

# DCI 图像规范 与 数字电影图像 DCP 加密打包

## 目录

一、 格式之争.....	1
二、 帧率 (Frame Rate) .....	1
三、 色彩空间 (Color Space) .....	2
四、 色彩分辨率 (Color Resolution) .....	3
五、 影像分辨率 (Image Resolution) .....	4
六、 数字电影的画幅 (Aspect Ratio) .....	5
七、 影像压缩 (Image Compression) .....	6
八、 数字电影音频 (Audio) .....	7
九、 打包和发布文件 (Wrapping And Distribution Files) .....	8
十、 DCP 的命名 (Naming OF DCPS) .....	10
十一、 安全与密钥管理.....	11
十二、 硬件加密技术.....	14
十三、 数字水印技术.....	15

## 一、格式之争

当 DCI（数字电影创导组织，由好莱坞七大制片公司合作建立）规范被创建并发布的那时起，其基本目的就是为了创建一种公开化的标准和规范，以防止格式之争重新上演。我们可能还记得当初胶片电影时代格式之争吧，比如单孔单画幅，四孔单画幅之争；还有上个世纪 80 年代的时候 SONY 的 Betamax 和 JVC 的 VHS 格式之争；胶片电影的数字化立体声技术的 SDDS、DTS、DOLBY SRD 之争；以及近些年来高清视频的 HD-DVD 和 BluRay 之争等等。争是好事，但是也会带来一些负面的影响，比如会迟滞新技术的开发和发展。而数字电影作为一个电影技术的革命性的转变过程，对于新技术的开发、应用以及发展是非常之全面的，如果各个企业都开发自己的一套技术，那就会大大迟缓数字电影的发展进程，这是我们所不愿意看到的，所以 DCI 规范才因此目的应运而生。这个规范应用在电影数字拷贝方面的就产生了一种崭新的格式-DCP（Digital Cinema Package）数字电影打包格式。我接下来会和大家一起讨论关于 DCP 的一些关键的属性。

## 二、帧率（Frame Rate）

毫无疑问，每秒 24 帧在电影领域已经应用了相当长的一段时间了，特别是胶片电影领域，24 帧每秒已经作为标准被使用着。所以数字电影一开始为了和胶片电影兼容，理所当然地也采用了这种帧率（所谓帧，其实就是画面；一帧就代表一个单独的画面）。但是 24 帧真的就完美无缺了吗？答案是否定的，比如我们在观看一些有大量运动画面的场景时，你有没有注意过运动模糊这种情况。请看下图。

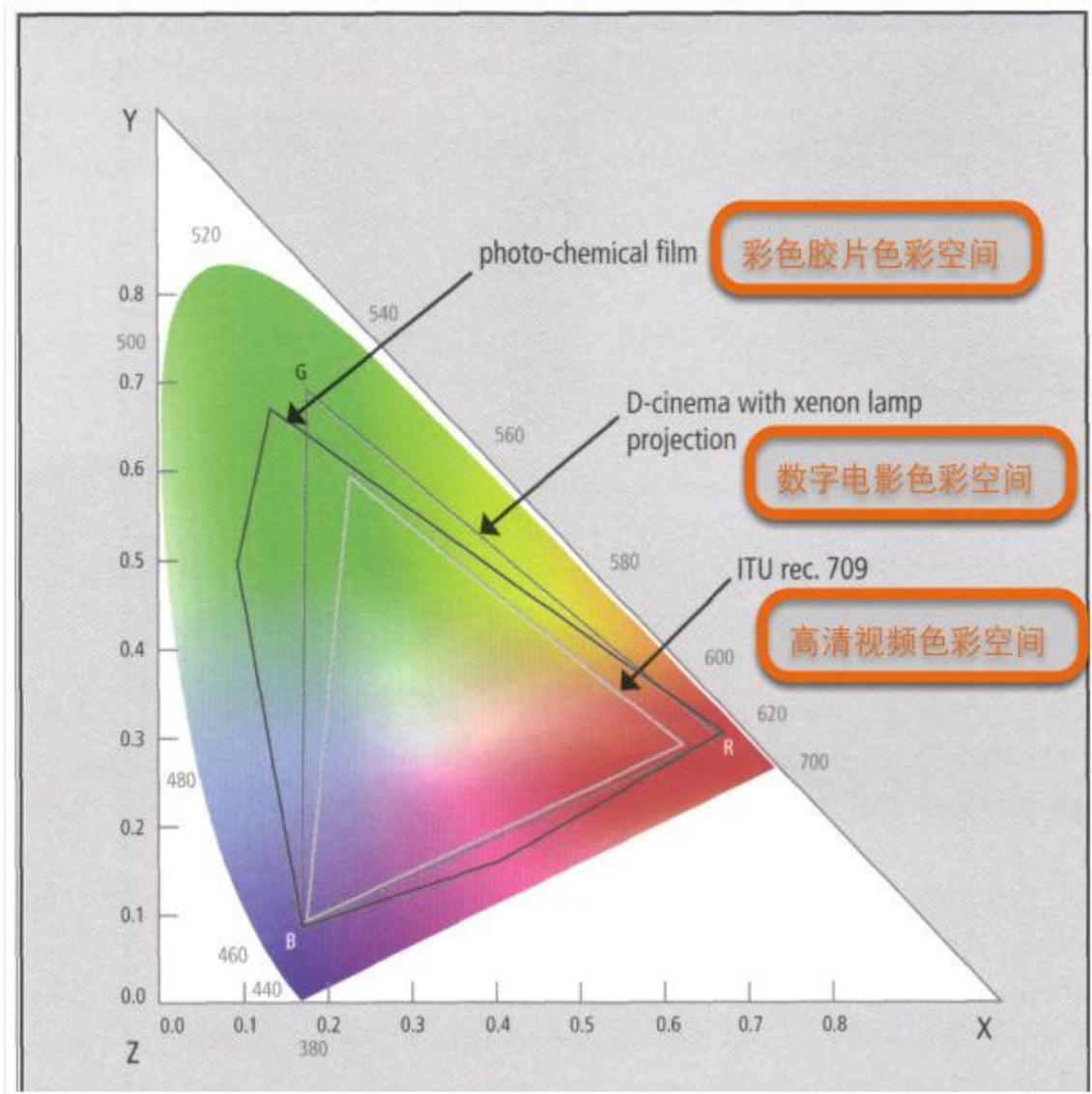


除了运动模糊这种现象，低帧还会有画面闪烁的情况。为了解决这些伪影现象，现在数字电影也开始使用比如 48 帧、60 帧每秒技术于 DCP 的制作和放映过程中了。但是高帧（HFR-High Frame Rate）技术也会产生种种不真实的感觉，因为人们已经习惯于每秒 24 帧观看，对于高帧技术带来的新的观影体验还需要一段时间的适应和养成。所以 DCI 和 SMPTE 也在不停地研究和开发到底什么样的

帧率才是适合于数字电影平台。再说明一下，目前 DCI 规范中还是以 24 帧为标准规范的，25、30、48、60 等高帧技术还没用被为 DCI 规范。

### 三、色彩空间 (Color Space)

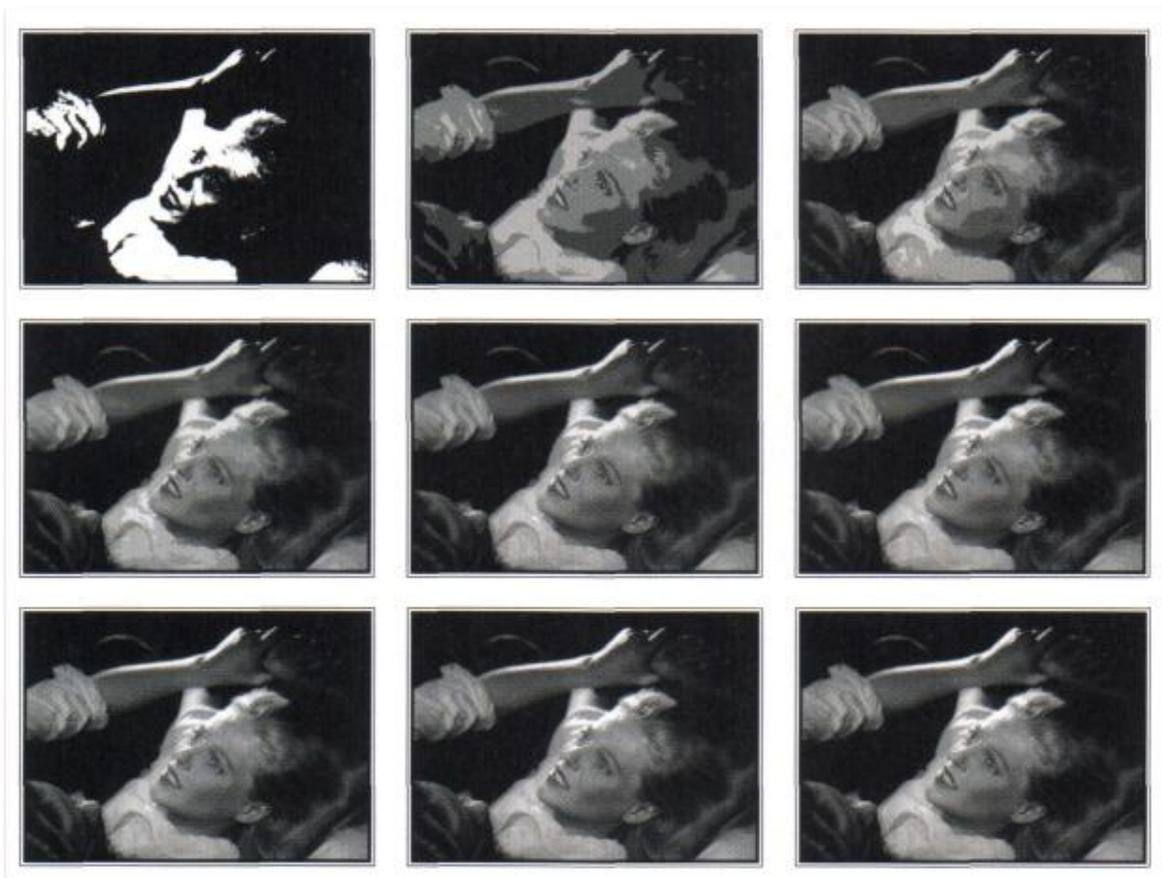
说起色彩空间，大家可能会感到很抽象，很难理解其真正的意义。所谓色彩空间其实就是以三个特定的字符及其数量的多少来定义一种特定的颜色而已，比如 RGB 色彩空间就是以 R、G、B 来分别代表红、绿、兰三种原色（所谓原色就是其本身无法用另二种色彩来合成的颜色，比如红色无法由绿和兰色来合成，其他二种原色也是同理，除了原色，其他的任何一种色彩都可以由原色的任意组合来形成）来形成其他的任何一种色彩。又比如 YUV 色彩空间等等。是不是很容易理解呢。说好了色彩空间的定义，我们来说说数字电影的色彩空间是什么，DCI 为了让数字电影能够表达自然界中的一切色彩，最后采用了 XYZ 色彩空间作为数字电影的色彩空间。为什么呢，当然是有理由的，所谓 XYZ 色彩空间其实一种虚拟的色彩空间，XYZ 不像 RGB 那样是人的真实能够体验的色彩空间，这种 XYZ 是不真实的是虚拟的，但是 XYZ 色彩空间有二大优点决定了其被采用于数字电影领域。一、XYZ 色彩空间可以表达人眼所能识别的所有色彩（见下图）；二、XYZ 色彩空间是一种与设备无关的色彩空间（也就是说不管什么设备，采用了 XYZ 色彩空间后，其所表达的色彩信息永远不会改变，永远是唯一的），这个第二点太重要了，这样就是说你在监视器上面看到的色彩和在银幕上所看到的色彩是完全一致的，不会因为改变了显示设备而改变了色彩的还原。这是如何来形成的呢，其实是这样的一过程，首先你在电脑前面对视频和图像进行剪辑、合成、最后是校色，当然这个校色完成后的效果是您所想展示给观众看的，对吧，而电脑显示器一般都是 RGB 色彩空间的，然后在打包 DCP 之前需要对其视频部分进行一个色彩空间的转换，也就是从 RGB 转换到 XYZ 色彩空间，然后因为 XYZ 色彩空间是一种比 RGB 更大范围的色彩空间，所以通过特定的转换算法可以把 RGB 所有的色彩信息一一对应到 XYZ 色彩信息，最后打包成 DCP，这个打包后的 DCP 上传到服务器当中进行播放对吧，在放映机进行播放的过程中放映机会对这个 XYZ 色彩空间再一次进行转换到原来的 RGB，而 XYZ 空间是大于 RGB 的，所以再次转换以后的 RGB 就是原来的在数字电影后期最终校色的 RGB 信息，这样一个完整的没有任何损失的正是您想要展示给观众的色彩就被忠实地还原出来了。（DMD 是 RGB 三原色的 $\hat{\sim}$ ）。



#### 四、色彩分辨率 (Color Resolution)

色彩分辨率也称为色深 (Bit Depth)，那如何来正确正解色深这个概念呢，我们知道，我们现在所讨论数字电影中的不管影像也好，声音也罢，都是基于数字的，说的更准确一点就是二进制数字，就是 0 和 1 这两个数字这个可以理解吧。好了理解了以后，我们再来说说色深概念，那么在数字领域我们如何来表示一种颜色呢，因为计算机只懂 0 和 1，不懂什么红色、蓝色神马的。那如何让计算机知道这是红色，这是蓝色等等颜色呢，我们就用 0 和 1 组成的数字串来表示色彩，也称为编码（就是用 0 和 1 的特定顺序来表示特定的信息，我们称为编码）。知道了这个以后，我们比如说要表示的色彩只有黑、白二种色彩信息的话，好是不是只要 0 或者 1 就行了，0 代表纯黑，1 代表纯白，就是说一位编码就够了（2 的一次方）如果要代表四种色彩呢，是不是只要 2 的二次方就可以

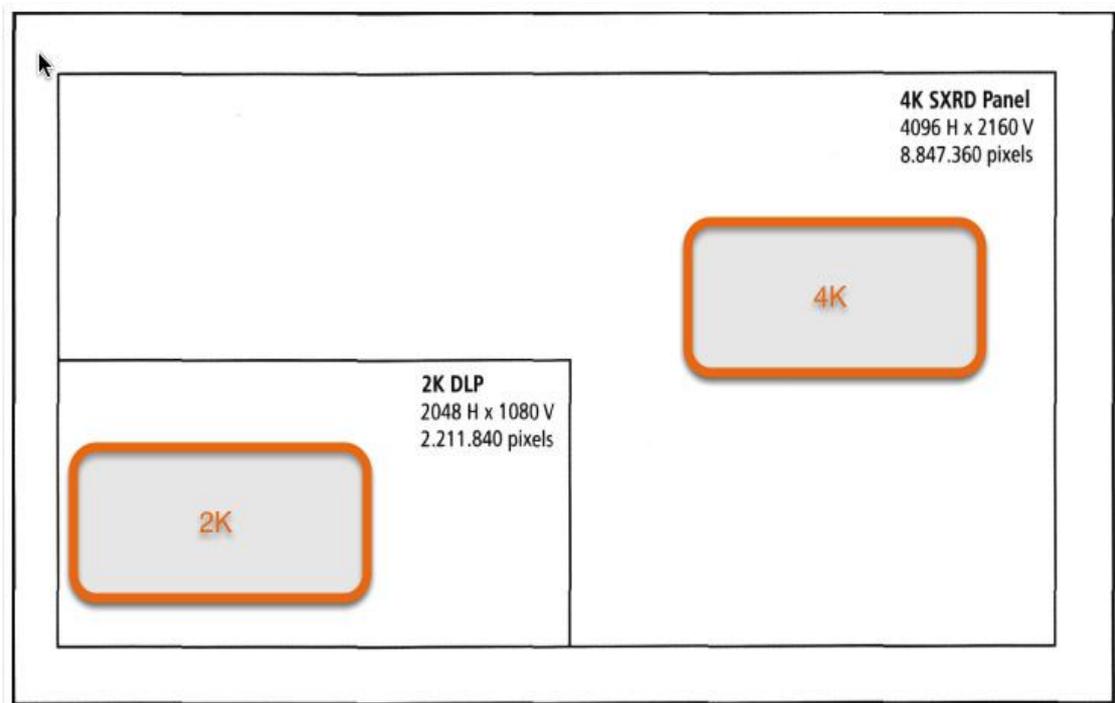
了对吧。如果要 8 种色彩呢，就是不是 2 的三次方呢。好了理解了这人概念以后就好理解色深的概念了，所谓色深就是 2 的 N 次方喽。比如说 2 的 8 次方其色深就是 8bit，是不是这个比特数越大所能表达的色彩就越多，对不对。（下图所示为采用不同位深的同一图像的效果）那数字电影的色深是多少呢，是 12 比特（12BIT），想想看，每个原色都是 12 比特编码，那三原色相加可以表达的色彩已经远远超出人眼所能识别的色彩范围了。但是真实的情况是这样吗，答案是有差距的，为什么会这样呢，原因在于我们现在数字电影放映机所采用的光源以氙灯为主，氙灯的白光和自然界的真实的白光还是有所差距的，这个差距决定了采用氙灯光源以后在色彩的还原方面还是达不到还原所有人眼所能识别的全部色彩（就是上图中马蹄形范围）。但是这个问题在激光光源来临以后会得到一个最终的解决。



## 五、影像分辨率 (Image Resolution)

当 DCI 规范 (DCI Specification) 还处于酝酿阶段的时候，就已经把 2K 定为数字电影影像分辨率的最低要求了（为什么会这样，大家可以参考我的关于像素篇的教程）。这里说个题外话，大家知道第一部正式公开放映的数字电影是哪一部电影吗，答案是星战前传一 (Star Wars Episode 1)，当时是以 1.3K

方式来进行放映的，时间是 1997 年。而且 1.3K 这种图像分辨率从来就没有作为过 DCI 规范。也就是说从一开始 2K 就作为数字电影的标准被普遍采用，而 1.3K 只是一种过渡形式的方案，最终会退出历史舞台，而且正在并且已经退出了。最终 DCI 组织在制定关于数字电影影像分辨率时采用了以 2K 为最低分辨率并且兼容 4K 分辨率的这样一种方案。这种方案的实质就是 4K 系统可以播放 2K 影片而不会产生任何伪影现象，反之亦然。那如何来实现这一种方案呢，答案就是对于数字影像采用了 JPEG2000 编码。这种编码的优点就是 4K 数据是基于 2K 的，说的更明白一些就是 4K 影像只是在 2K 影像基础上不同的部分的增量，而不是独立的 4K 影像，或者说 4K 的 DCP 中包含了 2K 的影像部分，这样 4K 和 2K 的 DCP 包不用做二个不同的 DCP 包，只要一个 4K 的 DCP 包即能被 2K 服务器提取其中的 2K 部分，也能被 4K 服务器提取 4K 部分，大大节约了资源。



## 六、数字电影的画幅 (Aspect Ratio)

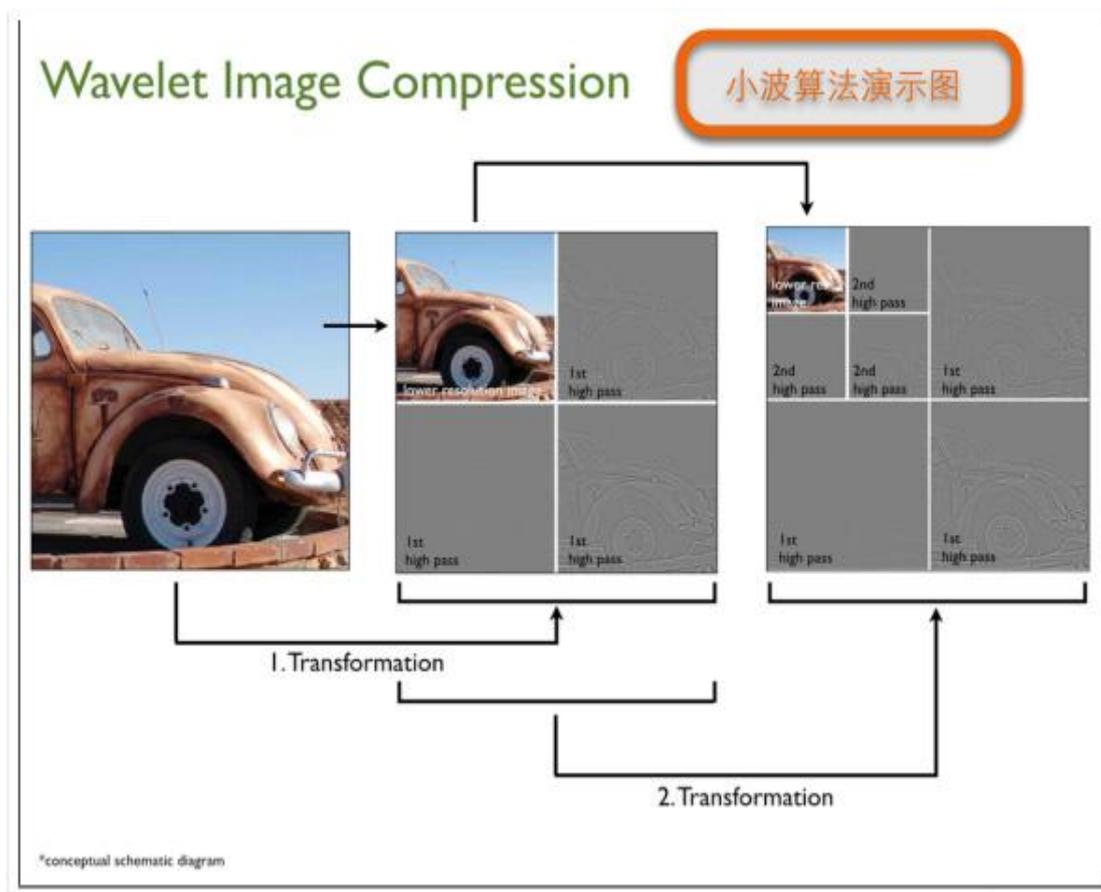
DMD (数字微镜) 当中的像素陈列是 2K (2048X1080) 4K (4096X2160) 这二种画幅习惯上称为全幅，并且数字电影影像的像素为方形像素 (也就是说像素的形状是正方形)。但是在实际的应用当中，全画幅很少被采用，一般现在数字电影 DCP 包的画幅格式有二种，分别是 2.39 (2048X858) 也称为宽银幕画幅 (Cinema Scope) 简称 S 和 1.85 (1998X1080) 也称为遮幅 (Cinema Flat) 简称 F。以上我所讲的都是针对 DCI 规范中所指明的，而实际上目前还有很多国产数字电影 (通常使用 MPEG2 编码) 使用的画幅分别为 1920X1038 (遮幅电影) 和 1920X804

（宽银幕），大家要记住一点，这二种画幅格式不是标准的 DCI 规范，最终也将退出历史舞台，完成其历史之使命。

	<b>2.39:1</b>	<b>1.85:1</b>
<b>2k</b>	2048 x 858 (1.76Mpx)	1998 x 1080 (2.16Mpx)
<b>4k</b>	4096 x 1714 (7.02Mpx)	3996 x 2160 (8.63Mpx)

## 七、影像压缩 (Image Compression)

就象上一章提到的那样，数字电影 DCP 影像压缩方案之所以采用 JPEG2000 的原因之一主是因为在一个 4K 的 DCP 包中即包含了 2K 的基础部分也包含了 4K 的增量部分，这样我们就可以用一个 4K 的 DCP 包来同时发布二个 DCP 版本（2K 和 4K）这个好处的作用是显而易见的。不同于 MPEG2 的 DCTs 算法，JPEG2000 采用的是小波算法。至于什么是小波算法，具体的内容又是啥，这个说白了我也说不明白。但是我可以和大家来说说这种算法的特点和优点，比如说上面提到的 4K 影像是基于 2K 影像的增量就是这种算法的优点之一；其二小波算法还是一种高效的、适合于复杂数据存储的方案，比如说应用于高分辨率影像领域；其三小波算法是一种非对称的数据编码方案，其特点在于编码要比解码相对更加复杂（注：编码我们可以理解为压缩、解码我们可以理解为解压缩）换句话说就是小波算法压缩要比解压来的更为复杂，当然压缩使用的时间要比解压的时间更长，我样如果有过打包 DCP 的经验的话就会明白，压缩 1 分钟的视频到 J2C 序列的时间是很长的，而我们在影城播放 DCP 几乎是实时的，就是这个原因，还有我顺带提一下，JPEG2000 序列压缩的比率一般为 8: 1 到 30: 1，而解压后几乎是视觉无损的（就是说 JPEG2000 压缩方案是一种视觉无损的方案，这个比起 MPEG2 来要强很多）；其四小波压缩算法是一种帧内压缩方案 (Intra Frame) 这种方案的好处就是可以大大提高后期制作时的效率，我们可以方便地提取整个图片序列中的任意一帧并且能做到很精确不出差错；其五小波算法的平均数据传输率（也称为码率）为 125M/sec 到 250M/sec，这个码率相当于传统 DVD 的 44 倍和兰光影片的 6 倍，画质的优良是很明显的；其六我们上面也提到过，小波算法是一种基于基值的增量算法，对于 2K 的 DCP 来说一般为 150G 左右，而 4K 也仅仅是 300G 左右，只增加了一倍的容量，虽然从像素上计算应该是 4 倍而不是 2 倍的关系，这个优点也是很重要的，对于 DCP 来说。



## 八、数字电影音频（Audio）

有别于数字电影影像采用了压缩方案，数字电影音频从采集、后期制作、打包、放映整个流程都是采用的无压缩的方案。DCI 规范中明确规定了数字电影音频为 16 个同步的分离的单声道（Mono）方案，每个声道采用了 48/96KHZ 的采样频率和 24BIT 的位深（哈哈这里第二次出现了位深的概念了，其实和数字影像的色深一样，音频位深的多少同时也决定了音频质量的好坏，在数字音频领域位深也称为动态范围，位深越大，动态越大，就是说从最高音量到最低音量之音的不失真声音就越多，主观上听觉就越好）以 PCM 为编码方案，以 WAV 为音频格式。目前数字电影领域采用的是 48KHZ 和 24BIT 的组合来对数字音频进行编码的。随着技术的发展，现在数字电影音频领域已经出现了更多声道的解决方案，比如 Dolby 公司的 Atmos 和巴可公司的 Auro3D 等等，这些方案也称为全景声方案，其目的就是为了达到更精确的声音定位和更完美的声音临场感，这也是以后数字电影音频解决方案的一个趋势。下图为数字电影音频的 16 声道图。

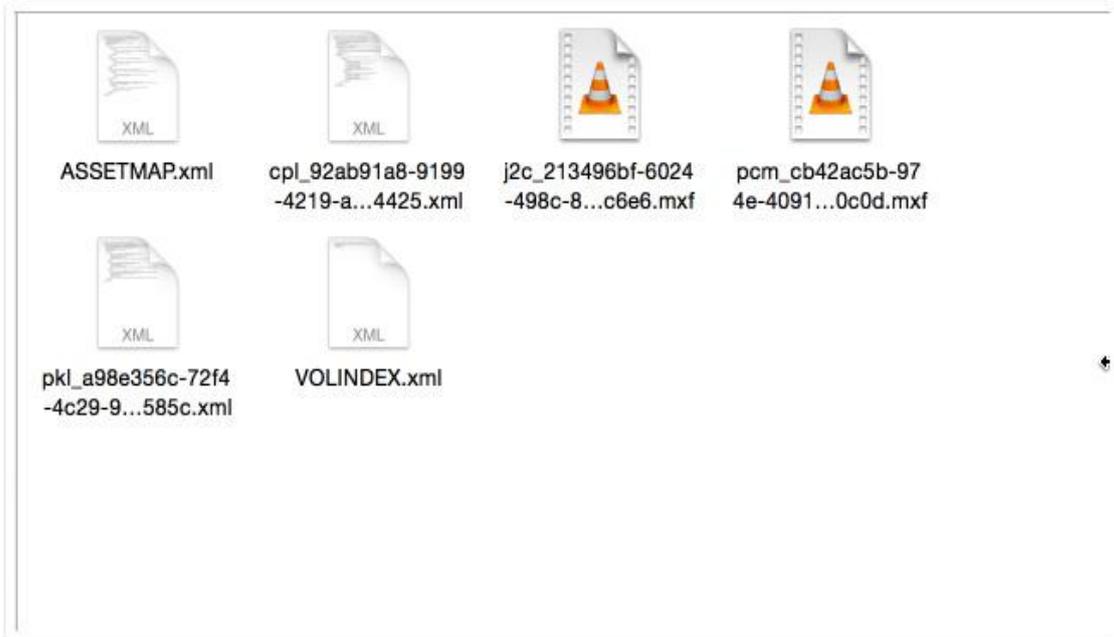
AES Pair#/Ch#	Channel #	Label / Name	Description
1/1	1	L / Left	Far left screen loudspeaker
1/2	2	R / Right	Far right screen loudspeaker
2/1	3	C / Center	Center screen loudspeaker
2/2	4	LFE / Screen	Screen Low Frequency Effects subwoofer loudspeaker
3/1	5	Ls / Left Surround	Left wall surround loudspeaker
3/2	6	Rs / Right Surround	Right wall surround loudspeaker
4/1	7	Lc / Left Center	Mid left to center screen loudspeaker
4/2	8	Rc / Right Center	Mid right to center screen loudspeaker
5/1	9		Unused
5/2	10		Unused / User Defined
6/1	11		Unused / User Defined
6/2	12		Unused / User Defined
7/1	13		Unused / User Defined
7/2	14		Unused / User Defined
8/1	15		Unused / User Defined
8/2	16		Unused / User Defined

## 九、打包和发布文件 (Wrapping And Distribution Files)

通过四个章节的学习，我想大家已经对于 DCP (Digital Cinema Package) 的基本组成元素 (视频、音频等) 的属性 (帧率、码率、压缩，编码等) 已经有一个大致的了解了，今天我来说一个 DCP 包到底是如何来组成的。我们影城收到的硬盘中的文件其实是以一个个 DCP 包为基本单位来组成的，而一个 DCP 包相当于一系列文件的合成 (Composition)，说的通俗点就是 DCP 包就是由视频、音频、字幕文件以及用于这些文件的同步播放、上传校验、打包说明等文件 (一般为 XML 文件) 来共同组成的一个合成文件，记住，DCP 包一定是由一系列文件组成的，而不是一个单一的文件，通常 DCP 包都是以文件夹的形式来发布的。好，那我们就来看看到底有哪些文件来组成一个标准的 DCP 包的，首先说说视频、音频、字幕文件，视频、音频文件一般是以 MXF 文件形式出现在 DCP 包中的，一般会有 1 到 8 个这样的视频、音频 MXF 文件组合，为什么会有 1 到 8 个甚至更多的视频、音频 MXF 文件呢，这其实来源于胶片电影的概念，以前一部胶片电影至少需要 5 到 8 盘胶片组成一部完整的电影，所以 DCI 组织引入了这个理念，称为 Reels，整个电影中的一段 (包含了视频、音频、字幕) 就称为一个 Reel，当然你也可以把整个一部电影做成一个 Reel，这样的 Reel 在有些打包软件 (比如说 easyDCP Creator) 中称为一个分卷，现在你知道了吧，其实一个分卷就是一个 Reel，相当于胶片电影的一卷胶片，这样是不是很容易就理解了所谓 Reel 的概念了呢^-^。那如何来管理 DCP 合成中的各个组成元素呢，那就会用到 UUID 这个概念，一个 UUID 对应于 DCP 合成中一个元素的识别码，这样就可以做到保证一个 DCP 中的各个元素之间不会产生冲突和混乱，这样电影放映的时候就是通

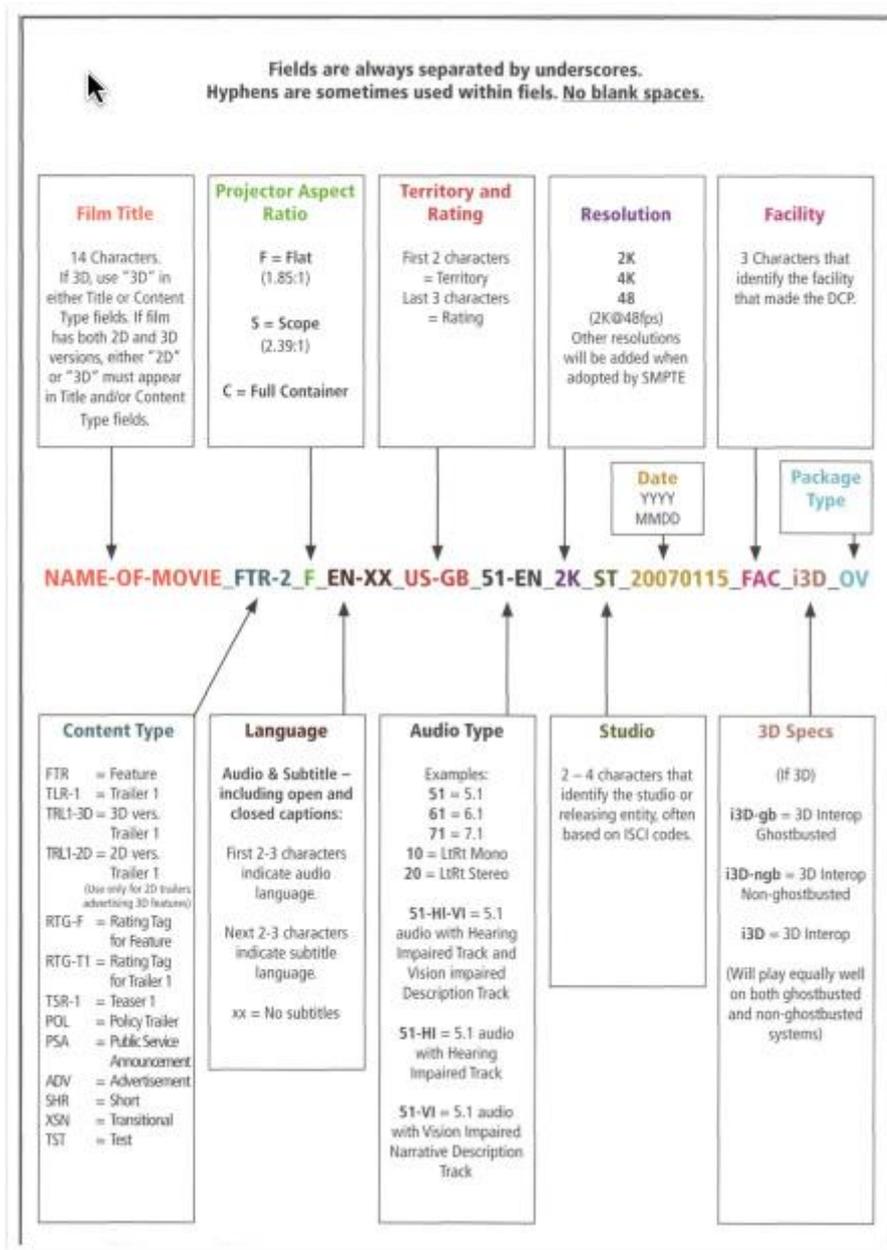
过管理和调用这些 UUID 来管理和调用数字电影 DCP 中各个视频，音频，字幕元素的同步和播放任务。一个 DCP 合成中的视频和音频往往是用 MXF 作为标准的文件格式的。这里要特别说一下字幕 (Subtitle) 文件，字幕文件有二种标准格式，一种是 XML 格式一种是 MXF 格式，分别对应 Interop (XML 格式) 和 SMPTE (MXF 格式) 打包标准，我们会在很多影片的名称中看到 IOP 的字样，现在我们应该知道了其字幕一定是 XML 格式了，相对应的 SMPTE 打包标准中的字幕是 MXF 格式的，这种 MXF 格式的字幕的优点之一是字幕是 PNG 图片序列，通过播放设备直接叠加到视频 MXF 上面，然后通过视频通道 (比如 HDS DI 通道) 传输到投影机后投影出去的，这样就能保证字幕在放映的时候不会丢失 (相对于 XML 字幕，是通过网线传输到放映机，然后通过放映机来叠加到画面上的，这样如果网线质量，接口松动，放映机固件等原因很容易造成放映中途字幕丢失的情况)；这种 MXF 格式字幕的第二个优点是可以加密字幕，保证字幕的安全性需要。所以 Interop (就是以视频 24 帧，字幕 XML 格式为打包标准) 打包标准最终会被 SMPTE (视频支持高帧放映，字幕是硬字幕) 打包标准所取代。好了，说完了视频、音频、字幕情况后，我再来说说除了这三大要素外的另几个 XML 文件的情况，首先是 CPL (Composition Play List) 文件，看到没有，CPL 中的 C 其实就是合成 (Composition) 的意思，而我们的 DCP 包我刚才也提到了，其实质就是一个合成，所以 CPL 文件也称为 DCP (合成) 播放列表文件，是不是这样呢。CPL 文件的作用主要是告诉服务器如何以及以怎样的顺序来播放 DCP 中的各个元素 (视频、音频、字幕)，说到 CPL 大家可能马上联想到 SPL (Show Play List)，大家千万不要混淆这二个概念呢，SPL 又叫播放列表，是服务器管理软件、TMS 系统中用于管理影片、贴片广告、预告片的管理列表，和 CPL 是二个概念，千万要记住哟。接下来说说 PKL (Packing List File) 文件的作用，PKL 文件主要用于在 DCP 上传服务器的时候对 DCP 进行验证和校验管理的，比如验证 DCP 的完整性以及 DCP 是否被篡改，如果发现 DCP 损坏或者被篡改，服务器就会发出相应的警告提示，比如此 DCP 不完整等。还有就是 Volume Index File 和 Asset Map 文件，这二个文件是 DCP 合成的资产说明文件，主要说明这个 DCP 打包文件是由哪些资产 (或者说元素) 组成的。





## 十、DCP 的命名 (Naming OF DCPS)

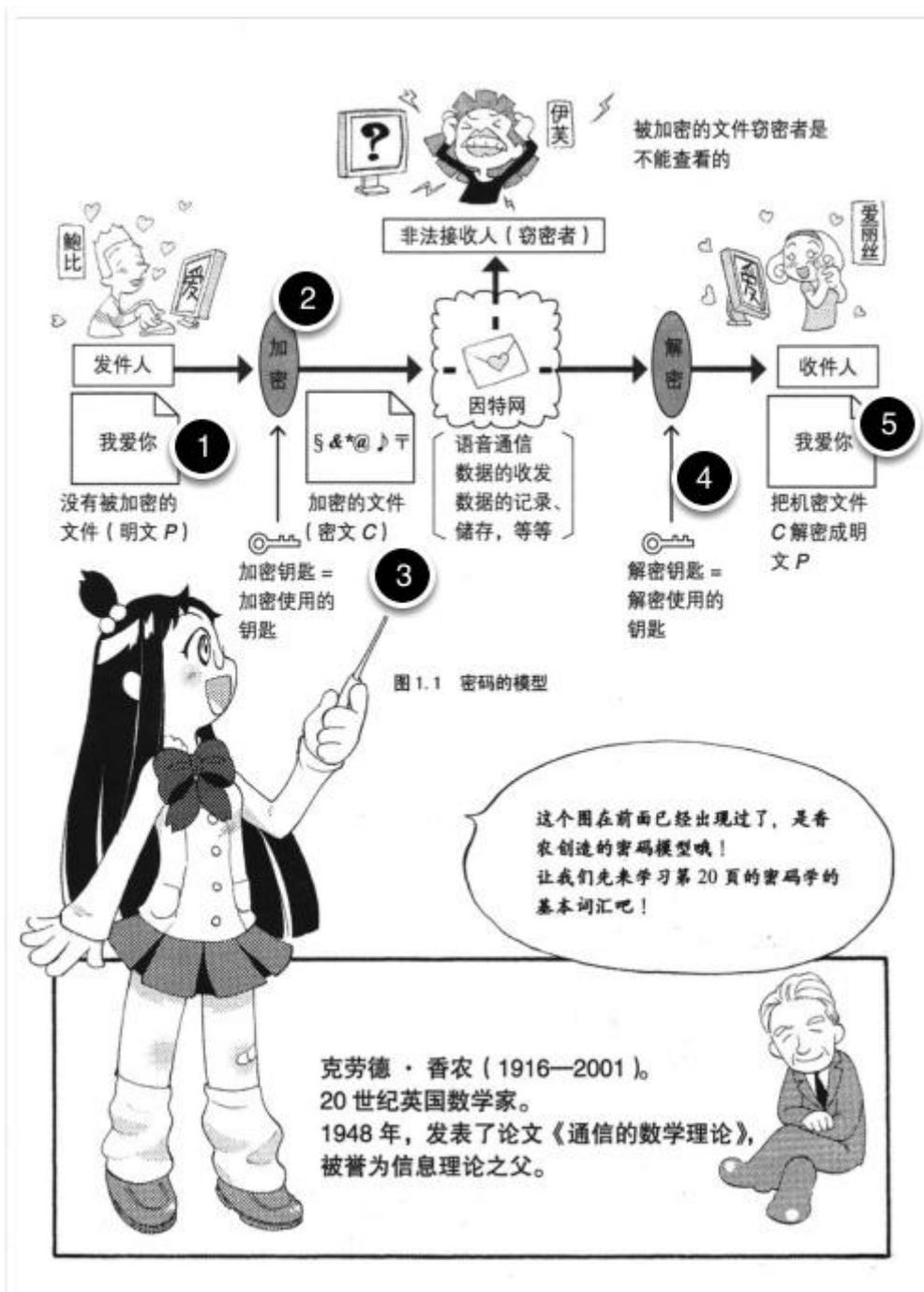
接下来说说关于 DCP 的命名。我们在工作中经常会收到存有数字电影 DCP 的硬盘，这些硬盘上面往往标有硬盘中的 DCP 电影的名称，而这些 DCP 在上传服务器后，我们也能通过 SMS 或者 TMS 管理系统界面来看到这些影片的名称。那么如何从这个电影名称中了解到这部影片的相关信息呢，比如这部影片叫什么，是遮幅的还是宽银幕的，是立体声的还是 5.1 声道的。所以 DCP 的命名的标准化就显得非常重要了。于是 ISDCF (Inter-society Digital Cinema Forum) 组织对于数字电影 DCP 的标准命名规则就应运而生了。具体 ISDCF 是如何来规范 DCP 命名的，由于篇幅很长，所以我就提供一下这个组织的官网地址 [digitalcinemanamingconvention.com](http://digitalcinemanamingconvention.com)，大家可以上这个网站学习有关数字电影标准命名的规范。



## 十一、安全与密钥管理

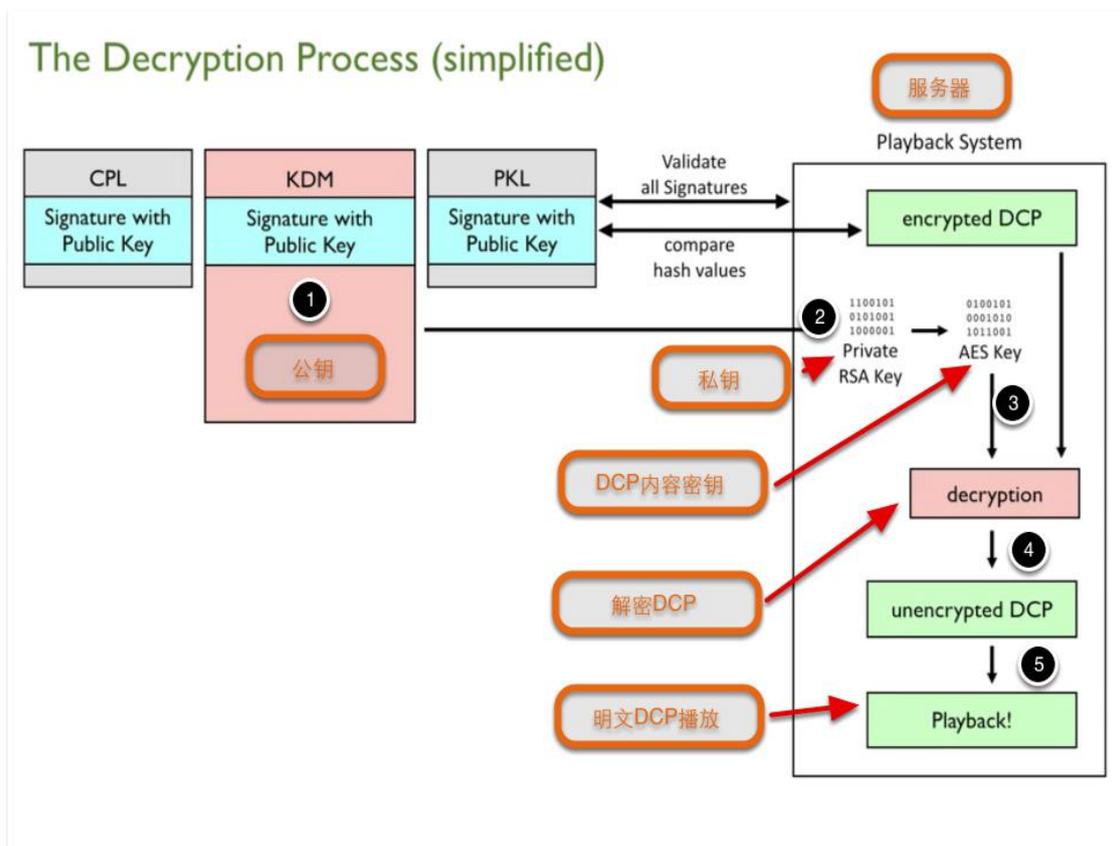
数字电影内容和其他任何节目内容一样，时刻都面临着安全问题，说的通俗一点就是如何防止数字电影内容被盗的事情发生。为了防止数字电影内容被盗，DCI 组织采用了多种技术来防止此类问题的发生。首先对于数字电影节目录包 DCP 采取了 AES128 和 RSA 双重加密技术。说到这里大家可能会马上一头雾水，什么是 AES128，什么是 RSA，什么又是加密，加密的原理是什么。好，为了说明

白这些,我首先来从什么是加密解密说起。其实无论多么复杂的加密和解密技术,其基础原理都是一样的,请看下图。



我们从这张漫画中可以看到,依据香农的理论,不管多么复杂的加密和解密方法,其基本原理或者说模型都是一样的,就象上图所标的 1、2、3、4、5,就是说加密、解密的流程都是从明文 (Plain Text) 开始,比如没有加密过的 DCP 内容,然后经过加密密钥变为密文 (Cipher Text),然后再用解密密钥把密文变为明文。好了,知道了加密和解密原理之后,我再来说说二种当今使用最为频繁的加密、解密技术。第一种是对称加密技术,顾名思义,所谓对称加密技

术就是用于加密和解密的密钥是同一把钥匙，比如 AES128 就是对称加密技术，这种加密技术主要应用于 DCP 内容的加密，就是说加密和解密 DCP 内容的是同一把钥匙，大家不要怀疑，我说的没错，DCP 内容使用的就是 AES128 对称加密。大家可能也注意到了，对称加密有一个致命的问题就是如果这个密钥丢失那么 DCP 内容也就外泄了，这不科学。接下来我再来说说第二种加密技术就是不对称加密技术，同理，一看名字大家就知道了，这个就是加密密钥和解密密钥不是同一把钥匙，说的更明白一些就是加密密钥和解密密钥不是同一把钥匙。那这个不对称加密技术应用于数字电影就是 KDM，就是我们平时从中影和中数密钥网站下载的密钥。且慢，有人会说，我开始晕了，什么又是对称加密，又是不对称加密，什么又是 AES128，又是 KDM。好了，那就让我们运用对称和非对称加密技术来进入数字电影的世界，看看这二种加密技术分别扮演了什么角色。首先说对称加密扮演的角色，这个我想大家很容易理解，对称加密是应用于 DCP 内容包的，采用的是 AES128 算法，就是说对于 DCP 内容包，加密和解密是一把钥匙，为什么会这样，因为 AES128 算法对于大文件解密来说非常快，这样可以保证电影的播放的实时性，但是同样会带来一个问题就是一旦 DCP 内容密钥丢失或者被盗，那后果是相当相当严重的，可以等同于电影内容的外泄。为了解决这个问题，我们采用了第二重加密，即对 DCP 内容密钥本身也采用加密技术来保证其（DCP 内容密钥）安全性，对于 DCP 内容密钥 DCI 采用了非对称加密，那如何实现这个非对称加密 DCP 内容密钥呢。方法如下，数字电影服务器在生产的过程中会产生一对密钥，即公钥和私钥，这二个密钥是不相同的，但是可以互为加密和解密，就是说可以用公钥（实际上就是数字证书）对 DCP 内容密钥进行加密，然后用私钥来进行解密以得到 DCP 内容密钥来对 DCP 进行解密。顺便说一下，私钥是固定在服务器中的，是唯一的，而公钥是公开给节目内容发行方来使用的。为什么非要这么复杂呢，这是因为非对称加密算法（比如 RSA 算法）非常复杂，对于大文件如果直接采用非对称加密后，解密的时间会很长，这样如果应用到数字电影 DCP 内容的直接加密解密的话，无法做到 DCP 内容解密的实时性。而对于小文件来说（比如 DCP 内容密钥本身，一般只有几十 K）应用非对称加密解密可以做到实时性。所以数字电影 DCP 安全性方面是采用二重加密技术，对于 DCP 内容本身采用对称加密技术（比如 AES128），对于 DCP 内容密钥本身采用了非对称加密技术（比如 RSA 算法）这样就做到了电影解密的实时性和电影安全的可靠性。好了说了这么多，大家应该对于数字电影内容的安全性方面应该有一个大致的了解了吧，我来总结一下，就是对于 DCP 包内容本身采用对称加密得到 DCP 内容密钥，然后对于 DCP 内容密钥本身采用公钥加密得到 KDM（KDM 中含有 DCP 内容密钥），然后我们上传 KDM 到服务器，服务器中有私钥对吧，然后私钥对 KDM 解密得到 DCP 内容密钥，再用这个 DCP 内容密钥来解密 DCP，最终得到 DCP 明文用于放映。



## 十二、硬件加密技术

上一节课我和大家聊了聊关于密钥方面的知识，但是大家有没有想过，有了密钥管理用于数字电影 DCP，那 DCP 真的就很安全了吗，答案是否定的。为什么会是否定的，大家有没有想过上一课的知识，DCP 在上传服务器，并经过 IMB 的解压和解密之后已经成了明文 (PLAIN TEXT) 了，就是说已经成了普通的视频流了，这时在 IMB 和放映机之间我们可以轻松地把整个 DCP 录制下来，你说对不对。为了防止此类情况的发生，IMB 和数字放映机之间的硬件加密技术就显得尤其重要了。依据 DCI 规范，服务器和放映机之间必须遵守联邦信息处理标准，简称 FIPS。说的通俗一点就是任何试图篡改媒体块和放映机之间的动作都会引起系统自动停止放映。并且对于媒体块和放映机之间的信息传递一定要有硬件级加密和解密方案。我们知道目前服务器和放映机之间的连接有二种方案，一种是 HD-SDI 连接，一种是整合媒体块于数字放映机中。先来说说 HD-SDI，既然说到 HD-SDI 技术，大家知道吗，HD-SDI 通道只能传递 10BIT 色深（关于色深概念请参考 DCP 基础教程第二章）和 2K 分辨率信息，也就是说如果你要放映 4K 的 DCP，那么这种信息传递技术已经不再适合你了。好了，现来说说 HD-SDI 和数字放映机之间采用的是链路加密技术 (Cinelink Encryption) 来保证数字电影视频信息不会被从媒体块和放映机之间盗取。也就是说 DCP 在媒体块中被解密和解压

变成明文之后，马上采用链路加密技术对解压之后的明文再次进行链路加密传递给放映机，然后放映机再实时进行解密完成放映。大家通过上一课的学习知道了，既然是加密、解密，那密钥是如何来传递给放映机的呢，是通过放映机和服务器之间的网线来传递的，所以大家也可能在实际工作中遇到这根网线一旦接触不良或者松动，都有可能造成系统自动停止放映（满屏雪花），这就是硬件加密技术在起作用。说了 HD-SDI，再来说说媒体块内嵌于放映机技术，这也是今后的一个趋势，为什么呢，有二个好处，一、刚才我也提到过 HD-SDI 只能传递 10BIT 和 2K 分辨率的信息，那如果要放映 4K 电影呢，HD-SDI 已经是无能为力了，所以如果采用基于 PCIE 接口的内嵌媒体块于放映机中的方案，这个问题（4K 放映）就可以解决了，这是其一；二、如果采用内嵌媒体块于放映机中的技术，那媒体块和放映机之间就无需再进行链路加密了，因为解压后的视频流直接进入放映机用于放映了，这样即有利于 4K 和高帧的放映（因为 PCIE 带宽比 HD-SDI 更宽）也能保证 DCP 视频不会被盗取了，一举二得，何乐不为呢。

### 十三、数字水印技术

俗话说做贼容易防贼难。现在很多电影被盗都是通过直接在观众厅通过摄像机的直接拍摄银幕来盗取的。正所谓我拍枪版我怕谁。为了解决这个问题，DCI 组织于是采用了一种叫做数字水印的技术来解决这个问题。所谓数字水印技术就是服务器通过实时叠加人眼看不到，但是可以通过特定技术提取出被偷拍的视频中的一些特定信息（比如是哪个影城、哪个影厅信息）来定位盗取地点，进而追究相关责任人的一种技术。DCI 规范要求，不管哪个服务器，至少要支持 Thomson NexGuard 和 Philips CineFence 这二种水印技术中的一种。