

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 9/00 (2006.01)

H04L 9/10 (2006.01)



[12] 发明专利说明书

专利号 ZL 200410057953.8

[45] 授权公告日 2009年12月16日

[11] 授权公告号 CN 100571121C

[22] 申请日 2004.8.27

[21] 申请号 200410057953.8

[73] 专利权人 国际商业机器公司

地址 美国纽约

[72] 发明人 罗琳 张健 阎蓉 邵凌

[56] 参考文献

US2004/0133794A1 2004.7.8

US6691229B1 2004.2.10

CN1321265A 2001.11.7

US2004/0111611A1 2004.6.10

一种抗共谋攻击的数字视频指纹算法改进方案. 纪震, 姜来, 李慧慧. 深圳大学学报理工版, 第21卷第1期. 2004

审查员 李晓利

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 李玲

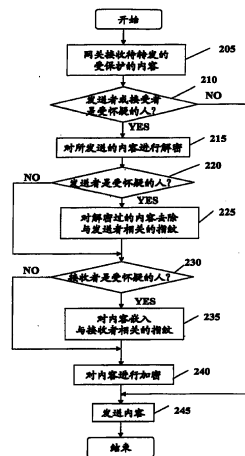
权利要求书2页 说明书11页 附图3页

[54] 发明名称

无线数字版权管理系统中的盗版跟踪和识别方法

[57] 摘要

本发明涉及一种无线数字版权管理系统中的盗版跟踪和识别方法, 其中, 内容提供商以超级分发模式递送受保护数字内容, 当检测到存在未经授权持有所述受保护的数字内容的盗版时, 基于无线数字版权管理系统中无线运营商的网关控制能力, 在所递送的受保护的数字内容中嵌入或删除特定的指纹, 以对受到怀疑的人进行跟踪并进一步识别盗版者, 其中所述特定的指纹与因未经授权持有所述受保护的数字内容而受到怀疑的人的信息有关。并进一步包括对受怀疑人进行筛选以确定高度受怀疑的人的处理。因此运营商能通过比较被盗版内容和该受怀疑人所持版本是否一致来确定该受怀疑的人是否是真正的盗版者, 实现了精确的盗版跟踪和识别。



1. 一种无线数字版权管理系统中的盗版跟踪和识别方法，其中，内容提供商以超级分发模式递送受保护数字内容，所述方法包括：

当检测到存在未经授权持有所述受保护的数字内容的盗版时，则在内容提供商所在的或与所述内容提供商相关的无线运营商的网关接收到待转发的受保护的数字内容时，根据转发数字内容的发送者或接收者是否持有被盗版数字内容的相应版本，判断转发数字内容的发送者或接收者是否为受到怀疑的人；

当接收所述数字内容的接收者为受到怀疑的人时，由内容提供商所在的网关或与所述内容提供商相关的网关在所述数字内容中嵌入一个与作为接收者的所述受到怀疑的人相关的指纹；

当转发所述数字内容的发送者为受到怀疑的人时，由内容提供商所在的网关或与所述内容提供商相关的网关去除所述数字内容中嵌入的与作为发送者的所述受到怀疑的人相关的指纹；以及

基于对所述含有与受到怀疑的人相关的指纹的数字内容版本的跟踪，识别泄露内容的盗版者。

2、根据权利要求1的方法，其中判断转发数字内容的发送者或接收者是否为受到怀疑的人的步骤进一步包括：

对所有持有被盗版数字内容的受到怀疑的人进行筛选，以确定最有可能泄露所述数字内容的一个或几个高度受到怀疑的人。

3、根据权利要求2的方法，进一步包括：

根据每个受到怀疑的人持有的多个不同盗版内容版本的频率，从所有持有被盗版数字内容的受到怀疑的人中筛选出高度受到怀疑的人。

4、根据权利要求2的方法，进一步包括：

根据每个受到怀疑的人处于转发路径层级的不同来设置不同的怀疑度，由此从所有持有被盗版数字内容的受到怀疑的人中确定高度受怀疑的人。

5、根据权利要求 1 的方法，进一步包括：

基于用户转发内容时运营商网关的转发记录，或者是用户索取使用权限的历史记录来识别和显示接收未经授权的数字内容的所有用户，并将所述用户标识为受到怀疑的人。

6、根据权利要求 5 的方法，进一步包括：运营商网关根据用户转发内容时其所记录的关于未经授权内容的分发记录来识别受到怀疑的人，其中所述记录包括：

转发所述数字内容的时间/日期；

发送者和接收者的 ID；以及

内容 ID。

7、根据权利要求 1 的方法，进一步包括：

检测所述被盗版的数字内容中由内容提供商在其中嵌入的指纹，由此确定所述被盗版内容的版本和一级用户，其中所述一级用户是指直接从所述内容提供商获权使用数字内容的用户。

8、根据权利要求 1 的方法，进一步包括：

通过比较被盗版内容和该受怀疑人所持版本是否一致来确定该受怀疑的人是否是真正的盗版者的步骤。

无线数字版权管理系统中 的盗版跟踪和识别方法

技术领域

本发明一般涉及无线数字版权管理 (DRM) 技术, 特别涉及一种无线数字版权管理系统中的盗版跟踪和识别方法。

背景技术

无线数字版权管理 (DRM) 技术是提供基于远程认证、数字水印 (指纹)、算法加密技术之上的, 对在线传播的文本、图像、音乐或媒体文件等的数字内容进行保护的技术解决方案。

有效的 DRM 解决方案允许网络数字内容提供商控制浏览、阅读其数字内容的访问权限, 而无论这些内容是文字内容、音乐还是图像或是其他的多媒体文件。DRM 方案保证只有获得合法授权的用户才能拥有相应的权利。每一个授权用户, 在支付一定费用后, 即会获得一个唯一对应的用户标识和口令, 并授予与加密算法相应的许可的终端播放器。

为了跟踪盗版行为, 在传统的 DRM 系统中, 对于用户所请求的数字内容, 例如数字形式的文字、音乐、图像等多媒体文件, 盗版跟踪方法使用数字指纹 (fingerprint) 技术向请求用户发送一个所请求内容的拷贝, 其中在所述拷贝中嵌入了与用户信息相关的指纹而形成同一内容的不同版本。为避免未经授权的拷贝制作和发行, 数字内容提供商可以将不同用户的 ID 或序列号作为不同的指纹嵌入 (可以采用水印技术实现) 作品的合法拷贝中。当出现盗版的情况时, 就可以根据此被盗版拷贝中恢复出的指纹来确定它的版本和来源, 从而可以找出与所述指纹相关的用户, 识别出盗版者。盗版现象的发现过程在本申请中不做探讨。

与传统 DRM 系统中受保护的内容被直接从内容提供商分发给终端用户的情况不同，无线 DRM 系统具有其特有的特征，即网络内容提供商希望其所提供的已用加密方法保护的数字内容能以一种超级分发（SUPER-DISTRIBUTE）的模式进行传播。内容提供商希望能有更多的合法用户得到其所提供的各种数字媒体内容。具体来讲，在内容提供商向一组用户（称为一级用户）提供了数字内容后，所述内容提供商通常还希望该一级用户能将其所接收的已受保护的内容再次合法地转发给其他用户（二级用户）以使所述内容更广泛的分发，其中在一级用户向二级用户转发所述内容的时候，二级用户在接收到受保护内容后，需要获得使用所述保护内容的授权而成为合法用户并正常使用该内容，类似地，二级用户还可以再进一步将内容转发给三级用户，由此内容提供商可在多次分发中从各级合法用户中收取适当的费用而获利。在这种多次转发（也可称为超级分发模式）的情况下，是鼓励用户进一步将其所接收的受保护内容进行合法的超级分发的。在当前的无线 DRM 系统中，数字内容的版权保护通常依赖于接收/使用受保护内容的用户（也就是合法的权利对象）的发布。但是，这种超级分发模式使得传统盗版跟踪方法不能有效找出泄露受保护内容的用户。具体来讲，如果盗版的内容（泄露内容）是由一级用户泄露的，则通过现有技术的 DRM 技术，通过在被盗版的内容中恢复出的指纹来确定盗版的来源，可以找出与所述指纹相关的用户而识别出盗版者（泄露点）。但是，当通过超级分发进行了多次转发以后，如果盗版的内容是由二级用户或是三级用户，甚至是更下一级的用户泄露的话，根据现有的 DRM 技术，由于转发内容（盗版内容）中只包含了与一级用户有关的指纹，则只能将盗版者定位到一级用户，而在当盗版者出现在二级用户或三级用户中的某些用户时，则无法具体识别出无线 DRM 系统中的数字内容的泄露点。

强健的 DRM 系统应该能经受黑客的攻击。这意味着系统应该能抵抗黑客的攻击，还应该能识别黑客。后者也就是所谓的盗版跟踪。只有在有效的跟踪后，运营商才能采取措施，或废除黑客的帐户，或

对黑客进行起诉。但现有技术的 DRM 系统不能有效、确切识别出盗版者/黑客，因此不能有效防止盗版。

发明内容

为解决现有技术中的上述问题，本发明的一个目的是对现有技术中的数字版权管理系统进行进一步的改进，以提供一种高效精确的无线数字版权管理技术中的盗版跟踪和识别方法。

本发明的另一个目的是利用无线运营商的控制能力，对所有转发给可能泄露受版权保护的数字内容的受到怀疑的人或从受到怀疑的人接收内容的人进行专门的跟踪，从而提供一种精确的无线数字版权管理技术中的盗版跟踪和识别方法。

本发明的再一个目的是进一步提高无线数字版权管理技术中的盗版跟踪的识别效率，通过首先对受到怀疑的人进行筛选，再对高度受到怀疑的人使用根据本发明的专用的跟踪技术，使受到怀疑的人的范围缩小，则可更高效地识别盗版的人或泄露点。

根据本发明，提出了一种无线数字版权管理系统中的盗版跟踪和识别方法，其中，内容提供商以超级分发模式递送受保护数字内容，当检测到存在未经授权持有所述受保护的数字内容的盗版时，基于无线数字版权管理系统中无线运营商的网关控制能力，在所递送的受保护的数字内容中嵌入或去除特定的指纹，以对受到怀疑的人进行跟踪并进一步识别盗版者，其中所述特定的指纹与因未经授权持有所述受保护的数字内容而受到怀疑的人的信息有关。

优选地，所述方法进一步包括：在内容提供商所在的或与所述内容提供商相关的无线运营商的网关接收到待转发的受保护内容时，根据转发内容的发送者或接收者是否持有被盗版数字内容的相应版本，判断转发内容的发送者或接收者是否为受到怀疑的人；当接收所述数字内容的接收者为受到怀疑的人时，由内容提供商所在的网关或与所述内容提供商相关的网关在所述数字内容中嵌入一个与所述受到怀疑的人相关的指纹；当转发所述数字内容的发送者为受到怀疑的人时，

由内容提供商所在的网关或与所述内容提供商相关的网关去除所述数字内容中嵌入的与所述受到怀疑的人相关的指纹；以及基于对所述含有与受到怀疑的人相关的指纹的内容版本的跟踪，识别泄露内容的盗版者。因此运营商能通过比较被盗版内容和该受怀疑人所持版本是否一致来确定该受怀疑的人是否是真正的盗版者。从而实现了精确的盗版跟踪和识别方法。

优选地，所述盗版跟踪和识别方法还包括：对所有持有被盗版数字内容的受到怀疑的人进行筛选，以确定最有可能泄露所述数字内容的一个或几个高度受到怀疑的人。只有这些高度受怀疑的人才执行专门的跟踪过程，则可更高效率地识别盗版的人或泄露点。对大多数通常的用户来说，在系统运营商一侧没有增加明显的附加工作，由此节省了大量的资源。

附图说明

本发明的特点、优点及有益效果将通过参考以下附图进行的详细描述而变得更加清楚和明显，其中：

图 1 示意性示出了无线 DRM 系统的超级分发模式的图；

图 2 是根据本发明的用于定位盗版者的专用识别方法的流程图；

以及

图 3 是根据本发明优选实施例的无线数字版权管理系统中的盗版跟踪和识别方法的示意图。

具体实施方式

以下结合附图对本发明的具体实施方式进行详细描述。

参照附图 1，附图 1 是基于 Open Mobile Alliance 的系统，在图 1 示意性示出了可应用本发明方法的无线 DRM 系统 100 的超级分发模式的图。所述 DRM 系统 100 包括至少一个内容发布者服务器 101，用于由内容提供商发布受到保护的数字内容，所述数字内容例如包括但不限于文字内容、音乐、图像或是其他的多媒体流，并且是由内容

提供商采用各种加密方法对所提供内容进行加密而得到受到保护的内容。通常，DRM 系统允许数字内容以加密的形式进行分发，通常还利用了现有的 Internet 传输协议，如 TCP/IP、SSL、HTTP 等技术。通过将一组权利与每个单个内容相关，且只有获取访问受保护的数字内容的权利后，用户才允许对其进行解密。内容提供商所采用的加密方法包括但不限于对称密钥加密（AES，DES 等）和非对称密钥加密（RSA 等）。多个用户设备 110 通过网络以有线或无线的方式与该内容发布者服务器 101 进行通信，浏览该内容发布者服务器 101 上提供的各种数字内容，并从该内容发布者服务器上下载所需要的受保护的数字内容。在附图 1 中，仅示出了与内容发布者服务器 101 进行直接通信的其中一个用户，例如 Jo。应该知道，与内容发布者服务器 101 进行直接通信的用户可以有多个，并且所述用户例如 Jo 所持有的设备包括但不限于：PDA（个人数字助理）、计算机、移动电话、机顶盒、数字电视等无线或有线设备。在 DRM 系统中，通常防止用户直接解密内容。受保护的内容仅能通过一些特定的播放器/浏览器来再现受保护的内容。用户设备 110 在对内容发布者服务器 101 提供的数字内容进行解密后，可在所述用户拥有的各种设备之间，例如该用户所持有的 PDA（个人数字助理）、计算机、移动电话、机顶盒、数字电视等，共享所述从内容发布者服务器 101 下载的解密的数字内容。

在用户设备从内容发布者服务器 101 下载受到保护的数字内容后，通常用户并不能正常浏览所述内容，还需要得到授权。在这种情况下，在用户设备从内容发布者服务器 101 下载受到保护的数字内容的同时，内容发布者服务器 101 会将所述受到保护的数字内容进行加密所对应的一个密钥传送给一个权利发布者服务器 105。用户设备 110 通过向权利发布者服务器 105 请求并购买所述密钥，在权利发布者和所述用户设备之间建立起信任后，用户可被授权使用、阅读所述受到保护的数字内容。在附图 1 中，示出的内容发布者服务器 101 和权利发布者服务器 105 是分立的，但在实际使用中，也可以使用一个单独的服务器来实现所述两个服务器的功能。

在无线 DRM 系统中，通常内容发布者是鼓励授权用户能再进一步转发其获权使用的数字内容的。在这种情况下，已被授权使用所述内容发布者服务器 101 提供的受保护的数字内容的一级用户，例如 Jo，通过有线或无线的方式，将所述内容转发给其他人，例如 Sarah。其中首次接收该转发数字内容的用户可被称为二级用户。该二级用户通过向所述权利发布者 105 发送请求并购买权利而获得使用所转发的数字内容的授权，并在所述二级用户与所述权利发布者之间建立起信用。类似地，二级用户可再次将其授权使用的数字内容再次转发给三级用户，而所述三级用户也通过向权利发布者发送请求并购买权利而获得使用所转发的数字内容的授权，并在所述三级用户与所述权利发布者之间建立起信用。如此，受保护的数字内容可分发给多级用户，从而通过这种方式建立所谓的超级分发模式。

此外，如前所述，为了跟踪盗版行为，在 DRM 系统中，对于用户所请求的数字内容，例如数字形式的文字、音乐、图像等多媒体文件，盗版跟踪方法使用数字指纹技术向请求用户发送一个所请求内容的拷贝，其中在所述拷贝中嵌入了与用户（一级用户）信息相关的指纹而形成同一内容的不同版本。

从以上对当前使用的无线 DRM 系统 100 的超级分发模式进行的描述可知，在进行每次内容转发的过程中，所转发的受保护的内容只是嵌入了有关一级用户的指纹，当受到保护的数字内容被未被授权的用户使用时，换句话说，也就是在出现盗版的情况下，由于转发内容中只包含了与一级用户有关的指纹，则只能将盗版者定位到一级用户，根据现有技术将无法识别出盗版发生在二级用户、或三级用户甚至更下一级用户的情况，从而无法确切知道盗版发生的确切泄露点。

类似于传统的跟踪系统，本发明要求内容分发者递送不同的内容的拷贝（所述内容嵌入不同的指纹）给不同的用户，同样这些用户可以再分发所述内容给其他用户。换句话说，直接从内容发布者接收内容的一级用户将接收嵌入了与该一级用户信息相关的独特的指纹的内容的唯一版本，另外，可选择地，也可以是在所分发内容中事先嵌入

特定的指纹，而在分发时由几个一级用户共享同一版本。

为了在所述的超级分发模式中跟踪和识别盗版者，本发明提出了一种在无线数字版权管理系统中使用的盗版跟踪和识别方法。为实现这个目的，本发明在现有技术的基础上，利用了网关对转发内容的控制，由此精确识别和跟踪盗版。

根据本发明提出的无线 DRM 系统中的盗版跟踪和识别方法，利用了无线运营商的网关对超级分发的内容的控制能力，来对盗版内容进行跟踪和识别。

首先，解释本发明方法所采用的盗版跟踪和识别方法的基本原理：

1、在以超级分发模式递送受保护数字内容时，基于无线 DRM 系统中无线运营商的网关控制能力，在所递送的应该受到保护的数字内容中嵌入或删除特定的指纹，来对被怀疑的人进行跟踪并进一步识别各个泄露的人，其中所述特定的指纹与受到怀疑的人信息有关。

2、基于第一点，如果被怀疑的人的数量较多时，本发明还提出使用一个初步筛选步骤，对所述多个受到怀疑的人进行过滤，以在实施专门的跟踪步骤之前，首先将受到怀疑的人群缩小。因此，只有一小群受怀疑的人（高度受到怀疑的人）需要进行专用的高成本的跟踪。对于大多数客户来说，在系统运营商一侧没有增加明显的附加工作。

以下结合附图 2、3 对本发明的方法进行具体描述，从而本发明的优点、有益效果和其他特点将会变得更清楚。附图 2 示意性示出了根据本发明的对盗版内容进行跟踪和识别的方法。具体地，在附图 2 中示出了：当检测到有盗版的数字内容后，开始根据本发明的专用跟踪处理对之后发送数字内容的过程进行盗版追踪。根据本发明，当出现盗版的情况时，根据之前转发的内容通过运营商的无线递送网关的记录，可以判断出持有与被盗版内容相同版本的人并将其确定为受到怀疑的人，之后对所有转发给受到怀疑的人或从受到怀疑的人发出的内容进行专门的跟踪。

参考附图 2 的示意流程图，在步骤 S205，由网关服务器接收待转发的受保护的数字内容。其中，网关服务器接收的数字内容通过使用

加密方法，例如对称密钥加密、非对称密钥加密等，进行加密而受到保护。特别地，在网关服务器中接收到的数字内容中，还嵌入了在内容提供商将受保护内容提供给一级用户时，在所述内容中嵌入的与所述一级用户有关的指纹；另外，可选择地，也可以是在所分发内容中事先嵌入特定的指纹而形成不同版本，而由几个一级用户共享同一版本。网关服务器例如可以是内容提供商的网关服务器，或者也可以是与内容提供商有关的网关服务器或中间服务器。

接下来，在步骤 S210，执行一个判断，以判断内容发送者或内容接收者是不是已知的被怀疑的人。对用户（发送者或接收者）是否是被怀疑人的判断是根据以下原则事先判断好的：在有内容被泄露的时候（盗版），运营商检测在所泄露的内容中嵌入的指纹，并且找出所泄露内容的版本和一级用户，根据从盗版内容中识别出的指纹，而将持有与所述内容的与该指纹相关的相应版本的人（将要转发所述内容的人或将要接收所述内容的人）判断为泄露内容的被怀疑者。确定被怀疑人通常基于用户转发内容时由无线运营商记录的以下内容：转发的时间/日期；发送者和接收者的 ID；内容 ID（可选地，为版本 ID，该版本 ID 用来识别内容的版本，注释不同的一级用户接收内容的不同版本）。如果一段内容被泄露，则运营商将检测在所泄露的内容中嵌入的指纹，并且找出所泄露内容的版本和一级用户。由于运营商具有所有转发的记录，因此能够重新构建泄露内容的分发图，也就是说，能够识别和显示接收泄露内容的所有用户，并将所述用户视为可能的泄露者（被怀疑的人）。

当在步骤 S210 中判断出内容发送者或内容接收者是泄露内容的被怀疑者时，过程进行到步骤 S215。否则，当在步骤 210 中判断出内容发送者和内容接收者都不是受到怀疑的人，则处理转到步骤 245，直接转发所述内容。

在步骤 S215，对网关对所要转发的内容进行数据解密。

接下来，在步骤 220 中进一步判断发送者是否是受怀疑的人。如果判断结果为“是”，则过程进行到步骤 225，在该步骤中，对解密

过的内容，通过与指纹嵌入对应的方法来去除掉所转发内容中的与发送者相关的指纹，然后过程进行到步骤 230。如果在步骤 220 中的判断结果为“否”，则过程直接进行到步骤 230。

在步骤 230，进一步判断接收者是否是受怀疑的人。如果判断结果为“是”，则过程进行到步骤 235，在该步骤中，在所要转发的内容中嵌入与接收者相关的指纹。然后过程进行到步骤 240。如果在步骤 230 中的判断结果为“否”，则过程直接进行到步骤 240。

在步骤 240 中，对所述转发内容进行加密，以及在步骤 245 中，发送所述经过加密的内容。至此，结束所述处理。

根据上述对本发明的专用跟踪处理的描述，可知：当出现盗版的情况时，首先根据之前转发的内容通过运营商的无线递送网关的记录可以判断出持有与被盗版内容相同版本的人并将其确定为受到怀疑的人，之后对所有转发给受到怀疑的人或从所有受到怀疑的人发出的内容进行专门的跟踪，即在所递送的受保护的数字内容中嵌入或删除特定的指纹，来对被怀疑的人进行跟踪并进一步识别各个泄露的人。当受怀疑人再次盗版时，由于被盗版的内容中存在与受怀疑人唯一相关的指纹，因此可以确定盗版者。

由上述对附图 2 的描述可知，当执行根据附图 2 的盗版跟踪和识别方法，如果对所有盗版怀疑者都进行专用跟踪处理，则花费将是很高的，因为指纹的嵌入/去除将消耗一些服务器资源。如果对所有用户都进行跟踪，则也将会使无线网关的性能降低。因此，本发明还进一步提出：在上述专用跟踪过程之前，首先进行一个初步筛选过程来将受怀疑的人群缩小。只有这些高度受怀疑的人才在第二跟踪阶段被跟踪，对大多数通常的用户来说，在系统运营商一侧没有增加明显的附加工作，由此节省了大量的资源。

参考附图 3，其中示出了根据本发明一种优选实施方式的对受到怀疑的人进行专门跟踪的两阶段跟踪方法。其中在附图 3 中的阶段 2 所示出的步骤与附图 2 中的步骤相同，包括：

- 1) 当一段内容被分发给或转发给受怀疑的人的时候，由运营商

的网关，或是内容提供商服务器的网关，为所述内容再嵌入一个特别的指纹，其中，所述指纹与所述用户（接收受保护内容的受怀疑的人）相关；

2) 而当一段内容从受怀疑的人转发时，在所述内容通过运营商的网关时，网关从所述内容中去除与发送者相关的指纹，以便接收者能接收到没有与受怀疑的发送者相关的指纹的“干净”的拷贝。

因此，即使在超级分发过程之后，受到怀疑的人实际上也可以获得所述内容的唯一版本，因此运营商能通过比较被盗版内容和该受怀疑人所持版本是否一致来确定该受怀疑的人是否是真正的盗版者。

以下进一步参考附图 3，详细描述附图 3 中的第一阶段，即根据本发明该优选实施例的对受到怀疑的人进行筛选的初步筛选过程。

在初步筛选过程中，首先基于用户转发内容时由无线运营商记录的以下内容：转发的时间/日期；发送者和接收者的 ID；内容 ID（可选地，为版本 ID，该版本 ID 用来识别内容的版本，注释不同的一级用户接收内容的不同版本）。如果一段内容被泄露，则运营商将检测在所泄露的内容中嵌入的指纹，并且找出所泄露内容的版本和一级用户。由于运营商具有所有转发的记录，因此能够重新构建泄露内容的分发图，也就是说，能够识别和显示接收泄露内容的所有用户，并将所述用户视为可能的泄露者。

如果存在有几段带有不同指纹的泄露内容，则内容发布者/运营商能够识别出几组可能的受怀疑者，并且当泄露内容的数量增加时，运营商能够识别出多组可能受怀疑者，由此能根据受怀疑者出现的频率识别出高度受到怀疑的人。当然，识别受怀疑的人的策略可灵活地加以定义，例如根据运营商网关的转发记录，或者利用用户申请授权时纪录的信息来判定某用户是否持有被盗版本的内容。识别高度受怀疑人的方法包括：根据受怀疑人拿到泄漏版本的频率来判定，以及根据受怀疑人在转发过程中所处的层级来制定怀疑度。识别出一组高度受到怀疑的人是初步跟踪阶段的目标，之后仅对高度怀疑的人进行附图 2 所示的专用跟踪步骤。

为此，例如运营商的网关：当一部分内容转发给高度受怀疑的人时，将一个特定的第二指纹嵌入到所述内容中。所述第二指纹不会影响到识别一级用户的第一指纹，并且能够唯一地识别所述受怀疑的人。当从高度受怀疑的人转发内容时，从所述内容中去除所述第二指纹，以便接收者能够得到一个“干净”的不带第二指纹的内容。因此，高度受怀疑的人实际上得到一个唯一的内容的版本。在采用第二跟踪阶段后，如果其他的泄露内容还包括所述第二指纹，则运营商可以确信哪个高度受怀疑的人是泄露点，实现了对盗版者进行精确的跟踪和识别。

由于只是对这些高度受怀疑的人才在第二跟踪阶段进行跟踪，对大多数通常的用户来说，在系统运营商一侧没有增加明显的附加工作，由此节省了大量的资源。

以上通过结合附图对本发明的具体实施方式进行了描述，但是以上这些实施例仅是示例的，本领域技术人员可以在本发明的精神和范围内作出各种变化和修改。因此，本发明不限于这些实施例，本发明的范围由随附权利要求限定为准。

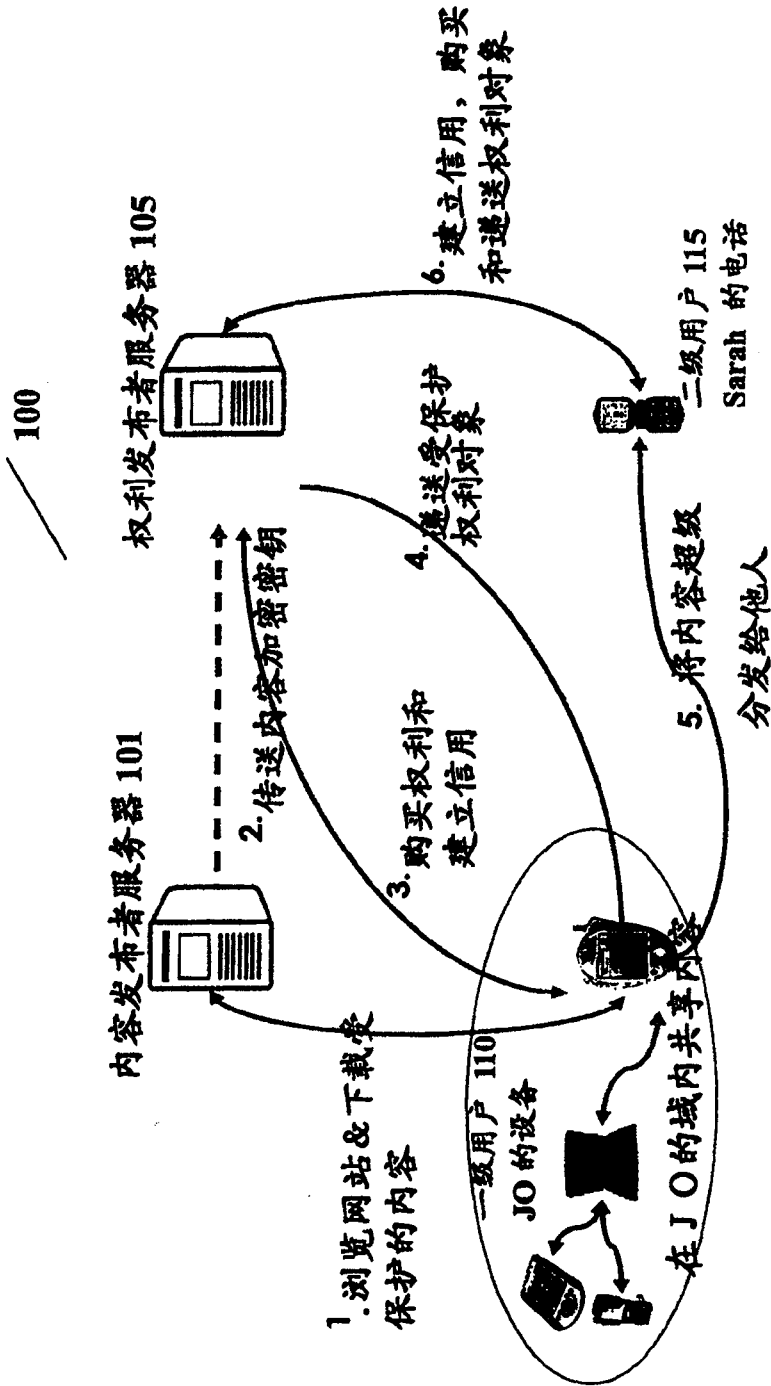


图 1

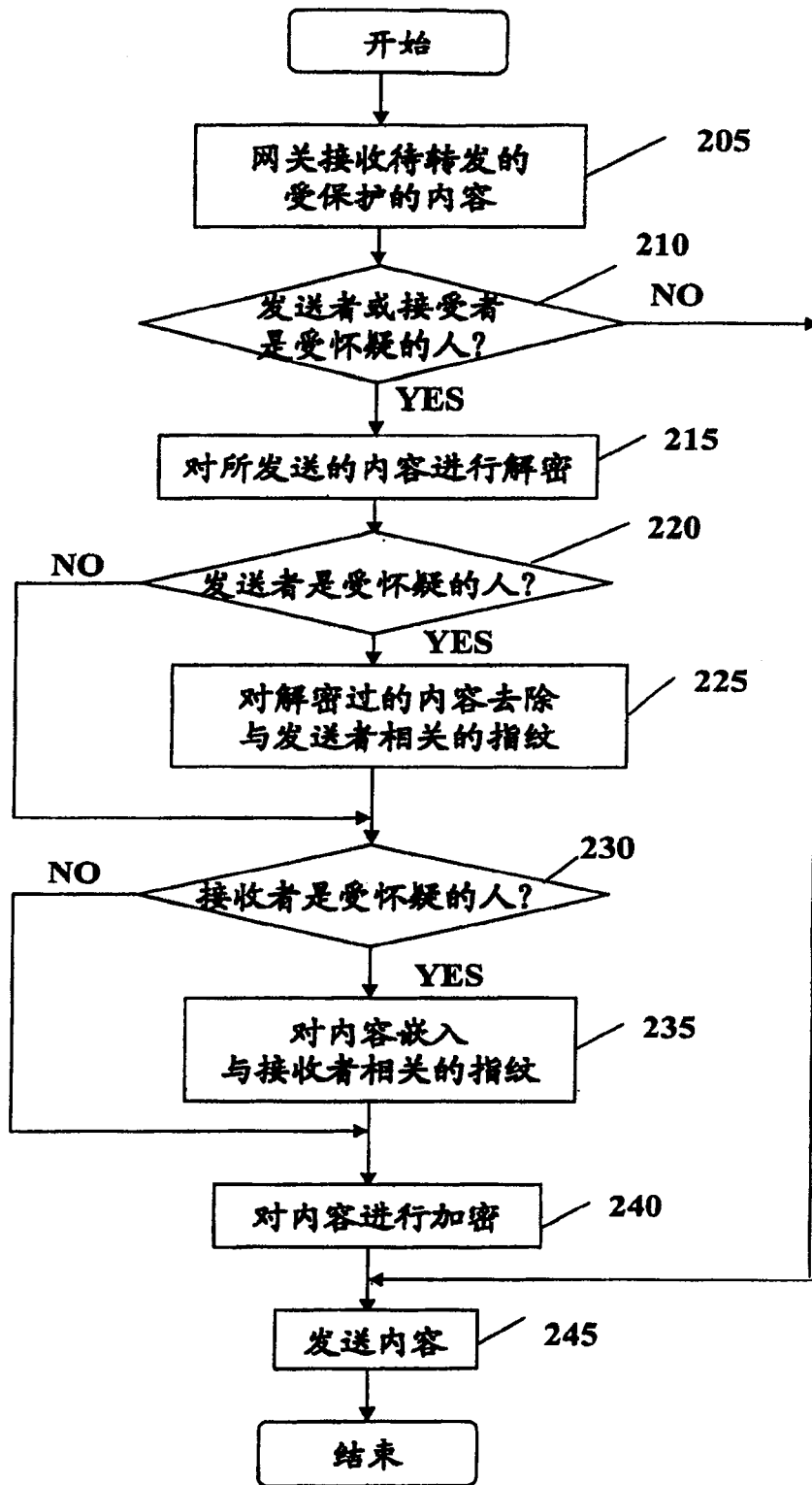


图 2

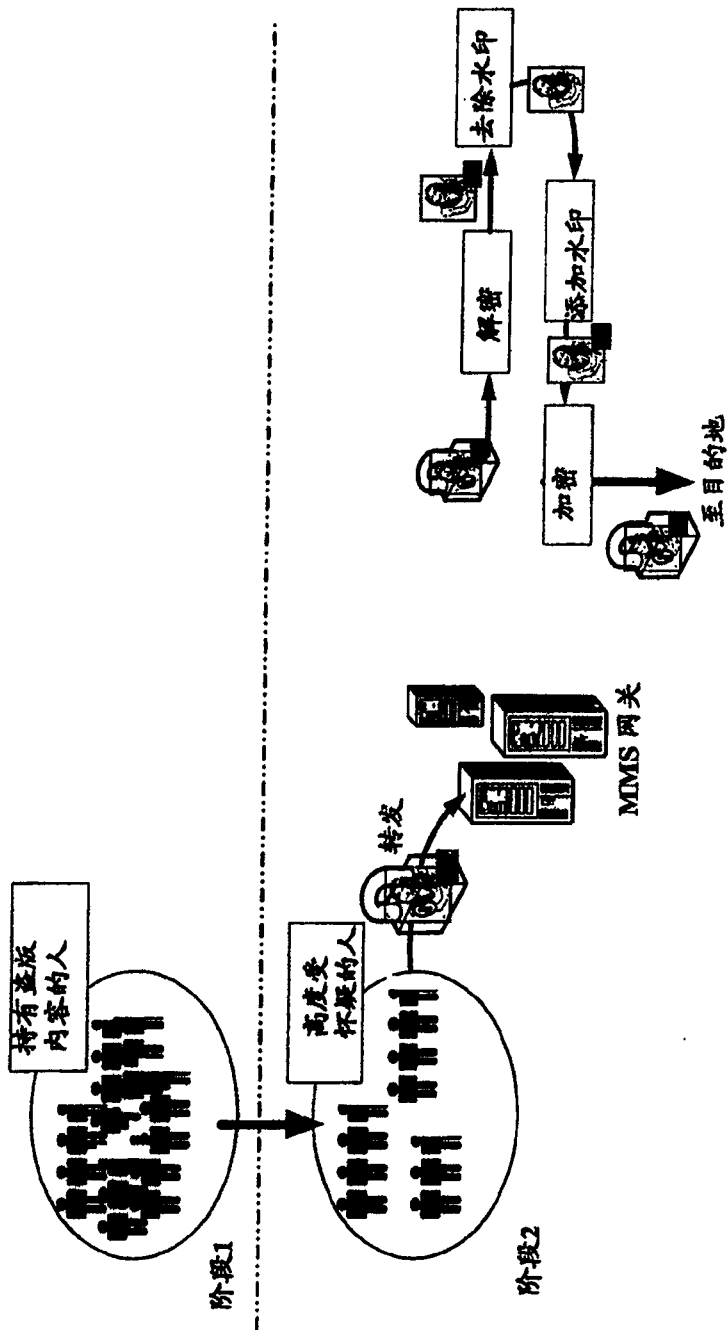


图 3