



(12) 发明专利

(10) 授权公告号 CN 101243464 B

(45) 授权公告日 2013.02.27

(21) 申请号 200680030076.2

H04L 12/58(2006.01)

(22) 申请日 2006.08.15

(56) 对比文件

(30) 优先权数据

11/206,010 2005.08.16 US

US 5832208 A, 1998.11.03,

US 6868436 B1, 2005.03.15,

CN 1510588 A, 2004.07.07,

(85) PCT申请进入国家阶段日

2008.02.18

US 6199103 B1, 2001.03.06,

US 6023723 A, 2000.02.08,

(86) PCT申请的申请数据

PCT/US2006/031966 2006.08.15

无. 电子邮件客户端软件-桌面. 《个人电脑》. 2004,

(87) PCT申请的公布数据

W02007/022253 EN 2007.02.22

审查员 王伟

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 B·J·特桑 S·格兰特

L·汉德尔沃 R·派格里

J·夏维尔

(74) 专利代理机构 上海专利商标事务所有限公

司 31100

代理人 张政权

(51) Int. Cl.

G06Q 10/10(2012.01)

权利要求书 3 页 说明书 7 页 附图 11 页

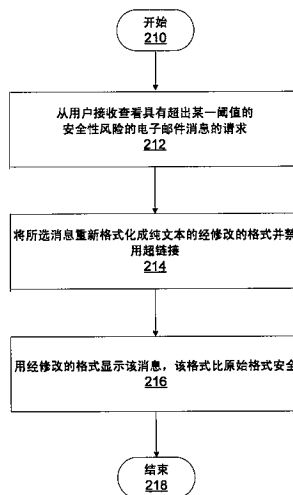
(54) 发明名称

增强电子邮件文件夹安全性

(57) 摘要

公开了增强电子邮件消息和文件夹的安全性的各种工艺和技术。被认为较不安全且具有较高安全性风险的消息,诸如未经请求的广告电子邮件(即, SPAM)和钓鱼消息,在某些情况中被重新格式化并用禁用超链接的纯文本显示。例如,垃圾电子邮件文件夹中的消息可被重新格式化并用禁用超链接的纯文本显示使得它们对用户交互而言更安全。

CN 101243464 B



1. 一种用于增强电子邮件应用程序中的电子邮件消息的安全性的方法,所述方法包括:

在电子邮件存储区中提供用户的垃圾文件夹,所述用户的垃圾文件夹用于存储发送给用户的被所述电子邮件应用程序标识为未经请求的广告电子邮件消息或钓鱼消息的多个垃圾电子邮件消息,其中所述用户的垃圾文件夹中的每个垃圾消息以从来源发送和由所述电子邮件应用程序接收的原始格式被存储;

在所述电子邮件存储区中提供用户的收件文件夹,所述用户的收件文件夹用于以由用户从所述垃圾文件夹移动到所述收件文件夹的原始格式来存储一所选消息,所选消息具有包含在该所选消息的正文中的至少一个超链接,所述至少一个超链接与统一资源定位符相关联;

响应于从用户接收查看所述垃圾文件夹中所选消息的请求,执行下述步骤:

将具有包含在该所选消息的正文中的至少一个超链接的所选消息从其原始格式重新格式化成经修改的格式,所述经修改的格式包括通过所述至少一个超链接被禁用来重新格式化所选消息的正文的纯文本格式(232);以及

用所述经修改的格式显示所选消息(234),其中,在所选消息的正文中,所述至少一个超链接可见但被禁用,而所述统一资源定位符以纯文本形式对用户可见;以及

响应于从用户接收查看由用户从所述垃圾文件夹移动到所述收件文件夹后的所选消息的请求,执行下述步骤:

如果该所选消息已经被标识为未经请求的广告电子邮件消息,则以原始格式来显示所选消息且所述至少一个超链接被启用;

如果该所选消息已经被标识为钓鱼消息,则以原始格式来显示所选消息且所述至少一个超链接被禁用。

2. 如权利要求1所述的方法,其特征在于,还包括以下步骤:

显示指示所选消息正用经修改的格式显示的通知(236)。

3. 如权利要求1所述的方法,其特征在于,还包括以下步骤:

从所述用户接收指示所述用户正试图访问在所选消息中被禁用的特定超链接的选择(232);以及

阻止所述用户对所述特定超链接的访问(232)。

4. 如权利要求1所述的方法,其特征在于,还包括以下步骤:

从所述用户接收将所述垃圾文件夹中的特定消息作为新消息的附件转发的请求(272);以及

将所述特定消息重新格式化以作为所述新消息的附件(274)。

5. 如权利要求1所述的方法,其特征在于,所述电子邮件消息在其原始格式中包括HTML和至少一个图像。

6. 一种用于增强电子邮件应用程序中的电子邮件消息的安全性的设备,所述设备包括:

用于在电子邮件存储区中提供用户的垃圾文件夹的装置,所述用户的垃圾文件夹用于存储发送给用户的被所述电子邮件应用程序标识为未经请求的广告电子邮件消息或钓鱼消息的多个垃圾电子邮件消息,其中所述用户的垃圾文件夹中的每个垃圾消息以从来源发

送和由所述电子邮件应用程序接收的原始格式被存储；

用于在所述电子邮件存储区中提供用户的收件文件夹的装置，所述用户的收件文件夹用于以由用户从所述垃圾文件夹移动到所述收件文件夹的原始格式来存储一所选消息，所选消息具有包含在该所选消息的正文中的至少一个超链接，所述至少一个超链接与统一资源定位符相关联；

用于响应于从用户接收查看所述垃圾文件夹中所选消息的请求的装置，包括：

用于将具有包含在该所选消息的正文中的至少一个超链接的所选消息从其原始格式重新格式化成经修改的格式的装置，所述经修改的格式包括通过所述至少一个超链接被禁用来重新格式化所选消息的正文的纯文本格式(232)；以及

用于用所述经修改的格式显示所选消息(234)的装置，其中，在所选消息的正文中，所述至少一个超链接可见但被禁用，而所述统一资源定位符以纯文本形式对用户可见；以及

用于响应于从用户接收查看由用户从所述垃圾文件夹移动到所述收件文件夹后的所选消息的请求的装置，包括：

如果该所选消息已经被标识为未经请求的广告电子邮件消息，用于以原始格式来显示所选消息且所述至少一个超链接被启用的装置；

如果该所选消息已经被标识为钓鱼消息，用于以原始格式来显示所选消息且所述至少一个超链接被禁用的装置。

7. 如权利要求6所述的设备，其特征在于，还包括：

用于显示指示所选消息正用经修改的格式显示的通知(236)的装置。

8. 如权利要求6所述的设备，其特征在于，还包括：

用于从所述用户接收指示所述用户正试图访问在所选消息中被禁用的特定超链接的选择(232)的装置；以及

用于阻止所述用户对所述特定超链接的访问(232)的装置。

9. 如权利要求6所述的设备，其特征在于，还包括：

用于从所述用户接收将所述垃圾文件夹中的特定消息作为新消息的附件转发的请求(272)的装置；以及

用于将所述特定消息重新格式化以作为所述新消息的附件(274)的装置。

10. 一种用于改进电子邮件应用程序中的电子邮件消息的安全性的方法，包括以下步骤：

在计算设备上的电子邮件应用程序处以发送给用户的原始格式接收电子邮件消息，所述电子邮件消息包括在该电子邮件消息的正文中的至少一个超链接(224)，所述至少一个超链接与统一资源定位符相关联；

确定所述电子邮件消息为垃圾消息(226)；

标识所述电子邮件消息为未经请求的广告电子邮件消息或钓鱼消息；

将所述电子邮件消息置于所述电子邮件存储区中的用户的垃圾文件夹中，所述垃圾文件夹被用于存储发送给用户的被所述电子邮件应用程序标识为未经请求的广告电子邮件消息或钓鱼消息的垃圾消息，其中所述用户的垃圾文件夹中的所述电子邮件消息以从来源发送和由所述电子邮件应用程序接收的原始格式被存储；

在所述电子邮件存储区中提供用户的收件文件夹，所述用户的收件文件夹用于以由用

户从所述垃圾文件夹移动到所述收件文件夹的原始格式来存储所述电子邮件消息；

响应于从用户接收的查看所述垃圾文件夹中的所述电子邮件消息的请求(230)；

将所述电子邮件消息从其原始格式重新格式化成经修改的格式,所述经修改的格式包括通过所述至少一个超链接被禁用来重新格式化所述电子邮件消息的正文的纯文本格式;以及

用所述经修改的格式显示所述电子邮件消息,其中,在所述电子邮件的正文中,所述至少一个超链接可见但被禁用,而所述统一资源定位符以纯文本形式对用户可见;

响应于从用户接收查看由用户从所述垃圾文件夹移动到所述收件文件夹后的所述电子邮件消息的请求,执行下述步骤:

如果该电子邮件消息已经被标识为未经请求的广告电子邮件消息,则以原始格式来显示所述电子邮件消息且所述至少一个超链接被启用;

如果该电子邮件消息已经被标识为钓鱼消息,则以原始格式来显示所述电子邮件消息且所述至少一个超链接被禁用。

11. 如权利要求 10 所述的方法,其特征在于,进一步包括:

从所述用户接收查看所述垃圾文件夹中多个垃圾消息中的每个垃圾消息的请求;以及响应于查看所述垃圾文件夹中每个垃圾消息的请求,重新格式化并以经修改的格式显示每个垃圾消息。

12. 如权利要求 10 所述的方法,其特征在于,还包括:

显示指示所述电子邮件消息正用所述经修改的格式显示的通知(236)。

13. 如权利要求 10 所述的方法,其特征在于,所述电子邮件消息在其原始格式中包括 HTML 和至少一个图像。

14. 如权利要求 10 所述的方法,其特征在于,所述电子邮件消息是未经请求的广告电子邮件(226)并被标识为 SPAM 消息。

15. 如权利要求 10 所述的方法,其特征在于,所述电子邮件消息是被设计成通过虚假地表示所述消息来自可信来源而从所述用户获取敏感信息的钓鱼消息(226)。

16. 如权利要求 10 所述的方法,其特征在于,还包括:

从所述用户接收指示所述用户正试图访问在所述电子邮件消息中被禁用的特定超链接的选择(232);以及

阻止所述用户对所述特定超链接的访问(232)。

17. 如权利要求 10 所述的方法,其特征在于,还包括:

从所述用户接收将所述垃圾文件夹中的特定消息作为新消息的附件转发的请求(272);以及

将所述特定消息重新格式化以作为所述新消息的附件(274)。

增强电子邮件文件夹安全性

[0001]

背景

[0002] 电子邮件 (email) 消息是各方之间通信的流行形式。不令人惊讶地,随着电子邮件使用的增加,电子邮件滥用也增加了。例如,公司通常使用电子邮件来向大量人员发送未经请求的广告电子邮件 (有时被称为 SPAM) 以推销其产品或服务。电子邮件消息也用于发送病毒作为附件,如被执行会引起损害,诸如通过用某种恼人的程序来感染接收方的计算机,或通过获取机密或敏感信息。近来,电子邮件消息也用于发送看上去是从接收方信任的来源发送的钓鱼 (phishing) 消息,并被设计来引诱接收方前往将从接收方获取机密信息的网站。某一用户每天都接收如数十甚至数百如此的不需要的消息并非是不常见的。这些不需要的消息因其本质而较不安全,且比接收方需要和 / 或期望的消息对用户的计算机潜在地更有破坏性。

[0003]

概述

[0004] 此处所述的是增强电子邮件消息和文件夹的安全性的各种工艺和技术。诸如未经请求的广告电子邮件 (即, SPAM) 和钓鱼消息 (即, 虚假地来自自己知且可信来源和 / 或包含至将从接收方获取机密信息的网站的链接的消息) 的往往较不安全且具有较高安全性风险的消息被重新格式化并在某些情况中用纯文本显示而禁用超链接。

[0005] 作为一个非限定性的示例,垃圾电子邮件文件夹的总体安全性可通过使用此处所述的一种或多种技术来改进,因为垃圾电子邮件文件夹中的消息被默认为往往是较不安全或潜在地更有破坏性的。当用户选择垃圾电子邮件文件夹中的特定消息来查看时,所选消息从原始接收的格式重新格式化为经修改的格式。经修改的格式包括禁用超链接的消息内容的纯文本。用户可将消息从垃圾电子邮件文件夹移动到另一文件夹,诸如收件箱。一旦处于收件箱或另一文件夹中,消息可用原始格式显示,但取决于消息的安全性风险情况而启用或禁用超链接。作为少数非限定性的示例,未经请求的广告电子邮件消息可在启用超链接的情况下用原始格式显示,而潜在地对用户更危险的钓鱼消息可能在禁用超链接的情况下用原始格式显示。各种其他变型均是可能的。

[0006] 提供该概述来以简化形式介绍将在以下详细描述中进一步描述的概念的选择。该概述并不旨在标识所述权利要求的主题的关键特征或本质特征,它也不旨在用于帮助确定所述权利要求的主题的范围。

[0007]

附图简述

[0008] 图 1 是本发明的一个方面的计算机系统的示意图。

[0009] 图 2 是本发明的一个方面中在图 1 的计算机系统上操作的电子邮件程序的示意图。

[0010] 图 3 是图 1 的系统的一个方面的高层过程流程图。

[0011] 图 4A 是用于图 1 的系统的一个方面、示出将电子邮件消息重新格式化成要向用户显示的经修改的格式所涉及各阶段的过程流程图的第一部分。

[0012] 图 4B 是用于图 1 的系统的一个方面、示出将电子邮件消息重新格式化成要向用户显示的经修改的格式所涉及各阶段的过程流程图的第二部分。

[0013] 图 5 是用于图 1 的系统的的一个方面、示出将电子邮件从一个文件夹移动至另一文件夹以及当从该另一文件夹选择时改变电子邮件显示的方式所涉及的各阶段的过程流程图。

[0014] 图 6 是用于图 1 的系统的的一个方面、示出用更安全的方式将现有电子邮件作为附件转发所涉及各阶段的过程流程图。

[0015] 图 7 是用于图 1 的系统的的一个方面、示出电子邮件消息如何用其原始格式出现的模拟屏幕。

[0016] 图 8 是用于图 1 的系统的的一个方面、示出如图 4A-4B 的各阶段中所述、图 7 的电子邮件消息如何用纯文本出现而超链接可见但被禁用的模拟屏幕。

[0017] 图 9 是用于图 1 的系统的另一方面、示出如图 4A-4B 的各阶段中所述、图 7 的电子邮件消息如何用纯文本出现而超链接被禁用并以纯文本呈现的模拟屏幕。

[0018] 图 10 是用于图 1 的系统的的一个方面、示出如图 6 的各阶段中所述将消息作为附件转发的模拟屏幕。

[0019] 详细描述

[0020] 为了促进对本发明的原理的理解,现在将参考附图中所示的实施例,并将使用特定的语言来描述它们。然而可以理解,并不旨在由此作出对本发明范围的限制。如本发明相关领域的技术人员通常会想到的,将会构思所述实施例的任何更改和其它修改,以及如此处所述的本发明的原理的任何其它应用。

[0021] 假设典型用户每天接收显著数量的不需要的电子邮件消息,并假设与这样的不需要消息相关联的安全性风险增加,这就需要帮助改进电子邮件消息和 / 或文件夹的安全的系统 and / 或技术。本发明在本系统的一个或多个方面中是针对增强电子邮件消息和 / 或文件夹的安全性,但本发明也用于除此以外的其它目的。此处所述的一个或多个技术可被实现为诸如 MICROSOFT[®] Office OUTLOOK[®] 的电子邮件软件程序内或来自与电子邮件交互的任何其它类型的程序或服务的功能部件。如将在此处更详细描述地,在本系统的一个方面中,往往较不安全且具有更高安全性风险的消息被重新格式化,并在某些情况中用纯文本显示而禁用超链接。

[0022] 图 1 示出了可在其上实现本发明的合适的计算系统环境 100 的示例。计算系统环境 100 只是合适的计算环境的一个示例,并不旨在对本发明的使用范围或功能提出任何限制。也不应该把计算环境 100 解释为对示例性操作环境 100 中示出的任一组件或其组合有任何依赖性 or 要求。

[0023] 本发明可用众多其它通用或专用计算系统环境或配置来操作。适合在本发明中使用的公知的计算系统、环境和 / 或配置的示例包括,但不限于,个人计算机、服务器计算机、手持或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费者电子产品、网络 PC、小型机、大型机、包含上述系统或设备中的任一个的分布式计算机环境等。

[0024] 本发明可在诸如程序模块等由计算机执行的计算机可执行指令的通用上下文中描述。一般而言,程序模块包括例程、程序、对象、组件、数据结构等,它们执行特定任务或实现特定抽象数据类型。本发明也可以在分布式计算环境中实现,其中任务由通过通信网络链接的远程处理设备执行。在分布式计算环境中,程序模块可以位于包括存储器存储设备在内的本地和远程计算机存储介质中。

[0025] 参考图 1, 用于实现本发明的一个示例性系统包括计算机 110 形式的通用计算设备。计算机 110 的组件可以包括, 但不限于, 处理单元 120、系统存储器 130 和将包括系统存储器在内的各种系统组件耦合至处理单元 120 的系统总线 121。系统总线 121 可以是若干类型的总线结构中的任一种, 包括存储器总线或存储器控制器、外围总线和使用各种总线体系结构中的任一种的局部总线。作为示例, 而非限制, 这样的体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、扩展的 ISA (EISA) 总线、视频电子技术标准协会 (VESA) 局部总线 and 外围部件互连 (PCI) 总线 (也被称为 Mezzanine 总线)。

[0026] 计算机 110 通常包括各种计算机可读介质。计算机可读介质可以是能够被计算机 110 访问的任何可用介质, 且包括易失性和非易失性介质、可移动和不可移动介质。作为示例, 而非限制, 计算机可读介质可以包括计算机存储介质和通信介质。计算机存储介质包括以任何方法或技术实现的用于存储诸如计算机可读指令、数据结构、程序模块或其它数据等信息的易失性和非易失性、可移动和不可移动介质。计算机存储介质包括, 但不限于, RAM、ROM、EEPROM、闪存或其它存储器技术; CD-ROM、数字多功能盘 (DVD) 或其它光盘存储; 磁带盒、磁带、磁盘存储或其它磁性存储设备; 或能用于存储所需信息且可以由计算机 110 访问的任何其它介质。通信介质通常具体化为诸如载波或其它传输机制等已调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据, 且包含任何信息传递介质。术语“已调制数据信号”指的是这样一种信号, 其一个或多个特征以在信号中编码信息的方式被设定或更改。作为示例, 而非限制, 通信介质包括诸如有线网络或直接线连接的有线介质, 以及诸如声学、RF、红外线和其它无线介质的无线介质。上述中任一个的组合也应包括在计算机可读介质的范围之内。

[0027] 系统存储器 130 包括易失性或非易失性存储器形式的计算机存储介质, 诸如只读存储器 (ROM) 131 和随机存取存储器 (RAM) 132。基本输入 / 输出系统 133 (BIOS) 包含有助于诸如启动时在计算机 110 中元件之间传递信息的基本例程, 它通常被存储在 ROM 131 中。RAM 132 通常包含处理单元 120 可以立即访问和 / 或目前正在操作的数据和 / 或程序模块。作为示例, 而非限制, 图 1 示出了操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

[0028] 计算机 110 也可以包括其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质。仅作为示例, 图 1 示出了从不可移动、非易失性磁介质中读取或向其写入的硬盘驱动器 141, 从可移动、非易失性磁盘 152 中读取或向其写入的磁盘驱动器 151, 以及从诸如 CD ROM 或其它光学介质等可移动、非易失性光盘 156 中读取或向其写入的光盘驱动器 155。可以在示例性操作环境下使用的其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质包括, 但不限于, 盒式磁带、闪存卡、数字多功能盘、数字录像带、固态 RAM、固态 ROM 等。硬盘驱动器 141 通常由诸如接口 140 的不可移动存储器接口连接至系统总线 121, 磁盘驱动器 151 和光盘驱动器 155 通常由诸如接口 150 的可移动存储器接口连接至系统总线 121。

[0029] 以上描述和在图 1 中示出的驱动器及其相关联的计算机存储介质为计算机 110 提供了对计算机可读指令、数据结构、程序模块和其它数据的存储。例如, 在图 1 中, 硬盘驱动器 141 被示为存储操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意, 这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 相同或不同。操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147 在这里被标注了不同的

标号是为了说明至少它们是不同的副本。用户可以通过输入设备,诸如键盘 162 和定点设备 161(通常指鼠标、跟踪球或触摸垫)向计算机 110 输入命令和信息。其它输入设备(未示出)可以包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等。这些和其它输入设备通常由耦合至系统总线的用户输入接口 160 连接至处理单元 120,但也可以由其它接口或总线结构,诸如并行端口、游戏端口或通用串行总线(USB)连接。监视器 191 或其它类型的显示设备也经由接口,诸如视频接口 190 连接至系统总线 121。除监视器以外,计算机也可以包括其它外围输出设备,诸如扬声器 197 和打印机 196,它们可以通过输出外围接口 195 连接。

[0030] 计算机 110 可使用至一个或多个远程计算机,诸如远程计算机 180 的逻辑连接在网络化环境下操作。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它常见网络节点,且通常包括上文相对于计算机 110 描述的许多或所有元件,尽管在图 1 中只示出存储器存储设备 181。图 1 中所示逻辑连接包括局域网(LAN)171 和广域网(WAN)173,但也可以包括其它网络。这样的联网环境在办公室、企业范围计算机网络、内联网和因特网中是常见的。

[0031] 当在 LAN 联网环境中使用时,计算机 110 通过网络接口或适配器 170 连接至 LAN 171。当在 WAN 联网环境中使用时,计算机 110 通常包括调制解调器 172 或用于在诸如因特网等 WAN 173 上建立通信的其它装置。调制解调器 172 可以是内置或外置的,它可以通过用户输入接口 160 或其它合适的机制连接至系统总线 121。在网络化环境中,相对于计算机 110 描述的程序模块或其部分可以存储在远程存储器存储设备中。作为示例,而非限制,图 1 示出了远程应用程序 185 驻留在存储器设备 181 上。可以理解,所示的网络连接是示例性的,且可以使用在计算机之间建立通信链路的其它手段。

[0032] 现在转向图 2 并继续参考图 1,示出了在本发明的一个方面中在计算机 110 上操作的电子邮件应用程序 200。在图 2 上示出的示例中,电子邮件应用程序 200 是驻留在计算机 110 上的应用程序 145 之一。作为替换或除此以外,电子邮件应用程序 200 的一个或多个部分可以是 RAM 132 中的应用程序 135 的一部分、或位于具有远程应用程序 185 的远程计算机 181 上,或计算机软件领域中的技术人员可以想到的其它这样的变型。

[0033] 电子邮件应用程序 200 包括电子邮件存储 201 和商业逻辑 205。尽管为清楚起见,电子邮件存储 201 被示为电子邮件应用程序 200 的一部分,但电子邮件存储 201 可驻留在与商业逻辑 205 相同或不同的位置和 / 或计算机中。例如,电子邮件应用程序 200 的电子邮件存储 201 可与计算机 110 的程序数据 147 一起驻留在数据库和 / 或一个或多个文件中,和 / 或电子邮件存储 201 可驻留在诸如远程计算机 180 的单独的计算机上。作为一个非限定性示例,电子邮件存储 201 可全部或部分驻留在操作系统 144 的文件系统中由用户指定的目录中。作为另一非限定性示例,电子邮件存储 201 可全部或部分驻留在电子邮件服务器数据库上(该数据库是安放在远程计算机 180 上的),诸如由 MICROSOFT® 制造的被称为 Exchange Server(交换服务器)的电子邮件服务器数据库产品。在图 2 所示的示例中,电子邮件存储 201 包括垃圾电子邮件文件夹 202、收件箱电子邮件文件夹 203 和 / 或其它电子邮件文件夹 204。其它文件夹变型也是可能的。如此处所使用的,术语文件夹指的是电子邮件消息的任何集合,然而它们被存储和 / 或表示在图形用户界面中。本领域的普通技术人员可以理解,当指电子邮件消息集合时,某些操作系统不使用术语文件夹,但这样

的情形仍由此处所示的使用术语文件夹的示例覆盖。

[0034] 商业逻辑 205 负责实现此处所述的某些或全部技术。商业逻辑包括用于接收用户输入的逻辑 206、用于在适当的情况下将所选消息重新格式化成更安全格式的逻辑 207、用于显示经重新格式化的消息的逻辑 208、以及用于操作电子邮件应用程序的逻辑 209。在图 2 中,商业逻辑 205 被示为作为应用程序 145 的一部分驻留在计算机 110 上。然而,可以理解,作为替换或除此以外,商业逻辑 205 可体现为一个或多个计算机上的计算机可执行指令和 / 或用与图 2 所示的不同的变型。作为一个非限定性示例,作为替换或除此以外,商业逻辑 205 的一个或多个部分可被实现为驻留在外部计算机上当需要时被调用的 XML web 服务。

[0035] 现在转向图 3-6 并继续参考图 1-2,将更详细地描述实现系统 100 的电子邮件应用程序 200 的一个或多个方面的各阶段。图 3 是本发明的一个方面的高层过程流程图。在一种形式中,图 3 的过程至少部分是在系统 100 的操作逻辑中实现的。该过程开始于起点 210,电子邮件应用程序 200 从用户接收查看具有超出某一阈值的安全性风险的电子邮件消息的请求(阶段 212)。电子邮件消息从其原始格式被重新格式化成经修改的格式,该格式包括纯文本并禁用了超链接(阶段 214)。该消息诸如在监视器 191 上用经修改的格式向用户显示,该格式比消息的原始格式安全(阶段 216)。该过程然后于终点 218 结束。现在将在图 4-6 中更详细地描述这些阶段。

[0036] 图 4A-4B 示出了将电子邮件消息重新格式化成要向用户显示的经修改的格式所涉及各阶段。在一种形式中,图 4 的过程至少部分是在系统 100 的操作逻辑中实现。在本发明的一个方面中,图 4A-4B 的过程被用于垃圾电子邮件文件夹 202 中的所有消息,因为置于垃圾电子邮件文件夹 202 中的消息因其本质一般是比较不安全的。然而,可以理解,图 4A-4B 中所述的各阶段可用于垃圾电子邮件文件夹 202 以外的其它文件夹 204 中的消息或仅用于垃圾电子邮件文件夹 202 中的某些消息。

[0037] 该过程在图 4A 上开始于起点 220,电子邮件应用程序 200 提供了用于存储被标识为垃圾的电子邮件消息的垃圾电子邮件文件夹 202(阶段 222)。电子邮件应用程序 200 接收原始格式的电子邮件消息(阶段 224)。作为少数非限定性的示例,原始格式可包括 HTML 代码、一个或多个图像、粗体、下划线、隐式字段、一个或多个文件附件和 / 或其它变型。电子邮件应用程序 200 确定消息被标识为垃圾消息,例如未经请求的广告电子邮件(SPAM)和 / 或钓鱼消息(被设计来通过看上去是来自可信来源而引诱机密的信息)(阶段 226)。当确定消息被标识为垃圾(阶段 226)之后,该消息被置于垃圾电子邮件文件夹 202 中(阶段 228)。

[0038] 电子邮件应用程序 200 从用户接收选择垃圾电子邮件文件夹 202 中的消息以便查看的请求(阶段 230)。继续参考图 4B,电子邮件应用程序 200 执行商业逻辑 207 来将所选消息重新格式化成纯文本且禁用超链接的经修改的格式(阶段 232)。纯文本格式将移除所有特殊格式,诸如粗体和 / 或下划线以及图像等。可用各种方式之一来禁用超链接。作为一个非限定性示例,一个或多个超链接可仍在电子邮件消息中可见,但当用户试图访问该超链接时,不跟随该超链接。作为另一非限定性的示例,一个或多个超链接的统一资源定位符可用纯文本格式来实际显示,就像消息中的其余部分一样。

[0039] 电子邮件应用程序 200 执行商业逻辑 208 用经修改的格式向用户显示消息,就用

户交互而言,它比原始格式安全(阶段 234)。作为少数非限定性示例,与以下其中的每一个相比,具有纯文本消息并禁用超链接的经修改的格式比较不会引起对用户的计算机或用户的损害(即,较安全):带有向远程服务器发送信号以验证电子邮件消息地址的有效性的图像的电子邮件消息;能够令用户访问超链接以访问外部网站并提供机密信息的钓鱼电子邮件消息;或能够令用户访问超链接以访问安装某些类型的病毒或从用户硬盘驱动器检索机密信息的外部网站的另一电子邮件消息。

[0040] 电子邮件应用程序 200 可向用户显示指示所选消息正用经修改的格式显示和/或指示用户可如何用消息的原始格式来查看它的通知(阶段 236)。这些阶段中某些或全部可被适当地重复,使得垃圾电子邮件文件夹 202 中的所有消息当由用户选择时用经修改的格式显示(阶段 238)。该过程于终点 240 结束。

[0041] 图 5 示出了将电子邮件从一个文件夹移动至另一文件夹以及当从该另一文件夹选择时改变电子邮件显示方式所涉及各阶段。在一种形式中,图 5 的过程至少部分在系统 100 的操作逻辑中实现。在本发明的一个方面中,当将消息从垃圾电子邮件文件夹 202 移动至收件箱电子邮件文件夹 203 时使用图 5 的过程。然而,可以理解,图 5 中所述的各阶段可用于除仅垃圾电子邮件文件夹 202 或收件箱电子邮件文件夹 203 以外的其它文件夹 204。

[0042] 该过程开始于起点 250,电子邮件应用程序 200 从用户接收将所选消息从垃圾电子邮件文件夹 202 移动至诸如收件箱电子邮件文件夹 203 的另一文件夹的请求(阶段 252)。该另一文件夹可具有用户想要进一步审阅和/或保存的消息。电子邮件应用程序 200 将所选消息移动至收件箱电子邮件文件夹 203 或其它电子邮件文件夹 204(阶段 254)。电子邮件应用程序 200 从用户接收查看收件箱电子邮件文件夹 203 中的所选消息的请求(阶段 256)。如果消息被标识为未经请求的广告电子邮件(SPAM),则电子邮件应用程序 200 用消息的原始格式显示该消息,并启用超链接(即,完全用其原始格式)(阶段 258)。如果消息被标识为钓鱼消息(从而造成比仅仅 SPAM 消息更高的安全性风险),则该消息用其原始格式显示但禁用超链接(阶段 260)。在钓鱼消息从收件箱电子邮件文件夹 203 打开时,在钓鱼消息中禁用超链接以降低用户会访问不可信来源的网站并泄露机密信息的风险(阶段 260)。用于格式化从垃圾电子邮件文件夹移动至收件箱的消息的其它变型也是可能的,诸如显示原始电子邮件,但对 SPAM 和钓鱼消息两者均禁用超链接。该过程然后于阶段 262 结束。

[0043] 图 6 示出了用更安全的方式将现有电子邮件作为附件转发所涉及各阶段。在一种形式中,图 6 的过程至少部分在系统 100 的操作逻辑中实现。该过程开始于起点 270,电子邮件应用程序 200 从用户接收将特定文件夹(例如,垃圾电子邮件文件夹 202)中的特定消息作为新消息的附件转发的请求(阶段 272)。电子邮件应用程序 200 用降低与该消息相关联的安全性风险的方式将该特定消息重新格式化为新电子邮件消息的附件,并保存消息的原始格式(阶段 274)。作为一个非限定性的示例,该消息可以是 .MSG 附件格式的新电子邮件的附件。当与新消息交互时,如果用户(接收方和/或发送方)希望查看包含在附件中的原始消息,则用户必须采取额外的动作来打开附件(阶段 276)。降低了当用户处理原始消息时无意中点击原始消息中的超链接和/或无意中将信息发送给第三方的安全性风险(阶段 276)。该过程然后于阶段 278 结束。

[0044] 现在转向图 7-10,将使用模拟屏幕来示出图 3-6 中所述的某些概念。图 7 是示出

特定电子邮件消息如何用其原始格式出现的示例的模拟屏幕 280。电子邮件消息的正文 282 包括各种格式,如图像 284 和超链接 286。在本发明的一个方面中,如果电子邮件消息被置于垃圾电子邮件文件夹 202 中,则这种原始格式将不能为用户所见,直到该消息被移动至收件箱电子邮件文件夹 203 中。用于该原始格式何时可向用户显示的其它变型也是可能的。

[0045] 现在转向图 8 和 9,模拟屏幕 290 和 200 示出图 7 中所示的电子邮件消息在如图 4 的阶段 232 和 234 中所述被重新格式化并用经修改的格式显示时如何显现。图 8 的屏幕 290 包括指示该消息用纯文本呈现、链接被禁用且如果该消息被移动至收件箱电子邮件文件夹 203 则该链接可被开启的通知 292(阶段 236)。在本发明的其它方面中,可显示各种其它类型的通知。消息的正文 294 用纯文本显示,图像 296 不见。超链接 298 可见,但被禁用。当用户试图跟随该超链接时,请求将被忽视(例如,点击事件被忽视或继之以某种其它变型以保持链接不被访问)。图 9 的屏幕 300 几乎与屏幕 290 完全相同,除了屏幕 300 示出了在经修改的消息格式中可如何禁用超链接的另一种变型。在此变型中,超链接 302 的统一资源定位符(URL)随消息的其余部分一起用纯文本显示。

[0046] 现在转向图 10,模拟屏幕 300 示出了如图 6 中的步骤所示如何将电子邮件消息作为附件转发。当用户选中作为附件转发选项 312 时,电子邮件应用程序 200 接收该请求(阶段 272),并创建将所选消息作为附件的新消息(阶段 274)。该附件保留其原始格式,但降低了与该消息相关联的安全性风险(阶段 274)。当与新消息交互时,如果用户(接收方和/或发送方)希望查看原始消息,则用户必须采取额外的动作来打开附件,从而降低了用户无意中点击原始消息中的超链接和/或无意中将信息发送给第三方的风险(阶段 276)。

[0047] 尽管用结构功能部件和/或方法动作所专用的语言描述了本主题,但可以理解,在所附权利要求书中定义的主题不必限于上述特定功能部件或动作。相反,上述特定功能部件和动作被公开为实现权利要求的示例形式。期望保护落入此处和/或所附权利要求书所述的本发明的精神内的所有等效方式、改变和修改。

[0048] 例如,计算机软件领域的普通技术人员可以认识到,如此处所讨论的示例中所述的客户机和/或服务器安排、用户界面屏幕内容和/或数据布局可在一个或多个计算机上不同地组织起来,以包括少于或多于这些示例中所描绘的选项或功能部件,而仍落入本发明的精神内。

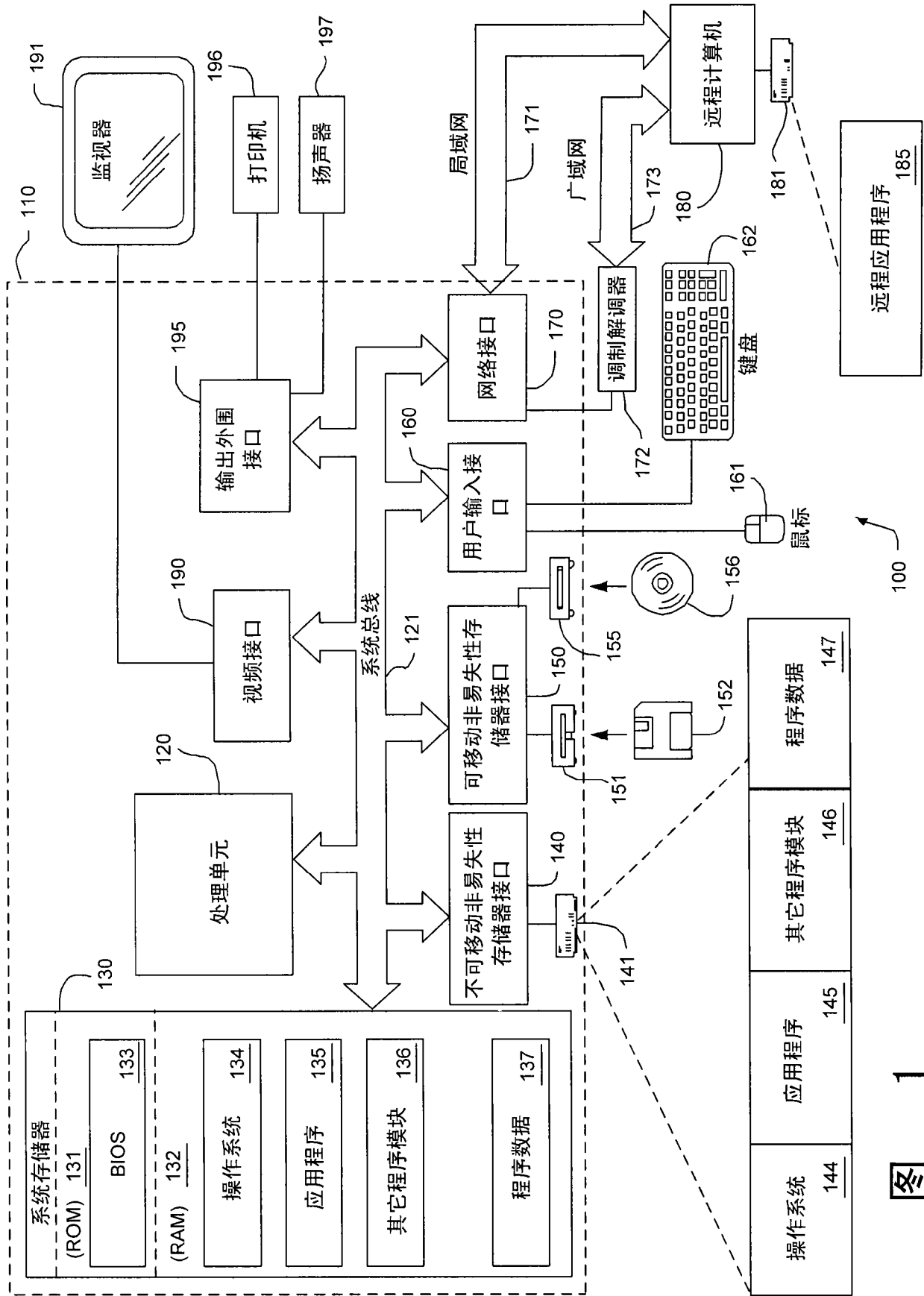


图 1

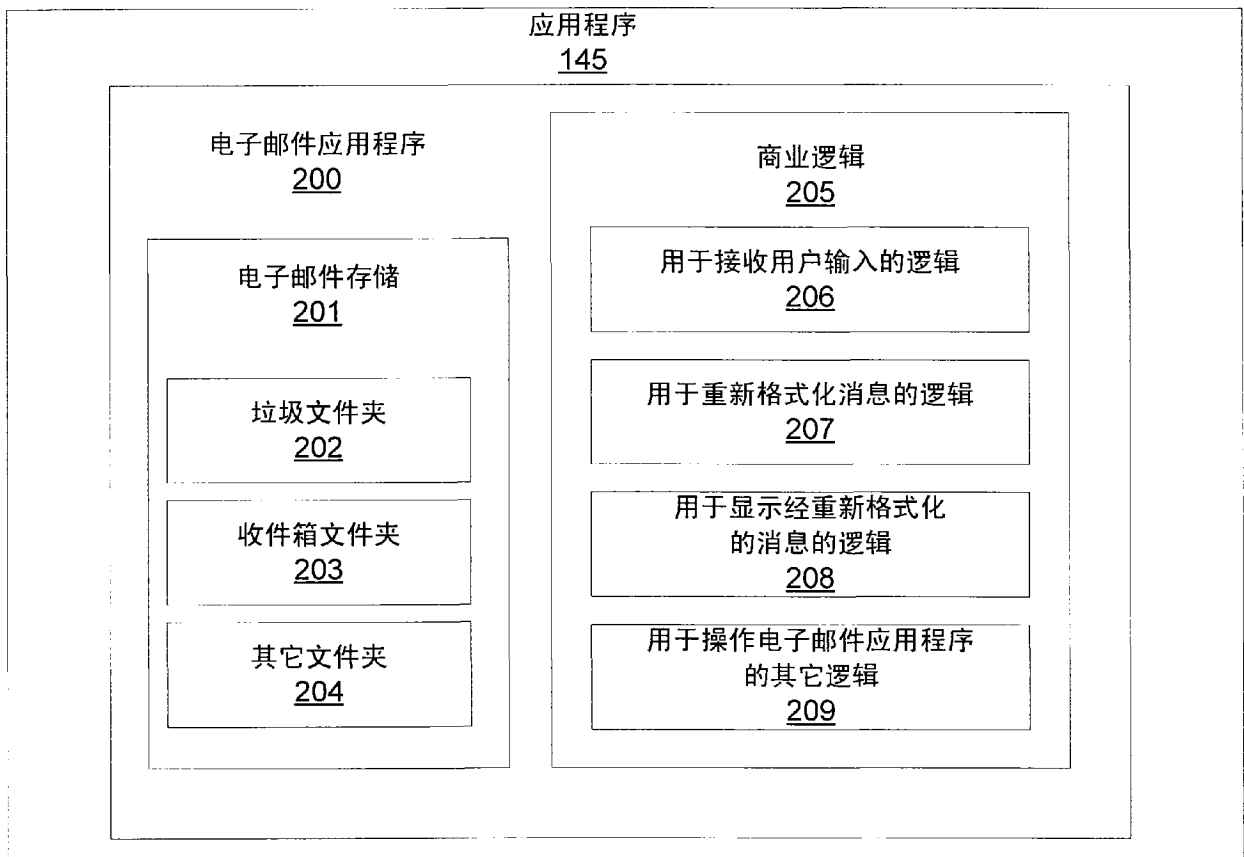
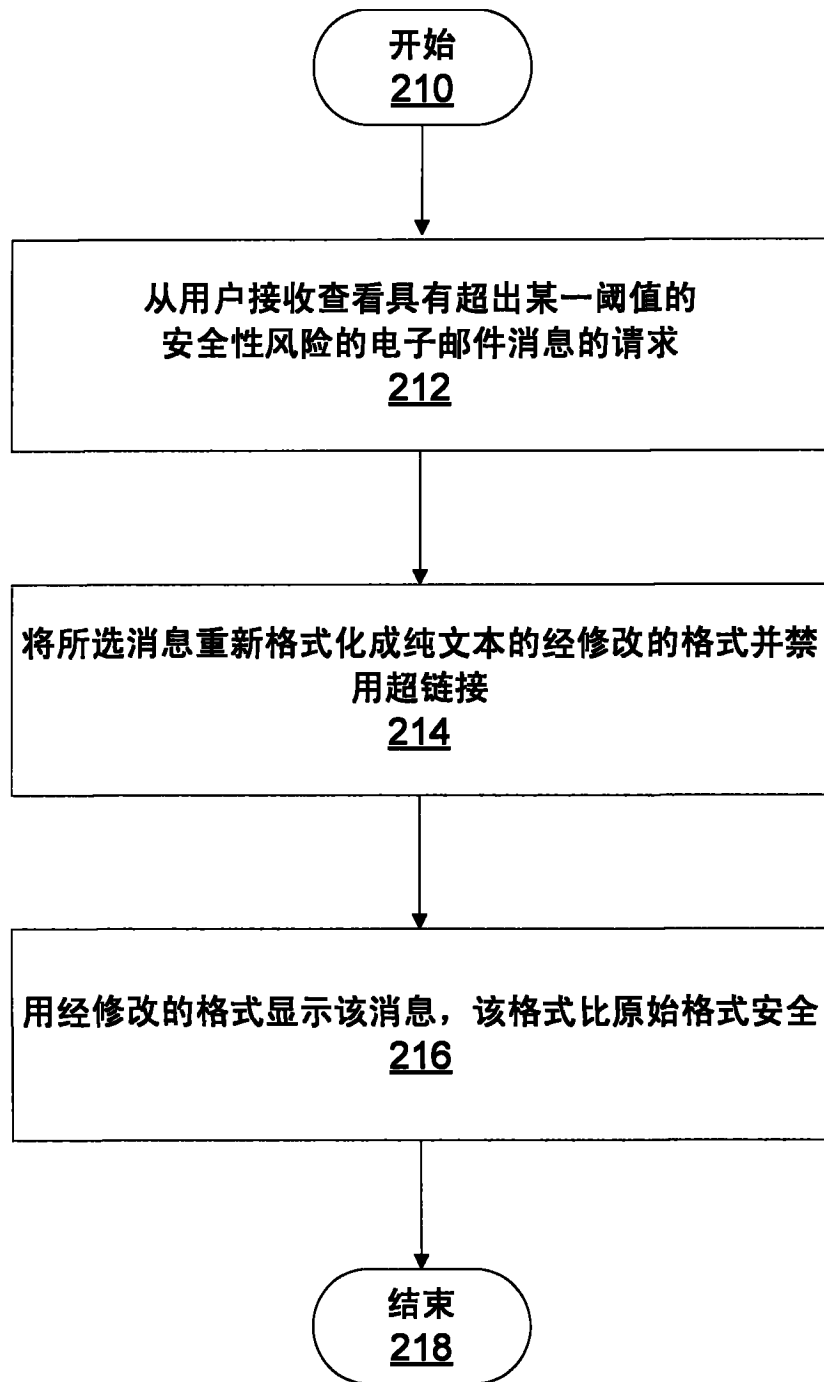


图 2

**图 3**

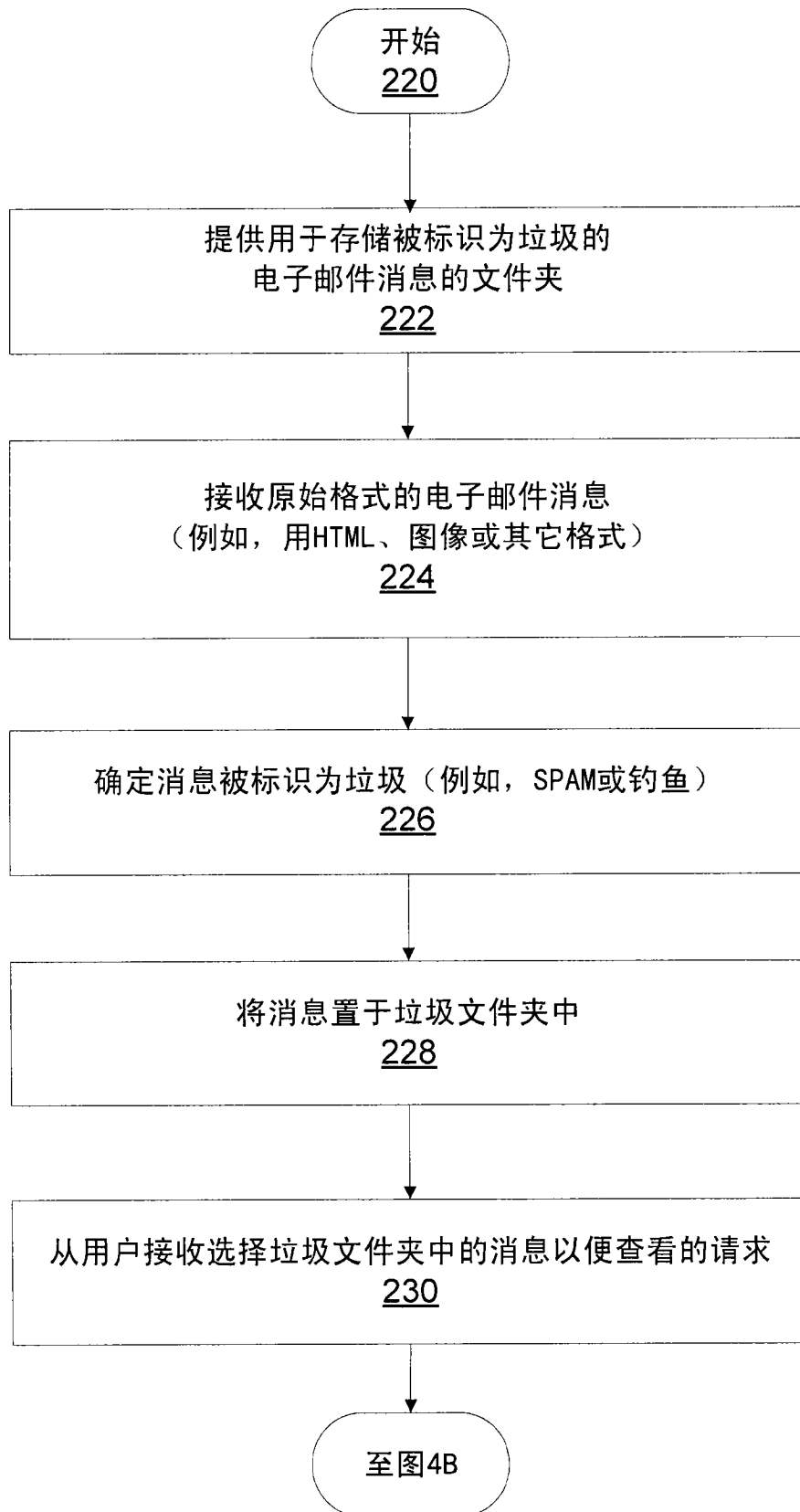


图 4A

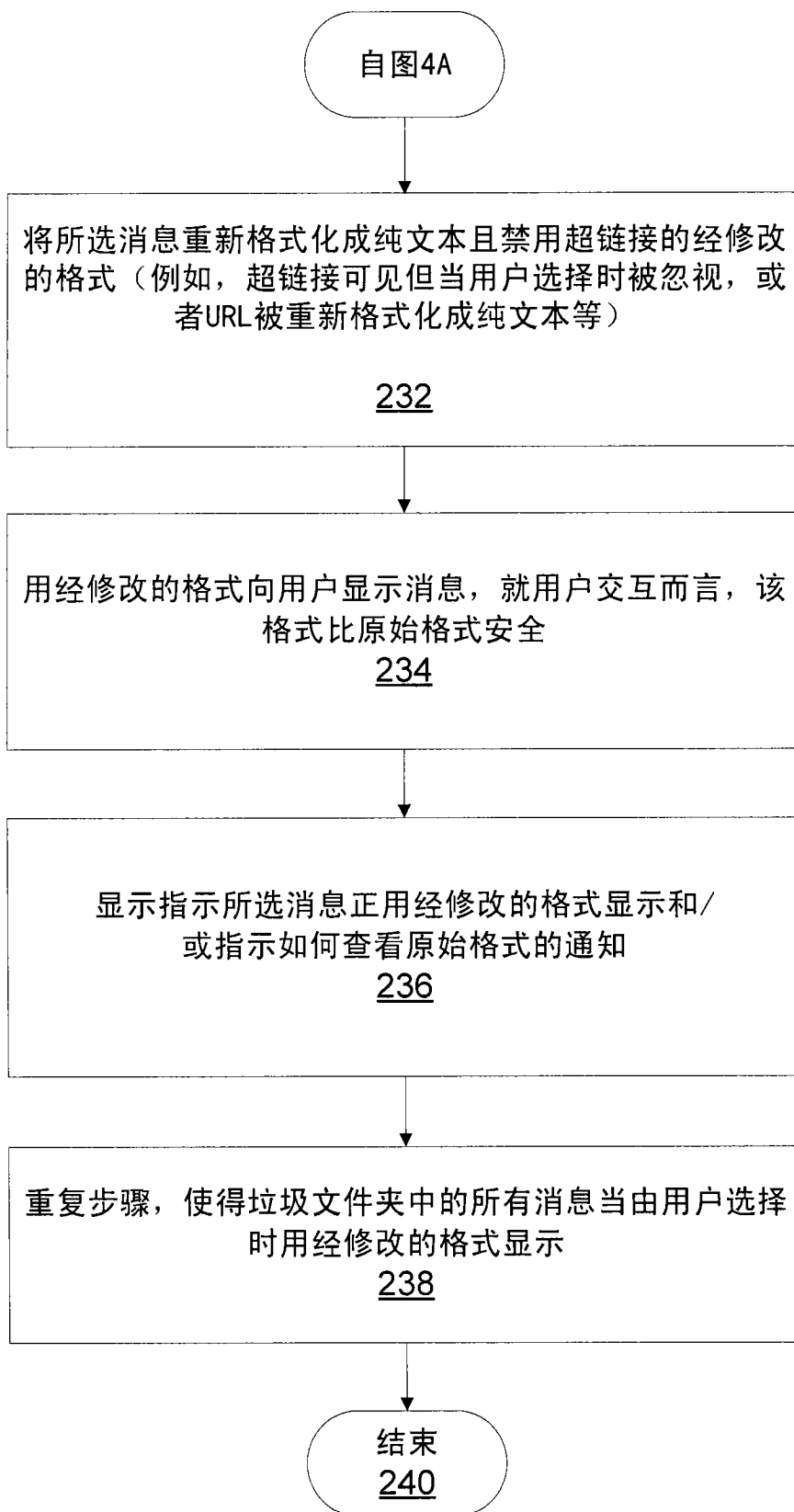


图 4B

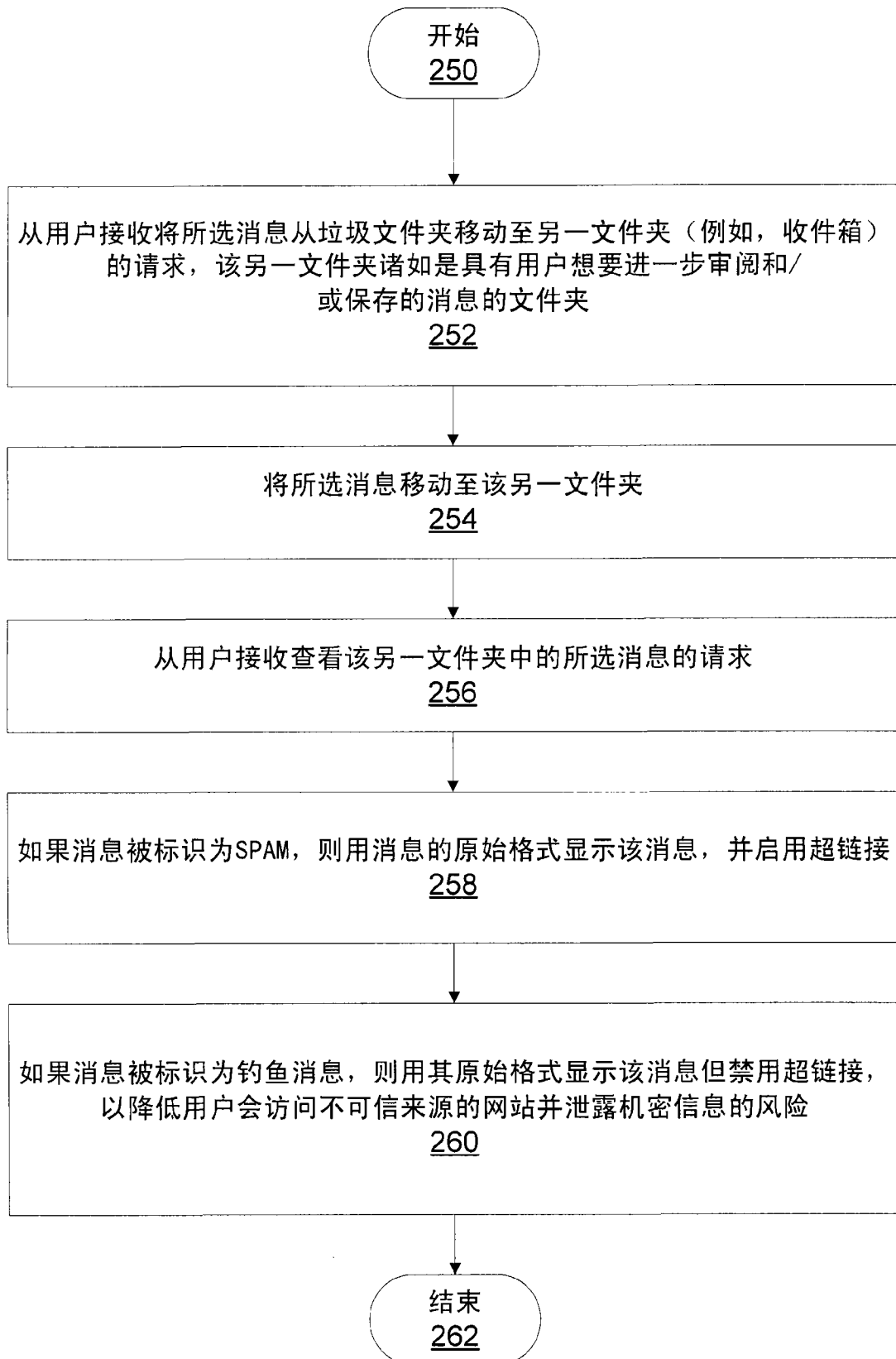


图 5

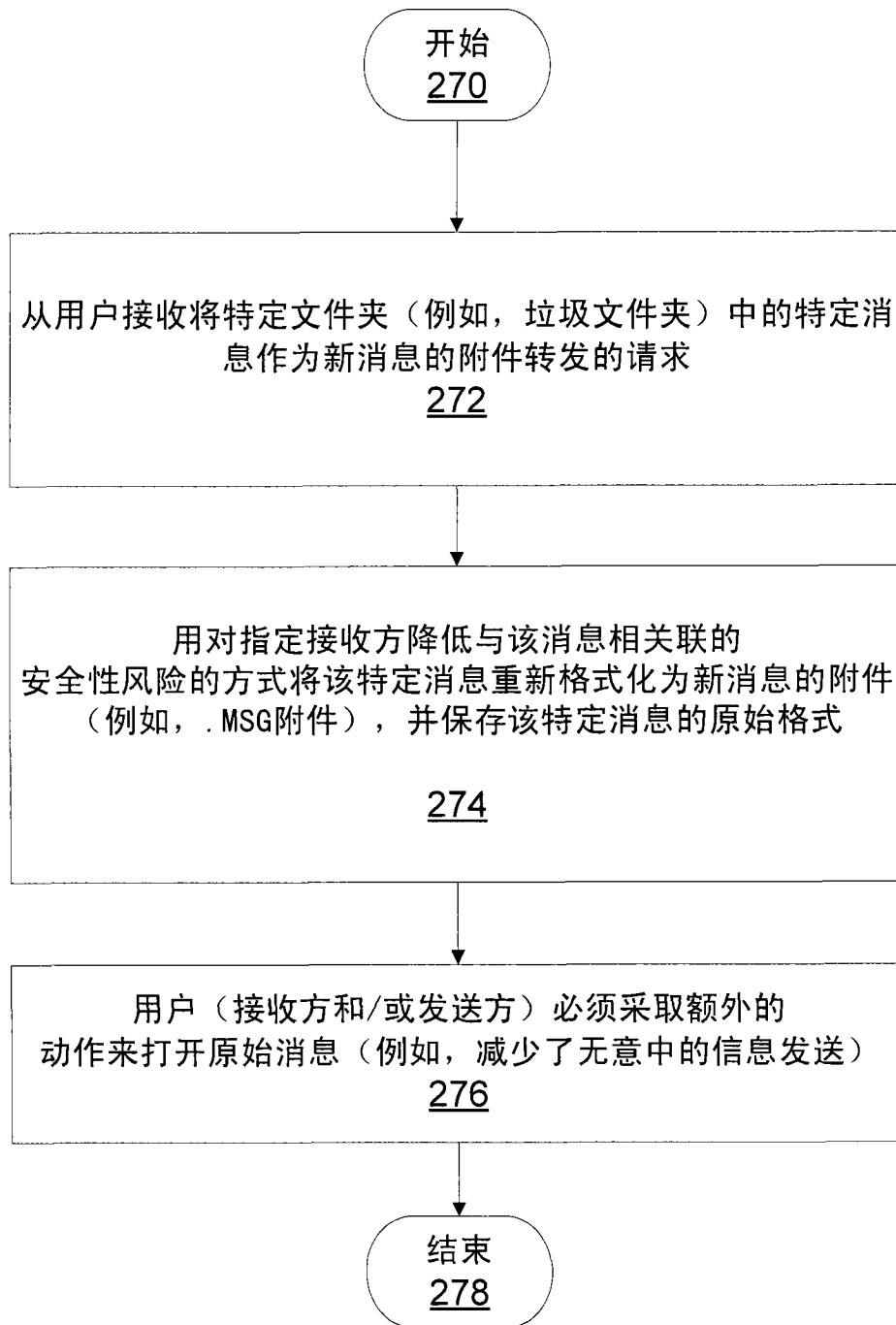


图 6

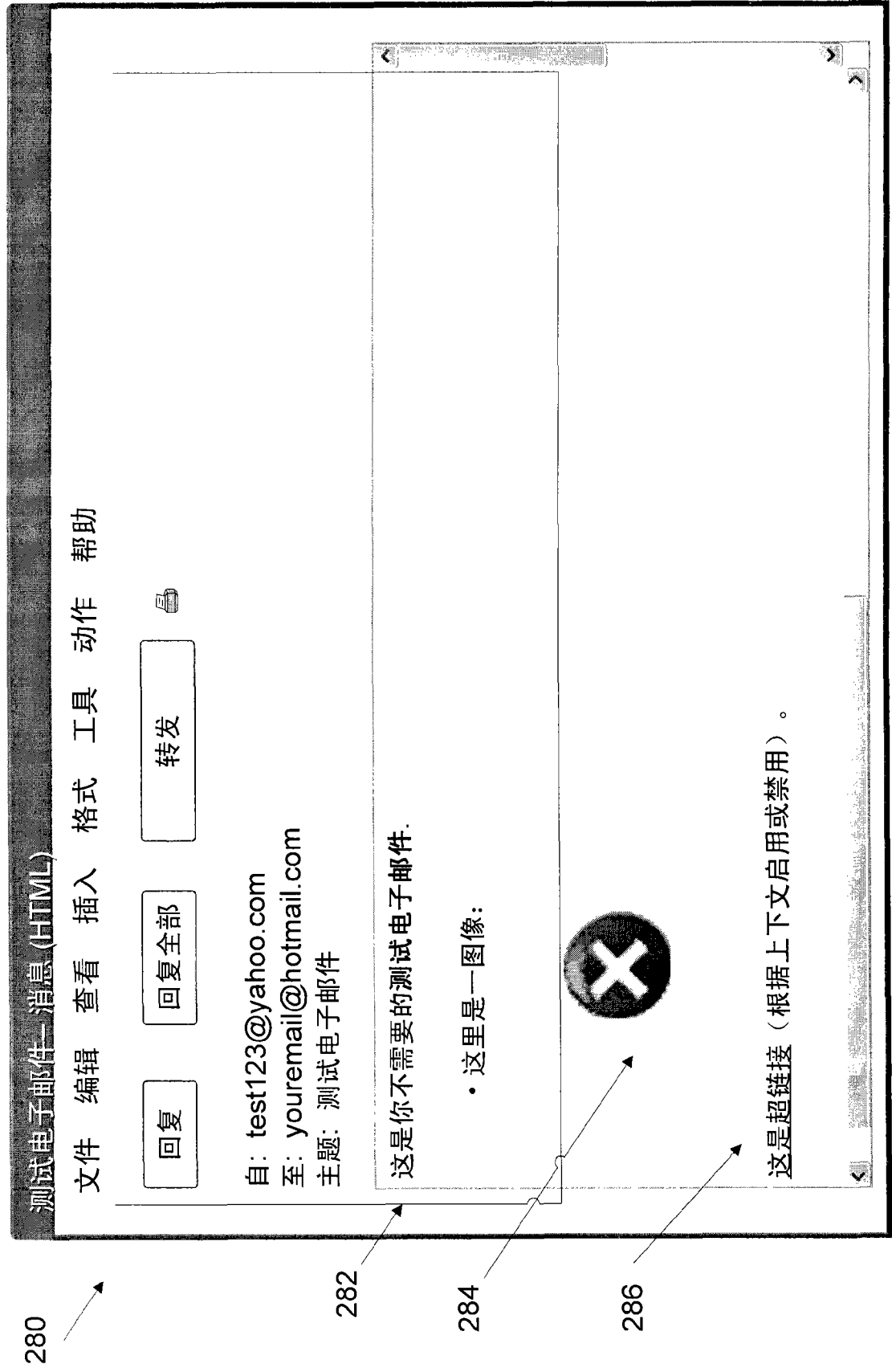
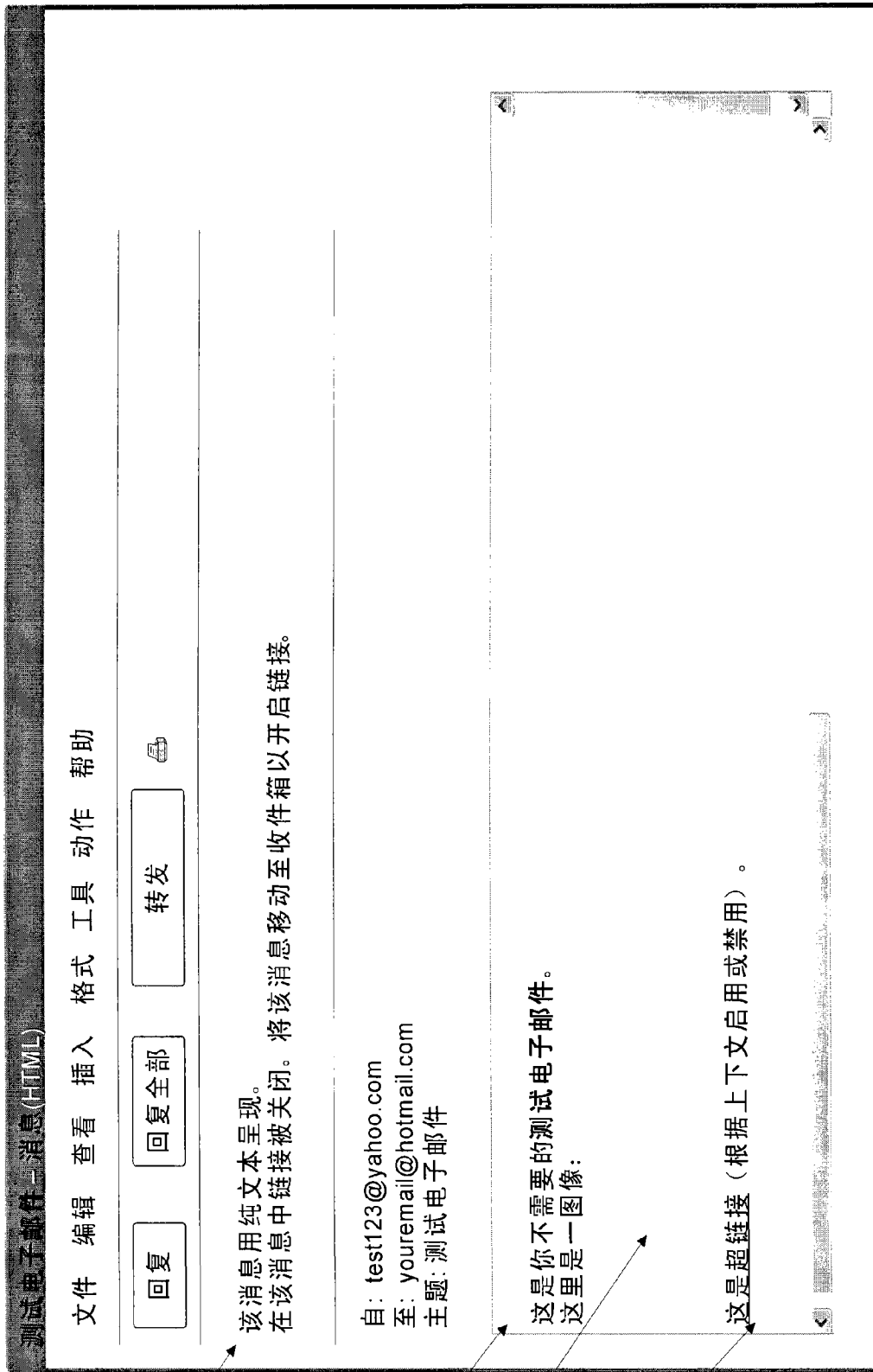


图 7



290

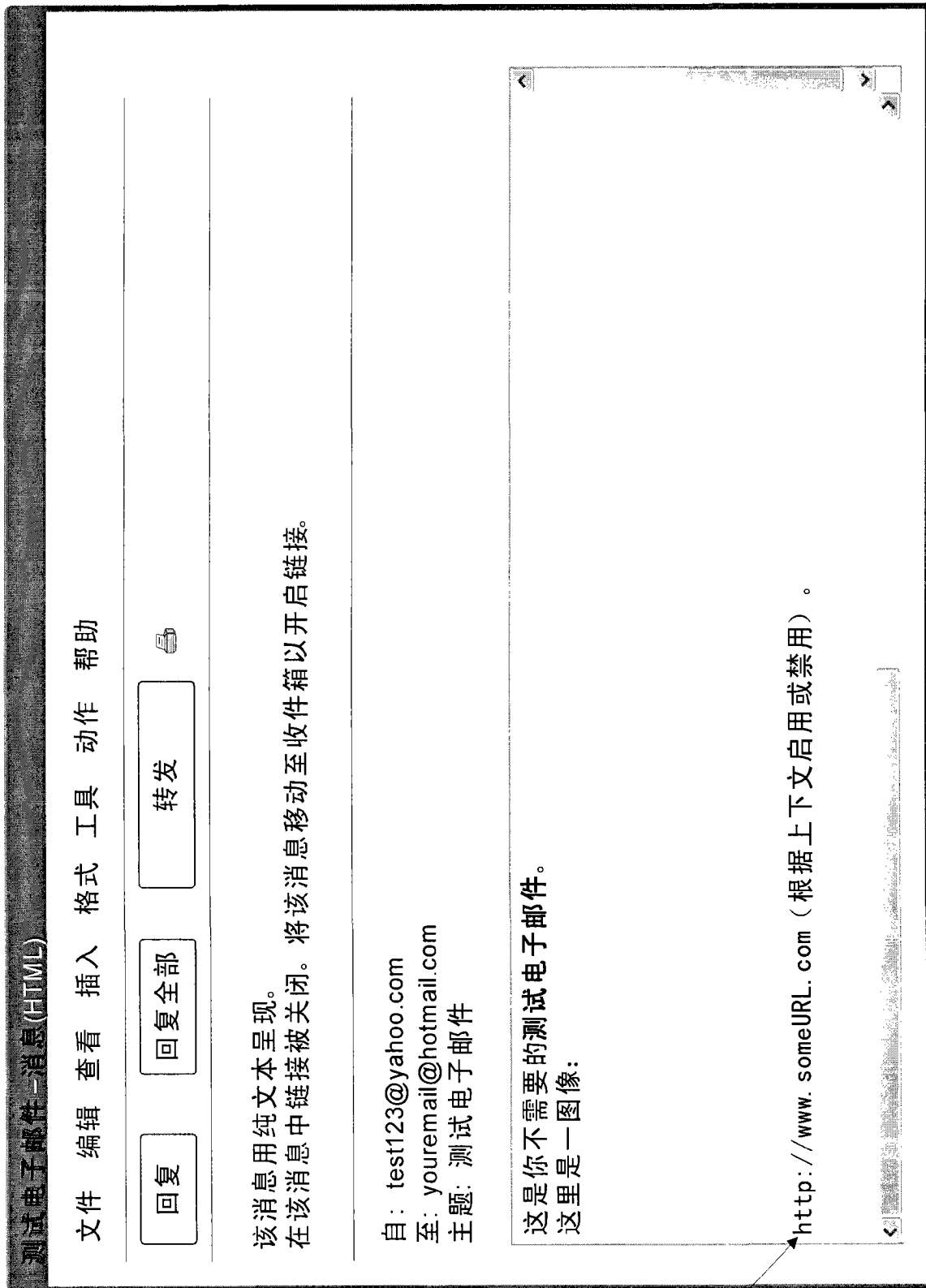
292

294

296

298

图 8



300

302

图 9

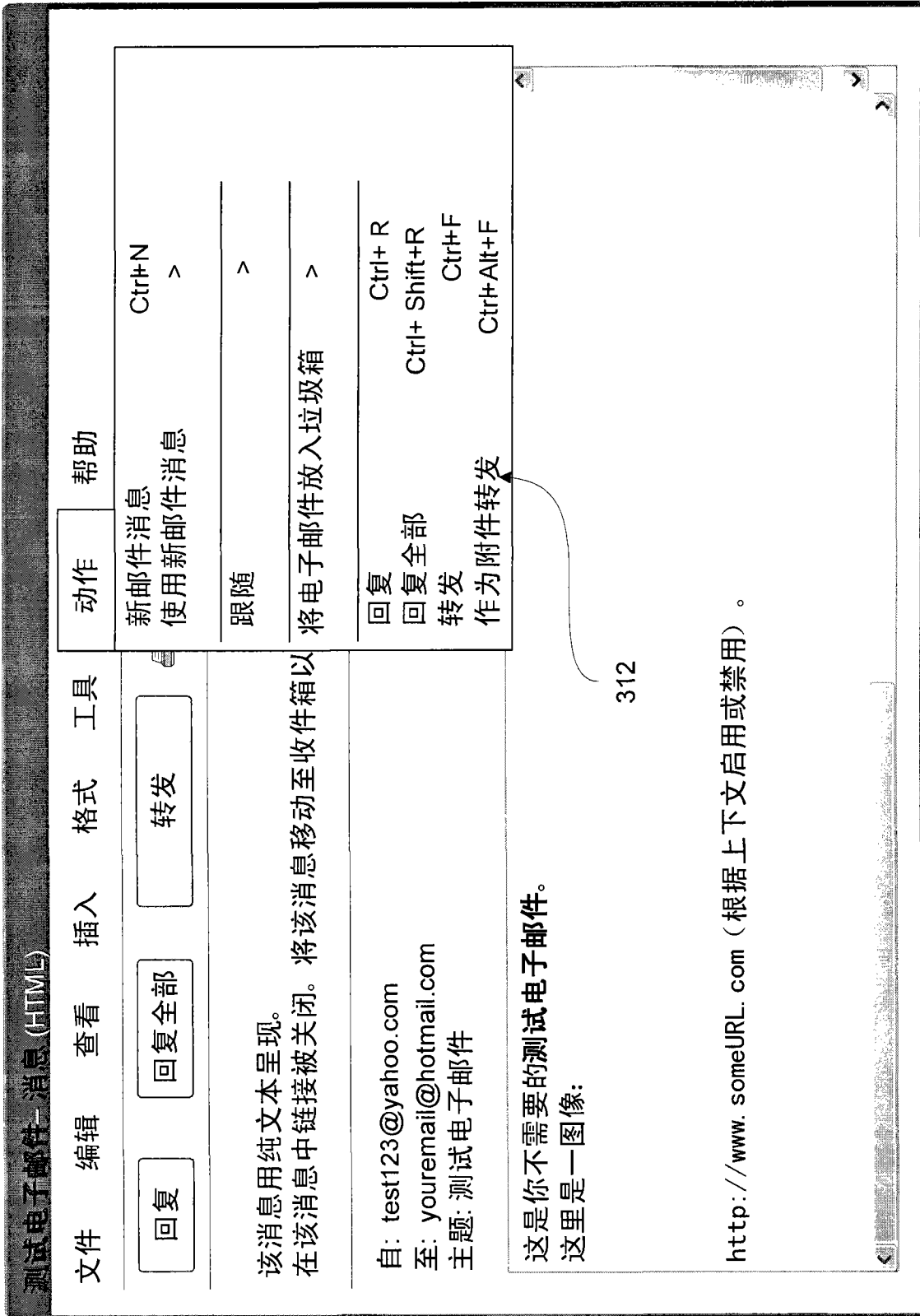


图 10