

## 生物特征识别技术综述

郑方<sup>1\*</sup>, 艾斯卡尔·肉孜<sup>1</sup>, 王仁宇<sup>2</sup>, 李蓝天<sup>1</sup>

<sup>1</sup> 清华信息科学技术国家实验室技术创新和开发部语音和语言技术中心

清华大学信息技术研究院语音和语言技术中心

清华大学计算机科学与技术系 北京 100084

<sup>2</sup> 江苏师范大学语言科学院 江苏徐州 221000

\*通讯作者: 郑方, 教授, E-mail: fzheng@tsinghua.edu.cn

**摘要:** 基于生物特征识别技术的身份认证是社会高度信息化和经济全球化的需求, 是政府和商业领域必不可少的重要技术。为此, 文章介绍了生物特征识别技术的基本原理、性能指标、关键技术、研究现状和技术应用等。文章全面调研了指纹、掌纹、虹膜、人脸、指静脉、声纹等不同的生物特征识别技术的研究现状, 比较了各种生物特征识别技术在错误率、稳定性、实用性、处理速度和仿冒程度等方面的差异。此外, 针对辨认和确认两种场景分别介绍了它们在各方面的应用情况, 分析讨论了生物特征融合技术、生物特征安全性问题, 介绍了该领域现有的行业和国家标准。最后文章对生物特征识别技术的发展前景给予展望。

**关键词:** 生物特征识别; 身份认证; 指纹; 声纹; 人脸; 掌纹; 虹膜; 指静脉

中图法分类号: TP391.4

## Overview of Biometric Recognition Technology

Thomas Fang Zheng<sup>1\*</sup>, Askar Rozi<sup>1</sup>, Wang Renyu<sup>2</sup>, Li Lantian<sup>1</sup>

<sup>1</sup> Center for Speech and Language Technologies, Division of Technical Innovation and Development, Tsinghua National Laboratory for Information Science and Technology; Center for Speech and Language Technologies, Research Institute of Information Technology; Department of Computer Science and Technology, Tsinghua University, Beijing, 100084

<sup>2</sup> School of Linguistic Sciences, Jiangsu Normal University, Xuzhou, 221116, China

\* Corresponding Author: Thomas Fang Zheng <fzheng@tsinghua.edu.cn>

**Abstract:** The biometric recognition based identity authentication is the demand with the development of information and economic globalization, and also one of the important technologies in governmental and commercial fields. In this paper, the fundamental principles, performance evaluation, key technologies, research status and application of biometric recognition are introduced. Through the overview of the research on different biometric recognition technologies of fingerprint, palmprint, iris, face, finger-vein, and voiceprint, we compare them in term of error rate, stability, usability, processing speed, and anti-spoofing. Then their applications in various aspects for both identification and verification scenarios are illustrated; the fusion technology and security problem are discussed; and the industrial and national standardization is introduced. Finally, the prospects of biometric recognition technologies are discussed additionally.

**Key words:** Biometric Recognition, Identity Authentication, Fingerprint, Voiceprint, Face, Palmprint, Iris, Finger-vein

## 0.引言

身份认证自古有之，其很大程度上关系到社会的安全问题。传统的身份认证大致可以分为两类：一是通过实物鉴别身份，例如身份证、护照、钥匙、智能卡等；二是通过约定相关口令鉴别身份，如口令、密码、暗号等。这些方式存在容易丢失、遗忘、被复制和破解等安全可靠性的问题。在实践中人们发现，每个人所特有的生物特征具有唯一且在一定时间内较为稳定不变的特性，并且其不会丢失也不会轻易被伪造和假冒，所以生物特征识别技术在身份认证中这种独特的优势使其被认为是一种终极的身份认证技术。

通常，人们会根据人的个体特征来直观地辨别人与人之间的差别。生物特征是指人体所固有的生理特征或行为特征。生理特征有指纹、人脸、虹膜等；行为特征有声纹、步态、签名、按键力度等。生理特征相对于行为特征较为可靠，但易被复制；尽管行为特征具有可变性但由于具有交互性因而不易被复制。生物特征识别技术就是以生物特征为依据，实现身份认证的技术。

生物特征识别技术在国家安全、公安、司法、金融等领域都有着广泛的应用。在出入境管理中，使用生物特征识别技术的电子护照既实现了快速通关又使安全性大大加强。在公安刑侦中，在犯罪现场采集到的犯罪嫌疑人所遗留的指纹、毛发等生物特征可以辅助公安人员确定犯罪嫌疑人身份，并成为指控其罪行的间接证据。在金融领域，基于声纹和人脸识别等技术的远程支付已经在电子商务中逐步使用。此外，使用指纹和人脸的考勤系统也已经商用化。

在信息高速发展和经济全球化的今天，人们对信息安全有更高的要求。基于生物特征的身份认证技术和传统的密码、证件等认证方式相比，具有难以盗取、伪造等特点，虽然它不是一项新技术，但是随着技术的发展，近几年来发展极为迅猛，已经成为发达国家高度重视并大力发展的关键技术和产业。

本文给出常用生物特征识别的原理、特点、研究现状和应用。本文组织结构如下：第一部分从当前身份认证方式所存在的问题引出生物特征识别技术用作身份认证的优势；第二部分对生物特征识别技术的基本原理、系统框架以及性能评价做简要介绍；第三部分分别详细介绍指纹、掌纹、人脸、虹膜、指静脉、声纹、签名等常用的生物特征识别技术的研究现状；第四部分根据不同生物特征的特点，着重分析比较了它们在研究和应用中的优缺点；第五部分介绍了当前生物特征识别技术的应用场景；第六部分分析和探讨了该技术存在的一些问题和未来的发展方向；最后一部分对全文进行总结。

### 1.生物特征识别基本原理

从本质上来说，生物特征识别技术是一个使用某人所具有的，可以表现其自身的生理或行为特征对其进行识别的模式识别技术<sup>[1]</sup>。该技术通常分为注册和识别两个阶段。注册过程首先通过传感器采集人体生物特征的表征信息，然后进行预处理去除噪声影响，利用特征提取技术抽取特征数据训练得到模板或模型，并存储起来。识别是身份鉴别的过程，前端特征提取都与注册过程相似，特征抽取完毕后利用特征信息与存储的模板 / 模型进行比对匹配，最终确定待识别者的身份。

生物特征识别技术可以分为辨认和确认两种。简单来说，辨认是解决把待识别的人判定为其所属于若干个参考者中的哪一个，是一个“多选一”的选择问题。而确认是解决待识别者是否是所声称的参考者，识别结果只有两种：是或否，是一个“一对一”的判决问题<sup>[2]</sup>，两者流程如图 1 所示。

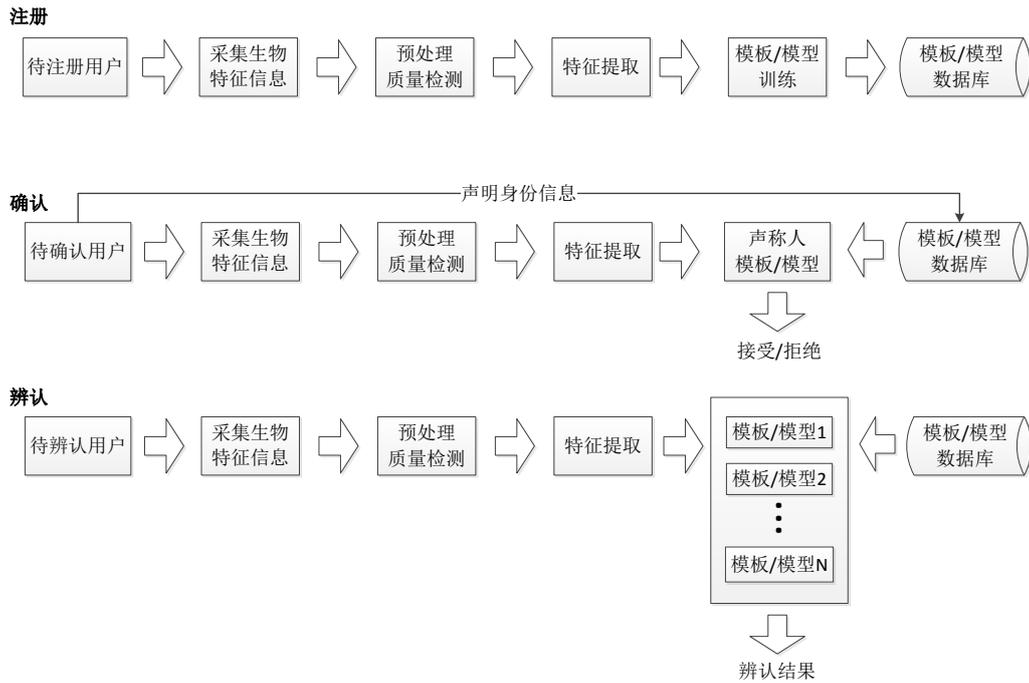


图 1 生物特征识别基本流程框图

通常，生物特征识别系统可以分为四个模块进行设计，传感器模块、特征提取模块、模板 / 模型数据集模块、模板 / 模型匹配模块<sup>[3]</sup>。传感器模块是生物特征信号的采集器，抽取个人的生物特征信号，是模数转换（ADC）过程，例如指纹传感器就属于传感器模块，用来获取用户的指纹图像。特征提取模块通常用来对采集的原始特征信号进行加工，获取具有个体辨识度的生物特征。模板 / 模型数据集模块用来存储生物特征识别系统的模板或模型，包括依据生物特征创建生物特征模板或模型以及它们的存储。模板 / 模型匹配模块依据提取的生物特征，对已存储的模板 / 模型进行比较，根据匹配得分评判结果。

衡量生物特征识别技术性能的两个重要指标是错误拒绝率（False Rejection Rate, 简称FRR）和错误接受率（False Accept Rate, 简称FAR）。FRR是指将来自真实人的测试样本误认作冒充者拒绝的比率，而FAR是指将来自冒充者的测试样本误认作真实人的比率。二者定义如下：

$$\text{错误拒绝率} = \frac{\text{被系统拒绝的真实人测试样本数}}{\text{总的真实人测试样本数}} \times 100\%$$

$$\text{错误接受率} = \frac{\text{被系统接受的冒充者测试样本数}}{\text{总的冒充者测试样本数}} \times 100\%$$

在生物特征识别系统中，这两种错误率很难都为零；在实际运用情况下，这两种指标是相关的，当FRR降低时，FAR就会升高，安全性就会降低；当FAR降低时，FRR就会升高，用户使用体验就会降低。两种错误率是个跷跷板，实际应用时常常在这两种情况下取一个折衷。用DET（Detection Error Trade-offs Curve）曲线能够较好的反映这两类错误率之间的关系：对一个特定的生物特征识别系统，以FAR为横坐标轴，以FRR为纵坐标轴，通过调整其参数得到的FAR与FRR之间关系的曲线图，就是DET曲线（参见图2）。显然DET曲线离原点越近，系统性能越好。在当前的技术不能使得两类错误率同时降为最低的情况下，我们根据具体应用的需要，调节阈值使得两类错误率可以满足实际应用需求。通常，研究者常用等错误率（Equal Error Rate, 简称EER）来描述总体性能，等错误率就是在DET曲线上两类错

误率相等时所对应的错误率取值，是衡量系统性能的重要参数。DET曲线与EER的取值如图2所例示。

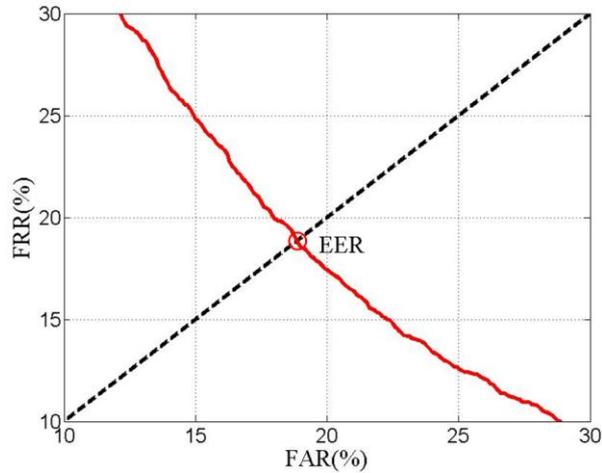


图2 DET 曲线与 EER 取值

## 2.研究现状

本部分介绍常见的几种生物特征识别技术的研究现状。

### 2.1 指纹

指纹作为一种生物特征用于认证已经由来已久。早在公元前 7000 年到公元前 6000 年，指纹就作为身份鉴定的工具在古代中国和古叙利亚使用。1880 年，亨利方德首先对指纹作为人体生物特征的唯一性做出了科学性的阐述，奠定了现代指纹识别技术的基石<sup>[4]</sup>。

最初的指纹识别是采用人工的方式。手工获取指纹的按印并整理存放于指纹库中，需要认证的时候再人工从指纹库中查找比对。上个世纪 60 年代之后，人们开始运用扫描设备将指纹转化成数字图像存储，并逐步使用数字图像处理，模式识别，人工智能等技术开发自动指纹识别系统（AFIS, Automated Fingerprint Identification System）<sup>[5]</sup>。1974 年，Osterburg 通过论证，证明了两枚指纹出现 12 处相同的特征却不属于同一个人的概率只有大约十亿分之一，这对之后使用计算机代替人工进行指纹自动识别和匹配的一系列研究提供了理论依据。

指纹识别技术是对人工指纹识别整个过程的模拟，因此 AFIS 也是一类模式识别系统，它由三部分组成，数据采集、数据处理、分类决策，其分别对应指纹采集、指纹预处理及特征提取、指纹匹配三个步骤。

指纹的采集通常使用各种物理传感器采集，其中光学传感器利用光的全反射原理来采集指纹图像，其采集图像成像好、造价低，是目前普遍使用的指纹采集传感器。由于指纹采集设备的局限性，指纹图像会产生畸变。另外柔性的手指表面由于按压用力不均，也会产生指纹扭曲，通常需要使用数学模型进行矫正。

指纹特征的提取是指纹识别的重要部分。指纹特征主要包括指纹的全局特征和局部特征。全局特征包括核心点和三角点，根据这些点的数量和位置关系可以对指纹进行初步分类。检测核心点和三角点最著名的方法是基于 Poineare 指数的方法。指纹的局部特征包括指纹脊线的端点和分叉点。端点位于指纹脊线的尾端，分叉点通常位于三条脊线的交叉部位。指纹特征提取就是提取这些特征的位置、类型、方向等信息并存储成特征文件的过程。

指纹匹配是基于指纹模式分类特征集的模式识别过程。早期的工作大多使用指纹的结构特征进行识别。Moayer<sup>[6]</sup>将指纹特征点集的拓扑结构表示成一维字符串或二维树，然后使用句法匹配进行粗分类；Isenor 和 Herhcka<sup>[7]</sup>使用图法表示指纹特征点的结构，并使用图相似性进行指纹匹配。目前最常用的指纹匹配算法是基于指纹细节点特征的模式匹配，该类方

法将指纹之间的匹配转化成特征点集之间的相似性度量。其中基于预配准的全局细节匹配算法最为常用<sup>[8,9,10]</sup>。

在指纹识别领域，公认的细节点是最具分辨力和鲁棒性的指纹特征。指纹的特征很大程度上依赖于获取的指纹的质量。所以指纹质量评估是指纹识别领域需要重点解决的问题。另一方面，指纹存储数据量较大，进行指纹辨认时需要对所有指纹进行匹配打分，因此指纹数据的压缩也是现行研究中所要解决的难题。

## 2.2 掌纹

掌纹识别方法大致可以分为四类，基于纹理和掌线的方法、基于子空间的方法、基于统计的方法和基于编码的方法<sup>[11]</sup>。

基于纹理和掌线的方法把掌纹的纹理结构和掌线图像作为掌纹的基本特征，以此来对掌纹进行分类和识别。Zhang 和 Shu<sup>[12,13]</sup>等使用掌纹线的特征实现识别，该方法对图像噪声的要求不高，但因其计算量大，识别运算时间较慢。Wu 等人<sup>[14,15]</sup>提出使用四个不同的检测算子对图像四个方向上的特征进行采集，由于该方法只检测四个方向信息，只能对掌纹粗略分类，适用于小型的数据集。Liu 等<sup>[16]</sup>提出基于宽线检测算子的方法进行特征提取，该方法不仅提取纹线位置信息，同时包含纹线宽度信息，识别性能显著提升。Duta 等<sup>[17]</sup>在提取纹线的基础上，通过形态学的方法提取代表纹线的特征点，根据特征点做匹配识别。Wu<sup>[18]</sup>综合利用掌纹的统计量信息作为特征，对质量差的图像具有更高的鲁棒性。总之，这些方法在掌纹识别的早期研究中使用，大部分都是借鉴指纹识别领域的方法。

基于子空间的方法通常使用主成分分析法（Principle Component Analysis, PCA），线性判别分析法（Linear Discriminant Analysis, LDA）等，对特征信息进行降维，变换后的特征向量往往具有更好的区分性特征，使用低维空间的特征对掌纹进行表示和匹配。Lu 等<sup>[19]</sup>首先提出基于 PCA 降维的 EigenPalm 方法。由于 PCA 主要考虑掌纹特征的表示，没有充分使用类别信息，Wu 等<sup>[20,21]</sup>又提出在 PCA 基础上使用 LDA 降维的 FisherPalm 方法。但是，基于子空间的方法较少用到掌纹信息的先验知识，往往得到的结果并不是很理想。

基于统计的方法可以分为局部统计方法和全局统计方法，局部的统计方法通常先把掌纹图像分块，分别计算每个局部图像的统计学信息，然后组合成为整个掌纹的统计信息。基于全局的统计方法则直接计算掌纹图像的全局统计量作为掌纹的特征参数进行特征匹配。Li 等<sup>[22]</sup>率先使用傅里叶变换提取掌纹图像的频域信息作为特征。Zhang 等<sup>[23,24]</sup>利用小波变换计算统计学特征，根据特征对掌纹分类。总的来说，基于统计量的方法对噪声不敏感，特征占用空间较小，匹配速度快，在掌纹识别中具有较高的性能。

基于编码的方法首先用特定滤波器对掌纹图像进行滤波，并将滤波后的信息以二进制的方法进行编码表示。该方法首先由 Daugman 在虹膜识别研究中提出<sup>[25]</sup>，文献<sup>[26,27]</sup>直接将该方法用于掌纹识别，并取名为 PalmCode。Kong 等<sup>[28]</sup>提出使用 6 个方向的 Gabor 滤波器对掌纹图像滤波后再赋值最小的方向编码，称为竞争编码。Sun<sup>[29]</sup>提出一种不同的序数编码方式。最近 Jia<sup>[30]</sup>提出一种更具鲁棒性的依据掌纹线方向的编码方法（Robust line orientation code, RLOC），利用 Randon 变换提取掌纹线的特征。文献<sup>[31]</sup>提出一种称为二指方向共生向量的掌纹识别方法，使用多个方向的 Gabor 滤波器对原图像滤波，每个方向的滤波结果都包含了丰富的特征信息，实验结果优于竞争编码和 RLOC。相比前几种方法，基于编码的方法具有更高的识别性能，因此在掌纹识别领域最具竞争力。

## 2.3 人脸

人脸识别技术是一种基于人脸的面部特征进行身份识别的技术。在识别时，一般通过两个阶段；第一阶段首先通过检测技术检测图像或者视频中是否存在人脸，如果存在人脸则收集人脸大小和各个面部器官位置信息，这部分信息可以提供代表身份的特征；第二阶段将收集到的特征与现存的人脸数据库进行对比识别出人脸身份。

人脸识别技术根据人脸数据的获取方式分为在线人脸识别和离线人脸识别。人脸识别技术研究最早开始于 1960 年，当时的系统是以半自动方式进行人脸识别。该系统只是检查人脸不同位置特征的连贯性，如眼睛之间的距离和前额发际线等，但是对不同方向的人脸，该系统无法正确识别。70 年代全自动人脸识别系统面世，该系统提取了 16 个人脸参数进行人脸识别。80 年代早期，Mark Nixon<sup>[32]</sup>在以往研究基础上提出了将眼部间距（eye-spacing）作为主要特征的人脸识别方法。后来人们利用人工神经网络提出诸多方法。1986 年，L Sirovich<sup>[33]</sup>等人提出了基于本征脸的识别技术，这种识别技术采用主成分分析（principle component analysis, PCA）在低维空间上重新组织并表征人脸数据。该技术对各种新的人脸识别方法打下了基础，该方法至今对人脸识别技术有显著影响。

人脸识别技术方法主要有主成分分析（PCA）<sup>[34]</sup>、线性判别分析（Linear Discriminant Analysis, LDA）<sup>[35]</sup>、神经网络（Neural Networks, NN）<sup>[36]</sup>、自适应增强算法（Adaboost）<sup>[37]</sup>、支持向量机（Support Vector Machine, SVM）<sup>[38]</sup>、本征脸（Eigenface）方法<sup>[39]</sup>、FisherFace 方法<sup>[40]</sup>和 LBP（Local Binary Pattern）方法<sup>[41]</sup>等。

本征脸（Eigenface）方法的主要思想是寻找主成分或者本征向量，数据库中的每一张图片对本征向量都有贡献，这些本征向量用于表示本征脸（Eigenface），每一张人脸能够通过本征脸的线性组合表示，一张人脸可用最大特征值的本征脸辨认。

相对于本征脸（Eigenface）方法，FisherFace 方法的优点是使用类相关映射矩阵来克服光照现象导致的问题，它使用区分性分析寻找区分性特征来区分人脸。

Ahonen 等人提出基于 LBP 的人脸识别方法，该方法区分性能力高、简单性、高效，并且对光照效果具有鲁棒性。

## 2.4 虹膜

人的虹膜是在眼角膜和晶状体之间的一层环状区域，它拥有复杂的结构和细微的特征，从外观上看呈现不规则的褶皱、斑点、条纹。虹膜具有唯一性的特征，每两个人的虹膜特征没有完全一样的，就算是双胞胎也不会相同。另外虹膜还具有稳定性的特征，其在人一岁之后几乎不再变化。所以，虹膜识别成为一种较好的生物特征识别技术。

虹膜识别的理论框架是由 Daugman 于 1993 年提出的<sup>[25,42,43]</sup>，其主要包括虹膜图像的定位、虹膜图像的归一化处理、特征提取和识别部分，后来的研究大多是基于此理论框架发展而来。

虹膜定位是指在对采集完成的人眼图像中准确定位并提取虹膜的区域，保证编码和识别结果的正确性。较早的定位方法是 Daugman 提出的基于圆周灰度梯度累加和最大值检测的方法<sup>[25]</sup>。这种方法在早期的虹膜定位上最为精确，但其算法复杂度较高，后续的许多研究都是在此基础上提高运算效率而改进的。另一类方法是基于圆哈夫变换（Circular Hough Transform）的参数投票方法，该方法由 Wildes 最早提出<sup>[44]</sup>。

由于虹膜图像的采集受到采集器拍摄远近和视角偏移等原因，会使虹膜识别的性能降低。通常研究者使用虹膜归一化的方法，把采集的虹膜图像转换成方便编码的矩形区域。经过归一化处理后，虹膜的图像消除或降低了这些因素对识别的影响。Daugman 提出从直角坐标系到极坐标系的映射方法，该方法在该领域被广泛运用<sup>[25]</sup>。Wildes 使用公式转换的方法，让转换得到的图像与标准图像之间的差异最小来进行参数归一化<sup>[44]</sup>。最近一些研究采用非线性变换的方法来描述瞳孔的缩放，提出一系列非线性归一化方法<sup>[45,46]</sup>，这些方法通常把线性和非线性归一化进行融合，得到了较好的效果。

虹膜图像的特征提取是虹膜识别中的重要部分，它在很大程度上决定虹膜识别的准确性。Daugman 的特征提取方法是对归一化后的虹膜图像进行分区域的特征提取和编码<sup>[25]</sup>，根据图像特征设计滤波器，滤波结果用二进制码的形式描述特征与模板的相似度，该方法存储空间较小，可以进行大规模的模型匹配。一些研究者直接将图像与滤波器卷积后形成的特

征矢量用于虹膜的识别，这方面的研究有<sup>[47,48,49]</sup>。此外，一些研究融合多种特征，期望以此提高识别的准确率。Sun 提出级联分类器的概念<sup>[50,51]</sup>，分别提取二进制编码和全局特征，该方法在一定程度上优于单一特征的方法。近年来，由于稀疏表示在信号处理中的研究进展，基于稀疏表示的虹膜识别也被逐步提出<sup>[52]</sup>。

在虹膜的匹配方面，分类器的设计一般根据特征提取的方式进行。提取特征是二进制编码时，往往使用基于汉明距离（Hamming distance）的方法来区别分类。在特征矢量的情况下一般先使用主成分分析法（Principle Component Analysis, PCA）给数据降维，再对降维后的特征采用线性判别分析方法或者使用核函数对特征进行分类。

## 2.5 指静脉

人们在进行医疗研究时偶然发现人体静脉血管中的失氧血红蛋白对特定范围内的近红外光线有很好的吸收作用，并且指静脉的分布特征具有很好的唯一性<sup>[53]</sup>。由于血液中的失氧血红蛋白能够吸收近红外光线，所以手指静脉能在近红外光下成像<sup>[53]</sup>，而且指静脉属于人体内部特征，不会收到外界影响，具有稳定性，所以可以对成像图像进行采集，通过预处理后进行特征提取，然后进行身份识别。

在指静脉识别技术产品开发中，日立公司最先开始研究并成功将研究成果推广到市场，该公司指静脉识别产品有 ATM 指静脉识别终端、指静脉识别电脑终端和指静脉识别门禁等。富士通公司同样进行指静脉识别产品的研发。在指静脉学术研究中，Miura, N, A<sup>[54]</sup>等人提出了线性追踪方法，另外 Naoto MIURA<sup>[55]</sup>等人提出了曲率方法。

国内指静脉研究如今处于实验室研究阶段，代表性研究机构有清华大学、中国科学院自动化所、中国民航大学、吉林大学、哈尔滨工业大学和同济大学等，其中中国民航大学和中国科学院自动化所联手建立联合实验室着手研究指静脉识别技术。

## 2.6 声纹

声纹识别是指根据待识别语音的声纹特征识别该段语音所对应的说话人的过程。这个领域的研究最早始于 20 世纪 30 年代，当时研究者们主要通过观察人类对语音的实际反应，研究人耳听辨来识别说话人的可能。进入 20 世纪下半叶，随着生物信息和计算机信息技术的发展，通过计算机进行自动的声纹识别成为可能。1945 年，Bell 实验室的 L.G. Kesta 等人借助肉眼观察，成功实现了语谱图匹配，首次提出了“声纹”的概念；并于 1962 年首次提出采用此方法进行声纹识别的可行性。Bell 实验室的 S. Pruzanshy 提出了基于模板匹配和统计方差分析的说话人识别方法，该方法引起了声纹识别研究的高潮。

现代声纹识别技术通常可以分为前端处理和建模测试阶段。前端处理包括语音信号的预处理和语音信号的特征提取。在声纹识别系统的前端处理阶段中，语音信号通常看作短时平稳的序列，语音特征提取的第一步是语音信号的分帧处理，并利用窗函数来减少由截断处理导致的 Gibbs 效应；同时用预加重来提升高频信息，压缩语音的动态范围，然后对每帧语音信号进行频谱处理，得到各种不同的特征参数。常用的特征提取参数有线性预测倒谱系数（Linear Predictive Cepstrum Coefficient, LPCC）<sup>[56]</sup>、感知线性预测系数（perceptual linear predictive, PLP）<sup>[57]</sup>、梅尔倒谱系数（mel-frequency cepstrum coefficient, MFCC）<sup>[58]</sup>等。

在声纹测试之前，首先得对多个声纹信号经过特征提取后进行训练建模，形成一个表征各个人的多复合声纹模型库。而声纹测试的过程是将某段来自某个人的语音经过特征提取后与多复合声纹模型库中的声纹模型进行匹配，进而识别打分，这个阶段可以判断该段语音是来自于集内说话人还是集外说话人。如果是来自集内说话人则进行下一步的辨认或确认操作。对于声纹辨认来说，是一个“一对多”的比较过程，即所提取的特征参数要与多复合声纹模型库的每一个的参考模型进行比较，并把与它分数最接近的参考模型所对应的说话人作为某段语音的发出者；而对于声纹确认来说，则是将某段语音提取的特征参数与特定的说话人的参考模型相比较，如果得出的分数大于预先规定的阈值，则予以确认，否则予以拒绝。

在声纹识别中,不同模式的匹配方法的区别就在于说话人模型的表示以及模型匹配的方法。常用的识别方法可以分为模板匹配法、概率模型法、人工神经网络法等。其中概率模型法具有灵活性强,理论意义完整等特点,是目前声纹识别中使用的主流匹配方法。

概率模型法有分段的高斯模型、高斯混合模型和隐马尔可夫模型等,其中高斯混合模型和隐马尔可夫模型是声纹识别中两种最常使用的概率模型。高斯混合模型用多个高斯分布的线性组合近似多维矢量的连续概率分布,能较为有效的刻画说话人特性。采用高斯混合模型的说话人识别系统有很高的识别率。在文本无关的说话人识别领域,高斯混合模型已经成为占统治地位的主流方法。隐马尔可夫模型可以描述语音随时间变化的情况,在文本相关的说话人识别中能充分利用已知的文本信息,达到更高的识别率。

近几年来,研究者提出一系列以高斯混合模型和通用背景模型(Gaussian mixture models-universal background models, GMM-UBM)<sup>[59]</sup>为基础的声纹识别建模方法,使得声纹识别技术的性能显著提高。前几年美国国家标准技术局(American national institute of standards and technology, NIST)组织的评测中高斯混合模型超矢量支持向量机(Gaussian mixture model super vector-support vector machine, GSV-SVM)、联合因子分析(joint factor analysis, JFA)<sup>[60]</sup>、i-vector (identify vector)<sup>[61]</sup>等建模方法都以 GMM-UBM 系统为基础,其中使用 i-vector 建模的声纹识别技术性能最优,成为当前国内外研究的主流系统。此外,研究者针对说话人识别中存在的问题也有一些相关研究。基于 F-ratio 准则的频带区分性特征算法和基于性能驱动的频带弯折算法,可以弱化声纹特征信息随时间变化的因素<sup>[62,63]</sup>。另外在基于短语音的声纹识别中,研究者也提出一系列方法和相应对策<sup>[64,65,66,67]</sup>。

## 2.7 签名

签名识别技术是一种依据人的行为特征进行生物特征识别的技术,它是一种广泛应用的生物特征识别技术。签名识别技术根据签名数据的获取方式可以分为两种模式,离线模式(off-line)和在线模式(on-line)<sup>[68]</sup>。

离线签名识别又称静态签名识别,该模式通常使用扫描仪把纸上的签名转换成数字图像,之后再对其进行识别。1998年一种基于矢量量化的方法被用来构建签名识别系统<sup>[69]</sup>;2001年,Justino, Bortolozzi 和 Sabourin 把隐马尔可夫模型作为一种统计识别模型框架,运用到静态签名识别中<sup>[70]</sup>。Moreno 等人使用压缩神经网络的方法,自动训练出每个人的签名特征<sup>[71]</sup>。Sansone 和 Vento 提出了一种连续的三级专家系统进行签名识别<sup>[72]</sup>。

在线签名识别又称动态签名识别,这种模式下常使用手写板或者压力传感笔作为获取用户签名的工具,用户签名信息样本通常会被表示成随时间变化的信号,这些信号包含用户书写过程中的行为特征信息,如书写时的速度、加速度、压力、旋转角度等等。对于如何区分在线签名时签名者的个人信息存在许多方法,这些方法可以大致分为两类,基于特征的方法和基于函数的方法<sup>[73]</sup>。基于特征的方法从签名的轨迹中获取全局特征,并组成一个整体的特征矢量<sup>[74,75]</sup>。基于函数的方法通常把局部的特征信息表示成时间的函数,用来进行签名模式的识别<sup>[76,77,78,79]</sup>。通常,依据对特征的关注点不同,基于函数的方法可以分为局部方法和区域方法。局部方法中,一般使用动态时间弯折等方法直接对时间函数进行距离的匹配<sup>[80,81,82]</sup>。区域方法中,一般把时间函数转换成一个向量序列描述该区域的过程特征。基于隐马尔可夫模型的方法往往会比运用函数表示的方法取得更好的结果<sup>[83,84,85]</sup>。最新的研究表明,基于特征的方法在某些方面会比基于函数的方法取得更好的识别准确率。

## 2.8 其他

生物特征识别技术远不止上面提到的几种,越来越多的生物特征识别技术正在被提出来满足不同领域的市场需求,每种生物特征识别技术在其应用领域较其他的生物特征识别技术都有一定的优越性,因为没有一种生物特征识别技术可以满足所有现实安全的需求<sup>[86]</sup>。

步态识别因其隐蔽性,较其他生物特征识别技术具有一定的潜在优越性。步态识别技术

通常捕捉人体的外形和运动信息,进行处理后与存储的数据进行比较,完成身份识别的任务。步态识别广泛运用各种特征技术以达到其识别目的<sup>[87]</sup>,这些方法通过外形、关节运动信息、个体相似性等原理进行分类识别。

人类外耳的形状、耳垂、骨架结构、大小等特征往往是独一无二的,因此,耳形识别也是一种无接触式的生物特征识别技术。

随着计算机技术的普及,键盘的使用成为现代人需要掌握的一项技能,击键的动态特征可以通过键盘内置传感器捕捉,进行身份认证。这种技术通过检测用户敲击键盘时的速度、压力、敲打某个特定字符串的时间以及用户每次击键的时间等,在用户持续使用键盘的过程中,完成对其身份认证。

基因识别<sup>[88]</sup>利用DNA序列上的具有生物学特征的基因片段,综合生物学和计算机技术,完成特定人身份的识别认证。基因识别中,其识别设备成本极高,识别算法较为复杂,识别鉴定方法难以快速实现,现在只在较少的特定应用中使用。

### 3.生物特征识别技术比较

生物特征识别技术研究领域,每种生物特征识别技术都有其独自的特点。总的来说,基于生理特征的识别技术需要近端采集,基于生理特征的识别技术因其稳定性也往往比基于行为特征的识别技术更加安全可靠。但因其需要近端采集,往往在远程认证的情景下应用不便,而且还有易被仿造的风险,而行为特征不易被仿造。下面我们对上文提到的各类生物特征的优缺点分别进行比较。这些优缺点一方面决定了其应用方面的特殊性,同时也为今后的研究发展提出了新的要求。

指纹特征通常独一无二,特征数量较多,指纹识别的定位精度也可以做到很高。另一方面,目前的指纹读取器造价不高,扫描指纹的速度很快,应用极其方便。然而由于指纹采集数据时需要人为按捺,每次按捺的方位不完全一样,着力点的不同也会带来不同程度的形变,这些往往使得精度较高的指纹识别达不到原本要求;另一方面,因为指纹常常在犯罪记录中使用,这使得某些人害怕把指纹“记录在案”。

人脸识别的优势在于其自然性和不易被被测者觉察的特点。人类在很大程度上就是根据人脸来确认对方身份的。人脸具有结构的相似性,不同的个体结构都很相似,这个特点对于定位人脸是有利的,但对于人脸的区分是不利的;人脸的外形也很不稳定,表情的变化极易改变人脸的特征,在不同观察角度,人脸的图像差异也较大。此外,人脸识别还容易受到光照条件、人脸遮盖物等因素的影响。

虹膜识别因其特征稳定性,可能会是目前最可靠的生物特征识别技术。但虹膜图像获取设备需要昂贵的摄像头设备,设备的尺寸也很难小型化。在实际应用中,摄像头可能产生图像的畸变,在较暗的环境下获取的虹膜图像往往质量较差,不能完成识别任务。

声纹识别因其不涉及用户隐私问题,往往用户接受程度较高。另一方面声纹的获取可以说是最方便的,只需要一个麦克风或者电话和手机就可以采集用户声纹特征信息,完成身份认证。这也使得声纹识别技术可以方便的用来作为远程身份确认技术。声纹识别技术是基于人的声纹不变性的,然而同一个人的声音易于受到年龄、情绪、身体状况等的影响,导致识别性能降低。另一方面,不同的麦克风和信道对识别性能都有不同程度的影响。环境噪声和混合说话人情形也会对声纹识别带来较大的影响。

签名识别作为一种基于行为特征的识别技术也具有容易被大众接受的特点。但随着人的经验和习惯的改变,签名的方式也会随之改变。用于签名识别的电子签名板结构复杂,价格较为昂贵,其与笔记本上的触摸板有着很大的差异,所以很难作为互联网上的远程身份认证

技术。同时，目前的物理和材料技术也很难将电子签名板小型化。

表 1 对当前常用的几种生物特征识别技术的性能、易用程度、易仿冒程度等方面进行了比较<sup>[89]</sup>。

	错误接受率	错误拒绝率	容易实用性	处理速度/人	易仿冒程度	生物特征
指纹	很低	较低	好	≤1s	一般	生理特征
掌纹	低	5%	使用困难	5s-10s	一般	生理特征
虹膜	很低	约 10%	需要培训才能使用,手工操作对虹膜有困难	一起自动对准虹膜需要 3s-5s,手工操作需要 5s-25s	极难	生理特征
视网膜	未知	未知	不好	15s-30s	极难	生理特征
人脸	低	<0.2%	非常好	≤5s	一般	生理特征
声纹	低	低	可以	1s-3s	难	行为特征
签名	低	10%	一般	5s-10s	一般	行为特征

表 1 常用生物认证技术的比较

#### 4.生物特征识别技术应用

生物特征不易遗忘和丢失，攻击者也较难伪造，目前该技术已经开始投入实际使用，并展现出广阔的应用前景。本节从生物特征辨认和确认两方面对当前主要应用场景进行介绍。

##### 4.1 基于生物特征辨认的应用场景

在刑事侦查中，刑侦人员对犯罪现场遗留的生物特征进行采集，并通过对比匹配存储的生物特征信息辨认犯罪嫌疑人。例如，通过犯罪现场遗留的指纹确认犯罪嫌疑人的方法由来已久，利用声纹和 DNA 的辨认技术在现代侦查中更是起到了重要的作用。

基于生物特征的辨认技术还经常应用在家庭、重要部门和单位的自动化门禁系统中，由于这类系统需要完成开集辨认的任务，且对安全性往往要求很高，目前基于生物特征的门禁系统还要结合传统的密码、钥匙等手段。虹膜识别技术因其准确性较高，已经在部分门禁系统中得到应用。随着生物特征识别技术的发展，在不久的将来，仅使用生物特征识别技术的门禁系统将会得到进一步普及使用。

生物特征识别技术在自动化考勤中也已经广泛运用。对于大多数公司来说，自动考勤系统的安全性要求并不高，使用人脸和指纹识别技术的考勤系统已经商用化。此外，基于开集辨认的生物特征识别技术在家用汽车驾驶人员的身份认证等方面也开始逐步使用。

##### 4.2 基于生物特征确认的应用场景

在出入境管理中，生物特征识别技术主要以电子护照为依托，在其中存储护照持有者的生物特征信息。在持有者通关时读取系统存储的生物特征信息和现场采集的信息进行验证匹配，来确认其身份。目前美国、新加坡、欧盟、中国香港等多个国家和地区已经采用包含生物特征识别技术的电子护照来进行出入境管理，该技术的使用在提高国家安全水平的同时，使得快速、便捷的自动通关成为了现实。

随着电子支付的普及使用，客户身份的鉴别变得尤其重要。现存的密码认证等技术对不法分子来说已经有各种窃取和伪造的手段进行破解，如使用取款机诈骗的金融案件屡见不鲜。所以，结合使用生物特征识别技术的电子支付对其安全性会有很大的提升。比如，在客户取款时使用生物特征识别技术对操作者进行身份认证，可以很大程度上阻止盗取和冒领的不法现象。同时，在互联网金融快速发展的时代，电子商务支付主要采用用户名、USB-key、

短信确认等与密码相结合的认证方式，这些都存在着被盗用的安全隐患。使用生物特征识别技术可以将电子商务的安全性大大加强。北京得意音通技术有限公司将声纹识别技术与移动支付相结合，其声密保服务已经在建行手机银行推出使用；阿里巴巴旗下在线支付服务支付宝在未来将采用人脸识别代替传统的密码输入，这个新功能被形象的称为“微笑支付”。

目前，因计算机和手机等电子产品而造成用户资料泄露的新闻不断报道。这些设备的用户登录验证系统，也逐渐从单一的密码登录方式，开始附带生物特征识别硬件模块作为安全管理。苹果、三星等多家智能手机生产商已经陆续在其设备上添加指纹识别功能，这也逐渐成为未来的发展趋势。

生物特征识别技术还可以用在会议参加人员的记录管理、考场身份的鉴别等方面。可谓只要是传统身份识别需要的场景，生物特征识别技术都可以得到应用。根据各种生物特征的特点，结合不同领域的应用需求，该技术在未来的相关领域普及使用将成为必然。

## 5. 分析与探讨

### 5.1 生物特征融合技术

迄今为止，生物特征识别技术的发展日益多样化，但是没有发现任何一种可以完美应用于各个领域的生物特征识别技术，每一种技术都有其各自的特点和优势。然而在实际应用中，单一的生物特征识别技术使用时具有一定的局限性如传感器噪声、特征提取和模板 / 模型匹配的缺陷等问题，这些问题使得这项技术的实际推广应用困难重重，因此多模态生物特征识别技术逐渐成为新的研究热点。

生物特征融合技术结合人的多种生物特征进行综合识别，是一种数据融合技术，它充分利用每种生物特征提供的信息，使得最终识别结果准确可靠。

生物特征融合技术在生物特征识别的各个阶段都有运用<sup>[90,91]</sup>。传感器数据层的融合技术通过不同的传感器，从不同角度采集同一种生物特征的不同数据，对各个传感器采集的数据进行融合使用。在特征提取阶段，每种生物特征通常表示为一组特征矢量，这些特征矢量可以串行融合成一组新的更高维的特征矢量用来表示人的特征信息，这种融合技术是在生物特征融合技术中目前表现最优的方式之一。在打分匹配阶段，融合技术把基于各种生物特征的打分进行综合分析，得到具有综合性的匹配分数。在决策阶段，多生物特征融合采用投票的方式对每种生物特征的判别结论进行投票，得到更加可靠的判别结果。

### 5.2 生物特征安全问题不容忽视

尽管生物特征识别技术的应用逐渐广泛，开始慢慢地影响消费者的生活，一场生物特征识别的革命即将到来。然而，这项技术的广泛应用会给人类社会带来什么样的长期影响还不得而知。其中，生物特征识别技术实际暗藏泄密陷阱，其安全问题不容忽视。

生物特征识别技术与传统的身份认证技术有天壤之别。一方面，传统的认证技术是基于我们拥有的实物如钥匙等，或我们所知的一些内容如密码等，这些东西往往在泄露后可以重新配置和改变，而生物特征是属于个人自身的，这种认证特征几乎不可能重新设置，一旦泄露将无法更改。另一方面，多数生物特征是天然公开的，传统的验证密钥都具有隐蔽性，用户的防范意识也较高，而我们一般不太注意也不便主动隐蔽自己的生物特征。比如我们碰触的任何地方都会留下指纹印记，我们的脸部图像会被任意一台眼前的摄像头采集。从这方面来讲，生物特征只是每个人所独有的特征，而并不能作为秘密。目前，生物特征识别技术的提供商都会把搜集到的用户的生物特征存进数据库，如果用户在预留其特征的时候不加注意，很容易被一些非法的提供商获取，从而造成用户的巨大损失。此外，从国家战略安全的角度来看，其国民生物特征信息泄露后，如被别有用心的人加以分析处理，甚至将间接危及到国家安全和民族安全。

另一个重要的方面是各类生物特征识别系统的安全性能还有待提高，以下将依次分析各类系统现存的性能和安全问题。对于指纹或掌纹识别系统，一个人的指纹或掌纹可以有很多

方式获取并用于攻击识别系统。比如可以通过数码相机在几米距离拍照获得拇指或者掌纹图片。高质量指纹或掌纹信息可以通过由若干张拇指或掌纹图片获取。另外还可以通过智能手机触摸屏、大门把手、茶杯和桌面等物品轻易获取指纹或掌纹信息，获取后可打印到锡纸作为制作模仿指纹或掌纹的基础。人脸识别系统可以通过打印的人脸图像欺骗攻击。这类欺骗如今能够被多数系统识破。然而视频攻击不容易识破，可以通过高清晰度摄像机摄像或者从电视机、网络等途径获取高清晰度人脸视频。这些都对人脸识别系统带来了挑战。对于声纹识别系统，可以通过合成和录音生成目标说话人的语音并进行攻击。其中，合成语音最容易识破，而录音是目标说话人本人的真实语音，所以很难识破。目标说话人的语音可以通过微信等各种语音通讯软件被不法分子轻易获取，这对声纹识别系统是一种极大挑战。虹膜识别系统中，可以通过眼睛图片、视频信号、人造眼睛和虹膜晶状体等方式进行攻击。相对于以上几种身份认证系统，指静脉识别系统相对安全。不同于指纹、掌纹和人脸等特征，指静脉特征很难通过各种物体表面和网络环境中获取，需要近距离的红外线设备用来获取指静脉在红外线下下的成像图片，这一般是非常困难获取的。当然如果一旦得到指静脉成像图片，攻击识别系统还是有可能。

针对特定生物特征识别系统中的攻击，相关生物特征识别研究者正在研究攻击识别方法并取得了一定的成果。

### 5.3 完善相关行业及国家标准

生物特征识别技术的实现门槛较高，也没用一个通用的技术可以适合全部的应用场景。然而，为了商业利益，某些应用厂商大肆宣扬其技术可靠性，更有甚者滥用生物特征识别技术，这无疑会对技术的研究和市场应用产生极大的伤害。因此，行业和国家标准的制订和质量检测对产业的发展尤其关键。国际标准化组织（International Organization for Standardization, ISO）在生物特征识别技术方面提出了相关的标准（JTC 1/SC 37）。美国国家标准化技术研究所（National institute of standards and technology, NIST）也对生物特征识别的相关术语及其产业技术制订了标准规范。

在我国，全国安全防范报警系统标准化委员会人体生物特征识别技术应用分技术委员会（SAC/TC100/SC2）于2007年9月成立，其以维护社会公共安全为目的，建立了一系列社会公共安全领域人体生物特征应用的标准体系。由清华大学、中国科学院自动化研究所、中国科学院计算技术研究所等机构单位共同起草的《安防生物特征识别应用术语》（GA/T 893-2010）标准于2010年12月1日起实施，该标准规范化了生物特征识别技术通用术语，其颁布实施给生物特征识别技术的研究带来了方便，同时也避免了研究人员因滥用自定义术语而对技术研究造成不良影响。此后，该组织又陆续发出特定生物特征识别应用的相关标准。2011年颁布人脸识别应用系统相关国家标准（GA/T922.2-2011），2014年9月19日，《安防声纹确认应用算法技术要求和测试方法》（GA/T1179-2014）审核通过批准颁布。

全国信息标准化委员会生物特征识别分技术委员会（SAC/TC28/SC37）和全国金融标准化技术委员会（SAC/TC180）也设有相关标准。这些标准对整个行业的发展将产生积极的推动作用。

然而，目前这些标准对于生物特征识别行业的发展是远远不够的，更多的、更精细的标准有待被制订，以满足生物特征识别技术的提升和产业的发展。

## 6. 总结与展望

本文重点地对人脸、声纹、指纹、掌纹、虹膜、指静脉和签名等7种生物特征识别技术目前的研究和应用现状进行了综述，并对这些生物特征识别技术在识别特点和安全等方面进行了对比与探讨。最后本文还对制订和完善生物特征行业及国家标准提出了期望。

身份识别技术对政府部门和商业领域是一项必不可少的重要技术，生物特征识别技术有传统的基于证件和密钥认证技术所无可比拟的优越性。然而单一的生物特征识别系统在实际应用

领域往往不够可靠,鲁棒的生物特征融合的认可系统是未来的研究方向。这项技术的成熟将会带来经济和社会的巨大变革。尽管现在想要预测未来生物特征识别技术最完善的应用方式还为之过早,但毫无疑问,这项技术的应用普及将会对我们未来的经济与社会生活带来深远的影响。

#### 参考文献

- [1] Prabhakar S, Pankanti S, Jain A K. Biometric recognition: Security and privacy concerns [J]. *IEEE Security & Privacy*, 2003 (2): 33-42
- [2] Jain A K, Flynn P, Ross A A. *Handbook of biometrics* [M]. Springer Science & Business Media, 2007
- [3] Jain A K, Ross A, Prabhakar S. An introduction to biometric recognition [J]. *IEEE Transactions on Circuits and Systems for Video Technology*, 2004, 14(1): 4-20
- [4] 张圆圆. 指纹识别技术相关算法的研究[D]. 北京: 北京邮电大学, 2012
- [5] Maltoni D, Maio D, Jain A K, et al. *Handbook of fingerprint recognition* [M]. Springer Science & Business Media, 2009
- [6] Moayer B, Fu K S. A tree system approach for fingerprint pattern recognition [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1986 (3): 376-387
- [7] Hrechak A K, McHugh J A. Automated fingerprint recognition using structural matching [J]. *Pattern Recognition*, 1990, 23(8): 893-904
- [8] Jain A, Hong L, Bolle R. On-line fingerprint verification [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1997, 19(4): 302-314
- [9] Jain A K, Hong L, Pankanti S, et al. An identity-authentication system using fingerprints [J]. *Proceedings of the IEEE*, 1997, 85(9): 1365-1388
- [10] Tico M, Kuosmanen P. Fingerprint matching using an orientation-based minutia descriptor [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2003, 25(8): 1009-1014
- [11] Kong A, Zhang D, Kamel M. A survey of palmprint recognition [J]. *Pattern Recognition*, 2009, 42(7): 1408-1418
- [12] Zhang D, Shu W. Two novel characteristics in palmprint verification: datum point invariance and line feature matching [J]. *Pattern Recognition*, 1999, 32(4): 691-702
- [13] Shu W, Zhang D. Palmprint verification: an implementation of biometric technology[C]. *Fourteenth International Conference on Pattern Recognition*, 1998, 1: 219-221
- [14] Wu X, Wang K, Zhang D. A novel approach of palm-line extraction [C]. *The Third International Conference on Image and Graphics (ICIG)*, 2004: 230-233
- [15] Wu X, Zhang D, Wang K. Palm line extraction and matching for personal authentication [J]. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 2006, 36(5): 978-987
- [16] Liu L, Zhang D. Palm-line detection [C]. *IEEE International Conference on Image Processing (ICIP)*. 2005, 3: III269-III272
- [17] Duta N, Jain A K, Mardia K V. Matching of palmprints [J]. *Pattern Recognition Letters*, 2002, 23(4): 477-485
- [18] Wu X, Wang K, Zhang D. An approach to line feature representation and matching for palmprint recognition [J]. *Journal of Software*, 2004, 15(6): 869-880
- [19] Lu G, Zhang D, Wang K. Palmprint recognition using eigenpalms features [J]. *Pattern Recognition Letters*, 2003, 24(9): 1463-1467
- [20] Wu X, Wang K Q, Zhang D. Palmprint recognition using Fisher's linear discriminant [C]. *International Conference on Machine Learning and Cybernetics*, 2003, 5: 3150-3154
- [21] Wu X, Zhang D, Wang K. Fisherpalms based palmprint recognition [J]. *Pattern recognition letters*, 2003, 24(15): 2829-2838
- [22] Li W, Zhang D, Xu Z. Palmprint identification by Fourier transform [J]. *International Journal of Pattern Recognition and Artificial Intelligence*, 2002, 16(04): 417-432
- [23] Li W, Zhang D, Xu Z. Palmprint identification by Fourier transform [J]. *International Journal of Pattern Recognition and Artificial Intelligence*, 2002, 16(04): 417-432

- [24] Zhang L, Zhang L. Characterization of palmprints by wavelet signatures via directional context modeling [J]. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 2004, 34(3): 1335-1347
- [25] Daugman J G. High confidence visual recognition of persons by a test of statistical independence [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1993, 15(11): 1148-1161
- [26] Zhang D, Kong W K, You J, et al. Online palmprint identification [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2003, 25(9): 1041-1050
- [27] Kong W K, Zhang D. Palmprint texture analysis based on low-resolution images for personal authentication [C]. *The 16th International Conference on Pattern Recognition*, 2002, 3: 807-810
- [28] Kong A W K, Zhang D. Competitive coding scheme for palmprint verification [C]. *The 17th International Conference on Pattern Recognition*, 2004, 1: 520-523
- [29] Sun Z, Tan T, Wang Y, et al. Ordinal palmprint representation for personal identification [representation read representation][C]. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2005, 1: 279-284
- [30] Jia W, Huang D S, Zhang D. Palmprint verification based on robust line orientation code [J]. *Pattern Recognition*, 2008, 41(5): 1504-1513
- [31] Guo Z, Zhang D, Zhang L, et al. Palmprint verification using binary orientation co-occurrence vector [J]. *Pattern Recognition Letters*, 2009, 30(13): 1219-1227
- [32] Nixon, Mark. *Feature extraction & image processing* [M]. Academic Press, 2008
- [33] Everson R, Sirovich L. Karhunen–Loeve procedure for gappy data [J]. *JOSA A*, 1995, 12(8): 1657-1664
- [34] Kirby M, Sirovich L. Application of the Karhunen-Loeve procedure for the characterization of human faces [J]. *Transactions on Pattern Analysis and Machine Intelligence*, 1990, 12(1): 103-108
- [35] He X, Yan S, Hu Y, et al. Face recognition using Laplacian faces [J]. *Transactions on Pattern Analysis and Machine Intelligence*, 2005, 27(3): 328-340
- [36] Rowley H, Baluja S, Kanade T. Rotation invariant neural network-based face detection [C]. *Computer Society Conference on Computer Vision and Pattern Recognition*, 1998: 38-44
- [37] Viola, Paul, and Michael Jones. Rapid object detection using a boosted cascade of simple features [C]. *Computer Society Conference on Computer Vision and Pattern Recognition*. Vol. 1. IEEE, 2001
- [38] Osuna E, Girosi F. Reducing the run-time complexity of support vector machines [C]. *International Conference on Pattern Recognition*. 1998
- [39] Turk M, Pentland A. Eigenfaces for recognition [J]. *Journal of cognitive neuroscience*, 1991, 3(1): 71-86
- [40] Belhumeur P N, Hespanha J P, Kriegman D J. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1997, 19(7): 711-720
- [41] Ritika Lohiya, Pooja Shah. *Face Recognition Techniques: A Survey for Forensic Applications* [J]. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 4 Issue 4, April 2015
- [42] Daugman J. The importance of being random: statistical principles of iris recognition [J]. *Pattern recognition*, 2003, 36(2): 279-291
- [43] Daugman J. Statistical richness of visual phase information: update on recognizing persons by iris patterns [J]. *International Journal of computer vision*, 2001, 45(1): 25-38
- [44] Wildes R P. Iris recognition: an emerging biometric technology [J]. *Proceedings of the IEEE*, 1997, 85(9): 1348-1363
- [45] Wei Z, Tan T, Sun Z. Nonlinear iris deformation correction based on Gaussian model [J]. *Advances in Biometrics*, 2007: 780-789
- [46] Yuan X, Shi P. A non-linear normalization model for iris recognition [M]. *Advances in Biometric Person Authentication*. Springer Berlin Heidelberg, 2005: 135-141
- [47] Boles W W, Boashash B. A human identification technique using images of the iris and wavelet transform [J]. *IEEE transactions on signal processing*, 1998, 46(4): 1185-1188
- [48] Gan J, Liang Y. Applications of wavelet packets decomposition in iris recognition [M]. *Advances in Biometrics*. Springer Berlin

- Heidelberg, 2005: 443-449
- [49] Jang J, Park K R, Son J, et al. A study on multi-unit iris recognition [C]. Conference on Control, Automation, Robotics and Vision, 2004, 2: 1244-1249
- [50] Sun Z, Wang Y, Tan T, et al. Improving iris recognition accuracy via cascaded classifiers [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 2005, 35(3): 435-441
- [51] Sun Z, Tan T, Qiu X. Graph matching iris image blocks with local binary pattern [M]. Advances in Biometrics. Springer Berlin Heidelberg, 2005: 366-372
- [52] Pillai J K, Patel V M, Chellappa R, et al. Secure and robust iris recognition using random projections and sparse representations [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 33(9): 1877-1893
- [53] 孙晓琳, 指静脉图像模式提取算法研究 [M], 吉林大学, 2012
- [54] Miura, N, A. Nagasaka, T. Miyatake. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification [J]. Machine Vision and Applications, 2004, 15(4): 194-203
- [55] Naoto MIURA, Akio NAGASAKA, Takafumi MIYATAKE. Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles [J], The Institute of Electronics, Information and Communication Engineers, 2007, 90(8): 1185-1194
- [56] Atal B S. Automatic recognition of speakers from their voices [J]. Proceedings of the IEEE, 1976, 64(4): 460-475
- [57] Hermansky H. Perceptual linear predictive (PLP) analysis of speech [J]. the Journal of the Acoustical Society of America, 1990, 87(4): 1738-1752
- [58] Davis S B, Mermelstein P. Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences [J]. IEEE Transactions on Acoustics, Speech and Signal Processing, 1980, 28(4): 357-366
- [59] Reynolds D A, Quatieri T F, Dunn R B. Speaker verification using adapted Gaussian mixture models [J]. Digital Signal Processing, 2000, 10(1): 19-41
- [60] Yin S C, Rose R, Kenny P. A joint factor analysis approach to progressive model adaptation in text-independent speaker verification [J]. IEEE Transactions on Audio, Speech, and Language Processing, 2007, 15(7): 1999-2010
- [61] Dehak N, Kenny P, Dehak R, et al. Front-end factor analysis for speaker verification [J]. IEEE Transactions on Audio, Speech, and Language Processing, 2011, 19(4): 788-798
- [62] Wang L-L, Wu X-J, Zheng T F, et al. An investigation into better frequency warping for time-varying speaker recognition [C]Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2012), 2012: 1-4
- [63] Wang L-L, Zheng T F. Creation of time-varying voiceprint database [J]. Proc. of O-COCOSDA 2010
- [64] Kwon S, Narayanan S. Robust speaker identification based on selective use of feature vectors [J]. Pattern Recognition Letters, 2007, 28(1): 85-89
- [65] Zhang C-H, Zheng T F. A fisher voice based feature fusion method for short utterance speaker recognition [C]. IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP 2013), 2013: 165-169
- [66] Zhang C-H, Wu X-J, Zheng T F, et al. A K-phoneme-class based multi-model method for short utterance speaker recognition [C]. Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC 2012), 2012: 1-4
- [67] Malegaonkar A, Ariyaeeinia A, Sivakumaran P, et al. On the enhancement of speaker identification accuracy using weighted bilateral scoring [C]. 42nd Annual IEEE International Carnahan Conference on Security Technology, 2008: 254-258
- [68] Faundez-Zanuy M. Signature recognition state-of-the-art [J]. IEEE Aerospace and Electronic Systems Magazine, 2005, 20(7): 28-32
- [69] Zhang B, Fu M, Yan H. Handwritten signature verification based on neuralgas' based vector quantization [C]. Fourteenth International Conference on Pattern Recognition, 1998, 2: 1862-1864
- [70] Justino E J R, Bortolozzi F, Sabourin R. Off-line signature verification using HMM for random, simple and skilled forgeries [C]International Conference on Document Analysis and Recognition, 2001: 1031-1034
- [71] Velez J F, Sanchez A. Robust off-line signature verification using compression networks and positional cuttings [C]. IEEE 13th

- Workshop on Neural Networks for Signal Processing, 2003: 627-636
- [72] Sansone C, Vento M. Signature verification: increasing performance by a multi-stage system [J]. *Pattern Analysis & Applications*, 2000, 3(2): 169-181
- [73] Fierrez J, Ortega-Garcia J, Ramos D, et al. HMM-based on-line signature verification: Feature extraction and signature modeling [J]. *Pattern recognition letters*, 2007, 28(16): 2325-2334
- [74] Lee L L, Berger T, Aviczer E. Reliable online human signature verification systems [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1996, 18(6): 643-647
- [75] Ketabdar H, Richiardi J, Drygajlo A. Global feature selection for on-line signature verification [C]. *International Graphonomics Society Conference*, 2005
- [76] Nalwa V S. Automatic on-line signature verification [J]. *Proceedings of the IEEE*, 1997, 85(2): 215-239
- [77] Fairhurst M C. Signature verification revisited: promoting practical exploitation of biometric technology [J]. *Electronics & Communication Engineering Journal*, 1997, 9(6): 273-280
- [78] Jain A K, Griess F D, Connell S D. On-line signature verification [J]. *Pattern recognition*, 2002, 35(12): 2963-2972
- [79] Li B, Zhang D, Wang K. Online signature verification based on null component analysis and principal component analysis [J]. *Pattern analysis and applications*, 2006, 8(4): 345-356
- [80] Munich M E, Perona P. Visual identification by signature tracking [J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2003, 25(2): 200-217
- [81] Kholmatov A, Yanikoglu B. Identity authentication using improved online signature verification method [J]. *Pattern Recognition Letters*, 2005, 26(15): 2400-2408
- [82] Faundez-Zanuy M. On-line signature recognition based on VQ-DTW [J]. *Pattern Recognition*, 2007, 40(3): 981-992
- [83] Yang L, Widjaja B K, Prasad R. Application of hidden Markov models for signature verification [J]. *Pattern Recognition*, 1995, 28(2): 161-170
- [84] Kashi R S, Hu J, Nelson W L, et al. On-line handwritten signature verification using hidden Markov model features [C]. *The Fourth International Conference on Document Analysis and Recognition*, 1997, 1: 253-257
- [85] Dolfing J G A, Aarts E H L, Van Oosterhout J. On-line signature verification with Hidden Markov Models [C]. *Fourteenth International Conference on Pattern Recognition*, 1998, 2: 1309-1312
- [86] Goudelis G, Tefas A, Pitas I. Emerging biometric modalities: a survey [J]. *Journal on Multimodal User Interfaces*, 2008, 2(3-4): 217-235
- [87] Boyd J E, Little J J. *Biometric gait recognition* [M]. *Advanced Studies in Biometrics*. Springer Berlin Heidelberg, 2005: 19-42
- [88] Hiller M, Zhang Z, Backofen R, et al. pre-mRNA secondary structure and splice site selection [J]. *PLOS Genet*, 2007, 3: 2147-2155
- [89] Zheng T F. Prove yourself by yourself with the use of speaker recognition technology [R]. *National Conference on Man-Machine Speech Communication (NCMMSC 2015)*
- [90] Faundez-Zanuy M. Data fusion in biometrics [J]. *IEEE Aerospace and Electronic Systems Magazine*, 2005, 20(1): 34-38
- [91] Ross A, Jain A. Information fusion in biometrics [J]. *Pattern Recognition Letters*, 2003, 24(13): 2115-2125

## 基金资助

本项研究工作得到了国家自然科学基金(编号. 61271389/61371136)和国家重点基础研究发展计划(973计划, 编号. 2013CB329302)的支持。

## 作者信息

**郑方** 清华大学信息技术研究院语音和语言技术中心 主任、教授、博士生导师  
fzheng@tsinghua.edu.cn



**艾斯卡尔·肉孜** 清华大学信息技术研究院语音和语言技术中心 博士研究生  
askar@csit.tsinghua.edu.cn



**王仁宇** 江苏师范大学语言科学院 硕士研究生  
jsnuwangry@163.com



**李蓝天** 清华大学信息技术研究院语音和语言技术中心 博士研究生  
lilt@csit.tsinghua.edu.cn

