(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 106295285 A
(43)申请公布日 2017.01.04

(21)申请号 201510284827.4

(22)申请日 2015.05.28

(71)申请人 联想(北京)有限公司
地址 100085 北京市海淀区上地西路6号

(72)发明人 高营 程孝仁

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 蒋雅洁 张颖玲

(51)Int.Cl.
G06F 21/32(2013.01)

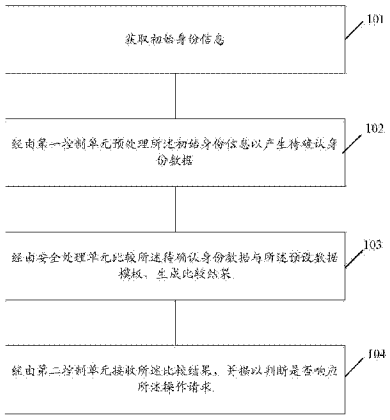
权利要求书1页 说明书7页 附图5页

(54)发明名称

一种信息处理方法及电子设备

(57)摘要

本发明公开了一种信息处理方法及电子设备，其中，所述信息处理方法，用于处理针对电子设备的操作请求的身份验证，所述方法包括：获取初始身份信息；经由第一控制单元预处理所述初始身份信息以产生待确认身份数据；经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果；经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。



CN 106295285 A

1. 一种信息处理方法，用于处理针对电子设备的操作请求的身份验证，所述方法包括：

获取初始身份信息；

经由第一控制单元预处理所述初始身份信息以产生待确认身份数据；

经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果；

经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。

2. 根据权利要求 1 所述的方法，所述方法还包括：

所述第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

3. 根据权利要求 1 所述的方法，所述经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果，包括：

比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果。

4. 根据权利要求 3 所述的方法，所述经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求，包括：

所述比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理。

5. 根据权利要求 3 所述的方法，所述经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求，包括：

所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

6. 一种电子设备，用于处理针对电子设备的操作请求的身份验证，所述电子设备包括：

获取单元，用于获取初始身份信息；

第一控制单元，用于预处理所述初始身份信息以产生待确认身份数据；

安全处理单元，用于比较所述待确认身份数据与所述预设数据模板，生成比较结果；

第二控制单元，用于接收所述比较结果，并据以判断是否响应所述操作请求。

7. 根据权利要求 6 所述的电子设备，所述第一控制单元，进一步用于通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

8. 根据权利要求 6 所述的电子设备，所述安全处理单元，进一步用于比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果。

9. 根据权利要求 8 所述的电子设备，所述第二控制单元，进一步用于所述比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理。

10. 根据权利要求 8 所述的电子设备，所述第二控制单元，进一步用于所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

一种信息处理方法及电子设备

技术领域

[0001] 本发明涉及通讯技术，尤其涉及一种信息处理方法及电子设备。

背景技术

[0002] 本申请发明人在实现本申请实施例技术方案的过程中，至少发现相关技术中存在如下技术问题：

[0003] 生物识别技术在移动设备上被广泛集成，深受用户的喜爱。生物识别技术可以用于智能解锁，智能开机等等涉及用户隐私和安全的验证。一种生物识别技术是指纹鉴定方案(fingerprint)，现有的fingerprint，其实现技术存在的问题是：1)使用软件技术实现的fingerprint非常容易被伪装用户恶意破解，从而无法保护用户的隐私和安全；2)使用软件技术实现的fingerprint需要引入额外的独立硬件来实现，增加成本。

[0004] 然而，相关技术中，对于该问题，尚无有效解决方案。

发明内容

[0005] 有鉴于此，本发明实施例希望提供一种信息处理方法及电子设备，至少解决了现有技术存在的问题。

[0006] 本发明实施例的技术方案是这样实现的：

[0007] 本发明实施例的一种信息处理方法，用于处理针对电子设备的操作请求的身份验证，所述方法包括：

[0008] 获取初始身份信息；

[0009] 经由第一控制单元预处理所述初始身份信息以产生待确认身份数据；

[0010] 经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果；

[0011] 经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。

[0012] 上述方案中，所述方法还包括：

[0013] 所述第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

[0014] 上述方案中，所述经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果，包括：

[0015] 比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果。

[0016] 上述方案中，所述经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求，包括：

[0017] 所述比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理。

[0018] 上述方案中，所述经由第二控制单元接收所述比较结果，并据以判断是否响应所

述操作请求，包括：

[0019] 所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

[0020] 本发明实施例的一种电子设备，用于处理针对电子设备的操作请求的身份验证，所述电子设备包括：

[0021] 获取单元，用于获取初始身份信息；

[0022] 第一控制单元，用于预处理所述初始身份信息以产生待确认身份数据；

[0023] 安全处理单元，用于比较所述待确认身份数据与所述预设数据模板，生成比较结果；

[0024] 第二控制单元，用于接收所述比较结果，并据以判断是否响应所述操作请求。

[0025] 上述方案中，所述第一控制单元，进一步用于通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

[0026] 上述方案中，所述安全处理单元，进一步用于比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果。

[0027] 上述方案中，所述第二控制单元，进一步用于所述比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理。

[0028] 上述方案中，所述第二控制单元，进一步用于所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

[0029] 本发明实施例的所述信息处理方法，用于处理针对电子设备的操作请求的身份验证，所述方法包括：获取初始身份信息；经由第一控制单元预处理所述初始身份信息以产生待确认身份数据；经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果；经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。

[0030] 采用本发明实施例，是通过第一控制单元对初始身份信息的预处理得到待确认身份数据，再经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果，最终根据比较结果由第二控制单元判断是否响应针对电子设备的操作请求，从而完成对操作请求发起者的身份验证。采用本发明实施例，一方面：安全等级高，不容易被伪装用户恶意破解，从而可以保护用户的隐私和安全；另一方面，不需要引入额外的独立硬件来实现，从而减低了成本。

附图说明

[0031] 图 1 为本发明方法实施例一的一个实现流程示意图；

[0032] 图 2 为本发明方法实施例的一个实现流程示意图；

[0033] 图 3 为本发明电子设备实施例的一个组成结构示意图；

[0034] 图 4 为本发明电子设备实施例的一个组成结构示意图；

[0035] 图 5 为应用本发明实施例的一应用场景的示意图；

[0036] 图 6 为基于图 5 所示系统硬件架构的身份验证流程示意图。

具体实施方式

[0037] 下面结合附图对技术方案的实施作进一步的详细描述。

[0038] 方法实施例一：

[0039] 本发明实施例的一种信息处理方法，用于处理针对电子设备的操作请求的身份验证，如图 1 所示，所述方法包括：

[0040] 步骤 101、获取初始身份信息。

[0041] 步骤 102、经由第一控制单元预处理所述初始身份信息以产生待确认身份数据。

[0042] 步骤 103、经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果。

[0043] 步骤 104、经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。

[0044] 采用本发明实施例，是通过第一控制单元对初始身份信息的预处理得到待确认身份数据，再经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果，最终根据比较结果由第二控制单元判断是否响应针对电子设备的操作请求，从而完成对操作请求发起者的身份验证。采用本发明实施例，一方面：安全等级高，不容易被伪装用户恶意破解，从而可以保护用户的隐私和安全；另一方面，不需要引入额外的独立硬件来实现，从而减低了成本。

[0045] 这里，步骤 101 由指纹识别传感器 (Fingerprint sensor) 执行，第一控制单元为 EC，安全处理单元为 Secure element，第二控制单元为 CPU 时，一个具体实例为：Fingerprint sensor 获取指纹信息，经由 EC 对指纹信息进行预处理，得到待确认的身份数据；经由 Secure element 比较所述待确认身份数据与所述预设数据模板，生成比较结果；经由 CPU 接收所述比较结果，并据以判断是否响应所述操作请求。

[0046] 方法实施例二：

[0047] 本发明实施例的一种信息处理方法，用于处理针对电子设备的操作请求的身份验证，如图 2 所示，所述方法包括：

[0048] 步骤 201、获取初始身份信息。

[0049] 步骤 202、经由第一控制单元预处理所述初始身份信息以产生待确认身份数据。

[0050] 步骤 203、第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

[0051] 步骤 204、经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果。

[0052] 步骤 205、经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求。

[0053] 方法实施例三：

[0054] 本发明实施例的一种信息处理方法，用于处理针对电子设备的操作请求的身份验证，如图 3 所示，所述方法包括：

[0055] 步骤 301、获取初始身份信息。

[0056] 步骤 302、经由第一控制单元预处理所述初始身份信息以产生待确认身份数据。

[0057] 步骤 303、第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元。

[0058] 步骤 304、第一控制单元比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果，如果是，则执行步骤 305，否则，执行步骤 306。

[0059] 步骤 305、所述比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理。

[0060] 步骤 306、所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

[0061] 这里需要指出的是：以下电子设备项的描述，与上述方法描述是类似的，同方法的有益效果描述，不做赘述。对于本发明电子设备实施例中未披露的技术细节，请参照本发明方法实施例的描述。

[0062] 电子设备实施例一：

[0063] 本发明实施例的一种电子设备，用于处理针对电子设备的操作请求的身份验证，如图 4 所示，所述电子设备包括：

[0064] 获取单元 11，用于获取初始身份信息；第一控制单元 12，用于预处理所述初始身份信息以产生待确认身份数据；安全处理单元 13，用于比较所述待确认身份数据与所述预设数据模板，生成比较结果；第二控制单元 14，用于接收所述比较结果，并据以判断是否响应所述操作请求。

[0065] 电子设备实施例二：

[0066] 本发明实施例的一种电子设备，用于处理针对电子设备的操作请求的身份验证，如图 4 所示，所述电子设备包括：

[0067] 获取单元 11，用于获取初始身份信息；第一控制单元 12，用于预处理所述初始身份信息以产生待确认身份数据，通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元 13；安全处理单元 13，用于比较所述待确认身份数据与所述预设数据模板，生成比较结果；第二控制单元 14，用于接收所述比较结果，并据以判断是否响应所述操作请求。

[0068] 电子设备实施例三：

[0069] 本发明实施例的一种电子设备，用于处理针对电子设备的操作请求的身份验证，如图 4 所示，所述电子设备包括：

[0070] 获取单元 11，用于获取初始身份信息；第一控制单元 12，用于预处理所述初始身份信息以产生待确认身份数据，通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元 13；安全处理单元 13，用于比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果；第二控制单元 14，用于比较结果为所述可信的身份验证结果时，判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理；或者，所述比较结果为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，

拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

[0071] 以一个现实应用场景为例对本发明实施例阐述如下：

[0072] 应用场景为 fingerprint 技术，是基于使用手指和拇指前端的纹理按下的纹印来鉴定身份。指纹是鉴别身份的一种可靠的方法，因为每个人的每个指头上的纹理排列各不相同而且不因发育或年龄而改变。指纹用于揭示一个人的真实身份，尽管本人否认，使用假名，或因年龄疾病、整形外科手术或事故而发生容貌上的变化。利用指纹作为一种鉴别身份的作法被称为指纹鉴定法，是现代执法中的一个不可缺少的辅助手段。

[0073] 随着智能终端，如智能手机的普及，上述这个 fingerprint 技术作为生物识别在移动设备上广泛集成，备受用户的喜爱。但 fingerprint 技术的安全问题也成为目前最为关注的问题。例如，一种现有的解决方案为：fingerprint 直接连接 CPU，该方案的缺点是：软件解决方案，会受到恶意软件盗取用户信息；另一种现有的解决方案为：fingerprint 直接连接安全控制器，该方案的缺点是：硬件解决方案，安全控制器需要一定的处理运算能力，价格比较贵，cost up ～ 1$，这种额外增加硬件的办法，会增加制造成本。

[0074] 本应用场景采用本发明实施例，为一种可靠的指纹鉴定 (fingerprint) 安全系统设计方案，是在笔记本上集成 fingerprint 的安全设计方案，当然，也可以在其他智能终端，如智能手机上使用本发明实施例，该方案可以为用户提供可靠的安全系统设计，保证用户在使用 fingerprint 过程中不会存在安全隐患。

[0075] 以在笔记本上集成 fingerprint 的安全设计方案为例，只需要利用笔记本现有控制器，而无需添加格外的硬件资源，不会增加额外的制造成本，同样可以为用户提供可靠的安全系统，提高产品竞争力。

[0076] 本方案采用的系统硬件架构如图 5 所示，包括：Fingerprint Sensor21，用于获取用户初始指纹信息，如 image 信息；EC22，用于获取 CPU 控制命令，读取 Fingerprint Sensor 的 image 信息，基于 image 信息进行预处理得到 image data，传递 image data 给 SE，得到 SE 结果后输出给 CPU；SE23，具有硬件加密的安全处理模块，用于存储用户指纹模板，并且接收 EC 传递的 image data 进行比对，将可信结果输出给 EC，之后由将可信结果输出给 CPU；CPU24，作为笔记本处理器，用于处理应用程序，对于从 EC 获取的可信结果来进行指纹对应用户的身份验证，以决定是否对用户针对电子设备的操作请求进行响应，比如，操作请求为用户开机请求，则根据可信结果判断出针对电子设备的操作请求由可信任的用户本人所发起，响应所述操作请求，开启与用户本人身份有关的权限处理，具体为开启笔记本，否则，为非可信的身份验证结果时，判断出针对电子设备的操作请求不是由可信任的用户本人所发起，拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理。

[0077] 从图 5 可以看出，关键点在于：利用增加的系统控制器 EC 作为 Fingerprint 的通信桥梁，设计了 CPU-EC-SE-Fingerprint Sensor 之间的通信链路，以保证用户的安全信息不会变恶意软件盗取，提供可靠的安全系统，无硬件成本，即：将 Fingerprint Sensor 和具有加密单元的安全控制器 (SE，Secure Element) 都连接到 EC，CPU 与 Fingerprint Sensor 不是直连，CPU 与 SE 也不是直连，都需要经由 EC 中转和处理。可见：本方案的监控系统由软硬件实现，利用系统 EC 控制器，EC 接到 CPU 控制命令后，读取 Fingerprint Sensor 的 image 信息，EC 处理 image 信息生成 image data，将 image data 传递给 SE 模块，SE 模块通过比对模板判断是否为可信 image，并将结果传递给 EC，EC 接到后输出给 CPU，完成用户识

别。整个辨识过程，CPU 无法直接从 Fingerprint Sensor 和 SE 模块获取 image 信息和比对模板。

[0078] 基于图 5 所示的系统硬件架构，执行的身份验证流程如图 6 所示，包括：

[0079] 步骤 501、当用户通过软件调用 fingerprint 功能时，通过 Fingerprint Sensor 扫描得到 image 信息。

[0080] 步骤 502、CPU 通知 EC 开启 fingerprint 功能，通过 EC 读取 fingerprint 的 image 信息。

[0081] 步骤 503、EC 对读取的 image 信息进行处理，生成 image data。

[0082] 步骤 504、EC 通过安全加密硬件接口，将处理后的 image data 传递给 SE，SE 接受 EC 传递的 image data，通过将 image data 与已存储的 image 模板进行匹配，以确认是否为可信 image，得到可信结果。

[0083] 步骤 505、SE 将可信结果反馈给 EC，再由 EC 传递给 CPU 进行最终的判断，以决定是否针对该操作请求进行响应，最后将响应结果返回给用户的 User APP。

[0084] 本应用场景采用本发明实施例，采用本方案之后的有益效果为：1) 本方案 fingerprint 得到的 image 信息不回直接通过 CPU 获取，保证其他恶意软件盗取用户信息，提供了可靠的安全系统；2) 本方案为硬件加密方案，提高了安全系数；3) 本方案利用现有的 EC 资源作为通信渠道，无需添加额外硬件资源，无 cost up；4) 本方案由底层控制器完成，不占用 CPU 资源，不会增加系统功耗；5) 智能识别用户需求，提高用户体验。

[0085] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0086] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元，即可以位于一个地方，也可以分布到多个网络单元上；可以根据实际的需要选择其中的部分或全部单元来实现本实施例方案的目的。

[0087] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0088] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器 (ROM，Read-Only Memory)、随机存取存储器 (RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0089] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以

是个人计算机、服务器、或者网络设备等）执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0090] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

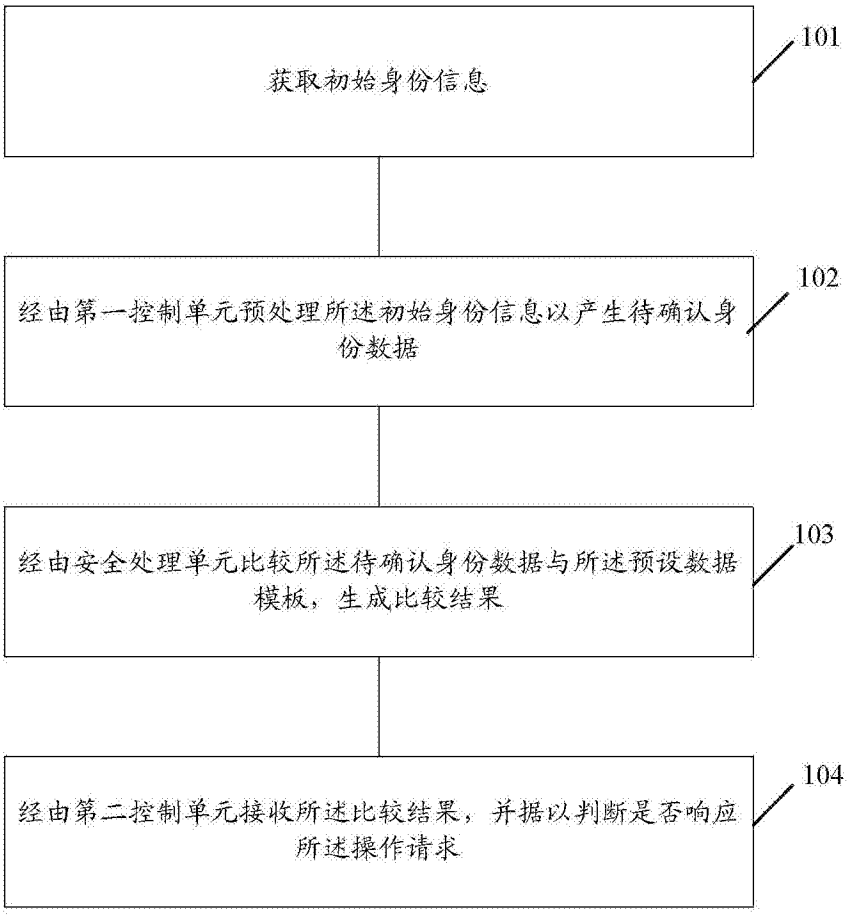

获取初始身份信息
101
经由第一控制单元预处理所述初始身份信息以产生待确认身份数据
102
经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果
103
经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求
104

图 1

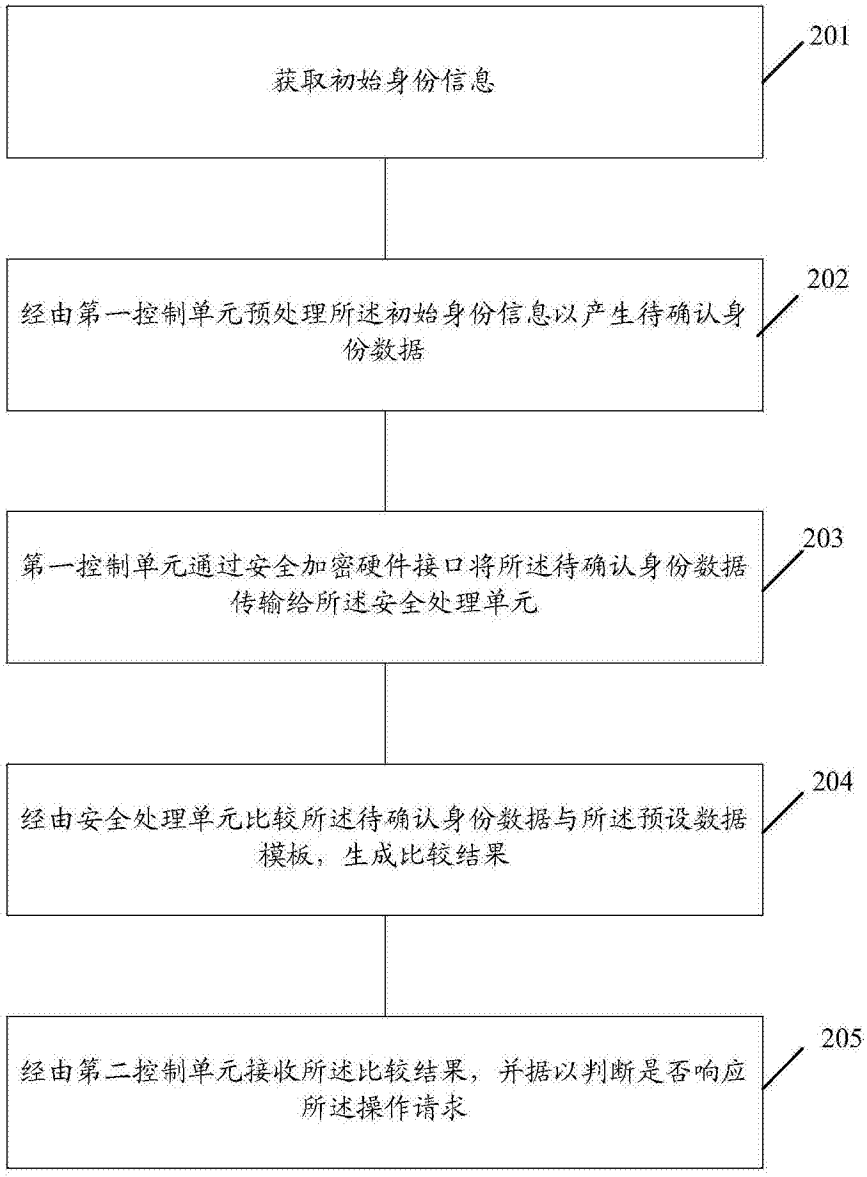

获取初始身份信息
201
经由第一控制单元预处理所述初始身份信息以产生待确认身份数据
202
第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元
203
经由安全处理单元比较所述待确认身份数据与所述预设数据模板，生成比较结果
204
经由第二控制单元接收所述比较结果，并据以判断是否响应所述操作请求
205

图 2

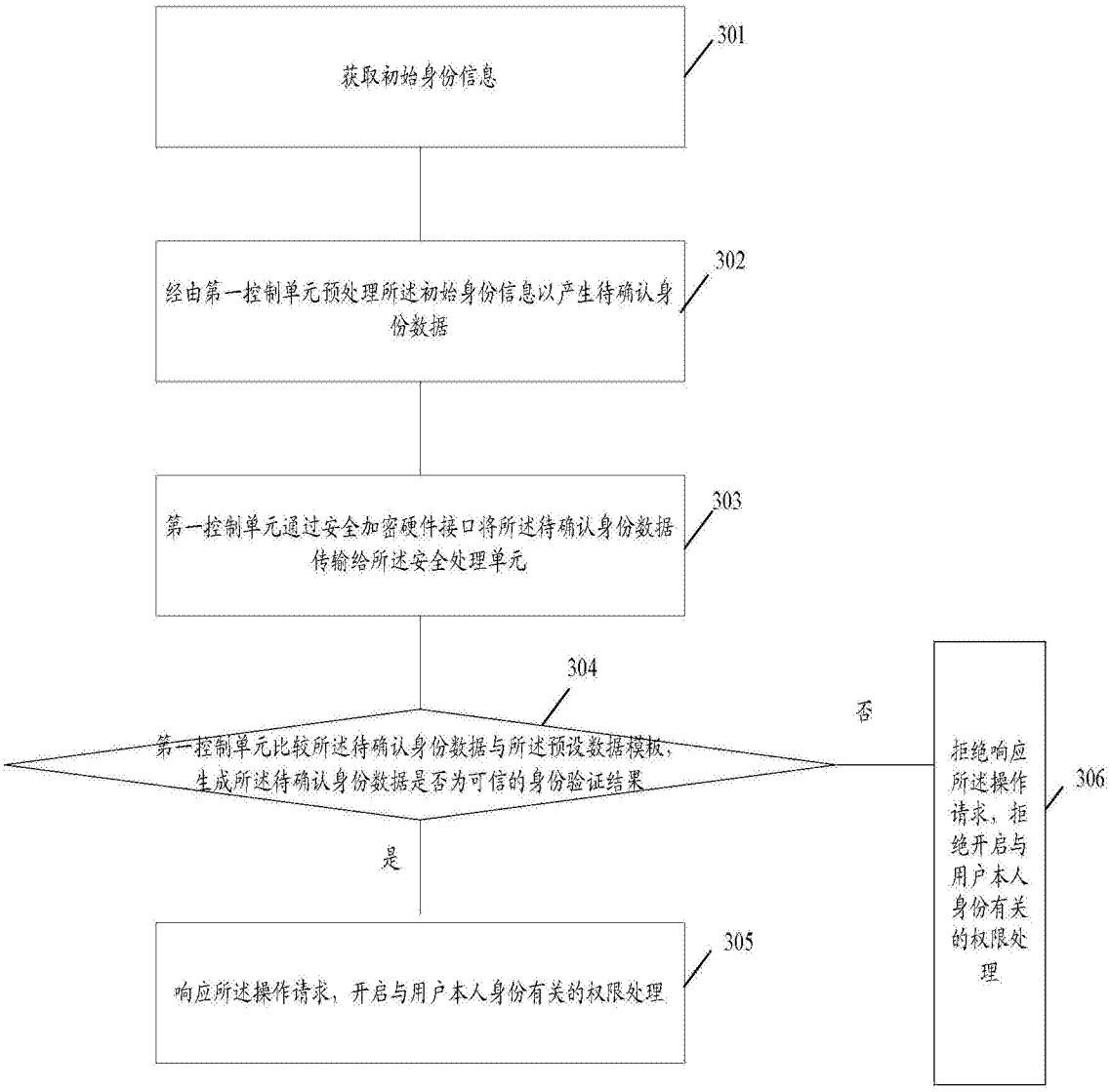

获取初始身份信息
301
经由第一控制单元预处理所述初始身份信息以产生待确认身份数据
302
第一控制单元通过安全加密硬件接口将所述待确认身份数据传输给所述安全处理单元
303
304
第一控制单元比较所述待确认身份数据与所述预设数据模板，生成所述待确认身份数据是否为可信的身份验证结果
否
是
拒绝响应所述操作请求，拒绝开启与用户本人身份有关的权限处理
306
响应所述操作请求，开启与用户本人身份有关的权限处理
305

图 3

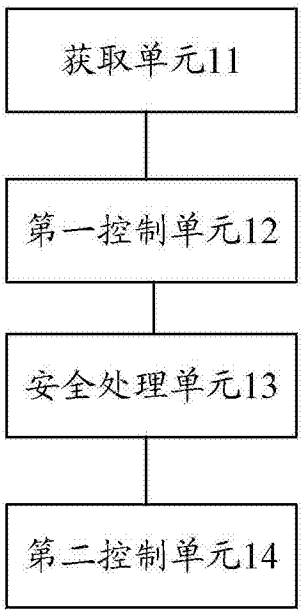

获取单元11
第一控制单元12
安全处理单元13
第二控制单元14

图 4

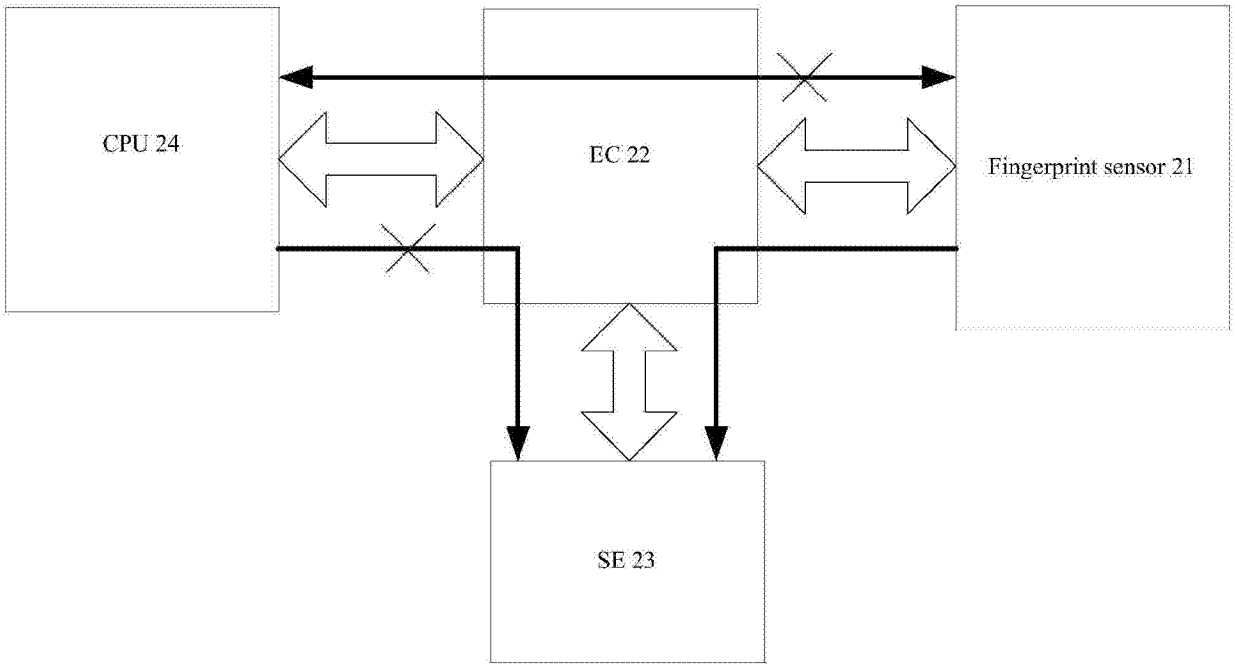

CPU 24
EC 22
Fingerprint sensor 21
SE 23

图 5

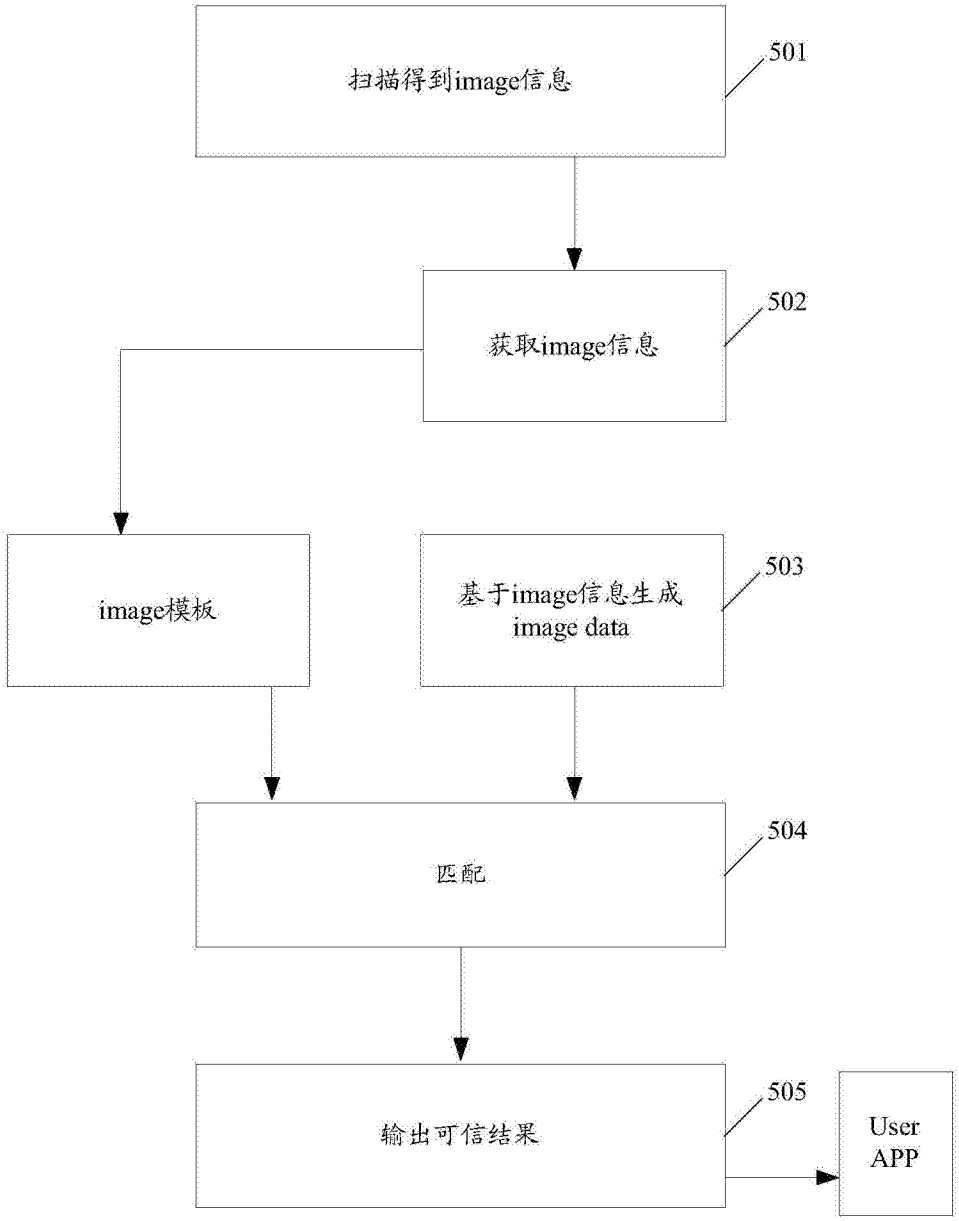

扫描得到image信息
501
获取image信息
502
image模板
基于image信息生成
image data
503
匹配
504
输出可信结果
505
User
APP

图 6