

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.  
G06F 17/00 (2006.01)



# [12] 发明专利说明书

专利号 ZL 200480026997.2

[45] 授权公告日 2009年3月18日

[11] 授权公告号 CN 100470534C

[22] 申请日 2004.9.17

[21] 申请号 200480026997.2

[30] 优先权

[32] 2003.9.19 [33] US [31] 60/481,402

[32] 2003.12.18 [33] US [31] 10/707,509

[86] 国际申请 PCT/US2004/030414 2004.9.17

[87] 国际公布 WO2005/029263 英 2005.3.31

[85] 进入国家阶段日期 2006.3.20

[73] 专利权人 皮特尼鲍斯股份有限公司

地址 美国康涅狄格州

[72] 发明人 小F·W·瑞安 B·R·汉穆尔

A·S·科坦

[56] 参考文献

US2003/0028497A1 2003.2.6

US6233565B1 2001.5.15

CN1438570A 2003.8.27

US5168444A 1992.12.1

US2002/0110397A1 2002.8.15

US6182565B1 2001.2.6

US2001/0030232A1 2001.10.18

审查员 王艳臣

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 李玲

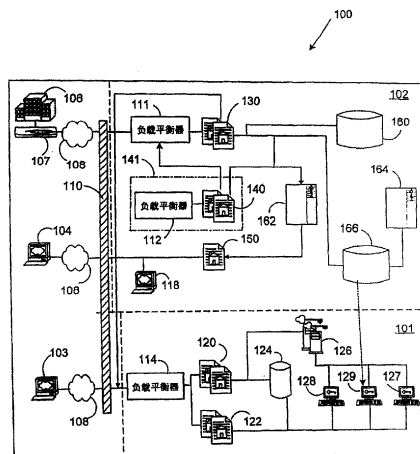
权利要求书2页 说明书14页 附图7页

[54] 发明名称

邮资系统中的欺诈检测

[57] 摘要

本文描述了用于处理和打印具有邮资的运送标签。在一个配置中，邮资分配系统允许在相对很短的一段时间内运送标签的重新打印。在另一个配置中，该系统在第二次打印尝试不成功以后提供退款，并将标签标识符作为无效标识符记入日志。如果打印成功，则将标识符作为成功的标识符记入日志。该系统时而接收邮件流中已被处理的标识符，如果出现了非预期的标识符则报告欺诈。



1. 一种用于控制带有标识符的具有邮资的第一运送标签的用户进行重复打印的方法，所述标识符与所述邮资相关，所述方法包括：

接收来自客户机系统的运送标签请求；

指示打印所述运送标签的请求；

启动运送标签打印任务，由此产生样本运送标签和所述运送标签，它们都可用于来自第一服务器的用户，并且其中所述运送标签在一预定的默认时间段内可用于用户；

从用户接收打印成功指示符；

如果所述打印成功指示符指示所述打印成功，则将所述标识符作为成功打印记入日志；

如果所述打印成功指示符指示所述打印没有成功，则向所述用户提供重新打印选项；以及

如果所述重新打印选项没有成功，则将所述标识符作为不成功打印记入日志，用于欺诈检测和提供所述邮资的退还。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

向所述客户机系统提供第一数据，用于将样本运送标签的至少一部分构造为客户机系统程序窗口中对用户可见的一部分；

向所述客户机系统提供第二数据，用于将第一运送标签的至少一部分构造为客户机系统程序窗口中对用户不可见的一部分。

3. 如权利要求 2 所述的方法，其特征在于：

所述第一数据是所述样本运送标签的图像的一部分。

4. 如权利要求 2 所述的方法，其特征在于：

所述第二数据是所述第一运送标签的至少一部分。

5. 如权利要求 1 所述的方法，其特征在于：

打印所述运送标签的请求的指示是来自所述客户机系统程序窗口中对用户可见的一部分。

6. 如权利要求 2 所述的方法，其特征在于：

所述客户机系统包括 web 浏览器应用程序；

所述 web 浏览器应用程序提供用于显示包括所述样本运送标签图像的第一框的可见部分；

所述 web 浏览器应用程序提供用于显示包括所述第一运送标签图像的第二框的不可见部分；以及

提供给所述客户机系统的数据是由第一 web 服务器提供的。

7. 如权利要求 6 所述的方法，其特征在于，还包括：

向所述客户机系统提供格式化指令，其中  
所述格式化指令防止用户访问所述第二框。

8. 如权利要求 6 所述的方法，其特征在于：

所述运送标签是使用从以下组中选择的图像文件格式的图像文件：GIF、BMP、TIFF、JPEG、PIX、PNG 和 PCX。

9. 如权利要求 6 所述的方法，其特征在于：

所述重新打印选项在一段时间内对所述用户可用。

10. 如权利要求 9 所述的方法，其特征在于：

所述一段时间是五分钟。

11. 如权利要求 9 所述的方法，其特征在于：

如果在所述一段时间内没有成功完成所述重新打印选项，则将所述标识符作为不成功打印记入日志。

12. 如权利要求 6 所述的方法，其特征在于：

所述运送标签包括从第二 web 服务器获得的图像部分；以及  
所述样本运送标签包括从第二 web 服务器获得的图像部分。

13. 如权利要求 7 所述的方法，其特征在于，

所述格式化指令防止对所述客户机显示进行滚动和大小调整。

## 邮资系统中的欺诈检测

### 相关申请的参照

本申请要求于2003年9月19日提交的题为 Fraud Detection for Postage Systems (邮资系统所使用的欺诈检测) 的美国临时专利申请序列号 60/481,402 的优先权。

本申请还要求于2003年12月18日提交的题为 System And Fraud Detection in a Postage System (邮资系统中的系统和欺诈检测) 的美国专利申请序列号 10/707,509 的优先权。

### 背景

在本申请中所描述的示意性实施例在包括用于提供资金记账和证明等的系统中有用, 尤其在包括用于提供邮资记账和邮资证明等的系统中有用。

资金记账、储备和分配系统是潜在的欺诈目标, 因为它们储备资金。某些资金系统受到调控, 并且通常被要求显示某个级别的安全能力来防止或阻止欺诈活动。此类系统还可提供一些法律证据以协助跟踪任何被保全的欺诈。

例如, 美国邮政服务局 (USPS) 批准的邮资机必须显示某些安全能力才能被批准使用。美国的许多邮资机提供资金记账, 从而当邮资在被放到邮件流中以前已被预付时, 资金源被记入借方。此外, 许多邮资机以放在邮件上 (通常是在信封的右上角) 的打印的邮戳的形式来提供邮资已付的证明。在诸如 USPS 等使用预付资金的邮资系统中, 邮资机可通过提供用于跟踪已经用掉的钱的升序记录、用于跟踪可用资金的降序记录、以及用于跟踪已盖免费邮戳的邮件总数的邮件计数记录来对资金进行记账。某些其它邮政系统使用收信人支付式的邮资, 其中邮资机可包含信用记账特征。

包括邮资机在内的邮件收发机可从美国康涅狄格州 Stamford 的 Pitney Bowes 有限公司购买。此外, 用于打印 CLICKSTAMP™ 因特网邮资的 CLICKSTAMP™ 在线系统可从 Pitney Bowes 有限公司获得。该程序是重客户机体系结构, 它包括对分配给顾客的邮资机许可证的虚拟邮资机的访问。该程序必须作为应用程序被安装在用户计算机上, 并且通常以存储在 CD-ROM 上的形式发售。顾客可下载该软件,

但在使用传统的调制解调器拨号因特网连接的情况下,这样一次下载可能要花数分钟。

在 2003 年 9 月 16 日授予 Bator 等人的美国专利第 6,619,544 号中描述了针对即时在线邮资的参考。

美国邮政服务局公布了题为 Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O)(基于信息的邮戳的性能准则以及开放式 IBI 邮资证明系统的安全体系结构)的规范草案,日期注为 2000 年 2 月 23 日。

邮资机的特性可被表述为以开放式计算器方式或封闭式计算器方式操作。典型的封闭式系统邮资机包括用于打印由该计算器分配和记账的邮资的证明的专用打印机。典型的开放式系统邮资机可使用通用打印机。邮政资金常常被存储在使用安全记账库的邮政安全设备(PSD)中。典型的邮资机用户租借邮资机,并向美国邮政服务局(USPS)注册该邮资机。

存在诸如 CLICKSTAMP™在线(CSO)系统等虚拟邮资机可用,且它们在用户具有通过远程访问来使用对应的虚拟邮资机的邮资机许可证的情况下作为数据中心处的账户存在。使用远程虚拟邮资机账户和远程密码处理器来产生供用户的本地处理器用来打印邮资邮戳的邮戳信息。如在所收录的参考中更完整地描述的,CSO 虚拟邮资机使用基于信息的邮戳程序(IBIP)邮戳,它是一种分布式的信托系统。用户将资金注入邮资库,然后通过将打印邮资邮戳施加于邮件来将资金作为邮资来分配,然后邮件被放到邮件流中。CSO 用户具有带唯一序列号的虚拟邮资机账户,并且该账户与在 USPS 当局下获得的邮资机许可证相关联。

在 2000 年 12 月 5 日授予 Cordery 等人的美国专利第 6,157,911 号中描述了针对开放式计数系统中重新发放数字令牌的参考。

在 1999 年 11 月 23 日授予 Pierce 等人的美国专利第 5,988,897 号中描述了针对防止对个人计算机上显示的邮资邮戳进行欺诈打印的参考。Pierce 系统描述确定输出设备是窗口还是打印机,并基于该确定选择适当的邮戳来呈现。因此,屏幕打印功能可打印样本邮戳。据此,下载的应用程序可挂钩到操作系统打印子系统中,从而用户将不能打印邮戳的多个副本。在 2004 年 1 月 20 日授予 Pierce 等人的美国专利第 6,680,783 号针对一种用于防止对 IBIP 邮戳进行重复打印的方法。

还对以下两个共同拥有的、共同待批的美国专利公开进行参考:2003 年 3 月 20 日公开的题为 Method And System For Optimizing Refill Amount For Automatic

Refill Of A Shared Virtual Postal Meter(用于共享的虚拟邮政邮资机的自动重注的优化重注量的方法和系统)的第 09/0055794 号, 以及 2003 年 5 月 8 日公布的题为 Method And System For Secure Printing Of Indicia Via A Web Based Browser(经由基于 Web 的浏览器进行邮戳的安全打印的方法和系统)的第 03/0088518 号。

一般在邮资支付系统, 特别是 USPS 中使用数种类型的价值转移系统。例如, 可购买邮票然后用它们来支付邮资。可使用允许系统, 其中邮寄者向 USPS 建立账户, 然后使用清单系统来对邮资进行记账。此外, 可使用邮资机系统。向邮资机加载一定量的邮资价值, 然后通过邮件上打印邮资邮戳来分配邮资价值。

在另一种支付模型中, 中介可代表顾客支付应付给诸如 USPS 等邮政公司的邮资, 只要 USPS 确信该系统足够安全。然后中介负责支付邮资。在这一系统中, 用户不需要邮资机许可证。中介为中介数据中心获得邮资机许可证, 并从用户获得位置信息。然后中介将诸如邮政编码等位置信息随邮件数据一起发送给 USPS。然后中介负责在 USPS 要求的情况下标识特定包裹的发件人。

### **概述**

本申请描述用于检测邮资系统中的欺诈的系统和方法。在一个实施例中, 一种邮资分配系统包括 web 浏览器, 它接收带有至少一个可见框和至少一个隐藏框的 HTML 页面。可见框包含样本邮资标签以及可由用户选择的两个打印按钮。第一个打印按钮被标记为样本, 当被选中时它使样本邮资标签被打印。此按钮可任由用户多次选择。隐藏框包含带邮资的实际运送标签。第二个打印按钮仅可被选择某个次数, 诸如两次。当第一次被按下时, 提示用户确定标签是否被成功打印。如果没有, 则再给用户一次机会在可配置的一段时间内请求重新打印。打印步骤的成功或失败被记入日志。在两次打印尝试失败以后, 向用户提供退款。

在另一个实施例中, 该系统在第二次打印尝试不成功以后提供退款, 并将标签标识符作为无效标识符记入日志。如果打印成功, 则将标识符作为成功的标识符记入日志。该系统时而接收到邮件流中已被处理的标识符。如果存在无效的标识符, 则报告可能有欺诈。如果有效标识符不止一次地进入邮件流, 则报告可能有欺诈。在一个替换方案中, 该系统从带有该标识符的标签的发放时起的六个月的时间轮询该标识符。

### **附图简述**

图 1 是根据本申请的一个示意性实施例的邮资分配系统的图示。

图 2 是根据本申请的一个示意性实施例的邮资分配事务的图示。

图 3 是根据图 1 中所示的示意性实施例的示意性邮资分配系统的逻辑组件和安全数据流的图示。

图 4 是示出根据本发明的一个示意性实施例用于分配带邮资的运送标签的处理流程的图示。

图 5 是根据本发明的一个示意性实施例的带样本邮资的示意性运送标签的图示。

图 6 是根据本发明的一个示意性实施例示出带样本邮资的示意性运送标签和带实际邮资的隐藏运送标签的显示的图示。

图 7 是示出根据本发明的一个示意性实施例用于分配带邮资的运送标签的过程的流程图。

图 8 是示出根据本发明的一个示意性实施例用于将打印数据记入日志和计算欺诈标志比的过程的流程图。

### **实施例详述**

参考 CSO 因特网邮资系统来描述本发明。可以理解，本发明适用于任何虚拟邮资机系统。

如本文中所描述的，示出了邮资分配系统的示意性实施例。在一个实施例中，邮资顾客使用 web 浏览器来接收带有至少一个可见框和至少一个隐藏框的标记语言页面。在一个替换方案中，隐藏框有一部分为用户可见，从而至少向用户隐藏该隐藏框的一部分。可见框包含样本邮资标签和可由用户选择的两个打印按钮。第一个打印按钮被标记为样本，当它被选中时，使样本邮资标签被打印。此按钮可任由用户多次选择。

隐藏框包含实际运送标签，它包括实际的邮资邮戳。第二个打印按钮仅可被选择某个次数，诸如两次。当第一次被按下时，提示用户确定标签是否被成功打印。如果没有，则再给用户一次机会。打印步骤的成功或失败被记入日志。在两次打印尝试失败以后，向用户提供退款。在一个替换方案中，重新打印次数是可配置的项目。此外，可在可配置的一段时间，诸如五分钟窗口中提供重新打印的机会。

在一个替换方案中，样本邮资可几乎与实际邮资相同。邮戳的条形码部分可包括实际邮戳，但可被清楚地标记为样本，或以某种方式模糊以使其不是机器可读

的。例如，可模糊足量的条形码，从而即使使用条形码的冗余特征，该条形码也是不可读的。

顾客所访问的 web 页面可使用嵌入逻辑，诸如通过使用 JavaScript、Active Server Pages（活动服务器页面）（ASP）或其它类似技术可用的嵌入逻辑等。该系统包括认证邮资顾客的邮资中介系统、以及邮资供应商数据中心，其中邮资中介向邮资供应商数据中心请求邮资。邮资供应商数据中心维护许可给邮资中介以供在通过中介进行的邮资事务中使用的邮资机。邮资中介系统响应于邮资顾客对邮资的请求。

在完成邮资/运送标签请求时，邮资中介向邮资供应商数据中心请求邮资。邮资中介从邮资供应商接收实际的邮资标签数据和样本邮资邮戳（假定满足了事务参数）。标签数据可包括邮戳数据（诸如用于组成 IBIP 条形码的数据），取决于标签的版本，该数据可以是样本数据或实际数据。标签数据可包括标签图像的链接或是该图像文件本身。

然后邮资中介使用接收到的标签数据来呈现标记语言文件格式的运送标签，以作为运送标签来向用户显示。该标记文件包括到由邮资供应商数据中心处单独定位的服务器生成的邮资邮戳的链接。在一个替换方案中，CLICKSTAMP™在线（CSO）系统虚拟邮资机服务器主存邮资邮戳。或者，邮资供应商直接向邮资中介发送整个邮资邮戳。

在另一个替换实施例中，使用 CSO 系统基础结构来主存标签，但在另一个实施例中，前端邮资中介基础结构主存标签。在其它替换方案中，可使用单独的服务器来主存标签。

在另一个说明性实施例中，邮资供应商向邮资中介发送邮戳数据。然后邮资中介构造包括邮资邮戳条形码、跟踪条形码和其它信息的运送标签。

参考图 1-3，描述了开放式邮资机环境中一种用于为用户打印带邮资的运送标签的示意性基础结构。在本发明中，不要求终端用户具有 USPS 邮资机许可证。

参考图 1，描述了根据本发明的一个说明性实施例的示意性运送和/或邮资标签处理系统 100 的系统示意图。

说明性的电子商务公司 xyz 公司 106 想要向其顾客提供邮资和/或运送标签。该公司 106 试图为其顾客担当邮资中介。该公司 106 具有到因特网 108 的连接 107，并可使用因特网或其它通信信道与其顾客通信。该图示是说明性的，典型的配置将包括数个邮资中介公司 106。



邮资供应商公司有防火墙 110，它过滤与来自公司外部的系统的因特网通信。常规的虚拟邮资机邮资系统包括在线因特网邮资计数系统环境 101，诸如具有生产冗余服务器 120 和 122、密钥管理服务器 126、邮资机账户数据库 124 的 CSO，并且负载由系统 114 平衡。

常规的重客户机 CSO 用户 103 通过防火墙 110 与通过负载均衡器 114 的常规 CSO 环境 101 通信。数个 CSO 事务服务器 120 使用内部通信信道与 CSO 数据库 124 和 CSO CCV（用于虚拟 PSD 的密码协处理器）通信。CSO 数据库 124 是可从 ORACLE®购买的数据库系统，并且它使用 RAID 存储技术。数个报告和管理服务器 122 与 CSO 数据库 124、管理员控制台 128、电子商务服务器（ECS）控制台 129 和远程金库（RCB）终端 127 通信。RCB 终端 127 是受到物理保护的密码引擎，它确保批准邮资重注的消息被安全地绑定到获得资金和向邮政当局进行支付的机制。ECS 控制台 129 使用 Broadvision®平台来提供电子商务前端的管理。

IBDS™（基于因特网的投递系统）环境 102 向常规 CSO 环境 101 提供新的前端。IBDS Web 服务器 130 使用负载均衡器 111 被连接到外部中介 106。IBDS Web 服务器 130 被连接到常规 CSO 负载均衡器 114 的前端。IBDS 环境 102 包括数据库 160 和数据日志记录服务器 162。

IBDS 环境 102 包括 IBDS 管理服务器 164，它被用来实例化新的邮资中介账户和邮资机。管理服务器 164 不可使用因特网来访问。IBDS 管理服务器 164 提供若干功能，包括允许为新的邮资中介 106 创建新的 CSO 邮资机记录的邮资机建立工具。此外，管理服务器 164 提供邮资机重注管理器、审计实用程序和欺诈警告系统。类似地，IBDS 管理服务器 164 提供其它用于监视系统性能和操作状态的状态系统。

IBDS 102 环境允许美国邮政服务局（USPS）职员系统 104 通过防火墙 110 进行访问。IBDS 环境 102 包括帮助台系统 118 和内部 USPS 客户服务代表（CSR）web 服务器 150。

IBDS 环境 102 包括 IBDS 数据库 166，后者与常规 CSO 环境 101 的 ECS 控制台 129 通信。IBDS 数据库 166 是使用 RAID 技术在诸如 WINDOWS® 2000 高级服务器等平台上运行的 MICROSOFT® SQL 服务器 2000 群集。

IBDS 环境 102 允许诸如 xyz 公司 106 等一个或多个外部邮资中介访问 IBDS web 服务器 130。邮资中介 106 可为顾客中介邮资，通过提供带跟踪号的运送标签来提供对运送服务的访问，并提供其它可选的特殊服务。类似地，邮资中介可使用

该系统来满足其内部的邮资和运送需求。可以理解,中介 106 和操作 IBDS 环境 102 的可以是同一实体。

邮资分配系统可能会遭受欺诈攻击。在本文中的说明性实施例中所描述的这些系统有数件可能被记入日志中并被用于欺诈检测目的的数据可用。例如,从中介接收到的每个数字地签署的邮资请求被记入日志。该系统还维护成功运送标签/邮资邮戳打印的列表,并将不成功的打印尝试和退款请求记入日志。欺诈检测机制检测记入日志的数据中的异常,并在本文中参考图 8 进行描述。

参考图 2,描述根据本发明的一个说明性实施例的示意性邮资分配事务 200 的图示。

包裹发货者使用发件人的 web 浏览器 220 来向邮资中介 web 服务器 224 发送打印请求(201)。发件人的 web 浏览器 220 和邮资中介服务器 224 执行认证(202b)。邮资中介服务器 224 向 IBDS 服务器 228 发送打印请求(203)。邮资中介服务器 224 和 IBDS 服务器 228 执行认证(202a)。

IBDS 服务器 228 向 IBDS web 服务器 234 发送打印请求(205)。然后请求/响应日志记录功能 230 向日志记录服务器 232 发送请求记录(204)。

IBDS web 服务器 234 向 IBDS 邮资机选择和管理系统 236 发送选择邮资机请求(206)。IBDS 邮资机选择和管理系统 236 向 CSO 环境 238 (图 1 中示为 101) 发送邮戳签署请求(207)。经签署的邮戳被发送(208)到 IBDS 邮资机选择和管理系统 236, 然后被发送(209)到 IBDS 分配系统 234, 后者随即向 IBDS web 服务器 228 发送 HTML 页面(210)。然后请求/响应日志记录功能 230 向日志记录服务器 232 发送响应记录(211a)。邮资标签图像 240 被从 web 服务 234 发送到 web 浏览器(220)。

使用安全信道 226 将 HTML 页面发送(211b)到中介 web 服务器 224, 然后在将其发送(212)到发件人的 web 浏览器 220 之前可对齐进行可任选的修改。例如,中介可使用中介图形来给该页面打上商标。该 HTML 页面可包含标签图像 240, 或可包含到存储在 IBDS 分配 web 服务器 234 上的邮资标签图像 240 的链接。然后用户使用打印机 222 打印该 HTML 页面, 或从该链接检索邮资标记图像然后进行打印。

IBDS 系统包括认证过程, 该过程包括传递打印请求(203), 打印请求包括标识特定邮资中介的唯一 ID 和标识邮资中介的特定顾客的标识符。可使用任何其它已知的认证过程。此外, 还包括标识特定事务的事务 ID。事务 ID 对来自一个邮

资中介的每个请求都是唯一的。可使用包括这三个认证元素的签名的数字签名。当该请求到达 IBDS 服务器 228 时，服务器在执行请求之前执行一系列有效性检查。如果其中任何检查失败，则 IBDS 服务器 228 将拒绝该请求，并向邮资中介服务器 224 发送出错消息。这些检查可包括检查请求的有效参数，包括安全报头、中介 ID、登录 ID、非空登录 ID、事务 ID、新的事务 ID。还可对请求检查请求中是否有数据的数字签名以及有效的数字签名。

参考图 3，描述根据本发明的一个示意性实施例的安全模型。顾客系统 340 包括具有 web 浏览器 343 的计算机，该 web 浏览器 343 包括支持 SSL/TLS 的安全通信子系统。此外，有打印机 342 可用于打印运送标签。

顾客系统利用使用 SSL/TLS 的因特网连接 339 来与 xyz 公司的邮资中介系统 330 通信。中介系统 330 包括 web 服务器 334，它响应于来自用户系统 340 的请求而提供 HTML 或其它标记语言文件。可任选地，邮资中介应用程序包括用来进行地址清除的地址引擎 333 和/或用来对包裹运送收费进行费率计算的运送费率计算器 332。中介系统 330 利用使用 VPN 的因特网连接 329 或其它安全信道来与 IBDS 系统 320 通信。

IBDS 系统 320 被用来与常规虚拟邮资机系统 310 相接。IBDS 系统 320 包括 web 服务 327，它使用 VPN 连接 329 与邮资中介系统 330 通信。IBDS 系统 320 还包括审计日志记录系统 326，它用于将打印成功及其它信息记入日志。

IBDS 系统 320 包括邮资机选择管理器 325。在常规的虚拟邮资机系统中，用户对每个事务都访问同一个邮资机账户。在此，邮资中介可具有一个或多个虚拟邮资机账户。使用邮资机选择管理器 325 来选择用于特定事务的虚拟邮资机账户。在一个实施例中，如果邮资中介有一个以上的邮资机账户，则选择具有最高余额的虚拟邮资机账户。在另一个实施例中，在前进至下一个虚拟邮资机账户以前先用完这一个的全部余额，从而将只需要重注最少的一组邮资机。此外，可使用各种已知的用于选择重注账户的系统，诸如在前文提及的 2003 年 3 月 20 日公开的题为 *Method And System For Optimizing Refill Amount For Automatic Refill Of A Shared Virtual Postal Meter*（用于共享的虚拟邮政邮资机的自动重注的优化重注量的方法和系统）的第 03/0055794 号等中所描述的那些系统。

邮资供应商系统 320 包括邮资重注管理器系统 322，它管理每个邮资中介的邮资机重注过程。

邮资供应商系统 320 包括用于处理邮资请求的邮资分配请求处理器 324。此

外，邮资呈现组件 323 呈现要包括在运送标签中的图像或其它数据文件。所呈现的邮资可包括 IBIP 邮戳。如本文中所描述的，邮资呈现组件可呈现样本邮戳和实际邮戳。可任选地，邮资呈现组件可驻留在邮资中介系统 330 内。邮资供应商系统 320 使用 SSL 协议，通过网络 319 与常规虚拟邮资系统 310 通信。或者，可使用其它网络拓扑结构和安全配置。例如，可使用双向认证 SSL。此外，可使用诸如专用线等实际专用网络。

较佳的是，常规虚拟邮资系统 310 是 CSO 系统 310。虚拟邮资系统 310 包括与常规 CSO 用户和 IBDS 邮资用户相接的外部接口层 316。该系统包括事务处理器 317、虚拟邮政安全设备 (VPSD) 服务器 314 和电子商务服务器 (ECS) 接口 315。该系统包括审计日志记录系统 312 和供虚拟 PSD (CCV) 服务器 311 使用的密码协处理器。使用安全链路 345 将 Web 浏览器 343 连接到 web 服务 327。

在此这些系统和子系统可被组织为一个应用程序的不同部分、一台计算机上的不同应用程序、或甚至是在不同计算机上运行的不同应用程序。类似地，可使用任何组合，或可使用任何已知形式的地理、吞吐量或其它负载平衡。

参考图 4-7，描述根据本申请的一个示意性实施例用于防止在 web 浏览器中进行重复打印的说明性系统和方法。在优选实施例中，该系统并不将应用程序下载到用户的计算机。在一个替换实施例中，可以使用诸如 Java 程序等具有和下述相同的功能的可在基于浏览器的虚拟机中执行的小程序。

参考图 4，示出根据本发明的一个说明性实施例的说明性运送标签/邮资分配系统 400，来说明用于分配带邮资的运送标签的过程。

使用诸如因特网等通信信道 412 将运送顾客系统 410 连接到 xyz 公司邮资中介系统 420。类似地，使用诸如因特网等通信信道 425 将顾客系统 410 连接到 IBDS 系统 430。系统 430 与图 1 中所示的系统 101 和 102 等价。可使用安全套接字层 (SSL)、虚拟专用网络 (VPN) 或其它技术来保护因特网连接。

在典型的事务中，顾客登录到诸如拍卖电子商务供应商等商家网站。可通过电子商务拍卖网站对其拍卖顾客使用的方法来认证顾客。然后顾客启动购买邮资的过程，并启动运送事务。从顾客系统 410 向 xyz 公司系统 420 发送打印邮资请求。xyz 公司系统 420 随即确认目的地地址并计算运送费率。如果需要可将目的地地址清除。xyz 公司系统 420 随即构造对 IBDS 系统的邮资分配请求，并用私钥签署该请求。然后 xyz 公司系统 420 将该请求发送给 IBDS 系统 430。

IBDS 系统 430 生成包含到邮资标签图像的链接的 HTML 页面，并将该 HTML

页面发送给 XYZ 公司系统 420。XYZ 公司系统 420 将 HTML 页面发送给顾客系统 410。顾客系统 410 随即可访问存储在 IBDS 系统 430 上的邮资标签图像以进行后续的打印。

参考图 5，示出在浏览器窗口 500 中显示了表示邮资标签文件的标记语言文件。浏览器下拉菜单 510 和所有用户控件都被禁用并且不可见。运送/邮资标签打印按钮 522 被放在浏览器窗口 500 的顶部。提供邮资事务取消按钮 525，并提供样本运送/邮资标签打印按钮 524。运送/邮资标签 526 包括顶部 590，它包括服务类别指示符 592 和样本邮戳条形码 594。标签 526 包括第二部分 580，它包括目的地 582 和源 584 地址信息。标签 526 包括第三部分 560，它包括投递确认条形码 562 和人类可读形式的投递确认数 564。提供了任何特殊服务的人类可读指示 566。标签 526 还包括第四部分 550，它包括人类可读的批准代码 552。

参考图 6，描述了依照本发明的一个说明性实施例，示出具样本运送标签 626 和带实际邮资的隐藏运送标签 632 的运送标签 600 的显示。浏览器控制条 610 高度为 A 并被禁用，从而用户不可控制菜单、工具条、滚动条及诸如键击扫视和右击菜单等其它控制功能。

可见框 620 的大小不可变，且其高度为 B。不可见框的高度为 C。屏幕被分成可见高度 D 和不可见高度 E。可见框 620 包括可见的样本运送标签 626。可见框中包括样本打印按钮 624 和邮资打印按钮 622。在一个替换方案中，框 620 是部分可见框。

不可见或隐藏框 630 包括要被打印的实际运送标签 632。打印按钮 622 背后的逻辑使具有运送标签 632 的隐藏框 630 被打印。打印按钮 622 的逻辑提示用户回答打印是否成功。如果用户不回复，则默认为肯定的回答。如果用户表示打印不成功，则提供用户重新打印一次的机会。或者，打印重试次数可以改变。如本文中所描述，打印按钮 622 的逻辑还将成功和/或失败的指示记录到邮资供应商系统 430，以便用于欺诈检测或诸如跟踪等其它目的。

因为实际的和样本运送标签文件可存储为 GIF 格式，所以文件可能会很大。可将这些文件存储在 IBDS 系统上，并在发送给顾客的 HTML 或其它标记语言页面中引用它们。这一配置提供较大的吞吐量，而接收到第一字节的时间 (TTFB) 很短。此外，在 xyz 公司系统和 IBDS 服务器之间传送了较少的数据。在每个顾客系统和 IBDS 系统之间传送了较多的数据，但该数据被分布在每个顾客用来到达 IBDS 系统的各个信道上。顾客一响应成功的打印提示 (回答或默认)，这些标签

图像即从服务器移除。如果没有接收到任何响应，则在 5 分钟后移除标签 GIF。或者，可使用诸如 10 分钟等其它默认时间段。

或者，可使用其它文件格式。客户机可使用 HTML 或其它链接来呈现标签的图像，以包括诸如 BMP、TIFF、JPEG、PIX、PNG 和 PCX 等不同格式的图像或图像部分。

或者，按钮 622、624 可被包括在不可见框 630 的空白部分中。例如，不可见框 630 的一部分可以是实际可见的，并包含这些按钮。据此，当用户选择打印按钮时，不可见框将成为活动框，并且将不会需要这些按钮进行跨框的控制。

在另一个替换方案中，可使用 Active Server Pages (ASP) 或诸如 Macromedia、Jscript、VBScript 或其它最好是独立于浏览器的商务逻辑语言等其它浏览器兼容的逻辑来实现打印按钮逻辑。

在另一个替换方案中，可使用是/否对话框来提供重新打印能力，该对话框被用于弹出和提示用户在该窗口按照脚本设定关闭以前回复是否正确地打印了标签。如果用户表示标签没有正确打印，则将重新打印该标签。可任选地，将向邮资供应商服务器提供重新打印通知。

在另一个替换方案中，诸框的顺序可被交换，并且隐藏信息可被重叠在屏幕上。此外，可添加其它隐藏或可见框。

IBDS 系统可向邮资中介提供模板和/或 API 以便进行顾客页面的开发。或者，邮资中介可针对终端用户的机器设计满足上述约束的网页。要在用户的计算机上的新的浏览器窗口中创建的网页把所有菜单、工具条、滚动条和状态栏从浏览器窗口实现中移除。键击扫视及诸如窗口大小调整等任何其它用户控制也被禁用。这一浏览窗口可说是安全的，因为用户不能够改变其中任何设置。

在可见框中呈现样本标签，而在隐藏框中有对应的可使用的标签。可见框中的打印按钮启动打印对话框，但是目标是不可见框。在打印以后，该窗口按照脚本设定关闭。

参考图 7，描述根据本发明的一个说明性实施例用于打印带邮资的运送标签的方法 700。

在步骤 710，用户通过运送顾客系统 410 向邮资中介系统 420 表示打印运送/邮资标签的愿望。在步骤 720，邮资中介系统 420 在认证用户以后向 IBDS 系统 430 发送请求。在步骤 725，IBDS 系统 430 提供创建具有邮资邮戳的新的安全窗口所需的数据。此信息可被直接发送到用户，或可被发送到邮资中介，然后转发给用户。

在步骤 730, 用户计算机 410 呈现新的安全浏览器窗口, 它具有如本文中所描述的可见框和打印按钮, 并且其中隐藏了实际图像。在步骤 740, 用户选择打印按钮。在步骤 750, JavaScript 代码从隐藏框打印带邮资的实际运送标签。在步骤 755, 用户指示是否清晰地打印了带邮资的运送标签。如果是, 则在步骤 760 关闭安全窗口。

如果用户指示没有正确地打印该标签, 则在步骤 770 进行另一次打印该标签的尝试。在步骤 780, 用户指示重新打印尝试是否成功。如果是, 则在步骤 760 关闭安全窗口。如果否, 则在步骤 790 将出错记入日志, 并调查该问题。然后在步骤 760 关闭安全窗口。

在一个替换方案中, 安全窗口仅在诸如五分钟等一段时间内可用。由此, 必须在五分钟的时间窗口中启动重新打印请求才能使该请求被处理。在另一个替换方案中, 该段时间以后的重新打印请求启动具有新标识符的新的运送标签事务。

用于定位标签或标签数据的 URI、URL 或其它标识符可包括相对很长的 URL, 从而在合理时间量中它不可能被猜出。在一个替换方案中, 可使用会话标识符或其它已知的用户访问方案来对主存标签的 URL 位置进行口令保护。在一个实施例中, 标签被主存在未被加密的 GIF 文件中。据此, 只要该 GIF 是使用很长且难以猜出的 URL 在很短的时间内对公众可用, 则用户信息(例如, 名字和地址)不应易受攻击。

或者, 可使 GIF 仅对来自某些 IP 地址的请求可用。例如, 可将从其接收所有请求的那些 IP 地址记入日志。据此, 如果从单个 IP 地址接收到不合理的数量的请求, 则可将该 IP 地址标识为某人用来探查标签的有敌意的 IP 地址。可拒绝此类地址访问。此外, 如果攻击者轮询了不合理数量的并不存在的标签地址(一个也可能是个不合理的), 则可将该 IP 地址记入日志, 封锁该 IP 地址并在稍后调查是否可能有欺诈。

分配邮资功能请求包括邮资中介标识符、事务标识符和消息签名。在此, 邮资中介标识符和事务标识符的组合至少在一定时间段上应该是唯一的。例如, 在线拍卖环境中, 应将拍卖事务标识符作为邮资请求事务标识符使用, 从而底层的事务和邮资事务被相互关联。

参考图 8, 示出根据本发明的一个说明性实施例用于将打印数据记入日志并计算欺诈标志比的过程。在一个实施例中, 可信任顾客不会在退款请求中进行欺诈。例如, 如果邮资标签两次不能正确打印, 则将向顾客收取没有使用的邮资。然后顾客将必须请求邮资退款。但是, 在一个优选实施例中, 使用跟踪信息来确定是否要

兑现退款请求。或者，可兑现退款请求，并收集数据以供稍后用于检测是否有任何欺诈。

欺诈检测过程在步骤 810 开始。在步骤 812，该过程确定它在分配的时间量中是否接收到来自最终用户浏览器的打印结果响应。如果没有，则该过程前进至步骤 814 并将注明没有接收到任何响应的默认响应记入日志，但前进至步骤 838 以将默认打印成功指示记入日志。如果接收到响应，则该过程前进至 816。在步骤 816，该过程确定打印是否成功。如果是，则该过程也前进至步骤 838 以将成功打印记入日志。如果指示显示打印没有成功，则该过程前进至步骤 818 并将不成功的打印尝试记入日志。在步骤 820，该过程向用户提供重新打印运送标签的机会。

在步骤 822，该过程再次轮询用户以确定重新打印是否成功。

在一个替换方案中，描述一种用于检测带标识符的运送标签的用户是否有欺诈的方法。该系统接收对应于运送标签的打印成功指示符。它还接收在运送流中所使用的标识符的列表。如果打印成功指示符是否定的，则若在指示符列表中出现该指示符，系统即报告可能有欺诈。如果打印成功指示符是肯定的，则若该指示符在指示符列表中至少出现两次，系统即报告可能有欺诈。在一个替换方案中，周期性地接收标识符列表，诸如每日、每周、每月或每两年。在另一个替换方案中，标识符列表包括在诸如前六个月或其它时间段中认可的标识符。

如果带有成功打印指示符的标识符没有在诸如一天、一周、一个月或六个月等预期的包裹周期内被认可，则系统报告可能有欺诈。

在一个替换方案中，改为结合如邮件等诸如可被跟踪的运输项目等一种或多种类型的运输项目来使用本文中所描述的实施例，这些运输项目诸如包括但不限于运送标签项目、信封、明信片、邮资标签、标签和包裹等邮件。所使用的标识符包括一组或数组唯一或伪唯一的标识符。例如，可从行星码（planet code）、投递确认号、IBI 邮戳、邮件计数和允许号的组合、以及邮资机号和升序记录的组合等中选择这一组或数组标识符。可使用标识符组类型来区别来自不同组的相似标识符。据此，替换系统可仅将 IBI 邮戳作为标识符使用。但是，在双标识符组解决方案中，该系统还可使用 IBI 邮戳和行星码。

使用了邮资分配作为说明性应用描述了以上实施例。在替换实施例中，可使用本文中所描述的诸实施例来控制诸如票证等项目及其它有价项目的打印。此外，可使用本文中所描述的实施例来对分发受控的条款和报告进行分配。诸如票证、收据、条款、报告、金融票据和合同等有价文档可被控制。此外，样本和实际框不一



定需要包括相同的项目或信息。例如，可将条款摘要发送到可见框，而将整个条款发送到不可见框部分，以便仅在购买后才进行打印。

还参考了共同待批、共同拥有的于 2003 年 12 月 18 日提交的题为 **System And Method For Preventing Duplicate Printing In A Web Browser**（用于防止在 Web 浏览器中进行重复打印的系统和方法）美国专利申请第 10/707,508 号，以及在 2003 年 12 月 18 日提交的题为 **System and Methods for Facilitating Refunds of Unused Postage**（便于对未使用的邮资进行退款的系统和方法）的美国专利申请第 10/707,510 号。

本申请描述了用于提供包括邮资中介、支付和欺诈检测的资金记账的系统和方法。这些实施例是说明性的，而并不试图给出可能的配置的穷举列表。在描述了替换元素的地方，应理解它们是为了在不重复普通元素的情况下完整地描述替换实施例，无论是否就此进行明确的陈述。类似地，应理解，为一个以上实施例中所使用的元素描述的替换元素是为了描述每一个具有该元素的所述实施例的替换实施例。

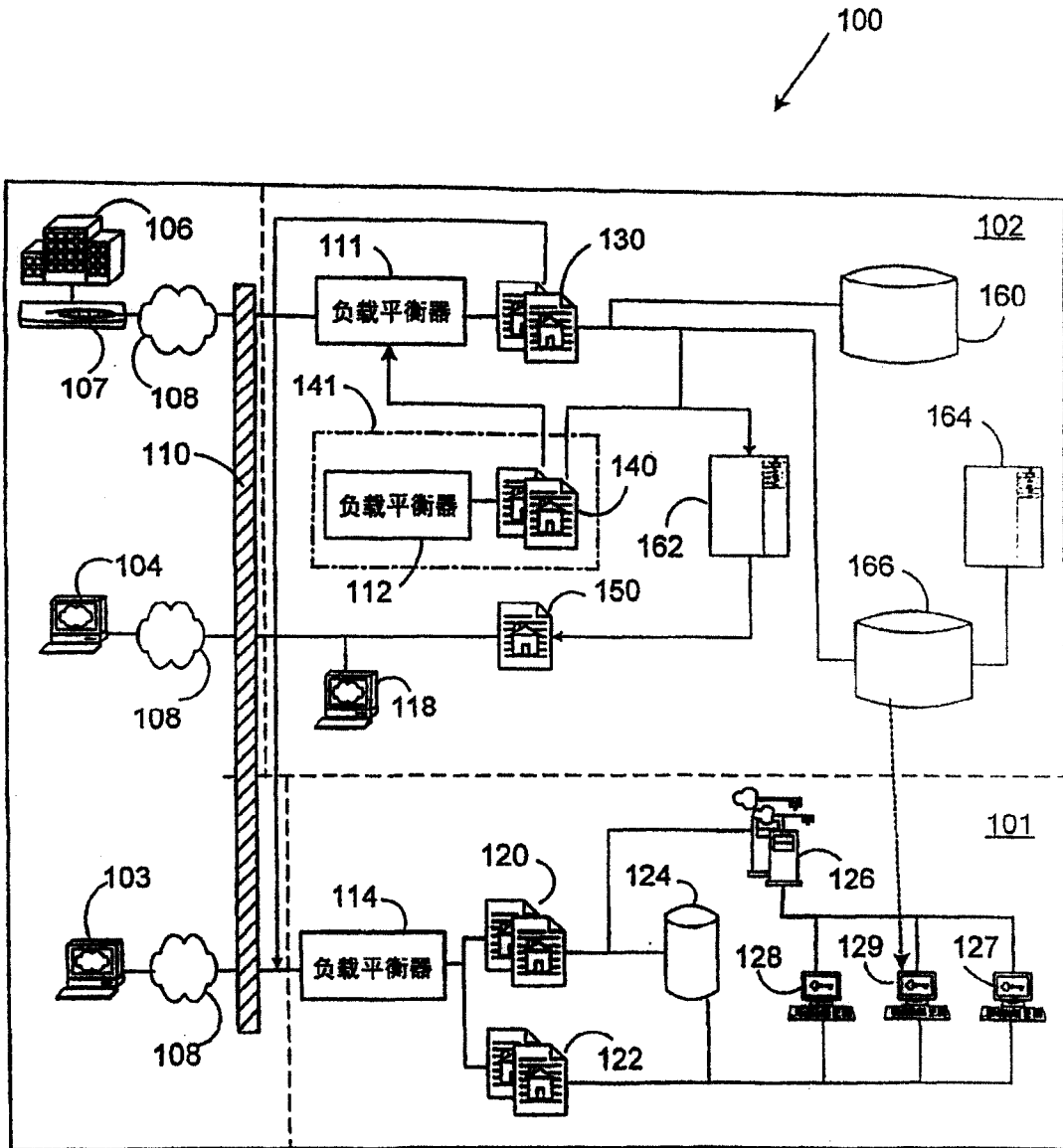


图 1

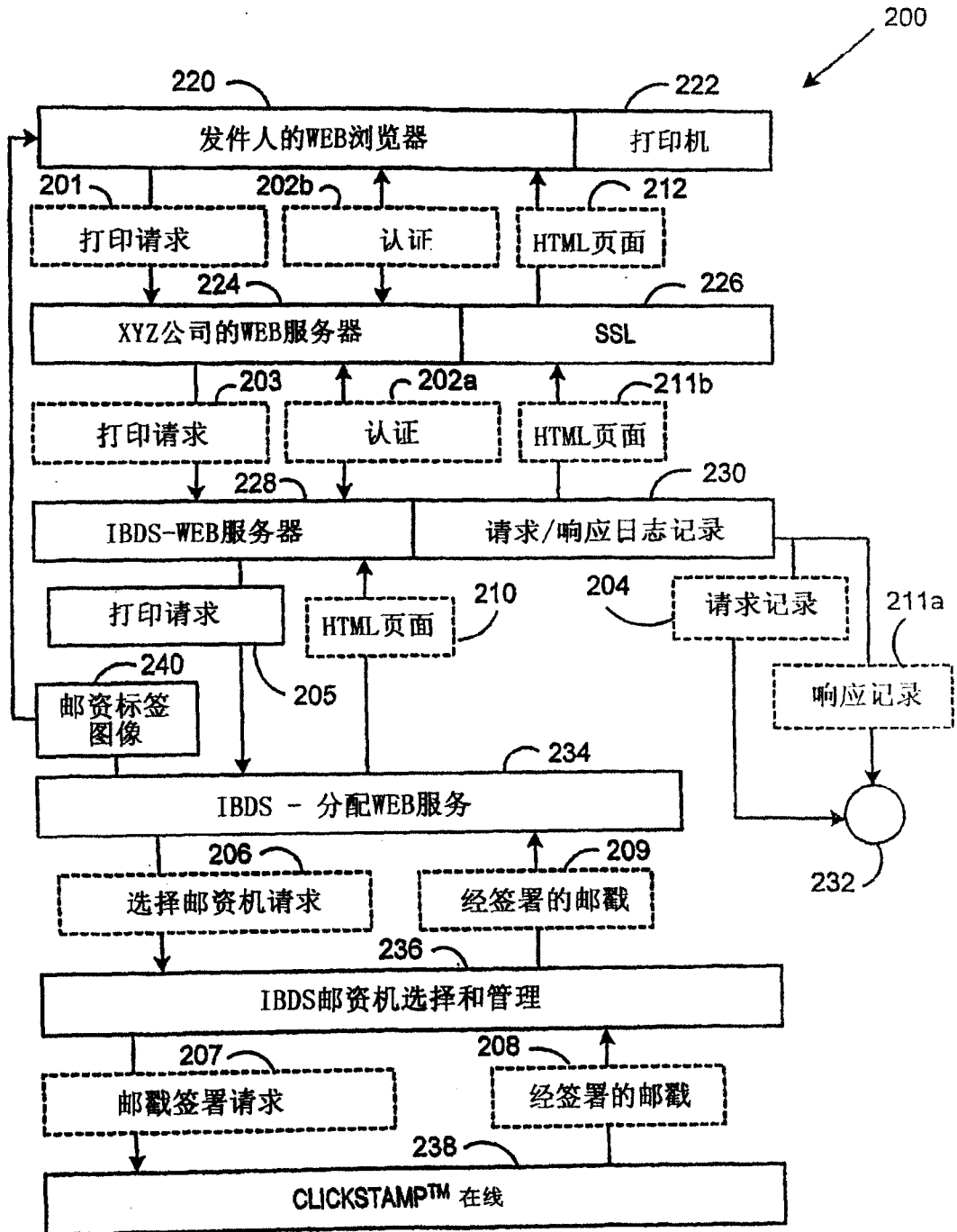


图 2

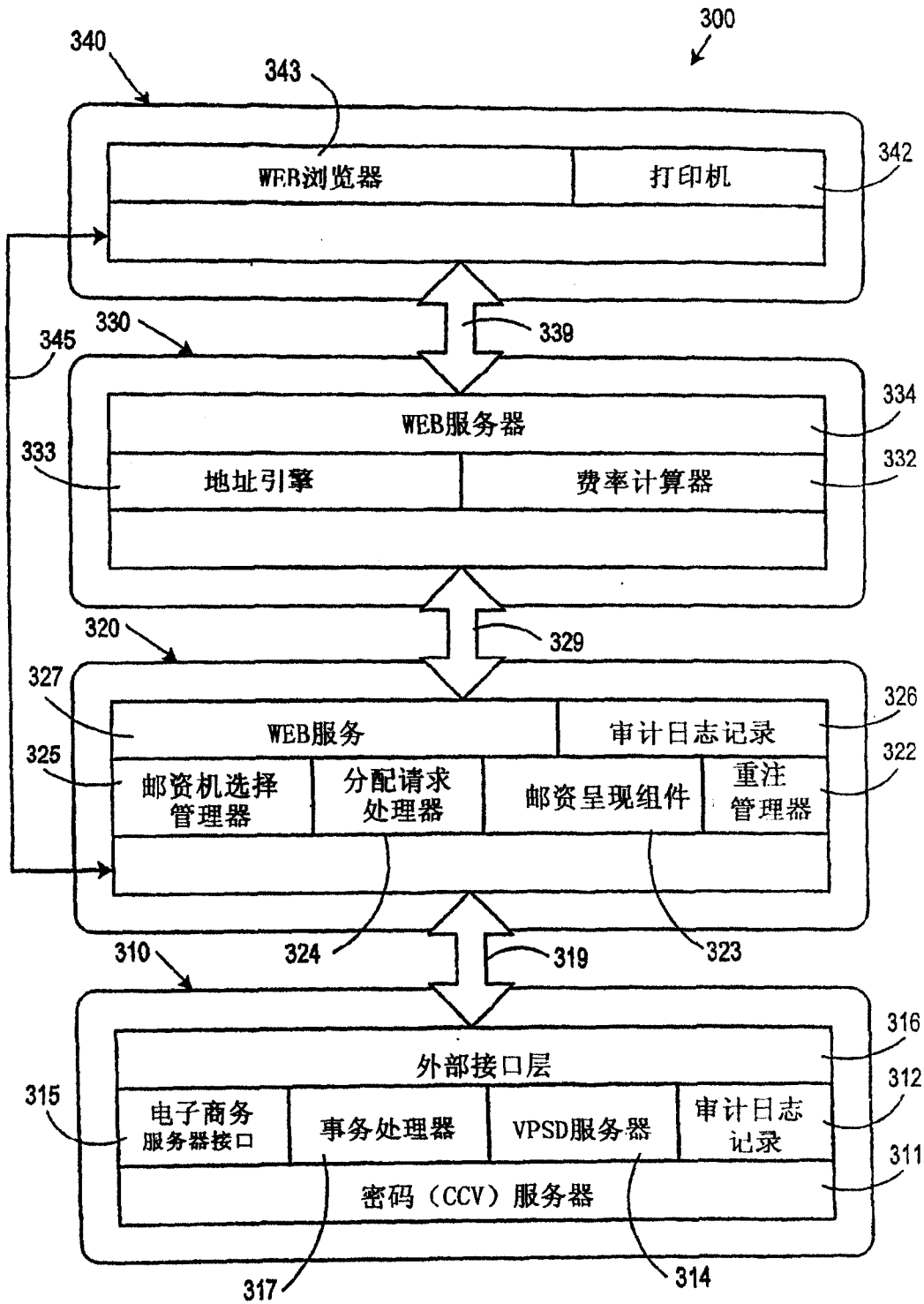


图 3

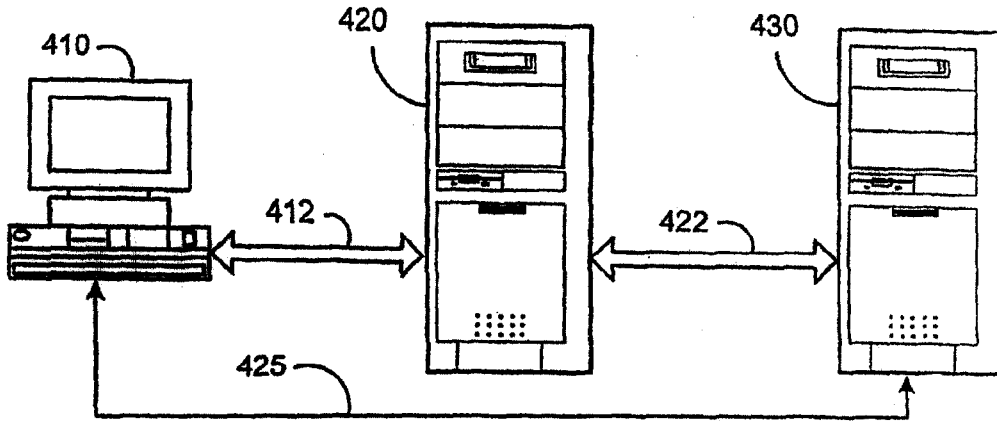


图 4

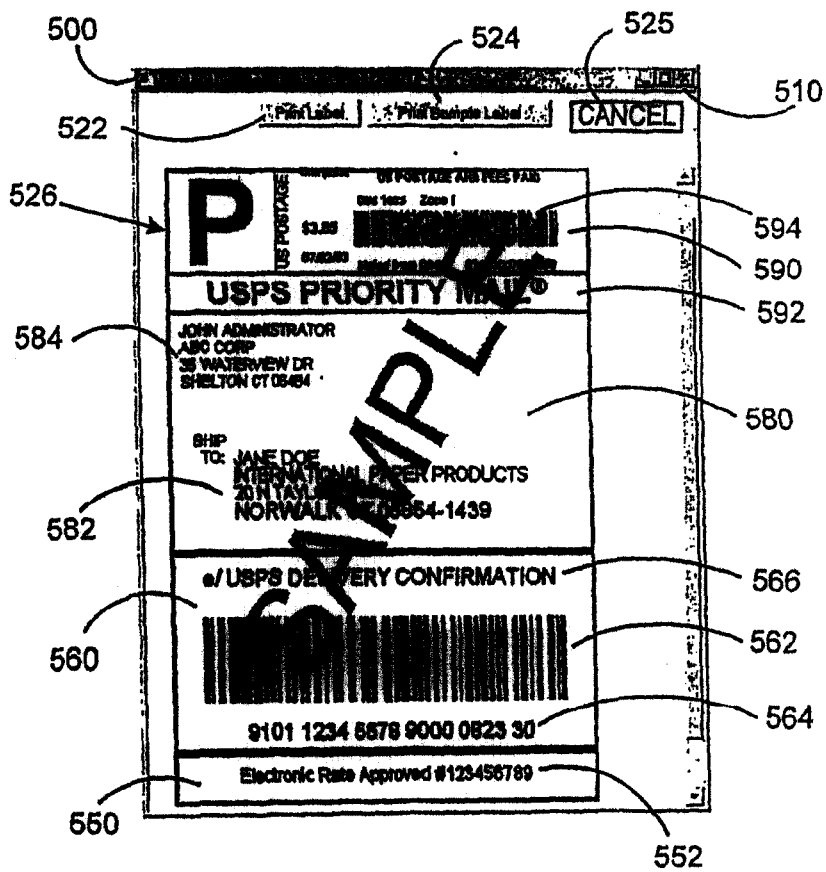


图 5

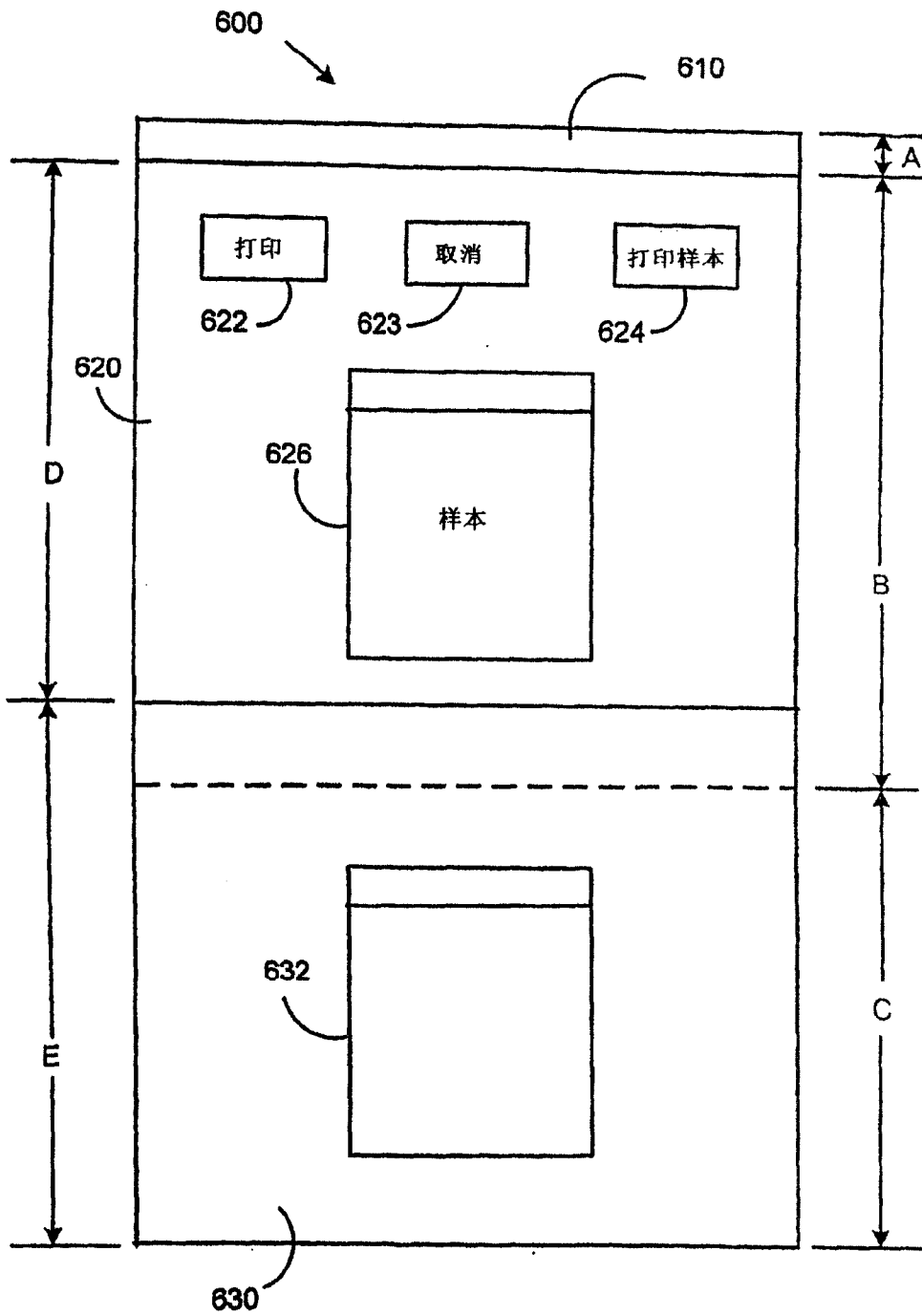


图 6

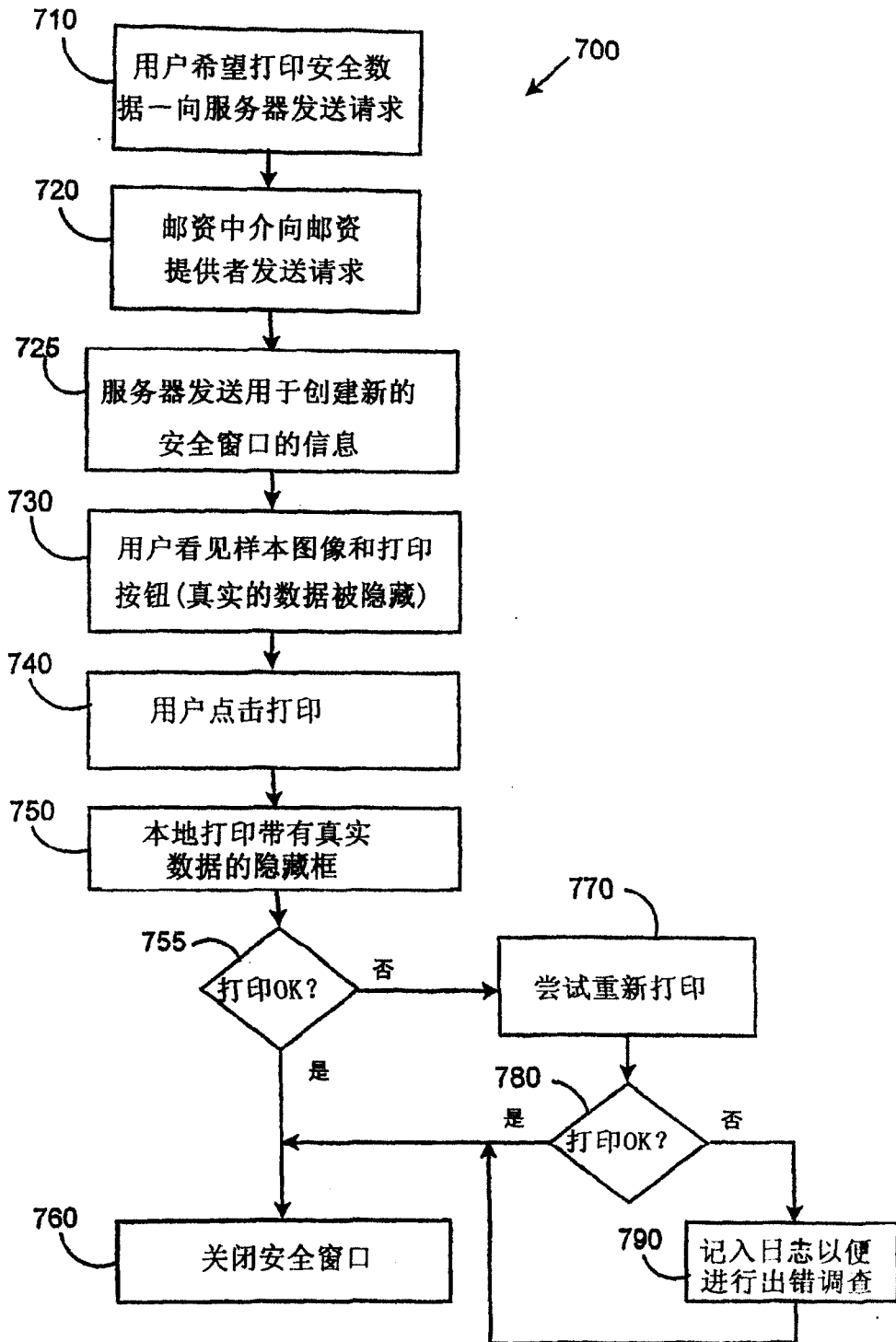


图 7

