状态，当前的信息安全研究忙于封堵现有信息系统的安全漏洞，要解决这些迫在眉睫的问题，取决于信息安全保障体系的建设。目前迫切需要根据国情，从安全体系整体着手，建立全方位的防护体系，加强我国自主产权的信息安全技术和信息设备的研究与开发，建立完善的信息安全系统，完善法律体系并加强管理体系，构建国家信息安全保障体系。只有这样，才能保证我国

信息化的健康发展，确保国家安全和社会稳定。信息安全问题解决好坏将直接影响我国的政治、军事、经济、文化、社会生活的各个方面，解决不好有可能使国家处于信息控制和威胁之中，将遭到无声的信息掠夺和信息控制。

历史上信息安全的实现都是通过加密来完成的。密码学的应用在很长一段时间内都被看成是外交情报和军事领域内极其隐秘的通信方法和手段，商业加密的应用将一些密码方法扩展到了民间，而目前互联网和数字信息可以扩散到各个地方，加密技术和方法更加公开，文献也随之增多。

密码学是一门古老的学科，它的起源可以追溯到四千多年前的古埃及、巴比伦、古罗马和古希腊。古代的保护信息安全方法是将传输信息的信号进行各种变化，使它们不能为非授权者所理解。当时的密码技术还不能算是一门科学，它更像一门艺术，人们凭借直觉和经验来设计和分析密码。现代密码学就是在古典密码学的基础上发展起来的。

Shannon 在 1949 年建立了单钥密码系统的数学模型，为密码学奠定了理论基础。1976 年，美国学者 Diffie 和 Hellman 建立了公钥密码系统(RSA)，使加密密钥和解密密钥相互独立，公钥密码使民用、商用通信系统的信息加密和保护成为可能。1977 年，美国国家标准学会(ANSI)公开征集并公布实施数据加密标准 DES，公开了它的加密算法，并批准用于非机密单位及商业的保密通信，使其作为联邦标准免费提交给美国公众使用。在此之后用于信息保密和加密的各种算法和软件、标准和协议、设备和系统、法律和条例、论文和专著等层出不穷，随着计算机网络不断渗透到各个领域，密码大规模地扩展到民用，密码学的应用范围也随之扩大，典型如数字签名、身份认证等都是由密码学派生出的新技术和应用。

采用传统密码学理论开发出来的加、解密系统，不管对称密钥系统(如 DES)还是安全性更高的公开密钥系统(RSA)，对于文件的处理都是将明文转变成密文进行传递，攻击者只能看到密文乱码，而无法破译其中的机密信息，从而达到保密的目的。但是传统加密方法往往把一段有意义的信息明文转换成看起来没有意义的密文，这密文就明确地提示给攻击者：通信双方进行了加密通信。此外，密文还容易引起攻击者的好奇和注意，从而造成攻击者明确知晓攻击的目标。

虽然历史上可以证明密码学(Cryptography)被公认为是信息安全的核心技术，但是，依靠密码学并不能完全解决现代信息社会涌现出的新问题。

互联网已由早期的浏览信息和收发邮件转变成多媒体、通信服务、服务应用和娱乐应用并重的交互网络。媒体印刷品如书报、杂志；电子出版物如电子音像、光盘、游戏软件，音像传播如影视、录像、广播等都逐渐以数字化形式出现在网络上。利用这些数字媒体信息资源进行创意、制作、开发、分销、交易的内容产品和服务的产业已经迅速发展起来。数字内容产品的互动性与个性化服务的优势，使得数字内容产品增值服务具有无限的发展空间，成为新的产业增长点，但同时引发了数字媒体和内容的健康性、保密性、隐私性、产权性、安全性等问题难以得到保障。

数字多媒体应用因其可视可听、丰富多彩的特点在世界各地已经蓬勃兴起，其发展渗透改变了人们的工作方式和日常生活，使人们更加方便地享受和体验到新技术带来的方便和愉悦。数字多媒体传播的某些成本大大降低，例如，复制成本几乎为零，分发的边际成本逼近零等，因此这些具有易复制、易修改和易传播特征的新技术和新应用在惠民的同时也成为双刃剑，使得多媒体信息的来源、通信和获取等阶段都存在着不同的安全问题。

多媒体应用具有可视观赏性、降质可容忍性、无损下载传播、复制容易等固有特点，加上多媒体软件的普及流行，导致数字多媒体在其应用的生命周期内随时面临着被窃取、篡改、非授权访问和非授权分发的威胁，使得以往的安全技术难以应对层出不穷的多种新型安全威胁，造成数字媒体价值的降低甚至丧失，这直接或间接地制约着各种数字媒体应用的发展和普及，因此多媒体信息安全问题成为新时代信息安全问题的挑战。

数字世界的崛起给现实世界保护知识产权的规则带来挑战，面对新的技术和威胁，传统的信息安全措施不够有效，需要发展崭新的信息安全手段，保护人类创造和拥有的软件、音乐和其他形式的数字化多媒体内容和多媒体资产的价值，为创造可信的数字化世界奠定坚实的基础。

1.2 多媒体信息安全的主要威胁

当今的信息环境发生了巨大的变化，海量多媒体信息时时刻刻在大量产生。数字化数据迅速增长，一方面可以催生出更好的产品和服务，另一方面使得目前多媒体信息安全的威胁日益加剧。因此需要对常规多媒体信息业务的通信模式和应用模式深刻理解，了解和掌握攻击者的目的与手段，分析和评估面临的安全风险和存在的漏洞，研究新的防御技术以减小或消除安全威胁和风险，构建一个政府、厂商和用户构成的具备多媒体信息安全保障的生态系统。

信息安全一般包括物理安全、系统安全、数据安全、应用安全和内容安全。物理安全涉及硬件设施方面的安全问题；运行安全涉及操作系统、数据库、应用系统等软件方面的安全问题；数据安全以保护数据不受外界的侵扰为目的，包括防止泄密、伪造、篡改、抵赖等有关的行为；信息内容安全则通过对内容的语义分析和理解，对数据进行选择性阻断、修改、转发等特定的行为。多媒体信息安全涉及数据安全和信息内容安全以及应用安全，因多媒体信息特有的数据特性和固有特点，安全保障内容有其特殊性。

多媒体信息安全的研究需要从多媒体应用的安全威胁出发，即从多媒体的产生、通信、传播，接收以及真实性等多媒体本身和应用的生命周期视角等方面考虑可能出现的攻击，同时以安全保障为目的，保持多媒体数据本身可用的灵活性。

一般类型的多媒体信息攻击如下。

(1)对可用性的攻击：该系统的多媒体被破坏或变得不可利用或不能使用，例如，包括在通信中多媒体的损坏、不能解码或观赏功能的失效。

(2)对保密性的攻击：未授权方通过截获等手段非法获取信息并对某多媒体信息非法访问。例如，在网络上搭线窃听以获取数据，违法复制文件或程序等。

(3)对完整性的攻击：未授权方破坏多媒体信息资产，改变多媒体数据文件中的数据，篡改在网络中传输的多媒体信息内容，采用软件修改多媒体信息内容等。

(4)对真实性的攻击：未授权方伪造和替换原有的多媒体信息，对多媒体来源进行伪造，在数字图像中伪造水印。

1.3 多媒体信息安全的研究内容

本书拟从多媒体信息应用的生命周期视角阐述其安全问题。其主要研究内容包括以下几个部分。

保障多媒体信息的源头安全：在数字产品产生中嵌入数字水印以便以后进行内容鉴别和作品认证，以期解决版权纷争；对需要保密的信息进行加密处理防止非授权访问和获取；利用生物特征识别用户，以便进行身份认证，并进行访问控制等。

保障多媒体信息的传输安全：可以进行信息加密，成为不可解读的密文进行传输；秘密信息进行伪装式的信息隐藏以便攻击者察觉不出有秘密通信存在；对用于身份认证的生物特征加密或者变形以防止通信中生物模板泄露造成安全威胁等。

多媒体信息获取的安全：数字媒体中嵌入数字指纹用于追踪数字产品分发和用户的权益，感知哈希对获取信息进行验证以保障获取信息的可信性。

多媒体信息的真实鉴别：主动方法是向数字作品中加入数字水印再进行来源鉴别或认证，被动方法是利用数字媒体取证技术对多媒体作品进行盲检测来源，并判断篡改与否。

以上研究内容既有关联又有区别。传统加密是隐藏内容，而信息隐藏主要是隐藏了信息通信的存在性。信息隐藏通信比加密通信更安全，它隐藏了通信的发方、收方，以及通信过程的存在，不易引起怀疑。加密后不能知晓通信的内容，但直接暴露了通信。多媒体内容的版权保护和真实性认证往往需容忍一定程度的失真，而加密后的数据不容许一个比特的改变，否则无法脱密。

人脸、指纹等生物认证本是身份认证和安全控制的新手段，但其模板数据如果泄露，会导致更严重的安全威胁，反而不如应用成熟的密码。

数字图像和视频可以轻易用免费软件篡改，在主动嵌入水印不广泛普及的今天，大多数多媒体没有附加任何附属信息，因此需要发展被动的多媒体取证技术以判断多媒体的来源和完整性。

以上多方面的内容可以从多媒体真实性、可信性、安全性、完整性和可追踪性等多方面进行保障，同时不影响多媒体的感知效果，使多媒体在应用和播放的同时获得安全保障。

1.4 多媒体信息安全的典型应用

(1)隐蔽通信和隐蔽标识：主要技术为隐密术。如图像数据的隐蔽标识和公开网络中的保密数据传输，如遥感图像的日期、经纬度等。

(2)版权保护：主要技术为鲁棒数字水印技术。源于数字媒体的版权保护，为 DVD、MP3 和网上图像的版权保护的解决手段。

(3)多媒体认证：主要技术为脆弱数字水印和鲁棒数字水印技术。多媒体的来源认证、历经的销售商和授权用户跟踪信息都可以通过数字水印技术实现。

(4)篡改提示：主要技术为脆弱数字水印。通过将数字水印哈希在图像中，可以对图像的篡改和替换进行自动检测和提示。

(5)数字广播电视分级控制：主要技术为鲁棒数字水印技术和数字指纹。利用数字水印和数字指纹在数字广播和数字影视中控制，对各级用户分发不同的内容进行不同的服务。

(6)内容鉴定的不可抵赖性认证：数字媒体的司法性验证和真实内容鉴定，如数码相机、数码摄像机拍摄和视频的来源鉴定。

(7)注释数字水印：将图像的注释加在数字水印之中，不占信道容量和带宽，其安全性要求不高，但容量要求大。

(8)视频数据的错误隐匿：利用视频中的数字水印对视频的传输误差进行隐匿。

第 2 章　多媒体的数据特性

人类为了记录物理世界和自然形态提出了多种实用的多媒体数据形式，如静止图像、视频、音频、文本和其他媒体等。数码相机图像记录了静止画面和人物，视频录像记录了运动的形态，如电影、比赛、新闻、纪实等，录音音频记录着自然界的声音以及音乐和话音等，还有及时传播信息的互联网网页文字和网络上的各种多媒体应用等。与这些多媒体信息相关的安全研究，无论是向数字媒体嵌入信息的信息隐藏和数字水印，还是应用于判断多媒体真实性和完整性的数字媒体取证，以及涉及身份认证的生物特征安全等，都关联着数字媒体安全应用和数字世界的可信保障，都充分利用了数字多媒体的数据特性、感知特性、冗余特性和相关的多媒体数据国际标准作为理论基础，下面分别介绍相关的内容。

2.1　多媒体感知冗余

就目前发表的文献来看，数字多媒体安全主要利用了数字媒体的感知冗余和数据特性，主要包括感知冗余、文件格式冗余以及媒体本身的数据特性。下面分别介绍这些方面。

2.1.1　视觉冗余

在基于可视媒体如图像、视频的信息隐藏方法中，无论设计何种信息隐藏方法，最终结果都要先经过人眼的感知判别，因此信息隐藏能否通过人类的视觉检验是判断该方法是否成功的首要因素，信息隐藏、数字水印和数字指纹等都涉及视觉冗余，首先有必要了解一下人眼的视觉特性。

人眼视觉系统特性对图像处理、图像识别、计算机视觉等系统的设计有重要的意义。人类的视觉特性不仅受人眼生理和物理特性的影响，而且受到环境状态的影响。由于人眼某些缺陷，例如视觉冗余，信息隐藏即利用这种冗余实现了秘密信息的嵌入。下面归纳了一些与信息隐藏相关的人眼视觉特性。

(1)Weber 定律。人眼所能感觉到的亮度范围称为亮度视觉范围。在不同的环境下，对同一亮度的主观感觉也不相同。明视觉时，1 至几百万尼特。暗视觉时，千分之几至几尼特，这主要靠人眼瞳孔的调节作用。但人眼并不能同时感觉这么宽的视觉范围，当人眼适应了某一环境的平均亮度之后，视觉范围有一定的限度和感觉局限性。一般能分辨的亮度上下限之比为 1000∶1。当平均亮度很低时，这一比值只有 10∶1。Weber 定律说明在均匀背景下，人眼可以识别的物体照度为 $I+\Delta I$，其中 I 表示背景照度，$\Delta I \approx I \times 0.02$。该定律说明虽然人眼可分辨的亮度范围较大，但在同一时刻只能区别其中很小的一部分，亮度变化较大的图像区域人的感知会下降。

(2)频率敏感性和纹理复杂性。人眼对图像不同空间频率成分具有不同的灵敏度。人的视觉系统对平滑区的变化很敏感，随着细节增多，纹理复杂性增加，人眼的分辨率则迅速降低，

即人们对细节较多、纹理较复杂的区域的变化敏感度相比较平滑的区域变化敏感度有所下降。人眼容易感觉边缘位置的变化，而对于边缘的附近灰度的误差则相对不敏感。

(3)亮度敏感性。在固定亮度背景下，人眼对信号的视觉感知效果受背景平均亮度和目标信号的亮度水平的影响较大。在平均亮度大的区域，人眼对灰度误差不敏感；而对于平均亮度小的区域，人眼对灰度误差较敏感。可以利用图像的局部特征，对这些亮度大的区域的强度进行微小调整，使得人眼难以感知。

(4)对比度特性。对比度指的是图像中明暗区域最亮的白和最暗的黑之间不同亮度层级的测量，差异范围越大代表对比度越大，差异范围越小代表对比度越小。即在给定的亮度背景下，一个信号在另一信号存在的情况下的可觉察性，即人眼对目标信号的视觉感知掩蔽特性。这种现象在这两个信号具有相同的空间频率、取向和位置时掩蔽特性最强。一般来说对比度越大，图像越清晰，色彩也越鲜明艳丽；对比度小会让整个画面感觉灰蒙蒙的，高对比度利于图像的清晰度、细节表现、灰度层次表现。

(5)方向敏感性。人眼对不同角度的空间频率视觉信号有不同的响应。具体表现在对垂直和水平方向的频率具有较强的视觉响应能力，而对对角线方向的频率响应能力显著下降。

(6)视觉掩盖效应。不同局部特性的区域，在不被人眼察觉的前提下，改变的信号强度不同。背景亮度变化越剧烈，视觉越高，即人眼的对比度灵敏度越低。这种现象称为空间域中的视觉掩蔽效应。人眼的视觉特性是一个多信道模型，它具有多频信道分解特性，人眼对图像不同灰度具有不同的敏感性，其中对中等灰度区最为敏感；而对高灰度区、低灰度区敏感度相对较低。

以上这些人眼的感知局部掩蔽效应都属于局部效应，不同个体、不同时间、不同环境都会对其造成影响。因此，可以充分利用这些视觉冗余特性设计算法，达到人眼无法辨别的效果。

2.1.2 听觉冗余

1. 听觉阈值

听觉阈值指的是低于这个阈值的声音信号就难以听到，听觉阈值的大小随声音频率的改变而改变。与个人的听觉阈值不同，大多数人的听觉系统对 2～5kHz 的声音最敏感。一个人能否听到声音取决于声音的频率，以及声音的幅度是否高于这种频率下的听觉阈值。如果声波的频率为 20Hz～20kHz，而声强又达到一定的强度，该声波就能被人耳所感知，此时的声波强度被称为听觉阈值。

2. 听觉掩蔽效应

听觉冗余掩蔽效应指的是人耳只对最明显的声音反应敏感，而对不敏感的声音，反应不敏感。当几个强弱不同的声音同时存在时，强声使弱声难以听见的现象称为同时掩蔽，它受掩蔽声音和被掩蔽声音之间的相对频率关系影响很大；声音在不同时间先后发生时，强声使其周围的弱声难以听见的现象称为异时掩蔽。如果时间上相邻的不同强弱声波同时存在，较弱的一个声波会因为较强声波的存在而被人耳听觉所忽略；此外，如果频率相近的两个声波同时存在，较弱的一个频率会因为较强频率的存在而被人耳所忽略。这两种现象在声学上被称为人耳听觉掩蔽效应，其中前一种称为时域听觉掩蔽效应，而后一种被称为频域听觉掩蔽效应。听

觉掩蔽效应是音频信息隐藏的一个重要理论基础，LSB 等音频信息隐藏技术都充分利用了这一特性。

3. 相位不敏感

人耳对不同强度、不同频率声音的听觉范围称为声域。在人耳的声域范围内，声音听觉心理的主观感受主要有响度、音高、音色等特征。响度、音高和音色可以分别用振幅、频率和相位三个物理量来进行描述。其中人耳对振幅、频率的变化较为敏感，而对相位变化的敏感程度则较弱，这使得相位成了实现音频信息隐藏的一个重要参考。

4. MPEG 心理声学模型

人类听觉系统的掩蔽效应可以用心理声学模型来描述，依据该模型可估算出各掩蔽者的掩蔽值。掩蔽阈值取决于掩蔽者的音调性、频率、声压级和持续时间。掩蔽阈值是时间、频率和声压级的函数，并且随掩蔽音调的变化而变化。

MPEG 音频标准提供了两个心理声学模型。两个声学模型都是先将音频信号经 FFT 变换到频域，再映射到临界频带，区分出有调和无调成分，依据所在频率位置及强度大小计算单独掩蔽阈值和总掩蔽阈值、最小听觉阈值曲线。不同的是，MPEG 模型Ⅱ在主要环节的处理上烦琐，计算量大，对频谱数据分区后，使用扩展函数卷积来决定噪声掩蔽阈值，根据分区能量和不可预测性度量来衡量有调的倾向性，所有的谱线都参与了掩蔽阈值计算，使得整个模型复杂度提高。而 MPEG 模型Ⅰ为降低模型复杂度使运行速度得到保证，做了很多折中，相对而言，MPEG 模型Ⅰ准确性不如 MPEG 模型Ⅱ。

2.1.3　视频冗余

1. 空间域中的掩蔽效应

视觉的大小不仅与邻近区域的平均亮度有关，还与邻近区域的亮度在空间上的不均匀有关。假设将一个光点放在亮度不均匀的背景上，通过改变光点的亮度测试视觉，背景亮度变化越剧烈，人眼的对比度、灵敏度越低。这种现象称为空间域中的视觉掩蔽效应(Masking)。

2. 时间域掩蔽效应

当电视图像序列中相邻画面的变化剧烈时，人眼的分辨力会突然剧烈下降，可以下降到原有分辨力的 1/10。如当新场景突然出现时，人基本上看不清新景物，在大约 0.5s 之后，视力才会逐渐恢复到正常水平。因此，在这 0.5s 内，传送分辨率很高的图像就没有必要。

3. 彩色的掩蔽效应

在亮度变化剧烈的背景上，例如，在黑白跳变的边沿上，人眼对色彩变化的敏感程度明显降低。类似地，在亮度变化剧烈的背景上，人眼对彩色信号的量化噪声也不易察觉，这些都体现了亮度信号对彩色信号的掩蔽效应。

4. 视觉冗余

人类视觉系统一般的分辨能力约为 26 灰度等级，一般图像量化采用 28 灰度等级，这类冗

余称为视觉冗余。通常情况下，人类视觉系统对亮度变化敏感，而对色度的变化相对不敏感；在高亮度区，人眼对亮度变化敏感度下降，对物体边缘敏感，内部区域相对不敏感；对整体结构敏感，而对内部细节相对不敏感。

2.2 文件格式冗余

数字媒体都是以某种格式存放在存储介质中，其中典型的文件格式都存在一定的冗余，这为多媒体处理和安全提供了资源。

2.2.1 静止无压缩图像格式及冗余

1. BMP 图像文件格式

BMP 是英文 Bitmap(位图)的简写，它是 Windows 操作系统中的标准图像文件格式。在 Windows 环境中运行的图形图像软件都支持 BMP 图像格式。这种格式的特点是包含的图像信息较丰富且无压缩，但占用磁盘空间较大。

BMP 图像文件由三部分组成：位图文件头数据结构包含 BMP 图像文件的类型、显示内容等信息；位图信息数据结构包含 BMP 图像的宽、高、压缩方法以及定义颜色等信息。它采用位映射存储格式，图像深度可选 1 位、4 位、8 位及 24 位，不采用其他任何压缩，因此，BMP 文件所占用的空间很大。存储数据时，图像的扫描方式按从左到右、从下到上的顺序。

优点：BMP 支持 1～24 位颜色深度；BMP 格式与现有 Windows 程序广泛兼容。缺点：BMP 不支持压缩，文件较大，不支持 Web 浏览器。

2. TIFF 图像文件格式

TIFF(Tag Image File Format)图像文件是由 Aldus 和 Microsoft 公司为桌上出版系统研制开发的一种通用的图像文件格式。TIFF 格式定义了四类不同的格式类型：TIFF-B 适用于二值图像；TIFF-G 适用于黑白灰度图像；TIFF-P 适用于带调色板的彩色图像；TIFF-R 适用于 RGB 真彩图像。

TIFF 文件以. tif 为扩展名。数据格式是一种三级体系结构，从高到低依次为文件头、一个或多个称为 IFD 的包含标记指针的目录和数据。TIFF 图像文件中的第一个数据结构称为图像文件头或 IFH，它是图像文件体系结构的最高层。它位于文件的开始部分，包含了正确解释 TIFF 文件的其他部分所需的必要信息，是一个 TIFF 文件中唯一有固定位置的信息。IFD 图像文件目录是 TIFF 文件中第 2 个数据结构，是一个字节长度可变的信息块，它是一个名为标记(Tag)用于区分一个或多个可变长度数据块的表，标记中包含了有关图像的所有信息。IFD 提供了一系列的指针(索引)，指示有关的数据字段在文件中的开始位置，并给出每个字段的数据类型及长度。由于允许数据字段定位在文件的任何地方，且可以是任意长度，所以文件格式十分灵活；图像数据是 TIFF 文件中的第三个结构，根据 IFD 所指向的地址，存储相关的图像信息。

优点：TIFF 图像应用广泛，不依赖于具体硬件，是可移植的文件格式。缺点：TIFF 图像格式复杂，不支持 Web 浏览器。