东 莞 理 工 学 院

本 科 毕 业 设 计

**毕业设计题目：****基于单片机的指纹密码锁设计**

**学生姓名：陈勇祺**

**学 号：201841301114**

**学 院：电子工程与智能化学院**

**专业班级：2018级电子信息工程1班**

**指导教师姓名及职称：张梅 副教授**

**起止时间：** 2021 年 11 月—— 2022 年5 月

摘 要

单独使用密码去解锁，对于人们现在生活还是不够便利。所以需要一种可靠方便的验证方式。识别指纹技术在目前是认证身份的一种可靠手段，而且各个领域都有指纹识别的身影。在单独的密码锁上添加指纹解锁来，设计一款具有两种开锁方式，用户权限分级的指纹密码锁。采用STM32F103C8T6作为微控制器，具有键盘单元、液晶显示、指纹模块、警告电路等部分。使用将数据写入stm32内部flash的方式，来保存密码，用户的指纹的信息。当输入密码错误3之后，会有声光警告功能。

通过实验测试表明，设计的指纹密码锁能够实现密码开锁和指纹开锁两种方式开锁，在管理员模式下进行指纹的添加、删除、更改密码等操作，满足安全性能的设计要求。

**关键词：**指纹识别；电子锁；管理员模式；警告

Abstract

Using the password alone to unlock is not convenient enough for people's life now. Therefore, a reliable and convenient verification method is required. At present, fingerprint recognition technology is a reliable means of authentication, and fingerprint recognition is used in various fields. Add fingerprint unlocking to a separate password lock, and design a fingerprint password lock with two unlocking methods and user permission levels. Using STM32F103C8T6 as microcontroller, it has keyboard unit, liquid crystal display, fingerprint module, warning circuit and other parts. Use the method of writing data to the internal flash of stm32 to save the password and the user's fingerprint information. When the wrong password 3 is entered, there will be an audible and visual warning function.

The experimental test shows that the designed fingerprint combination lock can realize password unlocking and fingerprint unlocking two ways to unlock, in the administrator mode to add, delete, change the password and other operations, to meet the design requirements of security performance.

**Keywords:** Fingerprint Identification; Electronic Lock; Administrator Mode; Warning Mode

目 录

[摘 要 I](#_Toc101002636)

[Abstract II](#_Toc101002637)

[1 引言 3](#_Toc101002638)

[1.1研究意义及背景 3](#_Toc101002639)

[1.1.1 研究意义 3](#_Toc101002640)

[1.1.2 工程背景 4](#_Toc101002641)

[1.2 本文的主要研究内容和任务 4](#_Toc101002642)

[2．整体方案设计 6](#_Toc101002643)

[2.1指纹密码锁方案总体设计思路及结构框架 6](#_Toc101002644)

[2.2指纹采集传感器选型 7](#_Toc101002645)

[2.3控制单元方案 8](#_Toc101002646)

[2.4其他模块方案 9](#_Toc101002647)

[2.5本章小结 10](#_Toc101002648)

[3.硬件电路设计 11](#_Toc101002649)

[3.1电源电路设计 11](#_Toc101002650)

[3.2单片机最小系统电路设计 12](#_Toc101002651)

[3.3 指纹电路设计 13](#_Toc101002652)

[3.4其他电路设计 14](#_Toc101002653)

[3.5硬件抗干扰设计 15](#_Toc101002654)

[3.6小结 16](#_Toc101002655)

[4．软件设计 18](#_Toc101002656)

[4.1指纹密码锁功能目标 18](#_Toc101002657)

[4.2指纹密码锁软件设计 19](#_Toc101002658)

[4.2.1系统初始化程序设计 20](#_Toc101002659)

[4.2.2解锁状态程序设计 20](#_Toc101002660)

[4.2.3设置状态程序设计 21](#_Toc101002661)

[4.3指纹算法 22](#_Toc101002662)

[4.3.1指纹图像获取 22](#_Toc101002663)

[4.3.2指纹图像特征点提取 23](#_Toc101002664)

[4.3.3指纹图像处理 24](#_Toc101002665)

[4.4本章小结 25](#_Toc101002666)

[5.方案测试分析 26](#_Toc101002667)

[5.1系统初始化测试 26](#_Toc101002668)

[5.2解锁状态测试 28](#_Toc101002669)

[5.3设置状态测试 29](#_Toc101002670)

[5.4本章小结 31](#_Toc101002671)

[6.结论与展望 32](#_Toc101002672)

[6.1结论 32](#_Toc101002673)

[6.2展望 32](#_Toc101002674)

[参考文献 34](#_Toc101002675)

[致谢 35](#_Toc101002676)

1 引言

在现实生活中的大部分居民门禁系统，机械锁使用的是最多的，剩下的就是一些密码锁，磁卡锁等等。这些门禁系统存在有着丢失钥匙和被别人伪造的钥匙可能，对于密码则有被遗忘的可能。这些问题往往给人们的生活带来困扰，甚至可能会造成生命财产的损害。在如今如此发达的社会，使用先进的传感器技术进行基于人体生物特征的识别，让人们有更加安全便捷的身份识别认证。

指纹是指人的手指末端正面皮肤上凹凸不平的排列成不同纹型的纹线。纹线的起点、终点、结合点和分叉点，称为指纹的细节特征点。指纹识别是指通过比较不同指纹的细节特征点来进行身份确认。由于每个人的每一个手指的指纹具有唯一性且终生不变，因此指纹可用于身份识别，指纹识别也几乎成为生物特征识别的代名词[1]。经过那么多年的发展，指纹识别技术是多种生物识别技术中比较稳定可靠的。通过指纹识别技术开发的指纹密码锁，安全性具有保障，在操作上也是简单便捷，在平常生活中可以广泛的应用。本文设计开发一款指纹密码锁，具有密码和指纹开锁两种方式，并且设计了管理员模式，警告等功能。该设计有助于更多人了解指纹识别技术和其广阔应用，促进智能锁的发展。

**1.1研究意义及背景**

1.1.1 研究意义

现在科学技术发展是日新月异的，特别是生物信息技术在各个领域的运用。现在锁具行业也朝着高科技方向和安全性强方向发展。在生物信息技术的运用中，指纹是相当重要的部分。

从以前的传统门锁，发展到现在的指纹锁，生物信息技术引导产品革命性的发展，改变了人类的生活方式。指纹锁是生物信息技术运用的高技术含量产品，逐渐代替传统的机械锁，成为安全便利生活的象征。

指纹锁从出现到现在，走过来20多年的发展，目前在国内民用市场上的占比仍然比较低，不足10%，有着很大的发展空间。有专业人士认识分析：“到2019年，全球智能锁具市场总值将从目前的2.61亿美元增长至36亿美元。中国有着巨大的市场空间分推这个市场总值，如今开发的市场份额只是总市场需求的冰山一角。”

现在国内指纹锁还是处于发展的阶段，市场是广阔的蓝海。未来几年之内，随着经济的发展，人们的生活水平挺高了，就会开始逐渐了解指纹锁，指纹锁必将走进千家万户。

1.1.2 工程背景

传感器技术和集成电路技术的成熟，使得生物信息识别技术得到很好的实现。现在智能门禁系统主要有指纹密码锁、虹膜门禁系统、面部识别门禁系统等。采用虹膜、指纹、脸部等生物信息的门禁系统，密码具有唯一性，安全性能高。目前一些重要的门禁系统均采用这些技术。

由于人体特征的生物信息拥有不可复制的唯一性，所以指纹、虹膜等生物密钥是基本无法失窃、被复制和被遗忘的。通过利用这些信息进行用户身份信息鉴定，同时可以解决常见IC卡、钥匙等丢失、遗忘或被盗用等问题。对于虹膜、面部识别需要用到比较复杂的设备，通常在保密性高的场所，比如机密实验室等。而指纹识别用到设备就比较简单，其检测的传感器也比较小，可运用在常见的门锁中，具有广泛推广的操作性。

指纹识别技术是通过获取采集到的指纹图像，然后与已注册的指纹图像进行对比，实现用户身份鉴定。指纹身为人体固有的生物特征，具有独一无二性，安全便利。指纹识别系统所使用设备的成本相对于其他生物识别技术设备成本，相对较低，通过指纹识别技术优化，可以开发适合广大群众的指纹密码锁。

1.2 本文的主要研究内容和任务

首先对市面大多数类型锁具进行分析，基于指纹密码锁的优越性，设计出指纹密码锁方案。主要工作如下：

（1）进行整体方案设计。先设计指纹密码锁的整体的操作逻辑及结构框架，确定指纹模块的选型、微控制器类型、电源、电源、显示、存储、警告等设计方案。

（2）硬件电路设计。硬件电路方案主体：电源电路、单片机最小系统模块、指纹模块、警告电路、TFTLCD显示电路等

（3）软件设计。明确指纹密码锁的系统设计实现的功能目标，确定整个软件设计框架。系统运行分为三个状态，系统初始化状态、解锁状态、设置状态。通过这些状态的切换实现整个指纹密码锁功能。

（4）指纹密码锁功能测试。通过验证指纹密码锁的开锁、更改密码、添加用户等一系列功能，以及意外输入的情况，从而检测指纹密码锁的设计方案的可靠性、安全性、精确性。

2．整体方案设计

2.1指纹密码锁方案总体设计思路及结构框架

指纹密码锁设计方案主要实现指纹和密码开锁、指纹和密码的管理、友好的界面提示、检测按键输入、存储数据信息、警告功能等功能。原理框图如图2-1所示。

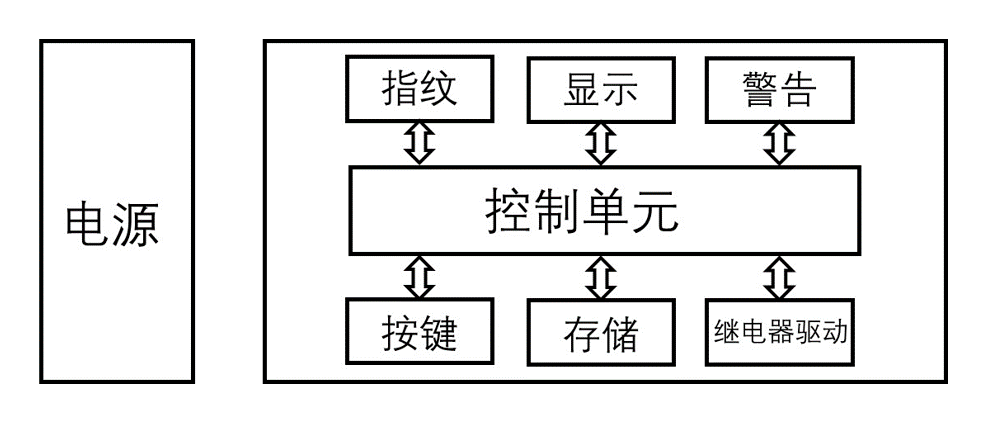


图2-1指纹密码锁控制方案原理框图

如上所示，本设计方案采用高性能的控制单元当作控制核心，来协调控制各个模块电路有序进行工作，实现良好的人机交互效果，从而让用户得到满意的使用体验。其它各个模块具体的功能如下：

1）指纹模块功能：获取用户的指纹信息并存储，检测比对用户指纹，返回识别对比效果；

2）显示模块功能：通过界面提示指引信息来指引用户使用；

3）警告模块功能：当密码输入错误，就会进行声光警告；

4）按键模块功能：通过检测按键输入来实现人机交互的功能；

5）存储模块功能：存储密码、用户信息、系统参数等数据：

6）继电器模块功能：模拟开门这个动作：

7）电源模块功能：给整个系统提供稳定可靠的电源输入。

2.2指纹采集传感器选型

采用高性能光学指纹识别模块，如图2-2所示。



图2-2光学式指纹传感器

ATK-AS608指纹识别模块是ALIENTEK推出的一款高性能的光学指纹识别模块。ATK-AS608模块采用了国内著名指纹识别芯片公司杭州晟元芯片技术有限公司（Synochip）的AS608指纹识别芯片。芯片内置DSP运算单元，集成了指纹识别算法，能高效快速采集图像并识别指纹特征[2]。它可以快速进行指纹录入、图像处理、指纹对比等功能，还具有以下优点：

1）采用蓝光LED背光，较之传统红光LED背光，蓝色照明可以让使用户有更加炫酷的感觉，同时还可以发挥出CMOS对蓝色分辨率更敏感的特性，获得清晰度更高的指纹图像。

2）模块配备了串口、USB通讯接口，用户无需研究复杂的图像处理及指纹识别算法，只需通过简单的串口、USB按照通讯协议通讯便可控制模块。

3）有触摸感应输出的功能。当有指纹放上去时，相关引脚就会产生高电平。方便去检测有无指纹放在传感器上，操作起来更方便。

4）同样支持手指360°旋转，方便根据不同的结构进行设计安装。

5）高强度的玻璃表面，保证了日常生活的各种应用需求。

6）价格较低，大大降低了方案的成本。

通过以上的分析可知得，高性能的光学指纹识别模块不仅有利于降低成本，而且还有触摸感应输出信号来检测，性能优异，良好的结构外形和蓝色的LED采集灯效果更可以丰富产品的设计。因此最终选择高性能的光学指纹识别模块，型号为ATK-AS608。

2.3控制单元方案

控制单元作为系统的控制核心，它的性能优劣直接决定了整个系统的性能。进行方案的设计时，发现系统对控制器的片上资源要求比较多，需同时满足如下要求：

1）光学指纹识别模块的控制需要使用UART外设。

2）用户信息，密码信息需要存储到微控制器的内部FLASH。

3）OLED屏的控制需要用到SPI接口。

4）平时调试也需要使用到UART外设

5）按键、继电器及LED等器件的控制需要用到诸多I/O接口资源。

为了满足上述要求，经过种种筛选后，最终确定使用ST公司的STM32F103C8T6芯片，如图2-3所示。

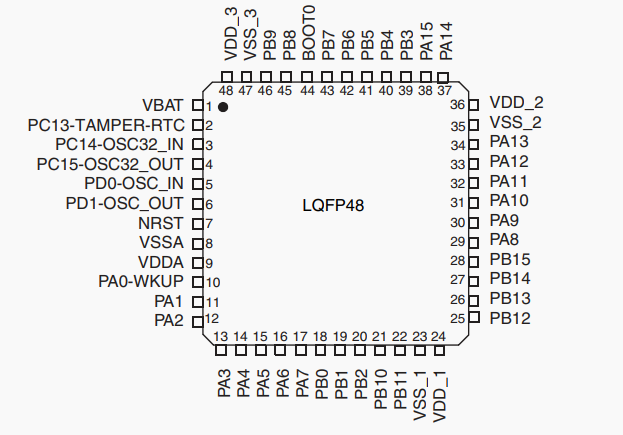


图2-3 STM32F103C8T6引脚图

STM32F103C8T6是采用ARM公司Cortex-M3内核、高集成、高性能32位微控制器。它的特性如下：

1）内核时钟最高可以到达72MHz，还可以根据自己需求去调整频率来降低功耗。

2）具有UART、GPIO、TIMER、AD、CMP、SPI、I2C、USB等外设。

3）多达37个I/O，多数引脚可通过寄存器配置从而实现复用的功能。

4）可以对Flash进行编程/擦除/读取操作。

5）内存空间具有高达128KB的闪存和20KB的RAM.

6）内置看门狗功能以防程序异常运行。

7）宽工作电压输入：2.0V-3.6V，

8）宽温度运行范围：-40~+85°C

以上的微控制器特性基本能够满足本文设计的要求，所以最终选择微控制器型号为STM32F103C8T6。

2.4其他模块方案

（1）电源方案。为了让板上硬件设计没有很复杂，所以板上提供了5V接口。由外部电源来提供5V，以后也方便去使用常见的220V转5V模块。这里为了使用方便，采用充电宝提供5V电源输入，在经过稳压电路减压提供3.3V的方案。这里选用型号为HT7333的3.3V低功耗线性稳压芯片，静态电流<3μA@6.0V，且精度高达±3%，能够满足方案需求。

（2）显示方案。屏幕作为产品和用户的信息交互窗口，显示的效果异常重要。现在市场上显示器件主要有数码管、断码屏、TFTLCD屏、OLED屏等。数码管不可以显示字符、汉字、图片等信息，只可以显示数字。断码屏则需要根据自身方案的需求开模去定制，而且显示的内容同样有限、灵活性不足。TFTLCD屏和OLED屏可以实际根据用户的需求，通过编程显示上述提到的任意内容。OLED屏的每个像素点能够单独发光，不需要背光源、发光转换效率高、能耗低，但是现有的技术比较难做出高分辨率的屏幕。OLED屏对标同等分辨率的TFTLCD屏比较昂贵。另外，用户通常都是在门锁前操作，都是从上到下俯视屏幕，现在TFTLCD屏的视角也可以达到170度，从侧面也不会失真。综合考虑选择了1.44寸的TFTLCD屏。

（3）存储数据方案。STM32F103C8T6内部有FLASH，可以掉电后保存数据。根据数据手册的描述，FLASH的擦写寿命的典型数值是10K次。在修改密码和修改用户信息的情况下，才会去擦写FLASH， 对于这个系统的寿命是足够的。同时需要保存的数据量不大，所以就没有选择外挂存储器件方案。最终方案选择使用内部FLASH保存信息。

（5）继电器方案。需要使用继电器去控制LED来模拟开门和关门的状态。在本文的设计中有5V的电源的提供，且继电器是用来控制LED，不需要承受大功率的工作。选择HF46F/5-HS1型号功率继电器，线圈电压5V、一个开关。足以满足设计

（4）警告方案。为了能够提醒他人，则选择一个蜂鸣器和一个LED去进行声光警告。

（6）按键方案。密码输入需要使用到0至9类型数值，还有确定键、取消键、设置键等类型按键，需要对应的按键与之对应。选用市面常见的4×4键盘，对于以上功能足够了。

2.5本章小结

本章主要明确指纹密码锁方案的整体思路和结构框架，对整体设计方案做了大致的说明。然后根据设计方案的实际需求，去选择核心元器件指纹传感器、微控制器进行了选型。同时对其他模块设计方案进行了说明。

3.硬件电路设计

硬件是整个系统的基础和框架，上一章已经介绍了系统的指纹传感器、微控制器、显示模块、继电器等核心器件。要达到预期的作品使用效果和实现整个系统的各个功能，各个器件之间连接需要相应的设计和优化，PCB的布局设计要合理，并且结构紧凑，相互干扰要少。

3.1电源电路设计

系统采用外接5V电源，而整个系统所需要的电压分别为5V和3.3V。因此需要电源电路设计出提供相应的电源。电源电路主要分为5V输入电路和3.3V稳压电路。

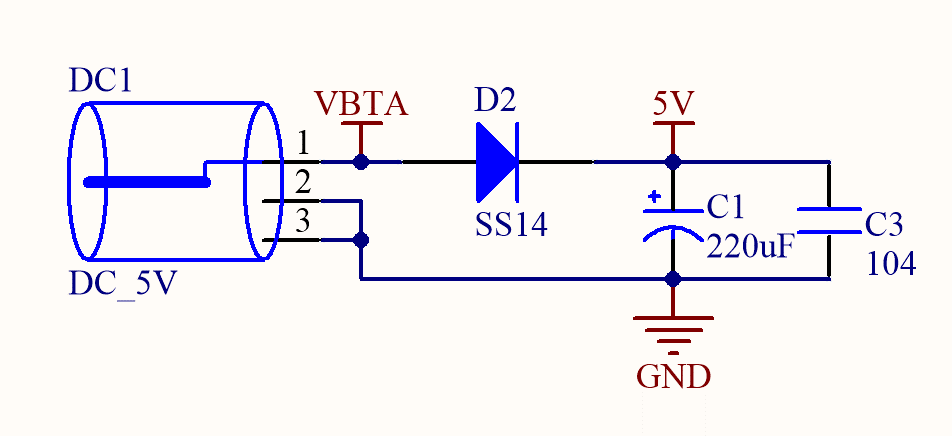


图3-1 5V输入电路

5V输入电路设计。如图3-1所示，采用DC接口，VBTA即是外部5V电压，输入后，经过单向导通二极管D2，主要是防止电流倒灌的情况，再经过一个大电容C1和一个小电容C3进行稳压滤波，得到稳定的5V。

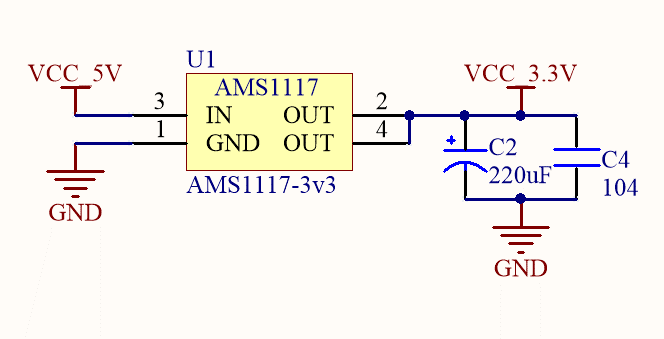


图3-2 3.3V稳压电路

如图3-2所示，VCC\_5V是稳定5V电压，输入到线性稳压器中，输出3.3V电压，同样的经过稳压滤波得到稳定的3.3V。

3.2单片机最小系统电路设计

微控制器仅依靠自身是无法运行的，需要其他元器件的配合才能运行。使用最少的元器件，让微控制器能独立工作的系统，称为单片机最小系统。本文采用单片机最小系统模块，然后在PCB上预留出相应的接口。如图3-3所示。这样的设计对于硬件后期出现问题修改比较方便。例如PCB某处设计不合理，需要重做，这时就不需要重新改动很多地方，重新焊接时也不需要焊接所有的东西。

单片机最小系统模块和大多数单片机设计差不多，都有电源、复位电路、晶振电路、参考电压电路、SWD/JTAG调试接口电路等。

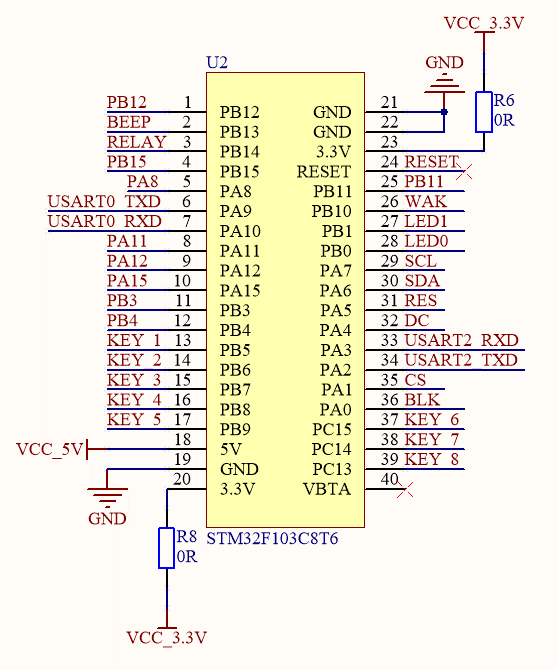


图3-3单片机接口电路

3.3 指纹电路设计

通过查询ATK-AS608指纹模块数据手册可获得指纹接口电路，如图3-4所示。

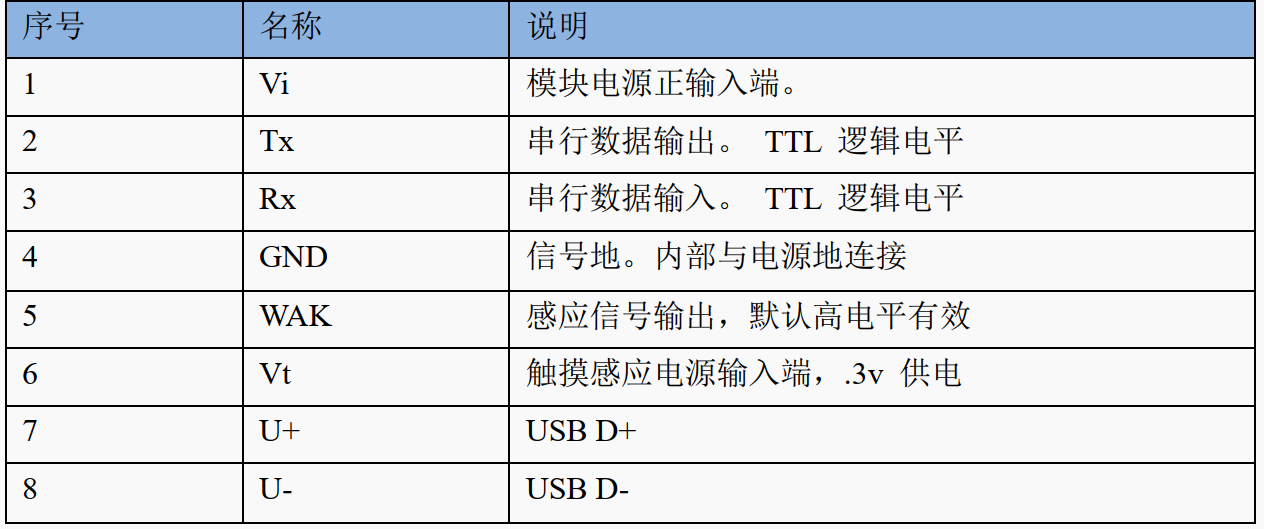


图3-4 ATK-AS608指纹模块接口说明

ATK-AS608指纹模块以杭州晟元芯片技术有限公司(Synochip)的AS608指纹识别芯片为核心，模块与微控制器通过串行通信接口直接与单片机进行通信：模块数据发送脚（2脚Tx）接微控制器的数据接收端（RXD），模块数据接收脚（3脚Rx）接单片机的数据发送端（TXD）。若需要与上位机（例如：PC机）进行通信，需在模块与上位机之间增加电平转换电路（例如：MAX232电路）。这里把模块的USB接口留空。WAK引脚接微控制器的普通IO口，Vi引脚要一直需要3.3V供电，Vt也接3.3V供电。在ATK-AS608指纹模块在没有检测指纹时就会关断触摸感应电源电路Vt引脚输入。微控制器一直检测WAK引脚状态，当有手指放置在指纹采集窗上，WAK引脚输出由低电平（0V）转换为高电平（3.3V），ATK-AS608指纹模块再控制Vt的电源输入。指纹采集传感器开始工作，等工作结束后，ATK-AS608指纹模再控制关断Vt的电源输入，从而达到省电的目的。这样的操作降低系统的功耗，不需要进行指纹比对时，关闭指纹模块的触摸感应电源，模块进入不工作状态。当需要进行指纹的录入、比对等操作时，开启指纹模块的触摸感应电源，指纹模块开始工作。指纹模块与微控制器接口如图3-5所示。

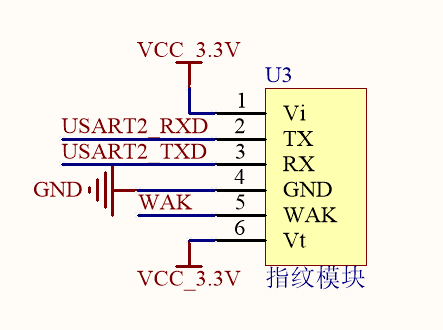


图3-5所示

3.4其他电路设计

1. TFTLCD屏显示电路设计。微控制器与TFTLCD屏通讯是使用软件SPI，因此使用微控制器的普通IO口。使用一个IO口与TFTLCD屏的BLK引脚相连，依此来控制背光源。SPI通讯需要SDI（串行数据输入）、SDO（串行数据输出）SCLK（Serial Clock,时钟信号）、CS（从设备使能信号）这四根线。TFTLCD屏接口如图3-6所示。

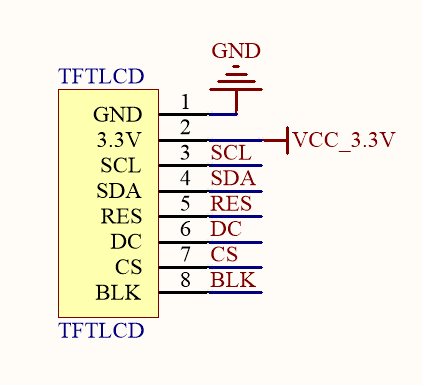
。

图3-6 TFTLCD屏接口电路

1. 警告电路设计。警告电路采用一个蜂鸣器和一个LED来进行声光警告。具体电路如3-7所示。

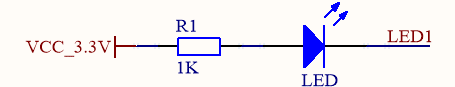
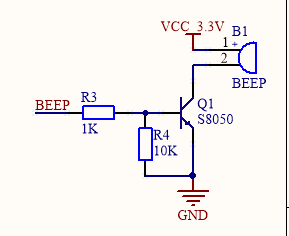


图3-7 警告电路设计

如图所示，通过改变BEEP引脚和LED1引脚的状态就可以实现蜂鸣器和LED的开启和关闭。

1. 继电器电路设计。继电器电路如图3-8所示。RELAY引脚控制着线圈的电流导通和截至。当RELAY引脚为高电平时，三极管导通，线圈有电流流过，开关闭合，LED点亮。当RELAY引脚为低电平时，三极管截至，线圈没有电流，开关断开，LED熄灭。这里在线圈并联一个二极管。因为三极管突然截至，线圈电流没了，线圈会维持自身现状，这时线圈就相当于电池。这就需要一个回路将线圈的能量释放掉。

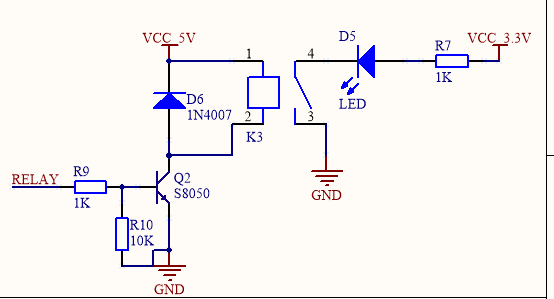


图3-8继电器电路

3.5硬件抗干扰设计

PCB板（印刷电路板）的结构复杂，布局紧凑，包含了电源电路、单片机最小系统电路、指纹采集传感器电路、TFTLCD显示电路等，并且是比较密集和集中的。所以在PCB板上如何布局上述电路就显得尤为重要。如果电路布局布置的不合理，电路之间就会相互干扰，造成信号失准，控制失灵等问题。所以还需要进行抗干扰设计。抗干扰设计又称为电磁兼容设计，为了防止系统之间电磁、信号相互干扰，本系统中采用下述抗干扰措施：

(1)地线设计

1)接地线加粗

如果PCB板上的地线不够粗，电路振荡引起的电路上电流急剧变化会在一定程度上造成传输信号的不稳定，从而影响信号的传输效果。因此本方案设计通过在PCB的Top Layer和Bottom Layer层进行铺铜来抑制电平信号的干扰。

2)接地线构成闭环电路

通过将电路中的PCB板接地形成闭环电路可以降低噪声。这个主要是因为在一块小型电路板上面布局了很多电路，如果遇到大元件，因为受到线条粗细的限制和地线宽度的限制，从而产生电阻使地线产生电位差，从而降低了抗击噪声的能力。如果通过Top Layer和Bottom Layer层在地网络设置足够多的过孔，就可以减低线条产生的电阻，为电流提供了最短的信号回流路径，同时也增加了散热量。

(2)电源线布置

各个支路的电流都会汇集到电源线，布置有两个原则：(1)在条件允许下，尽量加粗线条的宽度，满足电路在各种情况下的电流变化。(2)电源线的布置走向尽量与数据的走向一致，这样可以有效的防止干扰。

(3)元器件布置

在元器件布置方面，要进行模块化的设计。在设计时将各个模块所需的元器件放得尽可能靠近模块，以此来提高抗干扰能力。同时根据各个模块电路功能之间的联系进行布局设计

(4)印刷尺寸

PCB板的尺寸要合适。尺寸过大，虽然带来布局的方便，但是会增加材料量，成本会增加；尺寸过小，布局的难度就会上升，工作量加大，也会影响散热。所以要选用合适的尺寸。

3.6小结

本章主要设计开发了指纹密码锁系统各部分的硬件电路，包括电源电路、单片机最小系统电路、指纹电路、TFTLCD屏显示电路等，而且依据系统抗干扰性的需求，采用了地线设计、印刷电路板的尺寸、器件布局、电源线设计相关的硬件抗干扰措施。

4．软件设计

在我们生活中常见的嵌入式电子设备，比如鼠标、键盘、显示器等硬件。如果没有软件在硬件上跑的话，产品是无法正常工作的。指纹密码锁作为嵌入式设备，只有硬件架构和硬件电路，根本无法运行，还需要配合合适的软件程序，才能发挥出硬件的功能和实现系统功能。

在本章中，介绍系统的功能目标和控制方式，重点探讨软件程序设计，用C语言编写软件控制程序，实现指纹密码锁的解锁功能和管理员模式功能。IDE使用Keil MDK-ARM软件，该软件为基于Cortex-M、Cortex-R4、ARM7、ARM9处理器设备提供了一个完善的开发环境。程序底层库使用ST公司提供的HAL(Hardware Abstraction Layer)库进行开发，节约开发的时间，

本设计所用指纹模块采用的指纹算法是基于特征点匹配的算法，通过采集个体指纹的图像，对指纹图像进行切割、增强、滤波、二值化等处理，转化成指纹特征，再进行特征匹配操作。

4.1指纹密码锁功能目标

指纹密码锁功能目标有：在第一次使用时，需要进行初始化，录入密码和管理员指纹。接下来就进入解锁状态，用户通过按键和触摸指纹模块来进行解锁，系统开始对比验证密码或指纹是否合法有效，并能通过人性化的交互界面来指引用户操作。用户按下设置键后就进入管理员模式，在管理员登入后，能够去进行用户添加、用户删除、更改密码等操作。详细功能定义详见下列表：

表4-1指纹功能定义

|  |  |  |
| --- | --- | --- |
| 指纹功能 | 总指纹数量 | 300枚 |
| 指纹是否可查询、添加、删除 | 是 |
| 是否可以用指纹开锁 | 是 |

表4-2密码功能定义

|  |  |  |
| --- | --- | --- |
| 密码功能 | 密码是否可查询、添加、修改、删除 | 是 |
| 是否可以用密码开锁 | 是 |
| 连续错误3次进行声光警告 | 支持 |

4.2指纹密码锁软件设计

该软件的核心设计功能是通过控制TFTLCD显示模块、指纹模块、内部FLASH存储、继电器模块等模块有序工作。为了让用户得到良好的使用体验，该软件设计了人性化的TFTLCD显示界面来提示内容引导用户进行操作，让用户能够直观的根据屏幕提示进行相应的操作。此外，在本软件里加入了菜单管理系统，主要应用在设置模式状态来对不同功能进行分级管理，主要包括添加用户、删除用户，更改密码等功能。为了用户使用的便利性和实用性，指纹管理又分为管理员指纹、普通用户指纹。

为了保证软件的稳定性和可靠性，本软件采用单任务机制来处理各个事件，只有一个事件结束之后才会去执行另一个事件。系统上电时执行系统初始化操作，然后进入到解锁状态，等待着外部输入操作。外部输入操作有按键输入操作和指纹触摸输入操作。在按键输入操作中输入不同的键值去到不同的处理，按下设置键，就会去到设置状态。操作流程图如图4-1所示

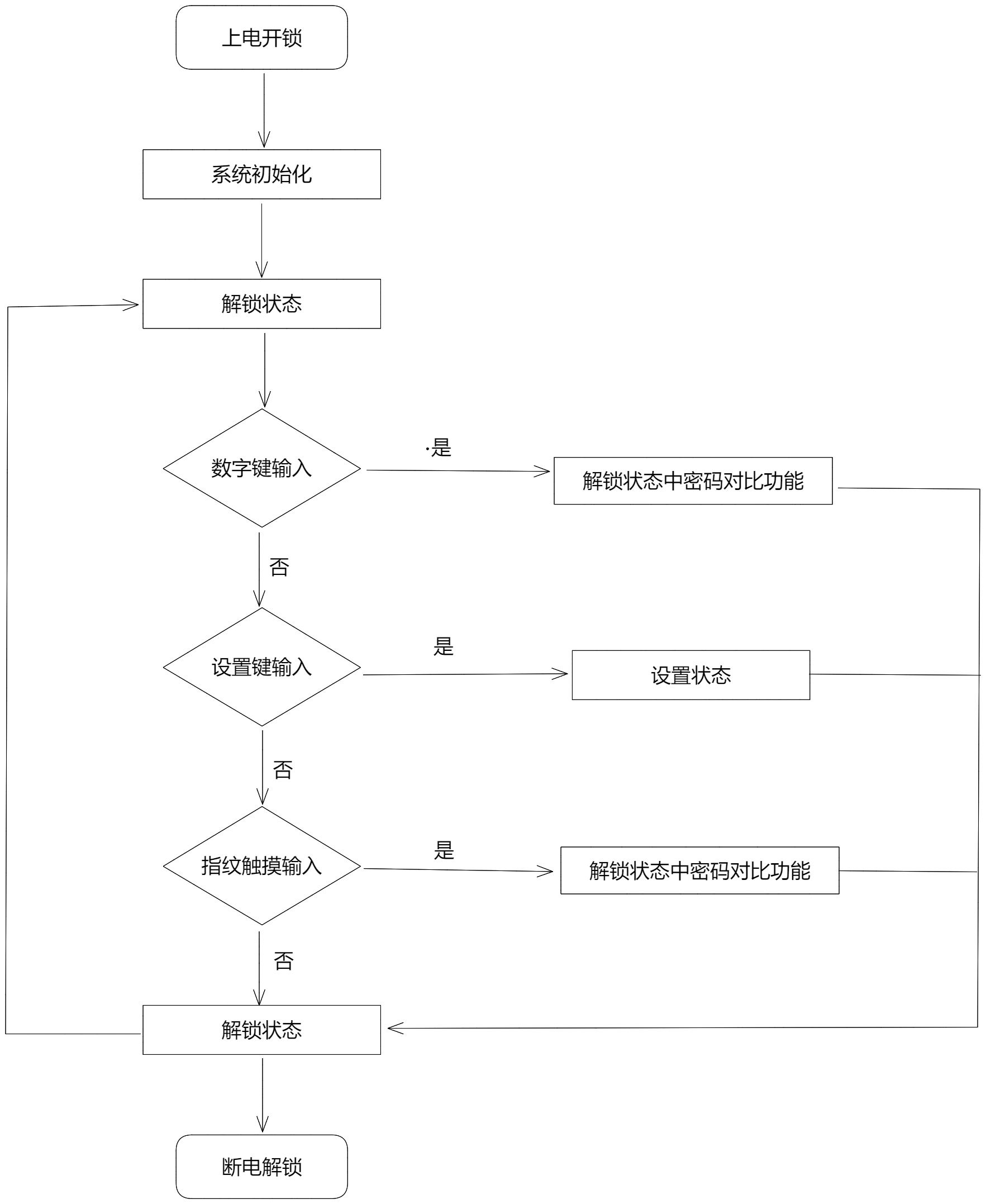


图4-1 软件总体框架图

4.2.1系统初始化程序设计

系统初始化主要的工作是初始化运行硬件所需的资源和用户第一次使用的情况，将系统各个外围电路设置到合理的状态。流程图如图4-2所示.

初始化硬件的主要工作包括：设置系统工作的主频率，确保系统能在稳定的系统时钟工作；设置微控制器相应IO口的状态；与外部模块进行通讯来初始化模块，并检测模块是否能正常工作。上电后，从STM32内部FLASH中读取系统关键信息。系统关键信息有六位数密码，用于判断是否第一次使用的标志位，用户信息，这些是系统正常运行所需的信息。

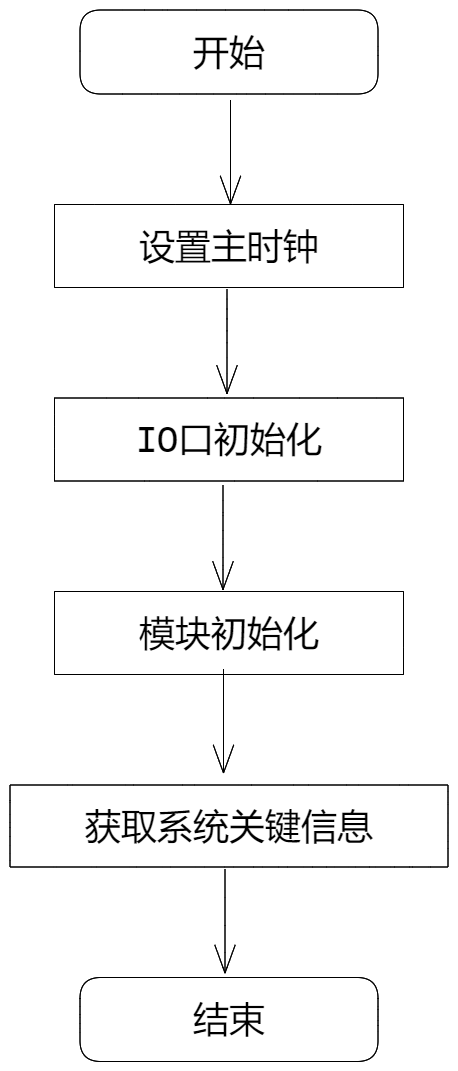


图4-2 系统初始化流程图

4.2.2解锁状态程序设计

系统初始化后就会进入到解锁状态。解锁状态流程如图4-3所示。这个解锁状态通过一个死循环实现，根据不同的外部输入去到不同的处理功能。在解锁状态中，不断进行按键检测和指纹检测。如果检测到数字键输入，就会去判断是否符合密码格式，再去判断密码是否正确，密码正确就会开锁。如果检测到设置键摄入，就跳转到设置状态。如果检测指纹模块的WAK变为高电平，说明检测到指纹，判断指纹是不是记录在系统的用户指纹，匹配成功后就会去开锁。

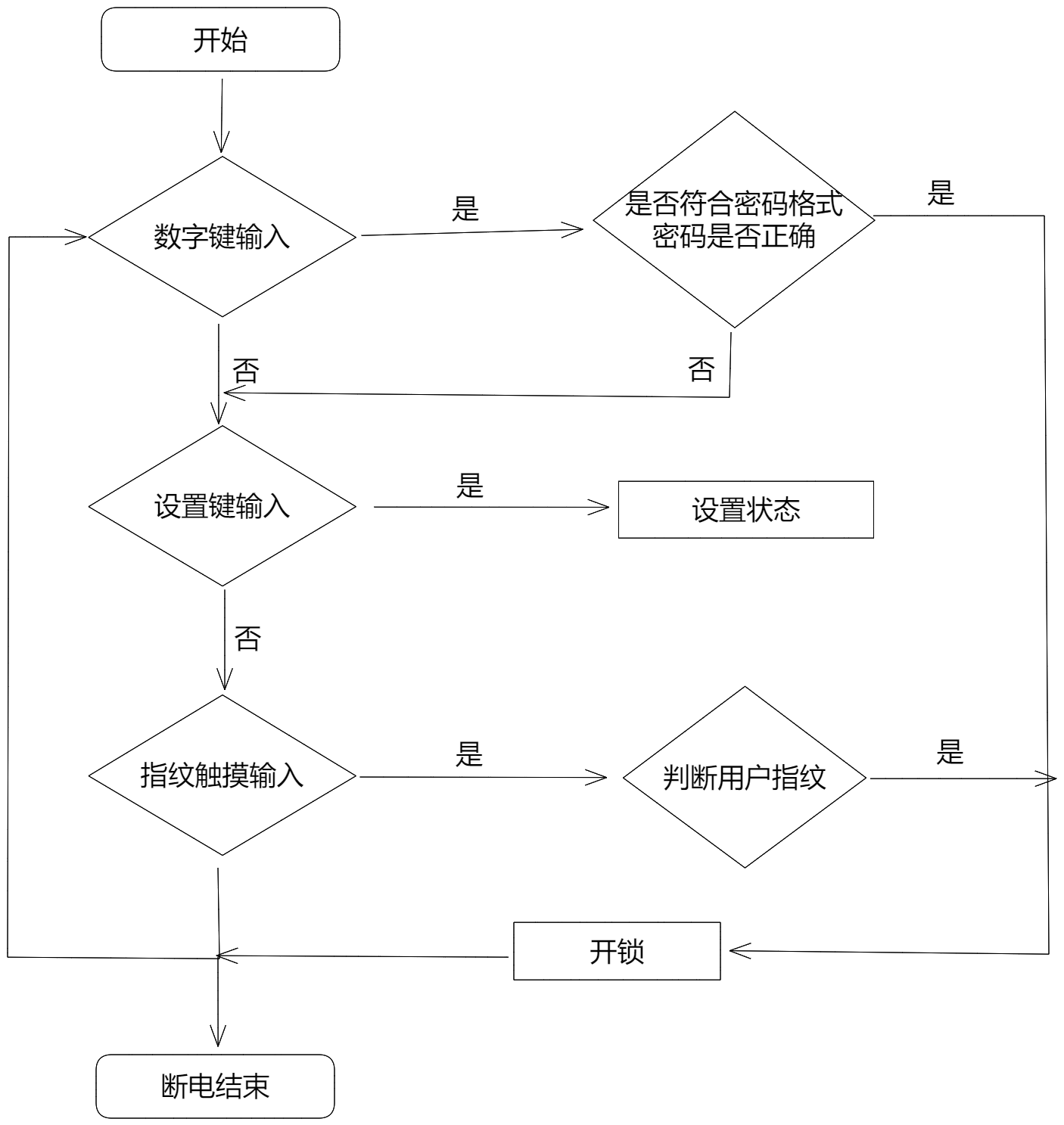


图4-3 解锁状态流程图

4.2.3设置状态程序设计

在解锁状态检测到设置键输入后，就开始进入设置状态。一开始需要管理员登入，将手指放在指纹传感器上，系统就会判断这个指纹是不是管理员指纹。只有将指纹判断为管理员指纹，才可以成功进入设置状态。设置状态也是通过一个死循环实现，里面运行一个简单菜单管理和按键检测。菜单管理着两级目录，比如“添加用户”是第一级目录，“添加管理员用户 添加普通用户”是第二级目录。不同的选项有着不同的功能。用户通过按下按键检去选择目录。退出设置状态只需要再按一次设置键就可以退出了。

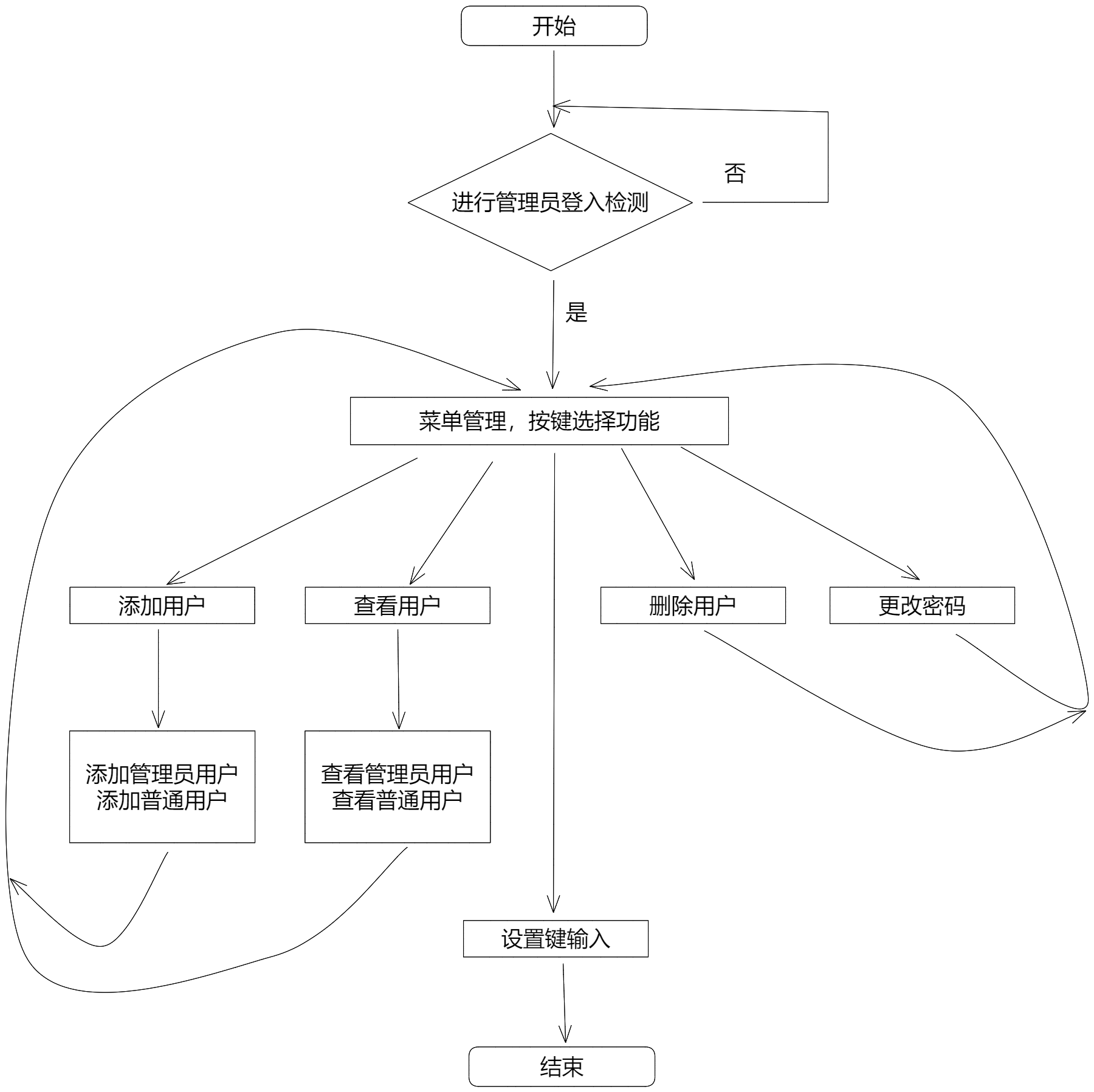


图4-4设置状态流程图

4.3指纹算法

4.3.1指纹图像获取

指纹图像获取是进行指纹识别的第一步，得到高质量指纹图像是运行指纹算法的关键。从指纹图像获取方式进行分类，主要有捺印指纹、活体指纹和模糊指纹这三类。捺印指纹是将手指沾上印油按压在纸上得到手指印迹，再经处理转化为数字信息，从而得到指纹图像。这种采集方式很难去控制指纹图像的质量，而且采集速度比较慢，现在这类采集方式比较少。活体指纹是经采集设备直接采集到的指纹。模糊指纹是指人们在无意中留下的指纹痕迹（比如在犯罪现场采集到的指纹），该指纹痕迹需经过显影、拍照和扫描等技术处理后才能得到较清晰的指纹图像[3]。通过以上的对比，通过活体指纹采集设备得到的数字化指纹图像的质量是最好的，本文使用的ATK-AS608指纹模块采用的是活体指纹采集方式。

根据采集设备的采集原理不同，可以分光反射式、超声波反射式、半导体式和感温式等。本文使用的是光反射式，光反射式的指纹图像获取原理是利用光线照射到玻璃表面进行反射，当手指按在指纹采集板上时，采集设备发出一束光线照射到手指上，由于指纹是由凹凸不平的脊线和谷线组成，反射光线的强度和角度由指纹脊线和谷线的深度决定，采集设备收集到这些反射强度和角度不同的光线，从而在CCD图像传感器形成图像，这样就可以获得脊线和谷线分明的指纹图像[4]。使用光反射式的指纹模块成本低，技术比较成熟。ATK-AS608指纹模块光路设计优秀，在指纹图像采集时，对干手指或湿手指都有反应和准确判断，可以获得质量比较好的指纹图像。

4.3.2指纹图像特征点提取

指纹特征点提取是从细化的指纹图像中提取全局特任点和局部特征点的位置、角度信息和类型等。全局特征点是可以通过人的眼睛直接观察到的特征，比如有中心点、三角点、弓形等。局部特征点又称细节特性点，比如分叉点、端点、环形、断线等。这些特征点中的分叉点与端点是构建特征信息最主要的细节特征点。目前绝大多数指纹识别系统都是采用分叉点和端点来进行提取比对，指纹图像的特征点的数量和精度决定了指纹识别系统的准确度，特征点数量越多，精度越高，系统的识别率就越高。

特征点提取是指将分叉点和端点等指纹特征的位置（坐标）、角度和类型等信息提取出来，存储在特征模板中，则将指纹图像转化为由特征数据组成的指纹模式空间向量，指纹图像经过预处理的各个步骤后，冗余的信息大大缩小[5]。只保留了区别于其他指纹图像的端点和分叉点（特征点），图4-5为纹线端点和分叉点示意图。判断一个特征点的类型只需参考其周边的8个像素点即可，如图4-6特征点表示形式所示，模式特征空间大大缩小。

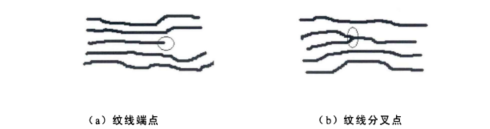


图4-5指纹特征点模板

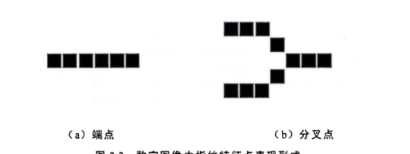
、

图4-6指纹特征点的数字化表达

4.3.3指纹图像处理

指纹图像的处理就是把一个人和他的指纹对应起来，通过提前录入好的指纹和现在检测到指纹进行比较，达到检验真实身份的技术。指纹识别理论依靠的是指纹的独一无二性和稳定性。指纹图像处理过程如图4-8所示。

在我们获取指纹图像时，要尽可能获取到高质量的指纹图像，指纹图像质量直接会影响后面的图像处理。然而在现实中，往往受各种因素的影响，获取到的指纹图像不理想。因此需要对获取的指纹图像进行预处理。预处理主要有指纹图像的分割、增强、二值化与细化等。指纹图像分割是将获取到达的指纹图像前景区域和背景区域区分开来，得到位线信息。指纹图像增强是将噪声除去，从而得到清晰准确的指纹纹线。进行指纹图像增强后的指纹纹线比较粗，还得进行细化处理，然后再进行指纹特征点的提取[6]。现在检测新获取的指纹特征与指纹数据库里的指纹特征进行相似度比较，再将相似度结果同系统设置好的阈值相比较，然后输出相似度比较的结果。

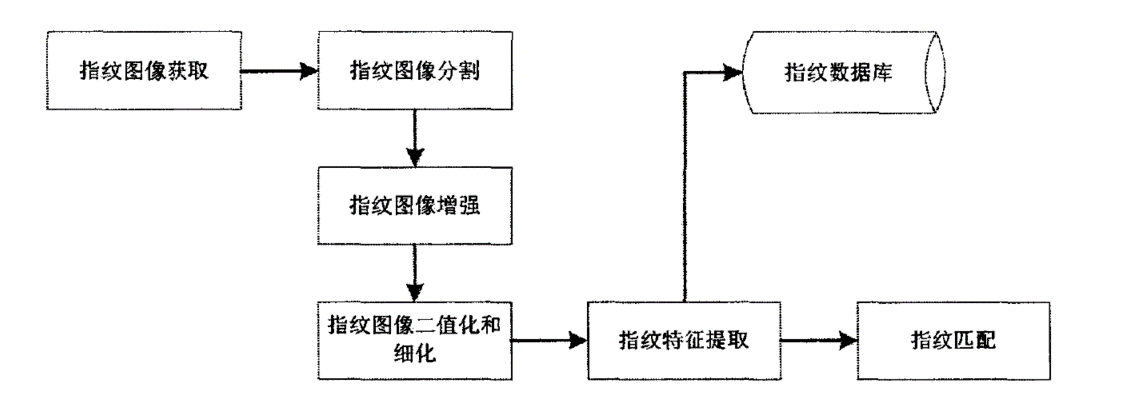


图4-8指纹图像处理过程

4.4本章小结

本章根据总体设计思想明确指纹密码锁的功能目标和功能参数指标，讲解了系统的总体流程，分为系统初始化流程、解锁状态流程和设置状态流程，并对它们处理流程进行讲解分析。与此同时，还介绍本系统采用的指纹图像处理流程。

5.方案测试分析

根据硬件电路设计和软件设计，制作出了指纹密码锁的实物，如图实物图5-1所示。

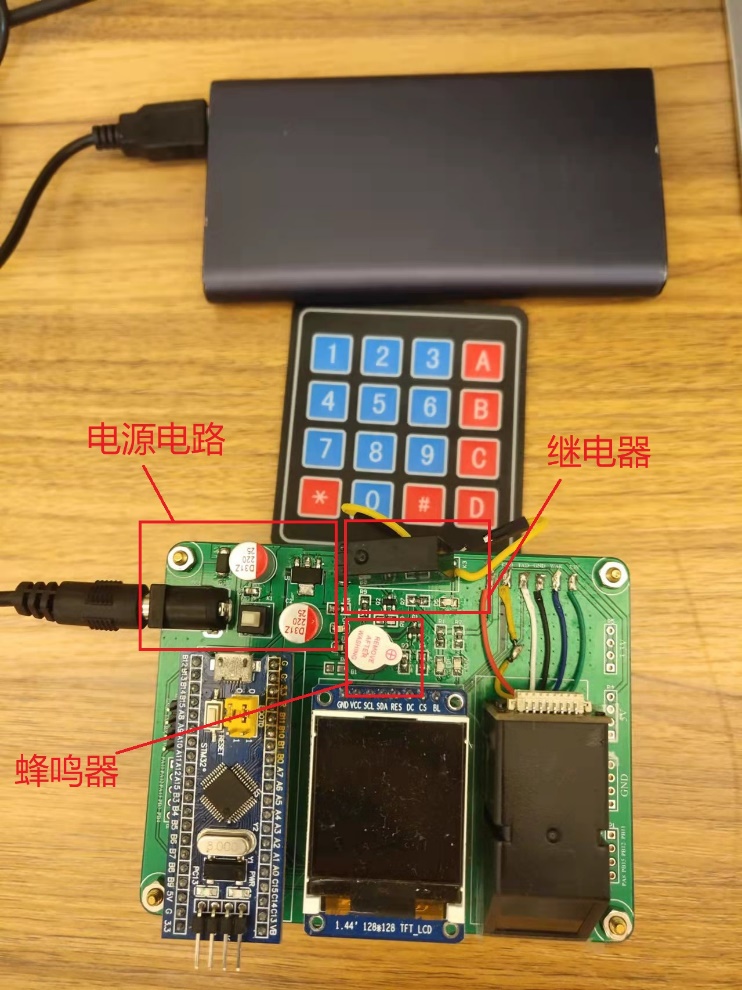


图5-1 指纹密码实物图

按键说明：0-9是数字按键、A代表着向上键、B代表着向下键、C代表着确定键、D代表着取消键或返回键、#代表设置键、\*代表关门这个动作。

5.1系统初始化测试

当系统上电开始，系统就开始进行初始化。测试结果是初步判断系统能否正常工作的证明。第一次上电初始化的测试项目和相关实际测试结果如表5-1和图5-2-

表5-1第一次系统上电初始化测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 第一次系统上电 | 1 | 显示“第一次使用设置密码”界面 | 成功 |
| 2 | 设置密码成功后，显示“第一次使用设置管理员”界面 | 成功 |
| 3 | 设置管理员成功后，进入解锁状态 | 成功 |

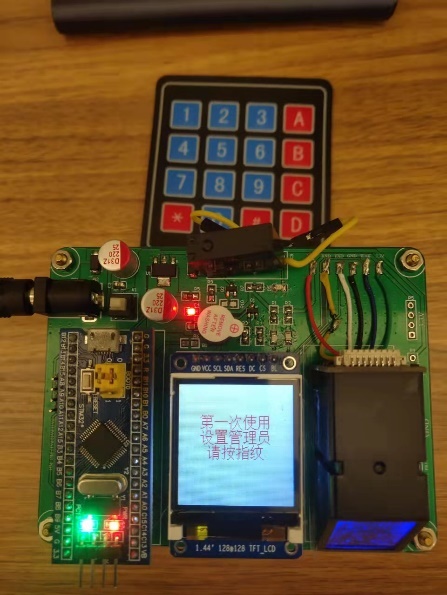


图5-2第一次系统上电初始化

接下进行系统上电初始化测试，测试项目和相关实际测试结果如表5-1和图5-3。

表5-2统上电初始化测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 系统上电 | 1 | 再次上电，系统能够完成初始化，进入解锁状态 | 成功 |

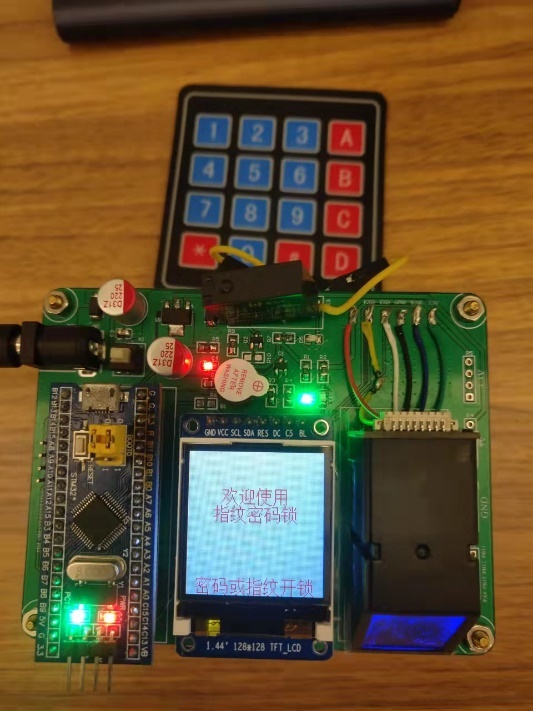


图5-3解锁状态

5.2解锁状态测试

在经过第一次系统上电初始化后，以后每次系统上电完成初始化后，就会直接进入解锁状态。以相关灯的亮和灭现象来代表开门和关门状态。在解锁状态可以进行密码解锁功能，相关测试项目和实际测试结果如表5-3和图5-4。

表5-3密码解锁测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 输入密码解锁 | 1 | 按下0-9数字键后，就开始密码解锁功能 | 密码正确，相关灯点亮 |
| 输入密码错误3次 | 2 | 当输入密码错误超过3次，就会进行声光警告。 | 成功 |

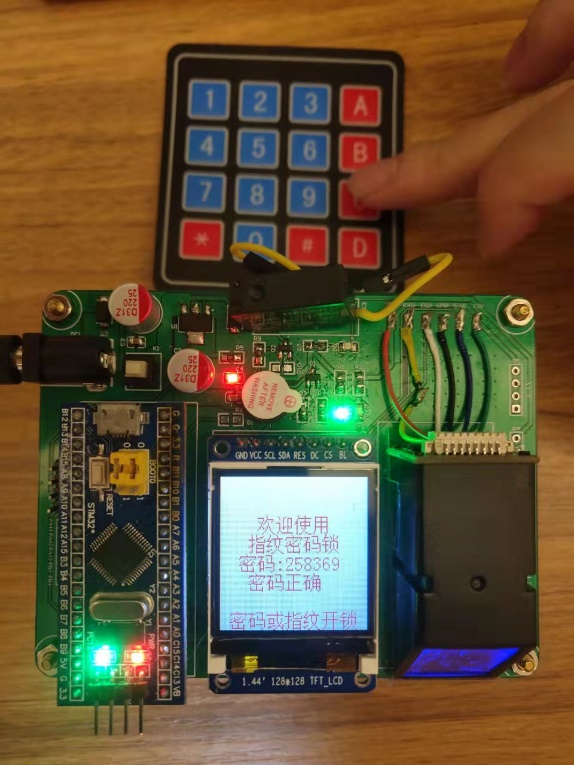


图5-4密码解锁测试图

当用户把指纹放在指纹传感器的采集窗上时，系统就会自动开始进行指纹检测功能。相关测试项目和实际测试结果如表5-4和图5-5。

表5-4指纹解锁测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 指纹解锁 | 1 | 将指纹放在指纹模块的采集窗上，系统自动进行指纹检测功能 | 指纹匹配成功，相关灯点亮 |

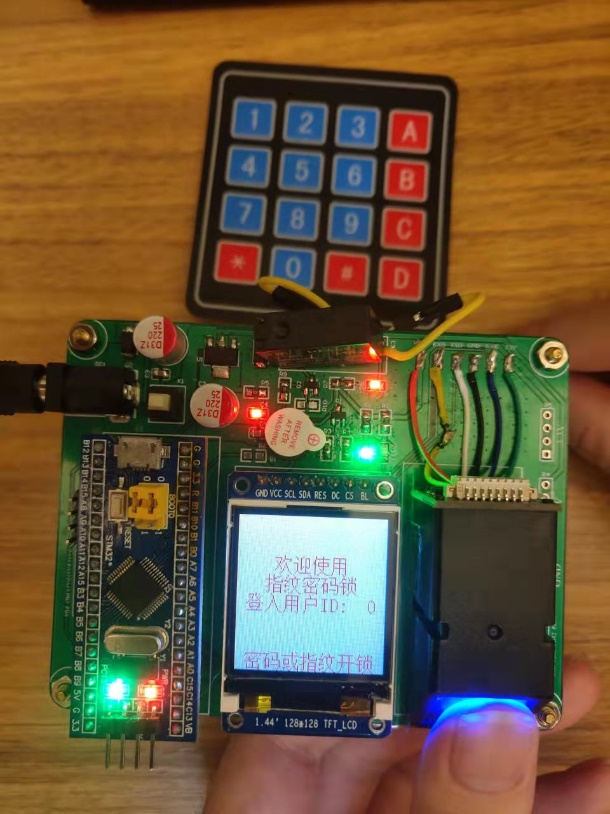


图5-5指纹解锁测试图

从图5-5可以看出，在指纹匹配成功后。系统会弹出当前用户的ID的提示，继电器控制的灯也会亮起。在指纹模块采集指纹过程中，由于受手指接触面积不一致、干湿程度、挤压程度等因素的影响，指纹匹配有时不是第一次就能成功。

5.3设置状态测试

在解锁状态按下设置键，就会进入设置状态。设置状态得管理员登入后才能继续操作。设置状态界面如图5-6所示。

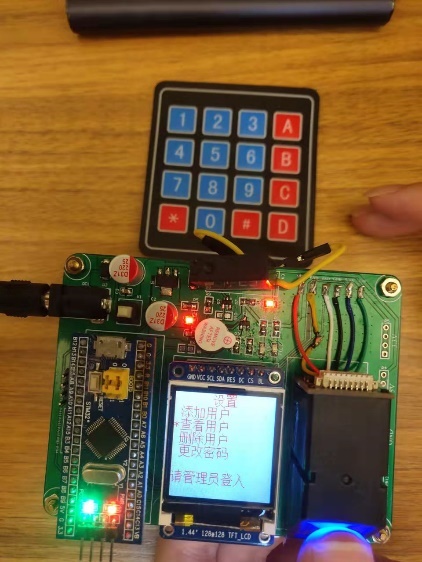


图5-6设置状态界面

在设置状态有四个选项，分别是“添加用户”、“查看用户”、“删除用户”、“更改用户”。接下依次进行测试。

表5-5添加用户测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 添加用户 | 1 | 选择添加管理员用户功能 | 录入指纹成功，显示新注册用户ID |
| 2 | 选择添加普通用户功能 | 录入指纹成功，显示新注册用户ID |

表5-6查看用户测试表

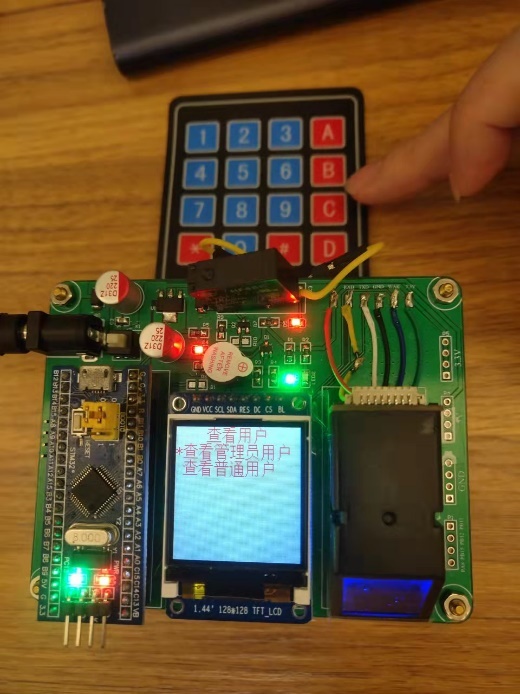
|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 查看用户 | 1 | 选择查看管理员用户功能 | 显示管理员用户ID |
| 2 | 选择查看普通用户功能 | 显示已有普通用户ID |

表5-7删除用户测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 删除用户 | 1 | 选择删除用户功能，然后输入删除用户的ID | 显示删除指纹成功 |

表5-8更改密码测试表

|  |  |  |  |
| --- | --- | --- | --- |
| 测试大项 | 序号 | 测试项目 | 测试结果 |
| 更改密码 | 1 | 选择更改密码功能 | 显示更改密码成功 |



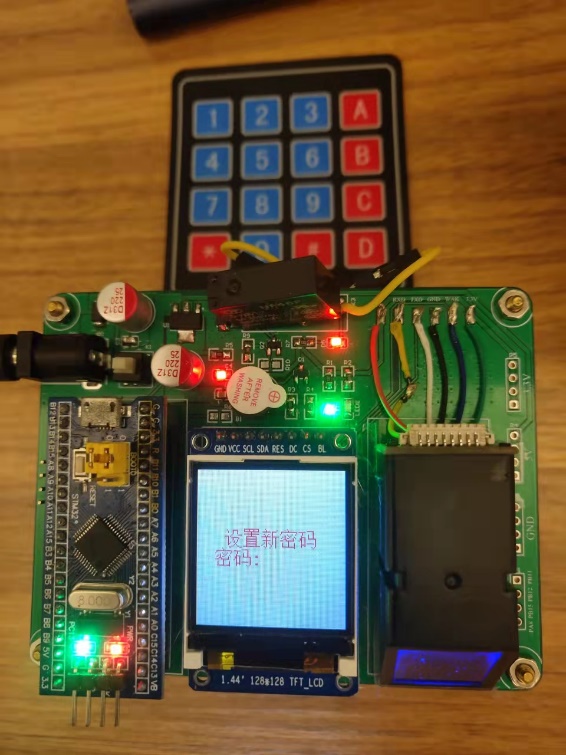
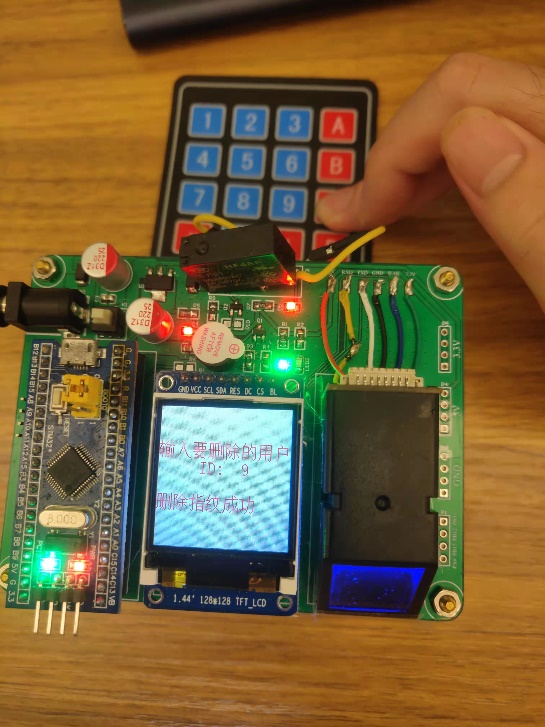


图5-7设置状态测试

每一枚新注册的用户指纹都会有一个固定ID号与之对应，同样可以通过ID号删除用户指纹。通过以上测试，验证设置状态下的“添加用户”、“查看用户”、“删除用户”、“更改用户”功能是能正确运行。

5.4本章小结

本章节使用设计出来的硬件结构，按照软件设计章节设定的功能目标进行相关测试。经过本章节的测试，介绍了详细的测试步骤，明确测试的结果。确认设计的指纹密码锁方案实现预定要求的目标，包括密码开锁和指纹开锁，管理员模式下添加用户等功能。

6.结论与展望

6.1结论

随着人们生活水平提高和科技水平提高，逐渐使用指纹密码锁来代替传统的机械锁。指纹密码锁可以解决由传统钥匙产生的易丢失、易被盗窃等问题。现在指纹密码锁拥有广阔的市场前景，一款无需佩戴实体钥匙和安全性高的指纹密码锁产品必然是未来的一种发展趋势。因此本课题设计一款便捷使用、安全可靠、管理员模式等功能的指纹面密码锁。

主要工作如下：

1）先进行研究指纹密码锁的理论知识，对比各种方案优缺点，明确指纹密码锁设计的总体方案。指纹模块方面：光学传感器类型指纹模块使用方便，而且成本相对较低，因而在传感器方面选择光学传感器。在微控制器方面，需要满足各个外设使用的需求，而且还可以擦写自带的内部FLASH，价格还不能太高

，因而最终选择STM32F103C8T6。其他方面，如对电源、显示、警告等方案选择也进行了研究介绍，确定了指纹密码锁的整体控制方案体思路和结构框架。

2）通过研究分析指纹密码锁硬件电路，设计开发了指纹密码锁系统各部分的硬件电路，包括电源电路、单片机系统电路、TFTLCD屏电路、继电器电路、警告电路等，并且根据系统抗干扰性的要求，采用了地线设计、印刷电路板的尺寸、器件布局、电源线设计相关的硬件抗干扰措施。

3）通过研究指纹密码锁的软件控制，根据总体的软件框架确定了指纹密码锁的功能目标，介绍系统的总体流程，分为系统初始化、解锁状态流程和设置状态流程，并分别对各个状态流程进行了介绍分析，

4）通过对指纹密码锁方案设计出来的实物进行了测试。测试分为系统初始化测试、解锁状态测试及设置状态测试。实际测试结果验证该设计完成达到功能目标。

6.2展望

指纹密码锁拥有各种优势，但仍有一些不足之处，比如：

1)对于一些特殊群体，如小孩和老人。指纹密码锁不能满足这些群体的需求。因为小孩随着年龄的增长，指纹纹路会发生变化，多数老人会有手指蜕皮现象、指纹纹路加深等现象。目前还没有特别好的指纹处理方式。

2)由于成本等原因，指纹模块采用的控制器芯片运算速度暂时还没办法达到很高机的水准，存储容量有限，无法容纳很多指纹模板，进而导致使用指纹的门禁方案还无法使用在用户众多的场合。

参考文献

1. 王瑞琦,郭柯延,薛晓冬.基于指纹识别的实验室门禁系统设计[J].国外电子测量技术,2021,40(07):160-163.DOI:10.19652/j.cnki.femt.2102546.
2. 张洋,刘建粉.基于STM32的新型智能防盗门[J].电子设计工程,2022,30(03):58-62.DOI:10.14022/j.issn1674-6236.2022.03.013.
3. 张学斌. 基于指纹识别的安全密码锁设计[D].湖南大学,2017.
4. 周鹏. 指纹密码锁的设计开发[D].杭州电子科技大学,2016.
5. 刘飞涛. 基于ARM的指纹识别算法的设计与实现[D].西安电子科技大学,2018.
6. 文祝青,吴志攀.一种基于ABC-BP神经网络的指纹识别算法研究[J].电脑知识与技术,2017,13(32):196-198.DOI:10.14004/j.cnki.ckt.2017.3518.

致谢

时光飞逝，从入学东莞理工学校学习到现在己经有四年了，大四这一年，老师和同学都给了我很大的帮助和鼓励。在此即将告别之际，甚是怀念。在东莞理工的学习及论文撰写中，我的导师张梅老师给予我许多关心和指导，使我知道了不少知识。他严谨的治学作风和崇高的品质亦给我留下了深刻的印象。在她的悉心教海下，我才能得以完成学业。在毕业论文的写作过程中，张梅老师牺牲许多时间，阅读我的拙作，给我提出宝贵的建议，使我的论文几易其稿，最终得以顺利完成。在这里，我要向他表示深深的谢意。

其次，我要感谢我舍友、同班同学等三年来陪伴，让我快乐的度过大学生涯。在外漂泊有了依靠。

。最后，我要感谢父母在生活和学习上对我的支持和关心，感谢所有关心和帮助我的老师、同学和朋友们。