FINGERPRINTS

生物认证技术

目录

1. 引言

指纹识别技术是一种易于使用的、可靠的以及具有成本效益的个人身份验证方式。这项技术有许多优点，使得指纹传感器在移动设备中广泛应用，如智能手机和平板电脑。但生物认证技术和指纹识别技术未来会有更多更具吸引力的应用方式，例如支付、门禁、汽车、可穿戴设备和家用电器。

《生物认证技术》这本书由Fingerprints™编写，旨在帮助了客户、潜在客户、合作伙伴和其他需要更好地了解生物世界的人。该书内容借鉴了Fingerprints™生物系统的丰富经验，并重点关注指纹识别，因为指纹识别是身份验证和识别的最主要的生物特征识别技术。本书涉及一般的认证和识别以及目前用于身份验证的各种生物识别方法，还包括对指纹识别的详细阐述。

那些想了解整个生物识别领域的人，可以从头到尾仔细地阅读《生物认证技术》，但也可以使用后面的索引，参考阅读。

本书中的所有陈述和信息在当前被认为是准确的，但并不担保其恒久的准确性。

2. 生物认证

我们的生活充满了你需要证明你是谁的情况，可能是出于个人原因，也可能是职业需要。你需要开锁，需要访问电子邮件帐户，需要购物-但这些都只有经过正确授权的人才可以做。我们可以很容易地列出大量的需要身份识别的情况，包括从银行交易到启动汽车的很多事情都需要快速、可靠和方便的用户认证。因此，身份识别和认证已成为当今社会的基石，在防止欺诈和犯罪行为的同时使得相互交流更为安全。

2.1 用户认证与识别

为了证明你的身份，你需要证明你是你所声称的那个人。验证所声称的身份是真实的这一验证过程，被称为用户认证，如果我们已经创建了一个自动认证系统，那么该过程或多或少就是自动化的。现如今，考虑到速度和方便方面的需求，在许多应用中，自动用户身份验证势在必行，例如，当打开你的手机或登录到您的电子邮件时。

图1. 你是谁?

一个相关的过程是用户识别，就是确定个人身份的行为。从一个给定的庞大人群中鉴定出某一个人称为识别，但识别这个术语，通常并不意味着验证了这个人所声称的身份，但它是用户认证的基础。用户认证意味着是一对一的关系（“我是那个我所声称的人”），而用户识别是多对一的映射关系（“我是美国人群中的X先生。”）。正如认证可以自动进行一样，也有许多自动识别系统的应用例子，比如警察扫描指纹搜查嫌疑人。

2.2 认证因素

根据身份认证的已知因素，认证某人身份的方式可以分为三个基本类别：用户知道的事物、用户拥有的事物、或用户本身具有的特征。每个认证因素都涵盖一系列的用于在授予访问、批准事务请求、签署文件、授予他人权限等事务前提前认证或验证一个人的身份的要素。

- ***知识因素***是用户所知道并希望记住的东西，如密码、个人身份识别密码、回答一个安全性问题等。
- ***所有权因素***是用户拥有的东西，如身份证、安全令牌、手机和物理密钥等。
- ***内在因素***是用户本身的特性或所做的事情，例如指纹、签名、声音等。生物认证技术是本文研究的范围，利用各种内在因素来验证用户的身份。

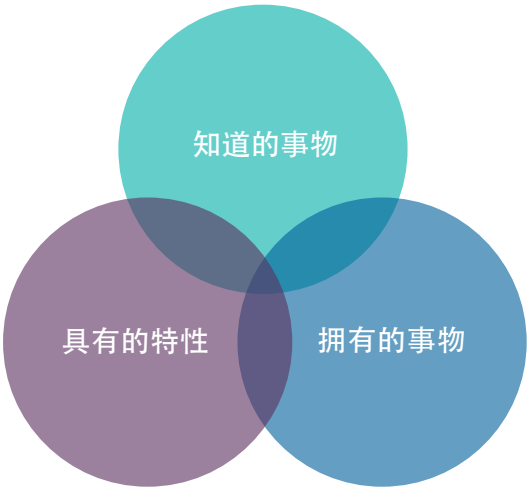


图2. 三类认证因素

一个完整的授权过程可能至少包括上述因素之一，因为安全研究已经确定了一个真实的认证，至少应验证来自两个因素的要素，最好是所有三个因素的要素。然后分别将其称为双因素和多因素认证。当然，也可以使用相同类型的几个因素，如PIN码和安全问题，但这不会给予如“真实”的多因素认证一样的安全水平。

现在我们可以更正式地定义生物认证技术：

生物认证技术-自动使用行为和生理特性，以验证某个人的身份。

1 ***出自希腊文字**"real, genuine"（“真正的”）*

当比较生物认证技术与其他认证因素时，几个方面的因素发挥了作用。基于知识因素的认证，如密码，在技术方面很容易通过软件实现，但也相对容易被计算机算法或用户设备中的间谍软件破解。此外，用户往往选择简单和常见的密码，甚至与他人共用密码，这就使得这种认证并不可靠。

基于所有权因素的身份认证通常更为安全，但依赖于物理密钥/卡/电话等的身份验证可能会被盗取、丢失或被遗忘在家里。而且所有权验证的任何专用物理设备还会引起相关生产成本。

一方面，在正确实施生物认证时，所使用的信息对于每个人都是唯一且终身不变的。这些都是生物认证的关键优点，使得生物认证在许多应用中成为首选认证因素。另一方面，生物认证也有其方便和生物认证有关的社会可接受的一面，这是必须考虑的。然而，根据所使用的生物认证的传感器要求的类型、成本、尺寸和功率，处理上的逻辑性可能是一个潜在的缺点。

2.3 安全性和便利性

比较自动认证系统时，安全性显然是需要讨论的一个最根本的因素，包括那些正在使用生物认证的认证系统。与以往一样，需要权衡考虑高安全性和用户便利性。彻底评估系统是否安全，不仅包括评估生物识别读取和匹配的唯一性，还必须包括评估可能的对处理引擎非法访问-黑客，以及评估系统是否可以被模拟生物识别码的人愚弄-电子欺骗。

作为一种反黑客措施的例子，它通常不是通过指纹图像，而是通过作为模板存储在移动设备上的数学表现来实现的。存储的该表现减少了黑客的风险，因为它不能被用来重新创建原始指纹图像。此外，模板并不是随便存储在设备的任何地方。该模板被存储，并且认证过程中所涉及的算法在可信执行环境（TEE）中运行。该系统架构功能进一步增强了安全性，因为它保存了生物识别数据，还具有远离潜在黑客和病毒的过程。它还存在其他防护方案，如使用安全的加密处理器（可信平台模块，TPM）和创建私有内存区（软件保护扩展，SGX），规避了不必要的访问。

信用卡同样可以配备一个安全要素，例如芯片，提供了一个动态的环境，使其安全地存储生物识别数据，安全地处理生物识别数据，安全地与外部实体进行交流。如果你试图以任何方式篡改芯片，它可能会自我毁灭，不会让你获得未经授权的访问。

欺骗即伪造货物或文件。在生物认证系统中，用户的面孔、声音和指纹等，均可以被复制，并将真实信息传递给传感器。已经开发了许多先进的技术，以最小化被欺骗的风险。例如，在指纹识别中，可以通过增加图像质量和使用复杂的匹配算法减少被欺骗的风险。通过各种反欺骗方案，如现场检测和使用一个以上的生物识别码来验证用户，实现额外的安全性。

没有任何系统是绝对安全的-只要有无限的时间（和金钱），你就可以攻击和欺骗任何东西。但无论怎样，现场检测和其他先进的生物认证技术使这样的恶意攻击变得非常昂贵。

为了适当地量化不同生物认证系统的安全性和便利性的特点，我们需要一个通用模型，即系统如何工作，以及所使用的一组适当的指标。因此，本部分还定义了一些用于生物认证系统行业的一般度量。

所有生物认证系统的设计都是用于执行下列一般操作:

- **数据捕获** – 捕获所使用生物识别码数据的某种传感器
- **注册** – 分析捕获的数据，存储其独特的功能作为数字模板
- **身份验证** – 当注册用户想要验证其身份时，他/她的生物特征数据再次被捕获，并和注册时所产生的模板进行对比
- **匹配** – 如果有/没有一个匹配的存储模板，需要用算法进行比较。除非和已验证的用户身份匹配，否则访问将被拒绝

2.3.1 容错率 (FAR)

用于评估生物认证系统安全性的一个指标是容错率FAR，（有时称为FMR，错误匹配率）。FAR数值告诉你，在没有正确的生物认证数据的情况下，传感器会基于统计学提供一个正确的匹配的几率。FAR比不仅依赖于传感器系统的软件（算法），还依赖于硬件。

$$FAR = \frac{\text{总错误接受值}}{\text{总错误尝试值}}$$

图 3. 容错率(FAR)的定义

目前智能手机使用的指纹传感器的标准FAR大约为1 / 50000，这基本上意味着，如果你随机选择一些人尝试使用指纹传感器登录你的手机，平均每50000个人中就有一个人会成功。

2.3.2 拒错率 (FRR)

通常用来衡量生物认证传感器便利性的指标是传感器的拒错率（FRR）（也叫FNMR，错误非匹配率）。FRR告诉你，在匹配算法中，传感器多久会错误地拒绝一次。

$$FRR = \frac{\text{总错误拒绝值}}{\text{总错误尝试值}}$$

图 4. 拒错率 (FRR)的定义

方便也涉及到传感器的其他属性，如使用的直观性、唤醒速度/唤醒传感器需要什么样的操作，以及传感器是如何被纳入终端产品的，虽然这更大程度上是传感器的尺寸和设计灵活性的结果。

绘制各种生物认证系统的FRR比和FAR比，非常有趣的洞察了安全性和便利性之间的权衡取舍。理想的传感器应具有最小的FAR和FRR，但在现实中，生物认证系统是一个曲线，你在获得高便利性（低FRR）的同时就只能获得低安全性（高FAR），反之亦然，详见图5。

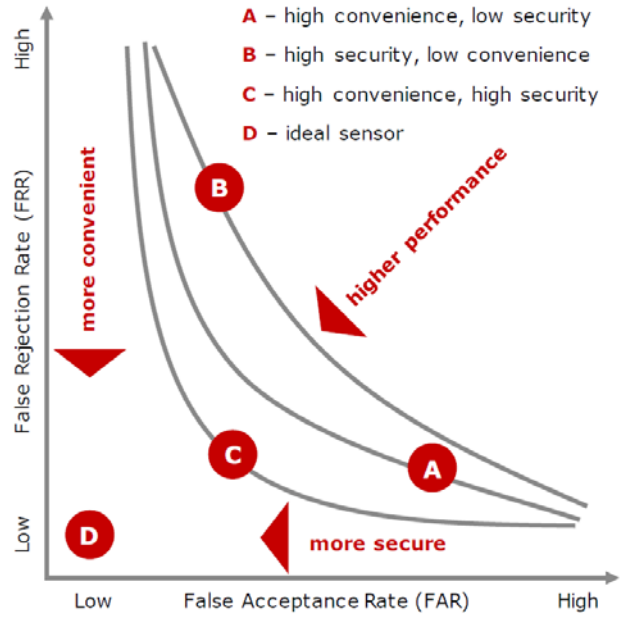


图 5. 安全与便利之间的权衡说明

3. 生物认证技术

生物识别这个词来源于希腊语“生物”（生命）和“度量”（测量）。生物识别允许基于你本身，而不是你知道的东西（例如PIN码或密码）或你拥有的东西（例如密钥或护照）进行认证。

生物认证技术的概念已经存在几百年甚至几千年了。其中一个最古老和最基本的典型例子就是，用于通过人脸识别人类。自文明诞生以来，人类就已经在使用人脸来识别已知和未知的个人。人类之间识别的概念也被视为行为主导型生物认证技术，如语音和步态识别。我们利用这些特性，经过日积月累，一定程度上不知不觉地就识别出了已知个体。

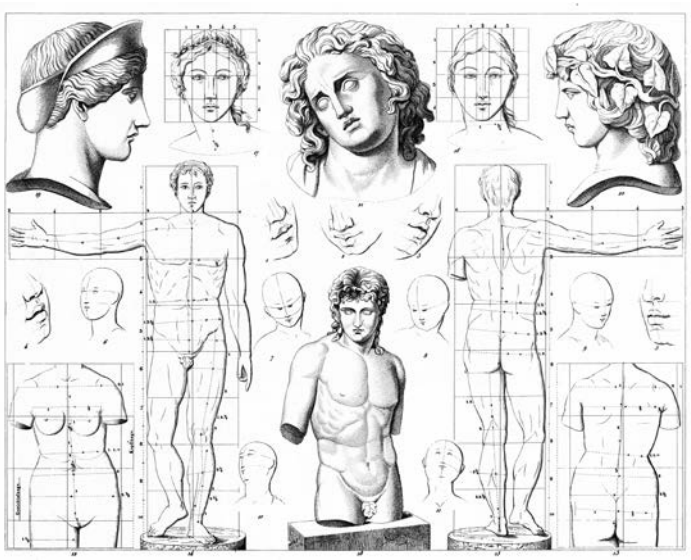


图 6. 生物技术

用自动化处理的生物识别取代我们每天执行的生物识别，在过去的几十年中才成为可能。由于日益高效的集成电路发展的驱动，计算机处理中的进步起到了推动作用。今天有各种各样的生物认证技术，而指纹识别是使用最广泛的一种。

3.1 生物标识符和生物认证系统

由于一个人身上综合了众多的特性，我们需要一些区分不同生物标识符的分类方法，也被称为生物识别方式。首先是将它们分组为行为或生理标识符。行为标识符是随着时间而变化获得的可度量特征。然后，通过使用模式识别技术，该特征可以被用于验证人的身份。行为标识符包括签名识别、语音识别和关键行程动态识别。

生理标识符是你自身的东西，而不是你所做的或所知道的东西。有许多类型的生理的标识符，包括指纹、掌纹、虹膜、视网膜、脸、DNA、脑电图等等。

生理标识符的例子	行为标识符的例子
指纹、手印、足迹	声音
眼睛的虹膜与视网膜	签名
脸、耳朵	手势
静脉血管形态	步态
气味	

图 7. 生物识别码(模式)的例子

生物认证系统是自动化系统，能够利用来自于生物标识符的生物识别数据（模式）进行识别。所有的生物认证系统在一个非常高的水平均可以被描述为一个自动化的过程：

- 通过生物识别装置捕获生物识别数据，例如指纹传感器和相关电路
- 从实际提交的样品中提取相关数据
- 将扫描数据与捕获的数据进行比较，以供参考
- 匹配提交的样本与模板
- 确定生物识别数据持有者的身份是否真实

生物认证系统包括硬件和软件。生物特征识别装置收集、读取和比较生物识别数据。生物识别数据取自个体，并且对于每个人来说，都是独一无二的。生物认证系统内的嵌入式软件包括处理采集的生物数据的生物识别工具。该软件通常与硬件协同工作，运行生物识别数据采集过程、提取数据并进行比对，包括数据匹配。

今天用于生物认证系统的常见的生物识别码是指纹、脸、语音、血管与签名。许多变化存在于每个基本标识符类别中市场上也有结合了若干标识符的系统，即进行多模式认证。

上述不同生物认证系统的市场份额，结合了独立生物认证系统和客户端服务系统，鉴于大多数生物认证系统属于这两个类别。以下几节简要概述生物识别的主要类型标识符及其重要特性。

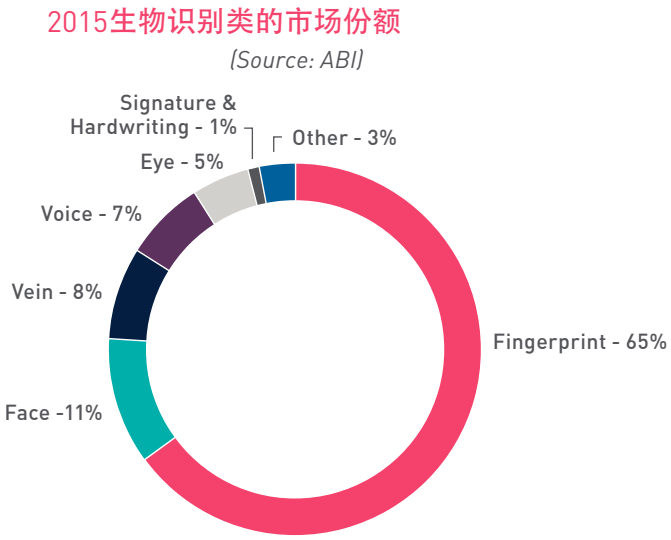


图 8. 不同类型的生物识别市场份额，基于营收
来源: ABI Research 2016

3.2 指纹识别

指纹识别作为使用的主要生物识别码，将在第4章中进行更详细的讲述。然而，为了能够与其他标识符进行比较，这里简要介绍了指纹识别的原理和特点。

我们的指尖皮肤上的脊，形成了我们的指纹所显示的独特图案。在生物识别中，由脊形成的模式被称为特征点 。特征点的例子是脊末端、交叉、核心和分岔，见图9。

几种不同的技术可用于捕获指纹–从在法医学中应用的传统手工方法，到苹果和Synaptics公司的先进的应用于柔性电路板（FPC）传感器的主动式电容技术。指纹的独特特性可以通过光学、电容、超声波、热或压电传感器类型来读取，每个类型有自己的好处和缺点，如第4章所述。

相比于其他生物识别码，如虹膜扫描和语音识别，指纹识别是一个非常有吸引力的生物识别码。今天，指纹识别信息作为主导生物形态用于商业性应用的主要原因，可以概括为：

- 每个指纹都具有很高的唯一性，即认证是明确的

图 9. 指纹的形成

2 Minutiae 是一个拉丁词，表示琐事和细枝末节

- 在一个人的整个生命期间，指纹通常一直保持不变
- 现有技术允许对指纹进行具有成本效益的传感和测量
- 可以很容易地量化感测到的指纹参数，并允许创建用于识别所有者的有效算法
- 许多与指纹识别相关的标准已经建立完善，为规模经济奠定了基础，例如降低了指纹硬件和软件的成本

生物识别方式的特点

	指纹	虹膜	视网膜	眼印	脸	语音	血管
独特性	●	●	●	●	◗	◔	●
永久性	●	●	●	●	◗	◔	●
可测性	●	◗	◔	◗	◗	◗	◗
可采集性	●	◗	◔	◗	◗	◗	◗
标准性	●	◗	◔	○	◗	◗	○

● Very high ◕ High ◗ Medium ◔ Low ○ Very low

图 10. 几种生物识别方式的比较. 来源: Redeye, April 2016

指纹识别在易用性、处理速度和一般安全性等方面也具有较高的性能。因此，在大多数情况下，指纹识别是一种极好的生物识别码，特别是在需要大量应用时成本和标准化极其重要。通常情况下，其他生物识别码可以用作补充，无论是在特殊的应用程序中，或出于安全所需，要求对一个人的身份进行多模式验证时。

没有技术是完美的，指纹识别间或被人提及的一个弊端就是社会可接受性方面：由于刑事鉴定和大量公民政府登记，一些用户认为指纹识别会带来很多麻烦。另一方面，肮脏或干燥的手指可能会影响指纹的感知，导致某些类型传感器的识别过程失败。

3.3 眼睛识别

基于眼睛特征的生物识别极其引人注目，因为人眼的几个特征具有很高的独特性，包括在我们的眼白-巩膜血管识别中的虹膜、视网膜和血管图案。因此，在执法部门和政府业务设定中，人眼生物认证系统是常见的识别和验证手段。最近，眼睛识别已经开始用于移动生物认证技术中。

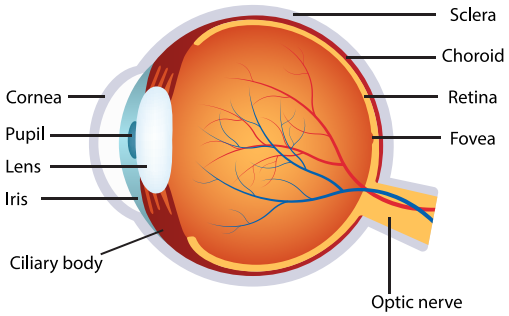


图 11. 眼解剖图

3.3.1 Retina

第一个生物识别眼睛扫描系统是1985年引进的视网膜扫描仪。视网膜是一层薄膜组织，位于眼睛的背面，有一个独特的毛细血管模式，甚至在同卵双胞胎中，也没有一个相类似的模式。此外，从出生到死亡，视网膜是不变的，也就是说，如果没有疾病，如糖尿病视网膜病变或通过新生血管及出血使得毛细血管的模式发生改变。

由于视网膜位于眼睛的后面，而不是肉眼可见的，不能由传统的智能手机摄像头或类似的设备进行图像采集。视网膜扫描是通过将一束红外光射进眼睛，在视网膜上形成一条标准路径，以检测用于认证的毛细血管的模式。

虽然视网膜扫描提供了高度安全性，这项技术仍然有许多缺点，导致其有限的商业用途：

- 难以获得有用的图像
- 繁琐的注册过程
- 需要专门设备
- 价格昂贵

视网膜扫描已被各种机构用于高安全性设置的识别（1：N），如联邦调查局、美国航空航天局和中央情报局。视网膜扫描也用于医疗诊断应用。出现了新的以激光为基础的视网膜相机/扫描仪，更善于捕捉患有某些疾病的人的图片，否则视网膜扫描图像是不可能实现的。但是，该设备是昂贵的，大概10万美元，主要在医院应用。

3.3.2 虹膜

我们眼睛中的彩色部分，即虹膜，实际上是一种控制光线进入眼睛的肌肉。虹膜的特点是具有冠状物、隐窝、细丝、斑点坑、沟纹、条纹和环，都是一个人的独一无二的特征。通常使用其中一种扫描技术，就可捕获了超过200种特征，包括图像传感器/ 互补金属氧化物半导体图像传感器和红外摄像机。通常情况下，有必要用红外线灯来照亮眼睛，所以一般的智能手机相机是无法用于扫描虹膜的。

虹膜识别是一个相对较新的技术，1994首次获得专利，并于1995年投入商业应用。自那时以来，虹膜识别技术实现了更好的算法和硬件的改进。虹膜识别首先用于执法和政府机构的识别系统，但现在已经开始应用于移动设备。

虹膜识别，就像任何生物认证技术一样，优点和缺点共存：

+ **非常高的精确度** – 假认证风险较小
+ **非接触式** – 使得它适合于识别
– **速度** – 虹膜识别的速度不如指纹识别
– **加工要求/功耗** – 运行算法所需的处理能力高于指纹识别，通常需要10个因素中的1个。相对于指纹识别，虹膜识别通常还需要存储更多的数据
– **反欺骗能力** – 虹膜识别技术是一种容易伪造的技术，防范各种欺骗攻击，的安全性较低

所有研究虹膜识别的生物认证技术正在进行中，以求进一步增强优势，解决这项技术的弱点。

3.3.3 巩膜血管（眼纹）

巩膜静脉识别是一种新兴的生物认证技术，已被集成在一些智能手机中。这种最常用的解决方案背后的技术，在设备中使用了常见的互补金属氧化物半导体（或图像传感器）图像传感器，以捕捉用户眼睛的图像。基于巩膜血管独特模式模板的图像，以及建立眼睛内部和周围的其他微观特征，然后将模板用于认证。

巩膜血管识别的主要优点是不需要专门的硬件；只需要1百万像素分辨率以上的摄像头就足够了。然而，由于速度、精度和处理能力等可能的要求，目前尚未充分了解这个非常年轻的技术。

3.4 人脸和耳朵识别

人脸识别联合利用人脸的多种特征，可以用来识别个人身份。可以使用的特征的例子，是鼻子的形状和眼睛之间的距离。

总体而言，我们的脸上大约80个类似的不同特征以及用于参考的节点。用于身份验证的生物识别模板就是以这些节点为基础。有时一些痣等个人特征，也增加了安全性。

面部识别的优点和缺点包括：

+ **低成本** – 在移动设备中，无需额外的硬件，对于其他应用程序来说，一个相机就足够了

+ **范围** – 取决于你想达到什么目的，面部识别具有一个优势，即可以在相当长的距离，令人毫无察觉的情况下进行识别

– **需要良好的灯光**

– **随着时间变化，稳定性变低** – 由于年龄的变化、疾病和体重增减，脸部会发生变化

– **安全性低** – 通过外科整容，很容易恶搞面部识别系统，往往用一张照片就可以实现

图 12. 人脸识别

- **失败率高** – 眼镜、帽子，头发和其它多种因素，均使得面部识别系统无法捕获认证所需要的节点

至于其他的生物认证技术，人脸识别的算法和方法的发展使其获得了改进。

人耳识别技术是一种与人脸识别密切相关的生物认证技术，它将外耳表面的许多脊和凹处作为生物特征识别。耳朵的细节结构不仅是独一无二的，而且是永久的，因为在人的一生中，耳朵的外观通常不会改变。此外，获取耳朵图像并不一定需要人的配合，但大多数人仍然认为是非侵入性的。

使用2D和3D人耳图像的人耳识别系统，具有和人脸识别系统相似的优势和劣势。

3.5 语音识别

声纹认证已得到了长时间的使用，广泛应用于客户服务中心，不要与行为性生物识别语音识别混淆。

另外，语音识别以较低的成本就可以实现，除了手机，不需要其他硬件，但是也有重要缺点。

– 声纹认证可以随着时间的变化而变化，因此需要定期更新声音样本

– 由于外部因素，如环境和健康，声纹认证会发生改变–试想一下，当你感冒的时候，你的声音是怎么样的

– 可以很容易地记录声纹认证，用于欺骗认证系统

语音识别技术已经取得了进步，但有些系统更具优势，例如在嘈杂的环境中时。仍然存在一个重大因素，即语音识别需要用户说话，不但费时，而且在许多情况下不方便。

3.6 血管识别和手的几何特征

手掌有一个复杂的血管[3]模式，对于每个人来说都是独一无二的。根据血管扫描仪提供商富士通的数据，由于血管模式在皮肤下面，几乎不可能对其进行复制/造假，并且认证安全性高，错误认知率低至0.00008%。血管识别也可以在用户的手指上进行。

高安全级别和非接触识别，使血管识别非常适合许多需要高安全性的应用程序。其应用领域的限制是扫描仪的大小和成本。

3 来自拉丁文"small vessel" (小容器)

由于扫描仪太笨重，无法安装于大多数移动设备中。此外，如果数据库保存有大量的生物识别模板，那么涉及1：N匹配的识别就需要相当长的时间。这是由于血管走行是非常复杂的，因此处理血管系统的要求较高。

作为血管识别的一种替代方法，可以对人手的几何特征进行扫描，用于创建个体的手几何标识。然而，如同血管识别一样，手几何识别也需要同样的传感器成本，也存在尺寸方面的缺点。

图13. 血管识别

3.7 行为生物辨识：步态与手势识别

步态的细微变化，可以用作身份验证和识别的生物识别码。需要测量的步态参数通常是时间-空间性的（步长、步宽、步行速度、周期时间）和运动学（髋关节、膝关节和踝关节的关节旋转，髋/膝/踝关节平均关节角度，以及大腿/躯干/脚的角度）。步距和身高之间也有很强的相关性。另一种基于外观识别个人的方法，即双重步态外形序列。

图 14. 手势识别

步态参数的精确测量，需要先进的设备，如若干摄像机，地板负载传感器等，目前，实现安全步态识别，需要一种复杂和昂贵的技术。

手势识别是步态识别的替代方法，通过数学算法，利用计算机系统对人工手势进行解释。手势识别演变为一种简化人与计算机之间的相互作用的手段，并相当受欢迎，例如控制电脑游戏。手势识别用于身份验证仍然处于起步阶段，借鉴的优势，除了相机，不需要任何其他硬件。然而，到目前为止，仍然存在安全性和造假方面的担忧，因此这是一个不太具有吸引力的认证方法。

3.8 生物认证技术的比较

有了大量的生物认证技术，为给定的应用作出正确的设计选择，并不是最容易的事情。以上描述了一些主要生物认证技术的基本特点，但也有许多更注重性能的特点需要考虑，以及所选择的技术的社会可接受性。

2016年4月，分析公司Redeye基于以下因素对各种生物认证技术进行了比较

- **成本效益** – 综合考虑不同的应用，生物识别的成本效益如何
- **处理速度** – 生成模板并匹配到一个或多个存储模板的速度，会影响所需的处理能力，因此也会影响功耗-速度越高越好
- **安全** – 综合考虑几个因素，包括但不限于反欺骗性和FAR

- **准确性** – 扫描设备如何在不同的环境中，准确地捕捉生物识别数据，及其抗干扰性
- **稳定性** – 切勿与持久性混淆，稳定性必须与时间有关，直到生物识别出现变化，或者换句话说，稳定性如何在短期内发生变化

生物认证技术的技术和性能因素

	指纹	虹膜	视网膜	眼纹	脸部	语音	血管
成本效益	High	Medium	Very low	Very high	Very high	Very high	Low
安全	High	High	Very high	High	Very low	Very low	Very high
处理速度	Very high	Medium	Medium	Medium	Medium	Very low	Medium
准确性	High	Very high	Very high	High	Low	Low	Very high
稳定性	Very high	Very high	Very high	High	Medium	Low	Very high

Very high　High　Medium　Low　Very low

图 15. 生物认证技术的一些技术和性能因素
来源: Redeye, April 2016

同样，Redeye也出具了比较每种技术"更柔软"方面的报告，例如，使用的方便程度以及被潜在用户的接受程度。相关因素包括：

- **使用容易程度** – 使用容易程度和便捷程度
- **私密性** – 高私密性意味着几乎没有人会注意到某人使用了生物认证技术，以及将其用于远程跟踪等
- **普及性** – 生物认证技术被人们所认识的程度以及使用范围大小
- **接受度** – 技术对这项技术的支持程度
- **引进时间** – 哪一年开始使用生物认证技术

生物认证技术的社会因素

	指纹	虹膜	视网膜	眼纹	脸部	语音	血管
使用容易程度	Very high	Medium	Low	High	Very high	Very high	Very high
私密性	Medium	Medium	Very high	Medium	Very low	Low	Very high
普及性	Very high	Medium	Low	Medium	Very high	Very high	Low
接受度	Very high	Medium	Low	Medium	Very high	Very high	Medium
引进时间	1981	1991	1995	2008	2000	1998	1994

Very high　High　Medium　Low　Very low

4. 指纹识别

指纹是已知的用于认证和验证的最古老生物标识。在埃及古墓的墙壁、克里特、希腊和中国陶器中均发现了指纹。在公元前2000年的古巴比伦，指纹被用作签名；为了防止伪造，法律合同的当事人将他们的指纹刻在一个写着合同的粘土片上。最近的十八世纪，指纹的解剖特征得到了详细描述。在十九世纪，提出了指纹分类方法，1975年，联邦调查局为第一台计算机指纹扫描仪的开发提供了资金。

人的指纹是很精细的，几乎是独一无二，很难改变，并在人的一生中都可以使用，使它们非常适合作为个人身份的长期标记。因此，很自然地，指纹识别系统在高安全性的应用和个人的自动识别中得到了广泛应用。便利性、安全性和性能特点，使指纹识别成为当今最广泛使用的生物认证技术。

如同在2.3节中提到的自动认证系统一样，通常执行以下操作：

- **数据捕获** – 捕获所使用生物识别码的数据的某种传感器
- **注册** – 对捕获的数据进行分析，并存储其独特的特征作为数字模板
- **验证** – 当注册用户想要验证自己的身份时，他/她的生物特征数据被再次捕获，并与所注册时产生的模板相比
- **匹配** – 如果有/没有一个匹配的存储模板，需要算法来比较。除非和已验证的用户身份匹配，否则访问将被拒绝。

这样一个系统的主要元素及其相互作用如图17所示。这一章重点关注指纹识别环境中的每个系统元素，并确定基于所扫描指纹的安全性和便利性的认证系统所必需的特性。但是，我们首先需要熟悉一下指纹的细节。

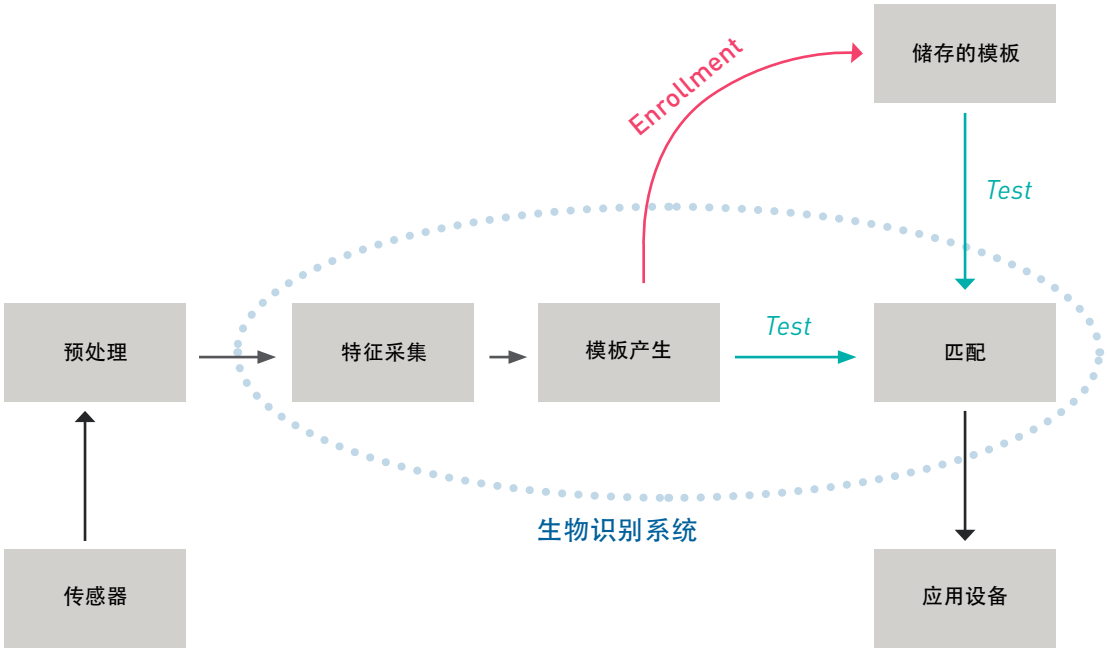


图 17. 生物认证系统主要元素的展示图

4.1 指纹

指纹是指人类手指的摩擦嵴留下的痕迹。摩擦嵴（表皮嵴）是手指、脚趾、手掌或足底表皮[4]的凸起部分。脊用来放大振动，例如，当指尖穿过不均匀表面时，可以更好地将信号传递到参与精细质感知觉的感可以更好地将信号传递到参与精细质感知觉的感觉神经。脊也可以帮助抓取粗糙的表面，并可能改善在潮湿条件下的接触物体表面。

表皮嵴形成独特的模式，每一个都有各自的特点，生物认证技术和指纹识别系统中，常被称为特征点[5]。每个人的特征点都是非常独特的，因此可用于身份验证和识别。

表皮嵴的形态有三种基本类型：拱形、环形或螺纹形（见图18）。在人群中，最常见的是环形（~65%），其次是螺纹形（~30%）和拱形（~5%）。

- **拱形**(Arch): 脊从手指一侧进入，在中心形成一个弧形，然后从手指的另一侧伸出
- **环形**(Loop): 脊从手指一侧进入，形成曲线，然后在同一侧伸出
- **螺纹形**(Whorl): 脊围绕手指的中心点形成圆形

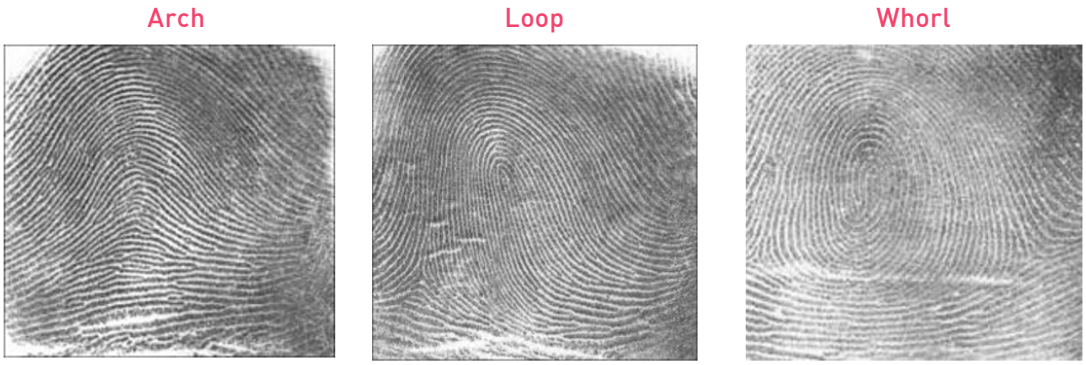


图 18. 表皮脊型的三种主要类型。这些图片代表"全尺寸"或"滚动"的指纹，例如那些通过墨水和纸张捕获的指纹

除了表皮脊的基本模式，指纹还有其他几个特点，其中一些如图19所示。

脊的开始和结束（结束点），相互交叉和分离（分岔）。

各孤立点之间有单独的脊，各脊（三角洲）之间的空间，也可以识别表皮中的单个毛孔。

用于匹配目的的指纹分析，通常需要比较几个指纹图案的特征。包括上述各种特征点点。为了成功地使用一些传感器技术，也有必要知道人皮肤的结构和性能。

自动指纹识别系统中使用的指纹匹配技术大致可分为两大类：

图 19. 指纹的其它特征。该图片表示部分或"按压"的指纹，例如移动电话上的触摸传感器所捕获的指纹

- **基于特征点的技术 –** 发展于十九世纪晚期，手动指纹识别是其根源。

4 表皮是构成皮肤的两层中的外层(希腊语的意思是"上")，内层是真皮

5 Minutiae 是一个拉丁词，是指琐事和细节

弗朗西斯·高尔顿先生描述了一些细节，加上全球脊模式类型，组成了传统上使用的指纹特征。标准匹配机构（国际标准化组织/ 美国国家标准协会）致力于这些特征（脊特征点和分支）的研究。鉴于这些特征点的密度，使用基于匹配的特征点的系统，需要研究大面积的皮肤，因此，通常需要使用大面积的传感器或刷卡传感器

- **非基于特征点的技术 –** 其它所有方法就是非基于特征点的方法，其包括广泛的匹配原则，从各子图像的直接相关，到v脊流矢量化和基于频率的方法。传感器的大小、类型和安全操作点（FAR水平）将决定哪些是可行的。其他系统资源，如可用的内存和处理能力，对于选择最佳方法当然是很重要的。

结合了传统特征点和非特征点方法的匹配算法通常被称为混合方法。

由于供应商相互操作性的强烈要求，配备了大传感器政府指纹识别/认证系统，通常是ISO / ANSI的特征点匹配。

由于传感器尺寸变小了，混合解决方案变得更受欢迎了，甚至更小的传感器，如那些在移动设备中的传感器，由于这是不常见的，导致特征点完全被忽视了。

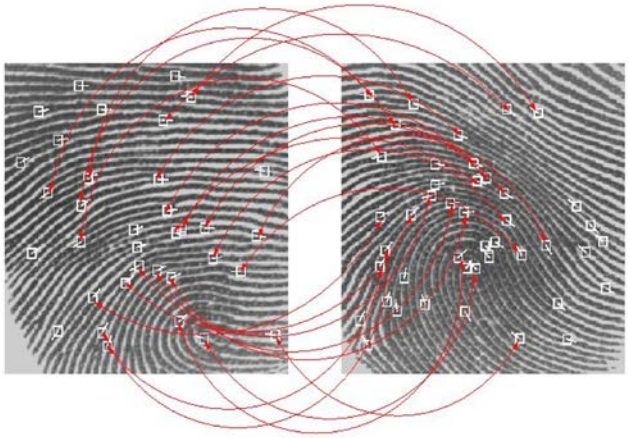


图 20. 基于指纹匹配的特征点

4.2 指纹传感器

指纹传感器是一种用于注册指纹图案数字图像的电子装置。这种图像现在被称为指纹的活扫描[6]，传感器有时是专用硬件实体的输入元件，但指纹扫描仪往往是其它设备的一部分，如移动电话。指纹传感器捕获相关的指纹特征，进行进一步的处理，因此是指纹识别系统中最重要的元素之一，其他特征是所使用的图像处理/特征提取和匹配算法。

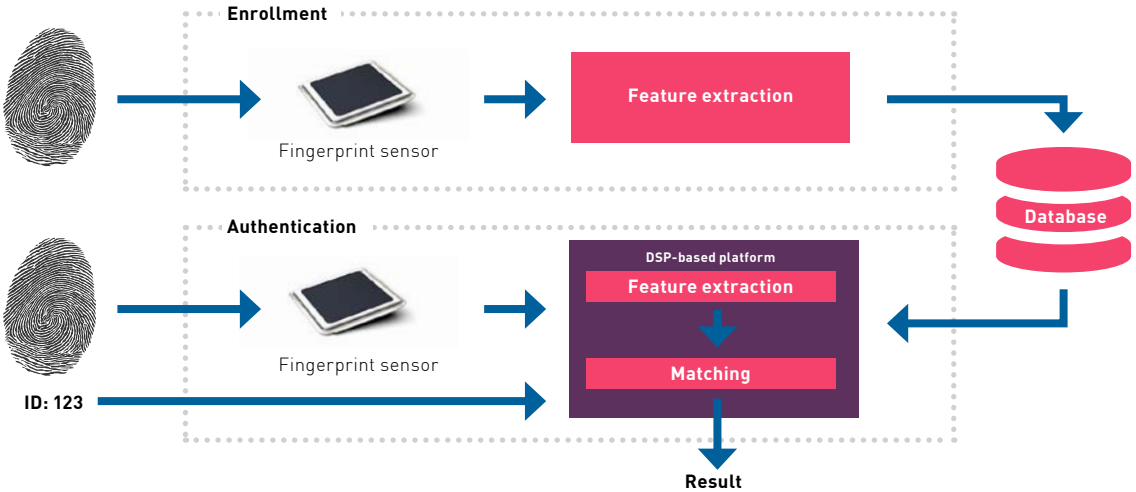


图 21. 自动指纹识别系统

根据操作模式，指纹传感器通常被归类为刷卡传感器或触摸传感器。刷卡传感器[7]，可发现于许多便携式电脑。当你在传感器上滑动手指时， 触摸传感器"逐行"扫描指纹，一下子捕获整个指纹。典型刷卡传感器的外形可以小于触摸传感器，从而降低其成本，但另一方面，捕捉指纹的难度可能较大，导致高拒错率（FRR）。下面主要描述的是使用任何以下任何一种技术的刷卡和触摸传感器。

6 相对于离线图像检索，例如用于识别的数据库

7 有时称为线性传感器。一些刷卡传感器是由一个以上的敏感元素构成，操作如同一个高度较小的矩形触摸传感器

图 22. 刷卡和触摸传感器

刷卡传感器的一个优点是，它经常捕获一个更大区域的指纹，例如，现场扫描可能比从触摸传感器包含更多的数据，这使得随后的匹配过程更简单。但从用户的角度来看，触摸传感器验证往往比刷卡传感器验证快得多，因此在许多情况下更方便。

4.2.1 光学传感器

光学传感器通过捕捉可见光并将其转换成用于创建指纹图像的电信号，从而成功注册指纹图案。该传感器有光电二极管或光电晶体管检测器，将冲击探测器的光中的能量转换为电荷。大多数光学传感器包还包括LED（发光二极管）或LED阵列，以照亮指尖，使探测器可以捕捉从手指反射的光的指纹图像。然后用覆盖了保护涂层的棱镜来反射朝向探测器的光。

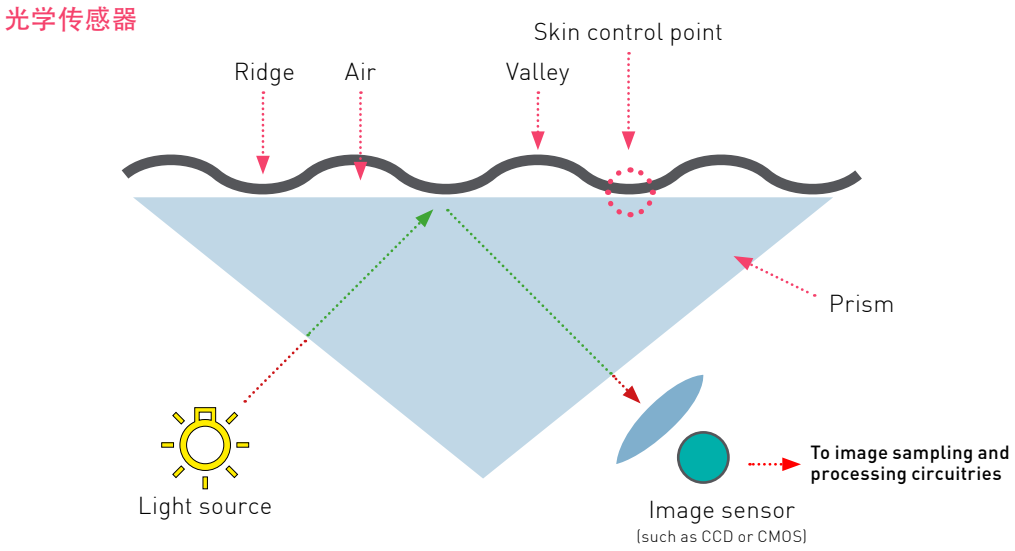


图 23. 光学指纹传感器的工作原理

今天，光学指纹传感器使用的探测器是CCD（电荷耦合器件）或CMOS光学成像器。CCD和CMOS探测器是相同的类型，可以发现于数码相机。CCD探测器对低水平的光特别敏感，因此有利于捕捉灰度。历史上的CCD探测器比CMOS探测器要好得多，但在过去的十年左右， CMOS技术已有了很大的发展，CMOS技术能力已经赶上了CCD。

与CMOS制造相比，CCD制造是相当昂贵的。除了成本之外，CMOS光学成像也具有明显的优势，因为它们可以在探测器之类的同一硅芯片上建立一些图像预处理逻辑。这催生了大多数的光学传感器电子消费品，其中的重要特征是成本以及功耗，使用CMOS探测器。

光学捕获是电子指纹传感器使用的第一个技术，并且可能是应用最广泛的技术。它的主要优点是成本相对较低，但这项技术也有几个缺点。

- **便宜** – 采用CMOS的光学传感器的制造成本较低
- **易于欺骗** – 用假手指来欺骗传统光学指纹扫描仪是相对容易的，通常情况下，甚至不需要制作一个假手指，但良好的指纹图像是不够的。更先进的光学扫描仪（FTIR）可以增加欺骗难度
- **尺寸** – 使用正常设计的光学传感器包括一个透镜和棱镜系统，是很笨重的，不适合在移动设备中使用
- **污染敏感性**– 光学传感器对环境中常见的几个污染物很敏感，包括杂散光、油、污垢、冷凝液、冰甚至另一个用户留下的指纹
- **老化** – 随着使用时间的延长，棱镜涂层和CCD传感器会出现耗损，减少了现场扫描精度

随着各种技术的发展，光学传感器也在不断改进，加上各种解决方案，已克服已经提出的欺骗风险和污染问题，如使用于电光技术和适用于相机。然而，所建议的解决方案产生了其他问题，而且往往是昂贵的。光学传感器在消费类电子产品中的劣势也变得更加明显，特别是在移动设备中，棱镜和透镜系统的大小使得传感器大得离谱。

4.2.2 电容式传感器

电容是物理实物保持电荷的能力。电容式指纹传感器通过使用包含成千上万个小电容板的阵列来生成指纹图像。阵列板构成了图像的“像素”：它们各自充当平行板电容器的一个极板，而手指的真皮层具有导电性，作为非导电表皮层绝缘层之间的另一个板。手指放置在传感器上时，产生微弱的电荷，在手指的脊或凹处之间建立一个模式。使用这些电荷，传感器测量横跨感测表面的电容图案。由传感器逻辑将测量值数字化，然后发送到相邻的微处理器进行分析。

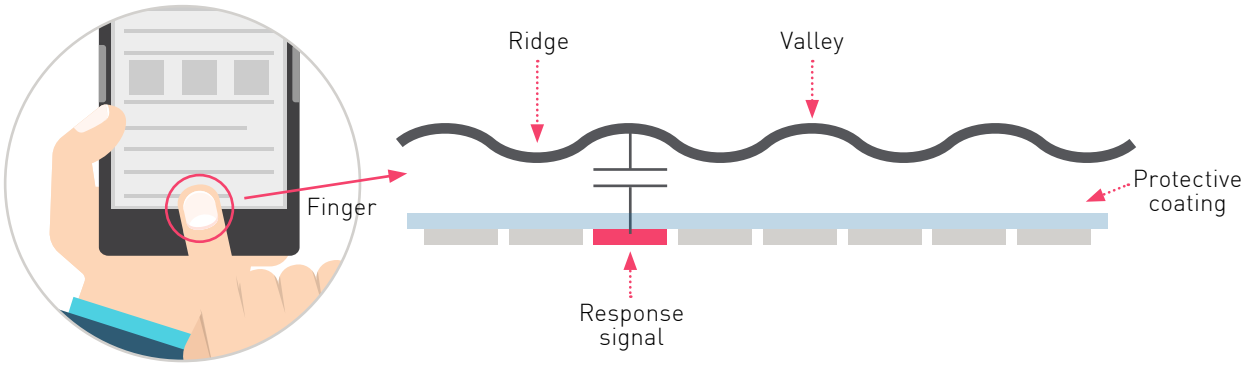


图 24. 电容传感原理：测得的电容随着指纹的脊和凹处而变化

你不能使用高质量的照片欺骗电容传感器，除非是真实的手指。电容式扫描仪传感器不产生像光学扫描仪那样的指纹图像中的脊和凹处的图像，而是产生一个复杂的电信号模式，对该电信号进行处理，以形成指纹的数字图像。由于电容式扫描仪需要人体手指的物理接触，以生成图像，因此比光学器件更难欺骗。电容感应指纹阅读器的另一个优点是其更紧凑，因此易于集成到便携式设备。

直接（被动式）电容测量

电容式传感器的表面是一个整齐的阵列板，能够测量这些板之间的电容和指纹图案。基于电荷可以直接进行测量，或通过对手指施加微弱的电信号。

被动式电容测量利用皮肤的导电特性，使电容与阵列板耦合。由于皮肤最外层的脊比凹处更接近传感器板，可以在板和存在脊的手指两者之间保留更多的电容，与该点的高电容流量保持一致。因此，手指上的谷和脊的图案被板电容复制，从而创建指纹的相应的图像。

被动电容式指纹传感器对静电放电（ESD）以及干燥和损伤的手指较敏感，但能很好地处理不同的光照条件。与主动电容指纹传感器相比，被动电容指纹传感器的一个主要障碍是其需要一层非常薄的涂层来捕捉指纹，因为它们依赖于手指和传感器之间的静态电荷。

有源（主动式）电容测量

主动式电容测量，有时称为射频、反射或感应电容测量，使用微弱的电信号，该电信号适用于电压测量前给皮肤提供电压。例如，通过放置在传感器阵列周围的导电挡板，可以给手指施加充电电压，如图25所示。

手指的充电发生在传感器的充电周期期间。在放电周期期间，将个别电容像素板的电荷和参考电荷做对比，并可以计算该电容。由于电容是依赖于电容像素板和表皮脊之间的距离，可以计算该距离，并用于形成指纹图像。

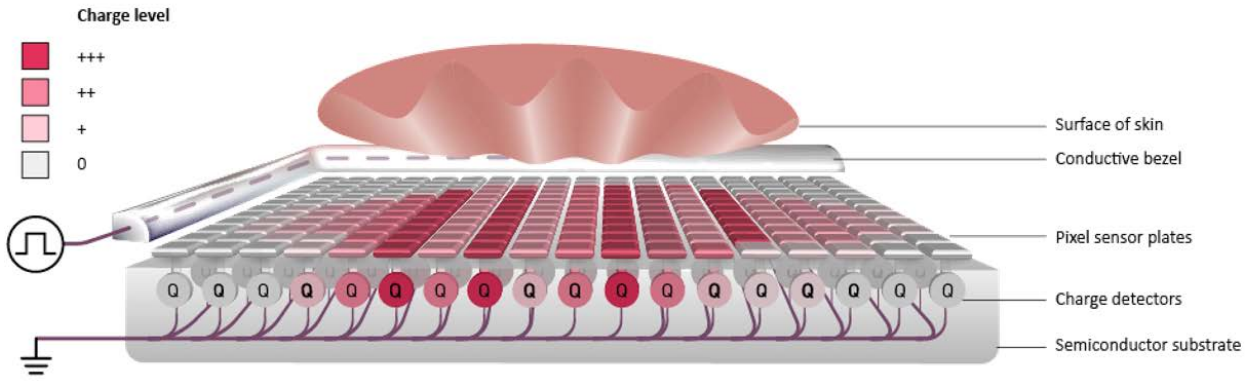


图 25. 配备给手指充电的有源挡板的有源电容测量

通过使用可以放置于相同半导体芯片作为传感器板的附加电路，可以根据不同的皮肤类型和条件，对传感器接收进行动态调整。这减少了清洁的需要，完好的皮肤表皮和干净的传感表面，从而使主动式电容测量是今天最常用的电容技术。

主动测量的另一个非常重要的优点，是加强了指纹表面与传感器板之间的信号通信，允许引入一个持久的保护涂层。

电容指纹传感器专用集成电路 (ASICs)

特定应用集成电路(ASIC)[8]可以产生电容测量的传感器。集成电路（IC，“芯片”）是一种半导体材料（硅），可见于成千上万的电子元件，如传感器板和晶体管，得到了建立并互相连接。尽管是高度复杂的产品，相对于以自动化光刻工艺蚀刻在硅晶片上的所有部件，集成电路的成本相对较小。

制造有源电容测量所需的专用集成电路时，最常见的技术应用是CMOS（互补金属氧化物半导体）。这种技术的一个固有优点，是可以将其用于同一芯片上的数字逻辑电路和模拟电路。由于CMOS技术的出现，因此，混合相同IC中的像素板和数字电路的模拟功能是可能的。

CMOS技术还具有两个对指纹传感器很重要的特性，即较高的抗噪声能力（在电信号中的随机变化小）和CMOS产生的数字电路静态功耗较低。其他用CMOS设计和制造的技术专用集成电路，包括数码相机的图像传感器和用于手机的微处理器。

由指纹传感器测量的信号是类似物[9]。从传感器输出到生物识别微处理器的必须是数字数据。在或接近传感器板矩阵时，必须有将模拟信号转换为数字格式的电路。然后发送给微处理器的数字数据是指纹图像。测量数千个甚至数万个电容像素板中每一个的距离，电容像素板以指纹图像像素灰度值表示。进一步处理数字图像，然后可以用于创建一个详细的指纹图像，甚至具有3D特性，如下图27所示，并捕捉特征点，这对于真实的识别和验证是必要的。

主动式电容传感器的封装替代方案

主动电容式指纹传感器封装方案主动电容式指纹传感器有许多形状和格式，以适应大量的应用。这项技术可用于各种尺寸的刷卡传感器和触摸传感器，其中较大的传感器能够读取整个指纹，而不仅仅是只读取部分指纹的区域传感器。

为了允许应用程序设计师在设计自己的产品时，拥有更多的自由度，传感器可用于不同的形状-矩形、椭圆形和方形，使传感器能够安装在侧面、前面或后面，例如移动设备。传感器也可以整合到其他设备的按钮，如果需要的话，还可以安装在保护性陶瓷或玻璃层下面。

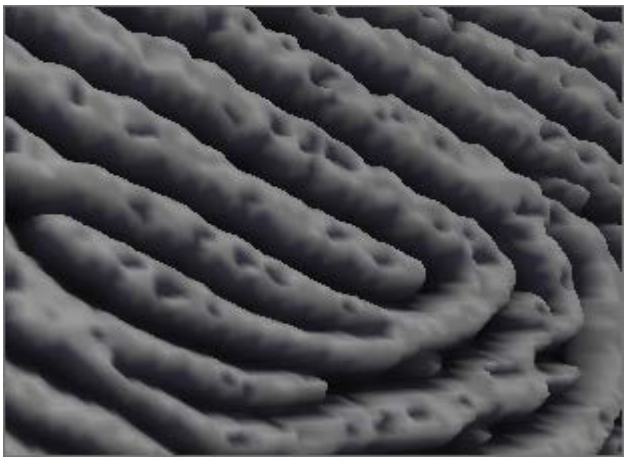


图 26. 3D 指纹图像

图 27. 不同封装的主动式电容传感器

8 *ASIC 是一种高度复杂度的硅基半导体电路。其他技术，如薄膜晶体管（TFT）和金属网格，也可用于创建电容式指纹传感器*

9 *模拟信号是一个连续变化的电信号，代表了其他一些随时间变化的量*

传感器通常是其他更复杂的产品的一部分，如手机、安全系统等。在制造过程中，允许传感器顺利有效地集成，主动式电容传感器能够以不同程度的精细度传递到模块供应商[10]和负责最终产品的 OEM[11] 。

- 制造晶片的模具/芯片/传感器尚未分离。传感器以晶片的形式出售，以防模块室内部存在自己的封装
- 封装传感器–不同类型的保护封装内的传感器，如栅格阵列（LGA），一种位于包装和可选定制涂层下面的矩阵焊盘封装技术。下面的焊盘将传感器连接到设备处理器上。准备好包装传感器，以用于模块集成，因为它们通常被出售给没有自己的包装设施的模块室
- 模块-传感器有一个完整的物理外壳，如挡板、框架等，已准备好直接将其集成到最终产品，例如移动电话
- 独立的嵌入式系统，传感器、包装、软件和生物微处理器都包含于一个完整的生物识别解决方案之中，可以嵌入不同的垂直式应用，如汽车和物联网

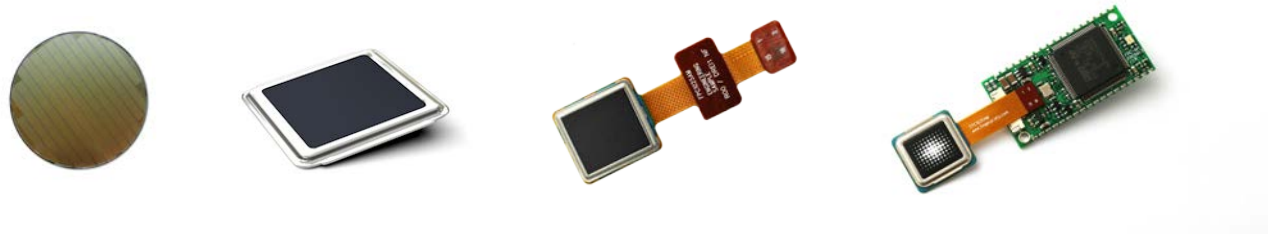


图 28. 晶片、LGA、模块和独立的嵌入式系统

主动电容式指纹传感器的优点

电容式传感器，特别是使用上述主动测量方法的电容式传感器，在许多应用中具有几个高价值的优点

+ **优异的图像质量** – 进行设计，以提供高质量图像，甚至使3D指纹绘制，提供卓越的安全性和反欺骗性
+ **活体检测** – 可以设置为只对活体组织起反应，进一步降低欺骗风险
+ **小型和紧凑型** – 可以很容易地集成于便携式产品，如手机和平板电脑
+ **最小的功耗** – 传感器ASIC应用的CMOS工艺，确保满足超低功耗的要求，在移动应用中得到了更进一步应用
+ **快速** – 使用有源电容式触式传感器，可以一步实现指纹采集，减少手指在阅读物上的滑动
+ **耐用性和易于集成** – 不需要用手指直接接触传感器板。有源电容传感器可以放置于保护层或移动电话玻璃后面，尽可能地避免性能退化
+ **低成本** – 任何硅基传感器芯片的成本与大小密切相关。由于有源电容传感器可以制作得较小，也可以以较低价格进行大量生产

10 模块的供应商是一家将多个电子元件

11 原始设备制造商是一家生产最终产品的公司，或另外一家公司的最终产品的子系统

主动式电容传感器没有太多的缺点。静电放电（ESD）的敏感性，是所有类型的半导体集成电路普遍存在的问题，很早就被人们提及。此外，随着传感器的尺寸减小，注册和验证需要更加仔细，并使用最好的匹配算法，这些条件变得更为重要。这种先进的算法可能意味着额外的处理周期，从而增加了功率和性能要求的处理器。

4.2.3 超声波传感器

超声指纹传感器利用医学超声原理创建指纹视觉图像。与光学成像不同，超声波传感器使用非常高频的声波，以穿透皮肤的表皮层。使用压电[12]换能器产生声波，而且也是利用压电材料测量反射的能量。

Since the dermal skin layer exhibits the same characteristic pattern of the fingerprint, the reflected wave measurements can be used to form an image of the fingerprint. Using the dermal skin layer eliminates the need for clean, undamaged epidermal skin and a clean sensing surface. This makes the ultrasonic sensors good at reading wet and damaged fingers whilst also verifying the liveness of the finger. Dry fingers can often be a problem though, think about the gel that doctors put on bellies before taking an ultra sound scan to look at babies.

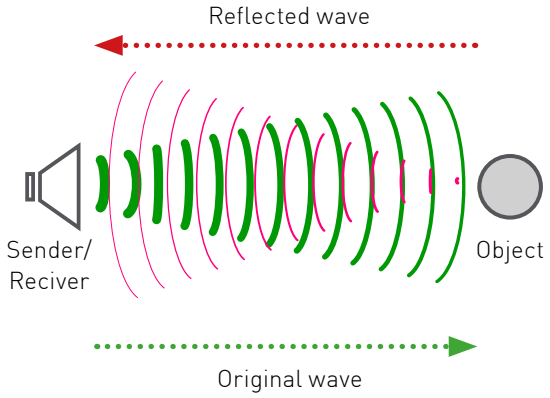


图29. 超声波指纹检测原理

超声波指纹传感器有一个优势，即其比大多数其他指纹传感器提供更多生物信息。之前一直存在的技术问题，在很大程度上仍然存在，它缓慢、昂贵的、功耗大、体积大（大传感器），由于具有大量的数据，它需要强大的算法处理能力。

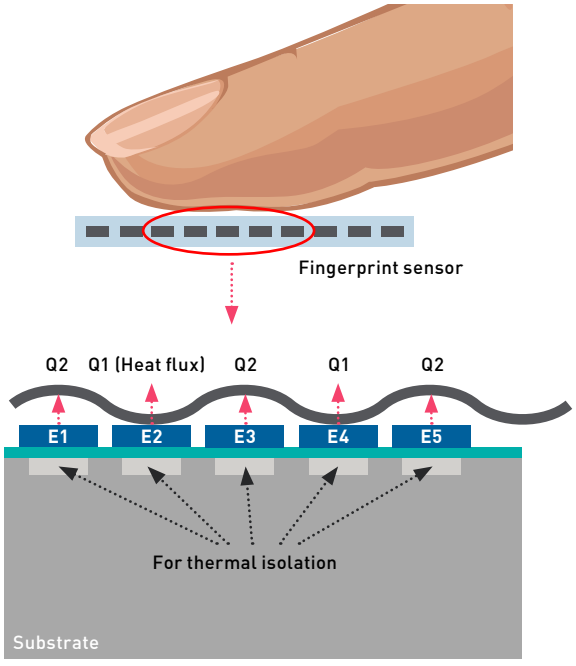
4.2.4 热传感器和主动式热传感器

热指纹传感器使用温度测量来创建指纹图像。传感器采用的热电材料阵列板的类型和和红外摄像机相同。当手指接触传感器时，手指的脊就会接触传感器表面，进行温度测量。然后基于脊皮肤温度和谷周围温度创建指纹图像。

热指纹传感器存在一些主要问题：

- 温度变化是动态的，因此，指纹图像是瞬时的，当传感器表面达到和手指同样的温度时，约十分之一秒后消失
- 容易磨损和污染
- 当周围温度接近手指表面的温度时，需要加热传感器，使得至少存在1摄氏度的温差，否则不能正确测量温度差，不能创建指纹图像

上述一些问题可以用有源热传感器进行解决。当手指稳定地放置在传感器表面时，主动热传感器向每个传感器像素发送低功率热脉冲。热脉冲打破了热平衡，从而静态采集指纹图像。



E1, E2,E3, E4 and E5: arrayed heater elements

图 30. 主动热指纹检测原理

12 压电效应是指由于施加机械应力，导致某些固体材料中积聚电荷。它也指对电荷起机械反应的材料。

然而，主动热技术也有其缺点：

- 高功率要求
- 没有能力捕捉细节，例如汗毛孔，因此需要更大的传感器面积
- 无法创建 3D 图像

4.2.5 压力敏感传感器

一种新兴的指纹传感器类型，是基于对其施加机械应力时，能够产生电信号的薄膜材料。传感器表面作为一个非常薄的和灵活的非导电电介质材料来应用。当手指放置在传感器上时，脊和谷对表面施加不同程度的压力，从而导致不同数量的电流，可以对其进行测量并用于生成指纹图像。

压力灵敏度传感器可以做得很小，而且是电容传感器以外，为数不多的可以集成于移动设备（如手机和平板电脑）的传感器类别。然而，现有的传感器是温度敏感性的，不太适合使用于恶劣的或迅速变化的环境条件。即使有，目前也只有少数认证的压力敏感性传感器用于商业用途。

4.3 指纹传感器的技术比较

在选择合适的指纹传感器技术和物理传感器用于某些产品、应用或过程中时，需要考虑非常多的因素。技术的选择将取决于性能参数，如图像质量、速度和功耗。当设计“真正的”产品时，需要更多的参数，如传感器的大小、成本和包装选项同样也必须考虑在内。

在本节中，我们将讨论一些最重要的因素，以选择最佳的指纹传感器技术和传感器。

4.3.1 图像质量和分辨率

指纹传感器产生的图像质量是一个基本的重要参数。高图像质量使得传感器更小，成本更低，因为每个区域单元可以捕获更多的细节。图像质量取决于传感器的检测微弱信号的能力，并过滤掉多余的噪声，最好不需要“曝光”太长和繁琐的指纹。图像质量可以用不同的方式来衡量，但在指纹识别系统中，一个常见的衡量是注册失败（FTE）参数。FTE比简单给出传感器无法充分读取生物标识，继续处理和用户注册的百分比。扫描指纹时或外部不存在语言识别系统时，可能会导致失败，例如潮湿的或破损的皮肤。通常使用的另一个指标，是指定了传感器分辨率的每英寸点（DPI）。无法捕获低分辨率（低DPI值）的细节，从而降低了图像质量。

目前，非常高的图像质量可以通过超声波和有源电容传感器读取皮肤层获得，和外表皮层相比，这明显得多，而且不容易变形。在主动式电容传感器中，每个像素单元都有其自身的电子电路，相同的ASIC，提高了灵敏度，显著降低了多余噪音进入的风险。

目前，有源电容传感器的正常分辨率是508 DPI，这也符合美国ANSI / NIST规范。

4.3.2 速度

指纹系统运行的速度对其使用便利性有很大的影响。在ASIC上的电子电路进行的数字转换类似物，以及指纹认证所涉及的计算，需要有效的，以实现高速传感器。以简约的方式来编写算法，对实现所需的性能是很重要的。

在使用专用的生物识别处理器的应用程序中，硬件执行算法中的计算密集型部分，可以使认证过程变得非常快速和准确。对于其算法在主处理器如移动电话中运行的应用来说，高效的算法对于快速认证是很重要的。

传感器系统的速度也取决于系统是否执行身份验证（1:1）或识别（1：N）。由于验证只需要对捕获的图像与存储模板进行比较，比识别系统生成的结果更快。然而，另一个决定系统速度的因素是让传感器准备好读取的时间。

以电容、热和压力为基础的传感器，都可以实现非常高的运行速度。目前，这样的传感器的启动和验证的时间，可以低于500ms。

4.3.3 功耗

传感器系统的功耗是一个非常重要的因素，并对很多应用起着重要的作用，如移动电话、智能卡和其他便携式设备。设备的电池不仅是高消耗功率的，也产生热量，这可能会损坏或干扰设备中的其他元件。

随着时间的推移，考虑传感器的功率要求是必要的，例如在一个给定的应用程序中，传感器实际消耗的能量。例如，在移动电话中，传感器每天可以活动大约20次左右，而在24小时中的剩余的时间，则保持空闲。很明显，它是备用（静态）的功率消耗，而不是激活传感器的功耗，这对电池寿命的影响是最大的。

功耗取决于传感器系统的硬件和软件。CMOS传感器通常具有低功耗，因为只有其晶体管处于开关状态时，也就是说，当它们被用来扫描手指时，消耗的功率才比较明显。此外，传感器的大小也影响功耗，较小的传感器消耗更少的功率。此外，传感器的详细的电气设计可以严重影响功耗。

即使一个较小的传感器具有较低的能量消耗，从硬件的角度来看，一个较小的传感器通常具有较少的电容性像素板，因此只能捕获图像中手指的一个较小区域。对于较小的图像，提供足够的注册和认证的细节，更高的图像质量和更先进的算法是必要的。更高质量的图像和更先进的算法都可能会导致更高的功耗，因为它需要更多的处理能力。这种效果可以降低较小的传感器的功耗，因此，非常有效的算法以产生指纹图像以及认证，是非常重要的。

目前，电容式传感器拥有市场上现有的最低功耗的传感器技术。光学、超声波和热传感器都需要更高的功率，因此不太适合移动应用。

有源电容传感器的典型功耗为5μA（休眠时）和20毫安（使用时）。

4.3.4 尺寸

选择指纹传感器，特别是移动应用时，尺寸或相当小的尺寸往往是一个决定性的参数。手机、平板电脑或相机所需的能够容纳所有组件的空间是有限的，设备的外部可能已经被屏幕、其他按钮和拨号所填充。塑造所需的产品时，使用允许额外的设计选项的小尺寸传感器时，较小的传感器也有较高的传感器的成本效益，仅仅是因为较小的ASIC使用更少的硅，因此可以便宜。

然而，有一个在指纹识别应用程序的大小和图像质量之间的权衡。使用过小的传感器，分辨率太低，会导致图像质量差，这反而需要更先进的和功耗匹配的算法，或者甚至不可能安全注册和认证。.

有源电容传感器的尺寸通常为84×84毫米到160×160毫米，可以是圆形、矩形或任何其他产品设计师所需的二维格式。

4.3.5 成本

不用说，成本是选择传感器系统时的一个重要因素。在推动指纹识别在廉价手机、智能卡和其它需要低成本组件的大体积片段中的应用中，成本越来越重要。

有源电容式指纹传感器的成本是硅基，与传感器的尺寸高度相关，因为材料是主要的成本来源。成本也受到生产过程、系统集成和技术的影响。

4.3.6 包装和其它设计方案

指纹传感器需要纳入最终产品，但不限制原产品的设计，而是辅助和提高其功能。智能手机制造商不仅在功能上同时也在设计上相互竞争。汽车制造商不愿意在车内设计上妥协，想要一个平顺与车辆内部相结合的传感器。入口控制系统中的传感器需要经历无数次的使用周期，而且常常是恶劣的天气条件。

要符合上述设计要求，传感器的包装和保护涂层变得非常重要。有源电容技术的最大优点之一，是它能通过玻璃和其他用于最终产品封装的材料来捕捉指纹。然而，对于一个能够通过400微米玻璃或彩色陶瓷捕捉指纹的传感器，它必须能够检测到非常微弱的信号。这需要在传感器内放大信号，先进的信号处理以及随后的匹配过程的高效的算法。

当将指纹传感器集成到最终产品时，一些其他特性也变得重要。传感器必须具有物理、电气和逻辑接口，可以填入产品日期。如果匹配算法应在专用的生物量处理器或产品的主处理器内运行，必须做出选择。如果使用了一个主机处理器，传感器供应商是否应为相关的操作系统提供算法，他们是否可以在受保护的环境中运行，并且可以对关键数据进行加密，只是提到一些重要的设计参数。

4.3.7 安全和便利

我们谈到了自动认证系统的安全和便利因素，以及如何在2.3节中测量，我们还定义了容错率（FAR）和拒错率（FRR）指标。这是直观清晰的，安全和方便之间是有关系的：认证必须要做到更安全（可靠），就需要对数据进行更多的采集和分析，这就需要对被认证的人停留更多的时间并配合，因此更感到不方便。

根据传感器的能力，例如，图像处理和匹配算法，不同指纹识别技术显示不同的FRR与FRR曲线。像往常一样，有一个成本（在这种情况下是尺寸）和能力之间的权衡， 以及FRR与FAR曲线。然而，当一个先进的主动式电容传感器和合适的相应的算法结合时，可以实现FAR低至1 / 100 000，但仍保持一个只有1%的FRR，移动设备中的小传感器同样如此。这使得有源电容传感器即便不是最方便的技术，至少也是今天最便利的传感器技术之一。

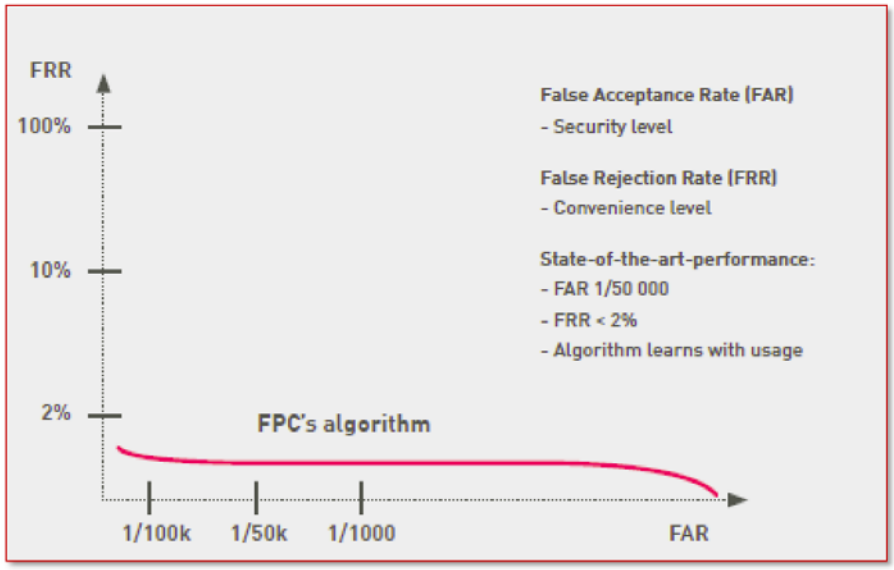


图 31. 一种先进的主动电容式指纹传感器的典型FRR与FAR曲线（DET曲线，检测错误权衡曲线）

4.3.8 结论

市场上多种指纹技术的可用性表明，没有一种技术适用于每一个应用程序。根据成本、功率效率、大小、便利性和其他特性的要求，一个特定的传感器类型可能是一个特定应用程序的最优选择。然而，放眼整个市场，我们发现有源电容技术有一系列吸引人的特点，使其成为大多数应用中的首选。

2016年4月，分析公司Redeye发表了一份研究报告，即《中国就在你的手中》。研究报告根据几个性能标准，对这几个指纹识别技术进行了比较。从下表中可以看出，有源电容技术在大多数类别中得分非常高，具有广泛的适用性。

指纹技术比较

	主动电容式	电容式	超声波	光学式	主动式热
成本效益	High	Medium	Low	Medium	Medium
设计弹性	Very high	Low	High	Low	Low
技术成熟	Very high	Very high	High	Very high	Medium
安全性	High	Low	Very high	Low	Medium
便利性	Very high	Medium	Very high	Low	Low
耗电效益	Very high	High	Medium	Medium	Very low
移动设备适用	Very high	Very low	Low	Medium	Very low

Very high　High　Medium　Low　Very low

4.4 指纹提取与匹配

如前所述，注册和认证是任何生物认证系统中的两个关键操作。有了指纹识别，这两个操作可以通过适当的支持措施，如机械指导，帮助用户正确地把手指上放置于传感器和和智能的用户界面，使用户更方便地通过注册过程。如果指纹传感器是没有自己的I / O功能的实体，如信用卡，必须支持其它功能，如智能手机的近场通信（NFC）。

由传感器捕获的指纹图像是一个单色数字图像，例如由一个数码相机所产生的相同类型的图像，但只包含一个指纹灰度图像。为了使登记和随后的匹配捕获的图像成为可能，必须在可以提取指纹特征并在匹配过程中使用之前，首先增强预处理步骤。图像处理、特征提取和匹配通常称为指纹识别算法。

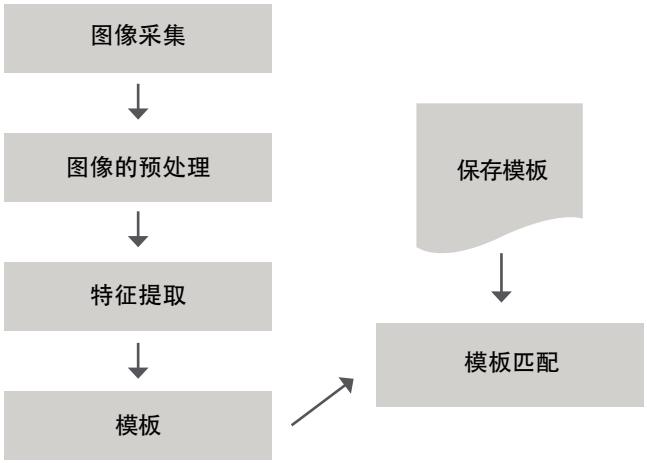


图 33. 指纹识别算法

4.4.1 预处理、特征提取和模板

通常情况下，原始灰度指纹图像有一个8位的位深度，根据传感器尺寸，每个这样的图像需要几兆字节的存储。无损或不可逆的压缩方法，如JPEG，可以通过10个因素中的一个或更多的因素来压缩图像，但每个图像仍会占用一些内存空间。这就是用于匹配的为什么是指纹的特征，而不是完整图片的原因之一；需要使用完整的图像时，数字化功能只需要更少的存储空间，更重要的是，应该需要不太复杂的匹配算法。

分析的第一步，是利用图像处理技术获得尽可能清晰的指纹图像。对于灰度图像，这可以通过丢弃比阈值轻的区域来实现，而那些比阈值较重的区域以黑色表示。或许也应用了其它基于指纹脊线方向和频率的增强算法，产生了极高对比度的指纹图像。

当使用基于特征点的匹配时，下一个步骤是识别和定位这些特征点。例如，脊结束点和一个分叉开始形成特征点的点。一旦一个特征点被确定，就注册该位置，作为与中心点的距离（中心）。除了布局特征点，通常还要登记特征点角度。例如，当一个脊结束时，它的方向为建立角度的终止点。

除了使用位置和特征点角度，可以根据特征点的类型和特征对其进行分类。这种分类的好处是，可以更快地搜索，作为一个特别显著的特征点，足以进行匹配。

伤痕、汗水或灰尘引起的异常现象，表现为错误的特征点，而定位任何点或图案的算法没有意义，比如孤立点上的脊，或相互交叉垂直的脊（可能是瘢痕或污垢）。在此过程中，将丢弃了很大一部分特征点。

认证系统匹配的准确度，依赖于随着时间的推移，与个人相关联的生物识别数据的稳定性。如果我现在的指纹看起来不像注册时的指纹，我将无法通过认证。

原始的

增强的

图 34. 原始的和增强的指纹图像

从个体身上所获得的生物认证数据是很容易发生改变的，这是由于与传感器错误的相互作用（例如，部分指纹）、传感器特性的修改（例如，优化指纹传感器与固态指纹传感器）、环境因素的变化（例如，天气干燥致使指纹不清晰）和生物自身性状临时改变（例如，指纹削减/疤痕）。因此，存储模板数据明显不同于认证过程中所获得的指纹是有可能的， 从而导致生物认证系统性能较差（错误拒绝数量较多）。

克服同一个体不同指纹这个问题的方法，是将模板数据库中相同的指纹存储于多个模板。例如，可以存储用户指纹的不同部分，以应付用户以不同方式将手指放在传感器上的事实。然而，需权衡使用和储存的模板数量，以及多个模板之间的计算要求。

4.4.2 匹配

基于特征点的算法

自动特征点检测是一个复杂的过程，特别是低质量的指纹，噪声和对比度不足，可以产生类似于特征点的原始像素聚合，隐藏的真正特征点。成功的匹配，需要已小心提取的指纹特征，可以发现具有匹配特性的模板，这样的匹配算法可以图像的特征点和模板上特征点进行有效比较。

非特征点基础算法

非特征点基础算法，例如各种替代算法，比较先前存储的模板和候选指纹之间的基本指纹模式（拱形、螺纹形和环形）。这通常要求图像可以在同一方向对齐。要做到这一点，该算法需要在指纹图像中找到一个中心点，并集中于此。在非特征点基础算法中，模板包含对齐指纹图像中模式的类型、大小和方向。将候选指纹图像与模板进行比较，以确定它们匹配的程度。

4.4.3 生物处理器

指纹识别算法的执行需要数字处理能力和存储空间。在一些应用程序中，有它们自己的强大处理器，如移动电话，这些算法可以由作为主机处理器的主处理器执行。其他应用程序，例如门锁和读卡器，在直接与指纹传感器交互的产品中没有主机处理器，因此需要一个专用的生物识别处理器，作为解决方案的一部分。

生物处理器是数字ASIC，专门用于生物认证。处理器运行相关的提取和匹配算法，以进行注册、识别和验证。由于在许多应用中，功耗和尺寸是重要的，生物识别处理器必须较小，并具有功率效率。然后通过标准接口将生物处理器连接到产品的主处理器，比如串行端口，通过这种方式执行命令并输出结果。

5. Summary

生物认证是众多方式中识别和验证人类的理想方式。生物传感器安全度很高，同时也很快速和易于使用–生物认证始终伴随着用户，不会忘记携带或留在家里。各种生物识别中（模式），指纹识别有若干优点，因此其首当其冲，驱动消费者使用和接受生物认证，例如移动设备如智能手机。

指纹识别依赖于手指外部皮肤上的脊和谷的独特模式，这种模式通常在人的一生中保持不变。可以通过各种方法读取指纹模式，如光学、电容和超声波，其中有源电容技术已被证明在大众市场设备中，是最可靠且具有成本效益的技术。由于体积小、功耗低和包装高灵活性，主动式电容传感器可以很容易集成于其他产品，例如电脑、智能卡、物联网。

高效指纹识别的一个重要元素，是提取算法和指纹图像的匹配。对最佳算法选择影响着传感器使用的便利性以及处理器进行匹配时所消耗的功率。

Fingerprints™是一家公开上市的公司，提供全系列用户友好指纹生物识别解决方案。该解决方案满足了终端用户体验和工业设计过程中的最高要求。硬件包括传感器和完整的模块。并与软件相结合，提高用户体验，为Fingerprints™的用户提供差异化的多种可能性。

关于 Fingerprints™ 的更多信息，请访问： **https://www. ingerprints.com/**

O

P

R

S

T

U

V,W