



(12) 发明专利申请

(10) 申请公布号 CN 106612259 A

(43) 申请公布日 2017. 05. 03

(21) 申请号 201510701276. 7

(22) 申请日 2015. 10. 26

(71) 申请人 阿里巴巴集团控股有限公司

地址 英属开曼群岛大开曼资本大厦一座四
层 847 号邮箱

(72) 发明人 沈英鹏

(74) 专利代理机构 北京国昊天诚知识产权代理
有限公司 11315

代理人 许志勇

(51) Int. Cl.

H04L 29/06(2006. 01)

G06Q 20/38(2012. 01)

G06Q 20/40(2012. 01)

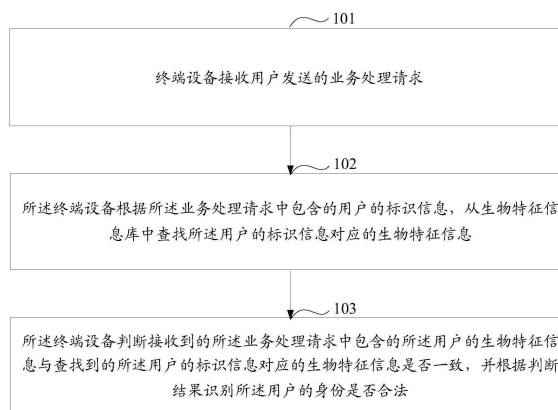
权利要求书5页 说明书18页 附图6页

(54) 发明名称

身份识别、业务处理以及生物特征信息的处
理方法和设备

(57) 摘要

本申请公开了一种身份识别、业务处理以及生物特征信息的处理方法和设备,包括:终端设备接收用户发送的业务处理请求;根据业务处理请求中包含的用户的标识信息,从生物特征信息库中查找用户的标识信息对应的生物特征信息;判断接收到的业务处理请求中包含的用户的生物特征信息与查找到的用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别用户的身份是否合法。终端设备根据用户的生物特征信息对用户的身份进行识别,增强生物识别技术的安全性,同时为后续启动服务器对用户的身份进行识别奠定基础,也避免用户的生物特征信息通过通信网络发送至服务器的过程中容易被非法窃取的风险,有效保证用户的生物特征信息的安全性。



1. 一种身份识别方法,其特征在于,包括:

终端设备接收用户发送的业务处理请求,其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;

所述终端设备根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;

所述终端设备判断接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

2. 如权利要求1所述的身份识别方法,其特征在于,所述方法还包括:

所述终端设备在识别所述用户的身份合法时,确定所述用户的生物特征信息的属性值,并将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器。

3. 如权利要求2所述的身份识别方法,其特征在于,所述终端设备将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器,包括:

所述终端设备将所述用户的标识信息和所述属性值进行加密,得到加密结果;

所述终端设备将携带所述加密结果的业务处理请求发送至服务器。

4. 如权利要求1至3任一项所述的身份识别方法,其特征在于,所述终端设备通过以下方式将所述用户的生物特征信息存储至所述生物特征信息库中,包括:

所述终端设备接收所述用户发送的注册请求,并获取所述注册请求中包含的所述用户的生物特征信息和所述用户的标识信息;

所述终端设备建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

5. 如权利要求4所述的身份识别方法,其特征在于,所述方法还包括:

所述终端设备在获取到所述注册请求中包含的所述用户的生物特征信息时,利用预设算法,计算得到所述用户的生物特征信息的属性值;

所述终端设备建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,包括:

所述终端设备建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系。

6. 如权利要求1所述的身份识别方法,其特征在于,所述方法还包括:

所述终端设备在识别所述用户的身份非法时,向所述用户返回身份识别结果。

7. 一种业务处理方法,其特征在于,包括:

服务器接收终端设备发送的业务处理请求,其中,所述业务处理请求中包含用户的生物特征信息的属性值和所述用户的标识信息;

所述服务器根据接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值,其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息的属性值;

所述服务器在确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业

务处理请求。

8. 如权利要求 7 所述的业务处理方法,其特征在于,所述服务器在接收到所述终端设备发送的业务处理请求后,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值之前,所述方法还包括:

所述服务器通过解密操作得到所述业务处理请求中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

9. 如权利要求 7 或 8 所述的业务处理方法,其特征在于,所述服务器通过以下方式将所述用户的标识信息对应的生物特征信息的属性值存储至所述生物识别数据库中,包括:

所述服务器接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备将用户发送的注册请求中包含的所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

所述服务器通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

所述服务器建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

10. 一种生物特征信息的处理方法,其特征在于,包括:

终端设备接收用户发送的所述用户的标识信息以及所述用户的生物特征信息;

所述终端设备根据所述用户的生物特征信息,利用预设算法,计算得到所述用户的生物特征信息的属性值;

所述终端设备建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

11. 如权利要求 10 所述的生物特征信息的处理方法,其特征在于,所述终端设备计算得到所述用户的标识信息对应的生物特征信息的属性值后,所述方法还包括:

所述终端设备将所述用户的标识信息以及所述用户的生物特征信息的属性值进行加密,得到加密结果;

所述终端设备将所述加密结果发送至所述服务器。

12. 如权利要求 10 所述的生物特征信息的处理方法,其特征在于,所述终端设备建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中,包括:

所述终端设备向所述生物特征信息库发送查询请求,其中,所述查询请求中包含所述用户的标识信息;

所述终端设备接收所述生物特征信息库返回的查询结果;

所述终端设备根据查询结果确定在所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息,利用接收到的所述用户的生物特征信息更新所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息;

所述终端设备根据查询结果确定在所述生物特征信息库中未存储与所述用户的标识信息对应的用户的生物特征信息,建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系,并将所述对应关系

存储在所述生物特征信息库中。

13. 一种生物特征信息的处理方法,其特征在于,包括:

所述服务器接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

所述服务器通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

所述服务器建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

14. 一种身份识别设备,其特征在于,包括:

接收单元,用于接收用户发送的业务处理请求,其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;

查找单元,用于根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;

识别单元,用于判断所述接收单元接收到的所述业务处理请求中包含的所述用户的生物特征信息与所述查找单元查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

15. 如权利要求 14 所述的身份识别设备,其特征在于,所述身份识别设备还包括:发送单元,其中:

所述发送单元,用于在识别所述用户的身份合法时,确定所述用户的生物特征信息的属性值,并将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器。

16. 如权利要求 15 所述的身份识别设备,其特征在于,所述发送单元将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器,包括:

将所述用户的标识信息和所述属性值进行加密,得到加密结果;

将携带所述加密结果的业务处理请求发送至服务器。

17. 如权利要求 14 至 16 任一项所述的身份识别设备,其特征在于,所述身份识别设备还包括:建立单元,其中:

所述接收单元,还用于接收所述用户发送的注册请求,并获取所述注册请求中包含的所述用户的生物特征信息和所述用户的标识信息;

所述建立单元,用于建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

18. 如权利要求 17 所述的身份识别设备,其特征在于,所述身份识别设备还包括:计算单元,其中:

所述计算单元,用于在获取到所述注册请求中包含的所述用户的生物特征信息时,利用预设算法,计算得到所述用户的生物特征信息的属性值;

所述建立单元建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,包括:

建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系。

19. 如权利要求 14 所述的身份识别设备,其特征在于,所述身份识别设备还包括:返回单元,其中:

所述返回单元,用于在所述识别单元识别所述用户的身份非法时,向所述用户返回身份识别结果。

20. 一种业务处理设备,其特征在于,包括:

接收单元,用于接收终端设备发送的业务处理请求,其中,所述业务处理请求中包含用户的生物特征信息对应的属性值和所述用户的标识信息;

查找单元,用于根据所述接收单元接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值,其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息的属性值;

响应单元,用于确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业务处理请求。

21. 如权利要求 20 所述的业务处理设备,其特征在于,所述业务处理设备还包括:解密单元,其中:

所述解密单元,用于在接收所述终端设备发送的业务处理请求后,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值之前,通过解密操作得到所述业务处理请求中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

22. 如权利要求 20 或 21 所述的业务处理设备,其特征在于,所述业务处理设备还包括:建立单元,其中:

所述接收单元,还用于接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备将用户发送的注册请求中包含的所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

所述解密单元,还用于通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

所述建立单元,用于建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

23. 一种生物特征信息的处理设备,其特征在于,包括:

接收单元,用于接收用户发送的所述用户的标识信息以及所述用户的生物特征信息;

计算单元,用于根据所述用户的生物特征信息,利用预设算法,计算得到所述用户的生物特征信息的属性值;

存储单元,用于建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

24. 如权利要求 23 所述的生物特征信息的处理设备,其特征在于,所述处理设备还包

括加密单元和发送单元,其中:

所述加密单元,用于在计算得到所述用户的标识信息对应的生物特征信息的属性值后,将所述用户的标识信息以及所述用户的生物特征信息的属性值进行加密,得到加密结果;

所述发送单元,用于将所述加密结果发送至所述服务器。

25. 如权利要求 23 所述的生物特征信息的处理设备,其特征在于,所述存储单元建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中,包括:

向所述生物特征信息库发送查询请求,其中,所述查询请求中包含所述用户的标识信息;

接收所述生物特征信息库返回的查询结果;

根据查询结果确定在所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息,利用接收到的所述用户的生物特征信息更新所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息;

根据查询结果确定在所述生物特征信息库中未存储与所述用户的标识信息对应的用户的生物特征信息,建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

26. 一种生物特征信息的处理设备,其特征在于,包括:

接收单元,用于接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

解密单元,用于通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

存储单元,用于建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

身份识别、业务处理以及生物特征信息的处理方法和设备

技术领域

[0001] 本申请涉及网络信息安全领域,尤其涉及一种身份识别、业务处理以及生物特征信息的处理方法和设备。

背景技术

[0002] 生物识别技术是将生物技术与信息技术相结合,利用人类生物特征信息进行身份识别和认证的一种新型识别技术。人类生物特征信息包括 DNA 信息、指纹信息、人脸信息、虹膜信息等,由于生物特征信息具备唯一性和不可复制等特点,使得基于生物特征信息的生物识别技术具有安全性、保密性、方便性等优点。

[0003] 随着人们对生物识别技术研究的不断深入,在对用户身份进行识别和认证的业务场景中,生物识别技术被广泛应用。例如,在智能终端设备或穿戴式设备等终端设备上配备生物特征信息传感器,通过生物特征信息传感器采集到的生物特征信息对用户身份进行识别和认证。

[0004] 以智能终端设备为例,当用户通过智能终端设备上安装的应用程序发起支付业务时,首先,智能终端设备通过生物特征信息传感器采集用户的生物特征信息(比如指纹信息),其次,智能终端设备将采集到的用户的生物特征信息携带的支付请求发送至服务器,由服务器根据接收到的用户的生物特征信息对用户身份进行验证,并在验证通过时,响应智能终端设备发送的支付请求。

[0005] 然而,在现有利用生物识别技术对用户身份进行认证的过程中至少存在以下问题:

[0006] 由于用户的生物特征信息由终端设备采集,并通过网络发送给服务器,由服务器通过对生物特征信息进行识别和验证,也就是说,假设终端设备发送给服务器的是一个非法的生物特征信息,这不仅增加了服务器的识别难度,而且也无法保证后续业务执行的安全性,进而影响了生物特征识别技术的安全性。

发明内容

[0007] 有鉴于此,本申请实施例提供了一种身份识别、业务处理以及生物特征信息的处理方法和设备,用于解决现有技术中存在的生物识别技术中安全性比较低的问题。

[0008] 本申请提供了一种身份识别方法,包括:

[0009] 终端设备接收用户发送的业务处理请求,其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;

[0010] 所述终端设备根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;

[0011] 所述终端设备判断接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所

述用户的身份是否合法。

[0012] 本申请提供了一种业务处理方法,包括:

[0013] 服务器接收终端设备发送的业务处理请求,其中,所述业务处理请求中包含用户的生物特征信息对应的属性值和所述用户的标识信息;

[0014] 所述服务器根据接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值,其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息属性值;

[0015] 所述服务器在确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业务处理请求。

[0016] 本申请提供了一种生物特征信息的处理方法,包括:

[0017] 终端设备接收用户发送的所述用户的标识信息以及所述用户的生物特征信息;

[0018] 所述终端设备根据所述用户的生物特征信息,利用预设算法,计算得到所述用户的生物特征信息的属性值;

[0019] 所述终端设备建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

[0020] 本申请提供了一种生物特征信息的处理方法,包括:

[0021] 所述服务器接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

[0022] 所述服务器通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

[0023] 所述服务器建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0024] 本申请提供了一种身份识别设备,包括:

[0025] 接收单元,用于接收用户发送的业务处理请求,其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;

[0026] 查找单元,用于根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;

[0027] 识别单元,用于判断所述接收单元接收到的所述业务处理请求中包含的所述用户的生物特征信息与所述查找单元查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

[0028] 本申请提供了一种业务处理设备,包括:

[0029] 接收单元,用于接收终端设备发送的业务处理请求,其中,所述业务处理请求中包含用户的生物特征信息对应的属性值和所述用户的标识信息;

[0030] 查找单元,用于根据所述接收单元接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值,其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息的属性值;

[0031] 响应单元,用于确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业务处理请求。

[0032] 本申请提供了一种生物特征信息的处理设备,包括:

[0033] 接收单元,用于接收用户发送的所述用户的标识信息以及所述用户的生物特征信息;

[0034] 计算单元,用于根据所述用户的生物特征信息,利用预设算法,计算得到所述用户的生物特征信息的属性值;

[0035] 存储单元,用于建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

[0036] 本申请提供了一种生物特征信息的处理设备,包括:

[0037] 接收单元,用于接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值;

[0038] 解密单元,用于通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

[0039] 存储单元,用于建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0040] 本申请有益效果如下:

[0041] 本申请实施例提供了一种身份识别、业务处理以及生物特征信息的处理方法和设备,终端设备接收用户发送的业务处理请求,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;所述终端设备根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;所述终端设备判断接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。这样,终端设备在接收到用户发送的业务处理请求时,根据用户的生物特征信息对用户的身份进行识别,增强生物识别技术的安全性,同时为后续启动服务器对用户的身份进行识别奠定基础,此外,也避免用户的生物特征信息通过通信网络发送至服务器的过程中容易被非法窃取的风险,有效保证用户的生物特征信息的安全性。

附图说明

[0042] 为了更清楚地说明本申请实施例中的技术方案,下面将对实施例描述中所需要使

用的附图作简要介绍,显而易见地,下面描述中的附图仅仅是本申请的一部分实施例,对于本领域的普通技术人员来讲,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。

- [0043] 图 1 为本申请实施例提供一种身份识别方法流程示意图;
- [0044] 图 2 为本申请实施例提供一种业务处理方法流程示意图;
- [0045] 图 3 为本申请实施例提供一种生物特征信息的处理方法流程示意图;
- [0046] 图 4 为本申请实施例提供一种生物特征信息的处理方法流程示意图;
- [0047] 图 5 为本申请实施例提供一种身份识别设备结构示意图;
- [0048] 图 6 为本申请实施例提供一种业务处理设备结构示意图;
- [0049] 图 7 为本申请实施例提供一种生物特征信息的处理设备结构示意图;
- [0050] 图 8 为本申请实施例提供一种生物特征信息的处理设备结构示意图;
- [0051] 图 9 为本申请实施例提供一种身份识别系统的结构示意图。

具体实施方式

[0052] 随着人们对生物识别技术研究的不断深入,在需要对用户身份进行识别和认证的业务场景中,生物识别技术被广泛应用,随着科学技术的飞速发展,现有的终端设备已经配备了生物特征信息传感器,以便于用户在使用终端设备进行业务操作时,终端设备通过生物特征信息传感器采集用户的生物特征信息,并利用生物识别技术对用户的身份进行识别和认证。

[0053] 为了实现提高生物特征信息的安全性的目的,本申请实施例中提供了一种身份识别、业务处理以及生物特征信息的处理方法和设备,终端设备接收用户发送的业务处理请求,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息;所述终端设备根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息;所述终端设备判断接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

[0054] 这样,终端设备在接收到用户发送的业务处理请求时,根据用户的生物特征信息对用户的身份进行识别,增强生物识别技术的安全性,同时为后续启动服务器对用户的身份进行识别奠定基础,此外,也避免用户的生物特征信息通过通信网络发送至服务器的过程中容易被非法窃取的风险,有效保证用户的生物特征信息的安全性。

[0055] 本申请实施例中所述的终端设备是指具有生物特征信息传感器的终端设备,用户在进行业务操作时,终端设备通过生物特征信息传感器采集用户的生物特征信息,其中,所述终端设备包括但不限于智能手机、电脑等终端设备。

[0056] 在本申请实施例中,用户的生物特征信息包括但不限于用户的 DNA(英文全称:Deoxyribonucleic acid;中文名称:脱氧核糖核酸)信息、用户的指纹信息、用户的虹膜信息、用户的人脸信息、用户的视网膜信息、用户的掌形信息、用户的静脉信息、用户的耳型信息等,这里不做具体限定。

[0057] 下面结合说明书附图对本申请各个实施例作进一步地详细描述。显然,所描述的

实施例仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例,都属于本申请保护的范围。

[0058] 图1为本申请实施例提供的一种身份识别方法流程示意图,所述方法如下所述。本申请实施例的执行主体可以是终端设备。

[0059] 步骤101:终端设备接收用户发送的业务处理请求。

[0060] 其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息。

[0061] 在步骤101中,用户使用终端设备进行业务操作时,为了保证用户信息的安全性,终端设备会提示用户输入验证信息。用户输入验证信息的方式可以包含用户直接输入验证码,也可以包含用户通过生物特征传感器输入用户的生物特征信息等,在本申请实施例中仅针对采集用户的生物特征信息进行了描述。

[0062] 具体地,终端设备通过生物特征信息传感器采集用户的生物特征信息视为用户输入的验证信息。

[0063] 例如:终端设备通过所述终端设备上的指纹信息传感器采集用户的指纹信息;或者终端设备通过所述终端设备上的人脸信息传感器采集用户的人脸信息;或者终端设备通过所述终端设备上的掌形信息传感器采集用户的掌形信息。

[0064] 在用户输入生物特征信息之后,触发用户向终端设备发送业务处理请求。终端设备接收所述用户发送的业务处理请求,其中,业务处理请求中包含所述用户的标识信息以及所述用户的生物特征信息。这样所述终端设备根据接收到的用户的生物特征信息,对用户的身份进行识别和认证。

[0065] 下面以支付业务为例进行说明。在支付业务场景中,用户通过终端设备上的支付软件发起支付业务时,终端设备上的支付软件将提示用户输入支付验证信息,这里的支付验证信息限于用户的生物特征信息,那么此时,终端设备通过生物特征信息传感器采集用户的生物特征信息,以完成用户的生物特征信息的输入。在所述用户输入支付验证信息后,触发用户向终端设备发起支付业务处理请求,这里的所述支付业务处理请求中包含所述用户的标识信息以及所述用户的生物特征信息。

[0066] 步骤102:所述终端设备根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息。

[0067] 其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息。

[0068] 在步骤102中,所述终端设备在接收到用户发送的业务处理请求时,确定所述业务处理请求中包含的所述用户的标识信息和所述用户的生物特征信息,并在生物特征信息库中,利用用户的标识信息查找与所述用户的标识信息对应的生物特征信息,以便于所述终端设备根据查找到的用户的标识信息对应的生物特征信息对用户的身份进行识别。

[0069] 由于生物特征信息库中预先存储了用户的标识信息以及该用户的生物特征信息,这样终端设备在需要对用户的身份进行识别时,可以利用用户的标识信息在生物特征信息库中查找与该用户的标识信息对应的生物特征信息。

[0070] 具体地,所述终端设备通过以下方式将所述用户的生物特征信息存储至所述生物特征信息库中:

[0071] 第一步 :所述终端设备接收所述用户发送的注册请求,并获取所述注册请求中包含的所述用户的生物特征信息和所述用户的标识信息。

[0072] 用户在使用终端设备上的应用软件之前,需要在该应用软件上进行注册操作,即发送注册请求,一般注册请求中包含所述用户的标识信息和所述用户的生物特征信息,终端设备在接收到用户发送的注册请求时,能够从注册请求中获取用户的标识信息和用户的生物特征信息,并将用户的标识信息和所述用户的生物特征信息发送至应用软件对应的服务器,以完成用户在该应用软件中的注册。

[0073] 例如 :用户需要使用终端设备上的支付应用软件,那么用户需要在该支付应用软件中进行注册,在支付应用软件的注册页面,用户输入标识信息和生物特征信息等注册信息,并发起注册请求。此时,终端设备接收该注册请求,并从注册请求中获取用户的标识信息以及用户的生物特征信息。此外,终端设备将用户的标识信息和所述用户的生物特征信息等注册信息进行加密处理后发送至支付应用软件的服务器,以完成用户在支付应用软件中的注册。

[0074] 第二步 :所述终端设备建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

[0075] 终端设备在获取到用户的标识信息和用户的生物与特征信息后,建立用户的标识信息和用户的生物特征信息之间的对应关系,并将用户的标识信息和用户的生物特征信息之间的对应关系存储在终端设备的生物特征信息库中,以便于终端设备根据用户的标识信息在所述生物特征信息库中查找与用户的标识信息对应的生物特征信息。

[0076] 可选地,所述方法还包括 :

[0077] 所述终端设备在获取到所述注册请求中包含的所述用户的生物特征信息时,利用预设算法,计算得到所述用户的生物特征信息的属性值。

[0078] 具体地,所述终端设备在获取到用户的注册信息中包含的用户的生物特征信息后,所述终端根据预设算法,根据用户的生物特征信息计算得到用户的生物特征信息的属性值,例如,所述终端设备利用 Rijndael 算法(密钥生成算法)计算得到用户的生物特征信息的属性值;所述终端设备利用 Hash 函数(散列函数)算法计算得到用户的生物特征信息的属性值;所述终端设备还可以利用其他计算机算法计算得到用户的生物特征信息的属性值,本申请实施例对所述终端设备采用的算法不作具体限定。

[0079] 所述终端设备在计算得到所述用户的生物特征信息的属性值后,建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系。

[0080] 所述终端设备将所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系存储在所述生物特征信息库中。这样,在所述生物特征信息库中,所述终端设备可以根据所述用户的标识信息和上述对应关系,查找到与所述用户的标识信息对应的所述用户的生物特征信息和 / 或所述用户的标识信息对应的所述用户的生物特征信息的属性值。

[0081] 可选地,终端设备可以对所述生物特征信息库中存储的用户的生物特征信息进行更新。

[0082] 具体地,所述终端设备中的所述生物特征信息库中存储的生物特征信息可以包含

使用所述终端设备的所有用户的生物特征信息,也就是说,所述终端设备将接收到的所述用户发送的注册请求中包含的生物特征信息存储在所述生物特征信息库中之前,所述终端设备查询所述生物特征信息库中是否存储所述用户的标识信息对应的生物特征信息,若根据查询结果确定所述生物特征信息库中已经存储所述用户的生物特征信息,那么所述终端设备将接收到的所述用户发送的注册请求中包含的生物特征信息存储在所述生物特征信息库中,以更新在所述生物特征信息库中已经存储的所述用户的生物特征信息。

[0083] 需要说明的是,所述终端设备在更新所述生物特征信息库中已存储的所述用户的生物特征信息之前,提示用户输入用于验证用户身份的验证信息,比如,用户的验证邮箱、用户密码、用户预先存储在生物特征信息库中的生物特征信息等,所述终端设备在根据用户输入的验证信息验证用户的合法身份后,将接收到的所述用户的生物特征信息更新已存储的所述用户的生物特征信息,并将接收到的所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息对应的属性值存储在所述生物特征信息库中。

[0084] 所述终端设备在查询到所述生物特征信息库中没有存储与所述用户的标识信息对应的用户的生物特征信息,将接收到的所述用户的注册请求中包含的所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息对应的属性值存储在所述生物特征信息库中,也就是说,在所述生物特征信息库中增加存储所述用户的生物特征信息、所述用户的标识信息以及所述用户的生物特征信息的属性值。

[0085] 通过所述终端设备对所述生物特征信息库中的生物特征信息进行更新,一旦所述用户的生物特征信息被损坏或者丢失后,使得所述生物特征信息库及时将所述用户的新的生物特征信息更新原有的所述用户的生物特征信息,保证所述生物特征信息库中的生物特征信息的有效性,同时也能够保证所述终端设备根据所述用户发送的业务处理请求中包含的用户的标识信息,在所述生物特征信息库中查找所述用户的标识信息对应的所述用户的生物特征信息。

[0086] 步骤 103:所述终端设备判断接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

[0087] 在步骤 103 中,终端设备在接收到用户的业务处理请求后,终端设备根据所述业务处理请求中包含的用户的标识信息,可以在所述生物特征信息库中确定所述用户的标识信息对应的生物特征信息,所述终端设备根据查找到的生物特征信息对用户的身份进行识别。

[0088] 具体地,由于所述生物特征信息库中存储了用户的标识信息、用户的生物特征信息以及用户的生物特征信息的属性值之间的对应关系或者存储了用户的标识信息与所述用户的生物特征信息之间的对应关系,因此,所述终端设备可以根据所述用户的标识信息以及所述对应关系,在所述生物特征信息库中查找到的所述用户的标识信息对应的生物特征信息。

[0089] 那么,所述终端设备判断接收到的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法,包括:

[0090] 假设生物特征信息库中存储了用户的标识信息与所述用户的生物特征信息之间

的对应关系,那么终端设备根据用户的标识信息从生物特征信息库中查找到与用户的标识信息对应的用户的生物特征信息,此时,所述终端设备在确定接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息一致时,说明执行业务操作的用户和之前注册的用户是同一个人,识别所述用户的身份合法;

[0091] 所述终端设备在确定接收到的所述业务处理请求中包含的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息不一致时,说明执行业务操作的用户和之前注册的用户不是同一个人,识别所述用户的身份非法。

[0092] 假设生物特征信息库中存储了用户的标识信息、用户的生物特征信息以及用户的生物特征信息对应的属性值之间的对应关系,那么终端设备根据用户的标识信息从生物特征信息库中查找到与用户的标识信息对应的用户的生物特征信息的属性值,此时,终端设备利用预设算法计算得到接收到的所述用户的生物特征信息的属性值,此时,所述终端设备在确定接收到的所述业务处理请求中包含的所述用户的生物特征信息的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值一致时,识别所述用户的身份合法;

[0093] 所述终端设备在确定接收到的所述业务处理请求中包含的所述用户的生物特征信息的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值不一致时,识别所述用户的身份非法。

[0094] 可选地,所述方法还包括:

[0095] 所述终端设备在识别所述用户的身份合法时,将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器。

[0096] 需要说明的是,在本申请实施例中,所述终端设备可以通过查找的方式确定所述用户的标识信息对应的生物特征信息的属性值,也可以通过利用预设的算法对所述用户的生物特征信息进行计算的方式确定所述用户的标识信息对应的生物特征信息的属性值,这里不做具体限定。

[0097] 需要说明的是,所述终端设备在识别所述用户的身份合法后,向服务器发送业务处理请求,这里的业务处理请求和步骤 101 中所述用户发送的业务处理请求所代表的业务相同,但包含的内容不相同,这里的业务处理请求包含所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值,步骤 101 中用户发送的业务处理请求包含所述用户的标识信息以及所述用户的生物特征信息。

[0098] 可选地,为了保证所述用户的生物特征信息的属性值在传输至服务器的过程中的安全性,所述终端设备将所述用户的生物特征信息的属性值和所述用户的标识信息执行加密操作,并将加密后的生物特征信息的属性值以及所述用户的标识信息发送至服务器。

[0099] 具体地,所述终端设备将所述用户的标识信息和确定的所述用户的生物特征信息对应的属性值进行加密,得到加密结果;

[0100] 所述终端设备将携带所述加密结果的所述业务处理请求发送至服务器。

[0101] 需要说明的是,所述终端设备和所述服务器通过协商之后分别得到各自的私钥和公钥,所述终端设备和所述服务器的私钥是保密的,所述终端设备和所述服务器的公钥是公开的,且所述终端设备/所述服务器的公钥和私钥是成对匹配的。

[0102] 所述终端设备向所述服务器发送所述用户的生物特征信息的属性值和所述用户的标识信息时,利用所述服务器的公钥对发送的所述用户的生物特征信息的属性值和所述用户的标识信息进行加密,得到加密结果,并将加密结果发送至所述服务器。所述服务器利用自己的私钥对接收到的加密结果进行解密,由于所述服务器的私钥是保密的,因此,所述终端设备发送的加密结果只有所述服务器可以解密得到,保证所述终端设备发送的用户的生物特征信息的属性值的安全性。

[0103] 为了进一步保证用户的生物特征信息的属性值的安全性,所述终端设备在利用所述服务器的公钥对发送的加密结果进行加密后,所述终端设备还可以利用自己的私钥对发送的用户的生物特征信息的属性值进行第二次加密。这样,当所述服务器接收到加密结果后,首先利用所述终端设备的公钥对接收到的加密结果进行解密,如果所述服务器解密成功,说明所述服务器接收到的加密结果是由所述终端设备发送的,即所述终端设备发送的用户的生物特征信息的属性值在传递的过程中没有被篡改,然后所述服务器利用自己的私钥对加密结果进行解密,得到所述终端设备发送的用户的生物特征信息的属性值以及用户的标识信息。

[0104] 在本申请实施例中,所述终端设备将所述用户的标识信息对应的生物特征信息的属性值和所述用户的标识信息进行加密后,发送至所述服务器,不仅保证所述用户的标识信息对应的生物特征信息的属性值在传递过程中的安全性,并且,相比于现有技术中所述终端设备直接将用户的生物特征信息发送至所述服务器,本申请实施例中的所述终端设备将与用户的标识信息对应的生物特征信息的属性值发送至所述服务器,避免用户生物特征信息在传输过程中容易被他人获取的风险,提高用户的生物特征信息的安全性。

[0105] 可选地,所述终端设备在识别所述用户的身份非法时,向所述用户返回身份识别结果,拒绝响应所述用户的业务处理请求,并提示用户身份识别没有通过,例如,所述终端设备提示所述用户重新登录、所述终端设备显示告警信息并提示所述用户身份非法、所述终端设备直接返回所述用户的业务操作界面等,这里对所述终端设备向所述用户放回的身份识别结果的内容和形式不做具体限定。

[0106] 通过本申请实施例所述的方案,终端设备在接收到用户发送的业务处理请求时,根据用户的生物特征信息对用户的身份进行识别,增强生物识别技术的安全性,同时为后续启动服务器对用户的身份进行识别奠定基础,此外,也避免用户的生物特征信息通过通信网络发送至服务器的过程中容易被非法窃取的风险,有效保证用户的生物特征信息的安全性。

[0107] 图2为本申请实施例提供的一种业务处理方法流程示意图,所述方法如下所述。本申请实施例的执行主体可以是服务器。

[0108] 步骤201:服务器接收终端设备发送的业务处理请求。

[0109] 其中,所述业务处理请求中包含用户的生物特征信息对应的属性值和所述用户的标识信息。

[0110] 在步骤201中,所述服务器接收所述终端设备发送的业务处理请求,业务处理请求中携带所述用户的标识信息和所述用户的标识信息对应的生物特征信息的属性值加密后的加密结果。

[0111] 所述服务器接收到所述终端设备发送的业务处理请求后,所述服务器对业务处理

请求中包含的加密的所述用户的生物特征信息的属性值和所述用户的标识信息进行解密操作,并通过解密操作得到所述业务处理请求中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0112] 所述服务器通过本申请提供的第一个实施例中的解密方法对所述加密后的所述用户的生物特征信息的属性值和所述用户的标识信息进行解密,这里不再重复描述。

[0113] 所述服务器对加密结果进行解密后,得到所述终端设备发送的业务处理请求中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0114] 步骤 202:所述服务器根据接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值。

[0115] 其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息的属性值。

[0116] 在步骤 202 中,所述服务器在接收到所述终端设备发送的业务处理请求时,确定所述业务处理请求中包含的所述用户的标识信息和所述用户的生物特征信息的属性值,并在生物识别数据库中,利用用户的标识信息查找与所述用户的标识信息对应的生物特征信息的属性值,以便于所述服务器根据查找到的用户的标识信息对应的生物特征信息的属性值对用户的身份进行验证。

[0117] 由于生物识别数据库中预先存储了用户的标识信息以及该用户的生物特征信息的属性值,这样服务器在需要对用户的身份进行验证时,可以利用用户的标识信息在生物识别数据库中查找与该用户的标识信息对应的生物特征信息的属性值。

[0118] 具体地,所述服务器通过以下方式将所述用户的标识信息对应的生物特征信息的属性值存储至所述生物识别数据库中:

[0119] 第一步:所述服务器接收所述终端设备发送的用户信息。

[0120] 其中,所述用户信息是所述终端设备将用户发送的注册请求中包含的所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值。

[0121] 由于终端设备在接收到用户发送的注册请求时,获取了注册请求中包含的所述用户的标识信息和所述用户的生物特征信息,并根据所述用户的生物特征信息确定所述用户的生物特征信息的属性值,进而通过对所述用户的生物特征信息的属性值和所述用户的标识信息进行加密,并将加密后的所述用户的生物特征信息的属性值和所述用户的标识信息发送至所述服务器,使得所述服务器接收到所述终端设备发送的加密后的所述用户的标识信息和所述用户的生物特征信息的属性值。

[0122] 第二步:所述服务器通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0123] 所述服务器利用所述终端设备的公钥对加密后的所述用户信息进行解密,验证业务处理请求是否是所述终端设备发送的,验证通过后,所述服务器确定携带所述加密结果的注册处理请求在传递的过程中没有被篡改,所述服务器利用自己的公钥对加密进行第二次解密,所述服务器得到所述用户的生物特征信息的属性值和所述用户的标识信息。

[0124] 第三步:所述服务器建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0125] 所述服务器在得到所述用户的生物特征信息的属性值以及所述用户的标识信息后,建立所述用户的标识信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述用户的标识信息以及所述用户的生物特征信息的属性值之间的对应关系存储在所述服务器中的所述生物识别数据库中。

[0126] 这样,在所述生物识别数据库中,所述服务器可以根据所述用户的标识信息和上述对应关系,查找到与所述用户的标识信息对应的所述用户的生物特征信息的属性值。

[0127] 可选地,服务器在接收到终端设备发送的用户的标识信息和所述用户的生物特征信息的属性值时,首先,确定生物识别数据库中是否已存储与所述用户的标识信息对应的用户的生物特征信息的属性值;其次,在确定已存储与所述用户的标识信息对应的用户的生物特征信息的属性值时,可以利用接收到的用户的生物特征信息的属性值更新已存储的用户的生物特征信息的属性值;在确定未存储与所述用户的标识信息对应的用户的生物特征信息的属性值时,可以将接收到的用户的生物特征信息的属性值存储至生物识别数据库中,以便于后续对用户的身份进行识别。

[0128] 步骤 203:所述服务器在确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业务处理请求。

[0129] 具体地,由于所述生物识别数据库中存储了用户的标识信息与用户的生物特征信息属性值之间的对应关系,因此,所述服务器可以根据所述用户的标识信息以及所述对应关系,在所述生物识别数据库中查找到所述用户的标识信息对应的生物特征信息的属性值。

[0130] 那么,所述服务器在所述生物识别数据库中查找到所述用户的标识信息对应的所述用户的生物特征信息的属性值后,所述服务器将接收到的所述用户的生物特征信息的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值进行对比,包括:

[0131] 所述服务器确定接收到的所述用户的生物特征信息的属性值与查找到的所述用户的生物特征信息的属性值相同,说明执行业务操作的用户和之前注册的用户是同一个人,所述服务器对验证所述用户的身份合法,所述服务器响应接收到的所述终端设备发送的业务处理请求;

[0132] 所述服务器确定接收到的所述用户的生物特征信息的属性值与查找到的所述用户的生物特征信息的属性值不相同,说明执行业务操作的用户和之前注册的用户不是同一个人,所述服务器验证所述用户的身份非法,所述服务器拒绝响应接收到的所述终端设备发送的业务处理请求。

[0133] 可选地,所述服务器验证所述用户的身份非法后,提示所述终端设备所述用户的身份非法,并返回告警信息,告警业务处理请求处理失败,这里对所述服务器返回告警信息的内容和形式不作具体限定。

[0134] 图 3 为本申请实施例提供的一种生物特征信息的处理方法流程示意图,所述方法如下所述。本申请实施例的执行主体可以是终端设备。

[0135] 步骤 301:终端设备接收用户发送的所述用户的标识信息以及所述用户的生物特征信息。

[0136] 在步骤 301 中,用户发送的用户的标识信息和用户的生物特征信息可以是用户在

注册应用软件时发送的,也可以是用户在执行其他操作时发送的,这里不做具体限定。

[0137] 终端设备接收用户发送的用户的标识信息和用户的生物特征信息,以便于终端设备对用户的生物特征信息进行处理。

[0138] 步骤 302:所述终端设备根据所述用户的生物特征信息,利用预设算法,计算得到所述用户的生物特征信息的属性值。

[0139] 所述终端设备根据所述用户的生物特征信息,利用本申请提供的第一个实施例中的预设算法,计算得到所述用户的生物特征信息的属性值,这里不再重复描述。

[0140] 可选地,所述终端设备得到所述用户的生物特征信息的属性值后,将所述用户的标识信息以及所述用户的生物特征信息的属性值进行加密,得到加密结果,并将所述终端设备将所述加密结果发送至所述服务器。

[0141] 本申请实施例中的所述终端设备使用本申请提供的第一个实施例中的加密方法对用户的生物特征信息的属性值和用户的标识信息进行加密,这里不再重复描述。

[0142] 步骤 303:所述终端设备建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

[0143] 在步骤 303 中所述终端设备将用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系存储在所述生物特征信息库中之前,所述终端设备在所述生物特征信息库中查询是否存在所述用户的生物特征信息,若所述生物特征信息库中可能已经存储所述用户的生物特征信息,那么所述终端设备将接收到的用户发送的生物特征信息存储在所述生物特征信息库中,以更新在所述生物特征信息库中已经存储的所述用户的生物特征信息。

[0144] 具体地,所述终端设备向所述生物特征信息库发送查询请求,其中,所述查询请求中包含所述用户的标识信息;

[0145] 所述终端设备接收所述生物特征信息库返回的查询结果;

[0146] 所述终端设备根据查询结果确定在所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息,利用接收到的所述用户的生物特征信息更新所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息。

[0147] 这里的生物特征信息库的更新方式与本申请提供的第一个实施例中的生物特征信息库的更新方式相同,不再重复描述。

[0148] 所述终端设备在确定所述生物特征信息库中没有存储所述用户的生物特征信息,那么所述终端设备确定接收到的所述生物特征信息的属性值,并在所述生物特征信息库增加存储所述用户的生物特征信息、所述用户的标识信息以及所述用户的生物特征信息的属性值之间的对应关系。

[0149] 图 4 为本申请实施例提供的一种生物特征信息的处理方法流程示意图,所述方法如下所述。

[0150] 步骤 401:所述服务器接收所述终端设备发送的用户信息。

[0151] 其中,所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值。

[0152] 步骤 402 :所述服务器通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0153] 所述服务器通过本申请提供的第一个实施例中的解密方法对所述加密后的所述用户的生物特征信息的属性值和所述用户的标识信息进行解密,这里不再重复描述。

[0154] 所述服务器对所述用户信息解密后,得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0155] 步骤 403 :所述服务器建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0156] 所述服务器在得到所述用户的生物特征信息的属性值以及所述用户的标识信息后,建立所述用户的标识信息以及所述用户的生物特征信息的属性值之间的对应关系,并将所述用户的标识信息以及所述用户的生物特征信息的属性值对应存储在所述服务器中的所述生物识别数据库中。

[0157] 可选地,所述服务器还可以对所述生物识别数据库中存储的用户的生物特征信息进行更新,更新的具体实现方式与图 2 中步骤 202 中所使用的方式相同,这里不再赘述。

[0158] 图 5 为本申请实施例提供的一种身份识别设备结构示意图。所述身份识别设备包括 :接收单元 51、查找单元 52、识别单元 53、发送单元 54、建立单元 55、计算单元 56 和返回单元 57,其中 :

[0159] 接收单元 51,用于接收用户发送的业务处理请求,其中,所述业务处理请求中包含用户的标识信息以及所述用户的生物特征信息 ;

[0160] 查找单元 52,用于根据所述业务处理请求中包含的用户的标识信息,从生物特征信息库中查找所述用户的标识信息对应的生物特征信息,其中,所述生物特征信息库中包含用户的标识信息以及所述用户的标识信息对应的生物特征信息 ;

[0161] 识别单元 53,用于判断所述接收单元 51 接收到的所述业务处理请求中包含的所述用户的生物特征信息与所述查找单元查找到的所述用户的标识信息对应的生物特征信息是否一致,并根据判断结果识别所述用户的身份是否合法。

[0162] 可选地,所述身份识别设备还包括 :发送单元 54,其中 :

[0163] 所述发送单元 54,用于在识别所述用户的身份合法时,确定所述用户的生物特征信息的属性值,并将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器。

[0164] 具体地,所述发送单元 54 将所述属性值以及所述用户的标识信息携带在业务处理请求中发送至服务器,包括 :

[0165] 将所述用户的标识信息和所述属性值进行加密,得到加密结果 ;

[0166] 将携带所述加密结果的业务处理请求发送至服务器。

[0167] 可选地,所述身份识别设备还包括 :建立单元 55,其中 :

[0168] 所述接收单元 51,还用于接收所述用户发送的注册请求,并获取所述注册请求中包含的所述用户的生物特征信息和所述用户的标识信息 ;

[0169] 所述建立单元 55,用于建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,并将所述对应关系存储在所述生物特征信息库中。

[0170] 可选地,所述身份识别设备还包括 :计算单元 56,其中 :

[0171] 所述计算单元 56,用于在获取到所述注册请求中包含的所述用户的生物特征信息时,利用预设算法,计算得到所述用户的生物特征信息的属性值;

[0172] 所述建立单元 55 建立所述用户的标识信息与所述用户的生物特征信息之间的对应关系,包括:

[0173] 建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系。

[0174] 可选地,所述身份识别设备还包括:返回单元 57,其中:

[0175] 所述返回单元 57,用于在所述识别单元 53 识别所述用户的身份非法时,向所述用户返回身份识别结果。

[0176] 需要说明的是,本申请实施例提供的身份识别设备可以通过硬件方式实现,也可以通过软件方式实现,这里不做具体限定。

[0177] 图 6 为本申请实施例提供的一种业务处理设备结构示意图。所述业务处理设备包括:接收单元 61、查找单元 62、响应单元 63、解密单元 64 和建立单元 65,其中:

[0178] 接收单元 61,用于接收终端设备发送的业务处理请求,其中,所述业务处理请求中包含用户的生物特征信息对应的属性值和所述用户的标识信息;

[0179] 查找单元 62,用于根据所述接收单元 61 接收到的业务处理请求中包含的所述用户的标识信息,从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值,其中,所述生物识别数据库中包含所述用户的标识信息以及所述用户的标识信息对应的生物特征信息的属性值;

[0180] 响应单元 63,用于确定接收到的所述业务处理请求中包含的用户的生物特征信息对应的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值相同时,响应所述业务处理请求。

[0181] 可选地,所述业务处理设备还包括:解密单元 64,其中:

[0182] 所述解密单元 64,用于在所述接收单元 61 接收所述终端设备发送的业务处理请求后,所述查找单元 62 从生物识别数据库中查找所述用户的标识信息对应的生物特征信息的属性值之前,通过解密操作得到所述业务处理请求中包含的所述用户的生物特征信息的属性值和所述用户的标识信息。

[0183] 可选地,所述业务处理设备还包括:建立单元 65,其中:

[0184] 所述接收单元 61,还用于接收所述终端设备发送的用户信息,其中,所述用户信息是所述终端设备将用户发送的注册请求中包含的所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的,所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值,所述注册请求中包含所述用户的生物特征信息和所述用户的标识信息;

[0185] 所述解密单元 64,还用于通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息;

[0186] 所述建立单元 65,用于建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0187] 需要说明的是,本申请实施例提供的业务处理设备可以通过硬件方式实现,也可以通过软件方式实现,这里不做具体限定。

[0188] 图7为本申请实施例提供的一种生物特征信息的处理设备结构示意图。所述生物特征信息的处理设备包括：接收单元71、计算单元72、存储单元73、加密单元74和发送单元75，其中：

[0189] 接收单元71，用于接收用户发送的所述用户的标识信息以及所述用户的生物特征信息；

[0190] 计算单元72，用于根据所述用户的生物特征信息，利用预设算法，计算得到所述用户的生物特征信息的属性值；

[0191] 存储单元73，用于建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的生物特征信息的属性值之间的对应关系，并将所述对应关系存储在所述生物特征信息库中。

[0192] 具体地，所述生物特征信息的处理设备还包括：加密单元74和发送单元75，其中：

[0193] 所述加密单元74，用于在所述计算单元72计算得到所述用户的标识信息对应的生物特征信息的属性值后，将所述用户的标识信息以及所述用户的生物特征信息的属性值进行加密，得到加密结果；

[0194] 所述发送单元75，用于将所述加密结果发送至所述服务器。

[0195] 可选地，所述存储单元73建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系，并将所述对应关系存储在所述生物特征信息库中，包括：

[0196] 向所述生物特征信息库发送查询请求，其中，所述查询请求中包含所述用户的标识信息；

[0197] 接收所述生物特征信息库返回的查询结果；

[0198] 根据查询结果确定在所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息，利用接收到的所述用户的生物特征信息更新所述生物特征信息库中已存储与所述用户的标识信息对应的用户的生物特征信息；

[0199] 根据查询结果确定在所述生物特征信息库中未存储与所述用户的标识信息对应的用户的生物特征信息，建立所述用户的标识信息、所述用户的生物特征信息以及所述用户的标识信息对应的生物特征信息的属性值之间的对应关系，并将所述对应关系存储在所述生物特征信息库中。

[0200] 需要说明的是，本申请实施例提供的生物特征信息的处理设备可以通过硬件方式实现，也可以通过软件方式实现，这里不做具体限定。

[0201] 图8为本申请实施例提供的一种生物特征信息的处理设备结构示意图。所述生物特征信息的处理设备包括：接收单元81、解密单元82和存储单元83，其中：

[0202] 接收单元81，用于接收所述终端设备发送的用户信息，其中，所述用户信息是所述终端设备得到所述用户的生物特征信息的属性值时对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密后发送的，所述用户信息中包含所述用户的标识信息和所述用户的生物特征信息的属性值；

[0203] 解密单元82，用于通过解密操作得到所述用户信息中包含的所述用户的生物特征信息的属性值和所述用户的标识信息；

[0204] 存储单元 83,用于建立所述用户的标识信息与所述用户的生物特征信息的属性值之间的对应关系,并将所述对应关系存储在所述生物识别数据库中。

[0205] 需要说明的是,本申请实施例提供的生物特征信息的处理设备可以通过硬件方式实现,也可以通过软件方式实现,这里不做具体限定。

[0206] 图 9 为本申请实施例提供的一种身份识别系统的结构示意图。所述系统包括:终端设备和服务器设备,其中,所述终端设备包含身份识别单元 91、身份识别返回单元 92,所述服务器设备包含:身份验证单元 93 和业务处理单元 94。

[0207] 在身份识别系统中,终端设备在接收到用户发送的业务处理请求时,将发起对该用户的身份识别。

[0208] 具体地,所述身份识别单元 91,用于根据用户发送的业务处理请求识别所述用户的身份是否合法,其中,所述业务处理请求包含所述用户的标识信息和所述用户的生物特征信息;

[0209] 所述身份识别返回单元 92,用于在所述身份识别单元 91 识别所述用户的身份非法后,向所述用户返回身份识别结果。

[0210] 可选地,所述身份识别单元 91 还包括:生物特征信息采集模块 911、生物特征信息计算模块 912、生物特征信息识别模块 913 和发送模块 914,其中:

[0211] 所述生物特征信息采集模块 911,用于采集用户的生物特征信息;

[0212] 所述生物特征信息计算模块 912,用于根据所述生物特征信息采集模块 911 采集的所述用户的生物特征信息,计算得到所述用户的生物特征信息的属性值;

[0213] 所述生物特征信息识别模块 913,用于根据所述用户的标识信息、所述生物特征信息采集模块 911 采集的所述用户的生物特征信息识别所述用户的身份是否合法;

[0214] 所述发送模块 914,用于对所述用户的标识信息和所述用户的生物特征信息的属性值进行加密,并将加密结果发送至所述服务器设备。

[0215] 具体地,所述终端设备接收用户发送的业务处理请求,所述生物特征信息采集模块 911 采集所述用户的生物特征信息,所述生物特征信息识别模块 913 根据所述用户的标识信息,从所述终端设备中的生物特征信息库中查找所述用户的标识信息对应的生物特征信息,此时,所述生物特征信息识别模块 913 确定接收到的所述用户的生物特征信息与查找到的所述用户的标识信息对应的生物特征信息一致时,所述生物特征信息识别模块 913 识别所述用户的身份合法。

[0216] 可选地,所述生物特征信息计算模块 912 根据所述用户的生物特征信息,计算得到所述生物特征信息的属性值,所述生物特征信息识别模块 913 从所述终端设备中的生物特征信息库中查找所述用户的标识信息对应的生物特征信息的属性值,此时,所述生物特征信息识别模块 913 在确定接收到所述用户的生物特征信息的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值一致时,所述生物特征信息识别模块 913 识别所述用户的身份合法。

[0217] 可选地,所述生物特征信息识别模块 913 识别所述用户的身份合法后,所述生物特征信息识别模块 913 从生物特征信息库中查找所述用户的标识信息对应的生物特征信息的属性值/所述生物特征信息计算模块 912 根据接收到的所述用户的生物特征信息计算所述用户的生物特征信息的属性值,所述发送模块 914 将所述用户的标识信息和所述用户

的生物特征信息的属性值进行加密,并携带加密结果的业务处理请求发送至所述服务器设备。

[0218] 在身份识别系统中,服务器设备在接收到终端设备发送的业务处理请求时,将发起对该业务处理请求者的身份识别。

[0219] 具体地,所述身份验证单元 93,用于根据接收到的用户标识信息和所述用户的生物特征信息的属性值,验证所述用户的身份是否合法;

[0220] 所述业务处理单元 94,用于在所述身份验证单元 93 验证所述用户的身份合法后,对所述用户发送的业务处理请求进行处理。

[0221] 可选地,所述身份验证单元 93 还包括:接收模块 931、解密模块 932、生物特征信息验证模块 933 和身份验证返回模块 934,其中:

[0222] 所述接收模块 931,用于接收所述发送模块 914 发送的加密结果;

[0223] 所述解密模块 932,用于对所述接收模块 931 接收到的加密结果进行解密,得到解密后的所述用户的标识信息和所述用户的生物特征信息的属性值;

[0224] 所述生物特征信息验证模块 933,用于根据所述用户的标识信息和所述用户的生物特征信息的属性值验证所述用户的身份是否合法;

[0225] 所述身份验证返回模块 934,用于在所述生物特征信息验证模块 933 验证所述用户的身份非法后,向所述用户返回验证结果。

[0226] 具体地,所述接收模块 931 接收所述终端设备发送的携带加密结果的业务处理请求,所述解密模块 932 对所述加密结果进行解密,得到解密后的所述用户的标识信息和所述用户的生物特征信息的属性值,所述生物特征信息验证模块 933 根据所述用户的标识信息,从所述服务器设备中的生物识别数据库中查找所述用户的标识信息对应的所述用户的生物特征信息的属性值。

[0227] 此时,所述生物特征信息验证模块 933 确定接收到的所述用户的生物特征信息的属性值与查找到的所述用户的标识信息对应的生物特征信息的属性值一致时,所述生物特征信息验证模块 933 验证所述用户的身份合法。

[0228] 本领域的技术人员应明白,本申请的实施例可提供为方法、装置(设备)、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0229] 本申请是参照根据本申请实施例的方法、装置(设备)和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0230] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指

令装置的制造品,该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

[0231] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0232] 尽管已描述了本申请的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例作出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0233] 显然,本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。这样,倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内,则本申请也意图包含这些改动和变型在内。

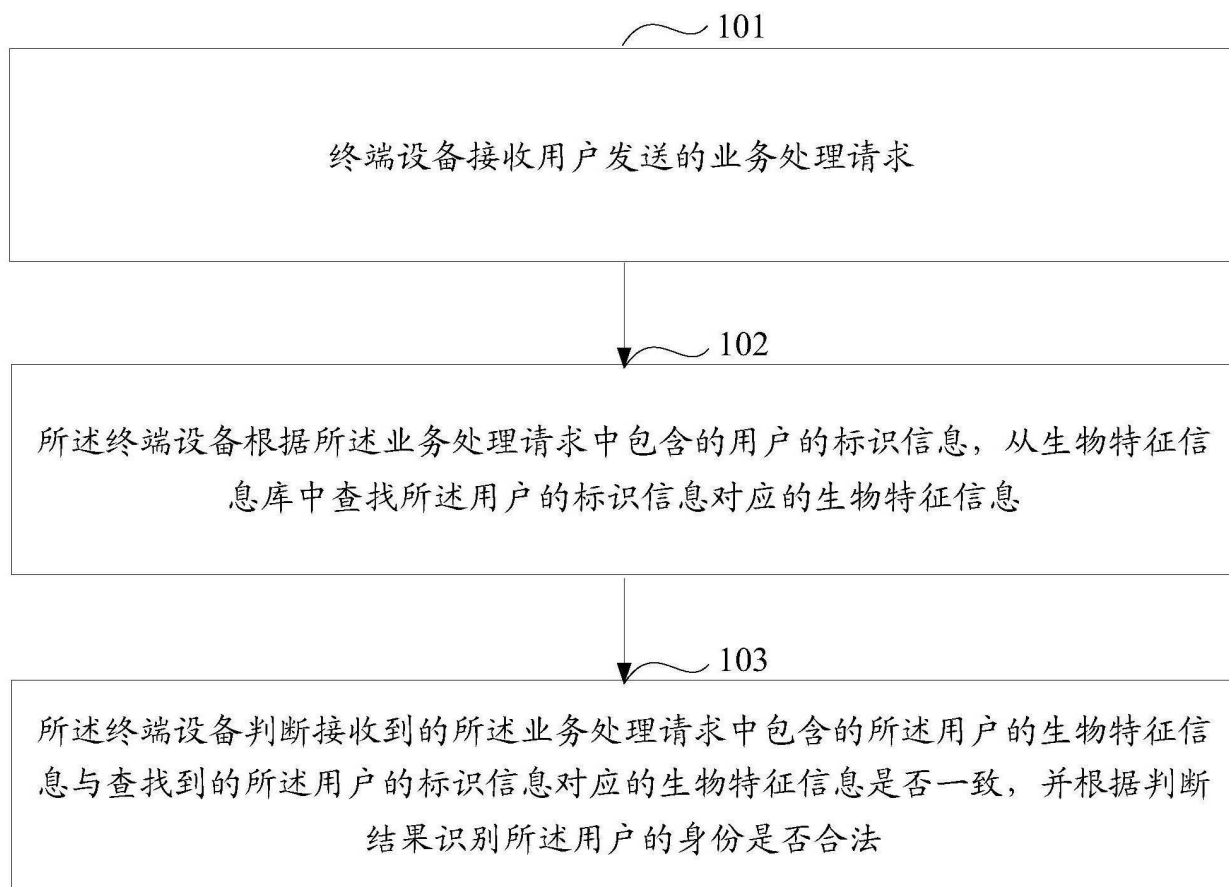


图 1

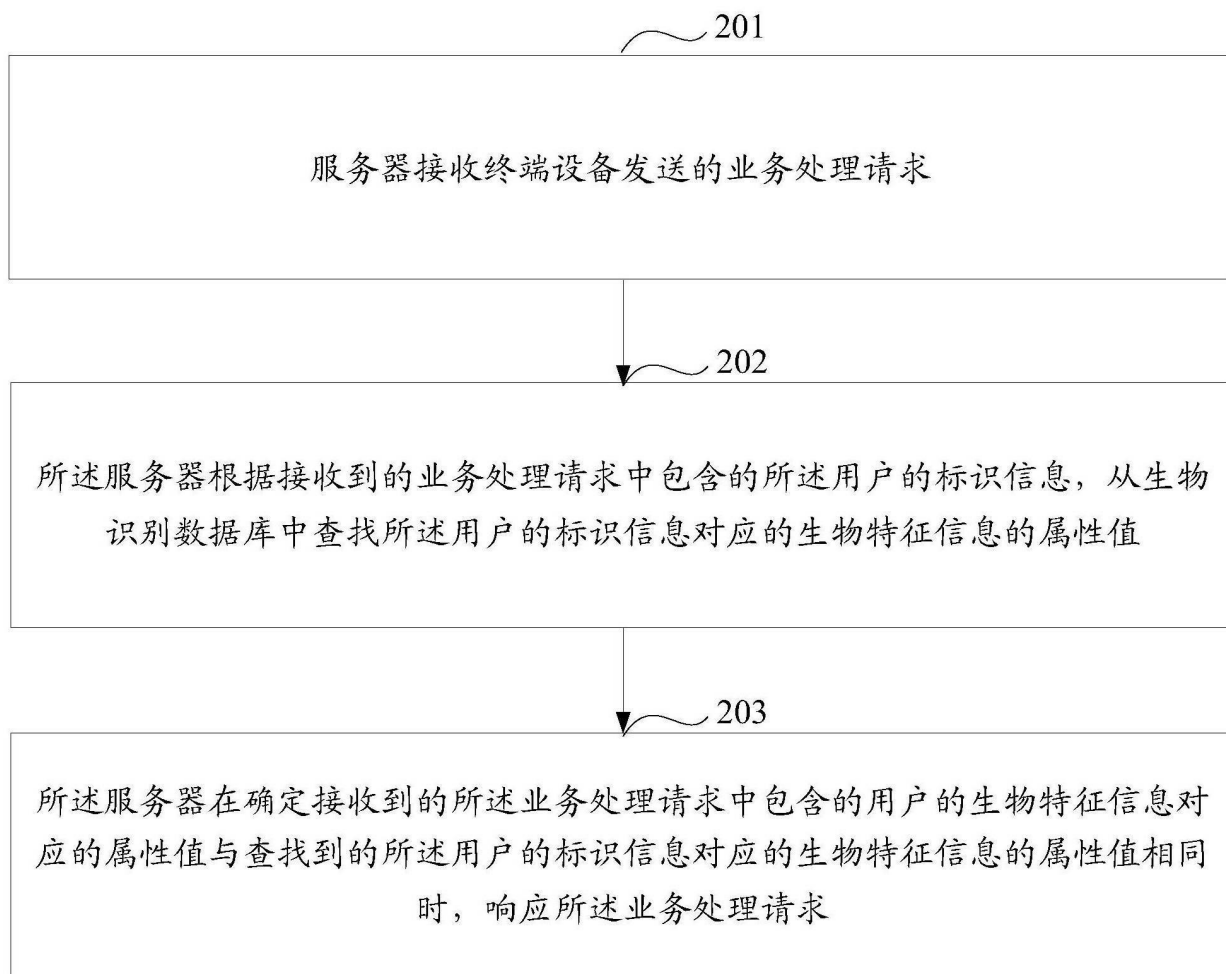


图 2

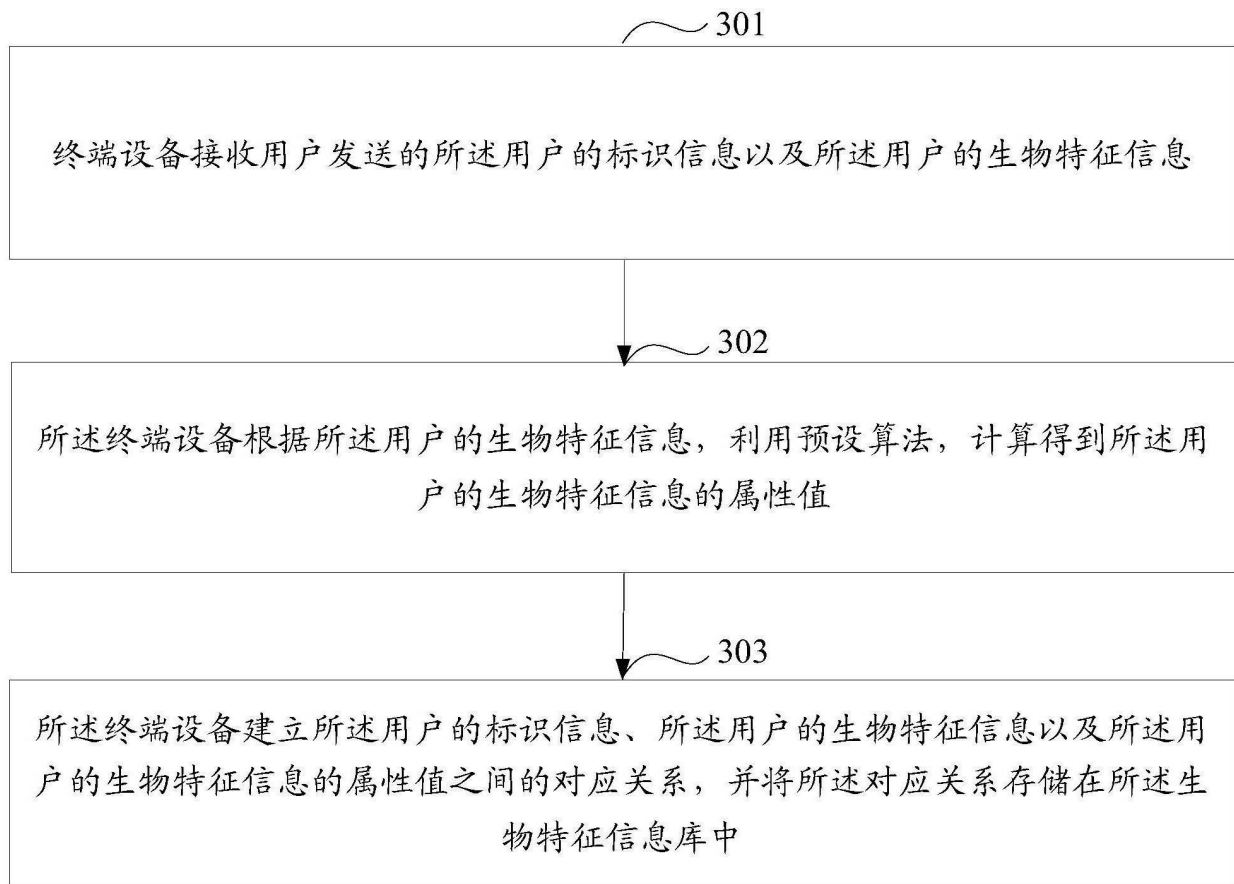


图 3

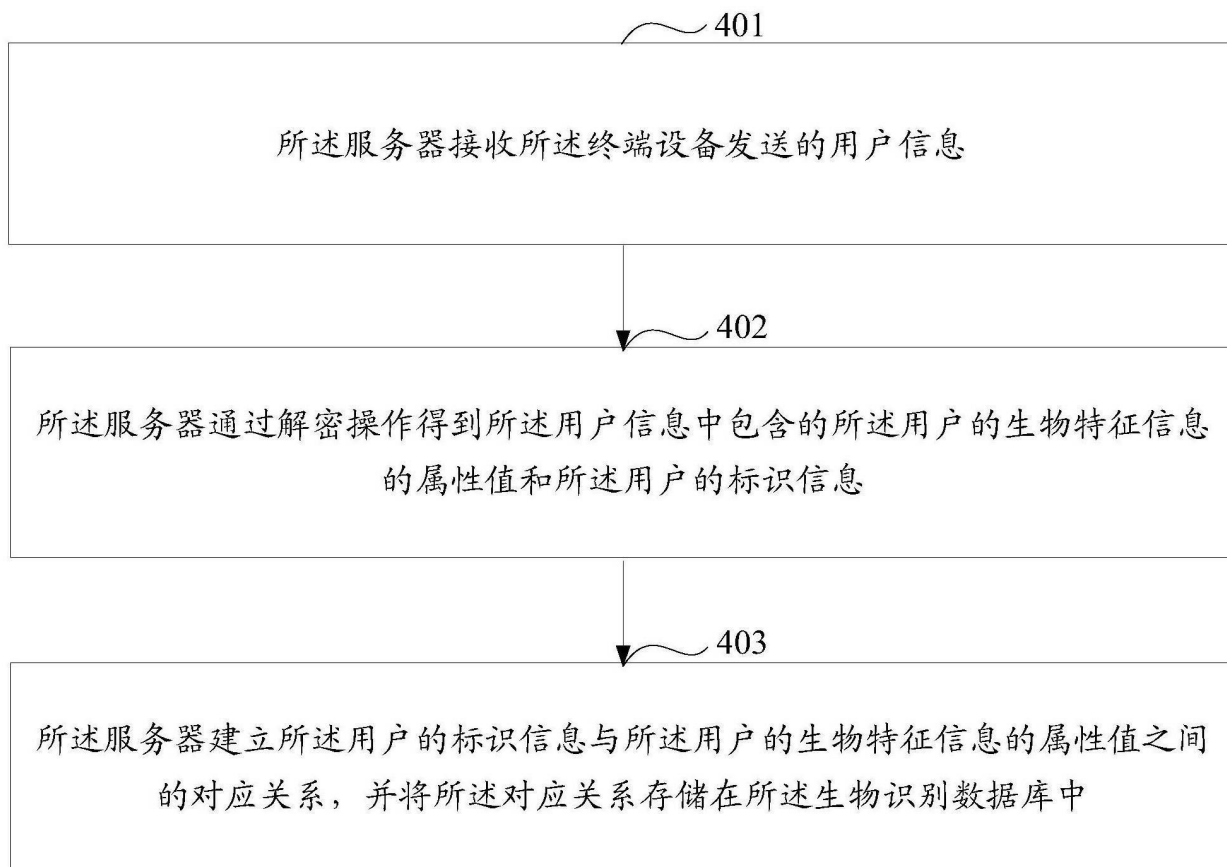


图 4

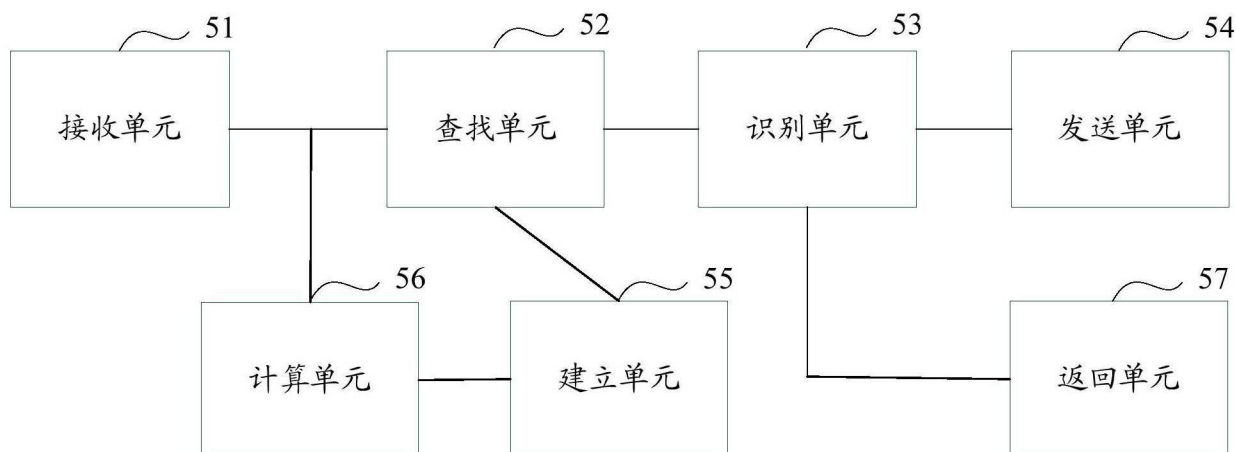


图 5

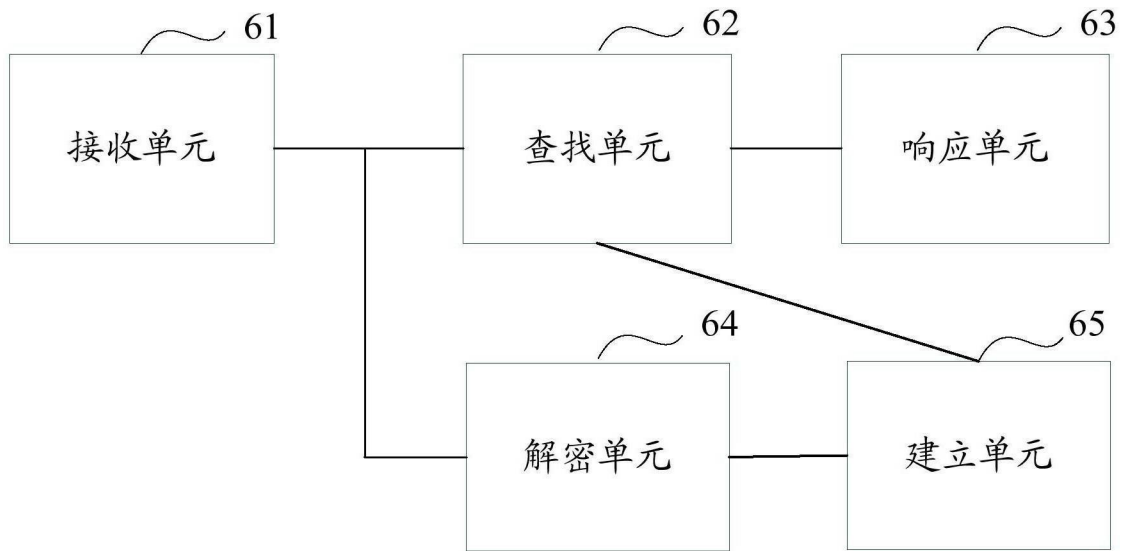


图 6

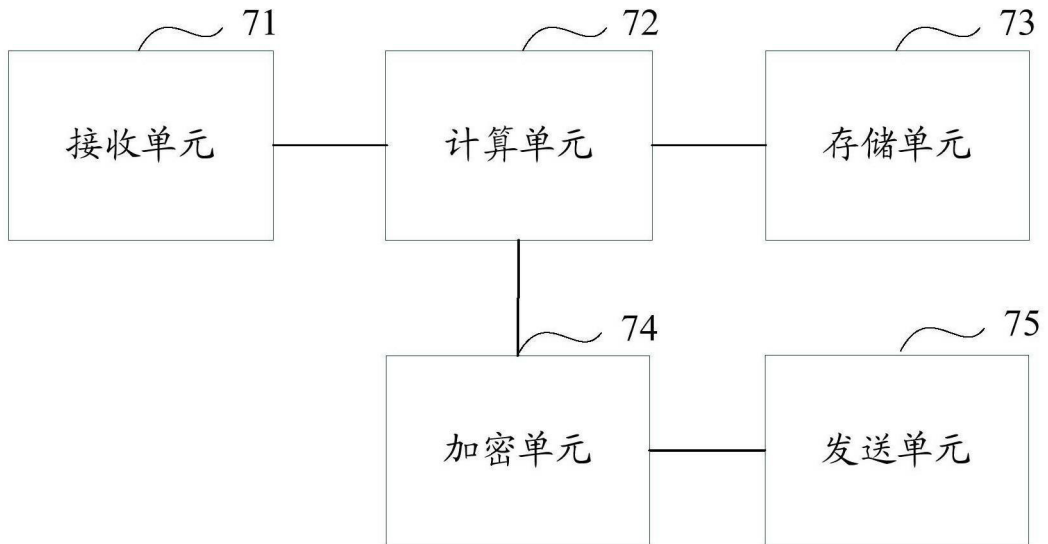


图 7

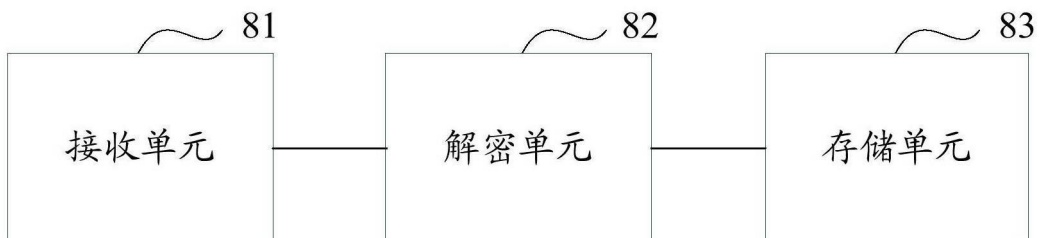


图 8

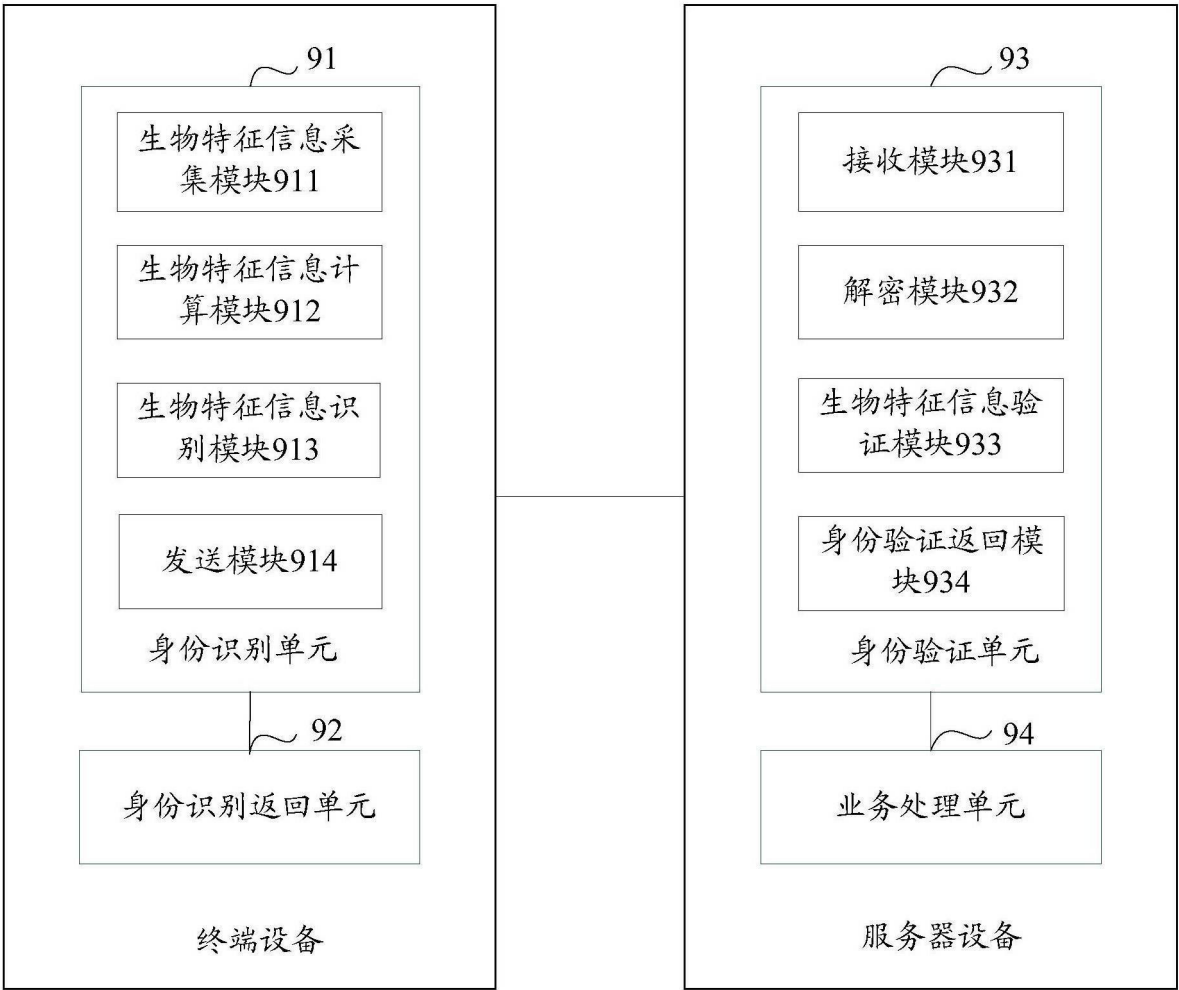


图 9

Abstract

The disclosure discloses an identity recognition, service processing and biological feature information processing method and device. The method comprises the steps that terminal equipment receives a service processing request sent by a user; according to identification information, which is contained in the service processing request, of the user, the terminal equipment searches biological feature information corresponding to the identification information of the user in a biological feature information base; and the terminal equipment judges whether biological feature information, which is contained in the received service processing request, of the user is consistent with the searched biological feature information corresponding to the identification information of the user or not, and recognizes whether the identity of use is legal or not according to a judgment result. The terminal equipment performs recognition on the identity of the user according to the biological feature information of the user, thereby enhancing the safety of a biological recognition technology, laying a foundation for subsequently starting a server to perform recognition on the identity of the user, also avoiding the risk that the biological feature information of the user is easy to be illegally stolen in the process of sending the biological feature information of the user to the server through a communication network, and effectively protecting the safety of the biological feature information of the user.