(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111970307 B
(45)授权公告日 2022.07.22

(21)申请号 202010904284.2
(22)申请日 2020.09.01
(65)同一申请的已公布的文献号
申请公布号 CN 111970307 A
(43)申请公布日 2020.11.20
(66)本国优先权数据
202010620450.6 2020.06.30 CN
(73)专利权人 冠群信息技术(南京)有限公司
地址 210019 江苏省南京市江北新区星火路17号创智大厦B座11层
(72)发明人 刘贵平
(74)专利代理机构 南京瑞华腾知识产权代理事务所(普通合伙) 32368
专利代理师 梁金娟
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 51/42(2022.01)
H04L 51/08(2022.01)
(56)对比文件
CN 1694436 A,2005.11.09
US 2004133774 A1,2004.07.08
CN 101572678 A,2009.11.04
CN 106209600 A,2016.12.07
刘亚峰等.基于电邮传输的文本隐藏技术.《信息安全与通信保密》.2005,(第02期),
余鹏飞等.基于信息隐藏技术的Outlook邮件隐藏插件开发.《计算机工程》.2006,(第19期),
萧萍.基于数字签名技术的安全电子邮件.《计算机安全》.2008,(第07期),
审查员 许伶俐

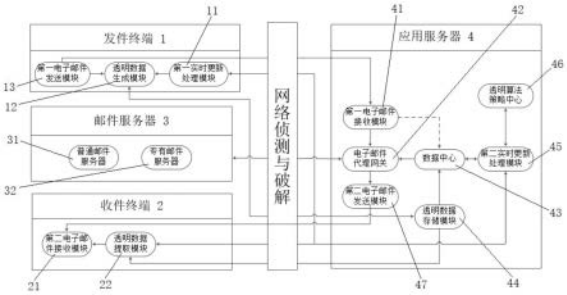
权利要求书2页 说明书5页 附图1页

(54)发明名称

透明数据传输系统、发件终端、服务器、收件终端与方法

(57)摘要

本发明公开一种透明数据传输系统、发件终端、服务器、收件终端与方法。发件终端根据透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识,透明数据发送至应用服务器存储,透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内并投递至收件终端,收件终端基于透明算法策略和透明数据的唯一标识生成提取码,以提取应用服务器中存储的对应的透明数据。本发明采用了透明算法策略中心、数据中心存储,在不影响传统邮件的正常投递下,甚至在不改变原有电子邮件的报文下,携带了高安全的透明数据,同时减少了邮件流转过程中产生的数据冗余;支持透明数据在邮件流转过程中对透明数据的实时更新,支持多人联机协作。



CN 111970307 B

1.一种透明数据传输系统,其特征在于,包括:发件终端、收件终端、邮件服务器和应用服务器;所述发件终端用于定义电子邮件是否进行透明传输,是,则所述发件终端根据应用服务器的下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识,并将生成的透明数据发送至应用服务器进行存储,所述透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内,所述发件终端具有对应用服务器中存储的透明数据的管理权限,未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容,则依次通过应用服务器和邮件服务器将电子邮件直接投递至收件终端,所述收件终端判断电子邮件中是否隐藏有透明数据的唯一标识,是则基于透明算法策略和透明数据的唯一标识生成提取码,以提取应用服务器中存储的对应的透明数据。

2.根据权利要求1所述的透明数据传输系统,其特征在于,所述邮件服务器包括普通邮件服务器和专有邮件服务器,所述专有邮件服务器用于从应用服务器接收携带透明数据的电子邮件中的非目标内容,并将携带透明数据的电子邮件中的非目标内容转发至普通邮件服务器,所述普通邮件服务器用于从应用服务器接收未携带透明数据的电子邮件,并将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容投递至收件终端。

3.根据权利要求1所述的透明数据传输系统,其特征在于,所述管理权限包括查询、只读、编辑、删除、撤消和销毁。

4.根据权利要求1所述的透明数据传输系统,其特征在于,所述透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合。

5.一种如权利要求1所述的发件终端,其特征在于,包括第一实时更新处理模块、透明数据生成模块和第一电子邮件发送模块;

所述第一实时更新处理模块用于定义电子邮件是否进行透明传输和设定对应用服务器中存储的透明数据进行管理,并接收应用服务器下发的透明算法策略;

所述透明数据生成模块用于通过第一实时更新处理模块接收应用服务器的下发的透明算法策略,并根据所述透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识;

所述第一电子邮件发送模块用于将生成的透明数据发送至应用服务器进行存储,并将透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内,且将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至应用服务器。

6.一种如权利要求1所述的应用服务器,其特征在于,包括第一电子邮件接收模块、电子邮件代理网关、数据中心、透明数据存储模块、第二实时更新处理模块、透明算法策略中心和第二电子邮件发送模块;

所述第一电子邮件接收模块用于接收发件终端发出的透明数据、未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容;

所述电子邮件代理网关用于实现第一电子邮件接收模块、数据中心、第二电子邮件发送模块和邮件服务器之间的数据交互;

所述数据中心用于存储透明数据;

所述透明数据存储模块用于访问数据中心存储的透明数据;

所述第二实时更新处理模块用于对应数据中心内存储的透明数据进行管理;

所述透明算法策略中心用于设定透明算法策略,并在检测到透明数据被创建或更新后

下发透明算法策略；

所述第二电子邮件发送模块用于将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至收件终端。

7.一种如权利要求1所述的收件终端，其特征在于，包括第二电子邮件接收模块和透明数据提取模块；

所述第二电子邮件接收模块用于接收未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，并判断电子邮件中是否隐藏有透明数据的唯一标识，是，则所述透明数据提取模块基于透明算法策略和透明数据的唯一标识生成提取码，以提取应用服务器中存储的对应的透明数据。

8.一种透明数据传输方法，其特征在于，包括：

定义电子邮件是否携带透明数据，是，则根据下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识，并将生成的透明数据进行存储，所述透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内；

未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容则直接以普通邮件投递；

判断电子邮件中是否隐藏有透明数据的唯一标识，是，则基于透明算法策略和透明数据的唯一标识生成提取码，以提取存储的对应的透明数据。

9.根据权利要求8所述的透明数据传输方法，其特征在于，所述透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合。

透明数据传输系统、发件终端、服务器、收件终端与方法

技术领域

[0001] 本发明属于数据传输技术领域，具体涉及透明数据传输系统、发件终端、服务器、收件终端与方法。

背景技术

[0002] 目前电子邮件作为互联网最重要的信息通讯工具，已得到广泛的应用。对于安全意识较高的用户，通过采用附件加密的方式传递内容，但当对方在非安全环境或密码泄露后，很容易导致加密文件的泄露。

[0003] 现有的电子邮件发送后只能通过对称加密、数字签名等传统安全技术处理加密数据，并且加密适应能力弱，存在易发现为加密邮件的典型特征，如普通客户端无法打开加密邮件，依赖第三方证书、无法查看邮件的正常内容等，若发现含有加密邮件的特征，无形给非法人员提供此封邮件含有重要信息，使得非法人员提高破解此封邮件的意愿。

[0004] 此外，现有的电子邮件系统发出加密的邮件后，如果想修改加密内容或者销毁加密内容都无法实现，因为加密数据已投递到对方的邮箱，此刻已处在失控管理中。

[0005] 因此，在复杂的网络环境中，面向高安全客户，设计一种新型携带透明数据的电子邮件在传输过程中的方法是至关重要的。

发明内容

[0006] 本发明解决的技术问题：提供一种基于电子邮件的透明数据传输系统、发件终端、服务器、收件终端与方法。

[0007] 技术方案：为了解决上述技术问题，本发明采用的技术方案如下：

[0008] 在第一方面，本发明提供了一种透明数据传输系统，其特征在于，包括：发件终端、收件终端、邮件服务器和应用服务器；所述发件终端用于定义电子邮件是否进行透明传输，是，则所述发件终端根据应用服务器的下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识，并将生成的透明数据发送至应用服务器进行存储，所述透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内，所述发件终端具有对应用服务器中存储的透明数据的管理权限，未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，则依次通过应用服务器和邮件服务器将电子邮件直接投递至收件终端，所述收件终端判断电子邮件中是否隐藏有透明数据的唯一标识，是则基于透明算法策略和透明数据的唯一标识生成提取码，以提取应用服务器中存储的对应的透明数据。

[0009] 进一步的，所述邮件服务器包括普通邮件服务器和专有邮件服务器，所述专有邮件服务器用于从应用服务器接收携带透明数据的电子邮件中的非目标内容，并将携带透明数据的电子邮件中的非目标内容转发至普通邮件服务器，所述普通邮件服务器用于从应用服务器接收未携带透明数据的电子邮件，并将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容投递至收件终端。

[0010] 进一步的，所述管理权限包括查询、只读、编辑、删除、撤消和销毁。

[0011] 进一步的，所述透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合。

[0012] 在第二方面，本发明提供了一种发件终端，包括第一实时更新处理模块、透明数据生成模块和第一电子邮件发送模块；

[0013] 所述第一实时更新处理模块用于定义电子邮件是否进行透明传输和设定对应用服务器中存储的透明数据进行管理，并接收应用服务器下发的透明算法策略；

[0014] 所述透明数据生成模块用于通过第一实时更新处理模块接收应用服务器的下发的透明算法策略，并根据所述透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识；

[0015] 所述第一电子邮件发送模块用于将生成的透明数据发送至应用服务器进行存储，并将透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内，且将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至应用服务器。

[0016] 在第三方面，本发明提供了一种应用服务器，包括第一电子邮件接收模块、电子邮件代理网关、数据中心、透明数据存储模块、第二实时更新处理模块、透明算法策略中心和第二电子邮件发送模块；

[0017] 所述第一电子邮件接收模块用于接收发件终端发出的透明数据、未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容；

[0018] 所述电子邮件代理网关用于实现第一电子邮件接收模块、数据中心、第二电子邮件发送模块和邮件服务器之间的数据交互；

[0019] 所述数据中心用于存储透明数据；

[0020] 所述透明数据存储模块用于访问数据中心存储的透明数据；

[0021] 所述第二实时更新处理模块用于对应数据中心内存储的透明数据进行管理；

[0022] 所述透明算法策略中心用于设定透明算法策略，并在检测到透明数据被创建或更新后下发透明算法策略；

[0023] 所述第二电子邮件发送模块用于将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至收件终端。

[0024] 在第四方面，本发明提供了一种收件终端，包括第二电子邮件接收模块和透明数据提取模块；

[0025] 所述第二电子邮件接收模块用于接收未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，并判断电子邮件中是否隐藏有透明数据的唯一标识，是，则所述数据提取模块基于透明算法策略和透明数据的唯一标识生成提取码，以提取应用服务器中存储的对应的透明数据。

[0026] 在第五方面，本发明提供了一种透明数据传输方法，包括：

[0027] 定义电子邮件是否携带透明数据，是，则根据下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识，并将生成的透明数据进行存储，所述透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内；

[0028] 未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容则直接以普通邮件投递；

[0029] 判断电子邮件中是否隐藏有透明数据的唯一标识，是，则基于透明算法策略和透明数据的唯一标识生成提取码，以提取存储的对应的透明数据。

[0030] 进一步的，所述透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合

[0031] 有益效果：与现有技术相比，本发明具有以下优点：

[0032] 本发明采用了透明算法策略中心、数据中心存储，在不影响传统邮件的正常投递下，甚至在不改变原有电子邮件的报文下，携带了高安全的透明数据，同时减少了邮件流转过程中产生的数据冗余；支持透明数据在邮件流转过程中对透明数据的实时更新，支持多人联机协作。

附图说明

[0033] 图1是透明数据传输系统结构示意图；

[0034] 图2是透明数据传输方法的流程图。

具体实施方式

[0035] 下面结合具体实施例，进一步阐明本发明，实施例在以本发明技术方案为前提下进行实施，应理解这些实施例仅用于说明本发明而不用于限制本发明的范围。

[0036] 如图1和2所示，本发明实施例的透明数据传输系统，包括：发件终端1、收件终端2、邮件服务器3和应用服务器4。

[0037] 其中，发件终端1用于定义电子邮件的性质，电子邮件的性质包括普通和透明，普通即电子邮件中没有透明数据，透明也就是电子邮件中携带有要通过透明传输的数据，如果发件人定义电子邮件的性质为透明，则发件终端1根据应用服务器4的下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识，目标内容即为用户需要将该内容进行透明传输的内容，发件终端1将生成的透明数据发送至应用服务器4进行存储，发件终端具有对应用服务器中存储的透明数据的管理权限，该管理权限包括查询、只读、编辑、删除、撤消和销毁。其中，销毁是逐位复写再删除，而不是直接物理删除。

[0038] 透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内，他人无法从这些内容中发现透明数据的唯一标识。发件终端1将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送给应用服务器，通过应用服务器和邮件服务器将电子邮件直接投递至收件终端2，当收件终端2接收到未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，收件人可直接通过收件终端2查阅电子邮件中的非透明数据内容。此时，用户并不知道非并根据电子邮件中是否具有经过透明传输的信息，收件终端2基于特定的方式可以自动发现电子邮件中是隐藏有透明数据的唯一标识的，则基于透明算法策略和透明数据的唯一标识生成提取码，以提取应用服务器4中存储的对应的透明数据。此时，收件人就可查阅到邮件中的全部内容。如果邮件被截取或者转发给他人，也不会泄露透明传输的信息。

[0039] 本发明实施例的邮件服务器3优选包括普通邮件服务器31和专有邮件服务器32，专有邮件服务器32用于从应用服务器4接收携带透明数据的电子邮件中的非目标内容，并将携带透明数据的电子邮件中的非目标内容转发至普通邮件服务器31，普通邮件服务器31

用于从应用服务器4接收未携带透明数据的电子邮件，并将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容投递至收件终端2。进而，具有透明传输内容的电子邮件中的一部分是通过普通邮件投递的，他人不易对该邮件产生怀疑并破解。

[0040] 本发明实施例的透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合。具体的实现方式如下：如在普通邮件的邮件头增加一个扩展类型：X-DocMail-Type＝M1，其中M1为可存在扩展协议策略，M2为图片签名策略，M3为正文特定摘要策略，同时组合策略有M12、M13、M23、M123。当普通邮件有标志：X-DocMail-Type，即可判定邮件为携带透明数据的邮件，其值就是透明数据唯一标识所在的位置，如果是M1则数据唯一标识存在另外一个扩展字段：X-DocMail-TK中，如果M2那么唯一标识存储在邮件签名图片中，如果是M3则通过计算邮件头收发人、主题、日期及加盐码的hash值作为数据的唯一标识。同样，收件终端2也是通过这些特性来判断接收的普通电子邮件中是否隐藏有透明数据的唯一标识的。

[0041] 如图1所示，本发明实施例的发件终端1，包括第一实时更新处理模块11、透明数据生成模块12和第一电子邮件发送模块13。

[0042] 其中，第一实时更新处理模块11用于定义电子邮件是否进行透明传输和对应用服务器中存储的透明数据进行管理，发件人通过第一实时更新处理模块11发出管理指令，进而完成应用服务器4中储存的透明数据的查询、只读、编辑、删除、撤消和销毁等操作。并接收应用服务器4下发的透明算法策略。透明数据生成模块12用于通过第一实时更新处理模块11接收应用服务器4下发的透明算法策略，并根据透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识。第一电子邮件发送模块13用于将生成的透明数据发送至应用服务器4进行存储，并将透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内，且将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至应用服务器4。

[0043] 如图1所示，本发明实施例的应用服务器4包括第一电子邮件接收模块41、电子邮件代理网关42、数据中心43、透明数据存储模块44、第二实时更新处理模块45、透明算法策略中心46和第二电子邮件发送模块47。

[0044] 其中，第一电子邮件接收模块41用于接收发件终端1发出的所有邮件数据，包括透明数据、未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容。电子邮件代理网关42用于实现第一电子邮件接收模块41、数据中心43、第二电子邮件发送模块47和邮件服务器3之间的数据交互。具体而言，第一电子邮件接收模块41将接收的透明数据发送给数据中心43存储，未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至电子邮件代理网关42，也可发送到数据中心43内存储备份，电子邮件代理网关42进一步将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容分别发送至普通邮件服务器31和专有邮件服务器32，电子邮件代理网关42还从普通邮件服务器31接收投递的电子邮件，并通过第二电子邮件发送模块47将电子邮件投递至收件终端2。收件终端2可通过透明数据存储模块44访问数据中心存储的透明数据。第二实时更新处理模块45用于对应数据中心内存储的透明数据进行管理，具体的，第二实时更新处理模块45接收发件终端1发出的管理指令，进而完成透明数据的查询、只读、编辑、删除、撤消和销毁等操作。透明算法策略中心46用于设定透明算法策略，在发件人定义邮件的性质后，透明算法

策略中心46会检测到透明数据被创建或更新后下发透明算法策略。第二电子邮件发送模块47从电子邮件代理网关42获取未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，并将未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容发送至收件终端2。

[0045] 如图1所示，本发明实施例的收件终端2包括第二电子邮件接收模块21和透明数据提取模块22。其中，第二电子邮件接收模块21用于接收应用服务器4发送的未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容，以供收件人直接查阅，并判断电子邮件中是否隐藏有透明数据的唯一标识，是，则透明数据提取模块22基于透明算法策略和透明数据的唯一标识生成提取码，以提取应用服务器4中存储的对应的透明数据。

[0046] 如图2所示，基于以上实施例，本领域技术人员可以轻易理解，本发明在另一方面还提供了一种透明数据传输方法，该方法包括：

[0047] 定义电子邮件是否携带透明数据，是，则根据下发的透明算法策略将电子邮件中的目标内容生成透明数据和透明数据的唯一标识，并将生成的透明数据进行存储，透明数据的唯一标识隐藏于携带透明数据的电子邮件中的非目标内容内。其中，目标内容即为发件人需要进行透明传输的内容，非目标内容即为不需要经过透明传输的内容。其中，透明算法策略包括可存在扩展协议、图片签名、正文特定摘要中的一种或任意组合。

[0048] 未携带透明数据的电子邮件和携带透明数据的电子邮件中的非目标内容则直接以普通邮件投递。

[0049] 判断电子邮件中是否隐藏有透明数据的唯一标识，是，则基于透明算法策略和透明数据的唯一标识生成提取码，以提取存储的对应的透明数据。

[0050] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

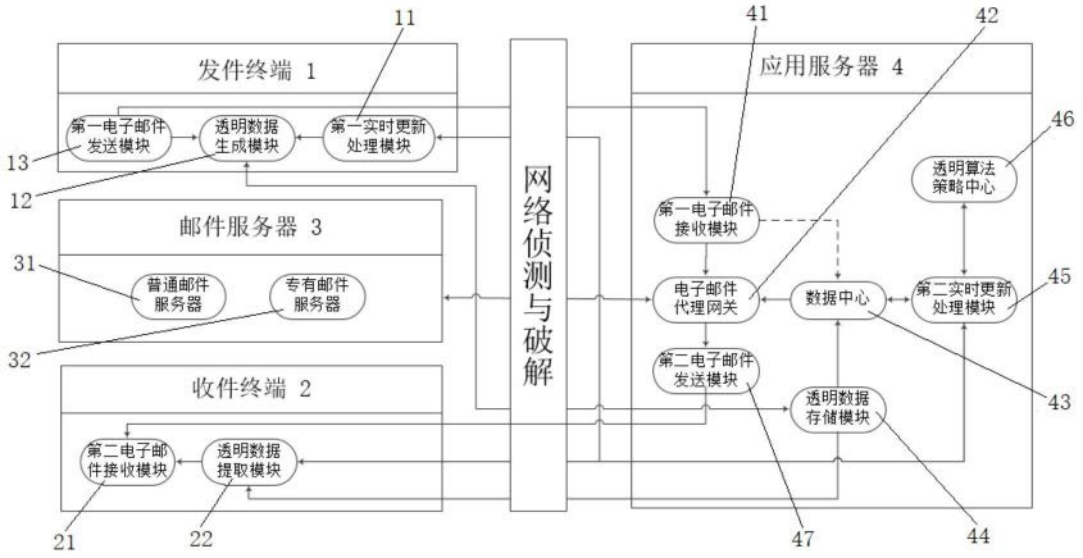

发件终端 1
第一电子邮件发送模块
透明数据生成模块
第一实时更新处理模块
邮件服务器 3
普通邮件服务器
专有邮件服务器
收件终端 2
第二电子邮件接收模块
透明数据提取模块
网络侦测与破解
应用服务器 4
第一电子邮件接收模块
电子邮件代理网关
数据中心
第二实时更新处理模块
第二电子邮件发送模块
透明数据存储模块
透明算法策略中心
11
12
13
21
22
31
32
41
42
43
44
45
46
47

图1

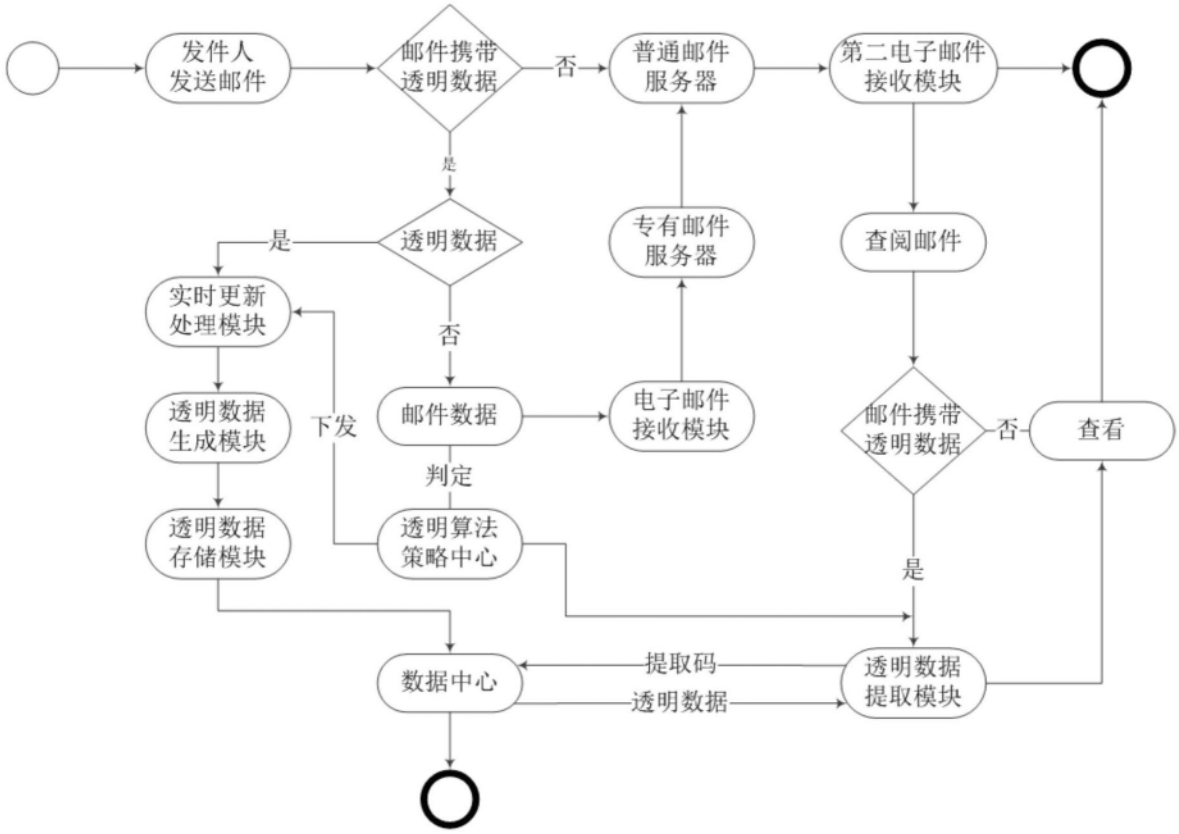

发件人发送邮件
邮件携带透明数据
否
普通邮件服务器
第二电子邮件接收模块
是
透明数据
是
专有邮件服务器
查阅邮件
实时更新处理模块
否
透明数据生成模块
下发
邮件数据
电子邮件接收模块
邮件携带透明数据
否
查看
判定
透明数据存储模块
透明算法策略中心
是
数据中心
提取码
透明数据
透明数据提取模块

图2