(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 5 月 18 日 (18.05.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/080166 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/083015

(22) 国际申请日: 2016 年 5 月 23 日 (23.05.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510781811.4 2015 年 11 月 13 日 (13.11.2015) CN

(71) 申请人: **乐视控股（北京）有限公司 (LE HOLDINGS (BEIJING) CO., LTD.)** [CN/CN]; 中国北京市朝阳区姚家园路 105 号 3 号楼 10 层 1102, Beijing 100025 (CN)。 **乐视云计算有限公司 (LECLOUD COMPUTING CO., LTD.)** [CN/CN]; 中国北京市海淀区中关村南大街 5 号 1 区 689 号楼 1153, Beijing 100081 (CN)。

(72) 发明人: **李洪福 (LI, Hongfu)**; 中国北京市海淀区中关村南大街 5 号 1 区 689 号楼 1153, Beijing 100081 (CN)。 **胡东旭 (HU, Dongxu)**; 中国北京市海淀区中关村南大街 5 号 1 区 689 号楼 1153, Beijing 100081 (CN)。 **李茗 (LI, Ming)**; 中国北京市海淀区中关村南大街 5 号 1 区 689 号楼 1153, Beijing 100081 (CN)。

(74) 代理人: **北京商专永信知识产权代理事务所（普通合伙） (SBZL IP LAW OFFICE)**; 中国北京市海淀区知春路 1 号 9 层 901 室, Beijing 100083 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ,

[见续页]

(54) **Title**: ANTI-HOTLINKING METHOD AND SYSTEM

(54) **发明名称** : 防盗链方法及系统

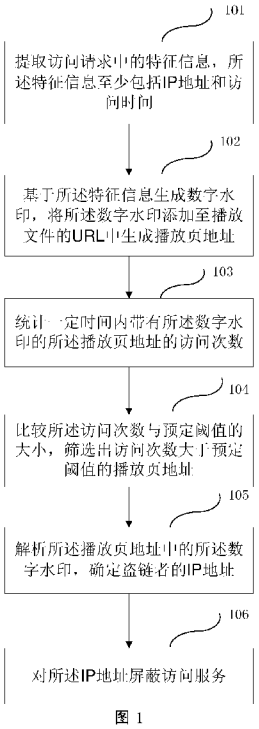


图 1

101 Extract characteristic information from an access request, the characteristic information comprising at least an IP address and time of access

102 Generate a digital watermark based on said characteristic information, and add said digital watermark to the file playback URL to generate a playback page address

103 Count the number of times the playback page address bearing said digital watermark is accessed in a given time period

104 Compare the number of times the playback address was accessed to a preset threshold, and screen out playback page addresses whose number of times accessed exceeds the preset threshold

105 Parse the digital watermark in the playback page address to determine the IP address of the hotlinker

106 Block access to services from said IP address

(57) **Abstract**: The present invention provides an anti-hotlinking method, comprising: extracting characteristic information from an access request, the characteristic information comprising at least an IP address and time of access; generating a digital watermark based on said characteristic information, and adding said digital watermark to the file playback URL to generate a playback page address; counting the number of times the playback page address bearing said digital watermark is accessed in a given time period; comparing the number of times the playback address was accessed to a preset threshold, and screening out playback page addresses whose number of times accessed exceeds the preset threshold; parsing the digital watermark in the playback page address to determine the IP address of the hotlinker; blocking access to services from said IP address. Also provided is an anti-hotlinking system, thereby making possible realization of more complete hotlinking prevention, increasing anti-hotlinking accuracy.

(57) **摘要**: 本发明提供一种防盗链方法，包括：提取访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；统计一定时间内带有所述数字水印的所述播放页地址的访问次数；比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；对所述 IP 地址屏蔽访问服务。本发明还提供了一种防盗链系统，从而能够实现更加彻底的防盗链，提高防盗链的精确度。

WO 2017/080166 A1

BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权要求在先申请的优先权(细则 4.17(iii))

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

防盗链方法及系统

技术领域

本发明实施例涉及互联网安全技术领域，尤其涉及一种防盗链方法及系统。

背景技术

随着互联网技术以及多媒体技术的快速发展，大量的安全问题应运而生，盗链就是其中的一方面。盗链是指服务提供商自己不提供服务的内容，通过技术手段绕过其它有利益的最终用户界面(如广告)，直接在自己的网站上向最终用户提供其它服务提供商的服务内容，骗取最终用户的浏览和点击率。

例如，实际应用中，一些不法商家可以通过相关技术(如网络爬虫技术)爬取多媒体服务提供商提供的流媒体文件的URL地址(Uniform Resource Locator，统一 资源定位符)，将URL地址里面的一些代码更改后放到自己的空间中，待用户想观看这个视频时，就直接点击这个链接后就可以直接播放，而真正的服务提供商却不知道自己的资源已经被盗链了，给真正的服务提供商造成了巨大的经济损失。

在盗链的过程中，受益者不提供资源或提供很少的资源，而真正的服务提供商却得不到任何的收益，并且还要承受因为被盗链所带来的一系列危害，

如：网站盗链会大量消耗被盗链网站的带宽，导致被盗链网站的访问速度变慢，真正的点击率也会很小，而且如果一台服务器中存在大量这样的盗链情况，服务器的速度就会下降，网络卡顿，给用户带来不好的体验，还严重损害了被盗链网站的利益，更严重的如果盗链网站还有色情、反动内容，更会对被盗链网站的名誉造成严重影响。因此互联网尤其是无线互联网安全领域，盗链安全防护势在必行。

现在传统的防盗链的方法主要包括判断引用地址法和使用动态文件名法。判断引用地址法是通过判断浏览器请求时HTTP 头的Referer 字段的值来确定是否盗链，但引用地址容易被伪造，防盗链不彻底。使用动态文件名法是当用户点击一个下载链接时，先在程序端计算一个Key，然后在数据库或Cache 里记录这个Key 以及它所对应的资源ID 或文件名，最后让网页重定向一个新的URL 地址，这个新URL 地址里需要包含这个Key。当浏览器或下载工具发出下载请求时，程序先检测这个Key 是否存在，如果存在则返回对应的资源数据，但当任意一个用户下载成功之后，你的资源就会被一些下载工具列入“ 资源候选名单” ，以后其他人在其他地方下载同样的文件时，只要Key 没有失效仍然可以下载，盗链也就持续下去了。

发明内容

为了解决防盗链中引用地址容易被伪造和使用动态文件名时非法厂商的信息被列入“ 资源候选名单” 而造成防盗链不彻底的情况，一方面，本发明

实施例提供一种防盗链方法，包括：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的IP地址；

对所述IP地址屏蔽访问服务。

本发明另一实施例提供一种防盗链方法，包括：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

向盗链者发送钓鱼访问请求；

接收盗链者返回的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的IP地址；

对所述IP地址屏蔽访问服务。

另一方面，本发明实施例提供了一种防盗链系统，包括：

特征信息提取模块，配置以：提取访问请求中的特征信息，所述特征信

息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

统计模块，配置以：统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

比较模块，配置以：比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析模块，配置以：解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述 IP 地址屏蔽访问服务。

本发明另一实施例提供了一种防盗链系统，包括：

特征信息提取模块，配置以：提取访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

钓鱼请求模块，配置以：向盗链者发送钓鱼访问请求；

播放页地址返回模块，配置以：接收盗链者返回的播放页地址；

解析模块，配置以：解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述 IP 地址屏蔽服务。

本发明通过防盗链方法及系统，保证了正常用户访问的同时也对盗链者进行了限制，而且因为访问用户特征信息的不同，使得基于所述特征信息生成数字水印也不同，不容易被伪造，进而实现了更加彻底的防盗链。

进一步地，本发明又一实施例的防盗链方法及系统，能够通过向盗链者发送钓鱼访问请求，接收盗链者返回的播放页地址，解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址，进而对所述 IP 地址屏蔽访问服务来避免在防盗链中对流媒体厂商的授权方发生误伤，提高了防盗链的精确度。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明一实施例的防盗链方法的流程图；

图 2 为本发明另一实施例的防盗链方法的流程图；

图 3 为本发明一实施例的防盗链系统的示意图；

图 4 为本发明另一实施例的防盗链系统的示意图;

图 5 为实施本发明实施例的防盗链方法及系统的架构图；

图 6 为实施本发明实施例的防盗链方法的服务器的结构示意图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

需要说明的是，在不冲突的情况下，本申请中的实施方式及实施方式中所涉及到的技术特征彼此之间可以相互组合。

本发明可应用在图片、音乐、视频、软件、zip 文件等相关的下载类资源上。例如，淘宝、拍拍、有啊等网站中的图片，乐视、优酷、PPTV、爱奇艺等媒体网站中的会员影片，新东方、环球雅思、韦博等培训机构的一些内部资料等相关资源上。

本发明实施例中可以通过硬件处理器（hardware processor）来实现相关功能模块。

图 1 为本发明防盗链方法实施例的流程示意图。如图 1 所示，本发明防盗链方法包括：

步骤 101：防盗链中心提取用户访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

步骤 102：防盗链中心基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

步骤 103：防盗链中心统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

步骤 104：防盗链中心比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

步骤 105：防盗链中心解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

步骤 106：防盗链中心对所述 IP 地址屏蔽访问服务。

上述步骤 104 中所述预定阈值是根据历史数据库中盗链者在所述一定时间内的平均盗链次数和/或受访服务器的工作能力来确定的。

为了提高判断盗链的精确度，上述预定阈值是可以定时或根据需求进行更新的。

图 2 为本发明防盗链方法的又一实施例的流程示意图。如图 2 所示，所述方法包括：

步骤 201：防盗链中心提取用户访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

步骤 202：防盗链中心基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

步骤 203：防盗链中心向盗链者发送钓鱼访问请求；

步骤 204：防盗链中心接收盗链者返回的播放页地址；

步骤 205：防盗链中心解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

步骤 206：防盗链中心对所述 IP 地址屏蔽访问服务。

上述访问请求中的特征信息例如还包括 MAC 地址、源物理端口号、以太网协议类型等。

上述“ 基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址” 包括：

防盗链中心利用随机数发生器至少对所述特征信息中的IP地址和访问时间进行处理生成数字水印；

将所述数字水印添加至播放文件的 URL 中生成播放页地址。

根据不同访问请求中的特征信息的不同，例如访问用户 IP 地址、访问时间、MAC 地址、源物理端口号、以太网协议类型的不同，能够做到每个独立的访问用户均拥有独立的数字水印信息，而且同一个用户的访问请求因为访问时间的不同，用户所拥有的数字水印信息也不同，进而生成的播放页地址也会不同，从而在判断时不会出现漏判、误判等情况发生。

上述在防盗链中心确定了盗链者的情况下，通过模拟用户，访问盗链者提供的服务（例如，Vst），获取盗链者的播放页地址，并解析所述播放页地

址中的所述数字水印，确定盗链者的 IP 地址，然后将所述 IP 地址上传到服务器中，直接对该 IP 地址屏蔽访问服务。

实际生活中，例如现在考研已经成为一种趋势，越来越多的学生投入到考研大军中去，为了在激烈的竞争中脱颖而出，学生都会在网上下载各种学习资料，但因为有些资料是某些培训机构（例如文都、新东方、启航等）的内部资料，只能该机构的学员才能下载观看，为了得到这些学习资料，学生会浏览各种学习网站，以期待能够获得这些学习资料，这时非法的商家会盗取培训机构资料的下载地址提供给学生进行非法盈利，为了有效地打击非法商家，维护培训机构的利益，这时可以基于内部学员的访问 IP 地址、访问时间、学员姓名等信息生成数字水印，并将所述数字水印添加至访问文件的 URL 中生成播放页地址，统计一定时间内带有所述数字水印的所述播放页地址的访问次数，进而比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址，解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址，对所述 IP 地址屏蔽访问服务，达到防止非法的运营商盗取学习资料的目的。

为了防止在防盗链的过程中出现误伤的现象，例如新东方可能授权韦博能使用新东方的一些内部资料，但是基于上述实施例中的方法可能会将韦博的服务也给屏蔽了，因而进一步地，防盗链中心先提取访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间，基于所述特征信息生成数字

水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址，然后向盗链者发送钓鱼访问请求，接收盗链者返回的播放页地址，解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址，对所述 IP 地址屏蔽服务。这样能有效防止在防盗链的过程中对授权方发生误伤。

本发明不会影响访问者所请求的链接，也不影响网站业务逻辑，保证了方便、便捷的使用效果；用于生成数字水印的访问者特征信息的可选性多样化，大幅度地减小了其被盗链的可能，并从原理上解决了多个访问者使用同一代理对网站进行访问，访问者IP 相同而导致无法被区分的问题。本发明的可行性高，大多数网站可以通过过滤器等简单技术实现，不会对网站原有业务造成影响。

本发明通过防盗链方法，保证了正常用户访问的同时也对盗链者进行了限制，而且因为访问用户特征信息的不同，使得基于所述特征信息生成数字水印也不同，不容易被伪造，进而实现了更加彻底的防盗链。

进一步地，本发明又一实施例的防盗链方法，防盗链中心（防盗链中心为服务器或者服务器集群）能够通过向盗链者发送钓鱼访问请求，接收盗链者返回的播放页地址，解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址，进而对所述 IP 地址屏蔽访问服务来避免在防盗链中对流媒体厂商的授权方发生误伤，提高了防盗链的精确度。

图 3 为本发明防盗链系统实施例的示意图。如图 3 所示，本发明防盗链

系统包括：

特征信息提取模块，配置以：提取用户访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息提取模块提取的特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

统计模块，配置以：统计一定时间内带有所述播放页地址生成模块生成的数字水印的所述播放页地址的访问次数；

比较模块，配置以：比较所述统计模块确定的访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析模块，配置以：解析比较模块确定的所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述解析模块确定的 IP 地址屏蔽访问服务。

上述比较模块中的所述预定阈值是根据历史数据库中盗链者的在所述一定时间内的平均盗链次数和/或受访服务器的工作能力来确定的。

本实施例中的防盗链系统中的防盗链中心，该防盗链中心为一个服务器或者服务器集群，其中每个模块可以是单独的服务器或者服务器集群，此时，上述模块之间的交互表现为各模块所对应的服务器或者服务器集群之间的交互，所述多个服务器或服务器集群共同构成本发明的防盗链系统。

具体地，所述多个服务器或服务器集群共同构成本发明的防盗链系统包括：

特征信息提取服务器或服务器集群，配置以：提取用户访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成服务器或服务器集群，配置以：基于所述特征信息提取服务器或服务器集群提取的特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

统计服务器或服务器集群，配置以：统计一定时间内带有所述播放页地址生成服务器或服务器集群生成的数字水印的所述播放页地址的访问次数；

比较服务器或服务器集群，配置以：比较所述统计服务器或服务器集群确定的访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析服务器或服务器集群，配置以：解析比较服务器或服务器集群确定的所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽服务器或服务器集群，配置以：对所述解析服务器或服务器集群确定的 IP 地址屏蔽访问服务。

在一种替代实施例中，可以是上述多个模块中的几个模块共同组成一个服务器或者服务器集群。例如：特征信息提取模块和播放页地址生成模块共同组成第一服务器或者第一服务器集群，统计模块和比较模块共同组成第二

服务器或者第二服务器集群，解析模块和屏蔽模块共同构成第三服务器或者第三服务器集群。

此时，上述模块之间的交互表现为第一服务器至第六服务器之间的交互或者第一服务器集群至第三服务器集群之间的交互，所述第一服务器至第六服务器或第一服务器集群至第三服务器集群共同构成本发明的防盗链系统。

图 4 为本发明防盗链系统的又一实施例的示意图。如图 4 所示，所述系统包括：

特征信息提取模块，配置以：提取用户访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息提取模块提取的特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

钓鱼请求模块，配置以：向盗链者发送钓鱼访问请求；

播放页地址返回模块，配置以：接收盗链者返回的播放页地址；

解析模块，配置以：解析所述播放页地址返回模块确定的播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述解析模块确定的 IP 地址屏蔽服务。

上述访问请求中的特征信息例如还包括 MAC 地址、源物理端口号、以

太网协议类型等。

上述播放地址生成模块，配置以：基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址包括：

利用随机数发生器至少对所述特征信息中的IP地址和访问时间进行处理生成数字水印；

将所述数字水印添加至播放文件的 URL 中生成播放页地址。

本实施例中的防盗链系统中的防盗链中心，该防盗链中心为一个服务器或者服务器集群，其中每个模块可以是单独的服务器或者服务器集群，此时，上述模块之间的交互表现为各模块所对应的服务器或者服务器集群之间的交互，所述多个服务器或服务器集群共同构成本发明的防盗链系统。

本实施例中由多个服务器或服务器集群共同构成本发明的防盗链系统详细实现，可参照前文防盗链系统系统实施例的叙述，在此不再赘述。本发明通过防盗链方法及系统，保证了正常用户访问的同时也对盗链者进行了限制，而且因为访问用户特征信息的不同，使得基于所述特征信息生成数字水印也不同，不容易被伪造，进而实现了更加彻底的防盗链。

进一步地，本发明又一实施例的防盗链方法及系统，能够通过向盗链者发送钓鱼访问请求，接收盗链者返回的播放页地址，解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址，进而对所述 IP 地址屏蔽访问服务来避免在防盗链中对流媒体厂商的授权方发生误伤，提高了防盗链的精确度。

如图 5 所示，为本实施本发明的防盗链方法和系统的架构图，包括防盗链中心 50、区域 A1 至区域 An，其中防盗链中心 50 包括多个服务器 S1~Si，区域 A1 至区域 An 中分别包括多个为用户提供流媒体等资源服务的边缘 CDN 节点 N；本架构图中防盗链中心的服务器接收用户通过客户端（客户端至少为智能终端）发送的访问请求后，执行本发明的如图 1 所示的防盗链方法，保证了正常用户访问的同时也对盗链者进行了限制。

如图 6 所示，为本发明的防盗链中心的服务器 600 的一实施例的结构示意图，本申请具体实施例并不对服务器 600 的具体实现做限定。如图 6 所示，该服务器 600 可以包括：

处理器(processor)610、通信接口(Communications Interface)620、存储器(memory)630、以及通信总线 640。其中：

处理器 610、通信接口 620、以及存储器 630 通过通信总线 640 完成相互间的通信。

通信接口 620，用于与比如客户端等的网元通信。

处理器 610，用于执行程序 632，具体可以执行上述方法实施例中的相关步骤。

具体地，程序 632 可以包括程序代码，所述程序代码包括计算机操作指令。

处理器 610 可能是一个中央处理器 CPU，或者是特定集成电路 ASIC

（Application Specific Integrated Circuit），或者是被配置成实施本申请实施例的一个或多个集成电路。

上述实施中的服务器中：

存储器，用于存放计算机操作指令；

处理器，用于执行所述存储器存储的计算机操作指令，以执行：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的IP地址；

对所述IP地址屏蔽访问服务。

和/或执行：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

向盗链者发送钓鱼访问请求；

接收盗链者返回的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

对所述 IP 地址屏蔽访问服务。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技

术方案的本质脱离本发明各实施例技术方案的精神和范围。

权 利 要 求 书

1、一种防盗链方法，包括：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的IP地址；

对所述IP地址屏蔽访问服务。

2、根据权利要求1所述的方法，其特征在于，所述预定阈值是根据历史数据库中盗链者在所述一定时间内的平均盗链次数和/或受访服务器的工作能力来确定的。

3、一种防盗链方法，包括：

提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间；

基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址；

向盗链者发送钓鱼访问请求；

接收盗链者返回的播放页地址；

解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

对所述 IP 地址屏蔽访问服务。

4、根据权利要求 3 所述的方法，其特征在于，所述基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址包括：

利用随机数发生器至少对所述特征信息中的IP地址和访问时间进行处理生成数字水印；

将所述数字水印添加至播放文件的 URL 中生成播放页地址。

5、根据权利要求 4 所述的方法，其特征在于，所述访问请求中的特征信息还包括 MAC 地址、源物理端口号、以太网协议类型。

6、一种防盗链系统，包括：

特征信息提取模块，配置以：提取访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息生成数字水印，将所

述数字水印添加至播放文件的 URL 中生成播放页地址；

统计模块，配置以：统计一定时间内带有所述数字水印的所述播放页地址的访问次数；

比较模块，配置以：比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址；

解析模块，配置以：解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述 IP 地址屏蔽访问服务。

7、根据权利要求 6 所述的系统，其特征在于，所述预定阈值是根据历史数据库中盗链者的在所述一定时间内的平均盗链次数和/或受访服务器的工作能力来确定的。

8、一种防盗链系统，包括：

特征信息提取模块，配置以：提取访问请求中的特征信息，所述特征信息至少包括 IP 地址和访问时间；

播放页地址生成模块，配置以：基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址；

钓鱼请求模块，配置以：向盗链者发送钓鱼访问请求；

播放页地址返回模块，配置以：接收盗链者返回的播放页地址；

解析模块，配置以：解析所述播放页地址中的所述数字水印，确定盗链者的 IP 地址；

屏蔽模块，配置以：对所述 IP 地址屏蔽服务。

9、根据权利要求 8 所述的系统，其特征在于，所述播放地址生成模块，配置以：基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的 URL 中生成播放页地址包括：

利用随机数发生器至少对所述特征信息中的IP地址和访问时间进行处理生成数字水印；

将所述数字水印添加至播放文件的 URL 中生成播放页地址。

10、根据权利要求 9 所述的系统，其特征在于，所述访问请求中的特征信息还包括 MAC 地址、源物理端口号、以太网协议类型。

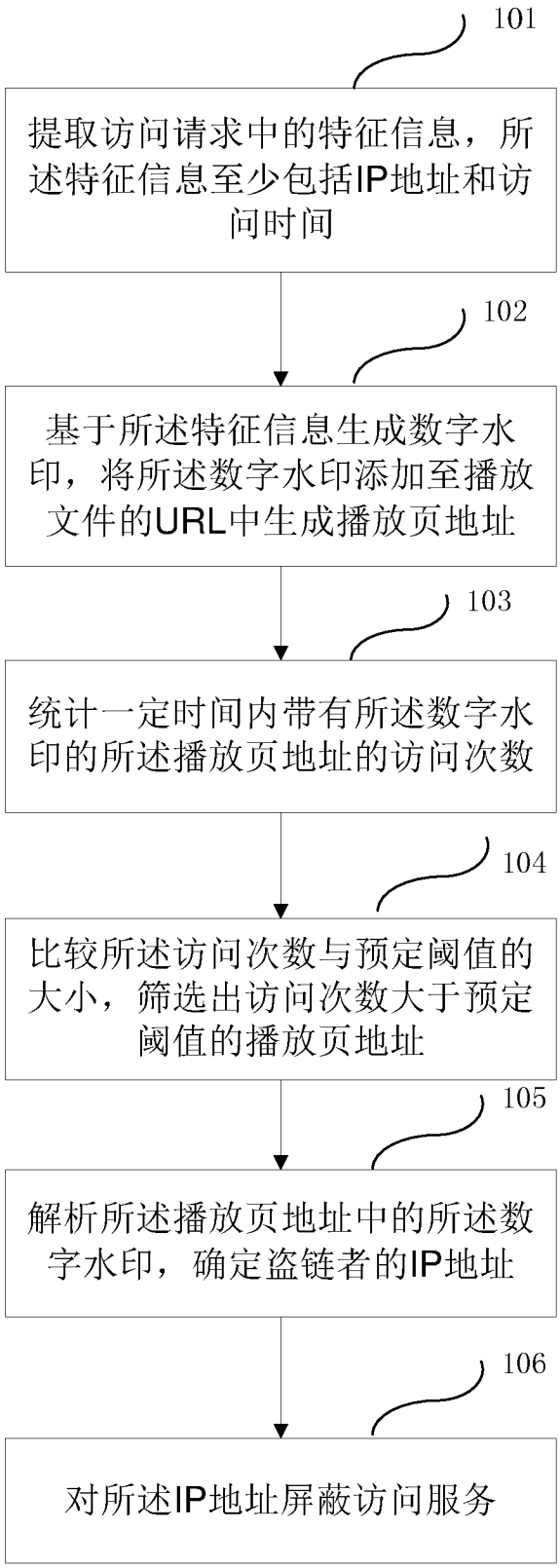

101
提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间
102
基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址
103
统计一定时间内带有所述数字水印的所述播放页地址的访问次数
104
比较所述访问次数与预定阈值的大小，筛选出访问次数大于预定阈值的播放页地址
105
解析所述播放页地址中的所述数字水印，确定盗链者的IP地址
106
对所述IP地址屏蔽访问服务

图 1

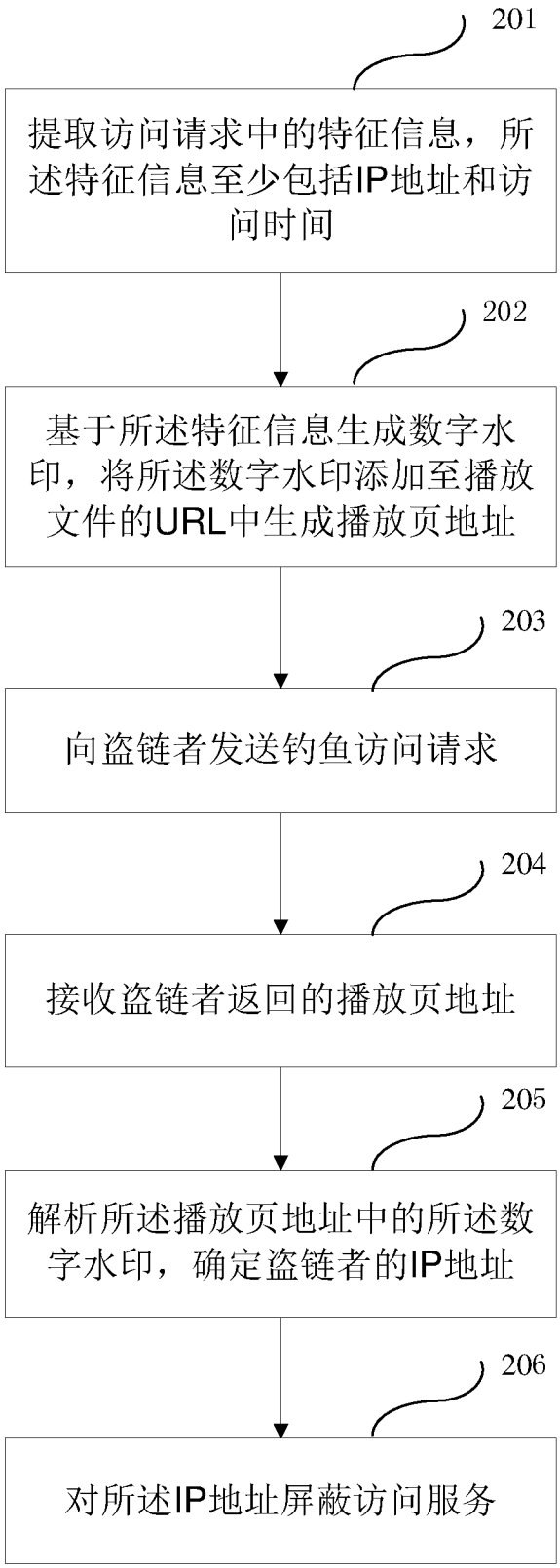

201
提取访问请求中的特征信息，所述特征信息至少包括IP地址和访问时间
202
基于所述特征信息生成数字水印，将所述数字水印添加至播放文件的URL中生成播放页地址
203
向盗链者发送钓鱼访问请求
204
接收盗链者返回的播放页地址
205
解析所述播放页地址中的所述数字水印，确定盗链者的IP地址
206
对所述IP地址屏蔽访问服务

图 2

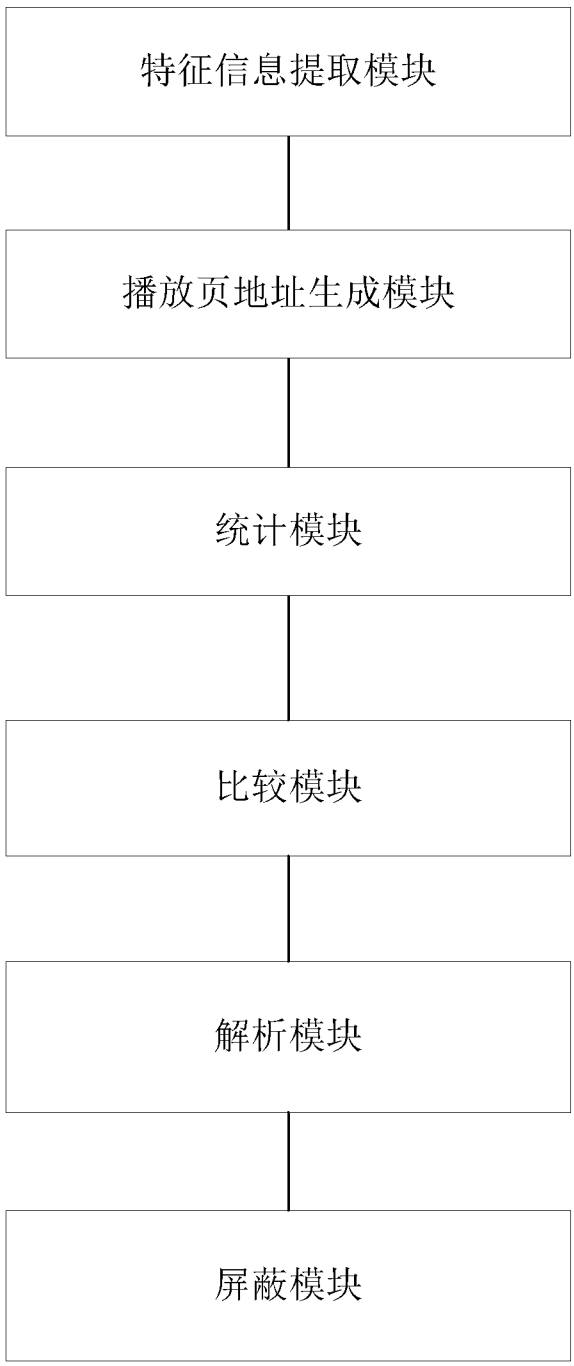


图 3

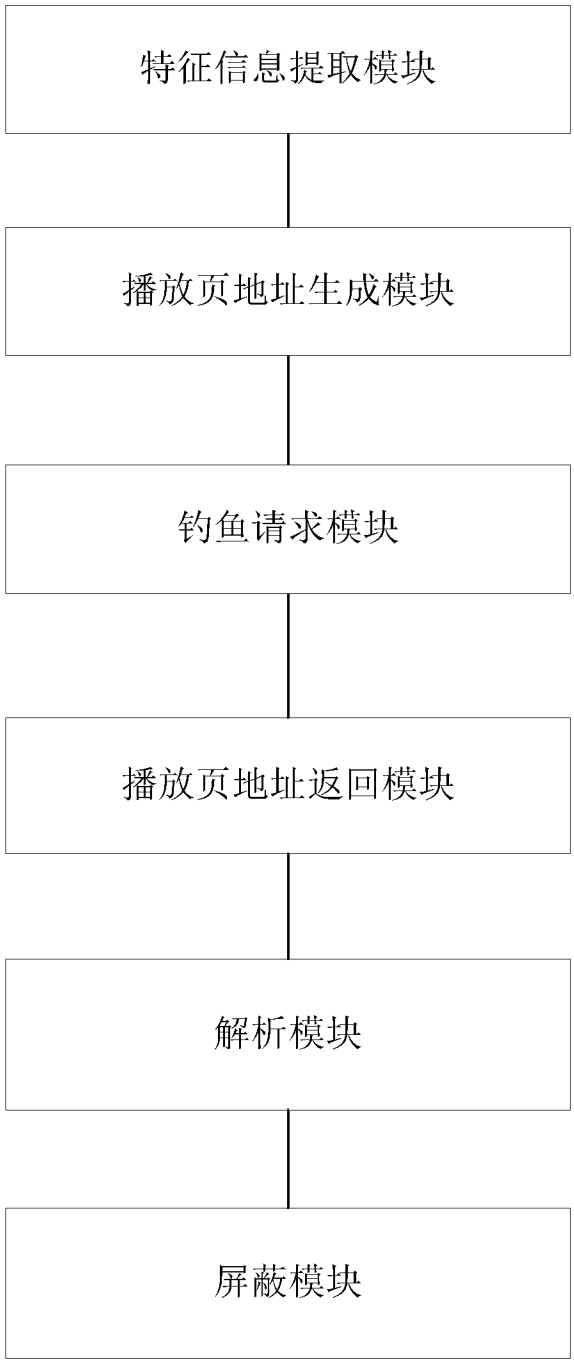


图 4

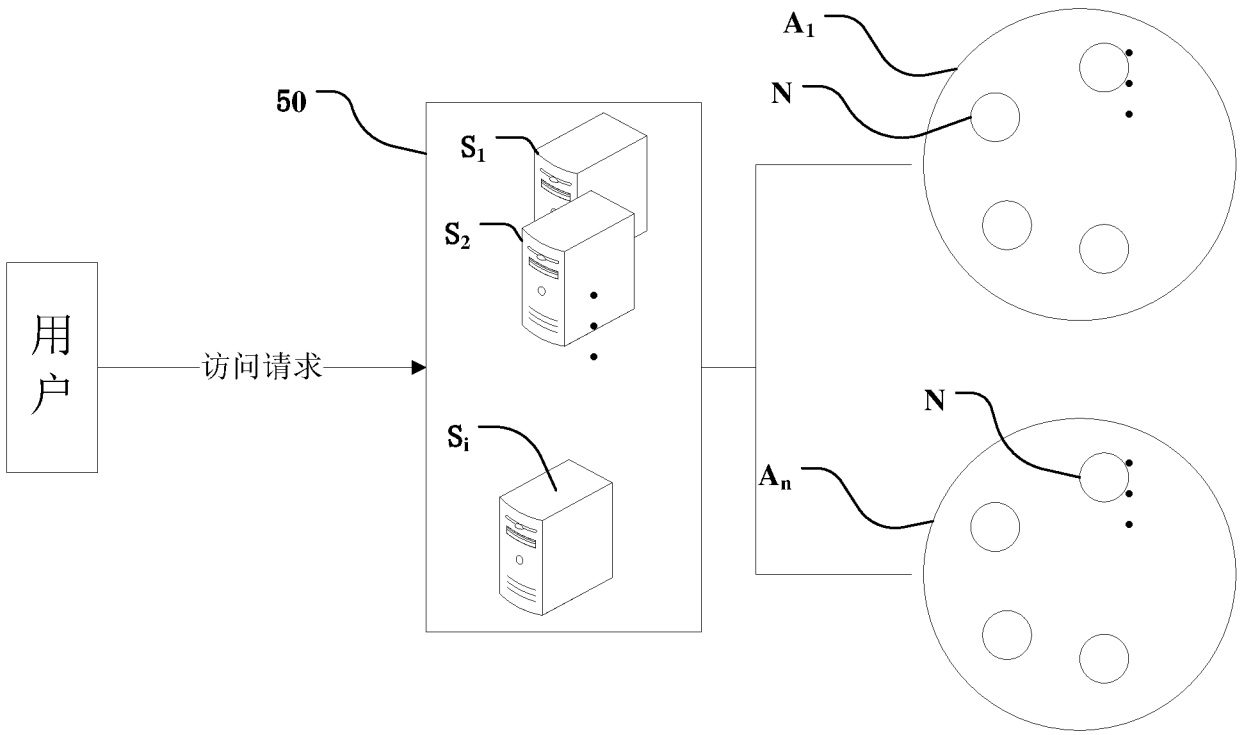

50
S_1
S_2
S_i
用户
访问请求
A_1
N
N
A_n

图 5

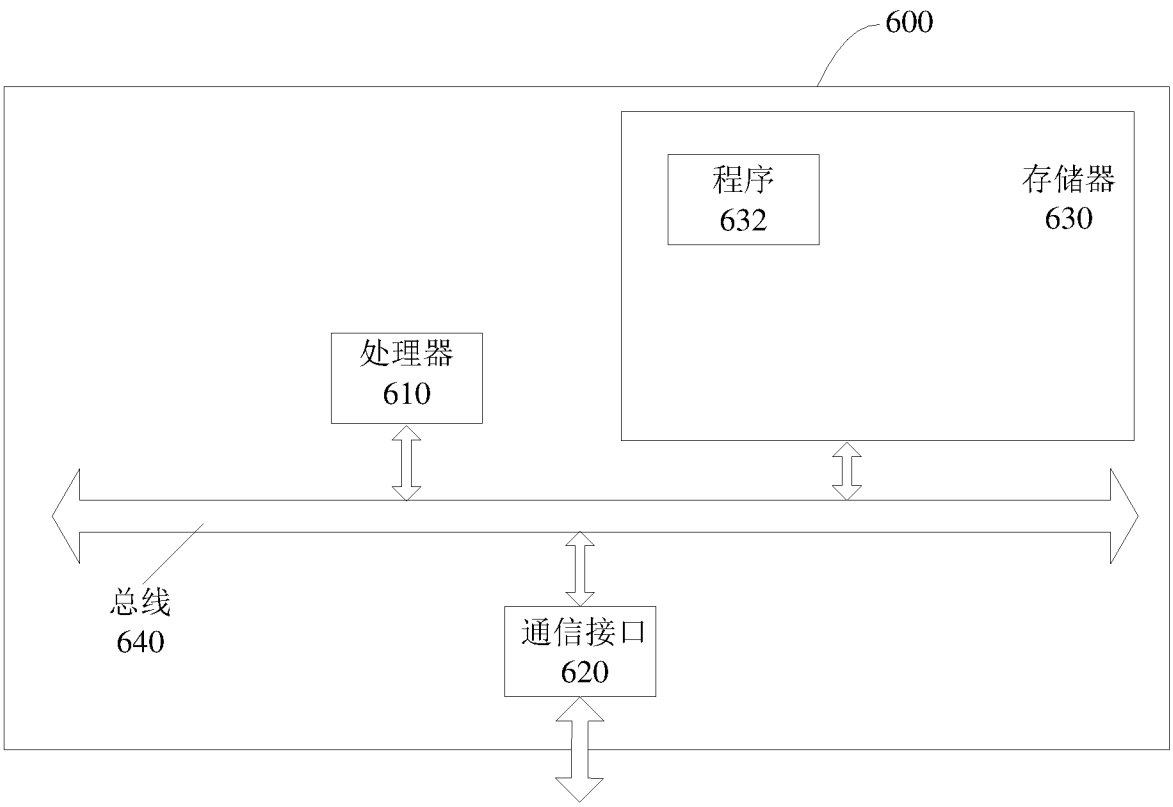

600
程序
632
存储器
630
处理器
610
总线
640
通信接口
620

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/083015

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: IP, URL, number of times, peculat+, anti-stealing, anti-leech, hotlinking, theft-proof, watermark, play, threshold, fishing, access, time, number, shield

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103957436 A (BEIJING QINGYUAN XINCHUANG TECHNOLOGY CO., LTD.), 30 July 2014 (30.07.2014), claims 1-4	1, 2, 6, 7
A	CN 103957436 A (BEIJING QINGYUAN XINCHUANG TECHNOLOGY CO., LTD.), 30 July 2014 (30.07.2014), the whole document	3-5, 8-10
Y	CN 104079531 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 01 October 2014 (01.10.2014), description, paragraphs [0067]-[0090]	1, 2, 6, 7
A	CN 104079531 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 01 October 2014 (01.10.2014), the whole document	3-5, 8-10
A	CN 103701796 A (SHANDONG CVIC COMMERCIAL MIDDLEWARE CO., LTD.), 02 April 2014 (02.04.2014), the whole document	1-10
A	WO 2007076685 A1 (ZTE CORPORATION), 12 July 2007 (12.07.2007), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 July 2016 (01.07.2016)	**21 July 2016 (21.07.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **LIU, Juan** Telephone No.: (86-10) **62413912**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/083015

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103957436 A	30 July 2014	None	
CN 104079531 A	01 October 2014	None	
CN 103701796 A	02 April 2014	None	
WO 2007076685 A1	12 July 2007	CN 1992594 A	04 July 2007

国际检索报告

国际申请号 PCT/CN2016/083015

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNKI，CNPAT，WPI，EPODOC：盗链，IP，水印，播放，阈值，门限，钓鱼，URL，访问，时间，次数，屏蔽，peculat+,anti-stealing,anti-leech,hotlinking,theft-proof, watermark,play,threshold,fishing,access,time,number,shield

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 103957436 A (北京清源新创科技有限公司) 2014年 7月 30日 (2014-07-30) 权利要求1-4	1，2，6，7
A	CN 103957436 A (北京清源新创科技有限公司) 2014年 7月 30日 (2014-07-30) 全文	3-5，8-10
Y	CN 104079531 A (中国移动通信集团公司) 2014年 10月 1日 (2014-10-01) 说明书第[0067]-[0090]段	1，2，6，7
A	CN 104079531 A (中国移动通信集团公司) 2014年 10月 1日 (2014-10-01) 全文	3-5，8-10
A	CN 103701796 A (山东中创软件商用中间件股份有限公司) 2014年 4月 2日 (2014-04-02) 全文	1-10
A	WO 2007076685 A1 (ZTE CORPORATION) 2007年 7月 12日 (2007-07-12) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 7月 1日	2016年 7月 21日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	刘娟
传真号 (86-10)62019451	电话号码 (86-10)62413912

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/083015

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103957436	A	2014年 7月 30日	无			
CN	104079531	A	2014年 10月 1日	无			
CN	103701796	A	2014年 4月 2日	无			
WO	2007076685	A1	2007年 7月 12日	CN	1992594	A	2007年 7月 4日