



(12) 发明专利

(10) 授权公告号 CN 101436175 B

(45) 授权公告日 2010. 12. 08

(21) 申请号 200810174051. 0

(22) 申请日 2008. 11. 12

(30) 优先权数据

11/941, 250 2007. 11. 16 US

(73) 专利权人 国际商业机器公司

地址 美国纽约阿芒克

(72) 发明人 蒂莫西·R·查维斯

雅各布·D·艾辛格 珍妮弗·E·金

威廉·A·赖克特三世

帕特里克·R·沃德罗普

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 黄小临

(51) Int. Cl.

G06F 17/21 (2006. 01)

审查员 于白

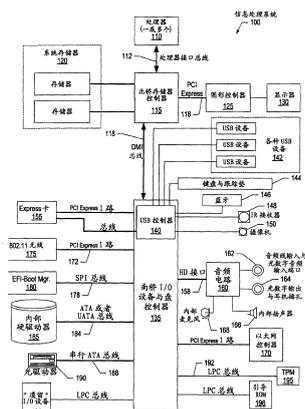
权利要求书 2 页 说明书 10 页 附图 9 页

(54) 发明名称

控制合作文档中的评注的系统与方法

(57) 摘要

提供了一种在打开在文档中的各个插入点处所插入的文档内容的字处理文档时操作的系统、方法以及程序产品。由对应于具体的用户标识符的用户打开文档。被包括在文档中的评注包括接收者标识符。选择用户的标识符被包括在相应评注的接收者标识符中的评注的第一集合, 并且选择用户的标识符未被包括在相应评注的接收者标识符中的评注的第二集合。字处理器将评注的第一集合显示在文档内容中的它们各自的插入点处, 而不呈现评注的第二集合。



1. 一种控制文档中的评注的方法,包含:

打开包括文档内容和在所述文档内容中的多个插入点处所插入的多个评注的字处理文档,其中,所述打开发生在当前被分配给用户标识符的字处理应用期间,并且其中,所述多个评注的一个或多个包括一个或多个接收者标识符;

从所述用户标识符被包括在相应评注的接收者标识符中的多个评注中选择评注的第一集合;

从所述用户标识符未被包括在相应评注的接收者标识符中的多个评注中选择评注的第二集合;

显示所述评注的第一集合,所述评注的第一集合中的每个被显示在所述文档内容中的它们各自的插入点处;以及

禁止显示所述评注的第二集合。

2. 根据权利要求1所述的方法,其中,不包括一个或多个接收者标识符的多个评注中的至少一个被包括在所述评注的第一集合中。

3. 根据权利要求1所述的方法,其中,一组评注被包括在评注的第一集合中,其中,该组评注包括一组接收者标识符,并且其中,所述评注的第一集合的选择还包含:

确定所述用户标识符被包括在对应于所述组接收者标识符的标识符列表中。

4. 根据权利要求3所述的方法,还包含:

在显示所述组评注之前:

确定所述组评注被加密;

响应于确定所述组评注被加密:

查找与所述用户标识符对应的加密的接收者包,其中,所述接收者包包括一个或多个组加密密钥;

检索与所述用户标识符对应的用户加密密钥;

使用所检索的用户加密密钥来对所述加密的接收者包解密;

从解密的接收者包中检索所选择的组加密密钥,其中,所选择的组加密密钥对应于所述组接收者标识符;以及

使用所选择的组加密密钥对加密的组评注解密。

5. 根据权利要求1所述的方法,还包含:

标识在所述评注的第一集合中所包括的一个或多个加密的评注的第一集合;

检索与所述用户标识符对应的加密密钥;以及

使用所检索的加密密钥对所述加密的评注的第一集合解密。

6. 根据权利要求5所述的方法,其中,一个或多个加密的评注的第二集合被包括在所述评注的第二集合中,并且其中,所检索的加密密钥不能够对所述加密的评注的第二集合解密。

7. 根据权利要求5所述的方法,其中,使用与所述用户标识符对应的公共加密密钥对从所述加密的评注的第一集合中所选择的加密的评注的至少一个进行加密,并且其中,用于对所选择的加密的评注进行解密的加密密钥是与所述公共加密密钥对应的私有加密密钥。

8. 一种控制文档中的评注的系统,包含:

打开部件,打开包括文档内容和在所述文档内容中的多个插入点处所插入的多个评注的字处理文档,其中,所述打开发生在当前被分配给用户标识符的字处理应用期间,并且其中,所述多个评注的一个或多个包括一个或多个接收者标识符;

第一选择部件,从所述用户标识符被包括在相应评注的接收者标识符中的多个评注中选择评注的第一集合;

第二选择部件,从所述用户标识符未被包括在相应评注的接收者标识符中的多个评注中选择评注的第二集合;

显示部件,显示所述评注的第一集合,所述评注的第一集合中的每个被显示在所述文档内容中的它们各自的插入点处;以及

禁止显示部件,禁止显示所述评注的第二集合。

9. 根据权利要求 8 所述的系统,其中,不包括一个或多个接收者标识符的多个评注中的至少一个被包括在所述评注的第一集合中。

10. 根据权利要求 8 所述的系统,其中,一组评注被包括在所述评注的第一集合中,其中,所述组评注包括一组接收者标识符,并且其中,第一选择部件还包含:

确定部件,确定所述用户标识符被包括在对应于所述组接收者标识符的标识符列表中。

11. 根据权利要求 10 所述的系统,还包含:

在显示所述组评注之前进行如下动作的部件:

确定所述组评注被加密;

响应于确定所述组评注被加密:

查找与所述用户标识符对应的加密的接收者包,其中,所述接收者包包括一个或多个组加密密钥;

检索与所述用户标识符对应的用户加密密钥;

使用所检索的用户加密密钥来对所述加密的接收者包解密;

从解密的接收者包中检索所选择的组加密密钥,其中,所选择的组加密密钥对应于所述组接收者标识符;以及

使用所选择的组加密密钥对加密的组评注解密。

12. 根据权利要求 8 所述的系统,还包含:

标识部件,标识在所述评注的第一集合中所包括的一个或多个加密的评注的第一集合;

检索部件,检索与所述用户标识符对应的加密密钥;以及

解密部件,使用所检索的加密密钥对所述加密的评注的第一集合解密。

13. 根据权利要求 12 所述的系统,其中,使用与所述用户标识符对应的公共加密密钥对从所述加密的评注的第一集合中所选择的加密的评注的至少一个进行加密,并且其中,用于对所选择的加密的评注进行解密的加密密钥是与所述公共加密密钥对应的私有加密密钥。

## 控制合作文档中的评注的系统与方法

### 技术领域

[0001] 本发明涉及控制合作文档中评注的系统与方法。更具体地,本发明涉及将文档中的评注呈现给所选择的人以及需要时保证评注安全的系统与方法。

### 背景技术

[0002] 文档(例如,字处理文档)是通信与文档管理的重要形式。由于其重要性,对于特定文档的读者可能包括各种类型的人。例如,一个文档可以具有一个以上的作者和一个以上的评论者。每一个作者和评论者可能具有关于文档的不同程度的重要性和范围,因此某些人可能负责编写或者评论整个文档,而其他人关注特定的部分。另外,某些评论文档的人可能是对那些编写或者评论文档的人的管理者。由于存在着不同类型的编写和评论文档的人,所以由于这样的文档对文档的所有用户可见,因而通常从传统评论中省去敏感的或保密的特性的文档。

[0003] 一种仅向所选择的人提供评注的方案是经由另一个介质比如在独立的电子邮件记录中发送评注。对这一方案的明显的挑战是,被包括在一个独立的电子邮件记录中的评注与实际文档相分离,使得难以确定评注应用在哪里。这一方案的另一个挑战是,基于电子邮件的评注与文档的生命期不同步,因此作者与评论者较难在时间上估计是否应在将来的草稿中适当地给出评注。

### 发明内容

[0004] 已经发现可以使用一种在打开包括文档内容和在文档内容中的不同插入点处所插入的评注的字处理文档时而操作的系统、方法以及计算机程序产品,解决上述挑战。由对应于具体的用户标识符的用户打开文档。被包括在文档中的评注包括一个或多个接收者标识符。选择用户的标识符被包括在相应评注的接收者标识符中的评注的第一集合,并且选择用户的标识符未被包括在相应评注的接收者标识符中的评注的第二集合。字处理器将评注的第一集合显示在文档内容中的它们的各个插入点处,而不呈现评注的第二集合。在一个实施例中,任何不具有接收者标识符的评注可以由任何人浏览,因此它们被包括在评注的第一集合中。

[0005] 在另一个实施例中,一组评注被包括在评注的第一集合中。该组评注包括一组接收者标识符。通过确定用户标识符被包括在与组接收者标识符对应的标识符列表中,将组评注包括在评注的第一集合中。在另一个实施例中,在显示组评注之前,把组评注标识为被加密的。检索包括组加密密钥的接收者包。用户加密密钥用于对接收者包进行解密,并且与组评注对应的组加密密钥被检索并被用于对加密的组评注进行解密。

[0006] 在一个实施例中,加密的评注的第一集合被标识为被包括在评注的第一集合中。为了打开加密的评注,检索与用户标识符对应的加密密钥。然后使用所检索的加密密钥对加密的评注进行解密。注意,不能使用用户的加密密钥对被包括在评注的第二集合中的加密的评注进行解密,因为被包括在评注的第二集合中的评注未被导向与用户标识符对应的

用户。在另一个实施例中,使用与用户标识符对应的公共加密密钥对加密的评注进行加密,并且用于对加密的评注进行解密的加密密钥是与该公共加密密钥对应的私有加密密钥。

[0007] 以上是概述,并因此必然包含简化、概括和细节的省略,因而,本领域技术人员将会意识到,此概述仅为说明性的,而非旨在以任何方式进行限制。在以下所给出的非限制性详细描述中,仅由权利要求加以定义的本发明的其它方面、发明特性以及优点将变得明显。

### 附图说明

[0008] 参照附图,将更好地理解本发明,以及对本领域技术人员显而易见的本发明的诸多目的、特性以及优点,附图中:

[0009] 图 1 是其中可以实现在此所述的方法的数据处理系统的结构图;

[0010] 图 2 提供了图 1 中所示的信息处理系统环境的扩展,用于图示可以在操作于网络环境中的各种信息处理系统上进行在此所述的方法;

[0011] 图 3 是被插入和导向于所选的接收者的评注的屏幕描述;

[0012] 图 4A 是当所选的接收者之一浏览具有图 3 中所插入的评注的文档时该文档的屏幕描述;

[0013] 图 4B 是当非所选的接收者浏览具有图 3 中所插入的评注的文档时该文档的屏幕描述;

[0014] 图 5 是示出用于建立接收者组的步骤的示范流程图;

[0015] 图 6 是示出用于打包图 5 中所建立的各个组的步骤的示范流程图;

[0016] 图 7 是示出用于创建导向于特定接收者的评注的步骤的示范流程图;

[0017] 图 8 是示出用于从导向于所选的接收者的文档中检索评注的步骤的示范流程图;以及

[0018] 图 9 是示出检索导向于一组接收者的加密的评注的步骤的示范流程图。

### 具体实施方式

[0019] 在以下的描述和图中,阐述了某些具体的细节,以提供对本发明的不同实施例的全面理解。然而,在以下公开中,未阐述某些通常与计算和软件技术相关的公知的细节,以避免不必要地模糊本发明各实施例。另外,相关技术领域普通技术人员将理解,他们可以实践本发明的其它实施例,而不采用以下所描述的一或多个细节。最后,尽管参考以下公开中的步骤与序列描述了不同的方法,但这种描述用于提供对本发明实施例的清楚实现,而不应把这些步骤与步骤序列视为实践本发明所要求的。替代地,以下旨在提供对本发明的例子的详细描述,并且不应将其视为对本发明自身的限制。而是,任何数目的变更均可能落入本发明的范围,这由此描述之后的权利要求加以定义。

[0020] 以下的详细描述将总体上遵循以上所给出的本发明的概述,并将在需要时进一步解释和扩展本发明的各个方面的定义与实施例。为此,该详细描述首先阐述图 1 中的计算环境,其适合于实现与本发明相关的软件和/或硬件技术。图 2 中将网络环境图示为对基本的计算环境的扩展,以强调可以通过多个离散的设备进行现代计算技术。

[0021] 图 1 图示了信息处理系统 100,其是能够进行在此所述的计算操作的计算机系统的简化例子。信息处理系统 100 包括耦合于处理器接口总线 112 的一个或多个处理器 110。

处理器接口总线 112 把处理器 110 连接于北桥 115, 北桥 115 已知作为存储器控制器集线器 (MCH)。北桥 115 连接到系统存储器 120, 并且向处理器 110 提供用于存取系统存储器的手段。图形控制器 125 也连接于北桥 115。在一个实施例中, PCI Express 总线 118 用于把北桥 115 连接于图形控制器 125。图形控制器 125 连接于诸如计算机监视器的显示设备 130。

[0022] 使用总线 119 把北桥 115 和南桥 135 相互连接。在一个实施例中, 总线是在北桥 115 和南桥 135 之间的每一方向上以高速传送数据的直接介质接口 (DMI) 总线。在另一个实施例中, 使用外围组件互连 (PCI) 总线来连接北桥和南桥。已知作为 I/O 控制器集线器 (ICH) 的南桥 135 是通常实现以低于北桥所提供的性能的速度而操作的性能的芯片。南桥 135 典型地提供了用于连接各种组件的各种总线。这些总线可以包括 PCI 和 PCI Express 总线、ISA 总线、系统管理总线 (SMBus 或 SMB)、低插针数 (LPC) 总线。通常把 LPC 总线用于连接诸如引导 ROM196 和“遗留 (legacy)” I/O 设备 (使用“超级 I/O”芯片) 的低带宽设备。“遗留” I/O 设备 (198) 可以包括串行和并行端口、键盘、鼠标、软盘控制器。LPC 总线还用于把南桥 135 连接于可信平台模块 (Trusted Platform module) (TPM) 195。通常被包括在南桥 135 中的其它组件包括直接存储器存取 (DMA) 控制器、可编程中断控制器 (PIC)、存储设备控制器, 其使用总线 184 把南桥 135 连接于诸如硬盘驱动器的非易失存储设备 185。

[0023] ExpressCard 155 是用于把可热插设备连接于信息处理系统的插槽。当使用通用串行总线 (USB) 和 PCI Express 总线两者将 ExpressCard 155 连接于南桥 135 时, ExpressCard 155 支持 PCI Express 和 USB 连接性两者。南桥 135 包括 USB 控制器 140, USB 控制器 140 向连接到 USB 的设备提供 USB 连接性。这些设备包括网络摄像机 (摄像机) 150、红外 (IR) 接收器 148、提供无线个人局域网 (PAN) 的蓝牙设备 146、键盘与跟踪板 144、以及其它各种 USB 连接的设备 142, 比如鼠标、便携式存储设备、调制解调器、网卡、ISDN 连接器、传真机、打印机、USB 集线器、以及许多其它类型的 USB 连接的设备。

[0024] 无线局域网 (LAN) 设备 175 经由 PCI 或 PCI Express 总线 172 连接于南桥 135。LAN 设备 175 典型地实现了空中调制技术 (over-the-air modulation technique) 的 IEEE 802.11 标准之一, 这些技术全部使用了相同的协议, 以在信息处理系统 100 和另一个计算机系统或者设备之间无线通信。使用串行 ATA (SATA) 总线 188 把光存储设备 190 连接于南桥 135。串行 ATA 适配器与设备通过高速串行链接来通信。串行 ATA 总线也用于把南桥 135 连接于其它形式的存储设备, 比如硬盘驱动器。经由总线 158 把诸如声卡的音频电路 160 连接于南桥 135。音频电路 160 用于提供诸如音频线输入与光数字音频输入端口 162、光数字输出与耳机插孔 164、内部扬声器 166、以及内部麦克风 168 的功能性。使用诸如 PCI 或 PCI Express 总线的总线把以太网控制器 170 连接于南桥 135。以太网控制器 170 用于把信息处理系统 100 与诸如局域网 (LAN)、因特网、以及其它公共和私有计算机网络的计算机网络相连。

[0025] 尽管图示出了一个信息处理系统, 但是信息处理系统可以采取多种形式。例如, 信息处理系统可以采取台式机、服务器、便携式、膝上型、笔记本的形式或者其它形状因素的计算机或者数据处理系统。另外, 信息处理系统还可以采取诸如个人数字助手 (PDA)、游戏设备、ATM 机、便携式电话设备、通信设备、或者包括处理器和存储器的其它设备的其它形状因素。

[0026] 图 1 中所示和在此所述的用于提供安全功能的可信平台模块 (TPM 195) 仅为硬件

安全模块 (HSM) 的一个例子。因此,在此所述和要求保护的 TPM 包括任何类型的 HSM,该 HSM 包括但不限于符合可信计算组 (Trusted Computing Groups) (TCG) 标准的硬件安全设备,并且被称为“可信平台模块 (TPM) 规范版本 1.2”。TPM 是可以被并入任何数目的信息处理系统例如图 2 中所示的信息处理系统的硬件安全子系统。

[0027] 图 2 提供了图 1 中所示的数据处理系统环境的扩展,用于图示可以在网络环境中操作的各种信息处理系统上进行在此所述的方法。信息处理系统的类型涵盖从诸如手持计算机 / 移动电话 210 的小型手持设备到诸如主机计算机 270 的大型主机系统的一个宽泛的范围。手持计算机 210 的例子包括个人数字助手 (PDA)、诸如 MP3 播放器的个人娱乐设备、便携式电视、以及紧致盘播放器。信息处理系统的其它例子包括输入笔或写字板计算机 220、膝上型或笔记本计算机 230、工作站 240、个人计算机系统 250、以及服务器 260。图 2 中未单独示出的其它类型的信息处理系统由信息处理系统 280 表示。如所示,可以使用计算机网络 200 把各种信息处理系统一起连网。可用于互连各种信息处理系统的计算机网络的类型包括局域网 (LAN)、无线局域网 (WLAN)、因特网、公共交换电话网络 (PSTN)、其它无线网络、以及可用于互连信息处理系统的任何其它网络拓扑。许多信息处理系统包括诸如硬驱动器和 / 或非易失存储器的非易失数据存储器。将图 2 中所示的某些信息处理系统描绘为具有单独的非易失数据存储器 (示出服务器 260 具有非易失数据存储器 265、示出主机计算机 270 具有非易失数据存储器 275、以及示出信息处理系统 280 具有非易失数据存储器 285)。非易失数据存储器可以是在各种信息处理系统外部的组件,或者可以在信息处理系统之一的内部。另外,尽管未示出,但是可以使用各种技术在两个或多个信息处理系统之间共享单一的非易失数据存储器。

[0028] 图 3 是被插入和导向所选的接收者的评注的屏幕描述。图 3 绘出了字处理应用 300,字处理应用 300 包括菜单栏 310 和评注按钮 320。使用字处理器书写文档内容 330。根据字处理应用 300 的用户的请求,把评注添加到文档。在一个实施例中,使用了诸如评注按钮 320 的可视图标。如本技术领域技术人员将意识到的,存在许多其他手段用于请求诸如键盘动作、话音激活命令等字处理应用的动作或操作。用户把光标放置在将插入评注的插入点 340 处,然后请求评注。尽管这些评注通常不出现在诸如打印出的最终结果中,但是其可以用于通信,特别是文档的一个或多个书写者和文档的一个或多个评论者的多个用户之间的通信。另外,也可以与每一个人或者仅与所选的接收者共享评注。所选的接收者可以被包括在组中,比如评论者的组和书写者的组。最后,由于评注可能包括仅仅旨在与一个或多个所选的接收者共享的敏感或保密的信息,因此可以对评注加密,以便未选择的接收者不能够“窃用 (hack)”文件以浏览这种评注。使用评注插入对话框 350 来管理接收者的选择。

[0029] 当选择了评注请求 (例如,评注按钮 320) 时,评注插入对话框 350 出现。对话框 350 包括各种组件,这些组件包括:评注内容区 360,用户在那里输入评注;评注接收者选择区 370,用户在那里选择哪些接收者将能够浏览评注;加密检验框 385,当用户希望对评注内容进行加密以致其他未被选择的接收者不能窃用字处理文档以便浏览评注内容时,选择该加密检验框 385。另外,对话框 350 包括添加评注命令按钮 390 和取消命令按钮 395。在用户已于评注内容区 360 中键入了评注内容并从接收者选择区 370 选择了一个或多个接收者之后,则用户选择“添加评注”命令按钮,以便在插入点处将评注添加到文档。如

果用户决定不添加评注,则用户可以选择“取消”命令按钮 395,以取消评注的添加。在所示例子中,可能的接收者的列表包括各种组和个人。用户能够在使用诸如鼠标或键盘键选择接收者的同时,通过使用输入技术比如按下键盘键(例如“控制”键)来选择多个组或者个人。在所示例子中,所选的接收者 380 包括被标识为文档的作者的“Andrew”和被标识为文档的评论者的“Rene”。在一个实施例中,自动地选择评注的书写者(“Richard”381),以便书写者可以继续浏览评注。如前所述,可能的接收者的列表包括诸如“所有接收者”、“所有作者”、或者“所有评论者”的组。这些组简单的例子,并且可以基于文档的类型创建和使用另外的或者不同的组。例如,当文档属于组织的结构或者管理时,接收者组可以包括“管理者”、“雇员”、“销售方”等。

[0030] 图 4A 是当所选的接收者之一浏览具有图 3 中所插入的评注的文档时该文档的屏幕描述。当所选的接收者之一使用字处理器 300 打开具有评注的文档时,评注窗口 400 出现。评注窗口 400 包括所插入的评注内容以及相应于评注的元数据。元数据包括评注的作者(在本例中,作者名为“Richard”)以及相应于何时插入评注的时间标签。

[0031] 图 4B 是当非所选的接收者之一浏览具有图 3 中所插入的评注的文档时该文档的屏幕描述。与图 4A 所示的图相比,在图 4B 中,评注不出现,因为字处理应用 300 的用户不是所选的接收者之一。使用图 3 中所提供的样本名字,由“Alice”、“Oscar”、“Wendy”或者“Xavier”的任何一个操作图 4B 中所示的字处理应用,因为没有把这些人中的任何一个选择为评注的接收者。

[0032] 图 5 是示出用于建立接收者组的步骤的示范流程图。处理开始于 500 处,于是,在步骤 510 处,系统接收组名(例如,从用户那里),并且把所接收的组名存储在组数据存储器 520 中。如所示,组数据存储器 520 用于存储组名和与各个组相关的公共密钥以及唯一标识每一个组的成员的诸如用户登录标识符或者电子邮件地址的成员(接收者)标识符。在步骤 525,对于在步骤 510 中所接收和存储的组名,生成非对称的公共密钥/私有密钥对。公共密钥被存储在组数据存储器 520 中,而私有密钥与各个组名一起被存储在私有组存储器 530 中。此时,单个组名与私有组存储器 530 中的私有密钥以及公共组数据存储器 520 中的公共密钥相关联。

[0033] 在步骤 540,从接收者数据存储器 550 中选择包括在新形成的组中的第一个成员(接收者)。如所示,接收者数据存储器 550 包括可能的接收者的名字以及接收者的标识符(例如,用户登录、电子邮件地址等)。另外,对于每个接收者生成了非对称的公共密钥/私有密钥对。对应于每个接收者的公共密钥与各个接收者相关联,并且被存储在接收者数据存储器 550 中。在步骤 555,在步骤 540 所检索的接收者标识符被存储在组数据存储器 520 中,并且与接收者所属的一个(或多个)组相关联。使用图 3 的例子,示出 Alice、Andrew、Oscar 以及 Wendy 都作为“作者”,因此应将他们添加到文档的“作者”组。同样,示出 Rene、Richard 以及 Wendy 都作为“评论者”,因此应将他们添加到文档的“评论者”组。注意,把 Wendy 被包括在这两个组中,因为她既被标记为文档的作者,也被标记为文档的评论者。而且注意,Xavier 既未被标记为文档的作者,也未被标记为文档的评论者,因此不应将其包含在任何组中。返回至图 5,在于步骤 555 存储了所选择接收者之后,判断是否还存在包括在组中的更多成员(决定 560)。如果存在更多要包括的成员,则决定 560 转向“是”分支 562,该分支循环回去以使用户可以选择包括在组中的下一个成员(接收者),并且相应地保存

接收者的数据。该循环继续,直至不再存在要包括在所选的组中的成员,此时,决定 560 转向“否”分支 564,于是,进行判断是否还存在要创建的更多的组(决定 565)。如果还存在更多要创建的组,则决定 565 转向“是”分支 566,该分支循环回去以接收和存储关于下一个组的数据,包括对于该组的组成员(单个接收者)的选择与存储。该循环继续,直至用户不再创建任何组,此时,决定 565 转向“否”分支 568。

[0034] 在已经创建了组并存储了关于组的数据之后,则对组进行打包(预定过程 570,参见图 6 以及对处理细节的相应文本)。组的打包产生了一或多个加密的接收者包 575,每个加密的接收者包 575 仅可由特定的接收者打开。在步骤 580,加密的接收者包 575 和组数据存储器 520 被包括在与接收者和组相关联的一个(或多个)文档 585 中。在一个实施例中,通过把组数据、加密的接收者包以及接收者数据附于将对其进行评注的文档来创建文档 585。以此方式,创建和浏览导向具体组或者个人的评注所需的组数据和接收者数据被保持在一起,以便当浏览或者编辑文档时每个用户具有对所有所需数据的存取,而不管用户的位置如何或者是对集中化的有组织的数据存储器的存取。在步骤 590,文档 585 被提供给各个接收者。可以使用传统的方法比如把文档存储在共享的非易失数据存储设备上、把文档附接于电子邮件消息并经由诸如因特网的网络发送到接收者、或者使用其它已知的方法来实现文档的提供。然而,既然字处理文档 585 包括组数据、加密的接收者包以及接收者数据,则可以使用字处理文档所包括的数据来处理被导向单个接收者和/或接收者的组的文本所包括的评注,以下将进一步加以说明。其后处理在 595 处结束。

[0035] 图 6 是示出了用于打包图 5 中所建立的各个组的步骤的示范流程图。处理开始于 600,于是,在步骤 610,从接收者数据存储器 550 中选择第一接收者。在步骤 620,从包括所选的接收者的组数据存储器 520 中(使用接收者的标识符)标识第一组。确定所选的接收者是否属于任何组(决定 630)。如果所选的接收者不属于任何组,则决定 630 转向“否”分支 632,该分支循环回去,以从接收者数据存储器 550 选择下一个接收者,并进行处理。当选择了属于至少一个组的接收者时,则决定 630 转向“是”分支 638,以创建接收者包。

[0036] 在步骤 640,从私有组存储器 530 中检索组的私有密钥和组的名字,并且把它们存储在接收者包 650 中。在步骤 660,试图标识包括所选的接收者作为成员的下一个组。确定是否标识了包括所选的接收者作为成员的下一个组(决定 670)。如果发现了下一个组,则决定 670 转向“是”分支 672,该分支循环回去,以从私有组存储器 530 中检索新选择的组的名字和私有密钥,并且将所检索的名字和私有密钥存储在接收者包 650 中。该循环继续,直到已经标识了所选择接收者所属的所有组,并且把组的名字和私有密钥存储在接收者的包中。在已经发现所选的接收者所属的所有组,并且对它们进行了处理之后,决定 670 转向“否”分支 674,于是,在步骤 675,使用接收者的公共密钥对刚刚创建的接收者的包(650)进行加密,从而产生加密的接收者包 680。

[0037] 然后,判断可用的接收者数据存储器 550 中是否存在要处理的更多接收者(决定 685)。如果存在更多接收者,则决定 685 转向“是”分支 688,该分支循环回去,以处理数据存储器中的下一个接收者。对于作为一个或多个组的成员的那些接收者,创建另外的加密的接收者包 680,并且将它们添加于加密的接收者包 682 的组中。将加密的接收者包 682 随字处理文档而包括,并且由于仅可以使用接收者的私有密钥来打开各个加密的接收者包,因此可以针对未经授权的接收者或字处理文档的使用保护被存储在加密的包中的组密钥。

在已经处理了所有的接收者之后,决定 685 转向“否”分支 690,并且处理在 695 处返回至调用例程(参见图 5)。

[0038] 图 7 是示出了用于创建导向具体接收者的评注的步骤的示范流程图。处理开始于 700,于是,在步骤 705,检索文档中的评注插入点。在一个实施例中,评注插入点是文档中光标的当前位置。在步骤 710,从用户处接收要显示在插入点处的评注内容。在步骤 715,从用户处接收第一评注接收者(例如,从诸如图 3 中所示的接收者列表 370 的接收者列表中选择)。确定用户是否已经选择使评注对所有接收者可见(决定 720)。在一个实施例中,当已经选择了“所有接收者”(例如,从诸如图 3 中所示的接收者列表 370 的接收者列表中选择“所有接收者”)时,或者当还没有选择具体的接收者时,确定所有接收者是所预期的读者。如果确定已经选择了所有接收者,则决定 720 转向“是”分支 722,于是,在步骤 725,插入点与评注内容一起被存储,以致评注内容将可由字处理文档的任何接收者浏览,其后,处理在 730 结束。

[0039] 返回到决定 720,如果没有选择所有接收者,则决定 720 转向“否”分支 732,以处理不同的接收者。在步骤 735,把将被插入文档中的评注接收者标签初始化为第一评注接收者的标识符。注意,每个接收者既可以是单个的接收者,也可以是一组接收者。确定用户是否请求对评注进行加密(决定 740)。如果用户请求加密评注,则决定 740 转向“是”分支 742,于是,在步骤 745,从接收者数据存储器 550(在单个接收者的情况下),或者从组数据存储器 520(在组接收者的情况下)检索与该单个或者组接收者相对应的非对称的“公共”密钥。在步骤 750,使用所检索的公共密钥来加密评注,并且在步骤 755,把插入点与评注接收者标签和加密的评注内容(例如,评注内容、图形、多媒体等)一起存储在字处理文档中。在步骤 760,从接收者的列表中检索下一个评注接收者(单个接收者或者组接收者)。确定是否在列表中发现了一个接收者(决定 765)。如果发现了另一个接收者,则决定 765 转向“是”分支 768,于是,在步骤 770,将评注接收者标签重新设置为下一个评注接收者的标识符,然后处理循环回去,以处理该接收者(检索接收者的公共密钥、加密评注内容、以及把数据存储在文档中)。该循环继续,直至已经处理了在接收者列表中所选择的所有接收者,此时,决定 765 转向“否”分支 772,并且加密的评注创建处理在 795 结束。

[0040] 返回至决定 740,如果评注未被加密,则决定 740 转向“否”分支 774,于是,在步骤 775,试图从接收者的列表中检索由用户选择的下一个评注接收者(组或个人)。确定用户是否选择了下一个接收者(决定 780,即,是否发现了一个接收者)。如果发现了另一个所选的接收者,则决定 780 转向“是”分支 782,于是,在步骤 785,把新发现的接收者标识符(组标识符或者个人标识符)附于评注接收者标签,并且处理循环回去,以检索另外的所选的接收者标识符。该循环继续,直至不再存在要处理的所选接收者,此时,决定 780 转向“否”分支 788,于是,在步骤 790,将插入点与评注内容一起存储,以便可由其标识符被包括在评注接收者标签中的任何接收者浏览评注内容。其后,对于所选择的受者的未加密的评注创建在 795 结束。

[0041] 图 8 是示出了用于从被导向所选的接收者的文档中检索评注的步骤的示例流程图。处理开始于 800,于是,在步骤 805,接收者之一打开具有已经根据本发明而插入的评注的字处理文档 585。而且,在步骤 805 中,从用户的存储器 810 中检索用于浏览加密的评注的用户的私有密钥。在步骤 815,检索组数据。在一个实施例中,如图 6 中先前所示,属于

一个组的每个接收者具有为各个接收者所创建的加密的接收者包。使用各个接收者的公共密钥来加密每个加密的接收者包。在此实施例中，检索为接收者所创建的组包，并且使用该接收者的与用于加密该接收者的组包的公共密钥相对应的私有密钥来对其解密。加密的接收者组包内的是接收者所属的组名字（组标识符）以及用于解密已经被导向该组的评注的私有密钥。例如，如果该接收者是“作者”组的成员，则该接收者的组包内的将是组标识符（例如，“作者”）以及对应于“作者”组的私有加密密钥。当遇到导向接收者或者导向接收者所属的组之一的加密的评注时，则接收者的私有密钥被用于解密被导向接收者的评注，并且组的私有密钥被用于解密被导向接收者所属的组之一的评注。字处理文档 585 的组数据部分包括已经建立的组名字（标识符）、对应于每个组的公共加密密钥、以及在一个实施例中的每个组的组成员的列表。在步骤 820，标识此接收者所属的组，并且将它们存储在诸如存储器位置的存储区 825 中。

[0042] 在步骤 830，扫描包括评注数据的文档的文本部分，以便查找第一评注插入点。确定是否在文档中发现了评注插入点（决定 832）。如果在文档中发现了评注插入点，则决定 832 转向“是”分支 834，以处理刚刚发现的评注。确定是否把评注导向文档的所有接收者（决定 835）。在一个实施例中，当已经选择了“所有接收者”（例如，从诸如图 3 中所示的接收者列表 370 的接收者列表中选择“所有接收者”）时，或者当还没有选择具体的接收者时，确定所有接收者都是预期的读者。如果评注被导向文档的所有接收者，则决定 835 转向“是”分支 838，于是，在步骤 840，检索评注，并且在评注插入点处将其提交（例如，显示等）给接收者。然后处理循环回去，以在文档中查找下一个评注插入点。

[0043] 返回至决定 835，如果不将评注导向所有接收者，则决定 835 转向“否”分支 848，于是，在步骤 850，解析评注接收者标签，以便确定接收者的标识符是否被包括在评注接收者标签中，或者接收者所属的组标识符之一是否被包括在评注接收者标签中。确定用户的标识符是否被包括在评注接收者标签中（决定 885）。如果用户的标识符被包括在评注接收者标签中，则决定 855 转向“是”分支 858，以处理评注。确定被导向接收者的评注是否被加密（决定 860）。如果评注被加密了，则决定 860 转向“是”分支 862，于是，在步骤 865，使用在步骤 805 中所检索的接收者的私有密钥来解密评注内容。在步骤 870，在评注插入点处把解密的评注内容呈现给接收者。然后处理循环回去，以查找文档中的下一个评注插入点。返回到决定 860，如果被导向接收者的评注未被加密，则决定 860 转向“否”分支 872，于是，在步骤 886，在评注插入点处把未加密的评注内容呈现给接收者。然后处理循环回去，以查找文档中的下一个评注插入点。

[0044] 返回至决定 855，如果用户的标识符未被包括在评注接收者标签中，则决定 855 转向“否”分支 876，用于进一步处理。判断评注接收者标签是否包括接收者所属的组标识符（决定 878）。如果评注接收者标签包括接收者所属的组标识符，则决定 878 转向“是”分支 880，于是，确定导向组的评注是否被加密（决定 882）。如果导向组的评注未被加密，则决定 882 转向“否”分支 884，于是，在步骤 886，在评注插入点处将未加密的评注内容呈现给接收者。然后处理循环回去，以查找文档中的下一个评注插入点。另一方面，如果导向组的评注被加密了，则决定 882 转向“是”分支 888，于是，在预定的过程 890，对加密的导向组的评注进行解密，并且将其呈现给用户（参见图 9 以及对于处理细节的相应文本）。然后处理循环回去，以查找文档中的下一个评注插入点。

[0045] 返回至决定 878, 如果用户不属于被包括在评注接收者标签中的任何组, 则决定 878 转向“否”分支 892, 于是, 在 894, 跳过评注, 并且不将其呈现给用户。然后处理循环回去, 以查找文档中的下一个评注插入点。

[0046] 上述处理继续查找字处理文档 585 中的评注, 直到不再存在要处理的评注。当已经处理了所有的评注时, 决定 832 转向“否”分支 892, 并且处理结束于 895。

[0047] 图 9 是示出了检索被导向一组接收者的加密的评注的步骤的示例流程图。处理开始于 900, 于是, 确定该用户的接收者包是否已经被解密。如果用户的接收者包还未被解密, 则决定 905 转向“否”分支 908, 于是, 在步骤 910, 在文档 585 中查找用户的加密的接收者包 925。在一个实施例中, 用接收者标识符标记用户的加密的接收者包。一旦查找到, 在步骤 920, 使用用户的私有密钥来解密用户的加密的接收者包, 并且将其作为解密的接收者包 930 存储在存储器区域中。返回到决定 905, 如果已经解密了用户的接收者包, 则旁路步骤 910 和 920, 决定 905 转向“是”分支 935。

[0048] 在步骤 940, 搜寻解密的接收者包来寻找在评注接收者标签中所发现的组标识符。判断该组是否是解密的接收者包 930 中所列的组之一 (决定 950)。如果该组是解密的接收者包 930 中所列的组之一, 则决定 950 转向“是”分支 955, 于是, 在步骤 960, 使用对应于该组的并且从用户的解密的接收者包中 930 所检索的组的私有密钥对加密的导向组的评注进行解密。确定使用所检索的组私有密钥对组评注的解密是否成功 (决定 970)。如果解密成功, 则决定 970 转向“是”分支 975, 于是, 在步骤 980, 在评注插入点处把解密的组评注呈现给接收者, 并且在 995, 处理返回至调用例程 (例如, 图 8)。另一方面, 如果解密不成功, 则决定 970 转向“否”分支 984, 于是, 在 990, 跳过评注, 并且不将其呈现给用户, 并且在 995 处, 处理返回至调用例程。返回至决定 950, 如果该组不是解密的接收者包 930 中所列的组之一, 则决定 950 转向“否”分支 988, 于是, 在 990, 跳过评注, 并且不将其呈现给用户, 并且在 995, 处理返回至调用例程。

[0049] 本发明的优选实现之一是客户端应用, 即, 可以存在于例如计算机的随机存取存储器中的代码模块中的指令 (程序代码) 的集合或其它功能的描述素材。在计算机需要之前, 可以将指令的集合存储在另一个计算机存储器中, 例如, 存储在硬盘驱动器中, 或者存储在诸如光盘 (用于 CD ROM 中的可能使用) 或者软盘 (用于软盘驱动器中的可能使用) 的可移除存储器中, 或者经由因特网或者其它计算机网络下载。因此, 本发明可以被实现为用于在计算机中使用的计算机程序产品。另外, 尽管在由软件选择性地激活或者重新配置的通用计算机中方便地实现了所述的各种方法, 然而本领域普通技术人员还将意识到, 可以在硬件、固件、或者在被构造用于进行所要求的方法步骤的更加专门化的装置中实现这样的方法。功能性描述素材是将功能性告知机器的信息。功能性描述示出包括但不限于计算机程序、指令、规则、事实、可计算函数的定义、对象以及数据结构。

[0050] 尽管已经示出和描述了本发明的具体实施例, 然而对于本领域技术人员很明显, 基于此处的教授, 在不脱离本发明及其较宽泛的方面的情况下, 可以进行变动与修改。因此, 所附权利要求将在其范围内涵盖只要处于本发明的真实精神与范围内的所有这样的变动与修改。而且, 应理解, 本发明仅由所附权利要求而限定。本领域技术人员将理解, 如果意指特定数量的所介绍的权利要求要素, 则将在权利要求中明确地阐述这一意图, 并且在不存在这样的阐述的情况下, 不存在这样的限制。对于非限制性的例子, 为了有助于理解,

以下所附权利要求包含对介绍性短语“至少一个 (at least one)”和“一个或多个 (one or more)”的使用,以介绍权利要求要素。然而,不应将这样的短语的使用认为是暗示具有不定冠词“一个 (a)”或者“一个 (an)”的权利要求要素的介绍将包含如此介绍的权利要求要素的任何具体的权利要求限制为仅包含一个这样的要素的发明,即使是当同一权利要求包括介绍性短语“一个或多个 (one or more)”或者“至少一个 (at least one)”以及诸如“一个 (a)”或者“一个 (an)”的不定冠词时也是如此,对于权利要求中使用定冠词的情况同样如此。

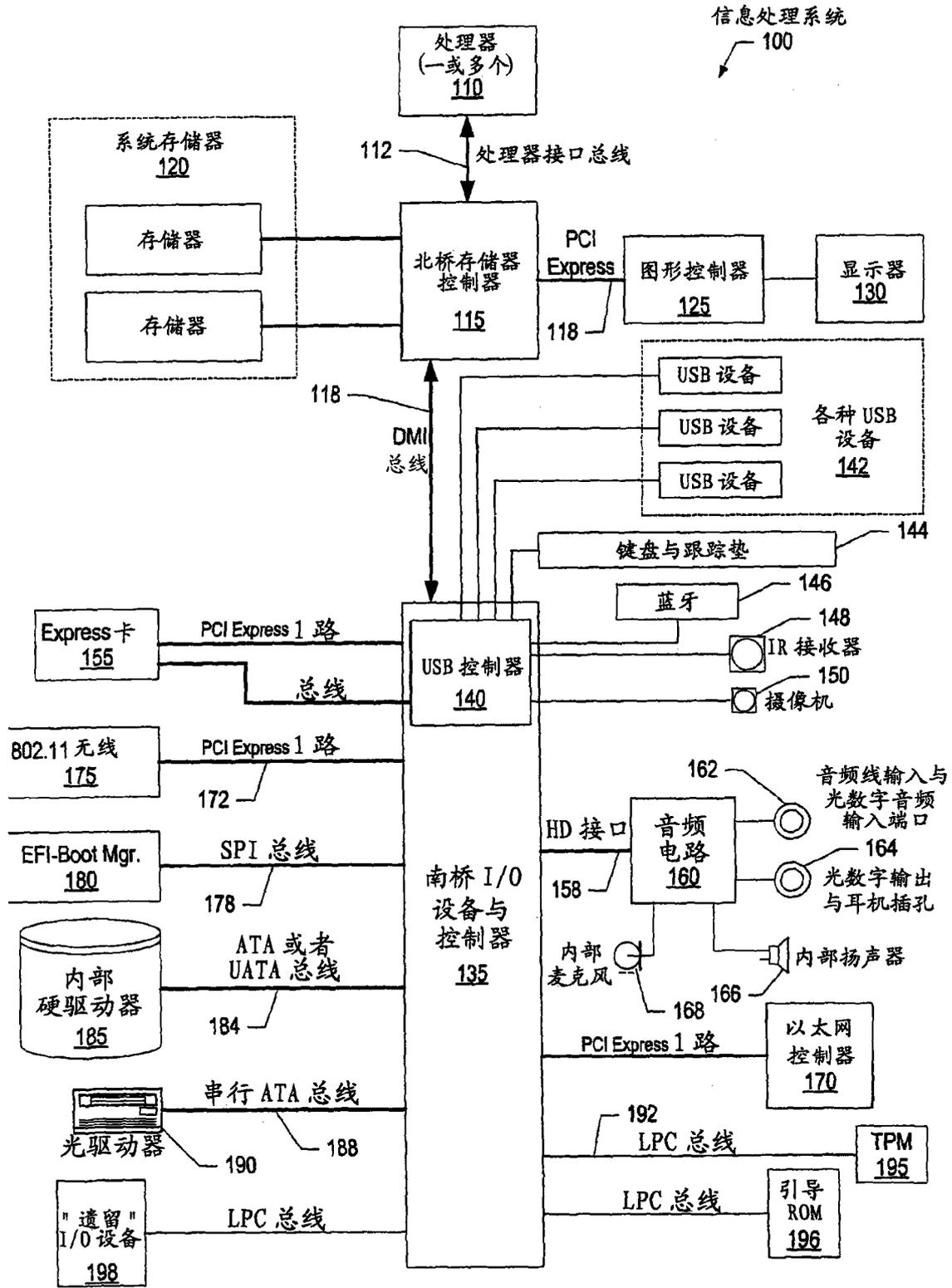


图 1

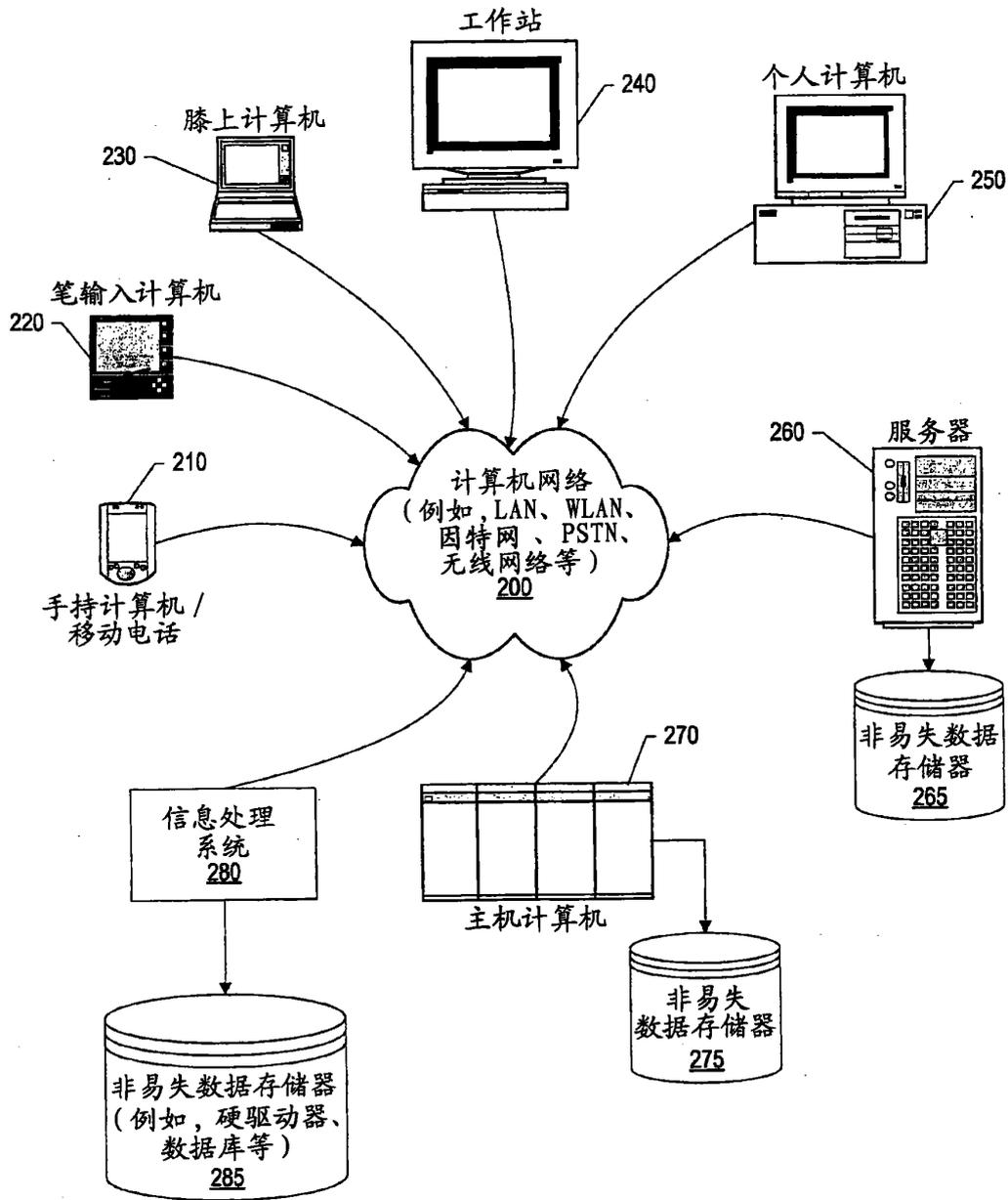


图 2

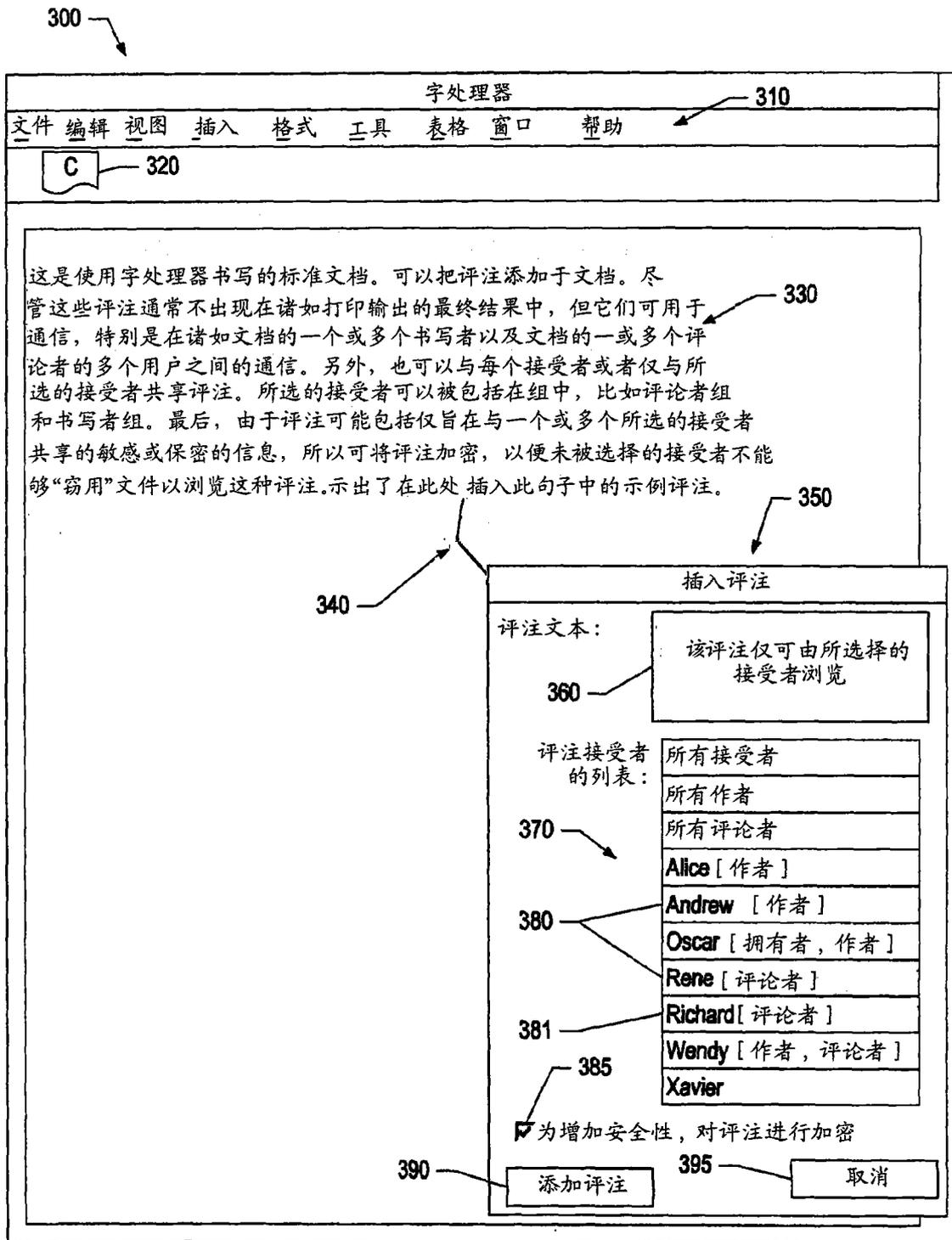


图 3

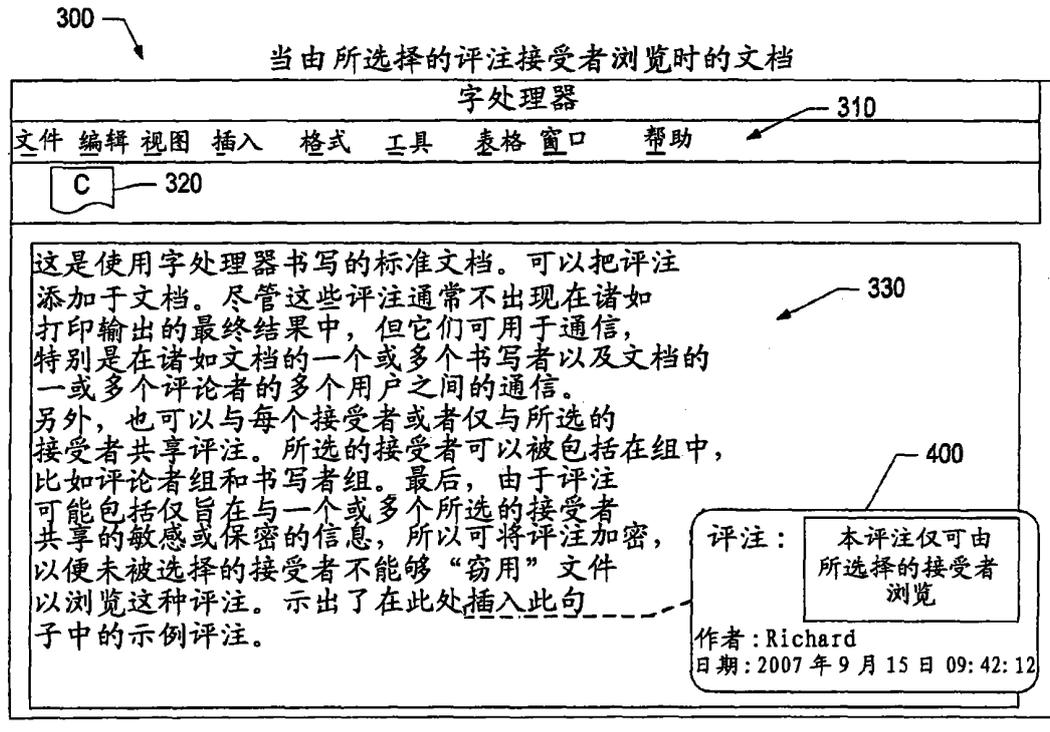


图 4A

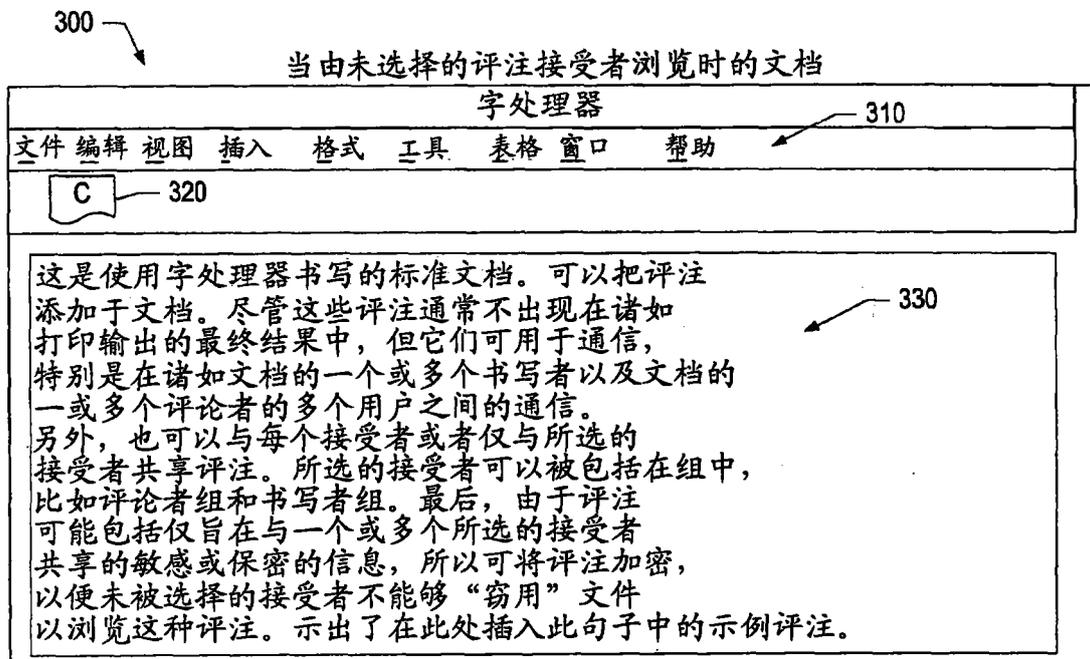


图 4B

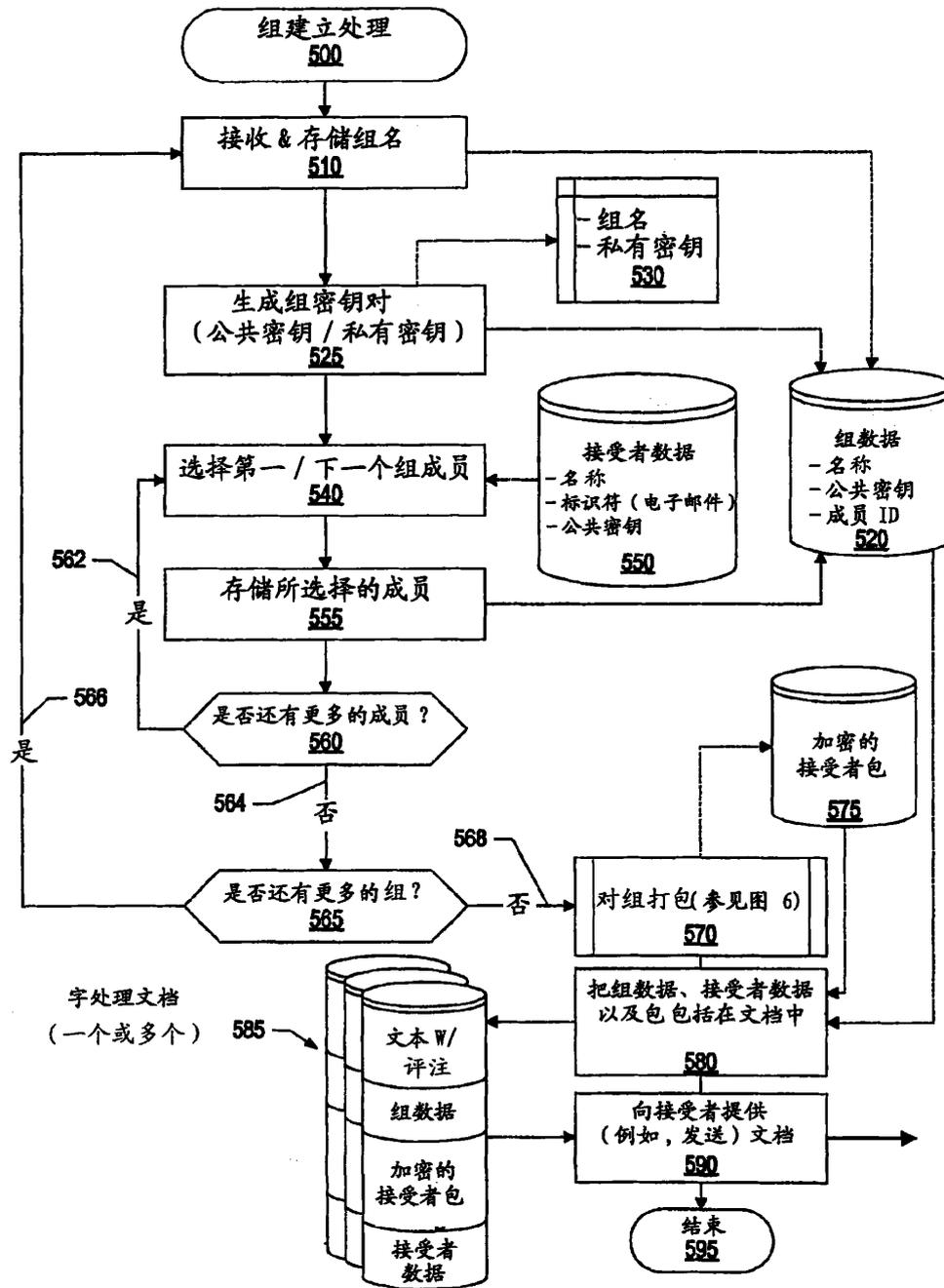


图 5

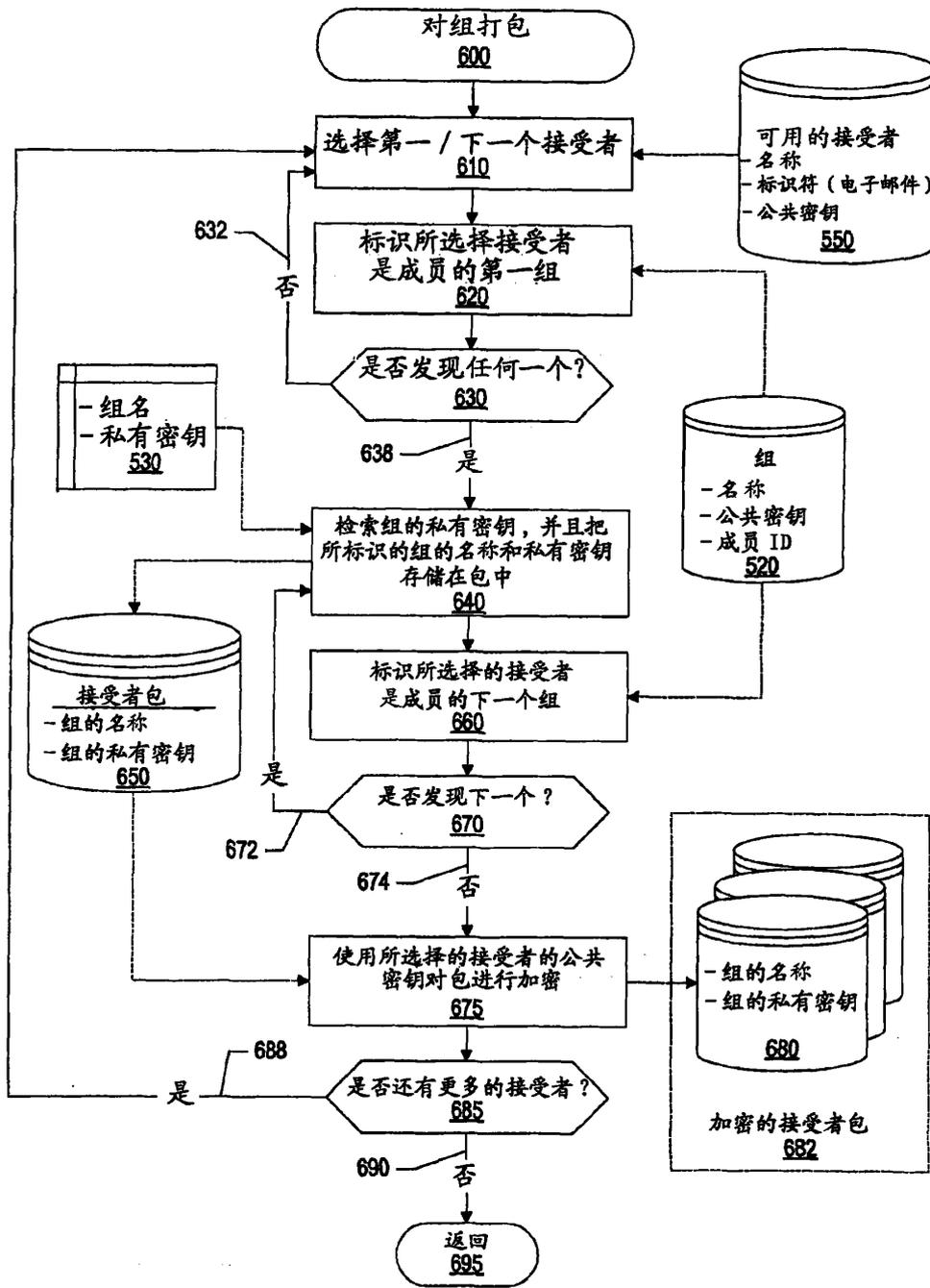


图 6

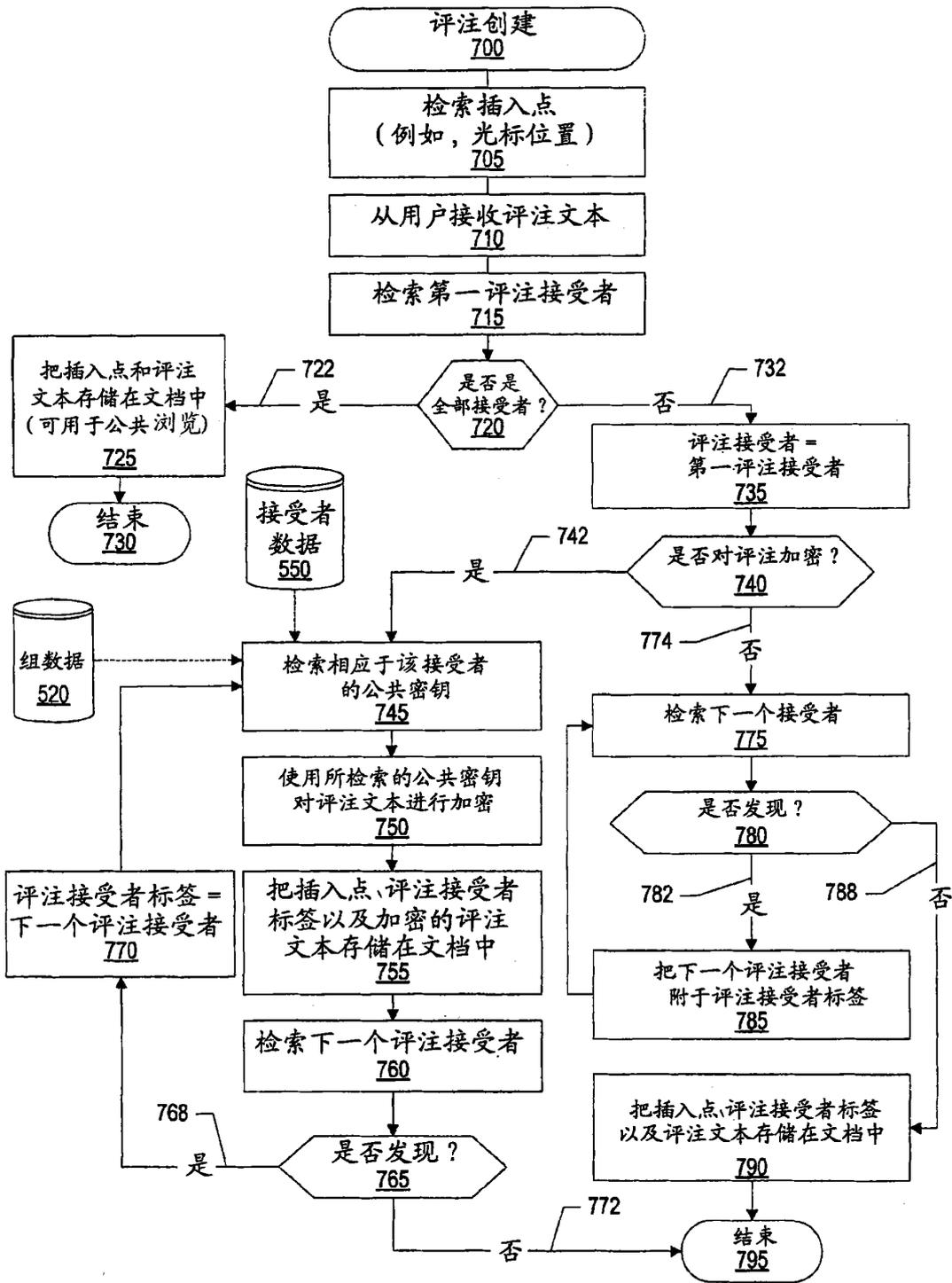


图 7

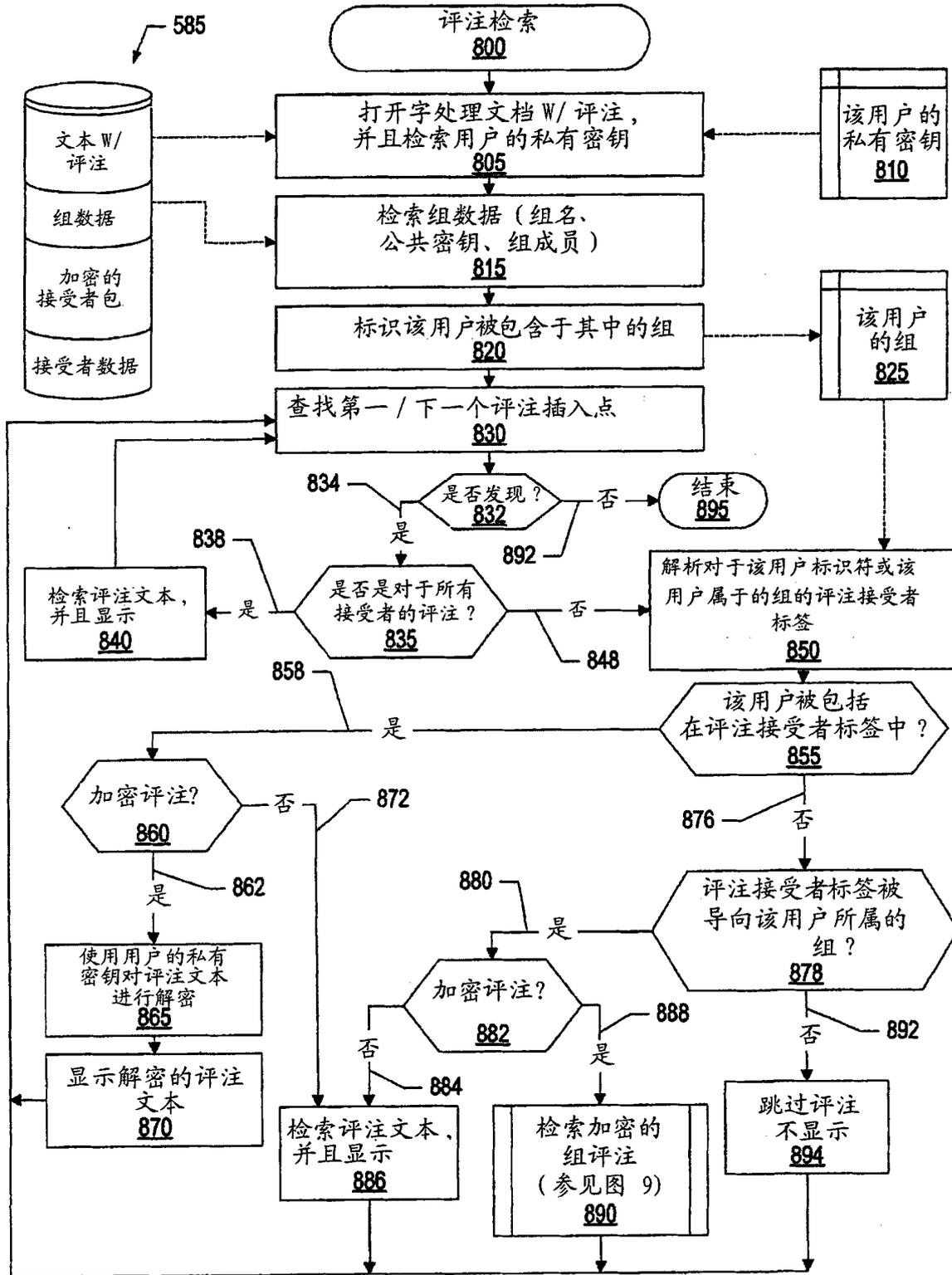


图 8

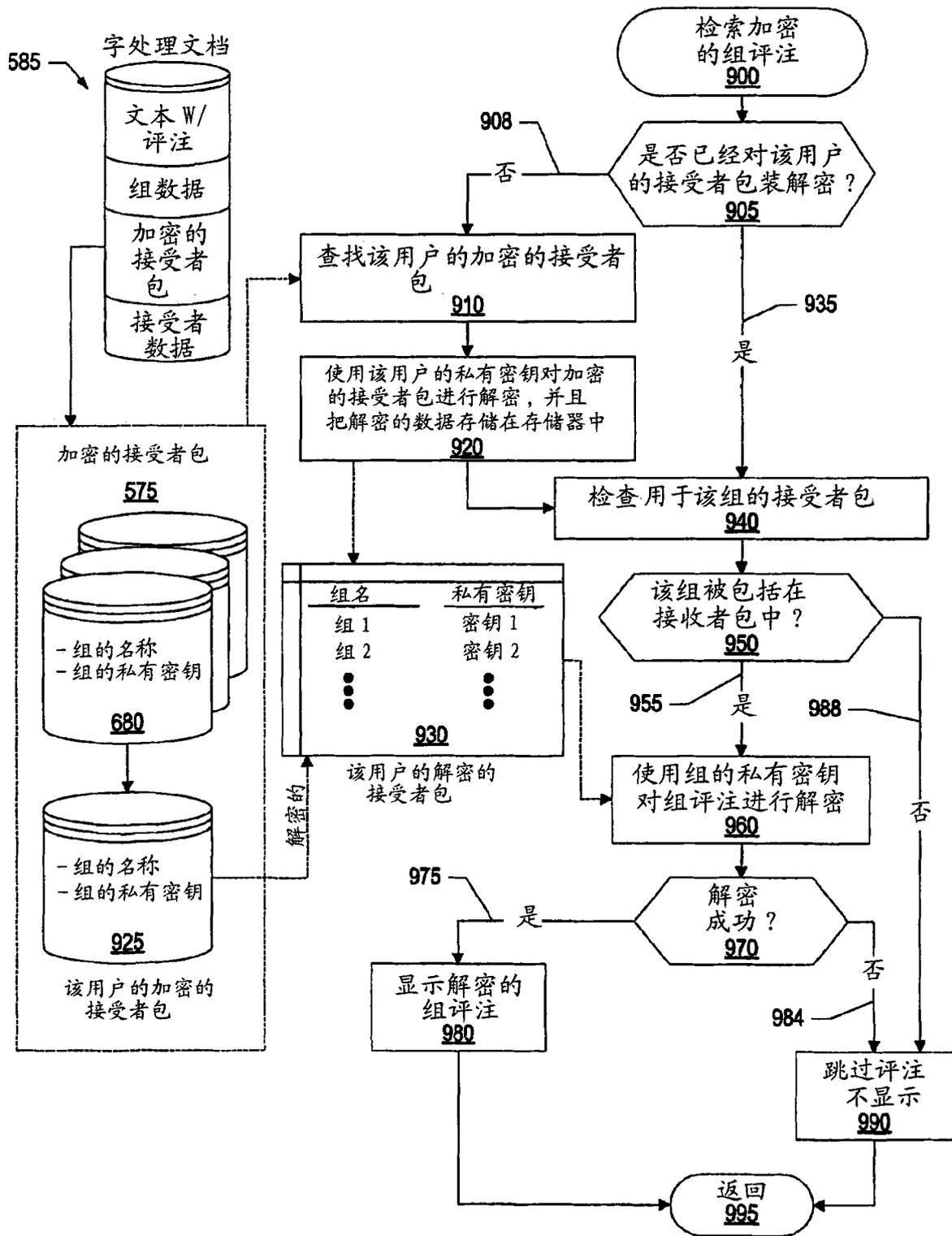


图 9