Visual Media Information Security

可视媒体信息安全

徐正全　徐彦彦　著

高等教育出版社
HIGHER EDUCATION PRESS

Visual Media Information Security

可视媒体信息安全

KESHI MEITI XINXI ANQUAN

徐正全　徐彦彦　著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

图书在版编目(CIP)数据

可视媒体信息安全 / 徐正全,徐彦彦著 . —北京:高等教育出版社,2012.12

ISBN 978-7-04-036357-9

Ⅰ.①可… Ⅱ.①徐… ②徐… Ⅲ.①媒体-信息安全-高等学校-教材 Ⅳ.①G206.2

中国版本图书馆 CIP 数据核字(2012)第 257716 号

策划编辑	陈红英	责任编辑	陈红英	封面设计	刘晓翔	版式设计	余 杨
责任校对	王 雨	责任印制	朱学忠				

出版发行	高等教育出版社	咨询电话	400-810-0598
社 址	北京市西城区德外大街 4 号	网 址	http://www.hep.edu.cn
邮政编码	100120		http://www.hep.com.cn
印 刷	涿州市星河印刷有限公司	网上订购	http://www.landraco.com
开 本	787mm × 1092mm 1/16		http://www.landraco.com.cn
印 张	18.5	版 次	2012 年 12 月第 1 版
字 数	360 千字	印 次	2012 年 12 月第 1 次印刷
购书热线	010-58581118	定 价	69.00 元

物 料 号 36357-00

前言

当前，包括图像、视频、数字几何在内的可视媒体已成为信息处理和信息资源建设的主体，网络环境下可视媒体的内容服务正在成为一种重要形式。但是，网络环境下的应用又使可视媒体不可控、内容虚假等安全问题日益突出。这些问题如不解决，不仅严重制约数字内容产业的发展，更关乎国家的安全与社会稳定。可视媒体的安全问题已成为当前信息安全领域的焦点，但迄今为止国内外关于可视媒体信息安全方面的专著还较为少见。

本书为关于可视媒体信息安全的专著。相对一般信息安全论著，本书的特点是侧重于可视媒体的内容安全保护，针对可视媒体特征，利用信息安全相关技术，关注可视媒体在传输、存储、访问控制、使用等环节的安全问题，在可视媒体压缩、编码和解码、密码学与网络安全等基础上，围绕可视媒体加密技术、面向内容的多级访问技术、信息隐藏技术等可视媒体信息安全的基础理论方法、关键技术和应用进行了较为全面的介绍。本书在涵盖可视媒体安全领域一般理论与方法的同时，也尽量总结吸取国内外的一些最新研究成果，其中包括作者研究团队近年来在该领域的部分研究成果，希望起到抛砖引玉的作用。

全书共分为7章，第一章介绍可视媒体基本概念及面临的主要安全问题；第二章介绍可视媒体基础，包括可视媒体的数据压缩、图像及视频编码国际标准等；第三章介绍可视媒体信息安全基础，包括密码算法、安全性分析和密钥管理等；第四章介绍可视媒体加密技术，包括可视媒体对加密的安全需求和加密算法评价标准、保持格式兼容的可视媒体加密方法以及一些典型的可视媒体加密方法；第五章介绍基于内容的可视媒体多级加密及多级访问技术，包括基于内容的可视媒体多级加密模型、多级加密算法和多级访问控制算法；第六章介绍可视媒体信息隐藏技术，包括信息隐藏技术基本原理、数字水印、数字指纹、可视媒体常用标记算法、结合加密与数字指纹的可视媒体内容安全保护技术、可视媒体交换密码水印技术等；第七章介绍可视媒体信息安全应用，包括可视媒体加密应用、面向内容的可视媒体安全共享服务、版权保护、安全分发应用等。

本书的第四章和第五章由徐彦彦撰写，其余部分由徐正全撰写并统编全书。

武汉大学博士生冯春晖、蒋力对本书的撰写给予了协助，其中冯春晖协助撰写了第二章和第三章，并负责全书的引用和参考文献的整理，蒋力协助撰写了第六章。本书部分内容参考和引用了武汉大学李伟、杨志云、姚晔、刘树波、刘进等同学的博士论文有关内容以及国内外学界同仁的研究成果和著述。在此一并向他们表示感谢！

本书的完成得到了国家973计划项目（编号：2006CB303104、2011CB302204）、国家自然科学基金面上项目（编号：40871201）、教育部博士点基金（编号：20110141110056）以及武汉大学测绘遥感信息工程国家重点实验室自主课题的支持，特此感谢！作者要特别感谢武汉大学李德仁院士、龚建雅院士、清华大学胡事民教授、中山大学黄继武教授以及武汉大学测绘遥感信息工程国家重点实验室全体同仁给予的关心、支持和帮助！最后，还要对高等教育出版社陈红英编辑为本书出版付出的辛勤劳动表示衷心的谢意。

由于作者水平有限，书中错误和疏漏之处在所难免，敬请读者谅解，并欢迎广大读者批评指正。

作者

2012年9月

目录

第一章　绪论

可视媒体又称视觉媒体，是多媒体信息中的主要类型，在多媒体信息中占有主导地位。视觉是人类认知世界最重要的手段之一，人类接受信息的80%以上来自视觉，视觉对象包括文字、图像、视频、数字几何等，本书的重点研究对象就是其中的图像和视频，并称之为可视媒体。当前大量的信息是以可视媒体呈现的，其安全日益受到重视。可视媒体的安全还存在很多问题需要解决，已成为目前信息安全领域的研究热点。

1.1　可视媒体

信息技术的快速发展为深度开发和广泛利用信息资源创造了前所未有的条件，信息已是与材料和能源同等重要的战略资源，是最活跃的生产要素。近年来随着信息技术的飞速发展，多媒体技术已广泛深入到生产和生活的各个领域，从影音光碟(Video Compact Disc，VCD)、数字影碟(Digital Video Disk，DVD)到视频点播(Video On Demand，VOD)、远程医疗、远程教学、视频会议、可视电话、网络流媒体、多媒体游戏、多媒体邮件、视频检索、移动多媒体电话等各种应用场合。当前无论是政府、军队，还是学校、企业，甚至是寻常百姓家都已离不开多媒体的应用，特别是政府机关、军队和经济团体，远程多媒体资料的传输已是提高效率和占领先机的重要手段。

多媒体技术是指把文字、音频、视频、图形、图像、动画等多媒体信息通过计算机进行数字化采集、编辑、压缩/解压缩、存储等加工处理，再以单独或合成形式表现出来的一体化技术。随着信息技术的高速发展和网络的普及，可视媒体的应用越来越广泛，其安全问题也日益受到重视。图像和视频这两类可视媒体涉及的安全问题，已经成为当前信息安全领域的研究热点。

1.1.1　媒体和可视媒体

媒体是承载信息的载体，是信息的表现形式。客观世界中存在着不同的信息形式，相应地也有不同的信息载体，如文字、图形、图像、声音等。人类的各种感觉器官是应信息交流的需要在自然进化过程中产生的。这些器官使人类能利用视

觉、听觉、味觉、嗅觉和触觉来全方位感受信息，获取知识，从而认识客观世界，改造客观世界。若从人类感受信息的感觉器官角度来看，媒体可划分为视觉类、听觉类、触觉类和其他感觉类等几大类[1]。

“多媒体”从字面上理解就是为多种媒体的综合。多媒体技术的定义为：以数字化为基础，能够对多种媒体信息进行采集、编码、存储、传输、处理和表现，综合处理多种媒体信息并使之建立起有机的逻辑联系，集成为一个系统并具有良好交互性的技术[2]。多媒体是信息发展的一个必然阶段，是一个崭新的技术时代。多媒体引起诸多信息技术的集成和融合的革命。多媒体技术与系统的产生和发展正是现代社会信息化发展的必然。

多媒体技术的应用之所以可以大大改善人类信息的交流，是由以下几个主要特点决定的：

多样性。由于信息的表现形式本身就是多种多样的，而人类感知往往也是多种信息类型的综合作用的结果，而多媒体适应了这种信息载体的多样性，可以提高人类信息感知的质量。

交互性。由于人类感知和思维的特点是形象、联想、多样、模糊、并行，而计算机的特点是符号、精确、串行，这种天然的差别导致人与计算机间的交互的障碍。而多媒体技术的引入使得计算机可以接收、处理和控制多媒体信息，并按人的要求以多种媒体形式表现出来，同时作用于人的多种感官，按照人所习惯的方式实现人与计算机间的互动。

集成性。能够对信息进行多通道统一获取、存储、组织与合成。集成性体现在两个方面，即多媒体信息媒体的集成，处理这些媒体的设备与设施的集成。

信息使用的方便性。用户可以按照自己的需要、兴趣、任务要求、偏好和认知特点来使用信息，任取图、文、声等信息表现形式。

多媒体的这些特点使得人们可以按照自己的思维习惯和自己的意愿主动地选择和接受信息，拟定观看内容的路径；交互性提供了易于操作、十分友好的界面，使计算机更直观、更方便、更亲切、更人性化；集成性可方便地与各种外部设备挂接，实现数据交换、监视控制等多种功能。此外，采用数字化信息有效地解决了数据在处理传输过程中的失真问题。

多媒体的研究内容几乎遍及所有与信息相关的领域，其研究一般分为两个主要的方面。一是多媒体技术，主要关心基本技术层面的内容，包括媒体的性质与相应的处理方法、多媒体数据压缩编/解码技术；二是多媒体系统，主要是多媒体系统的构成与实现，包括多媒体软硬件平台、多媒体数据库、多媒体通信等。另外，还有专门研究多媒体创作与表现的，但更多的属于艺术而不是技术范畴。

可视媒体即视觉类媒体，包括图像、图形、动画、视频和文本等。可视媒体是通过视觉来传递信息的。视觉是人类最丰富的信息来源。在人类通过感觉器官获取的各种信息中，可视媒体约占 80%[3]。当前信息技术的高速发展，使得我们需要

海量信息的处理能力。而可视媒体是人类获取知识和信息的重要来源，视觉信息经数字化后数据量非常大，对计算机的运算、存储、传输和处理等能力提出了更高的要求。对视觉信息的高效处理与利用是当前可视媒体研究中迫切需要解决的问题。

加强可视媒体资源的深度开发、及时处理、传播共享和有效利用，是积极推进信息化的重要组成部分，可视媒体的智能处理已成为经济发展、社会安定和政治军事等国家重大需求中的共性基础技术。当前可视媒体的研究主要包括四个方面：可视媒体的获取，包括可视媒体的数字化、建模及可视化；可视媒体的处理，包括表示、分析、计算、组织、理解等；可视媒体的利用，包括重构、显示、交互等；可视媒体的传播，包括编码、权限管理、内容认证等。本书重点关注可视媒体的安全问题，系统介绍解决视觉媒体安全存储和传输应用中的安全威胁的理论与方法。

由于视觉是人类获取外界信息的最主要的途径，同时视觉信息也最丰富，信息量最大，所以一直以来，多媒体技术的发展主要是以可视媒体技术的发展为标志的。

1.1.2 可视媒体的分类

可视媒体的基本类型可以分为四类，即符号（文字）、图形、图像、视频。

图像（Image）泛指反映二维空间上属性强弱变化所形成的形象。所反映的属性可以是各种不同的物理量，但最终都要转化为光学属性（亮度、颜色）才能为人类视觉感知，所以图像一般特指光学图像。图像经过数字化处理，形成适合计算机处理的数字图像。图像经过对空间量进行离散化和对属性进行量化，就形成以二维数组形式表示的数字图像。其中每一数值代表了特定的位置和色彩属性，称为像素。每个像素具有整数行（高）和列（宽）位置坐标，同时每个像素都具有整数灰度值或颜色值。数字图像放在显示缓存区中，与显示器上的点一一对应，这就是位图图像。图像是最基本的可视媒体类型，其他类型都是由图像派生的。

图形（Graphics）是一种抽象化的图像，是对图像依据某个标准进行分析而产生的结果。它不直接描述数据的每一点，而是描述产生这些点的过程及方法。因此被称为矢量图形，一般直接称为图形。矢量图形是以一组指令的形式存在的，这些指令描述一幅图中所包含的直线、圆、弧线、矩形的大小和形状，也可以用更为复杂的形式表示图像中曲面、光照、材质等效果。在计算机上显示一幅图时，首先要解释这些指令，然后将它们转变成屏幕上显示的形状和颜色。图形的矢量化使得有可能对图中的各个部分分别进行控制。计算机可以对其中任何对象分别进行任意的变换：放大、缩小、旋转、变形、扭曲、移位、叠加等，并仍保持图形特性。图形变换的灵活性，使其在处理上获得了更大的自由度。

符号是对特定图形某种抽象的结果。描述量、语言、数据、标识符、数值、字符等都是符号媒体。由于符号具有明显的结构性，大脑可以识别这种结构，进而可识

别出由这一组符号所代表的信息。这种结构可以组成文本,即字符串;也可以组成数据组,如数据库中的一个元组均可表达特定的信息。符号媒体表达精度高,存储量小。文本媒体是用得最多的符号媒体形式,每个文本都对应特定的形状,最终要变为图像信息进行显示。

视频(Video)又叫动态图像,指连续渐变的静态图像序列沿时间轴顺次更换显示,从而构成运动视感的媒体。当序列中每帧图像是由人工或计算机产生的图像时,称为动画;当序列中每帧图像是通过实时摄取自然景象或活动对象时,称为影像视频,或简称为视频。动态图像演示常常与声音媒体配合进行,二者的共同基础是时间连续性。一般意义上谈到视频时,往往也包含声音媒体[4]。但在这里,视频(动画)特指不包含声音媒体的动态图像。视频是一组静态图像的连续播放。这里的连续既指时间上的连续,也指图像内容上的连续,即播放的相邻两幅图像之间内容相差不大。而图像可以被理解为离散的视频或视频在某一个时刻上的采样。

可视媒体除了按上述基本类型分类外,还可以有其他的不同分类法:

按照不同来源分类,可以分为人工媒体和自然影像媒体。人工媒体是指通过人工或者计算机生成的可视媒体,包括文字、图形、动画等。自然影像是指通过专用设备采集到的自然景象或其他物理量的自然分布影像形成的媒体,包括照片、影像视频或者遥感影像[5]等。

按照数据的表示模式可以分为矢量型、栅格型和编码型媒体。矢量型是抽象表达的可视媒体。这类媒体通常是由高度结构化的数据来表示,只记录生成图的算法和图上的某些特征点,而不直接表示图的像素。人工媒体通常是矢量型的。由于数字图像是由二维空间排列的像素点组成,这些像素点的值按照逐行扫描的规律转化为一维记录的数据序列,便形成了所谓的栅格型的图像媒体。由于图像和视频的数据量非常大,同时也存在着非常大的冗余[6]。为节省图像或视频的存储容量,增加访问速度,使数字视频便于在计算机上实现,需要进行视频和图像的压缩。这种经过压缩的图像或视频就是编码型的可视媒体。

按照媒体的空间表现属性来划分,可视媒体又可以分为二维媒体和三维媒体。三维图像一般是指通过三维数据建模,模拟人眼观看外部世界的机理,主要是利用投影和视差的原理,通过光影、虚实、明暗对比等在二维图像上形成具有三维立体效果,即可以使眼睛感观上可以在二维图像看到物体的上下、左右、前后三维关系的图像。三维图像的连续播放就形成三维动画或视频。

总之,各种可视媒体具有不同特点和性质,它们通常具有不同的格式,所表达信息的特点和程度也各不相同,这些可视媒体类型之间可以相互转换,并且它们之间的关系也具有丰富的信息。可视媒体具有空间性质,具体体现在它们具有不同的表现空间,可以按相互的空间关系进行组织和转换。可视媒体虽然种类较多,但由于其内在的关联性,所以在大多数情况下,可视媒体主要还是指图像和视频。

1.1.3 可视媒体的特征

经过千百万年的进化，人类获得了通过视觉系统，快速、准确地获取外部世界信息的能力，以形象、联想、模糊、并行为特点的人类视知觉系统，能够从纷繁复杂的可视媒体数据中快速实现物体、场景的认知和信息知识的抽取。虽然计算机的速度越来越快，处理能力越来越强，但是计算机系统在处理可视媒体信息时，却面临着巨大的挑战。迄今为止，相对于人类的处理功能而言，计算机对可视媒体的处理水平还停留在很低的层次，而高层次的处理如解构、认知处理还基本无法进行。之所以如此，是由可视媒体具有的特征决定的。而可视媒体的一些重要特征对可视媒体的信息安全保护同样起着决定性的作用。相对于大量的数据和文本信息，以图像和视频为主的可视媒体信息具有以下显著的特征：

数据量大。可视媒体的第一个显著特征就是数据量大。例如一幅中等分辨率(1024×768 像素/幅)真彩色(24 b/像素)图像，其数据量高达 19 Mb。而视频的数据量更是惊人，如一幅中等分辨率(640×480 像素/幅)真彩色图像，若要达到 25 帧/s 的全动态显示要求，每秒片段所需的数据量为 184 Mb，每小时片段的数据量高达 663 Gb。而对全高清视频(1920×1080 像素/幅)的视频信息来说，每小时片段的数据量高达 4.48 Tb。即使通过压缩处理，也只能降低 1 至 2 个数量级，其数据量仍然很巨大。可视媒体海量数据的特点，使得可视媒体的数据压缩问题成为一个重要研究课题，同时其在存储、计算和传输时也不能不考虑数据的负荷问题。

非结构性。非结构性反映在可视媒体中的每个数据和它所体现的信息之间并没有存在一个直接的、确定的和显式的关系。可视媒体的非结构性特点使得计算机很难提取可视媒体的关键特征、结构、语义和高级属性信息，即很难通过较少的维数实现对这些可视媒体信息的表示，从而导致计算机在进行可视媒体处理时，往往需要进行非常复杂的运算，再加上可视媒体数据本身的海量特点，使得可视媒体的处理是典型的计算密集型任务。

语义多样性。可视媒体信息的语义多样性体现在两个方面：一方面是可视媒体内容的语义多样性，主要表现在可视媒体数据与其结构语义单元(如对象)和场景结构(如背景)之间的不确定性；另一方面是其数据的组织和表示的多层次的语法结构信息和丰富的语义信息，主要体现在压缩码流中的语法结构信息指明压缩码流中的各个编/解码参数和状态，而语义信息描述图像和视频中的物体的颜色、纹理、轮廓、运动等。可视媒体包含复杂、多层次的语义结构以及丰富的结构语义上下关联信息，而这些信息对于人们分析和识别图像信息又起到了决定作用，一般不能破坏，导致了可视媒体信息处理时通常需要考虑语义不变性(如格式兼容性)的约束条件，增加了处理计算的困难。

实时性。实时性是可视媒体处理时必须面对的一个重要问题。一方面，可视媒体应用，如人机交互、传输以及视频播放都必须是实时的，同时由于可视媒体的

数据海量性,处理的复杂性以及语义不变性,导致实时性通常不是那么轻易就可以实现的。所以实时性要求是可视媒体信息处理经常需要顾及的约束条件。

可视媒体的以上特征,决定了可视媒体信息处理是典型的数据密集型和计算复杂型任务,且常常需要满足语义(格式)不变性和实时性等约束条件,凸显了可视媒体信息处理中的困难,同时也成为相关研究包括信息安全理论与技术研究的动力。

1.1.4 可视媒体的发展

从一开始,可视媒体就是随着计算机技术,信息处理、数字存储技术和网络技术发展而发展的。纵观可视媒体技术的发展,大概可以分为两个阶段:可视媒体兴起阶段和可视媒体发展阶段。从20世纪80年代到90年代中期,可视媒体技术开始兴起,其标志性的事件包括:

美国Apple公司推出的Macintosh计算机首次使用了窗口和图标作为用户界面,使得以图形为代表的多媒体引入计算机系统。

激光只读存储器的问世以及CDI激光光盘系统标准、交互式数字视频(Digital Visual Interface,DVI)系统、HyperCard计算机处理卡的相继出现,实现了多媒体内容的大容量的存储、检索、处理的规范化、标准化和实用化。

多媒体个人计算机(Multimedia Personal Computer,MPC)标准的制定,为多媒体技术制定了相应的标准和规范,对多媒体软硬件进行了规范,对声音、动画和视频的播放作出了规定,有力地促进了多媒体市场的发展;视频压缩标准MPEG的出现,使得视频技术更加成熟和规范,催生了一批多媒体产品的出现,如VCD、VOD等;一系列多媒体国际会议(如ACM Multimedia,1993,1995)的召开,对多媒体工具、媒体同步、超媒体、视频处理和应用、压缩与编码、通信协议等问题的关注与讨论,标志着多媒体技术开始进入成熟发展的阶段。

经过短暂沉寂之后,从20世纪90年代后期开始,可视媒体技术又进入成熟发展阶段,其标志性的事件包括:

一大批多媒体产品如VCD、DVD、VOD等大量进入家庭,标志着多媒体开始进入普及阶段,开始深入社会经济生活中。

一批多媒体协议与标准如图像编码标准(JPEG、GIF等)、音频系列编码标准G.7xx、视频编码标准MPEG系列标准和H.26x系列标准,以及多媒体通信系列标准H.32x的制定,使多媒体及多媒体通信技术走向全面成熟。

一大批多媒体通信产品如会议电视系统、网络视频会议系统、监控系统的出现,以及它们所衍生的远程医疗、远程教学、视讯会议、远程监控等应用的普及,标志着多媒体通信的时代开始。

随着网络技术的发展和普及,网络多媒体,如网络流媒体、多媒体游戏、多媒体邮件、多媒体浏览器等,开始全面渗透到人们工作、学习、生活的各个方面。

近年来，随着数码相机、数码摄像机以及网络即时通信工具的普及，多媒体已全面进入人们的日常生活和社会经济的各个方面；多媒体移动终端的出现，标志着移动多媒体时代的到来；可视媒体不再局限在二维显示，三维图形、图像和视频开始大量出现，相应的技术也从二维处理发展到三维处理时代，可视媒体进入更加全面纵深发展阶段。

1.2 可视媒体安全

绝大多数多媒体的应用都是在开放环境中，信息安全是一个不容忽视的问题，特别是涉及敏感信息时，防窃取、截取、遗失、破坏等是多媒体信息安全中首要考虑的问题[7,8]。可视媒体是多媒体中最重要的组成部分，包含了多媒体的重要信息，这些重要信息可能涉及个人隐私、商业秘密以及社会安全、国民经济命脉、政治军事秘密等敏感信息。随着网络技术的飞速发展，可视媒体在这个“开放”式网络上的传输已成必然，所以在多媒体信息安全中，可视媒体的安全是重中之重。当前网络犯罪日益猖獗，黑客入侵、网络间谍、木马病毒等的存在，使信息安全面临严峻形势，使得可视媒体普遍存在安全隐患，其安全问题日益受到重视。图像和视频这两类可视媒体涉及的安全问题已经成为当前信息安全领域的研究热点。

1.2.1 可视媒体面临的安全问题

信息安全是一个广泛而抽象的概念。信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。可视媒体，作为重要的信息资源建设的主体，其价值是在利用过程中体现的，而利用的过程就不可避免地涉及保管、传播、共享和自增值四个环节，而信息安全就要求可视媒体资源的保管是可靠的，传播是可控的，共享是授权的，增值是确认的。具体来讲就是：在保管过程中，要保证存储的可靠性，即数据不被破坏，不被非法窃取、泄露和扩散；在传播过程中，要保证数据的完整性，即数据的来源、去向、内容真实无误，要保证传输的不可否认性或不可抵赖性，即数据的发送和接收者无法否认自己所做过的操作行为等；在共享过程中，要保证可用性，即网络传输和数据内容随时可用；在使用过程中，要保证可控性，即使用的方式、时间、范围等被限定在合法授权的范围内。这些要求从不同角度诠释了信息安全的五个基本属性，即保密性、完整性、可用性、不可否认性及可控性。

所谓信息安全问题，就是如何防范信息面临的安全威胁的问题。安全威胁来自多方面，从宏观上可以分为人为威胁和自然威胁。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等给信息内容或存储媒体造成的危害。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故），另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。自然威