数字版权管理技术

2021/12/23

1 数字版权管理技术概述

2 DRM在商业应用中的需求

3 DRM标准及技术体系

4 数字加密技术

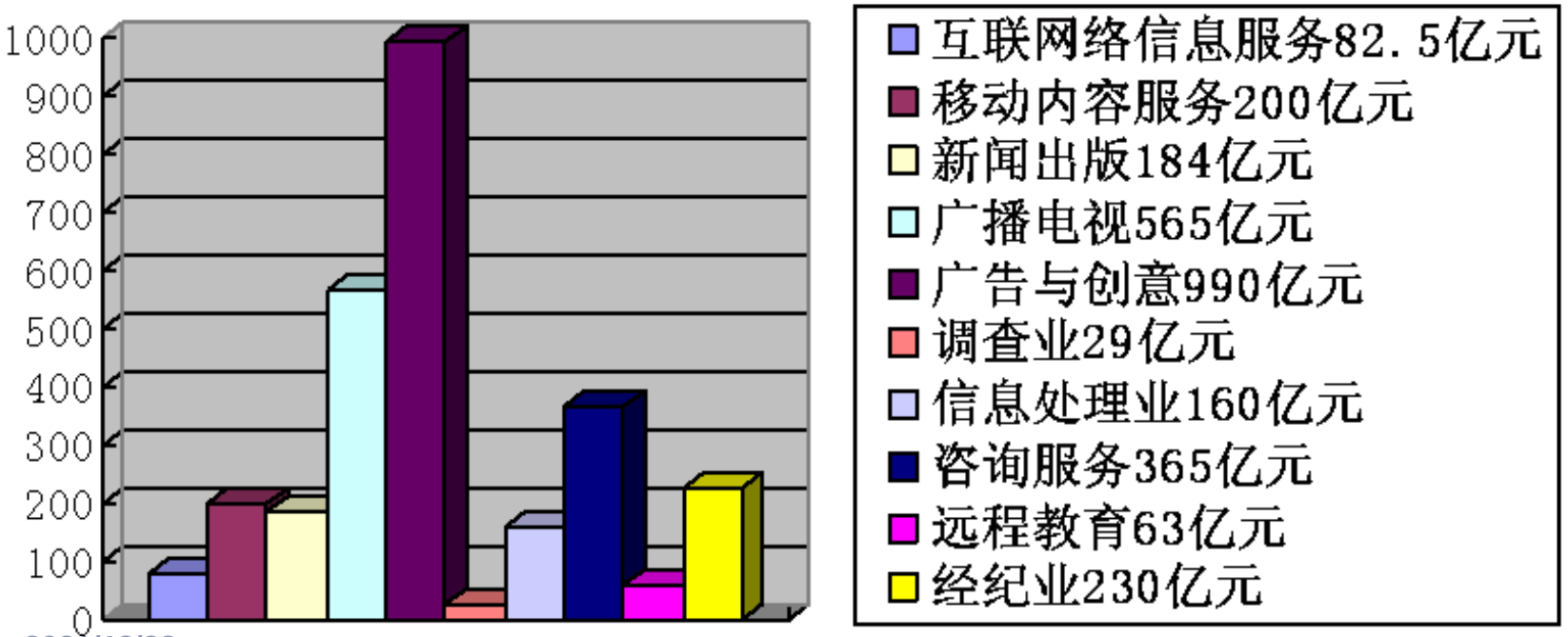
5 数字水印技术

1.1 数字版权管理技术的基本特征

- **数字版权管理**，即所谓的DRM（Digital Rights Management），也称数字版权保护，就是采取信息安全技术手段在内的系统解决方案，在保证合法的、具有权限的用户对数字信息（如数字图像、音频、视频等）正常使用的同时，保护数字信息创作者和拥有者的版权，根据版权信息使其获得合法收益，在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪，并确定盗版数字作品的来源。

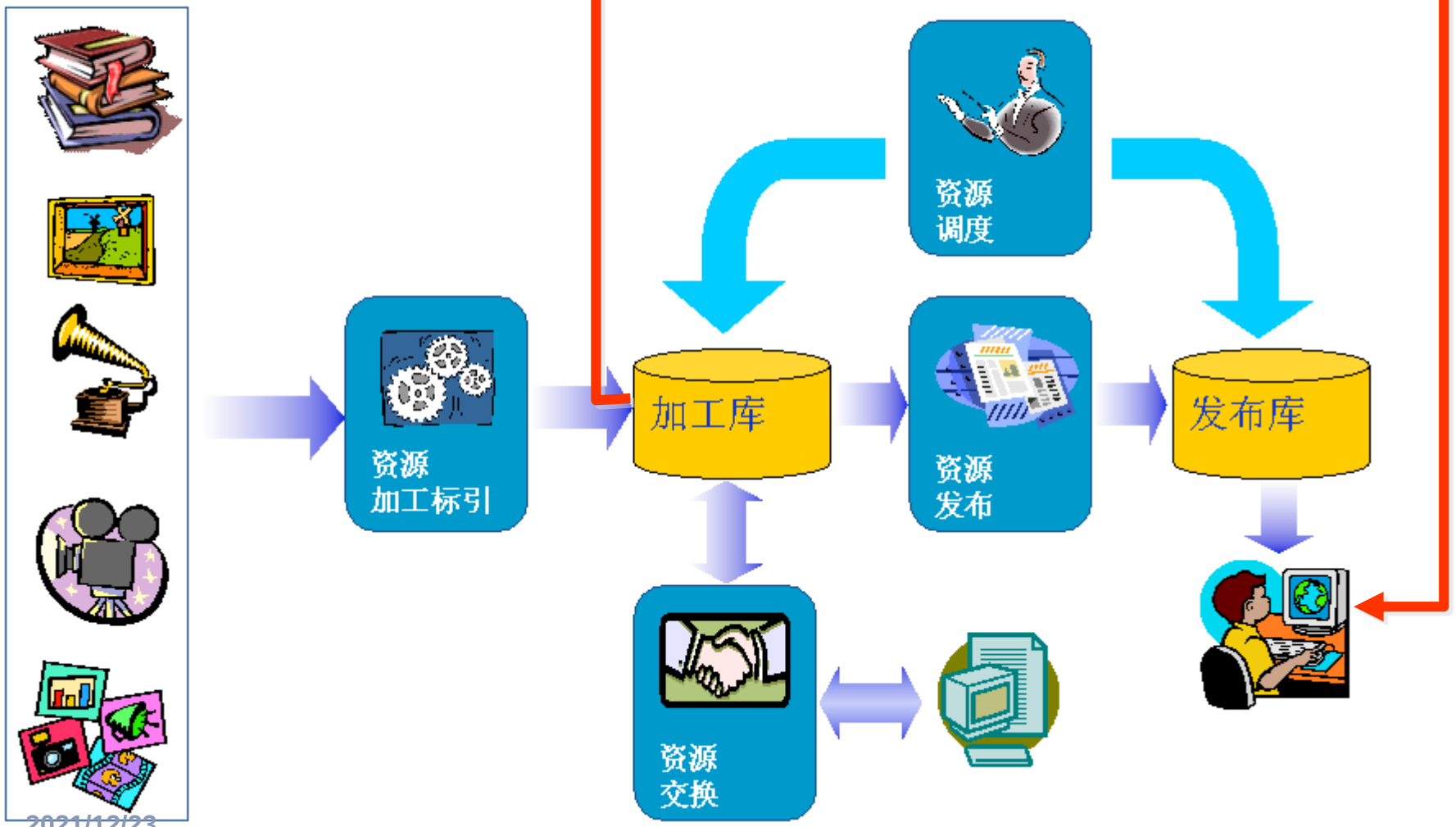
1.1 数字版权管理技术的基本特征

- 信息技术与互联网的迅猛发展为多媒体信息的存取和交换提供了极大的便利。
- 但同时数字化技术精确、廉价、大规模的复制功能和互联网全球传播能力为版权保护带来极大冲击。



1.1 数字版权管理技术的基本特征

MEDIA ASSET MANAGEMENT



1.1 数字版权管理技术的基本特征

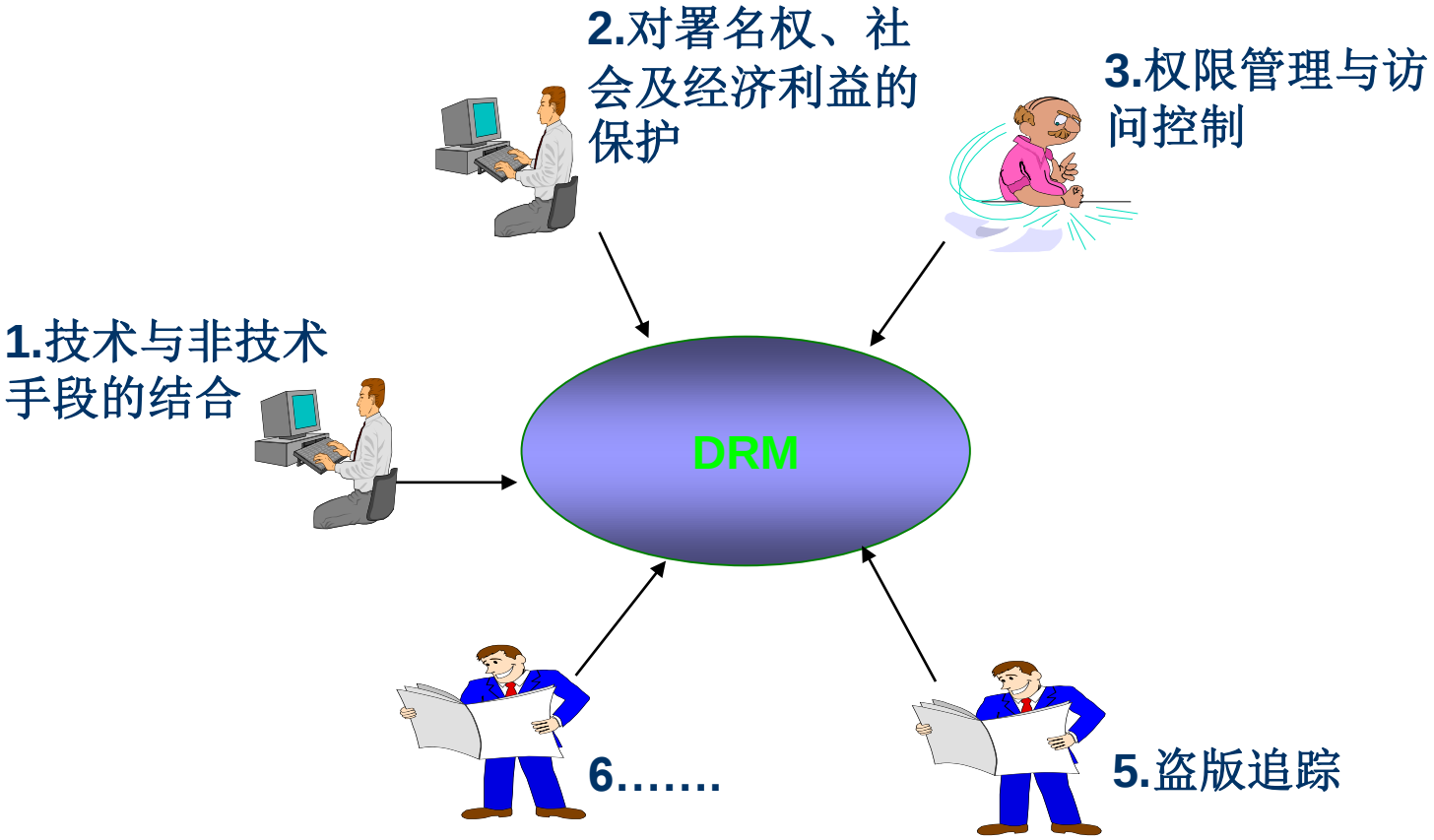
- **DRM**是内容安全的一种具体应用，即对数字内容使用权限的确认、封装、分发、控制、追踪的机制。
  - 权限确认即用户对感兴趣的内容提出使用权限的需求，服务器对其资格和要求验证的过程；
  - 权限封装即对赋予用户的使用权限及相关信息的加密或保护的过程；
  - 权限分发即将封装好的权限对象安全交付给用户的过程；
  - 权限控制即内在的权限内容的具体生成和外在的权限内容的具体实施；
  - 盗版追踪即保证版权拥有者的合法权利，并对盗版者予以打击。数字内容盗版追踪主要靠数字水印技术或者一些网络追踪来实现。

1.1 数字版权管理技术的基本特征

- DRM为数字内容产品创作—发行—消费的价值链中的各个环节都带来了实际的利益。
- 对于消费者来说可以获得更多所需要的数字信息；
- 对发行者而言，利用发行资源（如网络带宽）、增加消费数量，从而获得收益。
- 创作者和版权拥有者的数字作品可以从保护中获得应有的收益。

1.1 数字版权管理技术的基本特征

❖ DRM的基本特征



1.2 数字版权管理技术的现状与趋势

- 国外数字版权保护工作起步较早，相关法律法规的制定工作比较完善，如《**WIPO版权条约**》。相关领域生产厂商技术储备也很丰富，在电子出版物制作、**DRM**、经营管理模式方面都已推出了自己的产品和解决方案。
- 但是，国外尚未出台由政府职能部门出面建设的网络数字版权保护平台。连美国、英国等数字版权发展较发达地区，在此领域取得的成果也主要基于技术层面，对此领域内的流程法规建设目前为止也没有拿出合理的解决方案。
- 现有的**DRM**依靠三种主要形式：
  - 通过设计特殊功能的硬件产品来支持，如电视机顶盒等。
  - 通过特殊格式传输多媒体内容。
  - 通过修改通用系统，从而支持安全功能。

1.2 数字版权管理技术的现状与趋势

- 2001年1月，W3C（World Wide Web Consortium）从Web框架和网络应用的角度提出了知识产权管理7项原则：
  - 1 普遍访问：使人们具有最广泛的信息共享和网络访问能力；
  - 2 语义Web：采用标准化的语义方法表示各种资源和工具，使计算机能够进行翻译、交换并解决问题；
  - 3 可信：提供一个可信任的环境，使人们对其网络行为负责；
  - 4 交换性：主要通过公开设计和推广的方法采用开放计算机语言和协议，避免零散的市场体系；
  - 5 可改进性：使整个Web容易进行改进和升级，所有的设计遵循简洁、模块化、兼容性和可延伸性；
  - 6 分散性：采用分散设计的方法限制核心化的Web设备数量，从总体上减少Web易受攻击的特性，增强整个网络的错误容忍性；
  - 7 更好的多媒体：不限制多媒体内容提供者的创造性，W3C通过不断了解用户和工作站的实际需求，不断采用更新的语言提供更有效的框架。

1.2 数字版权管理技术的现状与趋势

- **Open Mobile Alliance**（OMA）是由移动电话生产商、计算机设备公司、无线设备制造商和内容提供商发起的产业联盟组织，现有300多名会员（其著名会员有诺基亚、微软、IBM等）。OMA DRM 提供更广泛的访问控制功能、安全功能、域控制和导出功能等。体系向支持更高附加值的内容转化。OMA DRM还提供了很多的权利功能，主要包括：多机享用、免费预览、赠与、权利管理功能和双向验证等等。
- 由美国**Real Networks Inc.**开发的Helix DRM是第一个能将媒体安全地传输至任意设备的多格式数字版权管理平台Helix DRM是一个综合、灵活的平台，支持标准格式和Internet格式，如RealAudio、RealVideo、MP3、MPEG-4、AAC、Sony的ATRAC3和H.263等媒体格式。它集合了所有现有的基础设备和后台系统，支持多种商业模式，如采购、租赁、视频点播和订阅服务。

1.2 数字版权管理技术的现状与趋势

- **美国微软公司**的Windows Media 权限管理机制包括了打包、分发、建立许可证服务器、获取许可证和播放数字媒体文件5个步骤。许可证可提供多种不同权限，如开始时间和日期、持续时间以及对操作计数。但是，许可证是不可转让的。如果用户将打包的数字媒体文件发送给一位朋友，则该朋友必须获取自己的许可证，然后才能播放该文件。

- **北大方正**于2001年推出以数字版权管理技术为核心的方正Apabi数字图书系统整体解决方案。方正阿帕比电子公文软件产品，实现公文的电子化处理及无纸化传输，并保证传输过程的安全、可控及公文内容的不可篡改。

1.2 数字版权管理技术的现状与趋势

- **韩国三星电子**设计了一种基于受保护对象使用计数的DRM方法。该方法需要播放器从服务器取得限制播放次数的策略信息，在播放终端上设计了一个使用计数器，通过网络链接向服务器发送使用次数的报告。当通过某种手段用户使用设备但是没有执行策略信息时，内容将不能使用。

- **中兴通讯**设计了一个基于IPTV的版权保护系统使用ORDL标准的XML文件承载版权信息。该系统可以支持点播和直播两种模式的视频播放方法的加密和密钥模式，包含了传送、加解密、密钥管理及版权发布。

1.2 数字版权管理技术的现状与趋势

- **武汉理工大学**发明了一种基于数字水印和移动代理的数字管理系统。该方法通过对受保护的媒体内容添加唯一水印标识并注册水印信息，通过移动代理检测水印，从而确定版权归属。

- **中国科学院研究生院**的一份专利在**OMA DRM 1.0**标准的基础上设计了基于数字水印技术的移动媒体版权保护系统。该方法利用抖动调制将数字水印信息载入**DCT**宿主信号中。其特点主要在于对**OMA**标准的支持。

- **达诺媒体有限公司**设计了一套可以用于点对点网络的分布式数字版权管理系统。这个系统通过双向验证方法在点对点网络上的各个节点之间验证并发放许可证书，即会话密钥，系统也可以为集中管理的证书管理模式服务。

1.2 数字版权管理技术的现状与趋势

- **华中科技大学**设计一个将用户使用数字资源计费和使用权利同步管理的系统模型。在查看用户使用情况的同时不会侵犯用户的隐私。许可证中的用户隐私信息通过自动系统处理，从而提高了保密性。系统设计减少了用户需多次申请许可证的情况。
- **索尼公司**提出了一套客户端与服务器端交换许可证书的方法。这个方法中包括一个特殊设计的信息处理设备。该设备中包括一个许可证书存储单元；一个解密单元；还有许可证书的发送器和接收器等等。这个信息处理设备包括一个终端标识（Terminal-ID）寄存器。许可证书的内容包括请求的内容的信息、使用内容的方法和终端标识信息。从服务器上提取出来的许可证书需要被一个密钥签名之后才发送给信息处理终端。

1.2 数字版权管理技术的现状与趋势

- 现有DRM系统、方法和设备的设计与制造开始向一个有机的结合点方向转化。从技术层面上看，将数字水印技术、实用密码技术、网络传输技术、电子和通信技术、计算机技术等为了保护多媒体内容版权归属、防止非法传播使用组合到了一起。
- 尽管形式多种多样，但目的很明确，即禁止超范围使用，禁止非授权传播。
- 现有国际技术标准，如OMA DRM及后来的OMarlin DRM等，以及国内技术标准，如ChinaDRM、AVS等，仅关注于协作方面的标准指定，即不同DRM参与者之间的相互协作通信协议和验证协议。标准化建设还需要向更深层次的技术层面发展，比如水印技术的统一化、权威化，密钥分发的统一化。

数字版权管理技术

MEDIA ASSET MANAGEMENT

1 数字版权管理技术概述

2 DRM在商业应用中的需求

3 DRM标准及技术体系

4 数字加密技术

5 数字水印技术

2.1 功能需求

- DRM源于数字化商业活动中对版权保护的需求，对其功能上的需求包括权限控制、版权认证、内容认证、盗版追踪、操作跟踪等内容。

2.1 功能需求

- **1. 权限控制**
- 对版权保护的最基本的要求就是权限控制。
- 权限控制包括两个方面：
  ① 具有权限的合法用户能够正常使用数字内容，无权限的用户将被部分或完全禁止对数字内容的访问，比如只可以浏览内容摘要等；
  ② 不同的权限具有不同的对数字内容的访问使用能力，版权保护系统应能区分不同的权限，并根据权限的不同控制用户对数字内容的访问。
- 拷贝控制、播放控制、处理能力控制、有效期限制都属于权限控制的范畴。

2.1 功能需求

- 拷贝控制对用户将数字内容在相同或不同设备上复制副本的操作进行限制；
- 播放控制主要对数字内容的播放次数、时间、对象进行限制。
- 处理能力控制是指对用户实施到数字内容上的旋转、剪辑、缩放、添加内容等操作的限制。
- 用户获得的权限往往是通过统一的格式即权力描述语言进行表述的，被描述的权限可能作为权限证书的一部分（如PMI，Privilege Management Infrastructure，授权管理基础设施），也可能直接形成特殊的权限对象与受保护的数字内容一起或分别传递给授权用户（如SDMI）。
- 权限控制的实现方式有很多种比如有第三方参与的身份认证、PMI权限证书、内容加密、安全容器等。

- **2. 版权认证**
- 版权认证属于数字内容版权保护的基本功能，它也包括两部分内容，即：
  1. 所有者鉴别，即验证数字内容的版权归属，即所有者是谁；
  2. 所有权验证，即当多个人声称拥有数字内容的版权时，能够验证数字内容的真正作者，为解决版权纠纷提供依据。
- 申请出版权认证的可能是数字内容制作、分发、使用全过程中的任何实体。
- 版权认证的方法有解密权限描述中的版权信息、提取版权水印、媒体桥技术等。版权信息应具有唯一性、可验证性的特点。

- **3. 内容认证**
- 也称为内容完整性认证，主要是对数字内容自生成以来是否发生过变化做出判断。这种变化可能是全局的也可能是局部的。
- 通常的内容认证方法是采用数字签名技术或信息摘要。
- 签名作为数字内容的辅助数据和内容一同传输、保存，容易丢失。可选的方法是采用水印技术，将签名作为脆弱水印嵌入到数字内容中，内容的改变同样将导致签名不匹配。
- 内容认证属于版权保护的高级功能，往往被司法机关或对内容修改敏感的应用使用。

4. 操作跟踪

- 操作跟踪也属于版权保护的高级功能。数字内容被加入到版权保护系统中后，被传播和使用，在这期间，数字内容可能会被有意、无意的修改，通过操作跟踪可以确定数字作品所经历的修改，进一步有可能恢复出最初的数字内容。
- 实现操作跟踪的简单方法就是在封闭的数字内容使用环境中建立修改日志，记录数字内容被修改所采取的操作。这种方式对服务器来说是有用的，但对用户终端来说却没有意义，因为将侵犯个人隐私，而且任何人也不会报告自己对数字内容的处理。

5. 盗版追踪

- 盗版追踪是指确定数字内容盗版的来源，即第一个把受保护的数字内容泄露出去的用户或实体，这个实体可能是数字作品的制作者本身，也可能是销售者、运营商，或者是终端用户。
- 比如在DiVX增强播放器中就存在盗版追踪技术，它在播放的影片中添加了播放器唯一的水印，通过检测盗版影片中的水印即可判断它的来源。此外，在影片拷贝分发中也可以采用类似的原理，来控制盗版的发生。
- 盗版追踪主要通过数字水印技术来完成，同时为了实现主动的追踪，还应建立网络监控手段，通过追踪代理或网络警察来及时发现存在的盗版。

2.2 性能需求

- DRM的性能上的需求，直接取决于应用环境对DRM的要求，一般包括安全性、可靠性、实时性、健壮性、可扩展性和低复杂度方面的要求。

2.2 性能需求

1. 安全性

- 安全性是版权保护系统最基本的要求，在基于密码技术的版权保护系统中还要建立安全环境来对受保护的数字内容及其相关数据，如权限、版权信息等进行管理，并负责完成与外界的交互。
- 安全性包括算法安全、协议安全、存储安全和认证安全等。
  - **算法安全**是指版权保护系统所使用的密码算法和数字水印算法是安全的，破解、伪造、删除版权将十分困难；
  - **协议安全**是指在不同实体之间交互时遵循的协议不应存在可利用的漏洞，否则即使不破解算法，也可能获得未经保护的数字作品；
  - **存储安全**主要保证在服务器、用户终端受保护的数字内容及其它敏感数据不被有意、无意的破坏。

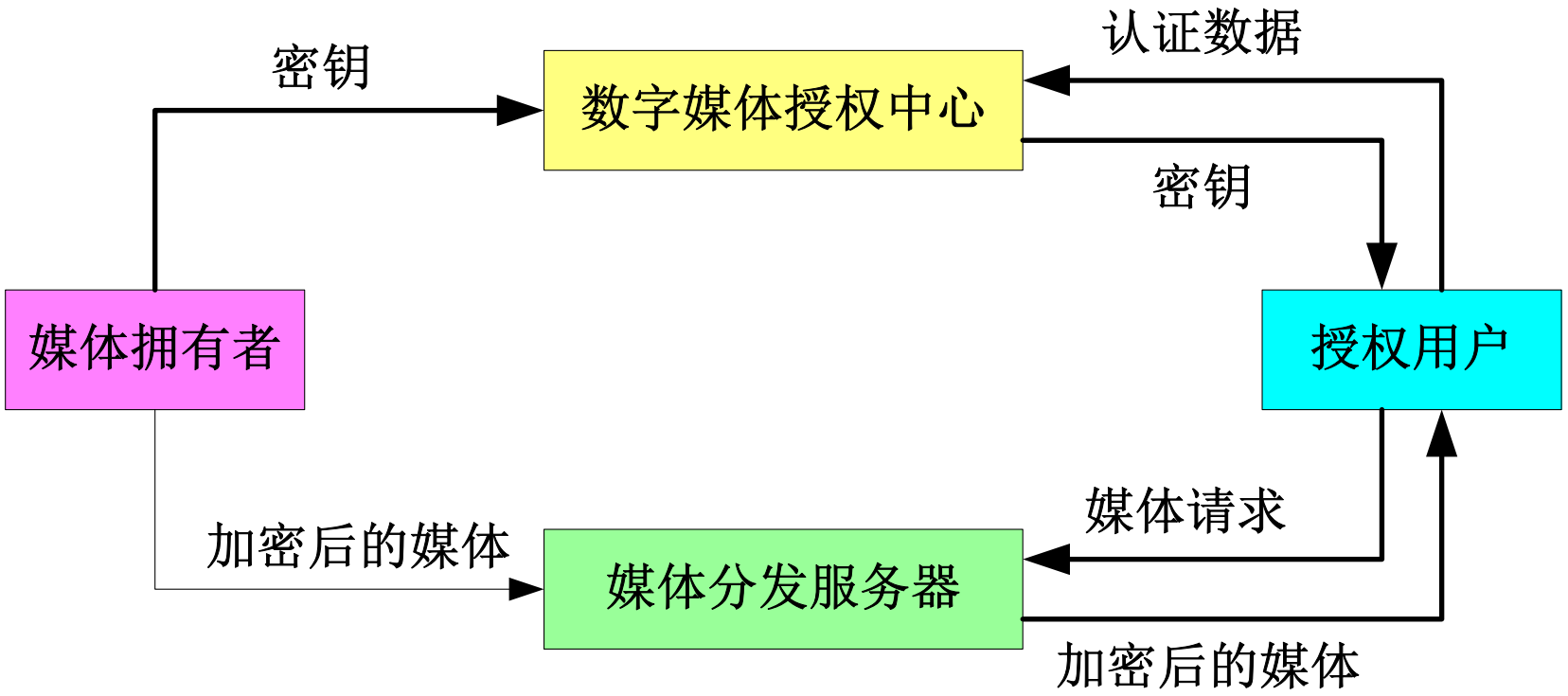
- **2. 可靠性**
- 是指受保护的数字内容不管经过多少次使用、传输、处理，其中的版权信息依然可以被正确的验证。
- 要达到可靠性要求，一方面可以对用户可能的处理操作进行限制，另一方面可以将受保护的数字内容与权限、版权信息等分离，要保证这种联系难以被破坏。
- 当采用数字水印技术时，就要求嵌入的水印能够在其鲁棒性范围内准确地提取出来，如抗打印扫描的数字水印，就应该能够在将数字内容变为纸质内容在变回纸质内容是提取出来。

- **3. 实时性**
- 在一些实时应用和大规模应用的场景中，要求版权保护系统要有好的实时性。比如在彩信的版权保护系统中，服务器端要求其版权认证的处理速度平均应达到100次/秒。实时性的要求给算法、协议的设计、选择、网络的拓扑结构、设备使用、数据库的设计都提出了高的要求。
- 实际实现中应针对应用环境对算法、协议进行优化，并建立具有并发处理、负载均衡等的网络结构，采用高效的分布式数据库设计，从软硬件两方面提高版权保护系统的性能。

- **4. 可扩展性**
- 从权限控制到盗版追踪，体现了功能的扩展，从仅能浏览到可以转发传播是权限的扩展，在数字家庭中异质设备之间的互联互通体现了协议的扩展和相容，从单一加密技术到融合密码和数字水印技术，以及将算法或系统的部分更新以适应新的需求反映了技术的扩展。
- 实现扩展可以采用模块机制设计，比如借鉴MPEG4 IPMP中的“挂钩”可以为系统非常方面的增加新的功能模块。此外，在版权保护的体系框架上可以融合多种标准和技术，建立类似TCP/IP的分层结构，为搭建有效的可扩展的系统平台提供指导。

- **5. 低复杂度**
- 低复杂度主要是指版权保护系统的实施难度和软硬件成本要求，在满足用户其他需求的前提下，应尽量降低其实施复杂度。比如避免在局部应用中使用**PKI**、**PMI**等庞大的基础设施，尽量通过对现有系统软硬件的利用与扩展来实现版权保护功能。
- 此外，如果版权保护系统针对的是终端用户，限制了用户的自由通信能力，那么应尽量少地更改用户设备或软件，否则任何用户都不会主动改变现有的通信方式。

1. 版权保护的一般框架



2.3 版权保护存在的问题

- 该系统的运行过程如下：
  - 系统建立数字内容授权中心，其目的是保存解密密钥并对用户的身份进行认证和授权。
  - 数字内容拥有者制作、编码、加密内容数据。
  - 数字内容拥有者将加密后的数据发送到内容分发服务器，同时将相应的解密密钥（可能与加密密钥不同）安全的发送给数字内容授权中心进行安全存储。
  - 用户根据所请求的媒体分发服务器中内容数据的相关信息，到数字内容授权中心进行用户认证。
  - 用户安全的从数字内容授权中心获得解密密钥，并从内容分发服务器获得所请求的内容数据。
  - 用户使用解密密钥对内容数据进行解密，然后以在线或下载方式使用。

2.3 版权保护存在的问题

2. 不良用户对版权的破坏

- 毫无疑问，加密保护技术在这个框架中起着重要的防盗版作用。但是该框架仅仅是一个数字内容的网络安全框架，只考虑了在服务器上的安全存储和密钥传输过程的安全性，防范网络窃听者和入侵者。
- 在盗版猖獗的今天，存在着大量这样的用户，这些用户以合法的身份进行非法的活动，更具有隐蔽性和不可控性，我们称之为不良用户。不良用户的存在使得防范盗版和最大限度的方便用户访问成为矛盾，如何解决好这一矛盾是进行流媒体版权保护的关键所在。

2.3 版权保护存在的问题

- 以Microsoft Windows Media DRM为例描述不良用户对数字内容版权的破坏。
  - 在服务器端，首先对数字内容用内容密钥加密，然后将内容密钥放入用XML描述的内容许可证中。在获取用户的公钥后，使用用户公钥加密内容许可证。最后，将加密后的数字内容和许可证传送给用户。
  - 在用户端，授权用户在获得加密的数字内容和用自己的公钥加密的内容许可证后，用自己的私钥对许可证进行解密，从而获得内容密钥。有了内容密钥，用户就可以使用它来对内容数据进行解密。
  - 它并没有防范不良用户对内容数据的盗用。只要用户拥有自己的公钥、私钥对，以及对内容数据访问权限，就可以对加密的内容数据进行解密，从而侵犯版权。

2.3 版权保护存在的问题

- 上面的DRM进行版权保护的基础就是，所有授权用户都是可靠的，他们不会作出侵犯版权的行为。但是在如今的网络世界里，这是不可能的。
- 有必要采取更进一步的手段和措施来对内容数据的版权进行更加全面的保护。
  - 一方面必须建立真正安全意义上的从制作、传输到使用的安全环境。在这种安全环境中，最基本的要求就是任何用户都不能通过缓冲区截获内容数据流。
  - 另一方面除了要保护内容数据在传输过程中不被盗用外，还要保护内容数据在播放过程中及播放结束后不被盗用，从而实现完善的数字内容版权保护。

数字版权管理技术

MEDIA ASSET MANAGEMENT

1 数字版权管理技术概述

2 DRM在商业应用中的需求

3 DRM标准及技术体系

4 数字加密技术

5 数字水印技术

3 DRM标准及技术体系

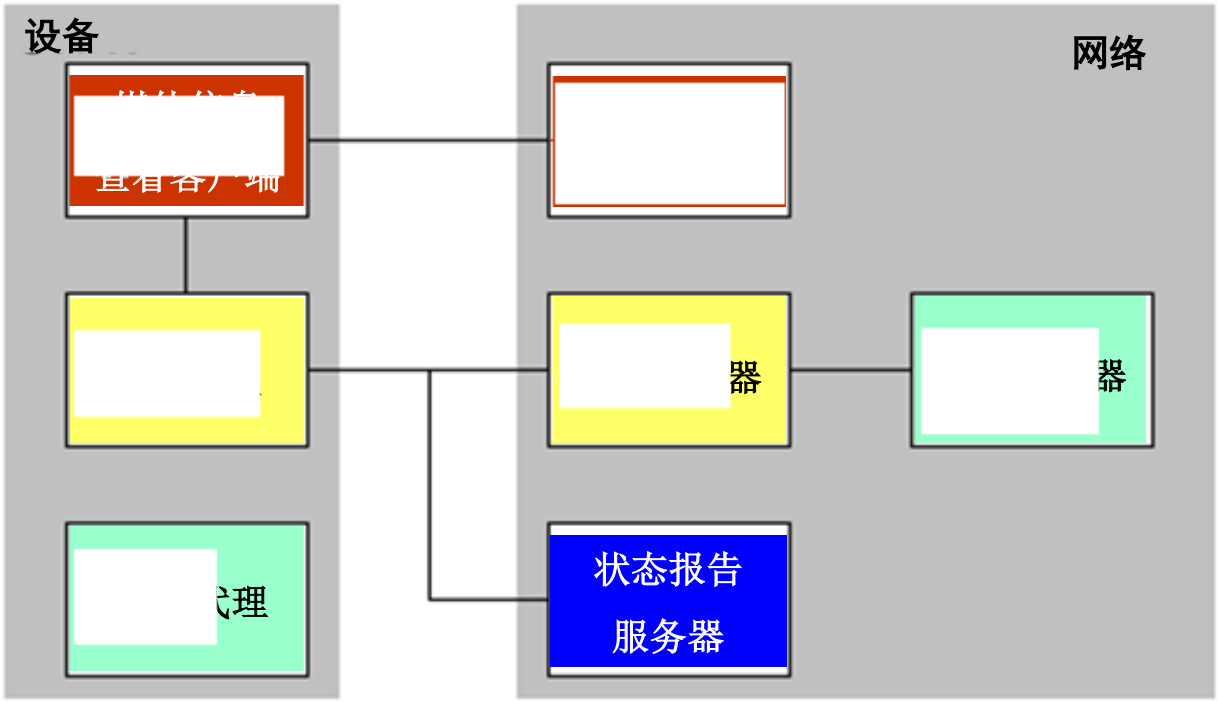
- 目前，国际上很多标准组织和企业联盟进行了DRM技术研究，推出了各自的技术标准。

3.1 OMADRM标准

- OMADRM是由OMA公布的版权保护标准，目前版本为2.0。
- OMADRM提供了一个基于移动终端和网络平台共同作用的版权保护机制，其核心是通过权利来体现媒体内容的价值，强调在用户终端DRMAgent的直接参与下对用户的使用权限进行管理，即根据由SP／CP描述的使用权限控制终端用户对下载内容的使用。用户只有通过购买方式才能获得对于媒体内容的使用权限（如显示等）。不同的使用权限赋予用户不同的处理能力。

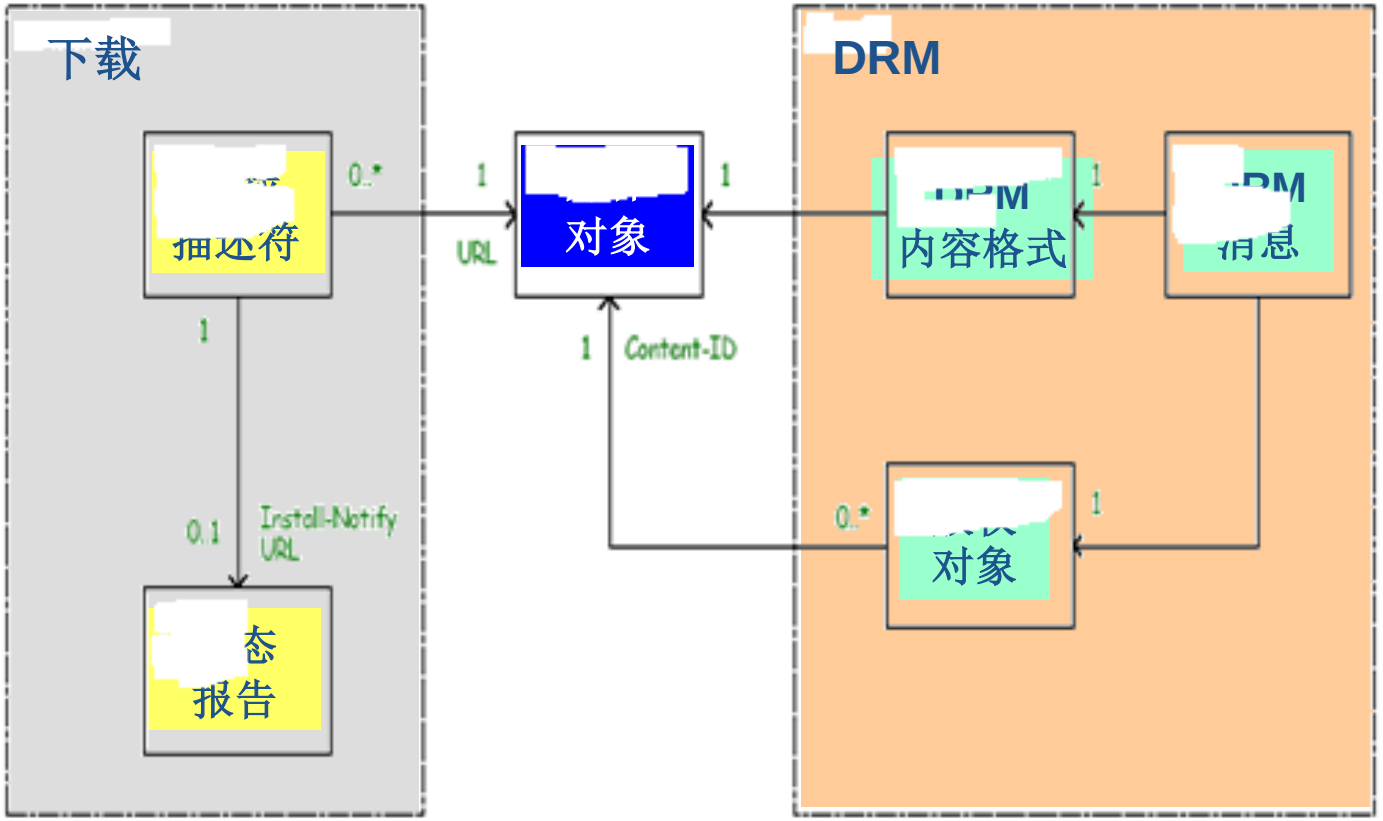
3.1 OMADRM标准

- OMADRM要求在用户移动终端需要有DRM的加解密支持，在网络平台提供CA认证等。同时它也支持网络与用户移动终端的交互，如预览、确认下载等，并可以为用户提供个性化的服务和灵活的商业模式。



- **OMADRM的体系结构**
- 其中“媒体信息服务器”向用户提供对各种媒体的预览，当用户需要下载某个媒体时就启动“下载代理”。网络端的“下载服务器”负责建立媒体的版权，并通过“DRM封装器”采用加密等技术封装版权、用户权限等信息，并与加密后的媒体一起或分别发送给用户。
- 用户的“DRM代理”在得到媒体和用户权限后，将根据用户权限对媒体进行解密并呈现给用户。另外，OMADRM中的“状态报告服务器”负责版权管理过程的调度。

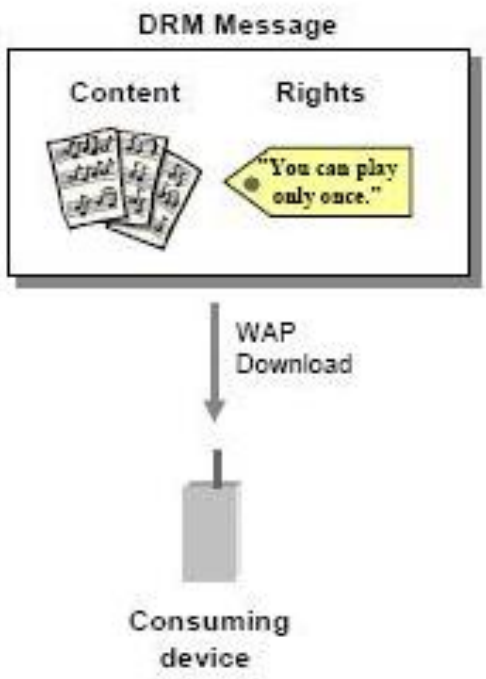
OMADRM的体系结构



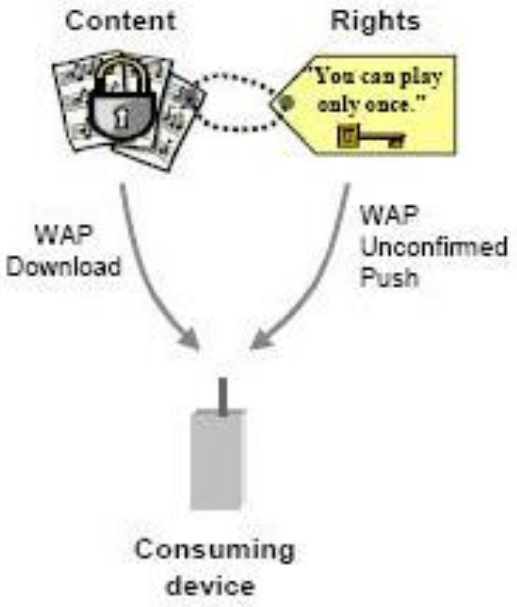
OMADRM媒体下载方式

禁止转发

合并方式



分离方式



- 这三种下载方式在用户终端、媒体封装和服务器等方面也存在一些差别：
- **1、媒体封装要求：**
  - 在禁止转发方式和合并方式下，媒体对象必须以DRM MIME的消息格式进行封装，并且在合并方式中权限对象也被一并封装到同一个DRM MIME消息中；
  - 在分离方式中，加密的媒体对象和包含解密密钥在内的权限对象存在于两个DRM消息中，分别通过WAP download和WAP push传递给用户，用户只获得其中一个是无法完成对媒体对象的使用的。

2、用户终端要求：

- 在用户终端DRM Agent方面，要求能够识别DRM MIME格式中的媒体，提供给用户，但不允许修改和转发；
- 在合并方式中，一方面DRM Agent要提供权限对象的安全存储和访问管理，另一方面DRM Agent需负责对权限对象解析，并根据其中的权限描述来控制用户对媒体的访问。禁止任何形式的转发；
- 在分离方式中，终端除了支持对DRM MIME消息格式的解析，提供安全存储和访问控制外，还必须有能力获得网络通过WAP push传递的权限对象消息，实现用户按权限对媒体的访问。此外，如果权限描述中允许用户对媒体进行转发，则DRM Agent成为转发中介，将媒体对象转发，禁止对权限和密钥的转发。

3、服务器要求：

- 最基本的要求是能够对媒体按照DRM MIME格式进行封装，包括媒体对象和权限对象的封装；
- 若系统需要支持用户对流媒体等的实时访问，服务器还应支持对媒体的实时封装，这就对服务器的组织、媒体的封装技术等提出了根高的要求；
- 对存在权限对象的系统，服务器应提供对权限、密钥的安全存储和管理以及分发。

3.2 WDRM标准

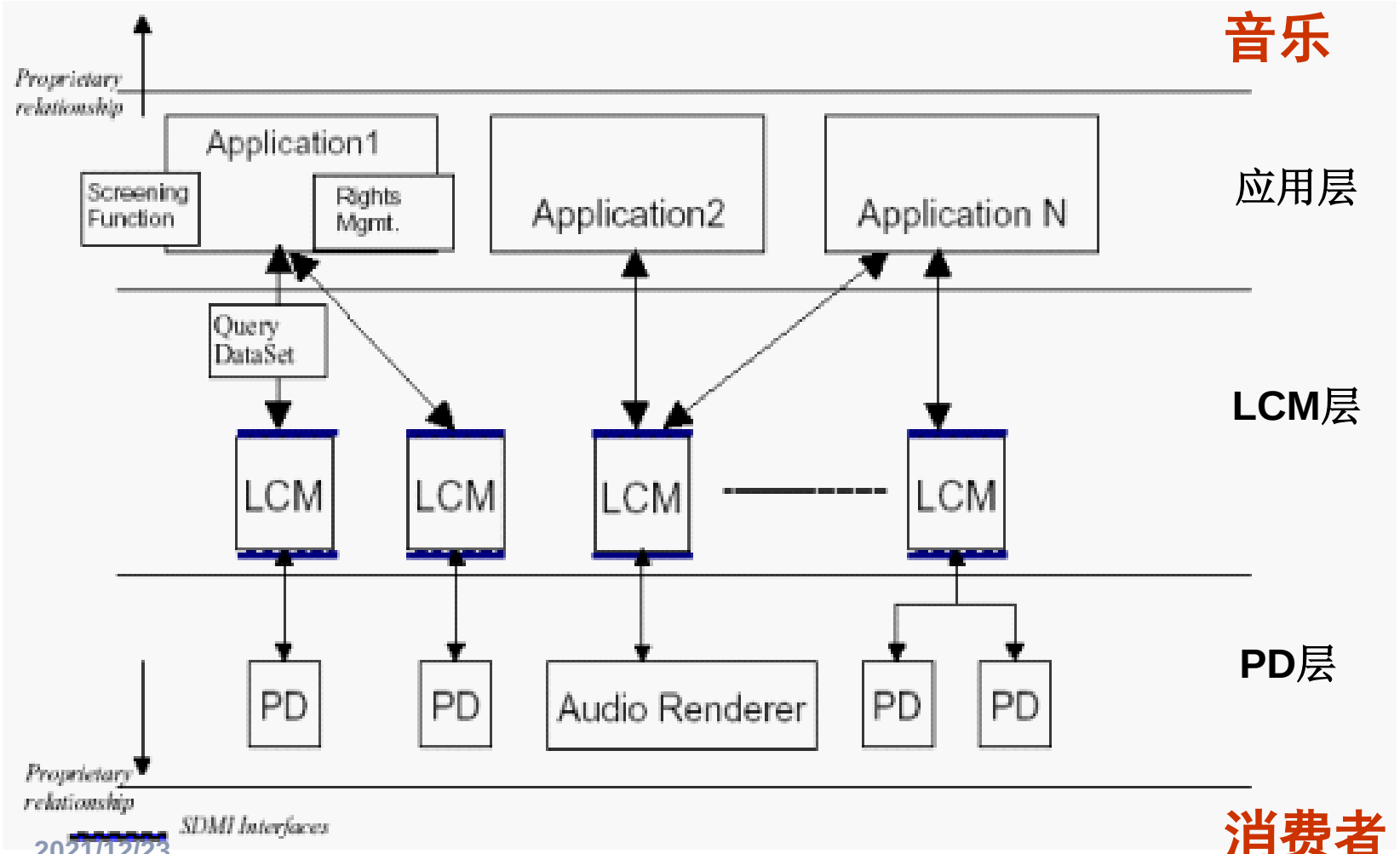
- **WDRM（Watermark-based DRM）基于数字水印的DRM**系统，是综合数字水印、密码学等的综合解决方案，其核心技术为数字水印技术。通过WDRM对版权的保护与管理，保持数字内容在网络中下载、转发、上传等过程中一致性，体现媒体内容本身的价值。
- 目前，通过终端的版权处理能力来实现对数字内容版权保护与管理还不可行。但是，数字水印技术由于其在版权保护方面的独特能力，成为目前的唯一之选。
- 考虑到WDRM的升级和与OMADRM的互补，其体系结构与OMADRM具有一致性，可以很方便的进行扩展，而且WDRM与OMADRM在安全性上也形成互补。
- 基于数字水印技术的版权保护与管理系统必然成为将来完善的版权保护与管理的重要组成部分。

3.3 SDMI规范

- 1999年，音乐界有关公司组成了SDMI（Secure Digital Music Initiative，安全数字音乐促进）组织，目前加入SDMI的技术和娱乐公司已经超过了160家。
- SDMI提出了面向计算机和各种数字设备上数字音频的开放的版权保护规范和技术框架，在为用户提供灵活方便的音频体验、诸如复制等的使用和访问方式的同时，为艺术作品在播放、存储、分发时提供了一个安全环境，最大限度的保护了艺术作品的版权，促进了与数字音频相关的商务和技术的发展。
- SDMI是一个开放的组织，涉及制作、销售、信息技术等领域的企业和团体。只要是符合SDMI规范的软硬件就可以播放符合SDMI规范的数字音频和普通的音频文件，来实现对版权的保护。

3.3 SDMI规范

- SDMI 1.0提供了针对便携设备数字音频的版权保护规范：



3.3 SDMI规范

- 应用层包括所有基于数字音频的应用，如建立媒体库、播放音频等。通过与LCM之间的通信来完成查询PD/PM的能力、进行播放等工作。并且应用层中的各应用在与其他应用和LCM之间传输受SDMI保护的内容时，首先要采用安全认证通道（SAC）对其他应用和LCM作出认证。
- LCM作为应用和PD的中间层，需要根据内容使用规则，对应用和PD的合法性进行认证，只有两者均符合要求时，才从应用获得的受保护的音频内容，并传送给PD/PM。并提供LCM-应用接口、文件管理及内容管理接口。
- PD层是播放设备层，同时也可以包括PM。PD从LCM或PM获得受SDMI保护的内容后，根据其使用规则进行音频内容的播放等处理。PD可以向LCM提供自己的状态和处理能力，并可以从内置的麦克风获得外部的模拟输入，并转换为仅能用于本地使用的、受SDMI保护的内容。

3.4 MPEG中的IPMP技术

- 在MPEG体系（MPEG2、MPEG4、MPEG21等）中定义了用于知识产权保护的IPMP（知识产权管理与保护）技术架构。
- MPEG-2中的IPMP工具有两种：
- 1. 版权描述符（copyright descriptor）：
  - 用于标识单个流以及形成节目流的集合物。版权描述符是一个32比特的惟一版权标识号，用于标识作品的类型（类似ISBN）。这个标识号指向一个注册机构，称为版权号。通过使用版权号，每一个注册机构能够定义自己的句法和文法以标识著作。
- 2. 实现保护的措施：
  - 用信号表示特定的数据包（元素流或传输流）是否被置乱（scrambled）。
  - 发送在条件访问（CA）系统中被使用的消息。

3.4 MPEG中的IPMP技术

- MPEG4中的IPMP提供了在不同领域的多种产品和服务的基础安全框架（IPMP-ES）和标准化的IPMP界面（IPMP-DS），实现了访问控制等用户功能，制定了各种安全技术的统一的接口标准，为媒体版权保护的应用提供了最大的灵活性。
- MPEG4 IPMP也为客户端的数字媒体版权保护提供了一个框架，该框架为来自网络和媒体设备的数据提供了保护。它是建立在原MPEG4标准基础上的，通过“挂钩”机制来实现媒体版权保护系统对数据流保护的。它提供了灵活、丰富的机制来实现并允许开发者为其进行扩展。
- 基本的IPMP系统是由IPMP规则提取、解密和水印检测、播放控制等组成。不同的应用可以采用插件的方式嵌入相应的技术实现。

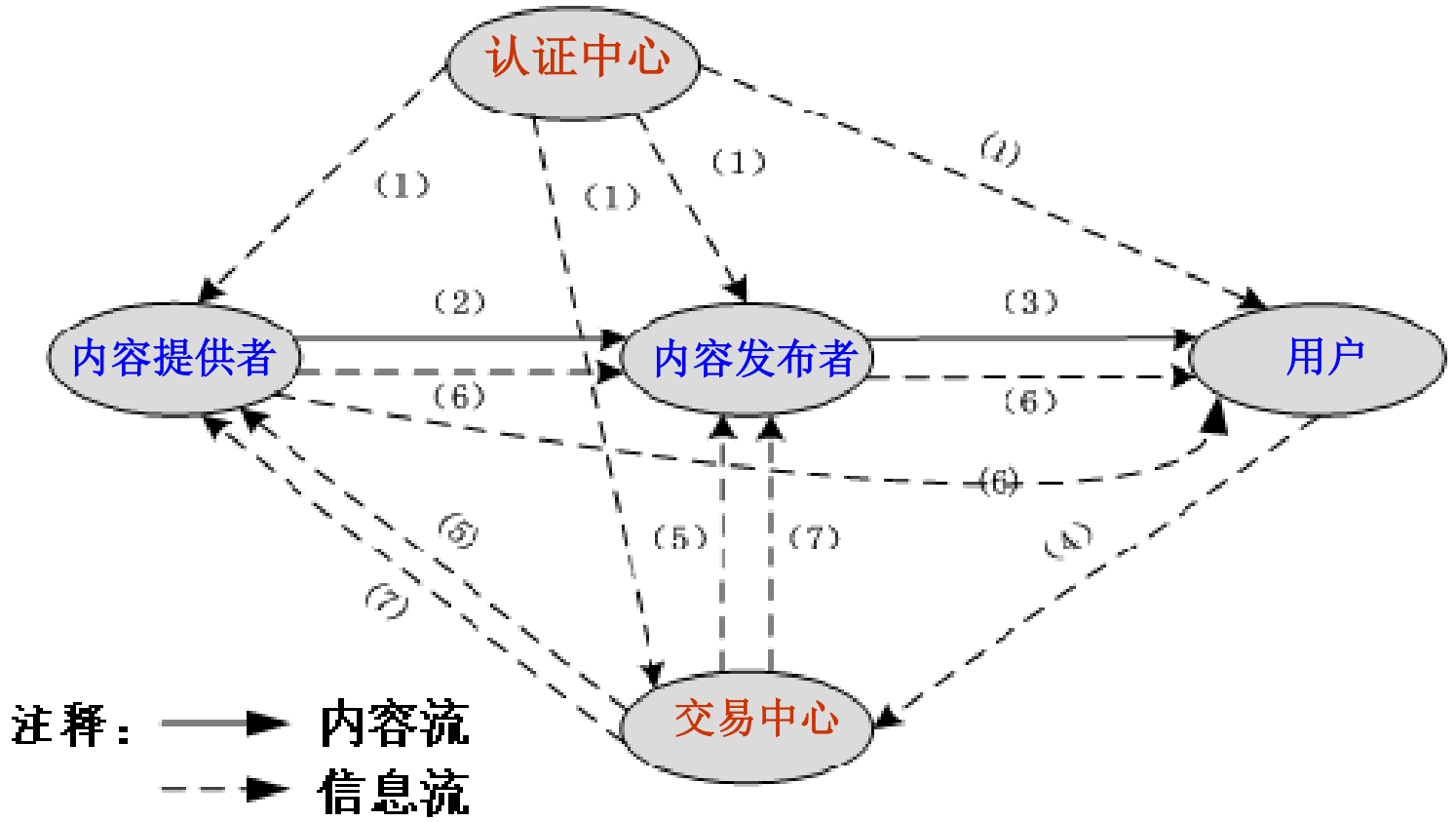
3.4 MPEG中的IPMP技术

- MPEG21 IPMP是对MPEG4 IPMP的扩充，通过定义权力数据字典和权力描述语言，提供了交互性IPMP的能力并通过MPEG21 IPMP透明化了不同数据源的安全管理。
- 包括：
  - 标准化方式在异地搜索IPMP工具；
  - 不同IPMP工具之间以及IPMP工具和终端之间的消息交换机制；
  - IPMP工具的认证；
  - …等内容。

3.5 ChinaDRM标准

- ChinaDRM是由广电总局、CCTV发起的针对中国广播影视资料版权保护与权限管理的开放论坛，清华大学、中国传媒大学等多家科研院校以及Intel、汤姆逊、Sony等多家广电企业积极参与。
- 目前其1.0白皮书已经公布，重点给出了中国广播影视资料DRM的参考模型。
- ChinaDRM参考模型定义了从内容提供者—内容发布者—用户的安全而公开的模型，从技术上实现对内容制作、集成、分发和消费所有环节的权利保护。
- 此模型不仅能够适应于数字电视、网络电视等实时的广播应用模式，同时也可以适应于非实时的应用。

- **ChinaDRM的参考模型框图。**



3.5 ChinaDRM标准

- 具体说明如下：
  - 1）认证中心向内容提供者、内容发布者、交易中心和用户签发身份证书。
  - 2）内容提供者根据某种交易把带版权信息的数字媒体内容发送给内容发布者，该数字媒体内容可能经保护，也可能未经保护。
  - 3）内容发布者从内容提供者处获得带版权信息的数字媒体内容后，根据用户申请，将经过处理得到的受保护的数字媒体内容发送给用户。
  - 4）用户向交易中心付费并申请许可证。
  - 5）交易中心通知内容提供者或内容发布者向用户签发许可证。基于不同的商业模式，内容提供者和内容发布者都有可能直接向用户签发许可证。
  - 6）内容提供者直接向用户签发许可证，或者根据交易合同通过内容发布者向用户签发许可证。
  - 7）交易中心向内容提供者和内容发布者提供利润分成和内容的使用信息。

3.6 其他DRM技术与标准

- ***Windows Media Player*** 内置有 DRM 组件。Windows Media 版权管理软件来完成对媒体文件打包的过程。打包后的媒体被采用特殊算法的密钥加密。该密钥被包含在一个加密的许可证中，而这个许可证将不随文件一同发送。同时打包后的文件中还包含其他信息，比如获取许可证的URL地址等。加密以后的音乐文件采用WMA扩展名，而视频文件采用WMV扩展名。
- ***ReadNetworks***的产品是helix drm。由于helix drm提供被称为“native support（基于helix drm自身的支持）”和“transfer to secure memory（向具有版权保护功能的存储进行发送）”的两种模式，因此可以在各种家电产品中处理多种安全格式。

3.6 其他DRM技术与标准

- *方正Apabi电子书*（eBook）是目前唯一有完整DRM技术的中文电子书系统，涉及制作、发行、销售、数字图书馆，以及包括手持阅读器在内的多种阅读平台，与国外同类系统相比，总体技术水平相当。而且，Apabi DRM在电子书交易的体系结构、数字图书馆对eBook DRM的支持以及eBook DRM计数机制等方面有所创新。在2002年，方正Apabi软件被认定为“北京市高新技术成果转化项目”，同年还被中国计算机报评为“2002年中国信息化最佳应用典型的经典案例”。

数字版权管理技术

MEDIA ASSET MANAGEMENT

1 数字版权管理技术概述

2 DRM在商业应用中的需求

3 DRM标准及技术体系

4 数字加密技术

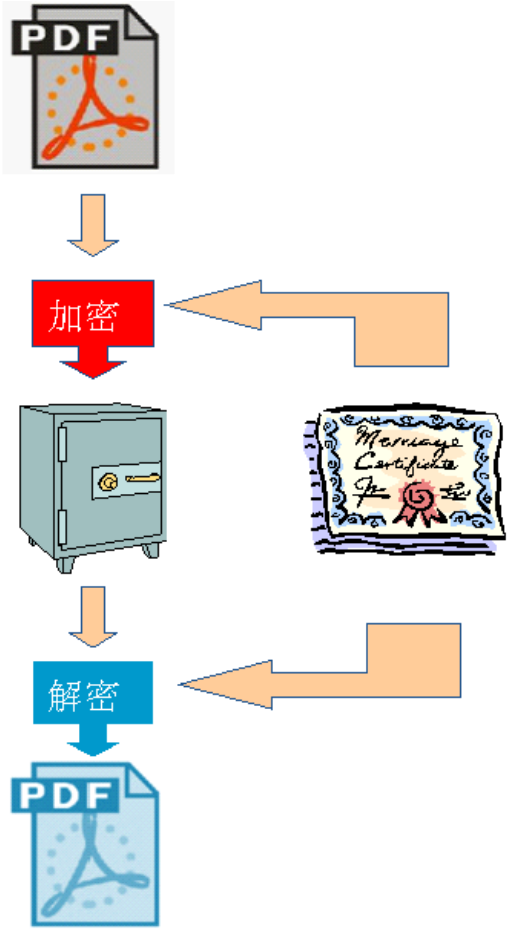
5 数字水印技术

4.1 数字加密技术概述

- 加密技术是电子商务采取的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再还原（解密）。
- 加密技术包括两个元素：算法和密钥。算法是将普通的文本或者可以理解的信息与一串数字（密钥）的结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解码的一种算法。

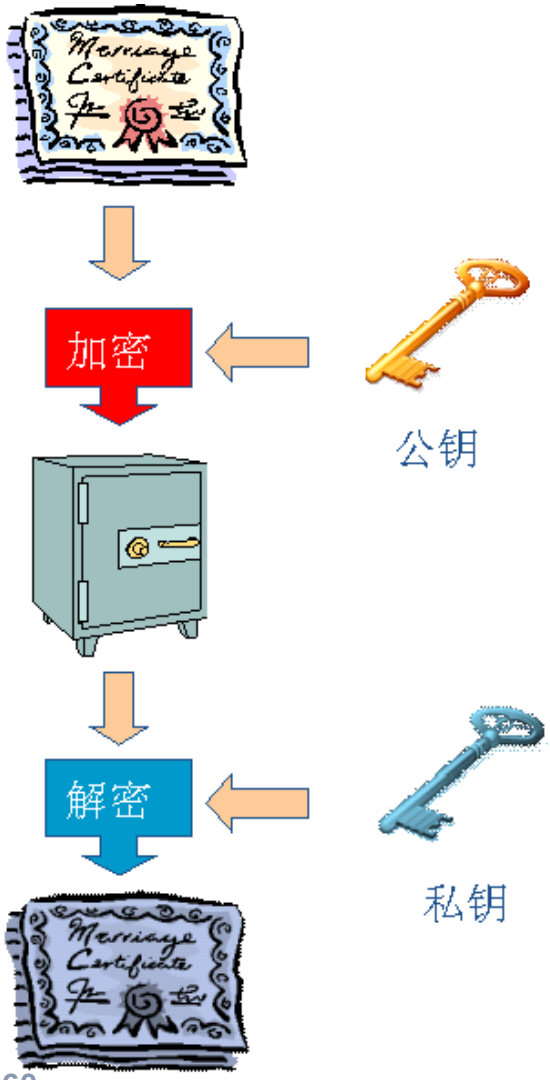
4.1 数字加密技术概述

- 密钥加密技术的密码体制分为对称密钥体制和非对称密钥体制两种。
- 对称加密以数据加密标准（DES，Data Encryption Standard）算法为典型代表。



4.1 数字加密技术概述

- 非对称加密通常以RSA（由MIT的Ron Rivest、Adi Shamirh和Len Adleman三人提出）算法为代表。
- 对称加密的加密密钥和解密密钥相同，而非对称加密的加密密钥和解密密钥不同。加密密钥可以公开而解密密钥需要保密。



4.1 数字加密技术概述

- 加密技术用于版权保护和版权管理，需要通过网络的分布式计算环境来实现。
- 这方面技术有比如数字指纹、数字签名、安全容器等都属于加密技术。
- 加密技术的核心是密码学。
- 许多科研机构和公司针对数字媒体的版权保护从各个角度分别展开了研究，比如Intertrust公司的DigiBox技术，该技术能根据一定的使用规则使受保护的信息在整个生命期内无论传到任何地方都将受到保护；IBM公司的Cryptolope技术，该技术的特征是用安全加密技术封装要保护的数字媒体信息的内容；Digimarc公司在研究基于数字水印的媒体信息版权保护等等。

4.2 安全容器技术

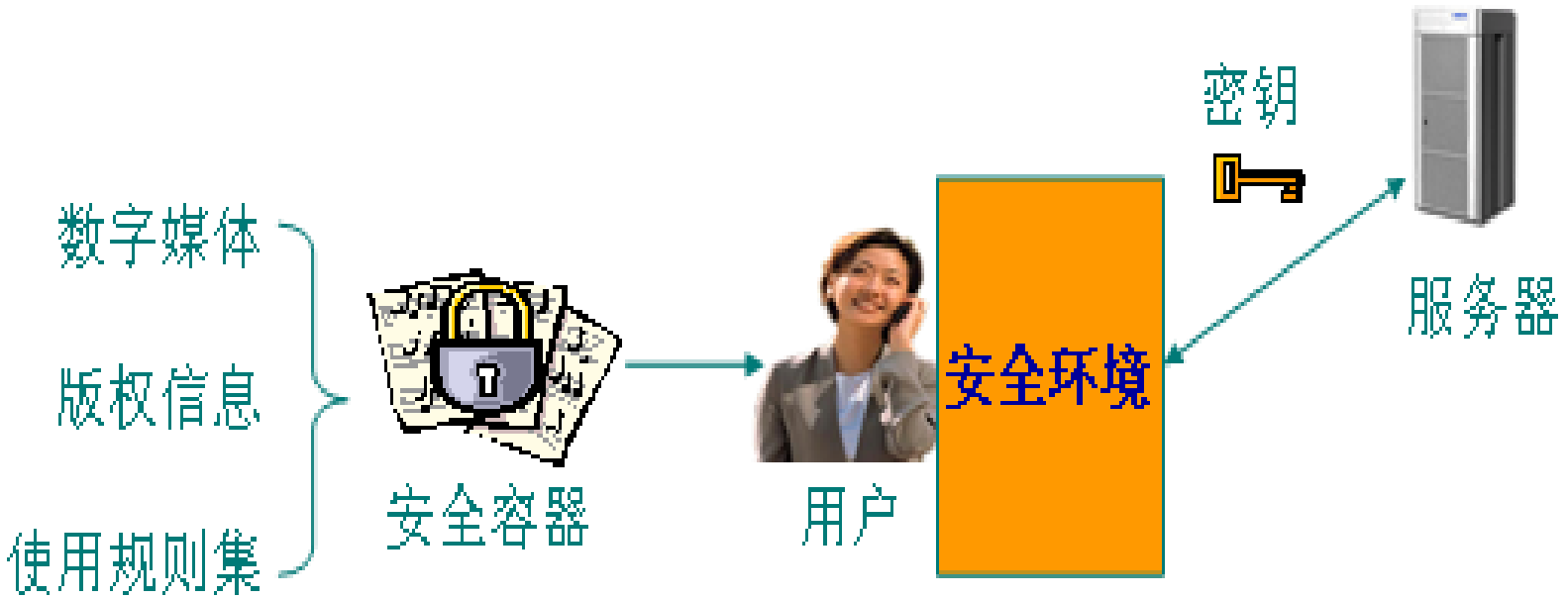
- 安全容器技术的核心是安全容器，它也是采用加密机制封装起来的一个防篡改的用于保护数字媒体及其版权信息、使用规则的信息包，即
- **安全容器=（数字媒体，版权信息，使用规则集）**
  - 采用基于安全容器技术的版权保护系统，数字媒体一经发布，不管是在客户端还是在服务器端，其都是以安全容器的形式存在。这样既能保证数字媒体信息在存储上的安全，也能保证数字媒体在传输上的安全，以及使用安全，比如防止非法使用和非法拷贝等，对版权的保护涉及媒体的整个生存期。

4.2 安全容器技术

- 采用安全容器技术进行数字版权保护的一般过程：
  - 1、采用三重DES、RSA等加密算法，将<数字媒体、版权信息、使用规则集>封装在一个安全容器中，安全容器作为产品进行发布，密钥被安全存储在服务器；
  - 2、用户获得安全容器，并被保存在用户的可信环境中；
  - 3、用户向服务器提交自己的ID，并申请解密密钥，服务器在认证用户身份成功后，将解密密钥发送给用户的可信环境；
  - 4、用户的可信环境将安全容器解密，并按使用规则控制用户对数字媒体的使用。

4.2 安全容器技术

- 采用安全容器技术进行数字版权保护的一般过程：



4.2 安全容器技术

- 安全容器技术被认为是现在最安全的版权技术。但是同样，它也使来源于密码学，也要求用户端有加解密能力，以及一些更高的支持要求，比如用户端要建立可信环境：安全文件系统、安全数据库等来保存媒体数据、使用规则、权限、解密密钥等一些敏感数据。因为一旦用户直接获得了这些数据，就有可能对版权构成威胁。

4.3 移动Agent技术

- 所谓移动Agent一般是指一段可执行的程序代码，它在复杂的网络系统中能自主地从一台主机移动到另一台主机，该程序能够选择何时、何地移动。
- Agent可以根据需要生成子Agent，子Agent与父Agent具有相同的性质，各Agent之间独立或相互协作来完成任务。
- 移动代理最主要的特性是自主性、移动性，其他还有安全性、协作性等。
  - **移动性**是指可以在运行过程中挂起，移动到目标网络或主机后继续执行。
  - **自主性**是指能在没有外部的干涉或指导的情况下持续运行。
  - **安全性**是指自身及其运行环境的安全保障。
  - **协作性**是指各Agent之间可以相互通信合作，共同完成任务。

4.3 移动Agent技术

- 移动**Agent**在数字版权保护中应用的一般过程。
  - 1、用户与服务器之间签订某种协议，规定了用户对媒体的使用权限，用户对该协议签名，服务器对其加密。加密签名后协议的成为移动代理的一部分；
  - 2、当用户需要某个媒体时，移动代理携带用户签署的协议等信息移动到服务器；
  - 3、移动代理通过服务器验证用户签名的有效性及用户拥有的权限；
  - 4、验证通过后，移动代理移动到内容服务器，将媒体数据打包，同时也产生计费数据，叫计费服务器处理；
  - 5、移动代理携带打包的媒体数据回到用户，交给用户端的安全环境，并根据用户权限控制对媒体数据的使用。

4.3 移动Agent技术

- 移动Agent只有在需要的时候才传输媒体数据，因此可以有效地节约网络带宽。而且由于移动Agent可以在网络上自主地运行，用户只需要接受其运行结果，因此用户在Agent运行期间可以断开网络，移动Agent也会等待用户重新连接后才反馈结果。
- 但是移动Agent离实际应用还有许多工作要做，主要集中在Agent命名、Agent通信、Agent寻址等方面，另外在版权保护方面也要考虑其安全环境的建立问题等。

4.4 数字签名及指纹技术

- 数字签名属于**加密技术**，通常用来进行身份认证、数据完整性、不可否认性认证等。要求用户有获得密钥并验证签名的能力。
- 采用数字签名可以保证签名者无法否认他签署过的信息，而验证者也无法伪造他人的签名。
- 数字签名技术主要采用的是公钥密码体制，签名者利用自己的私钥对信息进行签名，验证者利用签名者的公钥进行验证。一个数字签名方案有两部分组成，即签名算法和验证算法。

4.4 数字签名及指纹技术

- 数字签名技术也可以用于版权保护而且数字签名往往与数字指纹技术结合使用。一般过程如下：
  - 1、版权拥有者使用公开的特殊的散列函数Hash（可以对任意长的信息产生固定长的输出）对媒体数据M处理得到固定长的散列值H；
  - 2、版权拥有者使用自己的私钥对H进行解密操作，得到签名S，该签名标识了版权拥有者对媒体数据M拥有版权；
  - 3、S和M将作为一个整体，在安全环境内传输，用户可以使用M而不破坏S；
  - 4、当发生版权问题或用户需要验证M的版权归属时，首先利用版权拥有者A的公钥对S进行加密操作，得到H，然后用散列函数Hash对M处理也得到一个H，比较这两个H，如果一致，则说明A拥有M的版权。

4.4 数字签名及指纹技术

- 数字签名与受保护的信息是互相分离的，也就是说，根据受保护的媒体得到签名后，指纹、签名可以作为一个独立的单位与媒体分别传输。因此，为了在验证签名之前签名不被破坏，通常采用将信息和签名一起加密进行传输。在用户端就必须存在相应的解密模块，并能为媒体数据提供安全的存储环境。
- 另外，**数字指纹**作为媒体数据的摘要，可以在服务器端加以保存，并通过匹配来跟踪和控制数字内容的分发。

4.4 数字签名及指纹技术

- 数字签名与受保护的信息是互相分离的，也就是说，根据受保护的媒体得到签名后，指纹、签名可以作为一个独立的单位与媒体分别传输。因此，为了在验证签名之前签名不被破坏，通常采用将信息和签名一起加密进行传输。在用户端就必须存在相应的解密模块，并能为媒体数据提供安全的存储环境。
- 另外，**数字指纹**作为媒体数据的摘要，可以在服务器端加以保存，并通过匹配来跟踪和控制数字内容的分发。

数字版权管理技术

MEDIA ASSET MANAGEMENT

1. 数字版权管理技术概述
2. DRM在商业应用中的需求
3. DRM标准及技术体系
4. 数字加密技术
5. 数字水印技术

5.1 数字水印技术概述

- 与加密技术相反，**数字水印技术**可以不考虑用户终端的情况，而融入被保护的媒体中，作为其完整的一部分被传输。数字水印技术是属于事后追究性质，它依赖于完善的法律体系，当产生版权纠纷时，它以检测媒体中是否含有水印信息作为法律上认定侵权的证据。因此，它与加密技术有着本质上的不同。

5.1 数字水印技术概述

- 数字水印技术是信息隐藏技术的一个分支，他在强调数据安全性的同时，保持载体的不变性，即将水印信息隐藏到载体中后，载体的特性不发生可见的变化，不产生可感知的失真。
- 根据在版权保护中的目的不同，可以分为脆弱性水印和鲁棒性水印两类。
- 脆弱性水印要求当含有水印信息的载体（隐秘载体）在遭到任何不可容忍的微小的破坏后，无法再次被检测出来。脆弱性水印主要用于完整性保护。
- 鲁棒性水印与此相反，他要求无论隐秘载体经受什么样的破坏和攻击，水印信息均可以被检测出来。利用鲁棒性水印可在数字媒体中嵌入版权信息，在产生版权问题时，可以提取来验证版权的归属。

5.1 数字水印技术概述

- 数字水印技术需要具备以下的基本条件：
  - 隐藏于数字作品中且不可感知；
  - 可以被专用的数字电路识别；
  - 不必获取完整数据，仅从数据流中即可检测到数字水印；
  - 可以标记复制信息；
  - 漏检概率低；
  - 对于常用的信号处理过程具有鲁棒性；
  - 水印内容（字段）的设计必须合理；
- 对于广播电视企业来说，在多媒体内容发布的时候是无法区分合法用户和非法用户的，因此，广电节目的版权所有者最关心的是内容是否被非法使用。所以，在广电业的应用中，强鲁棒、低感知多媒体内容水印技术与应用是研究的重点。

- 比较水印技术与加密技术的不同之处：
  - 1．在**版权保护的原理**方面，密码技术实现了对数字内容的访问控制，拥有密钥或权限的合法用户才能使用数字内容；数字水印技术则通过特定的嵌入提取算法实现了对数字内容版权归属的验证，进一步还可以实现对版权真伪的鉴别和盗版来源的追踪；
  - 2．基于密码技术的版权保护，其权限、签名与受保护的数字内容是相互分离的，或者要通过外在的数据结构（如指针、多部分消息）将两者联系起来，用户可能破坏这种关系；而在基于数字水印技术的版权保护中，版权信息、权限、签名等都被作为水印嵌入到了数字内容当中，与内容融为一体，如果要破坏他们的联系，就必须破坏内容的可用性；

5.1 数字水印技术概述

- 3．通过破解密钥可以破坏密码系统；而要完全破坏数字水印系统，除了要破解密钥外，还要通过信号处理等方式对数字内容进行修改，但会降低数字内容的可用性；
- 4．密码系统无法抵抗不良用户对数字内容版权的破坏，往往需要在用户端添加安全模块，如智能卡、DRM代理等，提高了用户成本，使得其实际安全性依赖于终端的安全性；由于嵌入水印的数字作品可以正常使用，版权的保护对用户来说可以是透明的，不良用户可能获得数字内容，但无法去除对内容的保护；
- 5．基于密码技术的版权保护，无论什么格式的数字内容，都可以采用相同的加密算法，算法的强壮性与实际应用场景无关；而在基于数字水印技术的版权保护中，水印算法的设计必须根据应用场景的鲁棒性、保真性和水印容量的需求进行，同时不同的内容格式，如图像和视频，其算法一般不同。

5.1 数字水印技术概述

- 从上面的比较和前面的分析可以看出，密码技术更适合进行权限控制，水印技术更适合于操作跟踪、盗版追踪。
- 单独靠密码技术无法达到完全的版权保护，而数字水印技术也无法替代密码技术的作用，两者必然是相互补充，结合各自的优势建立完善的版权保护体系。

5.2 数字水印技术的一般需求

- **1. 技术需求**
- （1）不可感知性与载体的保真性
  - **不可感知性**是大多数多媒体应用对数字水印的最基本技术要求，水印的嵌入应不影响载体的保真度或品质。
- （2）水印模式与容量要求
  - 根据应用场景的需求确定采用的水印模式和实际需要嵌入的水印比特数。
  - 主要的水印模式有两种，固定模式水印与任意信息水印。
  - **固定模式水印**嵌入的水印是预先定义的有限的几种水印标记，在检测时通过假设检验等方法确定水印的存在；
  - **任意信息水印**嵌入的是多符号序列，采用时（空）分、频分、码分等复用方式嵌入水印。

5.2 数字水印技术的一般需求

- （3）安全性与授权访问
  - 为了增强水印的安全性，水印的嵌入应与对称或非对称密钥相结合。
- （4）与应用场景相关的鲁棒性
  - 在理想的情况下，嵌入数字水印可以抵抗任何攻击，但实际上这样的数字水印是不存在的，往往只能根据应用场景的特点和可能遭遇的攻击来确定对数字水印的鲁棒性需求。通过冗余嵌入或纠错编码可以提高水印的鲁棒性，甚至可以从部分载体中恢复水印，但是却对载体的水印容量有极大的影响。

5.2 数字水印技术的一般需求

- （5）算法的实时性和低复杂度
  - 一方面，在流媒体等现场实时广播中，要求在这些媒体中嵌入、检测水印的算法简单、快速，满足实时性的要求；另一方面，对于用户也需要实时的媒体播放和体验，还要考虑有限的存储空间，要根据时间复杂度和空间复杂度的要求对数字水印算法进行设计和选择。
- （6）盲检测与非盲检测水印
  - 盲检测 (Blind Detection) 是指检测时不需要原始图像的检测；非盲检测就是检测时需要提供原始图像的检测。➔

- 非盲检测水印比盲检测水印具有更高的鲁棒性。在水印检测和提取时，可以利用原始载体与攻击后载体的差异，对遭受到的攻击进行估计和逆向恢复，可以有效地抵抗同步攻击，从而提高水印的鲁棒性。但是在大量的应用，如数字视频和移动媒体版权保护、数据监控与跟踪等，都需要盲检测水印技术，由于受保护的载体数据量很大，在检测和提取时无法获得关于原始载体的任何信息。

❖ （7）多水印技术

- 在实际商用的数字水印系统中，往往需要嵌入多个水印，来分别表示不同的信息。多水印的嵌入将会对各水印的可验证性产生影响，一个水印的嵌入自然构成了对前面嵌入水印的一次攻击，同时载体的保真度也将受到影响。在设计选择这些水印算法时，必须从原理上避免或减少相互之间的影响。

5.2 数字水印技术的一般需求

- **2. 功能需求**
- （1）内容认证：利用嵌入其中的数字水印可以鉴定数字照片的来源和证实其完整性，以及注册的照片是否来自认证的数码相机和是否被篡改。
  - 内容认证对水印的鲁棒性要求较低。它包括三个层次的任务，即完整性证明、定位修改、内容重构。
  - **完整性证明**保护载体不被任何形式和非合理形式的修改。脆弱水印、半脆弱水印、半脆弱签名都被用于完整性证明。
  - **定位修改**，即局部认证，用来确定载体所发生的局部变化，包括块认证、像素认证等。

5.2 数字水印技术的一般需求

- （2）拷贝控制与数字指纹：在每一份数字作品的拷贝中添加使用者的唯一标识，即指纹，当发现盗版时，即可根据该标识确定哪一个用户进行了非法的复制传播。
  - 作为**数字指纹**的数字水印技术应具有较高的鲁棒性，应能抵抗各种数据处理和恶意攻击。数字指纹应具有匿名性，即发行者、使用者都不知道水印的确切内容，无法伪造、抵赖、删除。需要可信的或半可信的第三方机构帮助完成水印的嵌入、检测、认证等。
  - 数字指纹的**嵌入和提取**实际上包括了水印算法和交互协议两方面，任何一方面的安全漏洞都会导致指纹的失效或失信。

5.2 数字水印技术的一般需求

- 数字指纹主要面对的是共谋攻击，即多个用户利用各自手中的拷贝，共同生成载体的一个新拷贝，并删除其中的指纹和版权。**抵抗共谋攻击**的方法主要有限制拷贝数量、共谋安全的编码等，但是却也妨碍了载体的传播，降低了载体的水印容量。

❖ （3）版权保护：版权保护对数字水印的鲁棒性要求最高，应能抵抗现有的各种攻击，同时对艺术作品等都要求较高的水印不可感知性，为了方便版权的鉴别和其他后续处理，要求水印算法应具有较高的水印容量。真正商用的版权保护系统需要水印算法、协议标准的共同支持，如欧洲委员会**DGIII**计划制定了网络数字产品的知识产权保护（**IPR**）认证和保护体系标准（**IMPRIMATUR**）等。

5.2 数字水印技术的一般需求

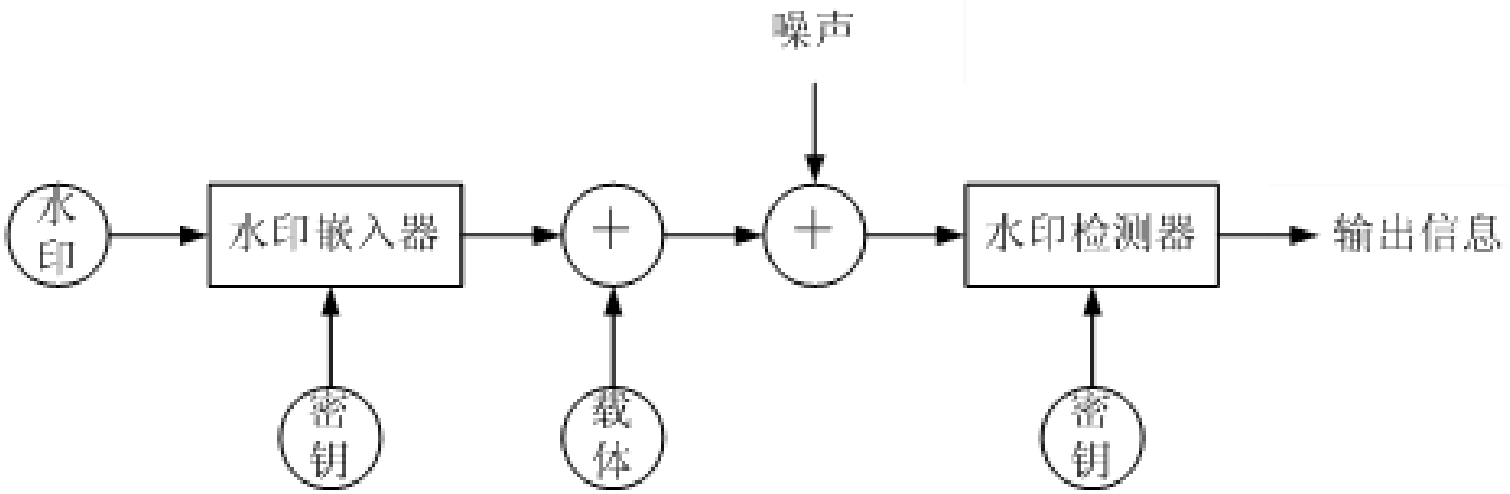
- （4）隐秘通信：把需要传递的秘密信息嵌入到公开的媒体中，这将有效地减少遭受攻击的可能性。如果再结合密码学的方法，即使敌方知道秘密信息的存在，要提取和破译该信息也是十分困难的。也可以把数字媒体附加描述和参考信息作为水印加到媒体中，供将来使用。
  - 替音电话技术就是把需要传递的秘密语音信息加密后嵌入到公开线路中的音频中，窃听者听到的是无关紧要的对话，这将有效地减少遭受攻击的可能性。即使敌方知道秘密语音的存在，要提取和破译该语音信息也是十分困难。
  - **隐秘通信**对数字水印的鲁棒性要求较低，主要是需要抵抗未经授权的访问、模数和数模转换等攻击，但它在军事、国家安全、电子商务等领域有较多应用。

5.3 数字水印系统模型

- **1. 数字水印中的矛盾关系**
- 水印信息的鲁棒性、载体作品的保真度、载体的水印容量三者之间存在着矛盾制约关系。
- **鲁棒性（Robust）、水印容量（Capability）、保真度（Fidelity）**之间的矛盾是由水印算法设计的基本思路决定的，不管是采用什么样的水印算法，水印信息往往是作为载体作品的冗余被嵌入的，是对载体作品的一种修改。
- 修改量越大，在同样水印容量下，载体作品在经过信号处理或攻击后遭受的破坏就相对原值较小，鲁棒性也就越强。但是同时，也越容易造成失真。
- 实际上，任何水印算法都是根据具体应用场景，在R、C、F之间得到一个平衡点。

2. 基本数字水印系统模型

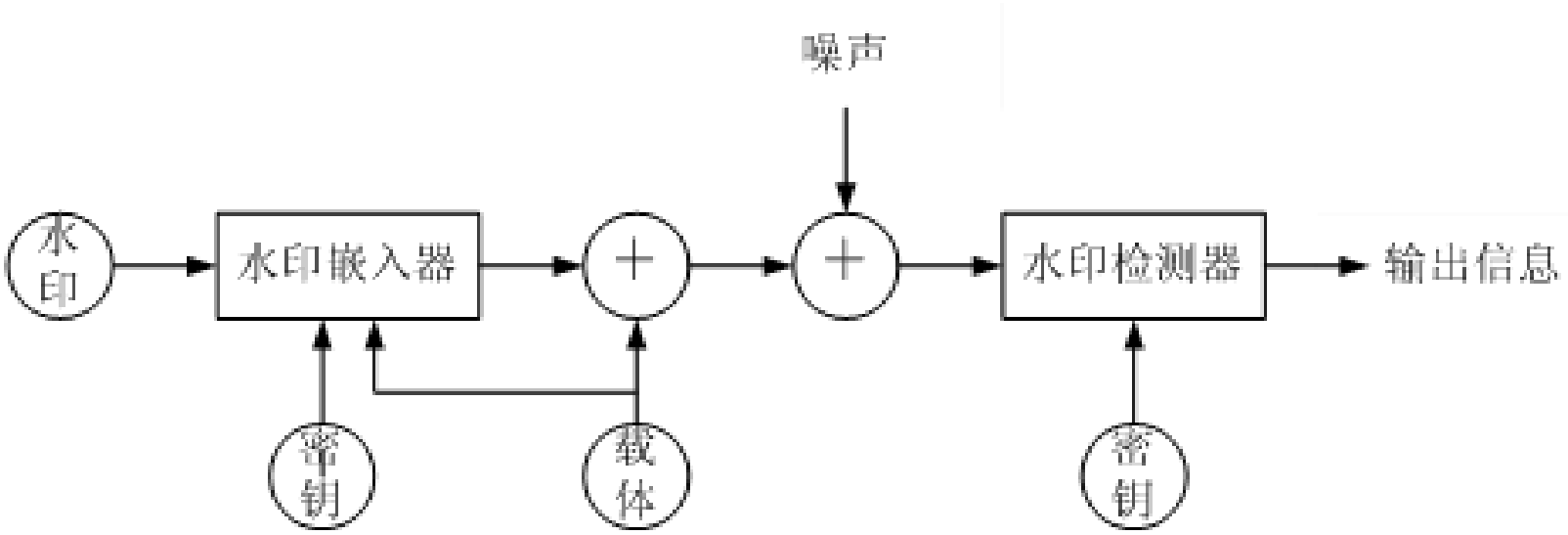
- 第一种称为基本模型，在这种模型中载体作品被当作纯噪声；



盲检测水印基本模型

2. 基本数字水印系统模型

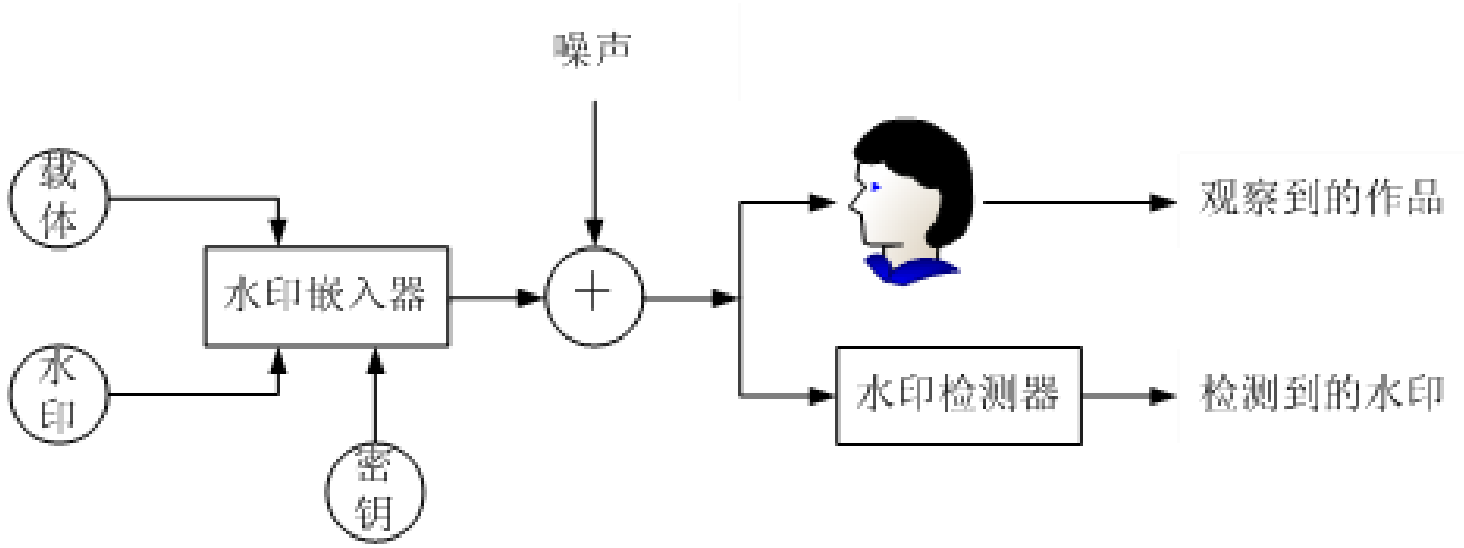
- 第二种称为发送端带边信息的水印模型，同样载体作品被视为噪声，但该噪声同时也被看作是边信息成为了水印嵌入器的输入；



发送端带边信息的水印模型

2. 基本数字水印系统模型

- 第三种称为基于信道复用的水印模型，它没有把载体作品看作噪声，而是当作另一类信息，和水印信息一起以信道复用的方式传输。



基于信道复用的水印模型

5.3 数字水印系统模型

- 在这三种水印模型中，应该说基于信道复用的水印模型比其它两种更合理，更接近实际的水印传输。在这种模型中，载体作品和水印信息具有对称性，因为作为载体作品的使用者来说，他希望载体作品不会因为嵌入了水印而破坏了其可用性，水印信息被看作是“噪声”；同时作为水印的验证者或检测者来说，他希望水印信息能正确无误的从载体作品中检测出来，载体作品被看作是“噪声”。这种对称性体现了实际应用对载体作品保真性要求和对水印信息有效性或鲁棒性要求的对称性。

5.4 鲁棒性水印技术

- 多媒体（视音频）鲁棒性水印的研究是目前的热点
- 对于**音频水印**，技术主要集中于研究低比特位编码、相位编码、回声隐藏和基于扩展频谱编码等四个方面。
  - **低比特位编码**音频数字水印方法是最简单的音频水印技术，但对某些信号处理技术比较敏感。
  - **相位编码**中，隐藏的数据用相位谱中特定的相位或相位变化来表示，但是相位改变会引起听觉上的感知。
  - **回声隐藏**是通过引入回声的方式嵌入数据。
  - **扩展频谱编码技术**的基本思想是将隐藏的数据流扩展到尽可能宽的频谱或者是指定的频段上，这两者都存在优化不可感知性和鲁棒性的问题。

5.4 鲁棒性水印技术

- 对于**视频水印**，有一些特殊的要求：实时处理性、盲检测性与随机检测性、视频速率的恒定性、与视频编码标准相结合、较大的水印容量和嵌入速率等。
- 视频水印嵌入方法可分为三种：
  - **第一种**是将水印信息直接嵌入到编码压缩之前的原始视频图像序列中，但过程比较复杂，增加了计算的复杂性并降低视频的质量；
  - **第二种**是在编码压缩时嵌入水印。但水印的嵌入和提取算法需要修改编码器和解码器，而且存在GOP的误差积累。
  - **第三种**是在压缩域中嵌入水印，这种方法不需要完全解码和再编码过程，因此计算量小，实时性好。 但水印数据量的大小受限制。

5.5 不可感知性水印技术

- 数字水印技术中使用的**人类感知模型**主要包括人类视觉系统（HVS）模型和人类听觉系统（HAS）模型，主要是考虑在这些模型中的人类感知特性，确定感知上的冗余和掩蔽。
- 利用JND（Just Noticeable Difference）门限或阈值来平衡水印不可见性与提高嵌入强度之间的矛盾，以此为依据建立水印的嵌入和提取算法，并根据载体作品的特点自适应的调整嵌入强度。

5.5 不可感知性水印技术

- **1. 数字水印的感知评价**
- 水印是不可感知的。
- 通过水印的感知模型来描述水印的不可感知性。
- 保真度是信号处理前后信号之间的相似程度，品质是对效果的绝对化衡量，二者都是感知特性。对于水印的某些应用，保真度是主要考虑的感知特性，如医学照片、艺术作品等；而另外的应用，可能主要考虑载体的品质，而不是保真度。如音频、视频等。
- 要解决不可感知性问题，一方面要有感知评价标准，另一方面要针对感知特征，寻找水印嵌入域，并建立感知模型，调谐各种嵌入参数，以期达到应用中的感知性要求水平。

2. 感知模型与水印嵌入方法

- 人类听觉系统（HAS）会根据输入的频率和响度的不同而做出不同的反应。
- 人类的视觉系统的反应也会因其输入的空间频率、亮度以及颜色的不同而不同。
- 感知模型一般都试图解决三种基本现象：灵敏度、掩蔽效应及合并。
  - **灵敏度**指的是人的眼睛或耳朵对直接激励的反应。
  - **掩蔽效应**指人的眼睛或耳朵只对最明显的图像或声音反应敏感。
  - **合并**敏感度模型和掩蔽模型可以用于估计某一特定特征变化的可感知度。

5.5 不可感知性水印技术

- 为了达到鲁棒性，Cox推荐在感知重要的系数上进行水印的嵌入，只有当媒体内容产生感知失真时，这些系数才会发生改变。
- 但是这种方法直接违反了水印的不可感知性原则。
- **一种解决方法**是使用扩频编码技术将水印信息嵌入到更多的感知重要的系数上，而降低单一系数的修改程度。
- **另一种方法**是将水印嵌入到中等程度感知重要的系数上，既不可感知，又能得到一定的鲁棒性。
- 不管是哪种方法，都需要对系数的修改调整，而如何自适应的进行调整，就需要感知模型来提供帮助。
- 在实际的算法设计中，必须与鲁棒性要求紧密结合，单独考虑不可感知性是不符合实际需要的。

5.6 广播电视中数字水印面临的问题

- 数字媒体技术迅速发展，引发的是人们对网络版权保护、盗版追踪、内容监控等方面的媒体内容安全需求。
- 这些需求要求数字水印技术能够是强鲁棒的、安全的。
- 现有的这些基于时空域、变换域的数字水印技术他们共同的特点就是从基本的像素级别和内容的单一层面进行分析设计，与内容本身的特性关联很少，在鲁棒性、感知性等方面不能适应新的需求。
- 近年来，图像解析和图形学等相关领域的一些新的理论和方法，特别是图像的基元/纹理表示研究的最新进展，促使我们从图像/视频处理中最底层问题——图像/视频的内容解析入手，寻求一种高效的内容信息层级表示模型，借助这种模型探索基于内容特征的新的数字水印技术方法，实现从像素水印到内容水印的跨越。

5.6 广播电视中数字水印面临的问题

- 为满足当前媒体内容安全发展的需要，主要问题如下：
- **1. 联合攻击、盲检测等媒体应用环境带来的强鲁棒性问题**
- 在媒体内容产业中，媒体内容经历了制作、编辑、集成、分发、传输、交易、使用等环节，各环节循环往复，直至媒体内容的使用价值丧失。
- 在这些环节当中，对数字水印技术的要求首先体现在表示版权等的水印信息能够抵抗各环节中存在的攻击的联合实施，比如各环节都普遍存在的**H.264/ MPEG2**压缩、广播与接收中的**AD/DA**、编辑制作中的重采样（时空分辨率调整）等。
- 在内容的非线性编辑、内容属性（如分辨率）的终端自适应调整中还存在着大量的同步攻击，如几何变换、拼接、裁剪等。

5.6 广播电视中数字水印面临的问题

- 虽然分别抵抗这些攻击的水印算法已经存在，但是他们的鲁棒性依然较弱，更重要的是由于技术特点不同，他们很难融合一起，来抵抗上述攻击的联合实施。
- 再加上在媒体内容安全中诸如版权水印、指纹水印要求的盲检测，更加提高了鲁棒性水印设计的难度。
- 往往在内容感知性很好的时候，水印信息已经部分甚至全部丢失。目前设计的各种鲁棒性水印算法，都属于像素或像素变换级的水印方法，都无法与内容特征紧密结合。
- 必须考虑内容本身在感知上的层次特点，构建与内容特征结合的强鲁棒水印模型，最大限度的利用内容本身的属性进行水印算法的设计，从根本上解决水印抵抗各种攻击的问题，提高其鲁棒性强度。

5.6 广播电视中数字水印面临的问题

2. 高清、高保真等媒体内容体验需求带来的低感知性问题

- 高压缩、高带宽带来的高清、高保真的内容体验正在成为市场的主流，这些媒体内容正成为业务增值的关键。
- 在高清、高保真等媒体内容体验需求下，水印的感知性、鲁棒性、容量之间的矛盾关系更加突出。很多算法为了能够抵抗更强烈的攻击，不得不提高嵌入阈值和强度，这样反而影响感知性。
- 与内容本身关联性更强的感知模型将为低感知性水印的研究提供新的思路。基于内容特征和层次分解的水印方法，更加符合人类的分层次感知特点，将更深入的从与媒体内容相结合（而非像素）的方法方面展开研究；在保障鲁棒性的同时，具有更好的感知特性；并重新审视水印的矛盾关系，建立新的感知模型，形成在某种感知阈值下的最优解决方案。

5.6 广播电视中数字水印面临的问题

- **3. 数字水印载体中内容特征的信息熵度量问题**
- 图像/视频等媒体内容表示模型可以遵从“像素-基元/纹理-对象-场景”的层次模型。
- 基元/纹理可以构成媒体内容的重要特征，对这些特征的感知也同样是分层次的。但是如何对这些特征和层次进行有效信息度量，是基于内容特征的水印方法需要考虑的重要问题。
- 大多数基于内容特征的水印算法仍然使用基于像素统计特性定义的信息量，而这些基于像素的信息量的熵值并不能准确反应人所感知的视觉信息量，如图像/视频中某些区域虽然具有高信息熵，但人眼对其内容的关注度却很低。这样的信息度量值，容易对水印的嵌入产生误导，并导致鲁棒性能和感知性能的下降。

5.6 广播电视中数字水印面临的问题

- 因此，我们需要找到更加适合于数字水印的内容信息表达方法。新的方法必须与层次分解相结合，分层次度量，形成感知层次，确定各层次的感知区域和范围。采用将像素信息熵与内容熵进行结合使用等方法进行探索研究，进一步深度挖掘媒体内容感知冗余，才能达到指导水印嵌入的作用，并以此提高数字水印在感知性、鲁棒性方面的性能。

5.6 广播电视中数字水印面临的问题

4. 视频载体的信息隐藏容量问题

- 数字水印技术在保证鲁棒性、不可感知性之外，提高信息隐藏容量，适应版权、指纹信息的可靠传输也是需要研究的问题。
- 在数字水印的视频应用中，水印信息往往因载体甚至载体使用环境不同而不同，并且要求能够唯一标识载体或者载体使用环境。这些水印信息量较大，同时为了实现可靠的检测，往往需要对水印信息进行纠错编码、扩频，对水印算法来说就需要在满足鲁棒性、感知性要求的同时，能够支持较大的信息隐藏容量，即更大的隐藏比特率。

5.6 广播电视中数字水印面临的问题

- 但是目前的信息隐藏容量研究是基于像素水印技术展开的，还无法完全体现从视频解析角度的信息隐藏容量，而且在传统的信息隐藏容量研究中，需要增加大量的推理假设，而这些假设往往与实际的应用环境不符，得出的结论和容量表达式无法准确反映理论容量和实际容量的上下限。
- 如何对视频解析中的感知特征与层次进行有效信息度量，是在针对视频内容进行信息隐藏容量研究中需要考虑的重要问题。
- 需要寻找新的视频信息量度量的方法，与视频解析相结合，分层次度量，确定各层次的感知区域和范围，在此基础上利用互信息游戏等研究其信息隐藏容量。

5.6 广播电视中数字水印面临的问题

- **5. 视频应用中的视频消息源追踪问题**
- 解决视频消息源追踪的问题是当前以及将来的迫切需求。
- 视频指纹水印技术在解决视频消息源追踪方面具有理论优势，但同时，如何适应视频应用环境在鲁棒性、不可感知性等方面的特殊需求是影响指纹水印技术得以应用的瓶颈。
- 首先，视频指纹水印的应用过程有服务提供商、消费者的多方参与，甚至需要第三方的监督，因此需要完善的视频消息源追踪模型支持。
- 其次，消息源追踪跨越视频的生成、分发、使用等多个阶段，视频指纹水印面临一般性的攻击，同时还将面临被恶意删除、修改等攻击，因此，视频指纹水印必然要适应这些攻击；
- 第三，视频应用中的视频消息源追踪系统必须是开放的、灵活的，需要开放协议的支持。

5.6 广播电视中数字水印面临的问题

- **6. 网络视频应用中的视频版权保护问题**
- 新媒体的发展在方便了人们工作和生活的同时，也助长了剽窃、盗版的歪风。因此，需要寻求更加有效的方法，建立包括内容保护和业务保护在内的一体化的版权保护体系结构、技术方案，适应三网融合的趋势和视频应用需求。
- 首先，视频版权保护需要密码技术与水印技术的有机结合，权限控制和版权保护并举，形成层次化的版权保护模型。
- 其次，版权保护跨越视频的全生存期，视频版权水印具有很高的鲁棒性和不可感知性要求，同时还将面临被恶意嵌入、删除、修改等攻击，视频版权水印也必然适应这些攻击；
- 第三，视频应用中的视频版权保护系统必须是开放的，灵活的，需要开放协议的支持。因此，需要对其系统模型、算法、协议展开应用研究。

5.6 广播电视中数字水印面临的问题

- **7. 网络视频应用中的视频合法性认证问题**
- 电视台以及新媒体形式在播出视频内容的同时，将面临内容被替换、被干扰的问题，导致消费者收看的是通过合法电视台和新媒体业务提供的非法视频内容，形成社会的不稳定因素。
- 首先，视频合法性认证水印的安全性和可靠性，甚至需要第三方的监督，因此需要完善的基于视频水印的视频合法性认证模型支持。
- 其次，视频合法性认证跨越视频的分发、使用等多个阶段，面临一般性攻击，同时还将面临被恶意嵌入等攻击，视频合法性认证水印算法的研究也必然能适应这些攻击；
- 第三，视频应用中的视频合法性认证系统必须是开放的，灵活的。针对视频的合法性认证问题，需要对其系统模型、算法、协议展开应用研究。

5.6 广播电视中数字水印面临的问题

- 第二代水印算法使用具有可见性的重要特征嵌入水印，重要特征可以被提取而且是具有语义意义的特征。
- 适合水印的特征一般应具有对于噪声的不可变性、对于几何变换的特征不变性、特征具有局域性等特点。这种算法具有很强的生命力，有非常好的应用前景，是数字水印技术发展的一个重要方向。
- 在这新一代水印的设计中必须将鲁棒性、不可感知性更加深刻的综合考虑，构建反映感知层次的特征，充分结合人类感知特性，对内容特征进行有效的信息度量，建立新的水印模型和方法，才能真正为媒体内容水印的设计与应用提供最好的支持。

Thank You !