(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 102592066 A
(43)申请公布日 2012.07.18

(21)申请号 201110008443.1

(22)申请日 2011.01.14

(71)申请人 金鹏科技有限公司
地址 中国香港九龙尖沙咀科学馆道 9 号新东海商业中心 6 楼 603 ～ 605

(72)发明人 萧旭峰

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 骆苏华

(51)Int.Cl.
G06F 21/00(2006.01)
G06K 9/00(2006.01)

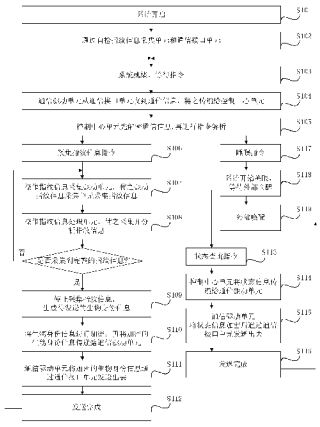
权利要求书 2 页 说明书 7 页 附图 4 页

(54)发明名称

一种适配于智能设备的指纹密码设备及其处理方法

(57)摘要

本发明提供了一种适配于智能设备的指纹密码设备及其处理方法。其中，该适配于智能设备的指纹密码设备的处理方法包括：基于与智能设备的通信接口接收来自所述智能设备的生物身份信息采集请求；采集智能设备用户的指纹信息；处理所述智能设备用户的指纹信息，生成待向外发送的生物身份信息；将所述生物身份信息通过所述通信接口单元发送至所述智能设备。



CN 102592066 A

1. 一种适配于智能设备的指纹密码处理方法，其特征在于，包括：

基于与所述智能设备的通信接口单元接收来自所述智能设备的生物身份信息采集请求；

采集智能设备用户的指纹信息；

处理所述智能设备用户的指纹信息，生成待向外发送的生物身份信息；

将所述生物身份信息通过所述通信接口单元发送至所述智能设备。

2. 如权利要求 1 所述的指纹密码处理方法，其特征在于，还包括：所述指纹信息的采集是在处于采集状态时实现的。

3. 如权利要求 1 所述的指纹密码处理方法，其特征在于，还包括：在接收到所述生物身份信息采集请求时，从空闲状态、或就绪状态、或睡眠状态转换为采集状态。

4. 如权利要求 1 所述的指纹密码处理方法，其特征在于，还包括：

基于所述通信接口接收来自所述智能设备的状态设置指令；

基于所述状态设置指令，从前状态转入到目标状态。

5. 如权利要求 1 所述的指纹密码处理方法，其特征在于，还包括：

基于所述通信接口接收来自所述智能设备的状态查询指令；

获取当前的状态信息，通过所述通信接口将状态信息发送到所述智能设备。

6. 如权利要求 1 至 4 任一项所述的指纹密码处理方法，其特征在于，所述生物身份信息采集请求是在锁定 / 解锁智能设备、智能设备电子支付、备份 / 恢复智能设备数据、或智能设备登录的情形下生成的。

7. 如权利要求 1 所述的指纹密码处理方法，其特征在于，对所述生物身份信息采集请求进行解密；在将所述生物身份信息通过所述通信接口单元发送至所述智能设备之前，将所述生物身份信息进行加密。

8. 如权利要求 7 所述的指纹密码处理方法，其特征在于，所述加密模式是 TDES 模式。

9. 一种适配于智能设备的指纹密码设备，其特征在于，包括：

指纹信息采集单元，用于采集所述智能设备的用户的指纹信息；

指纹信息采集驱动单元，用于驱动所述指纹信息采集单元；

指纹信息处理单元，用于处理来自所述指纹信息采集单元的指纹信息，生成待向外发送的生物身份信息；

通信接口单元，适于建立与所述智能设备进行通信的物理通道；

通信驱动单元，用于驱动所述通信接口单元，实现与智能设备之间的数据通信；

控制中心单元，用于读取来自通信接口单元的智能设备的指令，启动所述指纹信息采集单元、指纹信息采集驱动单元和指纹信息处理单元的工作，将所述生物身份信息通过所述通信接口单元发送至所述智能设备。

10. 如权利要求 9 所述的指纹密码设备，其特征在于，所述指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元和控制中心单元集成于微处理器中。

11. 如权利要求 9 所述的指纹密码设备，其特征在于，所述指纹信息处理单元和控制中心单元集成于微处理器中；所述指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元与所述微处理器之间具有通信通道。

12. 如权利要求 9 所述的指纹密码设备，其特征在于，所述通信接口单元包括 USB 接口，

或串行接口，或无线通信接口。

13. 如权利要求 9 所述的指纹密码设备，其特征在于，还包括 ：状态指示器，用于指示该指纹密码设备的工作状态。

14. 如权利要求 9 所述的指纹密码设备，其特征在于，还包括 ：状态控制单元，用于控制所述指纹密码设备的工作状态。

15. 如权利要求 9 所述的指纹密码设备，其特征在于，所述控制中心单元对所述来自通信接口单元的智能设备的指令进行解密 ；所述控制中心单元对所述从通信接口单元向智能设备发送的指令和生物身份信息进行加密。

16. 如权利要求 9 至 15 任一项所述的指纹密码设备，其特征在于，还包括壳体，所述壳体具有适于容纳所述智能设备的容纳空间 ；

所述指纹信息采集单元、指纹信息采集驱动单元、指纹信息处理单元、通信接口单元、通信驱动单元、控制中心单元设置于壳体上或壳体内。

17. 如权利要求 9 至 15 任一项所述的指纹密码设备，其特征在于，还包括封装结构，所述指纹采集单元、指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元、控制中心单元通过所述封装结构封装，所述指纹采集单元和通信接口单元位于封装结构表面。

一种适配于智能设备的指纹密码设备及其处理方法

技术领域

[0001] 本发明属于半导体传感器和嵌入式应用技术领域，尤其是涉及一种适配于智能设备的指纹密码设备及其处理方法。

背景技术

[0002] 现在的嵌入式技术高速发展，可与各种网络通信的智能设备随处可见，如智能手机、PAD 和 iPad 等。在这些智能设备上，可以通过无处不在的各种通信网络连接到互联网上，运行各种基于互联网的应用程序，或访问各种 Web 站点，极大地方便了人们的生活、学习和工作。

[0003] 在所述各种基于互联网的应用程序和各种 Web 站点中，通常需要输入账号和密码进行登录，并且为了达到一定的安全性，通常会针对不同的互联网应用程序和 Web 站点设置不同的账号和密码。例如，手机支付、访问电子邮箱和登录聊天工具等等。这些需要管理和维护一定量的账号和密码，很可能会弄错互联网应用程序或 Web 站点对应的账号和密码。

[0004] 如果直接将用户账号和用户密码存储起来，很可能因为各种原因而导致这些信息的泄露，导致用户一定程度上的经济损失和精神伤害。例如，网上银行的账号和密码的泄露可能造成经济上的损失，聊天工具的账号和密码的泄露可能造成精神上的伤害等。

发明内容

[0005] 本发明解决的技术问题在于提供一种适配于智能设备的指纹密码设备及其处理方法，可辅助智能设备通过指纹信息管理、维护，加密保护和使用各种账号和密码，增强账号和密码的最高安全性级别，提高使用智能设备的便捷性。

[0006] 本发明实施方式提供一种适配于智能设备的指纹密码设备，包括：

[0007] 指纹信息采集单元，用于扫描指纹，在指纹信息采集驱动单元的控制下采集指纹信息；

[0008] 指纹信息采集驱动单元，用于在控制中心单元的操作下，驱动指纹信息采集单元，使之实施指纹信息的采集，或使之处于就绪、空闲、睡眠状态；

[0009] 指纹信息处理单元，在控制中心单元的操作下，从指纹信息采集驱动单元处获取并分析指纹信息，生成待向外发送的生物身份信息；

[0010] 通信驱动单元，驱动通信接口单元，实现与智能设备之间的数据通信；

[0011] 通信接口单元，适于建立与智能设备通信的物理通道；

[0012] 控制中心单元，用于读取来自通信接口单元的智能设备的指令，启动所述指纹信息采集单元、指纹信息采集驱动单元和指纹信息处理单元的工作，将所述生物身份信息通过所述通信接口单元发送至所述智能设备。

[0013] 可选地，所述指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元和控制中心单元集成于微处理器中。

[0014] 可选地，所述指纹信息处理单元和控制中心单元集成于微处理器中；所述指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元与所述微处理器之间具有通信通道。

[0015] 可选地，所述控制中心单元对所述来自通信接口单元的智能设备的指令进行解密，对所述从通信接口单元向智能设备发送的指令和生物身份信息进行加密。

[0016] 可选地，所述通信接口单元包括 USB 接口，或串行接口，或无线通信接口。

[0017] 可选地，所述指纹密码设备还包括状态指示器，用于指示该指纹密码设备的工作状态。

[0018] 可选地，所述指纹密码设备还包括状态控制单元，用于控制所述指纹密码设备的工作状态。

[0019] 可选地，所述指纹密码设备还包括壳体，所述壳体具有适于容纳所述智能设备的容纳空间；所述指纹信息采集单元、指纹信息采集驱动单元、指纹信息处理单元、通信接口单元、通信驱动单元、控制中心单元设置于壳体上或壳体内。

[0020] 可选地，所述指纹密码设备还包括封装结构，所述指纹采集单元、指纹信息采集驱动单元、指纹信息处理单元、通信驱动单元、控制中心单元通过所述封装结构封装，所述指纹采集单元和通信接口单元位于封装结构表面。

[0021] 本发明实施方式提供一种适配于智能设备的指纹密码处理方法，包括：

[0022] 基于与所述智能设备的通信接口接收来自所述智能设备的生物身份信息请求；采集智能设备用户的指纹信息；处理所述智能设备用户的指纹信息，生成待向外发送的生物身份信息；将所述生物身份信息通过所述通信接口单元发送至所述智能设备。

[0023] 可选地，所述适配于智能设备的指纹密码处理方法，还包括：在接收到所述生物身份信息采集请求时，从空闲状态、或就绪状态、或睡眠状态转换为采集状态。

[0024] 可选地，所述适配于智能设备的指纹密码处理方法，还包括：基于所述通信接口接收来自所述智能设备的状态设置指令，基于所述状态设置指令，将系统从前状态转入到目标状态。

[0025] 可选地，所述适配于智能设备的指纹密码处理方法，还包括：基于所述通信接口接收来自所述智能设备的状态查询指令，获取当前的状态信息，通过所述通信接口将状态信息发送到所述智能设备。

[0026] 可选地，所述适配于智能设备的指纹密码处理方法，还包括：所述生物身份信息采集请求是在锁定 / 解锁智能设备、智能设备电子支付、备份 / 恢复智能设备数据、或智能设备登录的情形下生成的。

[0027] 可选地，所述适配于智能设备的指纹密码处理方法，对所述生物身份信息采集请求进行解密；在将所述生物身份信息通过所述通信接口单元发送至所述智能设备之前，将所述生物身份信息进行加密。

[0028] 可选地，所述适配于智能设备的指纹密码处理方法，所述加密模式是 TDES。

[0029] 与现有技术相比，本发明的实施方式的适配于智能设备的指纹密码设备及其处理方法的有益效果在于：智能设备可以非常方便地与所述指纹密码设备实现通信，易于控制和使用，以获取指纹信息，辅助智能设备安全可靠地便捷地管理、维护和使用不同的账号和密码，减少用户泄露个人信息的可能性，有效降低用户的经济损失，有效减轻用户可能受到的精神伤害；在此基础上还可以在一定程度上实现自动登录，有效提高智能设备的实用性。

附图说明

[0030] 图 1 是本发明实施方式的一种适配于智能设备的指纹密码设备的示意图；

[0031] 图 2 是本发明实施方式的另一种适配于智能设备的指纹密码设备的示意图；

[0032] 图 3 是本发明实施方式的另一种适配于智能设备的指纹密码设备的示意图；

[0033] 图 4 是本发明实施方式的一种适配于智能设备的指纹密码处理方法的示意图。

具体实施方式

[0034] 为使本发明的上述目的、特征和优点能够更为明显易懂，下面结合附图对本发明的具体实施方式做详细的说明。

[0035] 针对背景技术中的问题，本发明提供一种适配于智能设备的指纹密码设备。参考图 1，示出了本发明实施方式的一种适配于智能设备的指纹密码设备的示意图，所述适配于智能设备的指纹密码设备包括：

[0036] 指纹信息采集单元 100，包括指纹传感器和其控制驱动电路，用于在用户指纹扫描过程中，采样用户的指纹信息，在指纹信息采集驱动单元 201 的驱动下工作。

[0037] 所述采样用户的指纹信息，可以是数字信号，指纹信息采集驱动单元 201 通过物理通信信道直接获取所述数字信号。

[0038] 所述采样用户的指纹信息，可以是模拟信号，之后再由指纹信息采集驱动单元 201 将之转换为数字信号。

[0039] 指纹信息采集驱动单元 201，用于在控制中心单元 204 的操作下，控制指纹信息采集单元 100，使之实施指纹信息的采集，或使之处于就绪状态，或使之处于空闲状态，或使之处于睡眠状态；驱动指纹信息采集单元 100 实施指纹信息采样，并正确地获取采样数据。

[0040] 指纹信息处理单元 202，在控制中心单元 204 的操作下，从指纹信息采集驱动单元 201 处持续接收并分析采样的指纹信息，获取并存储一次生物身份信息，生成待发送的生物身份信息，再在控制中心单元 204 的操作下将所述生物身份信息传递给通信驱动单元 203。

[0041] 通信驱动单元 203，将从与之连接的智能设备收到的指令信息传递给控制中心单元 204，基于控制中心单元 204 的控制，向与之连接的智能设备发送所述指令信息的响应，或将从指纹信息处理单元 202 处获取的所述生物身份信息，通过通信接口单元 300 发送给与之连接的智能设备。

[0042] 通信接口单元 300，与智能设备进行通信的物理通道，由通信驱动单元 203 控制和驱动。

[0043] 所述通信接口单元可以是任意的物理信号传输接口，如 USB 接口和串口等通信接口，或如蓝牙、WSN 等无线通信接口等。

[0044] 控制中心单元 204，整个系统的控制中心，直接控制指纹信息采集驱动单元 201、指纹信息处理单元 202 和通信驱动单元 203。从通信驱动单元 203 处获取与之连接的其他设备的指令信息，基于所述指令信息，操作指纹信息采集驱动单元 201 和指纹信息处理单元 202，完成相应的任务。

[0045] 所述任务可以是采集指纹信息、查询和设置所述指纹密码设备的工作状态。

[0046] 完成所述任务过程中，与智能设备之间的通信可以是经过加密的，可以由控制中

心单元 204 在收到加密数据后进行解密，将发送的数据进行加密后再发送。

[0047] 所述整个系统的工作状态可以有睡眠、就绪、空闲和采集等状态。

[0048] 所述睡眠状态是指，整个系统处于完全不工作状态，需要外部信号唤醒。如与本系统相连接的外部设备通过向通信接口单元 300 发送数据，可以唤醒系统，开始接收通信数据信息；或者通过可手动操作的按键来实施唤醒操作。

[0049] 所述就绪状态是指，整个系统都处于正常状态，随时可以开始工作，通常在启动系统、完成当前任务或从睡眠中唤醒后，可处于就绪状态。

[0050] 所述空闲状态是指，整个系统处于等待任务状态。

[0051] 所述采集状态是指，整个系统正在采集指纹信息。

[0052] 所述指纹密码设备还可以有一个状态指示器（图未示），用以表示当前的工作状态。

[0053] 所述指纹密码设备还可以有一个状态控制单元（图未示），用于控制所述指纹密码设备的工作状态。

[0054] 参考图 2，示出了本发明实施方式的另一种适配于智能设备的指纹密码设备的示意图，所述适配于智能设备的指纹密码设备包括，指纹信息采集单元 100，微处理器 200，通信接口单元 300，以及外壳 400。

[0055] 其中微处理器 200 包括指纹信息采集驱动单元 201、指纹信息处理单元 202、通信驱动单元 203 和控制中心单元 204。

[0056] 微处理器 200 还可以只包括控制中心单元 204 和指纹信息处理单元 202，再通过通信信道连接通信驱动单元 203 和指纹信息采集驱动单元 201。

[0057] 所述指纹信息采集单元 100、通信接口单元 300，以及处理器 200 包括的指纹信息采集驱动单元 201、指纹信息处理单元 202、通信驱动单元 203 和控制中心单元 204 在功能上均可以与图 1 中的一致。

[0058] 所述外壳 400 用以承载微处理器 200、通信接口单元 300 和指纹信息采集单元以及连接这些单元的电路，这些单元的位置可以合理的任意放置。

[0059] 所述外壳 400 中空，用以放置与之连接的智能设备。

[0060] 参考图 3，示出了本发明实施方式的另一种适配于智能设备的指纹密码设备的示意图，所述适配于智能设备的指纹密码设备包括：指纹信息采集单元 100，微处理器 200，通信接口单元 300，以及封装壳 500。

[0061] 其中微处理器 200 包括指纹信息采集驱动单元 201、指纹信息处理单元 202、通信驱动单元 203 和控制中心单元 204。

[0062] 微处理器 200 还可以只包括控制中心单元 204 和指纹信息处理单元 202，再通过通信信道连接通信驱动单元 203 和指纹信息采集驱动单元 201。

[0063] 所述指纹信息采集单元 100、通信接口单元 300，以及处理器 200 包括的指纹信息采集驱动单元 201、指纹信息处理单元 202、通信驱动单元 203 和控制中心单元 204 在功能上均可以与图 1 中的一致。

[0064] 所述封装壳 500 用以承载微处理器 200、通信接口单元 300 和指纹信息采集单元 100 以及连接这些单元的电路，这些单元的位置可以合理的任意放置。

[0065] 参考图 4，示出了本发明实施方式的一种适配于智能设备的指纹密码处理方法示

意图，所述适配于智能设备的指纹密码处理方法包括：

[0066] 步骤 S101，系统开启。

[0067] 所述系统开启可是上电开启，也可以由重启按钮重新开启，还可以是通过与之连接的智能设备发送的指令来重新开启。

[0068] 步骤 S102，控制中心单元 204 通过控制驱动指纹信息采集驱动单元 201 和通信驱动单元 203，自检指纹信息采集单元 100 和通信接口单元 300 是否可以正常工作，如果均可以正常工作，则通过自检。

[0069] 步骤 S103，系统转入就绪状态，等待操作指令。

[0070] 步骤 S104，通信驱动单元 203 从通信接口单元 300 收到通信信息，将之传递给控制中心单元 204。

[0071] 步骤 S105，控制中心单元 204 先对收到的通信信息进行解密，再进行指令解析，基于支持的指令种类进入相应的操作。如果分析的指令是采集指纹信息指令，执行步骤 S106；如果是状态查询指令，执行步骤 S113；如果是睡眠指令，执行步骤 S117；如果不支持当前指令，可将错误信息通过通信驱动单元 203 发送出去。

[0072] 步骤 S106，所述收到的指令为采集指纹信息，准备开始采集。

[0073] 步骤 S107，控制中心单元 204 操作指纹信息采集驱动单元 201，使之驱动指纹采集单元 100 开始采集指纹信息。

[0074] 步骤 S108，控制中心单元 204 操作指纹信息处理单元 202，使之采集并分析指纹信息。

[0075] 所述分析指纹信息可以是分析当前采集的数据，判断用户开始扫描指纹和指纹扫描结束的时刻，之间的采样数据可以合成一次生物身份信息，生成生物身份信息；并且可以判断出当前获取的指纹信息是否有效。

[0076] 采集到生物身份信息后，执行步骤 S109。

[0077] 步骤 S109，停止采集指纹信息，生成待发送的生物身份信息。

[0078] 步骤 S110，先将所述生物身份信息进行加密，再将加密后的生物身份信息传递给通信驱动单元 203。

[0079] 步骤 S111，通信驱动单元 203 将所述生物身份信息通过通信接口单元 300 发送出去。

[0080] 步骤 S112，发送完成，系统回到就绪状态，等待下一次指令。

[0081] 步骤 S113，所述收到的指令是状态查询指令，获取当前状态信息。

[0082] 步骤 S114，控制中心单元 204 将状态信息加密后，传递给通信驱动单元 203。

[0083] 步骤 S115，通信驱动单元 203 通过通信接口单元 300 将状态信息发送出去。

[0084] 步骤 S116，发送完成，系统回到就绪状态，等待新的指令。

[0085] 步骤 S117，所述收到的指令是睡眠指令，系统准备进入睡眠状态。

[0086] 步骤 S118，系统开始进入睡眠状态，等待外部唤醒，直至外部唤醒中断，再回到就绪状态，等待新的指令。

[0087] 所述通信驱动单元 203 发送数据的过程，可以根据实际使用的通信接口设计相应的通信协议，以保证通信的正确性。

[0088] 如上所述，与智能设备之间的通信数据也可以是未经加密的。与此对应，在步骤

S105 中可以直接进行指令解析；在步骤 S110 中，直接将为加密的生物身份信息传递给通信驱动单元 203；在步骤 S114 中，直接将状态信息传递给通信驱动单元 203。

[0089] 如上所述，与智能设备之间的通信数据是否需要加密可以根据安全级别的需要来选择。加密的通信方式可以更安全，可以防止生物身份信息的泄露。而非加密方式的安全级别相对低一些，可能会造成生物身份信息的丢失，但成本相对低一些。

[0090] 如上所述，系统支持的指令种类可以根据需要增减，相关技术人员可以在上述基础上扩展和实现。

[0091] 如上所述的指纹密码设备及其处理方法，可以相当方便地在智能设备上实现指纹信息的采集，智能设备就可以通过采集到的指纹信息来加密存储众多的账号和密码，提高账号和密码的安全性，不会因智能设备的管理不善而导致账号和密码的泄露。

[0092] 还可以通过在智能设备上修改应用程序，在需要用户输入账号和密码时，启用指纹认证，使用所述的指纹密码设备及其处理方法，采集用户的指纹信息，与加密存储众多账号和密码的指纹信息比对，如果匹配成功，则表示生物身份认证成功，可以用以解密加密存储众多账号和密码，并从中选择所需的指纹和密码，实现自动输入，从而达到只需要通过指纹认证，就能便捷地使用众多的账号和密码的功效。

[0093] 使用所述指纹密码设备与智能设备通过通信接口连接，可以实现智能设备的自动登录，实现方法可以包括：通过所述指纹密码设备采集指纹信息，设置并存储用于指纹自动登录功能的原始指纹信息，设置标识指纹自动登录功能已启用的标识符，设置并加密存储用于登录的账号和密码信息；指纹自动登录，需要用户输入账号和密码时，生物身份认证成功后，从自动登录账号和密码信息中查询当前应用对应的账号和密码，自动输入之后登录。

[0094] 使用所述指纹密码设备与智能设备通过通信接口连接，可以实现备份和恢复智能设备上的数据信息，实现方法可以包括：通过指纹密码设备采集指纹信息，设置并存储用于指纹恢复和备份数据信息功能的原始指纹信息，设置标识指纹恢复和备份数据信息功能已启用的标识符，启用指纹恢复和备份数据信息功能；备份智能设备上的数据信息，生物身份认证成功后，融合本地的数据信息，通过服务器将本地的融合数据信息备份到备份数据库中；恢复智能设备上的数据信息，生物身份认证成功后，通过服务器从备份数据库中获取的备份数据信息，基于获得的备份数据信息恢复本地的数据信息。

[0095] 使用所述指纹密码设备与智能设备通过通信接口连接，可以实现在智能设备上完成自动电子支付功能，实现方法可以包括：启用指纹电子支付功能，通过所述指纹密码设备采集指纹信息，设置并存储用于指纹电子支付功能的原始指纹信息，设置标识指纹电子支付功能已启用的标识符，设置并加密存储电子支付过程中需要输入的个人信息；实施自动电子支付，在电子支付开始时，通过指纹密码设备采集指纹信息，生物身份认证成功后，解密指纹电子支付个人信息列表，从中选择所需的电子支付个人信息，自动完成电子支付。

[0096] 使用所述指纹密码设备与智能设备通过通信接口连接，可以通过指纹信息来锁定和解锁智能设备，实现方法可以包括：智能设备首先通过指纹密码设备采集指纹信息，设置并存储用于锁定和解锁智能设备的原始指纹信息，设置锁定条件，如开机锁定，超过设定时间未使用锁定等，设置标识指纹锁定和解锁功能已激活的标识符，激活指纹锁定和解锁功能；在智能设备需要解锁时，通过指纹密码设备采集指纹信息，与所述设置并存储的用于指纹锁定和解锁功能的原始指纹信息比对，成功认证后，从锁定状态转入解锁状态。

[0097] 虽然本发明已通过较佳实施例说明如上，但这些较佳实施例并非用以限定本发明。本领域的技术人员，在不脱离本发明的精神和范围内，应有能力对该较佳实施例做出各种改正和补充，因此，本发明的保护范围以权利要求书的范围为准。并且，本发明中用到的术语、字词以及权利要求的含义不能仅限于其字面和普通的含义去理解，还应包括与本发明的技术相符的含义和概念。

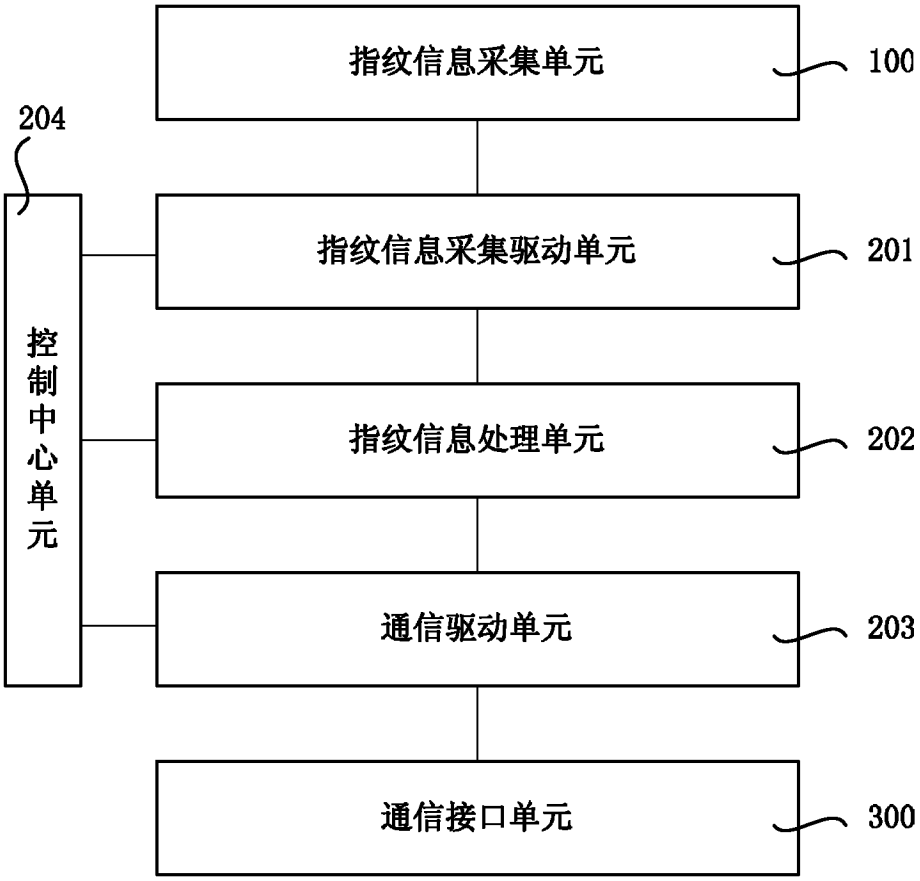

指纹信息采集单元
100
204
指纹信息采集驱动单元
201
控制中心单元
指纹信息处理单元
202
通信驱动单元
203
通信接口单元
300

图 1

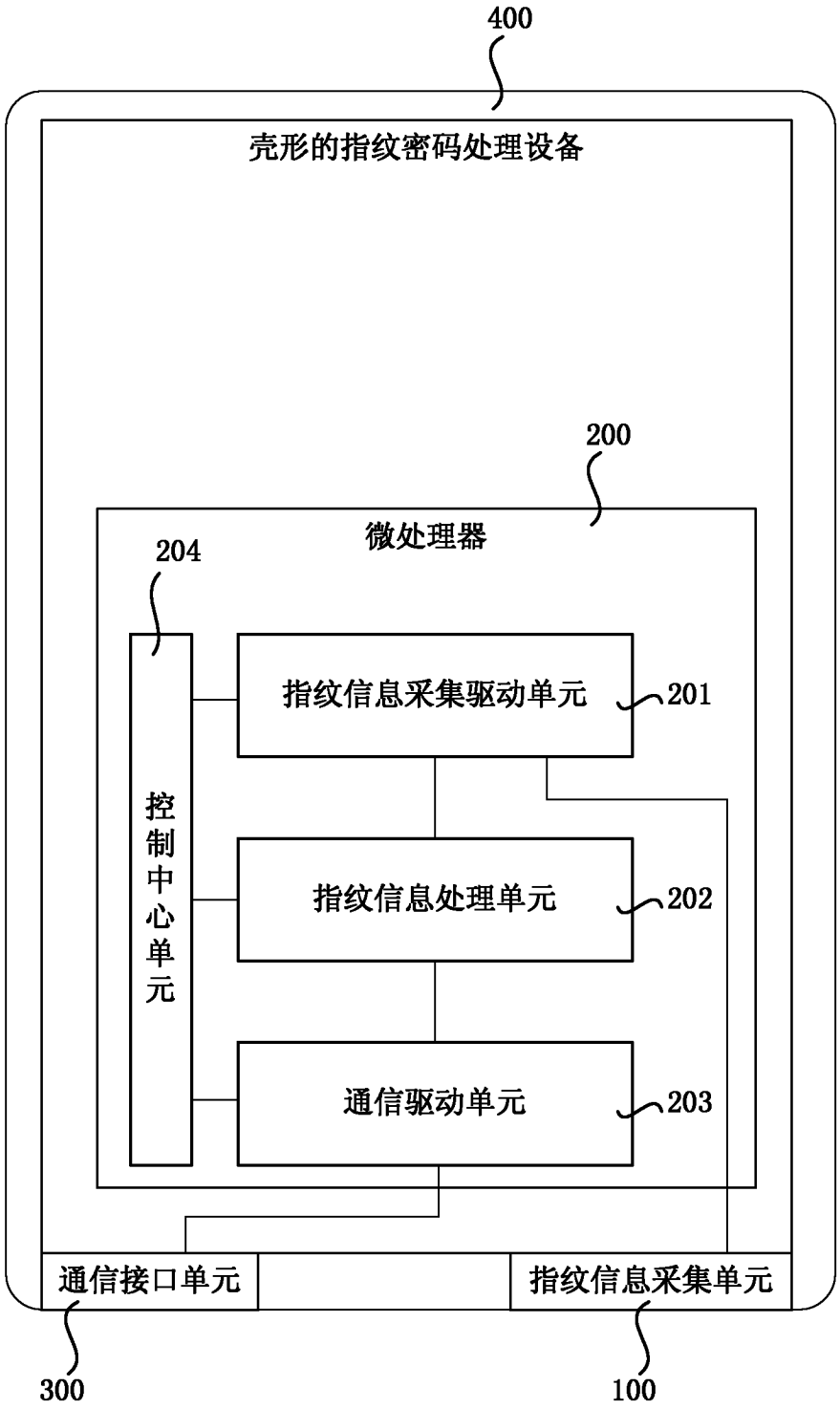

400
壳形的指纹密码处理设备
200
微处理器
204
控制中心单元
指纹信息采集驱动单元
201
指纹信息处理单元
202
通信驱动单元
203
通信接口单元
指纹信息采集单元
300
100

图 2

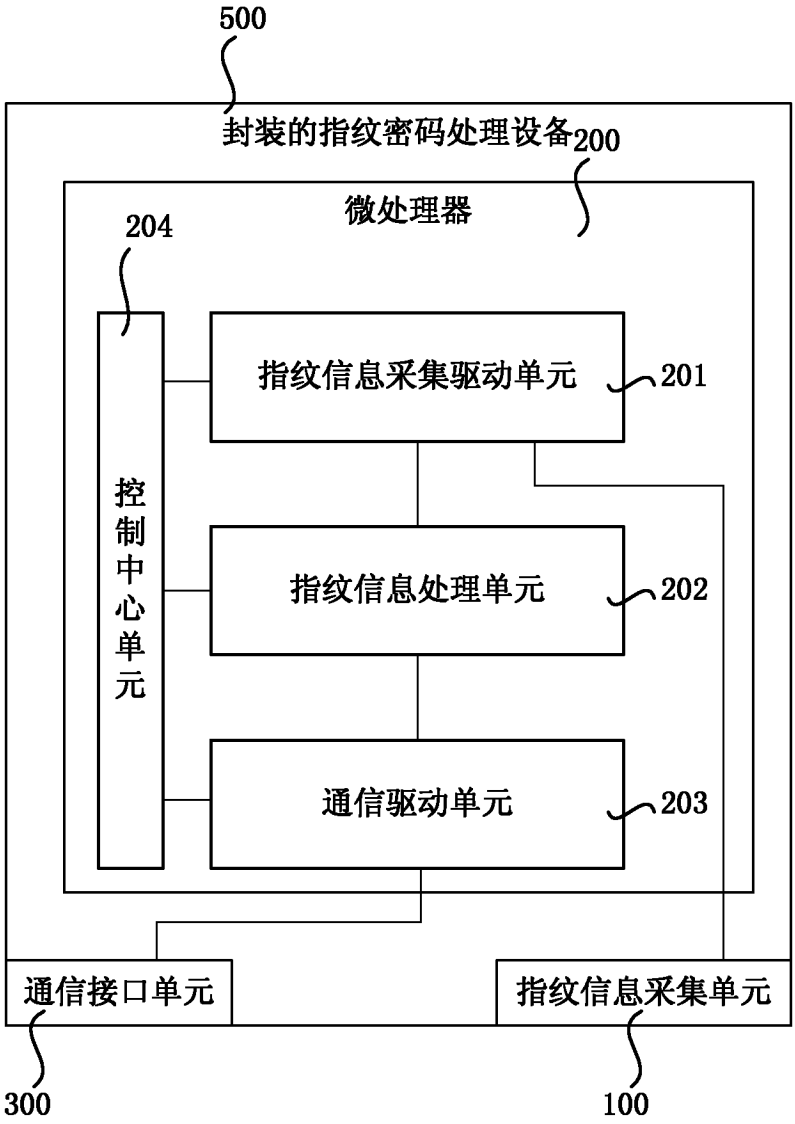

500
封装的指纹密码处理设备
200
微处理器
204
控制中心单元
指纹信息采集驱动单元
201
指纹信息处理单元
202
通信驱动单元
203
通信接口单元
指纹信息采集单元
300
100

图 3

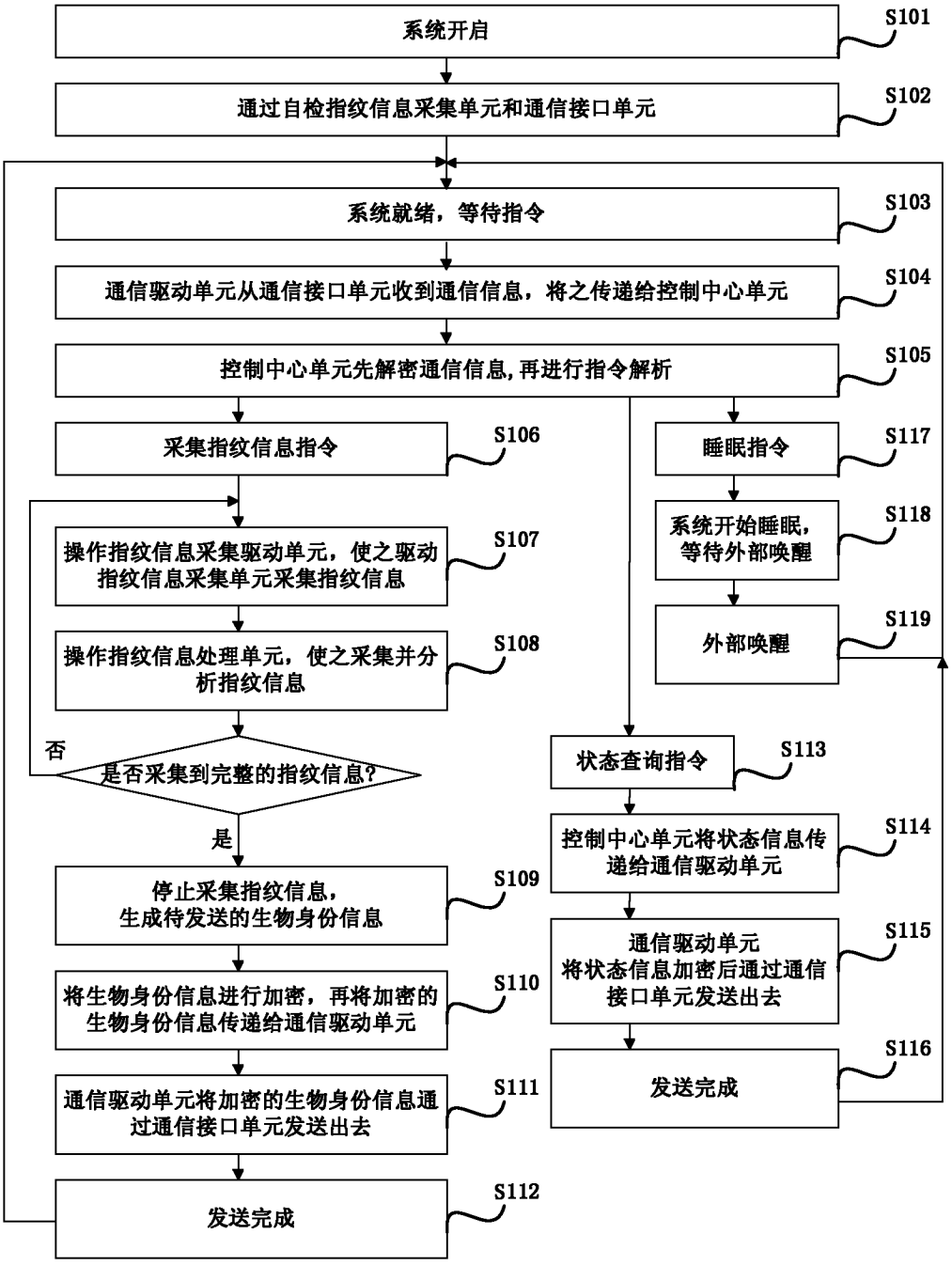

系统开启
S101
通过自检指纹信息采集单元和通信接口单元
S102
系统就绪，等待指令
S103
通信驱动单元从通信接口单元收到通信信息，将之传递给控制中心单元
S104
控制中心单元先解密通信信息,再进行指令解析
S105
采集指纹信息指令
S106
操作指纹信息采集驱动单元，使之驱动指纹信息采集单元采集指纹信息
S107
操作指纹信息处理单元，使之采集并分析指纹信息
S108
否
是否采集到完整的指纹信息?
是
停止采集指纹信息，生成待发送的生物身份信息
S109
将生物身份信息进行加密，再将加密的生物身份信息传递给通信驱动单元
S110
通信驱动单元将加密的生物身份信息通过通信接口单元发送出去
S111
发送完成
S112
睡眠指令
S117
系统开始睡眠，等待外部唤醒
S118
外部唤醒
S119
状态查询指令
S113
控制中心单元将状态信息传递给通信驱动单元
S114
通信驱动单元将状态信息加密后通过通信接口单元发送出去
S115
发送完成
S116

图 4