(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112347488 B
(45)授权公告日 2023.11.03

(21)申请号 201910726722.8

(22)申请日 2019.08.07

(65)同一申请的已公布的文献号
申请公布号 CN 112347488 A

(43)申请公布日 2021.02.09

(73)专利权人 北京京东振世信息技术有限公司
地址 100086 北京市海淀区知春路76号6层

(72)发明人 王茹

(74)专利代理机构 北京律智知识产权代理有限公司 11438
专利代理师 孙宝海 袁礼君

(51)Int.Cl.
*G06F 21/60*(2013.01)
*G06F 21/62*(2013.01)

(56)对比文件
CN 107181816 A,2017.09.19
CN 109088845 A,2018.12.25
CN 105096172 A,2015.11.25
US 2011154031 A1,2011.06.23
闫鑫;杨凯凡.基于快递运输中隐私单面的加密研究.高师理科学刊.2017,(12),全文.

审查员 孙旭

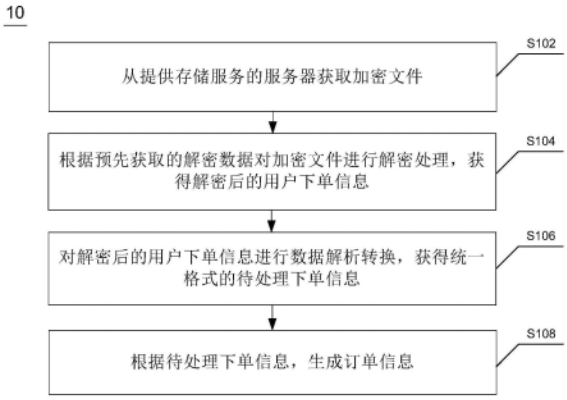
权利要求书2页 说明书13页 附图6页

(54)发明名称

# 订单信息处理方法及装置、设备及存储介质

(57)摘要

本发明公开一种订单信息处理方法及装置、设备及存储介质。所述订单信息处理方法包括：从提供存储服务的服务器获取加密文件，所述加密文件中包括经加密处理的用户下单信息；根据预先获取的解密数据对所述加密文件进行解密处理，获得解密后的用户下单信息，其中所述解密数据包括解密密码及解密文件；对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息；根据所述待处理下单信息，生成订单信息。根据本发明提供的订单信息处理方法，能够安全、高效地生成统一格式订单，有效地避免了物流方与下单方通过公共网络传输信息可能导致的用户隐私泄露。




CN 112347488 B

1.一种订单信息处理方法,其特征在于,包括:

从提供存储服务的服务器获取加密文件,所述加密文件中包括经加密处理的用户下单信息;

根据预先获取的解密数据对所述加密文件进行解密处理,获得解密后的用户下单信息,其中所述解密数据包括解密密码及解密文件;

以字节数组信息流的形式输出解密后的用户下单信息,根据预设的文本字段位置,从第一列开始依次放置字段,从而将对应用户下单信息的字节数组输出流解析为文本集合对象;

将所述文本集合对象转换为物流平台内部下单接口的入参对象,获得下单接口输出的待处理下单信息;

根据所述待处理下单信息,生成订单信息。

2.根据权利要求1所述的方法,其特征在于,从提供存储服务的服务器获取加密文件包括:

基于预设通信协议与所述服务器端建立通讯连接;

根据预设的登录账号及密码,登录所述服务器;以及

根据所述服务器中指定的文件夹目录信息及文件类型信息,获取所述加密文件。

3.根据权利要求2所述的方法,其特征在于,所述预设通信协议包括:文件传输协议或安全文件传送协议。

4.根据权利要求1-3任一项所述的方法,其特征在于,所述加密文件为通过优良保密协议进行加密的文件。

5.一种用户通信方式获取方法,其特征在于,包括:

接收客户端发送的与订单信息中关联用户通信的请求,所述订单信息为根据权利要求1-4任一项所述的方法生成;

根据所述订单信息,查询获取所述关联用户虚拟号码的访问接口;以及

通过所述访问接口,获取所述关联用户的虚拟号码。

6.一种包裹面单生成方法,其特征在于,包括:

从提供存储服务的服务器获取加密文件,所述加密文件中包括经加密处理的用户下单信息;

根据预先获取的解密数据对所述加密文件进行解密处理,获得解密后的用户下单信息,其中所述解密数据包括解密密码及解密文件;以及

以字节数组信息流的形式输出解密后的用户下单信息,根据预设的打印文字字段位置,从第一列开始依次放置字段,从而将对应用户下单信息的字节数组输出流解析为包裹面单文本集合对象;

将所述包裹面单文本集合对象转换为物流平台内部下单接口的入参对象,获得下单接口输出的待打印包裹面单。

7.根据权利要求6所述的方法,其特征在于,还包括:

对所述加密文件进行校验,判断所述加密文件是否为通过预设加密算法进行加密的文件;以及

当所述加密文件为通过所述预设加密算法进行加密的文件时,将所述加密文件上传至

所述服务器存储。

8.根据权利要求7所述的方法,其特征在于,还包括:

将所述用户下单信息中的涉及用户隐私的内容使用特殊字符进行替换,并将进行替换处理后的所述用户下单信息存储于预设格式文件中;以及

通过所述预设加密算法对所述预设格式文件进行加密处理,生成所述加密文件。

9.根据权利要求7或8所述的方法,其特征在于,所述预设加密算法为优良保密协议。

10.一种订单信息处理装置,其特征在于,包括:

文件获取模块,用于从提供存储服务的服务器获取加密文件,所述加密文件中包括经加密处理的用户下单信息;

文件解密模块,用于根据预先获取的解密数据对所述加密文件进行解密处理,获得解密后的用户下单信息,其中所述解密数据包括解密密码及解密文件;

解析转换模块,用于以字节数组信息流的形式输出解密后的用户下单信息,根据预设的文本字段位置,从第一列开始依次放置字段,从而将对应用户下单信息的字节数组输出流解析为文本集合对象;将所述文本集合对象转换为物流平台内部下单接口的入参对象,获得下单接口输出的待处理下单信息;以及

订单生成模块,用于根据所述待处理下单信息,生成订单信息。

11.一种用户通信方式获取装置,其特征在于,包括:

请求接收模块,用于接收客户端发送的与订单信息中关联用户通信的请求,所述订单信息为根据权利要求1-4任一项所述的方法生成;

接口查询模块,用于根据所述订单信息,查询获取所述关联用户虚拟号码的访问接口;以及

号码获取模块,用于通过所述访问接口,获取所述关联用户的虚拟号码。

12.一种包裹面单生成装置,其特征在于,包括:

文件获取模块,用于从提供存储服务的服务器获取加密文件,所述加密文件中包括经加密处理的用户下单信息;

文件解密模块,用于根据预先获取的解密数据对所述加密文件进行解密处理,获得解密后的用户下单信息,其中所述解密数据包括解密密码及解密文件;以及

面单生成模块,用于以字节数组信息流的形式输出解密后的用户下单信息,根据预设的打印文字字段位置,从第一列开始依次放置字段,从而将对应用户下单信息的字节数组输出流解析为包裹面单文本集合对象;

将所述包裹面单文本集合对象转换为物流平台内部下单接口的入参对象,获得下单接口输出的待打印包裹面单。

13.一种计算机设备,包括:存储器、处理器及存储在所述存储器中并可在所述处理器中运行的可执行指令,其特征在于,所述处理器执行所述可执行指令时实现如权利要求1-9任一项所述的方法。

14.一种计算机可读存储介质,其上存储有计算机可执行指令,其特征在于,所述可执行指令被处理器执行时实现如权利要求1-9任一项所述的方法。

# 订单信息处理方法及装置、设备及存储介质

## 技术领域

[0001] 本发明涉及信息处理领域，具体而言，涉及一种订单信息处理、用户通信方式获取、包裹面单生成方法及装置、设备及存储介质。

## 背景技术

[0002] 随着当前物流行业的高速发展，越来越多的企业选择和物流公司合作相关业务。企业客户所属行业的类型不同，客户的信息敏感度可能不同，对接的合作方式也可能有所不同。一般地，对于大多数客户来说，都可以通过物流公司发布的标准接口实现对接：通过对接接口，使来自客户的订单信息流入物流公司内部系统。在接口规范中，物流系统接收到按规定字段传入的寄件人信息、下单货物信息等订单信息，进而将所接收的订单信息流转到下游各个生产系统。生产系统在实际生产时，可以通过物流公司预先提供的且被客户捆绑于实际订单的运单号查看该订单的详细信息。

[0003] 然而对于一些特殊企业客户，例如银行客户，一方面其对用户的隐私保护要求较高，在与物流公司合作下单时不愿意将诸如用户姓名、联系方式、家庭住址等隐私信息通过接口传给物流系统，因此通过接口传给物流系统的信息都是部分隐藏的。同时，银行客户也不愿意通过公共网络进行信息传输，而是希望通过专用线路完成整个下单流程。此外，由于用户的隐私信息在整个物流系统对应存储的原始信息中是被隐藏的，目前并没有获取详细信息的方法，因此配送员难以在配送途中联系用户。

[0004] 另一方面，对于通过系统对接实现下单的场景，包裹面单的打印需要在银行客户侧完成，这一点并不适合通常情况下的揽收场景，因此在现场操作时将运单号与货物一一对应存在很大的难度。

[0005] 在所述背景技术部分公开的上述信息仅用于加强对本发明的背景的理解，因此它可以包括不构成对本领域普通技术人员已知的现有技术的信息。

## 发明内容

[0006] 有鉴于此，本发明提供一种订单信息处理、用户通信方式获取、包裹面单生成方法及装置、设备及存储介质。

[0007] 本发明的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本发明的实践而习得。

[0008] 根据本发明的一方面，提供一种订单信息处理方法，包括：从提供存储服务的服务器获取加密文件，所述加密文件中包括经加密处理的用户下单信息；根据预先获取的解密数据对所述加密文件进行解密处理，获得解密后的用户下单信息，其中所述解密数据包括解密密码及解密文件；对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息；根据所述待处理下单信息，生成订单信息。

[0009] 根据本发明的一实施方式，从提供存储服务的服务器获取加密文件包括：基于预设通信协议与所述服务器端建立通讯连接；根据预设的登录账号及密码，登录所述服务器；

以及根据所述服务器中指定的文件夹目录信息及文件类型信息，获取所述加密文件。

[0010] 根据本发明的一实施方式，所述预设通信协议包括：文件传输协议或安全文件传送协议。

[0011] 根据本发明的一实施方式，对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息包括：根据预设的文本字段位置，将所述解密后的用户下单信息解析为文本集合对象；以及对所述文本集合对象进行转换，获得所述待处理下单信息。

[0012] 根据本发明的一实施方式，所述加密文件为通过优良保密协议进行加密的文件。

[0013] 根据本发明的另一方面，提供一种用户通信方式获取方法，包括：接收客户端发送的与订单信息中关联用户通信的请求，所述订单信息为根据上述任一项订单信息处理方法生成；根据所述订单信息，查询获取所述关联用户虚拟号码的访问接口；以及通过所述访问接口，获取所述关联用户的虚拟号码。

[0014] 根据本发明的再一方面，提供一种包裹面单生成方法，包括：从提供存储服务的服务器获取加密文件，所述加密文件中包括经加密处理的用户下单信息；根据预先获取的解密数据对所述加密文件进行解密处理，获得解密后的用户下单信息，其中所述解密数据包括解密密码及解密文件；以及对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单。

[0015] 根据本发明的一实施方式，所述方法还包括：对所述加密文件进行校验，判断所述加密文件是否为通过预设加密算法进行加密的文件；以及当所述加密文件为通过所述预设加密算法进行加密的文件时，将所述加密文件上传至所述服务器存储。

[0016] 根据本发明的一实施方式，所述方法还包括：将所述用户下单信息中的涉及用户隐私的内容使用特殊字符进行替换，并将进行替换处理后的所述用户下单信息存储于预设格式文件中；以及通过所述预设加密算法对所述预设格式文件进行加密处理，生成所述加密文件。

[0017] 根据本发明的一实施方式，所述预设加密算法为优良保密协议。

[0018] 根据本发明的一实施方式，对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单包括：根据预设的打印文字字段位置，将所述解密后的用户下单信息解析为所述待打印包裹面单。

[0019] 根据本发明的再一方面，提供一种订单信息处理装置，包括：文件获取模块，用于从提供存储服务的服务器获取加密文件，所述加密文件中包括经加密处理的用户下单信息；文件解密模块，用于根据预先获取的解密数据对所述加密文件进行解密处理，获得解密后的用户下单信息，其中所述解密数据包括解密密码及解密文件；解析转换模块，用于对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息；以及订单生成模块，用于根据所述待处理下单信息，生成订单信息。

[0020] 根据本发明的再一方面，提供一种用户通信方式获取装置，包括：请求接收模块，用于接收客户端发送的与订单信息中关联用户通信的请求，所述订单信息为根据上述任一种订单信息处理方法生成；接口查询模块，用于根据所述订单信息，查询获取所述关联用户虚拟号码的访问接口；以及号码获取模块，用于通过所述访问接口，获取所述关联用户的虚拟号码。

[0021] 根据本发明的再一方面，提供一种包裹面单生成装置，包括：文件获取模块，用于

从提供存储服务的服务器获取加密文件，所述加密文件中包括经加密处理的用户下单信息；文件解密模块，用于根据预先获取的解密数据对所述加密文件进行解密处理，获得解密后的用户下单信息，其中所述解密数据包括解密密码及解密文件；以及面单生成模块，用于对所述解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单。

[0022] 根据本发明的再一方面，提供一种计算机设备，包括：存储器、处理器及存储在所述存储器中并可在所述处理器中运行的可执行指令，所述处理器执行所述可执行指令时实现上述任一种方法。

[0023] 根据本发明的再一方面，提供一种计算机可读存储介质，其上存储有计算机可执行指令，所述可执行指令被处理器执行时实现上述任一种方法。

[0024] 根据本发明实施方式提供的订单信息处理方法，为实现整个下单流程搭建了一条“专用线路”，能够从提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式订单，有效地避免了物流方与下单方通过公共网络传输信息可能导致的用户隐私泄露。

[0025] 根据本发明实施方式提供的用户通信方式获取方法，能够根据订单信息，调用相应的访问接口以获取用户的虚拟号码，而不曝光用户的实际号码，有效地保护了用户隐私在订单的整个生命周期内不被泄露到任何外部系统中。

[0026] 根据本发明实施方式提供的包裹面单生成方法，能够从提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式的待打印面单，有效地避免了下单方与物流方通过公共网络传输信息可能导致的用户隐私泄露，同时便捷、可靠地保证了在后续配送过程中货物与运单号一一对应。

[0027] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性的，并不能限制本发明。

## 附图说明

[0028] 通过参照附图详细描述其示例实施例，本发明的上述和其它目标、特征及优点将变得更加显而易见。

[0029] 图1是根据一示例性实施方式示出的一种订单信息处理方法的流程图。

[0030] 图2是根据一示例性实施方式示出的另一种订单信息处理方法的流程图。

[0031] 图3是根据一示例性实施方式示出的再一种订单信息处理方法的流程图。

[0032] 图4是根据一示例性实施方式示出的一种用户通信方式获取方法的流程图。

[0033] 图5是根据一示例性实施方式示出的一种包裹面单生成方法的流程图。

[0034] 图6是根据一示例性实施方式示出的另一种包裹面单生成方法的流程图。

[0035] 图7是根据一示例性实施方式示出的再一种包裹面单生成方法的流程图。

[0036] 图8是根据一示例性实施方式示出的一种订单信息处理装置的框图。

[0037] 图9是根据一示例性实施方式示出的一种用户通信方式获取装置的框图。

[0038] 图10是根据一示例性实施方式示出的一种包裹面单生成装置的框图。

[0039] 图11是根据一示例性实施方式示出的一种计算机设备的结构示意图。

## 具体实施方式

[0040] 现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本发明将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。附图仅为本发明的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。

[0041] 此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施方式中。在下面的描述中，提供许多具体细节从而给出对本发明的实施方式的充分理解。然而，本领域技术人员将意识到，可以实践本发明的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、装置、步骤等。在其它情况下，不详细示出或描述公知结构、方法、装置、实现或者操作以避免喧宾夺主而使得本发明的各方面变得模糊。

[0042] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0043] 如上所述，对于像银行等特殊客户，一方面其对用户的隐私保护要求较高，在与物流公司合作下单时不愿意将诸如用户姓名、联系方式、家庭住址等隐私信息通过接口传给物流系统，同时也不愿意通过公共网络进行信息传输，而是希望通过专用线路完成整个下单流程。此外，由于用户的隐私信息在整个物流系统对应存储的原始信息中是被隐藏的，目前并没有获取详细信息的方法，因此配送员难以在配送途中联系用户；另一方面，对于通过系统对接实现下单的场景，包裹面单的打印需要在银行客户侧完成，这一点并不适合通常情况下的揽收场景，因此在现场操作时将运单号与货物一一对应存在很大的难度。

[0044] 因此，本发明本发明提供了一种订单信息处理方法和一种包裹面单生成方法，为实现整个下单流程搭建了一条“专用线路”，下单方和物流方均能够从同一个提供存储服务的服务器获取到相同的经加密处理的用户下单信息，并分别对其解密以安全、高效地生成统一格式的订单和待打印面单，有效地避免了双方通过公共网络传输信息可能导致的用户隐私泄露，同时便捷、可靠地保证了在后续配送过程中货物与运单号一一对应。更优地，根据本发明实施方式提供的用户通信方式获取方法，还能够根据订单信息调用相应的访问接口以获取用户的虚拟号码，而不曝光用户的实际号码，有效地保护了用户隐私在订单的整个生命周期内不被泄露到任何外部系统中。

[0045] 图1是根据一示例性实施方式示出的一种订单信息处理方法的流程图。如图1所示的订单信息处理方法例如可以应用于物流平台的服务器端。

[0046] 参考图1，订单信息处理方法10包括：

[0047] 在步骤S102中，从提供存储服务的服务器获取加密文件。

[0048] 其中，加密文件中包括经加密处理的用户下单信息。

[0049] 该提供存储服务的服务器例如可以由上述的商家客户提供，并授权给物流公司可以登录的用户名和密码等信息。

[0050] 在一些实施例中，加密文件可以是通过优良保密协议(PGP，Pretty Good Privacy)进行加密的文件。PGP协议由一系列散列、数据压缩、对称密钥加密以及公钥加密

的算法组合而成。由于PGP协议支持多种算法，在具体的文件解密过程中可以选择使用任意一种算法，本发明不以此为限。

[0051] 在步骤S104中，根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息。

[0052] 其中，解密数据包括解密密码及解密文件(如解密私钥)。

[0053] 如上述，物流平台服务器端可以以输入文件流的方式持续获取批量PGP加密文件。在对输入文件流进行解密操作后，服务器端也可以以信息流的方式输出解密得到的用户下单信息，输出的信息流可以是对应用户下单信息的字节数组输出流。物流平台服务器端预先获取的解密数据可以是针对所有加密文件预先配置的固定解密数据，例如在一段业务周期内，物流平台服务器端可以通过同一个解密密码和同一个解密文件对输入文件流搭载的所有PGP加密文件进行解密处理，而无需切换解密数据。其中，解密文件例如可以是扩展名为.asc的解密私钥文件，物流平台服务器端例如可以基于Java Bouncy Castle加密组件下的PGPUtil工具类进行PGP文件的解密，但本发明并不以此为限。

[0054] 在步骤S106中，对解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息。

[0055] 根据预定的统一格式，将解密后的用户下单信息解析并转换为适用于物流平台系统的待处理下单信息。

[0056] 在步骤S108中，根据待处理下单信息，生成订单信息。

[0057] 对待处理下单信息进行处理，生成可在物流平台系统内部流转的订单信息。

[0058] 根据本发明实施方式提供的订单信息处理方法，为实现整个下单流程搭建了一条“专用线路”，能够从提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式订单，有效地避免了物流方与下单方通过公共网络传输信息可能导致的用户隐私泄露。

[0059] 应清楚地理解，本发明描述了如何形成和使用特定示例，但本发明的原理不限于这些示例的任何细节。相反，基于本发明公开的内容的教导，这些原理能够应用于许多其它实施方式。

[0060] 图2是根据一示例性实施方式示出的另一种订单信息处理方法的流程图。与图1所示方法10的不同之处在于，图2所示的方法20进一步提供了从提供存储服务的服务器获取加密文件的方法，即进一步提供了上述方法10中步骤S102的一实施例。同样地，如图2所示的订单信息处理方法例如也可以应用于物流平台的服务器端。

[0061] 参考图2，方法10中的步骤S102还包括：

[0062] 在步骤S202中，基于预设通信协议与服务器端建立通讯连接。

[0063] 在一些实施例中，预设通信协议可以是文件传输协议(FTP，File Transfer Protocol)或安全文件传送协议(SFTP，Secure File Transfer Protocol)。

[0064] 在步骤S204中，根据预设的登录账号及密码，登录服务器。

[0065] 以支持FTP协议的服务器(以下简称“FTP服务器”)为例，用户通过一个支持FTP协议的客户机程序连接到在远程主机上的FTP服务器程序。需要物流运输业务的企业客户，例如银行客户将包括经加密处理的用户下单信息的PGP加密文件上传并存储至FTP服务器之后，授权给物流平台用于登录FTP服务器的专属登录账户和密码。物流平台服务器端根据授

权的账号及密码信息连接到预配置的FTP服务器地址,实现登录FTP服务器。

[0066] 在步骤S206中,根据服务器中指定的文件夹目录信息及文件类型信息,获取加密文件。

[0067] 承上述,仍以FTP服务器为例进行说明:与大多数Internet服务一样,用户可以通过客户机程序向服务器程序发出请求,服务器程序执行用户所发出的请求,并将执行的结果返回到客户机。例如,物流平台服务器端连接并登录FTP服务器后,请求FTP服务器根据文件夹目录信息及文件类型信息传回指定的加密文件或其拷贝份;FTP服务器响应该请求,将物流平台指定的加密文件传送至物流平台服务器端。物流平台服务器端的客户机程序代表物流平台接收并存储指定加密文件。例如,通过一种开源规则引擎的FTP组件实现登录FTP服务器,并在指定的文件夹下获取匹配加密文件的代码示例如下。代码中的Apache Camel是一种基于规则路由和中介引擎,提供企业集成模式的Java对象实现,通过应用程序接口或陈述式Java领域特定语言(DSL,Domain-Specific Languages)配置路由和中介的规则;Apache Camel中的“endpoint”代表某个资源的位置,类似于web应用程序中的端点:

[0068] <camel:endpoint id＝"CEBFrom"

[0069] uri＝"${CEB.camel.ftp.protocol}:${CEB.camel.ftp.username}@${CEB.camel.ftp.hostName}:${CEB.camel.ftp.port}/${CEB.camel.ftp.directoryName}?password＝${CEB.camel.ftp.password}&delete＝${CEB.camel.ftp.delete}&include＝.*.xls.pgp"/>

[0070] 其中:

[0071] CEB.camel.ftp.protocol用于指定通信协议为FTP;

[0072] CEB.camel.ftp.hostName用于指定登录FTP服务器的地址;

[0073] CEB.camel.ftp.port用于指定登录FTP服务器的端口;

[0074] CEB.camel.ftp.username用于指定登录账号的用户名;

[0075] CEB.camel.ftp.password用于指定登录账号的密码;

[0076] CEB.camel.ftp.directoryName用于指定获取文件的文件夹目录;

[0077] include＝.*.xls.pgp用于指定获取的文件类型,如PGP加密文件。

[0078] 在配置完成上述用于获取加密文件的前提配置端点endpoint后,配置加密文件的路由Route示例如下,该配置用于指定后续由哪个具体的业务实现类处理获取到的加密文件:

```
< route id="CEBRoute" >
    < from ref="CEBFrom"/ >
[0079]  < !--业务逻辑处理类-- >
    < process ref="CEBProcessor"/ >
< /route >
```

[0080] 在一些实施例中,物流平台服务器端还可以通过其它预设通信协议例如HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer,超文本传输安全协议),向支持相应协议的服务器端发送获取加密文件的请求。

[0081] 图3是根据一示例性实施方式示出的再一种订单信息处理方法的流程图。与图1所示方法10的不同之处在于，图3所示的方法30进一步提供了对解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息方法，即进一步提供了上述方法10中步骤S106的一实施例。同样地，如图3所示的订单信息处理方法例如也可以应用于物流平台的服务器端。

[0082] 参考图3，方法10中的步骤S106还包括：

[0083] 在步骤S302中，根据预设的文本字段位置，将解密后的用户下单信息解析为文本集合对象。

[0084] 如上所述，物流平台服务器端基于步骤S104可以以字节数组信息流的形式输出解密后的用户下单信息。物流平台服务器端进而可以根据预设的文本字段位置，例如从第一列开始依次放置字段：运单号、收件人姓名、收件人联系方式、收件人地址、订单号等，其中运单号可以是物流平台事先提供给企业客户的批量运单号，从而将对应用户下单信息的字节数组输出流解析为文本集合对象。在一些实施例中，文本集合对象可以是List集合对象。List集合对象包括JavaList接口以及List接口的所有实现类，其中各元素的排列顺序即是对象执行插入的顺序，且允许同一元素重复出现。类似于Java语言中的数组，物流平台服务器端可通过索引元素在List集合对象中的位置来访问各元素。

[0085] 在步骤S304中，对文本集合对象进行转换，获得待处理下单信息。

[0086] 承上述，物流平台服务器端可对List集合对象进行进一步解析，将List集合对象转换为物流平台内部下单接口的入参对象，从而获得下单接口输出的待处理下单信息。根据待处理下单信息，在步骤S108中，物流平台服务器端可调用内部接口生成最终的可推送订单信息。

[0087] 图4是根据一示例性实施方式示出的一种用户通信方式获取方法的流程图。如图4所示的用户通信方式获取方法例如也可以应用于物流平台的服务器端。

[0088] 参考图4，用户通信方式获取方法40包括：

[0089] 在步骤S402中，接收客户端发送的与订单信息中关联用户通信的请求。

[0090] 其中，订单信息为根据上述任一种订单信息处理方法所生成，因此关联用户即为经加密处理的用户下单信息所对应的用户。

[0091] 在步骤S404中，根据订单信息，查询获取关联用户虚拟号码的访问接口。

[0092] 在物流配送场景中，配送员如果想要联系收件用户，可以通过手持式终端设备例如POS一体机提供的一键拨号按钮，向物流平台服务器端发送与订单信息中关联用户通信的请求。在一些实施例中，运单信息可以是预存于POS一体机中的，也可以是POS一体机通过扫描包裹面单获得的，本发明不以此为限。物流平台服务器端接收到POS一体机发送的通信请求后，调用平台内部访问接口根据运单信息中的企业客户信息，通过预先配置查找到对应企业客户提供的用于获取收件用户虚拟号码的外部访问接口。

[0093] 在步骤S406中，通过访问接口，获取关联用户的虚拟号码。

[0094] 承上述，物流平台服务器端获取到外部访问接口后，即可与企业客户交互信息以获得收件用户的虚拟号码。物流平台服务器端获得用户虚拟号码的方式有多种，例如可通过企业客户提供的支持HTTPS协议或者其它任何协议的外部访问接口进行获取。POS一体机继而可根据访问接口返回的虚拟号码，通过一键拨号功能直接与收件用户进行手机通信。

[0095] 根据本发明实施方式提供的用户通信方式获取方法，能够根据订单信息，调用相应的访问接口以获取用户的虚拟号码，而不曝光用户的实际号码，有效地保护了用户隐私在订单的整个生命周期内不被泄露到任何外部系统中。

[0096] 图5是根据一示例性实施方式示出的一种包裹面单生成方法的流程图。如图5所示的包裹面单生成方法例如可以应用于企业客户的服务器端。

[0097] 参考图5，包裹面单生成方法50包括：

[0098] 在步骤S502中，从提供存储服务的服务器获取加密文件。

[0099] 其中，加密文件中包括经加密处理的用户下单信息。

[0100] 在步骤S504中，根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息。

[0101] 其中，解密数据包括解密密码及解密文件。

[0102] 在步骤S506中，对解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单。

[0103] 在一些实施例中，对解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单包括：根据预设的打印文字字段位置，将解密后的用户下单信息解析为待打印包裹面单。

[0104] 与物流平台服务器端以信息流的方式输出解密后的用户下单信息相类似，企业客户服务器端也可以信息流的方式输出解密后的用户下单信息，进而根据预设的文本字段位置将之解析为待打印的包裹面单文本集合对象，并将包裹面单文本集合对象转换为统一格式的待打印包裹面单，其中对待打印字段属性的解析和转换需按照预先约定的顺序进行。

[0105] 在后续的物流揽收场景中，企业客户服务器端例如可以通过物流平台服务器端提供的离线版打印软件，调用内部打印接口以连接打印机设备，在企业客户侧完成待打印包裹面单的统一打印。企业客户将打印好的包裹面单一一对应贴附于实际的包裹上，等待物流公司上门揽收。

[0106] 需要说明的是，下单方生成包裹面单所使用的源文件和物流方生成订单信息所使用的源文件是同一份文件，也就是下单方事先上传并存储至提供存储服务的服务器中的加密文件，因此步骤S502及S504获取及解密文件的过程与步骤S102及S104对应相同，在此不予赘述。

[0107] 根据本发明实施方式提供的包裹面单生成方法，能够从提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式的待打印面单，有效地避免了下单方与物流方通过公共网络传输信息可能导致的用户隐私泄露，同时便捷、可靠地保证了在后续配送过程中货物与运单号一一对应。

[0108] 应清楚地理解，本发明描述了如何形成和使用特定示例，但本发明的原理不限于这些示例的任何细节。相反，基于本发明公开的内容的教导，这些原理能够应用于许多其它实施方式。

[0109] 图6是根据一示例性实施方式示出的另一种包裹面单生成方法的流程图。与图5所示方法50的不同之处在于，图6所示的方法60进一步提供了上传并存储加密文件的方法，即进一步提供了上述方法50的一实施例。同样地，如图6所示的包裹面单生成方法例如也可以应用于企业客户的服务器端。

[0110] 参考图6,方法50还包括:

[0111] 在步骤S602中,对加密文件进行校验,判断加密文件是否为通过预设加密算法进行加密的文件。

[0112] 在一些实施例中,预设加密算法可以是优良保密协议PGP,本发明并不以此算法为限。

[0113] 在步骤S604中,当加密文件为通过预设加密算法进行加密的文件时,将加密文件上传至服务器存储。

[0114] 如上述,下单方和物流方所有的操作都是基于下单方事先上传至提供存储服务的服务器的同一份加密文件,因此需要在下单方上传文件的同时校验所上传文件的合法性,即判断上传文件是否是通过预设加密算法进行加密的文件,如PGP加密文件。只有当文件通过校验,企业客户服务器端才向提供存储服务的服务器上传该文件,并允许在后续执行文件的解密、解析等操作。

[0115] 图7是根据一示例性实施方式示出的再一种包裹面单生成方法的流程图。与图6所示方法60的不同之处在于,图7所示的方法70进一步提供了生成加密文件的方法,即进一步提供了上述方法60的一实施例。同样地,如图7所示的包裹面单生成方法例如也可以应用于企业客户的服务器端。

[0116] 参考图7,方法60还包括:

[0117] 在步骤S702中,将用户下单信息中的涉及用户隐私的内容使用特殊字符进行替换,并将进行替换处理后的用户下单信息存储于预设格式文件中。

[0118] 如上述,为了保证旗下用户的原始数据在订单的整个生命周期内不被泄露到任何外部系统中,企业客户将需要下单的部分数据进行隐藏,例如可使用由“*”或“#”等特殊符号形成的字符串替换诸如用户姓名、联系方式、家庭住址等隐私信息,并将替换后的用户下单信息存储于预设格式文件中。在一些实施例中,企业客户服务器端可将替换后的用户下单信息存入Excel表格文件或者txt文本文件,本发明并不限定用户下单信息的载体文件格式。

[0119] 在步骤S704中,通过预设加密算法对预设格式文件进行加密处理,生成加密文件。

[0120] 在一些实施例中,预设加密算法可以是优良保密协议PGP,企业客户服务器端通过PGP算法对用户下单信息的载体文件进行加密处理,对应生成PGP加密文件。

[0121] 本领域技术人员可以理解实现上述实施方式的全部或部分步骤被实现为由CPU执行的计算机程序。在该计算机程序被CPU执行时,执行本发明提供的上述方法所限定的上述功能。所述的程序可以存储于一种计算机可读存储介质中,该存储介质可以是只读存储器,磁盘或光盘等。

[0122] 此外,需要注意的是,上述附图仅是根据本发明示例性实施方式的方法所包括的处理的示意性说明,而不是限制目的。易于理解,上述附图所示的处理并不表明或限制这些处理的时间顺序。另外,也易于理解,这些处理可以是例如在多个模块中同步或异步执行的。

[0123] 下述为本发明装置实施例,可以用于执行本发明方法实施例。对于本发明装置实施例中未披露的细节,请参照本发明方法实施例。

[0124] 图8是根据一示例性实施方式示出的一种订单信息处理装置的框图。

[0125] 参考图8，订单信息处理装置80包括：文件获取模块802、文件解密模块804、解析转换模块806以及订单生成模块808。

[0126] 其中，文件获取模块802用于从提供存储服务的服务器获取加密文件。

[0127] 其中加密文件中包括经加密处理的用户下单信息。

[0128] 在一些实施例中，文件获取模块802可进一步包括：建立通讯单元、登录中继单元以及获取文件单元。其中，建立通讯单元用于基于预设通信协议与服务器端建立通讯连接；登录中继单元用于根据预设的登录账号及密码，登录服务器；获取文件单元用于根据服务器中指定的文件夹目录信息及文件类型信息，获取加密文件。

[0129] 文件解密模块804用于根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息。

[0130] 其中解密数据包括解密密码及解密文件。

[0131] 解析转换模块806用于对解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息。

[0132] 在一些实施例中，解析转换模块806可进一步包括：解析信息单元以及对象转换单元。其中，解析信息单元用于根据预设的文本字段位置，将解密后的用户下单信息解析为文本集合对象；对象转换单元用于对文本集合对象进行转换，获得待处理下单信息。

[0133] 订单生成模块808用于根据待处理下单信息，生成订单信息。

[0134] 根据本发明实施方式提供的订单信息处理装置，为实现整个下单流程搭建了一条“专用线路”，能够通过提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式订单，有效地避免了物流方与下单方通过公共网络传输信息可能导致的用户隐私泄露。

[0135] 图9是根据一示例性实施方式示出的一种用户通信方式获取装置的框图。

[0136] 参考图9，用户通信方式获取装置90包括：请求接收模块910、接口查询模块912以及号码获取模块914。

[0137] 其中，请求接收模块910用于接收客户端发送的与订单信息中关联用户通信的请求。

[0138] 其中订单信息为根据上述任一种订单信息处理方法所生成。

[0139] 接口查询模块912用于根据订单信息，查询获取关联用户虚拟号码的访问接口。

[0140] 号码获取模块914用于通过访问接口，获取关联用户的虚拟号码。

[0141] 根据本发明实施方式提供的用户通信方式获取装置，能够根据订单信息，调用相应的访问接口以获取用户的虚拟号码，而不曝光用户的实际号码，有效地保护了用户隐私在订单的整个生命周期内不被泄露到任何外部系统中。

[0142] 图10是根据一示例性实施方式示出的一种包裹面单生成装置的框图。

[0143] 参考图10，包裹面单生成装置100包括：文件获取模块1010、文件解密模块1012以及面单生成模块1014。

[0144] 其中，文件获取模块1010用于从提供存储服务的服务器获取加密文件，加密文件中包括经加密处理的用户下单信息。

[0145] 文件解密模块1012用于根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息。

[0146] 其中解密数据包括解密密码及解密文件。

[0147] 面单生成模块1014用于对解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单。

[0148] 在一些实施例中，面单生成模块1014可进一步包括：解析信息单元。解析信息单元用于根据预设的打印文字字段位置，将解密后的用户下单信息解析为待打印包裹面单。

[0149] 在一些实施例中，参考图10，包裹面单生成装置100还可包括：文件校验模块1006以及文件上传模块1008。

[0150] 其中，文件校验模块1006用于对加密文件进行校验，判断加密文件是否为通过预设加密算法进行加密的文件。

[0151] 文件上传模块1008用于当加密文件为通过预设加密算法进行加密的文件时，将加密文件上传至服务器存储。

[0152] 在一些实施例中，继续参考图10，包裹面单生成装置100还可包括：信息替换模块1002以及文件生成模块1004。

[0153] 其中，信息替换模块1002用于将用户下单信息中的涉及用户隐私的内容使用特殊字符进行替换，并将进行替换处理后的用户下单信息存储于预设格式文件中。

[0154] 文件生成模块1004用于通过预设加密算法对预设格式文件进行加密处理，生成加密文件。

[0155] 根据本发明实施方式提供的包裹面单生成装置，能够通过提供存储服务的服务器获取到经加密处理的用户下单信息，并对其解密以安全、高效地生成统一格式的待打印面单，有效地避免了下单方与物流方通过公共网络传输信息可能导致的用户隐私泄露，同时便捷、可靠地保证了在后续配送过程中货物与运单号一一对应。

[0156] 需要注意的是，上述附图中所示的框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0157] 图11是根据一示例性实施方式示出的一种计算机设备的结构示意图。需要说明的是，图11示出的计算机设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0158] 如图11所示，计算机设备2000包括中央处理单元(CPU)2001，其可以根据存储在只读存储器(ROM)2002中的程序或者从存储部分2008加载到随机访问存储器(RAM)2003中的程序而执行各种适当的动作和处理。在RAM 2003中，还存储有设备2000操作所需的各种程序和数据。CPU 2001、ROM 2002以及RAM 2003通过总线2004彼此相连。输入/输出(I/O)接口1005也连接至总线2004。

[0159] 以下部件连接至I/O接口2005：包括键盘、鼠标等的输入部分2006；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分2007；包括硬盘等的存储部分2008；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分2009。通信部分2009经由诸如因特网的网络执行通信处理。驱动器2010也根据需要连接至I/O接口2005。可拆卸介质2011，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器2010上，以便于从其上读出的计算机程序根据需要被安装入存储部分2008。

[0160] 特别地，根据本发明的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本发明的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分2009从网络上被下载和安装，和/或从可拆卸介质2011被安装。在该计算机程序被中央处理单元(CPU)2001执行时，执行本发明的设备中限定的上述功能。

[0161] 需要说明的是，本发明所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本发明中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本发明中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0162] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0163] 描述于本发明实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中，例如，可以描述为：一种处理器包括发送单元、获取单元、确定单元和第一处理单元。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定，例如，发送单元还可以被描述为“向所连接的服务端发送图片获取请求的单元”。

[0164] 作为另一方面，本发明还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的设备中所包含的；也可以是单独存在，而未装配入该设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该设备执行时，使得该设备包括：

[0165] 从提供存储服务的服务器获取加密文件，加密文件中包括经加密处理的用户下单信息；根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息，其中解密数据包括解密密码及解密文件；对解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息；根据待处理下单信息，生成订单信息；

[0166] 接收客户端发送的与订单信息中关联用户通信的请求，订单信息为根据上述任一种方法生成；根据订单信息，查询获取关联用户虚拟号码的访问接口；通过访问接口，获取关联用户的虚拟号码；以及，

[0167] 从提供存储服务的服务器获取加密文件，加密文件中包括经加密处理的用户下单信息；根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息，其中解密数据包括解密密码及解密文件；对解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单。

[0168] 以上具体地示出和描述了本发明的示例性实施方式。应可理解的是，本发明不限于这里描述的详细结构、设置方式或实现方法；相反，本发明意图涵盖包含在所附权利要求的精神和范围内的各种修改和等效设置。

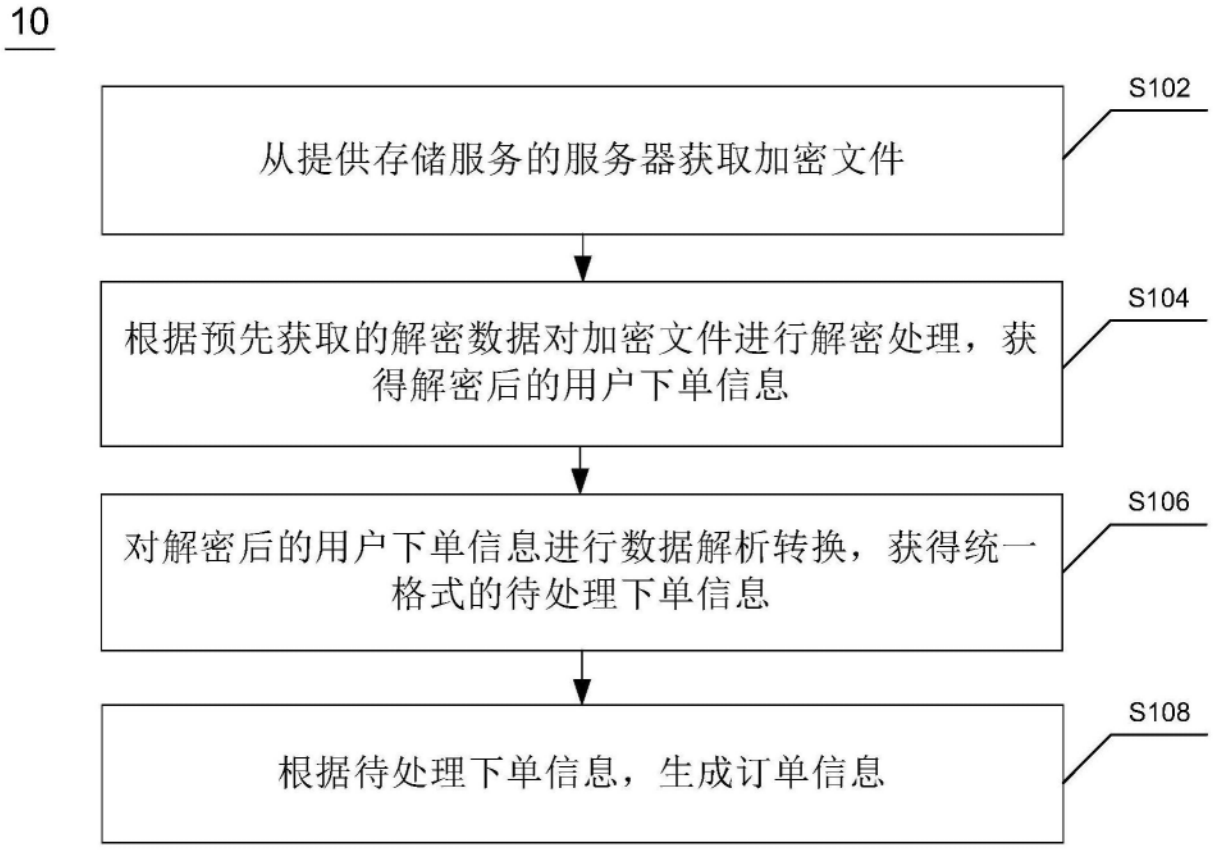

10
S102
从提供存储服务的服务器获取加密文件
S104
根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息
S106
对解密后的用户下单信息进行数据解析转换，获得统一格式的待处理下单信息
S108
根据待处理下单信息，生成订单信息

图1

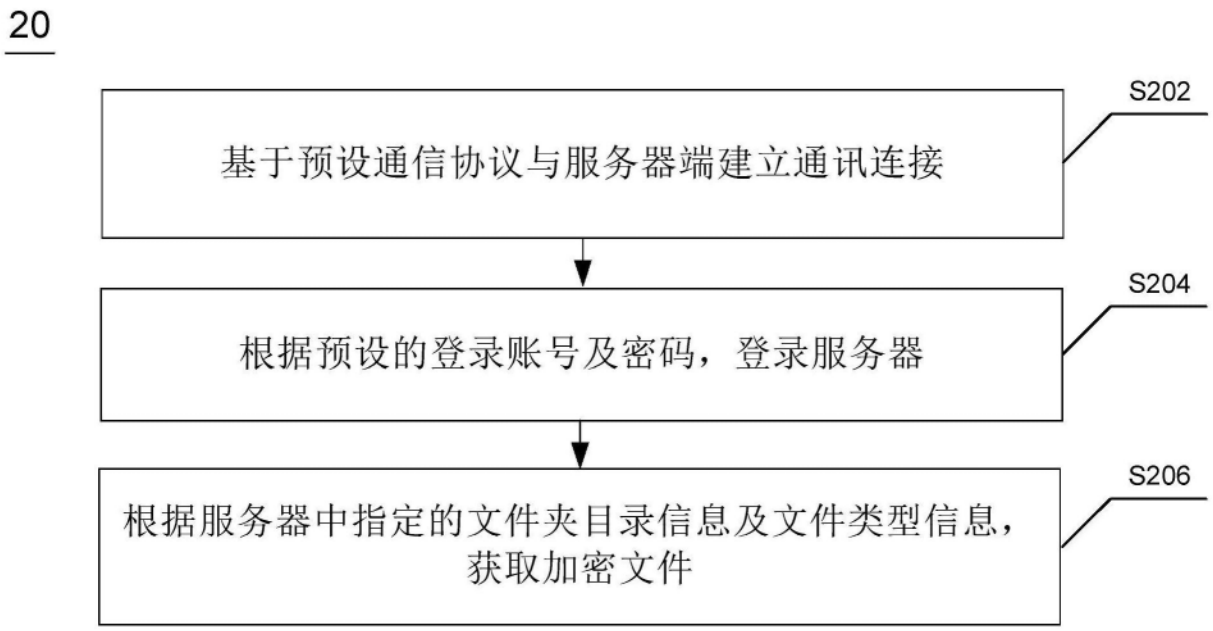

20
S202
基于预设通信协议与服务器端建立通讯连接
S204
根据预设的登录账号及密码，登录服务器
S206
根据服务器中指定的文件夹目录信息及文件类型信息，获取加密文件

图2

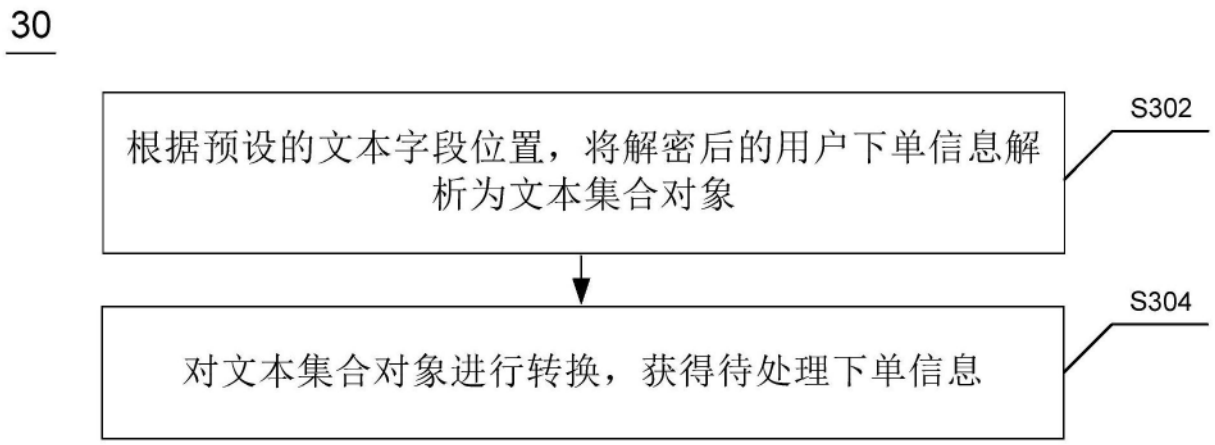

30
根据预设的文本字段位置，将解密后的用户下单信息解析为文本集合对象
S302
对文本集合对象进行转换，获得待处理下单信息
S304

图3

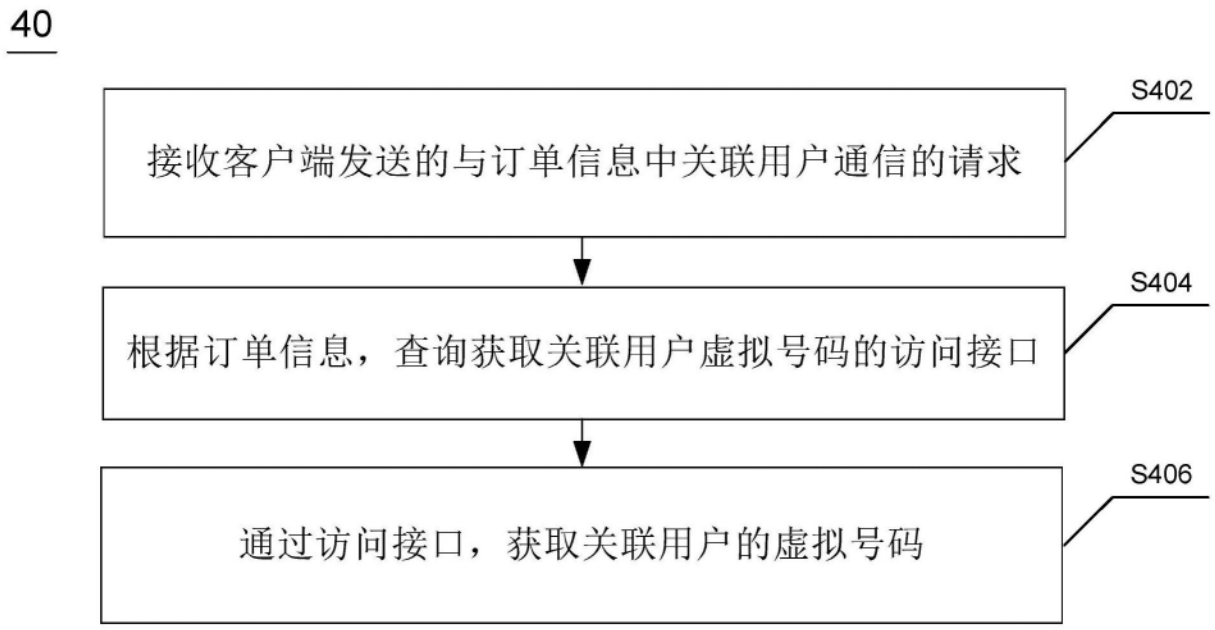

40
接收客户端发送的与订单信息中关联用户通信的请求
S402
根据订单信息，查询获取关联用户虚拟号码的访问接口
S404
通过访问接口，获取关联用户的虚拟号码
S406

图4

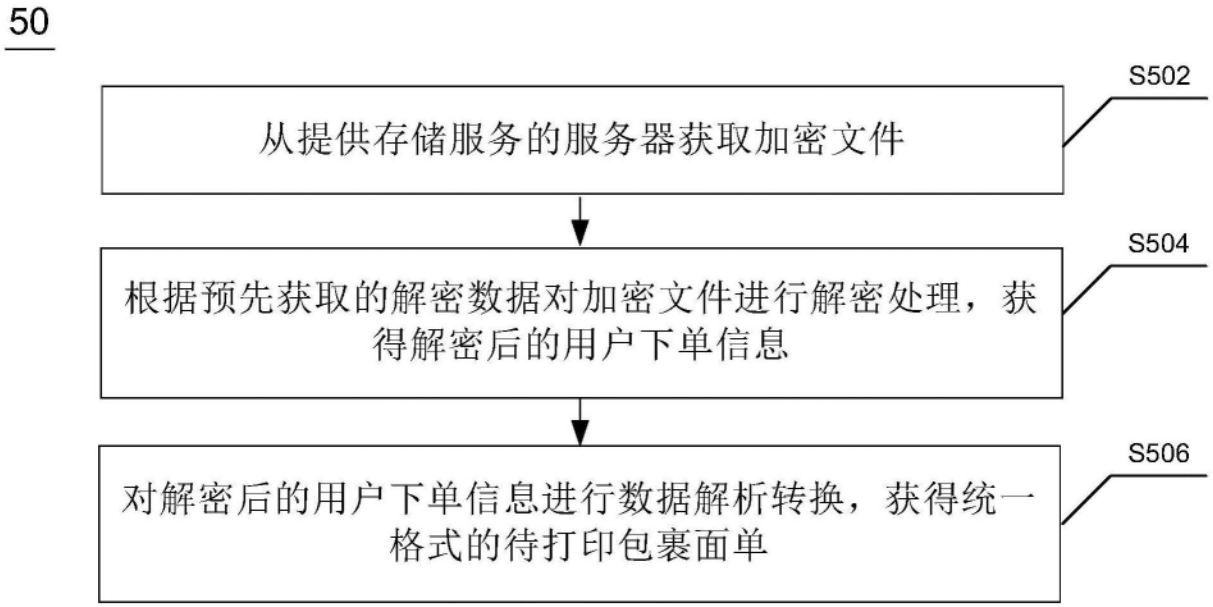

50
S502
从提供存储服务的服务器获取加密文件
S504
根据预先获取的解密数据对加密文件进行解密处理，获得解密后的用户下单信息
S506
对解密后的用户下单信息进行数据解析转换，获得统一格式的待打印包裹面单

图5

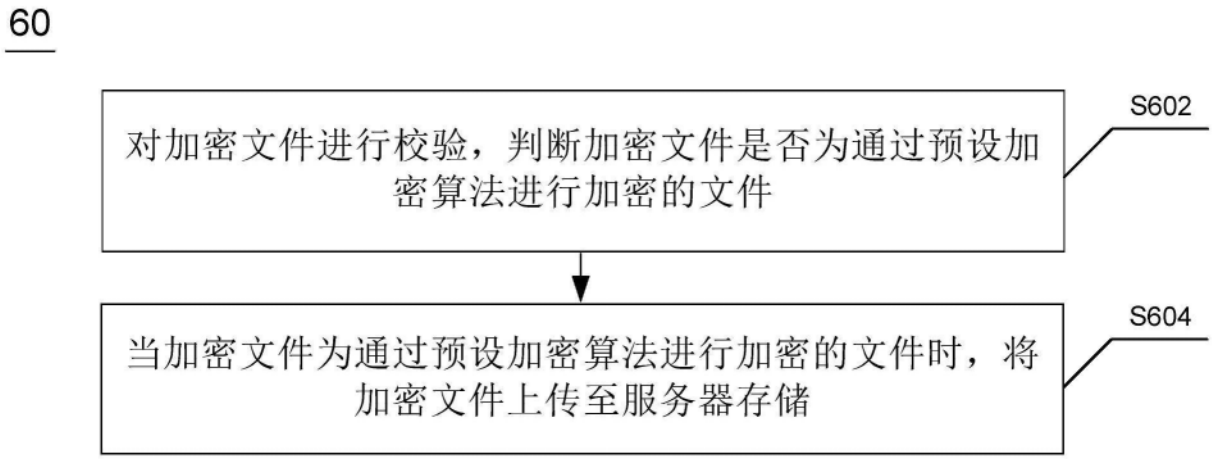

60
S602
对加密文件进行校验，判断加密文件是否为通过预设加密算法进行加密的文件
S604
当加密文件为通过预设加密算法进行加密的文件时，将加密文件上传至服务器存储

图6

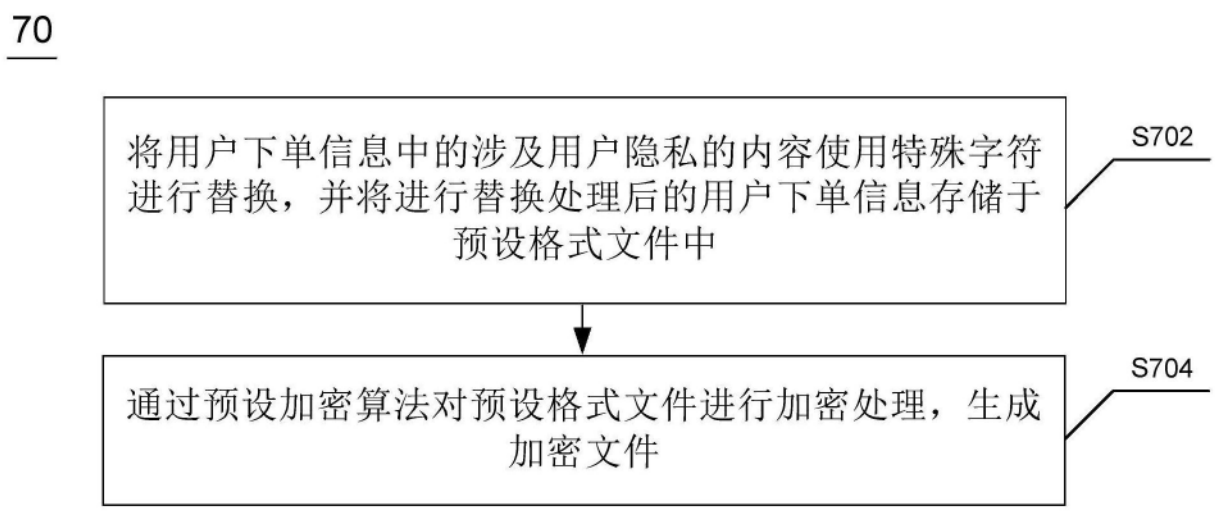

70
将用户下单信息中的涉及用户隐私的内容使用特殊字符进行替换，并将进行替换处理后的用户下单信息存储于预设格式文件中
S702
通过预设加密算法对预设格式文件进行加密处理，生成加密文件
S704

图7

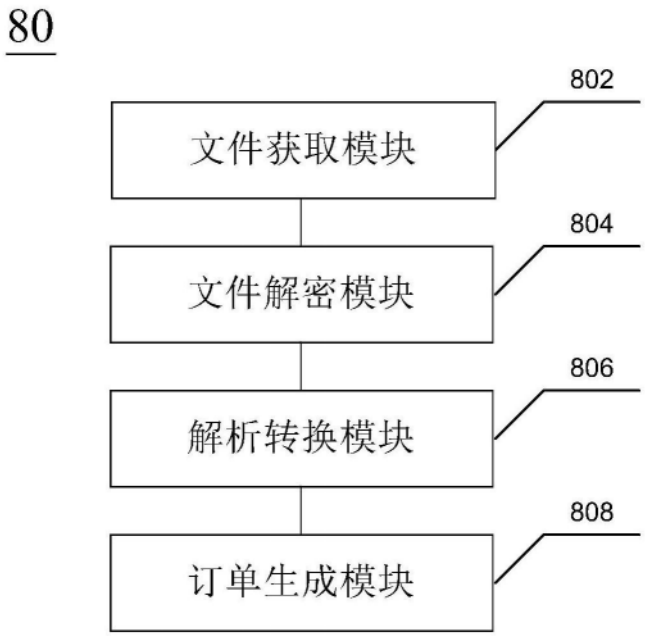

80
文件获取模块
802
文件解密模块
804
解析转换模块
806
订单生成模块
808

图8

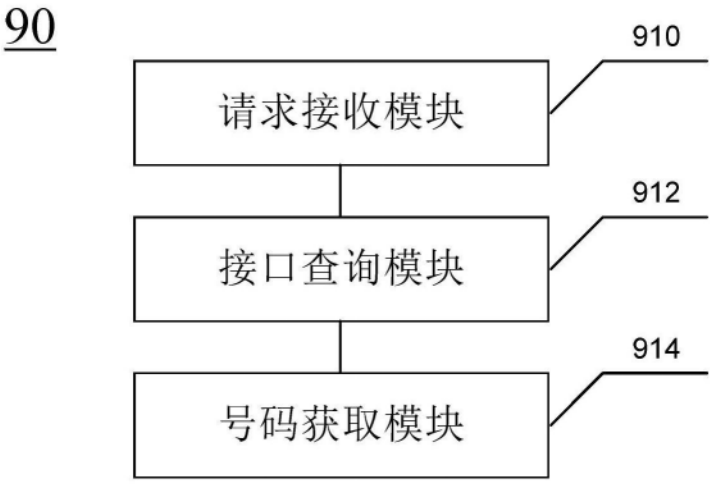

90
910
请求接收模块
912
接口查询模块
914
号码获取模块

图9

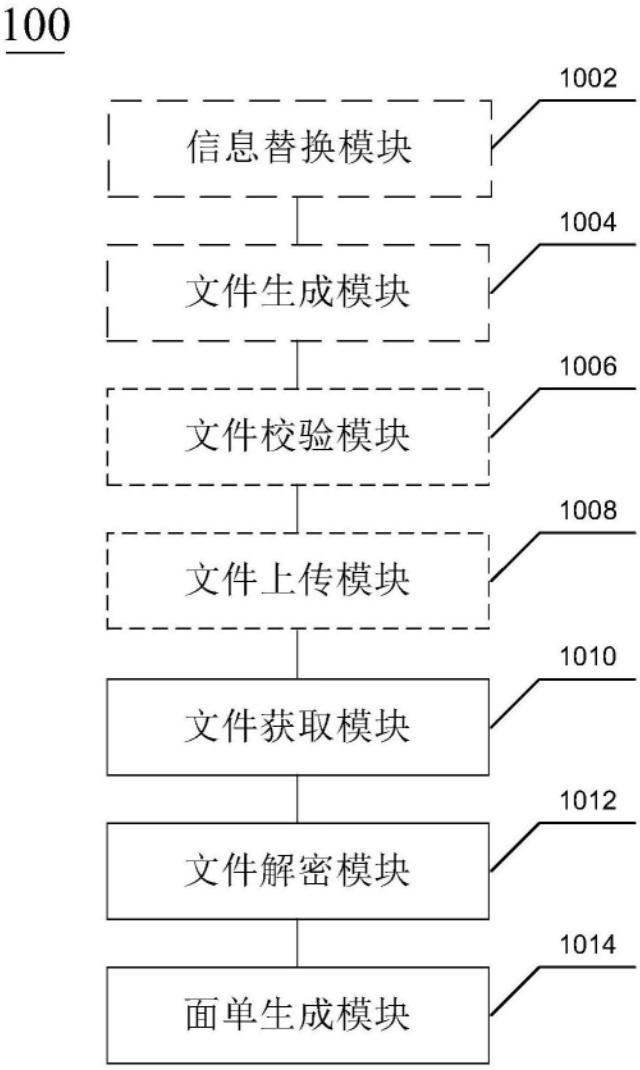

100
1002
信息替换模块
1004
文件生成模块
1006
文件校验模块
1008
文件上传模块
1010
文件获取模块
1012
文件解密模块
1014
面单生成模块

图10

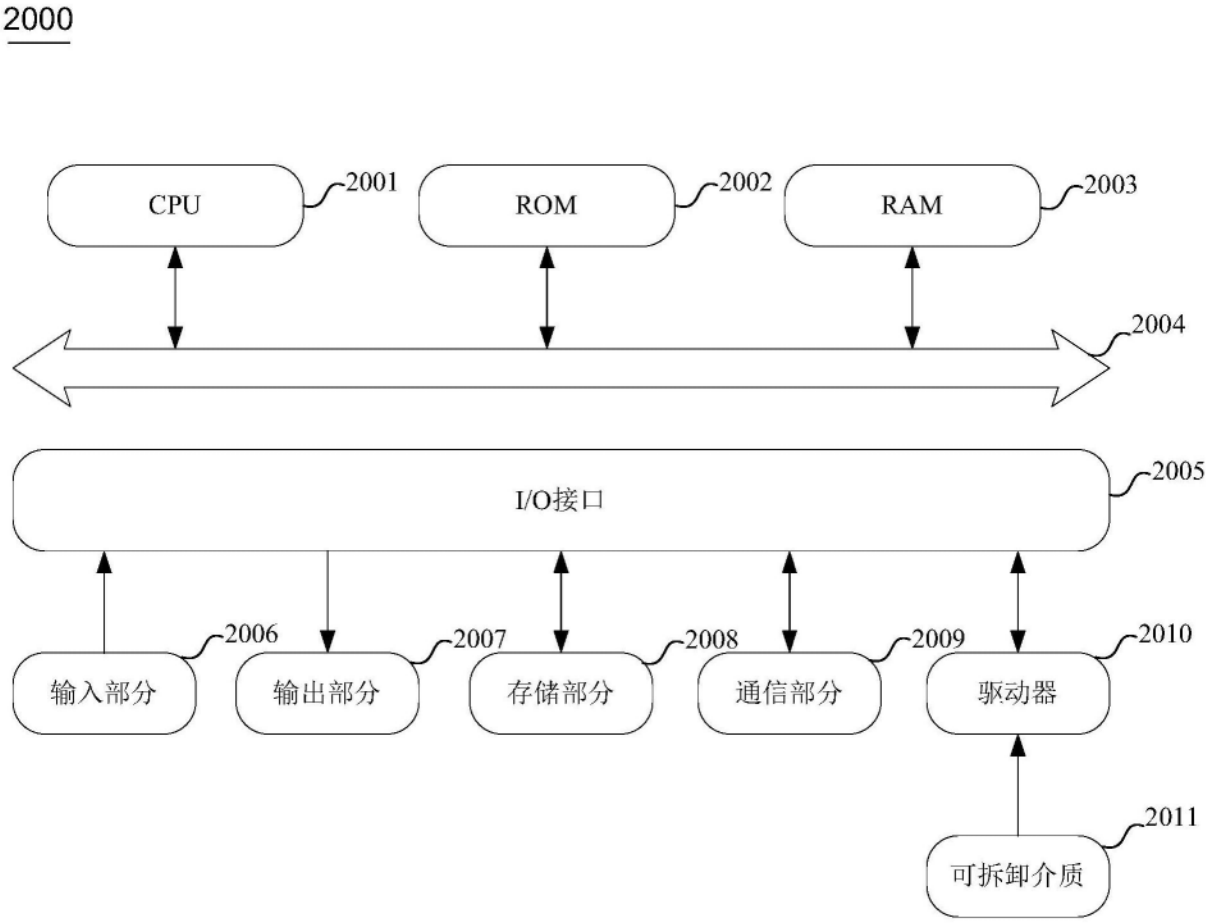

2000
CPU
2001
ROM
2002
RAM
2003
2004
I/O接口
2005
输入部分
2006
输出部分
2007
存储部分
2008
通信部分
2009
驱动器
2010
可拆卸介质
2011

图11