生物特征的安全与隐私

Security and Privacy in Biometrics

〔意〕帕特里齐奥　肯佩斯　编著
陈驰　翁大伟 等 译

科学出版社

生物特征的安全与隐私

〔意〕帕特里齐奥·肯佩斯 编著

陈 驰 翁大伟 等 译

科学出版社

北 京

图字：01-2016-5510 号

内 容 简 介

全书主要内容涵盖了生物特征识别与密码学这个交叉学科的各个方面的问题：生物特征的安全与隐私、安全的生物特征识别系统面临的问题、生物密码框架、生物特征模板的保护、生物特征识别系统中的隐私泄露、指纹生物特征模板的保护、生物特征加密、增强生物特征识别安全性和隐私性的智能卡、生物特征数据保护的标准、生物特征识别在实现定量安全中的角色、具有隐私保护的生物特征识别的最佳应用案例、生物特征识别在欧洲遇到的人权问题等。

本书可作为开发和研究安全模式识别系统的科技人员的专业参考书，也可作为高等院校信息安全、计算机科学、媒体处理、模式识别、计算机视觉、人工智能等专业的高年级本科生或硕士研究生的教材，其中生物特征数据保护的标准、具有隐私保护的生物特征识别的最佳应用案例等内容可作为企业管理人员是否引进生物特征识别系统的判断依据。

图书在版编目(CIP)数据

生物特征的安全与隐私/（意）帕特里齐奥·肯佩斯（Patrizio Campisi）编著；陈驰等译. —北京：科学出版社，2017.6

书名原文：Security and Privacy in Biometrics

ISBN 978-7-03-052152-1

Ⅰ. ①生… Ⅱ. ①帕…②陈… Ⅲ. ①特征识别－研究 Ⅳ. ①O438

中国版本图书馆 CIP 数据核字（2017）第 055334 号

责任编辑：童安齐 / 责任校对：王万红
责任印制：吕春珉 / 封面设计：东方人华设计部

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

三河市骏杰印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2017 年 6 月第 一 版 开本：B5（720×1000）
2017 年 6 月第一次印刷 印张：24 1/2
字数：470 000

定价：100.00 元

（如有印装质量问题，我社负责调换〈骏杰〉）
销售部电话 010-62136230 编辑部电话 010-62135120-2016（BP02）

译 者 序

近几十年来，生物特征识别技术获得了长足发展并日渐成熟，各种类型传感器成本逐渐降低，生物特征识别系统已经逐渐进入人们生活的方方面面，但这些系统普遍缺乏安全技术的支撑，储存的生物特征数据面临数据泄露、隐私泄露等安全性问题。近年来，生物特征识别系统的安全性不但备受产业界的关注，也成了国内外模式识别领域和信息安全领域科研人员的研究焦点。

用信息安全的理论和技术来解决生物特征识别系统的安全性问题，并借用生物特征技术解决传统的密钥体制存在的使用不便和记忆困难等缺陷，由此，产生了一个新的交叉学科——生物密码学，而目前这方面的成果不多，国外与此相关的书籍更是很少，国内尚未发现与此相关的专业书籍。

《生物特征的安全与隐私》一书的作者帕特里齐奥·肯佩斯（Patrizio Campisi）是目前国际生物特征识别系统安全领域的专家，他收集整理了国外学者对生物特征识别系统安全性问题研究的杰出成果，同时兼顾理论和实践两个层面，从伦理道德、法律和程序三个方面调研了目前最新的生物特征和隐私保护方法。具体而言，全书聚焦在单模多模生物特征模板保护、加密域的信号处理、安全和隐私泄露评估、安全标准这几个方面的新方法和新框架。书中也介绍了具有安全和隐私保护功能的系统的实际应用，重点介绍了基于生物特征的电子文档、基于人脸和指纹的用户识别系统和用智能卡增强安全性与隐私性的生物特征系统。此外，书中还详细分析了生物特征在日常生活中的广泛使用给人的伦理和尊严带来的影响，最后建立了一个法律上的框架。

这本书内容全面、写作思路清晰、便于理解，可作为开发和研究安全模式识别系统的实践者和科技人员的专业参考书，也可作为信息安全、计算机科学、媒体处理、模式识别、计算机视觉、人工智能等专业的高年级本科生或硕士研究生的教材，其中生物特征数据保护的标准、具有隐私保护的生物特征识别的最佳应用案例等内容可作为企业管理

人员是否引进生物特征识别系统的判断依据。

全书由陈驰和翁大伟博士主持翻译，并最终统稿和定稿。参与翻译和校对的人员还有翁大伟（第1、12章）、朱峰（第4、8、9、11章）、章程（第2、5、6章）、孙博武（第3、10、14章）、宋洁（第7、13、15、16章）。本书的出版得到了中国科学院战略性先导科技专项（项目编号：XDA06040601）的资助，在此一并表示感谢。

由于译者的水平有限，书中不足之处在所难免，敬请读者指正。

陈　驰

2016年10月11日

前　言

在过去的 10 年间，生物特征识别技术因其固有的优势逐渐成为一种重要的身份识别方式。传统的身份认证方法考查的是这个人知道什么，如是否知道密码，或者考查的是这个人有什么，如是否有 ID 卡或令牌，而生物特征识别考查的是这个人是谁，或者这个人有什么样的习惯行为。因而，基于生理特征或者行为特征的认证系统不存在传统认证方法常有的密码遗忘、令牌丢失等问题。近年来，基于生物特征识别技术的认证系统，如人脸、虹膜、指纹认证系统，已经广泛应用于犯罪调查、边防、电子商务、电子银行、在线支付、访问控制等领域。

在设计生物特征认证系统时需要考虑各方面的因素。首先，所选择的生物特征是否满足普遍性、独特性、永久不变性，并且是否便于采集和易于被人接受。除此之外，生物特征识别系统的准确性和计算速度也是非常重要的因素，这一点在系统应用于大规模的人群识别时表现得尤为突出。

随着生物特征识别的广泛使用，生物特征数据的保护成为了新的挑战。如果生物特征数据被攻击者偷取，这些数据可能被复制和滥用。而且，由于生物特征具有不可改变性，无法像 PIN 码一样更新，一旦泄露将造成很大的安全隐患。这也引起了对用户隐私泄露的担忧，因为一些敏感信息，如健康状况，可能会在未经许可的情况下被随意散布，进而可能会造成医疗歧视，如健康状况的泄露会导致保险公司拒绝为具有潜在健康问题的人上保险。不论是政府部门还是私人企业，如果收集了大量的用户生物特征信息却不采取有效的保护措施，那么这些数据从长远来看将面临极大的泄露风险。

从程序、法律和技术三个层面研究生物特征数据及用户隐私保护是一个新的课题。本书同时兼顾理论和实现两个层面，从伦理道德、法律和程序三个方面调研目前最新的生物特征和隐私保护方法。具体而言，本书聚焦在单模多模生物特征模板保护、加密域的信号处理、安全和隐

私泄露评估、安全标准等几个方面的新方法和新框架。书中也介绍具有安全和隐私保护功能的系统的实际应用，重点介绍基于生物特征的电子文档、基于人脸和指纹的用户识别系统和用智能卡增强安全性与隐私性的生物特征系统。此外，本书还详细分析生物特征在日常生活中的广泛使用给人的伦理和尊严带来的影响，最后给出了一个法律上的框架。

本书内容安排如下：

第 1 章　简单介绍生物特征识别系统中的安全和隐私保护问题以及相关的解决方法。

第 2 章　介绍生物特征处理流程中的主要安全要求和一般性的安全性设计原理与方案，简单介绍信息技术中普遍的安全原理，并综述通过生物特征哈希和生物特征加密的方式实现生物特征模板保护的方法，同时简单介绍加密域的生物特征匹配算法的设计原理。

第 3 章　指出 PKI（公钥基础设施）在密钥管理上的缺陷，并提出一个新的密钥管理方法，该方法利用生物特征识别技术缓解 PKI 中的发生在用户层面和证书颁发机构层面的信任问题。借此，提出一种新的基础设施——生物密钥基础设施，它能够在建立信任的同时实现高水平的隐私保护。

第 4 章　探讨生物特征模板保护的问题，综述目前最好的方法。从理论分析和具体实现两个层面探讨针对现实世界生物特征的模板保护方法。

第 5 章　在信息理论框架内分析生物密钥绑定系统的隐私性和机密性。具体来说，确定独立同分布高斯生物特征源情况下密钥速率和隐私泄露率之间的平衡，分析模糊承诺密码协议中编码选择和二进制量化的影响。

第 6 章　探讨多生物特征识别系统中的模板保护问题。具体来说，提出一个基于模糊承诺方案的多生物特征密码系统，该系统能够利用多生物特征数据产生生物密钥，详细叙述基于两个虹膜的系统和基于一个虹膜、一幅人脸的系统的密钥生成方案。该系统除生成强密钥，还同时实现模板的可撤销和隐私保护。

第 7 章　描述源自“安全两方计算理论”的加密域的生物特征数据处理的方法。具体来说，讨论同态密码和乱码电路，并详细叙述怎样用

它们设计生物特征匹配算法。尽管这些方法的计算效率还不能满足现实生活中的应用，但它们已显示出的巨大优势，即完全消除了生物特征识别过程中生物特征泄露的风险。

第 8 章　展示生物特征模板保护在指纹识别系统中的应用。具体来说，解决一些指纹应用相关的技术挑战，如指纹模板保护、高可区分性及鲁棒的指纹特征提取，并分析怎样平衡安全性和匹配准确性之间的矛盾。

第 9 章　生物特征密码系统作为隐私保护技术被应用于基于面部生物特征的敏感人群识别系统中，且该系统已成功应用于安大略省彩票购买与博彩公司自检程序中。在该系统中，生物特征密码系统是具有多层特性的安全和隐私保护方法中的重要组成部分。

第 10 章　介绍智能卡技术如何帮助生物特征识别系统的实现，重点介绍大多数智能卡所自带的安全机制，以及如何将这些安全机制应用于保护生物特征数据。提出多种实现生物特征与智能卡结合的框架，并特别介绍电子护照和西班牙的电子身份证。

第 11 章　描述现实应用中的两个带安全和隐私保护的生物特征识别系统，一个专用于局部访问控制，另一个专用于遥控识别。它们混合使用生物特征密码系统、基于卡的匹配、高级的加密策略以确保系统的安全性和准确性。

第 12 章　从标准化的角度来讨论生物特征数据保护的问题。涵盖 ISO 和其他标准化组织所制定的技术标准（如 SC27、SC37 和 TC68），以及由这些组织所出版的相关技术报告。除了这些直接相关生物特征/身份数据的保密性和完整性的标准外，还探讨有关生物特征识别系统安全性的标准。

第 13 章　介绍生物特征识别在日常生活中的广泛应用给社会伦理带来的影响。此外，一方面，生物特征识别技术被认为能够增强安全性，防止个人身份盗窃；另一方面，随着生物特征数据的广泛使用，威胁网络空间和现实生活中个人或集体身份安全的电子犯罪却越来越多。该章就探讨这其中的矛盾。

第 14 章　讨论带有隐私和数据保护的最佳的生物特征数据处理实例。具体来说，从隐私和数据保护的角度来看，生物特征模板的可撤销

性、不可逆性和不可链接性对于实际运用来说是至关重要的。

第 15 章　综合分析管理个人数据的法律原则，并详述欧洲的生物特征数据保护框架，获得对生物特征数据安全和隐私保护问题的深刻理解。从法律的角度整体分析如下这些选择所带来的不同影响，即不同的系统架构、自愿还是强制注册、原始生物特征数据还是生物特征模板、不同模态的生物特征数据，最终还给出一些建议。

第 16 章　基于丹麦数据保护机构评估过的两个生物特征应用实例，丹麦技术委员会就生物特征识别技术的适当使用向立法者、监管者、企业和个人提出一系列建议。该章讨论这些建议，并与欧洲第 29 条数据保护工作小组提出的一些类似建议进行比较。

帕特里齐奥·肯佩斯

2013 年 7 月

目　录