高等院校信息技术规划教材

数字内容安全原理与应用

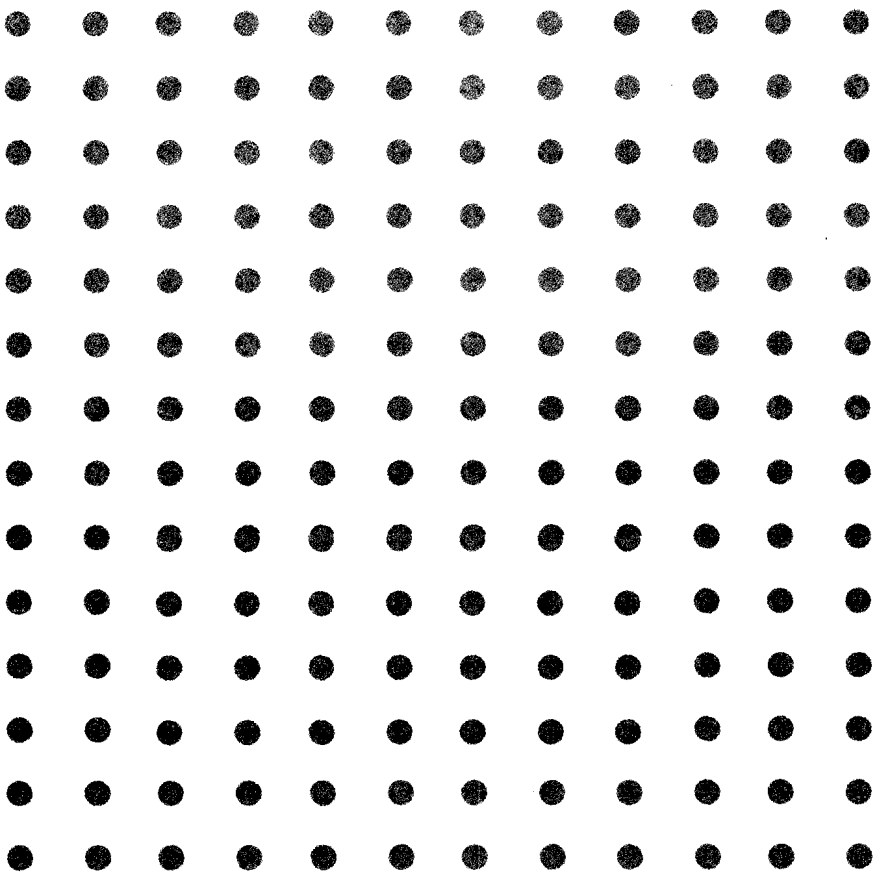
彭飞 龙敏 刘玉玲 编著
李仁发 主审

清华大学出版社

高等院校信息技术规划教材

数字内容安全原理与应用

彭飞 龙敏 刘玉玲 编著



清华大学出版社
北京

内 容 简 介

本书全面介绍了数字内容安全技术的起源、研究发展和应用。全书共分为10章，内容包括绪论、信息加密技术、消息认证与数字签名、信息隐藏与数字水印、数字取证技术、文本内容安全、数字图像内容安全、数字音频内容安全、数字视频内容安全和数据库安全。

本书适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业技术人员阅读参考。

图书在版编目（CIP）数据

数字内容安全原理与应用/彭飞等编著. --北京：清华大学出版社，2012.7
（高等院校信息技术规划教材）
ISBN 978-7-302-28429-1

Ⅰ. ①数… Ⅱ. ①彭… Ⅲ. ①信息安全－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2012)第060477号

责任编辑：白立军　顾　冰
封面设计：傅瑞学
责任校对：白　蕾
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京世知印务有限公司
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张**：18.25　　**字　数**：435千字
版　　次：2012年7月第1版　　**印　次**：2012年7月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：045555-01

前言 foreword

随着信息技术的发展，数字内容已成为信息的重要表现形式。由于数字内容在互联网上使用的便捷性大大超过了传统模拟形式的信息内容，其应用的广度和深度还在不断增加，数字内容产业已初见规模。然而，数字内容在给人们生活和工作带来便利的同时，也面临着严重的安全威胁。这些威胁主要包括数字内容的非法复制和传播，导致重要信息泄露、数字资产被盗窃；数字内容的非授权篡改，严重影响正常工作进行；数字内容的伪造，导致系统混乱，以至造成各种负面影响；数字内容的可用性，由于非法数据或非正常数据等导致其他数字内容的无法正常和有效使用。安全问题已逐渐成为制约数字内容推广应用的主要瓶颈之一。因此，提高全社会的安全意识和加强信息安全专业知识的教育是保障数字内容产业健康、稳步、快速发展的前提和基础。

数字内容安全是当前信息安全领域的一个重要研究领域，其相关技术还在不断完善。本书的作者在数字内容安全领域开展了一些教学和研究工作，并深感数字内容安全领域的重要性和良好的发展前景。作者结合自己所在单位信息安全专业本科生和相关方向研究生培养的实际情况，编著和出版本书作为专业课程教材。

全书共分为 10 章，其中第 1～5 章主要为原理方面的介绍；第 6～10 章是应用方面的介绍。第 1 章介绍数字内容的特征、功能以及分类等基本概念，分析数字内容所面临的威胁，并介绍数字内容安全的研究内容与发展历程。第 2 章介绍密码学的基本原理，主要包括古典密码学、对称密码技术、公钥密码技术以及一些新兴的密码技术（如混沌密码技术与量子密码技术等），并列出一些经典的密码算法。第 3 章介绍消息认证与数字签名的基本概念、消息认证的模式与认证方式、单向 Hash 函数与消息认证码的基本原理、常用的数字签名及一些认证的方法和技术。第 4 章介绍信息隐藏与数字水印的基本原理，主要包括信息隐藏与数字水印技术的基本概念、空域和变换域的信息隐藏技术、数字水印技术以及信息隐藏与数字水印的发展与应用等。第 5 章介绍数字取证的基本原理与相关技

术，主要包括数字取证的技术分类、数字内容篡改取证、数字内容来源取证以及数字内容隐秘分析取证，并介绍一些经典的取证案例与取证方法。第6章介绍文本信息的基本概念与文本内容的安全技术，具体包括文本内容加密、文本水印及文本隐写分析技术等。第7章针对数字图像的特点，介绍数字图像以及数字图像内容的相关概念，对数字图像加密技术、数字图像水印技术以及数字图像隐写分析技术进行深入的阐述。第8章对数字音频内容安全的有关概念和方法进行介绍，主要包括数字音频内容加密、数字音频隐写与水印等方面。第9章对数字视频内容安全的有关概念和方法进行介绍，主要包括数字视频内容加密、数字视频隐写与水印、数字视频隐写分析技术与数字视频取证等方面的知识。第10章介绍数据库的基本特性以及数据库所面临的安全威胁，对当前数据库安全技术进行全面的介绍。具体包括数据库的机密性、完整性、访问控制以及安全管理等方面的知识。每章末均给出了适量的思考题作为巩固所学内容之用。

本书作为教材适合于48～64学时的教学，建议的教学方式为课堂讲授与实验相结合，教师可根据书上的练习题，指导学生进行编程或仿真实验，通过对原理和应用算法的实验，进一步加深学生对所学内容的理解。

本书适合作为信息安全专业本科高年级学生以及研究生的专业课教材，也可供从事信息安全专业的技术人员和研究人员阅读参考。

本书作者多年来一直从事信息安全的教学和研究工作，本书也是网络与信息安全湖南省重点实验室全体师生多年从事数字内容安全研究工作成果的结晶。

本书由彭飞负责编写，全书由龙敏和刘玉玲负责整理修改。在本书的编写过程中，陈丽、朱小文、李洪淋、刘娟、李姣婷等研究生参与了部分资料收集与整理工作；湖南大学信息科学与工程学院李仁发教授对本书进行了认真细致的审阅并提供了宝贵的修改意见和建议；清华大学出版社为本书的出版提供了帮助；此外本书的编写还得到了湖南大学信息科学与工程学院赵欢教授的大力支持。在此对他们表示由衷的感谢。

数字内容安全是一门正在发展中的学科，对本书的编著是作者在该领域的一次尝试，由于作者水平有限，书中难免存在疏漏和错误之处，望读者提出宝贵意见，以方便作者日后修改和完善。

作　者

2012年4月

目录 Contents

第 1 章　绪论 …… 1

1.1　数字内容的基本概念 …… 1
1.1.1　数字内容的概念与特征 …… 1
1.1.2　数字内容的分类 …… 2
1.1.3　数字内容的特性 …… 2
1.1.4　数字内容相关技术 …… 3
1.2　数字内容面临的威胁与分类 …… 3
1.2.1　数字内容面临的威胁 …… 3
1.2.2　威胁的分类 …… 4
1.3　数字内容安全技术 …… 4
1.3.1　数字内容安全技术的发展历程 …… 4
1.3.2　数字内容安全的研究内容 …… 5
思考题 …… 6
参考文献 …… 6

第 2 章　信息加密技术 …… 7

2.1　密码学基础 …… 7
2.2　古典密码技术 …… 8
2.2.1　代替密码 …… 8
2.2.2　置换密码 …… 14
2.3　对称密钥密码技术 …… 15
2.3.1　基本概念 …… 15
2.3.2　流密码技术 …… 15
2.3.3　分组密码技术 …… 18
2.3.4　对称密钥密码的分析方法 …… 25
2.4　公钥加密技术 …… 27
2.4.1　基本概念 …… 27

2.4.2 RSA 公钥密码算法 …… 28
2.4.3 ElGamal 算法 …… 29
2.4.4 椭圆曲线公钥密码算法 …… 30
2.5 新型密码技术 …… 32
2.5.1 新型密码技术简介 …… 32
2.5.2 混沌密码技术 …… 32
2.5.3 量子密码技术 …… 37
思考题 …… 40
参考文献 …… 42

第 3 章 消息认证与数字签名 …… 43

3.1 消息认证与数字签名概述 …… 43
3.2 单向 Hash 函数 …… 44
3.1.1 基本概念 …… 44
3.1.2 常见的单向 Hash 函数 …… 45
3.1.3 单向 Hash 函数的攻击方法 …… 51
3.2 消息认证码 …… 53
3.2.1 基本概念 …… 53
3.2.2 常见的消息认证码算法 …… 54
3.2.3 分组加密与消息认证码 …… 56
3.3 数字签名技术 …… 58
3.3.1 基本概念 …… 58
3.3.2 常用的数字签名体制 …… 59
3.3.3 盲签名和群签名 …… 61
3.4 消息认证模式 …… 63
3.4.1 消息的完整性与消息认证 …… 63
3.4.2 消息认证模式 …… 65
3.4.3 消息认证方式 …… 65
思考题 …… 65
参考文献 …… 67

第 4 章 信息隐藏与数字水印 …… 68

4.1 基本概念 …… 68
4.2 信息隐藏技术 …… 73
4.2.1 信息隐藏技术的发展历程 …… 73
4.2.2 信息隐藏技术的分类与要求 …… 74
4.2.3 信息隐藏技术的基本原理与模型 …… 75

4.2.4 空域信息隐藏技术 …… 76
4.2.5 变换域信息隐藏技术 …… 78
4.2.6 其他信息隐藏技术 …… 79
4.3 数字水印技术 …… 80
4.3.1 数字水印的框架和分类 …… 80
4.3.2 数字水印的评价指标 …… 82
4.3.3 数字水印的攻击方法 …… 83
4.3.4 版权保护数字水印技术 …… 85
4.3.5 内容认证数字水印技术 …… 87
4.3.6 可逆水印技术 …… 87
4.3.7 软件水印技术 …… 97
4.4 信息隐藏与数字水印的应用与发展 …… 100
4.4.1 信息隐藏技术的应用与发展方向 …… 100
4.4.2 数字水印技术的应用和发展方向 …… 101
思考题 …… 102
参考文献 …… 102

第5章 数字取证技术 …… 104

5.1 数字取证基本概念 …… 105
5.1.1 数字取证概念 …… 105
5.1.2 取证过程模型 …… 106
5.1.3 数字取证常用工具 …… 108
5.2 数字取证分类 …… 108
5.2.1 数字取证技术的分类 …… 108
5.2.2 证据取证分析技术分类 …… 111
5.2.3 取证技术产品、标准和规范 …… 112
5.3 数字内容篡改取证 …… 112
5.3.1 数字内容篡改手段 …… 112
5.3.2 数字内容篡改取证方法的评价指标 …… 115
5.3.3 数字内容篡改取证方法 …… 116
5.4 数字内容来源取证 …… 119
5.4.1 数字内容的来源渠道 …… 119
5.4.2 数字内容来源取证方法的评价指标 …… 121
5.4.3 数字内容来源取证方法 …… 122
5.5 数字内容隐密分析取证 …… 124
5.5.1 隐密分析取证研究概念及系统模型 …… 124
5.5.2 隐密分析取证分类 …… 125
5.5.3 隐密分析方法的评价指标 …… 126

5.5.4 常见的隐密分析方法 …… 127
思考题 …… 130
参考文献 …… 130

第6章 文本内容安全 …… 133

6.1 文本内容安全基本概念 …… 133
6.1.1 文本数据的概念、分类及表示 …… 134
6.1.2 文本字符的编码方式 …… 135
6.1.3 自然语言处理 …… 136
6.1.4 文本内容安全的技术分类 …… 139
6.2 文本内容加密技术 …… 140
6.2.1 文本内容加密技术的分类 …… 140
6.2.2 典型的文本加密方法 …… 140
6.3 文本隐写与文本水印技术 …… 141
6.3.1 文本隐写技术 …… 142
6.3.2 文本数字水印技术 …… 144
6.3.3 典型的文本隐写与水印方法 …… 150
6.4 文本过滤与分类技术 …… 153
6.4.1 文本过滤技术 …… 153
6.4.2 文本分类技术 …… 157
6.4.3 典型的文本过滤和分类方法 …… 159
6.5 文本隐写分析技术 …… 164
6.5.1 文本隐写分析技术概述 …… 164
6.5.2 典型的文本隐写分析方法 …… 167
思考题 …… 169
参考文献 …… 169

第7章 数字图像内容安全 …… 172

7.1 数字图像内容安全基本概念 …… 172
7.1.1 数字图像的概念、分类及特点 …… 172
7.1.2 数字图像的编码方式 …… 174
7.1.3 数字图像处理技术 …… 180
7.1.4 数字图像内容安全的技术分类 …… 183
7.2 数字图像内容加密技术 …… 184
7.2.1 数字图像加密技术分类 …… 184
7.2.2 典型的数字图像加密算法 …… 185
7.3 数字图像内容隐写与水印技术 …… 188

7.3.1 数字图像水印的分类 …… 189
7.3.2 典型的数字图像水印算法 …… 190
7.4 数字图像内容隐写分析技术 …… 191
7.4.1 数字图像隐写分析技术分类 …… 191
7.4.2 典型的数字图像隐写分析算法 …… 192
思考题 …… 197
参考文献 …… 197

第8章 数字音频内容安全 …… 200

8.1 数字音频内容安全基本概念 …… 200
8.1.1 音频信号的数字表示 …… 200
8.1.2 音频文件的存储格式 …… 201
8.1.3 音频信号的传输环境 …… 201
8.1.4 人类听觉特性 …… 202
8.2 数字音频内容加密技术 …… 203
8.2.1 数字音频加密技术简介 …… 203
8.2.2 数字音频加密技术分类 …… 203
8.3 数字音频隐写与水印技术 …… 204
8.3.1 音频数据中的常用隐写算法 …… 204
8.3.2 音频隐写工具 …… 205
8.3.3 音频数字水印基本原理 …… 206
8.3.4 数字音频水印的基本要求 …… 207
8.3.5 数字音频水印的算法分类 …… 207
8.3.6 常见数字音频水印算法 …… 209
8.3.7 数字音频水印的评价标准 …… 211
8.3.8 数字音频水印的发展趋势 …… 213
8.3.9 音频隐写术与数字水印的区别 …… 213
8.4 数字音频隐写分析技术 …… 214
8.4.1 隐写分析原理 …… 214
8.4.2 数字音频隐写分析分类 …… 215
8.4.3 隐写分析常用算法 …… 217
8.4.4 隐写分析方法评价 …… 220
8.5 数字音频取证技术 …… 220
8.5.1 数字音频取证技术步骤 …… 221
8.5.2 数字音频取证的分类 …… 222
8.5.3 数字音频取证常用算法 …… 223
8.5.4 数字音频取证发展趋势 …… 224
思考题 …… 225

参考文献 …… 225

第 9 章 数字视频内容安全 …… 229

9.1 数字视频内容安全基本概念 …… 229
9.1.1 数字视频概述 …… 229
9.1.2 数字视频压缩编码基础 …… 231
9.1.3 数字视频常见格式 …… 232
9.1.4 数字视频编码技术 …… 234
9.1.5 数字视频内容安全技术分类 …… 237
9.2 数字视频内容加密技术 …… 238
9.2.1 数字视频加密技术概述 …… 238
9.2.2 数字视频加密典型算法 …… 240
9.3 数字视频隐写与水印技术 …… 242
9.3.1 数字视频隐写技术 …… 242
9.3.2 数字视频水印技术 …… 244
9.3.3 数字视频隐写与水印典型算法 …… 245
9.4 数字视频隐写分析技术 …… 249
9.4.1 数字视频隐写分析概述 …… 249
9.4.2 数字视频隐写分析典型算法 …… 251
9.5 数字视频取证技术 …… 254
9.5.1 数字视频取证技术分类 …… 254
9.5.2 数字视频取证技术典型算法 …… 257
思考题 …… 259
参考文献 …… 260

第 10 章 数据库安全 …… 262

10.1 数据库安全基本概念 …… 262
10.1.1 数据库的基本概念 …… 262
10.1.2 常用数据库系统与 SQL 语言 …… 263
10.1.3 数据库的数据特点 …… 265
10.1.4 数据库安全概述 …… 266
10.1.5 数据库安全标准 …… 268
10.2 数据库面临的安全威胁 …… 269
10.3 数据库安全访问策略 …… 271
10.3.1 访问控制技术 …… 271
10.3.2 数据库其他安全访问策略 …… 273
10.4 数据库水印技术 …… 274

10.4.1 数据库水印分类 …… 274
10.4.2 数据库水印的技术要求 …… 274
10.4.3 数据库水印的攻击 …… 275
10.4.4 数据库水印算法 …… 276
10.5 数据库安全管理 …… 277
10.5.1 数据库安全管理要求 …… 277
10.5.2 数据库加密技术 …… 277
10.5.3 数据库审计技术 …… 278
思考题 …… 278
参考文献 …… 279

第1章 chapter 1

绪　论

本章学习目标

随着信息技术的发展，数字内容已成为信息的重要表现形式。由于互联网络的不安全性，数字内容的安全问题开始引起广泛的关注。本章介绍数字内容的特征、功能以及分类等基本概念，分析数字内容所面临的威胁，并介绍了数字内容安全的研究内容与发展历程。

通过本章的学习，应掌握以下内容：

(1) 数字内容的特征、功能以及分类。

(2) 数字内容所面临的威胁及其分类。

(3) 数字内容安全的研究内容与发展的历程。

1.1 数字内容的基本概念

信息是人类社会最重要的资源之一，几乎人类的一切活动都依赖于信息的获取与处理。在现代社会里，信息技术的发展程度已成为衡量一个国家或民族是否进步的重要指标。“信息”一词有着悠久的历史，早在两千多年前的西汉，即有“信”字出现。“信”常可作消息来理解。但对于“信息”一词而言，至今还没有一个公认的定义。从信息的本质来看，它实际上是指事物在相互作用中所“刻画”出的记录。信息的记录方法和社会技术的进步密不可分。古人从“结绳记事”、在龟甲与兽骨上刻画象形文字、在青铜器上铸字、使用木简竹简作为文字载体，到纸张记录，每一次信息记录方法的改变，都是当时社会进步的一个重要标志。进入20世纪中叶以来，随着计算机技术与数字化技术的发展，越来越多的信息开始以数字化的方式存在，为了使敏感的数字化信息内容安全可靠，必须保证数字内容的安全。

1.1.1 数字内容的概念与特征

所谓数字内容，“就是以数字形式存在的文本、图像、声音等信息，它可以存储在如光盘、硬盘等数字载体上，并通过网络等手段传播”。从数字内容的定义来看，它包含如下三个方面的含义：

(1) 数字内容是信息的一种表现形式。也就是说,信息的概念更加广泛,数字内容也隶属于信息的范畴,它只是信息的一种表现形式而已。相对于其他信息的表现形式,数字内容的不同之处在于,数字内容是以数字化的方式存在的。

(2) 数字内容的记录载体是数字化设备。与以往采用麻绳、龟甲与兽骨、青铜器、木简竹简和纸张不同,数字内容记录在数字化设备中,如光盘、U 盘、硬盘以及各种类型的存储卡等。与此同时,存储在数字化设备中的数字内容,通常需要专门的设备才能进行读取。

(3) 数字内容的传播手段是网络。数字内容是可传播的,数字内容只有通过传播才能体现出它的有用性。对于数字内容而言,其传播的手段主要是网络,相对于其他手段,数字内容的传播速度更加快捷。

数字内容是当前信息记录的主要手段,但它自身不能独立存在,它必须依附于某种物质载体。与信息一样,数字内容来源、数字内容归宿以及数字内容的传播信道是组成数字内容的三大要素。数字内容来源是数字内容创建的发源地或出处。数字内容归宿是数字内容的接收者。数字内容的传播信道是数字内容传递的通道,是数字内容来源与数字内容归宿之间的联系纽带。

1.1.2 数字内容的分类

随着数字化技术的发展,数字内容的内涵日益丰富,主要包括数字音像、科学出版、远程教育、动漫游戏、金融信息、政府公告、网络博客、网络论坛、短信彩信、彩铃音乐等,涉及教育、科学、金融、文化、娱乐、商业、通信等多个领域。围绕着这些数字内容的开发制作、传递配送和消费使用,一个影响全社会的大规模的产业链正在形成。

从数字内容的表现形式来看,主要包括数字化的文本、图像、图形、音频、视频等形式。就数字文本而言,比较常见的有电子文档、网络新闻、电子邮件、即时通信、博客、微博等;图像、图形则包含栅格图像(如 JPEG、BMP 等格式的图像)与矢量图形(如 CAD、3ds Max、Coredraw 等图形)。此外,音频、视频也是目前在新闻与娱乐中最为常见的数字内容形式。

从技术方面来讲,数字内容开发、数字内容传递和数字内容安全是组成数字内容的三大支柱。数字内容开发一方面与文化创意和艺术创造紧密结合,同时也与图像、音频、视频、Web 2.0 等技术不可分割;随着宽带技术的发展,数字内容传递正在由传统的离线配送向互联网在线传递和移动传递的方向急剧转变,网络门户、搜索引擎、无线宽带、移动交互等技术成为数字内容传递的核心技术;从一般的信息安全的概念出发,数字内容安全主要应保证内容的隐私性、完整性和真实性。

1.1.3 数字内容的特性

数字内容是一种以电子形式存在的数据,通常是集文本、图像、图形、音频与视频于一体的综合信息,其主要特性如下所示。

(1) 数字化:在此之前的信息内容几乎都是以模拟的方式进行存储和传播,而数字

内容则是以比特的形式通过数字化设备进行存储、处理和传播的。

(2) 交互性：在模拟领域中，要实现交互性是非常困难的。但在数字内容中，“人机交互作用”则成为可能，故也是数字内容的一个显著特点。

(3) 多样性：主要是指数字内容的表现形式的多样化。人们可以通过视觉、听觉、触觉等多种方式产生、接收数字内容；数字内容通常是技术与艺术的融合，且具有趣味性。

(4) 集成性：主要表现为数字内容通常是多种媒体信息(如文本、图像、音频、视频等)的集成，就是将各种媒体信息按照一定的规则构成一个有机的数字内容整体，用来表现某种信息，使得信息以更为形象的方式进行传播。

(5) 易复制/分发性：人们也可以借助数字技术和互联网，免费并且没有任何质量损失地批量复制和发行数字内容或数字产品。

1.1.4 数字内容相关技术

与数字内容相关的技术范围较广，它是多种学科和多种技术交叉的领域，其主要技术范畴包括以下内容。

(1) 数字内容的表示与操作：包括数字化文字的处理、数字音频处理、数字图像处理、数字视频处理等。

(2) 数字内容压缩：包括通用压缩编码、专用压缩编码技术(声音、图像、视频)等。

(3) 数字内容的存储：包括光盘存储、移动存储、网络硬盘存储等。

(4) 数字内容的管理：包括数字内容管理、数字内容的版权保护等。

(5) 数字内容传输：包括网络传输技术、移动传输技术、流媒体技术、P2P 技术等。

(6) 数字内容的安全：包括保证数字内容的保密性、完整性、可验证性、抗抵赖性、可用性等方面的信息安全技术。

1.2 数字内容面临的威胁与分类

网络技术的飞速发展使得数字内容在互联网上使用的便捷性大大超过了传统的模拟形式的信息内容，数字内容在给人们生活和工作带来便利的同时，也同时面临着严重的安全威胁。

1.2.1 数字内容面临的威胁

数字内容主要包括文档材料、图纸、语音、视频、程序源代码等以电子形式存在的数据，它们所面临的威胁主要包括：

(1) 数字内容的非法复制和传播，导致重要信息泄露、数字资产被盗窃。

(2) 数字内容的非授权篡改，严重影响正常工作进行。

(3) 数字内容的伪造，导致系统混乱，以造成各种负面影响。

(4) 数字内容的可用性，由于非法数据或非正常数据等导致其他数字内容无法正常和有效地使用。

1.2.2 威胁的分类

根据数字内容所面临的威胁，可以将威胁分为主动攻击和被动攻击两类。

主动攻击是指攻击者对数字内容进行某些修改，或者生成一个假的数字内容。它包括非授权的篡改、伪造、内容重放、拒绝服务、伪装等，通常主动攻击较容易被发现。

被动攻击则指攻击者不对数字内容进行任何的改变，只是通过收集通信内容，对其进行分析来获取数字内容中的信息，其攻击方法包括嗅探、信息收集等攻击方法。相对于主动攻击，被动攻击的检测十分困难，但是对这些攻击进行阻止是可能的。

1.3 数字内容安全技术

针对数字内容所面临的安全威胁，数字内容安全技术应运而生。数字内容安全技术是伴随着数字化技术以及网络技术的发展而发展的。

1.3.1 数字内容安全技术的发展历程

数字内容安全技术的发展与信息安全技术的发展是密切相关的，根据不同数字内容安全技术的特征，可分为如下三个阶段。

1. 基于密码术的数字内容安全技术

在这一阶段，数字内容安全主要体现为数字内容的通信安全，通常采用密码技术（如对称密钥密码、公开密钥密码、单向 Hash 函数、数字签名等）保证数字内容的机密性、完整性、可用性和不可否认性。但是，此类方法无法阻止某些被动攻击，如攻击者可以进行通信流量的分析，得到通信的双方以及通信内容的长度。

2. 基于信息隐藏与数字水印的数字内容安全技术

针对基于密码术的数字内容安全技术的不足，研究人员提出了基于信息隐藏与数字水印的数字内容安全技术。该类技术通常通过将重要信息（如版权信息、机密信息等）嵌入到没有安全要求的载体中，通过隐藏重要信息的存在性确保了信息的安全。通过基于信息隐藏与数字水印的数字内容安全技术，可保证载体的版权，内容的完整性。但由于要在载体上加载额外的信息，此类方法通常都会给载体带来一定程度的失真，影响载体的视听效果，严重时甚至会影响到载体的可用性。

3. 基于数字取证的数字内容安全技术

针对基于信息隐藏与数字水印的数字内容技术的不足，研究人员提出了基于数字取证的数字内容安全技术。该类技术通过分析载体的特性（如统计特性、物理特性、环境特性等）来判断载体的真实性或来源。此类技术不需要在载体中加入额外信息，是当前数字内容安全技术中的一个重要研究内容。

上述三类数字内容安全技术的侧重点各有不同，却均有各自的特色。在实际应用中，任何一类技术均无法解决数字内容的所有安全问题，需要三类技术协作实现。

1.3.2 数字内容安全的研究内容

数字内容安全研究的内容主要包括数字内容加密/解密、数字内容信息隐藏、数字内容取证等。

1. 数字内容加密/解密

数字内容加密就是按确定的加密变换方法（加密算法）对需要保护的数字内容（也称为明文）作处理，使其变换成为难以识读的数据（密文）。其逆过程，即将密文按对应的解密变换方法（解密算法）恢复出现明文的过程称为解密。

为了使加密算法能被许多人共用，在加密过程中又引入了一个可变量，即加密密钥。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。

加密的基本功能包括：防止不速之客查看机密的数据文件，防止机密数据泄露或被篡改；防止特权用户（如系统管理员）查看私人数据文件，使入侵者不能轻易地查找一个系统的文件等。

2. 数字内容信息隐藏

信息隐藏是将秘密消息隐藏在其他消息中，这样，真正存在的秘密就被隐藏了。通常发送者将秘密信息隐藏在大家耳熟能详的信息载体中，如人民日报的社论、Internet 上广为流传的图片、流行音乐或电影等。

信息隐藏是继加密技术之后，保护数字内容的又一强有力的工具。信息隐藏与传统的信息加密的明显区别在于，传统的加密技术以隐藏信息的内容为目的，使加密后的文件变得难以理解，而信息隐藏是以隐藏秘密信息的存在性为目标。所以科学技术的发展使信息隐藏技术在信息时代成为新的研究热点。它既发扬了传统隐藏技术的优势，又具有了现代的独有特性。

3. 数字内容取证

功能强大的多媒体编辑软件使得数字图像和音视频数据等数字内容的处理变得简单，尽管多数人对数字内容的修改只是为了增强表现效果，但也存在有人出于各种目的传播经过精心伪造的数字图像和音视频数据。篡改和伪造的数字图像和音视频一旦被用于媒体报道、科学发现、保险和法庭证物等，将会对政治、军事和社会的各方面产生严重的影响。因此，需要一种客观、公正、能够澄清事实真相的验证技术，数字内容取证正是为这一目的而提出的。

数字内容取证通常按以下两个原理工作：

（1）通过对数字内容特征进行分析来判断多媒体内容的完整性、原始性和真实性。

（2）通过对残留在数字内容内部的设备印迹以及数字信号处理后的噪声进行分析来追溯数字内容数据的来源。