用激励机制下的分布式计算建立注册内容的搜索引擎

白皮书简介

Samuel Brooks
Veredictum

2017 年 7 月

摘要

盗版行为将视频和音频文件在版权所有者不知情的情况下从授权的给版权所有者带来收入的地方移动到其他给盗版者带来收入的地方，造成版权所有者的损失。及时发现这些行为是发出删除通知从而保护正当收入的关键。现代视 (音) 频隐码技术可以给数字内容打上水印，区块链技术可以永久地不可篡改地记录内容版权所有者对该内容的所有权。用中心化的方式下载并解码视 (音) 频文件来确定文件是否包含水印是非常昂贵的。本文探讨用分布式系统从开放互联网上下载并解码视频文件从而发现盗版视频和音频内容的可行性。

V0.9.3

参考实现有可能和本文描述的设计有些许不同

目录

1 简介

本文讨论一种标记和搜索互联网上的视频的全新方法。

由于互联网的客户-端服务器架构，追踪在线数字内容的动态是一个巨大挑战；文件存贮在不透明的远程服务器上，我们必须浏览、下载和检视文件的内容来了解特定的数字内容是否存在。而且，数字文件可以被轻易地并且经常地重新发布到不受控的未被授权的网站服务器上(数字盗版)。文件名可以被轻易更改，文件可以被压缩，视频音频文件可以被减采样，或用其他方式转换，仍然可供人们观看欣赏。

由于这样的客户端-服务器架构，遥测数字文件 (状态信息从远端配置的设备送回到中央服务器) 实际上是不可能的。 文件遥测需要远端设备配合安装额外的软件，发送它的所有数字内容的相关信息。并没有特别的激励机制让远端服务器的主人来发布准确的数字内容目录。

基于区块链的加密货币可以激励庞大网络的计算设备进行所谓工作量证明(proofs-of-work)[1]的计算工作。 在视频内容普遍被盗版的现实情况下 (比如在油管(YouTube)和脸书(Facebook)之间盗用)， 本文探讨一种激励机制下的对用现代隐码技术做标记的数字创意内容进行分布式搜索的技术可行性。它也包括通过分布式的计算机网络(而不是一个专门的中央服务器集群) 下载和处理互联上的数字内容，来发现盗版内容在互联上的分布情况。我们目前主要解决视频(包含音频)内容的盗版问题。

2 概观

2.1 问题陈述

视频盗版对于大的电影工作室和小的内容创造者来说都是巨大的附加成本。数项研究发现，仅对美国电影业，这项成本就达 200 亿美元 [2]。

2016 年，脸书(Facebook)产生了超过 300 亿美元的营业收入，但该社交网络上的 73%的最受欢迎视频 是从 YouTube 上盗版而来的[3]。这通常被称为 "Freebooting"。

目前，为了让 Facebook 移除内容创作者的被盗内容，内容创作者必须：

1. 首先被通知他们的原创内容被盗并重新上载到脸书(Facebook)了，然后
2. 完成一个冗长的在线表单，并且上传原版内容到脸书(Facebook)来证明他们的版权。

虽然油管-脸书(YouTube-Facebook)之间的互相盗版是这个问题的备受瞩目的实例(具有讽刺意味的是，最近一个讨论盗版问题的 YouTube 视频在 Facebook 上获得了更多的观看 [4])，但它并不是唯一的例子 [5]。一个消除这种低效率的解决方案将会大幅度减少在线视频内容的收入损失，为消费者带来更高质量的内容和更低的价格。

2.2 集中式的计算和分布式的计算

单个实体要在浩瀚网络上搜寻特定视(音)频内容需要手工复审无数文件。以 Facebook 为例，每天大约 1 Petabyte (1024 Terabytes)的数据会增加到它的服务器集群上，其中大约 1/3 是视频数据[6]。 为了验证这些视频的版权，这大约 3000 TB 的新视频数据需要每天被下载复审。使用中心化的云服务，像亚马逊云服务(AWS)，这样的分析需要大约 10 万美元一天[7]。

2.3 解决方案概述

本文探讨用分布式网络上被激励的计算节点进行内容下载和复审的技术可行性。本系统依赖于对数字文件的隐码预处理(水印)和公开区块链上的所有权注册。对可疑的提供有版权内容的搜索空间(某地理区域部署的一系列内容服务器)进行内容搜索、下载和复审将会提供何时何地内容被(合法地和非法地)发布的轮廓。

我们的系统由以下两个关键阶段定义：

1. **内容编码和注册：** 第一个阶段，内容在中心化的服务器上用一个唯一标识编码。然后我们在公开区块链(比如以太坊 Ethereum)上记录内容版权所有者对该内容(由唯一标识确定)的所有权，再将内容发布到指定目标。
2. **内容搜索和报告：** 我们假设非常可能发生一些盗版事件。我们用一组被激励的计算节点搜索、下载并复审一定数量的可疑视频文件，把结果报告给这项服务的购买者。这个阶段部分是中心化的，部分是分布式的。

我们关于互联网上可用的计算和带宽资源的边际成本做了一些假设，提出一个利用它们建立注册内容的搜索引擎的可行方案。我们受到以太坊(Ethereum)的启发，描述一种激励机制来保证计算结果有很高的可靠性。

随着分布式技术生态系统的成熟完善，最终有可能让目前中心化的操作完全以分布式的方式进行。我们把这种可能性留给将来的工作。

3 顶层解决方案

3.1 定义

3.1.1 数字内容和文件

我们区分开数字*内容*和数字*文件*。内容是静态的，不可变的；文件是多形态的，可变的。文件只是内容的容器。文件的特性可以有很大的改变，而内容的属性保持不变 (例如，一个音乐文件可以被减采样，文件名和文件类型都可以改变，但文件包含的内容依然是 Chuck Berry 唱着 Johnny B. Goode)。

3.1.2 客户端和服务器

我们把计算节点从中心服务器下载用于参与到系统中的应用程序称为“客户端”。

我们把集中式的用于协调指挥的服务器(或服务器的集群)简单称为“服务器”。

3.1.3 角色定义

3.1.3.1 服务订户

服务订户是指为搜索功能付费的客户。我们设想搜索费用将以订阅方式收取，这样可以提高搜索节点获得报酬的确定性。

3.1.3.2 节点

节点是指参与到分布式计算网络中的一台计算设备。他们也可以被称为“矿工”，跟比特币圈子对比特币网络节点的称谓一样。我们设想每个客户端/节点对应一个账号，如果单个人或公司控制多台计算设备，他们将有多个账号 (通常一台计算设备运行一个客户端程序，但是如果计算设备足够强大，一个客户端程序可以有多个虚拟机运行)

3.2 解决方案各阶段

3.2.1 内容编码和注册

内容注册过程如下。我们假设这些任务都是可操作的，本文主要讨论分布式的搜索引擎。我们内部的隐码技术抗破解测试结果也会列出：

- 安全地建立希望注册新的创意内容的内容拥有者的账号
- 生成内容的唯一标识符
- 把新生成的唯一标识符用隐码技术嵌入到文件中

- 用智能合约在公开的区块链上注册内容拥有者对内容的所有权(通过建立内容拥有者账号和内容唯一标识符之间的所属关系)
- 发布文件到授权目标

3.2.2 内容搜索和报告

搜索阶段包括：

- 抓取感兴趣的服务器上的视频文件，形成一个列表(搜索空间)以供下载。
- 对视频文件按照包含水印的可能性进行排序，对有更高可能性的视频优先处理。
- 把搜索空间分成一系列区间，让每个区间可以被单个节点在合理时间内下载并处理 (比如每个区间 1GB).
- 雇佣一系列节点对每个区间下载并处理。
- 节点把处理结果返回给中心服务器来创建一个包含水印的文件列表。

3.3 视频隐码技术

视频隐码技术可以在视频中隐藏信息。现代隐码技术可以在视频文件中嵌入一个不可察觉的内容标识符。这就提供了一种标记内容的方法。这个内容标识符可以通过解码从视频中恢复出来，结合区块链上的内容版权所有者对该标识符的所有权记录，就能声明版权。由于区块链上的记录不可篡改的特性，这样的声明非常有力。

为了让打上水印标记的视频有价值，它必须和原视频有相同的质量，同时能在被转换格式或翻录的过程中有效地保持水印标记。

现代隐码技术可以做到以上。它对视频质量的影响无法察觉，同时具有很高的抗转换能力(抵抗强度跟视频质量指数正相关，视频分辨率音频采样率越高的视频越难被转换格式发现水印)。这意味着 除非把视频质量降到不可观赏的地步，很难发现水印。

我们的隐码软件的测试结果将会在第 5 节提供给大家。

3.4 搜索空间准备

数字内容的搜索空间会被索引产生目标 URL 的列表以供进一步处理。这一过程首先利用网络爬虫产生一个视频文件的索引。该爬虫根据为我们的应用优化的条件进行数据抓取，比如不跟随超链接，仅仅索引种子域名。

搜索空间的范围是有限但并非固定的，以使发现标记数字内容的可能性最大。这可以通过，比方说，优先搜索那些特别可疑拥有未授权内容的特定域名或子域名。贝叶斯法则以及机器学习算法可以用来改善搜索优先级和搜索策略来尽可能地缩小搜索空间，来减少需要的计算资源。我们可以用 Web 服务器或特定子域名的“盗版名声”，或者社交网路上特定用户的盗版行为历史记录来作为重要参数。

一旦搜索空间准备好了，它将被分段，提供给分布式计算网络上的客户端处理。

3.5 客户端下载、配置和连接

参与分布式计算网络的用户从中心服务器上下载并安装一个应用程序(“客户端”)。 校验码会被用来确认软件的真实有效，我们需要获取应用程序运行时的内部状态的快照 —— 具体细节请参看后面章节可验证计算的部分。校验码确认过程可以作为安装的一部分被自动化。

客户端包含一个轻量级的虚拟机，负责和中心服务器的交互，同时也负责和公开区块链上的智能合约的交互。客户端也提供用户界面，管理文件下载，以及虚拟机的状态散列。

用户需要从客户端登录来确保用户帐户有足够的虚拟货币作为参与分布式网络的保证金。这是为了防止作弊，比如女巫(Sybil)攻击——参见后面的攻击列表章节。获取加密货币的过程超出了本文的讨论范围，但至少可以通过延迟释放一部分赚取的加密货币，直到保证金数额达到后开始释放的方式做到。客户端也被设计成可扩展的；如果用户有更多的计算资源，客户端可以启动更多的虚拟机来充分利用可用的资源。这将同质化网络上的节点，从而简化重执行设计中计算资源的匹配，同时也让更多的连接组合成为可能(更好的随机性)。

一旦用户建立了服务器连接，客户端会把用户定义的设置以及设备上的硬件资源发送给服务器。

一旦隔断时间到了，服务器会

1. 停止接受客户端连接，但会让客户端连接请求进入队列等候。搜索“周期”是指有限的文件集合被下载并处理，一定数量的加密货币从服务订阅者转移支付给分布式网络上的节点的时间段。
2. 盘点网络上所有的计算能力并分配子网络：节点被分成小组(比如 3 个一组)搜索同一个搜索空间的分段(子搜索空间)。分组方式要经可能减少共谋的可能性，比方说，从三个不同的地理位置各随机选择一个节点。子网络被随机编号。特殊情

况下，子网络数量会超过搜索空间的分段数量，如果这种情况发生，多余的子网络会被分配到下一个搜索周期。我们不认为子网络会需要等待超过一个搜索周期。

3. 和客户端通讯，为他们提供 URL 列表(子搜索空间)。到这一步，子网络和子搜索空间是一一对应的。

子网络中的节点并不需要相互连接；服务器甚至不会提供哪些节点在同一个网络中的信息。子网络的节点数量甚至可以降到 2 以下，子网络中有 1.5 个节点意味着，每个节点的一半计算结果会用另一个节点的计算结果验证，比方说，节点 1，2，3 形成两个子网络，节点 1 处理子搜索空间 A，节点 2 处理子搜索空间 B，节点 3 处理一半的子搜索空间 A 和子搜索空间 B。

3.6 客户端处理

所有连接到分布式网络的计算节点利用它们的带宽和处理能力来下载和处理被分配到的子搜索空间。

为了验证节点计算结果的正确性，不返回假的结果，虚拟机的状态会被散列形成一系列 Merkle 树。这些 Merkle 树的根会通过一个事务被发送到公开的区块链，用智能合约记录并相互比较。如果子网络上所有节点的 Merkle 树的根是相同的，那就意味着，要么所有节点的计算都是正确的，要么它们互相串通好了欺骗这个系统。攻击和计算结果的验证将在本文后面的部分探讨。

一旦被分配的搜索空间处理完毕，被恢复的内容标识符最终被送回给服务器进行比较，如果结果一致，则认为结果有效，客户端就等待下一个搜索周期的到来。

3.7 虚拟化的文件遥测

在分布式网络解决了所有子搜索空间的文件标识符之后，中心服务器会把所有结果保存到数据库。该数据库就包含了哪些内容存在于哪些服务器上，可供服务订阅者查询。为了保护隐私，服务订阅者只能查询和自己的内容有关的信息。该信息可以被用来自动发送 DMCA (数字千年版权法) 删除通知到有盗版内容的服务器，或者发送律师函，该律师函基于简单的指标，比如该视频已经被观看了多少次。罚金可以由用户手动设置成任意金额。

总结一下，网络编配管理以下过程：

- 用户下载客户端和基于用户名密码的身份验证

- 客户端检查系统是否在运行其他客户端
- 如有必要，提交保证金
- 客户端收集设备硬件信息，网络连接信息，以及用户设定，并提交给服务器。
- 服务器创建一个子网络池和一个排序的搜索空间，把搜索空间分段成子搜索空间，并分配给各个子网络中的节点。
- 客户端下载并处理这些 URL，并提交状态信息。
- 服务器收集分布式网络的计算结果，形成一个可搜索的关于注册内容所在 URL 的数据库。

3.8 客户端补偿

搜索请求者(希望搜索自己内容的人)和服务提供者(进行下载和解码的节点)之间通过加密货币进行价值传递。这个价值传递过程由智能合约管理。计算任务开始之前，服务器会把费用存到合约指定的账户，从而保证每个计算节点会在完成计算后获得报酬。一旦成功完成传送它们的状态，节点的账户会被更新为有一个待确认的支付。支付被延迟一段时间，这段时间内服务器会验证计算结果的真实性。

智能合约也会保管所有参与节点的保证金。服务器会在提供子搜索空间给节点前验证保证金。保证金的作用是在节点提交虚假信息的情况 (比如状态信息和子网络的其他节点不一致)下作为罚金。

我们通过智能合约(而不是通过中心服务器)进行状态信息的交叉验证。这非常重要，因为这将决定客户端是否进行了正确的计算，只有当子网络中所有节点的状态一致时，智能合约才会触发支付。

如果合约正确执行，在一段时间后，每个节点的账户将被更新(账户的数字钱包中的加密货币数量将会增加)。这个时候，赚取到加密货币的人就可以在交易所卖给要使用搜索服务的人。

3.9 系统组件

我们的系统在逻辑上包含以下的软件组件：

- **Web 应用程序** (用于用户和系统的交互)
- **转码器** (把内容标识符嵌入视频的应用程序)
- **注册器** (注册内容版权的智能合约)
- **索引程序** (搜索空间的网络爬虫)
- **排序程序** (搜索空间的排序算法程序)

- **协调器** (协调分布式节点的中心化的服务)
- **客户端** (分布式节点上运行的应用程序)
- **仲裁者程序** (进行状态匹配和管理保证金及支付的智能合约)

这些会在技术白皮书中逐一探讨。

4 参考文献

[1] filecoin.io, “Filecoin: A Cryptocurrency Operated File Storage Network,” 2015.

[2] C. Bialik, “Putting a Price Tag on Film Piracy,” 5 Apr 2013. [Online]. Available: https://blogs.wsj.com/numbers/putting-a-price-tag-on-film-piracy-1228/.

[3] Tubular Labs, “The Rise of Multi-Platform Video: Why Brands Need a Multi-Platform Video Strategy,” Social@Ogilvy, 2015.

[4] Kurzsegagt, “How Facebook is Stealing Billions of Views,” 10 November 2015. [Online]. Available: https://www.youtube.com/watch?v=t7tA3NNKF0Q.

[5] L. Overweel, “Stop Freebooting Now,” [Online]. Available: http://stopfreebootingnow.com/#wall.

[6] Facebook, “Facebook’s Top Open Data Problems,” October 2014. [Online]. Available: https://research.fb.com/facebook-s-top-open-data-problems/.

[7] Amazon, “AWS Cost Calculator,” 2017. [Online]. Available: https://calculator.s3.amazonaws.com/index.html.