



[12] 发明专利申请公布说明书

[21] 申请号 200680022105.0

[43] 公开日 2008年10月15日

[11] 公开号 CN 101288093A

[22] 申请日 2006.5.19
 [21] 申请号 200680022105.0
 [30] 优先权
 [32] 2005.5.20 [33] US [31] 60/683,437
 [32] 2005.12.6 [33] US [31] 11/295,754
 [86] 国际申请 PCT/IB2006/004285 2006.5.19
 [87] 国际公布 WO2008/004027 英 2008.1.10
 [85] 进入国家阶段日期 2007.12.20
 [71] 申请人 维布兰特媒体有限公司
 地址 英国伦敦
 [72] 发明人 理查德·布林德利 托比·多伊格

[74] 专利代理机构 北京律盟知识产权代理有限公司
 代理人 刘国伟

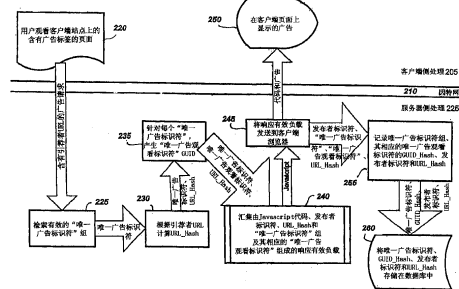
权利要求书 3 页 说明书 7 页 附图 5 页

[54] 发明名称

在线广告的防欺诈和侦查

[57] 摘要

本发明揭示一种用于侦查并防止在线广告环境中的欺诈的系统和方法。在一个实施例中，所述系统和方法包含具有网页的发布者，当用户请求所述网页时，连同所述网页将广告组和唯一请求标识符发送给用户浏览器。对于单个实例，所述唯一请求标识符是唯一的、发布者特定的、广告特定的。数据库跟踪所述唯一请求标识符，使得当用户“点击”链接以访问广告商的网站时，可对照所述数据库中的所述唯一请求标识符检查与所述广告相关联的所述唯一请求标识符，以确定所述“点击”是否为可能是非欺诈性的或有效的点击。



1. 一种跟踪与网站相关联的行为的方法，所述方法包括：

从请求者处接收对补充所述网站上的内容的信息的请求，所述请求包含唯一请求标识符和发布者标识符；

检索唯一信息标识符，对于一个实例，所述唯一信息标识符包含对于所述请求是唯一的的信息；

产生唯一请求标识符，所述唯一请求标识符包含所述唯一信息标识符；

将所述唯一请求标识符传输给所述请求者；以及

将所述唯一请求标识符和所述发布者标识符记录在数据库中。
2. 根据权利要求1所述的方法，其进一步包括将用于与在可由引荐者统一资源定位符（URL）识别的发布者的所述网站上发布的内容相关联的标签传输给所述发布者，所述标签包括可执行代码和所述发布者标识符。
3. 根据权利要求1所述的方法，其进一步包括产生可由所述请求者执行的回复代码，所述回复代码包含所述唯一请求标识符。
4. 根据权利要求1所述的方法，其中所述唯一信息标识符包括广告。
5. 根据权利要求1所述的方法，其进一步包括响应于对所述网站上的所述信息的选择，接收所述唯一资源标识符和所述唯一信息标识符。
6. 根据权利要求5所述的方法，其进一步包括验证所述唯一信息标识符。
7. 根据权利要求6所述的方法，其进一步包括以下中的一者：

响应于无效的唯一信息标识符，记录无效的唯一信息标识符和发布者标识符；以及

响应于有效的唯一标识符，记录有效的唯一信息标识符和发布者标识符。
8. 根据权利要求7所述的方法，其进一步包括响应于记录有效的唯一信息标识符，将所述请求者重新引导到第二URL。
9. 根据权利要求6所述的方法，其中所述验证的步骤包括：将所述接收到的唯一资源标识符和所述唯一信息标识符与所述记录的唯一资源标识符和所述唯一信息标识符进行比较。
10. 根据权利要求9所述的方法，其中所述验证的步骤进一步包括：确定所述接收到的唯一资源标识符和所述唯一信息标识符与所述记录的唯一资源标识符和所述唯一

- 信息标识符的所述比较是否已配对。
11. 根据权利要求 3 所述的方法，其进一步包括：响应于用户对所述广告的“点击”，从所述 web 浏览器接收所述唯一请求标识符和所述唯一广告标识符。
 12. 根据权利要求 4 所述的方法，其中将所述唯一请求标识符和所述唯一广告标识符与数据库中的所述唯一请求标识符和唯一广告标识符进行比较，以确定匹配。
 13. 一种用于跟踪与网站相关联的行为的系统，所述系统包括：
 - 接收器模块，其经配置以从请求者处接收对补充所述网站上的内容的信息的请求，所述请求包含唯一请求标识符和发布者标识符；
 - 检索模块，其经配置以检索唯一信息标识符，对于一个实例，所述唯一信息标识符包含对于所述请求是唯一的消息；
 - 产生器模块，其经配置以产生唯一请求标识符，所述唯一请求标识符包含所述唯一信息标识符；
 - 传输模块，其经配置以将所述唯一请求标识符传输给所述请求者；以及
 - 记录模块，其经配置以将所述唯一请求标识符和所述发布者标识符记录在数据库中。
 14. 根据权利要求 13 所述的系统，其中所述传输模块进一步经配置以将用于与在可由引荐者统一资源定位符（URL）识别的发布者的所述网站上发布的内容相关联的标签传输给所述发布者，所述标签包括可执行代码和所述发布者标识符。
 15. 根据权利要求 13 所述的系统，其中所述产生器模块进一步经配置以产生可由所述请求者执行的回复代码，所述回复代码包含所述唯一请求标识符。
 16. 根据权利要求 13 所述的系统，其中所述唯一信息标识符包括广告。
 17. 根据权利要求 13 所述的系统，其中所述接收器模块进一步经配置以响应于对所述网站上的所述信息的选择，接收所述唯一资源标识符和所述唯一信息标识符。
 18. 一种计算机可读存储媒体，其存储指令，所述指令在由处理器执行时执行以下方法：
 - 从请求者处接收对补充所述网站上的内容的信息的请求，所述请求包含唯一请求标识符和发布者标识符；
 - 检索唯一信息标识符，对于一个实例，所述唯一信息标识符包含对于所述请求是唯一的消息；
 - 产生唯一请求标识符，所述唯一请求标识符包含所述唯一信息标识符；
 - 将所述唯一请求标识符传输给所述请求者；以及

将所述唯一请求标识符和所述发布者标识符记录在数据库中。

19. 根据权利要求 18 所述的计算机可读存储媒体，其中所述存储的指令进一步包括当由所述处理器执行时进一步执行以下方法的指令：将用于与在可由引荐者统一资源定位符（URL）识别的发布者的所述网站上发布的内容相关联的标签传输给所述发布者，所述标签包括可执行代码和所述发布者标识符。
20. 根据权利要求 18 所述的计算机可读存储媒体，其中所述存储的指令进一步包括当由所述处理器执行时进一步执行以下方法的指令：产生可由所述请求者执行的回复代码，所述回复代码包含所述唯一请求标识符。

在线广告的反欺诈和侦查

技术领域

本发明大体上涉及在线广告领域，且更明确地说，涉及在线广告的反欺诈和/或侦查。

背景技术

已知常规的在每次点击时进行支付情形下的在线广告。常规的设置包含在网页上供应 web 内容的发布者和在网页上登广告的广告商。在这种安排中，广告商通常在网页上具有统一资源定位符（URL）链接。在终端用户浏览发布者的网页时，如果该终端用户对广告商的链接感兴趣，那么该终端用户进行点击。对于每次点击，广告商以赊帐方式向发布者支付可实时收益的某一预定金额，或在每次点击或每组点击基础上进行支付的某一其它财务安排。

这种常规的在线广告的问题在于其易于进行欺诈。欺诈的一个实例被称为竞争性欺诈。在竞争性欺诈中，竞争者（或利益与广告商相悖的其它组织）可能从网页点击中获得广告商的 URL 地址。具体来说，竞争者可能利用个人来点击网页上的其它广告商的链接，使得那些广告商中每个广告商最终都得到巨额财务帐单，但其中没有任何广告商获得相关联的销售额，这导致财务损失。

常规的在线广告的另一问题是点击欺诈。在某些广告安排中，可针对广告在每次点击的基础上向发布者付款，使得对网页上的广告商的 URL 的每次点击都为发布者带来收入。对于点击欺诈，为了使收入最大，发布者可能利用个人或技术（例如，机器人）来触发网页上的点击。同样，这导致广告商从发布者处收到巨额财务帐单，但广告商并未得到相关联的销售额，这导致财务损失。

因此，需要一种用于侦查并防止在线广告环境中的欺诈以允许广告商和发布者跟踪欺诈情形并采取适当补救措施的系统和方法。

发明内容

本发明包含一种用于侦查并防止在线广告的欺诈的系统（和方法）。在一个实施例中，所述系统跟踪与网站相关联的行为。所述系统从请求者处接收对补充网站上的内容的信息的请求。所述请求包含唯一请求标识符和发布者标识符。所述系统检索唯一信息标识符。对于一个实例，所述唯一信息标识符包含对于请求是唯一的的信息。所述系统产生唯

一请求标识符。所述唯一请求标识符包含所述唯一信息标识符。所述系统将所述唯一请求标识符传输给所述请求者，并在数据库中记录所述唯一请求标识符和所述发布者标识符以用于随后比较。

随后，当请求者在所述网站上时，在所述请求者选择已传输给所述请求者的信息时，系统接收唯一资源标识符和所述唯一信息标识符。一旦从所述请求者处接收到此信息，所述系统便验证所述唯一信息标识符，并将其记录为有效或无效。确切地说，所述系统将接收到的唯一资源标识符和唯一信息标识符与记录的唯一资源标识符和唯一信息标识符进行比较，以确定它们先前是否配对。如果它们先前已配对，那么所述请求无效，且如果它们先前未配对，那么所述请求有效。如果所述唯一信息标识符被记录为无效，那么将响应发送回到请求者以如此指示。如果其被记录为有效，那么所述系统响应于记录有效的唯一信息标识符而将请求者重新引导到第二 URL。

本发明的优点包含，以包含信息的标识符和与所述信息相关联的网站的 URL 的方式提供额外信息（例如，广告），使得当选择所述信息时，其可与所存储的标识符数据配对（匹配），以确实所述选择是否“有效”。因此，所述信息对于将受益于此类数据的应用（例如，广告提供商或与网站上的内容相关联的购买者）来说是可核实的，或可审核的。此类数据接着将用于识别网站上的点击是否为由（例如）点击获得机制的行为而引起的欺诈。

本说明书中所描述的特征和优点并不是全都包含的，且确切地说，根据图式、说明书和权利要求书，所属领域的普通技术人员将明白许多额外的特征和优点。另外，应注意，本说明书中所使用的语言主要是出于可读性和指导目的而选择的，且可能不是经选择以描述或限制发明性主旨。

附图说明

本发明具有其它优点和特征，通过结合附图阅读以下对本发明的详细描述和所附权利要求书，将更容易了解所述其它优点和特征，附图中：

图 1a 说明防欺诈和侦查系统的产生操作结构的一个实施例。

图 1b 说明广告产生和核对系统的一个实施例。

图 2 说明用于广告产生的客户端-服务器交互的一个实施例。

图 3 说明如所揭示的配置的广告呈现的一个实施例。

图 4 说明如所揭示的配置的点击核对的一个实施例。

具体实施方式

图和以下描述仅以说明的方式涉及优选实施例。应注意，根据以下论述，可容易将本文所揭示的结构和方法的替代性实施例视为在不脱离所主张的本发明的原理的情况下可采用的可行的替代方案。

现在将详细参考若干实施例，在附图中说明所述实施例的实例。应注意，无论何处可实行的类似或相同参考标号可用于图中，且可指示类似或相同功能性。所述图仅出于说明目的来描绘实施例。所属领域的技术人员根据以下描述将易于认识到，在不脱离本文所描述的的原理的情况下，可采用本文所说明的结构和方法的替代性实施例。

为易于论述，在以下情形下描述系统（或方法）的实施例：产生广告以用于放置在网页上，且随后对所述产生的广告进行选择 and 核对，以确定此类选择是有效还是无效的选择。应注意，本文所揭示的原理还可适用于其它配置，所述其它配置产生信息的特定实例，转发所述信息，允许对所述信息进行选择，且通过核对过程验证所述信息。

现在参看图 1a，其说明防欺诈和侦查系统的一般操作结构的一个实施例。所述结构包含广告商 110、发布者 120 和欺诈监控器 130。广告商 110 经配置以购买网页（或网站）上的广告点击。通常，发布者 120 基于“每次点击”或每组点击向广告商 110 出售点击广告。发布者 120 记录网页上的每个点击（或选择）或每组点击（选择），以因其向广告商 110 收费。

在一个实施例中，发布者 120 是因特网上的主机或 web 服务器。在此类实施例中，发布者 120 允许客户端计算系统（客户端系统、计算机和/或站点）通过客户端系统上的浏览器（例如，Microsoft® Internet Explorer 或 Mozilla Firefox）访问内容。随后，客户端系统处的用户可通过“点击”广告商 110 在发布者网页上的广告中的一者或一者以上而选择所述广告。然而，广告商 110 在发布者的网页上的广告可能被偶然地或恶意地反复连续地选择。另外，计算机构（例如，“机器人”）可能经配置以连续地选择所述广告。在此类实例中，广告商 110 为对广告的每次选择而支付费用。因此，为了抵制这种行为，在系统和过程的实施例中配置欺诈监控器 120 以侦查、报告且/或防止欺诈。

欺诈监控器 130 经配置以监控和报告点击行为。此外，欺诈监控器 130 可经配置以产生广告组，其允许随后进行核对，以用于在选择所述组中的任一广告时进行监控（或审核）。在一个实施例中，可如本文所述对广告的选择进行核对，所述选择被视为有效；否则就将其视为无效。因此，在一个实施例中，欺诈监控器 130 可配置为广告产生和核对系统。

图 1b 说明根据本发明的广告产生和核对系统的一个实施例。广告产生和核对系统可

配置为客户端服务器处理配置的主机（或服务器）侧的 web 服务器。web 服务器可以是经配置以提供处理能力的一个或一个以上物理和/或逻辑计算机器（包含处理器、存储器、存储装置、操作系统、用于执行的软件等）的配置。

广告产生和核对系统包含广告标识符引擎 140、广告数据库 145、请求标识符引擎 150、代码（产生）引擎 155、记录引擎 160、所产生记录的数据库 165、验证引擎 170、验证记录数据库 175 和命令引擎 180。这些组件通过数据总线 190 以通信方式耦合在一起。应注意，数据总线 190 可以是有线或无线的，且通信耦合可以是直接（例如，物理的）或间接的（例如，逻辑的）。参考图 2 到图 4 进一步描述组件的操作。

转到图 2，其说明根据本发明用于广告产生的客户端-服务器交互的一个实施例。过程配置包含客户端侧处理 205 和服务器侧处理 225，其通过通信媒介（例如，因特网 210 或内联网）以通信方式耦合。在一个实施例中，客户端侧处理 205 包含执行 web 浏览器的客户端系统，且服务器侧处理 225 包含经配置以执行下文进一步描述的过程的一个或一个以上 web 服务器。

所说明的过程开始于用户观看 220 客户端系统（例如，客户端计算机上的浏览器）上的网页。网页中有经嵌入的广告链接。所述过程继续从客户端系统接收请求（例如，在网页显示于浏览器中时用户点击链接），以提供嵌入的广告链接以及网页的统一资源定位符（URL）（引荐者 URL）。具体来说，在一个实施例中，客户端系统将发布者 120 的标识或发布者标识符转发给 web 服务器，识别将要向其中提供广告链接的发布者 120 网页（或网站）。

当 web 服务器接收到请求时，其通过广告标识符引擎 140 确定返回来自广告数据库 145 的哪组广告以用于显示。所述组广告可以是一个广告，或两个或两个以上广告。每个广告具有也从广告数据库 145 中检索 225 的唯一广告标识符。

过程继续计算 230 引荐者 URL 的“URL_hash”。作为实例，引荐者 URL 是终端用户键入浏览器以试图访问所述 URL 地址处的网页的 URL。所计算 230 的 URL_hash 是向其中提供广告链接的网页的引荐者 URL 的单向散列。另外，对于每个广告来说，过程产生 235 唯一广告观看标识符。在一个实施例中，所述唯一广告观看标识符是全球唯一标识符（GUID），其可为针对每个唯一网页和每个唯一广告标识符而产生的唯一的伪随机数。配对的唯一广告标识符和唯一广告观看标识符提供一个提供特定广告的单例的指纹，稍后对其进行核对 420。

过程继续进行，代码引擎 155 汇集 240 客户端系统的响应有效负载。响应有效负载

包括可执行代码，例如 Javascript，其包含发布者标识符、URL_hash、唯一广告标识符和相应的唯一广告观看标识符的散列。唯一广告观看标识符的散列还可被称作 GUID_hash。一旦经汇集，web 服务器便将响应有效负载发送 245 到客户端系统。

客户端系统接收可执行代码（其含有发布者标识符、URL_hash 和唯一广告标识符组与相应的唯一广告观看标识符对），连同将要显示的内容和链接格式，以及指向点击处置页面的 URL，并在浏览器中的网页上显示 250 其中的适当的广告。当用户选择链接（如本文进一步描述）时，客户端系统上的浏览器可执行可执行代码，将浏览器重新引导到指向点击处理页面的 URL。

应注意，在一个实施例中，过程将发布者标识符、URL_hash、唯一广告标识符和相应的唯一广告观看标识符的散列写入到数据库（例如，有效链接表）。记录引擎 160 记录 255 此数据以用于存储 260 在所产生记录的数据库 165 中，以用于稍后访问。另外，应注意，有效链接表被周期性地复制到后端统计服务器。

转向图 3，其说明根据本发明的广告交互的一个实施例。首先参看客户端侧处理 205，结合从服务器侧处理 225 接收到的可执行代码来执行过程。具体来说，过程显示链接，且确立鼠标经过 310（例如，OnMouseOver），且点击（例如，OnClick）每个链接上的事件陷阱（event trap）。鼠标经过 310 包含将指向装置（例如，鼠标、跟踪球、计算笔等）的光标移动到浏览器中的链接（例如，广告链接）上。

如果指针经过事件启动（或触发），那么所述过程通过借助状态旗标将链接设置为活动并且可点击，而启用 320 对对应于唯一广告标识符的点击。当用户“点击”（选择或触发）315 浏览器中的广告链接时，过程确定 325 是否已启用所述点击（即，已作出选择）。具体来说，如果点击事件启动（或触发），那么过程便进行检查以确定是否已启动指针经过事件。如果未启用点击，那么过程忽略 330 所述点击，并且不作出任何动作。

如果点击事件启动且已启动指针经过事件，那么过程产生目的地 URL（含有 web 服务器上的点击处置页面的目的地 URL）和查询字符串（含有唯一广告标识符、唯一广告观看标识符、发布者标识符、URL_hash）。在一个实施例中，过程打开 335 目标为目的地 URL 的浏览器的新实例（窗口或标签）。在一个实施例中，用户可观察到浏览器的这个开始于空白屏幕的新实例。将唯一广告标识符、唯一广告观看标识符、发布者标识符、URL_hash 从浏览器发送到服务器侧处理 225 上的 web 服务器。

在服务器侧处理 225 上，web 服务器从客户端侧处理 205 接收带有信息的页面调用。web 服务器中的验证引擎 170 在其有效广告列表中查找唯一广告标识符，以确定 340 广

告是否有效，且检索有效的广告目的地 URL。过程通过确定所述唯一广告商标标识符是否有效来确定所述广告是否有效。在一个实施例中，它们是一对一链接的。如果唯一广告商标标识符无效，那么过程记录 345 无效的唯一广告标识符、发布者标识符和 URL_hash 以供存储在验证记录数据库 175 中。命令引擎 180 接着将窗口（标签）关闭命令发送 350 到客户端系统上的浏览器。这关闭 360 客户端系统上的浏览器窗口。

如果广告有效，那么验证引擎 170 将有效的唯一广告标识符、唯一广告观看标识符的散列（GUID_hash）、发布者标识符和引荐者 URL 的散列（URL_hash）记录 365 在验证记录数据库 175 中。应注意，验证记录数据库 175 可经配置以充当后端统计数据库。命令引擎 180 接着将命令发送 370 到客户端系统上的浏览器，以将浏览器重新引导 375 到目标 URL，所述目标 URL 为有效的广告目的地 URL。

在一个实施例中，过程将有效的唯一广告标识符记录 365 为“点击令牌”，其对应于发布者标识符、唯一广告标识符、唯一广告观看标识符的散列（GUID_hash）和引荐者 URL 的散列（URL_hash）。“点击令牌”的表被周期性地复制到验证记录数据库 175（例如，后端统计数据库）。

验证唯一广告标识符的过程包含核对过程，其将从客户端系统上的浏览器接收到的数据与服务器侧系统上的产生记录数据库 165 中先前存储的数据进行比较。图 4 说明根据本发明的点击核对过程的一个实施例。

首先，针对来自经整理的点击记录文件的每个“点击”（或选择或触发）415，处理 410 一组唯一广告标识符、发布者标识符、GUID_hash 和 URL_hash。在一个实施例中，处理包含在“针对每一者”的循环中的 415 到 445 中的步骤。在例如图 2 所示的记录数据库中记录信息。另外，过程获得对有效的唯一广告标识符、发布者标识符、GUID_hash 和 URL_hash 的验证记录数据库 175 的访问 425。确切地说，验证记录数据库 175 提供后端统计数据库，所述后端统计数据库维持在预定义的滚动时期内发出的所有有效的唯一广告标识符和 GUID_hash 对的列表，所述有效的唯一广告标识符和 GUID_hash 对是从来自 web 服务器的产生记录数据库 165 的有效链接表导出的。

通过参看验证记录数据库 175 中的条目，过程确定 420 唯一广告标识符和 GUID_hash 是否与验证记录数据库 175 中的条目（例如，“指纹”）匹配 420。在一个实施例中，检查来自验证记录数据库的“点击令牌”以确定其是否对应于产生记录数据库中的有效的唯一广告标识符和 GUID_hash 条目。

如果在条目对之间没有匹配，那么过程将无效的唯一广告标识符、发布者标识符和

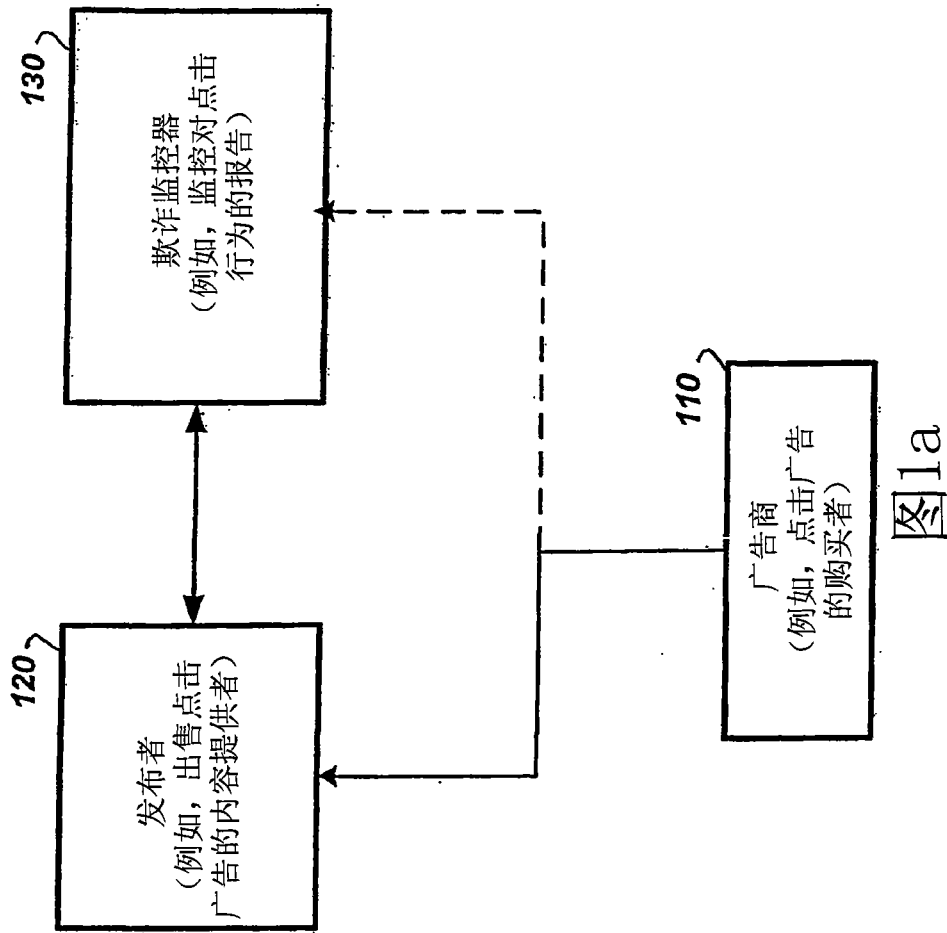
URL_hash 点击信息记录 430 到数据库中。所述数据可经组织以通过报告功能进行传播。如果存在匹配，即，两个条目适当配对，那么过程确定 435 是否已对所述对计数。举例来说，过程确定是否已提供与和所述对相关广告相关的链接。

如果唯一广告标识符和 GUID_hash 对是有效的（即，其匹配），且先前尚未提供所述链接，那么过程（例如，通过统计服务器）从相对于发布者标识符的收入报告的角度，将激活记录（或计数）445 为有效点击。如果唯一广告标识符和 GUID_hash 对无效，或先前已提供此链接，那么过程将信息（包含发布者标识符、点击详情，和无效点击的时间和日期戳）记录 440 到数据库（例如，无效点击表）中。

过程在预定时间（例如周期性的）基础上监控无效点击数据库（或表），以基于预定义的阈值对无效点击的发生作出响应。基于管理预定义的阈值的规则（例如，预定义的用户定义的系统），过程执行与所述规则相关联的预定义的动作。举例来说，所述规则可经组织，使得当超过预定义的阈值时，将警告通信传输到监控事务的机器。

本发明的优点包含，以包含信息的标识符和与所述信息相关联的网站的 URL 的方式提供额外的信息（例如，广告），使得当选择所述信息时，其可与所存储的标识符数据配对（匹配），以确实所述选择是否“有效”。因此，所述信息对于将受益于此类数据的应用（例如，广告提供商或与网站上的内容相关联的购买者）来说是可核实的，或可审核的。此类数据接着将用于识别网站上的点击是否为由（例如）点击获得机制的行为而引起的欺诈。

通过阅读本揭示内容，所属领域的技术人员将了解用于通过本发明所揭示的原理侦查并防止在线广告的欺诈的系统及其过程以及方法的额外的替代性结构和功能设计。因此，虽然已说明并描述本发明的特定实施例和应用，但应了解，本发明不限于本文所揭示的精确构造和组件，且在不脱离所附权利要求书中所界定的本发明的精神和范围的情况下，可在本文所揭示的本发明的方法和设备的安排、操作和细节中作出所属领域的技术人员将明白的各种修改、改变和变化。



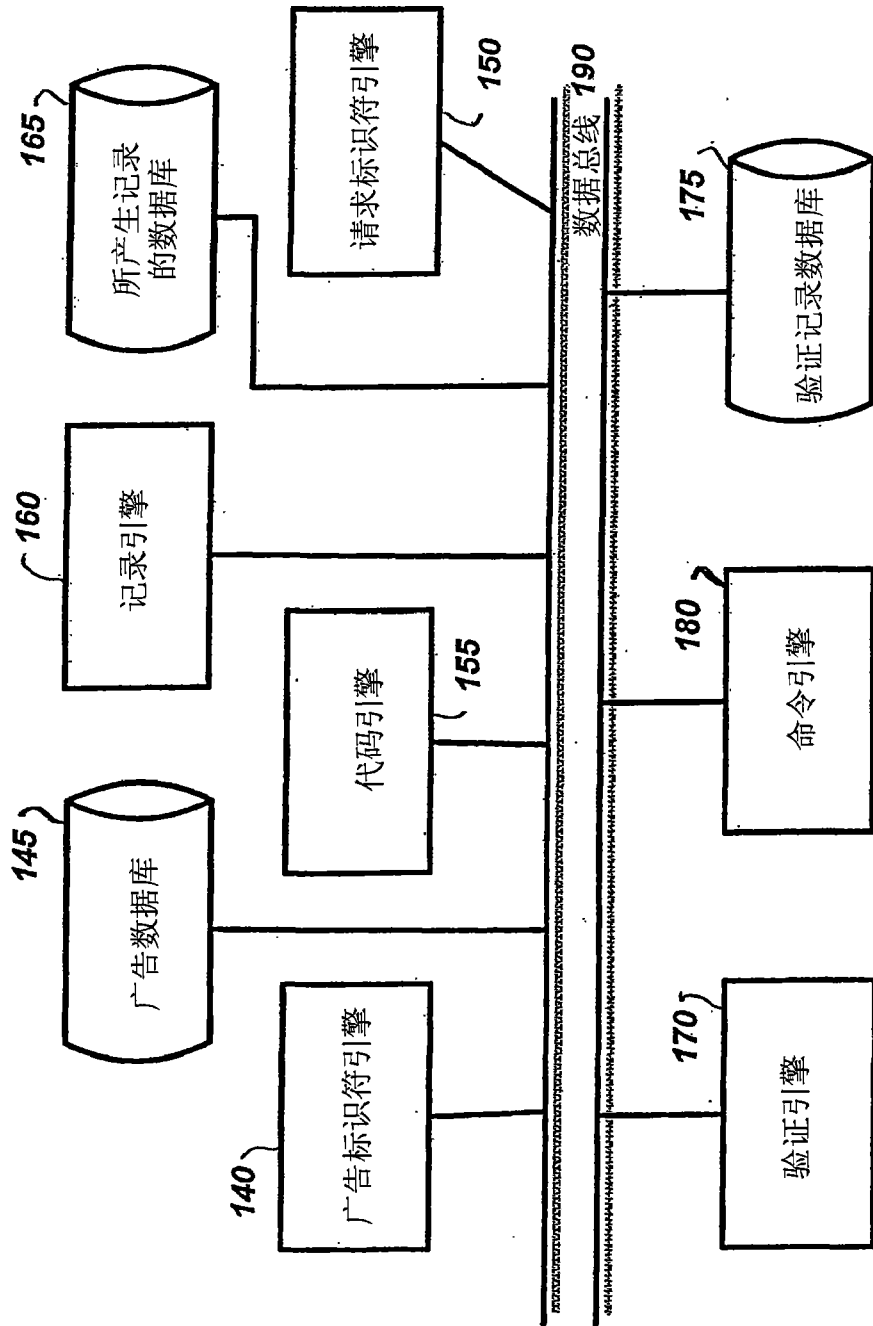
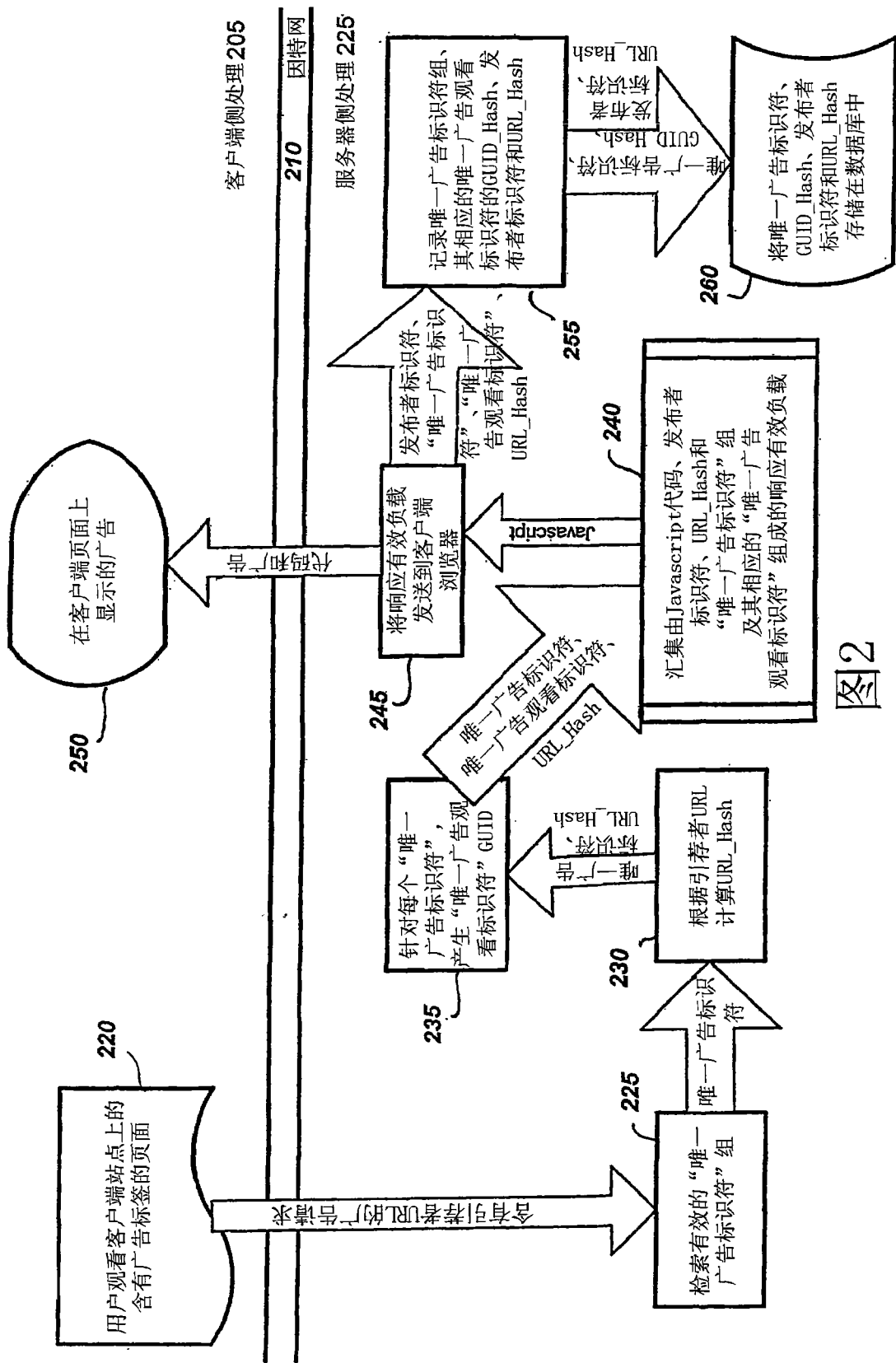


图1b



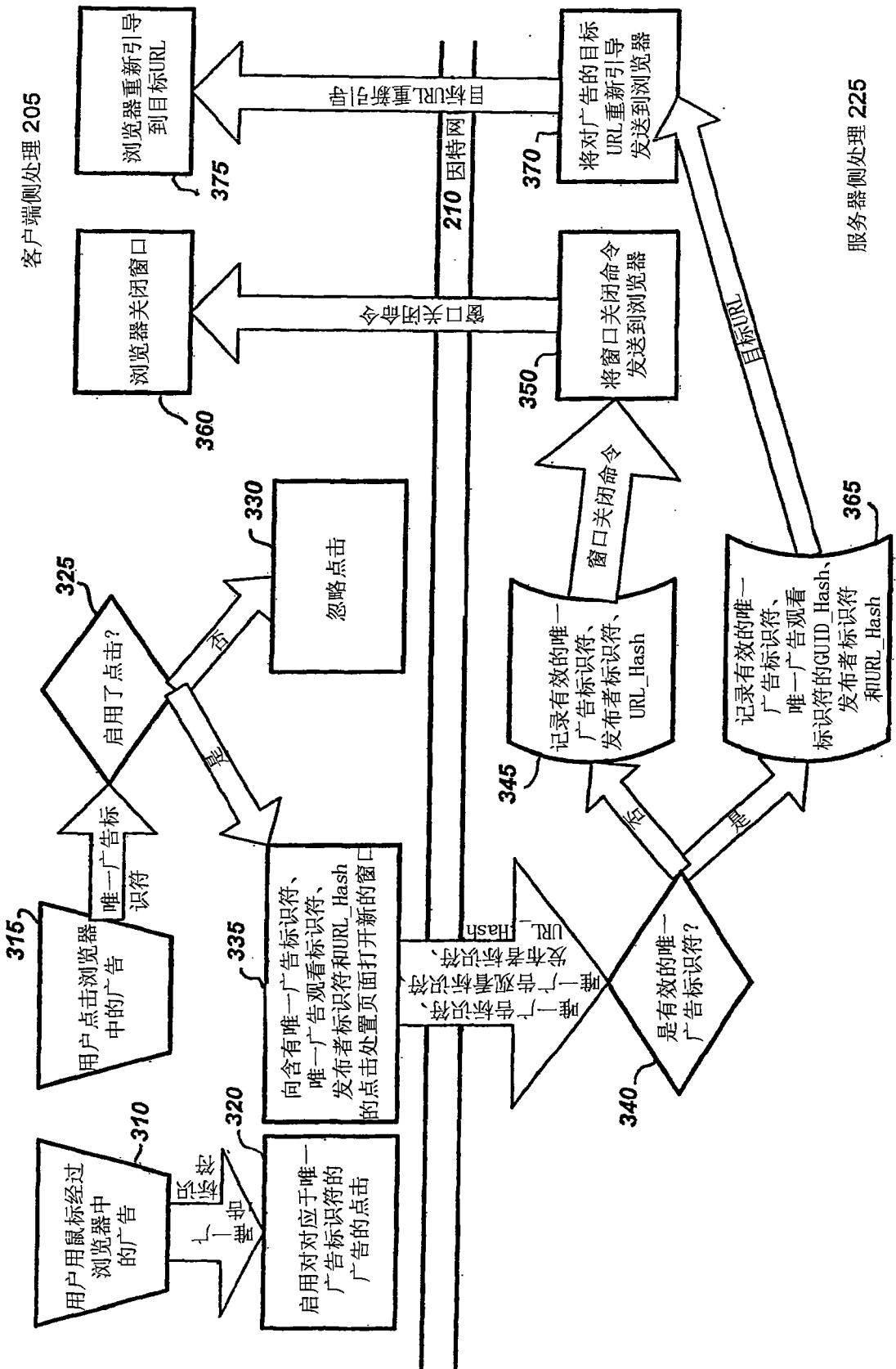


图3

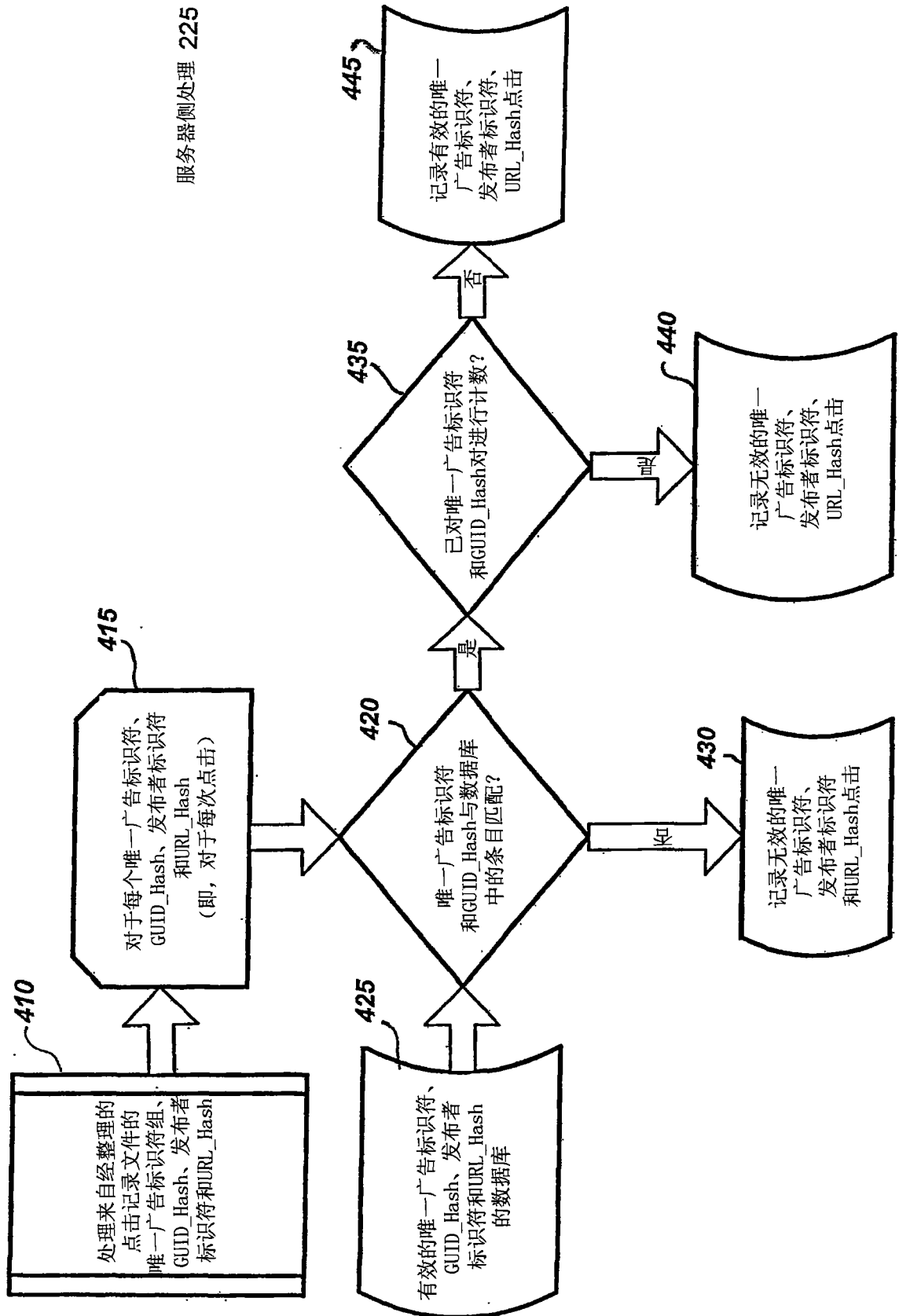


图4