



(12) 发明专利

(10) 授权公告号 CN 1522516 B

(45) 授权公告日 2010.10.06

(21) 申请号 02813238.6

(22) 申请日 2002.06.18

(30) 优先权数据

0102437/1 2001.07.04 SE

(85) PCT申请进入国家阶段日

2003.12.30

(86) PCT申请的申请数据

PCT/SE2002/001220 2002.06.18

(87) PCT申请的公布数据

W02003/005636 EN 2003.01.16

(73) 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

(72) 发明人 刘易斯·巴里加 简一埃里克·芒斯

(74) 专利代理机构 中国专利代理(香港)有限公司

72001

代理人 杨凯 罗朋

(51) Int. Cl.

H04L 9/00(2006.01)

(56) 对比文件

Heiko Thimm 等. A Mail-Based Teleservice Architecture for Archiving and Retrieving Dynamically Composable Multimedia Documents. Lecture Notes In Computer Science

Proceedings of the International COST 237 Workshop on Multimedia Transport and Teleservices Vol. 882. 1994, Vol. 88214-34.

审查员 唐明明

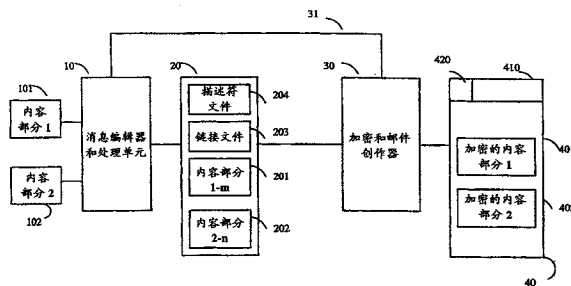
权利要求书 2 页 说明书 7 页 附图 4 页

(54) 发明名称

多内容电子邮件的安全标题信息

(57) 摘要

多内容电子邮件具有包括单独加密的内容部分的正文部分和包括明文部分和加密部分的标题部分。加密标题部分包括描述符段和链接段。链接段指定内容部分之间的关系。描述符段提供诸如信息格式等与各正文内容部分有关的信息。描述符段还提供信息用于对诸如授权要求等任何内容部分进行访问。访问信息可包括可执行代码,例如用于建立协商过程以访问远程信息服务器处的链接信息。还公开了用于下载和解密电子邮件标题部分和分析描述符段的装置。用户可以根据从描述符段确定的要求来选择任何正文内容部分进行下载。



1. 一种用于创建多内容电子邮件的方法,所述多内容电子邮件具有标题部分和正文部分,其特征在于以下步骤:

形成所述正文部分,使得它包括至少一个单独加密的信息单元;以及

形成所述标题部分,使得它包括加密标题部分,所述加密标题部分包括与所述正文部分的所述至少一个单独加密的信息单元相关的加密描述信息和加密访问信息,并使得所述标题部分可与所述正文部分分开下载。

2. 如权利要求 1 所述的方法,其特征在于所述加密访问信息至少包括程序可执行代码。

3. 如权利要求 2 所述的方法,其特征在于所述可执行代码被配置为在接收所述多内容电子邮件的客户机终端执行,以及在执行所述可执行代码时,使所述客户机终端通过安全连接连接到远程服务器。

4. 如权利要求 1 所述的方法,其特征在于从输入文件提取至少部分所述加密描述信息,其中所述输入文件通过文字处理软件、照相装置生成或从存储单元进行检索。

5. 如权利要求 4 所述的方法,其特征在于从远程服务器检索所述输入文件。

6. 如权利要求 1 所述的方法,其特征在于从至少一个远程服务器检索与所述正文部分的所述至少一个单独加密的信息单元相关的所述加密访问信息。

7. 一种用于创建多内容电子邮件的装置,所述多内容电子邮件具有标题部分和正文部分,其特征在于所述装置包括:

用于形成所述正文部分的单元,使得所述正文部分包括至少一个单独加密的信息单元;以及

用于形成所述标题部分的单元,使得所述标题部分包括加密标题部分,所述加密标题部分包括与所述正文部分的所述至少一个单独加密信息单元相关的加密描述信息和加密访问信息,并使得所述标题部分可与所述正文部分分开下载。

8. 如权利要求 7 所述的装置,其特征在于所述加密访问信息至少包括程序可执行代码。

9. 如权利要求 8 所述的装置,其特征在于所述可执行代码被配置为在接收多内容电子邮件的客户机终端执行,以及在执行所述可执行代码时,使所述客户机终端通过安全连接连接到远程服务器。

10. 如权利要求 7 所述的装置,其特征在于所述装置还包括用于从输入文件提取至少部分所述加密描述信息的单元,其中所述输入文件通过文字处理软件、照相装置生成或从存储单元进行检索。

11. 如权利要求 10 所述的装置,其特征在于所述装置包括用于从远程服务器检索至少所述输入文件的单元。

12. 如权利要求 7 所述的装置,还包括用于从至少一个远程服务器检索与所述正文部分的所述至少一个单独加密的信息单元相关的所述加密访问信息的单元。

13. 一种用于经电信链路访问多内容电子邮件的装置,其特征在于所述装置还包括:

用于与电子邮件的正文部分分开下载和解密所述电子邮件的标题部分的单元;

用于从所述标题部分提取描述信息和访问信息的单元,所述描述信息和访问信息与所述正文部分的至少一个信息单元相关;

用于根据所述描述信息生成显示的用户界面,用于从所述正文部分的所述至少一个信息单元中选择信息单元的单元;以及

用于处理与所选信息单元相关的所述访问信息以及用于根据所处理的访问信息来访问所选信息单元的单元。

14. 如权利要求 13 所述的装置,其特征在于所述访问信息至少部分包括程序可执行代码。

15. 如权利要求 14 所述的装置,其特征在于所述用于处理所述访问信息的单元包括用于执行所述程序可执行代码从而使所述装置通过安全连接连接到远程服务器的单元。

16. 一种用于经电信链路通过设备访问多内容电子邮件的方法,其特征在于所述方法包括以下步骤:

与电子邮件的正文部分分开下载和解密所述电子邮件的标题部分;

从所述标题部分提取描述信息和访问信息,所述描述信息和访问信息与所述正文部分的至少一个信息单元相关;

根据所述描述信息生成并显示用户界面,用于从所述正文部分的至少一个信息单元中选择信息单元;以及

处理与所选信息单元相关的所述访问信息,以及

根据所处理的访问信息访问所选信息单元。

17. 如权利要求 16 所述的方法,其特征在于所述访问信息至少部分包括程序可执行代码。

18. 如权利要求 17 所述的方法,其特征在于在所述设备执行所述程序可执行代码,使所述设备通过安全连接连接到远程服务器。

多内容电子邮件的安全标题信息

技术领域

[0001] 本发明一般涉及电子邮件通信,更具体地说,涉及在传输多内容电子邮件时提高安全性的方法及其装置。

背景技术

[0002] 电子邮件是众所周知并且广泛使用的异步通信形式。同样变得普遍的是将文件附在电子邮件或者将到存储在远处的信息的链接附在电子邮件上。进一步的技术发展允许创建复杂的多内容电子邮件,也称为带附件的电子邮件,其中包括多个不同类型的链接邮件正文部分。由于电子邮件成为许多商业的基础结构的重要部分,因此安全性方面成为主要问题。常见的是通过因特网传送电子邮件。但是,标准因特网电子邮件是不安全的。因此,加密和/或数字签名常被用于保护电子邮件内容免受不想要的公开或用于保持完整性。实际上,在因特网上,当强烈地需要端到端的安全性时,安全电子邮件是当今在处理机密电子邮件、比如公司或私人电子邮件时唯一可接受的解决方案。

[0003] 变得普遍的还有通过移动装置,比如移动电话或者个人数字助理(PDA)访问邮箱,它们通过无线接口与网络通信。尽管这样的装置功能日益增加,但在限制可以处理并显示给用户的信息方面仍然存在局限。同样重要的是有效地利用无线链路并且仍能捕获基本的电子邮件信息。因此,可能有利的是,如果客户具有有关收到的多内容电子邮件的结构的信息,并且还能选择复杂多内容电子邮件的若干部分在有限能力的无线链路上传送。还可能有利的是,对需要有关电子邮件结构和内容的信息的电子邮件执行复杂操作。为了在传统电子邮件系统中执行这样的操作,服务器必须完全有权使用电子邮件正文。因此,在这种情况下,在客户机和服务器之间必须具有信托关系,但在服务器位于因特网的公用域时却没有这种关系。相反,如果对电子邮件加密,服务器就没有办法确定其结构,因为电子邮件作为整体加密了因而无法执行上述操作。客户机只能下载整个电子邮件并对其解密,以便得到有关其结构的信息。

[0004] 因此,存在涉及对复杂多内容电子邮件的处理的问题,其中该邮件通过有限能力的无线链路在公共域中的邮件服务器中处理。

[0005] 另一问题涉及移动装置的使用,这些装置通过无线链路通信,并在处理复杂多媒体电子邮件时具有有限能力。如果用户可以选择下载复杂电子邮件的哪些部分将是有益的,以免不必要地使移动装置超负荷而导致过长的处理时间。

[0006] 还有一个问题涉及这样的事实:电子邮件在承载的数据量方面可能是有限的。复杂多内容电子邮件可能包括大的多媒体文件,容易超过对电子邮件大小的任何限制。允许将大文件附在电子邮件上,超过最大电子邮件大小的限制但仍允许用户安全访问所附信息将是有益的。

[0007] 因此,需要消除上述已知电子邮件系统不足的方法和装置。

[0008] 已知几种用于在因特网上保护电子邮件的方法,如基于标准 S/MIME。事实上, Pretty Good Privacy(极好的隐私性, PGP) 标准在本领域也是众所周知的。但是,这些方

法只允许安全电子邮件进行点到点的通信,即在双方具有认证或者公共密钥对的情况下。对于域到点的邮件,例如,从公司(公司域)到公共域中的接收方的邮件,已经提议了基于网关的解决方案。1998年2月24日提交的例示性的、申请人的受让人的共同未决的美国专利申请系列号09/198822,题为“安全性数据对象的方法和系统”中,公开了一种方法,其中来自一个域的明文电子邮件在离开一个域之前由网关自动进行安全保护。IETF提议的协议描述了一种安全电子邮件方法,用于域到域的安全性,它同样也基于网关。在域到点或者域到域的安全电子邮件中,在各域边缘的网关执行部分或全部电子邮件保护。在部分保护的情况下,网关保护(例如,通过加密)电子邮件消息的一些部分,一般是正文,使电子邮件消息的一些部分安全,但标题仍为明文。在完全保护的情况下,整个电子邮件,正文加标题,都受到保护(例如加密)。最小限度的标题部分包括传递该消息所需的信息(一般为接收方的地址),并且该部分仍不被保护。保护至少部分标题的理由是标题可以揭示潜在的机密信息并且还可以使跟踪用户的通信行为成为可能。整个标题作为完全保护的电子邮件的受保护正文部分中的正文部分提供。

[0009] 在客户侧,在利用完全保护电子邮件时,标准电子邮件客户机,为了访问整个标题进行分析,它必须请求下载整个电子邮件。如果客户是通过空中接口连接的移动客户,这是不方便的。2000年9月26日提交的申请人的受让人的共同未决的美国专利申请系列号09/671758,题为“基于代理的电子邮件标题信息的安全处理”中,公开了一种完全保护电子邮件的方法,该方法还允许客户机在下载正文部分之前分析标题信息。但是,这种方法仅限于具有单个正文部分的电子邮件并且不适用于多内容电子邮件。

[0010] 多内容邮件还可包含复杂结构,比如链接邮件正文不同部分的结构。H. Thimm等人的(“用于归档和检索动态组成的多媒体文件的基于邮件的电信业务体系结构”,XP 000585292)描述了用于归档和检索多媒体文件的配置。邮件正文的特定链接部分描述邮件的不同内容部分之间的关系。客户机使用专用的协议访问多内容邮件的部分或者根据客户喜好建立电子邮件的实例。H. Thimm等人的配置还包括在特定网络节点存储信息并在电子邮件中包括检索该信息的引用。对这种配置的需要源于这样的事实:可能对附到电子邮件上的文件的大小存在限制。

[0011] R. Ludwig(德国专利19718654,“Kommunikationssystem für Elektronische Nachrichten”)公开了一种配置,该配置使用分配数据块来描述复杂多内容电子邮件的结构。

[0012] 但是,这些文件既没有解决保护电子邮件的问题,也没有解决安全访问存储在网络节点并只通过引用包括在电子邮件中的信息的问题。

[0013] C. Gehrman 在题为“保护任意通信业务”的瑞典专利申请0002962-9中描述了如何保护任意通信业务,例如用于访问存储文件。根据Gehrman,请求访问例如加密信息等安全信息的用户首先下载包括可执行代码的代理。在该方法的第一步骤中,对业务提供商以及用户的客户机进行验证。代理可以包括用于访问诸如付款要求的条件,并且还包括用于密钥的安全交换以及用于加密/解密数据的方法。成功执行代理代码将实现业务提供商和客户机之间的安全通信。代理代码最好使用公共计算平台以及语言,例如Java™虚拟机以及Java™字节代码计算语言。因此,该方法中用于保护服务器中的信息的详细情况可包括在可执行代码中。所以,通过这种保护存储在网络服务器中的信息的方法提供了灵活的访

问。

[0014] 利用描述符文件来描述对象文件的内容也可从电子邮件通信以外的其它领域得知。例如, Microsoft Office 工具生成的文件具有描述对象文件的各种属性的属性文件。图像标准, 例如 MPEG7 和 JPEG2000, 允许包括描述信息。这种信息中的一些, 例如对象文件的大小, 可以由系统生成, 而用户可以指定其它信息。变得常见的是使用可扩展标记语言 (XML), 该语言由万维网组织 (<http://www.w3.org/>) 规定以得到通用的描述格式。

[0015] 附在电子邮件上的多媒体文件可以由用户在本地生成。但是, 通过连接到业务节点从业务提供商得到多媒体信息也是常见的。然后, 业务提供商可允许自由访问有限的信息, 但将只在付款之后才允许访问完整信息。国际申请 WO 00/31964 公开了一种方法和装置, 用于部分加密和逐行传输图像。例如根据 JPEG 格式对图像编码, 比如形成可独立加密的编码单位流。图像标题包括指定各编码单位是如何加密的加密标题。该信息可包括会话关键字和加密算法标识符。可以保护与安全性有关的数据, 例如利用诸如 Diffie Hellmann 或 RSA (Ravest-Shamir-Adleman) 等公共密钥算法。

[0016] 尽管上述参考文献一般地解决了描述对象文件的属性以及通过数据网络安全访问文件的问题, 但是, 它们没有公开编译来自几个源的多内容安全电子邮件, 从而允许对各个电子邮件正文部分的独立安全访问。

发明内容

[0017] 本发明的一个目的是提供一种方法和系统, 用于安全访问多内容结构的电子邮件。

[0018] 本发明的另一目的是提供一种方法和系统, 使用户能够控制下载安全电子邮件的正文部分。

[0019] 本发明的又一目的是提供一种方法和系统, 用于分析安全电子邮件标题信息, 从而至少部分地考虑到无线信道特征、客户机终端容量以及用户要求来确定下载控制动作。

[0020] 本发明的再一个目的是提供一种用于保护电子邮件的方法, 其中包括常规的对位于特定网络节点的信息的安全访问。

[0021] 根据本发明的最佳实施例, 安全多内容电子邮件包括至少一个加密正文部分和至少部分加密的标题部分。所述至少加密正文部分可表示完整的媒体文件、媒体文件的一部分或者到存储在网络节点中的信息的链接。所述至少部分加密的标题部分具有: 第一明文标题部分, 其中包括用于传递电子邮件的最小限度的信息; 以及第二加密部分, 该部分至少包括完整的标题信息、正文结构描述部分以及用于访问正文部分的信息。客户机, 例如移动终端, 可以请求下载标题信息以及单独地从其中下载指定的正文部分。通过对所述加密标题结构部分解密并对其进行分析, 客户机可确定要后续下载的正文部分。位于电子邮件服务器之外的位置的明文状态的正文部分可以按 H. Thimm 等人所述的进行引用。但是, 在远程信息被保护的情况下, 需要进行包括验证和加密的过程。本发明公开了一种方法, 用于常规地访问通过引用包括在安全电子邮件中的这种信息。

[0022] 按照本发明的实施例, 提供一种方法, 用于创建多内容电子邮件, 所述多内容电子邮件具有标题部分和正文部分, 其特征在于以下步骤: 形成所述正文部分, 使得它包括至少一个单独加密的信息单元; 以及形成所述标题部分, 使得它包括加密标题部分, 所述加密标

题部分包括与所述正文部分的所述至少一个单独加密的信息单元相关的加密描述信息和加密访问信息,并使得所述标题部分可与所述正文部分分开下载。

[0023] 按照本发明的实施例,提供一种装置,用于创建多内容电子邮件,所述多内容电子邮件具有标题部分和正文部分,其特征在于所述装置包括:用于形成所述正文部分的部件,使得所述正文部分包括至少一个单独加密的信息单元;以及用于形成所述标题部分的部件,使得所述标题部分包括加密标题部分,所述加密标题部分包括与所述正文部分的所述至少一个单独加密信息单元相关的加密描述信息和加密访问信息,并使得所述标题部分可与所述正文部分分开下载。

[0024] 按照本发明的实施例,提供一种设备,用于通过电信链路访问多内容电子邮件,所述设备包括显示部件和输入部件,其特征在于所述设备还包括:用于与电子邮件的正文部分分开下载和解密所述电子邮件的标题部分的部件;用于从所述标题部分提取描述信息和访问信息的部件,所述描述信息和访问信息与所述正文部分的至少一个信息单元相关;用于根据所述描述信息生成显示的用户界面,用于从所述正文部分的所述至少一个信息单元中选择信息单元的部件;以及用于处理与所选信息单元相关的所述访问信息以及用于根据所处理的访问信息来访问所选信息单元的部件。

[0025] 按照本发明的方法,提供一种方法,用于经电信链路通过设备访问多内容电子邮件,所述设备包括显示部件、处理部件和输入部件,其特征在于所述方法包括以下步骤:与电子邮件的正文部分分开下载和解密所述电子邮件的标题部分;从所述标题部分提取描述信息和访问信息,所述描述信息和访问信息与所述正文部分的至少一个信息单元相关;根据所述描述信息生成并显示用户界面,用于从所述正文部分的至少一个信息单元中选择信息单元;以及处理与所选信息单元相关的所述访问信息,以及根据所处理的访问信息访问所选信息单元。

[0026] 这些目的通过所附权利要求中陈述的系统和方法实现。此外,本发明适用性的范围从下文给出的详细描述变得显而易见。但是,应该理解,尽管详细描述以及特定例示显示了本发明的最佳实施例,但它们只是作为例示给出的,因为根据这里的详细描述,本发明范围内的各种变化和修改对本领域的技术人员都将变得显而易见。

附图说明

[0027] 可以通过参考以下详细描述连同附图获得对本发明的系统和方法的更完全理解,其中:

[0028] 图 1 显示发送侧的例示配置。

[0029] 图 2 是说明建立多内容电子邮件的步骤的流程图。

[0030] 图 3 说明接收侧的例示配置。

[0031] 图 4 是说明在访问收到的多内容电子邮件时的步骤的流程图。

具体实施方式

[0032] 现在就参考显示本发明最佳实施例的附图在下文中更全面地描述本发明。参考图 1,标号 10 表示输入处理单元。单元 10 对包括多个消息部分的消息进行编译,多个消息部分中的两个图示为 101 和 102。诸如输入文件 101 的输入文件可以例如通过文字处理软件、

通过照相装置用多种方式生成或从存储单元进行检索。单元 10 具有识别输入文件类型并相应调整其处理的能力。

[0033] 用户可通过定义正文部分之间的链接来建立超媒体电子邮件。链接也可以指在链接激活时检索相应正文部分的外部位置。单元 10 可包括用于识别诸如输入文件 101 和 102 的输入文件类型的功能,以及用于提取任何相关属性文件,例如涉及字处理文件或涉及诸如 JPEG 文件的图像文件的属性文件的功能。从单元 10 的输出显示为 20。正文部分之间的链接在链接文件 203 中编译。对内容部分 101 和 102 的编辑和处理得到正文部分 1-m 和 2-n,其中 m 和 n 表示原始正文部分现在可能存在的几种型式,例如,表示不同的图像信息部分。图像信息部分可以例如表示更高阶的位平面或者特定的图像部分,比如 JPEG2000 标准中定义的感兴趣区("JPEG2000 Part I Final Draft International Standard", ISO/IEC FDIS15444-1)。此外,从单元 10 的输出包括描述符文件 204,其中包括与各种内容部分(例如内容部分 201 和 202)有关的数据。描述符文件数据可包括访问信息,用于定位和检索正文部分,以及与内容部分的大小、内容部分的类型和编码方法有关的数据。客户机可利用这种信息请求下载所选部分,例如图像,并可在几个与内容和分辨率有关的步骤中重新建立图像。可以提供输入文件,图 1 的 101 例示的内容部分 1,用于在信息服务器进行下载。在这种情况下,信息提供商可能只允许自由访问有限的信息,而完全访问要求满足某些条件。在准备多内容电子邮件时,用户可检索免费信息,以及另外的用于对完整信息进行条件访问的可执行访问代码。访问代码可以包括在图 1 所示描述符文件 204 中或者从其引用到电子邮件正文部分中的存储位置。部分免费信息可包括对完整信息的描述。在电子邮件接收方尝试访问免费信息以外的其它信息的任何时候,执行访问代码并且可以在满足特定条件时对所请求的信息部分进行下载。从业务提供商检索信息共同的第一步骤是验证该提供商。通过在电子邮件中包括访问代码,就已经进行了验证,并不需要由电子邮件接收方执行。但是,如果在接收方激活到远程服务器的链接的时候下载访问代码,那么对各个这样的远程服务器的验证就消耗不必要的计算能力。根据最佳实施例,接收客户机将有利地只需要验证电子邮件的发送方。

[0034] 输入文件,例如图 1 所示 102 处的内容部分 2,还可涉及电子邮件的发送方拥有的信息,但该信息最好存储在业务节点处。原因可能是信息量很大和/或发送方希望在其它通信中重新利用该信息。在这种情况下,电子邮件的发送方将加密内容部分存储在远程服务器中并准备如上所述将包括在电子邮件中的访问代码和描述信息。在正文部分包括完整信息的情况下,即不是到远程位置的链接的情况下,则访问代码减少为电子邮件中的内部地址。访问代码还可以包括关键字和加密算法,允许用户对正文部分进行解密。在电子邮件的发送方已在电子邮件中存储了到远程存储位置的链接时,访问代码包括到存储信息的地址信息,并且还可以包括关键字和加密算法。最后,如果至少部分电子邮件正文部分是从业务提供商检索得到的,则访问代码包括可执行代码。可执行代码使客户机连接到业务节点,并交换密钥和其它信息,如信用卡信息,用于建立安全下载所请求信息的条件。

[0035] 在 30,显示了加密和邮件创作者单元。单元 30 单独加密各种正文部分,如正文部分 1-m 和 2-n,并在图示为 401 和 402 的输出电子邮件 40 的正文部分中插入加密部分。单元 30 还加密描述符文件 204 并将加密的结果描述符文件插入到电子邮件标题,作为扩展字段 410。本发明的此实施例中加密和邮件创作者 30 利用了因特网标准 RFC822 的功能,根据

该标准,在某些情况下可以产生受保护的电子邮件。具体地说,RFC822 标准允许电子邮件的标题包含附加的任意长度的扩展标题字段。链接文件 203,修改为反映加密正文部分的正确位置,可以包括在扩展字段 410 中或者作为电子邮件 40 的单独正文部分。此外,单元 30 在 31 从输入处理单元 10 接收有关到预定接收方的电子邮件的路由选择的信息。该信息作为明文输入到电子邮件中作为最小标题 420。标题部分 420 最少包括路由传递所需的有限信息,因此,不允许对电子邮件内容或流量进行分析,或者对电子邮件通信进行网络分析。这种类型的信息只在邮件的加密部分中提供。

[0036] 图 2 是说明根据本发明的多内容安全电子邮件的创建中涉及的步骤的流程图。

[0037] 在步骤 201,用户编译各种内容部分,内容描述信息和用于访问如位于远程服务器的内容部分的访问信息。在 202,对内容部分进行分析,并生成电子邮件描述符文件,其中包括含远程存储的内容部分的内容部分的描述。该步骤还包括对访问代码的处理,以便插入到电子邮件描述符文件中或者单独的正文部分中。

[0038] 步骤 203 涉及创建内容部分之间的链接以及链接文件的生成。在步骤 204,各内容部分单独加密并被插入到所得到的安全电子邮件的正文部分中。

[0039] 在步骤 205,对描述符文件进行加密并将其插入到所得到的电子邮件标题中作为扩展字段。在步骤 206,将链接文件加入到所得到的电子邮件中,作为扩展标题字段的一部分或者单独的正文部分。在步骤 207 创建最小电子邮件标题。最小标题允许路由传递,但其中不包括任何其它信息。在步骤 208 将所得到的安全多内容电子邮件存储在非可信的邮件服务器中。

[0040] 最好,移动客户机能够分析电子邮件的内容和结构,并请求只下载这样的一些部分:它们能够通过空中接口有效传递并且考虑移动客户机的处理能力能够由其进行处理。

[0041] 图 3 是接收客户机侧的例示装置。装置 30 可以实现为通过无线链路和网络通信的移动装置。根据图 3,在 301 提供无线电收发信机。控制单元 306 控制装置 30 的内部处理。在 302,显示了解密部件。下载的电子标题扩展部分,包括描述符文件,由部件 302 进行解密,并存储在存储部件 303,还包括链接信息。部件 308 执行对描述符文件的分析并通过控制单元 306 生成显示在显示和输入部件 307 上的用户界面。存储部件 304 包括至少第一解密内容部分,该部分可能还包括链接信息,如 309 所示。存储部件 304 可高速缓存几个内容部分或者在显示器 307 显示信息期间作为缓存部件。在单元 307 显示信息之前,信息处理单元 305 对信息进行处理,例如对 JPEG 图像进行解压缩。单元 305 可利用单元 303 描述符文件中提供的类型信息。从单元 303 通过内部链接 312 检索用于单元 305 的处理的这些和其它信息。取决于用户在显示和输入装置 307 上的输入,控制单元可在 310 请求部件 303 生成与所选内容部分有关的新用户界面,或者在 311 请求下载该内容部分。下载请求首先在 313 进行处理,其中涉及访问条件并可能导致执行用于与远程服务器进行通信的访问代码。单元 313 的输出导致直接向电子邮件服务器的负载请求或者通过收发信机 301 向远程服务器的负载请求。

[0042] 图 4 说明操作装置 30 中的例示步骤。

[0043] 在步骤 401,用户联络电子邮件服务器并选择电子邮件。附在电子邮件上的可以是签名或者证书,其中包括允许接收方验证发送方的公共密钥。然后,用户请求下载所述电子邮件的标题。在步骤 402,执行描述符文件并对其解密,如利用公共密钥算法。在步骤 403,

系统分析描述符文件并创建用户界面。涉及内容部分的基本数据可以通过指向表示符号来显示或得到,例如图示的所关注的 JPEG 图像区。在步骤 404,用户选择下载第一内容部分。第一内容部分例如包括含有到各种附件的超文本链接的总文本消息。在步骤 405,流程图区分具有链接的超文本消息的情况和具有普通附件的普通无链接消息的情况。在步骤 411,根据用户的手动中断过程结束。

[0044] 在步骤 407,用户激活超文本内容部分中与链接的内容部分有关的所选链接。类似的,在无链接内容部分的情况下,用户在步骤 406 选择附件。在步骤 408,系统向用户显示涉及所选正文部分并表征所述部分的型式的参数选择。这些参数可以例如涉及图像分辨率、图像颜色以及只包括所关注区域的标志,图像或音频的编码。在步骤 409,确定所选正文部分是否包括在电子邮件中,或者是否必须从远程服务器下载。在后一种情况下,可以执行访问代码,以建立与远程服务器的通信。在步骤 410,如果满足所有访问条件,则请求下载所选信息。

[0045] 尽管以上已经详细描述了本发明的例示实施例,但它并不限制本发明的范围,本发明可以用各种实施例实践。

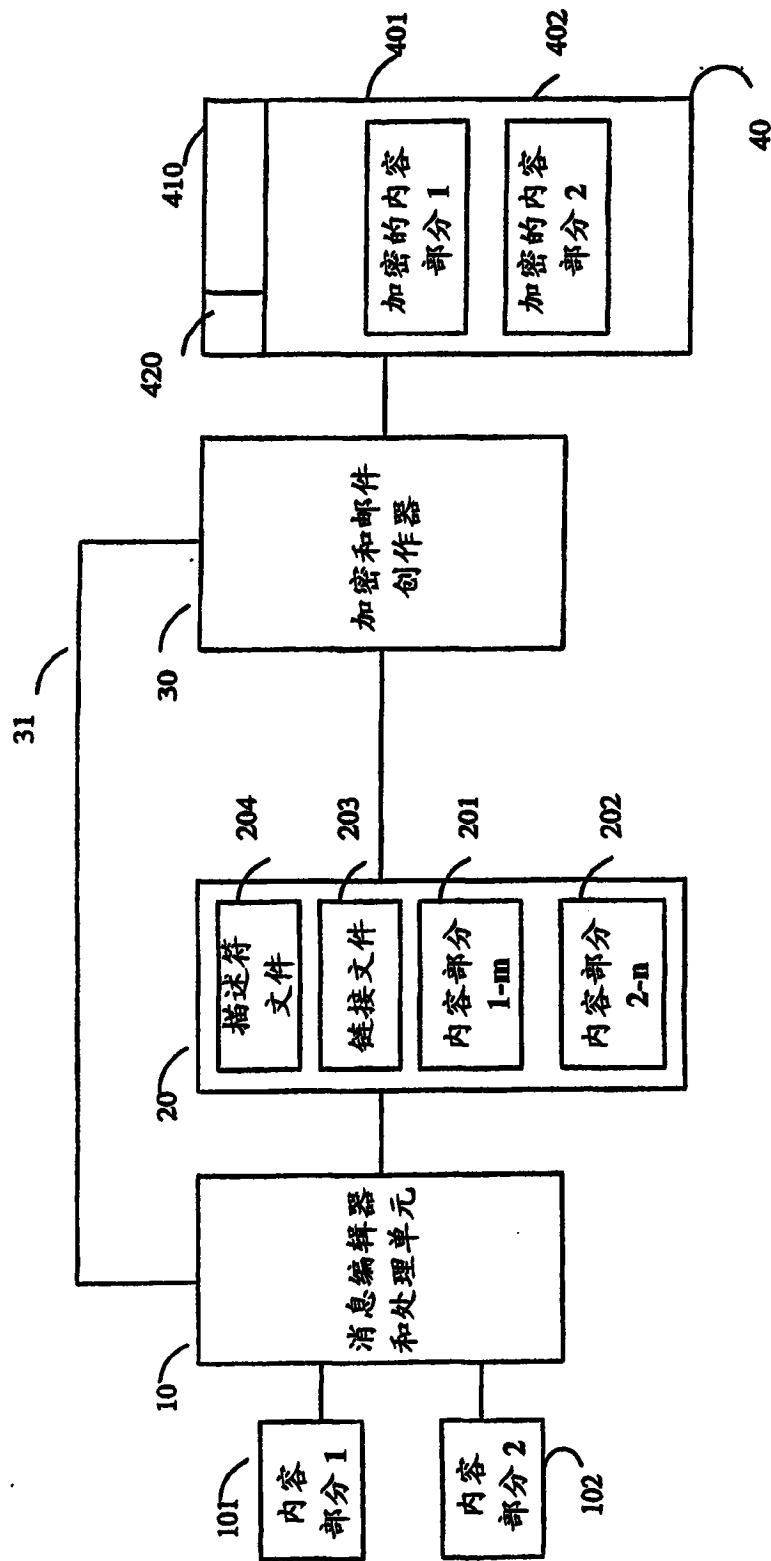


图 1

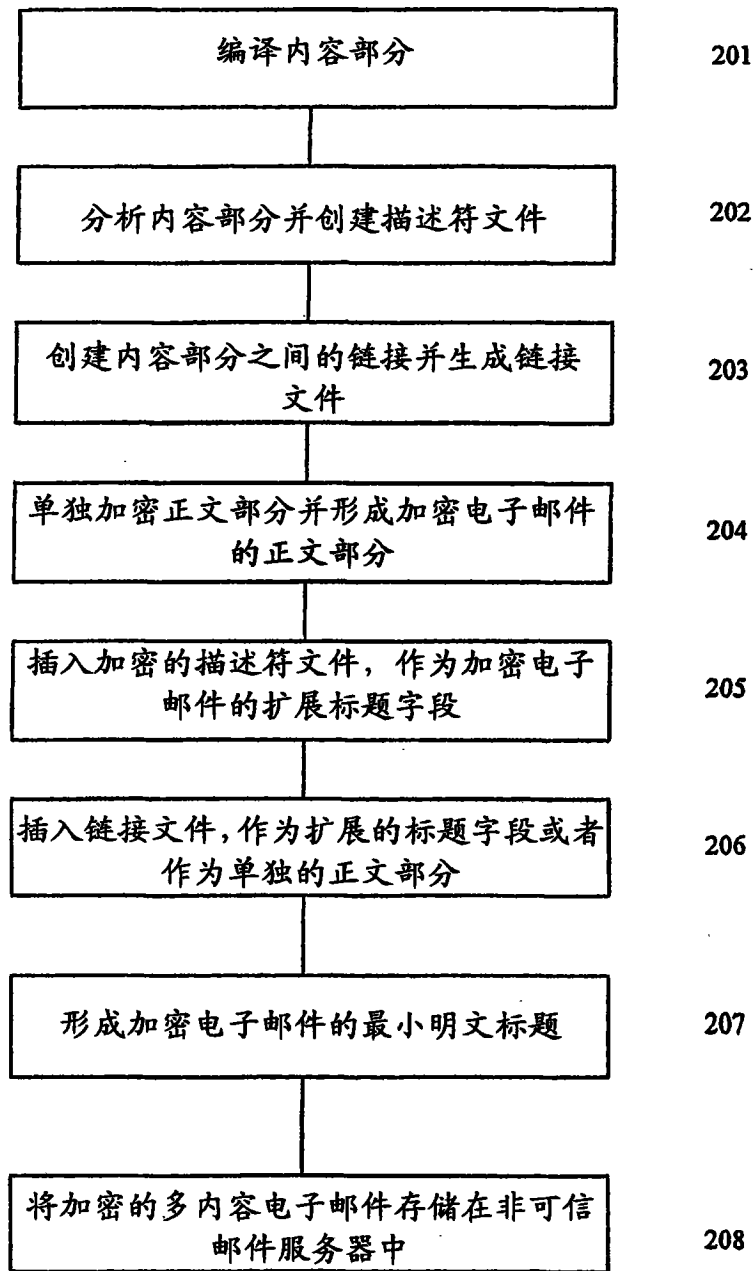


图 2

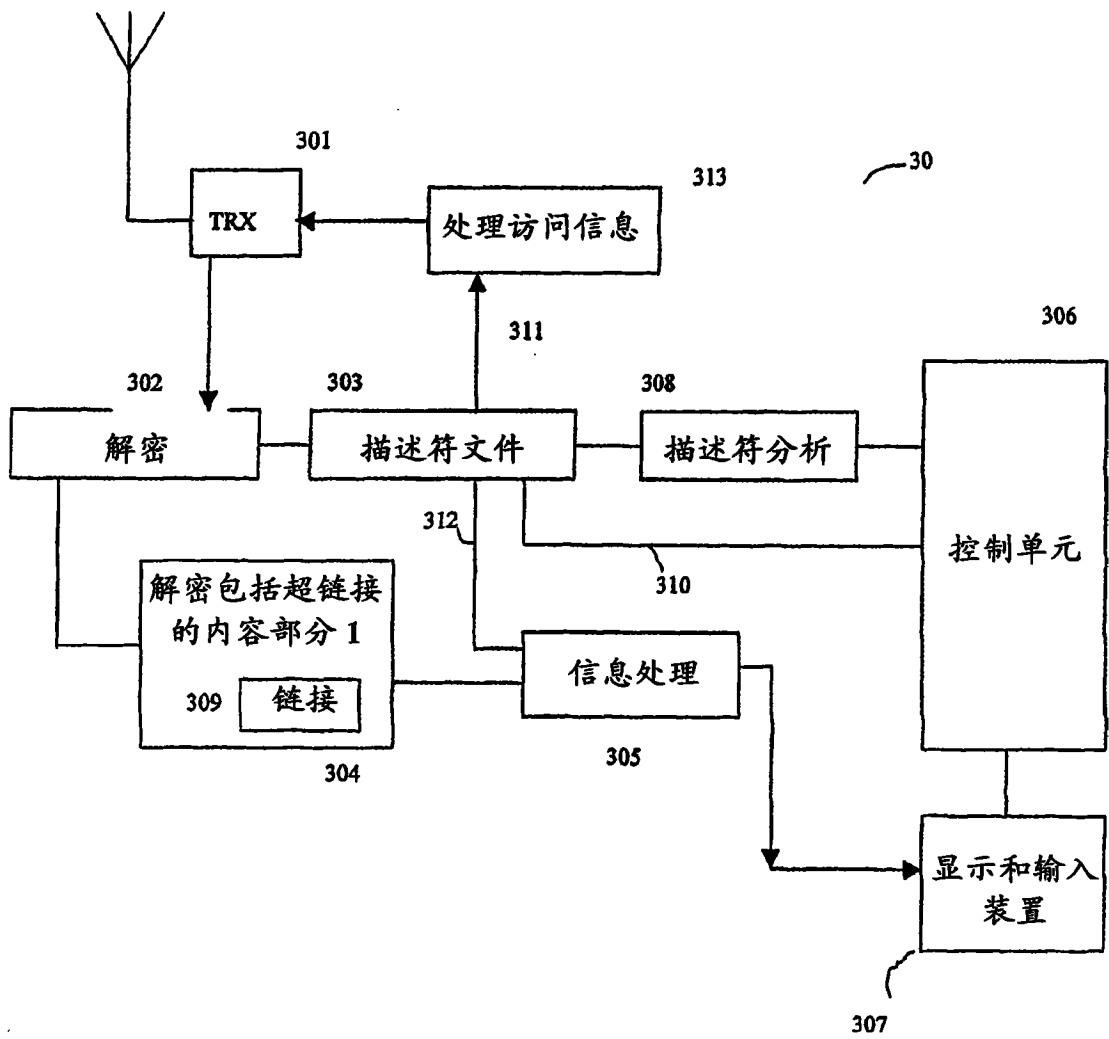


图 3

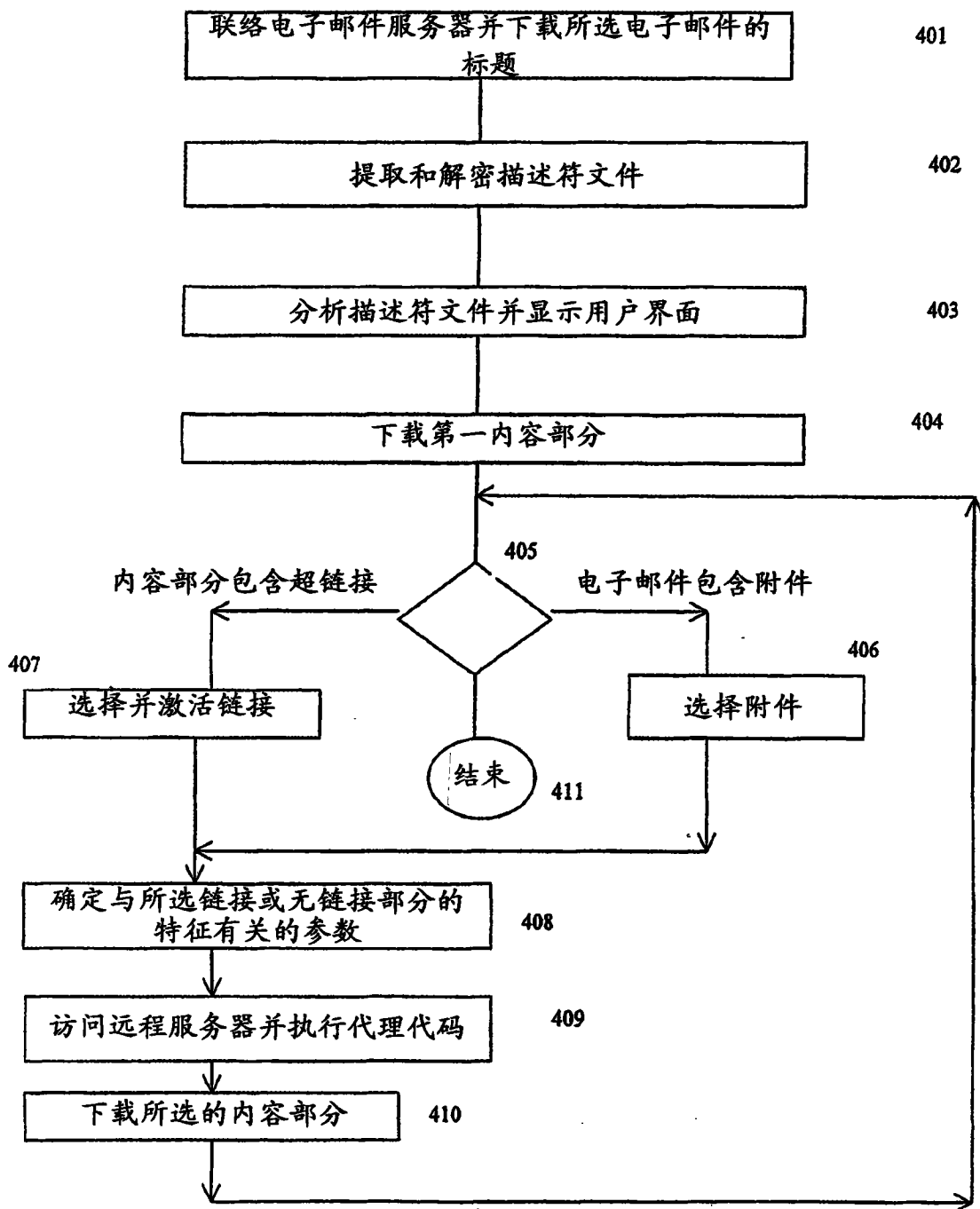


图 4