智能管理系统

半导体指纹仪

V1.0

使用说明书

前　言

指纹仪有完善的用户权限管理。但为了避免拥有管理权限的用户不在场，而客户又急需设置本系统，本系统特设了一个系统复位功能。管理员可以进入系统将设备恢复到出厂时的设置。

特别注意事项：

1、　系统复位功能不需要复位密码，在设备没有管理员的状态下，任何人均可以恢复出厂设置，当设备中有管理员用户，则需管理员登录成功后才能恢复出厂设置，客户在成功安装后，正式使用前，需自行注册管理员，并妥善保管好管理员登录密码。

2、　系统复位是在客户不得已的情况下才使用的。若使用系统复位功能，则该系统中原有的用户数据将全部丢失，参数设置也将恢复成出厂时的设置。需重新登记用户才可使用。

3、　系统复位之前必须先做好数据备份，若没做备份，数据丢失后无法找回。

◆ **主要技术参数指标：**

项目	技术参数
传感器类型	电容式 CMOS 传感器
传感器分辨率	508dpi
传感器有效面积	33.4 *20.4 *3.57mm
指纹处理器外形尺寸	35 * 28 * 1.6 mm
拒真率	＜1.0%（安全等级为 3 时）
认假率	＜0.001%（安全等级为 3 时）
指纹比对时间	≤1S
指纹接受平面角度	±30º
验证模式	仅使用指纹、指纹或密码、指纹与密码
指纹验证方式	1：1、1：N
工作方式	脱机工作，可联网辅助管理
最大用户容量	1000 个用户（每个用户最多 3 枚指纹）
最大指纹容量	1000 枚
工作电流	70mA
安全等级	1～5 级
工作温度	－10℃～55℃
工作湿度	相对湿度 40%～90%
动态功率（不含锁具功率）	直流 12V　小于 2W

*注：这里所说的脱机使用是指通电后在指纹处理器上即可完成用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、提示信息的显示等，这些工作不需要与 PC 联网就能完成.处理器输出维根信号，配合维根控制器可控制门锁的开合。

保修服务

尊敬的用户：

感谢您选用本产品,为了您能够充分享有完善的售后服务支持,请您在购买后认真阅读本产品保修卡的说明并妥协保存。

1. 凭此卡享受保修期内的免费保修及保修期外的优惠性的服务。

2. 用户自购买之日起因质量问题免费包换期限为 7 天，保修期 2 年。

3. 优先得知新产品的信息或优惠活动的机会。

4. 下列情况造成的产品故障不在保修之列：

4.1) 不能出示产品有效保修凭证和有效购物发票或收据；

4.2) 使用环境或条件不当，如电源不合、环境温度、湿度、雷击等而导致产品故障；

4.3) 由于事故、疏忽、灾害、操作不当或误操作等导致产品故障；

4.4) 由非公司授权机构的维修人员安装、修理、更改或拆卸而造成的故障或损坏；

4.5) 产品超出本公司所规定的保修期限。

5. 当用户对经销商所提供的技术服务有任何异议时，可以向制造商客户支持服务中心投诉。

6. 保修卡需经保修单位盖章后方有效。

产品保修卡

客户名称：_____

地　　址：_____

电　　话：_____

型　　号：_____

机身编码：_____

购买日期：_____

注：请您在购机后填妥此页保修卡内容后寄回

目　录

传感器

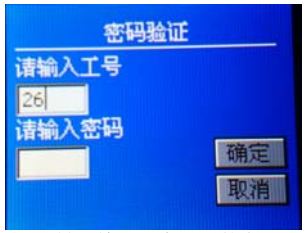
指纹仪安装说明：

1. 固定铁板
   1） 从包装盒中取出固定铁板和安装用的顶针；
   2） 确定固定铁板的固定，指纹仪一般安装在外部入口处墙面上，安装高度为距地面约 1.4 米。在墙上确定固定铁板的位置，在铁板位置下边预留一个用于将线引出来的孔；
2. 将连接线引出来，将压制好 RJ45 水晶头插入指纹仪背部的 RJ45 接口；
3. 用配套安装用的顶针，平面朝下，插到指纹仪右下角的小孔，向上推动顶针，压住弹片，露出两个固定孔，见下图，然后将指纹仪的两个固定孔对准固定铁板上的两个柱子，扣住后再松开顶针，这样指纹仪就安装好了。

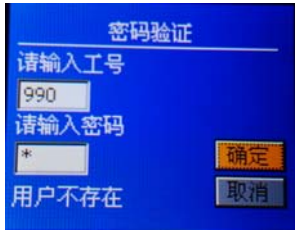
注意事项：

1. 安装完后左右摇一下指纹仪，确定孔都已卡住，已固定好。
2. 网线走线要与强电线隔开。
3. 安装时注意卡好网线，以免重新拆装。
4. 把指纹仪其他线接好，最后再上电。
5. 此产品满足电磁兼容 B 级，在生活环境中，该产品可能会造成无线电骚扰。在这种情况下，可能需要用户对其骚扰采取切实可行的措施。

在待机状态下按数字键输入完整的用户编号，屏幕显示如下：

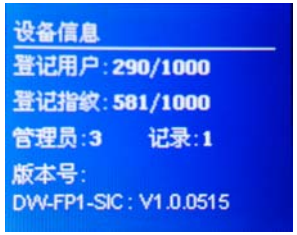


把用户编号完整输入后，再按“Next”键，输入用户设置的密码后将光标移至“确定”按钮再按下“OK”键，如果编号存在，则直接验证成功；如果编号不存在则提示“用户不存在”，并“嘀嘀嘀嘀”响 4 声，屏幕显示如下图：



3.6 系统版本信息查询

在待机状态下，按“Next”键，可以查询系统版本号、序列号及设备节点号等信息。屏幕显示：



登记用户：已登记用户数（包含了“管理员”和“普通用户”）：290/总用户数：1000；
登记指纹：已登记指纹数：581/总指纹数：1000；
管理员：设备中管理员个数：3　　记录：设备中的记录数：1
版本号：DW-FP1-SIC：V1.0.0515
本系统可容纳的总用户数为 1000 人（包括用户和管理员）。此功能提供了对系统现时用户容量使用情况的查询途径。

3.7 指纹仪维护及安装说明

设备维护：

1. 避免本设备工作在恶劣环境，如日晒、雨淋、强磁强电环境下；
2. 严禁金属物，导电物质接触或者靠近传感器录入窗口的表面，以防物理伤害，传感器如下图所示；
3. 尽量避免尖锐的金属物对传感器表面的撞击；
4. 保持环境卫生，避免在会传感器窗口上堆积大量灰尘或其他影响光学透射的物质；
5. 按照下文说明的方法定期清洁传感器窗口

在长时间的使用以后，传感器可能会堆积较多的灰尘，会影响采集到的指纹，可用干净的软布擦拭传感器采集窗口或吹去采集窗口灰尘，如有他难以清除的脏东西，可使用干净棉布/棉纱加上外用酒精进行清洁，进行自然干。

1 概述

指纹仪最多能容纳 1000 名用户，每名用户最多 3 枚指纹，胁迫指纹不是必须录入。 指纹模块能存储最多 1000 枚指纹，也就是说每个人只注册 1 枚指纹时，能注册 1000 个用户，当有用户注册多枚指纹时，实际能注册的用户不足 1000 人，刷指纹时，建议用户让手指在传感器上停留 2-3 秒左右，提高验证效率。

1.1 指纹门禁系统构成

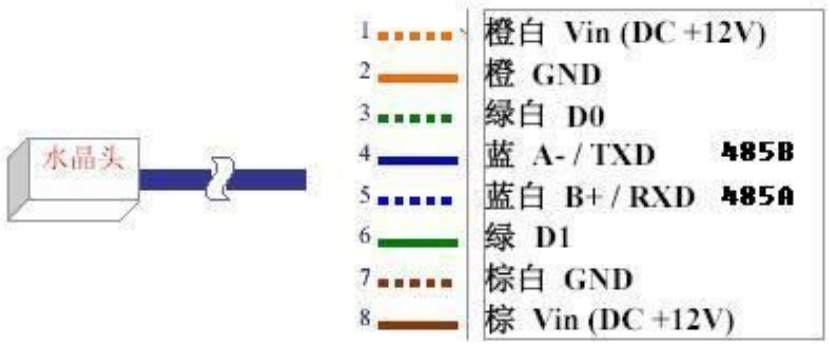
处理器：它实现了用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、提示信息的显示等。主要包括指纹处理模块、液晶显示屏、键盘、指纹传感器、复位键、外壳等部分（下文中也将之称为“设备”）.

1.2 指纹仪接线说明

指纹识别仪主要实现脱机实时指纹登记、对比及安全控制、指纹数据存储、跟 PC 机进行联机通信等功能。该产品可以方便地接入 IC 卡门禁系统，取代原系统的 IC 读卡器，独立完成各项指纹处理功能，然后把指纹验证成功后得出的 ID 号（个人身份号码），以维根信号方式发送到门禁控制器进行应用处理，从而组成了韦根通信标准的指纹门禁控制系统。既可通过指纹验证控制出入，同时配合考勤管理软件也可组成高效完善的指纹考勤系统。

指纹识别仪背部的 RJ45 接口用于连接主控制器的线缆。用户可根据实际需要购置相应长度的五类或超五类网线，一头使用 8P8CRJ45 水晶头压制插入指纹仪的 RJ45 接口，制作方法与以太网网线的制作相同，水晶头连接线的制作图示如下图所示，连接线另一头根据具体定义连接到主控制器上。

注：水晶头上定义顺序是左 1 右 8。



1） 1、2、7、8 脚用于主控制器提供DC+12V电源到指纹仪，1、8脚同时接到DC+12V，2、7脚同时接到GND；
2） 3、6 脚是指纹仪与主控制器之间的韦根信号通讯线；
3） 4、5 脚是PC 与指纹仪 通过RS485 方式通讯的数据收发线，如果用户需要从指纹仪 中读取指纹数据保存到PC上时，就需要应用2、4、5 脚接线到RS232/RS485 转换器，再接到PC的串口，并使用专用的软件读取数据。
4） DC+12V 供电线路（1、2、7、8 脚）建议使用0.5 平方MM 以上线材，信号线（3、4、5、6 脚）采用16AWG~24AWG 型号的线材，尽量使用屏蔽线串管走线，减低外部干扰。
5） 如果由于距离过远，主控制器无法接收指纹仪的信号，提供以下两点建议—— a、在指纹仪安装位置就近取电，例如使用DC+12V电源适配器； b、建议加粗DC+12V供电线路（1、2、7、8 脚），例如使用 0.5 平方MM 以上线材。

1.3 名词解释

用户的概念：指纹仪指纹系统存在有两类的用户概念，第一类是指指纹仪指纹设备的用户，这类用户包括设备的管理员及普通用户；第二类是指使用PC工具软件的用户，由于使用PC工具软件的用户可对设备的数据、参数进行设置、管理，因此也称为PC管理员。两类用户的大体职责如下：

1）第一类：

“管理员”和“普通用户”是设备的真正使用者，能根据不同的权限使用此系统进行验证开门、查询、管理等操作；其中“普通用户”只具有使用权限，“管理员”具有设备管理权限；

2）第二类：

PC管理员的职责是使用PC 工具软件对设备的数据进行维护，主要负责系统参数的维护、用户数据的备份和恢复等。(注：PC管理员使用PC 工具软件与设备进行通讯时，应该保证设备处于空闲的待机状态，否则将无法与之成功通信)

用户权限：设备上的两种用户具有不同的操作权限，按从高到低，排列：管理员 > 普通用户。

普通用户：普通用户不具有任何管理权限，只能进行一般的开门验证操作。

管理员：除了能进行普通用户所能进行的操作外，还可以增加、删除或修改“管理员”或“普通用户”的数据。

空机状态：指纹仪处于无用户状态，也就是处理器端没有登记任何用户数据（包括管理员和普通用户）或所有用户数据都已被删除：这种状态称为空机状态。

待机状态：当指纹仪没有接收到任何按键输入而处于空闲等待的状态时，就称为待机状态；在待机状态下，液晶屏幕会显示当前的日期和时间。

门状态：指门的开关状态。若用户安装了门状态检测开关（如门磁开关等）并接入指纹仪指纹门禁系统，则系统可时刻检测门的开关状态。

锁状态：指锁的开关状态。若用户安装了锁状态检测开关（大多数电控门锁本身即带有锁状态检测开关）并接入 指纹仪指纹门禁系统，则系统可时刻检测锁的开关状态。

出门开关：指纹门禁系统的一个选装部件。可安装在门内，用户在门内按动此开关即可开锁。

脱机使用：本文所述的脱机使用是指通电后在指纹处理器上即可完成用户数据的登记与存储、系统信息的查询与设置、指纹数据的验证、提示信息的显示等，这些工作不需要与 PC 联网就能完成。

联网辅助管理：本门禁系统各机型都提供与 PC 机的连接方式，可通过 RS485/TCP 等实现与 PC 机的联网，使得客户可以在 PC 机端通过辅助的工具软件实现对门禁系统的管理，进行各项参数的设置，并可实现用户数据的备份和恢复等，大大方便了客户管理多台门禁系统。

下文多处提到与 PC 机的联网通讯功能。但若要成功实现与 PC 机的通讯，还需要参见下文与“通信”有关的描述来设置指纹处理器上的某些参数。若客户不需要与 PC 机联网通讯，可忽略。

本地报警：由锁控单元内部蜂鸣器产生报警声。在报警的门禁系统附近的人都可听到此报警声。

远程报警：从指纹门禁系统中向外引线至远方的报警器，在远处（例如警卫室等地方）产生报警声。在报警的门禁系统附近的人听不到此报警声。

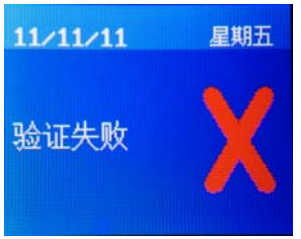
报警手指：用户登记指纹时可以指定某一个手指为报警手指（未被指定为“报警手指”的手指称为“正常手指”)。当用户用该手指完成“验证开门”操作或“菜单登录”操作时，系统将发出远程报警信号。报警手指一般在人身安全受到威胁时使用。

正常开门：用户使用已授权手指（包括正常手指或报警手指）通过本门禁系统来进行“验证开门”，或通过“出

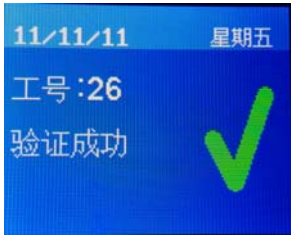
3.4 使用指纹进行开门验证

在待机状态下用登记过的手指，直接轻压传感器；当听到“嘀”的一声响后（表示系统已取图成功）用户可以把手指移开。

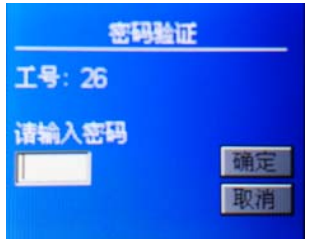
如果验证失败，在比较急促的“嘀嘀嘀嘀”4 声响后，屏幕显示“验证失败”如下图所示：然后返回待机状态；



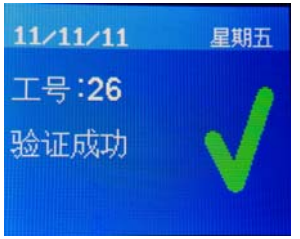
若验证成功，将听到“嘀”1 声的提示声，屏幕提示“验证成功”如下图所示：然后返回待机状态；



如果所有手指都验证成功，在“指纹与密码”验证模式下，屏幕还会提示用户输入密码，如下图：



密码验证成功后，屏幕再输出验证成功的信息（而在“指纹”或“指纹或密码”模式下，则会跳过密码验证，直接显示这个信息）：



3.5 使用密码进行开门验证

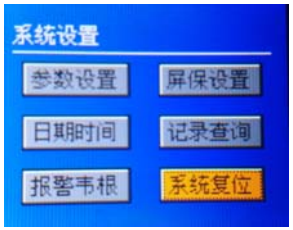
只有在“指纹或密码”验证模式下，才可以仅使用密码（不使用指纹）而能通过验证开门；以下说明假定系统已设置为该模式：

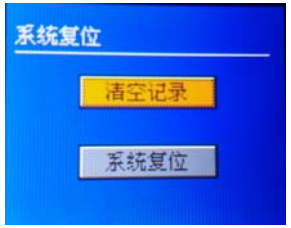
（图 4）

每条记录上的“日期、时间”，表示了该条验证记录在当天发生的具体时间；如果信息多于 4 条，屏幕显示不完时，可以通过按数字键“4”上翻屏或者按数字键“6”下翻屏，继续查阅余下信息。

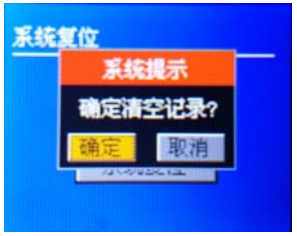
3.3.2.6 系统复位

选中“系统复位”按“OK”键，进入“系统复位”界面如下图所示：

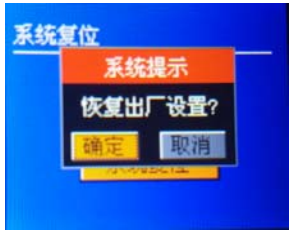




按“Next”键选中“清空记录”，再按“OK”键，系统提示如下图：此时按下“OK”键则清空设备中所有记录，清空成功蜂鸣器“滴”两声，系统提示窗口消失，若清空不成功则停留在系统提示界面，可再次进行清空；若无需清空，按“Next”键将光标切换至“取消”按钮处按下“OK”键即可。



按“Next”键选中“系统复位”，再按“OK”键，系统提示如下图：此时按下“OK”键则系统删除所有用户数据，并把系统的所有参数设置恢复到出厂状态，恢复成功蜂鸣器“滴”两声，系统提示窗口消失，若恢复不成功则停留在系统提示界面，可再次进行恢复出厂设置；若无需恢复出厂设置，按“Next”键将光标切换至“取消”按钮处按下“OK”键即可。



门开关”开门的过程，称为正常开门。

非法开门：在本门禁系统正常工作时，在使用过程中如有除正常开门外的其他开门动作，均称为非法开门。例如有人通过非正当手段（如使用暴力方法撬开门锁等）打开门锁或用钥匙（若用户配备的电控门锁附带钥匙）打开门锁等。

指纹验证和密码验证：本系统支持指纹和密码的单独验证以及指纹与密码的组合验证。其中的密码单独验证方式是针对部分用户指纹质量较差，指纹登记或验证时可能存在困难的情况，而特别设计出的验证方式。至于指纹与密码的组合验证则可以提高整个系统的安全性。

拒真率：其含义是指将相同的指纹误认为是不同的指纹，而加以拒绝的出错概率。常用百分比来表示，其数值越小越好。

认假率：其含义是指将不同的指纹误认为是相同的指纹，而加以接受的出错概率。常用百分比来表示，其数值越小越好。

2 功能概述

2.1 设备管理功能

2.1.1 用户管理

用户管理功能包括了：1）新增用户，2）管理用户；

2.1.1.1 新增用户

1）增加新用户必须输入新增用户的编号。系统中每个用户编号都是唯一的，不能重复；合法的编号范围为 0~999 之间的任意数值。

2）进行新增用户登记时，可以选择新增用户的使用权限，并且可以选择：a.只登记指纹，b.只登记密码，c.同时登记指纹和密码（该选择需根据验证模式而定，当验证模式为“指纹”时新增用户必须登记指纹；当验证模式为“指纹或密码”可只登记密码或指纹；当验证模式为“指纹与密码”时必须同时登记指纹和密码）； 但如果新增的用户权限是“管理员”，则必须同时登记指纹和密码。

3）每用户最多可登记 3 枚指纹（每枚指纹采样两次），可三枚都设定为报警手指，也可不设。（后续不再对此功能进行赘述）

2.1.1.2 管理用户

进入管理用户界面，可查看到用户工号、是否登记有指纹及指纹枚数、是否登记有密码、是否是管理员（管理员工号前带#号）、根据工号查找用户、编辑用户、删除用户、上移或者下移光标、翻页。

2.1.1.2.1 查找用户

进入管理用户界面，按数字按键“1”，进入查找用户界面，可根据工号查找用户。

2.1.1.2.2 编辑用户

管理员都可以编辑所有用户的如下信息：

1） 验证密码

2） 管理员权限

也就是说，用户的验证“密码”以及管理员“权限”等两项信息，在使用的过程中可以根据需要由管理员进行灵活的更改。

若需要修改用户的其他信息，则只能删除该用户后重新登记。

2.1.1.3 删除用户

1）删除操作有两种操作形式：a.逐个删除，b.批量删除；
2）“管理员”在设备中只能逐个删除设备中的用户，能删除自己；
3）批量删除用户只能通过管理软件批量删除，（全部删除设备中的用户，系统将变为空机）。

2.1.1.4 上移/下移

光标上下移动或者上下翻页查看用户信息。

2.1.2 系统设置

系统设置功能包括了：各种安全参数、通信参数的设置，以及日期、时间等设置；

2.1.2.1 参数设置

参数设置包含以下设置：

1） 验证模式：系统的验证模式可以设置为以下 3 种。当设置为其中一种验证模式之后，系统中的所有用户都只能使用该验证模式验证进入系统。系统默认的验证模式是“指纹或密码”。（按“OK”键可在这三种模式中任意切换）

只使用指纹

用户想进入管理功能或进行开门验证时，必须通过系统的指纹验证才能进入。也就是说，对于只登记了密码的用户，在此模式下将无法使用系统；

指纹或密码

用户想进入管理功能或进行开门验证时，只需要通过指纹验证或密码验证两种方式中的任意一种，就可进入系统；

指纹与密码

用户想进入管理功能或进行开门验证时，必须同时通过指纹验证和密码验证两种验证方式才能进入系统。也就是说，对于只登记了密码而没登记指纹，或只登记了指纹而没登记密码的用户，在此模式下将无法使用系统；

☛在进行新增用户登记时，建议同时登记指纹和密码，以避免在系统转换验证模式后用户无法进门

2） 安全等级：用户可以对系统指纹验证的“安全等级”进行设置,可选范围为 1-5；设置的等级数值越大，安全性就越高；系统默认的安全等级为 3。建议不要轻易修改此设置，尤其是不要轻易将其置低。

注意：设置的安全等级越高，拒真率就越高（相应的误认率则越低）；设置的安全等级越低，拒真率就越低（相应的误认率就越高）

3） 区号：区号可选范围 1-254，区号又称设备号。注：例如：用户编号为 326、区号为 254，输出韦根号为 00025400326。

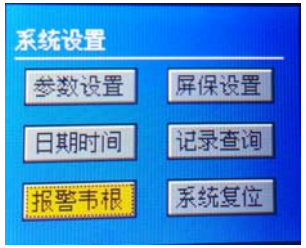
4） 节点号：“节点号”是 PC 与设备通信时指定的设备目的地址，合法范围为 0～254；处于同一个局域网内的指纹处理器的节点号不能相同。系统出厂时默认的节点号为 0。若客户需要使用 PC 与指纹门禁系统联网，实现远程管理，则需要在设备上设置正确的通信参数。若不需要与 PC 联网通讯，可不做任何设置、修改。

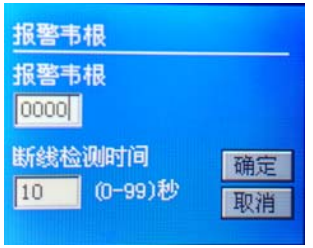
2.1.2.2 日期和时间

对系统的实时时钟进行设置，支持从 2000 年到 2099 年间的所有合法日期和时间的设定，对超出范围或非法的输入将给出错误提示；

2.1.2.3 报警韦根

1） 报警韦根：设置胁迫报警用。韦根号即为门禁系统对应的胁迫码，默认报警韦根：0000；
2） 断线检测时间：设置设备离线报警的时间，取值范围：0-99 秒。断线报警设置为 0 时，断线

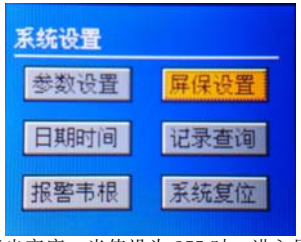


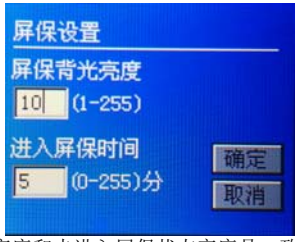


1） 报警韦根：设置胁迫报警用。韦根号即为门禁系统对应的胁迫码。
2） 断线检测时间：设置指纹仪断线报警的时间。断线报警设置为 0 时，离线报警功能不启用。
根据用户的需求，输入相应数值后，按“Next”键将光标移至“确定”按钮处，按“OK”键保存；若无需保存最新更改，则按“Next”键将光标移至“取消”按钮处，按“OK”键返回上一级菜单。

3.3.2.4 屏保设置

选中“屏保设置”按“OK”键，进入“屏保设置”界面如下图所示：

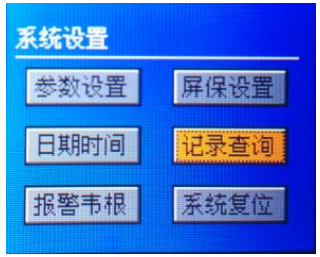




1） 屏保背光亮度：当值设为 255 时，进入屏保状态的亮度和未进入屏保状态亮度是一致的。
2） 进入屏保时间：设置进入屏保状态时长，0 表示关闭屏保功能。
根据用户的需求，输入相应数值后，按“Next”键将光标移至“确定”按钮处，按“OK”键保存；若无需保存最新更改，则按“Next”键将光标移至“取消”按钮处，按“OK”键返回上一级菜单。

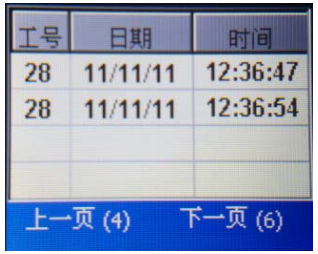
3.3.2.5 记录查询

选中“记录查询”按“OK”键，进入“记录查询”界面如下图 2 所示：在工号输入框中输入所需查询用户的工号，再到日期输入框中输入起止年月日的时间，选中“确定”按钮按下“OK”键，若该用户存在且有验证记录，则如图 3 所示，被查询用户在这个指定日期的全天 24 小时内曾经通过了系统的身份验证，系统将会按用户通过验证的时间顺序列出这期间的所有记录信息；若该用户存在但没有记录或者是该用户不存在则查询结果为空，如图 4 所示：

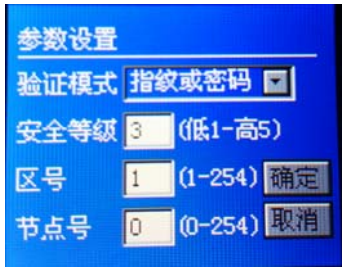


（图 1）

（图 2）



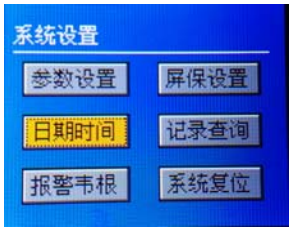
（图 3）



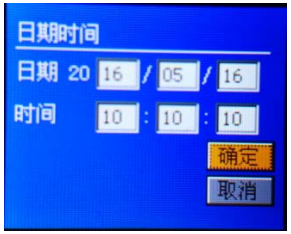
1） 验证模式：将光标切换至验证模式，按“OK”键，验证模式在“指纹或密码、指纹与密码、指纹”这三者之间循环切换，根据用户的需求来选择。
2） 安全等级：按“Next”键，将光标切换至安全等级输入框，用户可以对系统的“安全等级”进行设置,选择范围：1-5；设置的等级数值越大，系统的安全性就越高（输入数值超出可选范围，则无法移动光标，有关数值设置的都一样，后续不再赘述）；
3） 区号：区号可选范围：1-254；
4） 节点号：用户可以根据需要设置当前设备的节点号,可取值范围为 0-254；

3.3.2.2 日期时间

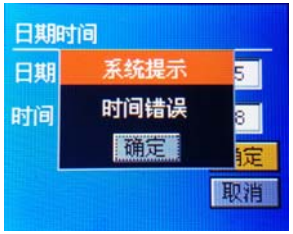
选中“日期时间”按“OK”键，进入“日期时间”界面如下图所示：



日期：系统支持从 2000-01-01 至 2099-12-31 间的所有合法日期的输入，系统的时间（24 小时制）。输入完成后将光标移至“确定”按“OK”键进行确认如下图 1 所示；如果输入日期/时间非法或超出范围，系统会给出错误提示，如下图 2 所示，此时用户应该按“OK”键并重新输入；如果用户想放弃日期/时间设定，可以通过按“Next”键选中“取消”后按“OK”键，直接返回到上层菜单。



（图 1）



（图 2）

3.3.2.3 报警韦根

选中“报警韦根”按“OK”键，进入“报警韦根”界面如下图所示：

报警功能不启用，默认值为 10 秒。

2.1.2.4 屏保设置

1） 屏保背光亮度：设置屏保亮度用，取值范围：1-255，默认值：10；
2） 进入屏保时间：设备无操作达到设定时间后进入屏保状态，即屏幕自动变暗（变暗程度与屏保背光亮度值相关），取值范围：0-255 分钟，默认值：5 分钟，0 表示关闭屏保功能。

2.1.2.5 记录查询

验证日志查询（最多能存 122880 条）

本系统在每次用户成功后，都会生成一条用户的验证日志记录，保存了用户通过验证的工号、日期、时间，具有完善的考勤功能；只有管理员可以在设备上查询验证日志。(管理员登录的身份验证及管理操作设备无管理记录产生)

注：如果记录数超过 122880 条，则自动覆盖最早生成的记录。记录较多时会影响查询的速度，为了提高查询效率，建议用户可以根据实际情况来定时清空设备中的记录

2.1.2.6 系统复位

指纹仪有完善的用户权限管理。但为了避免拥有管理权限的用户不在场，而客户又急需设置本系统，本系统特设了一个系统复位功能。管理员可以进入系统将设备恢复到出厂时的设置。

特别注意事项：

1、 系统复位功能不需要复位密码，在设备没有管理员的状态下，任何人均可以恢复出厂设置，当设备中有管理员用户，则需管理员登录成功后才能恢复出厂设置，客户在成功安装后，正式使用前，需自行注册管理员，并妥善保管好管理员登录密码。

2、 系统复位是在客户不得已的情况下才使用的。若使用系统复位功能，则该系统中原有的用户数据将全部丢失，参数设置也将恢复成出厂时的设置。需重新登记用户才可使用。

3、 系统复位之前必须先做好数据备份，若没做备份，数据丢失后无法找回。

2.2 开门验证功能

由于进入管理菜单时的身份验证操作与开门验证的操作流程基本相同，后文只针对开门验证操作进行具体说明。

两者的不同点在于：

1、 前者验证通过之后的动作是进入管理菜单，后者验证通过之后的动作是进行开门操作。
2、 前者不论在哪种验证模式下，使用何种验证方式，都必须输入完整的用户编号、密码、指纹，即只能使用 1：1 验证；后者则在非密码开门的情况下，可由用户根据情况自行选择是否输入用户编号，即可以使用 1：1 和 1：N 验证。

如果用户使用报警手指进行验证且验证成功，则门禁系统在开锁或进入管理菜单的同时，会发出远程报警信号，但不发出本地报警信号。

2.2.1 开门方式

2.2.1.1 指纹开门

在“只使用指纹” 或在“指纹或密码”的验证模式下，用户可直接用已登记过的手指进行指纹验证，如果指纹比对正确则开门。

2.2.1.2 密码开门

在“指纹或密码”验证模式下，用户除了可使用上述的指纹方式开门外，还可采用输入密码的方式开门，具体步骤如下：首先输入用户完整的编号并按“Next”键后，再输入密码进行验证，如果密码验证正确则开门。

2.2.1.3 指纹与密码开门

在“指纹与密码”验证模式下，用户必须同时通过上述指纹开门验证和密码开门验证，才能开门。此开门方式提高了整个系统的安全性。

在此验证模式下，用户既可先通过指纹开门验证后，再直接输入密码进行密码开门的验证；也可先通过密码开门验证后，再直接放手指进行指纹验证。

2.2.2 指纹验证的比对方式

用户使用指纹验证方式开门时，根据操作方式的不同，会得到不同的比对速度：
1）输入完整用户编号并确认后再用指纹验证（1:1）；
2）直接用指纹验证（1:N）；
以上 2 种操作方式所得到的比对速度依次为：1:1 最快； 1:N 最慢。
用户可根据需要选择不同的验证比对方式。
可以使用不同速度的验证比对方式。以下是对 2 种不同的比对方式的详细介绍：
注：只有验证模式为“指纹与密码”时才能使用 1:1、1：N 对比方式，“指纹或密码”和“指纹”这两种验证模式只能使用 1：N 的对比方式。

2.2.2.1 完整用户编号 + 指纹 （1：1 验证）

在待机状态下，用户输入完整的用户编号并按确定键确认后，再用此用户已登记的某枚手指轻按传感器进行指纹比对。在此情况下，指纹比对仅对该用户编号的指纹数据进行比对，最大限度地缩小了比对范围，加快比对速度。若指纹比对成功，则验证通过。

2.2.2.2 直接指纹验证 （1：N 验证）

指纹“一比多”验证不需要输入用户编号。在待机状态下，用户直接用已登记的某枚手指轻按传感器，该手指指纹将和设备指纹库内所有指纹进行比对，若比对成功则验证通过。

3 操作说明

特别提示：在本说明书中，如无特别指明，在指纹处理器的键盘区域的“OK”键表示“回车”、“确定”、“是”等确认键，“Esc”键表示“退出”、“取消”、“删除”“否”等取消键，“Next”键表示“下一个”、“下一位”等切换键。

3.1 传感器的使用

指纹传感器是精密元件，应避免用尖硬物件戳其表面以防划伤（尤其是安装时更要注意!），应保持其表面干净清洁，如有污迹可用药用脱脂棉花沾水横向擦拭清洁。一般情况下，推荐登记左右拇指、食指、中指，推荐至少登记两枚指纹，如：左右食指，这样户可以使用已登记的任一手指验证，也避免因忘记登记了哪一个手指或者指纹受到了磨损而导致识别不方便的情况。

手指的放置

为了取得清晰的指纹图像，手指指纹面应紧贴传感器，手平压于指纹采集窗口上指纹纹心尽量对正窗口中心，并按照下图正确位置放置，如图1g：

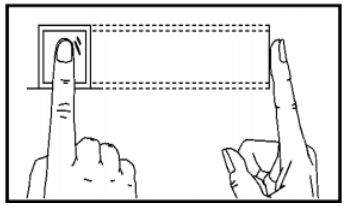
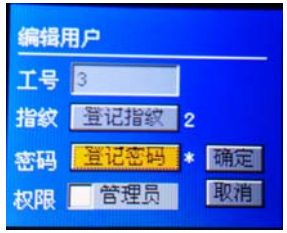


图 1g

只能编辑密码和权限这两项，编辑完成后将光标切换至“确定”按钮并按“OK”键保存如下图；



若无需保存可直接按“Esc”键返回“管理用户”界面。

3. 删除用户

在“管理用户”界面，按上移或者下移键选中所需删除的用户，然后按下数字“0”键，如下图所示：此时按下“OK”键则删除工号为 3 的用户；若无需删除则按“Next”切换至“取消”按钮后按下“OK”键。在设备中只能逐个删除用户。

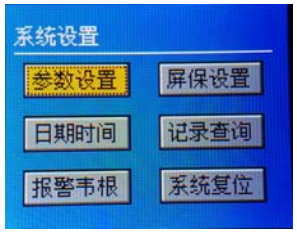
4. 上移/下移

在“管理用户”界面，按数字键“2”则光标上移一个单位，按数字键“8”则下移一个单位，按数字键“4”则向前翻一页，按数字键“6”则往后翻一页。

5. 右下角数字 A/B 表示：以 10/50 为例，10 表示当前页为第 10 页，50 表示总共有 50 页。

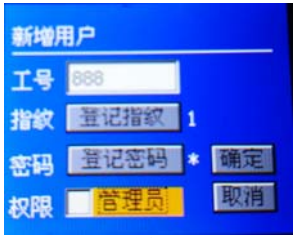
3.3.2 系统设置界面

在管理界面选中“系统设置”，按“OK”键进入“参数设置”界面，如下图所示：



3.3.2.1 参数设置

选中“参数设置”按“OK”键，进入“参数设置”界面如下图所示为默认设置：

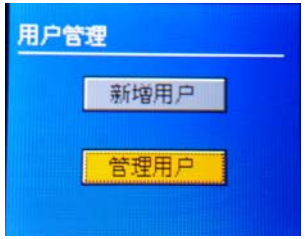


（图 12）

（图 13）

3.3.1.2 管理用户

在“用户管理”界面按“Next”键选中“管理用户”按“OK”键，进入“管理用户”界面（如下图 2）



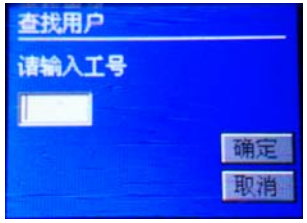
（图 1）

（图 2）

进入管理用户界面，可查看到用户工号、是否登记有指纹及指纹枚数、是否登记有密码、是否是管理员（管理员工号前带#号）、根据工号查找用户、编辑用户、删除用户、上移或者下移光标、翻页。

1. 查找用户

1） 查找（1）：按数字键“1”进入“查找用户”界面，如下图



2） 输入所需查找用户的完整工号，按“Next”键将光标切换至“确定”按钮，按下“OK”键，若工号不存在系统提示：用户不存在；若工号存在，则锁定该用户，如下图所示（以 260 为例）：

2. 编辑用户

在“管理用户”界面，按上移或者下移键选中所需编辑的用户，然后按下“OK”键进入编辑用户界面，

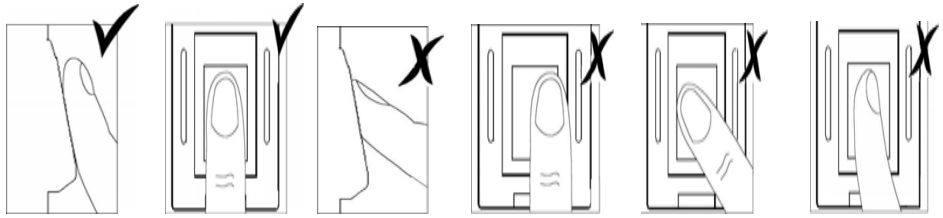


图 1a 图 1b 图 1c 图 1d 图 1e 图 1f

说明：

图1g、图1a和图1b显示正确的手指放法，图1a为侧面图，图1b、图1g为正面图。

图1c、图1d、图1e和图1f为错误的手指放法，图1c为侧面图（垂直），图1d（太偏）、图1e（太歪）和图1f（倾斜）为正面图。

（注：轻放手指到传感器上自动验证，须按键触发【手指务必要接触金属边框】。此说明在下文中不再赘述）

表1-1登记不成功或者质量不高的常见原因

使用干燥或脏的手指	1.处理干燥皮肤的方法是用力摩擦手指与手掌，因为摩擦可以产生油脂。 2.若手指很干燥，可采用哈气等办法，适当湿润手指。
施加压力不够或者过大	用户应该将手指平按在指纹采集头上。
如何选择手指	1.推荐登记左右食指或者左右中指选择指纹质量比较好的手指，没有磨损或损坏的用户通常选择食指，但是如果食指指纹质量不高，可选择中指或者无名指。 2.如果用户的手指比较小，那么通常选择大拇指。 3.如果用户想要多登记备份指纹的话，那么选择不容易受磨损和伤害的手指，如无名指。
按手指的位置	1.保存手指水平按在指纹采集头上，并且覆盖尽可能大的面积。 2.不要垂直点击指纹在指纹采集头上；不要快速的敲击手指；也不要滑动手指。
指纹图像变化的影响	1.由于某些特殊原因如脱皮、受损等导致指纹图像变化，会影响考勤效果。 如果用户的手指质量差，主要指手指脱皮的情况，以至一个星期以后验证就难以通过，需要重新登记；或者采用密码考勤的方式。
其它的原因	1.不管怎样努力，有极少一部分的人的指纹质量很差，不能正常验证。在这种情况下，考虑使用 ID+指纹的验证方式，适当降低 1：1 匹配阀值或采用密码考勤方式

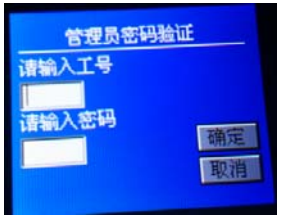
3.2 待机状态

在连接好指纹仪和控制器，并给系统上电后，数秒后进入待机状态，显示日期和时间，如下图所见：

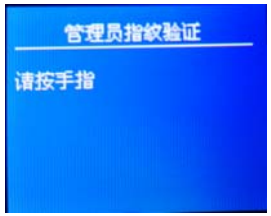
3.3 管理界面

在“空机”或设备中无管理员的待机状态下按“Esc”键，会出现如下图 1 的屏幕信息；在有管理员的待机状态下按“Esc”键，则出现如下图 2 的屏幕信息：

（图 1）



（图 2）

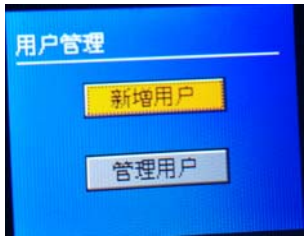


（图 3）

图 1 状态按键 “OK”，可进入用户管理界面，图 2 状态需输入正确管理员工号和密码，按“Next”键将光标切换到“确定”按钮，按“OK”键，进入图 3 界面后成功验证管理员指纹才能进入图 1 界面。

3.3.1 用户管理界面

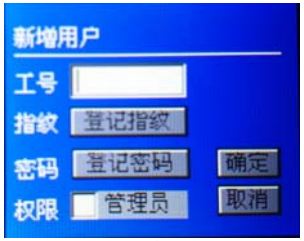
选中“用户管理”，按“OK”键，进入“用户管理”界面，屏幕显示如下



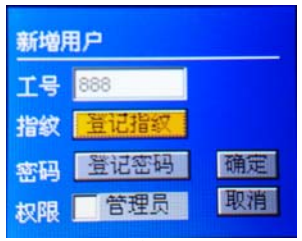
3.3.1.1 新增用户

在“用户管理”界面选中“新增用户”按“OK”键，进入“新增用户”界面（如下图 1），用户可通过键盘输入一个取值范围在 0～999 之间的数值作为工号（如下图 2），按“Next”键选中“登记指纹”后再按“OK”键，将出现下面的登记指纹界面（如下图 3）：

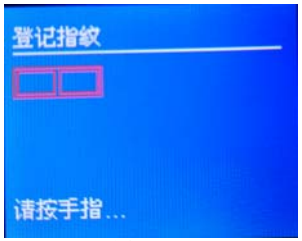
注意：如果用户输入的“工号”带有前零，如“086”，系统会自动忽略前零并将之解释为“86”，即验证通过时显示的用户编号是“86”；同一枚指纹在同一台指纹设备中不能重复注册，此说明在下文中不再重复；



（图 1）



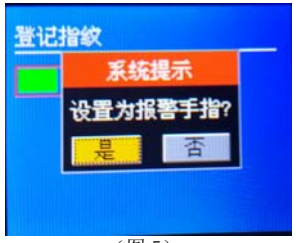
（图 2）



（图 3）

此时应当用需要登记指纹的手指轻按传感器，按照设备上提示语来操作，登记一个手指要对指纹采样两次，所以当第一次指纹图象的采集成功后如图 4 所示；第二次指纹采样成功如图 5 所示时用户可以把手指移开，根据用户的选择是否将该指纹设置为报警指纹，按下“OK”键后如图 6 所示：

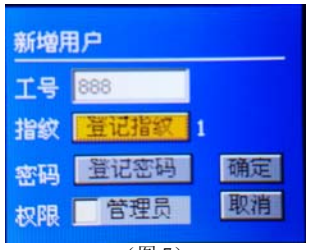
（图 4）



（图 5）

（图 6）

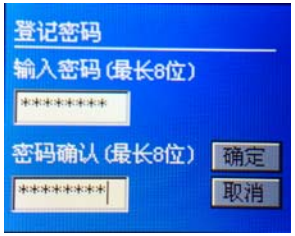
按“Esc”键返回新增用户界面，如图 7 所示表示已成功登记一枚指纹，第二、第三枚指纹的登记与第一枚指纹的登记步骤雷同，在此不再赘述。



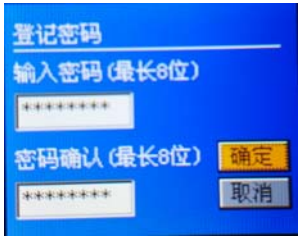
（图 7）

按“Next”键选中“登记密码”后（如图 8）再按“OK”键，将出现下面的登记密码界面（如图 9），密码可以设置为 1-9 位的任意数值，最长为 8 位数，如果用户设置的“密码”带有前零：如“0123456”，则系统会保留前零；也就是用户在进行密码验证时也必须输入“0123456”，才能验证成功；此说明在下文中不再重复，如图 9 所示，设置密码要连续输入两次，两次相同才算设置成功；正确设置密码后按“Next”键选中“确定”按钮，按“OK”键，如图 11 所示；

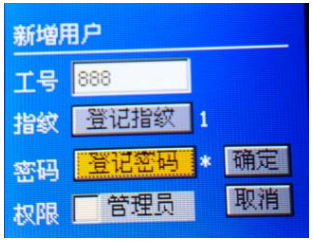
（图 8）



（图 9）



（图 10）



（图 11）

按“Next”键选中“管理员”选项，按“OK”键可以取消勾选管理员/勾选管理员选项（如图 12、13），勾选管理员表示将该用户设置为管理员，反之亦然。（管理员必须同时注册指纹和密码；非管理员可以只注册指纹或密码，也可以注册指纹和密码），登记完成后按“Next”键选中“确定”按钮，按“OK”键，保存完成后返回用户管理界面。