(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 106302472 A
(43)申请公布日 2017.01.04

(21)申请号 201610686677.4

(22)申请日 2016.08.18

(66)本国优先权数据
201610648146.6 2016.08.09 CN

(71)申请人 厦门乐享新网络科技有限公司
地址 361000 福建省厦门市思明区软件园二期望海路55号B303

(72)发明人 黄亮

(74)专利代理机构 杭州裕阳专利事务所(普通合伙) 33221
代理人 应圣义

(51)Int.Cl.
H04L 29/06(2006.01)
H04M 3/42(2006.01)
H04L 29/08(2006.01)

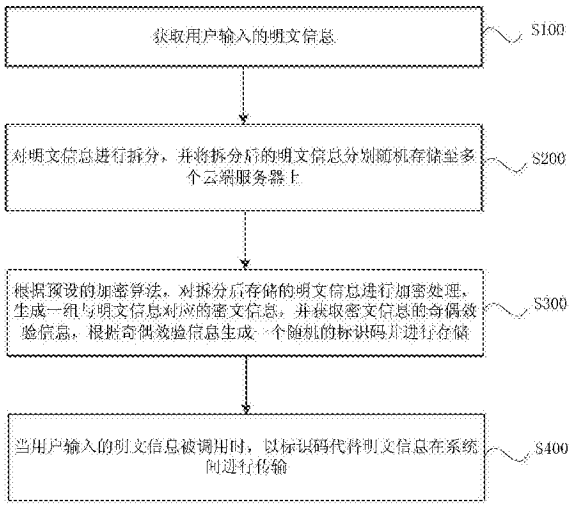
权利要求书2页 说明书7页 附图2页

(54)发明名称

信息的隐藏方法及装置

(57)摘要

本发明公开了一种信息的隐藏方法及装置，其中方法包括：获取用户输入的明文信息，对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，根据奇偶效验信息生成一个随机的标识码并进行存储；当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输。本发明使得信息在互联网或系统与系统之间传递的过程中，无论怎么被截取，都无法获得用户真正输入的明文信息，避免了用户信息被随意的获取、利用，有效的实现信息的隐藏。



CN 106302472 A

1.一种信息的隐藏方法，其特征在于，包括以下步骤：

获取用户输入的明文信息；

对所述明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；

根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与所述明文信息对应的密文信息，并获取所述密文信息的奇偶效验信息，根据所述奇偶效验信息生成一个随机的标识码并进行存储；

当用户输入的明文信息被调用时，以所述标识码代替所述明文信息在系统间进行传输。

2.根据权利要求1所述的信息的隐藏方法，其特征在于，所述明文信息包括用户的姓名、手机号码、座机号码以及通信地址中的一种或多种。

3.根据权利要求1所述的信息的隐藏方法，其特征在于，所述标识码的组成形式为：字母、数字、或字母与数字的组合。

4.根据权利要求1至3任一项所述的信息的隐藏方法，其特征在于，在当用户输入的明文信息被调用时，以所述标识码代替所述明文信息行传输之后，还包括以下步骤：

接收所述标识码；

根据所述标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；

根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息。

5.根据权利要求4所述的信息的隐藏方法，其特征在于，所述根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息后，还包括以下步骤：

当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

6.根据权利要求5所述的信息的隐藏方法，其特征在于，所述当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接发起对当前调用的电话号码建立通信连接，包括以下步骤：

对当前调用的电话号码发起通信连接；

在与当前调用的电话号码通信连接成功后，以回呼的方式发起对使用方的回呼连接；

在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

7.一种信息的隐藏装置，其特征在于，包括获取模块、存储模块、加密模块以及传输模块；

所述获取模块，用于获取用户输入的明文信息；

所述存储模块，用于对所述明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；

所述加密模块，用于根据预设的加密算法对拆分后存储的明文信息进行加密处理，生成一组与所述明文信息对应的密文信息，并获取所述密文信息的奇偶效验信息，并根据所述奇偶效验信息生成一个随机的标识码并进行存储；

所述传输模块，用于当用户输入的明文信息被调用时，以所述标识码代替所述明文信息在系统间进行传输。

8.根据权利要求7所述的信息的隐藏装置，其特征在于，还包括接收模块、定位模块以及解密模块；

所述接收模块，用于接收所述标识码；

所述定位模块，用于根据所述标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；

所述解密模块，用于根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息。

9.根据权利要求8所述的信息的隐藏装置，其特征在于，还包括拨号模块；

所述拨号模块，用于当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

10.根据权利要求9所述的信息的隐藏装置，其特征在于，所述拨号模块包括第一通信单元、第二通信单元以及控制单元；

所述第一通信单元，用于对当前调用的电话号码发起通信连接；

所述第二通信单元，用于在所述第一通信单元发起的与当前调用的电话号码通信连接成功后，以回呼的方式发起对使用方的回呼连接；

所述控制单元，用于在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

信息的隐藏方法及装置

技术领域

[0001] 本发明涉及信息处理技术领域，特别涉及一种信息的隐藏方法及装置。

背景技术

[0002] 为了保护用户的隐私，电信运营商在呼叫转移的基础上，推出手机小号服务，通过用户选定的小号或临时小号，以呼叫转移的方式将呼叫转接到用户真实的号码上，达到较少暴露或隐藏真实号码的目的。某些情况在可视状态下以*号将敏感信息隐藏起来，做到敏感信息表面不可以见，当敏感信息在互联网上或在系统与系统间传递时，却实际以明文方式进行传递。

[0003] 这种信息的隐藏方式存在以下缺陷：首先，小号转接的方式功能单一，虽然可以通过小号来转接，使用的范围有局限性，原理还是呼叫转移。最早的呼叫转移是号码与号码间的转接，现在只是变成了以小号方式进行呼叫转接，实质上还是呼叫转移。在很多场合都没有办法隐藏真实号码，例如，通过手机号码进行移动应用的注册时，通常需要以获取短信验证的方式来验证手机号码的真实性，验证过程中，第三方就能获取用户的真实号码。其次，呼叫转接也增加了用户的使用成本。

[0004] 最重要的是，当信息以明文方式在互联网或系统间传递，传递的数据一旦被截获，信息将完全的泄露，根本无法有效的实现信息的隐藏。

发明内容

[0005] 为了更加全面有效的实现信息的隐藏，本发明提供了一种信息的隐藏方法及装置，其针对用户的手机号码等需要隐藏的信息提供了一种更可靠的隐藏方式，能够避免信息在传输过程中出现泄露。

[0006] 本发明提供的信息的隐藏方法，包括以下步骤：

[0007] 获取用户输入的明文信息；

[0008] 对所述明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；

[0009] 根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与所述明文信息对应的密文信息，并获取所述密文信息的奇偶效验信息，根据所述奇偶效验信息生成一个随机的标识码并进行存储；

[0010] 当用户输入的明文信息被调用时，以所述标识码代替所述明文信息在系统间进行传输。

[0011] 作为一种可实施方式，所述明文信息包括用户的姓名、手机号码、座机号码以及通信地址中的一种或多种。

[0012] 作为一种可实施方式，所述标识码的组成形式为：字母、数字、或字母与数字的组合。

[0013] 作为一种可实施方式，在当用户输入的明文信息被调用时，以所述标识码代替所

述明文信息行传输之后，还包括以下步骤：

[0014] 接收所述标识码；

[0015] 根据所述标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；

[0016] 根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息。

[0017] 作为一种可实施方式，所述根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息后，还包括以下步骤：

[0018] 当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

[0019] 作为一种可实施方式，所述当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接发起对当前调用的电话号码建立通信连接，包括以下步骤：

[0020] 对当前调用的电话号码发起通信连接；

[0021] 在与当前调用的电话号码通信连接成功后，以回呼的方式发起对使用方的回呼连接；

[0022] 在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

[0023] 相应地，本发明还提供一种信息的隐藏装置，包括获取模块、存储模块、加密模块以及传输模块；

[0024] 所述获取模块，用于获取用户输入的明文信息；

[0025] 所述存储模块，用于对所述明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；

[0026] 所述加密模块，用于根据预设的加密算法对拆分后存储的明文信息进行加密处理，生成一组与所述明文信息对应的密文信息，并获取所述密文信息的奇偶效验信息，并根据所述奇偶效验信息生成一个随机的标识码并进行存储；

[0027] 所述传输模块，用于当用户输入的明文信息被调用时，以所述标识码代替所述明文信息在系统间进行传输。

[0028] 作为一种可实施方式，本发明的信息的隐藏装置，还包括接收模块、定位模块以及解密模块；

[0029] 所述接收模块，用于接收所述标识码；

[0030] 所述定位模块，用于根据所述标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；

[0031] 所述解密模块，用于根据预设的解密算法对所述密文信息进行解密，获取对应的明文信息。

[0032] 作为一种可实施方式，本发明的信息的隐藏装置，还包括拨号模块；

[0033] 所述拨号模块，用于当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

[0034] 作为一种可实施方式，所述拨号模块包括第一通信单元、第二通信单元以及控制单元；

[0035] 所述第一通信单元，用于对当前调用的电话号码发起通信连接；

[0036] 所述第二通信单元，用于在所述第一通信单元发起的与当前调用的电话号码通信

连接成功后，以回呼的方式发起对使用方的回呼连接；

[0037] 所述控制单元，用于在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

[0038] 本发明相比于现有技术的有益效果在于：

[0039] 本发明提供的信息的隐藏方法及装置，首先，通过获取用户输入的明文信息，对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；其次，根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，根据奇偶效验信息生成一个随机的标识码并进行存储；最后，当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输。本发明通过对用户输入的信息进行了信息组合，信息在互联网或系统与系统之间传递的过程中，无论怎么被截取，都无法获得用户真正输入的明文信息。由此避免用户信息被随意的获取、利用，有效的实现信息的隐藏。

附图说明

[0040] 图1为本发明一实施例提供的信息的隐藏方法的流程示意图；

[0041] 图2为本发明一实施例提供的信息的隐藏装置的结构示意图。

具体实施方式

[0042] 以下结合附图，对本发明上述的和另外的技术特征和优点进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明的部分实施例，而不是全部实施例。

[0043] 请参阅1，本发明一实施例提供的信息的隐藏方法，包括以下步骤：

[0044] S100、获取用户输入的明文信息。

[0045] 用户输入的明文信息可以是用户的姓名、手机号码、座机号码以及通信地址中的一种或多种，也可以是其他的数字或文字信息。

[0046] S200、对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上。

[0047] 用户输入的完整的明文信息被拆分后，随机分别存储在不同的云端服务器上。这样，当某台云端服务器发生安全事故信息泄露时，被泄露的拆分后的随机信息，完全无法独立使用，增强了信息安全。

[0048] S300、根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，根据奇偶效验信息生成一个随机的标识码并进行存储。

[0049] 对拆分后存储的明文信息采用预设的加密算法进行加密，使其成无意义的密文信息，完成一次加密。在此基础上，对加密后的信息再通过奇偶效验，生成一组独立的奇偶效验信息，相当于二次加密。该奇偶效验信息会产生一个随机的标识码并进行储存，供给个人用户直接使用或是第三方系统通过接口调用的方式使用。

[0050] S400、当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输。

[0051] 需要说明的是，本发明中的所有明文信息仅在本方法所应用的系统的内部调用，

不在外部系统间传输。系统仅以奇偶校验信息产生的标识码在互联网或系统与系统间传输。任意用户或第三方，需要调用用户输入的明文信息时，必须发出调用指令。互联网或系统之间传输的内容是独立的奇偶校验信息产生的一个随机的标识码，该标识码的内容与实际的调用信息的内容无关，其组成形式可以为：字母、数字、或者字母与数字的组合，也可以是其他的图形编码，例如二维码等。

[0052] 例如在第三方平台、软件、硬件通过接口与本发明所应用的系统交互时，涉及到用户保存到系统内部的信息内容进行交互时，仅在系统间传递标识码。如果用户保存的内容为电话号码，则系统通过获得标识码，以回呼的方式，让第三方系统(例如手机)无需获得用户的手机号码、座机号码，就能够联系到用户。

[0053] 具体实现过程如下：

[0054] 作为一种可实施方式，在步骤S400之后还包括以下步骤：

[0055] S500、接收标识码；

[0056] S600、根据标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；

[0057] S700、根据预设的解密算法对密文信息进行解密，获取对应的明文信息。

[0058] 在收到随机的标识码后，通过奇偶校验对标识码进行用户信息存储位置的复原，将实际调用的信息取回系统内部，并通过解密还原用户存储的信息。

[0059] 更进一步地，在步骤S700之后，还包括以下步骤：

[0060] S800、当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

[0061] 作为一种可实施方式，S800具体包括以下步骤：

[0062] S810、对当前调用的电话号码发起通信连接；

[0063] S820、在与当前调用的电话号码通信连接成功后，以回呼的方式发起对使用方的回呼连接；

[0064] S830、在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

[0065] 利用本发明提供的信息的隐藏方法，对用户的输入信息进行加密后，可按特定的形式公开在任何场合，任何第三方需要通过调用系统对应应用接口，在获取交互授权后才能获得可公开的必要传递的非敏感可视信息。

[0066] 本发明对用户输入的信息进行了信息组合，信息在互联网或系统与系统之间传递的过程中，无论怎么被截取，都无法获得用户真正输入的明文信息。

[0067] 下面根据针对具体的应用场景，对本发明的实现过程进行举例说明。

[0068] 假设，本发明提供的信息的隐藏方法的实现平台(即其应用系统)称为“隐藏宝”，其使用过程如下：

[0069] 步骤S110、用户在“隐藏宝”进行账号注册；

[0070] 步骤S120、用户在“隐藏宝”中将常用情景涉及到的信息(明文信息)输入，并保存；

[0071] 步骤S130、“隐藏宝”对用户保存的信息，进行加密处理后，保存在“隐藏宝”平台，主要针对指定的敏感信息生成可视化带*号的内容，同时生成一个加密过的用户独有二维码。

[0072] 使用场景一：第三方购物平台进行信息调用

[0073] 步骤S210、用户在互联网第三方平台购物；

[0074] 步骤S220、用户选购完毕，需要填写物流信息，用户选择从“隐藏宝”授权将信息自动填入对应对话框；

[0075] 步骤S230、第三方购物平台通过与“隐藏宝”合作的授权数据接口，调用本次需要的且用户已保存在“隐藏宝”的数据；

[0076] 步骤S240、第三方平台将从“隐藏宝”获得的用户数据代入相应输入对话框；

[0077] 步骤S250、用户对代入数据进行确认后，进入支付环节，支付完毕后待商家发货；

[0078] 步骤S260、商家端将收到“隐藏宝”加密后的用户信息；

[0079] 步骤S270、商家将用户的配送信息打印到物流单上，打印处理的信息是经过“隐藏宝”处理过后的可视信息；

[0080] 步骤S280、物流在商户取件，根据实际可视的物流地址进行配送；

[0081] 步骤S290、物流公司将商品送至目的地后，在需要联系收件人(用户)时，快递员通过与“隐藏宝”配套的软件或硬件，扫描快递单上的二维码或者输入特定的数字串后，配套的软件或硬件设备(例如，APP、智能手机、智能终端)，通过与“隐藏宝”的交互，获得被加密后的用户数据；

[0082] 步骤S291、快递员通过配套的软件或硬件设备可以和收件(用户)发起语音联系(电话联系等)，进行配送沟通，完成配送。

[0083] 信息交互流程如下：

[0084] 步骤S310、用户将信息输入并保存在“隐藏宝”上；

[0085] 步骤S320、通过接口，“隐藏宝”与授权第三方相互连接，数据可以在二者之间传递；授权第三方通过接口请求查询、获取用户信息；

[0086] 步骤S330、通过接口，“隐藏宝”将第三方查询、获取的结果反馈给第三方；

[0087] 步骤S340、当第三方需要连接(联系)用户时，通过接口，调取加密的用户数据，通过“隐藏宝”发起对用户的连接(联系)；

[0088] 步骤S350、“隐藏宝”执行第三方发出的指令，与“隐藏宝”内对应的用户信息进行配对后，发起对应用户的连接(联系)；

[0089] 步骤S360、第三方在无需获得用户实际信息的情况下，通过“隐藏宝”随时可以连接(联系)到用户。

[0090] 使用场景二：公司、企业通信录隐藏

[0091] 步骤S410，用户在“隐藏宝”注册企业/公司账号；

[0092] 步骤S420，用户在“隐藏宝”中录入企业/公司的通讯录(例如：手机号码、部门、职位等)，按“隐藏宝”平台的设置要求，操作完毕并保存；

[0093] 步骤S430，“隐藏宝”平台用*号隐藏用户录入的号码等信息，生成“隐藏宝”平台上可视的带*号的用户通讯录，当企业内部需要拨打通讯录上电话时，“隐藏宝”平台通过拨打界面(拨号模块)呼叫被联系者。

[0094] 本发明可以方便、简洁的将用户信息进行加密，通过授权接口，可以方便任何第三方在系统规定的范围内，快速、便捷的获取加密的可视用户信息。需要连接(联系)用户时，直接在系统内部对用户进行连接(联系)，由此避免完整的用户信息被随意的获取、利用，有效的保护了用户的信息隐私。

[0095] 上述步骤S270中，用户信息内容为带*号的可视信息，对用户姓名、用户手机、座机进行了部分隐藏。例如，用户的姓名为张三丰，联系电话为13333445566，010-88776655，“隐藏宝”提供的可视信息为姓名：张***，联系电话：133******66，010-8******5，姓名被隐藏了几个汉字，不可知晓，联系电话中*号部分不可见。

[0096] 传统方式的*号隐藏，是独立、非公开形式运行方式，可以在内部起到信息保护作用，一旦采取开放方式，虽然信息表面上是部分处于不可见状态，但信息在系统间传递时，无需通过专业软件，就能非常容易的获取在系统间传递的明文数据，无法有效实现信息的隐藏。

[0097] 上述实施例“隐藏宝”所提供的隐藏方式，与传统的信息隐藏方式不同，信息在系统间传递时，是以标识码进行传递的，即系统与系统间传递的是非明文状态的用户信息，当“隐藏宝”收到标识码后，即使返回的是明文信息，明文信息状态还是部分带*号的内容。即使发生泄露，也无法获得完成的用户信息。

[0098] 基于同一发明构思，本发明实施例还提供了一种信息的隐藏装置。

[0099] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。

[0100] 参见图2，本发明一实施例提供的信息的隐藏装置，包括获取模块100、存储模块200、加密模块300以及传输模块400。其中，获取模块100用于获取用户输入的明文信息；存储模块200用于对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；加密模块300用于根据预设的加密算法对拆分后存储的明文信息进行加密处理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，并根据奇偶效验信息生成一个随机的标识码并进行存储；传输模块400用于当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输。

[0101] 本发明另一实施例提供的信息的隐藏装置，在上述实施例的基础上还包括接收模块、定位模块以及解密模块，已完成调用后的动作。具体如下：

[0102] 接收模块用于接收标识码；定位模块用于根据标识码，利用奇偶效验对需要调用的信息的存储位置进行复原，获取对应的密文信息；解密模块，用于根据预设的解密算法对密文信息进行解密，获取对应的明文信息。

[0103] 进一步地，本发明又一实施例提供的信息的隐藏装置在上述实施例的基础上还包括拨号模块，该拨号模块用于当调用的明文信息为电话号码且需要建立通信连接时，则在系统内部直接对当前调用的电话号码发起通信连接。

[0104] 具体地，拨号模块包括第一通信单元、第二通信单元以及控制单元。其中，第一通信单元用于对当前调用的电话号码发起通信连接；第二通信单元用于在第一通信单元发起的与当前调用的电话号码通信连接成功后，以回呼的方式发起对使用方的回呼连接；控制单元用于在当前调用的电话号码与使用方通话连接成功后，结束当前调用。

[0105] 接下来，本发明再一实施例还提供了一种信息的隐藏装置，该装置包括处理器以及用于存储处理器可执行指令的存储器；

[0106] 其中，该处理器被配置为：

[0107] 获取用户输入的明文信息；对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上；根据预设的加密算法，对拆分后存储的明文信息进行加密处

理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，根据奇偶效验信息生成一个随机的标识码并进行存储；当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输。

[0108] 在上述实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器，上述指令可由信息的隐藏装置的处理器执行以完成上述方法。例如，所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0109] 以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者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者全部模块来实现本公开方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0110] 本发明提供的信息的隐藏方法及装置，无论是在公开还是非公开场合，无论是独立、非公开形式运行，还是以开放形式提供给第三方应用、使用，都能够有效的将用户需要隐藏的信息隐藏起来，而且在确保信息不发生泄露的基础上，又能够让第三方需要联系用户时，根据隐藏的信息与用户建立通信连接，安全可行。

[0111] 以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步的详细说明，应当理解，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围。特别指出，对于本领域技术人员来说，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

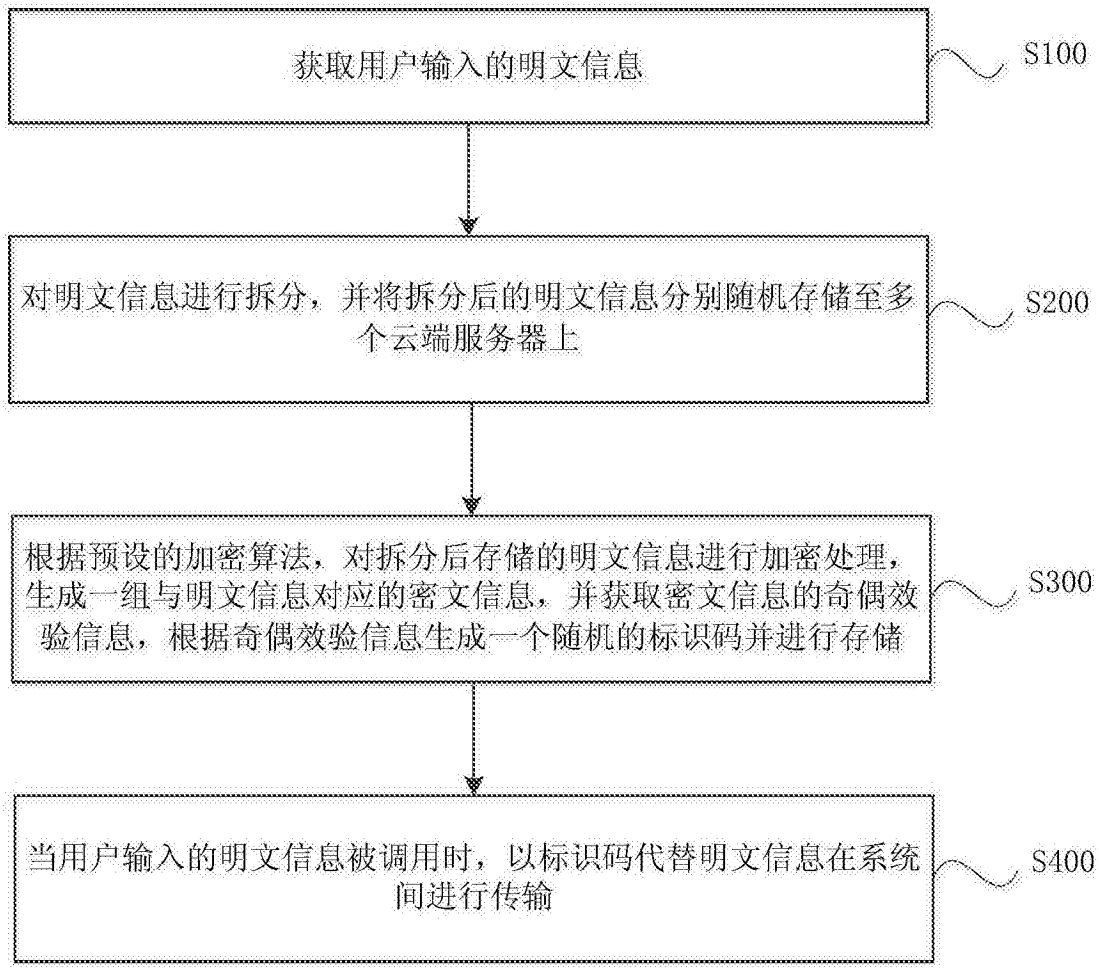

获取用户输入的明文信息
S100
对明文信息进行拆分，并将拆分后的明文信息分别随机存储至多个云端服务器上
S200
根据预设的加密算法，对拆分后存储的明文信息进行加密处理，生成一组与明文信息对应的密文信息，并获取密文信息的奇偶效验信息，根据奇偶效验信息生成一个随机的标识码并进行存储
S300
当用户输入的明文信息被调用时，以标识码代替明文信息在系统间进行传输
S400

图1

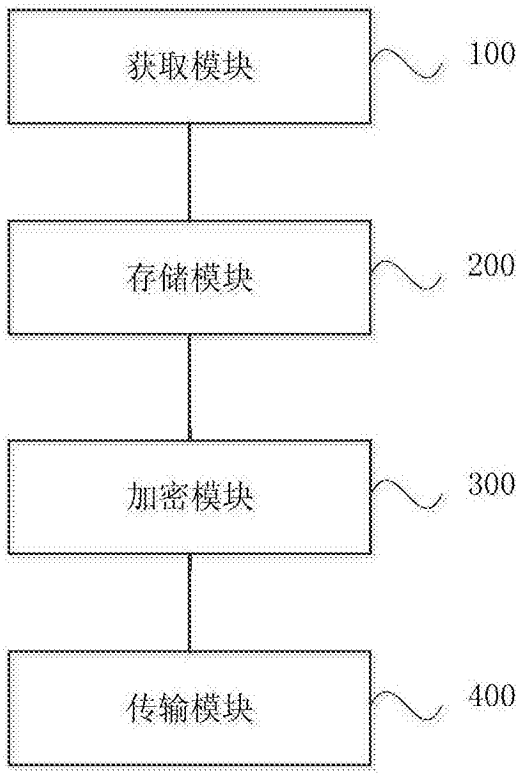


图2