
基于单片机和指纹识别技术的物联网智能门禁的设计

目 录

摘 要	I
1. 绪论	1
1.1 门禁系统的概述	1
1.2 门禁系统的研究现状	2
1.3 课题的主要研究内容	3
2. 系统的总体设计	4
2.1 指纹识别技术原理简介	4
2.2 指纹图像的预处理	5
2.3 指纹图像特征点的提取	7
2.4 指纹图像特征匹配	7
3. 硬件部分的设计	8
3.1 系统硬件设计方案	8
3.2 指纹录入模块	9
3.3 STM32 单片机模块	11
3.4 显示电路模块	11
3.5 报警电路模块	12
3.6 串口电路模块	13
4. 系统软件设计	14
4.1 指纹识别部分的主程序设计	14
4.2 蓝牙控制系统的设计	15
5. 设计实物的测试	17
6. 总结与展望	18
参考文献	19

1. 绪论

1.1 门禁系统的概述

门禁系统是实现未来建筑的智能化设计的必要部分。这里介绍的门禁系统并不是指传统意义上的门，它更广泛地拓展为一种通道，不仅限制人也用于限制车辆等。门禁控制器是一个完整门禁系统中最重要的一部分，系统中输入信息、输出信息数据的处理、存储以及状态控制都由它负责；门禁前端通过各类读卡器和生物识别仪器作为识别设备，同时也承担对用户身份信息信息采集的工作。门禁的具体执行要靠锁具来实现，通常选择是要考虑到自身需求和应用场所。最能体现门禁智能化的地方就是管理软件，通过一台电脑进行集中化管理和监控，可以自定义识别方式，将出入信息存档管理，开拓其他功能。还有一些其它的相关设备，包括出门按钮，卡片，电源，交换器 HUB 等^[1]。

当前，按照我国门禁系统广泛采用的三种识别方式和技术原理进行分类，门禁系统可以粗略分为以下三类：

（1）密码式门禁系统：这类门禁系统只需要通过使用者设置独特的一串数字，通过判断输入的数字密码与初始设置数字密码是否相同来控制门锁上的开关。密码门禁系统安装成本低，操作非常方便，对使用场合、操作流程要求低。但是其安全性较低，密码设置过于简单会导致密码泄露，密码设置过于繁琐则容易忘记。

（2）刷卡门禁系统：这类门禁所使用的卡片大致被分为接触式刷卡和非接触式刷卡两种。其中接触式卡片现仍广泛应用于高校图书馆，宿舍门禁等场合。接触卡式门禁卡片与传统钥匙一样容易丢失，而且更容易损坏，由于此类卡片所带信息太多，丢失后造成不良后果的可能性较大。非接触式门禁 IC 卡系统克服掉了其他接触式卡系统容易出现磨损失效和密码丢失问题的等种种技术缺点，同时还具有体积小、读取速度快和卡片信息不会被盗取从而将其安全性大大提高等多种优势，逐渐成为当前智能卡门禁系统的主流。

（3）生物识别门禁系统：这类门禁利用人本身所拥有的身体特征独特之处来建立生物信息数据，通过这些数据反过来确立身份。现如今，应用于日常生活中比较常见的生物特征有指纹，面部和虹膜等等。面部与虹膜用到的技术对各方面要求都比较严格，面部易于通过装饰改变而造成识别混乱。指纹利用每个人手指纹路形状走向不同来区分身份，不随年龄和身体形态改变。这种门禁系统的识别介质来自使用者自身，无需特地携带和记忆，安全性非常高，非人为故意伪造情况下的重复几率非常低。

^[1]杨晶晶. 基于 STM32 的智能门禁系统的设计[D]. 华北理工大学, 2019.

1.2 门禁系统的研究现状

我国在 90 年代初期开始使用指纹技术实现识别功能。从 2000 年开始供求关系发生巨大的变化，随之而来的相关技术、工具器件和处理方法等一系列相关共性技术成果以及衍生产品得以发展壮大，这项技术获得突破的同时也日益蓬勃，发展道路逐渐产业化。尽管如此，产品种类依然比较单一，应用场合不够广泛。从 2004 年以后，随着手机、电脑和储存设备的迅猛发展，指纹识别技术才开始进入综合发展的阶段^[2]。

随着物联网技术和各类识别技术以及大众对门禁的安全性和智能性的要求的提高，市场中现有的门禁系统种类已经非常丰富了。其中常见的生物识别特征技术有人脸、指纹、掌形、掌纹、虹膜以及语言识别等等。应用场合也从公共图书馆，安全性要求高的研究所，电力变电站等场合应用到普通住户家中。

生物特征识别技术可通过以下几个特点来评判^[3]：

- (1) 广泛性，该生物特征是否可以应用于大众场合。
- (2) 独特性，该生物特征与其他个体相似程度。
- (3) 持久性，该生物特征是否随年龄改变。
- (4) 采集性，该生物特征所需采集技术与场所是否易于实现。
- (5) 性能，该生物特征的精度等性能。
- (6) 接受性，该生物特征作为工具被使用时，大众接纳的接纳程度。
- (7) 防伪性，该生物特征是否易于伪造。

表 1-1 为五种市面常见的身份鉴定方式在上文中列举的几点参数方面的比较。

表 1-1：生物特征参数比较

鉴定方式 ^⓪	广泛性 ^⓪	独特性 ^⓪	持久性 ^⓪	采集性 ^⓪	性能 ^⓪	接受性 ^⓪	防伪性 ^⓪
人脸 ^⓪	H ^⓪	L ^⓪	M ^⓪	H ^⓪	L ^⓪	H ^⓪	H ^⓪
指纹 ^⓪	M ^⓪	H ^⓪	H ^⓪	M ^⓪	H ^⓪	M ^⓪	L ^⓪
掌形 ^⓪	M ^⓪	M ^⓪	M ^⓪	H ^⓪	M ^⓪	M ^⓪	M ^⓪
掌纹 ^⓪	M ^⓪	M ^⓪	M ^⓪	M ^⓪	M ^⓪	M ^⓪	H ^⓪
虹膜 ^⓪	H ^⓪	H ^⓪	H ^⓪	M ^⓪	H ^⓪	L ^⓪	H ^⓪

^[2] 王莹. 基于指纹识别技术的智能门禁系统的设计[D]. 天津科技大学, 2014.

^[3] 刘倩颖, 刘季. 生物特征识别技术在身份验证领域发展趋势[J]. 电子世界, 2020 (05) :23-24.

对上文中的生物识别特征技术的优劣性进行比较, 得到结论: 人脸识别的独特性与性能较低, 虹膜识别的接受性低, 语音识别的独特性、持久性以及防伪性低, 掌纹识别和指纹识别这两种识别方式的持久性、独特性、采集性、接受性、防伪性均没有大的弊端和缺点, 同时也没有大的亮点。对于需要应用在大多数场合, 被大多数人使用的系统, 采用指纹识别更易于实现。

采用指纹技术也有一些弊端, 由于手指摩擦指纹磨损, 沾上污染物无法识别指纹或手指受伤等情况时均无法通过指纹识别打开门禁。这时通过物联网技术, 附加手机 APP 控制门禁系统, 采用高性能的无线收发传输系统 HC-06 蓝牙模块, 实现对手机终端发送信息的采集^[4]。作为指纹无法使用时的备用选择。物联网通过将物体信息转化为数字信息, 建立联系实现识别和管理的功能。本设计将指纹识别与物联网结合起来, 改善了传统防盗锁安全系数相对较低的问题, 同时提高了门禁的性能。

1.3 课题的主要研究内容

本课题采用生物识别系统中应用较为广泛, 实现较为简单的指纹识别, 同时考虑到指纹识别无法使用的常见情况, 结合物联网技术, 实现双重保障。本论文分为六个部分来阐述设计, 将各章节核心内容简要概括如下:

第一章(绪论): 主要介绍课题研究背景及意义, 概括传统门禁的弊端, 阐述生物识别技术为门禁系统带来的便利, 提出物联网技术的加入对指纹门禁的完善与提高, 并列举了本文所做的工作。

第二章(系统的总体设计): 通过介绍指纹识别技术的原理, 阐述指纹信息的提取、处理和比对方法。

第三章(硬件部分的设计): 本章介绍了该系统的硬件部分, 内容包括 STM32 单片机模块, 指纹录入识别模块, LCD1602 显示模块, 晶振电路报警模块以及蓝牙串口模块。

第四章(软件部分的设计): 大致分为指纹识别与蓝牙控制两个部分。

第五章(设计实物的调试): 对实物电路板的个功能进行测试观察, 总结系统的功能。

第六章(总结与展望): 对整个设计系统的设计思路进行总结, 逐条展示各部分功能的实现, 最后根据现有技术反思本设计的不足, 列举提高点。

^[4] 徐富强, 卢闻州, 熊化亮, 孙英伦, 杨欢, 屈笑. 基于物联网技术的新型智能门锁设计与实现[J]. 物联网技术, 2017, 7(08): 65-68+71.

2. 系统的总体设计

本设计中的门禁系统主要实现途径是通过指纹特征识别技术，附加蓝牙功能实现手机控制手段。指纹识别技术的途径，所使用采集的指纹采集工具以及指纹处理算法和流程都影响门禁系统的可靠性和使用性能。下文将通过分析指纹识别技术的基本原理、指纹图像的处理流程、指纹的匹配原则来介绍本系统的实现过程。

2.1 指纹识别技术原理简介

人类的皮肤纹路在形状、走向和结构具有或大或小的差异，其中指纹就表现为独特的和终生不变这两个关键的特点，将一个人的身份信息唯一确定且长久有效，一份指纹信息代表一个人的身份证据，将采集的指纹信息与留存的信息比对，用来鉴别身份。广泛应用于警察部门对各类犯罪违法嫌疑人身份的精确锁定，智能手机开机，门禁系统身份的认证等等^[5]。

采用指纹识别控制门禁系统是众多生物特征识别技术门禁系统中应用得最广泛、价格也相对最低廉的、操作起来也很简便的一种门禁类型。指纹锁识别指纹主要通过指纹图像获取、预处理获取的图像、提取纹线信息、标记并提取细节特征、保存提取数据并算法比对^[6]。通过指纹技术识别身份大致可以分为指纹信息的采集，对采集图像进行一系列的操作程序，从而获得一个符合检测标准的图像，具体分为五个步骤，如图 2-1 所示。

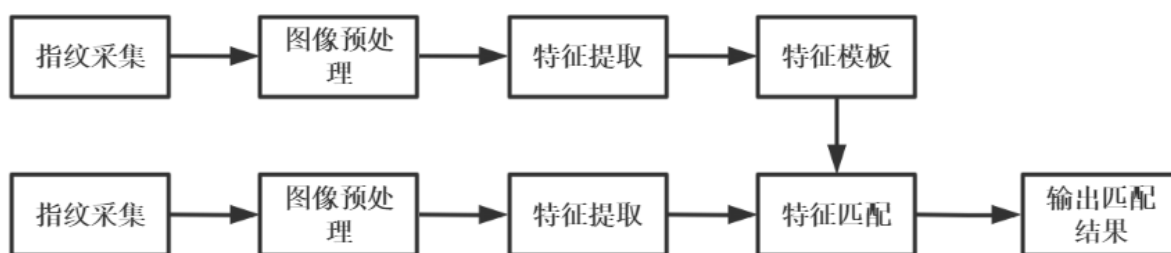


图 2-1. 指纹识别过程

^[5] 李颖. 基于半监督学习的指纹识别方法研究[D]. 山东大学, 2013.

^[6] 田师思. 指纹锁的发展研究[J]. 科学技术创新, 2020(12):81-82.

2.2 指纹图像的预处理

指纹图像预处理是为了帮助加强图像清晰度，得到满足后续提取和匹配工作所需要的标准快速准确识别指纹信息。由于采集指纹会受到外界静电干扰导致图像明暗度不符合要求，或手指沾有汗渍灰尘使得指纹模糊不清，又或手指接触传感器不均压力过小出现纹路断裂不完整的情况。这个过程就是要处理噪音污染产生的影响、图案残缺获取不完整、甚至无法识别等问题。此环节通常包含对图像进行去噪处理、增强可识别性、增强清晰度等部分，对于应用场景的差异，对指纹图像有高低不同的质量要求，考虑到处理过程的经济高效不同情况下的预处理过程可适当改变。

通过对原图像进行均衡化、分割、平滑、增强、二值化、细化等算法处理，尽量还原指纹最完整的形态，获取尽可能多的有效识别信息，提高识别结果的效率和准确率^[7]。

1) 均衡化

在一幅指纹图像中，不同的像素点拥有不同的灰度级，而且拥有不同的灰度级点的像素数量灰度分布都不十分均匀。均衡化个数通常用一个直方图来表示，根据这个直方图所得函数关系并结合有关概率论知识，将初始数据中所得像素值多的灰度级扩充，相应的如果灰度个数少，灰度级将变窄。经过均衡化处理后形成的指纹图像，灰度值随概率变化分布而变得更为均匀，同时使图像灰度级次的可取值的范围又得到较大扩展，原始图像中的谷线和脊线对比度增强，从而图像的清晰度得以增强。

2) 分割处理

采集过程中诸多因素的影响，图像出现部分区域清晰而部分区域模糊的差别，将这两种差异称为前景区和背景区。其中前景区即图像清晰区，具有较深的颜色和较低的灰度值，呈现的是指纹的纹线信息，比如显示指纹的断续、形状、反应指纹的结构。背景区即图像模糊区，其颜色较淡，但是灰度值较高，是一些无关的数字信息，对后续的信息处理有不利影响。

基于指纹的梯度和灰度特性，可以通过分别确定一个灰度阈值和一个梯度阈值来分隔区域。灰度分隔阈值的确定：将指纹图像的相关数据用直方图来表示，可以直观地看出前景和背景呈现出峰值与谷值，两个峰值分别表示前景与背景的中心灰度值，观察发现存在一个低谷处在俩峰值间，该低谷处即为前景和背景图像的分界点^[8]

^[7] 杨磊. 基于 STM32 的指纹识别系统设计[D].杭州电子科技大学,2012.

^[8] 杨磊,张文超,秦会斌.基于 STM32 的指纹识别系统设计与实现[J].机电工程,2011,28(12):1531-1535.

。指纹的形状纹路在灰度图像上呈现为黑白相间的图像，通过两种颜色差异来反映脊谷的变化。前景区反应的是指纹的主要识别信息，具有相对比较明显的黑白区域间隔，也具有相对较大范围的梯度值，相对的背景区就没有显示出此特点，根据这一差异，选择合适的梯度分隔值后就基本可以完成图像的分割部分。

3) 平滑处理

图像平滑处理的目的是为了消除由于采集中灰尘、污渍粘附于手指和采集仪器表面给图像带来的噪声干扰。通常采用领域平均法，通过对大量像素点的灰度值求平均值来消去噪声。进行平均计算的图像面积越大，选取的像素点越多，得到的像素值越多，去噪声的效果也就越好，但是不能只为了满足去噪效果而盲目增大面积，面积的增大会导致清晰度不足，所以需要充分考虑清晰的和去噪效果再确定面积，才能达到一个去噪与清晰的结果。

4) 滤波增强

图像增强是预处理过程中不可缺少的环节之一，能够加强图像的可识别性，消除指纹采集设备本身和用户操作产生的噪声干扰，同时对前期图像处理操作中无法解决和新产生的影响进行处理。通过滤波增强的指纹图像能够提高黑白对比度，即呈现白色的谷线更白，呈现黑色的脊线变得更黑。另一方面，图像中指纹断裂处和纹线模糊松散处也得到弥补和收敛增强。

通过小波函数可在该位置方向场上对图像进行增强,以实现及时的弥补指纹图像中纹线之间发生的断裂情况,在垂直方向上,函数正好符合指纹纹线相间的特点,对纹线进行振荡增强^[9]。

5) 二值化

二值化即将图像中像素点的灰度值转化成两个值0和255,这样可以使得指纹图像中本来显现为黑色的脊线区域更黑,显示为白色的谷线区域更白。各灰度值需要确立一个值,以此为阈值由此将原本灰色的指纹图像彻底变成黑白两色图。这个灰度固定的阈值可通过先将指纹图像中的所有灰度像素点数值取的平均值来得到,再逐一将其中每一个灰度像素点位的灰度值与该灰度固定的阈值来逐一比对。若灰度值小于阈值,则可以直接用灰度0值来表示,认为该灰度点即为纹线部分;若灰度值大于阈值,则用255表示,认为该点为非纹线部分。

6) 细化

^[9] 樊相奎. 指纹识别在智能门禁系统的研究与应用[D].四川师范大学,2010.

采集的指纹图像中通常存在伪特征点，主要是毛刺、短棒、断线和小孔等，这些伪特征点作为冗余信息，为后续工作带来很大的干扰。通过细化处理，多像素宽纹线变为单像素宽纹线，由于经过细化操作处理的图像能够保持原本指纹纹线的连续性不变，保持纹线的位置不变还能保持纹线的结构特征，所以在满足提高信息处理速度的同时还能保证信息的准确性。

2.3 指纹图像特征点的提取

指纹的匹配工作建立在足够多的特征点相同证明确为同一幅指纹，指纹特征由纹路的起始位置、交叉分裂点以及汇聚点等组成，其中指纹的中心点和三角点相比较更容易获得。由于技术的局限性以及操作的不规范等一些难以避免的客观或主观原因，采集到的指纹数据往往与指纹本身存在或大或小的差异。除了采集过程中的问题，图像处理操作过程中，产生一些新增的数值偏差，为达到匹配条件，需要对伪特征值进行一系列的筛选和删除操作，保证获得的特征点达到识别数量且有效判别。

2.4 指纹图像特征匹配

指纹识别流程的最后关键一步就是特征匹配。经过特征提取操作后，用获得的指纹特征与特征模板相比较，若匹配度高于设定的阈值，则认为指纹识别成功^[10]。需要进行匹配的特征点有纹路大概粗略走向，还有指纹包括形态、端点和交叉点在内的各种细节特征具体流程如图 2-2 所示。

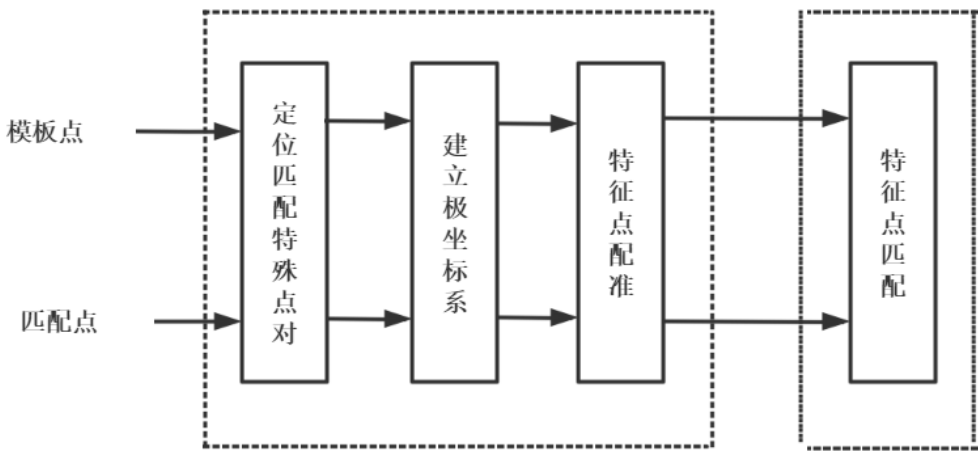


图 2-2. 指纹匹配具体流程

^[10] 袁进.智能门锁指纹识别方法设计[J].电子世界,2021(21):148-149.

3. 硬件部分的设计

本文从满足门禁系统最基本的安全的基础上，将门禁系统智能化发展作为主要目标。结合物联网技术和指纹识别技术两大热门的自动识别技术，利用指纹识别模块和蓝牙串口通信模块对门禁系统的整体设计提出如下设计构思：

- 1) 指纹作为钥匙，指纹匹配正确与否控制门的开关；
- 2) 手机作为钥匙，在手机界面操作直接控制门的开关。

3.1 系统硬件设计方案

本系统采用 STM32 单片机、光学指纹识别模块、蓝牙模块、按键模块、锁模块以及蜂鸣器模块来实现门禁的双重控制。基本实现框图如图 3-1 所示：

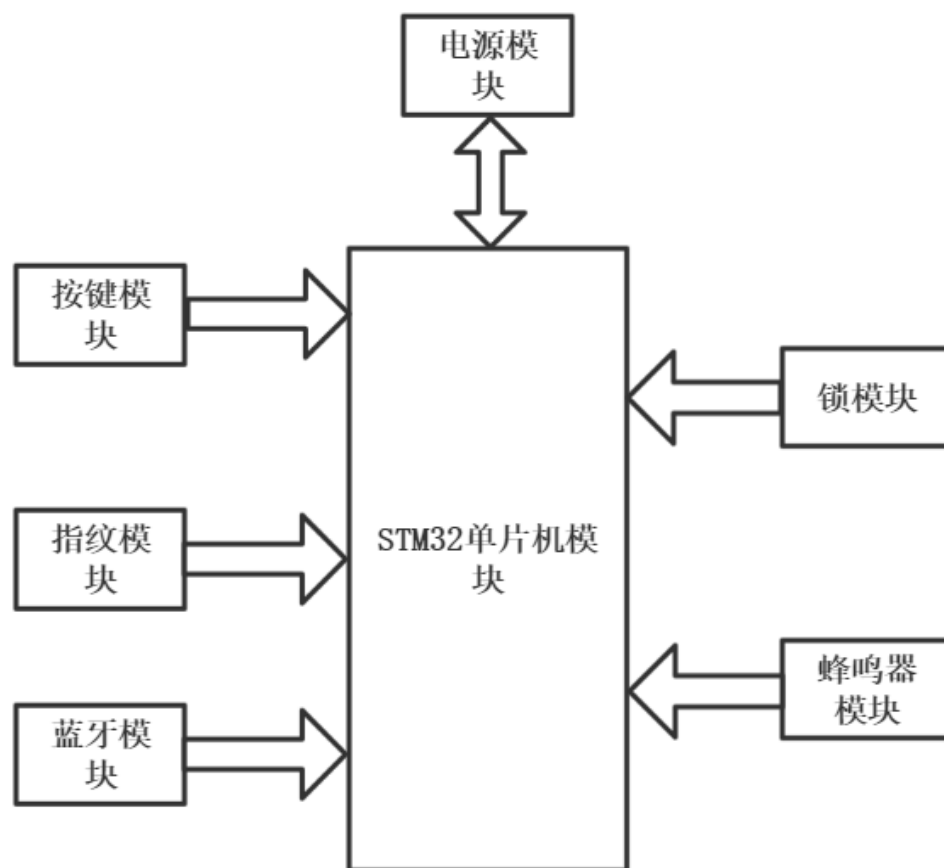


图 3-1. 系统模块基本框图

3.2 指纹录入模块

3.2.1 指纹传感器种类

最初，通过将手指蘸取油墨，有色墨水使得不同的手指纹路显现出来，从而起到手机指纹的作用，但是展现在纸张上的指纹图案既受纸张材料的影响也难以保存，肉眼更是难以辨别。随着电子计算机技术的出现，新型指纹采集设备得到了迅猛的发展，传统的采集方法被替代，存在的问题也相继解决。指纹的采集是整个指纹识别系统的关键，选择合适的传感器决定了指纹的图像的质量。采集指纹所用传感器主要分为三种：

（1）光学传感器

光学传感器是根据光的全反射原理设计而得，光线照射时产生反射，由于人手指上指纹的脊谷时凹凸不平的，在脊线处无法发生反射，而在谷线处发生全反射，利用人手指指纹的唯一性，在光学传感器上得到不同的反射结果。光线从不同位置不同方向照射到光学器件会形成明暗程度不同的一幅图像，明暗程度的差异通过灰度值表现出来。但是光学传感器使用后的镜片容易出现痕迹残留的现象，再次使用新的指纹与残留重叠影响检测，大大降低了准确性。

（2）半导体传感器

此类传感器根据半导体分为电容和电感。由于指纹的纹路深浅差异，通过传感器指纹采集面进行采集时，手指的不同位置与传感器采集表面上已集成的一些半导体存在距离差异，从而获得的数值大小是不同的，将这些数值表示图像的灰度值，得到一幅指纹图像。半导体传感器有小功耗的特点，较小的规模也为集成带来便利，选择传感器时比光学传感器更有优势。但是同样会存在缺点，静电干扰，手指汗渍等都会影响采集。

（3）超声波传感器

超声波传感器是利用超声波具有穿透性这一特质，利用其在不同成分制成的物体表面有强度不同的回波。克服掉了一般光学传感器和其它半导体传感器都无法一一克服掉的干扰问题，同时又能够真正拥有了高质量高清晰度的指纹图像。运用超声波技术完成指纹的采集工作还未被太广泛使用，仍需要不断完善才能大量投入使用。

3.2.2 MBF200 指纹传感器概述

传感器阵列包括 256 列和 300 行，由大量的这些小单元构成一个完整的 MBF200 传感阵列。传感器阵列中每一行的数据都通过两个采样电路获取。将行工作分为充电与放电两个时期。充电时期即通过 VDD 接口让电容板充电，与此同时，被选中开始工作所在行的电容单元也在内部信号的作用下为采样电路提供电压保持工作状态。对于电容板放电阶段，

这个阶段存在放电快慢之分，

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/588065037015007032>