抗共谋数字指纹实现问题研究

周国瑞[1] 孙世新[1] 王文江[2]

(电子科技大学计算机科学与工程学院 成都 610054)[1] (龙旗科技(上海)有限公司工程部 上海 200233)[2]

摘 要 与数字指纹相关的指纹编码、嵌入、共谋用户识别3个环节已有一定研究成果。若数字指纹走向实用,则还需解决一个问题:抗共谋数字指纹实现问题。详细阐述了该问题的涵义;分析了抗共谋指纹编码、内容分发机制及终端消费环境对该问题的影响并探讨了相关解决方法;从通信代价、计算及存储代价等软硬件成本、安全性及实时性等方面对现有典型抗共谋数字指纹实现算法的性能进行了比较分析;最后,讨论了该领域的未来研究方向。

关键词 数字指纹,共谋攻击,数字版权管理,多播通信

中图法分类号 TP391 **文献标识码** A

Research on the Realization of Anti-collusion Fingerprinting

ZHOU Guo-rui[1] SUN Shi-xin[1] WANG Wen-jiang[2]

(School of Computer Science and Engineering, University of Electronic Science and Technology, Chengdu 610054, China)[1]

(Engineering Department, Longcheer Co., Ltd, Shanghai 200233, China)[2]

Abstract Considerable progress has been made in fingerprinting technology, particularly with regard to fingerprinting codes, embedding methods and colluder identification. But applying fingerprinting technology to engineering, it faces the problem on how to realize anti-collusion fingerprinting in real system. The concept of anti-collusion fingerprinting realization was introduced firstly, and then effects of three factors on it were studied. These factors are anti-fingerprinting codes, content delivery system and user's multimedia consumption pattern. The trade-off strategies between these factors and the problem were proposed. Some major anti-collusion fingerprinting realization algorithms were reviewed. Their performance was analyzed from following aspects: communication price, hardware and software costs which include computing and storage price, safety and real-time characteristics, etc. Finally, the future trend of the problem was discussed.

Keywords Digital fingerprinting, Collusion attack, Digital rights management(DRM), Multicast communication

1983年,Wagner首次提出数字指纹技术[1]。1985年,Blakley等人提出了共谋攻击[2],这是一种十分有效的攻击。1998年,Boneh和Shaw提出了BS码[3],从而大大推进了抗共谋数字指纹技术的发展。近年来,在抗共谋数字指纹技术的指纹编码、嵌入、共谋用户识别等方面,已有诸多理论成果,具体可参阅文献[3-19]。若使该技术走向实用,还需解决一个问题:实现问题。它是抗共谋数字指纹技术从理论走向实用不可避免的环节。

本文旨在结合抗共数字指纹编码、内容分法机制及终端消费环境,探索与基础设施、日新月异的通信技术的有机结合,以便很好地平衡授权用户、内容提供商、内容运营商三者间利益关系的抗共谋数字指纹实现问题。第1节详细阐述了该问题的涵义。第2节介绍了媒体生存周期及承载机制现状。第3节以寻找把承载机制差异屏蔽掉的抗共谋指纹实现模式为出发点,以带宽有效、减少终端负载为核心,对抗共谋指纹的实现问题进行了深入探讨,对比了现有典型算法的性能及各自的优缺点。最后讨论了进一步的研究方向。

1 抗共谋数字指纹实现

每个授权用户的数字指纹都是(n,M,q)-编码[4]中的一个码字[3]。

定义1 抗共谋数字指纹[3]

对于一种(n,M,q)-编码方案,如果存在一种追踪算法A,对由至多t个授权用户组成的共谋集团U所伪造的同一数字产品的任意拷贝y,都有$A(y)\in U$,则称该数字指纹为抗t个人共谋的数字指纹。

定义2 抗共谋数字指纹实现

恰当选择指纹嵌入媒体的时机,并把含指纹媒体有效地、安全地分发给授权用户。

由定义2知,抗共谋数字指纹实现包含3方面内容:1)选择指纹嵌入媒体的时机;2)把含指纹媒体有效地分发给授权用户;3)把含指纹媒体安全地分发给授权用户。三者相互关

到稿日期:2009-02-27 返修日期:2009-05-07

周国瑞(1974-),女,博士研究生,主要研究方向为信息压缩、小波理论、图形图像、数字水印等,E-mail:mimi5988@126.com;**孙世新**(1940-),男,教授,博士生导师,主要研究方向为信息压缩、并行/分布式计算等;**王文江**(1974-),男,高级工程师,主要研究方向为图形图像、3G移动通信等。

联相互影响。具体将在第 3 节进行讨论。

抗共谋数字指纹实现问题的实质就是在一定环境中，解决抗共谋指纹信息的有效安全分发问题。一定环境由内容分发机制、终端消费环境等所构成。目前，媒体传送平台等硬件基础设施已经基本成型，对其进行大的改动不太可行。如何结合现有的蓬勃发展的媒体内容分发机制、终端消费模式，从前端到终端的诸多环节中，合理引入指纹实现过程，是解决问题的关键。有效安全分发可由授权用户、内容提供商及运营商的满意度来衡量。只有照顾了三者利益的设计，才是实际可行的解决方案。三者利益关系在第 2 节进行讨论。

2 媒体生命周期与承载机制

2.1 媒体生命周期

媒体生命周期[20]见图 1，家庭网关为可选项。合法的媒体生命周期不包括“盗版非法传播”环节。在整个生命周期中，经过的流通环节有：前端、通信信道、终端；所涉及的利益实体有：内容提供商、运营商、授权用户，其利益关系见图 2[21]。对于内容提供商、运营商来说，媒体版权保护是重中之重，非授权用户无法使用媒体，授权用户只能正常使用媒体且不能进行授权之外的侵权。而对于授权用户来说，获取授权之外的利益可能很具有诱惑力。

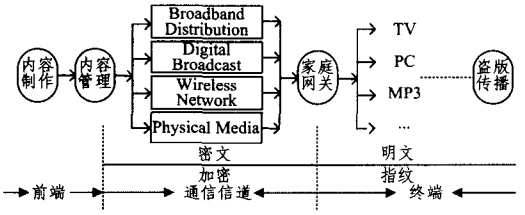

图 1 媒体生命周期示意图

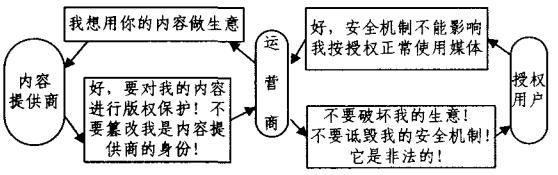

图 2 内容提供商、运营商、授权用户之间的利益关系

由于在生命周期的各环节进行侵权操作及逃避追踪的难易程度不同，因此导致不同环节发生盗版的概率不同。前端盗版概率最小，通信信道及终端盗版的概率相对较大。通常，通过加|解密技术实现连接及链路保护，对合法用户获得的解密明文采用指纹技术进行保护。两种技术的作用区间示意在图 1 中标出。原则上，一旦媒体被解密，媒体就进入数字指纹技术的保护范围。

2.2 承载机制

媒体的承载机制由内容分发机制和终端消费机制所构成。

目前，运营商提供的几种典型内容分发机制有：1）介质：采用 VCD/DVD 光盘形式；2）DTV（Digital TV）；3）下载播放；4）在线 DVD；5）IPTV（Internet Protocol TV 或 Interactive Personal TV）；6）移动媒体。其中 4）—6）支持流媒体，与下载播放相对应，客户端在播放前并不需要将媒体文件完整下载，而是在将缓存区中已经收到的信息进行播放的同时，媒体文件的剩余部分在持续不断地从服务器下载到客户端，即“边下载，边播放”，给用户带来“实时播放”的业务感知体验。具体承载网络[22]，从结构上可分为：serve-client[23]，P2P[23]，CDN[24]，CDN 与 P2P 融合[25]等。

终端消费设备有：电脑、电视、手机、MP3、DVD/VCD 等。消费方式分为离线消费和在线消费。特别地，不同终端所支持的媒体编码格式不尽相同，从不同内容分发机制获得的媒体格式也不尽相同，为方便媒资共享，提出了数字家庭的思想，家庭网关被引入（见图 1）。转码是家庭网关的主要功能之一[26]，网关检测到所接收的数据类型与用户终端默认类型不匹配时，自动进行转码。

数字媒体内容分发机制的多样、终端消费形式的丰富，为用户在不同时间、地点以及应用场景中使用媒体带来了方便，因此将会长期并存，并随着相关技术的发展而发展。在设计抗共谋数字指纹实现算法时，需要与这些基础设施、媒体消费环境相结合，才能设计出实用的方案。

3 抗共谋数字指纹实现方法

为了实现数字指纹对媒体的保护功能，必须保证授权用户仅能够获得已经含有指纹的媒体明文，见图 1。这就需要在从前端到终端的诸多环节中合理引入抗共谋数字指纹的实现过程，本节就引入环节及带来的影响进行分析。采用介质或单播机制的网络，指纹实现问题比较简单，而采用 broadcast，multicast 机制的网络及 P2P 网络，指纹实现问题会就很复杂。其实，结合实际环境解决数字指纹实现问题，从通信角度讲，就是在传输媒体信息的基础上，增加传输用户指纹信息；从安全角度讲，就是把信道安全通信技术与数字指纹技术紧密结合，防止没有任何保护的媒体明文在这种环境下泄露；从计算存储代价角度讲，就是尽量解决好媒体信息传输与指纹传输的同步问题，减少用户端缓存开销及计算代价。因此，在评价算法性能时可以从通信代价、安全性、软硬件成本等方面进行。

3.1 介质

对于介质形式提供的媒体，可先在媒体中嵌入指纹，再制作成光盘分发。

3.2 unicast 环境

指纹嵌入媒体的时机宜选择在 serve 处进行。如果指纹嵌入操作不影响 unicast 和终端用户的实时下载，可采用边嵌入指纹边下发数据的方式；如果影响，则可采用 AFR_unicast 算法。

AFR_unicast 算法的基本步骤为：

1）根据指纹长度把媒体 X 进行分段，不妨设分成 L 段；

2）根据指纹字母表 $\Omega=\{0,1,2,\cdots,q-1\}$，每段都复制 q 次并依据某种数字水印嵌入算法，分别嵌入信息 $0,1,\cdots,q-1$，形成每段 q 个含指纹信息的复本，存储在 serve 处，见图 3。

3）当 client 请求服务时，根据用户指纹，serve 挑选含指纹信息的段复本进行组合，组合成含用户指纹的复本，下发给用户。

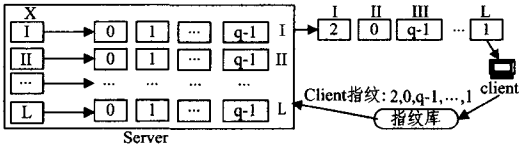

图 3 Unicast 环境指纹实现示意图

依据 AFR_unicast 算法，serve 处的存储开销为原始媒体 X 的 q 倍，以增大 serve 处存储开销为代价，来满足 unicast 和终端用户的实时下载要求。

3.3 multicast 及 broadcast 环境

multicast[27] 及 broadcast 环境能把相同信息广播给多个用户。在这种环境中，如何传输指纹信息呢？加载指纹信息后，引入多少通信代价增加呢？可以借助 γ，γ^{fm} 参数对指纹实现算法的通信性能进行定量分析[27]。下面仅给出 multicast 情况下的计算公式，broadcast 情况与此类似。

$$\gamma(M)=\frac{C^{fm}(M)-C^{mo}(M)}{C^{mo}(M)}\times 100\% \tag{1}$$

$$\gamma^{fm}(M)=\frac{C^{fm}(M)}{C^{pu}(M)}\times 100\% \tag{2}$$

其中，M 是 multicast 用户组大小，$C^{mo}(M)$[27] 是“multicast only”通信代价，$C^{fm}(M)$ 是解决指纹实现问题所需的通信代价，$C^{pu}(M)$[27] 是“unicast”通信代价。$C^{fm}(M)$ 依据指纹实现算法所使用的通信量来计算。其实，γ 是同“multicast only”相比，引入指纹信息传输后通信代价增加的百分比；γ^{fm} 是与“unicast”通信代价的比例。

3.3.1 前端嵌入指纹

出于减少终端负载考虑，指纹与媒体的结合选择在前端进行。基于 multicast 及 broadcast 的广播特性，提出了 JBFE 算法和 JBFD 算法。由于是广播环境，两种算法都使用加解密操作，使非授权用户无法解密。

JBFE 算法

JBFE 算法[28] 的基本步骤如下：

1)同 AFR_unicast 算法第 1)步；

2)同 AFR_unicast 算法第 2)步；

3)用 $q\times L$ 个密钥分别加扰 $q\times L$ 个含指纹信息段；

4)发给每个授权用户唯一 L 个解扰密钥；

5)把第 3)步加扰后的信息段广播给所有用户；

6)授权用户用所接收到的解扰密钥，对所接收的加扰信息段进行解扰。

由于每个解扰密钥仅能解扰 $q\times L$ 个加扰信息段中的一个，因此，每个授权用户用所接收的 L 个密钥就能从广播信息中解扰出 L 个信息段，并且在 L 唯一的情况下，解扰的 L 个信息段也是唯一的。实质上，每个授权用户所获得的这些解扰信息段(明文)已经是含有该用户指纹的媒体了。

JBFE 算法优点：

1)解扰与指纹实现过程之间不存在安全漏洞；

2)终端用户不必为指纹的嵌入准备额外的软硬件；

3)在解扰密钥层进行共谋，也可以抓获共谋者；

4)广播数据量与用户量 M 无关。

JBFE 算法缺点：

1)对于 q 值指纹[3,4]，广播数据量不低于媒体长度的 q 倍；对每个授权用户来说，在所接收的广播数据中，仅有 $1/q$ 数据量与自己有关，其它 $(q-1)/q$ 浪费。此时，$\gamma>q-1$。

2)密钥更换时间，决定指纹长度。

在现有 DTV 系统中，CW 控制字更换时间间隔为 2～10 秒，不妨用参数 t 表示该时间间隔，在该系统中使用 JBFE 算法，则需要每段视频的最小时长为 t 秒，1 小时视频最多能分成 $3600/t$ 段。因此，1 小时视频可嵌入的最大指纹长度为 $l=3600/t$。若 $t=2$，则 $l=1800$，而现有文献[3,9,12,29,30]给出的抗共谋指纹编码长度远大于 1800。

当 $c\leqslant 3$ 时，Sebé 等[31] 给出的指纹长度最短，计算公式为：$l=(N-1)(2t+1)d$，其中 t,d 为固定常数，可分别取为 5，N 为发行用户量，l 为指纹编码长度。依据该公式，当 $l=1800$，$c=3$ 时，则 $N\leqslant 33.7273$。由此可见，除非 CW 控制字更换时间能够进一步缩短，否则，此算法难以用于现有广播系统中。

Chu 等[32] 指出，在 CW 字更换没有特殊时间限制的环境中，若分段能以每帧为单位，则使用二值 BS 码[3]，在 2 小时视频，10000 用户，至多抗 3 个人共谋的情况下，JBFE 算法可实现以 90% 正确的概率抓获一个叛逆者。

JBFD 算法

把 JBFE 算法中的分段思想改为细分数据思想，媒体数据流分为两部分，一部分是与指纹无关的数据，用密钥 K^m 加密后广播给所有用户；另一部分是用来携带指纹信息的数据，在该部分数据中嵌入指纹信息形成个性化流，用用户密钥加密后，单播[27,33]，在保证个性化流不被其它用户解密的情况下，也可以采用广播，不同用户依据密钥摘取自己的个性化流，见图 4(a)。

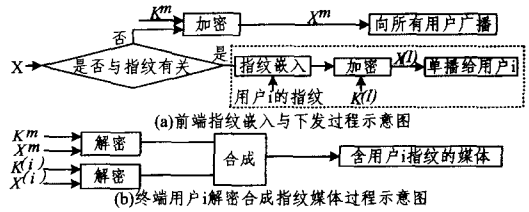

图 4 JBFD 算法指纹实现过程示意图

在图 4(a)中，设多播数据 X^m、单播数据 $X^{(i)}$ 的比特流长度分别为 len^{fm}_{multi}，len^{fm}_{uni}，则 JBFD 算法所需的通信代价为：

$$C^{fm}(M)=C^{unit}_{multi}(M)\times Len^{fm}_{multi}/Len^{unit}+M\times C^{unit}_{uni}(M)\times Len^{fm}_{uni}/Len^{unit} \tag{3}$$

结合式(1)、式(2)，可计算出 γ，γ^{fm}。从式(3)及图 4(a)不难看出，len^{fm}_{uni} 越小，由指纹信息传输引入的通信代价越少。依据文献[27]中个性化流形成方法，仿真测试结果显示，一般指纹多播算法的 γ^{fm} 通常在[16%，52%]范围内，γ^{fm} 受 M 和媒体特征影响，并随着 M 的增大逐渐下降；γ 在[10%，40%]范围内受媒体所携带指纹信息量的影响。

Zhao 等[27] 提出一种结合树结构指纹编码的指纹实现算法，意在减少 JBFD 算法的单播数据量。虽然该算法的通信代价有所下降，但增加了前端的多播群组管理代价及终端侦听信道的数量。Zhao 等[27] 进而提出了在一定多播群组管理和侦听信道数量限制下的指纹实现算法，但其计算量明显增加。

若要 JBFD[27,34] 算法在通信代价上优于 JBFE 算法，需要满足[34]：

$$(c-1)\times\lambda<1 \tag{4}$$

其中，$\lambda=\dfrac{len^{fm}_{uni}}{len^{fm}_{uni}+len^{fm}_{multi}}$，$c$ 为抗共谋人数。

使用 JBFD 算法，终端需要接收 X^m 与 $X^{(i)}$ 两路流，使用 K^m 与 $K^{(i)}$ 两种密钥，且安装具备两路流合成功能的软件，才能正确解密合成出含指纹媒体。通过合理安排前端下发 X^m，$X^{(i)}$，K^m 及 $K^{(i)}$ 的时间，可以降低终端存储开销。使用该算法，终端用户获得的媒体明文数据一直处于保护之中，安全级

别高。另外 JBFD 算法支持的指纹容量较大。指纹容量指的是可嵌入到媒体中的最大指纹位长度[34]。

3.3.2 终端嵌入指纹

指纹与媒体的结合选择在终端进行，前端不需要做较大改动。前端对媒体加密后，广播下发。终端用户需要解密并进行指纹嵌入操作，见图 5(a)。图中，K'为加密密钥，K 为解密密钥，F_i 为用户 i 的指纹，X_i 为含 F_i 的媒体，D 为解密操作模块，EF 为指纹嵌入操作模块。使用此方式，除了要考虑终端嵌入指纹所需的软硬件开销、实时性、可升级性、成本等因素外，最关键的是安全问题。如果 D 与 EF 是两个独立的过程，则用户可对两个过程的连接处进行攻击，截获解密后未嵌入指纹的媒体，见图 5(a)。另外，此方式下，终端出现指纹明文，这样会造成指纹泄露，引发伪造等攻击。为增加安全性，可以考虑：1)把两个过程固化在一个芯片或电路中[35,36]，且确保指纹明文仅在虚线框内出现，见图 5(a)，此方法需要硬件支持，且安全级别比较低，但算法设计简单。2)两个过程设计为一个原子过程，即解密的同时完成指纹嵌入(JFD:joint fingerprint and decryption)，见图 5(b)，K_i 既控制用户 i 的媒体解密又控制指纹嵌入。此方法的优点是安全级别高。缺点是算法设计相对困难，指纹的嵌入量可能受限；用户可进行密钥级共谋攻击(Key collusion)[37]，但可以用抗共谋数字指纹编码来设计密钥予以抵抗。下面给出 JFD 方案的两种典型算法及其性能分析。

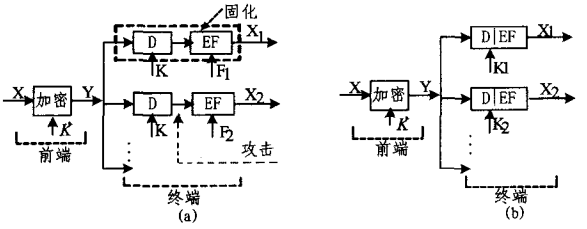

图 5 终端嵌入指纹示意图

算法 JFD1 Mask-based fingerprinting scheme for digital video broadcasting[38]

指纹加密下发，指纹嵌入与媒体解密过程融为一个原子过程，见图 6。

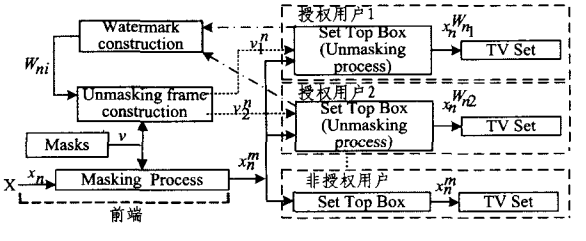

图 6 JFD1 算法实现过程示意图

算法基本过程如下：

1)产生 v(mask frame)

v 的大小与视频帧大小一致。为了提高安全性，过一段时间后应对其进行更新。

2)Masking process(相当于加密过程)

根据媒体的存储格式选择是空域还是压缩域进行 Masking process，形成的结果 x_n^m 采用广播形式下传。

空域 Masking process：

记视频第 n 帧为 x_n，与 v 按式(5)进行运算形成 x_n^m：

$$x_n^m(k,l)=\alpha x_n(k,l)+\beta v(k,l),\ \forall k,l \tag{5}$$

其中，$\alpha+\beta=1$，α,β 为尺度因子，(k,l)为像素位置坐标。

压缩域 Masking process：

通过对压缩流进行半解压及压缩操作，获取等效于式(5)的处理效果，具体操作方法见文献[38]。

3)Watermark construction

用户指纹在用户请求媒体并经过认证后产生，扩频调制和尺度缩放后形成与视频帧同样的大小。设为用户 i 产生的嵌入于视频第 n 帧的 watermark 为 W_{ni}。

4)Unmasking frame construction(相当于构造解密密钥)

$$v_i^n(k,l)=\beta v(k,l)-\alpha W_{ni}(k,l),\ \forall k,l \tag{6}$$

v_i^n 通过安全信道单播给终端用户。在图(6)中，用 v_1，v_2 替代 v_i^n，分别表示传给用户 1 及用户 2 的解密密钥。

5)Unmasking processing(相当于解密过程)

$$x_n^{w_{ni}}(k,l)=\frac{1}{\alpha}(x_n^m(k,l)-v_i^n(k,l)),\ \forall k,l \tag{7}$$

算法性能评价

优点：1)实现了指纹的加密传输，终端用户无法得到指纹明文；2)广播系统中用户的动态加入更方便，即用户加入系统时，引发 watermark construction 构造用户指纹。

缺点：1)额外传输了 v。前端除了传输指纹和媒体数据到终端外，还额外传输 2 次 v，随指纹传输一次，随媒体传输一次。这样做的目的是实现指纹、媒体的加密传输。v 的参与，导致广播数据量比原来增大了 0.001%～0.4%。当 $\beta\in[0.3,0.7]$时，随着 β 增加，广播数据量增加。单播数据量为 $\sum_{i=1}^{M}\sum_{n=1}^{t}v_i^n$，其中 M 表示需要单播的用户总数，t 表示需要传送给授权用户的含指纹帧总数。视频的第 $n,n+1,\cdots,n+k$ 帧，可共用一个 v 来 masking，一个 v_i^n 来 unmasking，以减少单播数据量，但这样会导致视频的第 n 到第 $n+k$ 帧含有相同指纹信息，由此导致整个视频所携带的指纹信息量减少。

2)在 Watermark construction 过程中，可以结合视觉模型进行计算，从而获取更好的指纹嵌入效果[38]。

3)计算代价。前端计算任务较重，需要完成算法的第 1)－4)步。终端需要完成算法的第 5)步，即侦听和接收含有 v_i^n，$x_n^{w_{ni}}$ 的两路流，并按式(7)进行计算，这些需要终端软硬件支持。

算法 JFD2 Joint fingerprint embedding and decryption based on coefficient set scrambling[34]

算法基本过程：

1)从媒体 X 中抽取视觉相关内容并加扰。

选择 X 中视觉重要的低频和中频系数，并把它们分成 n 个子集。对每个子集中系数的符号使用一个密钥进行加扰。加扰后的数据及视觉不重要数据形成压缩流 Y 后广播。加扰过程使用两类密钥，一类用于确定系数属于哪个子集，另一类是子集加扰密钥。两类密钥构成加密密钥集 K_S。重要系数的选择和加扰方法一定要使得 Y 解压后，没有商业价值。否则，没有起到对 X 的加密效果。X 与 Y 的含义见图 5(a)。

2)发给授权用户 i 解密密钥 K_i，且 $K_i\subset K_S$。

3)用户 i 使用 K_i 对接收到的$\hat{Y}$($\hat{Y}$是 Y 经过信道传输后的结果)进行解密，获得 X_i。

由于 $K_i\subset K_S$，因此仅能实现部分解密。比如，n 个加密子集仅有 p 个被解密，X_i 中含有其余 $k=n-p$ 个没有被解密

的子集，这些没有被解密的系数符号及其它们在帧中的位置，构成用户 i 的指纹。

算法性能评价：

优点：同算法 JFD1 相比，额外传输的数据量较少。

缺点：1）解密秘钥与抗共谋指纹编码联系密切。首先解密密钥的设计必须以抗共谋指纹编码为基础，否则难以抵抗 Key collusion 及解密后含指纹媒体的共谋攻击。并且需要在视觉重要系数数量（要实现成功加扰）、解密百分比（指纹嵌入量）、X_i 质量三角关系中进行权衡。没有被解密的系数越多，指纹的嵌入量越大，X_i 的质量越差。

2）如果仅对亮度系数进行加扰，彩色成分中仍含有原有信息，利用这些信息可对加扰进行攻击。如果对彩色成分也进行加扰，在解密时，因部分不解密，可能会引起颜色混叠。

3）加扰时，没有结合视觉模型。

K. Karthik 等[37]对 JFD2 算法进行了改进，引入了视觉模型，但与常用视觉模型相比[39]，其显得比较粗糙。本文还比较详细地分析了解密密钥设计与抗共谋指纹编码的结合问题。

3.3.3 *路由器参与*

对路由器功能进行扩充，以减少终端负载及通信代价。典型算法有 Watercasting[40] 和 WHIM[41]。

Watercasting 算法

基本步骤如下：

1）前端、路由器、用户从拓扑结构上，构成一颗多播分布树。不妨记树的最大深度为 d；

2）前端为媒体的每个传输包，产生 $n \geqslant d$ 个含不同指纹的复本，加密每个包，多播；

3）路由器根据一定的规则，滤掉不必要的包后，把其余的包向下一个路由器广播；

4）拓扑树结构中，离终端用户最近的路由器仅从所收到的包中选择一个向用户传送。

算法的优点：通信代价由 d 决定，与终端用户数量无关。前端负载轻，指纹的引入不需要终端软硬件支持。

缺点：1）路由器知道所接收到的哪些包中含有指纹信息，并决定包的去向；前端需要获取拓扑树结构，要求路由器向前端逐级汇报自己的拓扑结构。这不仅需要相应的路由协议支持，还要求路由器是可信任的，避免路由器级欺骗。2）路由器间传递丢包规则，引入通信代价。3）包丢失及路由器故障对系统性能影响较大，可能导致盗版追踪过程复杂化及准确率下降。

WHIM 算法

在媒体服务器处，向媒体中嵌入时间戳后进行广播。从前端到终端的通信路径上，每经过一个 intermediary[41]，就嵌入 intermediary 的 ID 号后向下广播。在进行信息嵌入时，可以参考视觉模型。

算法优点：结合广播特点，在媒体传输过程中，逐步嵌入指纹信息，γ 较小。用户端没有引入与指纹相关的额外开销。

算法缺点：1）所嵌入的指纹信息，实质是媒体下发的路径标识，不是一种抗共谋数字指纹。最后一个 intermediary 所管辖的终端用户组获得的指纹是相同的，无法对该组内用户进行区分；2）intermediary 必须是可信任的，否则可能参与共谋；3）由于在每个 intermediary 处都需要进行指纹信息嵌入，可能导致通信延迟增加。

3.4 P2P 环境

在 P2P 环境下，终端用户获取媒体的路径具有事先不确定性，导致在前端嵌入指纹，再把含有指纹的媒体下发到特定用户是不可能实现的。在用户端嵌入指纹是唯一可行的方案，可参考 3.3.2 节的安全性思想进行设计。对所有授权用户都相同的数据部分不妨用 X 表示，X 可通过 P2P 环境传输，是 P2P 环境的公有数据[42]。与指纹相关的数据为用户私有数据，通过安全信道下发。只有 P2P 协议支持这些限制[42]，才能有望在 P2P 环境下，解决抗共谋数字指纹实现问题。

结束语 抗共谋数字指纹实现问题是数字指纹技术走向实用必须解决的问题。目前，关于这方面的研究刚刚开始。本文对该问题的涵义、研究现状及解决方案进行了较深入的探讨。该领域未来的研究方向有：

1）保证终端客户消费实时性的设计

现有算法对通信带宽占用、安全性、软硬件成本的分析较多，对指纹实现过程所引入的通信延迟没有进行分析。特别是从用户媒体请求到使用媒体的时间，不要因为指纹实现过程而延迟较大。如果采用 JBFD，JFD1 算法的两路流思想，应该合理安排下发算法，力求避免用户端长时间等待两路流的同步。流媒体情况下，指纹实现过程不要影响终端用户的实时播放效果。在家庭网关转码时，指纹实现过程不要影响转码的实时性。

2）支持终端用户动态加入、离开和吊销设计

在设计算法时，力求单个用户的动态加入和离开对抗共谋数字指纹实现过程的各项指标影响小，系统升级方便，暂时及永久吊销用户方便[43]。

3）结合其它技术，恰当引入抗共谋数字指纹实现过程

结合现有 CAS（conditional access system）和 DRM 版权保护技术，结合数字水印、数字指纹编码等相关技术，真正做到抗共谋数字指纹的安全有效下发。现有不少算法使用的指纹不是抗共谋数字指纹，如 WHIM 算法等；现有算法没有很好利用视觉模型，如 JFD1，JFD2 算法等，在与现有成果的结合上，有待于进一步研究。

4）结合现有的蓬勃发展的媒体业务，进行算法设计

例如，视频在流媒体服务器上以位率 a 存储，而终端只能以位率 $b(b>a)$ 消费，则流媒体服务器会使用一个转码器把视频从位率 a 转到 b[19]。在这样的环境中，传输的指纹位率是否也需要随之变化以及怎样变化，有待研究。

5）方便用户设计

方便用户，同保护内容制作者及内容运营商的利益一样重要。若指纹实现需要终端软件支持，则会出现多个公司的指纹实现软件彼此不同，使用哪个公司的媒体，则需要先下载该公司相应的支持指纹实现的软件，这给用户带来不便，特别在无线环境中，将更难以接受。当然，指纹实现软件同用户所需要的媒体相比，越小越好。同理，需要终端硬件支持的指纹实现方案，难度就更大些。

随着媒体的广泛应用、侵权行为的日益严重，期待具有盗版追踪功能的数字指纹技术从理论走向实际。抗共谋数字指纹实现问题是一个既有理论又有实际价值的课题，迫切需要学者及相关工作者进行研究。

参 考 文 献

[1] Wagner N R. Fingerprinting [C] // Proc. IEEE Symp. Security and Privacy. 1983:18-22

[2] Blakley GR, Meadows C, Purdy GB. Fingerprinting long forgiving Messages[C]//LNCS. 1986,218:180-189

[3] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data [J]. IEEE Trans. on Information Theory, 1998, 44(5): 1897-1905

[4] Staddon J, Stinson D, Wei R. Combinatorial properties of frameproof and traceability codes[J]. IEEE Trans. Inform. Theory, 2001,47(3):1042-1049

[5] Zhao H, Wu M, Wang Z, et al. Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting[J]. IEEE Trans. on Image Processing, 2005, 14(5):646-661

[6] Wu M, Liu B. Data hiding in image and video: Part-I — Fundamental issues and solutions[J]. IEEE Trans. Image Processing, 2003,12(6):685-695

[7] He S, Wu M. Joint coding and embedding techniques for multimedia fingerprinting[J]. IEEE Trans. on Info. Forensics and Security, 2006, 1(2):231-247

[8] Wang ZJ, Wu M, Trappe W, et al. Group-oriented fingerprinting for multimedia forensics[J]. EURASIP J. Appl. Signal Process, 2004, 14:2153-2173

[9] Schaathum H G, Fernandez M. Boneh-Shaw fingerprinting and soft decision decoding[OL]. http://www.computing.surrey.ac.uk/personal/st/H.Schaathun/research/public/Reports/2005-289.pdf

[10] Schaathum H G. On watermarking/fingerprinting for copyright protection[OL]. http://www.nik.no/2005/Schaathun.pdf

[11] Yang J, Xu X X. A robust anti-collusion coding in digital fingerprinting system[C]//ICSP2006 proceedings

[12] Peikert C, Shelat A, Smith A. Lower bounds for collusion-secure fingerprinting[C]//Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms. 2003:472-479

[13] Ergun F, Kilian J, Kumar R. A Note on the Limits of collusion-Resistant Watermarks[D]. Eurocrypt, 1999

[14] Barg A, Kabatiansky G. A class of I. P. P codes with efficient identification[J]. Journal of Complexity, 2004, 20(2/3):137-147

[15] Encheva S, Cohen G. Frameproof codes against limited coalitions of pirates[J]. Theoretical Computer Science, 2002, 273:295-304

[16] Cox I J, Miller M L, Bloom J A. Digital watermarking [J]. Elsevier, 2001

[17] Zhao HV, Liu KJ. Fingerprint multicast in secure video streaming[J]. IEEE Trans. on Image Processing, 2006, 15(1):12-29

[18] He S, Wu M. Collusion-resistant video fingerprinting for large user group[C]//Proc. of IEEE International Conference on Image Processing. Oct. 2006

[19] Sun QB, He DJ, Tian Q. A secure and robust Authentication scheme for video transcoding[J]. IEEE Trans. on Circuits and Systems for Video Technology, 2006, 16(10):1232-1244

[20] Eskicioglu MA, Town J, Delp EJ. Security of digital entertainment content from creation to consumption[J]. Signal Processing: Image Communication, 2003(18):237-262

[21] Andreaux J P, Durand A, Furon T, et al. Copy protection system for digital home networks[J]. IEEE Signal Processing Magazine, 2004:100-108

[22] Saroiu S, Gummadi P K, Dunn R J, et al. An analysis of internet content delivery system [OL]. http://www.cs.washington.edu/homes/gribble/papers/p2p_osdi.pdf

[23] Kozamernik F. EBU Seminar report- From P2P to broadcasting [OL]. http://www.ebu.ch/en/technical/trev/trev_306-p2p.pdf

[24] 郭宗明. IPTV 中的若干关键技术分析[OL]. http://www.founder.com.cn/cn/News/2006-11/03/content_1070.htm

[25] 时明亮,赵玲玲. 基于 CDN 与 P2P 技术的 IPTV 系统平台的设计与实现[OL]. http://www.bcu.edu.cn/truekxyj/journal/78/22.htm

[26] NuHome digital home technology[OL]. http://www.nufront-soft.com/Nuhome.html

[27] Zhao H, Liu K J R. Fingerprint multicast in secure video streaming[J]. IEEE Transactions on Image Processing, 2006, 15(1): 12-29

[28] Parviainen R, Parnes P. Large scale distributed watermarking of multicast media through encryption[C]//IFIP TC6 and TC11. 2001:145-581

[29] Ferrer J D, Joancomarti J H. Short collusion-secure fingerprints based on dual binary hamming codes[J]. Electron. Lett, 2000, 36 (20):1697-1699

[30] Yacobi Y. Improved Boneh-Shaw content fingerprinting[C]// Proc Cryptographer's Track at RSA Conf. 2001, 2020:378-391

[31] Sebé F, Ferrer JD. Collusion-secure and cost-effective detection of unlawful multimedia redistribution[J]. IEEE Trans. System, Man, and Cybernetics-part C: Applications and Reviews, 2003, 33(3):382-389

[32] Chu H, Nahrstedt K. A secure multicast protocol with copyright protection[C]//Proc. ACM SIGCOMM Computer Communications Rev. 2002, 32:42-60

[33] Luh W, Kundur D. New paradigms for effective multicasting and fingerprinting of entertainment Media[J]. IEEE Communications Magazine, 2005, 43(6):77-84

[34] Kundur D, Karthik K. Video fingerprinting and encryption principles for digital rights management [J]. Proceedings of the IEEE, 2004, 92(6):918-932

[35] Thomson to introduce Forensic marking solution for set-top boxes[OL]. http://www.contentsecurity.thomson.net

[36] VideoMark Forensic Watermarking[OL]. http://www.verimatrix.com/solutions/forensic_watermarking.php

[37] Karthik K, Hatzinakos D. Decryption key design for joint fingerprinting and decryption in the sign bit plane for multicast content protection[J]. International journal of network security, 2007, 4(3):254-265

[38] Emmanuel S, Kankanhalli MS. Mask-based fingerprinting scheme for digital video broadcasting[J]. Multimed tools Appl, 2006, 31:145-170

[39] Biswas S, Das SR, Petriu EM. An adaptive compression MPEG-2 video watermarking scheme[J]. IEEE Transactions on instrumentation, 2005, 54(5):1853-1860

[40] Brown I, Crowcroft J, Perkins C. Watercasting: distributed watermarking of multicast media[J]. Networked group communications, 1999:286-300

[41] Judge P, Ammar M. WHIM: watermarking multicast video with a hierarchy of intermediaries[C]//NOSSDAV. North Carolina, June 2000

[42] Kalker T, Epema PH, Lagendijk RL, et al. Music2Share—copyright-compliant Music sharing in P2P systems[J]. Processings of IEEE, 2004, 92(6):961-970

[43] Kim M, Kobara K, Imai H. Dynamic fingerprinting over broadcast using revocation scheme[C]//WISA. 2004:251-263