(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 105743884 A
(43)申请公布日 2016.07.06

(21)申请号 201610044252.3

(22)申请日 2016.01.22

(71)申请人 广东信鉴信息科技有限公司
地址 510000 广东省广州市越秀区豪贤路101号3A楼18室
申请人 广东数字证书认证中心有限公司

(72)发明人 王胜男 张永强

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 潘桂生 钟杰婷

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/58(2006.01)
H04L 9/32(2006.01)

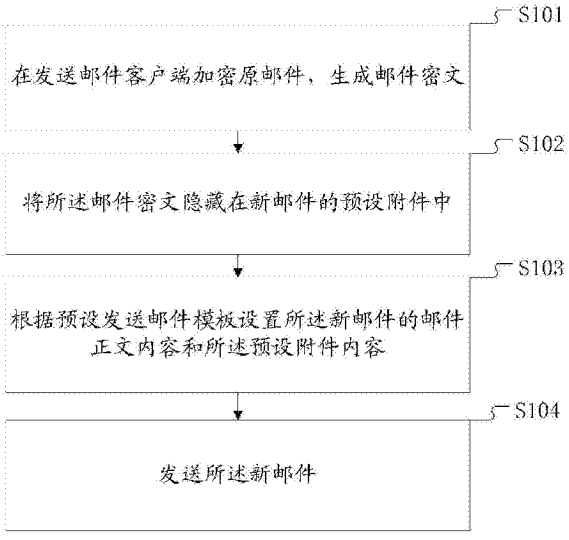
权利要求书2页 说明书6页 附图7页

(54)发明名称

邮件隐藏方法和系统

(57)摘要

本发明公开了一种邮件隐藏方法和系统，所述方法包括：在发送邮件客户端加密原邮件，生成邮件密文；将所述邮件密文隐藏在新邮件的预设附件中；根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；发送所述新邮件。本发明将加密邮件隐藏到新邮件附件中，作为普通邮件的附件发送，避免加密邮件被邮件服务器或客户端当作垃圾邮件处理；当无法解密加密邮件时，用户可以看到根据预设发送邮件模板设置的邮件内容，提升用户体验，适合应用。



CN 105743884 A

1.一种邮件隐藏方法，其特征在于，包括以下步骤：

在发送邮件客户端加密原邮件，生成邮件密文；

将所述邮件密文隐藏在新邮件的预设附件中；

根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；

发送所述新邮件。

2.根据权利要求1所述的邮件隐藏方法，其特征在于，在所述根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容之后，发送所述新邮件之前，还包括步骤：

对所述预设附件进行签名。

3.根据权利要求1或2所述的邮件隐藏方法，其特征在于，在所述生成邮件密文之前，还包括步骤：

给所述原邮件的邮件正文添加正文标记，和/或给所述原邮件的附件添加附件标记。

4.一种邮件隐藏方法，其特征在于，包括以下步骤：

接收并打开发送邮件客户端发送的邮件；

读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

查询是否有与所述邮件密文对应的解密密钥；

当查询结果为是时，根据所述解密密钥解密所述邮件密文；

当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。

5.根据权利要求4所述的邮件隐藏方法，其特征在于，在所述接收并打开发送邮件客户端发送的邮件之后，所述读取隐藏在所述邮件附件中的邮件密文之前，还包括步骤：

查询所述邮件附件是否有签名；

当查询结果为是时，验证所述签名。

6.根据权利要求4或5所述的邮件隐藏方法，其特征在于，在根据所述解密密钥解密所述邮件密文之后，还包括步骤：

查询解密后的邮件中是否有正文标记和/或附件标记，所述正文标记添加在所述原邮件的邮件正文上，所述附件标记添加在所述原邮件的附件上；

当查询结果为是时，根据所述正文标记和/或附件标记，将解密后的邮件恢复为所述原邮件。

7.一种邮件隐藏系统，其特征在于，包括：

加密模块，用于在发送邮件客户端加密原邮件，生成邮件密文；

隐藏模块，用于将所述邮件密文隐藏在新邮件的预设附件中；

设置模块，用于根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；

发送模块，用于发送所述新邮件。

8.根据权利要求7所述的邮件隐藏系统，其特征在于，还包括签名模块，用于在所述设置模块根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容之后，对所述预设附件进行签名；

所述发送模块发送进行签名后的新邮件。

9.根据权利要求7或8所述的邮件隐藏系统，其特征在于，还包括添加模块，用于在所述加密模块生成邮件密文之前，给所述原邮件的邮件正文添加正文标记，和/或给所述原邮件的附件添加附件标记。

10.一种邮件隐藏系统，其特征在于，包括：

接收模块，用于接收并打开发送邮件客户端发送的邮件；

读取模块，用于读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

查询模块，用于查询是否有与所述邮件密文对应的解密密钥；

解密模块，用于当查询结果为是时，根据所述解密密钥解密所述邮件密文；

显示模块，用于当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。

11.根据权利要求10所述的邮件隐藏系统，其特征在于，还包括查询验证模块，用于在所述接收模块接收并打开发送邮件客户端发送的邮件之后，查询所述邮件附件是否有签名；当查询结果为是时，验证所述签名；

所述读取模块在验证所述签名正确后，读取隐藏在所述邮件附件中的邮件密文。

12.根据权利要求10或11所述的邮件隐藏系统，其特征在于，还包括查询恢复模块，用于在所述解密模块根据所述解密密钥解密所述邮件密文后，查询解密后的邮件中是否有正文标记和/或附件标记，所述正文标记添加在所述原邮件的邮件正文上，所述附件标记添加在所述原邮件的附件上；当查询结果为是时，根据所述正文标记和/或附件标记，将解密后的邮件恢复为所述原邮件。

邮件隐藏方法和系统

技术领域

[0001] 本发明涉及计算机数据通信技术领域，特别是涉及一种邮件隐藏方法和系统。

背景技术

[0002] 随着因特网的普及，电子邮件已经成为现代人生活和工作中最常用的通信工具之一。据不完全统计，因特网上每天传送的电子邮件达数十亿份。针对电子邮件的犯罪案件越来越多，用户在享受电子邮件快捷便利的服务时，还要承受邮件泄密带来的后果，有些邮件泄密后果非常严重，是灾难性的。为了提高邮件信息的安全性，目前有效的方法是进行邮件加密，通过加密使邮件只能被指定的人进行浏览，确保邮件的安全。

[0003] 现有如利用对称加密算法加密邮件，利用传统非对称密钥体系(PKI/CA)加密邮件，利用链式加密体系加密邮件，利用基于身份的密码技术加密邮件等邮件加密方式，都是以密文的方式传送邮件，由于加密邮件不具备可读性，可能会被邮件服务器或客户端当作垃圾邮件处理；如果用户收到了加密邮件，但暂未获取解密密钥，只能看到乱码，无法判断邮件内容。

发明内容

[0004] 基于上述情况，有必要针对现有加密邮件被邮件服务器或客户端当作垃圾邮件处理，用户阅读未解密邮件时无法判断邮件内容的问题，提供一种邮件隐藏方法和系统。

[0005] 为了实现上述目的，本发明技术方案的实施例为：

[0006] 一种邮件隐藏方法，包括以下步骤：

[0007] 在发送邮件客户端加密原邮件，生成邮件密文；

[0008] 将所述邮件密文隐藏在新邮件的预设附件中；

[0009] 根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；

[0010] 发送所述新邮件。

[0011] 一种邮件隐藏方法，包括以下步骤：

[0012] 接收并打开发送邮件客户端发送的邮件；

[0013] 读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

[0014] 查询是否有与所述邮件密文对应的解密密钥；

[0015] 当查询结果为是时，根据所述解密密钥解密所述邮件密文；

[0016] 当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。

[0017] 一种邮件隐藏系统，包括：

[0018] 加密模块，用于在发送邮件客户端加密原邮件，生成邮件密文；

[0019] 隐藏模块，用于将所述邮件密文隐藏在新邮件的预设附件中；

[0020] 设置模块，用于根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预

设附件内容；

[0021] 发送模块，用于发送所述新邮件。

[0022] 一种邮件隐藏系统，包括：

[0023] 接收模块，用于接收并打开发送邮件客户端发送的邮件；

[0024] 读取模块，用于读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

[0025] 查询模块，用于查询是否有与所述邮件密文对应的解密密钥；

[0026] 解密模块，用于当查询结果为是时，根据所述解密密钥解密所述邮件密文；

[0027] 显示模块，用于当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。

[0028] 与现有技术相比，本发明的有益效果为：本发明邮件隐藏方法和系统，将加密邮件隐藏到新邮件附件中，作为普通邮件的附件发送，避免加密邮件被邮件服务器或客户端当作垃圾邮件处理；当查询没有与邮件密文对应的解密密钥时，用户可以看到根据预设发送邮件模板设置的邮件内容，提升用户体验，适合应用。

附图说明

[0029] 图1为本发明邮件隐藏方法第一实施方式的流程示意图；

[0030] 图2为本发明邮件隐藏方法第二实施方式的流程示意图；

[0031] 图3为基于图1、2所示方法一个具体示例中邮件隐藏方法流程图；

[0032] 图4为一个实施例中标准的PDF文档结构示意图；

[0033] 图5为一个实施例中隐藏邮件密文并添加签名后的PDF文档结构示意图；

[0034] 图6为本发明邮件隐藏系统第一实施方式的结构示意图；

[0035] 图7为本发明邮件隐藏系统第二实施方式的结构示意图。

具体实施方式

[0036] 为使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步的详细说明。应当理解，此处所描述的具体实施方式仅仅用以解释本发明，并不限定本发明的保护范围。

[0037] 一个实施例中邮件隐藏方法，如图1所示，包括以下步骤：

[0038] 步骤S101：在发送邮件客户端加密原邮件，生成邮件密文；

[0039] 步骤S102：将所述邮件密文隐藏在新邮件的预设附件中；

[0040] 步骤S103：根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；如设置新邮件的邮件正文内容为“这是一封加密邮件”，预设附件内容可与邮件正文内容一致；

[0041] 步骤S104：发送所述新邮件。

[0042] 从以上描述可知，本发明邮件隐藏方法，将加密邮件隐藏到新邮件附件中，作为普通邮件的附件发送，避免加密邮件被邮件服务器或客户端当作垃圾邮件处理。

[0043] 此外，在一个具体示例中，在所述根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容之后，发送所述新邮件之前，还包括步骤：

[0044] 对所述预设附件进行签名。如把发件人的名字签在邮件附件中，使收件人通过该签名核实邮件，以防邮件在发送过程中被篡改。

[0045] 此外，在一个具体示例中，在所述生成邮件密文之前，还包括步骤：

[0046] 给所述原邮件的邮件正文添加正文标记，和/或给所述原邮件的附件添加附件标记。

[0047] 当原邮件只有邮件正文时，在生成的邮件密文之前在原邮件添加正文标记；当原邮件只有附件时，在生成的邮件密文之前在原邮件添加附件标记；当原邮件有邮件正文和附件时，在邮件正文添加正文标记，在附件添加附件标记，然后进行邮件加密；方便后续处理，满足多种应用需要。

[0048] 一个实施例中邮件隐藏方法，如图2所示，包括以下步骤：

[0049] 步骤S201：接收并打开发送邮件客户端发送的邮件；

[0050] 步骤S202：读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

[0051] 步骤S203：查询是否有与所述邮件密文对应的解密密钥；

[0052] 步骤S204：当查询结果为是时，根据所述解密密钥解密所述邮件密文；

[0053] 步骤S205：当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。如显示根据预设发送邮件模板设置的新邮件的邮件正文内容“这是一封加密邮件”，附件内容“这是一封加密邮件”，这样避免用户阅读未解密邮件时无法判断邮件内容，提升用户体验。

[0054] 从以上描述可知，本发明邮件隐藏方法，当查询没有与邮件密文对应的解密密钥时，用户可以看到根据预设发送邮件模板设置的邮件内容，提升用户体验。

[0055] 此外，在一个具体示例中，在所述接收并打开发送邮件客户端发送的邮件之后，所述读取隐藏在所述邮件附件中的邮件密文之前，还包括步骤：

[0056] 查询所述邮件附件是否有签名；

[0057] 当查询结果为是时，验证所述签名。

[0058] 在验证附件签名正确后才进行后续处理，如果不正确，停止处理，避免解密被篡改的邮件，在邮件发送中增多了一层安全保证。

[0059] 此外，在一个具体示例中，在根据所述解密密钥解密所述邮件密文之后，还包括步骤：

[0060] 查询解密后的邮件中是否有正文标记和/或附件标记，所述正文标记添加在所述原邮件的邮件正文上，所述附件标记添加在所述原邮件的附件上；

[0061] 当查询结果为是时，根据所述正文标记和/或附件标记，将解密后的邮件恢复为所述原邮件。

[0062] 当解密后的邮件中只有正文标记，说明原邮件只有邮件正文，结合所述正文标记将解密后的邮件恢复为所述原邮件，得到原邮件的邮件正文；当解密后的邮件只有附件标记，说明原邮件只有附件，结合所述附件标记将解密后的邮件恢复为所述原邮件，得到原邮件的附件；当解密后的邮件中有正文标记和附件标记，说明原邮件有邮件正文和附件，结合所述正文标记和附件标记将解密后的邮件恢复为所述原邮件，得到原邮件的邮件正文和附件，方便用户阅读邮件，适合应用。

[0063] 为了更好地理解上述方法，以下详细阐述一个本发明邮件隐藏方法的应用实例。

[0064] 如图3所示，该应用实例可以包括以下步骤：

[0065] 步骤S301：在发送邮件客户端给原邮件的邮件正文添加正文标记，给原邮件的附件添加附件标记，原邮件包括邮件正文和附件；

[0066] 步骤S302：加密添加正文标记和附件标记的原邮件，生成邮件密文；

[0067] 步骤S303：将邮件密文隐藏在新邮件的PDF附件中；

[0068] 步骤S304：对上述PDF附件进行签名；可对PDF附件进行标准PDF签名；

[0069] 标准的PDF文档结构如图4所示，隐藏邮件密文并添加签名后的PDF文档结构如图5所示，在PDF文档目录下面添加了加密电子邮件节点，用于存储加密邮件内容，并将签名添加到PDF页面下面；

[0070] 步骤S305：根据预设发送邮件模板设置新邮件的邮件正文内容和上述PDF附件内容；如设置新邮件的邮件正文内容为“这是一封加密邮件”，PDF附件内容与邮件正文内容一致；

[0071] 步骤S306：通过邮件服务器发送上述新邮件；

[0072] 步骤S307：在接收邮件客户端接收并打开上述新邮件；

[0073] 步骤S308：验证上述PDF附件的签名；若为标准PDF签名，可由adobe reader之类的工具直接验证，方便、准确；

[0074] 步骤S309：在验证签名正确后，从上述PDF附件中读取上述邮件密文；

[0075] 步骤S310：查询是否有与上述邮件密文对应的解密密钥；

[0076] 步骤S311：当查询结果为是时，根据上述解密密钥解密上述邮件密文，查询解密后的邮件中是否有上述正文标记和附件标记；当查询结果为是时，根据上述正文标记和附件标记，将解密后的邮件恢复为上述原邮件，得到原邮件的邮件正文和附件；

[0077] 步骤S312：当查询结果为否时，显示上述根据预设发送邮件模板设置的新邮件的邮件正文内容和上述PDF附件内容。如根据预设发送邮件模板设置的新邮件的邮件正文内容“这是一封加密邮件”，PDF附件内容与邮件正文内容一致。

[0078] 本应用实例将邮件密文隐藏到PDF文档中，PDF文档作为普通邮件的附件发送，避免加密邮件被邮件服务器或客户端当作垃圾邮件处理；设置新邮件的内容，避免用户阅读未解密邮件时无法判断邮件内容，提升用户体验；对PDF文档进行签名，接收方可以通过验证签名有效性来判断邮件是否被篡改，在邮件发送中增多了一层安全保证。

[0079] 一个实施例中邮件隐藏系统，如图6所示，包括：

[0080] 加密模块601，用于在发送邮件客户端加密原邮件，生成邮件密文；

[0081] 隐藏模块602，用于将所述邮件密文隐藏在新邮件的预设附件中；

[0082] 设置模块603，用于根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；如设置新邮件的邮件正文内容为“这是一封加密邮件”，预设附件内容可与邮件正文内容一致；

[0083] 发送模块604，用于发送所述新邮件。

[0084] 如图6所示，在一个具体示例中，所述系统还包括签名模块605，用于在所述设置模块603根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容之后，对所述预设附件进行签名；如把发件人的名字签在邮件附件中，使收件人通过该签名核实

邮件，以防邮件在发送过程中被篡改；

[0085] 所述发送模块604发送进行签名后的新邮件。

[0086] 如图6所示，在一个具体示例中，所述系统还包括添加模块606，用于在所述加密模块601生成邮件密文之前，给所述原邮件的邮件正文添加正文标记，和/或给所述原邮件的附件添加附件标记。

[0087] 当原邮件只有邮件正文时，在生成的邮件密文之前在原邮件添加正文标记；当原邮件只有附件时，在生成的邮件密文之前在原邮件添加附件标记；当原邮件有邮件正文和附件时，在邮件正文添加正文标记，在附件添加附件标记，然后进行邮件加密；方便后续处理，满足多种应用需要。

[0088] 基于图6所示的本实施例的系统，一个具体的工作过程可以是如下所述：

[0089] 首先在发送邮件客户端添加模块606给所述原邮件的邮件正文添加正文标记，和/或给所述原邮件的附件添加附件标记；加密模块601加密添加正文标记和/或附件标记的原邮件，生成邮件密文；隐藏模块602将上述邮件密文隐藏在新邮件的预设附件中；设置模块603根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容；签名模块605对所述预设附件进行签名；发送模块604发送进行签名后的新邮件。

[0090] 从以上描述可知，本发明邮件隐藏系统，将加密邮件隐藏到新邮件附件中，作为普通邮件的附件发送，避免加密邮件被邮件服务器或客户端当作垃圾邮件处理；对新邮件附件进行签名，接收方可以通过验证签名有效性来判断邮件是否被篡改，在邮件发送中增多了一层安全保证。

[0091] 一个实施例中邮件隐藏系统，如图7所示，包括：

[0092] 接收模块701，用于接收并打开发送邮件客户端发送的邮件；

[0093] 读取模块702，用于读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文；

[0094] 查询模块703，用于查询是否有与所述邮件密文对应的解密密钥；

[0095] 解密模块704，用于当查询结果为是时，根据所述解密密钥解密所述邮件密文；

[0096] 显示模块705，用于当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容。如显示根据预设发送邮件模板在所述发送邮件客户端设置的新邮件的邮件正文内容“这是一封加密邮件”，PDF附件内容“这是一封加密邮件”，这样避免用户阅读未解密邮件时无法判断邮件内容，提升用户体验。

[0097] 如图7所示，在一个具体示例中，所述系统还包括查询验证模块706，用于在所述接收模块701接收并打开发送邮件客户端发送的邮件之后，查询所述邮件附件是否有签名；当查询结果为是时，验证所述签名；

[0098] 所述读取模块702在验证所述签名正确后，读取隐藏在所述邮件附件中的邮件密文。

[0099] 在验证附件签名正确后才进行后续处理，如果不正确，停止处理，避免解密被篡改的邮件，在邮件发送中增多了一层安全保证。

[0100] 如图7所示，在一个具体示例中，所述系统还包括查询恢复模块707，用于在所述解密模块704根据所述解密密钥解密所述邮件密文后，查询解密后的邮件中是否有正文标记和/或附件标记，所述正文标记添加在所述原邮件的邮件正文上，所述附件标记添加在所述

原邮件的附件上；当查询结果为是时，根据所述正文标记和/或附件标记，将解密后的邮件恢复为所述原邮件。

[0101] 当解密后的邮件中只有正文标记，说明原邮件只有邮件正文，结合所述正文标记将解密后的邮件恢复为所述原邮件，得到原邮件的邮件正文；当解密后的邮件只有附件标记，说明原邮件只有附件，结合所述附件标记将解密后的邮件恢复为所述原邮件，得到原邮件的附件；当解密后的邮件中有正文标记和附件标记，说明原邮件有邮件正文和附件，结合所述正文标记和附件标记将解密后的邮件恢复为所述原邮件，得到原邮件的邮件正文和附件，方便用户阅读邮件，适合应用。

[0102] 基于图7所示的本实施例的系统，一个具体的工作过程可以是如下所述：

[0103] 接收模块701接收并打开发送邮件客户端发送的邮件；查询验证模块706查询所述邮件附件是否有签名；当查询结果为是时，验证所述签名；读取模块702在验证所述签名正确后，读取隐藏在所述邮件附件中的邮件密文；查询模块703查询是否有与所述邮件密文对应的解密密钥；当查询结果为是时，解密模块704根据所述解密密钥解密所述邮件密文；当查询结果为否时，显示模块705显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容；查询恢复模块707在所述解密模块704根据所述解密密钥解密所述邮件密文后，查询解密后的邮件中是否有正文标记和/或附件标记，所述正文标记添加在所述原邮件的邮件正文上，所述附件标记添加在所述原邮件的附件上；当查询结果为是时，根据所述正文标记和/或附件标记，将解密后的邮件恢复为所述原邮件。

[0104] 从以上描述可知，本发明邮件加密系统，当查询没有与邮件密文对应的解密密钥时，用户可以看到根据预设发送邮件模板设置的邮件内容，提升用户体验；接收方通过验证邮件附件签名有效性来判断邮件是否被篡改，在邮件发送中增多了一层安全保证。

[0105] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0106] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

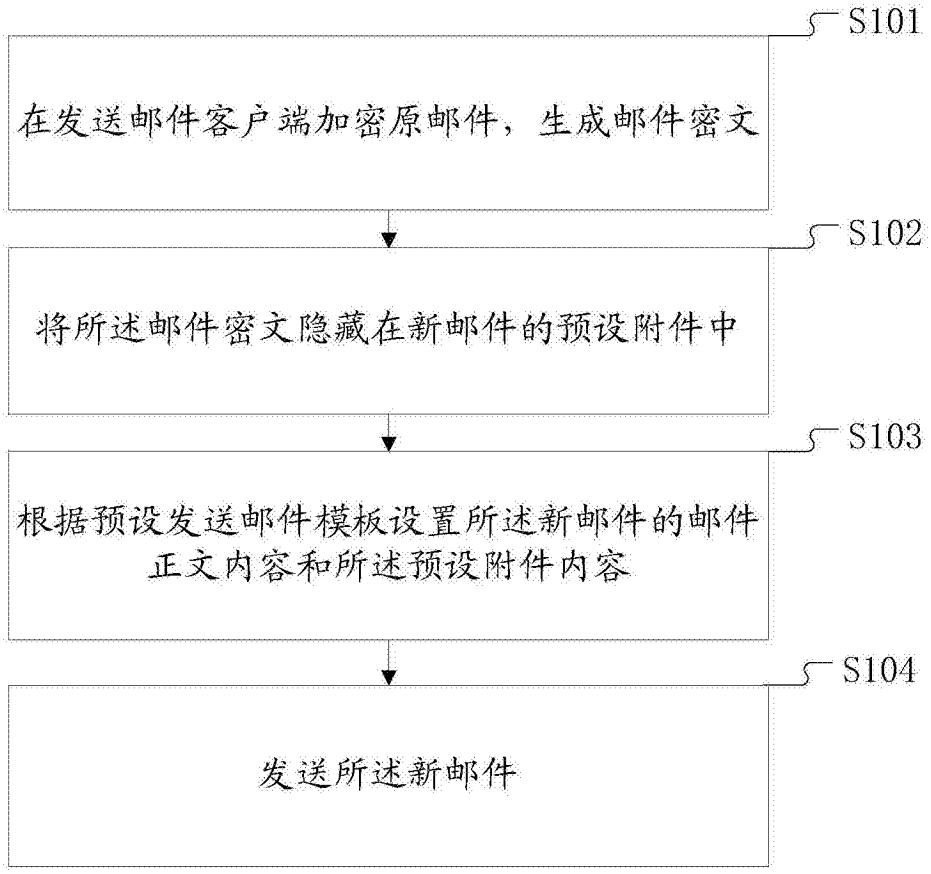

S101
在发送邮件客户端加密原邮件，生成邮件密文
S102
将所述邮件密文隐藏在新邮件的预设附件中
S103
根据预设发送邮件模板设置所述新邮件的邮件正文内容和所述预设附件内容
S104
发送所述新邮件

图1

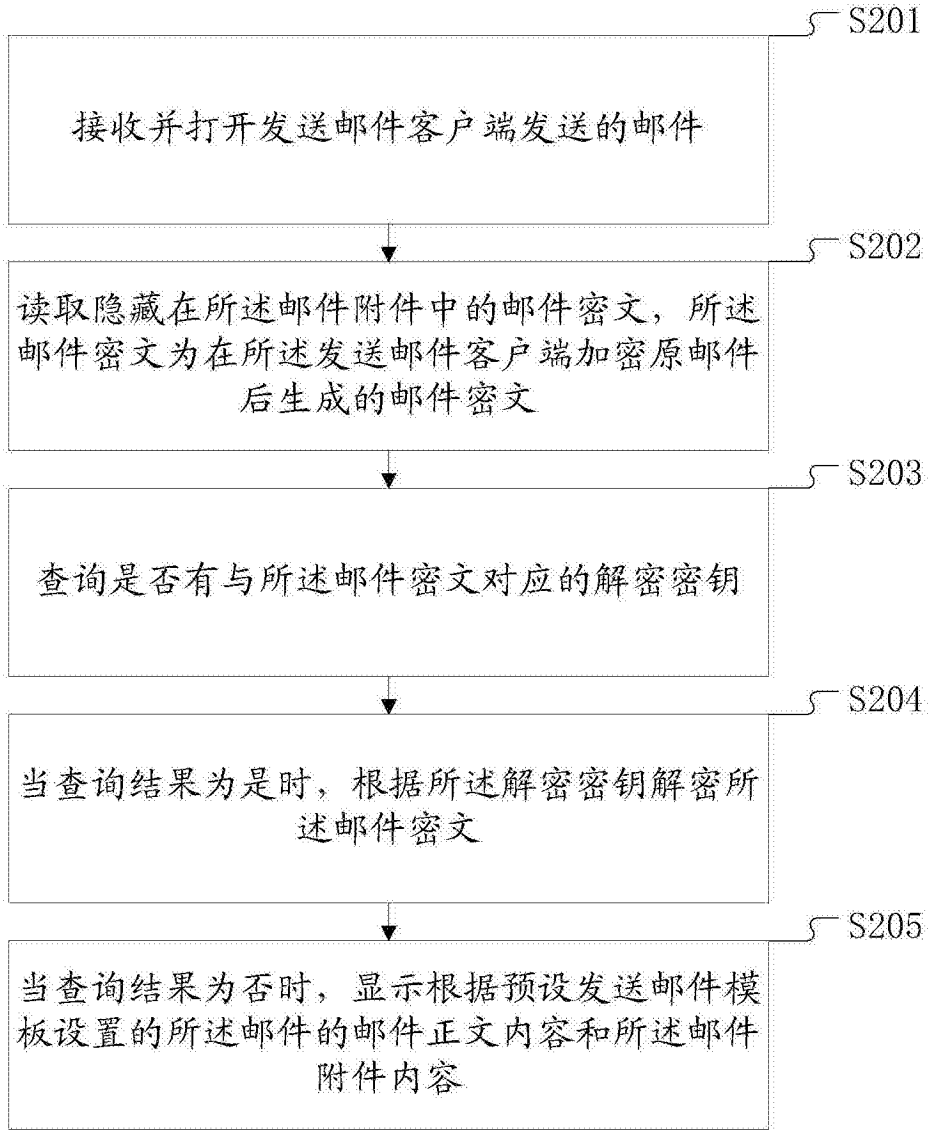

S201
接收并打开发送邮件客户端发送的邮件
S202
读取隐藏在所述邮件附件中的邮件密文，所述邮件密文为在所述发送邮件客户端加密原邮件后生成的邮件密文
S203
查询是否有与所述邮件密文对应的解密密钥
S204
当查询结果为是时，根据所述解密密钥解密所述邮件密文
S205
当查询结果为否时，显示根据预设发送邮件模板设置的所述邮件的邮件正文内容和所述邮件附件内容

图2

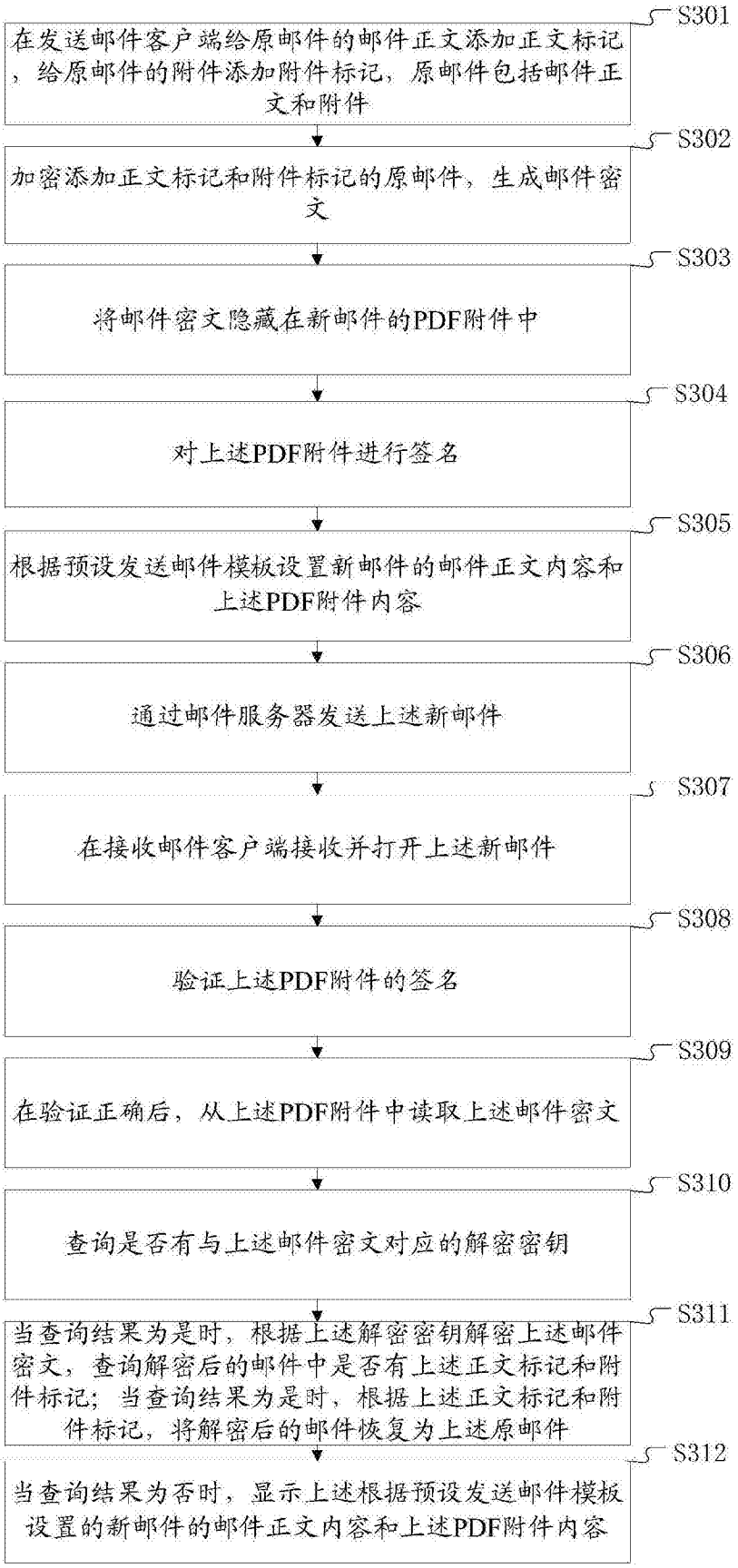

S301
在发送邮件客户端给原邮件的邮件正文添加正文标记，给原邮件的附件添加附件标记，原邮件包括邮件正文和附件
S302
加密添加正文标记和附件标记的原邮件，生成邮件密文
S303
将邮件密文隐藏在新邮件的PDF附件中
S304
对上述PDF附件进行签名
S305
根据预设发送邮件模板设置新邮件的邮件正文内容和上述PDF附件内容
S306
通过邮件服务器发送上述新邮件
S307
在接收邮件客户端接收并打开上述新邮件
S308
验证上述PDF附件的签名
S309
在验证正确后，从上述PDF附件中读取上述邮件密文
S310
查询是否有与上述邮件密文对应的解密密钥
S311
当查询结果为是时，根据上述解密密钥解密上述邮件密文，查询解密后的邮件中是否有上述正文标记和附件标记；当查询结果为是时，根据上述正文标记和附件标记，将解密后的邮件恢复为上述原邮件
S312
当查询结果为否时，显示上述根据预设发送邮件模板设置的新邮件的邮件正文内容和上述PDF附件内容

图3

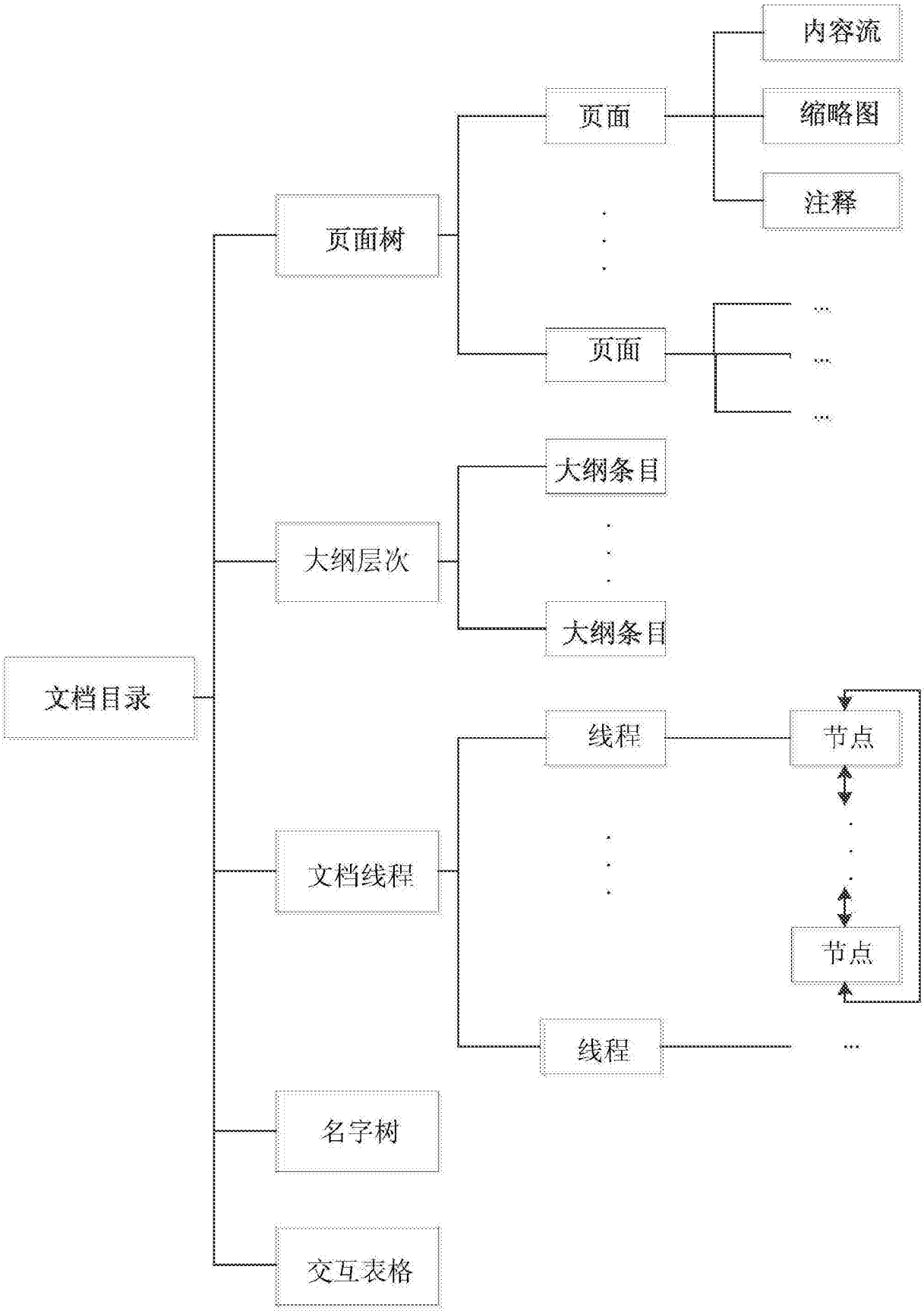

文档目录
页面树
页面
内容流
缩略图
注释
页面
大纲层次
大纲条目
大纲条目
文档线程
线程
节点
节点
线程
名字树
交互表格

图4

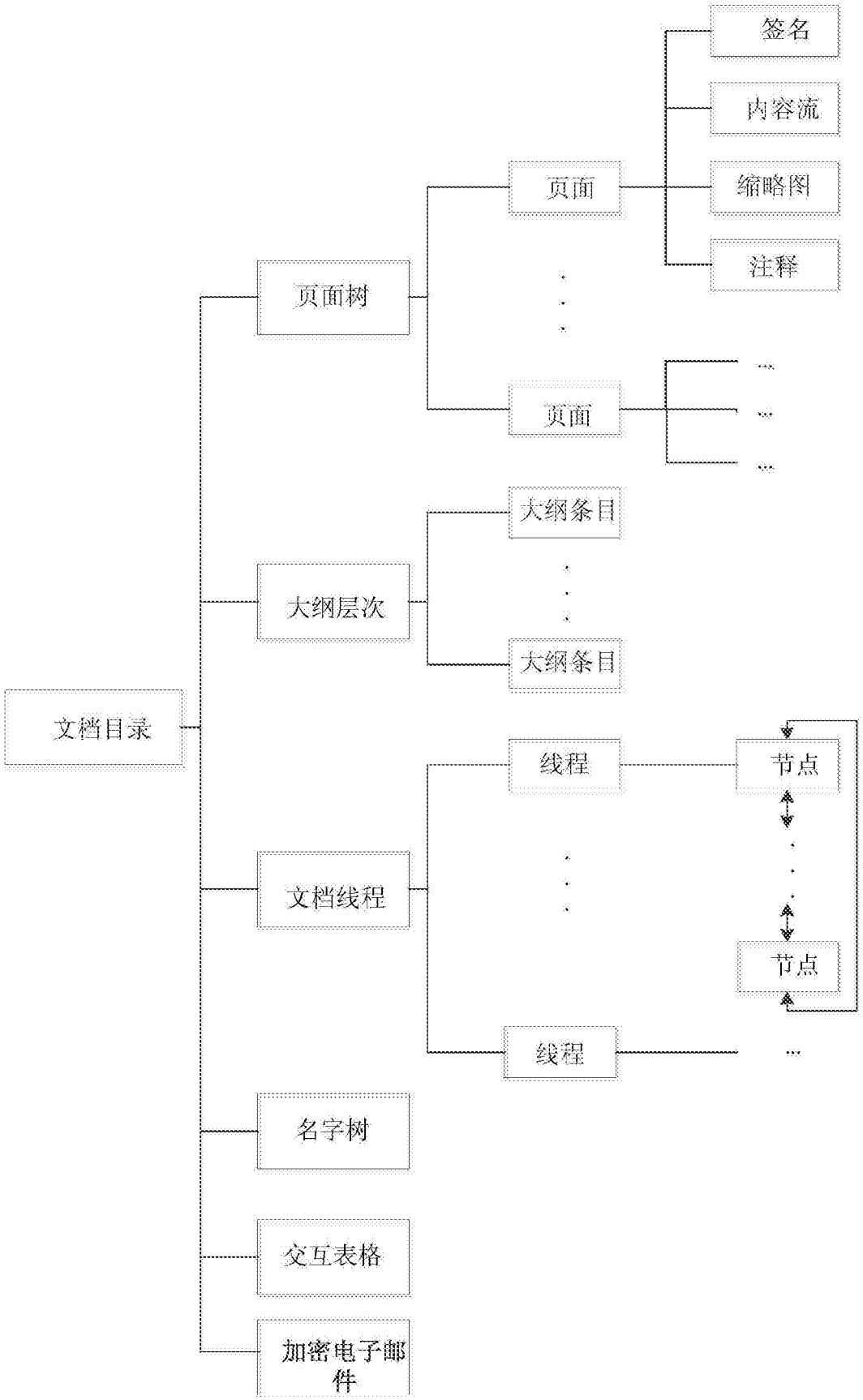

文档目录
页面树
页面
签名
内容流
缩略图
注释
页面
大纲层次
大纲条目
大纲条目
文档线程
线程
节点
节点
线程
名字树
交互表格
加密电子邮件

图5

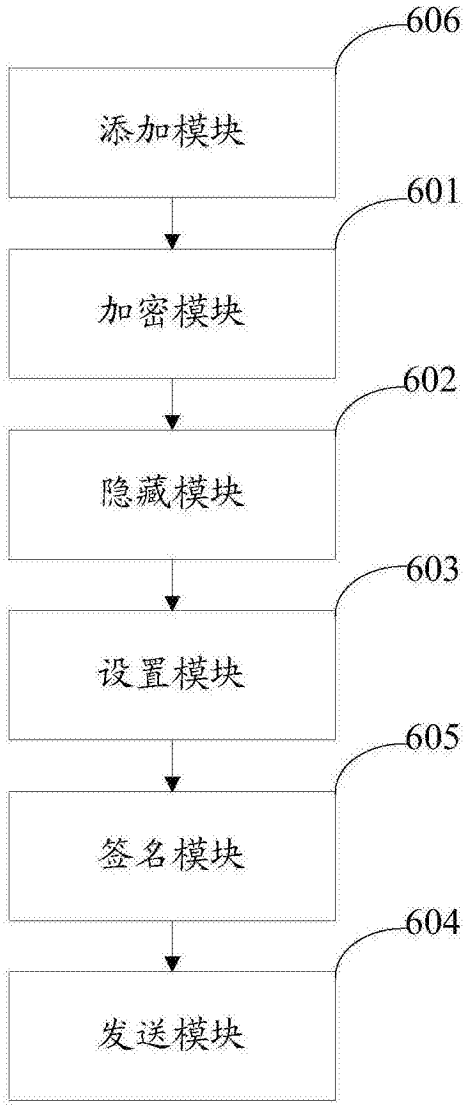


图6

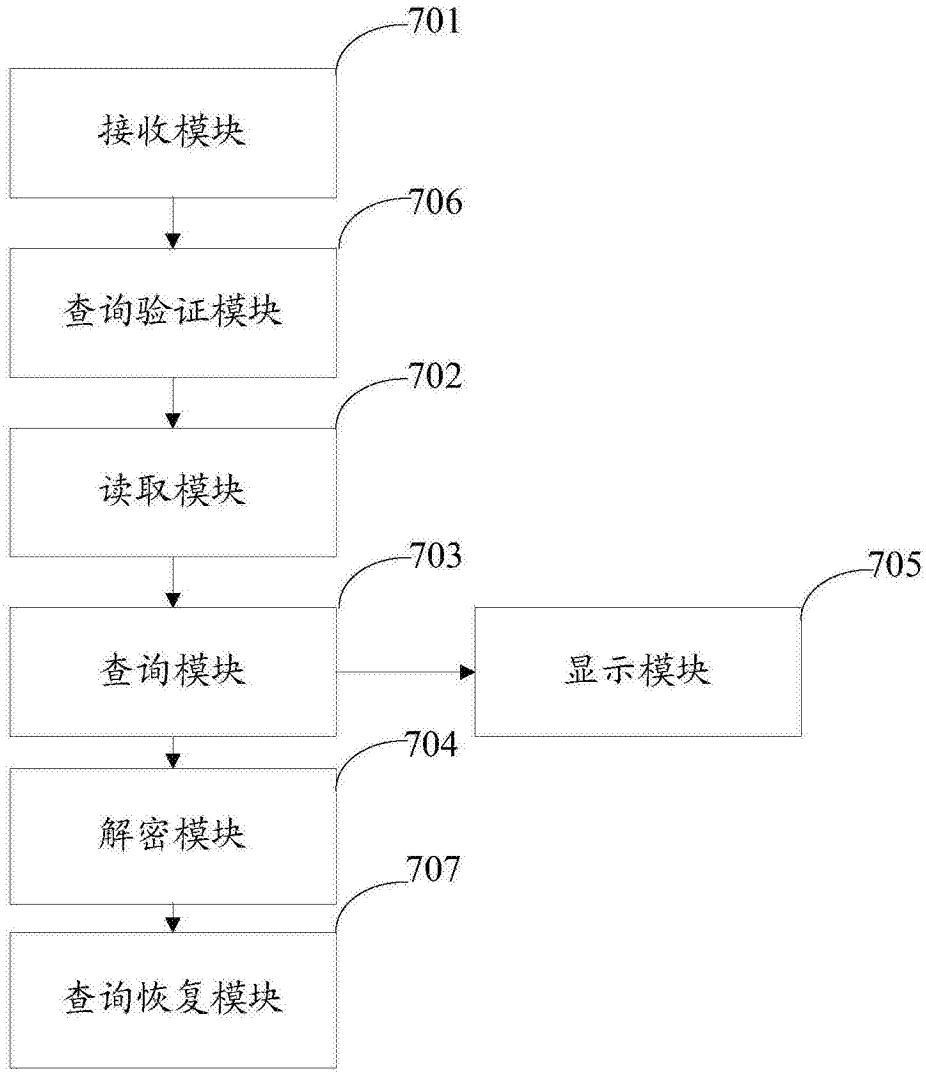

701
接收模块
706
查询验证模块
702
读取模块
703
查询模块
705
显示模块
704
解密模块
707
查询恢复模块

图7