(2019春季　课程编号：011184)

中国科大曾凡平billzeng@ustc.edu.cn

曾凡平
2019信安导论

信息安全导论

第5章 信息隐藏技术

中国科学技术大学 曾凡平
billzeng@ustc.edu.cn

课程回顾：第4章 授权与访问控制技术

4.1 授权和访问控制策略的概念	
4.2 自主访问控制	• 基本概念，授权管理，不足之处 • 完善自主访问控制机制
4.3 强制访问控制	• 基本概念，授权管理，不足之处
4.4 基于角色的访问控制	• 基本概念，授权管理，RBAC的优势
4.5 基于属性的访问控制	• ABAC模型，ABE基本概念
4.6 PMI技术	• PMI基础，PKI和PMI的关系 • PMI授权管理模式、体系及模型 • PMI基础设施的结构和应用模型

第5章 信息隐藏技术

5.1 信息隐藏的概念	
5.2 隐藏信息的基本方法	• 空域算法，变换域算法 • 压缩域算法，NEC算法，生理模型算法
5.3 数字水印	• 技术模型，分类与应用 • 空域水印，DCT水印
5.4 数字隐写	• 技术模型， • 典型数字图像隐写算法
5.5 数字指纹	• 基本概念和模型 • 数字指纹编码，数字指纹协议

5.1 信息隐藏的概念

- **信息隐藏是把一个待保护的秘密信息隐藏在另一个称为载体的信息中**，非授权者不知道这个普通的载体信息中是否隐藏了其他的信息，而且即使知道也难以提取或去除隐藏的信息。所用的载体可以是文字、图像、声音及视频等。
- **现代信息隐藏是一种解决媒体信息安全的新方法**，通过把秘密信息永久地隐藏在可公开的媒体信息里，达到**证实该媒体信息的所有权归属、验证数据完整性或传递秘密信息的目的**，从而为数字信息的安全问题提供一种新的解决方法。
- 这里的安全有两方面的含义：一是可公开的媒体信息在版权和使用权上的安全，二是秘密信息在传输和存储中的安全。

信息加密与信息隐藏的区别

- 信息加密是利用密钥把信息变换成密文，通过公开信道传输。如果要使用这些受保护的信息，必须有正确的解密密钥，没有密钥的非法用户无法从密文中恢复原始信息，从而无法正确使用信息。换言之，**信息加密通过密钥控制信息的使用权**，从而**隐藏秘密信息的内容**，但没有隐藏秘密信息的存在。
- 而信息隐藏更进一步，它是把秘密信息隐藏于可以公开的信息中，使攻击者难以知道秘密信息的存在，从而**掩盖通信过程中存在秘密信息的事实**。其主要目的并不是限制对信息的访问，而是确保宿主信息中隐藏的秘密信息不被改变或消除，从而在必要时提供有效的证明信息。

信息隐藏技术的分类

1. **按载体类型分类**，有文本、图像、音频和视频的信息隐藏技术。
2. **按密钥分类**，若嵌入和提取采用相同的密钥，则称为私钥信息隐藏技术，否则称为公钥信息隐藏技术。
3. **按嵌入域分类**，可分为空域（或时域）和变换域方法。空间域替换方法处理是用待隐藏的信息替换载体信息的冗余部分，而变换域方法处理是对载体信息进行各种各样的变换后嵌入隐秘信息。
4. **按检测是否需要载体信息参与分类**，可分为非盲检测算法和盲检测算法。非盲检测算法中隐秘信息的检测需要原始载体的参与，而盲检测算法中隐秘信息的检测不需要原始载体的参与。

5. 按照保护对象分类

- **(1)隐写术：目的是在不引起任何怀疑的情况下秘密传送消息**，因此它的主要需求包括难以检测和大容量。必须充分考虑到在公开信道中被检测和干扰的可能性。隐写术是相对比较成熟的信息隐藏技术。
- **(2)数字水印：它是指嵌在数字产品中的数字信号**，可以是图像、文字、符号、数字等一切可以作为标识和标记的信息，其目的是进行版权保护、所有权证明、指纹（追踪发布多份拷贝）和完整性保护等，因此，它的性能要求是鲁棒性和不可感知性等。数字水印还可以根据应用领域不同而划分为许多具体的分类，例如用于版权保护的鲁棒性水印，用于保护数据完整性的脆弱性水印等。

按照保护对象分类

- **(3)数据隐藏和数据嵌入：**数据隐藏和数据嵌入通常用在不同的上下文环境中，它们一般指隐写术，或者指介于隐写术和水印之间的应用。在这些应用中嵌入数据的存在是公开的，但不必要保护它们。例如，嵌入的数据是辅助的信息和服务，它们可以是公开得到的，与版权保护和存取控制等功能无关。
- **(4)指纹和标签：**这里指水印的特定用途。有关数字产品的创作者和购买者的信息作为水印而嵌入。每个水印都是一系列编码中唯一的一个编码，即水印中的信息可以唯一地确定每一个数字产品的拷贝，因此，称它们为指纹或者标签。
- 当前，比较活跃的信息隐藏技术主要有两个：隐写术和数字水印。

成功的信息隐藏通常需要满足的技术要求

- **(1)透明性(invisibility)或不可感知性(imperceptibility)：** 指载体在隐藏信息前后没有明显的差别，除非使用特殊手段，否则无法感知机密信息的存在。当然，个别场合也需要可见水印。
- **(2)鲁棒性(robustness)：** 指隐藏对象抗拒常用的信号处理操作而带来的信息破坏能力，即常用的信号处理操作不应该引起隐藏对象的信息丢失。这里的信号处理操作包括滤波、有损压缩、打印、扫描、几何变换、D/A或A/D转换等。
- **(3)安全性(security)：** 指隐藏算法具有较强的抗恶意攻击能力，即它必须能够承受一定程度的人为攻击而使嵌入对象不被破坏。此外，与信息加密一样，信息隐藏技术最终也需要把对信息的保护转化为对密钥的保护。因此，密码学中对密钥的基本要求也适用于隐藏技术。

成功的信息隐藏通常需要满足的技术要求

- **(4)不可检测性(undetectability)：** 指隐藏对象与载体对象需要有一致的特性，例如，具有一致的噪声统计分布等，以便使隐藏分析者无法判断隐藏对象中是否隐藏有嵌入对象。
- **(5)自恢复性(self-comeback)：** 经过某些操作或变换后，可能会使隐藏对象产生较大的破坏。如果只从留下的片断数据，仍能恢复嵌入信号，而且恢复过程不需要载体信号，这就是所谓的自恢复性。当然，并不是所有场合都需要自恢复性。
- **(6)嵌入强度((embedding strength)信息量)：** 载体中应能隐藏尽可能多的信息。在满足不可感知的条件下，隐藏的信息越多，鲁棒性就越差。因此，在具体的隐藏系统中，通常都会涉及不可感知性、鲁棒性和嵌入强度随三者之间的折中。

5.2 隐藏信息的基本方法

- 信息隐藏技术横跨了信号处理、数字通信、密码学、模式识别等多个学科，各专业领域的研究者均有独特的研究角度，使得近年来信息隐藏技术研究取得了很大发展。
- 研究者们提出了很多算法，这些算法大多是在数字图像上发展起来的，大多数算法也适用于数字音频和视频。
- 我们以基于图像载体的信息隐藏技术为例，介绍几种典型算法。

5.2.1 空域算法

- **该类算法中最典型的是将隐秘信息嵌入到随机选择的取样点的值的最低几位上的最低有效位LSB(least significant bits)算法。**
- **LSB是由L.F.Turner和R.G.vanSchyndel等人最早提出的。由于隐秘信息在最低位，相当于叠加一个能量微弱的信号，因而在视觉和听觉上很难察觉。**
- Stego Dos、White Noise Storm和STools等在早期提出的信息隐藏算法都采用了LSB算法。虽然可以隐藏较多的信息，但由于使用的是不重要的像素位，算法对信道干扰及数据操作的鲁棒性差，编码信息很容易遭到信道干扰、数据压缩、滤波、量化和变形等破坏。另一个常用方法是利用像素的统计特征将信息嵌入像素的亮度值中，如Patchwork算法。这是麻省理工学院媒体实验室WalterBander等人提出的，主要用于打印票据防伪。通过适当的调整参数，Patchwork算法可以达到较强的鲁棒性，对剪切、灰度校正、JPEG压缩及FIR滤波等攻击有一定抵抗力，缺陷是嵌入的信息量较低，大信息量嵌入就需要牺牲其鲁棒性。

5.2.2 变换域算法

- **此类信息隐藏算法中的大部分都基于离散余弦变换(DCT)和离散小波变换(DWT)。**这是因为DCT变换是静态数字图像压缩编码标准JPEG和运动图像压缩编码标准MPEG2.0的核心算法，而DWT变换是静态数字图像压缩编码标准JPEG-2000和运动图像压缩编码标准MPEG-4的核心算法。
- DCT变换域的基本思想是：先计算原始图像D的离散余弦变换(DCT)，然后将隐秘信息叠加到变换域的系数上（不包括直流分量），这些系数通常为图像的低频分量。即使载体图像经过一些通用信号处理操作，但仍能从中提取出一个比较可信赖的隐秘信息的拷贝。

- 在此算法的基础上，有不少改进算法。
- 常出现的改进是按照应用条件选择变换域，可以将数字图像的空域数据通过离散余弦变换(DCT)、离散傅里叶变换(DFT)或离散小波变换(DWT)转化为相应的频域系数。
- 第二种改进是根据待隐藏的隐秘信息的类型，对它进行适当的预编码或变形，以提高嵌入的信息量。
- 第三种改进是根据隐藏信息量的大小和其相应的安全目标，有目的地选择某种变换的频域系数序列（实际应用中可能是高频、中频或低频）。一个简单的方法是将隐秘信息嵌入变换域的中频分量而不是低频分量上，以调节算法的稳健性与隐蔽性之间的矛盾。
- 总的来说，这类算法的隐藏和提取隐秘信息的过程复杂，隐藏信息量不能很大，但抗攻击能力强，很适合应用在数字作品版权保护的数字水印技术中。

5.2.3 压缩域算法

- 隐秘信息的检测与提取直接在数据的压缩域中进行。
- MPEG-4压缩视频数据流的信息隐藏算法原理是：首先，对DCT编码数据块中每一个输入的Huffman码进行解码和逆量化，以得到当前数据块的一个DCT系数；其次，把相应隐秘信息的值与之相加，从而得到隐秘信息叠加的DCT系数；再重新进行量化和Huffman编码；最后，对新的Huffman码字的位数n_1与原来的无隐秘信息的码字n_0进行比较，只在n_1不大于n_0的时候，才能传输隐秘信息码字，否则传输原码字，这就保证了不增加视频数据流位率。该方法有一个问题值得考虑，即隐秘信息的引入是一种引起降质的误差信号，而基于运动补偿的编码方案会将一个误差扩散和累积起来。为解决此问题，该算法采取了漂移补偿的方案来抵消因隐秘信息的引入所引起的视觉变形。

5.2.4 NEC算法

- 该算法由NEC实验室的Cox等人提出，在信息隐藏算法中占有重要地位。其实现方法是，首先以密钥为种子来产生伪随机序列，该序列具有高斯分布$N(0，1)$，密钥一般由作者的标识码和图像的哈希值组成；其次对图像做DCT变换；最后用伪随机高斯序列来调制（叠加）该图像除直流(DC)分量外的1000个最大的系数。
- 该算法具有较强的鲁棒性、安全性、透明性等。
- 该算法还提出了增强隐秘信息鲁棒性和抗攻击算法的重要原则，即隐秘信息应该嵌入原数据中对人感觉最重要的部分。这种隐秘信息由独立同分布随机实数序列构成，且该实数序列应该具有高斯分布$N(0，1)$的特征。

5.2.5 生理模型算法

- 人类生理模型包括人类视觉系统HVS(human visual system)和人类听觉系统HAS(human audio system)。该模型不仅被多媒体数据压缩系统利用，同样可以供信息隐藏系统利用。
- 利用视觉模型的基本思想均是利用从视觉模型导出的JND(just noticeable difference)描述来确定在图像的各个部分所能容忍的嵌入隐秘信息的最大强度，从而能避免破坏视觉质量。也就是说，利用视觉模型来确定与图像相关的调制掩模，然后再利用其来嵌入隐秘信息。这一方法可以同时具有好的透明性和强健性。

5.3 数字水印

5.3.1 数字水印的技术模型

- 水印技术是将特定的标记（水印）嵌入到某一媒体信息中，以此实现对该媒体信息进行的某种程度的保护或监控。
- 水印技术主要包括水印嵌入与水印提取两个环节，数字水印技术模型如图5-1所示。

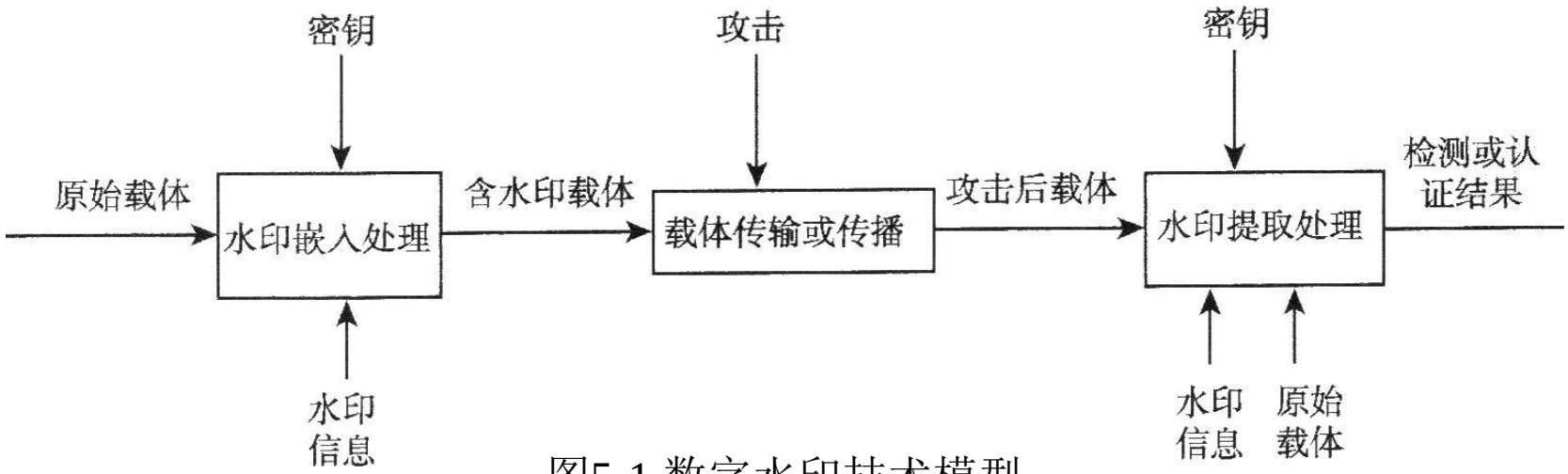
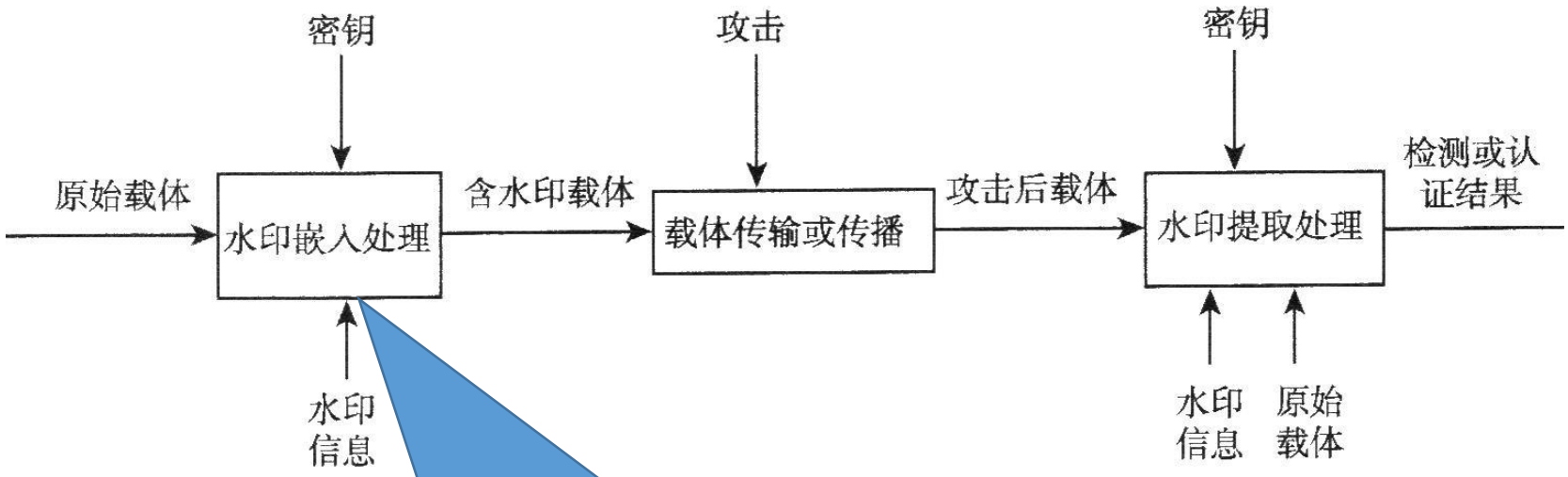


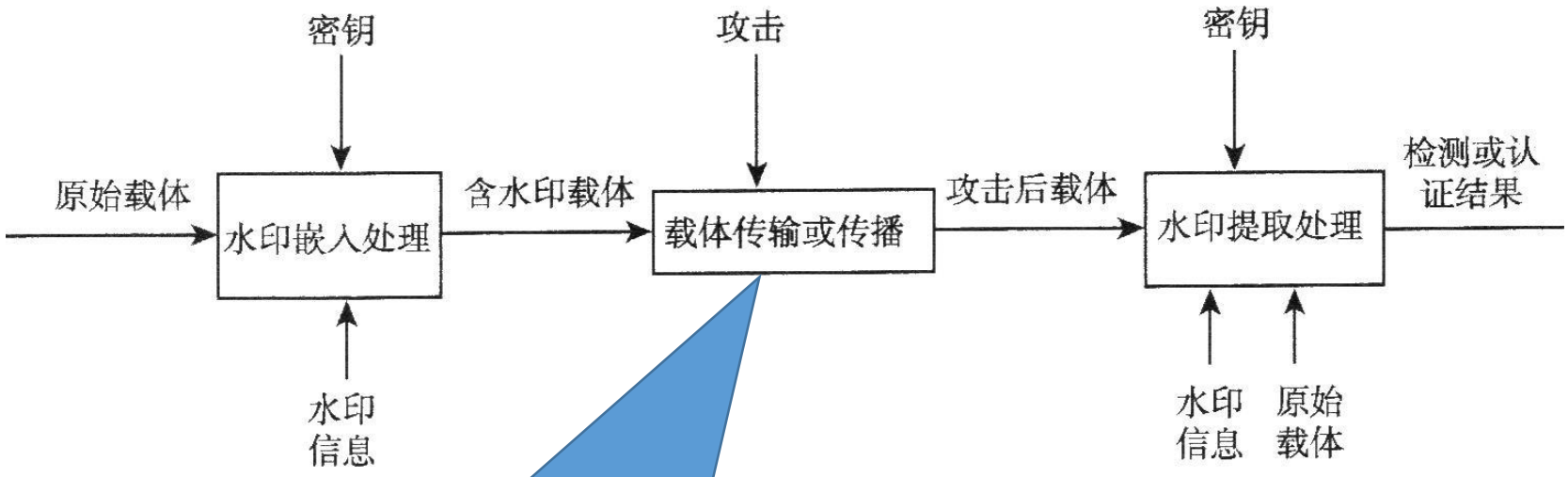
图5-1 数字水印技术模型

数字水印技术模型



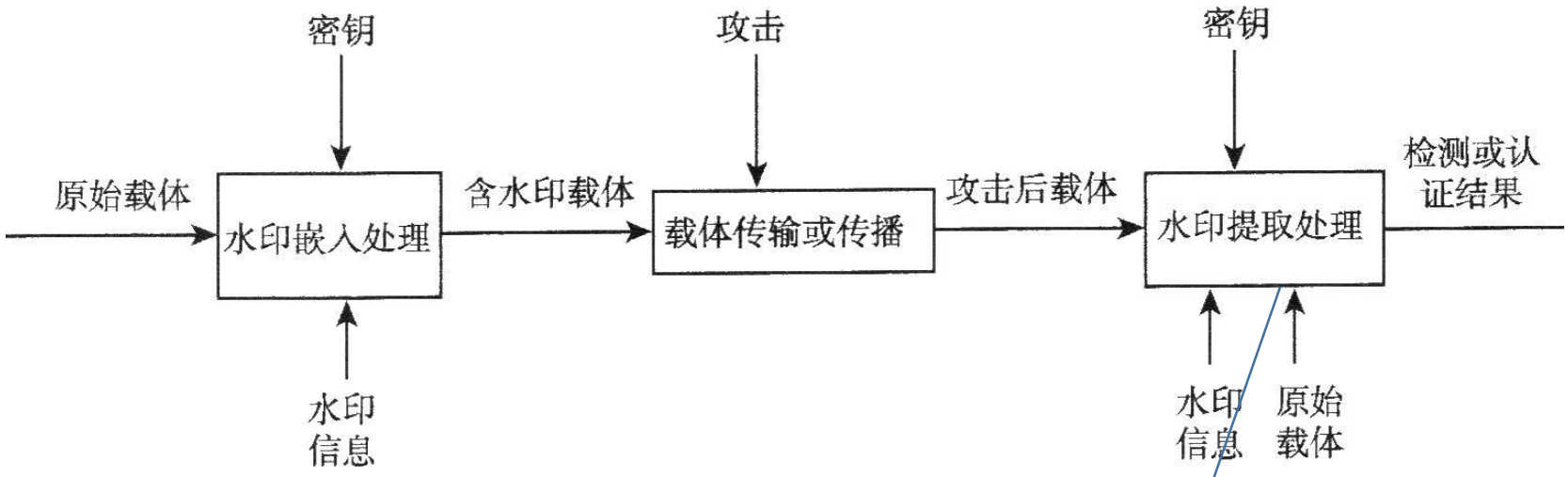
首先，在水印嵌入模块中，系统通过密钥的控制将水印信息嵌入原始载体数据中，形成含水印载体信息，水印的嵌入不应影响载体信息的使用价值；

数字水印技术模型



然后，载体信息在公用信道中进行传输，这一过程中含水印的载体信息可能受到某种形式的信号处理或恶意攻击，形成处理或攻击后的载体信息；

数字水印技术模型



最后，水印提取模块要能够从处理或攻击后的载体中正确地提取水印信息，并作为版权保护或认证的依据。

在一些版本应用系统中，提取过程可能需要原始载体信息作为参照，在认证系统中还会需要原始水印信息作为认证样本。

5.3.2 数字水印的分类与应用

1．鲁棒性水印(robust watermarking)和脆弱性水印(fragile watermarking)

- **鲁棒性水印是指恶意攻击下仍然不能被修改、去除的水印，主要用于版权标识。**数字指纹也属于鲁棒性水印，它主要是使用者的信息嵌入数字媒体中实现知识产权的跟踪保护，当发现非法复制品时可根据数字指纹确定非法复制品是从哪一个使用者那里流出来的。
- **而脆弱性水印则是能够察觉载体信息的细微变化，并可根据被破坏的情况记录产品受到的攻击。**应用中还有半脆弱性水印，它对一些如压缩编码、滤波等正常信号处理具有鲁棒性，而对剪切、篡改等恶意处理是脆弱的。
- 而结合鲁棒性水印、脆弱性水印和数字指纹技术所形成的**综合版权管理系统**则可以对数字化产品同时实现版权认证、完整性认证和非法复制跟踪的保护功能。

2．可见水印和不可见水印

- **所谓可见水印就是嵌入的保护标识是可见的**，最常见的可见水印的例子是有线电视频道或图像上的半透明标识，其主要目的在于明确标识版权，防止非法使用。不可见水印则把水印信息完全隐藏起来，目的是为了获得惩罚盗版者的证据。

3．私有水印和公有水印

- **检测水印时必须采用原始数据作为参照的水印系统称为私有水印，而不需要采用原始数据进行检测的称为公有水印。**私有水印的应用范围相对较窄，版权所有者根据私有水印鉴别非法复制品时，必须连同原始信息一并作为证据。公有水印的应用范围则更广泛，任何一个拥有检测软件的使用者都可以鉴别信息产品是否为盗版。通常私有水印有更好的性能，往往能抵御相当强大的攻击。但从应用角度来看，公有水印系统更具优势。

4．对称水印和非对称水印

- **对称水印的嵌入与水印的提取互逆。**当水印算法公开的条件下，如果攻击者知晓密钥，就能轻易删除水印，所以目前水印密钥一般是不公开的。
- **非对称水印要求在公开水印检测算法和密钥的时候，任何人都可以方便地检测水印，但却无法根据检测算法和密钥去除已嵌入的水印信息。**国外有些学者已经在非对称水印方面做了有益的探索，但切实可行的真正意义上的非对称水印方案研究还有待后来者的努力。

5.多比特水印和1比特水印

- 如果嵌入的水印信号没有具体含义，只是表示“有水印”或“无水印”两种情况，这实际上只含有1比特信息，称为1比特水印。而嵌入多比特有意义的信息（如版权所有者姓名、地址、出品时间）的水印称为多比特水印。同1比特水印相比，多比特水印更有实际应用价值，但其设计难度将加大。

5.3.3 空域水印

- Bender等人提出了两种数据隐藏方法，**第一种是称作“Patchwork”的方法**，随机地选取一对像素(a_i，b_i)，通过对a_i加1而同时对b_i减1达到隐藏1比特的目的。
- 假设图像满足一些统计特性：N个像素对的a_i与b_i差的和为2N，即

$$\sum (a_i - b_i) = \begin{cases} 2N, & \text{用于嵌入水印} \\ 0, & \text{没有水印} \end{cases} \qquad (5\text{-}1)$$

第二种方法称作纹理块编码(texture block coding)，通过把图像的一种纹理块复制到该图像中具有相似纹理特性的区域来完成水印的嵌入，恢复时必须计算自相关特性。这种算法的优点是稳定性高，几乎可以抵抗任何形式的攻击，这是因为即使图像所有区域都被破坏，但其自相关特性仍然存在。

- Pitas和Kaskalis利用Patchwork算法的基本原理，提出了**数字图像签名**的思想。水印S={$S_{m,n}$}是一个与原始图像相同大小的二进制矩阵，且其中“1”和“0”个数相同。给定原始图像I，假设其亮度值为$X_{m,n}$，其中m与n分别表示图像矩阵的行与列，将I分成两个大小相同的子阵A与B，具体分割如下：

$$\boldsymbol{A} = \{X_{mn} \in I, S_{mn} = 1\}$$
$$\boldsymbol{B} = \{X_{mn} \in I, S_{mn} = 0\} \qquad (5\text{-}2)$$

令k为一常数因子，用于控制水印嵌入强度，将水印嵌入子阵A中，方式如下：

$$\boldsymbol{A}' = \{x_{mn} + k, \quad x_{mn} \in \boldsymbol{A}\} \qquad (5\text{-}3)$$

式中，A'为加入水印后的子阵，联合A'和B这两个子阵构成加入水印后的图像矩阵。

数字图像水印的检测

在水印检测时利用假设检验，计算子阵A'的均值与子阵B的均值的差异并归一化得到检测概率q，如式5-4所示：

$$q = \frac{\overline{b} - \overline{a}'}{\sigma_\lambda^2 + \sigma_\beta^2} \qquad (5\text{-}4)$$

式中，σ_λ^2 与 σ_β^2 分别为子阵 A' 和 B 的方差。

当q大于给定阈值时，则证明水印存在；反之，则水印不存在。这种算法可以有效抵抗二次采样攻击与JPEG压缩。

- **Chen和Wornell提出了量化水印算法，他们称这种算法为量化索引调制(quantized index modulation，QIM)。**这种算法的关键是，量化器的设计必须满足给定的限制条件，这样可以保证对每一个量化器重构数据都远离重构点。嵌入数据与所选择量化器下标对应，通过量化过程，在空间域或DCT域中利用所选择的量化器嵌入信息。在解码过程中，计算所有量化器的距离，具有最小距离的量化器所对应的下标值就是嵌入数据。他们给出的性能分析表明，这种水印算法好于利用标准扩频调制原理的算法，但忽略了水印权重设计的水印算法。
- 除了上述几种与调制有关的空域水印算法外，**Maes等人提出了改变图像几何特征的水印算法。**这种方法是基于密度线模型的，伪随机地产生一密度线并用作水印，计算图像中的突变点，如利用边缘检测滤波器，改变这些突变点使得在相邻线内有足够多的点。检测时，只要检测相邻线内是否具有足够多的点就可以确定水印是否存在。

5.3.4 DCT域水印

- **与空域图像水印相比，DCT域图像水印鲁棒性更强且与常用的图像压缩标准JPEG兼容**，因此得到了广泛的重视。
- E.Koch和J.hZao首先利用DCT分解设计水印算法，他们不是把水印加载到整幅图像上，而是随机地选取图像的一些区域加以改动以嵌入水印。
- Coxls等人首先提出了将水印嵌入图像中感知性较强区域的思想，他们对整幅图像作二维DCT变换，然后选取1000个低频DCT系数并加以改变，用一高斯序列代替水印序列。检测时，通过计算高斯序列与从加水印图像中得到的1000个改动过的低频DCT系数的相关性来判断水印是否存在。另一大类方法不是对整幅图像作DCT变换，而是把图像分成块，如8x8块DCT变换。嵌入水印时也不是在每一块系数中嵌入水印，而是仅选取感知性强的块进行水印嵌入，如选取人眼较敏感的中频DCT系数。

Tao和Dickisnon提出的自适应DCT域水印算法

- Tao和Dickisnon给出了一种自适应DCT域水印算法，它是基于给定灵敏度下的区域敏感性分类的，把水印加载在N个AC DCT系数上。根据JPEG压缩中的量化表，由低到高地选取N个AC系数，对选取的系数作如下修改：

$$\hat{x}_i = x_i + \max\left[x_i a_m, sign(x_i)\frac{D_i}{K}\right] \quad (5\text{-}5)$$

式中，α_m表示当前块的噪声敏感度，D_i为x_i的量化步长，K满足$5 \le K \le 6$。值得注意的是，水印信号不是随机产生的。噪声敏感度的确定有许多方法，都是利用人类视觉系统的掩蔽特性。

Tao和Dickisnon提出的一种区域分类算法

- Tao和Dickisnon提出一种区域分类算法，他们把每一块分成6类，这种分类算法利用了人类视觉系统的亮度掩蔽、边缘掩蔽及纹理掩蔽特性，以噪声敏感性递减的顺序，把这六类分别定义为：边缘、均匀、低敏感、中敏感、敏感及很敏感，每一类分配一噪声敏感度。
- 恢复过程需要原始图像及水印信号且是基于假设检验的。实验结果证明，运用这种加载的水印能够有效抵抗JPEG压缩，即使压缩质量因子为5%时，效果仍然很好。同时，这种水印还有很好的抗噪特性，即使噪声的PSNR为22.1dB时，仍然可以检测到水印。

5.4 数字隐写

5.4.1 隐写的技术模型

- 隐写又称信息隐密，是信息隐藏的一个重要分支。古希腊的“蜡版传书”和中国古代的“藏头诗”，都是隐写技术。
- “藏头诗”举例，《水浒》：

  芦花丛中一扁舟，
  俊杰俄从此地游。
  义士若能知此理，
  反躬难逃可无忧。

- 暗藏“卢俊义反”四字。结果，成了官府治罪的证据，终于把卢俊义“逼”上了梁山。

现代隐写技术的模型

- 由于对数字媒体的修改非常方便，可以根据给定的算法和密钥将秘密信息嵌入到图像、音频或视频等数字多媒体信号中，使得秘密信息在传输过程中不引起第三方或信道监控者的怀疑。接收方在得到载有秘密信息的数字载体后，可以根据提取算法和同样的密钥恢复秘密信息。
- 秘密信息的提取一般不需要原始载体，这和一些需要载体信息作为参照的数字水印提取方法有所不同。
- 隐写的一般模型如图5-2所示。

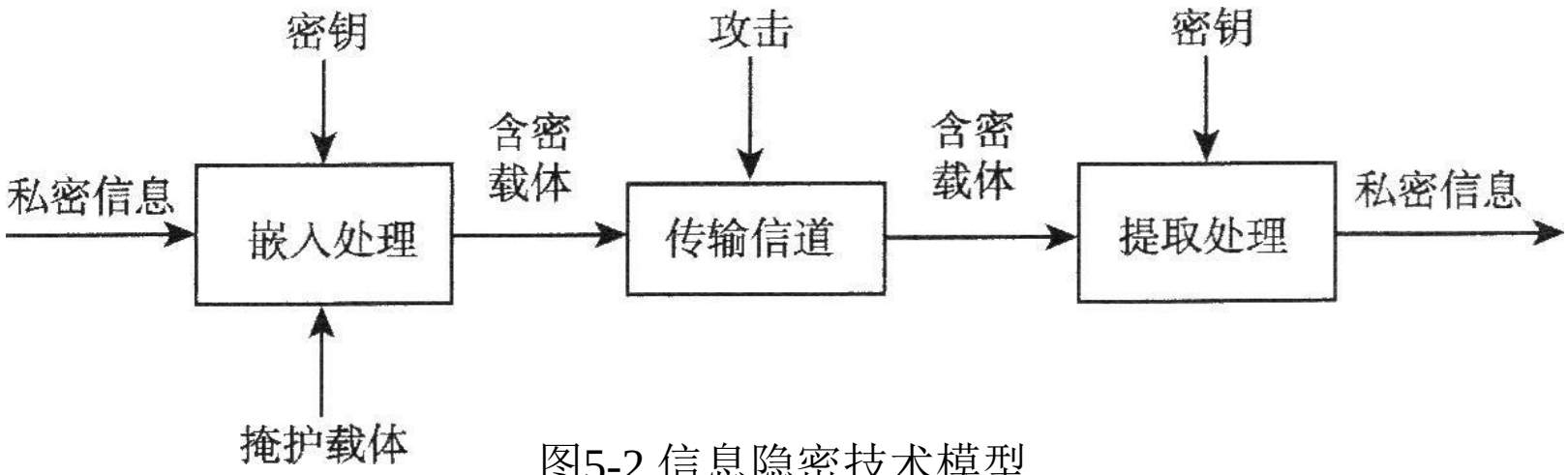


图5-2 信息隐密技术模型

5.4.2 典型数字图像隐写算法

- 目前流行的隐写主要以数字图像、数字语音、数字视频等流行多媒体为载体，同其他信息相比，这些多媒体有较大的容纳秘密信息的冗余空间。
- 基于数字图像的隐写研究目前比较成熟，实用研究成果较多，并为基于其他载体的隐写算法提供了理论借鉴。

1．LSB算法

- 数字图像隐写方法中，**LSB(least significant bit，最低有效位)**隐写算法出现较早、通用性较好，其原理几乎可以应用于所有媒体。这种隐藏方法实现比较容易，而且可以隐藏大量的秘密信息。

- 在非压缩通用数字图像格式中，灰度图像多采用8比特数值逐点表示像景，而彩色图像中像素多采用红、绿、蓝三个分量表示，每个分量由8比特数值表示。由于人眼视觉在灰度和色度细节分辨能力的局限性，很难察觉到较小幅度的灰度、色度变化，所以，**LSB算法直接用秘密信息来取代图像像素值的最低位来实现秘密信息的传递。**
- **LSB是一种最基本的隐写方法，其他很多种流行的隐写算法大都是由LSB方法派生出来。**例如，将空域像素值LSB推广到频域DCT系数就形成了JPEG图像隐写技术；把LSB与视觉特性结合起来就形成了隐藏容量相对较大的、基于位平面复杂度的隐藏方法；在图像索引值上做些调整形成的基于索引色图像的隐写算法。基于其他媒体的隐藏算法也或多或少的参考了LSB算法的基本思路。

LSB隐写算法的改进

- 由于LSB是一种实用、成熟的隐写算法，许多隐写分析算法都以LSB算法为目标进行针对性的攻击。
- 针对这些检测攻击算法，LSB隐写算法又进行了许多改进，形成了许多具有抗分析能力的LSB算法变种。

- 比如信息嵌入不再是简单替代，而是通过像素值规律性调整来携带信息；有的还采用了一些补偿修改来保证信息嵌入不留下明显的痕迹。

2. 自适应嵌入的隐写算法

- **隐藏容量是隐写技术一个非常重要的指标**，它要求在满足视觉不可感知的前提下，尽可能多地隐藏信息。为了提高隐藏容量，很多隐写方法利用人类视觉特性进行自适应嵌入，把最低有效位方法进行了推广，不但利用图像最低位平面来携带信息，其他符合条件的位平面也参与携带信息。
- **基于位平面复杂度分割的隐写算法BPCS(bit plane complexity segmentation)就是一种典型的充分利用人眼视觉冗余的信息隐藏方法**。具体做法是，将图像的多个位平面分块，计算所分子块的复杂度，对于复杂度较高的块，人眼的分辨能力较低，因此可以利用这些变化复杂的块来携带秘密信息。BPCS最初是基于空间域的图像设计的，随后该方法的提出者又将其应用于小波压缩域。

PVD(pixel value differencing)隐藏算法

- PVD(pixel value differencing)隐藏算法的原理与BPCS基本相同，只是PVD方法不是通过图像分块来确定图像的复杂度，而是根据相邻像素的差异情况来确定图像的复杂程度。
- 这两种方法的机理均是建立在人的视觉对复杂变化的图像信号不敏感的基础之上。
- 研究人员对上述算法作了改进，实现了性能更为优越的隐藏算法。

3．流行的JPEG图像隐写算法

- 隐写算法中的载体信息的格式是影响隐写安全性的一个很重要的因素。基于BMP格式的24位真色彩图像隐写算法虽然具有优良的携密性能，但由于其自身数据量较大，很难适应带宽并不十分宽裕的互联网络信道传输。
- 因此，更具伪装特性的图像隐写算法往往选择通用性强的媒体信息作为载体，基于最为流行的JPEG压缩编码格式的隐写算法就是典型代表。
- 目前网上流行的JSteg、Outguess、F5等隐写方法中的信息载体均为JPEG格式图像，这些流行算法大都采用频域DCT系数的LSB算法或其改进算法来实现。

JPEG图像隐写算法

- 一种较新的JPEG图像隐密算法是首先修改DCT量化步长来调整载体图像的DCT系数，在调整后的DCT系数上进行秘密信息的嵌入，此方法确实增加了隐藏容量，但量化表的调整却容易被检出异常，使其系统安全性降低。
- 虽然上述这些流行软件和算法在隐藏容量和不可感知特性上都有一定的品质，但目前已有专门的隐密分析算法可对它们进行有针对性的分析攻击。而与之同时，具有抗分析能力的图像隐藏算法也在不断推出，并成为该方向上的研究热点。而图像格式中的新贵JPEG-2000标准的出现又为该类信息隐藏算法的研究提供了一个崭新的舞台。

4．调色板图像的隐密算法

- 以GIF格式为代表的调色板图像是因特网上一种常见的图像资源，普通格式的彩色图像多采用24比特表示每个像素的三种基色，可以组合成2^{24}种不同颜色。
- 但实际一幅彩色图像中出现的颜色数目往往远小于这个值，调色板图像就是用较少的颜色种类（如256色）显示出可接受的彩色视觉效果。在调色板图像中，如果一幅调色板图像中仅出现256种颜色，则图像格式为每一种出现的颜色分配一个8比特颜色索引值，而每个像素也采用8比特颜色索引值表示当前像素的数值，这使得存储图像所需的数据空间仅为原来的三分之一。

基于调色板的隐写方法

- 现有基于调色板图像的隐密算法可分为两大类：基于调色板的方法和基于像素索引值的方法。
- **基于调色板的方法**通过改变调色板中颜色的排列顺序来嵌入秘密信息。如果调色板颜色种类为N，那么排列顺序共有N!种，可以携带$\log_2(N!)$比特信息。因此N为256时，一幅图像最多可以嵌入1675比特信息。这个方法的优点是信息隐藏不会改变图像的视觉效果，其嵌入量不会随载体图像尺寸的增大而增大，同时调色板的杂乱无章也会引起监控者的怀疑，而且许多图像处理软件可以根据亮度、出现频率对调色板进行重排，这样就会删除已嵌入的秘密信息。

利用索引色图像的像素值来携带秘密信息

- 以EZ Stego为代表的隐密算法则是利用索引色图像的像素值来携带秘密信息。该方法将颜色按照亮度排序，用奇数位置的颜色代表秘密信息“0”，偶数位置的颜色代表秘密信息“1”。
- 如果像素原始颜色代表的信息与嵌入的秘密信息不同，则将该像素的索引值改变为相邻位置的索引值，使其能够对应相应的秘密信息。该方法与LSB方法有类似之处，但是由于亮度接近的不同颜色之间的差异可能较大，会导致产生较大的失真。
- 其后，Fridrich提出了一种改进算法，当像素的原始颜色与欲嵌入的秘密信息不同时，将其改为最接近的颜色。换言之，一种颜色与其最接近的颜色必然代表不同的秘密信息，这种方法被称着最佳奇偶分配(optimal parity assignment)隐密。

5．二值图像的信息隐密

- 二值图像是一种只有黑白两种像素的特殊图像格式，对这两个反差极大的色调做直接修改很容易引起视觉异常，典型的LSB算法并不适用。
- 因此，针对该类载体信息，必须在信息嵌入时重点考虑视觉上的不可感知性的实现（即视觉的空间屏蔽效应）。

- 目前研究中，二值图像信息隐藏主要有三种实现思路：大块图像做微小平行移位，小范围图像做修改，有条件的以空间分辨率换取灰度分辨率。

6．文本文档信息隐密

- 作为一种特殊的数据载体，文本文档信息的冗余空间有限，因此，基于文本文档的隐密算法设计具有一定难度。目前主要有以下几种方法：

✓一是利用空格、标点、回车换行等不可显示字符携带信息，这种方法主要针对纯文本载体（如TXT文件）；二是利用文档的格式，如行间距、字符间距、字符大小、字符位置等参数携带秘密信息，这种方法适用于带有格式定义的文本载体（如PDF文件、DOC文件、NH文件、电子图书等）；三是利用语义，通过同义词或近义词替代的方法进行信息隐藏。此外，还有利用文件结构进行信息隐藏的方式。

5.5 数字指纹

- 数字指纹技术是和数字水印技术一同发展起来的新型数字版权保护技术。比较而言，数字水印是向数字产品中嵌入版权拥有者的一些信息，当发生争议时能够有效确认出版权归属，对相同的作品嵌入的水印信息是相同的。
- 而数字指纹是在原产品中嵌入与用户有关的信息，产品提供者（也称发行商）能够根据该信息对非法用户进行跟踪，嵌入的内容对不同购买者是不同的。
- 通常来讲，**数字指纹是指与用户和某次购买过程有关的信息。**当发行商发现被非法分发的授权信息时，可以根据该信息对进行非法分发的用户实现跟踪。

数字指纹体制

- **数字指纹体制主要由两部分构成：一是用于向拷贝中嵌入指纹并对带指纹拷贝进行分发的拷贝分发体制；二是实现对非法分发者进行跟踪并审判的跟踪体制。**
- 这两部分通常通过发行商、用户之间的一系列协议实现。因此数字指纹体制也可以分为算法和协议两部分。
- 其中，算法包括指纹的编码和解码、指纹的嵌入和提取以及拷贝的分发策略等内容，而协议部分则规定了各实体之间如何进行交互以实现具有各种特点的拷贝分发和跟踪体制（如实现用户的匿名性等）。
- 数字指纹体制的简单模型如图5-3所示。

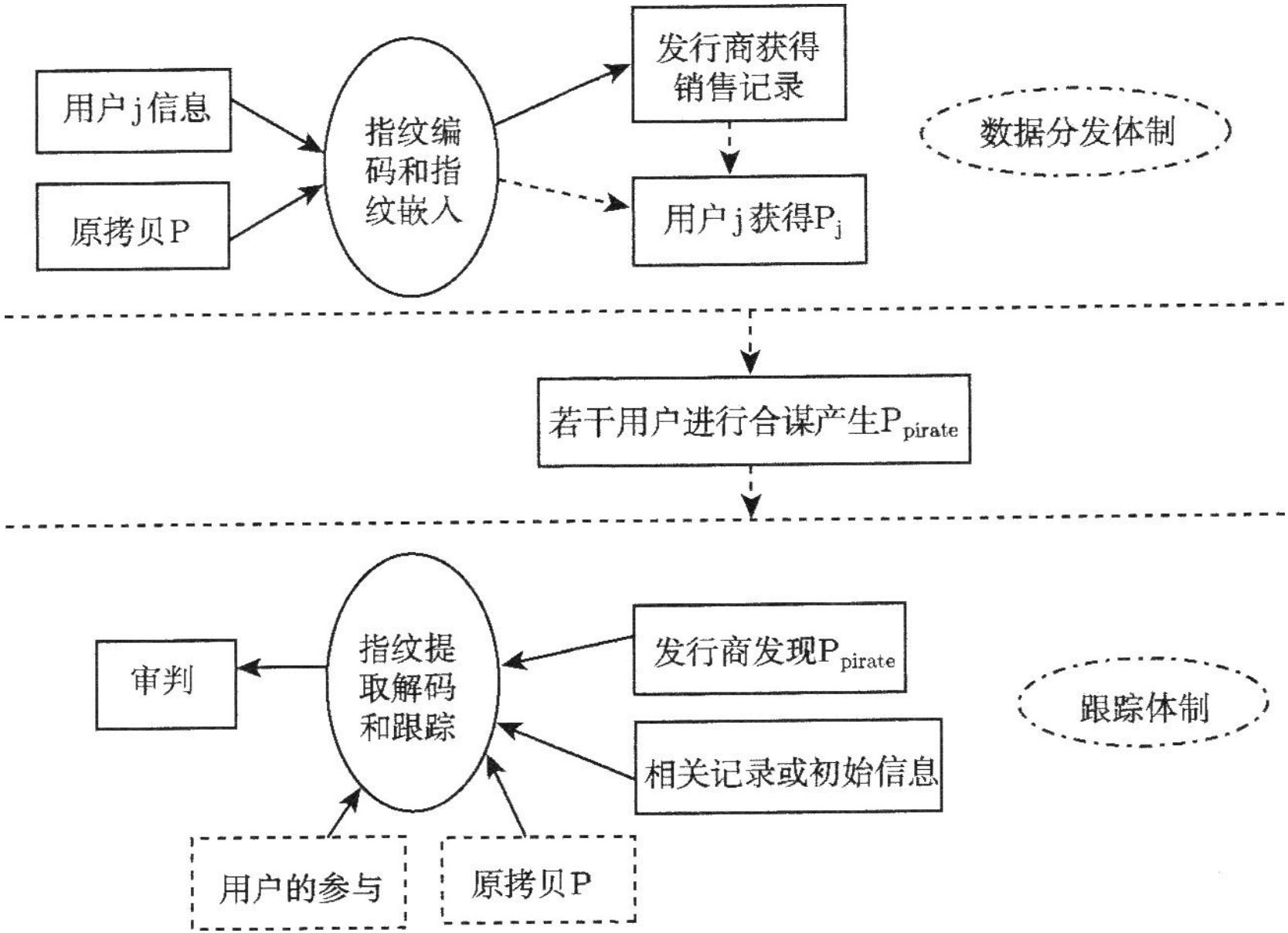


图5-3 数字指纹体制的简单模型

- 用户j的信息由用户提供或由其与发行商（或登记中心等实体）通过一系列交互后生成，通常包括用户的身份信息及购买过程的描述信息。有关用户j的信息将被按照一定规则进行编码并嵌入到发行商要出售的原拷贝中。用户直接得到带有其指纹的拷贝或由发行商将带有指纹的拷贝发放给用户，同时发行商和用户得到有关交易记录。
- 不诚实的用户可能会直接分发他所得到的拷贝，也可能与其他用户联合获得新的拷贝后分发。无论是哪种情况，非法分发的拷贝中都会留下参与非法活动用户的指纹信息。一旦发行商发现了非法拷贝，他将运用相应的指纹提取及指纹解码技术，并采用跟踪算法跟踪非法分发者。一般来说，只要发行商能够成功地跟踪出一个非法分发者，就认为该跟踪算法是成功的；如果该跟踪过程不能给出一个合谋者或者将一个无辜用户认为是非法分发者，则认为该跟踪算法是失败的。
- 指纹的编码方法以及合谋人数多少是影响跟踪成败的关键因素。

数字指纹方案通常应满足以下几项基本要求

- **(1)保真性。**嵌入指纹后的数据拷贝相对于原拷贝，其质量不应降低。这实际是信息隐藏方案的基本要求。
- **(2)鲁棒性。**嵌入的指纹信息要能够抵抗可能受到的处理、操作甚至是恶意攻击，使得提取出的信息足以跟踪出非法分发者。鲁棒性要求攻击者不能对指纹进行随意修改，其理想目标是使攻击者无法在不破坏原拷贝的情况下伪造出一个新的可用拷贝。
- **(3)嵌入量。**因为嵌入的内容要实现用户攻击后能留下足够的信息使发行商进行跟踪，因此要求有足够的嵌入量。
- **(4)合谋容忍性。**这是对数字指纹的一个关键要求。通常从以下两个方面考虑合谋容忍性：①在一定的合谋人数下，发行商能够确定出至少一个非法分发者，该人数称为合谋安全尺寸；②无论合谋人数的多少（即使超过了上述尺寸），无辜购买者也不能受到指控。
- **(5)效率。**要求带指纹拷贝的生成算法和跟踪算法的实现具有很好的效率。
- 以上是对数字指纹体制的若干基本要求。此外还有其他的一些要求，如实现用户的不可否认性、用户的匿名性等。

5.5.2 数字指纹编码

- 由于数字指纹方案要对抗用户的合谋攻击，通常发行商会对用户的指纹进行编码，以增加该指纹方案的合谋容忍能力，这种编码称为合谋容忍编码。**若一个数字指纹体制能够抵抗合谋攻击，则称该指纹编码方案是合谋安全的**。
- 指纹的合谋容忍编码通常包括两个部分：指纹的编码算法（生成带有用户指纹的拷贝）和跟踪算法(如何对非法用户进行跟踪）。
- 指纹编码方案是指，在一定假设下，将获得的与用户有关的信息按照一定的规则进行编码，生成具有一定抗攻击能力的码字的过程。跟踪方案则是指，当发行商获得盗版拷贝时，运用一定的解码规则判断出非法分发者的过程。

指纹编码方案的分类

- 可以从多个角度对指纹编码方案进行分类。

① 从跟踪成功的概率来讲，指纹编码方案可以分为确定性跟踪方案和概率性跟踪方案。

② 从码字的分布而言，可以分为连续指纹方案和离散指纹方案。

③ 从码字是否随机来讲，还可以分为随机指纹方案和利用某些特殊的组合结构构造的指纹编码方案。

- 现有的指纹编码方案主要是概率性跟踪方案，通过使用连续的或离散的随机信号实现指纹的编码。
- 下面简单介绍一个连续指纹方案。

连续指纹编码方案

- 在连续指纹编码方案中，用户码字中的每一个码元取自一个连续的集合，如一个实数区间。典型代表是Cox等提出的CKLS方案。
- 这个方案用独立随机的正态采样序列作为要嵌入的水印信息，当用作指纹时，为每个用户选取不同的采样序列，序列间是独立的。这里指纹的取值不限于离散的整数值，而是服从正态分布N(0，1)的随机实数序列X。
- 跟踪时，发行商从非法拷贝中提取出嵌入信息X'，将其与X做相关检测，如果相关值大于某一个门限值，则认为非法拷贝中含有该指纹X，称这种体制是CKLS体制。

CKLS体制的指纹嵌入方法

- CKLS体制的指纹嵌入方法是一种基于图像全局变换的嵌入方法。
- 首先对整个图像进行离散余弦变换DCT，然后将嵌入内容叠加在DCT域中幅值最大的前k个系数上（不包括直流分量），通常为图像的低频分量。
- 数字指纹序列记为$X=\{x_i\}$，$i=1，\ldots，k$，记所选择的k个系数为$V=\{v_i\}$，$i=1，\ldots，k$。则嵌入算法为$V_i'=V_i(1+ax_i)$，其中，常数a为尺度因子，控制信息嵌入的强度，其大小正比于相应频率分量的信号强度（简单情况下可用同一强度加载信息）。最后用新的系数做反变换得到水印图像。
- 提取时，分别计算原始图像和水印图像的离散余弦变换便可得到嵌入的水印。
- 该算法不仅具有较好的保真性，而且有较强的鲁棒性。

5.5.3 数字指纹协议

- 在早期的指纹方案中，通常由发行商生成带指纹拷贝发放给用户。因为发行商和用户都知道该拷贝，当发现被非法分发的带有某用户指纹的拷贝时，将无法确定谁应该对它负责。因为拷贝可能是该用户分发的，也可能是发行商本人分发的以对该用户进行陷害。
- 针对这一问题，Pfitzmann和Schunter引入了非对称(asymmetric)指纹的概念。
- 类似于非对称的加密体制能够实现不可否认性，非对称指纹体制最主要的特点是实现非法用户的不可否认性。

非对称指纹体制

- 非对称指纹体制一般由4个基本协议组成：初始化协议（用户进行购买登记和发行商的有关初始化工作）、指纹添加协议（为用户生成带指纹的拷贝）、跟踪协议（确认非法分发者的身份）、审判协议（发行商向第三方提供用户有罪的证据）。
- 目前，非对称指纹体制的构造手段主要有基于一般的安全多方计算协议、利用特殊的密码学协议、利用密码算法等。
- 此外，将公钥密码算法与防篡改硬件相结合也是一种设计非对称数字指纹体制的思路。

匿名(anonymous)数字指纹

- 无论是对称还是非对称指纹协议，用户均需在购买过程中提交自己的身份信息，这破坏了购买过程的隐秘性。正是在这种背景下，Pfitzmann和Waidner中提出了匿名(anonymous)数字指纹。
- 采用这种指纹机制，用户在购买拷贝的过程中不会泄露自己的身份信息。但如果用户进行非法分发活动，凭借非法拷贝中的信息，发行商可以识别非法者的身份。
- 匿名指纹协议的实现通常是引入一个登记中心，负责为用户的真实身份进行登记，同时为用户发放购买过程中需要的一些验证信息（通常是假名及其相应的证书）。

第5章作业

- 作业
  3. 信息隐藏的基本方法有哪些？基本思想是什么？
  4. 简述各种数字水印的应用。
  6. 数字指纹和数字水印的应用场合的不同点是什么？

- 实践（自己研究，不考核）