人脸门禁一体主机

快速操作手册

V1.0.2

前言

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 防静电	表示静电敏感的设备。
 当心触电	表示高压危险。
 激光辐射	表示强激光辐射。
 风扇警告	表示危险运动部件，请远离运动风扇叶片。
 当心机械伤人	表示设备部件机械伤人。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

版本号	修订内容	发布日期
V1.0.2	• 更新错误。 • 更新使用安全须知。	2021.07
V1.0.1	更新“10 寸设备”章节，增加一个 10 寸设备。	2020.12
V1.0.0	首次发布。	2020.09

使用安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

操作要求

注意

- 请在设备运行前检查供电电源是否正确。
- 请勿在适配器上电时拔下设备侧电源线。
- 仅可在额定输入输出范围内使用设备。
- 请在允许的湿度和温度范围内运输、使用和存储产品。
- 请勿将液体滴到或溅到设备上，并确保设备上没有放置装满液体的物品，防止液体流入设备。
- 请勿拆卸设备。

安装要求

警告

- 严禁将电源适配器上电后再连接设备，请在断电状态下连接电源适配器和设备。
- 请严格遵守当地各项电气安全标准，确保环境电压稳定并符合设备供电要求。
- 请勿同时对设备提供两种及以上供电方式，否则可能导致设备损坏或造成安全风险。

注意

- 高空作业人员须佩戴安全帽、使用安全带，做好防护措施，以确保人身安全。
- 请保持设备的水平安装，或将设备安装在稳定场所，注意防止本产品坠落。
- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请将设备安装在通风良好的场所，切勿堵塞设备的通风口。
- 请使用产品制造商提供的适配器或机箱电源。
- 请使用满足 SELV（安全超低电压）要求的电源，并按照 GB8898（IEC60065）或 GB4943.1（IEC60950-1 符合 Limited Power Source（受限制电源））的额定电压供电，具体供电要求以设备标签为准。
- 请将 I 类结构的产品连接到带保护接地连接的电网电源输出插座上。

目录

第 1 章 结构外观

1.1 7 寸设备

7 寸设备分为不带指纹和带指纹两种。

图1-1 7 寸 A 外观尺寸（1）（单位：mm[inch]）

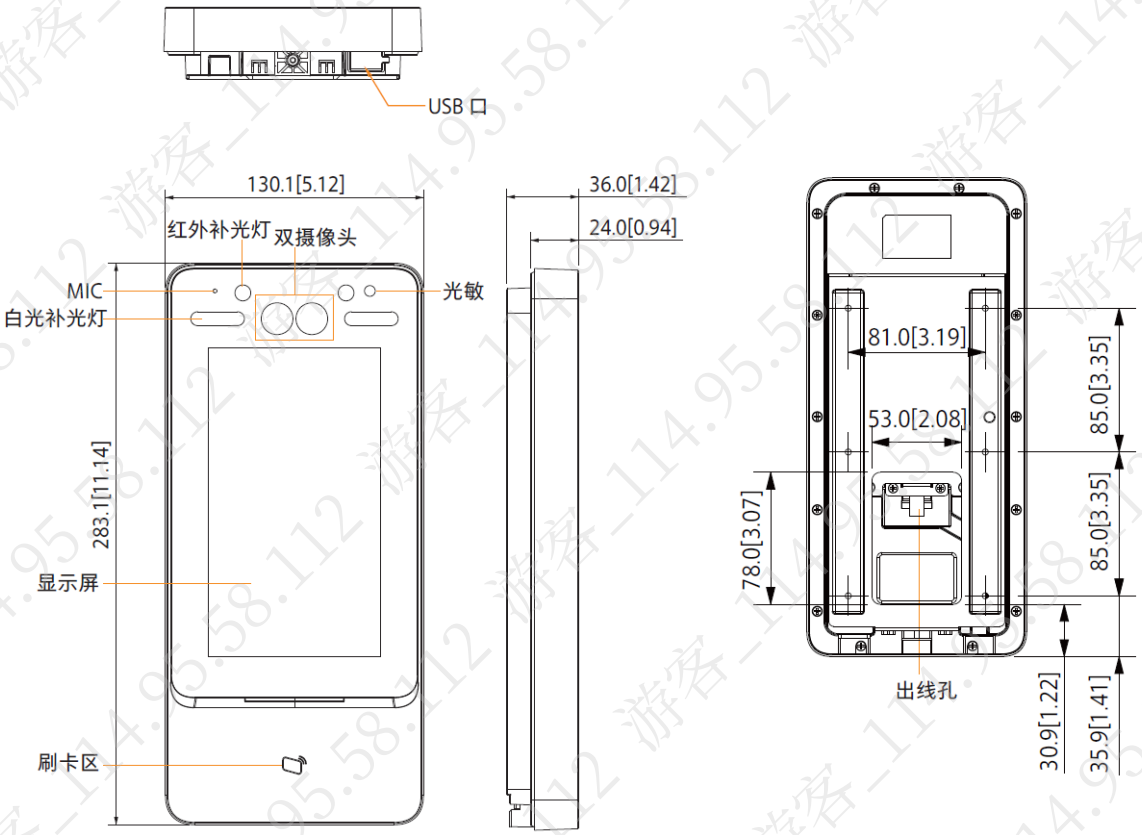


图1-2 7 寸 A 外观尺寸（2）（单位：mm[inch]）

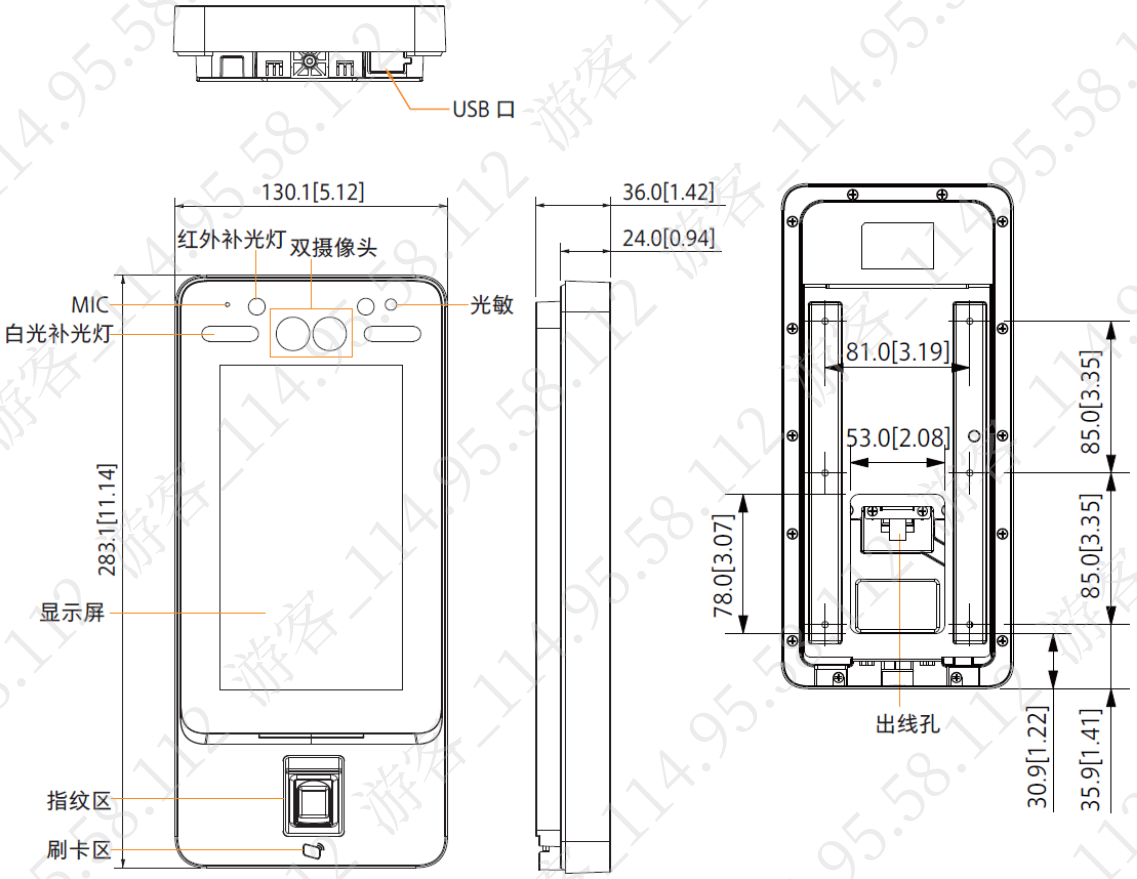


图1-3 7 寸 B 外观尺寸（1）（单位：mm[inch]）

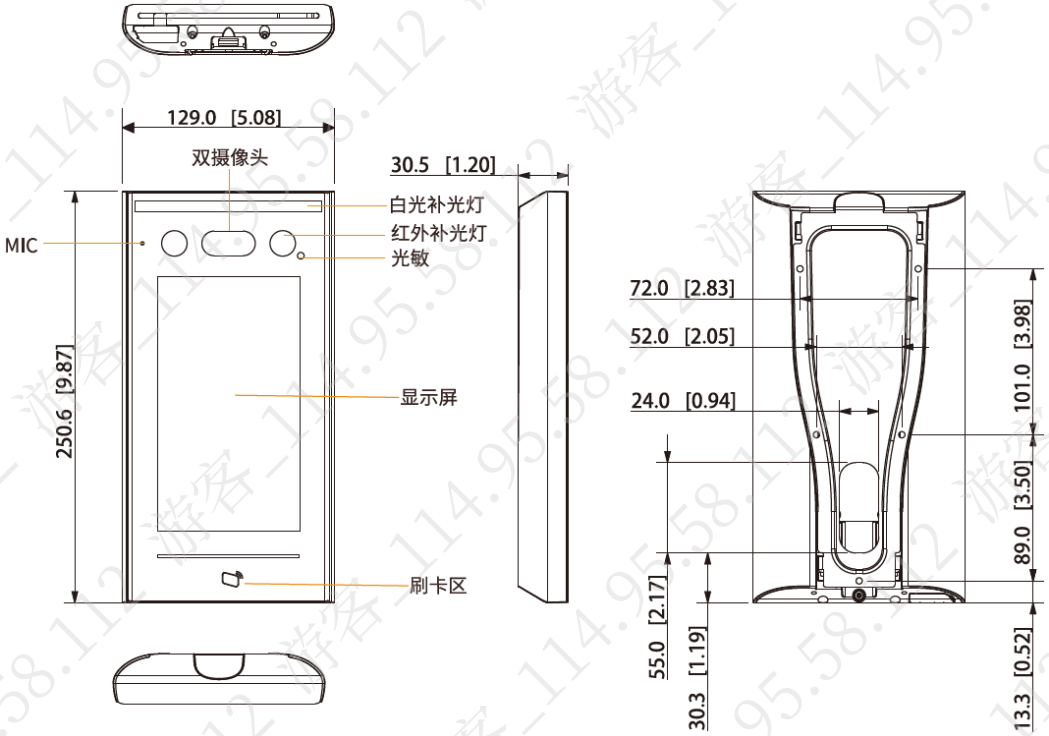


图1-4 7 寸 B 外观尺寸（2）（单位：mm[inch]）

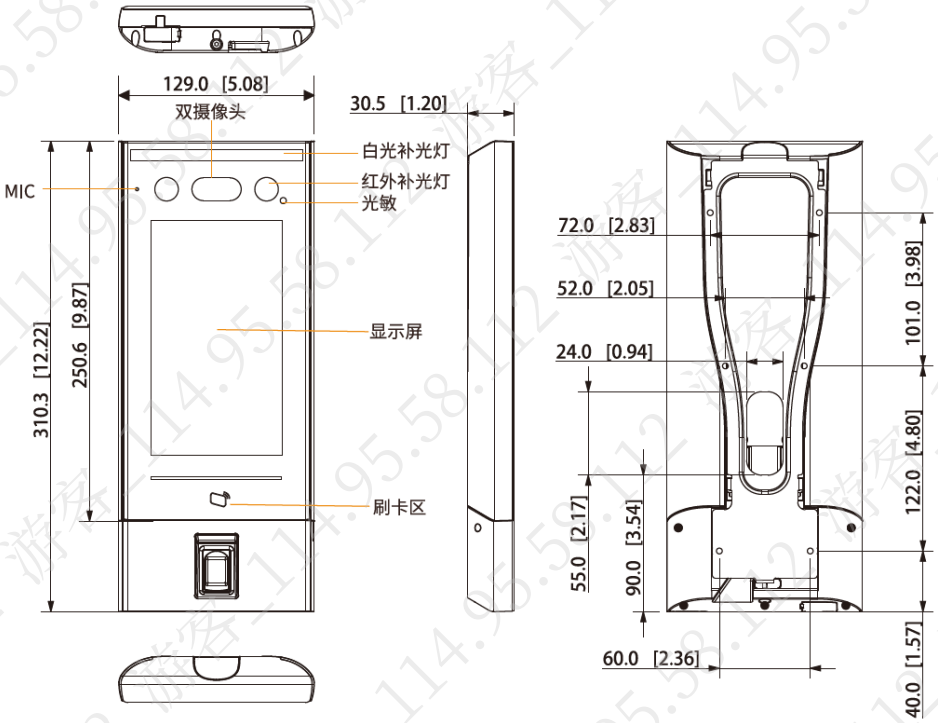
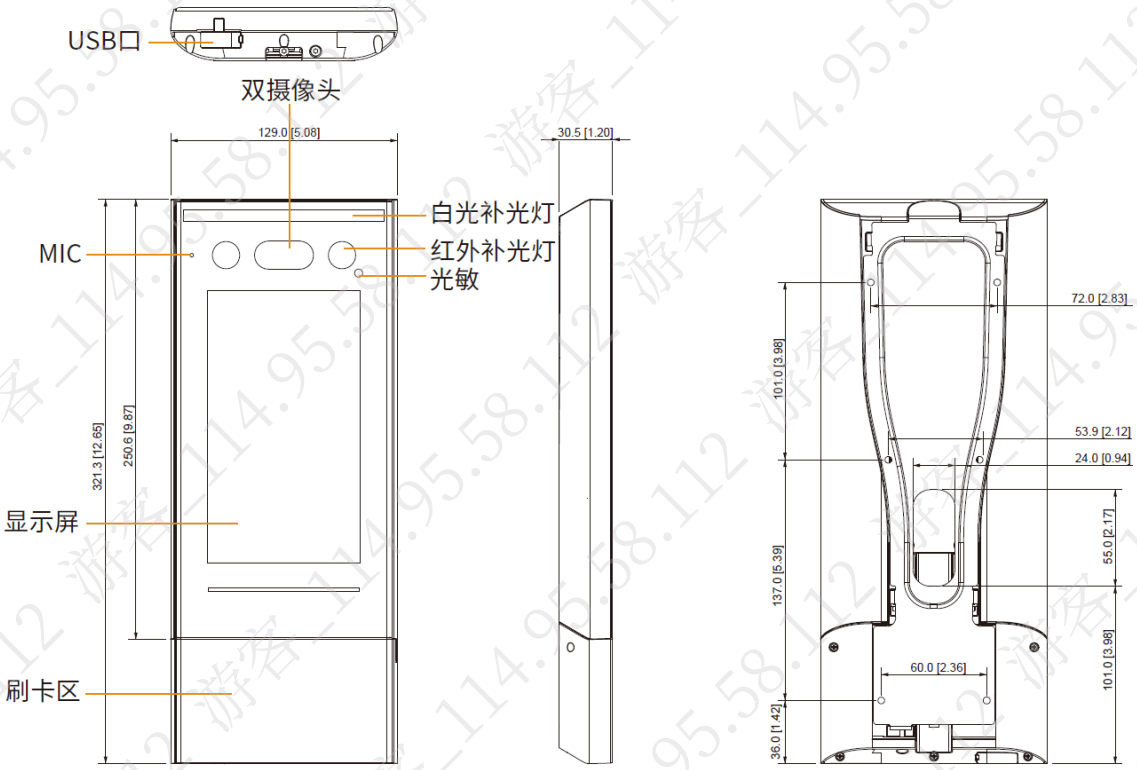


图1-5 7 寸 B 外观尺寸（3）（单位：mm[inch]）



1.2 10 寸设备

图1-6 10 寸外观尺寸（1）（单位：mm[inch]）

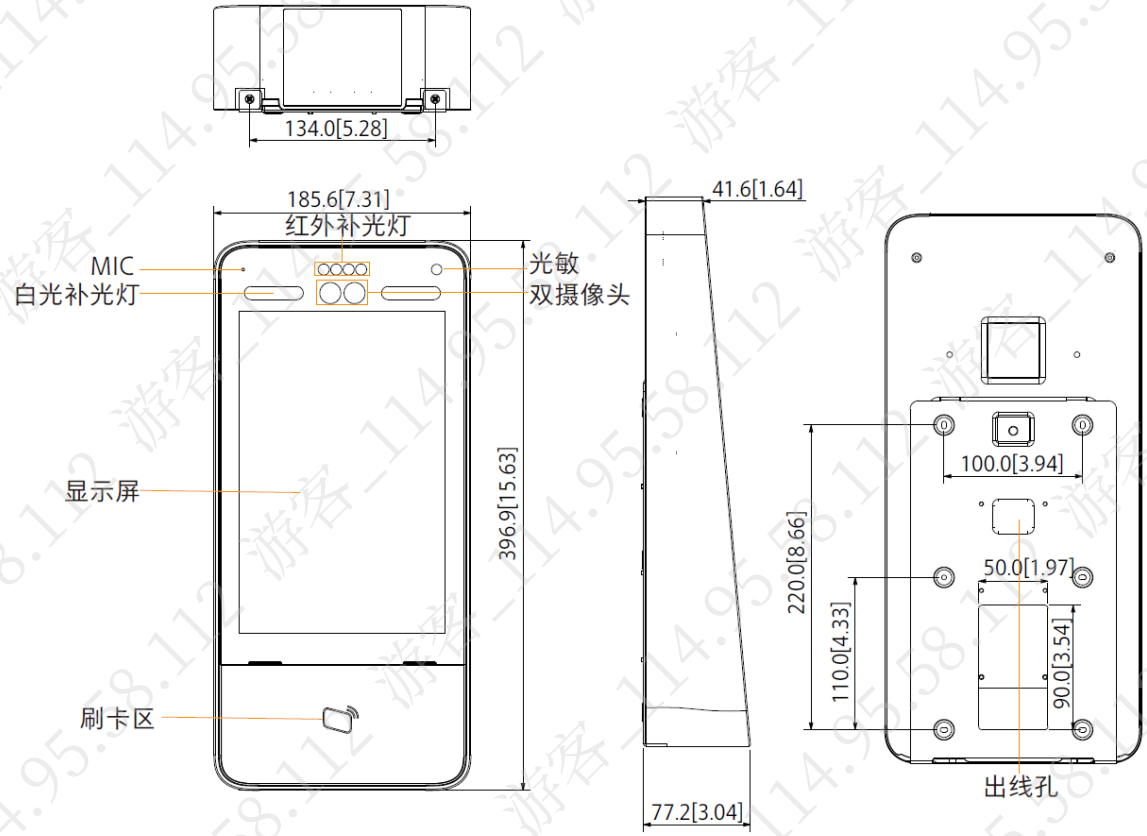


图1-7 10 寸外观尺寸（2）（单位：mm[inch]）

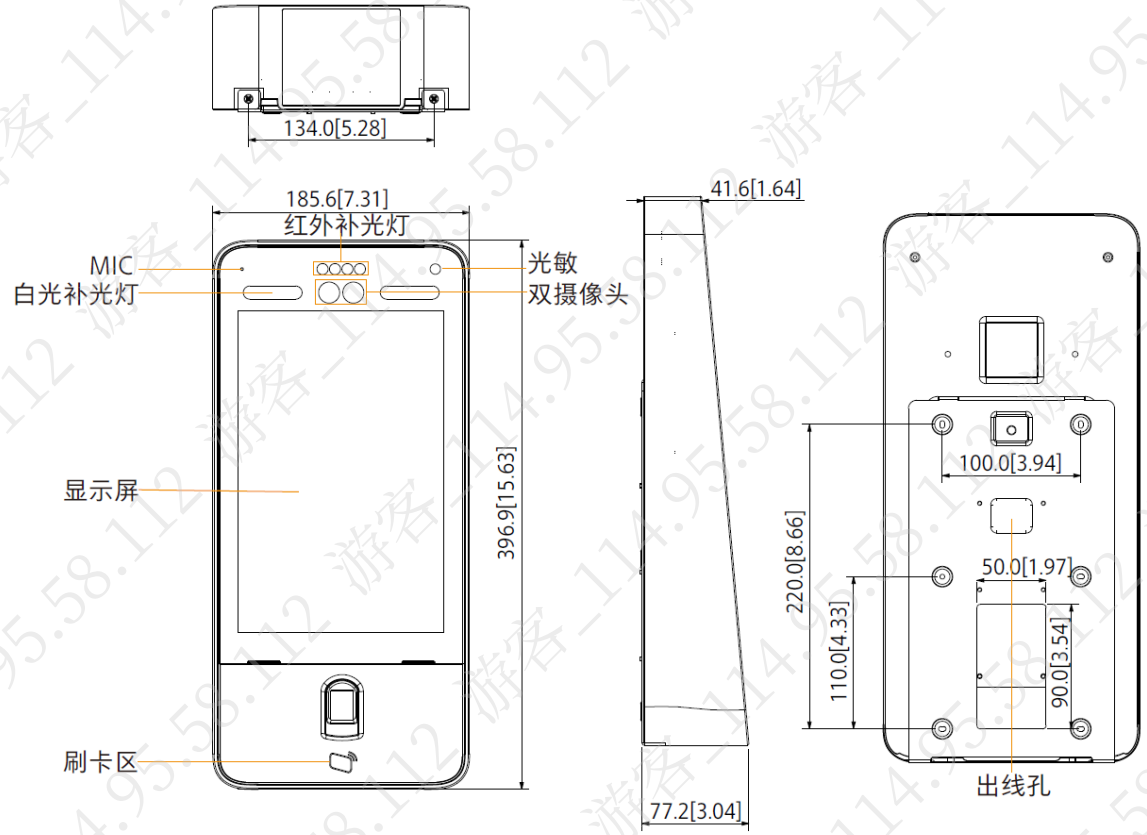
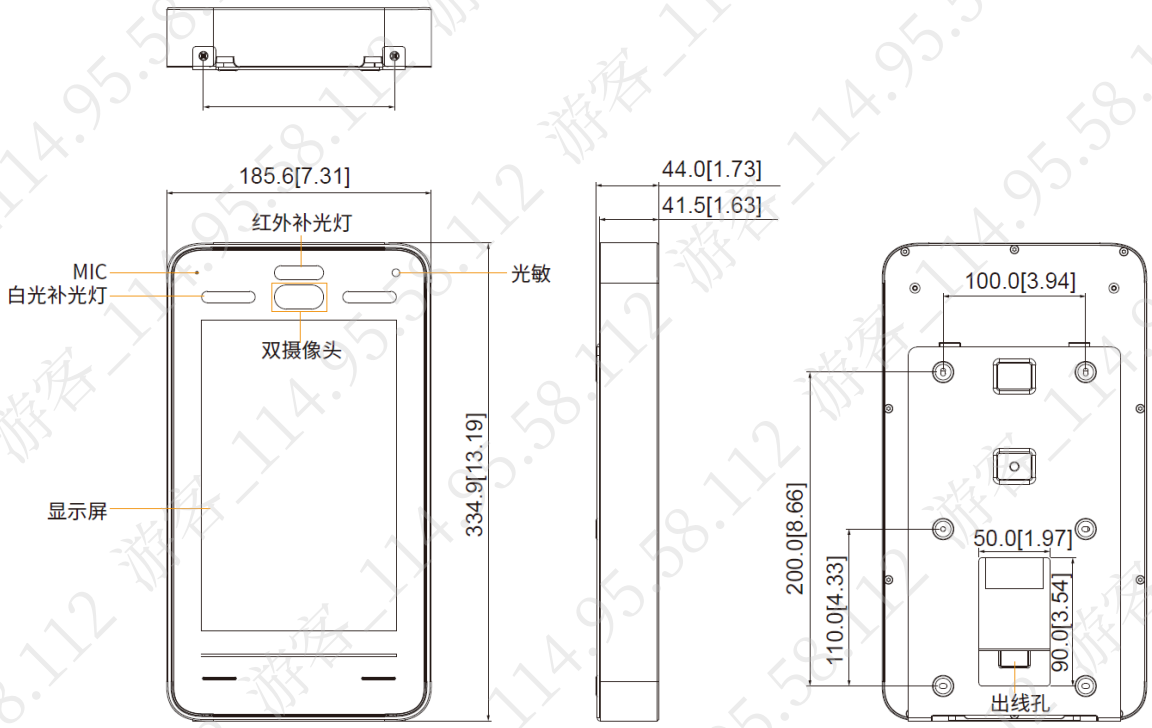


图1-8 10 寸外观尺寸（3）（单位：mm[inch]）



第 2 章 安装指导

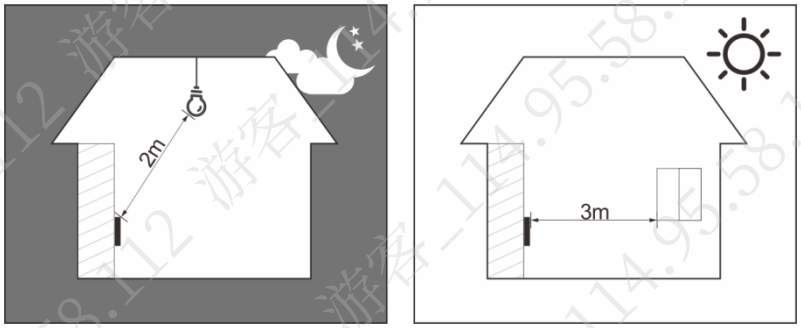
2.1 安装环境

- 离设备 0.5 m 处的最小光源照度不低于 100 Lux。

图2-1 安装环境光源参考值

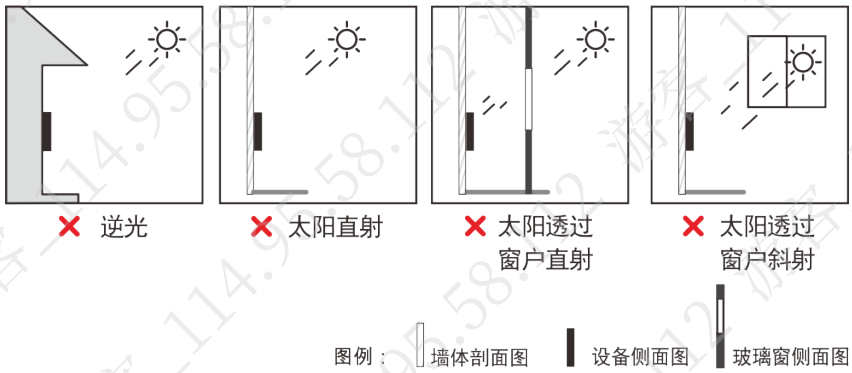
- 建议将设备安装在室内，距离窗口、门口 3 m 以外，距离灯源 2 m 以外。

图2-2 推荐安装位置



- 避免逆光、阳光直射、斜射或灯光近距离照射。

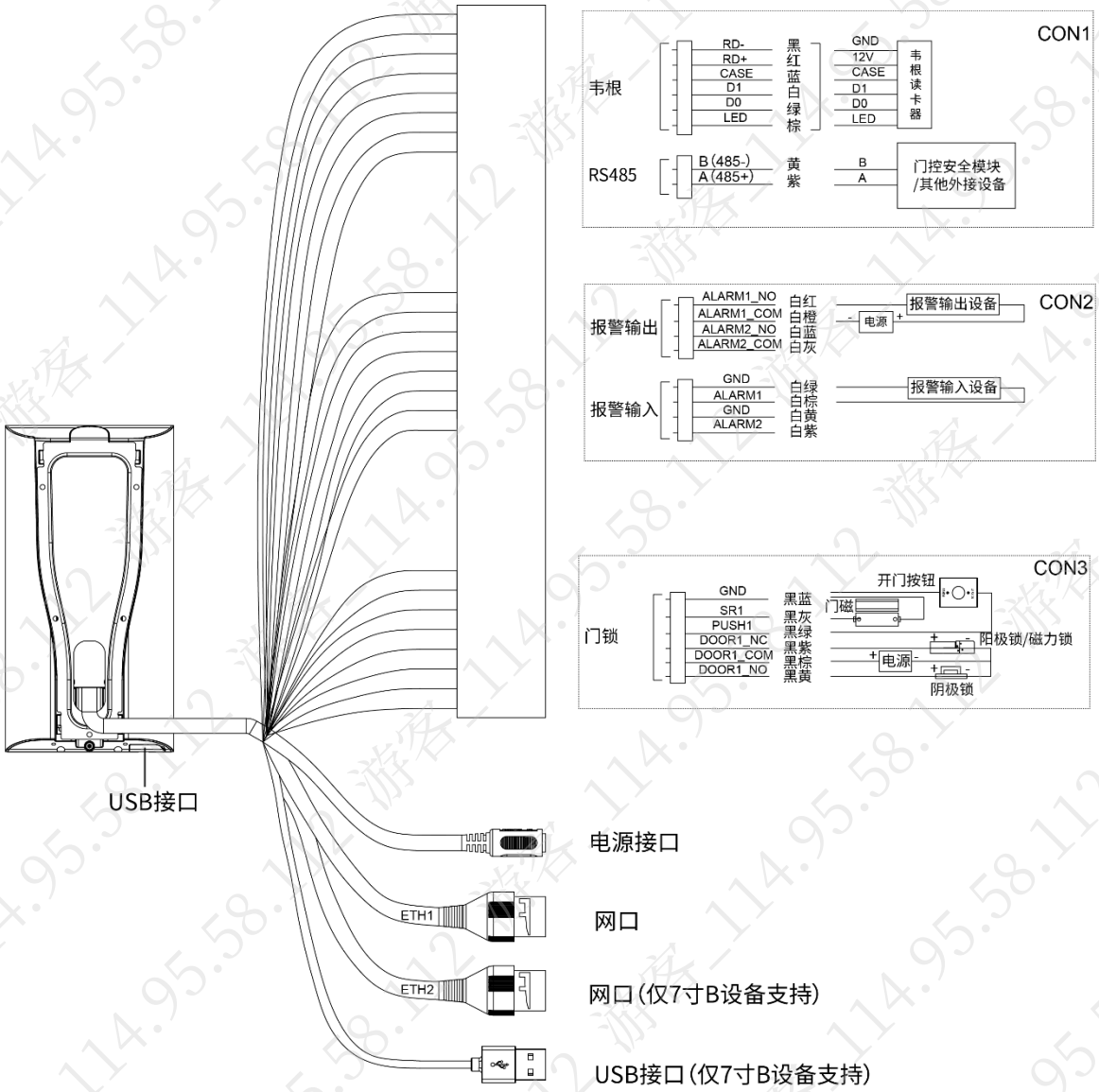
图2-3 影响使用效果的安装位置



2.2 设备接线

所有的设备接线说明相同，以 7 寸 B 设备为例介绍。

图2-4 接线说明



说明

- 请查看“功能设置 > 门控安全模块”是否启用，如启用，则需购买配套的门控安全模块，门控安全模块需单独外接电源供电。
- 门控安全模块启用时，本设备的开门按钮、锁控制和消防联动开门均无效。

2.3 设备安装

7 寸设备和 10 寸设备安装方式相同，推荐安装高度(以镜头中心到地面高度)为 1.4 米。

图2-5 安装距离

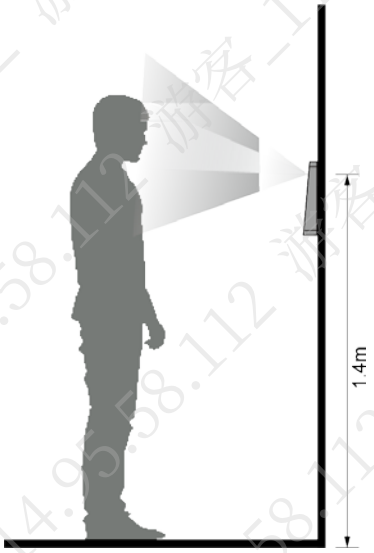


图2-6 7 寸 A 设备墙面安装

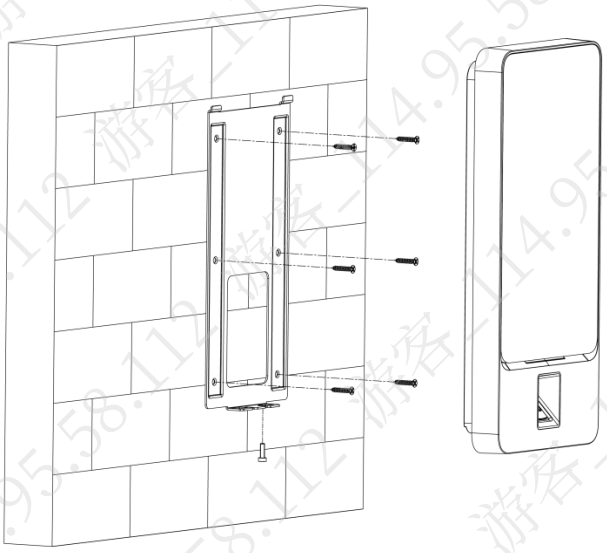
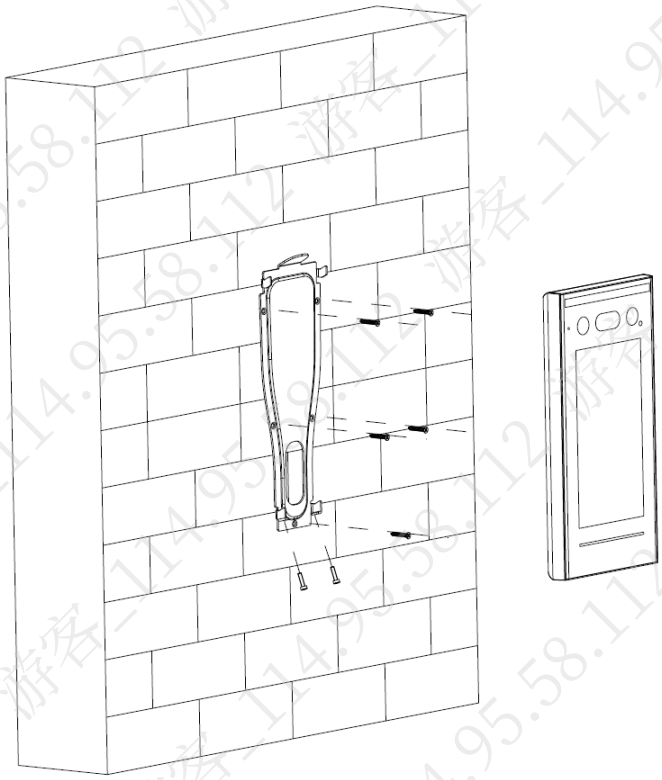


图2-7 7 寸 B 设备墙面安装



步骤1　按照支架上的孔位，在墙上打 6 个支架安装孔和一个出线孔，并将膨胀管安装到安装孔内（以 7 寸 B 设备为例）。

步骤2　通过螺钉将支架直接固定于墙体。

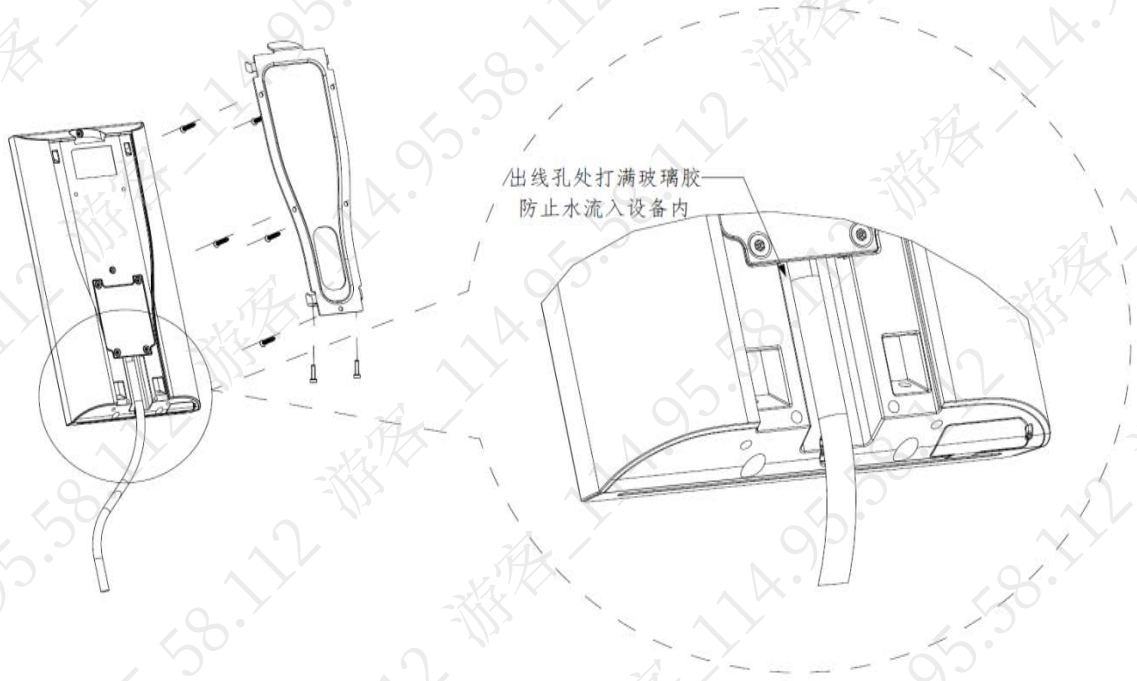
步骤3　参照“2.2 设备接线”为主机设备接线。

步骤4　将设备通过挂孔挂在安装支架的挂钩上。

步骤5　从设备底部，拧入螺钉，锁紧安装支架，完成设备安装。

步骤6　（可选）7 寸 B 设备线缆出线口需要点胶。

图2-8 7 寸 B 设备点胶示意图



第 3 章 系统操作

3.1 设备初始化

设备初次上电启动时，需要设置 admin 用户密码和手机号。该用户名和密码用于操作设备菜单，或登录配套的 WEB 端和软件平台。

图3-1 设备初始化

说明

- 手机即手机号码，若忘记设备管理员密码，可通过该手机号重置密码。
- 密码可设置为 8 位～32 位非空字符，可以由大写字母、小写字母、数字和特殊字符（除“'”、“"”、“;”、“:”、“&”外）组成，且至少包含 2 类字符。新密码和确认密码需保持一致。请根据密码强弱提示设置高安全性密码。

3.2 添加用户

可以通过录入编号、姓名、人脸等信息添加新用户。

步骤1 在待机界面中，按  。

步骤2 使用管理员权限登录系统，选择“人员管理 > 新建用户”。

说明

界面图以 7 寸设备为例，请以实际界面为准。

图3-2 新建用户

步骤3　设置参数项。

表3-1 新建用户参数说明

参数	说明
编号	输入用户编号，用于识别不同的用户，每个编号都是唯一的，最多支持 32 个字符（包括数字、字母或者数字和字母的组合）。例如：工号。
姓名	输入用户姓名，最多支持 10 个汉字或者 32 个字符（包括数字、符号和英文）。
指纹	采集用户指纹，一个用户最多可采集 3 枚指纹，每枚指纹需要验证 3 次，请根据语音提示进行操作，完成后提示“登记成功”。 选择对应指纹下面的单选框，可将对应指纹设置为胁迫指纹。设备开启胁迫报警后，使用该指纹开门时，将触发胁迫报警。详细介绍请参见配套的使用说明书。 **说明** ● 不建议将第一枚指纹设置为胁迫指纹。 ● 仅带有指纹功能的设备支持指纹开门功能。
人脸	注册时请将人脸放置于采集框中心区域，自动完成抓拍，如对抓拍到的图片不满意，则选择重新录入。详细介绍请参见“附录 1 人脸录入/比对说明”。
卡片	卡片信息，每个用户可以登记 5 张卡片。在卡片登记界面，输入卡号或在刷卡区刷卡，系统将自动识别该卡卡号。 可将卡片设置为胁迫卡片。设备开启胁迫报警后，使用该卡片开门时，将触发胁迫报警。详细介绍请参见配套的使用说明书。
密码	开门密码，用户开门时所需输入的密码，密码支持 1 位～8 位数字。

参数	说明
用户权限	设置用户权限。 ● 用户，仅有门禁权限。 ● 管理员，可登录系统，配置设备相关参数。
时段	为用户配置门禁时段序号，在该时段内，用户门禁权限有效。时段详细配置请参见配套的使用说明书。默认值为 255，即不为该用户配置任何时段。
假日计划	为用户配置假日时段序号，在该时段内，用户门禁权限有效。假日时段详细配置请参见配套的使用说明书。默认值为 255，即不为该用户配置任何假日计划。
有效期	设置该人员门禁有效时间。
用户类型	用户类型可设置为以下类型： ● 普通用户，该类型用户可以正常使用门禁权限。 ● 黑名单用户，该类型用户进入时，后台会对服务人员进行提醒。 ● 来宾用户，该类型用户有门禁使用次数/时间的限制，超过使用次数/时间后，门禁权限失效。 ● 巡逻用户，该类型用户可在任何时间巡逻打卡，但没有门禁权限。 ● VIP 用户，当该类型用户进入时后台对服务人员提醒。 ● 特殊用户，当该类型用户进入时，开门持续时间增加 5 s。
使用次数	使用次数，当用户类型为来宾用户时，可设置该用户门禁权限的使用次数。

步骤4　参数配置完成后，按  保存。

系统提示“添加用户成功”。

第 4 章 WEB 操作

可以在 WEB 界面配置设备的网络参数、视频参数和门禁参数等，具体请参见配套使用说明书，本文只介绍 WEB 登录。

步骤1　打开 IE 浏览器，在地址栏里输入设备的 IP 地址（默认地址为 192.168.1.108），按【Enter】键。

说明

- PC 与设备在同一局域网内。
- 7 寸 B 设备支持双网口，网口 1 的默认地址为 192.168.1.108，网口 2 的默认地址为 192.168.2.108。

系统显示登录界面。

图4-1 登录

步骤2　输入“用户名”和“密码”。

说明

- 设备默认管理员用户名为 admin，密码为设备初始化时设置的登录密码。为确保安全，建议定时更改管理员密码，并妥善保存。
- 如果遗忘了 admin 的登录密码，可单击“忘记密码？”进行重置，重置密码的详细操作请参见配套使用说明书。

步骤3　单击“登录”。

附录1 人脸录入/比对说明

注意事项

- 登记时戴眼镜、戴帽子和胡子都可能影响登记效果。
- 戴帽子请勿遮住眉毛。
- 胡子过长或者面积过大会影响登记效果，建议登记和使用中胡子变化不要太大，否则会影响识别。
- 登记和验证时，请保持脸部清洁。
- 设备距离灯源至少 2 米，距离窗口及门口至少 3 米；避免逆光、阳光直射、斜射或灯光近距离照射。

注册说明

可以在设备端和平台端注册人脸信息，平台端注册请参见配套的平台使用说明书。

附录图1-1 人脸注册-设备端

说明

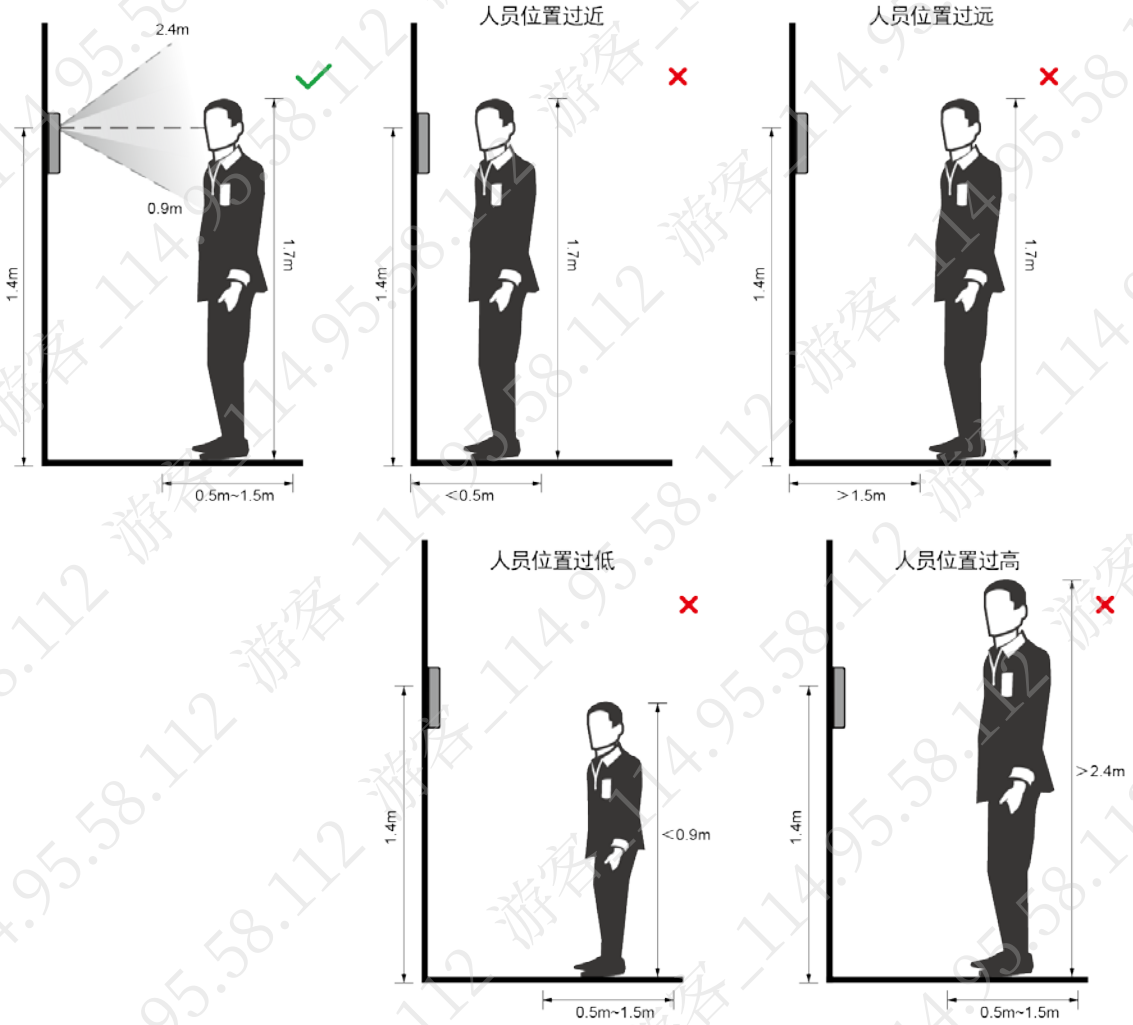
- 注册过程中请勿晃动，以免注册失败。
- 录入时请避免 2 张人脸同时出现在框内。

将人脸放置于采集框中心区域，设备自动完成抓拍，结束后完成人脸采集。

人脸位置

人脸距离设备过高、过低、过近或者过远，均会影响录入和比对的效果，请参照正确示例录入和比对。

附录图1-2 人脸位置示意



人脸要求

为了保证人脸录入和比对的精确度，请注意以下事项。

- 请保持脸部清洁，建议露额，头发不要遮挡。
- 请勿戴眼镜、戴帽子、胡子过长或者面积过大，以及佩戴影响人脸特征采集的饰品。
- 请双眼睁开、表情自然，请勿偏头、侧面、仰头和低头。
- 录入和比对时，请将人脸尽量位于窗口中心位置，请勿过近或者过远。

附录图1-3 头部示意图

附录图1-4 人脸位于窗口位置示意

录入说明

- 使用设备录入人脸时，录入过程中请勿晃动，以免录入失败。
- 通过软件平台导入图片时，请参考导入模板；图片像素范围处于 150×300≤分辨率≤600×1200 之间，建议图片像素在 500×500 像素以上，小于 100KB，图片名称与人员编号一致。
- 人脸在图片中的占比要求大于整张图片的 1/3，小于整张图片的 2/3。整张图片的宽：高之比不超过 1：2。

附录2 对讲功能操作说明

人脸门禁一体主机可作门口机使用，实现可视对讲功能。

前提条件

已在人脸门禁一体主机和对讲系统中做好配置，实现人脸门禁一体主机和室内机、管理机、平台客户端、手机 APP 的协议互通。详细介绍请参见配套使用说明书的“对讲设置”章节。

操作步骤

步骤4　在待机界面，按  。

步骤5　输入呼叫的号码，按  。

附录图2-1 拨号界面

附录3 扫描二维码说明

为了保证二维码扫描效果，请将二维码置于距离人脸门禁上的摄像头 0.3m～0.5m 处，二维码大小应不小于 30mm×30mm，二维码字节容量应小于 100 字节，并且需要保证二维码纸张平整。

附录图3-1 二维码与摄像头距离

附录4 指纹录入说明

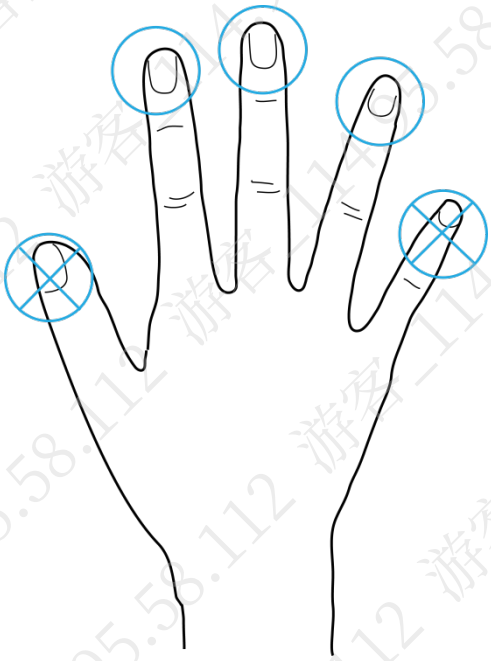
注意事项

- 指纹录入前手指及指纹采集面板应保持清洁，不沾油污、不沾水。
- 录入指纹时，手指平压于指纹采集窗口上，指纹纹心尽量对正窗口中心。
- 请勿将指纹采集面板置于阳光强光直射、温度过高、湿度过高环境。
- 指纹磨平或指纹较浅，请选择其他认证方式。

推荐手指

推荐使用食指、中指和无名指。大拇指和小拇指不容易放到采集窗口上。

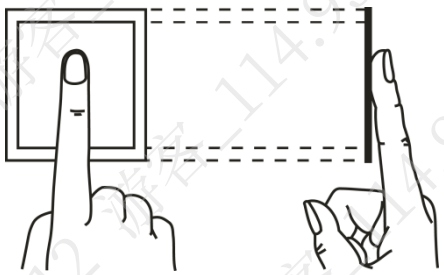
附录图4-1 推荐手指



按压方法

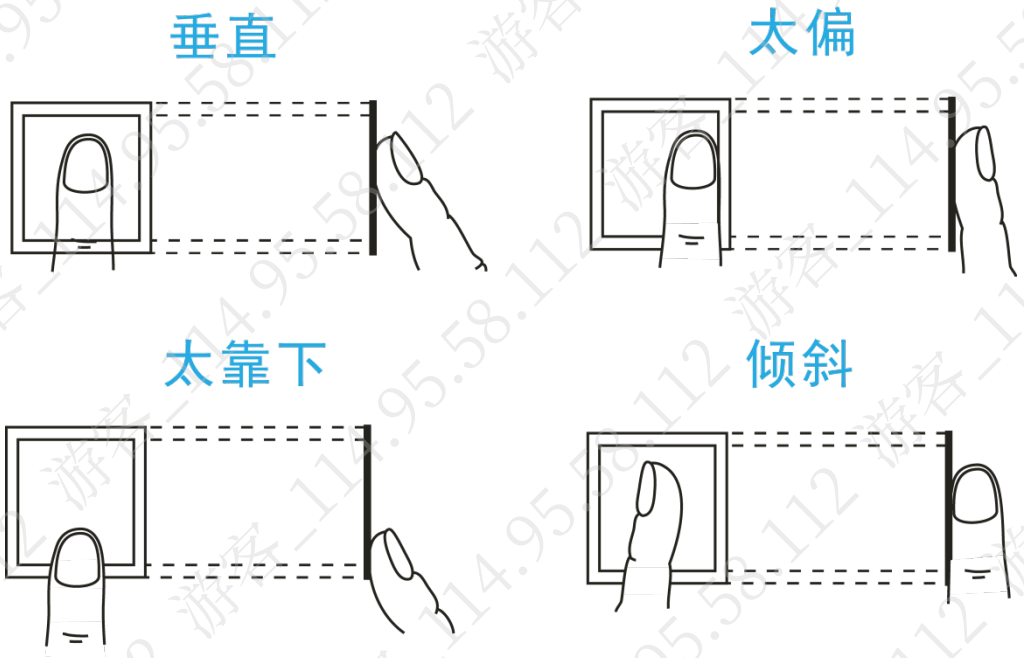
- 正确方法

附录图4-2 正确按压示意图



- 错误方法

附录图4-3 错误方法



附录5 法律声明

商标声明

- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的 PDF 文档无法打开，请使用最新版本或最主流的阅读工具。

附录6 网络安全建议

保障设备基本网络安全的必须措施：

1. **使用复杂密码**

   请参考如下建议进行密码设置：

   - 长度不小于 8 个字符。
   - 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
   - 不包含账户名称或账户名称的倒序。
   - 不要使用连续字符，如 123、abc 等。
   - 不要使用重叠字符，如 111、aaa 等。

2. **及时更新固件和客户端软件**

   - 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
   - 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

1. **物理防护**

   建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如 U 盘、串口）等物理接触行为。

2. **定期修改密码**

   建议您定期修改密码，以降低被猜测或破解的风险。

3. **及时设置、更新密码重置信息**

   设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. **开启账户锁定**

   出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源 IP 将会被锁定。

5. **更改 HTTP 及其他服务默认端口**

   建议您将 HTTP 及其他服务默认端口更改为 1024～65535 间的任意端口，以减小被攻击者猜测服务端口的风险。

6. **使能 HTTPS**

   建议您开启 HTTPS，通过安全的通道访问 Web 服务。

7. **MAC 地址绑定**

   建议您在设备端将其网关设备的 IP 与 MAC 地址进行绑定，以降低 ARP 欺骗风险。

8. **合理分配账户及权限**

   根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

9. **关闭非必需服务，使用安全的模式**

   如果没有需要，建议您关闭 SNMP、SMTP、UPnP 等功能，以降低设备面临的风险。

   如果有需要，强烈建议您使用安全的模式，包括但不限于：

   - SNMP：选择 SNMP v3，并设置复杂的加密密码和鉴权密码。
   - SMTP：选择 TLS 方式接入邮箱服务器。
   - FTP：选择 SFTP，并设置复杂密码。
   - AP 热点：选择 WPA2-PSK 加密模式，并设置复杂密码。

10. 音视频加密传输

如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

11. 安全审计

- 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
- 查看设备日志：通过查看日志，可以获知尝试登录设备的 IP 信息，以及已登录用户的关键操作信息。

12. 网络日志

由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

13. 安全网络环境的搭建

为了更好地保障设备的安全性，降低网络安全风险，建议您：

- 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
- 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用 VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
- 建立 802.1x 接入认证体系，以降低非法终端接入专网的风险。
- 开启设备 IP/MAC 地址过滤功能，限制允许访问设备的主机范围。