(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103366423 A
(43)申请公布日 2013.10.23

(21)申请号 201210093516.6

(22)申请日 2012.03.31

(71)申请人 深圳光启创新技术有限公司
地址 518034 广东省深圳市福田区香梅路1061号中投国际商务中心A栋18B

(72)发明人 刘若鹏 栾琳 刘敏 孙文超

(51)Int.Cl.
G07C 9/00(2006.01)

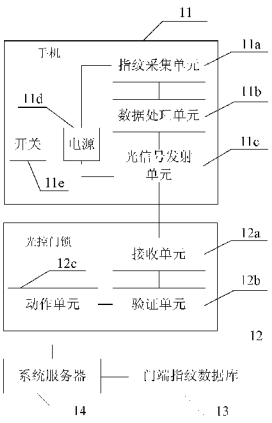
权利要求书1页 说明书4页 附图4页

(54)发明名称

基于手机指纹识别的光控门禁系统

(57)摘要

本发明公开了一种基于手机指纹识别的光控门禁系统，其包括手机、光控门锁、门端指纹数据库及系统服务器，所述手机用于扫描指纹信息，并将所述指纹信息以可见光信号的形式发送出去；所述光控门锁用于提取所述可见光信号中携带的信息并执行相应的动作；所述门端指纹数据库用于存储指纹信息；所述系统服务器用于监控所述光控门锁并为所述门端指纹数据库提供指纹信息。本发明由于指纹信息通过用户随身携带的手机采集，手机携带及使用方便，提高了安全性及用户体验；另外，指纹信息通过可见光信号发送及通过所述系统服务器的实时监控，可提高系统的管理效率及安全性。



CN 103366423 A

1. 一种基于手机指纹识别的光控门禁系统，其特征在于，包括手机、光控门锁、门端指纹数据库及系统服务器，所述手机包括指纹采集单元、数据处理单元、以及光信号发射单元；所述指纹采集单元用于扫描指纹信息；数据处理单元用于将所述指纹信息转换成表征所述指纹信息的数字信息；所述光信号发射单元，用于将所述数字信息通过可见光信号发送出去；

所述光控门锁包括接收单元、验证单元、以及动作单元；所述接收单元用于接收所述可见光信号，并提取所述可见光信号中携带的数字信息；验证单元，用于将所述接收单元提取的数字信息与预设的校验信息进行比对，当提取的数字信息与所述预设的校验信息匹配时，控制所述动作单元执行相应的动作；

所述门端指纹数据库用于存储指纹信息，该指纹信息与所述校验信息相对应；

所述系统服务器用于监控所述光控门锁并为所述门端指纹数据库提供指纹信息。

2. 根据权利要求 1 所述的指纹验证系统，其特征在于，所述手机还包括：加密单元，用于对所述数据处理单元转换得到的数字信息进行加密；

相应地，所述光控门锁还包括：解密单元，用于对所述接收单元提取的数字信息进行解密。

3. 根据权利要求 1 或 2 所述的指纹验证系统，其特征在于，所述光控门锁还包括报警单元，用于当所述数字信息与所述预设的校验信息不匹配时，发出报警信息。

4. 根据权利要求 1 或 2 所述的指纹验证系统，其特征在于，所述手机还包括存储单元，用于存储用户的指纹信息。

5. 根据权利要求 1 或 2 所述的指纹验证系统，其特征在于，所述手机还包括特征比对单元，用于获取指纹采集单元扫描的指纹信息的特征值，将该特征值与存储单元存储的指纹信息进行比对，如果对比结果一致，向所述数据处理单元发送指纹信息。

6. 根据权利要求 1 或 2 所述的指纹验证系统，其特征在于，所述光信号发射单元为发光二极管。

7. 根据权利要求 1 或 2 所述的指纹验证系统，其特征在于，所述手机还包括电源，用于向所述指纹采集单元、数据处理单元、以及光信号发射单元供电。

8. 根据权利要求 7 所述的指纹验证系统，其特征在于，所述手机还包括开关，用于控制所述电源的开关状态。

9. 根据权利要求 8 所述的指纹验证系统，其特征在于，所述开关是触摸开关。

10. 根据权利要求 8 所述的指纹验证系统，其特征在于，所述开关是按键开关。

基于手机指纹识别的光控门禁系统

技术领域

[0001] 本发明涉及门禁系统技术领域，尤其涉及一种基于手机指纹识别的光控门禁系统。

背景技术

[0002] 无线光通信技术又称可见光通讯，其通过 LED 光源的高频率闪烁来进行通信，有光代表 1，无光代表 0，其传输速率高达每秒上千兆。无线光通信通过可见光来进行数据传输，与微波技术相比，有相当丰富的频谱资源，是一般微波通信和无线通信无法比拟的；同时可见光通信可以适用任何通信协议、适用于任何环境；在安全性方面，不必担心通信内容被人窃取；无线光通信的设备灵活便捷，且成本很低，适合大规模普及应用。

[0003] 指纹识别是指利用生物识别技术，对目标的指纹特征进行识别分析处理后进行判断的一种技术。通过采用对指纹特征点的描述，来表示指纹及目标的信息。该指纹验证系统移动设备可以采集并分析人体的指纹信息，并将指纹信息加入到该设备的数据库中，保存当前指纹和时间等信息，并记录其对应的个人信息，然后通过通信技术，将获取到的指纹特征和个人信息发送出去。

[0004] 现有技术中，指纹识别技术被广泛的应用在各类领域，其在用户识别、安全性、管理性等相关领域发展迅速，如今在门禁系统和考勤系统中普遍应用。由于指纹具有唯一性，对指纹信息的识别可以被用来确定个人信息。但由于指纹识别设备大多都是固定在某处，用户的指纹信息容易留在指纹识别设备上，从而造成信息丢失，存在安全隐患。

发明内容

[0005] 本发明实施方式所要解决的技术问题在于，提供一种基于手机指纹识别的光控门禁系统，其可提高指纹验证系统的安全性及管理效率，且手机携带及使用方便，从而提高用户体验。

[0006] 为了解决上述技术问题，本发明提供了一种基于手机指纹识别的光控门禁系统，包括手机、光控门锁、门端指纹数据库及系统服务器，所述手机包括指纹采集单元、数据处理单元、以及光信号发射单元；所述指纹采集单元用于扫描指纹信息；数据处理单元用于将所述指纹信息转换成表征所述指纹信息的数字信息；所述光信号发射单元，用于将所述数字信息通过可见光信号发送出去；

[0007] 所述光控门锁包括接收单元、验证单元、以及动作单元；所述接收单元用于接收所述可见光信号，并提取所述可见光信号中携带的数字信息；验证单元，用于将所述接收单元提取的数字信息与预设的校验信息进行比对，当提取的数字信息与所述预设的校验信息匹配时，控制所述动作单元执行相应的动作；

[0008] 所述门端指纹数据库用于存储指纹信息，该指纹信息与所述校验信息相对应；

[0009] 所述系统服务器用于监控所述光控门锁并为所述门端指纹数据库提供指纹信息。

[0010] 进一步地，所述手机还包括：加密单元，用于对所述数据处理单元转换得到的数字

信息进行加密；

[0011] 相应地，所述光控门锁还包括：解密单元，用于对所述接收单元提取的数字信息进行解密。

[0012] 进一步地，所述光控门锁还包括报警单元，用于当所述数字信息与所述预设的校验信息不匹配时，发出报警信息。

[0013] 进一步地，所述手机还包括存储单元，用于存储用户的指纹信息。

[0014] 进一步地，所述手机还包括特征比对单元，用于获取指纹采集单元扫描的指纹信息的特征值，将该特征值与存储单元存储的指纹信息进行比对，如果对比结果一致，向所述数据处理单元发送指纹信息。

[0015] 进一步地，所述光信号发射单元为发光二极管。

[0016] 进一步地，所述手机还包括电源，用于向所述指纹采集单元、数据处理单元、以及光信号发射单元供电。

[0017] 进一步地，所述手机还包括开关，用于控制所述电源的开关状态。

[0018] 进一步地，所述开关是触摸开关。

[0019] 进一步地，所述开关是按键开关。

[0020] 综上所述，由于指纹信息通过用户随身携带的手机采集，相对于固定设备，可避免指纹信息泄露，提高了安全性，且手机携带及使用方便，提高了用户体验；另外，指纹信息通过可见光信号发送，由于光信号的直线传输，用户识别信息不易外泄，因此可提高指纹验证系统的安全性；通过所述系统服务器的实时监控，可进一步提高系统的管理效率及安全性。

附图说明

[0021] 为了更清楚地说明本发明实施方式或现有技术中的技术方案，下面将对实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0022] 图 1 是本发明实施例一提供的一种基于手机指纹识别的光控门禁系统示意图；

[0023] 图 2 是本发明实施例二提供的一种基于手机指纹识别的光控门禁系统示意图；

[0024] 图 3 是本发明实施例三提供的一种基于手机指纹识别的光控门禁系统示意图；

[0025] 图 4 是本发明实施例四提供的一种基于手机指纹识别的光控门禁系统示意图。

具体实施方式

[0026] 下面将结合本发明实施方式中的附图，对本发明实施方式中的技术方案进行清楚、完整地描述，显然，所描述的实施方式仅仅是本发明一部分实施方式，而不是全部的实施方式。基于本发明中的实施方式，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施方式，都属于本发明保护的范围。

[0027] 在本发明实施方式中，通过用光信号传输用户指纹信息，由于光信号的保密性强，从而提高指纹验证系统的安全性。

[0028] 参见图 1，是本发明实施例一提供的一种基于手机指纹识别的光控门禁系统示意图，该指纹验证系统包括手机 11、光控门锁 12、门端指纹数据库 13 及系统服务器 14。

[0029] 所述手机 11 包括指纹采集单元 11a、数据处理单元 11b、光信号发射单元 11c、电源 11d、以及开关 11e，指纹采集单元 11a 用于扫描用户指纹信息；数据处理单元 11b 用于将指纹信息转换成表征指纹信息的数字信息；光信号发射单元 11c，用于将表征指纹信息的数字信息通过可见光信号发送出去，光信号发射单元 11c 可以为发光二极管，例如手机的照明灯或闪光灯。电源 11d 内嵌于手机的电池槽中，电源 11d 通过外设于手机上的开关 11e 与指纹采集单元 11a、数据处理单元 11b、及光信号发射单元 11c 电连接，向指纹采集单元 11a、数据处理单元 11b、及光信号发射单元 11c 提供电能。本实施例中，所述开关 11e 是按键式开关，当所述开关 11e 按下时，电源 11d 与指纹采集单元 11a、数据处理单元 11b、及光信号发射单元 11c 实现电导通，从而指纹采集单元 11a 采集用户指纹信息，数据处理单元 11b 将指纹信息转换为数字信息，驱动光信号发射单元 11c 发出表征用户指纹信息的可见光信号。当然，在其他实施方式中，手机 11 也可以不包括电源 11d 及开关 11e，而采用 USB 等接线方式直接通电。电源 11d 可以采用充电电池或纽扣电池。

[0030] 在具体的实施过程中，数据处理单元 11b 可将获取的指纹信息转换为二进制数据，再根据曼彻斯特编码方式将二进制数据转换为上下沿触发信号。具体地，在一个时间周期内，将二进制数据“1”转换为上升沿触发信号，将“0”转换为下降沿触发信号。光信号发射单元 11c 接收到下降沿触发信号时发光，接收到上升沿触发信号时不发光。

[0031] 光控门锁 12，包括接收单元 12a、验证单元 12b、以及动作单元 12c；接收单元 12a 用于接收光信号发射单元 11c 发出的可见光信号，并提取可见光信号中携带的数字信息；验证单元 12b，用于将接收单元 12a 提取的数字信息与预设的校验信息进行比对，当提取的数字信息与预设的校验信息匹配时，控制动作单元 12c 执行相应的动作。其中，提取的数字信息与预设的校验信息匹配是指：预设的校验信息与提取的数字信息相同或者存在对应关系。

[0032] 所述门端指纹数据库 13 与所述验证单元 12b 电连接，并用于存储指纹信息。所述指纹信息与所述校验信息相对应，即所述校验信息与所述指纹信息相同或存在某种映射关系。在本实施例中，所述校验信息与所述指纹信息相同，所述门端指纹数据库 13 为所述验证单元 12b 直接提供所述校验信息。所述系统服务器 14 用于监控所述光控门锁并为所述门端指纹数据库 13 提供指纹信息。

[0033] 具体地，当门端系统将收到的指纹信息进行校验和解码后，将解码后的指纹信息与门端指纹数据库 13 所存的指纹数据进行对比，如果可以从数据库中识别该指纹的所属者，则允许他进入，并将时间、人员等相关信息记录在门端日志文件中。

[0034] 所述门端指纹数据库 13 及日志文件通过无线局域网与系统服务器 14 连接，并每隔一段时间由门端指纹数据库 13 主动将日志记录发送至系统服务器 14。当系统服务器 14 内对应门的数据库信息发生改变时，系统服务器 14 主动与门进行数据同步，以保证数据同步性，而门端指纹数据库 13 也会定时向系统服务器 14 发起数据同步请求来确保数据更新。

[0035] 当管理员更新系统服务器 14 内对应门的指纹数据库信息时，系统服务器 14 会发送同步请求信号，请求与对应的门端指纹数据库 13 内的数据进行同步，光子门锁 12 会将数据同步信息写入门端日志中；更新成功后，门端指纹数据库 13 系统会通过无线网络返回给服务器同步成功信号，系统服务器 14 收到同步成功信号后，将该同步记录到日志中。

[0036] 参见图 2，是本发明实施例二提供的一种基于手机指纹识别的光控门禁系统示意

图，相对于实施例一，手机 11 还包括 ：

[0037] 加密单元 21，两端分别与数据处理单元 11b 和光信号发射单元 11c 连接，用于对数据处理单元 11b 转换得到的数字信息进行加密。

[0038] 相应地，光控门锁 12 还包括 ：

[0039] 解密单元 22，两端分别与接收单元 12a 和验证单元 12b 连接，用于对接收单元 12a 提取的数字信息进行解密。

[0040] 本实施例相对于实施一，对数字信息在传输过程中进行加密、解密处理，进一步提高了指纹验证的安全性。

[0041] 参见图 3，是本发明实施例三提供的一种基于手机指纹识别的光控门禁系统示意图，相对于实施例二，光控门锁 12 还包括 ：

[0042] 报警单元 31，用于当所述数字信息与预设的校验信息不匹配时，发出报警信息。

[0043] 其中，提取的数字信息与预设的校验信息匹配指 ：预设的校验信息与提取的数字信息相同或者存在对应关系。

[0044] 本实施例相对于实施二，增加了报警单元 31，发送的指纹信息与预设的信息不匹配时，发送报警信息，进一步提高了指纹验证系统的安全性。

[0045] 参见图 4，是本发明实施例四提供的一种基于手机指纹识别的光控门禁系统示意图，相对于实施例三，还包括 ：

[0046] 存储单元 41，用于存储用户的指纹信息。存储单元 41 可以采用可编程只读存储器、可擦除可编程只读存储器或快闪存储器。所述指纹信息可以由厂商直接编写或由用户编写。所述指纹信息可以采用二进制编写或采用其他便于识别的汇编语言、高级语言等计算机程序设计语言编写。本实施方式中，为了便于阅读，所述指纹信息采用高级计算机语言编写。

[0047] 特征比对单元 42，用于获取指纹采集单元 11a 扫描的指纹信息的特征值，将该特征值与存储单元 41 存储的指纹信息进行比对，如果对比结果一致，向所述数据处理单元 11b 发送指纹信息。

[0048] 本实施例中，由于对采集的指纹信息进行特征对比，因此当该手机丢失的时候，陌生人无法通过捡到的手机发送携带指纹信息的可见光信号，进一步提高了指纹验证系统的安全性。

[0049] 综上所述，由于指纹信息通过用户随身携带的手机 11 采集，相对于固定设备，可避免指纹信息泄露，提高了安全性，且手机 11 携带及使用方便，提高了用户体验 ；另外，指纹信息通过可见光信号发送，由于光信号的直线传输，用户识别信息不易外泄，因此可提高指纹验证系统的安全性 ；通过所述系统服务器的实时监控，可进一步提高系统的管理效率及安全性。

[0050] 以上所揭露的仅为本发明一种较佳实施方式而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

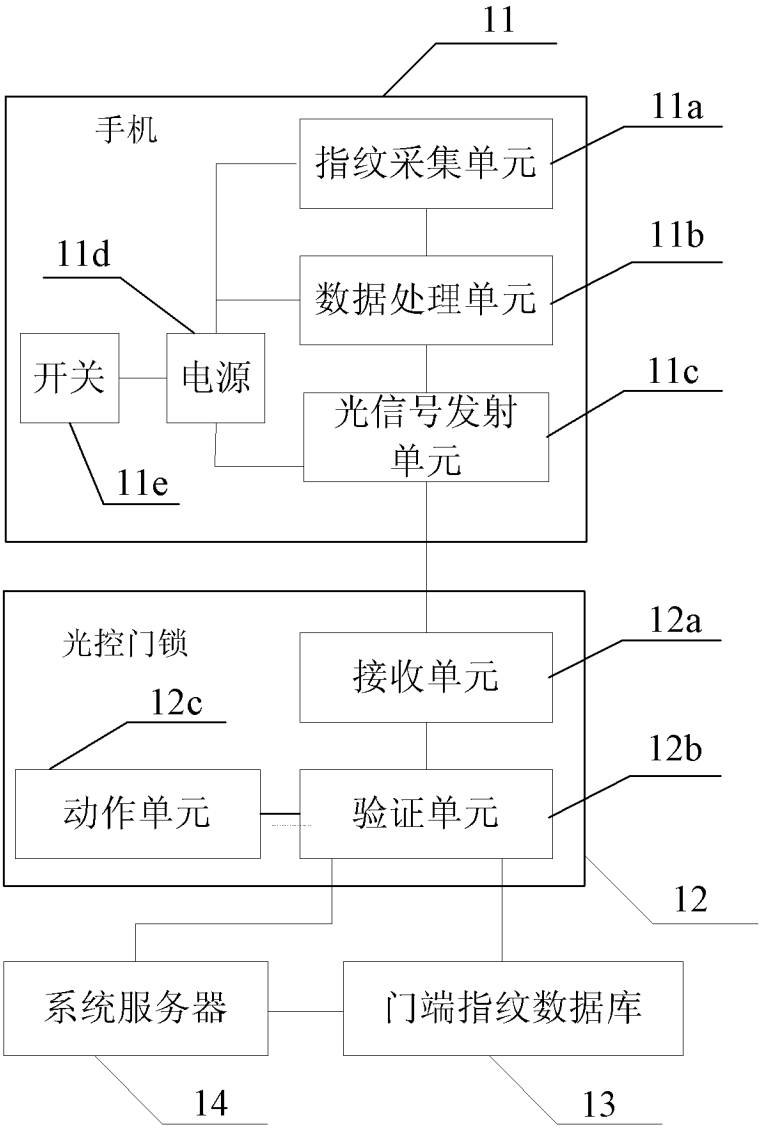

11
手机
11a
指纹采集单元
11b
数据处理单元
11d
开关
电源
11c
光信号发射单元
11e
光控门锁
12a
接收单元
12c
动作单元
12b
验证单元
12
系统服务器
门端指纹数据库
14
13

图 1

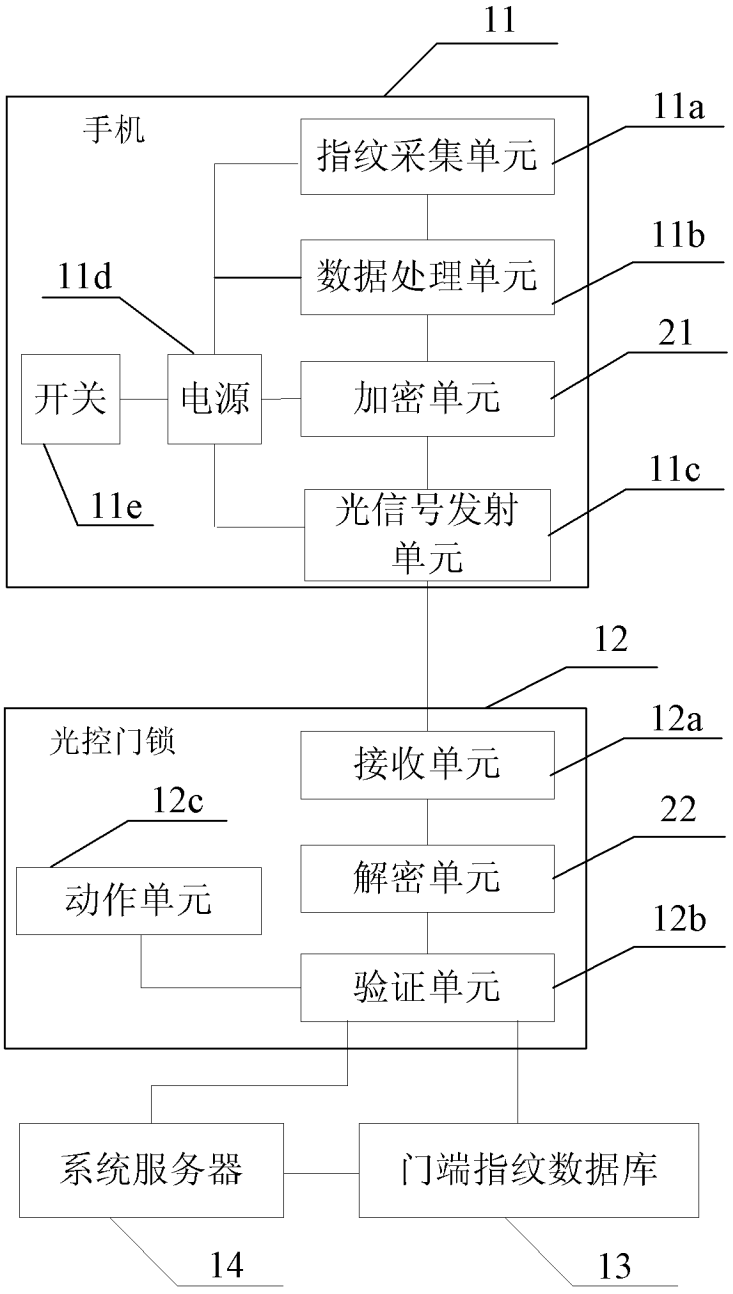

11
手机
11a
指纹采集单元
11b
数据处理单元
11d
21
开关
电源
加密单元
11e
11c
光信号发射单元
12
光控门锁
12a
接收单元
12c
22
动作单元
解密单元
12b
验证单元
系统服务器
门端指纹数据库
14
13

图 2

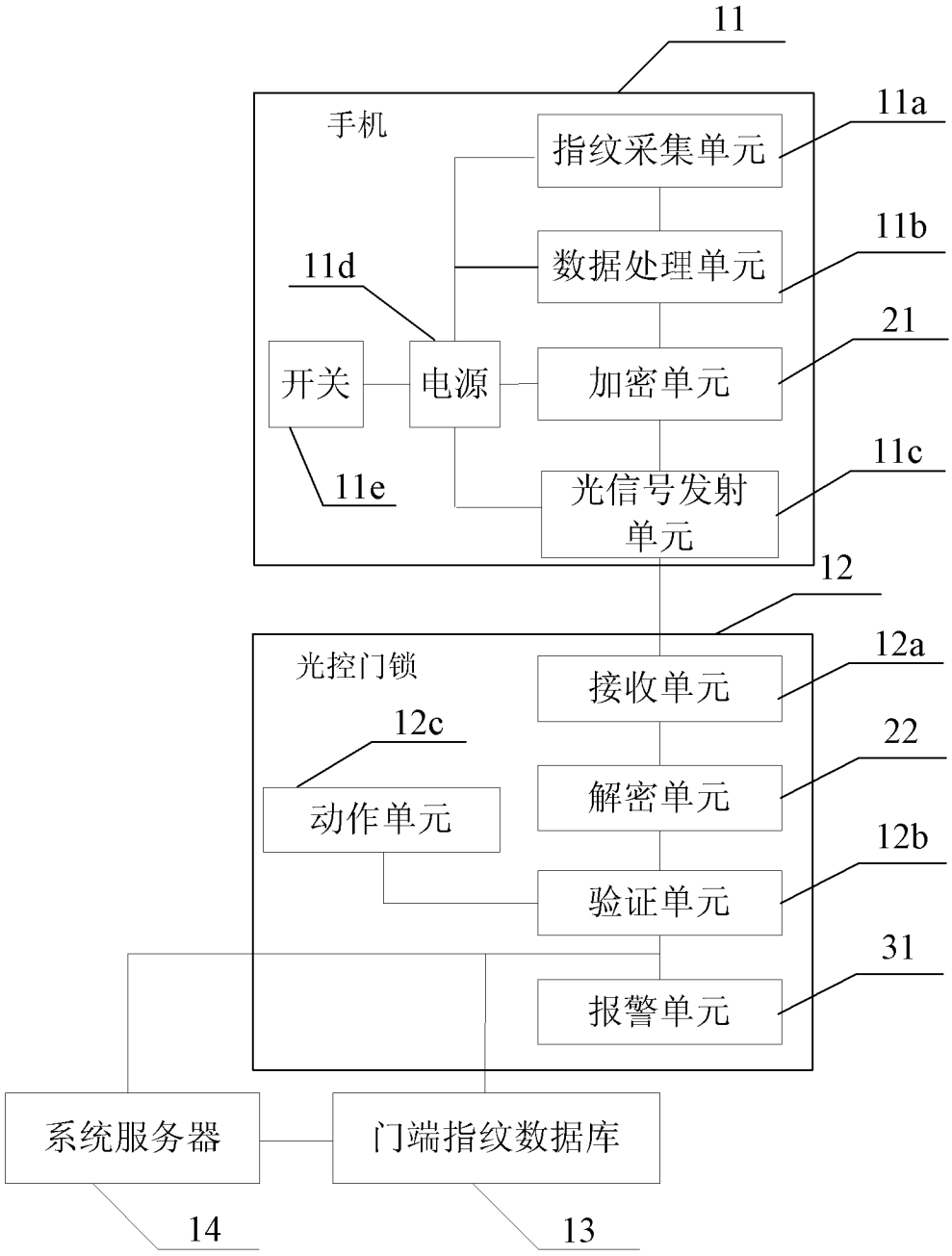

11
手机
11a
指纹采集单元
11b
数据处理单元
11d
21
开关
电源
加密单元
11e
11c
光信号发射单元
12
光控门锁
12a
接收单元
12c
22
动作单元
解密单元
12b
验证单元
31
报警单元
系统服务器
门端指纹数据库
14
13

图 3

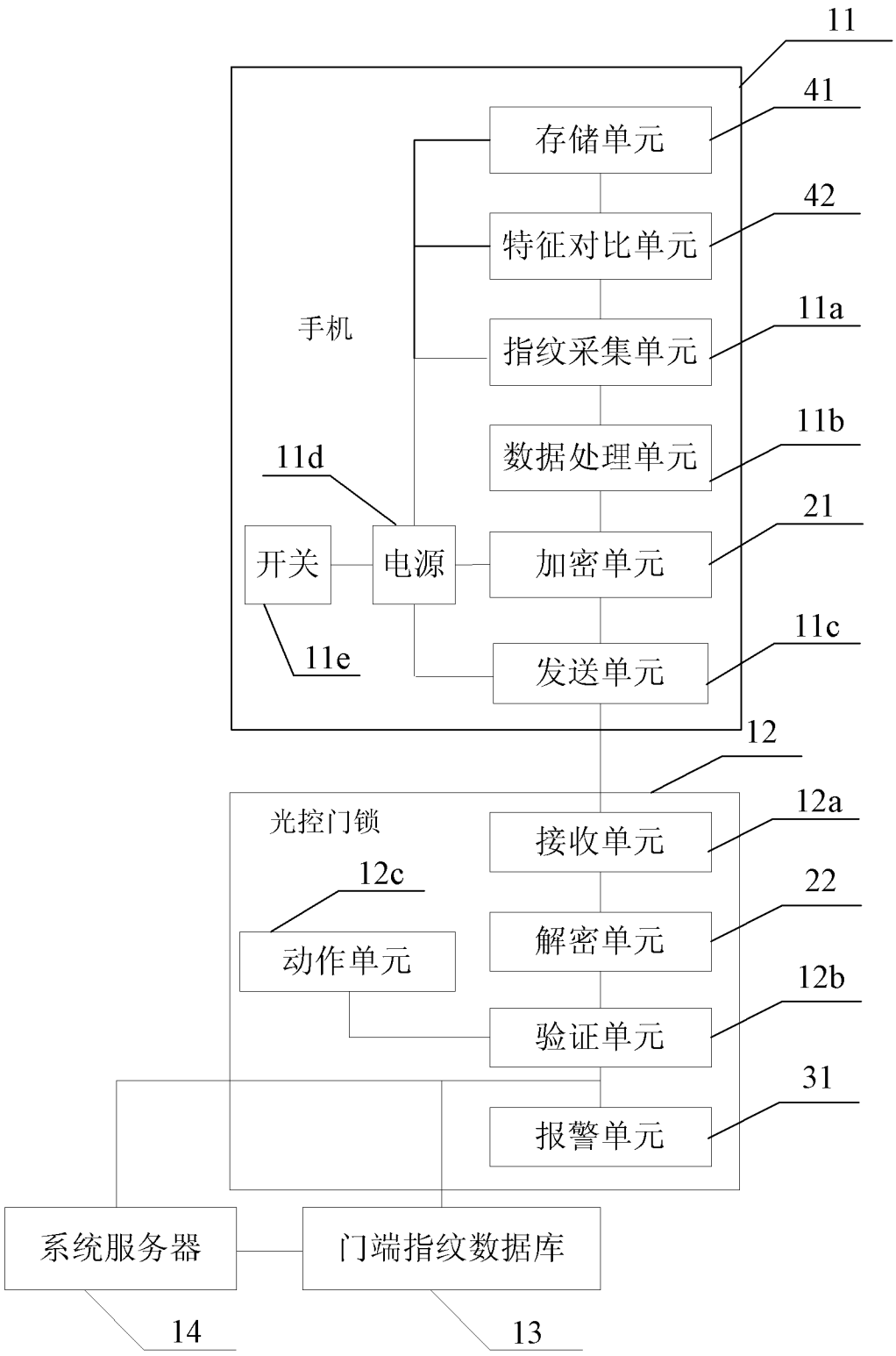

11
41
存储单元
42
特征对比单元
手机
11a
指纹采集单元
11b
数据处理单元
11d
21
开关
电源
加密单元
11e
11c
发送单元
12
光控门锁
12a
接收单元
12c
22
动作单元
解密单元
12b
验证单元
31
报警单元
系统服务器
门端指纹数据库
14
13

图 4