(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101228770 B
(45)授权公告日 2011.12.14

(21)申请号 200680027013.1
(22)申请日 2006.04.27
(30)优先权数据
05106928.4 2005.07.27 EP
(85)PCT申请进入国家阶段日
2008.01.23
(86)PCT申请的申请数据
PCT/EP2006/061873 2006.04.27
(87)PCT申请的公布数据
WO2007/014790 EN 2007.02.08
(73)专利权人 国际商业机器公司
地址 美国纽约
(72)发明人 F·英瑟蒂斯·卡罗
(74)专利代理机构 北京市金杜律师事务所 11256
代理人 朱海波
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
CN 1252198 A,2000.05.03, 全文.
CN 1481533 A,2004.03.10, 全文.
US 20050021984 A1,2005.01.27, 全文.
US 20030135740 A1,2003.07.17, 说明书第11段,58段,146段,165段,202段-213段,图3,图12.
审查员 秦晓芳

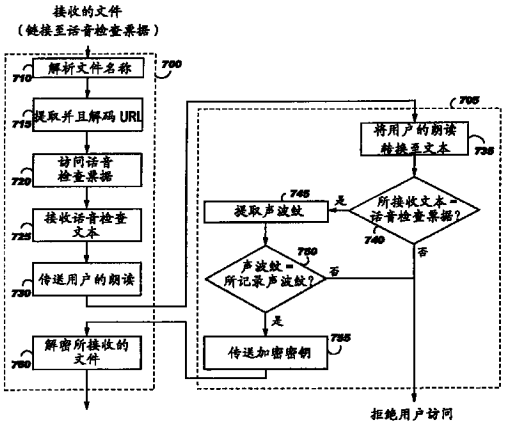
权利要求书 3 页 说明书 8 页 附图 5 页

(54)发明名称

用于将文件安全发送至被授权的接收者的方法和装置

(57)摘要

通过要求从网络服务器获取的加密接收文件的接收者大声朗读检查文本(其地址或者URL被编码于加密接收文件的文件名称内),本发明的系统自动检验接收者的身份,确认该文件已经由期望的接收者所接收,并且然后解密该文件。借助于自动语音识别组件来处理由接收者说出文本的说话方式。基于先前登记到系统的期望的接收者的话音,系统应用自动讲话者识别算法来确定诵读检查文本的人具有的声音特征是否匹配于期望的接收者的声音特征,在此情况下,系统确定所说出的文本是否对应于向朗读者呈现的检查文本。当系统确认接收者的标识之后,传送解密密钥,并且自动解密加密接收文件,并且向接收者显示该文件。在一个优选的实施方式中,系统记录并且标记有接收者诵读话音检查文本的时间戳,以便之后如果接收者否认接收时,可以与期望的接收者的话音比较。



CN 101228770 B

1. 一种对将在计算机网络中传送至期望的接收者的文件进行编码的方法，以便使用生物测定话音标识来认证所述接收者并且确认所述期望的接收者接收到所述文件，所述方法包括步骤：

- 选择加密密钥；

- 将话音检查票据与接收者的声波纹以及所述加密密钥相关联，所述话音检查票据包括声波纹 ID、所述加密密钥和话音检查文本；

- 确定包括至少所述加密密钥的所述话音检查票据的地址；

- 使用所述加密密钥来加密将要传送的所述文件；以及

- 在发送者端，将所述话音检查票据地址与所述文件相关联。

2. 根据权利要求 1 所述的方法，其中将所述话音检查票据地址与所述文件相关联的步骤包括在所述文件的文件名中编码所述话音检查票据地址的步骤。

3. 根据权利要求 1 所述的方法，其中选择加密密钥的所述步骤包括生成所述加密密钥的步骤。

4. 根据权利要求 2 所述的方法，其中选择加密密钥的所述步骤包括生成所述加密密钥的步骤。

5. 根据权利要求 1 所述的方法，其中选择加密密钥的所述步骤包括从另一计算机设备接收所述加密密钥的步骤。

6. 根据权利要求 2 所述的方法，其中选择加密密钥的所述步骤包括从另一计算机设备接收所述加密密钥的步骤。

7. 根据前述权利要求的任一项所述的方法，其中确定包括至少所述加密密钥的话音检查票据的所述地址的所述步骤包括生成所述话音检查票据的步骤。

8. 根据权利要求 1 至 6 的任一项所述的方法，其中确定包括至少所述加密密钥的话音检查票据的所述地址的所述步骤包括以下步骤：

- 传送所述加密密钥以及请求包括至少所述加密密钥的话音检查票据；以及

- 接收所述话音检查票据的所述地址。

9. 根据前述权利要求 1 至 6 的任一项所述的方法，其中所述话音检查票据进一步包括文本的一部分。

10. 一种用于将根据前述权利要求的任一项的方法编码的文件进行解码的方法，所述方法包括以下步骤：

- 从所述文件提取话音检查票据的所述地址，以及将所述话音检查票据地址解码；

- 在所述话音检查票据地址处访问与所述话音检查票据相关联的话音检查文本；

- 传送所述话音检查文本的朗读；

- 如果所述朗读的声波纹匹配于与所述话音检查票据相关联的声波纹，则接收解密密钥；以及

- 使用所述解密密钥来解密所述文件。

11. 根据权利要求 10 所述的方法，其中如果所述朗读的声波纹匹配于与所述话音检查票据相关联的所述声波纹并且如果所述朗读的所述文本匹配于与所述话音检查票据相关联的所述话音检查文本，则传送所述解密密钥。

12. 根据权利要求 10 或 11 所述的方法，其中所述话音检查票据的所述地址在所述文件

的名称中编码。

13. 一种用于对根据权利要求 1 至 9 的任一项的方法编码的文件的接收者进行认证的方法，包括以下步骤：

- 基于来自所述接收者的请求，传送与所述话音检查票据相关联的话音检查文本，其中连同所述请求接收所述话音检查票据的地址；

- 基于从所述接收者接收到的文本朗读，从所述文本朗读提取声波纹；

- 将所述提取的声波纹与关联于所述接收者的所述声波纹进行比较；以及

- 如果所述提取的声波纹匹配于与所述接收者相关联的所述声波纹，则向所述接收者传送与所述话音检查票据相关联的所述加密密钥。

14. 根据权利要求 13 所述的方法，进一步包括步骤：

- 基于从所述接收者接收到的文本朗读，将所述文本朗读转换至文本；

- 将所述转换的文本与关联于所述话音检查票据的所述话音检查文本进行比较；以及

- 如果所述提取的声波纹对应于与所述接收者相关联的所述声波纹并且如果所述转换的文本对应于与所述话音检查票据相关联的所述话音检查文本，则向所述接收者传送与所述话音检查票据相关联的所述加密密钥。

15. 根据权利要求 13 或 14 所述的方法，其中所述方法在服务提供者服务器之中实现。

16. 一种对将在计算机网络中传送至期望的接收者的文件进行编码的装置，以便使用生物测定话音标识来认证所述接收者并且确认所述期望的接收者接收到所述文件，所述编码的装置包括：

- 用于选择加密密钥的装置；

- 用于将话音检查票据与接收者的声波纹以及所述加密密钥相关联的装置，其中所述话音检查票据包括声波纹 ID、所述加密密钥和话音检查文本；

- 用于确定包括至少所述加密密钥的所述话音检查票据的地址的装置；

- 用于使用所述加密密钥来加密将要传送的所述文件的装置；以及

- 用于在发送者端，将所述话音检查票据地址与所述文件相关联的装置。

17. 根据权利要求 16 所述的编码的装置，其中用于将所述话音检查票据地址与所述文件相关联的装置包括用于在所述文件的文件名中编码所述话音检查票据地址的装置。

18. 根据权利要求 16 所述的编码的装置，其中所述用于选择加密密钥的装置包括用于生成所述加密密钥的装置。

19. 根据权利要求 17 所述的编码的装置，其中所述用于选择加密密钥的装置包括用于生成所述加密密钥的装置。

20. 根据权利要求 16 所述的编码的装置，其中所述用于选择加密密钥的装置包括用于从另一计算机设备接收所述加密密钥的装置。

21. 根据权利要求 17 所述的编码的装置，其中所述用于选择加密密钥的装置包括用于从另一计算机设备接收所述加密密钥的装置。

22. 根据前述权利要求 16 至 21 的任一项所述的编码的装置，其中用于确定包括至少所述加密密钥的话音检查票据的所述地址的所述装置包括用于生成所述话音检查票据的装置。

23. 根据权利要求 16 至 21 的任一项所述的编码的装置，其中用于确定包括至少所述加

密密钥的话音检查票据的所述地址的所述装置包括以下装置：

-用于传送所述加密密钥以及请求包括至少所述加密密钥的话音检查票据的装置；以及

-用于接收所述话音检查票据的所述地址的装置。

24. 根据前述权利要求16至21的任一项所述的编码的装置，其中所述话音检查票据进一步包括文本的一部分。

25. 一种用于将根据权利要求16至24的任一项所述的编码的装置编码的文件进行解码的装置，所述解码的装置包括以下装置：

-用于从所述文件提取话音检查票据的所述地址，以及将所述话音检查票据地址解码的装置；

-用于在所述话音检查票据地址处访问与所述话音检查票据相关联的话音检查文本的装置；

-用于传送所述话音检查文本的朗读的装置；

-用于如果所述朗读的声波纹匹配于与所述话音检查票据相关联的声波纹，则接收解密密钥的装置；以及

-用于使用所述解密密钥来解密所述文件的装置。

26. 根据权利要求25所述的解码的装置，其中所述话音检查票据的所述地址在所述文件的名称中编码。

27.-种用于对根据权利要求16至24的任一项的编码的装置编码的文件的接收者进行认证的装置，包括以下装置：

-用于基于来自所述接收者的请求，传送与所述话音检查票据相关联的话音检查文本的装置，其中连同所述请求接收所述话音检查票据的地址；

-用于基于从所述接收者接收到的文本朗读，从所述文本朗读提取声波纹的装置；

-用于将所述提取的声波纹与关联于所述接收者的所述声波纹进行比较的装置；以及

-用于如果所述提取的声波纹匹配于与所述接收者相关联的所述声波纹，则向所述接收者传送与所述话音检查票据相关联的所述加密密钥的装置。

28. 根据权利要求27所述的进行认证的装置，进一步包括以下装置：

-用于基于从所述接收者接收到的文本朗读，将所述文本朗读转换至文本的装置；

-用于将所述转换的文本与关联于所述话音检查票据的所述话音检查文本进行比较的装置；以及

-用于如果所述提取的声波纹对应于与所述接收者相关联的所述声波纹并且如果所述转换的文本对应于与所述话音检查票据相关联的所述话音检查文本，则向所述接收者传送与所述话音检查票据相关联的所述加密密钥的装置。

29. 根据权利要求27或28所述的进行认证的装置，其中所述进行认证的装置在服务提供者服务器之中实现。

用于将文件安全发送至被授权的接收者的方法和装置

技术领域

[0001] 本发明一般涉及电子文档的安全传递，并且更具体地涉及用于使用自动语音识别和生物测定话音讲话者标识来验证和确认期望的接收者接收到文件的方法和系统。

背景技术

[0002] 电子邮件允许个人（或者甚至自动机器人技术的机器）来将文本消息和其他信息（诸如，图片集合、声音记录以及格式化的文档）快速并容易地电子发送至世界上任何位置的其他电子邮件用户。在电子邮件附件中可以包括可作为文件访问的任何事物（例如，在硬盘文件夹中或者在网络共享的文件夹中）。电子邮件附件可以是图像、文档、电子制表、mp3 文件、程序等。一旦将文件附加至电子邮件，则电子邮件以及所附加的文件可以通过通信网络（例如，因特网）来传送至其他计算机系统。访问所附加文件的接收用户或者其他用户可将文件分离到本地系统存储用于进一步处理。

[0003] 关于在开放的并且不安全的网络（尤其是因特网）上交换电子信息的一个严重风险在于，冒充者可以截取电子通信或者访问诸如电子邮件的某些信息，并且将其自身伪装成为所述电子通信的被授权接收者。

[0004] 通常，需要将电子文档发送至期望的接收者，并且然后确保期望的接收者而不是其他不同人员已确实接收到所述文档。类似地，通常希望的是将电子文档发送至期望的接收者，并且然后在已经接收到所述文档之后，接收到期望的接收者确实打开并且查阅了所述文档内容的确认。

[0005] 通过验证并且确认期望的接收者接收到这种发送的文档来确保 向期望的接收者发送文档例如在各种法律或者安全相关的应用中可能是需要的。此外，在这种类型的应用中，通常希望接收者不能容易地抵赖 (repudiate) 曾经接收了或者查看了文档。

[0006] 在用于确保向期望的和被授权的接收者发送电子文档和文件（例如，附加到电子邮件的文件）、以及获得由期望的接收者的接收确认的先前方法中，存在某些缺陷。第一限制在于，通常发送确认不能肯定地证明接收者实际上已经查看、阅读或者另外注意到所接收文档的内容。例如，根据基于提供接收者私人信息、或者数字签名确认消息的现有方法，期望的接收者可以之后抵赖确认并且声称他或者她没有发送确认。例如，期望的接收者可以宣布其私人信息（诸如，密码）一定已经受到危害并且是由另一接收者提供的。另外，电子邮件的发送者可以接收电子邮件已经成功地发送至接收者的邮件服务器、并且该电子邮件已经被打开的自动确认，但是不验证和确认访问并且打开电子邮件附件的人员实际上是期望的被授权接收者；此外，不存在关于文档打开的任何确认，即，如果接收者（无论是期望的授权接收者或者另一人）实际上已经打开或者读取了由发送者附加到所传送电子邮件的文件或者文档。在这种情况下，期望的接收者可以确认已经接收了电子邮件，但是之后否认他们实际上知晓了电子邮件的内容和 / 或电子邮件附件文件的全部内容。

[0007] 尽管现代电子邮件系统的大多数能够配置电子邮件来向发送者传送确认由接收者接收以及打开电子邮件（假定，由期望的接收者）的消息，不存在等同的机制用于向发送

者通知由接收者已经打开了附加至电子邮件的文件。此外，没有提供机制以向电子邮件的发送者确保并且确认附加至电子邮件的所有文件（即使在已经将其分离并且保存用于未来的处理）已经由所述文件的授权期望的接收者打开和访问。

[0008] 结果，需要一种方法和系统，其能够使得附加至电子邮件的电子文档和文件的发送者能够以不可抵赖 (none-repudiable) 的方式确 保、验证和确认将那些文档和文件发送至期望的接收者。

发明内容

[0009] 由此，本发明的宽泛的目的在于克服如上所述的现有技术的缺点。

[0010] 本发明的另一目的在于，提供一种用于将电子文档和文件安全传送至期望的接收者的改进的方法和系统。

[0011] 本发明的另一目的在于，提供一种用于将电子文档和文件安全传送至期望接收者的改进的方法和系统，适用于在使得用户能够访问所述文件的内容之前验证请求访问所述文件的用户的身份。

[0012] 本发明的又一目的在于，提供一种用于将电子文档和文件安全传送至期望的接收者的改进的方法和系统，适用于向文件的发送者提供由期望接收者对文件内容的访问的不可抵赖的确认。

[0013] 本发明的又一目的在于，提供一种用于通过使用声波纹来将电子文档和文件安全传送至期望的接收者的改进的方法和系统。

[0014] 通过以下方法来实现这些以及其他相关的目的，该方法对将在计算机网络中传送至期望的接收者的文件进行编码，以便使用生物测定的话音标识来认证接收者并且所述期望的接收者接收到所述文件，所述方法包括步骤：

[0015] - 选择加密密钥；

[0016] - 将话音检查票据与所述加密密钥相关联；

[0017] - 确定包括至少所述加密密钥的所述话音检查票据的地址；

[0018] - 使用所述加密密钥来加密将要传送的所述文件；以及

[0019] - 将所述话音检查票据地址与所述文件相关联，

[0020] 通过用于将根据前述方法编码的文件进行解码的方法，所述方法包括：

[0021] - 从所述文件提取话音检查票据的所述地址，以及将所述话音检查票据地址解码；

[0022] - 在所述话音检查票据地址处访问与所述话音检查票据相关联的话音检查文本；

[0023] - 传送所述话音检查文本的朗读；

[0024] - 如果所述朗读的声波纹匹配于与所述话音检查票据相关联的所述声波纹，则接收解密密钥；以及

[0025] - 使用所述解密密钥来解密所述文件，

[0026] 以及通过用于对根据前述方法编码的文件的接收者进行认证的方法，包括步骤：

[0027] - 基于来自所述接收者的请求，传送与所述话音检查票据相关联的所述话音检查文本，其中连同所述请求接收话音检查票据的地址；

[0028] - 基于从所述接收者接收到文档朗读，

[0029] - 从所述文本朗读提取声波纹；

[0030] - 将所述提取的声波纹与关联于所述接收者的所述声波纹进行比较；以及

[0031] - 如果所述提取的声波纹对应于与所述接收者相关联的所述声波纹，则向所述接收者传送与所述话音检查票据相关联的所述加密密钥。

[0032] 通过对附图和详细说明的阅读，本发明的进一步优点将对于本领域技术人员变得清楚。期望的是在此结合任意附加的优点。

附图说明

[0033] 图 1 描述了根据本发明的方法，用户如何记录他 / 她期望向其发送文档的另一个人的话音的示例；

[0034] 图 2 示出了用于确定和存储声波纹的系统的示例；

[0035] 图 3 示出了根据本发明如何将与待发送的加密文件相关联的话音检查票据从发送者的计算机上传至话音检查服务器；

[0036] 图 4 示出了本发明的特定示例，其中发送者向电子邮件附加了链接到存储在话音服务器中的话音检查票据的加密文件；

[0037] 图 5 描述了当接收者接收到嵌入在话音检查票据的 URL 或者地址中的加密的文件时的话音检查票据的处理的示例；

[0038] 图 6 示出了用于加密将要传送的文档的一般算法的示例；

[0039] 图 7 示出了根据本发明的方法的主要步骤，用于确认期望的接收者接收到文件，用于验证接收者的身份，以及用于将加密密钥发送至授权的接收者；以及

[0040] 图 8 示出了用于解码文件名中地址的算法的示例。

具体实施方式

[0041] 根据本发明，公开了一种方法和系统，用于安全地对电子传送的文件进行访问、以及用于验证和确认期望的接收者（而不是其他人）已经接收并且打开所述文件。主要原理包括将加密密钥与接收者声波纹结合以便由接收者所接收的加密文件仅能由所述加密密钥来解密，如果此朗读的声波纹与接收者声波纹相对应，则在接收者朗读预定的文本之后将所述加密密钥传送至他 / 她。

[0042] 公知的是，大多数话音生物测定的方案创建了用户的声波纹，当用户由系统登记时创建的个人唯一的话音特征的模板。对系统进行访问的所有后续的尝试都需要用户讲话，以便他们的现场话音采样可以与预先记录的模板进行比较。例如，关于此主题的一个参考是由 Kanevsky 提交的名称为“Apparatus and method for speakerverification/identification/classification employing non-acoustic and/oracoustic models and database”的美国专利 6,529,871。

[0043] 图 1 描述了根据本发明的方法，用户如何记录他 / 她期望向其发送文档的另一个人的话音的示例。在此示例中，在话音记录的数据库中记录电话交谈的一部分。如所示出，具有电话 105 的用户 100 可通过标准公共交换电话网络 (PSTN)120 来呼叫具有电话 115 的用户 110。在此情况下，用户 100 是指发送者而用户 110 是指接收者。在呼叫期间，发送者 100 可记录谈话的一部分，以便之后确定接收者 110 的声波纹。在优选的实施方式中，发送

者 100 在话音记录数据库中存储接收者话音记录。同样，在优选的实施方式中，每个接收者话音记录包括接收者的姓名、接收者声波纹的标识符以及接收 者话音的记录，如由标记 125 所示出。话音记录的数据库可以在发送者的计算机或者手持设备 130 中本地存储、或者在通过公共网络（例如，因特网或者私有网络）可访问的远程服务器（未示出）中存储。

[0044] 在已经记录了接收者的话音的采样之后，发送者必须确定接收者的声波纹。这可以在普通的服务器上或者在特定话音检查服务器上本地执行。为了图示，如图 2 所示，在特定的话音检查服务器上执行声波纹的确定和声波纹存储。在发送者 100 已经将接收者的话音采样作为接收者话音记录进行存储之后，通过私有网络或者公共网络 200（例如，因特网）来向特定话音检查服务器 205 完全地或者部分地发送采样。同样，在优选的实施方式中，将话音的采样作为匿名音频文件来传送。话音检查服务器 205 处理话音采样，计算并且存储接收者的声波纹，并且对声波纹指定标识符 (ID)。在话音数据库 210 中本地存储声波纹以及相关联的 ID。声波纹 ID 然后传送至对其进行本地存储的发送者的计算机 130。例如，如上所述，声波纹 ID 可存储在接收者话音记录 125 之中。

[0045] 为了加密将要发送的文件，发送者 100 必须首先获得接收者的话音采样以及上述的声波纹 ID。然后优选地，发送者创建话音检查票据。发送者还可以向话音检查服务器或者第三方服务器要求话音检查票据。话音检查票据主要包括声波纹 ID、加密密钥和话音检查文本。由发送者使用与话音检查票据相关联的加密密钥以加密将要传送的文件。然后，话音检查票据传送至话音检查服务器，所述话音检查服务器传送回话音检查票据的地址或者 URL（例如，可以从其下载话音检查票据的地址）。话音检查票据的地址或者 URL 在将要传送的编码的文件的名称之中编码。

[0046] 图 3 示出了根据本发明如何将与将要发送的加密文件相关联的话音检查票据从发送者的计算机 130 上传至话音检查服务器 205。在发送者的计算机已经将话音检查票据传送至话音检查服务器之后，话音检查票据优选地存储在话音检查服务器 205 的话音检查票据数 据库 300 中。如所示，话音检查服务器 205 通过发送话音检查票据的地址或者 URL（即，从其可以下载话音检查票据的地址或者 URL）来响应于发送者的计算机 130。优选地，地址或者 URL 存储在发送者的计算机 130 中的话音检查票据的本地副本的保留字段之中。

[0047] 图 4 示出了本发明的应用的示例，其中发送者 Lewis Carroll 将链接到存储在话音检查服务器中的话音检查票据的加密文件附加至电子邮件。当接收到电子邮件时，话音检查票据必须由接收者 (JaneR.Friday) 访问，用于验证她的身份、用于确认文件的接收、以及用于解密该文件。该图还示出可以如何使用特定的词典编纂来在所附文件的名称之中编码话音检查票据的地址或 URL（例如，超链接“http://www.voicecheck.com/tickets/R7KWW56T.vct”）。例如，特殊的词典编纂包括，分别通过在文件名称的词典编纂中有效的字符（如，“；”和“,”）来替换在 URL 的词典编纂中有效的字符或者字符组（如“://”和“/”）。根据本发明，当电子邮件接收者点击链接到话音检查票据的文件附件的图标时，解析附加文件的名称、并且提取话音检查票据的 URL 并且从相同的文件名称解码。使用所提取的 URL，触发超链接，用于在话音检查服务器上访问和执行话音标识和话音检查票据有效操作，该操作对于验证期望的接收者接收文件，以及对于从话音检查服务器获取解密所接收文件所需的加密密钥来说是所需的。

[0048] 图5描述了当接收者接收到嵌有话音检查票据的URL或者地址的加密文件时的话音检查票据处理的示例。当接收者110在话音检查服务器205的话音检查票据数据库300中访问话音检查票据时，从话音检查服务器提取话音检查票据的话音检查文本、并传送至接收者的计算机或者手持设备400。显示所接收的话音检查文本，并且向接收者110提示大声读出此文本，用于执行文件接收确认和接收者身份认证。如上所述，向接收者提示大声读出话音检查文本以便通过语音识别和话音标识来验证所述接收者是允许打开文件的人。当接收者大声读出所接收的话音检查文本时，接收者110的说话方 式优选地记录在接收者的计算机400上，并且传送至话音检查服务器205。在话音检查服务器205上接收的说话方式由语音识别来解码、并且与话音检查票据的话音检查文本部分进行比较。另外，计算所接收的说话方式的声波纹，并且将其与相同声波纹ID相对应的记录的声波纹文件进行比较。如果两个检查的结果是肯定的，则验证期望的接收者的身份，并且将加密密钥传送至接收者的计算机400用于解密文件。通过访问和获取在话音检查服务器205上存储的话音检查票据，发送者100得到了期望接收者110接收文件的不可否认的确认，或者可以意识到由非授权接收者或者冒名者打开文件的不成功尝试。

[0049] 图6示出了用于加密将要传送的文档的一般算法的示例。根据其实现，该算法可以划分成为在一个或者不同计算机或者服务器上运行的多个模块。根据图6的示例，该算法划分成为三个不同部分，发送者的计算机模块600（或者对于发送者可访问的网络服务器）、安全服务器模块605、以及话音检查服务器模块610。在通过输入接收者名称而已经选择了应该将文档或者文件传送至的接收者的名称之后，在列表中、或者根据类似的已知接口方法来选择名称（步骤615），发送者的计算机模块600确定是否已经存在所选择的接收者的声波纹（步骤620）。例如，发送者的计算机模块600可以管理表格，其中接收者姓名与接收者标识符（ID）相关联，以便这样的ID可以用来选择在话音检查服务器中存储的声波纹数据库中的特定声波纹。根据这样的示例，检查接收者声波纹是否存在包括检查在表格中出现的接收者名称。如果不存在用于选择的接收者的声波纹，则发送者的计算机模块600经由网络接口、电话系统或者等效的系统来接收接收者记录（步骤625）。接收者记录被传送话音检查服务器模块610，从其接收相应的ID（步骤630）。话音检查服务器模块610从所接收的接收者记录提取声波纹、确定ID、并且在声波纹数据库中存储带有相应ID的声波纹（步骤635）。应该注意，可替换地，接收者可以将他/她的话音的音频记录直接传送至话音检查服务 器模块610。

[0050] 如果声波纹已经与所选择的接收者相关联，则发送者的计算机模块600向安全服务器模块605发送针对加密密钥和话音检查票据（VCT）的请求（步骤640）。如上所述，安全服务器模块605可以与发送者的计算机模块600合并，以便在发送者的计算机中生成加密密钥，并且还由发送者的计算机创建话音检查票据。安全服务器模块605生成将由标准预定的加密算法使用的加密密钥（步骤645），例如诸如RSA的公共密钥算法。由发送者的计算机模块600接收加密密钥（步骤650），所述发送者的计算机模块600使用该加密密钥来加密将要发送的文件（步骤655）。另外，安全服务器模块605生成话音检查票据（步骤660）。如上所述，每个话音检查票据优选地包括声波纹ID、加密密钥和话音检查文本。声波纹ID由发送者的计算机模块600根据所选择的接收者来确定，而加密密钥和话音检查文本由安全服务器模块605来确定。根据标准密钥生成算法来随机地生成加密密钥。可以以不

同方式生成话音检查文本。例如，可由发送者来写出话音检查文本，诸如由接收者接收加密文件的公告确认。还可以由发送者选择话音检查文本，例如通过复制附加所加密文件的电子邮件文本的一部分。可替换地，可以由话音检查服务器 610 来自动生成话音检查文本，例如，通过从所述服务器所访问的或者存储的文档库来随机地选择文本。

[0051] 然后，话音检查票据传送至话音检查服务器模块 610（步骤 655），以便在话音检查票据数据库中存储（步骤 670）。话音检查服务器模块 610 将存储的话音检查票据的地址或者 URL 返回至安全服务器模块 605（步骤 675），安全服务器模块 605 接着将所存储的话音检查票据的地址或 URL 传送至发送者的计算机模块 600（步骤 665）。然后，在发送者的计算机模块 600 中，所存储的话音检查票据的地址或者 URL 在将要传送的文件的名称之中编码（步骤 680）。然后，由于所述文件被编码并且包含允许期望的接收者将其解密的信息，所述文件准备被传送。

[0052] 图 7 示出了根据本发明的所述方法的主要步骤，用于确认期望的接收者接收到文件，用于验证接收者的身份，以及用于将加密密钥发送至授权的接收者。在优选的实施方式中，这种算法包括两个不同部分，第一部分是指在接收者的计算机或者手持设备中执行的部分 700，以及第二部分是指在话音检查服务器中执行的部分 705。在已经接收到根据本发明的方法而加密的文件之后（诸如参考图 6 所述，例如作为电子邮件的附件），解析文件名称（步骤 710），并且从解析的文件名称提取和解码话音检查票据的地址或者 URL（步骤 715）。根据用于编码步骤的词典编纂来从解析的文件名称提取和解码地址或者 URL。在此下文中描述编码和解码的词典编纂的示例。一旦已经恢复地址或者 URL，则访问话音检查票据（步骤 720），以便接收包含在此话音检查票据中的话音检查文本（步骤 725）。在接收者计算机显示器上显示话音检查文本，以便接收者可以大声朗读该文本。接收者的朗读作为音频信号（或者是模拟信号或者是数字信号）传送至话音检查服务器（步骤 730）。根据标准语音识别引擎，由话音检查服务器将所接收的音频信号转换至文本（步骤 735），并且执行测试以比较所转换的文本和话音检查文本（步骤 740）。如果转换的文本不同于话音检查文本，则拒绝接收者的请求；否则，如果转换的文本等于话音检查文本，则计算所接收的语音信号的声波纹（步骤 745）。然后，将此声波纹与关联于存储在话音检查服务器的声波纹数据库中的接收者标识符的声波纹进行比较（步骤 750）。例如，接收者标识符可通过由接收者自身随音频记录来传送。如果声波纹不同，则拒绝接收者的请求；否则话音检查服务器将加密密钥传送至接收者的计算机或者手持设备（步骤 755），以便由接收者的计算机解密所接收的文件（步骤 760）。在本发明的特定优选实施方式中，由话音检查服务器将话音检查票据的话音检查文本自动修改至不同的文本，从而，对于访问文件的每次尝试，将不同的话音检查文本传送至接收者用于标识。根据此实施方式，当已经识别了接收者并且解密密钥已经发送至接收者时，修改话音检查文本。可 替换地，在本发明的另一实施方式中，一旦已经将接收者识别、并且已经第一次将解密密钥发送至接收者，则自动擦除接收者检查票据、并且从话音检查服务器丢弃，从而，一旦已经第一次解密所述文件，则用以解密相同文件的进一步尝试将失败。

[0053] 为了对将要传送的文件的名称之中的地址或者 URL 进行编码，确定特定的词典编纂，以便避免由文件系统禁止的特殊字符，例如，Microsoft Windows 系统禁止使用“\”(Windows 是 Micrisoft 公司的商标），和 / 或编码地址以便降低它们的大小。将被编码

的地址可以是任意形式，例如，本地地址、私有网络中的地址或者因特网地址，然而，为了图示，在下文的描述中给出的示例是基于 URL 类型的地址。

[0054] 图 8 示出了用以编码文件名称中的地址的算法的示例。如图 8a 所示，第一步骤包括获得文件的基本名称（步骤 800），即，文件的文件名、以及话音检查票据的地址或者 URL（步骤 805）。然后，将地址编码（步骤 810），并且在由包含基本文件名和编码的地址的文件名将文件重命名（步骤 820）之前，使用特殊分隔符来将地址与文件的基本文件名称合并（步骤 815）。

[0055] 图 8b 描述在图 8a 中表示为步骤 810 的编码算法的示例。将变量 i 设置为零（步骤 825），并且从地址串提取第 i 个字符（步骤 830）。执行测试以确定所提取的字符是否有效，或者另外由用户的设备的文件系统所强加的文件名语法规则所禁止（步骤 835）。如果所提取的字符是文件名有效字符，则变量 i 以一递增（步骤 850），并且执行测试以确定变量 i 是否达到其最大值，即，是否已经处理了地址串的所有字符（步骤 855）。如果变量 i 没有到达其最大值，则重复算法的最后四个步骤（步骤 830 至 850）。否则，如果变量 i 已经到达其最大值，则停止处理。如果从地址串提取的字符被文件名称语法规则所禁止，则在词典编纂表 845 中选择相应的有效字符或者字符组，并且此选择的字符或者字符组替换被禁止的字符或者字符组（步骤 840）。然后，将变量 i 以一递增，并且执行与前述相同的测试以 确定变量 i 是否已经到达其最大值。

[0056] 如上述算法示出，让我们考虑命名为“Biometric.txt”的文本文件的情况，用户希望将所述文件作为加密的电子邮件附件向其他某人发送，出于此目的使用词典编纂表来将话音检查票据地址串编码成为文件名，其中：

[0057] “://”关联于“；”

[0058] “/”关联于“,”

[0059] 为了获得允许文件打开的话音检查票据，需要访问与此文件相对应的话音检查票据。为了图示，可以考虑能够从以下 URL 下载此话音检查票据：

[0060] http://www.voicecheck.com/tickets/R7KWW56.vct

[0061] 在文档“Biometric.txt”的发送者发送或者附加所述文档之前，可以选择诸如“加密文件”的选项以加密文件，以便生成话音检查票据，并且用以获取此话音检查票据的地址或者 URL。

[0062] 根据图 8 所示出的算法来修改文件名。首先，通过先前的词典编纂表将地址编码如下：

[0063] http ;www.voicecheck.com, tickets, R7KWW56.vct

[0064] 然后，将编码的地址与文件名称合并。在此示例中，编码的地址被包括在用作分隔符的括号内。编码的地址插入到基本文件名的扩展点的前部，如下：

[0065] Biometric(http ;www.voicecheck.com, tickets, R7KWW56.vct).txt 并且使用修改的文件名来重命名该文件。

[0066] 必须注意，为了图示，此编码算法目的非常简单。一个优选的方式将包含，由单一字符来替换禁止字符的序列，以及以更为紧凑的代码来替换多组字符，例如由“H！”来替换“http://”。

[0067] 在本发明的优点之中，应该注意：

[0068] - 发送者保护发送至接收者的文件，确保并且获得那些文件仅由期望的接收者打开的确认；

[0069] - 文件的发送者获得由期望的接收者接收到所述文件的不可否 认的确认，并且针对由非授权的接收者或者冒名者打开文件的不成功尝试而获得通知；以及

[0070] - 记录他或者她自己的话音，任何用户可选择性地保护任意文件免受其他人员的非授权访问。

[0071] 当然，为了满足局部的和特定的要求，本领域技术人员可以对上述方案应用多种修改和替换，然而，所有这些修改和替换都包括在由以下权利要求书所限定的本发明的保护范围之中。

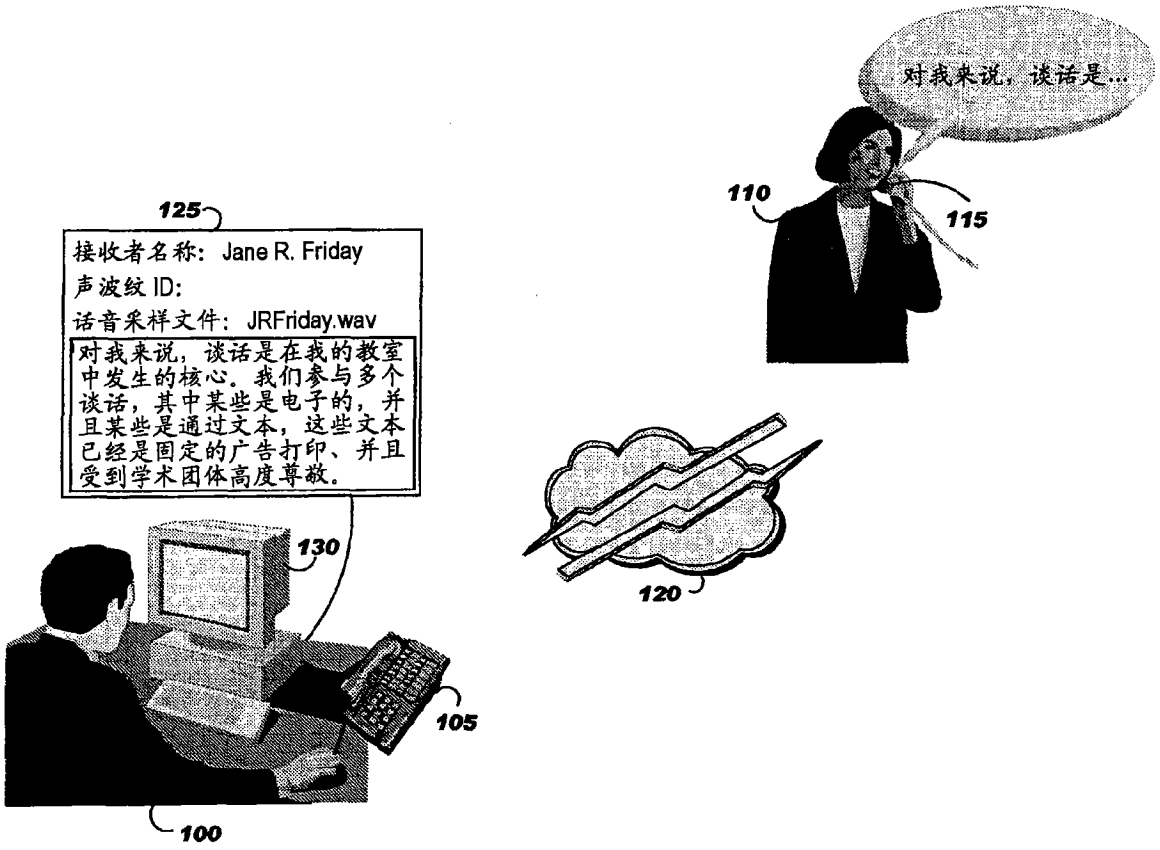

对我来说，谈话是...
110
115
125
接收者名称：Jane R. Friday
声波纹 ID:
话音采样文件：JRFriday.wav
对我来说，谈话是在我的教室中发生的核心。我们参与多个谈话，其中某些是电子的，并且某些是通过文本，这些文本已经是固定的广告打印、并且受到学术团体高度尊敬。
130
105
100
120

图 1

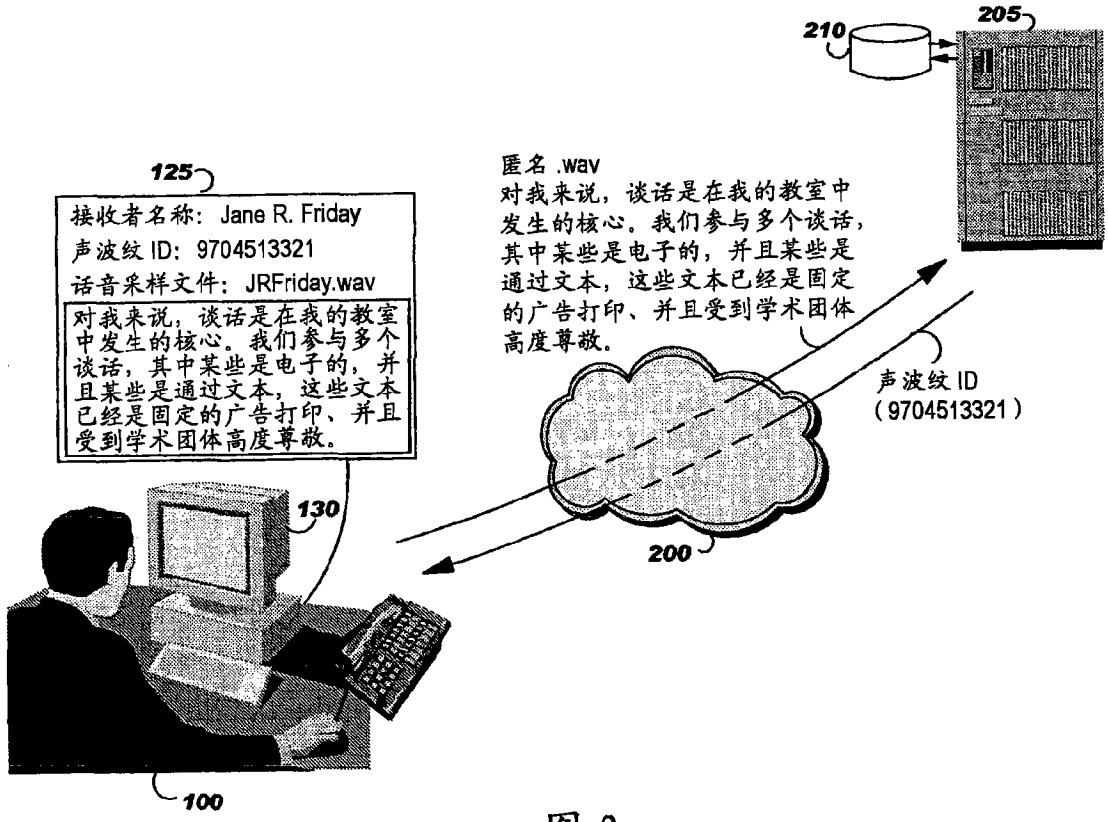

205
210
匿名 .wav
对我来说，谈话是在我的教室中发生的核心。我们参与多个谈话，其中某些是电子的，并且某些是通过文本，这些文本已经是固定的广告打印、并且受到学术团体高度尊敬。
125
接收者名称：Jane R. Friday
声波纹 ID：9704513321
话音采样文件：JRFriday.wav
对我来说，谈话是在我的教室中发生的核心。我们参与多个谈话，其中某些是电子的，并且某些是通过文本，这些文本已经是固定的广告打印、并且受到学术团体高度尊敬。
声波纹 ID
（9704513321）
130
100
200

图 2

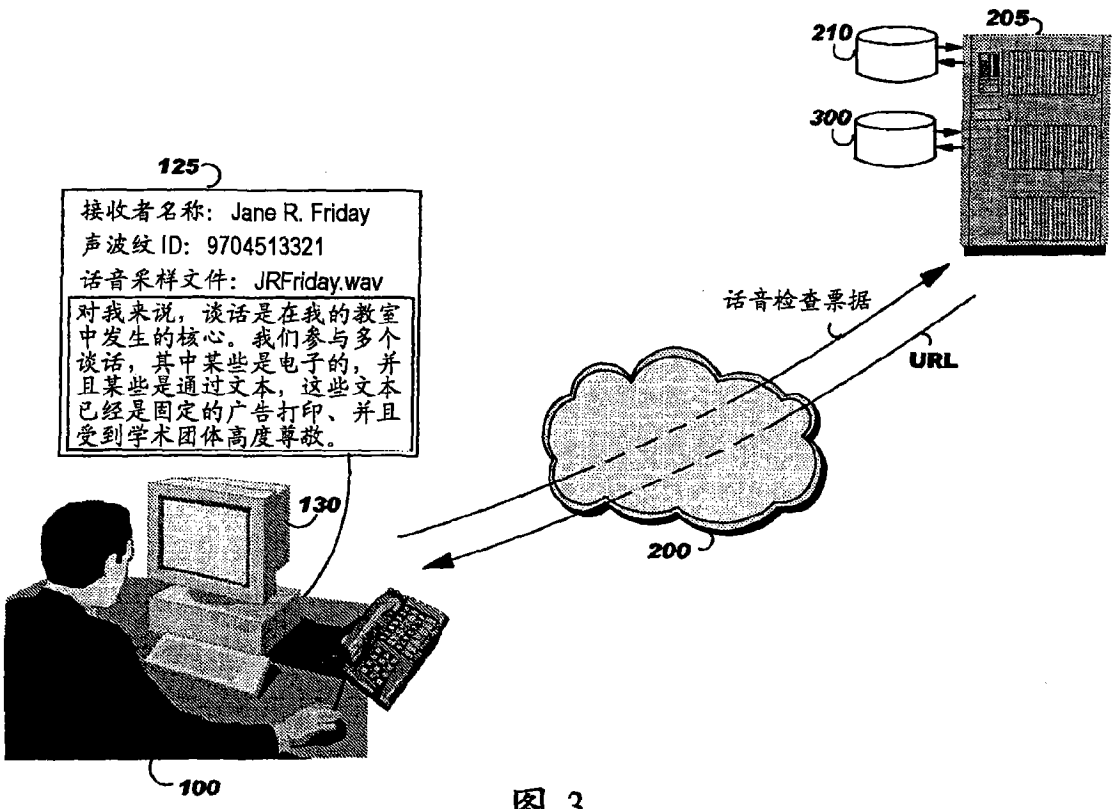


图 3

Lewis-Carroll@icm.com 02/09/2005 18：33	收件人：jfriday76@yahoo.com 抄送： 主题：谈话生物测定

Jane：

谈话生物测定将声学的谈话者检验与谈话知识检验进行结合，以便做出更为准确的标识确定。为了管理附加的复杂性水平，引入了多形式的用户识别方法，我们的研究提出了以可用以编程策略管理器的有限状态机形式的使用检验策略。一旦写出了检验策略，则策略管理器在进行时（on the fly）解译策略管理器，并且在会话正在进行时动态确定是否接受用户、拒绝用户或者继续交互并且采集更多数据。

我附加了这个描述我们最后的实验性结果的话音加密的文件，用于你的分析和评估。

谈话 _ 生物测定（http;www.voicecheck.com,ticket,R7KWW56T.vct）.doc

此致，
Lewis Carroll

图 4

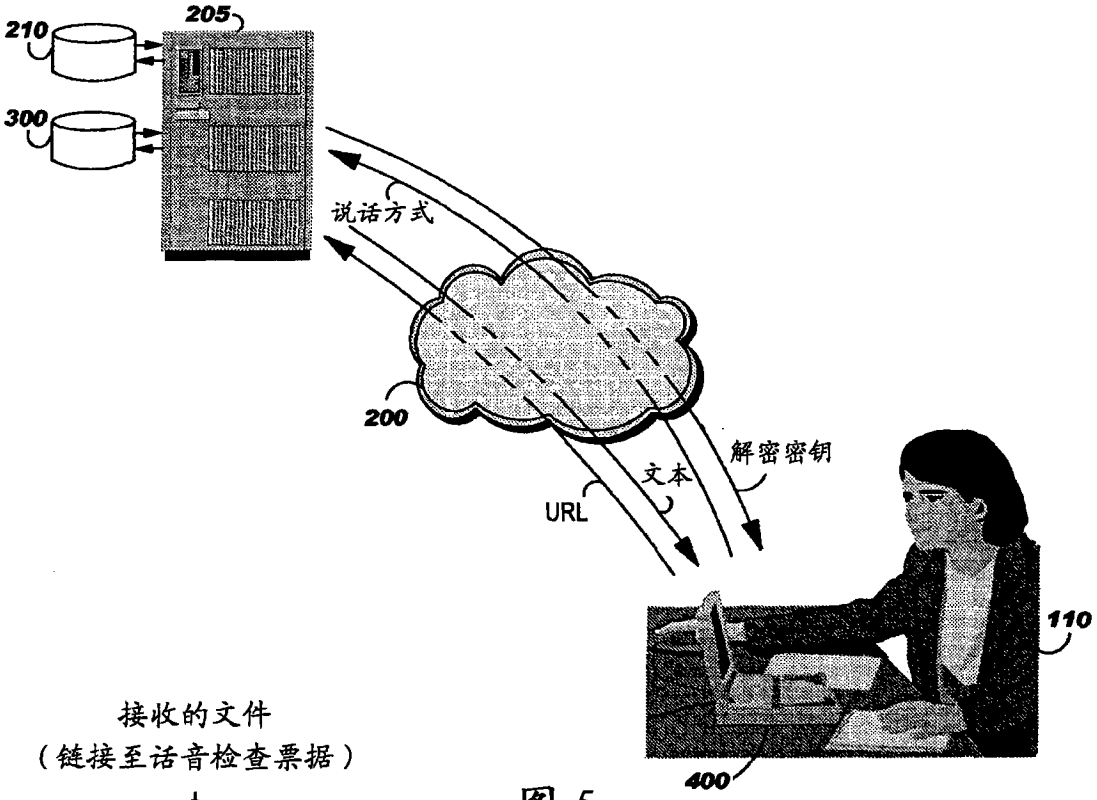

205
210
300
说话方式
200
解密密钥
文本
URL
110
400

图 5

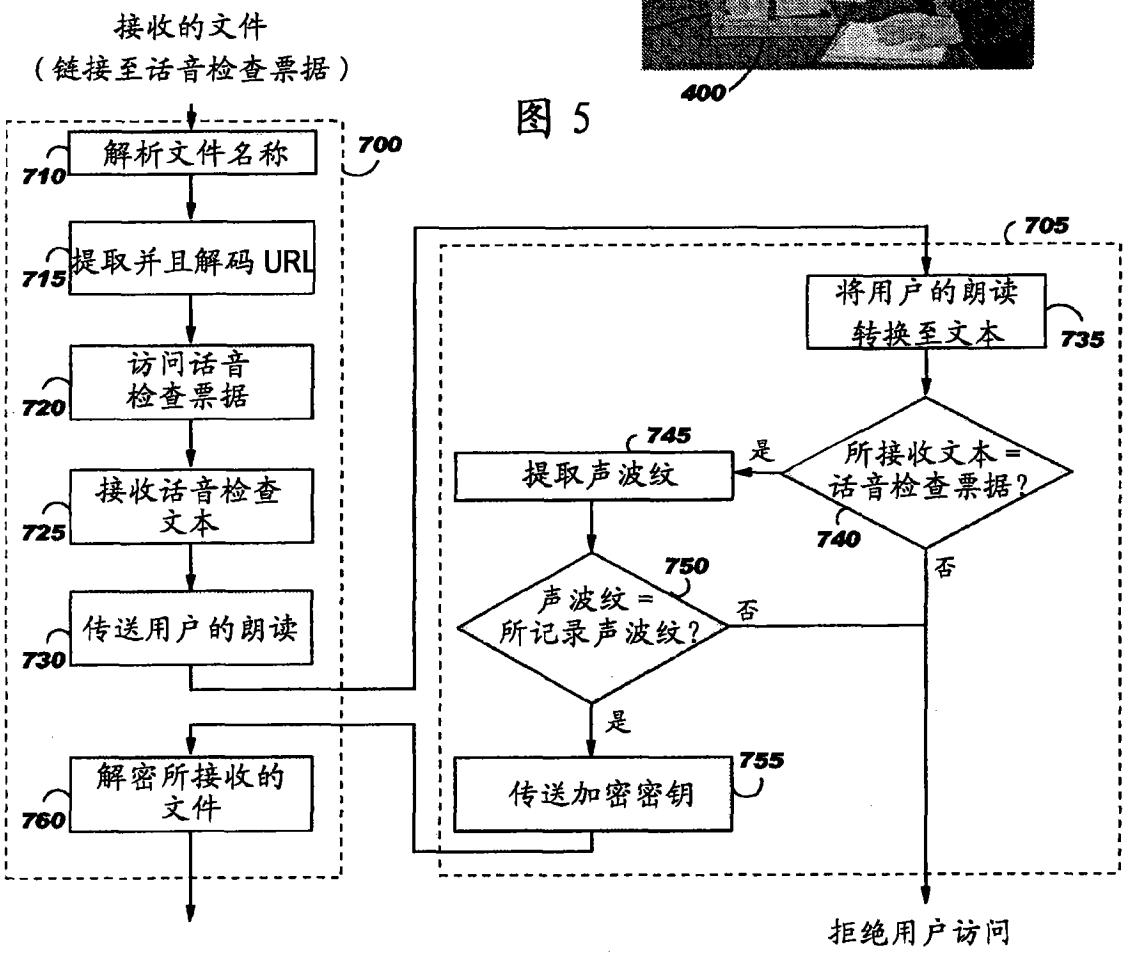

接收的文件
（链接至话音检查票据）
700
710
解析文件名称
715
提取并且解码 URL
720
访问话音
检查票据
725
接收话音检查
文本
730
传送用户的朗读
760
解密所接收的
文件
705
735
将用户的朗读
转换至文本
745
提取声波纹
是
740
所接收文本 =
话音检查票据?
否
750
声波纹 =
所记录声波纹?
否
是
755
传送加密密钥
拒绝用户访问

图 7

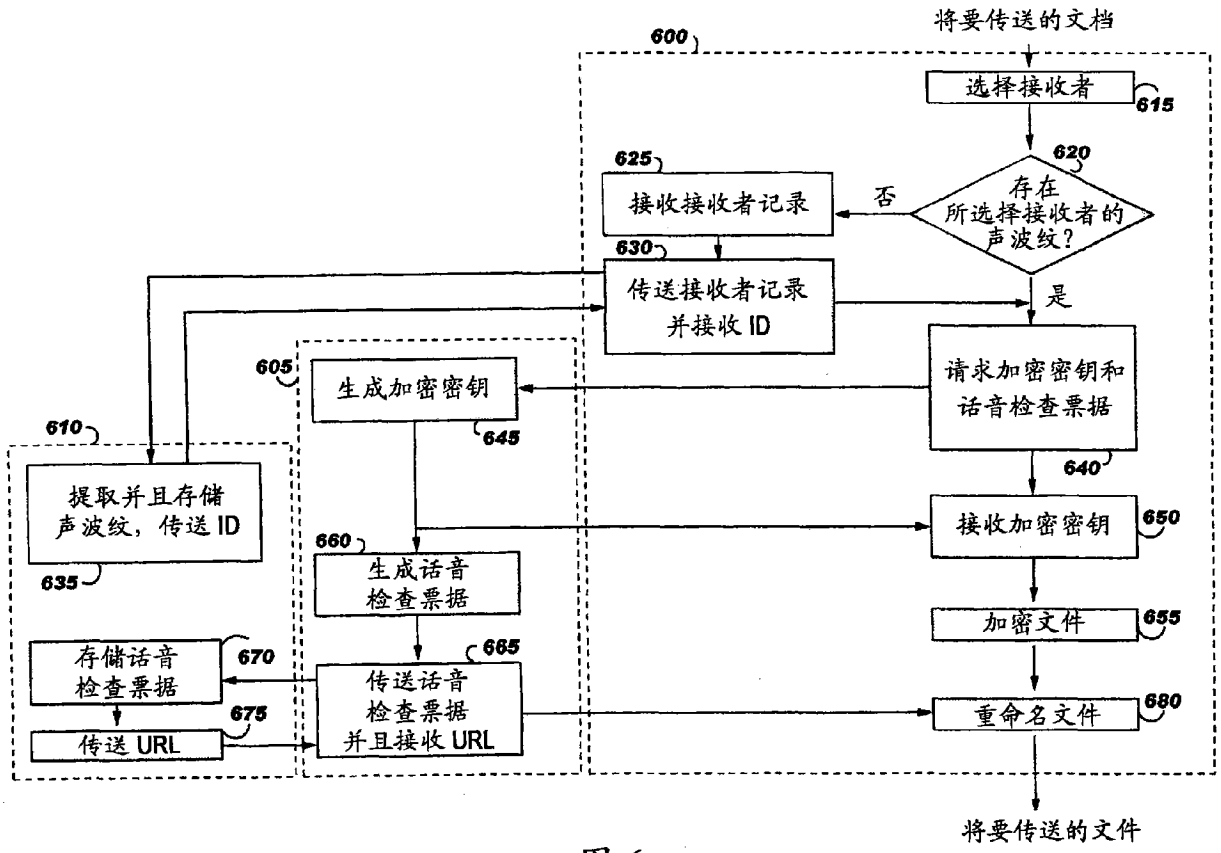

将要传送的文档
600
选择接收者
615
620
存在
所选择接收者的
声波纹?
否
625
接收接收者记录
630
传送接收者记录
并接收 ID
是
请求加密密钥和
话音检查票据
640
605
生成加密密钥
645
610
提取并且存储
声波纹，传送 ID
635
660
生成话音
检查票据
接收加密密钥
650
加密文件
655
665
存储话音
检查票据
670
传送话音
检查票据
并且接收 URL
675
传送 URL
重命名文件
680
将要传送的文件

图 6

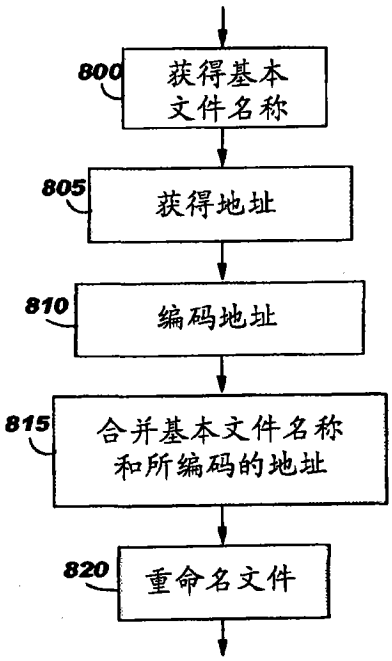

800
获得基本文件名称
805
获得地址
810
编码地址
815
合并基本文件名称和所编码的地址
820
重命名文件

图 8a

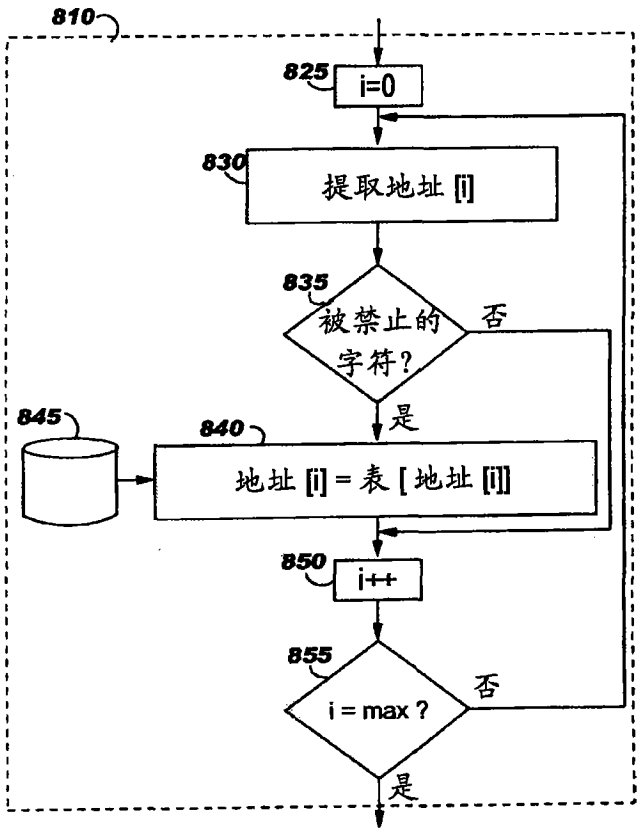

810
825
i=0
830
提取地址 [i]
835
被禁止的字符?
否
是
845
840
地址 [i] = 表 [地址 [i]]
850
i++
855
i = max ?
否
是

图 8b