



生物特征识别 理论与应用

田捷 杨鑫 等编著



清华大学出版社

生物特征识别理论与应用

田捷 杨鑫 等编著

清华大学出版社
北京

内 容 简 介

本书以指纹识别技术为主线,系统地介绍了生物特征识别技术的理论和应用。主要内容包括指纹图像的增强、指纹的特征提取、指纹图像的分类与检索及压缩技术、指纹图像匹配算法、指纹识别算法在嵌入式系统中的实现与应用、人脸识别技术以及其他生物特征识别技术、生物特征识别系统与评测方法、生物特征标准化工作、生物特征识别技术的典型应用实例等,并重点介绍了生物特征识别技术安全性研究,给出基于指纹加密的安全邮件系统设计实例。

本书内容系统、全面、新颖,理论与典型应用实例相结合。本书的读者对象为从事生物特征识别、图像处理、计算机应用、模式识别等领域研究的专业人员和应用开发人员,以及高等学校相关专业的师生。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

生物特征识别理论与应用/田捷,杨鑫等编著. —北京:清华大学出版社,2009.2

ISBN 978-7-302-18419-5

I. 生… II. ①田… ②杨… III. 自动识别—研究 IV. TP391.4

中国版本图书馆 CIP 数据核字(2008)第 125633 号

责任编辑:丁 岭 李玮琪

责任校对:李建庄

责任印制:

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

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:

装 订 者:

经 销:全国新华书店

开 本:185×260 印 张:31 插 页:2 字 数:751千字

版 次:2009年2月第1版

印 次:2009年2月第1次印刷

印 数:1~ 000

定 价: .00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。
联系电话:010-62770177 转 3103 产品编号:



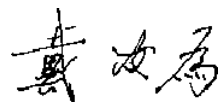
序言

21 世纪是数字化和网络化的时代,目前国内的互联网用户已近 3 亿,而手机用户已过 5.4 亿。在网络化环境下,人们以用户名和密码代表其身份,这种数字身份与其物理身份并非一一对应。因此,要想在数字化网络环境下保持自由,在现实中保持自我,使我们的网络化数字身份与现实的物理身份统一起来,是个挑战性的研究与应用领域。而生物特征识别正是面向这一挑战而快速发展起来的学科。

目前,一方面生物特征识别已在网络环境下的电子政务、电子商务和个人信息安全中得到了广泛应用,成为网络环境中数字化身份识别最安全有效的技术;另一方面,生物特征识别仍是理论研究的热点问题。近年来,国际著名的学术期刊 IEEE PAMI、IEEE SMC 分别推出生物特征识别的专刊,IEEE、ICPR、SPIE 等国际协会也分别连续召开生物特征识别的国际学术会议,充分说明了该领域理论研究的紧迫性。同时,生物特征识别还与密码学相融合,产生了生物特征识别加密的新方向与新应用。

综上所述,我们可以看出生物特征识别是一个充满挑战的研究与应用领域,作者及其团队在生物特征识别研究与应用领域开展了持续十多年的大量理论研究与技术推广应用工作,不仅在 IEEE PAMI、IEEE IP、IEEE SMC 等国际杂志上发表了高水平的学术论文,还积极开展技术推广应用工作,相关技术在电子政务、电子商务系统中得到了成功应用,相应工作还获得了国家科技进步奖和信息产业部重大技术发明奖,以及第十五届全国发明博览会金奖等多项奖励,本书是基于这些理论与应用成果的总结。

希望本书的出版能有利于推动国内生物特征识别研究的深入开展,促进生物特征识别更广泛的应用。



中国科学院院士

中国自动化学会理事长

2009 年 1 月

1. 与传统的密码、钥匙等相比,生物识别技术的优势主要在哪些方面?

我们先来看一个例子,在央视的《新闻调查》节目中,进行了一期关于“谁动了我的隐私”的专题报导,是关于网上银行频频被盗,导致5成以上的中国网民不敢使用网上银行。这说明,传统的身份认证方式已面临是否安全的挑战,如何让个人的隐私乃至国家的信息有更可靠的保证,已逐渐引起重视。那么,为什么传统的密码、钥匙等身份认证方式已不能满足这方面的需求呢?这是因为,利用钥匙等所拥有的令牌方式,存在丢失、被窃和复制等安全隐患;利用密码等所知道的口令方式,则存在遗忘、被攻击的问题。而利用人自身所具有的物理特征,如生物识别技术,可以避免上述问题,因为这些特征具有稳定性、永久性、唯一性和安全性等独特的优势。

生物特征识别技术逐渐成为一种公认的、更安全的身份认证技术。采用“您本身所具有的”(例如指纹、虹膜、声音等)方式验证身份远比采用“您所拥有的”(例如带照片的身份证件)和“您所知道的”东西(例如用户号和密码)方式验证身份更可靠、更安全。

以指纹为例,每个人的指纹都是唯一的,这一点已经分别从经验和理论上被加以证明,而且是相当固定的,很难发生变化;指纹样本便于获取,实用性强;一个人的十指指纹皆不相同,这样可以方便地利用多个指纹构成多重口令,提高系统的安全性;指纹识别中实用的模板并非指纹图像,而是由指纹图像提取的特征信息,这样一方面系统对模板库的存储容量较小,另一方面也保护了用户的隐私。因此你就不必要去记忆很多的密码,也不用随身携带大量的卡片,使用自己的生物特征就可以方便地进行身份的确认。

2. 生物特征识别涉及哪些公众可以接受的概念和技术细节?

首先,我们所说的生物特征识别是通过计算机自动地进行图像采集、特征提取和匹配的过程。一百多年以来,指纹一直被应用于刑事犯罪的侦查中,来确认罪犯的身份。但是在传统的指纹识别中,识别阶段的最终决策是由人工专家来完成的,而其他认证方法,例如DNA、毛发、纤维分析则需要花费几小时甚至几天的时间,这些方式都不适合商业应用。

指纹的传统采集方式是用油墨按压的方式,这种方式至今还在被政府和公安部门所采用。随着技术的发展,基于光学、固态、热成像、超声和多频谱的传感器都已经出现,这些传感器都是把立体的手指表面映射到一个平面,根据脊线和谷线不同的物理特性(例如反射率和电容)来产生数字图像。还有无接触式的传感器,例如高分辨率摄像机,可以直接记录下手指表面的立体图像。这些传感器中很多都价格廉价,集成性也非常好,可以很方便地集成到手机、PDA和笔记本电脑等消费电子产品中去。

一般的生物特征识别系统都是由四部分组成的。(1)传感器,用来读取指纹、虹膜、签名、声音等生物特征;(2)特征提取模块,从原始生物特征数据中提取出一些固有的、基本不变的特征,提取出的特征成为模板;(3)数据库,用来存储所有用户的模板数据;(4)特征匹配模块,用来比对输入的特征和存放在数据库中的模板特征。

我们可以把认证分为两种:1:1和1:N。1:1认证非常简单,假设你的笔记本电脑集成了指纹登录模块,而该数据库中只有你自己的指纹模板,比对任务就是验证你某次登录输入的指纹与唯一的模板是否匹配。简单的说,就是验证“是不是你”的问题。而1:N就比较有挑战性,如果你想要考取驾照,而发证机关怎么确认你不是想要重复考取呢?如果你用伪造的身份证的呢?假如驾照的发证机关配备了指纹认证系统,你就要提供自己的指纹,然后在存储了所有考取过驾照的人地指纹数据库中进行查询,以确认你是否由于被吊销驾照而要重复考取。这是一个验证“你是谁”的问题。

1:1和1:N的认证模式都有成功的应用典型。最具有说服力的1:1系统是美国佛罗里达州奥兰多市的迪斯尼乐园装备的多频谱指纹认证系统,每个购买门票的用户同时要提供拇指指纹,每一枚指纹和门票是唯一绑定在一起的。如果想要进入迪斯尼乐园,必须提供对应的拇指指纹来验证门票的真伪。这个系统目前工作非常正常,每天可以处理100 000人次的身份验证任务。最典型的1:N系统也是美国的,就是著名的US-VISIT计划,每个进入美国国境的人必须提供指纹和脸部扫描图像给边境检查站,开始是只提供左右两个拇指的指纹,最近又升级成提供全部十指指纹。每次要在10秒钟以内完成和数据库中的250万条记录进行比对的任务,自2004年1月份实施以来,这套系统已经处理了7500万左右访问美国的人的指纹。

生物特征识别如何来评测系统的性能呢?通过两个参数:误识率(FAR)和拒识率(FRR)。误识率是非法用户被错误接受的概率,而拒识率是合法用户被错误拒绝的概率。对于特定系统来说,这两个参数并不是独立的,一个拒识率很低的系统很可能会接受很多非法用户,导致误识率很高。所以应该根据不同应用场合的特点来选择这两个参数。有时候为了提高性能,会选择多种生物特征融合的方法,这样可以避免某种生物特征固有的缺陷,取长补短。

3. 生物识别技术作为一种安全措施可能取代密码、钥匙等传统的安全系统吗?

Bill Gates曾做过这样的断言:“生物特征识别技术,利用人的生理特征,例如指纹等来识别个人的身份,将成为今后几年IT产业的重要革新”。Gates的这段言论是因为有越来越多的消费者、公司和政府机关都承认,现有的基于智能卡、身份证或密码的身份识别系统是远远不够的。生物特征识别技术为此提供了一种解决方案。生物特征识别技术是目前最为方便与安全的识别系统,你不需记住身份证号码或密码,也不需随身携带像智能卡之类的东西。“钥匙”就是你自己,没有什么能比这更安全和更方便的了。

同时,这样的断言也是根据目前的理论技术的发展和市场的需求所做出的。一方面,人们对于安全和身份保护的需求越来越高,国家政府的边境检查系统需要快速地确定每个人的身份,公司机构也需要更加便捷、安全地了解员工的考勤和控制对某些敏感数据的访问;更重要的是,经过广大科技工作者的努力,公众对生物特征技术的接受程度越来越高,普遍都能接受使用生物特征来控制诸如笔记本电脑和手机的访问权限,为广泛普及生物特征识别系统奠定了一定的社会基础。另一方面,社会需求也促使硬件制造商制造出价格低廉而

且集成性优良的传感器,以及用于实时采集和识别的软件系统。例如一款可以集成在手机或者笔记本电脑中的刮擦式的指纹传感器芯片,国际价格只有5美元左右。

当今社会,人们生活节奏越来越快,对安全性和便捷性的要求越来越高,这就决定生物特征识别技术终将取代传统的身份认证系统。前一段时间,北京农村商业银行推出了一个新的项目,即“指纹银行”:不用银行卡、存折,也不需要密码,仅凭客户自己的指纹,就可以在银行的自助机上轻松完成缴费、转账等金融业务。这个案例说明,身份识别已从传统的密码、口令的方式,逐渐由生物识别技术替代,并渗透到国家社会安全,甚至普通人的生活中。生物特征身份确认技术将彻底改变人们现有的生活方式和商业模式。

4. 生物特征识别理论和技术面临哪些挑战?发展的趋势如何?

首先是国内公众对生物特征识别的接受程度还有待进一步提高。以指纹识别为例,之前大家普遍认为指纹只会用在公安刑侦领域应用,其实,生物识别技术的应用不仅仅局限于公安刑侦领域,在国家信息安全、电子商务、电子政务及至普通人群,都是生物识别技术的受益者,其应用领域覆盖面是非常广泛的。这个任务需要科技工作者和媒体共同努力,为国内生物特征技术的应用创造良好的环境和氛围。

另外,针对生物识别认证的专门法律以及行业应用中关键技术标准,也是生物特征识别技术发展及广泛应用所面临的挑战。美国是代表国际上生物特征识别先进技术的主要国家。20世纪90年代,美国生物特征识别技术应用的标准化工作就开始启动。国际标准化工作也在2002年成立的ISO/IEC JTC1/SC37下开展相关工作,而我国则刚刚开始标准化制定和推广工作,因此制约了我国生物识别技术的推广和应用。

任何一种技术的发展都是一个循序渐进的过程。随着生物特征系统越来越广泛的应用,对生物特征识别理论和技术提出了更高的要求。识别算法的性能需要进一步提高,以满足越来越大的数据库的要求,而对低质量生物特征数据的增强在一定程度上可以缓解这个问题,同时采用多模态生物特征的融合能够很好地发挥多种生物特征的优势。

传统的身份认证方式实现的是人的数字身份的认证,而生物特征识别技术作为安全级别更高的身份识别技术,则实现了人的物理身份的验证,如果将两种验证方式结合起来,即生物识别技术与密码技术相结合,则可以实现物理身份和数字身份的统一,安全级别更高、更有效。因此,目前国内外研究的一个热点问题就是生物特征加密技术。

简单地说,生物特征加密就是以某种方式把用户的生物特征和密钥唯一的、单方向的绑定在一起,达到双因子认证的更高的安全级别,将用户的数字身份和物理身份统一起来。这样做还可以防止密钥丢失和生物特征信息泄漏的问题,虽然后者目前还仅仅是理论上才存在的,但是很多学者已经前瞻性地注意到了这个问题。这方面国际上有很多研究者和公司在做,也有很多成果,例如有文献称飞利浦公司的研究院已经成功研制出人脸加密系统,可以达到更高的安全性,但是要牺牲一定的识别精度。在国内这个领域,我们实验室一直走在前列,2000年的时候我们已经提出了将指纹和密码结合起来用于网络身份认证的概念,最近又刚刚完成基于指纹的网络授权系统的研究,可以说是国内第一个真正应用生物特征加密概念的实用系统,而该领域还有待进一步的理论创新和算法的实用化,相信这项研究使得应用生物特征进行身份认证的安全性和隐私性将更有保障。

本书以指纹识别技术为主线,系统地介绍了生物特征识别技术的理论和应用。主要内容包括:指纹图像的增强、指纹的特征提取、指纹图像的分类与检索及压缩技术、指纹图像

匹配算法、指纹特征对识别性能的影响、指纹识别算法在嵌入式系统中的实现与应用、人脸识别技术以及其他生物特征识别技术、生物特征识别系统与评测方法、生物特征识别技术的典型应用实例等,并重点介绍了生物特征识别技术安全性研究,给出基于指纹加密的安全邮件系统设计实例。

本书的主要内容是基于作者带领的团队在国家自然科学基金委(60225008,60332010,60303022,60575007,60875018),863(2008AA01Z411)和北京市自然科学基金委(09D0532,4052026)的资助下自1996年以来的研究与应用工作积累,在此感谢陈新建、陈宏、罗西平、何余良和漆远为团队做出的突出贡献。参与本书的编写以及相关工作并做出贡献的还有:曹凯、程建刚、邓翔、段少雄、李恒华、李建杰、李亮、李鹏、刘旭、何晓光、胡瑾、任群、时鹏、苏琪、陶训强、王星明、吴哲、武岩、夏勇、谢卫华、张堂辉、张逊、张阳阳、张瑶瑶(按姓氏字母先后排序)。

最后,特别感谢戴汝为院士从推动生物特征识别技术发展的大局出发,百忙之中为本书写序!

作 者

于北京中关村中国科学院自动化研究所

2009年1月

目录

第 1 章 生物特征识别基础知识	1
1.1 引言	1
1.2 通用概念和术语	1
1.3 生物特征识别技术简介	4
1.3.1 指纹识别.....	5
1.3.2 人脸识别.....	7
1.3.3 虹膜识别.....	8
1.3.4 视网膜识别	10
1.3.5 掌形识别	10
1.3.6 语音识别	12
1.3.7 签名识别	13
1.3.8 其他生物特征识别技术	13
1.3.9 多模态识别	15
1.4 生物特征识别技术的横向比较.....	17
1.5 生物特征识别技术发展现状和趋势.....	18
1.6 本书主要内容.....	21
本章参考文献	21
第 2 章 传感器技术与嵌入式平台	22
2.1 引言.....	22
2.2 指纹图像采集技术.....	22
2.3 其他生物特征采集技术.....	27
2.4 嵌入式指纹识别技术.....	29
2.4.1 嵌入式指纹识别系统简介	29
2.4.2 基于 DSP 的嵌入式指纹识别模块.....	31
2.4.3 基于 ARM 的嵌入式指纹识别模块	39
2.4.4 基于 ASIC 的指纹识别技术的实现	41
2.4.5 嵌入式指纹识别系统中的关键技术	49
2.5 小结.....	50
本章参考文献	50
第 3 章 指纹图像的增强	51
3.1 引言.....	51

3.2	指纹预处理	53
3.2.1	基于傅里叶变换的指纹预处理	53
3.2.2	归一化	54
3.3	方向场的计算	54
3.3.1	掩膜法	54
3.3.2	公式法	56
3.3.3	带反馈的指纹方向场计算方法	59
3.4	图像的增强	62
3.4.1	Gabor 滤波增强	62
3.4.2	基于傅里叶滤波的低质量指纹增强算法	63
3.4.3	基于知识的指纹图像增强算法	68
3.4.4	非线性扩散模型及其滤波方法	71
3.4.5	多尺度滤波	78
3.4.6	基于各向异性的滤波方法	83
3.5	小结	87
	本章参考文献	88
第4章	指纹特征的提取	91
4.1	引言	91
4.2	指纹的整体特征描述	91
4.2.1	指纹奇异点的特征和提取	92
4.2.2	指纹的类型特征	94
4.2.3	指纹的频谱特征	95
4.3	指纹的局部特征描述	103
4.3.1	指纹的细节点特征	104
4.3.2	高分辨率的指纹特征——汗孔	111
4.3.3	指纹的纹理特征	112
4.4	结构化的指纹特征描述方法	113
4.5	小结	115
	本章参考文献	116
第5章	指纹图像的分类与压缩	120
5.1	引言	120
5.2	指纹分类技术	120
5.2.1	基于规则的指纹分类方法	124
5.2.2	基于句法的指纹分类方法	125
5.2.3	结构化的指纹分类方法	125
5.2.4	基于统计的指纹分类方法	127
5.2.5	基于神经网络的指纹分类方法	127
5.2.6	多分类器的方法	128
5.3	基于反馈环节的多分类器方法	129
5.4	基于混合特征的指纹连续分类方法	131

5.4.1	指纹分类特征提取	131
5.4.2	指纹分类	135
5.5	指纹检索	136
5.6	指纹压缩简介	139
5.6.1	图像压缩的衡量标准	139
5.6.2	图像压缩技术分类	140
5.6.3	小波图像压缩的基本方法	141
5.6.4	小波图像压缩算法的新发展	143
5.6.5	几种主要的小波图像压缩算法	144
5.7	小结	150
	本章参考文献	150
第 6 章	指纹图像的匹配	156
6.1	引言	156
6.2	基于点模式的匹配算法	157
6.2.1	基于串距离的匹配算法	158
6.2.2	基于细节点对的指纹匹配	163
6.2.3	基于三角结构的指纹匹配	172
6.2.4	基于拓扑结构的指纹匹配	175
6.2.5	基于点模式匹配算法的比较分析	185
6.3	图匹配及其他方法	186
6.4	基于纹理模式的匹配	189
6.5	混合匹配方法	190
6.5.1	混合匹配方法综述	190
6.5.2	基于混合特征的匹配	190
6.6	非线性形变指纹图像的匹配	195
6.6.1	非线性形变指纹匹配算法综述	196
6.6.2	非线性形变的配准模式研究	197
6.7	多采集仪间的指纹匹配	201
6.8	小结	212
	本章参考文献	213
第 7 章	人脸识别	217
7.1	引言	217
7.2	人脸检测	218
7.2.1	人脸检测方法概述	219
7.2.2	基于启发式模型的方法	221
7.2.3	基于统计模型的方法	226
7.3	人脸正则化	239
7.4	人脸识别	240
7.4.1	人脸识别方法概述	241
7.4.2	基于局部或全局特征的人脸识别算法	242

7.4.3	基于子空间分析方法的人脸识别	251
7.4.4	基于相对差分空间的人脸识别	257
7.5	小结	261
	本章参考文献	261
第8章	其他生物特征识别	273
8.1	引言	273
8.2	掌形识别	273
8.2.1	掌形识别简介	273
8.2.2	掌形的特征及预处理	274
8.2.3	掌形识别算法	277
8.3	虹膜识别	283
8.3.1	虹膜图像的获取	283
8.3.2	虹膜图像的增强	284
8.3.3	虹膜识别算法	287
8.4	签名识别	291
8.4.1	签名识别简介	291
8.4.2	签名识别应用	292
8.4.3	签名采集硬件	292
8.4.4	签名识别算法	292
8.5	小结	295
	本章参考文献	296
第9章	生物特征识别系统及其性能评测	303
9.1	引言	303
9.2	系统要求	303
9.3	系统模型	304
9.4	系统层次框架	307
9.4.1	系统层	307
9.4.2	算法层	309
9.4.3	评估层	310
9.4.4	应用层	310
9.5	生物特征识别系统性能评估	311
9.5.1	标准生物特征识别数据库	311
9.5.2	生物识别算法的评估	327
9.5.3	指纹识别算法的准确性评估	331
9.6	生物特征识别标准化简介	342
9.6.1	标准的需求	342
9.6.2	国际标准化进程	343
9.6.3	国际标准化组织简介	344
9.6.4	ISO/IEC JTC1 SC37 简介	345
9.6.5	现有国际标准简介	347

9.6.6 国内标准化现状	349
9.7 生物特征识别的通用软件接口规范 BioAPI	351
9.7.1 BioAPI 简介	351
9.7.2 BioAPI 的应用程序接口	351
9.8 小结	356
本章参考文献	356
第 10 章 生物特征识别系统安全性研究	358
10.1 引言	358
10.2 生物特征识别系统的安全性分析	358
10.2.1 传统生物特征识别系统存在的缺陷	358
10.2.2 对生物特征识别系统的攻击	359
10.3 活体指纹检测	360
10.3.1 基于薄板样条模型的活体指纹检测方法	361
10.3.2 算法的具体步骤	363
10.4 生物特征模板的保护	368
10.4.1 生物特征加密概述	368
10.4.2 与密钥相关的方法	368
10.4.3 可以撤销的生物特征	375
10.4.4 加密域指纹配准算法	379
10.4.5 实验分析	382
10.5 小结	384
本章参考文献	385
第 11 章 指纹模糊密钥绑定算法设计与实现	387
11.1 引言	387
11.2 模糊密钥绑定算法	387
11.2.1 加密流程	387
11.2.2 配准流程	388
11.2.3 解密流程	389
11.3 细节点过滤算法	390
11.3.1 指纹图像局部质量判断	391
11.3.2 局部脊线结构构造	392
11.4 基于 SHA-1 安全散列算法的多项式重构	393
11.5 配准结构特征提取	394
11.6 加密域内配准	397
11.7 算法平台设计与实现	400
11.7.1 指纹模板加密保护平台	400
11.7.2 算法安全性分析	406
本章参考文献	406
第 12 章 基于指纹加密的网络身份认证方案及其典型应用系统	408
12.1 引言	408

12.2	现有网络信息安全技术的问题与不足	409
12.2.1	PKI 存在的问题	409
12.2.2	IBE 的优点与不足	409
12.2.3	FIBE 的特点和能解决的问题	410
12.3	方案设计	412
12.3.1	TA 系统参数设置	413
12.3.2	用户注册	413
12.3.3	安全通信	414
12.3.4	TA 提供的其他服务	415
12.4	密钥管理方案	416
12.5	核心算法	417
12.5.1	签名算法 Sig 及验证算法 Ver	417
12.5.2	指纹摘要匹配算法	418
12.5.3	算法安全性分析	419
12.5.4	算法实验结果	419
12.6	方案安全性分析	420
12.7	典型应用系统：基于指纹认证的安全邮件系统	421
12.7.1	系统协议分析	421
12.7.2	系统设计与实现	422
12.7.3	系统使用操作	425
12.7.4	FingerMail 指纹安全电子邮件系统	426
12.8	小结	429
	本章参考文献	429
第 13 章	生物特征识别系统的典型应用	430
13.1	引言	430
13.2	生物特征识别技术在电子政务领域的应用	430
13.2.1	生物特征识别技术在公安刑侦领域的应用	431
13.2.2	基于指纹身份认证的异地网络授权管理系统	437
13.2.3	生物特征识别技术在通关系统中的应用	443
13.3	生物特征识别技术在电子商务领域的应用	448
13.3.1	基于指纹加密技术的电子商务新模式简介	448
13.3.2	方案 1 简介	450
13.3.3	方案 2 简介	451
13.4	生物特征识别技术在个人信息安全领域的应用	453
13.4.1	指纹计算机登录系统	453
13.4.2	指纹认证技术与 TPM 技术的结合	457
13.4.3	指纹文件加密系统	461
13.4.4	指纹移动存储设备	463
13.5	小结	465
	本章参考文献	465

附录 A 有关生物特征识别技术的问答·····	466
附录 B 生物特征识别数据库资源·····	470
附录 C 生物特征识别平台资源·····	472
附录 D 国外从事生物特征识别研究的部分机构·····	473
附录 E 与生物特征识别技术研究有关的网站、学术期刊和会议·····	474
全书参考文献·····	475

生物特征识别基础知识

1.1 引言

生物特征识别技术就是为了进行身份验证而采用自动技术测量生物身体的特征或是个人的行为特点,并将这些特征或特点与数据库的模板数据进行比较,完成认证的一种解决方案。人的生物特征是唯一的,生物特征识别技术的基本工作就是对这些基本的、可测量或可自动识别和验证的生理特征进行统计分析。所有的工作大多进行了这样4个步骤:图像获取、抽取特征、比较和匹配。生物特征识别系统捕捉到生物特征的样品,唯一的特征将会被提取并且被转化成数字的符号,接着,这些符号被存成个人的特征模板,这种模板可能会在识别系统中,也可能在各种各样的存储器中,如计算机的数据库、智能卡或条码卡中,人们同识别系统进行交互,认证其身份,以确定匹配或不匹配。

Bill Gates 曾做过这样的断言:“生物特征识别技术,利用人的生理特征,例如指纹等来识别个人的身份,将成为今后几年 IT 产业的重要革新”。Gates 的这段言论是因为有越来越多的消费者、公司和政府机关都承认,现有的基于智能卡、身份证或密码的身份识别系统是远远不够的。生物特征识别技术为此提供了一种解决方案。生物特征识别技术是目前最为方便与安全的识别系统,无须记住身份证号码或密码,也不需要随身携带像智能卡之类的东西。“钥匙”就是你自己,没有什么能比这更安全和更方便的了。

生物特征识别技术逐渐成为一种公认的身份认证技术。从最基本的到最健壮的,存在着多种不同级别的安全技术,生物特征识别技术将是最安全的。采用“您本身所具有的”(例如指纹、虹膜、声音等)方式验证身份远比采用“您所拥有的”(例如带照片的身份证件)和“您所知道的”东西(例如用户名和密码)方式验证身份更可靠、更安全。专家们一致认为生物特征身份确认技术将彻底改变人们现有的生活方式和商业模式。

1.2 通用概念和术语

生物特征识别系统(Biometric Identification System),是基于对行为或者生理(解剖学和生理学)特征的观察,对人类活体进行自动身份识别的系统。生物特征识别系统是一种自动系统,能够获取生物特征采集仪从用户处采集到的信息,并从处理后的数据中提取特征信息,然后将处理后的特征信息与已获取的一个或多个生物特征模板进行比对,决定它们之间匹配的程度,并描述一个辨识或识别过程是否成功,其运行流程如图 1-1 所示。