(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1716293 B
(45)授权公告日 2012.04.18

(21)申请号 200510082282.5

(22)申请日 2005.06.29

(30)优先权数据
10/879,626 2004.06.29 US

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 D·M·黑佐尔 E·E·莫菲
G·J·胡尔藤 J·T·古德曼
R·L·朗斯威特

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 钱慰民

(51)Int.Cl.
G06Q 10/10(2012.01)
H04L 29/06(2006.01)
G06F 17/30(2006.01)
H04L 12/58(2006.01)

(56)对比文件
WO 99/67731 A1,1999.12.29, 第14-38页, 图3,5-6.
CN 1350246 A,2002.05.22, 全文.
US 2003/0069652 A1,2003.04.10, 全文.

审查员 唐嫣

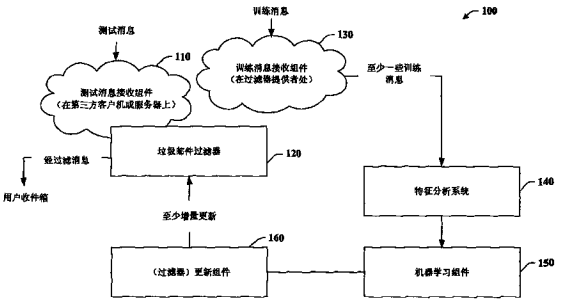
权利要求书 4 页 说明书 12 页 附图 9 页

(54)发明名称

增量反垃圾邮件查找与更新服务

(57)摘要

本发明提供一种便于几乎实时或实时地增量更新垃圾邮件过滤器的独特系统与方法。增量更新可部分地通过差异学习来生成。差异学习涉及基于新数据来训练一新垃圾邮件过滤器,然后寻找该新垃圾邮件过滤器和现有垃圾邮件过滤器之间的差异。差异可至少部分地通过比较参数变化的绝对值(两个过滤器间特征的权重变化)来确定。也可使用诸如参数频率等的其他因素。此外,关于特定特征或消息的可用更新可使用一个或多个查找表或数据库来查找。例如,当增量和/或特征专用更新可用时,它们可由诸如客户机下载。增量更新可被自动提供,或可依照客户机或服务器的偏好根据请求来提供。



CN 1716293 B

1. 一种反垃圾邮件更新系统，其特征在于，包含：

一垃圾邮件过滤器，所述垃圾邮件过滤器被训练成在垃圾邮件和好的邮件之间进行区分；

一更新组件，所述更新组件用更新信息来增量地增加或替换所述垃圾邮件过滤器的至少一部分，以便于防止垃圾邮件，其中，所述更新组件至少部分地通过使用一机器学习组件来构建；以及

机器学习组件，所述机器学习组件用从一个或多个新接收的邮件中提取的数据来训练第一新过滤器；确定所述第一新过滤器和所述垃圾邮件过滤器之间的差异是否满足一个阈值；训练第二新过滤器，该第二新过滤器被约束为当所述第一新过滤器和所述垃圾邮件过滤器之间的差异不满足所述阈值时维持所述垃圾邮件过滤器的特征的权重；以及确定所述垃圾邮件过滤器和所述第二新过滤器之间的差异是否满足一个或多个阈值，用于增加或替换所述垃圾邮件过滤器的至少一部分，其中所述更新组件所使用的更新信息至少部分基于所述垃圾邮件过滤器和所述第二新过滤器之间的差异。

2. 如权利要求 1 所述的系统，其特征在于，所述更新组件至少更新所述垃圾邮件过滤器的数据部分。

3. 如权利要求 1 所述的系统，其特征在于，所述系统在客户机或服务器的至少一个上运行。

4. 如权利要求 1 所述的系统，其特征在于，所述更新组件是用基于匹配或基于散列的数据来训练的。

5. 如权利要求 1 所述的系统，其特征在于，还包含一支付确认组件，它在向所述垃圾邮件过滤器提供一个或多个更新前，确定客户机或服务器是否已为接收更新付款。

6. 如权利要求 1 所述的系统，其特征在于，所述更新组件通过多个 IP 地址向所述垃圾邮件过滤器提供更新信息，以减轻拒绝服务攻击。

7. 如权利要求 1 所述的系统，其特征在于，所述更新信息包括对应于一个或多个参数改变的一个或多个增量更新文件。

8. 如权利要求 1 所述的系统，其特征在于，所述垃圾邮件过滤器的至少一部分包含专用于至少一个特征的数据。

9. 如权利要求 8 所述的系统，其特征在于，所述至少一个特征包含 IP 地址和 URL 的至少一个。

10. 如权利要求 1 所述的系统，其特征在于，所述学习组件学习现有垃圾邮件过滤器和新过滤器之间的最少数量参数改变，以便于将增量更新大小最小化。

11. 如权利要求 1 所述的系统，其特征在于，所述更新组件向所述垃圾邮件过滤器顺序地应用多个不同的更新。

12. 如权利要求 1 所述的系统，其特征在于，所述更新组件合并多个更新的至少一个子集，以提高所述更新信息的下载效率。

13. 如权利要求 1 所述的系统，其特征在于，所述更新组件以一种独立方式选择性地提供特征专用更新，使得至少一个特征独立于至少一个其他特征来更新。

14. 如权利要求 1 所述的系统，其特征在于，所述垃圾邮件过滤器包含多个子过滤器，它们被彼此独立地训练或更新，且结果是可分解的。

15. 如权利要求 1 所述的系统，其特征在于，还包含一隔离组件，它延迟邮件的至少一个子集的分类，直到所述垃圾邮件过滤器从所述更新组件接收到所述更新信息。

16. 一种反垃圾邮件查询系统，其特征在于，包含：

一机器学习垃圾邮件过滤器，它被训练成在垃圾邮件和好的邮件之间进行区分；

一查找组件，它在邮件到来时接收对于特征相关信息的查询，以便于更新所述机器学习垃圾邮件过滤器；

特征分析系统，用于基于从训练消息的至少一部分中提取的各特征及其相应的权重来生成最新近的数据；以及

用于存储由所述特征分析系统生成的数据的查找数据库，

其中，如果任何来自所述查找数据库的数据满足所述查询，则发送或下载相对应的信息来更新所述机器学习垃圾邮件过滤器，并且

其中所述基于从训练消息的至少一部分中提取的各特征及其相应的权重来生成最新近的数据包括：用从一个或多个新接收的邮件中提取的数据来训练第一新过滤器；确定所述第一新过滤器和所述机器学习垃圾邮件过滤器之间的差异是否满足一个阈值；训练第二新过滤器，该第二新过滤器被约束为当所述第一新过滤器和所述机器学习垃圾邮件过滤器之间的差异不满足所述阈值时维持所述机器学习垃圾邮件过滤器的特征的权重；以及确定所述机器学习垃圾邮件过滤器和所述第二新过滤器之间的差异是否满足一个或多个阈值，用于增加或替换所述机器学习垃圾邮件过滤器的至少一部分，其中被发送或下载的用于更新所述机器学习垃圾邮件过滤器的所述相对应的信息至少部分基于所述机器学习垃圾邮件过滤器和所述第二新过滤器之间的差异。

17. 如权利要求 16 所述的系统，其特征在于，所述特征相关信息包含关于多个特征或邮件的正或负数据。

18. 如权利要求 16 所述的系统，其特征在于，所述特征相关信息包含关于多个特征的特征得分和名誉得分，所述多个特征包括 IP 地址、URL、主机名、字符串及单词的至少一个。

19. 如权利要求 16 所述的系统，其特征在于，所述机器学习垃圾邮件过滤器是特殊地训练的。

20. 如权利要求 16 所述的系统，其特征在于，所述机器学习垃圾邮件过滤器是至少部分地被增量更新的。

21. 如权利要求 16 所述的系统，其特征在于，所述机器学习垃圾邮件过滤器是至少部分地由所述查找组件更新的。

22. 如权利要求 16 所述的系统，其特征在于，所述查找组件将增量查找查询写入文件或将增量查找查询存储在磁盘上，并在存储器中将其组合。

23. 如权利要求 16 所述的系统，其特征在于，所述查找组件包含：

一后端数据库，它包含一组特征及相关联的权重，及在训练过程中生成的一个或多个模型；

一中间件层，它在所述后端数据库和所述机器学习垃圾邮件过滤器之间传递信息；以及

所述机器学习垃圾邮件过滤器，它以预定或自动频率调用所述中间件层，以获取最新近的更新模型，并将一在线模型与本地存储的模型文件合并。

24. 如权利要求 16 所述的系统，其特征在于，所述查询包含对来自客户机或服务器的至少一个的所述机器学习垃圾邮件过滤器的信息增量更新的请求。

25. 如权利要求 16 所述的系统，其特征在于，还包含一更新的垃圾邮件过滤器，它以至少两个阶段从服务供应者传播到终端用户，其中，所述阶段的至少一个是自动的，使得有一在所述两阶段间进行人工干涉的选项。

26. 如权利要求 16 所述的系统，其特征在于，还包含一组件，它将所述机器学习垃圾邮件过滤器的代码自动地从服务供应者传播到终端用户。

27. 如权利要求 16 所述的系统，其特征在于，根据终端用户或管理员偏好，查询以指定时间间隔发送到所述查找组件。

28. 如权利要求 16 所述的系统，其特征在于，对于所述机器学习垃圾邮件过滤器的更新无须重启一消息通信程序即可起效。

29. 一种反垃圾邮件更新方法，其特征在于，包含：

提供一现有的已训练垃圾邮件过滤器；

有区别地用机器学习和来自一个或多个邮件的数据来训练一第一新垃圾邮件过滤器；

确定现有的已训练垃圾邮件过滤器和所述第一新垃圾邮件过滤器间的第一组差异是否满足一阈值或试探；

用新邮件数据训练第二新垃圾邮件过滤器，所述第二新垃圾邮件过滤器被约束为当所述第一新垃圾邮件过滤器和所述现有的已训练垃圾邮件过滤器之间的差异不满足所述阈值时维持所述现有的已训练垃圾邮件过滤器的特征的权重；

确定所述第二新垃圾邮件过滤器和现有的已训练垃圾邮件过滤器之间的第二组差异；以及

用所述第二组差异的子集来增量地更新所述现有的已训练垃圾邮件过滤器。

30. 如权利要求 29 所述的方法，其特征在于，所述现有的已训练垃圾邮件过滤器是用机器学习来训练的。

31. 如权利要求 29 所述的方法，其特征在于，所述现有的已训练垃圾邮件过滤器当前正由一消息通信程序使用，以将消息分类为垃圾邮件或好的邮件。

32. 如权利要求 29 所述的方法，其特征在于，所述第一和第二新垃圾邮件过滤器是在较新近的或新的数据上训练的。

33. 如权利要求 29 所述的方法，其特征在于，所述第一组和第二组差异分别包含所述现有的已训练垃圾邮件过滤器和所述第一和第二新垃圾邮件过滤器之间的一个或多个参数改变。

34. 如权利要求 29 所述的方法，其特征在于，所述方法基于 web。

35. 如权利要求 29 所述的方法，其特征在于，还包含至少部分地通过搜索查找表和数据库的至少一个，来请求对所述现有的已训练垃圾邮件过滤器的特征专用更新。

36. 如权利要求 29 所述的方法，其特征在于，所述增量地更新所述现有的已训练垃圾邮件过滤器至少部分地基于客户机、服务器或用户的任何一个收到的消息的分发。

37. 如权利要求 29 所述的方法，其特征在于，对于所述现有的已训练垃圾邮件过滤器的一或多个增量更新是特征专用的，使得至少一个特征被独立于另一特征而更新。

38. 如权利要求 35 所述的方法，其特征在于，所述查找表和数据库由对应于多个特征的多个增量更新组成。

39. 一种反垃圾邮件更新系统，其特征在于，包含：

用于提供一现有的已训练垃圾邮件过滤器的装置；

用于有区别地使用机器学习和来自一个或多个邮件的数据来来训练一第一新垃圾邮件过滤器的装置；

用于确定现有的已训练垃圾邮件过滤器和所述第一新垃圾邮件过滤器之间的第一组差异是否满足一阈值或试探的装置；

用于用新邮件数据训练第二新垃圾邮件过滤器的装置，所述第二新垃圾邮件过滤器被约束为当所述第一新垃圾邮件过滤器和所述现有的已训练垃圾邮件过滤器之间的差异不满足所述阈值时维持所述现有的已训练垃圾邮件过滤器的特征的权重；

用于确定所述第二新垃圾邮件过滤器和现有的已训练垃圾邮件过滤器之间的第二组差异的装置；以及

用于使用所述第二组差异的子集来增量地更新所述现有的已训练垃圾邮件过滤器的装置。

40. 如权利要求 39 所述的更新系统，其特征在于，还包含用于至少部分地通过搜索查找表和数据库的至少一个来请求对于所述现有的已训练垃圾邮件过滤器的特征专用更新的装置。

增量反垃圾邮件查找与更新服务

(1) 技术领域

[0001] 本发明涉及识别合法邮件（例如好邮件）和不受欢迎的信息（例如垃圾邮件）的系统与方法，尤其涉及在消息处理过程中向现有的经训练的垃圾邮件过滤器提供几乎实时或实时的更新。

(2) 背景技术

[0002] 诸如因特网之类的全球通信网络的出现提供了与大量潜在顾客建立联系的商业契机。电子消息，尤其是电子邮件（“e-mail”），作为向网络用户散布不需要的广告与促销（也称“垃圾邮件”）的手段，正变得越来越普遍。

[0003] Radicati 集团有限公司—一家咨询与市场研究公司，估计到如在 2002 年 8 月，每天有 20 亿垃圾电子邮件消息被发送—此数字预期每两年增至三倍。个人与企业（例如公司、政府机构）感觉日益不便，并时常不胜垃圾邮件之烦。同样地，垃圾电子邮件如今或即将成为对于可信计算的一种主要威胁。

[0004] 一种用于阻碍垃圾电子邮件或兜售信息的关键技术是使用过滤系统和 / 或方法。然而，垃圾邮件发送者为了规避过滤器而不断地改变他们的技术。因而期望能随垃圾邮件发送者技术改变而迅速并自动地更新过滤器，并将其传播到由消息客户机和 / 或服务器运行的终端应用程序。

[0005] 例如，可能有大约 1 亿个消息通信程序的副本正被客户机使用。此外，每天都能创建出新的垃圾邮件过滤器。因为垃圾邮件过滤器可能相当大，且可能需要每天将其分发到运行该过滤器副本的每一客户机，在客户机方和过滤器供应者方，这一实行即使不是被禁止的，也是有问题的。尤其是，可能要求客户机经常下载大文件，因而消耗了大量处理器内存，并降低了处理速度。因为过滤器供应者可能必需每天为所有用户和 / 或客户机更新该过滤器的所有副本，因此可能需要的带宽和服务器是极大量且不可行的。在此类情况下，比每天一次更频繁地提供新过滤器如果不是完全不可能，也是几乎不可能的。

(3) 发明内容

[0006] 为了提供对于本发明某些方面的基本理解，下文提出了本发明的简化概述。此概述不是本发明的广泛综览。它不试图标识本发明的关键 / 决定性元素，或描绘本发明的范畴。它唯一的目的是以简化的形式提出本发明的某些概念，作为将于后文提出的更详细描述的序言。

[0007] 本发明涉及一种便于以实时或几乎实时的方式向垃圾邮件过滤器提供局部或增量更新形式的新信息或数据的系统和 / 或方法。提供一种可用最新信息更新过滤器的几乎实时的机制可以是提供对抗到来的垃圾邮件攻击的最有效保护的一种策略。

[0008] 具体地，本发明涉及向现有过滤器传递信息的增量部分，以便于保持过滤器对于新的好消息和 / 或新的垃圾邮件是最新的。这部分地可通过差异学习来达成，其中可将现有过滤器的一个或多个参数与新过滤器的相应参数进行比较。显示某些改变的参数可被相

应地更新，从而减轻了替换整个过滤器的每一个副本的需要。因而，可发送现有过滤器和新过滤器间的“差异”来更新现有过滤器。结果，每个更新的大小可以相对较小甚至更小，取决于更新的频率。这部分地归功于下面事实：更新的信息主要基于新的好消息或新的垃圾邮件；并且每小时只收到这么多垃圾邮件或好的消息。因而，在任意给定时帧内进行同样多次的更新在对抗垃圾邮件的斗争中变得相当高效且有效。

[0009] 根据本发明的一个方面，增量更新部分地可由服务器来确定。服务器可决定更新其过滤器的哪些部分、获得这些更新、随后将其提供给决定参与或付费接收它们的用户或客户机。

[0010] 根据本发明的另一方面，增量更新部分地可由用户或客户机经由基于 web 的服务来确定。具体地，客户机可收到一消息，其当前过滤器在将该消息分类为垃圾邮件或好的邮件时存在困难。基于 web 的服务可提供一查找表或数据库，该查找表或数据库包括关于新近被确定为指示好的消息或垃圾邮件的消息或消息特征的数据或其他信息。通过从该消息中提取某些信息，客户机可查询该基于 web 的服务，来确定对于其过滤器是否存在任何更新的信息。

[0011] 例如，客户机收到一消息，且该客户感到难以将其分类为垃圾邮件或是好的邮件。该客户机可提取该消息的某一部分，诸如发送者的 IP 地址、消息中的 URL、或该消息的散列，来向基于 web 的查找服务请求更新的信息。在一实例中，可向基于 web 的服务提交一查询。可选地或另外地，客户机可参考由查找服务用当前信息构建并维护的一个或多个查找表或数据库。当找到至少一个更新时，可相应地更新该客户机的过滤器。如果服务确定客户机需要一系列更新，则服务可仅提供最新的更新，来减少需要下载的更新总数。

[0012] 在任意给定垃圾邮件过滤器上可以有数以千计的可更新的不同参数。由于这些过滤器的特性，对一个参数值的一个小改变可引起几乎所有参数的值的某种改变。因而，可有各种方法来确定要更新过滤器的哪些部分，以提供最有效的垃圾邮件保护。在本发明的一个方面，可以检查参数变化的绝对值。可选择显示值的最大变化的参数来更新。或者，可设置一阈值变化量（例如基于绝对值）。可标记超出该阈值的任何参数来进行更新。也可考虑诸如在到来的消息中的参数或特征的频率等其他因素。

[0013] 在本发明的另一方面，增量更新可以是特征专用的，并以服务器或客户机偏好所期望的速度发生。此外，可构建过滤器来使旧过滤器与新过滤器间的参数变化数量最小化。因而，任何一次过滤器更新（例如数据文件）的总的大小，及要更新的参数个数可比其他情况下小得多。

[0014] 为达成前述及相关目的，此处结合以下描述与附图，描述了本发明的某些说明性方面。但是，这些方面只是示意可使用本发明原理的各种方法中的几种，并且本发明旨在包括所有此类方面及其等效方面。当结合附图考虑时，从以下本发明的详细描述中，本发明的其他优点与新颖特征将变得显而易见。

(4) 附图说明

[0015] 图 1 是根据本发明的一个方面的反垃圾邮件更新系统的框图，该系统便于向垃圾邮件过滤器提供机器学习的更新。

[0016] 图 2 是根据本发明一个方面的增量更新系统的示意性框图。

[0017] 图 3 是一示意图，它根据本发明的一个方面展示了用于生成具有限数量参数变化的垃圾邮件过滤器或其更新的系统或机制。

[0018] 图 4 是根据本发明一个方面的反垃圾邮件更新系统的框图，该系统至少部分地基于客户机请求。

[0019] 图 5 是根据本发明一个方面的反垃圾邮件更新系统的框图，该系统至少部分地基于客户机请求。

[0020] 图 6 是根据本发明一个方面的示例性反垃圾邮件查找 web 服务的示意图。

[0021] 图 7 是根据本发明的一个方面示出一示例性方法的流程图，该方法便于至少增量地更新垃圾邮件过滤器。

[0022] 图 8 是根据本发明的一个方面示出一示例性方法的流程图，该方法便于生成呈现与前一过滤器的最小数量的更新或改变的过滤器。

[0023] 图 9 示出了用于实现本发明各个方面的示例性环境。

(5) 具体实施方式

[0024] 现参考附图对本发明进行描述，贯穿附图，相同的参考标号指相同的元素。在以下描述中，出于解释的目的，阐述了大量具体细节以提供对本发明的彻底理解。然而，明显的是，无须这些具体细节即可实施本发明。在其他实例中，为了便于描述本发明，以框图形式示出众所周知的结构与设备。

[0025] 如在本申请中所使用的，术语“组件”与“系统”意指计算机相关实体，它或者是硬件、硬件与软件的组合、软件或执行中的软件。例如，组件可以是，但不限于，运行在处理器上的进程、处理器、对象、可执行码、执行线程、程序及计算机。作为示例，运行在服务器上的应用程序和该服务器都可以是组件。一个或多个组件可以驻留在进程和 / 或执行线程内，且组件可以位于一台计算机上和 / 或分布在两台或多台计算机之间。

[0026] 本发明可结合各种关于向机器学习或非机器学习垃圾邮件过滤器至少提供局部或增量更新的推断方案和 / 或技术。如本文中所使用的，术语“推断”一般指根据一组经由事件和 / 或数据捕捉到的观测，来推理或推断系统、环境和 / 或用户状态的过程。例如，推断可用于标识一特定上下文或行为，或可生成各状态的概率分布。推断可以是概率性的——即，基于对数据和事件的考虑对所关注的状态概率分布的计算。推断也可指用于从一组事件和 / 或数据中组成更高级事件的技术。此类推断导致从一组观测到的事件和 / 或存储的事件数据中构造新的事件或行动，而无论这些事件是否在时间上密切相关，也无论这些事件和数据是否来自一个还是数个事件和数据源。

[0027] 本发明的各个方面可应用于机器学习和非机器学习过滤器。在一普通实现中，机器学习垃圾邮件过滤器通过使用一种机器学习算法来计算从消息中提取的各个特征的权重，从而获知什么是好的消息和垃圾邮件的特征的定义。当一主机应用程序收到一消息时，可对该消息流进行语法分析，并检查被强调为垃圾邮件或好消息指示符的特征或特性。随即组合这些被强调的特征，以生成该消息是否为垃圾邮件的总概率。如果消息满足一特定概率“阈值”，那么该消息可基于主机应用程序的设置采取一道所分配的行动。例如，好消息可被引导到收件人的收件箱，而垃圾邮件消息可被路由到一特殊文件夹或被删除。

[0028] 垃圾邮件发送者在不断改编他们的方法。通过以前的反馈循环和机器学习技术，

可自动且容易地生成新的过滤器。然而，有效率地向其用户迅速地（诸如实时或几乎实时地）传播这些新过滤器可以是同样重要的。新过滤器的传播可分解成两部分。第一部分涉及大小的问题。被传播的过滤器可以很大，且难以作为整体来容易地分发。幸运的是，这可至少部分地通过经由一查找系统发送旧过滤器和新过滤器间的“差异”来克服。如下文将讨论的，差异可根据大量因素和／或偏好（客户机或服务器）来确定和／或基于这些因素和／或偏好。

[0029] 第二个问题涉及过滤器更新的管理。在一方面，许多人可能希望包括新代码和新数据在内的对垃圾邮件过滤器所有改变可被自动传播。在另一方面，许多管理员可能希望在自动传播到其整个组织之前先在测试机器上安装新文件和／或数据。如在下面的图中所讨论的，通过经由在线查找服务仅将有差异的特征（权重）传递到存储器，可以减轻传播大过滤器的需要。

[0030] 现参考图 1，有一根据本发明的一个方面的反垃圾邮件更新系统 100 的概括性框图，该系统便于向旧的或现有的垃圾邮件过滤器提供差异信息。系统 100 包含测试消息接收组件 110，该组件使用至少一个垃圾邮件过滤器 120 来将到来的测试消息分类为垃圾邮件或好的邮件。测试消息接收组件 110 可位于第三方客户机或服务器（例如，家用计算机）中。可使用 SVM（支持矢量机）、最大熵模型（逻辑回归）、感知器、决策树和／或神经网络中的任一种对垃圾邮件过滤器 120 进行特殊训练。

[0031] 系统 100 还包含可接收各种训练消息的训练消息接收组件 130。例子包括反馈循环数据（例如，来自参与对到来的消息中至少一被选择的部分进行分类（垃圾邮件或好的邮件）的用户的数据）、用户抱怨、蜜罐 (honeypot) 数据等等。训练消息接收组件 130 可在过滤器供应者处找到。

[0032] 到来的训练消息的至少一部分可被路由到特征分析子系统 140，在那里对这些消息进行语法分析，并检查其类似垃圾邮件和／或非类似垃圾邮件的特征。具体地，诸如 IP 地址、URL 和／或特定文本等多个特征的特征可从每个消息中提取出来，随即被分析。使用机器学习组件 150，可用有区别的方法来训练更新组件 160。或者，可使用基于匹配或散列的数据来训练更新组件 160。被路由到特征分析子系统 140 的消息可以是未经过滤的或已过滤的消息，或者是两者的组合。将已过滤的消息分类为垃圾邮件或好邮件无需影响更新组件 160 的训练，或对垃圾邮件过滤器 120 的更新的产生。

[0033] 更新组件 160 包含诸如为多个消息和／或可从到来的消息中提取的特征（诸如单词、IP 地址列表、主机名、URL 等等）计算的权值之类的数据。此类数据可被组织成由更新组件 160 控制的一个或多个数据文件或者数据库。

[0034] 当由消息接收／分发系统（例如，一个或多个服务器）110 提示时，更新组件 160 可用附加信息至少增量地增加垃圾邮件过滤器 120 的至少一部分。例如，通过添加新的特征权重数据和／或用任何给定特征的新权重数据取代旧权重数据，更新组件 160 可更新垃圾邮件过滤器的数据部分。更新组件 160 还可被定制成在定时或调度的基础上提供增量更新（如果可用的话），从而将任一更新的相对大小最小化。更新本身也可以在定时基础上，或在收到的到来消息个数的基础上生成。例如，每小时和／或每接收到第 30 个消息后，可创建更新。

[0035] 现参考图 2，示出了一便于防止垃圾邮件的反垃圾邮件更新系统 200 的示意性框

图。概括而言，更新系统 200 将新参数数据与由现有垃圾邮件过滤器 210 所使用的旧参数数据进行比较。系统 200 包含特征提取－分析组件 220，该组件可检查从到来的消息中提取的特征，以识别相关特征（例如，指示垃圾邮件或好的消息）并确定其权重、得分及其他相关数据。此数据可在参数更新数据库 230 中存储及维护。可由参数分析组件 240 根据现有过滤器 210 中的旧参数数据来分析数据库中的新参数数据，从而确定是否有任何参数数据改变了。

[0036] 例如，参数的权重可升高或降低，以指示更重要或更次要的垃圾邮件特性。此外，可向现有过滤器 210 添加或删除参数。在后一情况中，当其权重跌至 0，参数或特征可从过滤器 210 中移除。

[0037] 如果确定对于任何特定参数集或子集存在更新，则此类参数可被传递给更新控制器 250。更新控制器 250 可从数据库 230 访问相关参数数据，并能随即将此类数据传递给现有过滤器 210。本质上，系统 200 向垃圾邮件过滤器提供一种更新服务，来保持它们对于新形式的垃圾邮件是最新且有效的。

[0038] 更新系统 200 可在客户机或服务器上自动运行。此外，该服务可通过订购来起作用，其中支付确认组件 260 可在提供任何更新前确定客户机或服务器是否已为更新或更新服务付款。或者，在允许查找或更新发生之前，过滤器 210 可核实该订购是最新的。

[0039] 更新查找系统（例如在图 1 和 2 中）可以是服务拒绝 (DOS) 或分布式 DOS 攻击的天然目标。因而可通过诸如将其遍及多个 IP 地址或对应于不同 IP 地址的多个主机名分布，来加强系统对抗此类攻击的能力。例如，在实践中，可将不同 IP 地址分发给不同用户（或客户机或服务器），从而使攻击者更难找出要攻击的 IP 地址的完全列表。

[0040] 有了机器学习技术，可有数以千计的可被更新的不同数字参数，因为实质上所有这些参数至少可作少量改变是可能的。结果，确定要作出什么更新可用数种不同的方法来决定。例如，一种方法涉及查看改变最大的参数的绝对值。然而，最大绝对值变化可能不是最能指示要更新哪些参数的。这在参数涉及很少被观测的特征的情况下尤其真实。因而，当确定要更新哪些参数时要考虑的其他因素可包括事件的发生、频率、或基于最新近数据的参数的共性。例如，如果参数改变很大，但对应特征仅在很少的消息中出现（例如，平均每 100,000 个消息中仅有 3 个），那么发送对此特征的更新可能不是对更新服务的有效使用。

[0041] 另一方法涉及查看参数的绝对值，该参数改变了某个使其变得重要的量（例如，改变了某个最小值或阈值），或者对于更普通的特征来说，改变了某一与较不普通的特征不同的最小值。如果满足一特定阈值，那么可更新参数。否则它保持不变。

[0042] 又一方法涉及构建试图限制参数改变的数量的过滤器或过滤器更新。一些被称作平衡特征的特征可彼此交互，并最终影响过滤器的行为。在训练期间，当没有在过滤器内恰当地虑及平衡特征时，该过滤器的性能可被改变。因而，构建限制参数改变数量的过滤器也可减轻跟踪是否恰当地虑及了平衡特征的需求。

[0043] 例如，设想当前使用的过滤器 A，对于单词“wet”有假定为 0 的权重，对于单词“weather”有一为负的很小权重。现在设想有包含单词“wet”（而不是 weather）的大量垃圾邮件到来。设想还有同时包含单词“wet”和“weather”的适量的好邮件。可学习新过滤器 B，它将“wet”加权为严重类似垃圾邮件，而“weather”有一平衡性的负（好）权值，因而

当这些单词同时出现时，它们的权重抵消，且该邮件不被分类为垃圾邮件。现在可能能够判定，与过滤器 A 相比，在过滤器 B 中的单词“wet”足够重要而要为其更新权重（它在大量邮件中出现），而单词 weather 则不然（它在少量邮件中出现，且作少量改变，因为它已经有一为负的很小权重）。因而，可传播对“wet”的更新，但无需传播对“weather”的平衡性更新，从而导致大量错误。为缓解此类不合需要的更新的创建，可构造将参数改变数量最小化的过滤器，如图 3 所示。

[0044] 根据该图，从包含旧数据的特征和权重的旧过滤器 X310 开始。现使用机器学习训练新过滤器 Y1320。根据某些试探 330 找到 X310 和 Y1320 之间重要的差异。例如，可测量该差异的绝对值；从该差异中得到的信息；该差异的绝对值乘以使用该参数的频率；等等。在线性模型的情况下（例如，SVM 模型、单纯贝叶斯模型、感知器模型、最大熵或逻辑回归模型），模型由特征（例如，消息中的单词）的权重组成。对于线性模型，这包括寻找根据这些度量之一改变最多的特征权重 (340)。

[0045] 接下来，可学习新过滤器 Y2 350，它服从下面约束：过滤器间的所有小的（或不够重要的 360）差异在 Y2 350 中必须有和在 X310 中相同的值。例如，对于线性模型，这意味着非改变很大的特征的权重在 Y2 350 和在 X310 中是相同的。然而，对于改变很大（例如，满足某一阈值或试探）的特征，在 Y2 350 中的权重不同。参考之前“wet”和“weather”的例子，当“wet”被认为是坏的，它不能被认为是太坏的词，因为其平衡权重（“weather”）将被固定。因而不再需要跟踪是否虑及平衡性特征。

[0046] 可任选地，此程序可被反复，以找出仅其权重一向不同的那些特征。例如，因为“weather”参数值不能改变，可决定不改变“wet”参数值。

[0047] 此外，可使用对 Y2 350 的更新代替对 Y1320 的更新来更新过滤器。Y2 350 和 X310 间的差异比 Y1 320 和 X310 间的差异小，因为该模型的许多部分被强制不变。

[0048] 另一种技术是仅更新数据的一部分，诸如改变较快的部分，或对模型有较大影响的部分。例如，IP 地址和 URL 数据可能比文本数据改变更快（或更慢）。此外，将这些特征独立于其他特征来训练可能较简单（见例如于 2004 年 3 月 25 日提交的美国申请第 10/809,163 号，题为 Training Filters for IP Addressand URL Learning（为 IP 地址和 URL 学习训练过滤器））。因而，可构建一模型，它保持某组特征不变，而允许其他特征改变。

[0049] 此外，通过选择性地更新特征的一个子集（例如，至少一个独立于其他的特征），对该模型的未来更新可更容易地完成。此类模型的一个例子是决策树，其中每个叶节点包含一独立模型，该独立模型可与其他叶节点处的模型相分离地更新。研究发现，这些模型能和当前构建的模型有同样数量的特征，但总体上有更好的性能。

[0050] 存在其他设计先验模型的方法，使之具有在模型构建时相互之间不允许、或不被允许对权重进行平衡的特征子集，包括通过将各特征类聚成相关的组群，或通过其他机制，来任意地划分特征空间。或者，如在决策树中，例如可通过将消息类聚成相关组群来划分消息（在该情况下，如同在决策树的情况下，在不同聚类中可有具有不同权重的重复特征，但它们可被独立更新）。

[0051] 增量更新也可至少部分地通过分发客户机、服务器、或用户接收到的消息的来确定——更新的特征首先集中在那些适用于特定顾客（服务器或客户机）所收到的最多的消息的特征。因而，举例来说，多个客户机可依照它们收到的消息类型，来接收对其过滤器的

不同更新。

[0052] 一旦确定了更新的类型，管理垃圾邮件过滤器的更新可以是具有挑战性的。消息系统管理员常常或有时有兴趣知道他们的用户在使用什么软件，包括数据文件。在某些情形下，管理员甚至可能希望他们所有的用户运行同样的数据，或者在他们有机会在中意的或合意的环境中测试新数据文件之前，他们可能不希望分发这些新数据文件。因而，他们可能不希望用户直接与更新服务通信。

[0053] 例如，在一情景中，在发送特定文件给用户前，管理员宁愿先下载这些特定文件，并彻底检验它们的可操作性、与其他系统文件的冲突，等等……。因而促进一种两阶段传播是合乎需要的，其中数据或代码的更新首先被发送给管理员，然后传播给用户。在某些情形下，管理员可以已经信任过滤器供应者，并可能更喜欢无须验证的完全自动的查找程序。

[0054] 应当理解，此查找或更新服务可要求代码，以在电子邮件客户机或服务器上运行。并且，查找或更新可以调度的时间间隔执行，该时间间隔可由终端用户或管理员指定。或者，可以在某些事件发生时执行查找或更新，诸如当启动或打开消息通信程序时。当一更新可用，可通知终端用户或管理员（例如，更新是可任选的），或者更新可以是自动的。可以给予终端用户或管理员这些选项间的选择。最后，对垃圾邮件过滤器的更新可以即时发生并生效，甚至无须重新启动该消息通信程序。

[0055] 如所讨论的，对垃圾邮件过滤器的更新可以至少是增量的，其中垃圾邮件过滤器最有用或最期望部分被更新，而剩下的部分保持不变，从而将更新和与其相关联的有关数据文件的大小最小化。在大多数情况下，服务器负责确定进行哪些更新、何时进行此类更新、和／或进行此类更新的方式。不幸的是，服务器在作出此类确定时可能很迟缓，或者此类更新的定时或内容可能与客户机或用户的过滤需求略为不重合。对客户机来说，任一情况都可能有问题，尤其是当现有垃圾邮件过滤器对特定消息的分类不确定，且客户机无法承受更久的延迟来等待服务器提示的更新时。

[0056] 在图 4 中，描绘了查找服务系统 400 的示意性框图，该系统允许在垃圾邮件过滤器正被客户使用时对其进行更新。查找服务系统 400 可类似于上述图 1 中的更新系统 100，尤其是在关于生成某类更新数据，以向垃圾邮件过滤器进行几乎实时或实时的更新方面。然而，此外，查找服务系统 400 可经客户机或终端用户的请求，而不是只经由服务器指令，向垃圾邮件过滤器提供更新。

[0057] 根据该图，到来的测试消息可被传递到测试消息接收组件 410，该组件使用至少一个垃圾邮件过滤器 420 以便于将消息分类为垃圾邮件或非垃圾邮件。测试消息可帮助确定在给定当前参数组时，垃圾邮件过滤器 420 的准确度。测试消息接收组件 410 可位于第三方服务器或客户机上。垃圾邮件过滤器 420 可以是机器学习训练的或是非机器学习训练的。

[0058] 更新学习可以如下执行：到来的训练消息的至少一部分可经由训练消息接收组件（位于过滤器供应者上）435 被路由到特征分析系统 430。该特征分析系统 430 可基于从训练消息的至少一部分中提取的各特征及其相应的权重，来生成最新近的数据，并将其存储在查找数据库 440 中。

[0059] 因为垃圾邮件发送者不断改编和／或修改其垃圾邮件，可能有一部分无法由现有垃圾邮件过滤器 420 分类为垃圾邮件或好邮件的消息。客户机可标记此类消息，并随即向查找组件 450 发送一基于该消息、该消息的散列、和／或该消息的一个或多个特征的查询或

请求。

[0060] 如果来自查找数据库的任何数据满足该请求，那么此类对应信息可被发送或下载，以更新垃圾邮件过滤器 420。然后，可对不确定消息和任何新消息应用更新了的垃圾邮件过滤器，来帮助该分类过程。

[0061] 现转到图 5，示出了在线查找系统 500 的示意图，该系统便于由客户机 510 使用的基于 web 的更新服务。设想使用用“旧”数据训练的现有垃圾邮件过滤器来分类到来的消息 515。不幸的是，客户机现有的过滤器在确定某些消息是垃圾邮件还是好邮件时感到困难。客户机 510 可采取消息 515 或某个从中提取的特征，诸如 IP 地址 520、URL525、主机名 530 或任何其他特征 535，并查询在线查找系统 500，而不是隔离消息 515 或等待服务器提示更新到来。在线查找系统 500 可由一个或多个查找表 540 和 / 或一个或多个数据库 545 组成。查找表 540 可包括对每个特征的更新数据 550——诸如每个 IP 地址 555。如果客户机对消息的 IP 地址执行查询，那么可在适当的查找或更新表中查找该 IP 地址。

[0062] 类似地，对于属于 IP 地址 520 的任何更新，可以参考或搜索数据库 545。数据库 545 也可按每个更新的特征排列—诸如每个 IP 地址 520。为控制表或数据库的大小，分别在查找表和数据库中只能提供具有更新的信息的特征。然而，实质上具有所有特征或参数、而无论其权重或值是否改变的查找表和 / 或数据库也是可用的。不管表和数据库的排列如何，如果找到一更新，它可被直接发送到客户机或由其下载，以更新垃圾邮件过滤器。因而，对垃圾邮件过滤器的更新可以基于客户机偏好，且可按需发生。

[0063] 如果服务器或客户机上的消息通信系统还没有收到所有以前的更新，可能需要查找一个以上系列的特征或更新。该系统可从最后记录的查找起执行查找，然后按照顺序应用它们。可任选地，更新服务器可将多个查找文件合并在一起，来提高下载的效率。最后，更新也可通过诸如 HTTPS 等安全信道发生。

[0064] 对较新数据的增量查找可被写入文件或被存储在磁盘上，随后在存储器中组合。此外，增量更新可指明不再需要模型的某个部分、特征或参数（例如，权重为 0），因而允许将其删除，并节省存储器或磁盘空间。

[0065] 现参考图 6，示出了依照本发明一个方面的反垃圾邮件查找基于 web 服务的示例性体系结构 600。体系结构 600 包含多个层，举例来说，诸如数据层级层（或后端数据库），它容纳特征子集及在训练中生成的相关联的权重和模型；中间件层，它在数据库和垃圾邮件过滤器间传递信息；以及以预定或自动频率调用中间件层，来获取最新更新的模型并将在线模型与本地存储的模型文件合并的垃圾邮件过滤器。

[0066] 更具体地，数据层级层容纳 2 个存储：训练存储 (TrainStore) 的副本 610（用于标准训练）及更新存储 (UpdateStore)620。这些存储可以是平面文件或数据库。专用训练存储 610 可任选地仅容纳受益于频繁更新的特征子集的特征和权重。更新存储 620 是一新数据库或平面文件组，包括了由来自专用训练存储 610 的信息子集所产生的二进制形式的模型输出，以及所部署的产品关联的一些新变量。此信息子集可包括：

[0067] • 包含很大程度受益于更频繁更新的特征的新模型；

[0068] • 这些特征的例子包括 URL 特征、IP 特征及新的特别特征；

[0069] • 新概率模型对于所部署的模型文件的较早版本的的关系；和 / 或

[0070] • 用于将新模型传递大小最小化的新模型的增量更新。

[0071] 中间件层 630 可担当更新存储 620 和垃圾邮件过滤器 .d11 文件间的接口。它展现了在垃圾邮件过滤器和在线查找服务间来回传递信息的 web 服务接口和功能。它可以是 SOAP 服务、HTTP 服务、HTTPS 服务或其他因特网服务。

[0072] 当结合某些其他垃圾邮件相关系统和方法时，该反垃圾邮件查找服务尤其强大。特别地，当结合消息隔离时它可以格外强大。在消息隔离中，某些消息可被放到一垃圾邮件文件夹或一隔离文件夹，或者暂时另保存在一边。在垃圾邮件过滤器更新后它们被重新评分。诸如“报告垃圾邮件按钮”等技术也可为垃圾邮件过滤器更新产生重要数据，在该技术中用户向中央知识库报告垃圾邮件消息。此外，在诸如蜜罐等技术中，发送到某些决不应收到消息的账号（例如新近创建的未启用账号）的数据对于垃圾邮件过滤器更新来说是有价值的消息来源。此外，在反馈循环中，由用户投票决定某些消息是好消息还是垃圾邮件。这为更新垃圾邮件过滤器提供了有价值的数据。因为该数据是相对无偏见的，它可比报告垃圾邮件或蜜罐数据更有用。

[0073] 现在将经由一系列动作来描述依照本发明的各种方法，必须理解和明白，本发明不受各动作次序限制，因为依照本发明，某些动作可按不同顺序发生，和 / 或与本文示出及描述的其他动作同时发生。例如，本领域技术人员会理解并明白，方法可被替换地表示为诸如在状态图中的一系列相互关联的状态或事件。此外，并非所有示出的动作是实现依照本发明的方法所必需的。

[0074] 现参考图 7，示出了示例性垃圾邮件过滤器更新程序 700 的流程图，它便于在使用过程中至少对垃圾邮件过滤器进行几乎实时的更新。程序 700 涉及在 710 诸如通过机器学习技术，用新的或较新近的数据来训练位于新过滤器。可在多个消息特征及其相关联的权重上特殊地训练新过滤器。特征的一些例子包括任何 IP 地址、URL、主机名或可从消息中提取的任何单词或文本。

[0075] 在 720，程序 700 可查找新过滤器和旧过滤器（在旧数据上训练的）之间的差异。在 730，找到或检测到的任何差异可被存储为一个或多个单独的数据文件。

[0076] 可任选地，数据文件可存储于数据库中，和 / 或其中包括的内容可被编排到一个或多个查找表中。可经由一基于 web 的查找服务使这些数据文件对客户机可用。尽管未在图中描绘，客户机可查询该查找服务，来确定特定更新是否可用——对用其现有垃圾邮件过滤器无法分类的消息或来自消息的特征。如果更新可用，则客户机可选择下载其希望的更新，来部分地或增量地更新现有垃圾邮件过滤器。

[0077] 再参考图 7，在 740，可用一个或多个数据文件来更新旧的垃圾邮件过滤器。因而，该旧过滤器用显示足量改变的数据进行增量更新，而不是用一全新的过滤器取代旧过滤器。

[0078] 举例来说，在实践中，可以比较新旧过滤器间的参数的绝对值。可设置一改变阈值。当任一参数的绝对值改变满足该阈值，那么可将此改变保存到一更新组件或数据文件。诸如消息中参数的频率之类的其他因素可能影响在特定“改变”是否包括在更新中。更新可作为数据文件存储、可编排到查找表中、和 / 或可保存到可搜索数据库中。

[0079] 此外，更新请求可由服务器和 / 或个别客户机做出。例如，服务器管理员可检查到来的消息及其过滤，并基于各种因素确定需要特定更新，这些因素诸如，观察到关于某些消息的越来越多的用户抱怨，和 / 或隔离中的消息数量或相似度的增加。为解决这些范围的

问题，服务器可至少部分地请求增量过滤器更新。从而这些更新将应用于服务器方，随即应用于个别客户机。

[0080] 相反，客户机可直接请求，甚至访问增量更新数据。掌握特定的可疑消息，或来自可疑消息的特征，客户机可经由在线查找表或数据库查询此特定消息或来自该消息的特征是否有与其相对应的任何更新。然后相关的更新（如果有的话）可被下载到该客户机，并应用于该客户机的过滤器。服务器或其垃圾邮件过滤器不受这些更新的影响。因而，至少部分地基于其接收的特定类型的消息，客户机能定制或个人化对其垃圾邮件过滤器的更新的内容。此外，向更新或查找系统查询更新近的数据会比在整个隔离过程中从头到底地等待要来得快。此外，旧过滤器可部分地被增量更新和／或部分地由查找服务／系统更新。

[0081] 垃圾邮件过滤器可训练数以千计的参数——每个参数都有一与之相关联的值。对一个参数的小量改变可导致所有其他参数至少小量的改变。因而，某种程度上，在各参数之间有大量“差异”或改变是可能的。为将改变的数量及过滤器更新的总大小最小化，可使用图 8 中所示的示例性程序 800。程序 800 的结果是，对于过滤器的更新可集中于新旧数据间较显著且有意义的改变。

[0082] 如图中所示，可在 810 用从新或最近接收到的消息中提取的数据来训练第一过滤器（例如过滤器 K）。机器学习技术可用于这一训练。例如，在 820，至少部分地基于一次或多次试探，新过滤器 K 和旧的或现有过滤器（当前使用中的）之间的差异可被分离出来。例如，在 830，可比较特征权重，且可确定差异的绝对值。消息中改变的特征或参数的频率也可被考虑。也可使用许多其他的试探。此外，可配置一个或多个阈值，并将其与差异的绝对值进行比较。也可对每个特征确定阈值，来虑及好的和／或垃圾邮件消息中各个特征的频率或发生率。例如，可为在好或坏消息中都较少出现的特征设置较低的阈值。

[0083] 在 840，可训练第二过滤器服从以下约束：过滤器 J 和 K 之间所有小的（或不足够大到满足阈值或试探）差异可有如其在过滤器 J 中所具有的同样的值。因而，这些特定特征的权重在该第二新过滤器中可保持不变。在 850，可找到旧过滤器 J 和第二新过滤器 Q 之间的差异。满足一个或多个阈值或试探的这些差异可存储在一更新数据文件中。因为第二新过滤器 Q 中的许多特征被强制有与旧过滤器 J 中相同的值，在这两个过滤器之间较少数量的改变是显然的。因而，该过滤器更新较小。随即在 860，旧过滤器 J 可被更新。

[0084] 或者，旧过滤器数据的一部分可被更新。例如，可以仅检查并更新 IP 地址或 URL 数据——独立于任何文本相关特征。一般而言，可按顺序应用各更新，特别是在当服务器或客户机已有一段时间没有连到因特网，且目前需要多个更新的情况下。每个更新可被下载，随即按顺序应用。相反，可以分析并合并必需的更新，来减小更新的总体大小。例如，从服务器最后一次更新以来，一权重可能已经改变了若干次。最后且最近的权值可被应用，其他“中间”值可被忽略，而不是用该权值的每个改变来更新过滤器。因而，产生较小或较少的更新。

[0085] 增量更新的存储取决于特定服务器或客户机可以是灵活的。例如，更新可被存储在单独的文件总，随后与一原始（过滤器）文件合并。然而，更新文件可在使用后不久即被丢弃。因此，可维护一基础过滤器文件，然后最新近的差异可在中途确定。有时，一些特征最后以 0 权值告终。这些特征可从过滤器中删除以节省空间。

[0086] 为了给本发明的各方面提供附加环境，图 9 和接下来的讨论旨在提供关于其中可

实现本发明各方面的合适的操作环境 910 的简明、概括的描述。尽管本发明是在计算机可执行指令（诸如由一个或多个计算机或其他设备执行的程序模块）的一般上下文中描述的，然而本领域技术人员会意识到，本发明也可结合其他程序模块来实现和 / 或被实现为硬件和软件的组合。

[0087] 然而，一般而言，程序模块包括执行特定任务或实现特定数据类型的例程、程序、对象、组件、数据结构等等。操作环境 910 只是合适操作环境的一个例子，并非意图对本发明的使用范围或功能提出任何限制。其他可适用于本发明的公知的计算机系统、环境和 / 或配置包括，但不限于，个人计算机、手持或膝上设备、多处理器系统、基于微处理器的系统、可编程消费者电子设备、网络 PC、微型计算机、大型计算机、包括上述系统或设备的分布式计算环境，等等。

[0088] 参考图 9，用于实现本发明各方面的示例性环境 910 包括计算机 912。计算机 912 包括处理单元 914、系统存储器 916 及系统总线 918。系统总线 918 将包括但不限于系统存储器 916 的系统组件耦合到处理单元 914。处理单元 914 可以是任何可用的处理器。双微处理器或其他多处理器体系结构也可用作处理单元 914。

[0089] 系统总线 918 可以是若干种总线结构中的任意一种，包括存储器总线或存储器控制器、外围总线或外部总线、和 / 或使用任一各种可用总线体系结构的局部总线，这些体系结构包括但不限于，11 位总线、工业标准体系结构 (ISA)、微通道体系结构 (MCA)、扩展的 ISA(EISA)、智能驱动器电子设备 (IDE)、VESA 局部总线 (VLB)、外围部件互联 (PCI)、通用串行总线 (USB)、高级图形端口 (AGP)、个人计算机存储卡国际协会总线 (PCMCIA)、及小型计算机系统接口 (SCSI)。

[0090] 系统存储器 916 包括易失性存储器 920 和非易失性存储器 922。包含例如在启动期间在计算机 912 内部各元件间传送信息的基本例程的基本输入输出系统 (BIOS) 存储在非易失性存储器 922 中。作为示例而非限制，非易失性存储器 922 可包括只读存储器 (ROM)、可编程 ROM(PROM)、电可编程 ROM(EPROM)、电可擦除 ROM(EEPROM) 或闪存。易失性存储器 920 包括担当外部高速缓存存储器的随机存取存储器 (RAM)。作为示例而非限制，RAM 可有多种形式，诸如同步 RAM(SRAM)、动态 RAM(DRAM)、同步 DRAM(SDRAM)、双数据率 SDRAM(DDR SDRAM)、增强型 SDRAM(ESDRAM)、同步链路 DRAM(SLDRAM)、及直接存储器总线 RAM(DRRAM)。

[0091] 计算机 912 还包括可移动 / 不可移动、易失性 / 非易失性计算机存储介质。例如，图 9 示出磁盘存储 924。磁盘存储 924 包括但不限于，如磁盘驱动器、软盘驱动器、磁带驱动器、Jaz 驱动器、Zip 驱动器、LS-100 驱动器、闪存卡或记忆棒之类的设备。此外，磁盘存储 924 可单独包括存储介质或与其他存储介质组合，其他存储介质包括但不限于光盘驱动器，诸如光盘 ROM 设备 (CD-ROM)、CD 可记录驱动器 (CD-R 驱动器）、CD 可重写驱动器 (CD-RW 驱动器）或数字多功能盘 ROM 驱动器 (DVD-ROM)。为方便磁盘存储设备 924 到系统总线 918 的连接，通常使用可移动或不可移动接口，诸如接口 926。

[0092] 应当理解，图 9 描述了在用户与在合适的操作环境 910 中描述的计算机资源间担当中介的软件。此类软件包括操作系统 928。可储存在磁盘存储 924 上的操作系统 928 用于控制及分配计算机系统 912 的资源。系统应用程序 930 利用了操作系统 928 通过存储在系统存储器 916 中或磁盘存储 924 上的程序模块 932 及程序数据 934 对资源的管理。应当理解，本发明可以用各种操作系统或其组合来实现。

[0093] 用户通过输入设备 936 输入命令或信息到计算机 912 内。输入设备 936 包括，但不限于，诸如鼠标、跟踪球、触针、触摸垫等的定位设备、键盘、话筒、操纵杆、游戏垫、圆盘式卫星天线、扫描仪、电视调谐卡、数码相机、数码摄像机、网络摄像头等等。这些及其他设备经由接口端口 938，通过系统总线 918 连到处理单元 914。接口端口 938 包括例如串行端口、并行端口、游戏端口及通用串行总线 (USB)。输出设备 940 使用一些和输入设备 936 相同类型的端口。因而，例如 USB 端口可用于提供到计算机 912 的输入，及从计算机 912 输出信息到输出设备 940。提供输出适配器 942，以示意在其他输出设备 940 中有一些需要专用适配器的输出设备，如监视器、扬声器及打印机。作为示例而非限制，输出适配器 942 包括，提供输出设备 940 与系统总线 918 之间一种连接手段的显卡与声卡。应当注意，诸如远程计算机 944 等其他设备和 / 或设备系统同时提供输入与输出性能。

[0094] 计算机 912 可使用到诸如远程计算机 944 等一个或多个远程计算机的逻辑连接在联网环境中操作。远程计算机 944 可以是个人计算机、服务器、路由器、网络 PC、工作站、基于微处理器的电器、对等设备或其他普通网络节点等等，且通常包括相对于计算机 912 所描述的许多或全部元件。为简单起见，仅随远程计算机 944 示出记忆存储设备 946。远程计算机 944 通过网络接口 948 逻辑地连接到计算机 912，然后经由通信连接 950 物理连接。网络接口 948 包含诸如局域网 (LAN) 和广域网 (WAN) 等通信网络。LAN 技术包括光纤分布式数据接口 (FDDI)、铜缆分布式数据接口 (CDDI)、以太网 /IEEE1102.3、令牌环 /IEEE1102.5 等等。WAN 技术包括，但不限于，点对点链接、如综合业务数字网及其变体的电路交换网络、分组交换网络及数字用户线 (DSL)。

[0095] 通信连接 950 指用于将网络接口 948 连到总线 918 的硬件 / 软件。尽管为说明清楚，将通信连接 950 示于计算机 912 内部，但它也可位于计算机 912 外部。仅为示例性目的，连接到网络接口 948 所必需的硬件 / 软件包括内部和外部技术，诸如包括常规电话级调制解调器、电缆调制解调器及 DSL 调制解调器在内的调制解调器、ISDN 适配器及以太网卡。

[0096] 上面的描述包括本发明的示例。当然，不可能为描述本发明而描述各组件或方法的每个可想到的组合，但本领域的普通技术人员会意识到，本发明的许多其他组合与变换是可能的。因此，本发明旨在包括归入所附权利要求书的精神与范畴内的所有此类改变、修改与变体。此外，在具体实施方式或权利要求书中使用术语“包括”的意义上，此类术语意图如术语“包含”那样具有包容性，如同“包含”在用作权利要求书中的过渡词时所解释的。

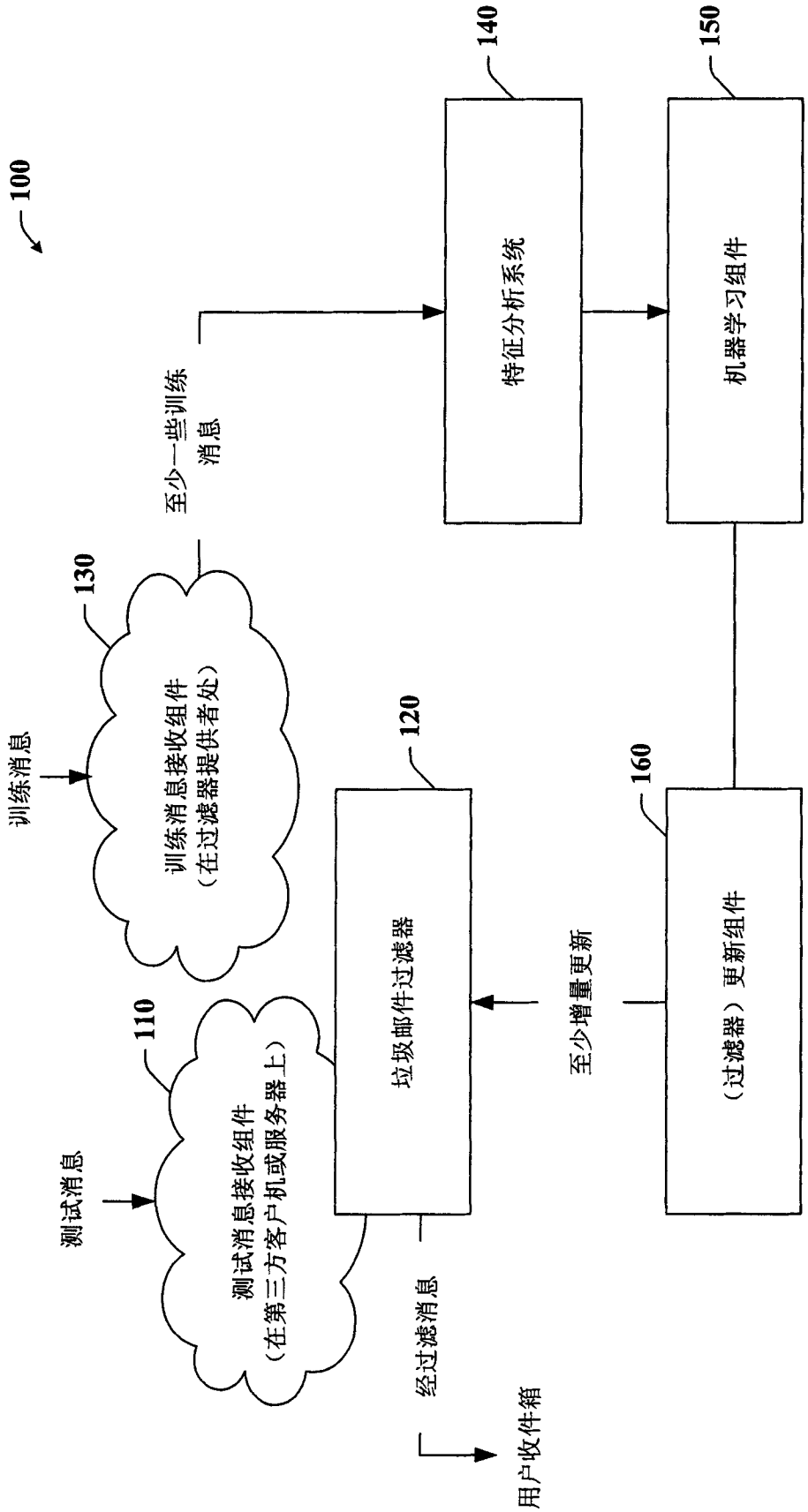

100
140
150
特征分析系统
机器学习组件
至少一些训练消息
130
训练消息接收组件（在过滤器提供者处）
训练消息
120
垃圾邮件过滤器
110
测试消息接收组件（在第三方客户机或服务器上）
测试消息
至少增量更新
160
（过滤器）更新组件
经过滤消息
用户收件箱

图 1

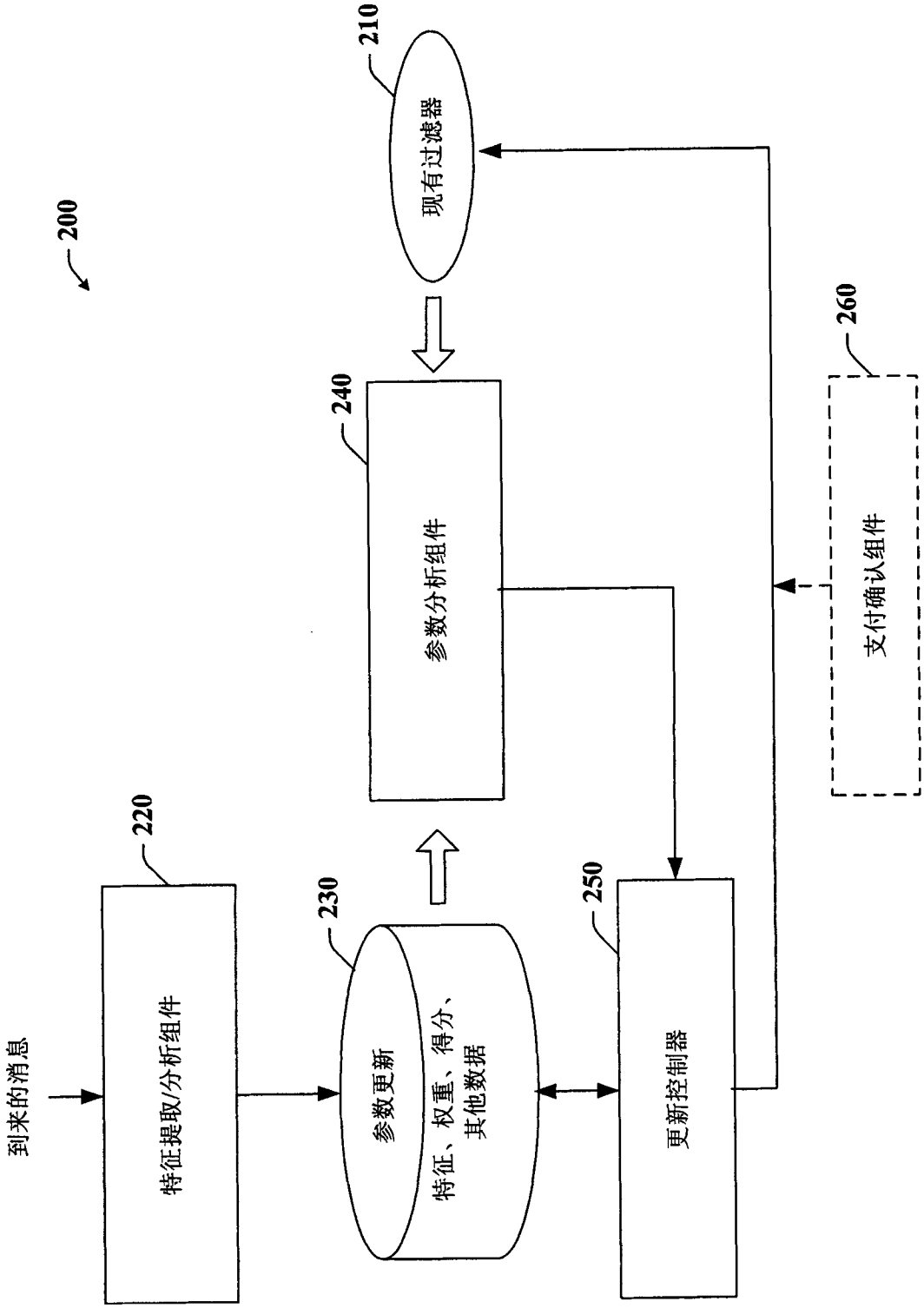

200
210
现有过滤器
240
参数分析组件
260
支付确认组件
220
特征提取/分析组件
230
参数更新
特征、权重、得分、
其他数据
250
更新控制器
到来的消息

图 2

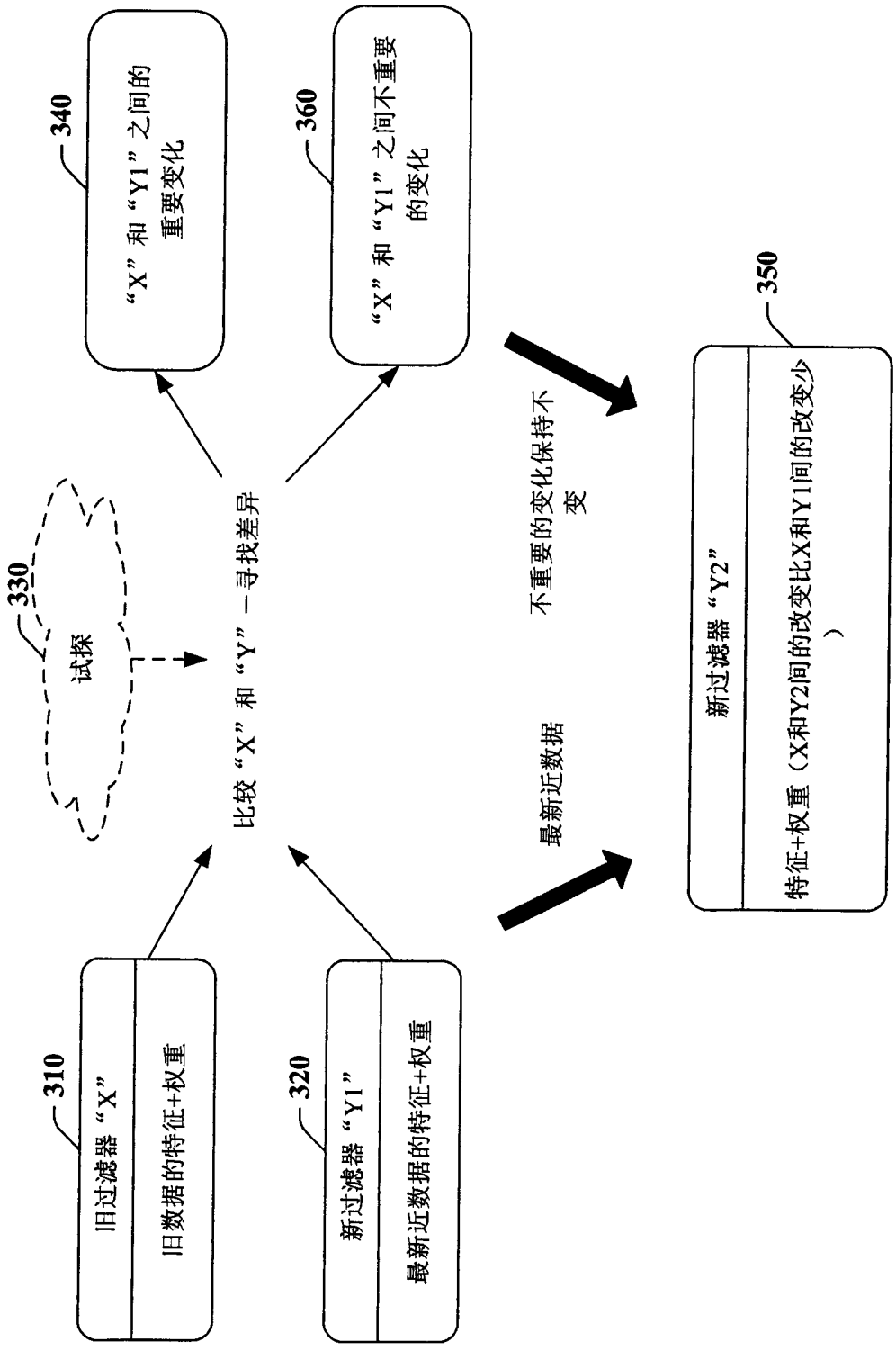

旧过滤器“X”
旧数据的特征+权重
310
新过滤器“Y1”
最新近数据的特征+权重
320
试探
330
比较“X”和“Y”－寻找差异
“X”和“Y1”之间的重要变化
340
“X”和“Y1”之间不重要的变化
360
最新近数据
不重要的变化保持不变
新过滤器“Y2”
特征+权重（X和Y2间的改变比X和Y1间的改变少）
350

图 3

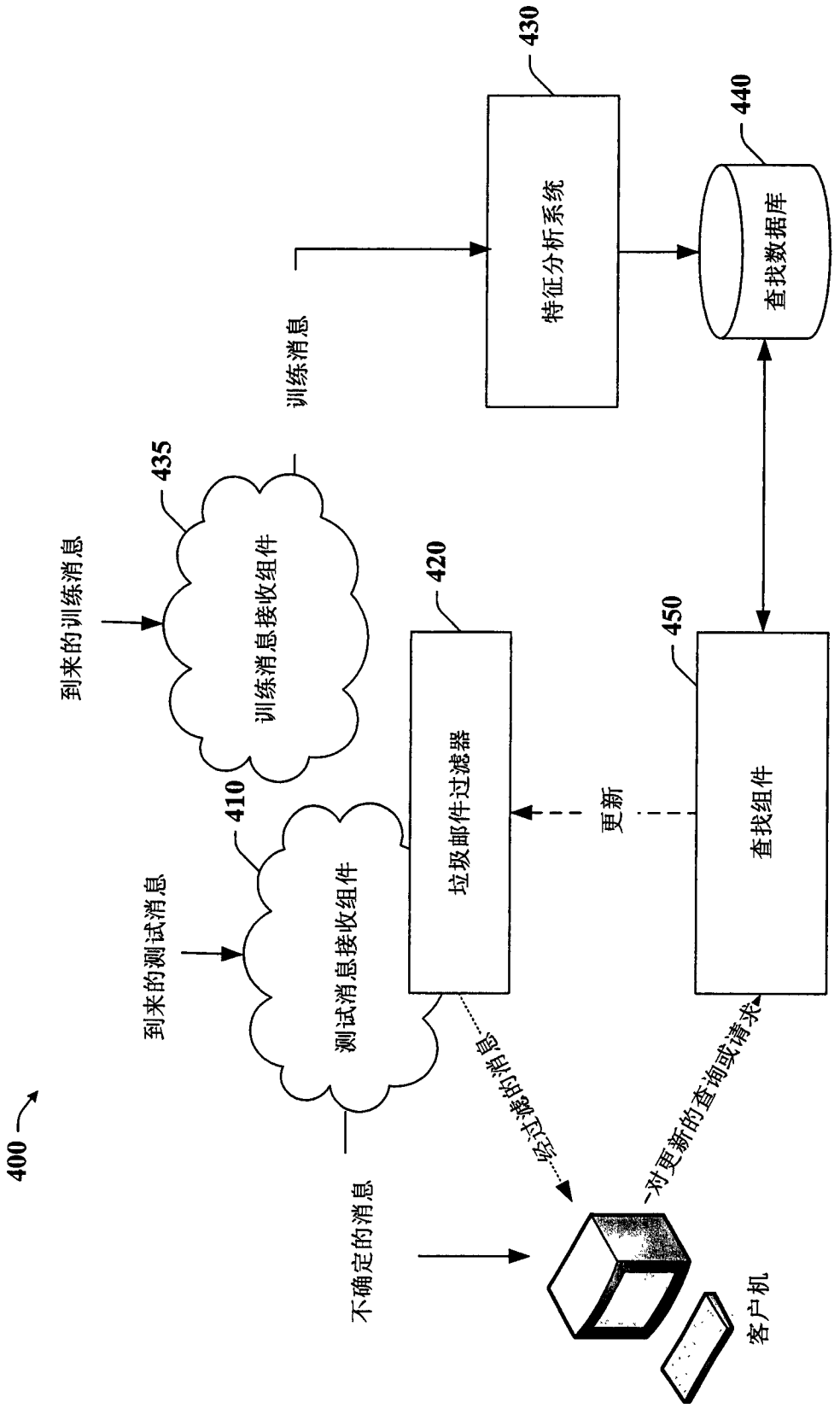

400
到来的测试消息
410
测试消息接收组件
不确定的消息
到来的训练消息
435
训练消息接收组件
训练消息
430
特征分析系统
440
查找数据库
420
垃圾邮件过滤器
更新
450
查找组件
经过滤的消息
对更新的查询或请求
客户机

图 4

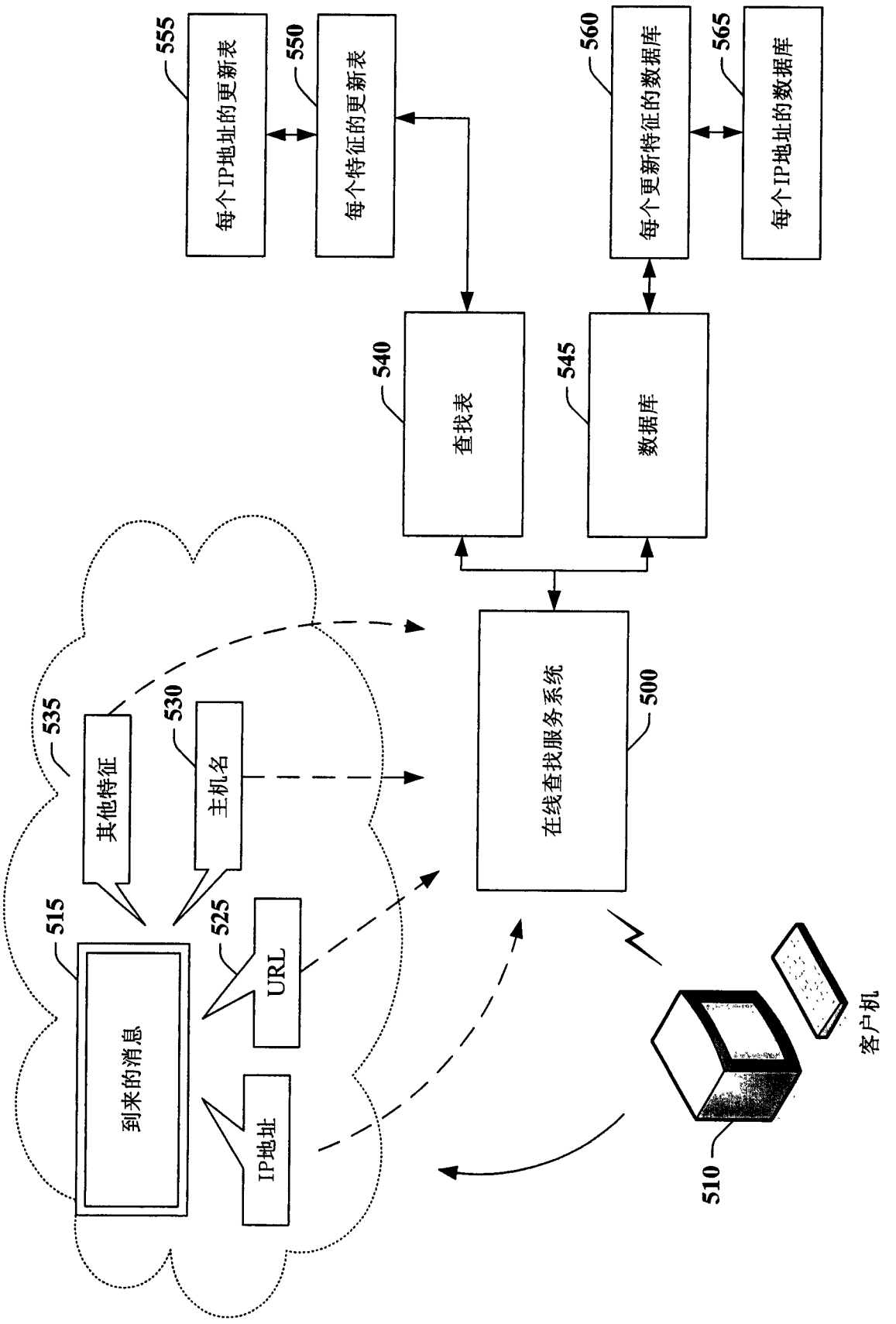

555
每个IP地址的更新表
550
每个特征的更新表
560
每个更新特征的数据库
565
每个IP地址的数据库
540
查找表
545
数据库
在线查找服务系统
500
535
其他特征
530
主机名
515
到来的消息
525
URL
IP地址
510
客户机

图 5

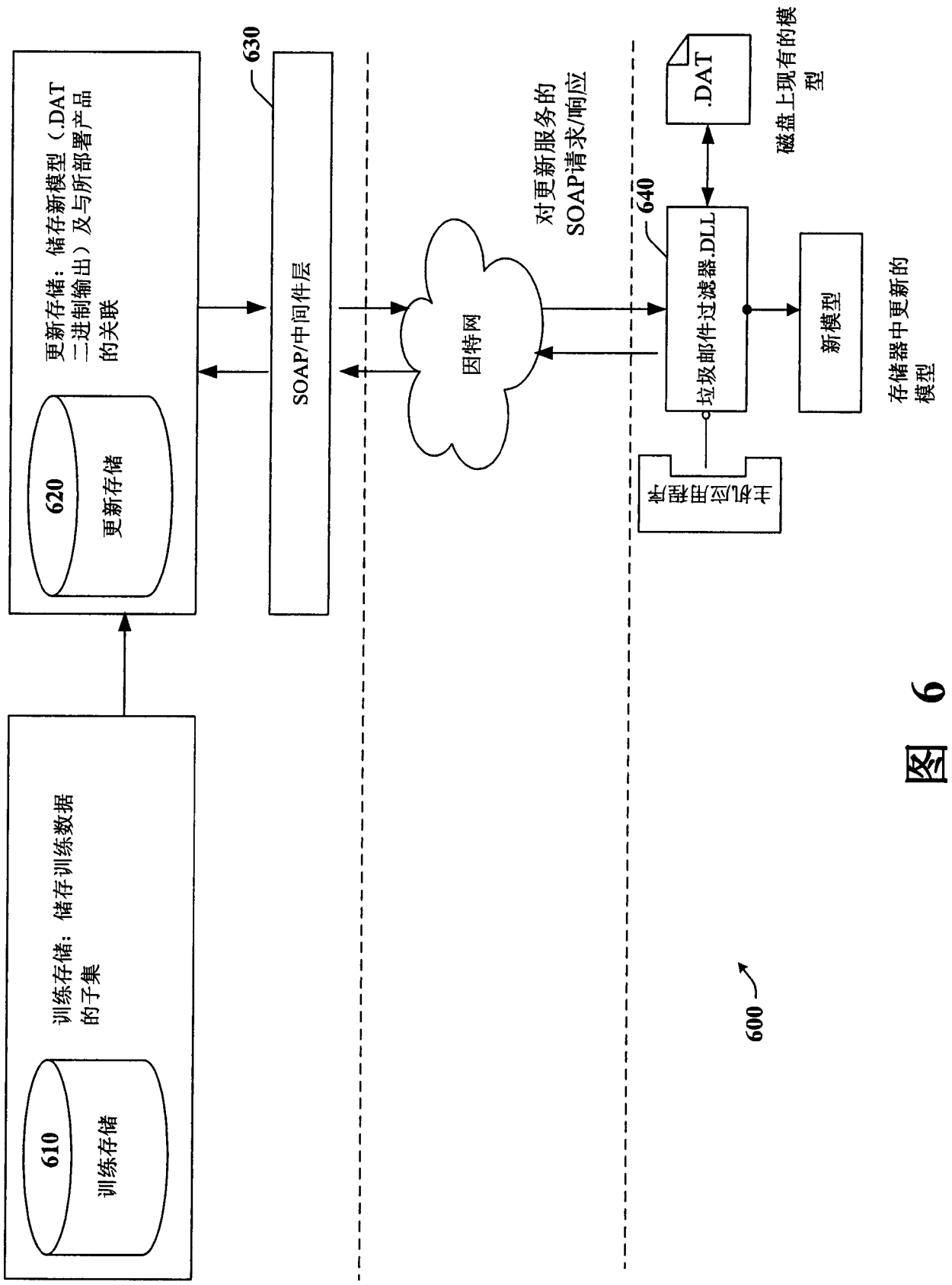

训练存储：储存训练数据的子集
610
训练存储
更新存储：储存新模型（.DAT二进制输出）及与所部署产品的关联
620
更新存储
630
SOAP/中间件层
因特网
对更新服务的SOAP请求/响应
640
垃圾邮件过滤器.DLL
主机应用程序
.DAT
磁盘上现有的模型
新模型
存储器中更新的模型
600

图 6

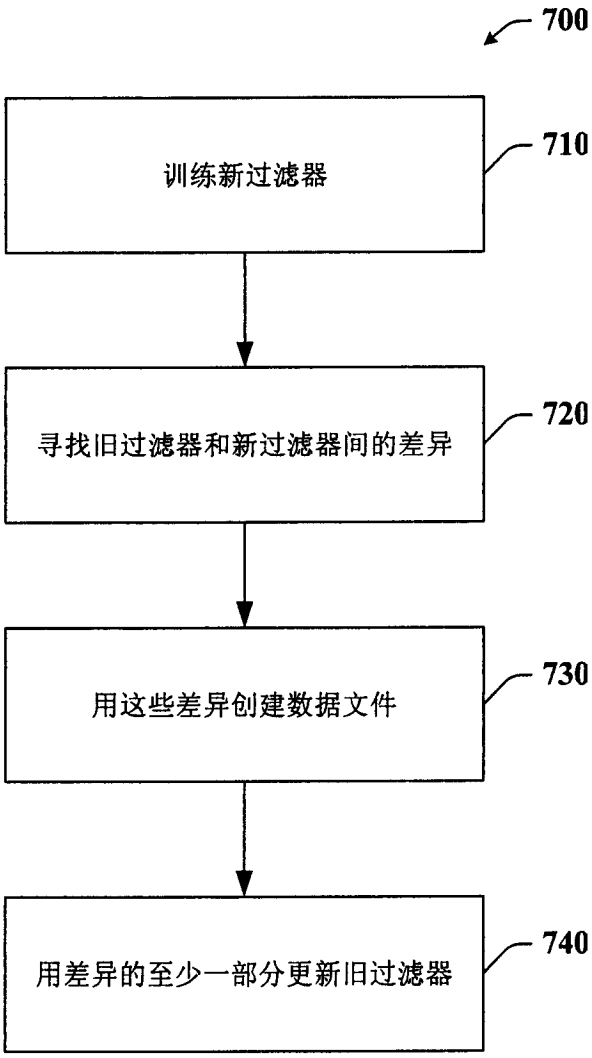

700
训练新过滤器
710
寻找旧过滤器和新过滤器间的差异
720
用这些差异创建数据文件
730
用差异的至少一部分更新旧过滤器
740

图 7

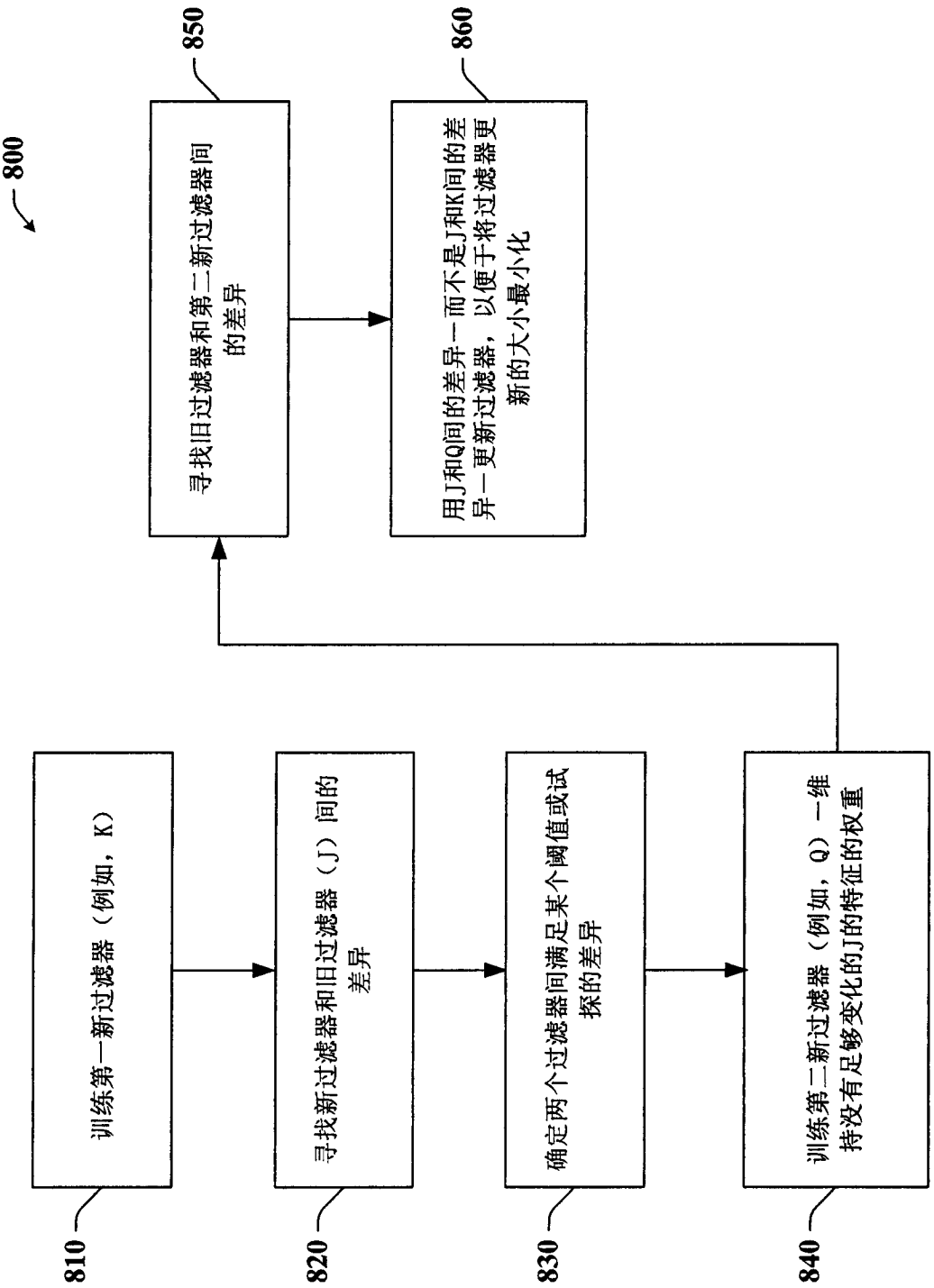

800
训练第一新过滤器（例如，K）
寻找新过滤器和旧过滤器（J）间的差异
确定两个过滤器间满足某个阈值或试探的差异
训练第二新过滤器（例如，Q）一维持没有足够变化的J的特征的权重
寻找旧过滤器和第二新过滤器间的差异
用J和Q间的差异－而不是J和K间的差异－更新过滤器，以便于将过滤器更新的大小最小化
810
820
830
840
850
860

图 8

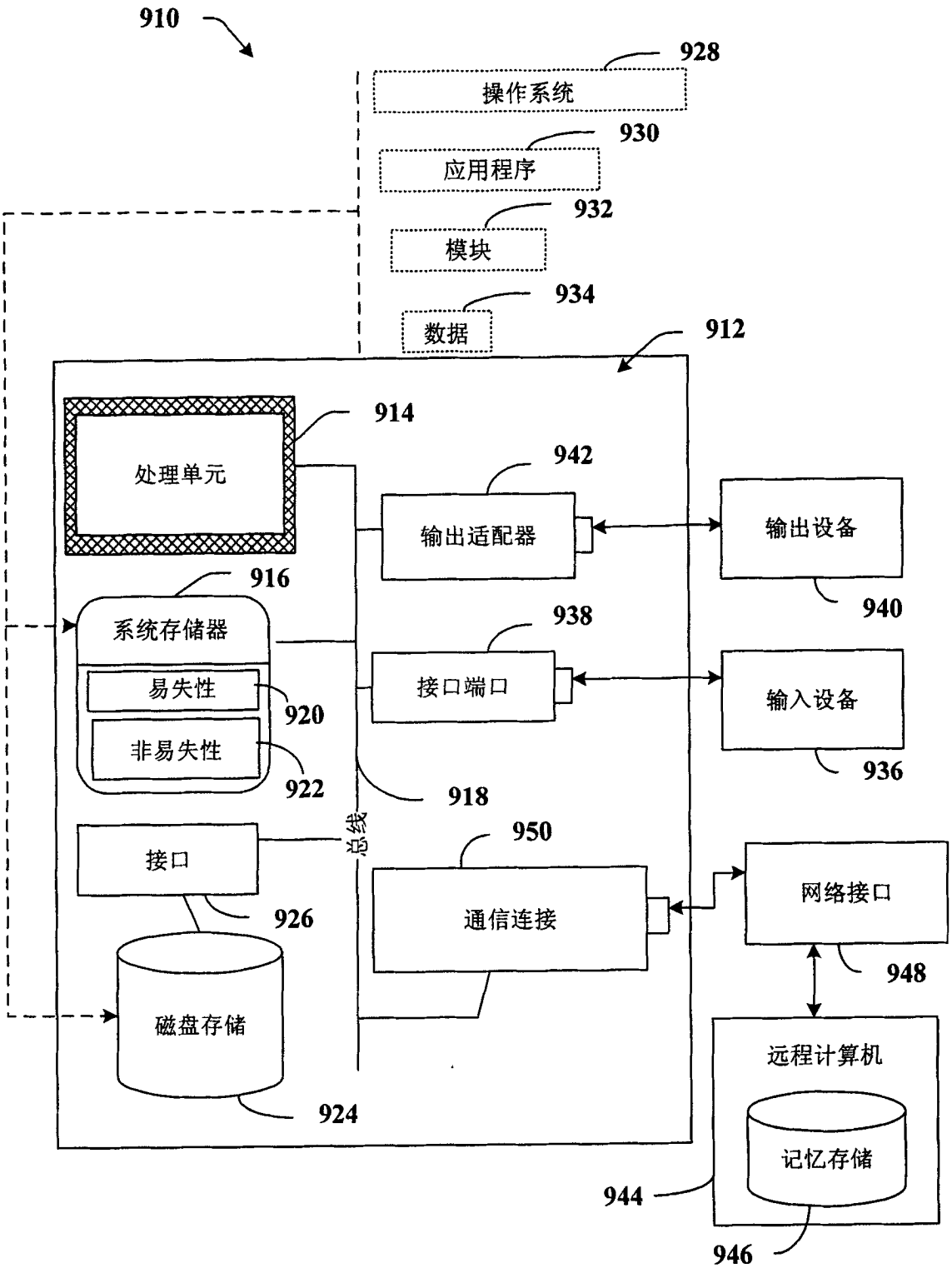

910
928
操作系统
930
应用程序
932
模块
934
数据
912
914
处理单元
942
输出适配器
输出设备
940
916
系统存储器
易失性
920
非易失性
922
938
接口端口
输入设备
936
918
总线
950
接口
926
通信连接
网络接口
948
磁盘存储
924
远程计算机
记忆存储
944
946

图 9