

《消息鉴别与生物认证》

图书基本信息

书名：《消息鉴别与生物认证》

13位ISBN编号：9787115372977

出版时间：2015-2

作者：王志芳

页数：273

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《消息鉴别与生物认证》

内容概要

生物识别技术专业书籍；

反映相关领域的新研究进展；

注重理论基础知识和新研究成果之间的平衡；

先进性和实用性的完美统一。

为读者全面系统地了解 and 掌握信息安全的本质、技术和方法，提供了极好的学习和研究平台。

以经典的应用密码学的角度，讨论了消息鉴别的概念、基于加密的消息鉴别、基于对称密码的消息鉴别、基于公钥密码的消息鉴别、基于Hash函数和认证码的消息鉴别等关键技术问题，为读者系统地捋清了上述各项技术对于消息的完整性与消息的真实性认证的思路、方法与手段。

《消息鉴别与生物认证》

作者简介

王志芳，黑龙江大学副教授、硕士生导师，中国计算机学会会员，黑龙江省仪器仪表学会理事。主要研究方向为信息安全、图像处理、生物识别等，近年来发表学术论文20余篇，主持国家级项目2项，省级项目2项，其他项目多项。从事信息安全方向教学多年，主讲《应用密码学》、《保密通信》、《信息安全数学基础》、《信号与系统》等多门本科生、研究生课程。

书籍目录

第1章 消息鉴别概述	1
1.1 信息安全与消息鉴别	1
1.2 消息鉴别的要求	2
1.3 消息鉴别的手段	3
第2章 基于加密的消息鉴别	5
2.1 密码学概述	5
2.1.1 密码学由来	5
2.1.2 密码学基本概念	6
2.1.3 密码体制的分类	10
2.2 古典密码	11
2.2.1 置换密码	11
2.2.2 替代密码	16
2.2.3 古典密码的统计分析	28
2.3 近代密码	32
2.3.1 加密的机械化	32
2.3.2 转轮机的爆发	33
2.3.3 Enigma传奇	34
2.3.4 Enigma的破译	41
2.4 现代密码	48
2.5 基于加密的消息鉴别方案	48
第3章 基于对称密码的消息鉴别	51
3.1 对称密码体制概述	51
3.2 分组密码	52
3.2.1 分组密码概述	52
3.2.2 分组密码结构	53
3.2.3 数据加密标准 (DES)	55
3.2.4 高级数据加密标准 (ADES)	63
3.2.5 分组密码工作模式	68
3.3 序列密码	75
3.3.1 序列密码概述	75
3.3.2 线性反馈移位寄存器	77
3.3.3 基于LFSR的序列密码	78
3.3.4 RC4	80
3.3.5 A5/1	82
3.4 基于对称密码的消息鉴别方案	84
3.4.1 基于分组密码的消息鉴别方案	84
3.4.2 基于序列密码的消息鉴别方案	85
第4章 基于公钥密码的消息鉴别	87
4.1 公钥密码体制的由来	87
4.1.1 对称密码的尴尬	87
4.1.2 Diffie-Hellman密钥交换	88
4.1.3 不对称密钥的奇思妙想	89
4.2 公钥密码体制的概述	90
4.3 RSA算法	92
4.3.1 RSA算法的数学基础	93
4.3.2 RSA算法原理及证明	95
4.3.3 RSA算法的可靠性	96

- 4.3.4 RSA算法的有效实现 97
- 4.4 EIGamal算法 100
 - 4.4.1 离散对数问题 100
 - 4.4.2 EIGamal算法原理 101
- 4.5 椭圆曲线密码算法 102
 - 4.5.1 椭圆曲线上的运算 102
 - 4.5.2 椭圆曲线算法原理 105
- 4.6 基于公钥密码的消息鉴别方案 107
 - 4.6.1 基于RSA的数字签名方案 107
 - 4.6.2 基于EIGamal的数字签名方案 109
 - 4.6.3 基于椭圆曲线公钥算法的数字签名方案 110
- 第5章 基于散列函数和认证码的消息鉴别 112
 - 5.1 散列函数概述 112
 - 5.1.1 散列函数的要求 112
 - 5.1.2 散列函数的结构 113
 - 5.1.3 散列算法的设计方法 113
 - 5.2 MD5及其家族 114
 - 5.2.1 MD5算法 114
 - 5.2.2 MD算法家族 117
 - 5.3 SHA-1及其家族 117
 - 5.3.1 SHA-1算法 117
 - 5.3.2 SHA家族 121
 - 5.4 感知散列 124
 - 5.4.1 感知散列的定义 124
 - 5.4.2 感知散列的性质 125
 - 5.4.3 感知散列的分类 125
 - 5.5 基于散列函数的消息鉴别方案 127
 - 5.5.1 基于传统散列的消息鉴别方案 127
 - 5.5.2 基于感知散列的消息鉴别方案 129
 - 5.6 基于认证码的消息鉴别方案 130
 - 5.6.1 HMAC设计目标 131
 - 5.6.2 HMAC算法 132
 - 5.6.3 HMAC的安全性 134
- 第6章 生物认证与消息鉴别 135
 - 6.1 消息源真实性认证——生物识别 135
 - 6.2 消息完整性认证——生物散列 136
 - 6.2.1 生物密钥 136
 - 6.2.2 生物模板保护 137
 - 6.3 生物特征的感知信息 137
- 第7章 生物识别技术 141
 - 7.1 生物特征与生物识别系统 141
 - 7.2 生物识别系统工作模式 142
 - 7.2.1 工作模式 142
 - 7.2.2 性能评价参数 143
 - 7.3 单模态生物识别技术 145
 - 7.3.1 生物识别技术的应用 145
 - 7.3.2 典型生物识别系统 148
 - 7.4 多模态生物识别技术 152
 - 7.4.1 多模态生物识别的背景和意义 152

- 7.4.2 多模态生物识别发展现状 153
- 7.5 多模态生物特征融合的层次结构 157
- 7.6 多模态生物感知特征融合模型 159
- 第8章 基于感觉信息的多模态生物特征融合 161
 - 8.1 指纹感觉特征提取 161
 - 8.1.1 指纹方向场的求取 162
 - 8.1.2 指纹图像增强 171
 - 8.1.3 指纹感觉特征 175
 - 8.2 虹膜感觉特征提取 175
 - 8.2.1 虹膜内外边界定位 176
 - 8.2.2 眼皮定位 179
 - 8.2.3 虹膜感觉特征 182
 - 8.3 人脸感觉特征提取 183
 - 8.4 多模态感觉特征融合算法 184
 - 8.4.1 指纹—虹膜感觉特征融合 185
 - 8.4.2 指纹—人脸感觉特征融合 186
 - 8.4.3 虹膜—人脸感觉特征融合 189
- 第9章 基于知觉信息的多模态生物特征融合 191
 - 9.1 知觉特征空间特性 191
 - 9.2 扩展普通向量算法 193
 - 9.2.1 基于类内散度矩阵值域求解法 194
 - 9.2.2 基于样本差分子空间求解法 198
 - 9.2.3 类内散度矩阵值域与样本差分子空间的等价性 200
 - 9.3 基于ECV的多模态知觉特征融合算法 202
 - 9.3.1 指纹—虹膜知觉特征融合 204
 - 9.3.2 指纹—人脸知觉特征融合 205
 - 9.3.3 虹膜—人脸知觉特征融合 207
- 第10章 基于感觉—知觉信息的多模态生物特征融合 209
 - 10.1 PCA复数域的非线性扩展 209
 - 10.1.1 中心化样本集 210
 - 10.1.2 非中心化样本集 213
 - 10.2 基于EKPCA的感觉—知觉多模态生物特征融合算法 216
 - 10.2.1 指纹—虹膜的感觉—知觉特征融合 217
 - 10.2.2 指纹—人脸的感觉—知觉特征融合 218
 - 10.2.3 虹膜—人脸的感觉—知觉特征融合 219
 - 10.3 FDA复数域的非线性扩展 221
 - 10.4 基于EKFDA的感觉—知觉特征融合算法 225
 - 10.4.1 指纹—虹膜的感觉—知觉特征融合 226
 - 10.4.2 指纹—人脸的感觉—知觉特征融合 227
 - 10.4.3 虹膜—人脸的感觉—知觉特征融合 229
- 第11章 生物散列技术 231
 - 11.1 生物密钥 231
 - 11.1.1 密钥管理 231
 - 11.1.2 生物密钥生成手段 232
 - 11.2 生物识别系统安全 237
 - 11.3 样本部分泄露的安全分析 240
 - 11.3.1 样本部分泄露区分性评测设计 240
 - 11.3.2 样本部分泄露区分性评测结果及分析 243
 - 11.4 生物模板保护 247

11.4.1 模板保护算法概述 247

11.4.2 基于自适应非均匀量化的多模态生物模板保护算法 249

参考文献 255

名词索引 272

《消息鉴别与生物认证》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com