国家自然科学基金项目
国家高技术研究发展计划（863计划）项目
中央高校基本科研业务费专项资金项目

SHENGWU TEZHENG
de Anquan Jisuan
Lilun yu Jishu

生物特征的安全计算理论与技术

李建平　林　劼　付　波　著

电子科技大学出版社

国家自然科学基金项目
国家高技术研究发展计划（863计划）项目
中央高校基本科研业务费专项资金项目

生物特征的安全计算理论与技术

李建平　林　劼　付　波　著

SHENGWU TEZHENG
de An-quan Jisuan
Lilun yu Jishu

电子科技大学出版社

图书在版编目（CIP）数据

生物特征的安全计算理论与技术 / 李建平，林劼，付波著. —成都：电子科技大学出版社，2011.9

ISBN 978-7-5647-0970-9

Ⅰ. ①生… Ⅱ. ①李… ②林… ③付… Ⅲ. ①计算机安全－加密技术－研究 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字（2011）第 191374 号

内 容 简 介

本书是关于生物特征如：指纹、声纹、人脸、虹膜等应用于信息安全与安全计算领域中的各方面技术的一本学术专著，侧重论述了基于单、多生物特征身份认证与加密的核心理论模型与应用技术，分析了现今生物特征身份认证与生物特征加密技术的重要文献及其相关作者的重要思想，从作者独立研究的角度重点介绍了生物特征在安全计算中两个重要领域的技术与应用，分别是：基于人脸、虹膜、指纹与声纹等多生物特征的鲁棒性融合识别技术及在信息安全中身份认证领域的应用案例；基于单或多生物特征加密理论与技术。特别介绍了作者在生物特征提取、鲁棒性说话人识别、鲁棒性人脸识别、多生物特征融合识别模型与策略、多生物特征加密技术中的科研成果；着眼于生物特征在安全计算领域的现状和未来，提示了生物特征信息安全理论撞击未触及学科的可能性和潜在的学术价值和应用价值。

本书内容由浅入深，理论介绍掌握分寸，定理推导详略适当，关键说明恰到好处，应用案例指明方向。

国家自然科学基金项目
国家高技术研究发展计划（863 计划）项目
中央高校基本科研业务费专项资金项目

生物特征的安全计算理论与技术

李建平 林 劼 付 波 著

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑：曾　艺
责任编辑：曾　艺
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都蜀通印务有限责任公司
成品尺寸：185mm×260mm　　印张 18　　字数 450 千字
版　　次：2011 年 9 月第一版
印　　次：2011 年 9 月第一次印刷
书　　号：ISBN 978-7-5647-0970-9
定　　价：35.00 元

作 者 简 介

李建平，1964 年 10 月出生，工学博士，教授，博士生导师，学术带头人。现任国际小波分析应用研究中心主任，国际学术进展 IPWAAMT，EI 检索学术期刊主编，国际学术期刊 IJWMIP，SCI 检索学术期刊副主编、主要创始人之一，先后担任国际计算机学术大会、第二届智能体媒介技术国际学术大会程序委员会等国际会议的主席。一直致力于小波分析与信息处理技术研究领域（重点是小波理论及其在信息安全中的应用）。在国际上独立提出并系统建立了“小波变换的加速方法”、“矢量积小波变换理论”、“基于小波分析的电子签名系统”等系列理论与方法，并在国际上提出了“基于‘三大特征’的信息安全传输的模型与方法”。先后主持国家 863 高技术项目、国家自然科学基金等 30 余项，在国内外学术期刊上发表论文 150 余篇，被国际三大检索机构 SCI、EI、ISTP 等检索收录论文 48 篇，出版学术著作 16 部，主编 10 部大型国际学术会议论文集。他主持研制的“小波指纹加密系统”、“分布式网络监控系统”等高技术产品产生了广泛的经济效益和社会影响。获得国家科技进步二等奖 1 项、全国优秀科技图书奖二等奖 1 项，西南、西北地区优秀科技图书一、二、三等奖各 1 项。

林　劼，1981 年 1 月出生。2003 年获电子科技大学计算机科学与工程学士学位，2006 年获电子科技大学计算机科学与工程硕士学位，2009 年获电子科技大学计算机学院工学博

士学位。2007～2008 年访问英国 Queen's University of Belfast 大学计算机科学系作联合培养博士生 1 年。从 2002 年开始从事语音及图像信号处理、模式识别、人工智能等领域的研究工作，研究重点是语音、说话人和人脸识别理论及其在信息安全中的应用。在语音信号处理和图像处理理论与应用研究方面有较多成果和较深积累。在国际上提出了“后验联合概率模型及其在语音识别和说话人识别中的应用”、“后验概率联合决策神经网络理论模型”、“M-exponent 相似度理论”等系列鲁棒性模式识别理论与方法。曾先后参与过国家 863 高技术项目、国家自然科学基金等 3 余项，在国内外学术期刊，包括在 EURASIP Journal on Applied Signal Processing ,Computer Vision IET, IEEE International Conference on Acoustics, Speech, and Signal Processing 等国内外信号处理领域权威期刊、国际会议上发表或录用论文 20 余篇，被国际三大检索机构 SCI、EI、ISTP 等检索收录论文 13 篇，参与编写 2 部大型国际学术会议论文集。参与编写论著《Speech Communication Research Trends》，参与编写专著《非常规小波变换与军事生物信息安全》等。同时，作为项目主要撰写人申报国家级科研项目多项，并作为项目负责人完成多项科研开发项目。主要研究兴趣：语音与图像信号处理，序列信号分析、模式识别（包括语音识别、人脸识别、序列信号行为识别）等。

付　波，2009 年毕业于电子科技大学获工学博士学位并留校任教，2007～2008 国家公派访问加拿大 Univ. of Guelph 1 年。从 2002 年开始从事信号处理、模式识别、密码学、人工智能等领域的研究工作，研究重点是生物特征加密算法理论及其在信息安全中的应用。目前主持包括国家自然科学基金在内科研项目 2 项，教改实验项目 1 项。并先后参与国家 863、国家自然科学基金项目等 4 余项纵向课题，5 余项横向课题研究和开发。在包括在 IEEE Trans., Chinese Journal of Electronics 等国内外权威期刊、国际会议上发表论文 10 余篇，包括 SCI 期刊 2 篇，EI 检索 5 篇，ISTP 检索 6 篇。参与完成译著 1 部，专著 2 部，教材 1 本。同时，作为项目主要撰写人申报国家级科研项目多项。

前　言

随着信息化、数字化、网络化的发展以及国家及社会生活在安全方面需求的不断提高，基于口令与数字型密码的传统安全技术呈现出许多弊端和缺陷。生物特征认证技术则较好地解决了此类问题。生物特征认证又名生物特征识别，是指通过计算机利用人体固有的生理或行为特征鉴别个人身份的认证方法。生物特征认证与传统的密码、证件等认证方式相比，具有依附于人体、不易伪造、不易模仿等优势，已经成为发达国家普遍重视并大力发展的关键技术和产业。常用的生物特征包括脸像、虹膜、指纹、声音、笔迹等。

现代生物特征最初主要应用于身份认证和系统准入。该领域始于20世纪70年代中期，由于早期的识别设备比较昂贵，因而仅限于安全级别要求较高的部门或设施。现在由于微处理器及各种电子元器件成本不断下降，精度逐渐提高，生物特征识别系统逐渐被应用于人们生活当中。在国家安全、军事安全和公共安全领域，智能门禁、智能视频监控、公安布控、海关身份验证、司机驾照验证等是典型的应用。在民事和经济领域，各类银行卡、金融卡、信用卡、储蓄卡的持卡人的身份验证，社会保险人的身份验证等都具有重要的应用价值。在互联网的资料检索、数据挖掘等方面也有着广泛的应用。将来，在家庭娱乐领域也将具有一些有趣、有益的应用，比如能够识别主人身份的智能玩具、家政机器人等。这些广泛的应用需求，有力地推动着生物特征识别技术的发展。

除身份认证外，生物特征技术与现代密码学的结合，产生出生物特征在安全领域的新型分支研究热点，即生物特征加密技术。生物特征加密的一个核心问题是如何运用模糊的生物特征安全地生成唯一的加密密钥，这需要防止生物特征信息的泄漏，保障密钥的安全存储和传输，提高特征信息和密钥信息的攻击复杂度。生物特征加密是生物特征识别技术的一个重要分支，是此项技术的又一个发展趋势。通过对生物特征加密的研究和开发工作，可解决困扰现今经济、军事等高安全性要求领域的身份认证和数据加密问题，使得生物特征加密技术能够广泛应用到各类重要部门和场所。在生物特征识别与加密技术的研究过程中发现，活体生物特征图像通常都存在噪声和扭曲，这大大降低了生物特征识别的精度，也限制了生物特征技术的应用。因此，生物特征系统必须对图像样本的变形或扭曲具有一定的鲁棒性，以达到预定的识别精度。另一方面，生物特征技术对一些常用的攻击显得很脆弱，比如，通用的重放攻击（Replay attacks）、中间人攻击（Man-in-the-middle attacks）和木马攻击（Trojan horse attacks）。此外，对欺骗攻击（Spoof attacks）和模板攻击（Template attacks）也显得尤为脆弱。由于生物特征无法撤消或替换，这导致生物个体的特征一旦丢失，则存在非常大的风险。采用生物特征技术的原始目的在于便捷性和安全性，但由此可能随之而来的问题和隐患，促使我们思考这样的问题，如果生物特征要大规模应用，这项技术该如何提升其识别性能？能否做到足够的安全和保密？其本身带来的安全性和隐私性的问题又将如何解决？本书将从多个方面阐述和回答以上问题。

本书的安排如下，在生物特征识别上，作者分别针对目前生物特征识别中所遇到的主要

问题，即含噪生物特征鲁棒识别技术进行了广泛和深入的研究。研究重点主要包括现代指纹识别技术、抗噪说话人识别技术、鲁棒性人脸识别技术和多生物特征融合识别技术等方面，研究内容与成果分别阐述在本书第 10、11、12 与 13 章。第 10 章中重点对现代的指纹识别技术和近几年在指纹识别上的技术革新进行了阐述。第 11 章中，作者首先对现今说话人识别中的典型技术进行了总结与比较，对噪声类型和噪声对识别系统的影响进行了分析，然后重点对窄带与宽带强背景噪声环境下说话人识别的鲁棒性技术进行了深入研究，提出了多种新方法与模型。第 12 章中，作者对目前典型的人脸识别技术进行了总结性阐述，通过分析人脸识别系统性能的各种影响因素的基础上，重点对影响人脸识别系统性能的两大因素：（1）光照条件；（2）局部图像污染，提出并研究了多种鲁棒性新识别模型与算法，并最终较好地解决了可变光照与局部图像污染同时存在条件下的鲁棒性人脸识别问题。单模式生物特征识别认证技术在准确率、用户接受程度、成本等方面都有一定的限制，而且各有缺点，仅适应于各自的应用场合。而多模式生物特征认证技术利用了多个生物特征，结合了数据融合技术,进一步提高了认证的准确率，有效地解决了单模式生物特征识别认证技术的限制和缺点。本书第 13 章，重点阐述了目前典型的多生物特征融合识别技术，并在此基础上进一步提出了多生物特征融合识别策略。

在生物特征加密上，重点在第 14、15 和 16 章进行描述。第 14 章主要对生物特征的研究背景及现状进行了总结和阐述。在第 15 章中，针对单模生物特征加密，介绍了 4 种加密方法：生物加密算法（BE）、模糊提交算法（FC）、模糊 Vault 算法（FV）和模糊提取算法（FE）。并在最后基于 FV 算法，介绍了基于指纹加密的一个实例算法。在第 16 章中，对多模生物特征加密理论模型进行了介绍。首先，通过对研究现状和相关文献的分析，引出了为什么会提出 MBC，并形式化地定义了在生物特征级和密码学级的加密融合思想。随后展示了 4 个融合模型：生物融合模型（Biometric fusion model）、MN 模型（MN model）、OR 模型（OR model）和 AND 模型（AND model）。Shannon 熵分析表明，即使在某些加密密文和生物特征被暴露的情况下，新的构造仍然能够获得可靠的数据安全性和生物隐私性。

为了增进读者对本书中所述各种算法的理解，本书遵循由浅入深，知识体系系统化的原则进行设计与章节安排。为了读者能更好地理解后三部分的内容，在第二部分的基础知识描述中，第 2～6 章对信号处理、模式识别、密码学等各方面相关知识点进行了描述。第三部分第 7～10 章描述了各种生物特征提取典型技术，为后面识别与加密过程中的生物特征提取过程做了铺垫。

作者在国家自然科学基金项目“基于小波分析的军事信息加密后解密的不可计算性研究”（批准号：10471151）、“小波分析的新理论及应用研究”（批准号：60216263）的资助下，对小波分析的理论、算法及军事安全应用作了深入研究，取得了很好的研究成果。这些成果又相继得到国家 863 项目“基于视觉感知与认知机理的多模人物特征身份认证新方法与技术”（批准号：2007AA01Z423）、“基于小波分析的网络信息内容分析与审计技术”(批准号：2003AA148040)、“多数据元安全强审计系统”(批准号：2003AA148010)和国家自然科学基金项目“多模态生物特征加密的理论模型及其实现算法研究”（批准号：61003121）的资助，作者深层次研究了信息安全、生物信息安全、军事信息安全、军事生物信息安全中的小波分析与神经网络应用，提出了许多新的概念、公式、算法、模型，围绕多生物特征识别技术的理论和应用、生物特征识别系统与评测方法等方面发表了 100 余篇学术论文，举办了 6 次国

际会议。在国家高技术研究发展计划（863 计划）项目(2007AA01Z423)、国家自然科学基金项目（基金号：61003121）、中央高校基本科研业务费专项资金项目（项目号：ZYGX2010J070，ZYGX2010J076）资助下，作者对生物特征认证与加密进行长达 5 年时间的研究工作，在鲁棒性生物特征识别与加密领域获得了大量的研究成果，这些研究成果构成了本书的主要内容。

本书由李建平发起组织，国际小波分析应用研究中心全体博士后、博士、博士生参与了工作，李建平在美国、法国、加拿大访问期间，得到了这些国家的大学和研究机构的支持和帮助。为本书作出主要贡献的是李建平、林劼、付波。李建平设计全书的撰写大纲和框架并撰写了部分重要内容；林劼主要撰写本书中第 1、2、3、4、8、9、11、12、13 章；付波主要撰写本书中第 1、5、6、7、10、14、15、16 章。对本书中第 11、12 章要特别感谢英国贝尔法斯特女王大学计算机系（Electrical Engineering and Computer Science,Queen's University Belfast）Ji Ming 和 Danny Crookes 教授所作的贡献。对本书中第 14、15、16 章要特别感谢加拿大圭尔夫大学工程学院（School of Engineering, University of Guelph）Simon X. Yang 教授所作的贡献。本书在撰写过程中引用了大量国内外参考文献，作者感谢为本书撰写提供文献、手稿的国内外专家，感谢他们为本书的撰写提供了十分宝贵的第一手材料，作者认为本书是国内外生物特征安全计算技术研究领域集体智慧的结晶，是研究工作者共同劳动的研究成果。由于作者水平有限，书中肯定会有不妥之处，欢迎国内外专家批评指正，联系 E-mails：jpli2222@{uestc.edu.cn,yahoo.com}，linjie@uestc.edu.cn, bxfu@163.com。

电 子 科 技 大 学
国际小波分析应用研究中心 李建平

2011 年 9 月 10 日

目　录

第一部分　引言

第二部分　基础知识

第三部分　生物特征提取技术

第四部分　生物特征匹配认证技术

第一部分
引　言

第1章 引 言

1.1 信息安全概述

“安全”在《高级汉语大词典》中的意思是“不受威胁，没有危险、危害、损失”。因此，根据信息安全字面的意思就是使得信息不受威胁、损失。然而，一方面，由于信息技术的快速发展和信息系统复杂性的增加而引起信息安全的内涵和外延不断发展，从信息安全的发展过程中，我们就可以看出在其发展的每一个阶段信息安全都有着不同的内涵；另一方面，由于人们对于信息安全本质的认识不断深入，至今也没有对“信息安全”一词达成共识，使得目前没有一个比较成熟的信息安全的定义。一个佐证是：2001年11月，第56届联大会议在通过的决议中呼吁所有会员国就“有关信息安全的各种基本概念的定义”等向秘书长及时通报，其目的在于消除概念上的混乱，更好地促进信息安全国际合作。然而，时至今日，国际上依然没有一个权威的、公认的有关“信息安全”的标准定义。

对于信息安全的定义，不少国家、组织和学者提出许多富有建设意义的看法。以下是一些有代表性的定义方式：

- 国家信息安全重点实验室给出的定义是：“信息安全涉及信息的机密性和完整性、可用性、可控性。综合起来说，就是要保障电子信息的有效性。”
- 国家计算机信息系统安全专用产品分类原则给出的定义是：“涉及实体安全、运行安全和信息安全三个方面。”
- 《中华人民共和国计算机信息系统安全保护条例》给出的定义是：“保障计算机及其相关的和配套的设备、设施（网络）的安全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。”
- 英国BS7799信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”
- 美国国家安全局信息保障主任给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部我们用‘信息保障’来描述信息安全，也叫‘IA’。它包含5种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。”
- 美国国家安全电信和信息系统安全委员会（NSTISSC）给出的定义是：“对信息、系统以及使用、存储和传输信息的硬件的保护，是所采取的相关政策、认识、培训和教育以及技术等必要的手段。”
- 欧共体对信息安全的定义是：“网络与信息安全可被理解为在既定的密级条件下，网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。”