抗共谋数字指纹研究综述

梁睿超　卢增祥　路海明
（清华大学信息技术研究院　北京 100084）

摘　要　随着互联网以及多媒体技术的发展，数字版权保护技术已经成为了人们广泛关注的话题，而多个用户联合进行的共谋攻击已经威胁到发行商和其他合法用户权益。本文主要对多媒体数据中的抗共谋攻击研究现状进行了综述，介绍了若干具有代表性的抗共谋攻击方案，并提出了一些可行的研究方向。

关键词　共谋攻击，数字水印，数字指纹

An Overview on Anti-Collusion Digital Fingerprint

LIANG Rui-Chao　LU Zeng-Xiang　LU Hai-Ming
(Research Institute of Information Technology, Tsinghua University, Beijing 100084)

Abstract　Digital rights protection has become an important issue as the development of the Internet and multimedia technologies. It is easy for a group of users to work together and collectively mount attacks against the fingerprints or the tracing information. Collusion attack provides a cost-effective method for attenuating each of the colluder's watermarks. In this article, we review some major design methodologies for anti-collusion fingerprint of multimedia, give a broad overview of the recent advances in this area, and discuss the future of anti-collusion methods.

Keywords　Collusion attack, Digital watermark, Digital fingerprint

1　引言

随着整个社会数字化程度的提高以及网络的发展，越来越多的图像和视频信息以数字化的形式影响着我们的生活。这些变化为人们带来了极大的方便，但同时也为一些人进行作品的非法拷贝和再分发提供了平台。由于传统的加密手段在用户解密之后就失去了防御能力，所以数字水印系统应运而生。然而普通的水印由于在每个拷贝中都嵌入相同的信息，只要能够抵抗像滤波，压缩/解压缩，DA/AD转换等一些较常规的攻击就足够了，但是由于数字指纹的出现（每个用户的作品内容相同，而其中的指纹各不相同），如果若干非法用户联合起来进行共谋，伪造一份新的图像或视频作品，就可能会大大削弱可检测出的水印或指纹的能量，从而躲过检测者的追踪，共谋者甚至可以使水印或指纹变成属于某个无辜用户的，通过诬陷他人来逃脱责任。同样，如果使用密钥对作品进行加密，也会出现若干用户联合起来产生新的密钥来逃避追踪的情况。我们把多个用户联合他们的拷贝，以再次进行分发为目的的逃避版权追踪的过程称为共谋。

1985年，从Blakley等人[1]最先提出共谋这个概念之后，人们开始认识到共谋现象的存在对于多媒体数据版权的威胁，特别是随着图像和视频的数字化程度的提高，这种潜在的隐患已经逐渐地变为现实，因此，就更需要对于现有的水印和指纹系统进行改进，来对抗这种攻击。

本文将在第2部分对抗共谋攻击的整体情况作以概述，在第3部分对抗共谋攻击研究中的主要成果进行介绍，最后是总结并提出展望。

2　抗共谋攻击简述

当前对于共谋攻击的研究可粗略划分为两个方向，一是设计抗共谋的编码，二是分析设计抗共谋系统的性能。

在设计编码方面，最早的关于一般多媒体数据的抗共谋攻击指纹的方案之一是由Boneh和Shaw提出的[2]。他们提出的编码方案，可以以较高的概率从最多k个共谋攻击者中抓到至少一名共谋者。这个指纹编码方案由Yacobi进行了改进，他将一个直接扩频序列的嵌入层和Boneh-Shaw编码层结合起来[3]。Domingo-Ferrer[6]提出了一种建立在鲁棒水印算法上的抗共谋编码，使用了对偶汉明码来抵抗不超过两个用户的共谋攻击。为了减少解码程序的计算时间和内存使用量，有人提出了一个双层的c-安全编码，在这种方法中，作者将内层的Cox水印编码与外层的纠错码结合起来，并且采用码间最小距离以保持水印的抗共谋性能[7]。Francesc等人使用对偶汉明码的纠错容量生成了一种新的码[8]，叫做散码（Scattering Code），解决了3人以内共谋的问题，并且码长要比Boneh-Shaw码短。Dittmann等人利用不同码向量之间的交叠来识别最多k个共谋者，他们根据有限射影几何的理论提出了一个新的思路[4]。这个思想打开了研究的一个新天地，Wade Trappe等人[5]受到启发提出了一种抗共谋码（ACC），他们在设计中使用了组合设计和区组编码的理论，比如BIBD等等。

在分析设计抗共谋系统性能方面，很多人把主要的着眼点放在研究某些水印系统或方案对于不同种类的共谋攻击的抵抗性能上。这类研究的主要目的是通过考查几个重要的量（需要被嵌入的信息的长度N，指纹系统中总的用户数n和参加共谋的敌手数量k）之间的关系，找到他们的联系或者在某些给定条件下的边界情况等等[9~11]。另有些人从视频的观点出发，利用相关性[12]，视频特性[13]和视频标准特性[14]来研究系统抵抗共谋攻击的能力。

梁睿超　硕士研究生；卢增祥　副研究员，博士；路海明　副研究员，博士。

涉及共谋攻击领域内的其它研究方向还有很多，有不少人提供了新颖的想法，比如 Celik 等人提出的预处理过程[15]，利用人对图像或视频作品局部微小几何失真的不敏感，在图像或视频的每帧中加入水印或指纹之前进行一些微小的扭曲。敌手如果再进行共谋攻击，由于每个拷贝之间几何变化的不同而造成不匹配，将得到一个质量很差的共谋版本。利用水印的感知特性[16]对水印或指纹进行研究的例子还有很多，比如 Zhao 等研究了假设指纹分布为有界的高斯分布时的情况[17]，其中利用 JND(Just Noticeable Difference)来控制对指纹的嵌入和检测等。

另有一些共谋攻击的研究切入点不同，例如有的研究从推翻现有的指纹研究出发，进行一些拓展[18]，根据共谋攻击的特点设计新的指纹系统[19]，还有根据向量的正交调制理论来设计指纹编码的[5,11]，利用密码学理论进行抵御共谋的叛逆者追踪方案[20~22]等。

3 抗共谋攻击方案

本节将介绍若干最具有代表性的抗共谋攻击方案。

3.1 利用编码设计的方案

1995 年，Boneh 和 Shaw 给出了多媒体数据共谋攻击领域内第一个比较清晰的解决方案[23]。该方案所解决的核心问题就是设计了一种编码方案，使得不超过 c 个用户联合进行共谋时，能够以一个较大的概率追踪到至少一名共谋者。

方案的实施是建立在他们所定义的概念嵌入假设(Marking Assumption)上的，即假设参与共谋的敌手只能修改彼此对应作品码字中不同的位。在此基础上，他们首先引入了 c-防陷害码，即当不超过 c 个用户联合时，没有一个联合能串通起来陷害一个不在联合中的用户。可惜的是这种码字在共谋人数超过 3 个时便失去作用。因此他们接着提出了 c-完全安全码的思路，通过逐个检测联合的某个子集来追踪到至少一个非法用户，但是在实际信道中码字传输以及被攻击后必然会受到一定的影响，通常只能以某个概率来保证追踪到一个共谋者，由此引出 c-安全码的概念：

如果至多 c 个用户的一个联合 C 生成一个码字 x，满足 $Pr[A(x)\in C]>1-\epsilon$，若具有这样的算法 A，那么 Γ 是具有 ϵ 一误差的 c-安全码。

以这个概念为核心，利用秘密置换 Π 以及特殊的统计均匀分布与否的设计，他们构造了一个能够追踪至少一名共谋者的算法，假设 N 代表系统中的用户总数，码长 $l=O(c^4\log(N/\epsilon)\log(1/\epsilon))$。

尽管这个算法第一次给出了对于共谋水印的一个系统全面的分析，并且设计中对于潜在用户数量和共谋者数量都没有限制，它的不足之处还是很明显的。首先是码长较长，不仅无法实际应用，而且距离作者自己给出的码长的一个下界 $l\geqslant(c-3)\log(1/\epsilon c)/2$ 也有一段距离。其次是没有利用先验知识，每次检测都要对所有用户集合进行操作，计算量较大。另外，误发的随机错误也会对于算法的判断产生严重的影响[28]。

3.2 利用组合学设计的方案

1999 年，Jana Dittmann 等人[4]就根据有限射影空间的理论提出了一种解决水印中共谋攻击的方案。Wade Trappe 等人结合向量的正交调制对于这种水印编码方案作了推广和改进[5]，利用组合学中的设计原理，即均衡不完全区组设计(Balanced Incomplete Block Design，以下简称 BIBD)来实现抗共谋水印方案。

Dittmann 的方案假设发布 $q+1$ 个拷贝，允许最多 d 个共谋者联合，则需要在数字图像中找到 n 个位置嵌入水印码字，要求满足 $n=q^d+q^{d-1}+\cdots+q+1$。这个算法对于嵌入位置的数量有很高的要求，而通常的数字图像中很难找到如此大量的标记位置。因此，有人也将此算法作以修改来适应视频水印的要求[24]。

Wade Trappe 等人从组合设计的理论出发，得到了和 Dittmann 方法一致的结果。但是他们仅讨论了“逻辑与”的共谋情况。将多个用户按“逻辑与”共谋后，产生的码字中的“1”称为特征码字，特征码字即在共谋集的不可探测位置上标记为 1 的码字。因此，可以根据共谋水印中的特征码字对共谋用户进行跟踪。

使用 $BIBD(v,k,1)$ 设计生成 BIBD 抗共谋码用于数字水印抗共谋攻击，方案可容纳的用户数为 n，参数 v 为用户水印的码长 l，$k-1$ 为方案允许的最大共谋用户数 c，即在共谋用户数小于或等于 $k-1$ 时，可跟踪到所有参与共谋的用户。根据 BIBD 的性质，有 $n=(l^2-l)/(c^2+c)$。因而，若该 BIBD 存在，n 用户的水印只需要 $l=O(c\sqrt{n})$ 个基向量，即水印长度的近似随着 $\sqrt{n}$ 线性增加，随着 c 线性增加。和 c-安全码等码字相比，它更接近理论上码长的下界。因此，BIBD 码能够极大地缩短水印码字的长度。例如，存在参数为(61,305,20,4,1)的 BIBD，户数为 $n=305$，c-安全码需要 305 个二进制码比特，而 BIBD 码则仅用 61 个二进制码比特能成功跟踪到参与共谋用户数小于等于 3 的共谋用户。

BIBD 码用作水印也存在问题。首先，它不能处理任意修改每一位水印位的情况，因为其前提是嵌入假设。另外，某参数下 BIBD 设计本身的存在性及相应的 BIBD 区组的获取都存在问题，尤其是水印要求参数 $\lambda=1$。在参数比较大的情况下，寻找 BIBD 区组的算法是相当复杂的。其次，对于 BIBD 共谋集的探测是通过特征码字进行跟踪的，因而跟踪过程的匹配算法不是将共谋水印与用户水印直接进行匹配检测，而是将共谋水印与所有共谋用户数为 $c\leqslant k-1$ 的共谋集的特征码字进行匹配，这一环节的计算开销比较大。

3.3 利用分组设计的方案

如果设计的抗共谋算法是基于用户指纹的，并且除了指纹以外没有任何预先假设，那么算法本身的设计难度就会比较高。实际上，原来的共谋算法都有一个共同的假定，那就是对于所有用户，他们中任意组合组成一个联合的概率都是相同的。然而这在现实中不够合理，因为在社会中人们有着各式各样的联系，那么在地域上相近或是社会关系上接近的人群更有可能组成联合进行共谋。

基于这样的想法，2004 年，Wang 等人[25]根据实际中抗共谋攻击的需要，把作品的分发进行分组，设计相应的水印和检测算法来增强水印系统的性能，又利用了水印向量正交调制的概念，即在某个内积的定义下，找到一组正交基，利用向量调制的方法进行编码。利用分组的先验知识，将同一组内用户的水印设计为相关的，而不在同一组的用户的水印之间则是不相关的。检测算法分成两个步骤，第一步确定共谋发生在哪些组中，第二步确定每个含有共谋用户的组中的具体用户。

和分组思路类似的，也有人[5]提出基于二叉树的检测算法，主要目的是降低相关性检测的次数。首先将所有待检测水印分为两大组，对于每一组分别检测，并与事先设定的阈值

相比较，若大于某个值则说明该组内包含有共谋用户，继续将其分成两组，再与相应的阈值进行比较，依此类推，直至最后检测出共谋用户，整个的检测过程形成一棵二叉树。

分组的思路比较接近作品分发中的实际情况，因此是一个比较可行的做法，但是如果只利用分组和码调制的方法却需要多次进行相关性检测，计算量仍然比较大。如果使用树形的分组检测算法，则相关性检测计算的数量级降下来了（为O(logN)，其中N为总的用户数），但是在设定每层节点的阈值上又会比较麻烦。

3.4 对偶水印-指纹系统

2004年，Kirovski等[19]提出了一种对抗共谋攻击的新思路，通过引入新的应用形式和算法，他们设计了一种对偶水印-指纹系统。通过在嵌入端使用统一的水印加密，而在客户端使用不同的指纹来解密，他们采用了一种与“传统水印模型+共谋编码”不同的思路，并且证明了在某些特定条件下能够达到相当不错的抗共谋性能。

算法假设所有终端都在发行商的控制之内，也就是说发行商完全清楚系统中所有用户的指纹。每个用户拥有不同的指纹，共谋用户混合他们的指纹来试图去除作品中的水印。当找到非法分发的内容后，算法通过参考原始的未加水印的拷贝来找出共谋者。

他们的主要思想是在嵌入端使用同一个秘密水印密钥（Secret Watermarking Key，简称SWK）。而在接收端的水印检测密钥（Watermark Detection Key，简称WDK）与SWK不同，破解了一个单独的检测器并不能为去除水印 w 提供足够的信息。媒体数据信号 x 像传统的方式一样由扩频编码方式的水印所加密。但是，对于每一个媒体播放器 i 来说，都对应一个个性化了的水印-指纹检测密钥 h_i，这个密钥是按照如下方式产生的。

设 $C=\{c_{ij}\}$ 表示一个 $m\times N$ 的矩阵，其中 m 表示系统中用户的总个数，N 表示在一个作品中标记的个数，$c_{ij}\in R$，$c_{ij}=N(0,B^2)$ 也就是说，每个元素都是一个零均值的，标准差为 B 的高斯随机变量。每一行 i 都包含一个水印载体，记作 c_i。第 i 个WDK定义为 $h_i=w+c_i$。水印载体 c_i 的目的是将SWK隐藏在 h_i 中，从而使敌手知道 h_i 却未必能推知真正的 w，这一点只要 B 足够大就可以做到。换句话说，没有一个播放器包含真正的 w，但是都包含了它的一个修改的版本。

数字电视广播等领域的发展对于允许参与共谋人数的要求越来越高，需要系统的追踪能力更强。对偶水印-指纹系统和传统的水印系统+共谋编码的方法相比，最大的优点在于它的抗共谋能力比较强，可以容许百万量级的用户参与共谋，而传统方法却只能抗击几十或最多几百个用户的共谋问题。这种系统的缺点在于由于它设计上的特点，水印密钥必须每隔100多个用户就要更换一次。

3.5 其他抗共谋方案

3.5.1 叛逆者追踪方案

Chor等人[20]最先提出叛逆者追踪的思想，来解决数据广播中的共谋问题。共谋攻击不仅会影响水印系统，甚至对于传统的密码学系统为基础的方案也会造成一定的威胁。例如在数字广播电视领域就存在这样的问题。叛逆者追踪方案就是在这类特定环境下产生的一种抗共谋方案。它利用数学上某些困难问题的难解性，通过检测非法播放器内的盗版指纹信息来追踪共谋用户。在水印系统中，共谋者操作伪造的是其中的水印；而在类似叛逆者追踪的密码学系统中，不同的是，共谋者通过混合各自的密钥来达到非法再分发的目的。

需要特别说明的是，在叛逆者追踪方案中并不应该只由发行商来控制系统的所有终端，像在对偶水印-指纹系统中所做的一样。如果这样，当算法找到某个用户参与了共谋以后，因为发行商也知道所有用户的密钥，该用户仍然可以声称是发行商对其进行了诬陷。解决这类问题的通常办法是引入第三方来控制密钥，从而使算法具有不可否认性。

他们假设每个用户拥有不同的密钥集，敌手只能通过获取各自播放器中的密钥来进行共谋（共谋者不知道除他们自己之外别人的密钥），生成伪造的共谋密钥来再分发给非法用户。通过找到非法的播放器，获取相应的共谋密钥，他们通过参考系统用户密钥集合来标定最可能的共谋者。

其主要思想是给所有用户一个稍有差别的秘密。数据提供商生成一个空间大小为 n 的基本密钥集，并在其中随机选取 m 个作为某一用户的个人密钥 $P(u)$。数据提供商广播的信息由两部分组成，即授权分组EB与密文分组CB。密文分组CB是明文信息分组在一个随机信息主密钥MK下通过对称加密方式所生成的密文组；而授权分组EB是MK在基本密钥集中所有密钥通过对称加密方式所生成的授权分组。这样，授权用户首先利用个人密钥 $P(u)$ 解密授权分组中 m 个相应的信息块获得信息主密钥MK，然后通过主密钥MK解密密文分组即可获得广播信息。

Chor等人提出了一系列对称叛逆者追踪系统方案，但是由于对称方案不满足不可否认性，所以其应用前景不如非对称叛逆者追踪方案广泛。一些公钥叛逆者追踪系统有希望投入实际应用，比如Boneh和Franklin[22]就利用了纠错码技术以及求解离散对数的困难问题建立了一套非对称的叛逆者追踪系统，能够保证不诬陷无辜用户，且抓到所有叛逆者。

另外，在数字电视应用中已经出现了利用共谋伪造控制字来进行非法转播的现象，所以动态的叛逆者追踪，即在有限时间内追踪到叛逆者的算法就显得尤为重要。Fiat等人[21]已经提出了一些动态叛逆者追踪的算法，但是仍然受限于计算量，网络带宽等的参数。

3.5.2 单用户共谋方案

为了比较清楚地阐述这个问题，必须简要介绍一下共谋的类型和模式。

在实际中存在着两种不同的共谋类型[26]。第一类共谋是将相同的水印嵌入到不同的作品中时发生的，这对应于版权保护的情况；第二类共谋则是将不同的水印嵌入到相同的作品拷贝中，对应于数字指纹的情形。

在视频里也存在着两种共谋的模式[12,26]。第一种称作视频间共谋，是指若干非法用户联合各自的拷贝生成伪造拷贝的过程，在所有多媒体数据中都有可能出现。而第二种共谋模式是视频中所特有的，称作视频内共谋，共谋者不需要其他的拷贝，只用一份拷贝就可能将加在视频中的水印去除。如果在视频中每帧都嵌入相同的水印，就可以看作是第一类共谋，可以通过求和平均的做法去除水印；如果在视频的每帧都嵌入各不相同的水印，则看作第二类共谋，近似静止的帧中的水印将面临被去除的危险。

针对这一新出现的共谋模式，最近人们作了一些探索性的工作。Karen Su等人[27]根据各帧之间统计相似性的程度调整在每帧中关键点处嵌入的水印的数量，并且提出了统计不可见性的概念[12]。他们认为两个原始帧之间的相似程度应该和嵌入水印后两帧之间的相似程度保持不变，这样就可

以有效地阻碍这种视频内共谋攻击。Doërr 等人对于这种视频内共谋的情况从理论上作了比较深入的分析[13]。先后提出了 SS,SS-1,SS-N 和 SS-α 系统,虽然这些系统抗的共谋攻击的能力逐级增强,但是仍然存在更高一级的共谋攻击手段可以攻破它们。在未来,抵抗这种模式的共谋攻击的研究将成为视频共谋攻击领域的研究重点。

总结与展望 共谋攻击是一种对多媒体数字作品构成威胁的广泛存在的一种攻击形式。如果不对其进行有效的限制,那么出版商和其他用户的合法权益就无法得到保障,数字版权市场也难以执行规范化的进程。本文对于多媒体数据中有代表性的抗共谋攻击的研究成果进行了介绍,并分析了算法的优缺点。

从本文介绍的各种方案中我们可以大概窥探出抗共谋研究的比较完整的脉络。在 c-安全码,BIBD 码,分组方案,对偶水印-指纹系统之间我们可以看出一条算法发展的轨迹。c-安全码是对于外部条件限制最少的一种算法,适用性也较强,但是有码长过长的缺点;因此,为了解决这个问题,着眼于减少码长,BIBD 码诞生了;当发现共谋攻击本身的一些特点之后,人们发现在地域和社会关系上靠近的人更容易产生共谋,因此利用分组的方案可以增强抗共谋的性能;最后,随着对于检测能力的进一步要求,算法将客户端纳入一并进行了改进限制,产生了对偶水印-指纹系统。

在这套研究脉络之外,共谋和抗共谋的对抗也在一些其他领域擦碰出火花,比如从传统密码学发展起来的叛逆者追踪方案,在视频水印中也产生了类似单用户共谋这样的新问题。

总的来讲,共谋攻击的研究仍然处于起步发展阶段,很多问题亟待解决。通过研究算法的整体发展和具体的实施方案,我们认为抗共谋算法未来的发展方向可以概括为 3 个:

①将算法的限制条件减到最少,从理论上研究抗共谋问题的本质;

②对于目前已经形成的方案和算法做进一步和更合理的假设,来设计新的方案;

③除了传统的指纹方向,在其他一些领域和特殊场合对于抗共谋算法进行广泛和深入地探索。

抗共谋攻击的研究也依赖于共谋攻击技术本身的发展,可以肯定地说,二者的发展脚步应该是大体同步的。没有道高一尺的攻击技术,也就没有魔高一丈的防御本领。同样,防御者的盾再硬,也仍然会存在更锋利的矛。从某种角度来说,共谋攻击的研究其实就是一个博弈的过程。

参 考 文 献

1 Blakley G R, Meadows C, Purdy G B. Fingerprinting Long Forgiving Messages. LNCS,1986,218: 180~189

2 Boneh D, Shaw J. Collusion-Secure Fingerprinting for Digital Data. IEEE Trans. Information Theory, 1998, 44:1897~1905

3 Yacobi Y. Improved Boneh-Shaw Content Fingerprinting. LNCS, 2001, 2020:378~391

4 Dittmann J, Behr A, Stabenau M, et al. Combining Digital Watermarks and Collusion Secure Fingerprints for Digital Images. IS&T/SPIE Conf Security and Watermarking of Multimedia Contents, California, 1999

5 Trappe W, Wu M, Wang Z J, et al. Anti-collusion Fingerprinting for Multimedia. IEEE Trans. Signal Processing, 2003, 51: 1069~1087

6 Domingo-Ferrer J, Herrera-Joancomarti J. Short Collusion-Secure Fingerprints Based on Dual Binary Hamming Codes. Electron Lett,2000,36:1697~1699

7 Zane F. Efficient Watermark Detection and Collusion Security. LNCS,2000,1962: 21~32

8 Sebe F, Domingo-Ferrer J. Collusion-Secure and Cost-Effective Detection of Unlawful Multimedia Redistribution. IEEE Trans. Systems, Man, and Cybernetics-Part C: Applications and Reviews,2003,33:382~389

9 Kilian J, Leighton T, Matheson L, et al. Resistance of Digital Watermarks to Collusive Attacks:[Tech Rep]. Princeton, Department of Computer Science, 1998

10 Stone H. Analysis of Attacks on Image Watermarks with Randomized Coefficients:[Tech Rep]. Princeton, NJ: NEC Res Inst, 1996

11 Wang Z J, Wu M, Zhao H V, et al. Anti-Collusion Forensics of Multimedia Fingerprinting Using Orthogonal Modulation. IEEE Trans. Image Processing, 2005,14: 804~821

12 Su K, Kundur D, Hatzinakos D. Statistical Invisibility for Collusion-Resistant Digital Video Watermarking. IEEE Trans Multimedia, 2005,7: 43~51

13 Doërr G, Dugelay J-L. Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking. IEEE Trans Signal Processing, 2004,52:2955~2964

14 Hauer E, Thiemert S. Synchronization techniques to detect MPEG video frames for watermark retrieval. In:Proc SPIE/IS&T Electronic Imaging, 2004,5306:315~324

15 Celik M U, Sharma G, Tekalp A M. Collusion-Resilient Fingerprinting by Random Pre-Warping. IEEE Signal Processing Letters, 2004,11:831~835

16 Wolfgang R B, Podilchuk C I, Delp E J. Perceptual Watermarks for Digital Images and Video. Proc IEEE, 1999,87:1108~1126

17 Zhao H V, Wu M, Wang Z J, et al. Forensic Analysis of Nonlinear Collusion Attacks for Multimedia Fingerprinting. IEEE Trans. Image Processing, 2005,14:646~661

18 Wu Y-D. Linear Combination Collusion Attack and its Application on an Anti-Collusion Fingerprinting. ICASSP, Philadelphia, USA, 2005

19 Kirovski D, Malvar H, Yacobi Y. A Dual Watermark Fingerprinting System. IEEE Multimedia, 2004. 59~73

20 Chor B, Fiat A, Naor M, et al. Tracing Traitors. IEEE Trans Information Theory, 2000, 46: 893~910

21 Fiat A, Tassa T. Dynamic Traitor Tracing. J Cryptology, 2001, 14: 211~223

22 Boneh D, Franklin M. An Efficient Public Key Traitor Tracing Scheme. LNCS, 1999, 1666: 338~353

23 Boneh D, Shaw J. Collusion-secure Fingerprinting for digital Data. LNCS, 1995, 963: 452~465

24 纪震,姜来,李慧慧. 一种抗共谋攻击的数字视频指纹算法改进方案. 深圳大学学报(理工版), 2004, 21:24~29

25 Wang Z J, Wu M, Trappe W, et al. Group-Oriented Fingerprinting for Multimedia Forensics. EURASIP Journal on Applied Signal Processing, 2004,14:2142~2162

26 Doërr G, Dugelay J-L. A Guide Tour of Video Watermarking. Signal Processing: Image Communication,2003,18:263~282

27 Su K, Kundur D, Hatzinakos D. Spatially Localized Image-Dependent Watermarking for Statistical Invisibility and Collusion Resistance. IEEE Trans Multimedia, 2005,7:52~66

28 吕述望,王彦,刘振华. 数字指纹综述. 中国科学院研究生报, 21: 289~29