

第 2 章 物联网感知技术

2.1 常见自动识别技术

1. 自动识别技术的基本概念

1) 识别的基本概念

识别是人类参与社会活动的基本要求。人们认识和了解事物的特征及信息就是一种识别,为有差异的事物命名是一种识别,为便于管理而为一个单位的每个人或一个包装箱内的每件物品进行编号也是一种识别。因此,识别是一个集定义、过程与结果为一体的概念。

随着技术的进步和发展,人们所面临的识别问题越来越复杂,完成识别所花费的人力代价也越来越大,在某些情况下,必须借助一些设备和技术才能完成更高效、更快速和更准确的识别,这就用到了自动识别技术。

2) 自动识别技术的含义

自动识别(Automatic Identification, Auto-ID)技术是指通过非人工手段获取被识别对象所包含的标识信息或特征信息,并且不使用键盘即可实现数据实时输入计算机或其他微处理器控制设备的技术。

下面我们从几个不同的角度对其特征进行定义。

(1) 综合技术概念

自动识别技术是以传感器技术、计算机技术和通信技术为基础的一门综合性科学技术,是集数据编码、数据采集、数据标识、数据管理、数据传输于一体的信息数据自动识读、自动输入计算机的重要方法和手段,是一种高度自动化的信息或者数据采集与处理技术。

(2) 应用设备概念

自动识别技术是应用一定的识别装置,通过被识别物品和识别装置之间的接近活动,自动地获取被识别物品的相关信息,并提供给后台的计算机处理系统来完成相关后续处理的一种技术。例如,商场的条码扫描系统就是一种典型的自动识别技术,售货员通过条码阅读器扫描条码,获取商品的代码信息,然后将代码信息传送到后台来获取商品的名称、价格,在 POS 终端即可计算出该批次商品的价格,从而完成顾客所购买商品的结算。

(3) 技术系统概念

自动识别技术是一个以传感器技术、信息处理技术为主的技术系统,最主要的目的是提供一个快速、准确地获得信息的有效手段,其处理的结果可作为管理工作的决策信息或自动化装置等技术系统的控制信息。

(4) 自动采集概念

在信息处理系统早期,相当部分的数据处理都是通过人工录入的,这样的录入方法不仅数据量十分庞大、操作者的劳动强度高,而且人为产生错误的概率也相应较高,造成录入的数据不准确,使得对这些数据的分析失去了实时的意义。

为了解决这些问题,人们研究和开发了各种自动识别技术,将操作者从繁重而又重复、且十分不准确的手工输入劳动中解放出来,提高了系统输入信息的实时性和准确性,这就是自动

识别技术的目的。

(5) 多种技术概念

自动识别技术包括条码识别技术、射频识别技术、磁卡识别技术、IC 卡识别技术、图像识别技术、光学字符识别技术、生物特征识别技术(指纹识别、人脸识别、虹膜识别、语音识别)等多种自动识别技术方法和手段。

3) 自动识别技术的特点

自动识别技术具有如下共同的特点:

- ① 准确性——自动数据采集,彻底消除人为错误;
- ② 高效性——信息交换实时进行;
- ③ 兼容性——识别技术以计算机技术为基础,可与信息管理系统无缝连接。

2. 自动识别技术分类

自动识别技术根据识别对象的特征、识别原理和方式可以分为两大类,分别是数据采集技术(定义识别)和特征提取技术(模式识别)。这两大类自动识别技术的基本功能是一致的,都是完成物品的自动识别和数据的自动采集。

(1) 定义识别

定义识别是赋予被识别对象一个 ID 代码,并将此 ID 代码的载体(条码、射频标签、磁卡、IC 卡等)放在要被识别的对象上进行标识,通过对载体的自动识读获得原 ID 代码,然后通过计算机实现对对象的自动识别。

(2) 模式识别

模式识别是指对表征事物或现象的各种形式的(数值的、文字的和逻辑关系的)信息进行处理和分析,以对事物或现象进行描述、辨认、分类和解释的过程,即通过采集被识别对象的特征数据,并通过与计算机存储的原特征数据进行特征比对,实现对对象的自动识别。模式识别是信息科学与人工智能的重要组成部分。

数据采集技术的基本特征是需要被识别物体具有特定的识别特征载体(如标签等,仅光学字符识别例外);而特征提取技术(特征识别)则根据被识别物体本身的属性特征和行为特征来完成数据的自动采集。

3. 自动识别技术的一般性原理

自动识别系统是一个以信息处理为主的技术系统,它也是传感器技术、计算机技术、通信技术综合应用的一个系统,它的输入端是被识别信息,输出端是已识别信息。

自动识别系统中的信息处理是指为达到快速应用目的而对信息所进行的变换和加工,例如为抗干扰性进行的信道编码处理和为了提高传输效率而进行的信源编码处理,还有诸如调制、均衡等信息处理、信息操作的总称。自动识别技术广泛地应用于各种商务活动和各类行业管理的信息采集与数据交换领域。

抽象概括自动识别技术系统的工作过程如图 2-1 所示,它是最一般的自动识别技术信息处理系统的模型框图,是适用于自动识别技术领域的通用研究模型。如果具体到各类信息的采集和处理,此模型可以再具体化,不同类别的信息采集对应着不同的信息处理部分。

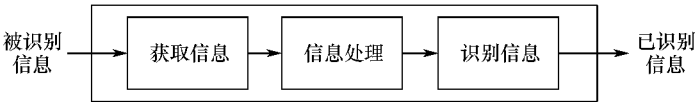


图 2-1 自动识别技术信息处理系统的模型框图

(1) 定义识别的数据信息的采集由于其信息格式的固定化,且具有量化特征,数据量相对较小,所对应的自动识别系统模型也较为简单,如图 2-2 所示。条码识别、射频识别、磁卡识别、IC 卡识别等自动识别技术即为这一类。

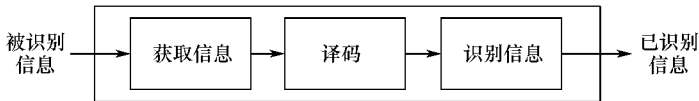


图 2-2 特定格式信息的自动识别系统的模型框图

(2) 特征识别的特征信息的采集和处理过程较定义识别的数据信息的采集来说要复杂得多。第一,它没有固定的信息格式;第二,为了让计算机能够处理这些信息,必须使其量化,而量化的结果往往会产生大量的数据;第三,还要对这些数据作大量的计算与特殊的处理。因此,其系统模型也较为复杂,如图 2-3 所示。图像识别、指纹识别、人脸识别、虹膜识别、语音识别等自动识别技术即为这一类。

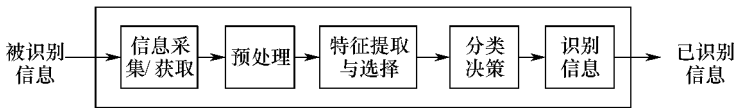


图 2-3 图像形式格式信息的自动识别系统模型

根据两种不同的输入格式信息建立的自动识别系统模型,主要的区别就在于“信息处理”部分,而“信息处理”部分的不同将造成系统构成的巨大差异。

(1) 对于定义识别,信息处理就是各种不同种类的译码。为了顺利地实现译码,需要事先有固定的编码规则,如各种码制规范;有载体,如条码标签、射频标签、磁条、IC 卡等,按编码规则制作相应的标签附于被识别物品上;有内置编码规则的译码器,按编码规则译码,识别效率非常高,误码率非常低。

(2) 对于特征识别,信息处理过程一般包括预处理、特征提取与选择、分类决策等几部分。
① 预处理操作是指对图像图形进行各种加工,即对获得的图像图形信息进行预处理以消除干扰、噪声,做几何、彩色校正等,以改善图像图形的质量,是从图像到图像的过程,强调图像之间进行的变换。有时还得对图像图形进行增强、分割、定位和分离、复原处理、压缩等。常见的图像图形预处理方法可分成两种:空间域的预处理方法和变换域的预处理方法。空间域的预处理方法有:灰度均衡化处理、尺寸的归一化处理、色彩空间的归一化处理等;变换域的预处理方法有:DCT 变换、DFT 变换、小波变换、滤波处理等。

② 特征提取与选择是指对处理后的图像图形进行分类和特征提取,并对某些特征参数进行测量、再提取、分类,有时还要对图像图形进行结构分析,对图像图形进行描述,它是以观察者为中心研究客观世界的一个过程。特征提取是一个从图像图形到数据的过程,常见的特征提取方法有基于代数特征的提取方法和基于几何特征的提取方法等。

③ 分类决策是指利用掌握的特征信息,对未知的训练样本按照某种判别准则进行分析,得出分类后的结果。常见的有两种分类识别方式:监督分类识别和非监督分类识别,例如距离分类器、神经网络分类器、支持向量机分类器、聚类分类器等。

2.1.1 条码自动识别技术

1. 条码的符号表示及结构

1) 条码的编码

条码是利用“条”和“空”构成二进制的“0”和“1”，并以它们的组合来表示某个数字或字符，反映某种信息的。但不同码制的条码在编码方式上有所不同，一般有以下两种不同的编码方式。

(1) 宽度调节编码法

宽度调节编码法，即条码符号中的条和空由宽、窄两种单元组成的条码编码方法。按照这种方式编码时，是以窄单元(条或空)表示逻辑值“0”，宽单元(条或空)表示逻辑值“1”，其中，宽单元通常是窄单元的 2~3 倍，如图 2-4 所示。

(2) 模块组配编码法

模块组配编码法，即条码符号的字符由规定的若干个模块组成的条码编码方法。按照这种方式编码，条与空是由模块组合而成的，一个模块宽度的“条”模块，表示二进制的“1”；而一个模块宽度的“空”模块，表示二进制的“0”，如图 2-5 所示。



图 2-4 宽度调节法条码符号结构

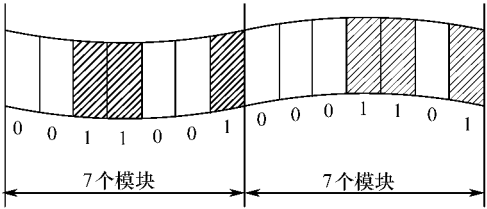


图 2-5 模块组配法条码符号结构

2) 条码的符号结构

条码符号通常由左右侧空白区、起始字符、数据字符、校验字符、终止字符等构成，具体结构如图 2-6 所示。

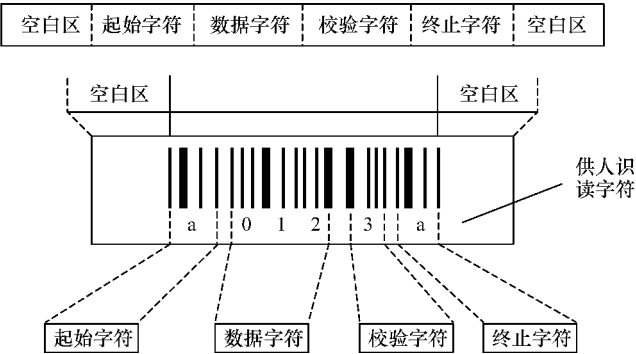


图 2-6 条码符号结构

① 左侧空白区：位于条码左侧无任何符号的空白区域，主要用于提示扫描器准备开始扫描。

② 起始字符：条码字符的第一位字符，用于标识一个条码符号的开始，扫描器确认此字符存在后，开始处理扫描脉冲。

③ 数据字符:位于起始字符后的字符,用来标识一个条码符号的具体数值,允许双向扫描。

④ 检验字符:用来判定此次扫描是否有有效的字符,通常是一种算法运算的结果。扫描器读入条码进行解码时,对读入的各字符进行运算,如果运算结果与检验码相同,则判定此次识读有效。

⑤ 终止字符:位于条码符号右侧,表示信息结束的特殊符号。

⑥ 右侧空白区:在终止字符之外的无印刷符号的空白区域。

2. 条码的种类及主要码制介绍

条码可分为一维条码和二维条码。一维条码必须与计算机的数据库联系起来应用;二维条码比一维条码包含更多的信息容量,自身可以携带文字信息,如商品的制造厂家、名称、生产日期、图书分类号、邮件起止地点、类别、日期等信息,它不需要与计算机数据库联系就能翻译出条码的含义。

一维条码是通常我们所说的传统条码,按其应用可分为商品条码和物流条码,商品条码包括 EAN 码和 UPC 码;物流条码包括 128 码、39 码、库德巴(Coda Bar)码等。

二维条码根据其构成原理、结构形状的差异,可分为两大类型:一类是行排式二维条码(2D Stacked Bar Code);另一类是矩阵式二维条码(2D Matrix Bar Code)。

1) 一维条码

(1) 物流条码

① 39 码:39 码(Code 39)是 1975 年由美国的 Intermec 公司研制的一种条码,它能够对数字、英文字母及其他字符等 44 个字符进行编码。由于具有自检功能,使得 39 码具有误读率低等优点,首先在美国国防部得到应用。一个 39 码如图 2-7 所示。

目前,39 码广泛应用在汽车、材料管理、经济管理、医疗卫生和邮政、储运等领域。我国于 1991 年研发制定了 39 码的国家标准(GB/T 12908—1991),2002 年发布了新版本(GB/T 12908—2002),替代了 1991 年的版本,推荐在运输、仓储、工业生产线、图书情报、医疗卫生等领域应用 39 码。



图 2-7 39 码举例

39 码的每 1 个条码字符由 9 个单元组成(5 个条单元和 4 个空单元),其中 3 个单元是宽单元(用二进制“1”表示),其余是窄单元(用二进制“0”表示),故称之为“39 码”。

② 库德巴码:库德巴码是于 1972 年研制出来的,广泛地应用于医疗卫生和图书馆行业,也用于邮政快件上。美国输血协会还将库德巴码规定为血袋标识的代码,以确保操作准确,保护人类的安全。

一个库德巴码如图 2-8 所示,由左侧空白区、起始字符、数据字符、终止字符及右侧空白区构成。它的每个字符由 7 个单元组成(4 个条单元和 3 个空单元),其中 2 个或 3 个是宽单元(用二进制数“1”表示),其余是窄单元(用二进制数“0”表示)。

库德巴码字符集中的字母 A、B、C、D 只用于起始字符和终止字符,其选择可任意组合。

(2) 商品条码

商品标识代码是由国际物品编码协会(EAN)和美国统一代码委员会(UCC)规定的、用于标识商品的一组数字,包括 EAN/UCC-13 码、EAN/UCC-8 码和 UCC-12 码。

① EAN/UCC-13 码:EAN/UCC-13 码的标准码共 13 位数,由“国家代码”、“厂商代码”、

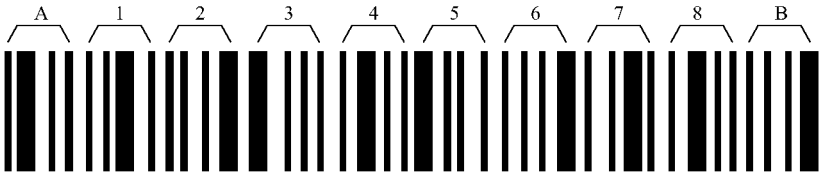


图 2-8 库德巴码符号结构

“商品代码”及“校正码”组成,具体结构说明见表 2-1 和表 2-2。EAN/UCC-13 码主要应用于超级市场和其他零售业,因此,这种码是我们平时比较常见的,随便拿起身边的一个从超市买来的商品都可以从包装上看到的。比如:中华人民共和国可用的国家代码有 690~695,如图 2-9所示。



图 2-9 EAN/UCC-13 商品条码举例

表 2-1 EAN/UCC-13 码的结构构成

结构种类	厂商识别代码	商品项目代码	校验码
结构一	X13 X12 X11 X10 X9 X8 X7	X6 X5 X4 X3 X2	X1
结构二	X13 X12 X11 X10 X9 X8 X7 X6	X5 X4 X3 X2	X1
结构三	X13 X12 X11 X10 X9 X8 X7 X6 X5	X4 X3 X2	X1

表 2-2 EAN/UCC-13 码的结构说明

名称	描 述	备 注
国家代码 (前缀码)	由 2 ~ 3 位数字 (X13X12 或 X13X12X11)组成	EAN 已将 690~695 分配给中国使用
厂商代码	由 7~9 位数字组成	由中国物品编码中心负责分配和管理,统一分配、注册,因此,编码中心有责任确保每个厂商的识别代码在全球范围内是唯一的
商品代码	由 3~5 位数字组成	由厂商负责编制,由 3 位数字组成的商品项目代码有 000 ~999,共有 1000 个编码容量,可标识 1000 种商品;同理,由 4 位数字组成的商品项目代码可标识 10000 种商品;由 5 位数字组成的商品项目代码可标识 100000 种商品
校正码 (校验位)	根据编码规则计算得出	

② UCC-12 码:UCC-12 码可以用 UPC-A 码和 UPC-E 码的符号表示。
UPC-A 码的代码结构说明见表 2-3。

表 2-3 UPC-A 码的代码结构

商品项目识别代码	校验码
X12 X11 X10X9 X8 X7 X6 X5 X4 X3 X2	X1

厂商识别代码:由左起 6~10 位数字组成,其中 X12 为系统字符。

商品项目代码:由 1~5 位数字组成。

校验码:校验码为 1 位数字,计算方法同 EAN/UCC-13 码。

UPC-E 码所表示的 UCC-12 码由 8 位数字(X8~X1)组成,是将系统字符为“0”的 UCC-12 码进行消零压缩所得到的。其中,X8~X2 为商品项目识别代码;X8 为系统字符,取值为 0;X1 为校验码,校验码为消零压缩前 UPC-A 码的校验码。

2) 二维条码

二维条码技术是在一维条码无法满足实际应用需求的前提下产生的。由于受信息容量的限制,一维条码通常是对物品的标识,而不是对物品的描述。

国外对二维条码技术的研究始于 20 世纪 80 年代末。在二维条码符号表示技术研究方面,已研制出多种码制,常见的有 PDF417、QR Code、Code 49、Code 16K、Code One 等。这些二维条码的密度都比传统的一维条码有了较大的提高,如 PDF417 的信息密度是一维条码 39 码的 20 多倍。

二维条码通过水平和垂直两个方向表示信息,可以承载大量数据,一维条码与二维条码的对比如图 2-10 所示,如图 2-11 所示是一些典型的二维条码。

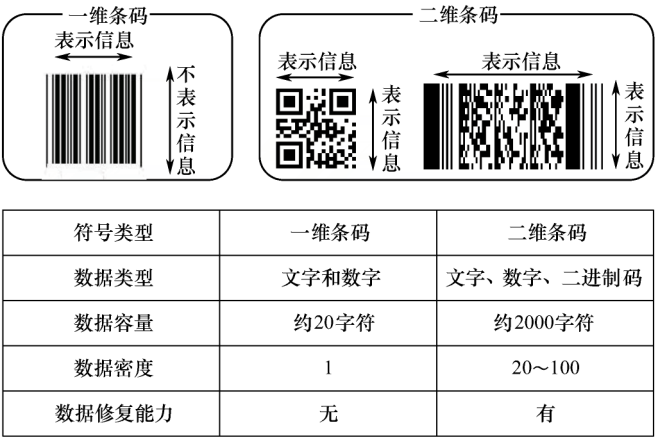


图 2-10 一维条码与二维条码的对比

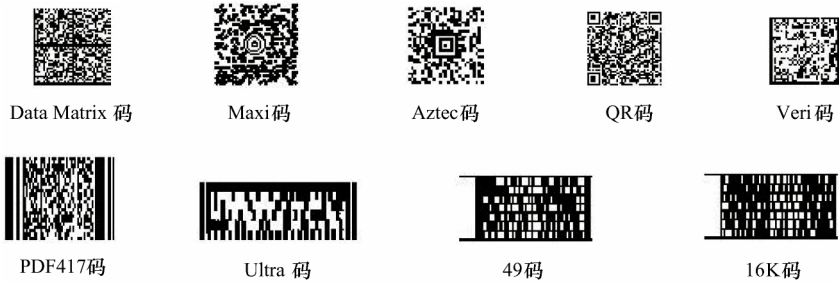


图 2-11 典型的二维条码

(1) 二维条码的特点

二维条码除了左右(条宽)的粗细及黑白线条有意义外,上下的条高也有意义。与一维条码相比,由于左右(条宽)、上下(条高)的线条皆有意义,故可存放的信息量比较大。

信息容量大、安全性高、读取率高、错误纠正能力强等特性,是二维条码的主要特点。对于行排式二维条码可用线扫描器多次扫描识读,而对于矩阵条码仅能用图像扫描器识读。一维条码通常是对物品的标识,而二维条码是对物品的描述。

(2) 二维条码的分类

二维条码通常分为以下两种类型:行排式二维条码和矩阵式二维条码。

① 行排式二维条码:又称堆积式二维条码或层排式二维条码,其编码原理是建立在一维条码基础上,按其需要堆积成两行或多行的。

行排式二维条码在编码设计、校验原理、识读方式等方面继承了一维条码的一些特点,识读设备和条码印刷与一维条码技术兼容。但由于行数的增加,需要对行进行判定,其译码算法与软件也不完全相同于一维条码。有代表性的行排式二维条码有 PDF417 码(见图 2-12(a))、49 码(见图 2-12(b))、16K 码(见图 2-12(c))等。

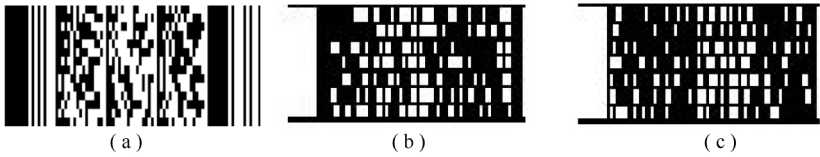


图 2-12 常见的行排式二维码

② 矩阵式二维条码:又称棋盘式二维条码,是在一个矩形空间内,通过黑、白像素在矩阵中的不同分布进行编码的。

在矩阵相应元素位置上,用点(方点、圆点或其他形状)的出现表示二进制的“1”,点的不出现在表示二进制的“0”,点的排列组合确定了矩阵式二维条码所代表的意义。矩阵式二维条码是建立在计算机图像处理技术、组合编码原理等基础上的一种新型图形符号自动识读处理码制,具有代表性的矩阵式二维条码有:QR 码(见图 2-13 (a))、Data Matrix 码(见图 2-13 (b))、Maxi 码(见图 2-13 (c))、One 码等。

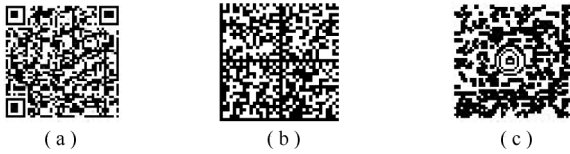


图 2-13 常见的矩阵式二维码

(3) 常用的二维条码举例

① PDF417 码:PDF 取自英文 Portable Data File 三个单词的首字母,意为“便携式数据文件”。因为组成条码的每个符号字符都是由 4 个条和 4 个空,共有 17 个模块构成的,故称为 PDF417 码。

PDF417 码是一种多层、可变长度、具有高容量和纠错能力的二维条码。每个码符号可以表示 1100 个字节,或 1800 个 ASCII 字符,或 2700 个数字的信息。

② QR 码:QR 码能实现超高速识读(是 PDF417 码的 10 倍)和全方位识读,能够有效表示中国汉字和日本汉字(1817 字符)、数字型字符(0~9)、字母数字型数据(数字 0~9、大写字

母 A~Z)、9 个其他字符(Space、\$、%、*、+、-、.、/、:)、符号规格 21×21 模块(版本 1)~177×177 模块(版本 40)(每种规格,每边增加 4 个模块),可用 1~16 个 QR 码连接,扩大信息表示规模,具有极强的纠错能力。一个 QR 码应用如图 2-14 所示。



图 2-14 QR 码的应用

2.1.2 射频自动识别技术

1. RFID 系统的构成

RFID 系统包括射频(识别)标签、射频识别读写设备(读写器)和应用软件。一个典型的 RFID 应用系统的结构如图 2-15 所示。下面主要简单介绍 RFID 系统相关知识,详细内容见第 3 章。

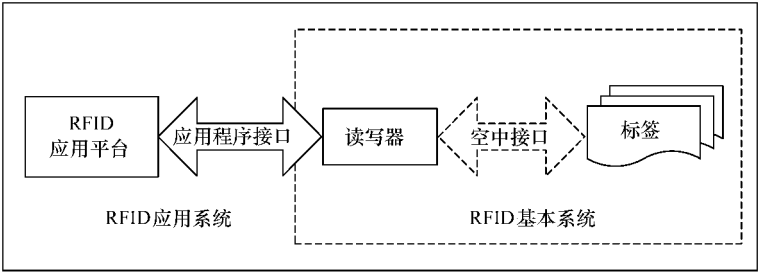


图 2-15 RFID 应用系统的结构图

射频(识别)标签:又称为射频标签、电子标签,主要由存有识别代码的大规模集成电路芯片和收发天线构成。每个标签具有唯一的电子编码,附着在物体上标识目标对象。

读写器:射频识别读写设备,是连接信息服务系统与标签的纽带,主要起到目标识别和信息读取(有时还可以写入)的功能。标签是被识别的目标,是信息的载体。

应用软件:针对各个不同应用领域的管理软件。

2. RFID 系统的基本工作原理

RFID 技术的基本工作原理是由读写器发射特定频率的无线电波能量,当射频标签进入感应磁场后,接收读写器发出的射频信号凭借感应电流所获得的能量,发送出存储在芯片中的产品信息(Passive Tag,无源标签或被动标签),或者由标签主动发送某一频率的信号(Active Tag,有源标签或主动标签),读写器读取信息并解码后,送至中央信息系统进行有关数据处理。工作原理如图 2-16 所示。

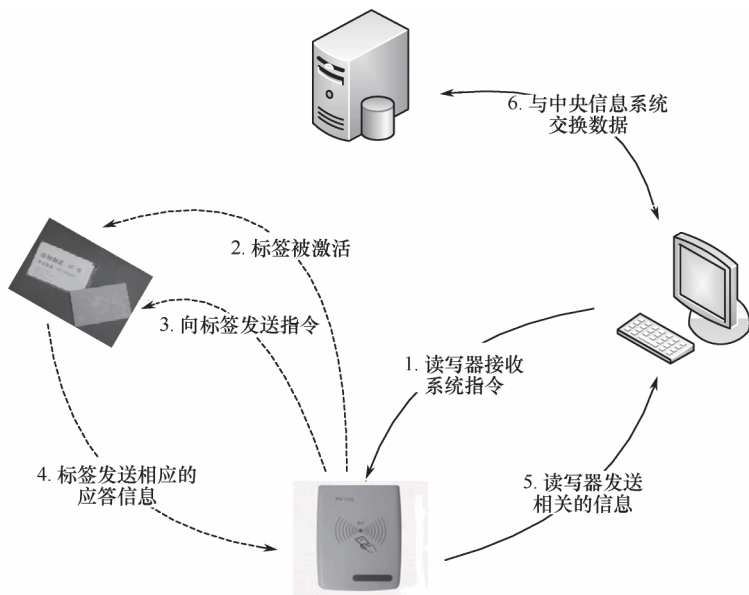
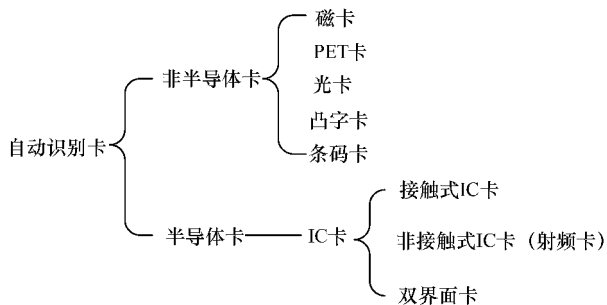


图 2-16 RFID 系统的基本工作原理

2.1.3 卡类自动识别技术

1. 卡类识别技术的分类

卡类识别技术的产生和推广使用加快了人们日常生活信息化的速度。用于信息处理的卡片大致可分为非半导体卡和半导体卡两大类,非半导体卡包括磁卡、PET 卡、光卡、凸字卡等;半导体卡主要有 IC 卡等,具体分类如下。



下面重点介绍磁卡技术和 IC 卡技术。

1) 磁卡技术

磁卡(Magnetic Card)是利用磁性载体来记录信息的,磁卡技术应用了物理学和磁力学的基本原理。常见的磁性载体通常以液体磁性材料或磁条为信息载体,将液体磁性材料涂覆在卡片上(如存折);或将宽 6~14mm 的磁条压贴在卡片上(如银行卡),如图 2-17 所示。

磁卡具有以下优点:

- 数据可读写,具有现场改造数据的能力;
- 数据的存储量能够满足大多数需要,便于使用,成本低廉;
- 具有一定的数据安全性;
- 能黏附于许多不同规格和形式的基材上。

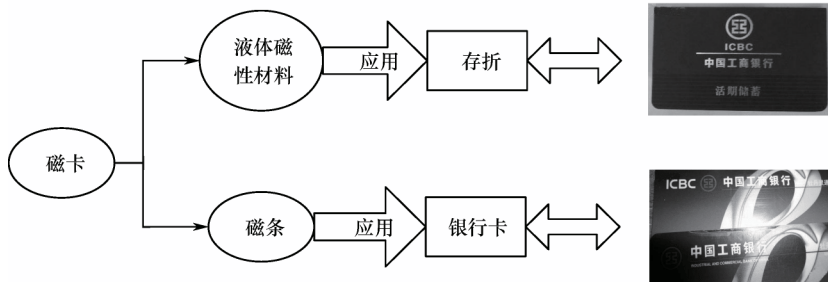


图 2-17 磁卡按载体分类应用

这些优点使得磁卡在许多领域得到广泛应用,如银行信用卡、ATM 卡、机票、公共汽车票、自动售货卡、会员卡、现金卡(如电话磁卡)等。

2) IC 卡技术

(1) IC 卡技术简介

集成电路(Integrated Circuit Card, IC)卡是继磁卡之后出现的又一种新型信息工具。IC 卡在有些国家和地区也称为智能卡(Smart Card)、智慧卡(Intelligent Card)、微电路卡(Micro-circuit Card)或微芯片卡等。它是将一个微电子芯片嵌入符合 ISO 7816 标准的卡基中,做成卡片形式,利用集成电路的可存储特性,保存、读取和修改芯片上的信息,已经十分广泛地应用于包括金融、交通、社保等很多领域。

IC 卡的主要特性如下所述:

- 存储容量大,其内部可含 RAM、ROM、EPROM、EEPROM 等存储器,存储容量从几字节到几兆字节;
- 体积小、质量轻、抗干扰能力强、便于携带;
- 安全性高,在无源情况下数据也不会丢失,数据的安全性和保密性都非常好;
- 智能卡与计算机系统相结合,可以方便地满足对各种各样信息的采集、传送、加密和管理的需要。

(2) IC 卡的种类

IC 卡按通信方式可分为接触式 IC 卡、非接触式 IC 卡和双界面卡,如图 2-18 所示。



(a) 接触式 IC 卡



(b) 非接触式 IC 卡

图 2-18 IC 卡

① 接触式 IC 卡:接触式 IC 卡是通过读写设备的触点与 IC 卡的触点接触后,进行数据的读写。

国际标准 ISO 7816 对此类卡的机械、电气特性等进行了规定。具有标准形状的铜皮触点,通过和卡座的触点相连后,实现外部设备的信息交换。按芯片的类型,接触 IC 卡可分为 4 种类型,即存储器卡、逻辑加密卡、CPU 卡和超级智能卡。

存储器卡——存储器卡内的集成电路是电可擦除的可编程只读存储器 EEPROM,只有数据存储功能,没有数据处理能力。该卡本身不提供硬件加密功能,只能存储通过系统加密的数据,很容易被破解。

逻辑加密卡——逻辑加密卡内的集成电路包括加密逻辑电路和电可擦除可编程只读存储器 EEPROM。卡中有若干个密码口令,只有在密码输入正确后,才能对相应区域的信息内容进行读出或写入。若密码输入出错一定次数后,该卡自动封锁,成为死卡。此类卡适用于需加密的系统,如食堂就餐卡等。

CPU 卡——CPU 卡也称为智能卡,卡内的集成电路包括中央处理器(CPU)、电可擦除可编程只读存储器 EEPROM、随机存储器 RAM、固化的卡内操作系统 COS(Chip Operating System)和只读存储器 ROM。该卡相当于一个带操作系统的单片机,严格防范非法用户访问卡中的信息。发现数次非法访问后,也可以锁住某个信息区域,但可以通过高级命令进行解锁,以保证卡内的信息绝对安全,系统高度可靠。此卡适用于绝密系统中,如银行金融卡等。

超级智能卡——超级智能卡上具有 MPU 和存储器,并装有键盘、液晶显示器和电源,有的卡上还具有指纹识别装置等。此卡也适用于绝密系统中。

② 非接触式 IC 卡(射频卡):非接触式 IC 卡与读写设备无电路接触,而是通过非接触式的读写技术进行读写(例如光或无线技术)。相关技术请参看第 3 章的内容,在此不再赘述。

2. 卡类识别技术基础

1) 磁卡技术基础

(1) 磁记录原理

磁条是由一些微小的磁粒(铁磁材料)附着于类似塑料胶带上形成的,铁磁材料是一种在外部磁场移走后仍可以保留磁性的物质。

磁条上数据的存储就是靠改变磁条上氧化粒子的磁性来实现的。在数据的写入过程中,需要输入的数据首先通过“编码器”变换成二进制的机器代码,然后控制器控制的“磁头”在与磁条的相对移动过程中,改变磁条磁性粒子的极性来实现数据写入。数据的读出是“磁头”先读出机器代码,再通过“译码器”还原成人们可识读的数据信息。

记录时,磁卡的磁性面以一定的速度移动,或记录磁头以一定的速度移动,并分别和记录磁头的空隙或磁性面相接触。磁头的线圈一旦通上电流,空隙处就会产生与电流成比例的磁场,于是,磁卡与空隙接触部分的磁性体就被磁化。

如果记录信号电流随时间而变化,则当磁卡上的磁性体通过空隙时(因为磁卡或磁头是移动的),便随着电流的变化而不同程度地被磁化。磁卡被磁化之后,离开空隙的磁卡磁性层就留下相应于电流变化的剩磁。

利用磁粒附着技术,通过以不同的频率改变磁条上附着的磁粒的极性实现了逻辑数据“0”和“1”的记录,再通过对二进制数据编码,就可以在磁条上记录各种信息了。

(2) 磁条和磁道

磁卡的一面印刷有说明提示性的信息,如插卡方向等;另一面则有磁层或磁条,具有 2~3 个磁道以记录有关信息数据。

磁道(Track):磁条上存储信息的分区叫磁道,如图 2-19 所示。

磁道 1:记录密度为 210bpi,可记录数字(0~9)、字母(A~Z)和其他一些符号(如括号、分隔符等),并包含 79 个 7 位的二进制码(6 位 ALPHA 编码+1 位奇校验位)。磁道 1 记录字母、数字型数据(字母用于记录持卡人的姓名),为只读磁道,在使用时,磁道上记录的信息只能

读出而不允许写入或修改。

磁道 2: 记录密度为 75bpi, 所记录的字符只能是数字(0~9), 并包含 40 个 5 位的二进制码(4 位 BCD 编码+1 位奇校验位)。磁道 2 记录数字型数据, 也为只读磁道。

磁道 3: 记录密度为 210bpi, 所记录的字符只能是数字(0~9), 并包含 107 个 5 位二进制码(4 位 BCD 编码+1 位奇校验位)。磁道 3 记录数字型数据, 如记录账面余额等, 为可读写磁道, 既可以读出, 也可以写入。

磁道必须符合 ANSI 及 ISO/IEC 标准的磁卡的物理尺寸定义, 这些尺寸的定义涉及磁卡读写的标准化。对磁卡上磁道 1(或磁道 2 或磁道 3)进行数据编码时, 如果数据在磁带上的物理位置偏高或偏低了哪怕几个毫米, 这些已编码的数据信息就会偏移到其他的磁道上。

磁道 1、磁道 2、磁道 3 的每个磁道宽度相同, 为 2.80mm(0.11 英寸)左右, 用于存放用户的数据信息; 相邻两个磁道约有 0.5mm(0.02 英寸)的间隙, 用于区分相邻的两个磁道; 整个磁带宽度在 10.29mm(0.405 英寸)左右(3 磁道磁卡), 或 6.35mm(0.25 英寸)左右(2 磁道磁卡)。实际上, 人们所接触的银行磁卡上的磁带宽度会加宽 1~2mm, 磁带总宽度为 12~13mm。

(3) 磁道的格式和内容

磁道的应用分配一般是根据特殊的使用要求而定制的, 如银行系统、证券系统、门禁控制系统、身份识别系统、驾驶员驾驶执照管理系统等, 都会对磁卡上 3 个磁道提出不同的应用格式, 如图 2-20 所示。

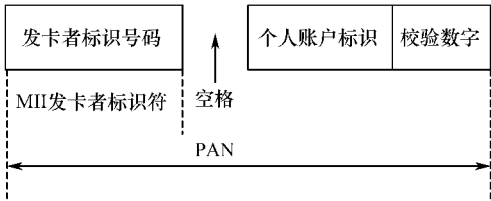


图 2-20 磁道格式

例如, MII=1 标识为航空业, MII=3 标识是旅游或娱乐业, MII=5 标识为银行/金融业。

2) IC 卡技术基础

如前所述, IC 卡可分为接触式 IC 卡和非接触式 IC 卡, 下面重点介绍接触式 IC 卡的工作原理。

(1) 接触式 IC 卡

① 接触式 IC 卡的结构: IC 卡读写器要能读写符合 ISO7816 标准的 IC 卡。IC 卡接口电路作为 IC 卡与卡内 CPU 的唯一通道, 为保证通信和数据交换的安全与可靠, 其产生的电信号必须满足特定要求。

接触式 IC 卡的构成可分为半导体芯片、电极模片、塑料基片几部分, 其内部结构如图 2-21 所示。

② 接触式 IC 卡的工作原理: 接触式 IC 卡获取工作电压的方法为接触式 IC 卡通过其表



图 2-19 磁卡的磁道

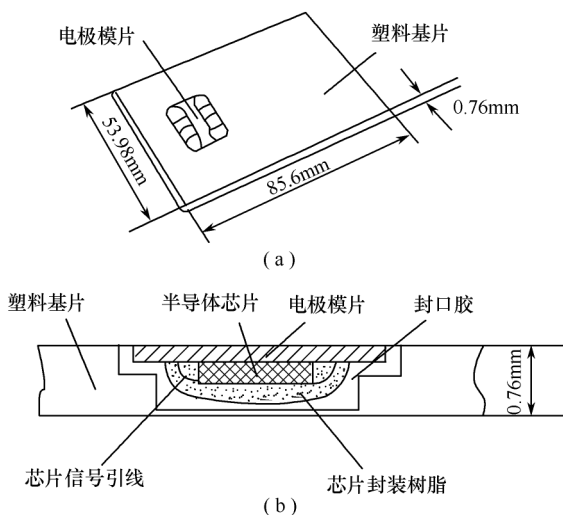


图 2-21 接触式 IC 卡的内部结构

面的金属电极触点将卡的集成电路与外部接口电路直接接触连接,由外部接口电路提供卡内集成电路工作的电源。

接触式 IC 卡与读写器交换数据的原理为接触式 IC 卡通过其表面的金属电极触点将卡的集成电路与 IC 接口电路直接接触连接,通过串行方式与读卡器交换数据(通信)。

(2) 接触式 IC 卡 CPU 技术

IC 卡从接口方式上分为接触式 IC 卡、非接触式 IC 卡;从器件技术上分为非加密存储卡、加密存储卡。非加密卡没有安全性,可以任意改写卡内的数据;加密存储卡在普通存储卡的基础上加了逻辑加密电路。

逻辑加密存储卡由于采用密码控制逻辑来控制对 EEPROM 的访问和改写,在使用前要校验密码,才可以进行写操作。因此,对于芯片本身来说是安全的,但在应用上是不安全的。具体存在以下不安全因素:

- ① 密码在线路上是明文传输的,易被截取;
- ② 对于系统商来说,密码及加密算法都是透明的;
- ③ 逻辑加密卡无法认证应用是否合法。

例如,假设有人伪造了 ATM,你无法知道它的合法性,当插入信用卡,输入密码的时候,信用卡的密码就被截获了。再如网上购物,如果用逻辑加密卡,购物者同样无法确定网上商店的合法性。

正是由于逻辑加密卡使用上的不安全因素,促进了 CPU 卡的发展。CPU 卡可以做到对人、对卡、对系统的三方合法性认证。

(3) CPU 卡的三种认证

CPU 卡具有以下三种认证方法:

- ① 对持卡者的合法性认证——密码校验,通过持卡人输入个人口令来进行验证;
- ② 对卡的合法性认证——内部认证;
- ③ 对系统的合法性认证——外部认证。

认证过程是通过系统,传送随机数 X ,用指定算法、密钥对随机数加密,用指定算法、密钥解密 Y ,得结果 Z ,比较 X 、 Z ,如果相同,则表示系统是合法的。

在以上认证过程中,密钥是不在线路上以明文出现的,它每次的送出都是经过随机数加密

的,而且因为有随机数的参加,可以确保每次传输的内容都不同,即使被截获也没有任何意义。这不单是密码对密码的认证,也是一种方法认证,就像早期在军队中使用的密码电报,发送方将报文按一定的方法加密后成密文发送出去,接收方收到后按一定的方法将密文解密。

通过这种认证方式,线路上就没有了攻击点,同时,卡也可以验证应用的合法性。但是由于系统方用于认证的密钥及算法还是在应用程序中,因此不能完全去除系统商的攻击性,为此,引进了 SAM 卡的概念。

(4) SAM 卡

SAM 卡是一种具有特殊性能的 CPU 卡,用于存放密钥和加密算法,可完成交易中的相互认证、密码验证和加密、解密运算,一般用作身份标志。由于 SAM 卡的出现,有了一套更完整的系统解决方案。

在发卡时,将主密钥存入 SAM 卡中,然后由 SAM 卡中的主密钥对用户卡的特征字节(如应用序列号)加密生成子密钥,将子密钥注入用户卡中。由于应用序列号的唯一性,使得每张用户卡内的子密钥都不同。

密钥一旦注入卡中,就不会在卡外出现。在使用时,由 SAM 卡的主密钥生成子密钥存放在 RAM 区中,用于加密、解密数据。

上述的认证过程就成为如下形式:通过 SAM 卡系统,传送随机数 X ,SAM 卡生成子密钥对随机数加密;SAM 卡解密 Y ,得结果 Z ;比较 X 、 Z ,如果相同,则表示系统是合法的。

这样,在应用程序中的密钥就转移到了 SAM 卡中,认证成为卡—卡的认证,系统商不再存在责任。

卡与外界进行数据传输时,若以明文方式传输,数据易被截获和分析,同时,也可以对传输的数据进行篡改。要解决这个问题,CPU 卡提供了线路保护功能。

线路保护分为两种,一是将传输的数据进行 DES 加密,以密文形式传输,以防止截获和分析;二是对传输的数据附加 MAC(安全报文鉴别码),接收方收到后首先进行校验,校验正确后才予以接收,以保证数据的真实性与完整性。

2.1.4 生物特征自动识别技术

1. 生物特征识别技术的基本原理

生物特征识别技术的核心在于如何获取这些生物特征,并将之转换为数字信息,存储于计算机中,再利用可靠的匹配算法来完成识别与验证个人身份的过程。

1) 基本原理

生物特征识别技术的原理如图 2-22 所示。

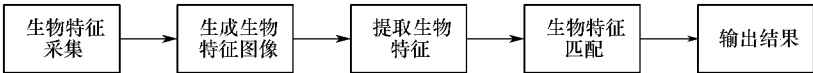


图 2-22 生物特征识别技术的原理

完成整个生物特征识别技术,首先要对生物特征进行取样,样品可以是指纹、面部、语音等;其次要经过特征提取系统,提取出唯一的生物特征,并转化为特征代码;再将特征代码存入数据库,形成识别数据库。当人们通过生物特征识别系统进行身份认证时,识别系统将获取被认证人的特征,然后通过一种特征匹配算法,将被认证人的特征与数据库中的特征代码进行比对,从而决定接受还是拒绝该人。

2) 生物特征识别技术的特点

生物特征识别技术的特点,决定了该技术是个人身份鉴别的有效手段。其主要特点如下:普遍性、唯一性和稳定性、不可复制性。

(1) 普遍性

生物特征识别技术所依赖的身体特征基本上是人类与生俱来的,不需要向有关部门申请或制作。

(2) 唯一性和稳定性

经研究和经验表明,每个人的指纹、掌纹、面部、发音、虹膜、视网膜、骨架等都与他人不同,且终生不变。

(3) 不可复制性

随着计算机技术的发展,复制钥匙、密码卡及盗取密码、口令等都变得越来越容易,然而,要复制人类的活体指纹、掌纹、面部、虹膜等生物特征,就困难得多。

综上所述,利用生物特征进行身份验证的方法,无须依赖于各种人造的和附加的物品来证明人的自身,而用来证明自身的,恰恰是人的本身。所以,它不会丢失、不会遗忘、很难伪造和假冒,是一种“只认人、不认物”的、方便安全的保安手段。

2. 生物特征识别技术的主要内容

1) 指纹

指纹在我国古代就被用来代替签字画押,证明身份。大致可分为“弓”、“箕”、“斗”三种基本类型,具有各人不同、终身不变的特性。指纹识别是目前最成熟、最方便可靠、无损伤和价格便宜的生物特征识别技术解决方案,已在许多行业领域中得到了广泛的应用。

(1) 优点

① 专一性强、复杂程度高。指纹是人体独一无二的特征,并且它们的复杂度足以提供用于鉴别的足够特征。

② 可靠性高。如果想要增加可靠性,只需登记更多的指纹,鉴别更多的手指,最多可以多达 10 个,而且,每个指纹都是独一无二的。用户将手指与指纹采集头直接接触,是读取人体生物特征最可靠的方法。

③ 速度快、使用方便。扫描指纹的速度比较快,使用非常方便。

④ 设备小、价格低。指纹采集装置更加小型化,可以很容易地与其他设备相结合,而且随着电子传感芯片的快速发展,价格也会更加低廉。

(2) 缺点

① 某些人或某些群体的指纹因为指纹特征很少,因此很难成像。

② 由于现在的指纹鉴别技术都可不存储任何含有指纹图像的数据,而只是存储从指纹中得到的加密的指纹特征数据。每次使用指纹时,都会在指纹采集装置上留下用户的指纹印痕,而这些指纹痕迹存在被用来复制指纹的可能性。

2) 掌纹

手掌几何学是基于几乎每个人的手的形状都是不同的,而且这个手的形状在人达到一定年龄之后就不再发生显著变化的基础上的事实。当用户把他的手放在手形读取器上时,一个手的三维图像就会被捕捉下来。然后,对手指和指关节的形状和长度进行测量。

根据用来识别的数据的不同,手形读取技术可划分为下列三种范畴:手掌的应用、手中血管的模式和手指的几何分析。映射出手的不同特征是相当简单的,不会产生大量数据集。但

是,即使有了相当数量的记录,手掌几何学也不一定能够把人区分开来,这是因为手的特征是很相似的。与其他生物特征识别方法相比较,手掌几何学不能获得最高程度的准确度。当数据库持续增大时,也就需要在数量上增加手掌的明显特征,用以清楚地将人与模板进行辨认和比较。

3) 眼睛

基于分析眼睛的复杂和独特特征的生物特征识别技术主要包括:虹膜识别技术、视网膜识别技术和角膜识别技术。其中常用的是虹膜识别和视网膜识别。

(1) 虹膜识别

虹膜是位于人眼表面黑色瞳孔和白色巩膜之间的圆环状区域,它在红外光下会呈现出丰富的纹理信息,如斑点、条纹、细丝、冠状、隐窝等细节特征。

虹膜识别技术是通过比对虹膜图像特征之间的相似性来确定人的身份的,其核心是使用模式识别、图像处理等方法,对人眼睛的虹膜特征进行描述和匹配,从而实现自动的个人身份认证。英国国家物理实验室的测试结果表明虹膜识别是各种生物特征识别方法中错误率最低的。从普通家庭门禁、单位考勤到银行保险柜、金融交易确认,应用后都可以有效地简化通行验证手续并确保安全。如果手机加载“虹膜识别”,即使丢失也不用担心信息泄露。机场通关安检中采用虹膜识别技术,将缩短通关时间,提高安全等级。

(2) 视网膜识别

视网膜是眼睛底部的血液细胞层。视网膜扫描是采用低密度的红外线去捕捉视网膜的独特特征,血液细胞的唯一模式就因此被捕捉下来。某些人认为,视网膜是比虹膜更为唯一的生物特征。

视网膜识别的优点就在于它是一种极其固定的生物特征,因为它是“隐藏”的,因此不可能受到磨损、老化等影响;使用者也无须和设备进行直接接触;同时,它是一个最难欺骗的系统,因为视网膜是不可见的,无法被伪造。另一方面,视网膜识别也有一些不完善的方面,如视网膜技术可能会给使用者带来健康的损坏,这需要进一步研究;设备投入较为昂贵,识别过程的要求也高。因此,视网膜扫描识别在普遍地推广应用上,具有一定的难度。

4) 面部

面部识别系统是通过分析面部特征的唯一形状、模式和位置来辨识人。其采集处理的方法主要是标准视频和热成像技术。

标准视频技术通过一个标准的摄像头来摄取面部的图像或者一系列图像,在面部被捕捉之后,一些核心点被记录,例如眼睛、鼻子和嘴的位置,以及它们之间的相对位置被记录下来,然后形成模板。热成像技术是通过分析由面部的毛细血管的血液产生的热线来产生面部图像,它与视频摄像头不同,热成像技术无须较好的光源条件,因此,即使在黑暗情况下,也可以使用。

面部生物特征识别技术的吸引力在于它能够人机交互,用户无须和设备直接接触。但相对来说,这套系统的可靠性较差,使用者面部的位置与周围的光环境都可能影响系统的精确性,并且设备十分昂贵,只有比较高级的摄像头才可以有效、高速地捕捉面部图像,设备的小型化也比较困难。

此外,面部生物特征识别系统对于因人体面部的如头发、饰物、变老以及其他的变化需要通过人工智能来得到补偿,机器的知识学习系统必须不断地将以前得到的图像和现在的进行比对,以改进核心数据并弥补微小的差别。鉴于以上各种因素,此项技术在推广应用上还存在着一定的困难。

5) 语音

语音识别主要包括两个方面:语言和声音。声音识别是对基于生理学和行为特征的说 话者的嗓音和语言学模式的运用,它与语言识别的不同在于,不对说出的词语本身进行辨 识,而是通过分析语音的唯一特性(例如发音的频率)来识别出说话的人。声音辨识技术 使得人们可以通过说话的嗓音来控制能否出入限制性的区域。

举例来说,通过电话拨入银行。语言识别则要对说话的内容进行识别,主要可用于信 息输入、数据库检索、远程控制等方面。现在身份识别方面更多的是采用声音识别。

声音识别也是一种非接触的识别技术,用户可以很自然地接受,使用方便。但由于非人 性化的风险、远程控制和低准确度,它并不可靠。并且声音的变化范围(如音量、速度和 音质等方面)直接会影响到采集与比对的精确度,一个患上感冒的人有可能被错误地拒 认,从而无法使用该声音识别系统。同时随着数字化技术的发展,音频数字处理技术很 可能欺骗声音识别系统,其安全性受到了挑战。

6) 签名

签名识别,也被称为签名力学辨识,它是建立在签名时的力度上的。它分析的是笔的 移动,例如加速度、压力、方向以及笔画的长度,而非签名的图像本身。签名识别和声 音识别一样,是一种行为测定学。签名力学的关键在于区分出不同的签名部分,有些是 习惯性的,而另一些在每次签名时都不同。

签名作为身份认证的手段已经用了几百年了,应用范围从独立宣言到信用卡都可见 到,是一种能很容易被大众接受,而且是一种公认的、较为成熟的身份识别技术。然 而,签名辨识的问题仍然存在于获取辨识过程中使用的度量方式以及签名的重复性。

7) DNA

人体内的 DNA 在整个人类范围内具有唯一性(除双胞胎可能具有同样结构的 DNA 外) 和永久性。因此,除了对双胞胎个体的鉴别可能失去它应有的功能外,这种方法具有绝 对的权威性和准确性。DNA 鉴别方法主要根据人体细胞中 DNA 分子的结构因人而异 的特点进行身份鉴别。

这种方法的准确性优于其他任何身份鉴别方法,同时有较好的防伪性。然而,DNA 的 获取和鉴别方法(DNA 鉴别必须在一定的化学环境下进行)限制了 DNA 鉴别技术的 实时性。此外,某些特殊疾病可能改变人体 DNA 的结构组成,系统无法正确地对这类 人群进行鉴别。

8) 其他

除了以上介绍的几种生物特征识别技术以外,现在开发和研究中的还有通过静脉、 耳朵形状、按键节奏、身体气味、行走步态等的识别技术。

表 2-4 为 5 类主要的人体生物特征的自然属性对比。

表 2-4 5 类主要的人体生物特征的自然属性

自然属性 特性	虹膜	指纹	面部	DNA	静脉
唯一性	因人而异	因人而异	因人而异	同卵双胞胎相同	唯一性
稳定性	终身不变	终身不变	随年龄段改变	终身不变	终身不变
抗磨损性	不易磨损	易磨损	较易磨损	不受影响	不受影响
痕迹残留	不留痕迹	接触时留痕迹	不留痕迹	体液、细胞中含有	不留痕迹