

# 数字水印技术

主讲 田捷博士

(研究员, 博士生导师)

Email: [tian@dr.com](mailto:tian@dr.com)

<http://www.digiark.com/tian>

第一节	数字水印简介
第二节	数字水印的概念
第三节	数字水印的分类
第四节	数字水印的关键技术
第五节	信息隐藏与数据加密的区别和联系
第六节	数字水印算法的特点
第七节	数字水印与版权保护
第八节	数字水印与数字作品的电子交易
第九节	基于数字水印技术的票据防伪
第十节	数字水印软件现状及发展
第十一节	典型的数字水印软件
第十二节	研究动态
第十三节	研究展望

# 第一节

## 数字水印简介

随着多媒体技术和网络技术的飞速发展和广泛应用，对图象、音频、视频等多媒体内容的保护成为迫切需要的问题。对多媒体内容的保护分为两个部分：一是版权保护，二是内容完整性（真实性）保护，即认证。

传统的加密方法对内容的保护只局限在加密通信的信道中或其他加密状态下，一旦解密，则毫无保护可言；密码学中的认证方法对多媒体内容的保护也无能为力：一方面由于多媒体内容的真实性认证往往需容忍一定程度的失真，而密码学中的认证方法不容许一个比特的改变；另一方面，用于多媒体认证的认证信息往往需要直接嵌入多媒体内容中，不另外保存认证信息，但密码学中的认证方法则需另外保存信息认证码（MAC）。

由于密码学对多媒体内容保护能力的局限，一种新的保护途径应运而生，即数字水印技术，它甚至被认为是多媒体内容保护的最后一道防线。数字水印技术是将与多媒体内容相关或不相关的一些标示信息直接嵌入多媒体内容当中，但不影响原内容的价值，并不能被人的知觉系统觉察或注意到。通过这些隐藏在多媒体内容中的信息，可以达到确认内容创建者、购买者，或者是否真实完整。

用于版权保护的数字水印一般称为鲁棒水印（Robust Watermarking），利用这种水印技术在多媒体内容的数据中嵌入创建者或所有者的标示信息，或者嵌入购买者的标示（即序列号）。在发生版权纠纷时，创建者或所有者的信息用于标示数据的版权所有者，而序列号用于标示违反协议而为盗版提供多媒体数据的用户。用于版权保护的数字水印要求有很强的鲁棒性，除了要求在一般图象处理（如：滤波、加噪声、替换、压缩等）中生存外，还需能抵抗一些恶意攻击。目前，尚无能十分有效用于实际版权保护的鲁棒水印算法。

用于多媒体内容真实性鉴定（即认证）的水印一般称为**易损水印**（**Fragile Watermarking**），这种水印同样是在内容数据中嵌入信息，当内容发生改变时，这些水印信息会发生一定程度的改变，从而可以鉴定原始数据是否被篡改。易损水印应对一般图象处理（如：滤波、加噪声、替换、压缩等）有较强的鲁棒性，同时有要求有较强的敏感性，即：既允许一定程度的失真，又要能将失真情况探测出来。

# 第二节

## 数字水印的概念

- 一、特征
- 二、定义
- 三、一般模型
- 四、应用前景

# 一、特征

数字水印（Digital Watermark）技术是指用信号处理的方法在数字化的多媒体数据中嵌入隐蔽的标记，这种标记通常是不可见的，只有通过专用的检测器或阅读器才能提取。数字水印是信息隐藏技术的一个重要研究方向。

嵌入数字作品中的信息必须具有以下基本特性才能称为数字水印：

## ■ 隐蔽性

在数字作品中嵌入数字水印不会引起明显的降质，并且不易被察觉。

## ■ 隐藏位置的安全性

水印信息隐藏于数据而非文件头中，文件格式的变换不应导致水印数据的丢失。

## ■ 鲁棒性

所谓鲁棒性是指在经历多种无意或有意的信号处理过程后，数字水印仍能保持完整性或仍能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。

在数字水印技术中，水印的数据量和鲁棒性构成了一对基本矛盾。从主观上讲，理想的水印算法应该既能隐藏大量数据，又可以抗各种信道噪声和信号变形。然而在实际中，这两个指标往往不能同时实现，不过这并不会影响数字水印技术的应用，因为实际应用一般只偏重其中的一个方面。

如果是为了隐蔽通信，数据量显然是最重要的，由于通信方式极为隐蔽，遭遇敌方篡改攻击的可能性很小，因而对鲁棒性要求不高。但对保证数据安全来说，情况恰恰相反，各种保密的数据随时面临着被盗取和篡改的危险，所以鲁棒性是十分重要的，此时，隐藏数据量的要求居于次要地位。

数字水印技术的基本思想源于古代的密写术。古希腊的斯巴达人曾将军事情报刻在普通的木板上，用石蜡填平，收信的一方只要用火烤热木板，融化石蜡后，就可以看到密信。使用最广泛的密写方法恐怕要算化学密写了，牛奶、白矾、果汁等都曾充当过密写药水的角色。可以说，人类早期使用的保密通信手段大多数属于密写而不是密码。然而，与密码技术相比，密写术始终没有发展成为一门独立的学科，究其原因，主要是因为密写术缺乏必要的理论基础。

如今，数字化技术的发展为古老的密写术注入了新的活力，也带来了新的机会。在研究数字水印的过程中，研究者大量借鉴了密写技术的思想。尤其是近年来信息隐藏技术理论框架研究的兴起，更给密写术成为一门严谨的科学带来了希望。毫无疑问，密写技术将在数字时代得以复兴。

## 二、定义

将数字水印于一个宿主信号中，但不被觉察到或不易被注意到，而且不影响宿主信号的知觉效果和使用价值。

### 三、一般模型

尚未与密码学一样有较完整的信息论理论基础，目前没有好的理论模型。

嵌入水印： $I' = I \otimes f(I, w, k)$

提取水印：从  $I'$  中提取  $\tilde{I}'$ ，其中

$$\tilde{I}' = I' \otimes n(I') = I \otimes f(I, w, k) \otimes n(I')$$

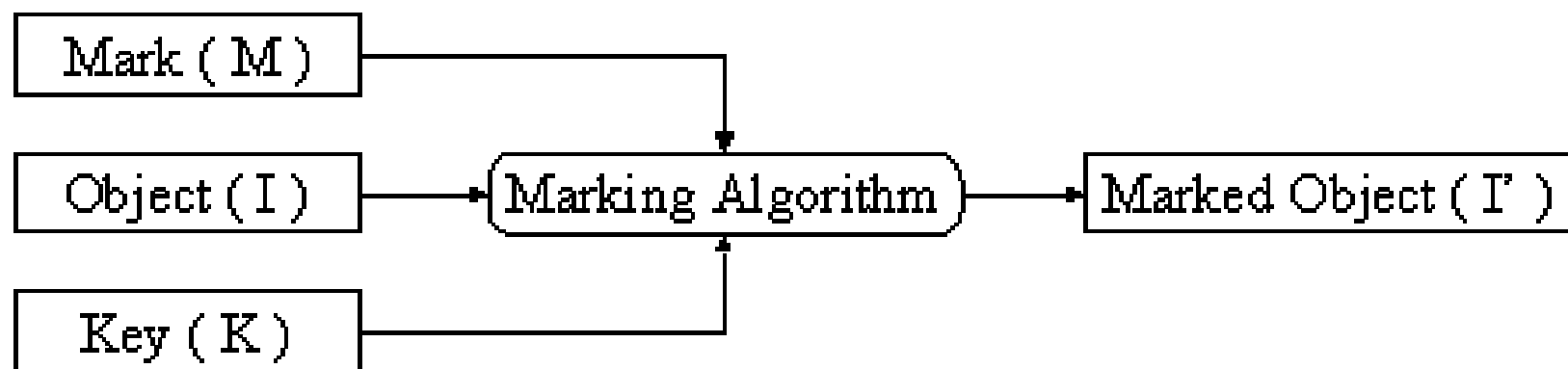


图1: 嵌入水印

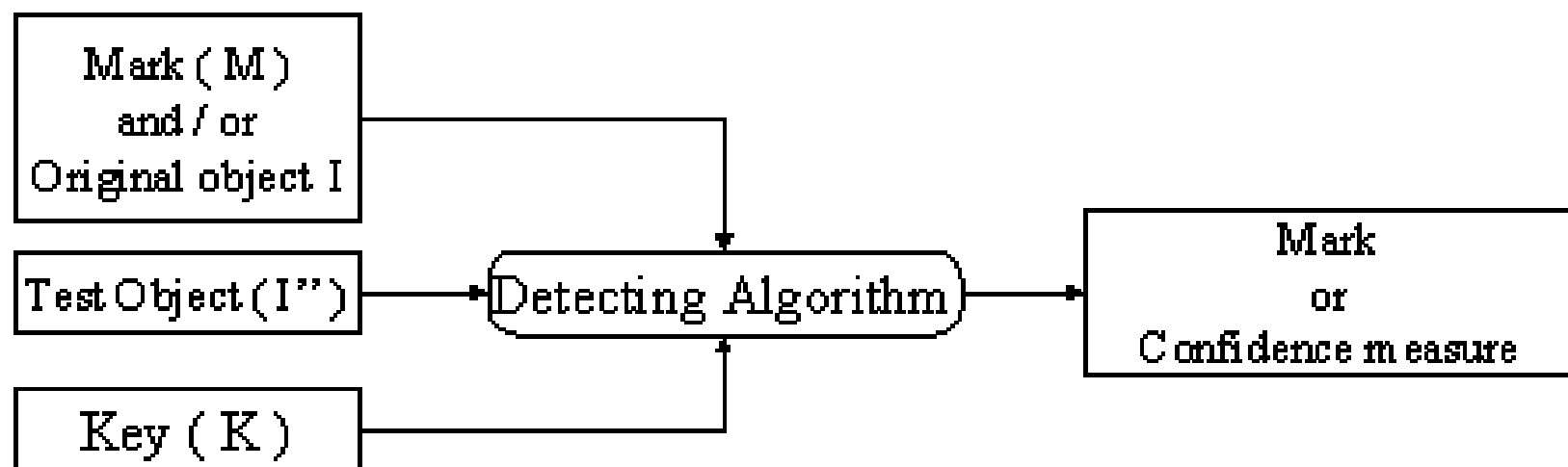


图2: 检测水印

## 四、应用前景

多媒体技术的飞速发展和Internet的普及带来了一系列政治、经济、军事和文化问题，产生了许多新的研究热点，以下几个引起普遍关注的问题构成了数字水印的研究背景。

# 1、 数字作品的知识产权保护

数字作品（如电脑美术、扫描图像、数字音乐、视频、三维动画）的版权保护是当前的热点问题。由于数字作品的拷贝、修改非常容易，而且可以做到与原作完全相同，所以原创者不得不采用一些严重损害作品质量的办法来加上版权标志，而这种明显可见的标志很容易被篡改。

"数字水印"利用数据隐藏原理使版权标志不可见或不可听，既不损害原作品，又达到了版权保护的目。目前，用于版权保护的数字水印技术已经进入了初步实用化阶段，IBM公司在其"数字图书馆"软件中就提供了数字水印功能，Adobe公司也在其著名的Photoshop软件中集成了Digimarc公司的数字水印插件。然而实事求是地说，目前市场上的数字水印产品在技术上还不成熟，很容易被破坏或破解，距离真正的实用还有很长的路要走。

## 2、 商务交易中的票据防伪

随着高质量图像输入输出设备的发展，特别是精度超过 1200dpi 的彩色喷墨、激光打印机和高精度彩色复印机的出现，使得货币、支票以及其他票据的伪造变得更加容易。

据美国官方报道，仅在1997年截获的价值4000万美元的假钞中，用高精度彩色打印机制造的小面额假钞就占19%，这个数字是1995年的9.05倍。目前，美国、日本以及荷兰都已开始研究用于票据防伪的数字水印技术。其中麻省理工学院媒体实验室受美国财政部委托，已经开始研究在彩色打印机、复印机输出的每幅图像中加入唯一的、不可见的数字水印，在需要时可以实时地从扫描票据中判断水印的有无，快速辨识真伪。

另一方面，在从传统商务向电子商务转化的过程中，会出现大量过度性的电子文件，如各种纸质票据的扫描图像等。即使在网络安全技术成熟以后，各种电子票据也还需要一些非密码的认证方式。数字水印技术可以为各种票据提供不可见的认证标志，从而大大增加了伪造的难度。

### 3、 声像数据的隐藏标识和篡改提示

数据的标识信息往往比数据本身更具有保密价值，如遥感图像的拍摄日期、经/纬度等。没有标识信息的数据有时甚至无法使用，但直接将这些重要信息标记在原始文件上又很危险。数字水印技术提供了一种隐藏标识的方法，标识信息在原始文件上是看不到的，只有通过特殊的阅读程序才可以读取。这种方法已经被国外一些公开的遥感图像数据库所采用。

此外，数据的篡改提示也是一项很重要的工作。现有的信号拼接和镶嵌技术可以做到“移花接木”而不为人知，因此，如何防范对图像、录音、录像数据的篡改攻击是重要的研究课题。基于数字水印的篡改提示是解决这一问题的理想技术途径，通过隐藏水印的状态可以判断声像信号是否被篡改。

## 4、 隐蔽通信及其对抗

数字水印所依赖的信息隐藏技术不仅提供了非密码的安全途径，更引发了信息战尤其是网络情报战的革命，产生了一系列新颖的作战方式，引起了许多国家的重视。

网络情报战是信息战的重要组成部分，其核心内容是利用公用网络进行保密数据传送。迄今为止，学术界在这方面的研究思路一直未能突破“文件加密”的思维模式，然而，经过加密的文件往往是混乱无序的，容易引起攻击者的注意。网络多媒体技术的广泛应用使得利用公用网络进行保密通信有了新的思路，利用数字化声像信号相对于人的视觉、听觉冗余，可以进行各种时（空）域和变换域的信息隐藏，从而实现隐蔽通信。

## 5、 使用控制

如DVD防拷贝系统：将水印信息嵌入DVD内容数据中，DVD播放机通过检测DVD数据中水印信息来判断其合法性和能否拷贝。

# 第三节

## 数字水印的分类

数字水印技术可以从不同的角度进行划分。

# 一、按特性划分

按水印的特性可以将数字水印分为鲁棒数字水印和脆弱数字水印两类。鲁棒数字水印主要用于在数字作品中标识著作权信息，如作者、作品序号等，它要求嵌入的水印能够经受各种常用的编辑处理；脆弱数字水印主要用于完整性保护，与鲁棒水印的要求相反，脆弱水印必须对信号的改动很敏感，人们根据脆弱水印的状态就可以判断数据是否被篡改过。

## 二、按水印所附载的媒体划分

按水印所附载的媒体，我们可以将数字水印划分为图像水印、音频水印、视频水印、文本水印以及用于三维网格模型的网格水印等。随着数字技术的发展，会有更多种类的数字媒体出现，同时也会产生相应的水印技术。

### 三、按检测过程划分

按水印的检测过程可以将数字水印划分为明文水印和盲水印。明文水印在检测过程中需要原始数据，而盲水印的检测只需要密钥，不需要原始数据。一般来说，明文水印的鲁棒性比较强，但其应用受到存储成本的限制。目前学术界研究的数字水印大多数是盲水印。

## 四、按内容划分

按数字水印的内容可以将水印划分为有意义水印和无意义水印。有意义水印是指水印本身也是某个数字图像（如商标图像）或数字音频片段的编码；无意义水印则只对应于一个序列号。有意义水印的优势在于，如果由于受到攻击或其他原因致使解码后的水印破损，人们仍然可以通过视觉观察确认是否有水印。但对于无意义水印来说，如果解码后的水印序列有若干码元错误，则只能通过统计决策来确定信号中是否含有水印。

## 五、按用途划分

不同的应用需求造就了不同的水印技术。按水印的用途，我们可以将数字水印划分为票据防伪水印、版权保护水印、篡改提示水印和隐蔽标识水印。

票据防伪水印是一类比较特殊的水印，主要用于打印票据和电子票据的防伪。一般来说，伪币的制造者不可能对票据图像进行过多的修改，所以，诸如尺度变换等信号编辑操作是不用考虑的。但另一方面，人们必须考虑票据破损、图案模糊等情形，而且考虑到快速检测的要求，用于票据防伪的数字水印算法不能太复杂。

版权标识水印是目前研究最多的一类数字水印。数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性和鲁棒性，而对数据量的要求相对较小。

篡改提示水印是一种脆弱水印，其目的是标识宿主信号的完整性和真实性。

隐蔽标识水印的目的是将保密数据的重要标注隐藏起来，限制非法用户对保密数据的使用。

## 六、按水印隐藏的位置划分

按数字水印的隐藏位置，我们可以将其划分为时（空）域数字水印、频域数字水印、时/频域数字水印和时间/尺度域数字水印。

时（空）域数字水印是直接信号空间上叠加水印信息，而频域数字水印、时/频域数字水印和时间/尺度域数字水印则分别是在DCT变换域、时/频变换域和小波变换域上隐藏水印。

随着数字水印技术的发展，各种水印算法层出不穷，水印的隐藏位置也不再局限于上述四种。应该说，只要构成一种信号变换，就有可能在其变换空间上隐藏水印。

# 第四节

## 数字水印的 关键技术

作为感觉器官的眼睛和耳朵并不是完美无缺的，它们有许多可以被数字水印技术利用的缺陷。近年来，认知科学的飞速发展数字水印技术奠定了生理学基础，人眼的色彩感觉和亮度适应性、人耳的相位感知缺陷都为信息隐藏的实现提供了可能的途径。

另一方面，信息论、密码学等相关学科又为数字水印技术提供了丰富的理论资源；多媒体数据压缩编码与扩频通信技术的发展为数字水印提供了必要的技术基础。

最有生命力的研究课题往往处在多学科交叉的位置上，数字水印就是这样一个涉及多个领域、涵盖多种技术的研究方向。

- 一、三个研究层次
- 二、理论模型与信量分析
- 三、典型算法
- 四、攻击与测试

# 一、三个研究层次

与其他技术类似，数字水印的研究也可以分为基础理论研究、应用基础研究和应用研究三个层次。

## 1、基础理论研究

数字水印基础研究的目的是建立数字水印的理论框架，解决水印信量分析、隐蔽性描述等基本理论问题。

数字水印源自古老的密写术。长久以来，密写技术由于缺乏理论依据，始终没有发展成为一门学科。但在认知科学和信号处理理论的基础上，充分借鉴密码学的成果，我们完全可以建立数字水印技术的理论框架，分析数据量与隐蔽性之间的关系，使得在给定需要保护的数据后，能有一套可靠的标准来选择水印方案，并能综合评判各种数字水印算法的优劣。

## 2、应用基础研究

应用基础研究的主要方向是针对图像、声音、视频等多媒体信号，研究相应的水印隐藏与解码算法，以及能抵御仿射变换、滤波、重采样、色彩抖动、有损压缩的鲁棒数字水印技术。

### 3、应用研究

应用研究以水印技术的实用化为目的，研究各种标准多媒体数据文件格式的水印算法。水印应用研究特别要面向Internet上广为使用的各种数据文件，包括JPEG压缩图像、MPEG2压缩视频、WAV、MIDI、MP3音频文件、AVI及三维动画文件、PS和PDF标准文本、voice mail或video mail等多媒体邮件格式。

另外，为了抢占先机，还必须注意研究针对尚未形成标准的多媒体数据文件的水印算法，如新一代视频压缩标准MPEG4、各种流媒体文件等。

票据防伪也是数字水印的一个重要应用领域，各种防伪票据水印的研究也不容忽视。

## 二、理论模型与信量分析

在信息论中，香农（Shannon）的信道公式与保密通信公式一直是通信科学发展的指南针，虽然信息论中的许多结论都是在大量假设的前提下得出的，其中一些假设与实际情况还相去甚远，但它们对通信技术发展的指导作用却是不可否认的。数字水印在应用中也要解决一些关键的理论问题，但至今还没有产生像香农公式那样能够指导学科发展的基本理论。

数字水印的信量分析要回答这样一个问题：“给定需要保护的数据文件和隐蔽性指标，可以加入多少隐藏的水印信息？”只有解决了这一问题，才能科学地设计水印标识的数据格式。

目前，通过对傅立叶变换域和DCT变换域系数的统计分布进行建模，并借助一些信号检测理论，学术界已经得出了一些典型数字水印算法的信量估计结果，但作为一个完整的理论描述，这些结果还缺乏说服力。

## 三、典型算法

数字水印技术横跨了信号处理、数字通信、密码学、模式识别等多种学科，各专业领域的研究者均有独特的研究角度，其算法可谓是五花八门，无所不用。主要的有以下几种：

## 1、最低有效位算法 (LSB)

最低有效位算法 (LSB) 是 L.F.Turner 和 R.G.van Schyndel 等人提出的第一个数字水印算法，是一种典型的空域信息隐藏算法。

LSB算法使用特定的密钥通过 $m$ 序列发生器产生随机信号，然后按一定的规则排列成2维水印信号，并逐一插入到原始图像相应像素值的最低几位。由于水印信号隐藏在最低位，相当于叠加了一个能量微弱的信号，因而在视觉和听觉上很难察觉。LSB水印的检测是通过待测图像与水印图像的相关运算和统计决策实现的。Stego Dos、White Noise Storm、STools等早期数字水印算法都采用了LSB算法。

LSB算法虽然可以隐藏较多的信息，但隐藏的信息可以被轻易移去，无法满足数字水印的鲁棒性要求，因此现在的数字水印软件已经很少采用LSB 算法了。不过，作为一种大数据量的信息隐藏方法，LSB在隐蔽通信中仍占据着相当重要的地位。

## 2、Patchwork算法

Patchwork是麻省理工学院媒体实验室Walter Bander等人提出的一种数字水印算法，主要用于打印票据的防伪。

Patchwork数字水印隐藏在特定图像区域的统计特性中，其鲁棒性很强，可以有效地抵御剪切、灰度校正、有损压缩等攻击，其缺陷是数据量较低，对仿射变换敏感，对多拷贝平均攻击的抵抗力较弱。

### 3、纹理块映射编码

纹理块映射将水印信息隐藏在图像的随机纹理区域中，利用纹理间的相似性掩盖水印信息。该算法对滤波、压缩和扭转等操作具有抵抗能力，但需要人工干预。

## 4、文本微调算法

文本微调算法用于在PS或PDF文档中隐藏数字水印，主要是通过轻微改变字符间距、行间距和字符特征等方法来嵌入水印。这种水印能抵御攻击，其安全性主要靠隐蔽性来保证。

## 5、DCT变换域数字水印算法

DCT变换域数字水印是目前研究最多的一种数字水印，它具有鲁棒性强、隐蔽性好的特点。其主要思想是在图像的DCT变换域上选择中低频系数叠加水印信息。之所以选择中、低频系数，是因为人眼的感觉主要集中在这一频段，攻击者在破坏水印的过程中，不可避免地会引起图像质量的严重下降，一般的图像处理过程也不会改变这部分数据。

由于JPEG、MPEG等压缩算法的核心是在DCT变换域上进行数据量化，所以通过巧妙地融合水印过程与量化过程，就可以使水印抵御有损压缩。此外，DCT变换域系数的统计分布有比较好的数学模型，可以从理论上估计水印的信息量。

## 6、直接序列扩频水印算法

扩频水印算法是扩频通信技术在数字水印中的应用。与传统的窄带调制通信方法不同，扩频通信将待传递的信息通过扩频码调制后散布于非常宽的频带中，使其具有伪随机特性。受信方通过相应的扩频码进行解扩，获得真正的传输信息。

扩频通信具有抗干扰性强、高度保密的特性，在军事上应用广泛。事实上，扩频通信也可以看作是一种无线电密写方法。抛开其信息论方面的理论依据不讲，单从感知的角度考虑，扩频通信之所以具有保密性，就在于它将信息伪装成信道噪声，使人无法分辨。

扩频水印方法与扩频通信类似，是将水印信息经扩频调制后叠加在原始数据上。从频域上看，水印信息散布于整个频谱，无法通过一般的滤波手段恢复。如果要攻击水印信息，则必须在所有频段上加入大幅度噪声，这无疑会严重损害原始数据的质量。

## 7、其他变换域数字水印算法

变换域数字水印并不局限于DCT变换域或傅立叶谱，只要能很好地隐藏水印信息，一切信号变换都是可行的。近年来，有很多学者尝试用小波变换或其他时/频分析的手段，在时间/尺度域或时/频域中隐藏数字水印信息，取得了比较好的效果。

## 四、攻击与测试

与密码学类似，数字水印也是一个对抗性的研究领域。正是因为有水印攻击的存在，才有水印研究的不断深入。另外，为了实现数字水印的标准化，必须对各种数字水印算法进行安全性测试。水印测试者既需要熟悉水印算法又要熟悉水印攻击算法，而且还要从水印算法的理论入手进行水印信息量和鲁棒性的定量分析。

# 1、水印攻击的分类

水印攻击与密码攻击一样，包括主动攻击和被动攻击。主动攻击的目的并不是破解数字水印，而是篡改或破坏水印，使合法用户也不能读取水印信息。而被动攻击则试图破解数字水印算法。相比之下，被动攻击的难度要大得多，但一旦成功，则所有经该水印算法加密的数据全都失去了安全性。

主动攻击的危害虽然不如被动攻击的危害大，但其攻击方法往往十分简单，易于广泛传播。无论是密码学还是数字水印，主动攻击都是一个令人头疼的问题。对于数字水印来说，绝大多数攻击属于主动攻击。

值得一提的是，主动攻击并不等于肆意破坏。以版权保护水印为例，如果将嵌入了水印的数字艺术品弄得面目全非，对攻击者也没有好处，因为遭受破坏的艺术品是无法销售的。对于票据防伪水印来说，过度损害数据的质量是没有意义的。真正的主动水印攻击应该是在不过多影响数据质量的前提下，除去数字水印。

密码攻击一般分为唯密文攻击(ciphertext only attack)、选择明文攻击(chosen plaintext attack)和已知明文攻击(known plaintext attack)。参照密码学的概念，可以定义水印攻击的几种情形。

## ■ 唯密写攻击(stego only attack)

唯密写攻击是指攻击者只得到了含有水印的数据，并不了解水印的内容，这是最常见的情形。

## ■ 已知掩蔽信息攻击(know cover attack)

已知掩蔽信息攻击是指攻击者不仅得到了含有水印的数据，而且还得到了不含有水印的原始数据，这显然是攻击者所希望的。

## ■ 已知水印攻击(known message attack)

有些攻击者为了破解水印，常常冒充合法使用者，得到一些已知水印内容的数据，然后分析水印隐藏的位置。这种攻击与密码学中的已知明文攻击非常相似。

## ■ 选择密写攻击(chosen stego attack)

如果攻击者得到了水印嵌入软件，就可以尝试在媒体数据中嵌入各种信息，从而构成选择密写攻击，这是一种最有希望破解数字水印算法的攻击。

## 2、典型的主动水印攻击方法

如前所述，破解数字水印算法十分困难，在实际应用中，水印主要面临的是主动攻击。

各种类型的数字水印算法都有自己的弱点，例如，时域扩频隐藏对同步性的要求严格，破坏其同步性（如数据内插），就可以使水印检测器失效。典型的主动水印攻击方法包括：

## ■ 多拷贝平均

对同一幅作品的多个发行版本进行数值平均，利用水印的随机性去除水印。

## ■ 各种线性滤波

针对频域水印算法，可以构造具有特定频率特性的线性滤波器，攻击频域上隐藏的水印信息。

## ■ 几何变形攻击

通过轻微的几何变形，可以破坏数据的同步性，同时也不过分影响数据质量，但却对许多直扩序列调制类的数字水印算法构成了威胁。

## ■ 非线性滤波

中值滤波或其他各种顺序统计滤波既可以改变信号的频域特性，又可以破坏同步性，是一种复合攻击。

## ■ 拼接攻击

拼接攻击是将含有水印的数字作品分割成若干小块，形成若干独立的文件，然后在网页上拼接起来。由于各种数字水印算法都有一定的解码空间，只靠少量的数据无法读取水印，所以很难抵御拼接攻击。

## ■ 二次或多次水印攻击

攻击者使用自己的算法在数字作品中加入水印，即使这种操作不能破坏真正的水印，也会造成水印标识的混乱，从而给司法鉴定带来困难。尤其是对于没有原始数据作证的盲水印系统，一般很难判断哪一个水印操作在前，哪一个在后。

### 3、 水印测试

为了最终确定水印的技术标准，信息安全测评机构必须对大量公开的水印算法进行测试。这种测试不仅要通过实验，而且还要进行理论分析，以免由于样本选择错误造成以偏概全。

面对大量而且烦琐的测试实验，数字水印自动测试系统的研究显得十分必要。剑桥大学开发的StirMark软件就是一个典型的数字水印测试系统，它集成了几十种水印攻击算法，可以比较全面地测试水印算法的鲁棒性。

对于一个有希望成为标准的数字水印，至少要测试这样几个方面：

## ■ 隐蔽性

数字水印的信息量与隐蔽性之间存在着矛盾，随着水印信息量的增加，作品的质量必然下降。隐蔽性测试需要对水印算法的信息量与能见度进行评估，给出水印信量与数据降质之间的准确关系。

对于图像、声音等多媒体数据质量的评估不能仅依据信噪比、峰值信噪比等信号处理中的指标，必须依赖视觉和听觉的生理模型，否则就不具有科学性，这不仅是数字水印也是数据压缩的基本准则之一。

## ■ 鲁棒性

鲁棒性测试实际上是一个主动攻击过程，主要测试数字水印对数据同步的依赖程度、抗各种线性和非线性滤波的能力，以及抵御几何变换等其他攻击的能力。

## ■ 安全性

安全性测试主要是对破解水印算法的时间及复杂性进行评估，以此作为水印安全性的指标。

数字水印技术从一开始就是一个多种技术相互综合的研究领域，来自通信、模式识别、信息安全等领域的研究人员各自从不同的研究角度进行探索，形成了百花齐放、百家争鸣的局面。作为一个新的研究领域，数字水印还有大量的理论和工程问题需要解决。相信随着研究工作的深入，数字水印会逐渐成熟，并最终形成一门颇具特色的独立技术学科。

# 第五节

## 信息隐藏与数据加密 的区别和联系

- 一、隐藏的对象不同
- 二、保护的有效范围不同
- 三、需要保护的时间长短不同
- 四、对数据失真的容许程度不同

# 一、隐藏的对象不同

加密是隐藏内容，而信息隐藏主要是隐藏信息的存在性。隐蔽通信比加密通信更安全，因为它隐藏了通信的发方、收方，以及通信过程的存在，不易引起怀疑。

## 二、保护的有效范围不同

传统的加密方法对内容的保护只局限在加密通信的信道中或其他加密状态下，一旦解密，则毫无保护可言；而信息隐藏不影响宿主数据的使用，只是在需要检测隐藏的那一部分数据时才进行检测，之后仍不影响其使用和隐藏信息的作用。

### 三、需要保护的时间长短不同

一般来说，用于版权保护的鲁棒水印要求有较长时间的保护效力。

## 四、对数据失真的容许程度不同

多媒体内容的版权保护和真实性认证往往需容忍一定程度的失真，而加密后的数据不容许一个比特的改变，否则无法脱密。

由于加密在通信中的缺陷以及对多媒体内容保护能力的局限，才导致了信息隐藏技术的发展，其中的数字水印技术甚至被认为是多媒体内容保护的最后一道防线。但是，密码学中的很多思想可以借鉴到数据隐藏中来（如数字水印系统的安全性应建立在密钥的基础上，不能通过对算法保密来得到安全性），而且信息隐藏（如数字水印）的应用系统往往要借助密码体制才能实现。

## 第六节

# 数字水印算法的特点

- 一、水印要直接嵌入数据中
- 二、不易觉察或不易被注意到  
(或称为"透明性")
- 三、鲁棒性
- 四、安全性
- 五、提取水印不需要原始数据
- 六、计算复杂度
- 七、比特率

# 一、水印要直接嵌入数据中

水印要直接嵌入数据中而不是将水印放在数据文件的头部或尾部等位置。

## 二、不易觉察或不易被注意到（或称为“透明性”）

不影响原数据的使用价值，如：  
不影响图像的视觉效果、真实性，  
不容易被人的知觉系统觉察，或不易引起人的注意。

### 三、鲁棒性

不同的应用对鲁棒性要求不一样，一般都应能抵抗正常的图像处理，如：滤波、直方图均衡等。用于版权保护的鲁棒水印需要最强的鲁棒性，需要抵抗恶意攻击，而易损水印、注释水印不需抵抗恶意攻击。

## 四、安全性

一个水印体制要走向商业应用，其算法必须公开。算法的安全性完全取决于密钥，而不是对算法进行保密以取得安全性。所以，密钥空间需足够大，而且分布比较均匀。另外，鲁棒水印需要能抵抗各种恶意攻击，易损水印要能抵抗“伪认证”攻击。

## 五、提取水印不需要原始数据

很多应用场合无法确定原始数据（如：在互联网上搜索很多图像的非法拷贝），或者根本没有原始数据（如：可用于数码相机的易损水印）。但也有一些场合可以利用原始数据，以提高提取水印的准确性。

## 六、计算复杂度

不同应用对水印嵌入算法和提取算法的计算复杂度有不同的要求。如指纹水印要求嵌入算法速度要快，而对检测算法则不需要很快；其它的水印一般对嵌入的速度要求不高，但对检测的速度要求很快。

## 七、比特率

不同应用对嵌入水印的比特率有不同的要求。一般来说，注释水印要求有较高的嵌入比特率，鲁棒水印次之，而易损水印在这方面的要求不是重点。

# 第七节

## 数字水印与 版权保护

中国古代印刷术的发明第一次使数字作品的大规模复制成为可能，印刷技术在世界范围内的广泛传播最终导致了现代版权制度的建立。综观版权制度发展的历史，我们可以发现，版权制度与传播技术之间总是存在着微妙的互动关系。一方面，传播技术的革命和传播方式的进步始终是推动版权制度不断发展的重要力量；另一方面，版权制度又对保护和促进传播技术的推广与发展起着不可估量的作用。

一个世纪以来，无线电广播、电视、录像等新技术的产生都曾在一定程度上造成过版权保护的困难，但最终都被版权制度所吸收和规范。近年来，数字化技术和Internet的飞速发展，在最大限度地拓宽权利人利益范围的同时，也带来了版权的危机。数字化技术精确、廉价、大规模的复制功能和Internet的全球传播能力都给现有版权制度带来了前所未有的冲击，数字作品的版权保护成为困扰各国政府、法律界、艺术界和计算机科学家的难题。

- 一、数字技术与Internet的挑战
- 二、基于数字水印的版权保护
- 三、面向攻击的解决方案
- 四、标准化

# 一、数字技术与Internet的挑战

现代版权制度最突出的特点之一是出现了专门的版权保护技术。在版权保护方面，法律与技术之间存在着密切的互补关系，当法律的威慑力不足以制止侵权行为时，技术手段就用来弥补法律的不足。

随着多媒体技术特别是声像数据压缩技术的发展，CD音乐、VCD/DVD影碟、电脑动画等数字化产品走进了人们的生活，Internet的迅猛发展更为数字作品的广泛传播创造了条件。相对于其他版权保护对象而言，数字作品有一系列突出特点，这些特点使得它很难得到现有版权制度的保护。

# 1、低廉的复制代价

绘画、雕塑、书法等传统艺术品的复制是一项专业性很强的技术，以至于一些赝品本身也具有相当高的艺术价值。但对于数字作品来说，即使是大批量复制，也不过是举手之劳。一幅辛辛苦苦创作出来的电脑绘画作品，只要成为网页的一部分，在短时间内就会产生成千上万份拷贝，以至于无法分清谁是创作者，谁是复制者。廉价的复制不仅导致了盗版的猖獗，也给追查侵权行为造成了困难。

## 2、司法鉴定的困难

针对纸质文书和传统艺术品的真伪辨别，目前的司法鉴定技术有一套完整的解决方案，如纸张鉴定、笔迹鉴定等。而对于数字作品来说，原作与复制品百分之百相同，在理论上就不存在鉴别的可能。

虽然文件本身还会携带诸如修改时间、所有者姓名、读写密码等附加信息，但这些信息很容易被篡改，只能构成一种脆弱的保护。原创者不仅可能“有理讲不清”，而且可能反遭诬告。因此，数字作品侵权的取证工作已经成为知识产权执法过程中的一个棘手问题。

### 3、篡改方便

对传统艺术品来说，篡改或引用是非常困难的，很难想像谁能够将达芬奇的油画剪切一部分贴到自己的作品中。然而，数字作品几乎允许一切可能形式的编辑，这就使原作品的完整性受到严重威胁，同时也模糊了侵权使用与合理使用之间的界线。

## 4、网页保护的难题

电子商务的兴起使Internet成为企业的生命线，网页的保护十分重要。除了作为企业的网上门户之外，网页本身还凝结着设计者的智慧和劳动，这种智慧和劳动直接关系到企业的经济利益。

因此，网页的保护既是知识产权保护又是商业利润保护，它必然包含两方面的内容：一是防篡改，二是防盗用。目前的网络安全技术还缺乏对于网页篡改的自动侦测机制，加之一些网站疏于管理，往往一个网页被黑客篡改了数小时后才被发现，严重损害了企业的经济利益和企业形象。对于网页资源的盗用，目前也没有很好的解决方案。1999年国内几起重大网页侵权案的顺利裁定，与其说是侵权取证技术的胜利，不如说是原告的企业声誉起了主要作用。

## 二、基于数字水印的版权保护

数字水印技术之所以在近几年中以惊人的速度发展，除了军事、安全方面的原因外，最主要的原动力就是数字作品版权保护的需要。为了解决日趋复杂的版权纠纷问题，现代版权法中出现了所谓“技术措施”和“权利管理信息”两个新概念。

技术措施和权利管理信息是版权人采取的权利保护及标示措施，这两个新概念出现在版权法中，是版权保护制度在新技术条件下的发展。数字水印不仅可以作为版权保护的技术措施，而且还提供了对版权管理信息及我国特有的“行政管理信息”的全面支持。

# 1、篡改提示与完整性保护

"脆弱水印"作为数字水印的一个重要研究分枝，可以用于保护数字作品的完整性。脆弱水印是由数字作品的原始数据通过一个散列函数得到的，隐藏在公开发表的数字作品中。图像、声音、视频等数字化媒体一旦遭到篡改攻击，哪怕是很小的改动，都会破坏脆弱数字水印。完整性检测程序通过读取数字作品中的水印就可以判断数据是否已经被篡改。

对于网页保护来说，可以定时检测隐藏在网页中的数字水印，如果遭受攻击，系统就能及时报警或自动修复。

## 2、充当权利管理信息

权利管理信息是指作品上标示的权利人姓名、创作时间等信息，主要用于保护版权人的经济利益。版权法对权利管理信息的保护客观上起到了保护署名权的作用。

在数字作品上直接标示权利管理信息会明显损害作品的质量，而利用文件的附加信息标示版权又很不安全。相比之下，在不过多损害作品质量的前提下，使用数字水印技术将权利管理信息秘密嵌入数据中，是一个非常理想的解决方案。

首先，数字水印是不可见或不可听的，因而对消费者的利益不构成侵害；其次，数字水印具有几乎不可破译性，偷换水印的难度非常大，权利管理信息非常安全。此外，随着数字水印技术研究的深入，数字水印抗各种信号变形的能力越来越强，若想通过主动攻击去除权利管理信息，则不得不以严重损害作品的质量为代价，从而难以对权利人的经济利益构成威胁。

### 3、“行政管理信息”与数字水印

对我国的法律制度来说，权利管理信息还是新概念，但我国现有的“行政管理信息”可以在一段时间内和一定程度上起到保护署名权的作用。与权利管理信息不同，行政管理信息的标注不是著作者完成的，而是一种国家行为。早在1995年，我国就规定国内激光数码存储盘片的复制生产单位必须在其生产模具上刻蚀“来源识别码”，即SID码。

与权利管理信息相同，数字水印也是对数字作品标识行政管理信息的理想技术途径。

### 三、面向攻击的解决方案

与密码技术类似，数字水印在实际应用中必然会遭到各种各样的攻击。盗版带来的巨大利润与对新技术的好奇都会成为攻击版权保护水印的动机。目前在数字水印的研究中，难以解决的是以下几种攻击：

# 1、二次水印攻击

真正安全的数字水印技术应该是公开算法的，其安全性仅依赖于产生水印的密钥。但公开算法也会导致技术的失控，并不是所有的人都有能力破解别人的水印，但每一个能读懂水印算法的人都可以在已经隐藏了水印的数字作品中加入自己的水印，从而导致权利管理信息标示的混乱。解决二次水印问题需要综合运用多种数字水印技术，这一直是数字水印技术研究的焦点之一。

## 2、拼接攻击

网页资源的盗用者可以将盗取的数字图像或声音分割成若干小文件，而后在网页上拼接起来，这样并不影响视觉和听觉效果，但却对大多数数字水印算法构成了威胁。

抗拼接攻击的数字水印在编码时一定存在冗余数据，而冗余数据过多又会影响水印的信息量。如何解决这一矛盾，也是研究者需要考虑的。

### 3、多图平均攻击

如果攻击者通过合法途径得到了含有水印的同一数字作品的多个拷贝，则他可以对这些复制品进行平均操作，利用水印的随机性去除水印。

解决多图平均攻击的途径是采用“基于内容”的数字水印，使数字水印与媒体数据有一定程度的相关，这种与内容相关的隐藏信息可以抗多图平均攻击。

## 四、标准化

作为一项关系司法认证的技术，尤其是作为标示行政管理信息的手段，数字水印的标准化工作十分重要。从市场经济的角度看，水印技术标准化还意味着相应产品的垄断，谁的技术成为法律认可的标准，谁就理所当然地享有巨大的市场份额。正因如此，IBM、NEC等信息产业巨头一直在积极参与有关版权保护水印技术标准的制定工作。

1998年，美国版权保护技术组织（CPTWVG）成立了数据隐藏小组（DHSG），着手制定版权保护水印的技术标准。在来自各大公司的7份技术方案中，DHSG确定了其中三个作为候选标准。这三个方案是：

- IBM与NEC共同制定的技术方案；
- Macrovision、Digimarc和Philips联合制定的方案；
- Hitachi、Pioneer和Sony共同制定的方案。

虽然DHSNG进行了大量的技术调研，但它并没有制定技术标准的权利，最终决定数字水印标准的是美国版权保护顾问委员会（CPAC）。IBM、HP、Apple、Microsoft、Intel、Zoran、ATI Tech.、Mediamatics 和 STMicroelectronics 等多家知名企业都是该委员会的会员。

另外，设在伦敦的国际摄影行业联盟（IFPI）和数字视听委员会（DAVIC）也开始了数字水印标准的制定。

尽管至今还没有形成数字水印的最终技术标准，但DHSG已经明确了用于版权保护的数字水印必须满足的一些基本条件，包括：

- 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“未曾复制”、“只可复制一次”和“不能再复制”等复制信息；
- 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；
- 必须使用成熟的技术嵌入或检测水印。

在我国，知识产权问题是一个敏感的话题，只有深入开展数字水印技术的研究，尽快制定我国的版权保护水印标准，才能使我们在未来可能的国际知识产权纠纷中取得主动权。

# 第八节

## 数字水印与数字作品 的电子交易

伴随着Internet的飞速发展，电子商务异军突起，成为时代的潮流。然而，在由传统商务向电子商务转化的过程中，配送体系一直是一个难以克服的瓶颈，即使是亚马逊这样的网上书店，从订购到收到一本图书往往也要几周的时间。

事实上，许多数字化产品完全可以通过Internet直接交易，从而回避配送问题。对于数字化的书籍、杂志和声像作品，Internet具有其他发行渠道所无法比拟的优势。仅以图书为例，纸质图书的发行很难实现全球化，而且纸质图书无法拆分，读者为了得到其中的部分章节，不得不付出整本书的代价。

数字作品的电子化发行省去了印刷、包装、库存、邮寄等许多环节，允许用户购买作品的指定片段，不仅大幅度降低了成本，拓宽了发行渠道，而且给用户以更大的选择空间。数字作品电子交易系统是实现这一目标的手段。

一、系统设计原则

二、对数字水印技术的要求

三、商业模式--IMPRIMATUR

# 一、系统设计原则

从消费者的角度考虑，数字作品电子交易系统首先应该是易于使用的。其次要有丰富的功能，除了传统意义上的买卖功能外，还应该支持诸如定制、转让等服务。

从技术上讲，这个系统至少要包含如下组成部分：

## ■ 数据压缩引擎

经营数字作品面临的第一个问题就是数据压缩。对于一个具有相当规模的网络音像商店来说，数据压缩算法直接关系到存储成本和作品质量。无论是为了保证作品的质量而牺牲存储空间，还是为了降低存储成本而牺牲作品质量，都不是最明智的作法。为了适应用户的多层次需要，数据压缩引擎应当采用可控质量的压缩算法。

## ■ 完整性保护

为了保证存储的数字作品不被破坏，必须建立一个由脆弱水印及密码方法共同构建的完整性保护机构。

## ■ 安全的支付系统

## ■ 版权标识机制

版权标识是数字作品电子交易系统的核心，数字水印是版权标识的主要技术手段，与之相配合的是著作者标识管理系统和作品标识管理系统，相当于传统发行系统中的ISBN体制。

## 二、对数字水印技术的要求

数字作品电子交易系统中的数字水印技术必须和数据压缩算法配合使用，最基本的要求是数据压缩不能破坏数字水印。

与一切商业系统类似，数字作品电子交易系统处在复杂的网络环境中，面临各种可能的攻击，因此数字水印必须具有足够的抗攻击能力。比如，为了抗拼接攻击，水印的长度不能太长，要有相当程度的冗余。此外，为了适应在线服务的需求，水印解读的速度要快，水印嵌入的算法也不能太复杂。

可行的数字水印方案有以下三种：

## ■ 在原始数据中嵌入水印

在原始数据中嵌入数字水印的优势在于可以使用各种标准的文件格式和大量的数字水印研究成果，因为大多数研究性的数字水印算法都与文件格式无关。然而，这种方式的缺点也很明显，系统的设计者必须在水印算法与压缩算法之间权衡。

## ■ 在压缩数据流中嵌入水印

这是另一种极端的解决方案，它与媒体信号的类型无关，数字水印的嵌入不会影响信号的内容，也不会影响传输速率。但这种算法不可能很复杂，因此也容易被破解，另外它不能抗D/A转换等信号处理过程的攻击。

## ■ 与数据压缩算法相结合

从理论上讲，将数字水印与数据压缩融合在一起是最佳的解决方案，对于JPEG和MPEG压缩来说，这一方案很容易实现。JPEG与MPGE算法都包含了DCT变换和变换系数量化过程，压缩的质量很大程度上取决于量化，而目前很多数字水印算法也是在DCT变换系数上隐藏信息。所以，只要在变换系数量化的同时考虑数据压缩与数字水印两方面的需求，就可以将压缩过程与水印过程合二为一。

### 三、商业模式--IMPRIMATUR

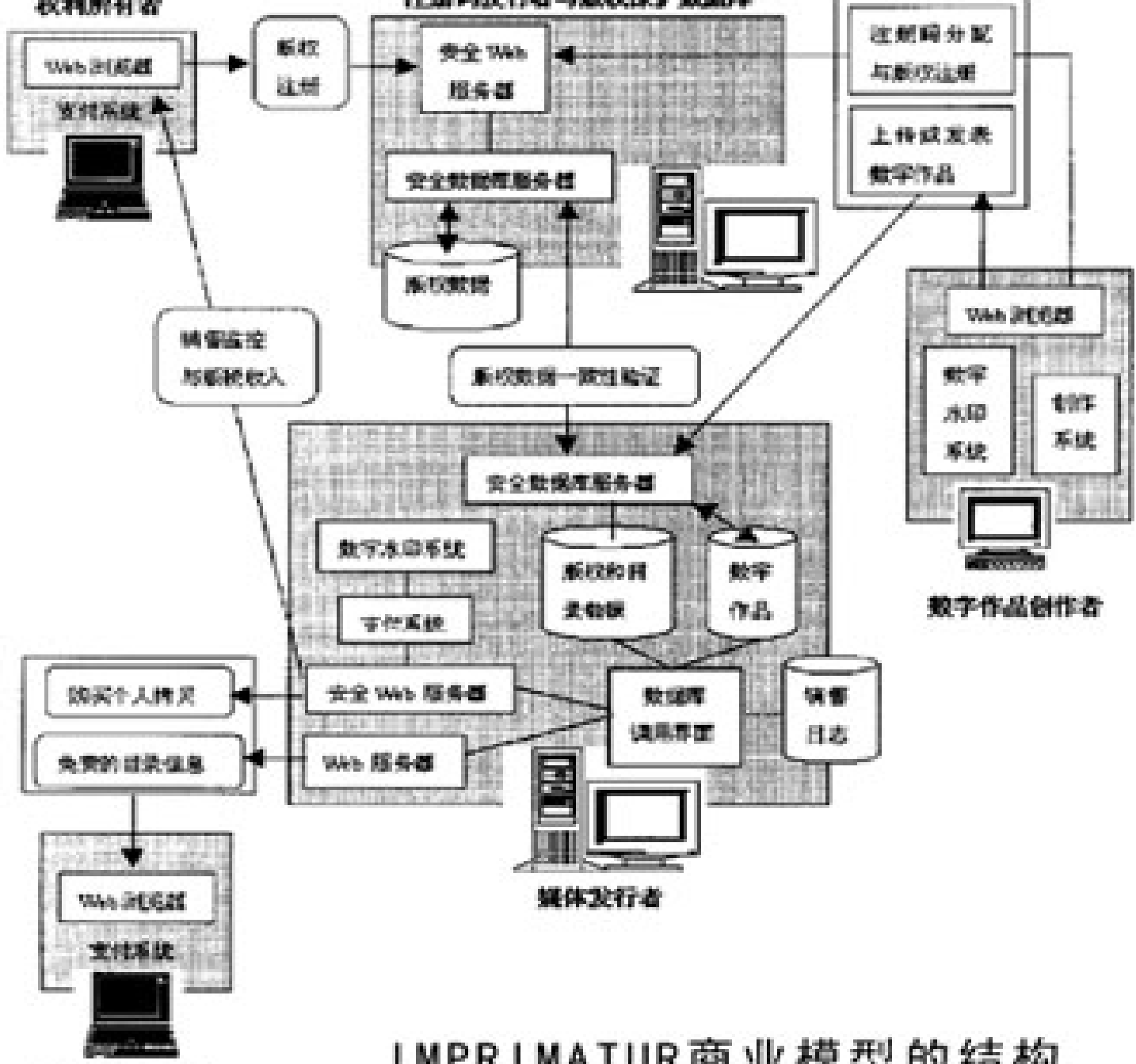
IMPRIMATUR是欧盟委员会的一个研究项目，主要研究电子商务中的知识产权保护方案，其目标是使欧盟成员国在数字作品电子交易方面达成协议。

IMPRIMATUR提出了所谓“版权敏感作品”网上交易的商业模式，同时开发了一个电子版权管理系统（ECMS）。

# 1、IMPRIMATUR商业模式

所谓商业模式，就是要定义交易过程中的基本角色和核心剧情。对于数字作品电子交易系统来说，基本的角色包括作品提供者、媒体发行人、作品购买者和知识产权持有者。

数字作品的创作者将作品交给作品提供者进行包装和出版，作品提供者成为知识产权的持有者；媒体发行者从作品提供者那里购买数字作品，存储于服务器中，通过WWW服务器进行广告宣传；购买者使用电子支付系统在线购买数字作品；版权持有者通过媒体发行者的服务器监控其作品的销售情况，并取得版税收入。这就是IMPRIMATUR商业模式的核心剧情（如图所示）。



IMPRIMATUR商业模型的结构

## 2、电子版权管理系统

电子版权管理系统是IMPRIMATUR的核心，也是该模型要验证的主要部分。

### ■ 传输安全与认证

在实际应用中，数字作品电子交易系统面临着各种攻击和欺骗，所以对电子版权管理系统的第一要求是可靠，此外还要提供与数字作品创作者之间的交互认证界面。

除了版权敏感信息之外，电子版权管理系统还要安全地传输其他重要数据。比如，为了计算版税，创作者需要得到反映数字作品销售情况的统计数字。为了保护消费者的利益，带有版权信息的媒体数据在网络上传输时也需要安全保护。

为了满足传输安全的需要，IMPRIMATUR采用了标准的 SSL安全协议，它既满足了客户端应用程序的开放性要求，又实现了基于公钥体制的客户 / 服务器认证和传输数据加密。目前，大多数网络浏览器都支持SSL协议和公钥体制，因此在应用中不会给用户带来麻烦。

## ■ 唯一标识

为了明确数字作品交易系统中的各种权益关系，电子版权管理系统提供了一个类似于ISBN体制的注册码发行机构。IMPRIMATUR共有三种唯一的标识信息，分别是著作者标识、版权所有者和发行者标识。

## ■ 数字水印系统

虽然IMPRIMATUR不能防止非法复制，但其中的数字水印系统可以提供对复制品的探测追踪。在数字作品转让之前，作品创作者可以嵌入自己的创作标志水印；作品转让后，媒体发行者对存储在服务器中的作品进行水印处理，加入发行者标记；在出售作品的一个拷贝时，媒体发行者在其中还要加入销售标记。

为了包容各种数字媒体，IMPRIMATUR开发了一系列水印模型，包括数字图像、音频、视频等。即使这样，也很难适应多媒体技术的快速发展，因此IMPRIMATUR还提供了对第三方数字水印插件的支持。

数字作品的电子交易系统还处于发展阶段，IMPRIMATUR也仅仅是一种研究性的模型。未来各种文化类电子商务系统的结构会是千差万别的，但无论数字作品电子交易系统的结构怎样，数字水印的作用是不会改变的，其地位也是其他技术无法取代的。

# 第九节

## 基于数字水印技术的 票据防伪

金融安全是国家安全的重要组成部分，无论对于传统商务还是电子商务，各种纸质票据和电子票据防伪的重要性都是不言而喻的。伴随着高质量、廉价复制设备的出现和电子商务的兴起，票据防伪技术也在不断地发展，数字水印将在其中扮演重要的角色。

一、彩色复印机带来的挑战

二、打印图像的隐蔽标识与打印机追踪

三、电子商务中的票据防伪

# 一、彩色复印机带来的挑战

1970年第一台商用彩色复印机的诞生带来了一个棘手的问题：重要票据的伪造不再需要特殊设备和专业化技术，每一位彩色复印机的使用者都成为潜在的票据伪造者。为了防止用彩色复印机伪造票据，许多国家都将重要票据印刷得非常精致，使复印件发生混频失真。此外，还使用了塑性条纹、变色墨水等特殊防伪技术。

除了对票据本身采取各种防伪措施之外，以美国财政部为代表的一些政府机构认为在彩色复印机中加入一定的防伪功能也是一条解决问题的途径。

这种观点导致了两种基本解决方案：其一是立足于“防范在先”，即通过复印机中的票据识别电路来监测复印文件，以期做到在伪造票据时复印机能自动拒绝工作，这种方案需要实时快速的模式识别技术，在当时还难以实现；其二是由美国众议院货币政策委员会主席Michael Castle提出的“事后追踪”方案，即在彩色复印机的每幅输出图像中嵌入唯一的、不可见的标识信息，以便于追踪。后者相对于当时的技术水平来说，更加现实一些。

如果说彩色复印机的出现只是带来了一定程度的恐慌的话，那么，近年来高精度的廉价扫描仪和彩色打印机所带来的麻烦就非同小可了。根据美国财政部的报告，1997年在美国收缴的伪币中，有19%来自彩色打印机，1998年的数字是43%，而1995年这一数字还仅仅是2.36%。目前，小面额货币和大多数常用票据都缺乏水印等复杂工艺的保护，而廉价的扫描仪和打印机却使得伪造者能够承担伪造的费用，并且有利可图。

为了解决打印票据的防伪问题，以麻省理工学院媒体实验室、IBM公司等为代表的一些研究机构在美国财政部的支持下开展了基于数字水印技术的扫描/打印票据防伪研究，这些研究的思路基本上源于彩色复印机票据防伪的两个解决方案。

## 二、打印图像的隐蔽标识与打印机追踪

为了在需要的时候能够追踪伪造票据的打印机，可以在打印机输出图像中嵌入能够标识打印机的序列号，作为伪造追踪的线索。

为了实现这一目标，MIT媒体实验室的W.Bender教授提出了Patchwork Patch Track方法。Patchwork 是防伪水印的嵌入过程，它集成在打印机驱动程序中。Patch Track是相应的解读过程(见图1)。

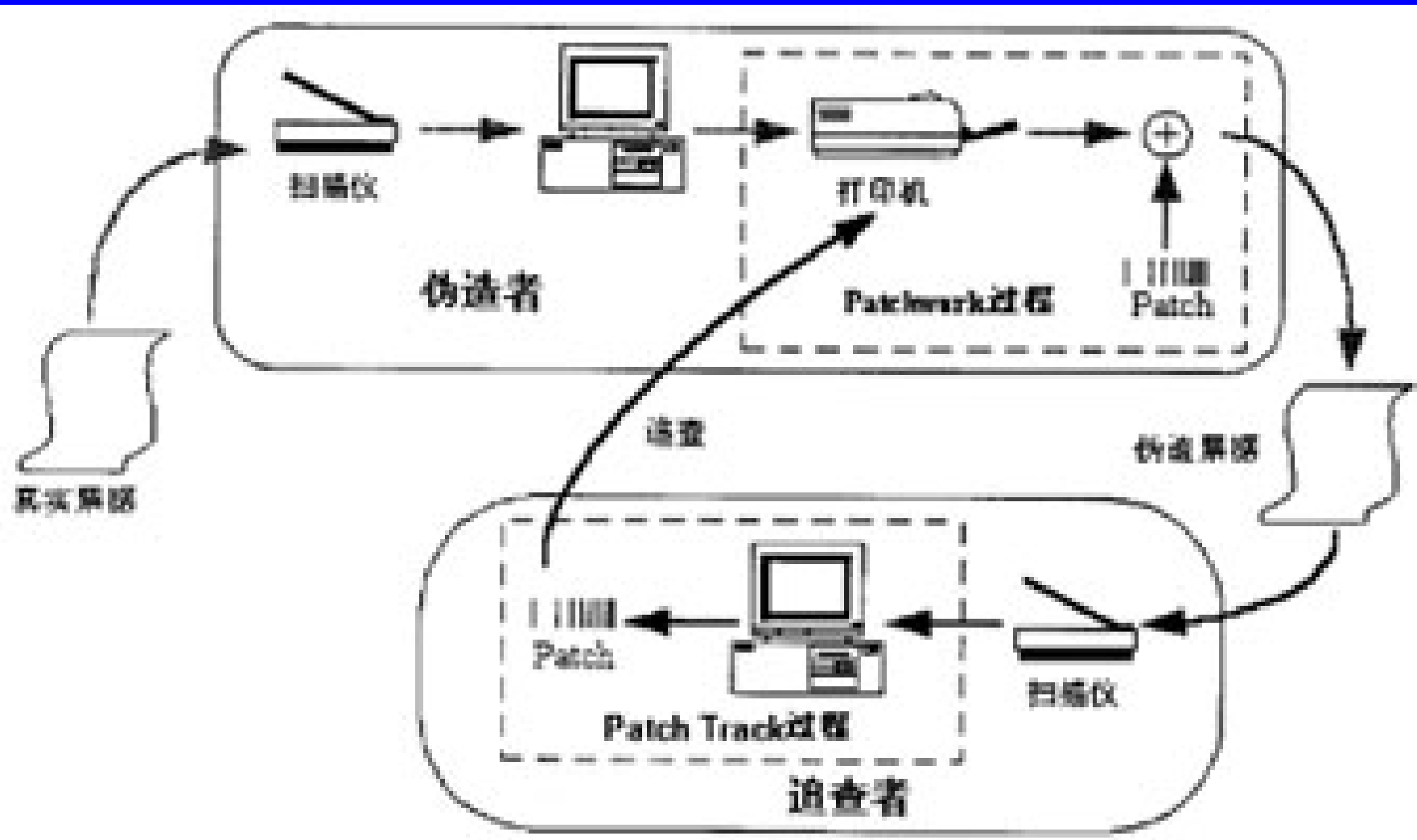


图1 Patchwork-Patch Track打印票据防伪方法

Patchwork算法嵌入的是一种数据量较小、能见度很低、鲁棒性很强的数字水印，能够抗图像剪裁、模糊化和色彩抖动。"Patchwork"一词原指一种用各种颜色和形状的碎布片拼接而成的布料，它形象地说明了该算法的核心思想，即在图像域上通过大量的模式冗余来实现鲁棒数字水印。与大多数图像域数字水印算法不同，Patchwork并不是将水印隐藏在图像数据的最低有效位（LSB）中，而是隐藏在图像数据的统计特性中。

以隐藏1bit数据为例，Patchwork算法首先通过密钥产生两个随机数据序列，分别按图像的尺寸进行缩放，成为随机点坐标序列。然后将其中一个坐标序列对应的像素亮度值降低，同时升高另一坐标序列对应的像素亮度。由于亮度变化的幅度很小，而且随机散布，并不集中，所以不会明显影响图像质量。为了提高鲁棒性，还可以改变随机点邻域中的像素亮度，这样就形成了图像域上亮、暗模式（即所谓Patch）的铺砌。

影响Patchwork算法使用效果的因素很多，主要有：

### ■ Patch的深度

Patch的深度是指对随机点邻域灰度值改变的幅度，深度越大，水印的鲁棒性越强，但同时也会影响隐蔽性，提高能见度。

## ■ Patch的尺寸

大尺寸的Patch可以更好地抗旋转、位移等操作，但尺寸的增大必然会引起水印信息量的减少，造成Patch相互重叠。具体应用时必须要在Patch的尺寸和数量两者之间进行折衷。

## ■ Patch的轮廓

具有陡峭边缘的Patch会增加图像的高频能量，虽然这有利于水印的隐藏，但也使水印容易被有损压缩所破坏。相反，具有平滑边缘的Patch可以很好地抗有损压缩，但易于引起视觉注意。合理的解决方案应该是在考虑到可能会遭受的攻击后确定，如果面临有损压缩的攻击，则应采用具有平滑边缘的Patch，使水印能量集中于低频；反之，如果面临对比度调整的攻击，则应采用具有陡峭边缘的Patch，使水印能量集中于高频。如果对所面临的攻击没有准确的估计，则应使水印的能量散布于整个频谱。

## ■ Patch的排列

Patch的排列应尽量不要形成明显的边界，因为人眼对灰度边界十分敏感，W.Bender建议采用随机的六角形排列。

## ■ Patch的数量

Patch的数量越多，解码越可靠，但这同时也会牺牲图像的质量。

除了这些因素之外，还可以在Patchwork水印算法中融合许多图像滤波技术，如采用视觉掩模技术等，来提高水印的隐蔽性或鲁棒性。

水印解码程序Patch Track实际上是一个统计信号检测器。Patch Track首先对扫描后的票据图像进行矫正处理，克服由旋转、破损等带来的水印特性变化。随后，Patch Track使用解密密钥产生二维随机点坐标序列，形成解码窗口。通过构造适当的像素灰度统计量，可以判断解码窗口中是否包含有Patchwork水印。数字隐线与快速水印解码。

为了实现打印机的自动票据识别与票据拒打功能，麻省理工学院数据隐藏研究小组提出了线状数字水印——数字隐线（Tartan Thread）技术。与隐蔽标识方法不同，Tartan Thread是一种主动防护技术，它必须与票据制作者配合，在真实的票据图案中加入防伪水印，这种线状的数字水印能够存在于扫描后的票据图像中，在打印输出时，打印机驱动程序中的水印解码模块能快速解读水印，一旦发现票据防伪隐线，就立即拒绝打印输出。

数字隐线防伪方案面临的最大难点是解码空间的问题。一般来说，打印机驱动程序只缓存几行像素，在打印过程中，内存中自始至终没有一个完整的打印图像，所以数字隐线的解码空间十分狭小。另外，数字隐线的解读过程必须非常迅速，如果过多地影响打印效率，则无论是打印机厂商还是用户都难以接受。

Tartan Thread数字隐线的核心技术是一维扩频调制，即将水印信息用扩频码调制成具有噪声性质的信号，叠加在票据图像上。解码器使用同样的扩频码通过解扩读取数字隐线。图2描述了Tartan Thread水印算法的基本过程。

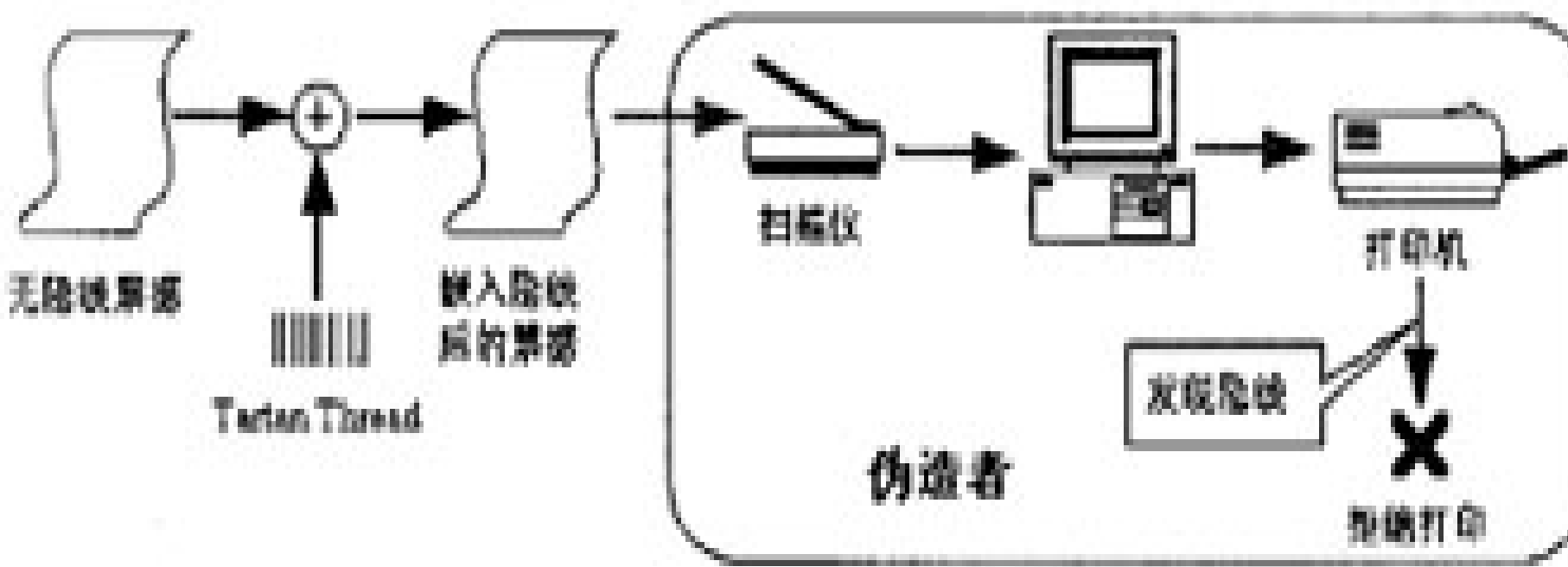


图2 Tartan Thread打印票据防伪方法

### 三、电子商务中的票据防伪

无论是传统商务还是电子商务，买卖双方都需要一定的票据作为交易的凭证，报价单、还盘单、定货单等电子票据在电子商务中占据着重要地位。因此，电子票据的防伪问题不仅直接关系到商家和消费者的利益，也关系到整个国家的经济秩序，是一个不容忽视的问题。

目前使用最多的电子票据文件是 Adobe 公司首创的 PS 和 PDF 文件，它集成了文本、图像等多种媒体格式，可以做到与平台无关。在 20 世纪 90 年代初期，Brassil 等人就开始研究用于 PS 文件的隐蔽标识方法，即所谓“文档结构微调算法”。数字标识信息经过编码转换为一系列对文档结构的轻微调整动作，包括垂直移动行距、水平调整字距和调整字体等。这种算法可以抵抗照相和扫描复制等一些标准的文件操作。

PS/PDF文件格式的多媒体性质决定了电子票据的防伪水印必定是多种水印技术的综合，包括图像水印、文本水印等。随着电子商务的飞速发展和数字水印技术研究的不断深入，PS/PDF文档水印的研究将越来越引起广泛的重视。

# 第十节

## 数字水印软件的 现状及发展

数字水印技术的研究虽然只有短短几年时间，但其软件产业已经有相当的规模。早在1995年，数字水印技术的研究还刚刚开始不久，美国的Digimarc公司就率先推出了世界上第一个商用数字水印软件，而后又以插件形式将该软件集成到Adobe Photoshop 4.0和Corel Draw7.0中。数字水印技术的商品化速度如此之快，从一个侧面反映出其迫切的市场需求。

- 一、市场前景
- 二、软件分类
- 三、发展趋势

# 一、市场前景

数字化技术和Internet的发展正改变着文化传播的载体和方式，数字图书馆、网上发行等新概念层出不穷，MIDI、CD、VCD、DVD、MP3 等数字化产品让人目不暇接。仅靠密码技术是不能完成多媒体数据的加密、认证和保护的，数字水印技术在数据安全中占有不可替代的地位。

与军事、金融领域不同，数字视听产品是公开销售的，经销商们关心的是盗版而不是盗用。版权就意味着利益，版权标识也因此而成为数字水印软件的最大市场。仅以DVD为例，参与研究其版权保护水印的就有包括IBM、NEC、Sony在内的数十家IT企业。

网络安全是近年来的热门话题，保护网页不被篡改的水印产品已经开始崭露头角，并且毫无疑问地将成为数字水印软件新的增长点。

先进的技术往往首先应用于军事和国家  
安全领域，数字水印技术也不例外。美国  
陆军实验室是最早进行数字水印研究的机  
构之一，各种军用影像数据的隐蔽标识与  
篡改提示是已经公开了的数字水印应用研  
究项目。作为数字时代的密写技术，用于  
隐蔽通信的大数据量信息隐藏技术也已引  
起各国情报部门的注意。数字水印一旦成  
为国防建设的急需，就会带来巨大的商业  
利润。除此之外，数字水印正在成为数字  
作品创作者的宠儿，其作为个人消费软件  
的潜在市场也是不容忽视的。

## 二、软件分类

从技术上讲，目前的数字水印软件可以分成两类：时（空）域水印软件和变换域水印软件。

### 1. 时（空）域数字水印软件

所谓时（空）域数字水印是指将通过密钥产生的随机序列直接加入声音、图像或视频信号中作为水印。由于嵌入信号的能量很低，所以不会被人的视觉和听觉所察觉。

常用的时（空）域数字水印技术有LSB和扩展频谱两种。LSB方法是将水印直接嵌入到原始信号表示数据的最低有效位中，是一种早期的数字水印技术。很显然，LSB方法对于要加入水印的信号是有一定要求的。以图像为例，如果原图的调色板不连续，则LSB方法会导致明显的色彩失真。

所以，这类软件一般都建议用户使用具有连续调色板的灰度或真彩色图像。对于索引色图像，一般要变换到真彩色空间中去隐藏水印，因此要求原图的颜色种类不要太多，否则从真彩色空间变换回索引色时会丢失水印信息。

时空域上的扩频隐藏方法是通过扩频码将水印信息调制成类似噪声的信号，这种信号的能量散布在整个频带上，难以通过频域滤波恢复。这种方法实际上就是扩谱通信系统的软件实现。

时空域数字水印技术的优点是隐藏的数据量大，而且可以根据信号的局部特性进行自适应。其缺点是太脆弱，常用的信号处理过程，如信号的缩放、剪切等，都可以破坏水印。此外，这类软件与具体的文件格式相关，经过这类软件处理的声像文件不能进行有损压缩。

## 2.变换域数字水印软件

变换域水印软件首先将原始的图像或声音信号进行DCT 或小波变换，在变换域上嵌入水印信息，然后经反变换输出。在检测水印时，也要首先对信号作相应的数学变换，然后通过相关运算检测水印。

DCT变换域上的数字水印具有很强的鲁棒性，可以抗各种信号变形。由于JPEG、MPEG等数据压缩方法也是在DCT变换域上操作的，所以DCT变换域数字水印具有与生俱来的抗有损压缩能力。不过，DCT变换域水印方法不能作到对图像、声音等信号内容的自适应，因此往往会造成对图像亮度等特征的明显损害。

小波变换域上的数字水印方法兼具时空域方法和DCT变换域方法的优点，是一种既有自适应功能，又有鲁棒性的技术，其缺点是计算量大。

## 三、发展趋势

数字水印软件的发展速度非常快，起初仅仅作为图像处理软件的插件，而今已经开始向大型商业化软件发展，呈现出面向Internet、多种技术集成的发展趋势，主要发展方向体现在以下几方面：

- ❑ 结合智能体技术，开发水印Agent和自动追踪版权标志。
- ❑ 面向电子商务，提供服务器端的完整性保护和客户端的数据认证。
- ❑ 建立水印认证中心，提供各种网上服务。
- ❑ 开发基于数字水印技术的数字作品电子销售系统，提供完整的安全与版权保护机制。

- ❑ 为各种付费点播服务，提供基于流技术的数字水印产品。
- ❑ 面向更广泛的数字媒体，如三维动画、数字地图等，开发基于数字水印的安全保护产品。
- ❑ 与密码技术，尤其是数字签名技术相结合，构造综合的数据安全系统。
- ❑ 使用各种生物认证技术（如指纹、视网膜）构造专人标识水印。

数字水印软件作为数据安全领域中的新生事物，具有很高的技术含量和很强的生命力，同时也孕育着巨大的商机。我们有理由相信，会有越来越多的有识之士投入到数字水印技术的研究和产业化进程中来。

# 第十一节

## 典型的数字水印软件

目前，数字水印软件既有商品化产品，也有供研究用的免费软件。

一、商品化软件

二、供研究用的软件

# 一、商品化软件

提供商品化数字水印软件的公司主要有以下一些：

- 1、Digimarc公司
- 2、Signum技术公司
- 3、Aliroo有限公司
- 4、Alpha技术公司
- 5、MediaSec 技术公司

# 1、Digimarc公司

(<http://www.digimarc.com>)

美国Digimarc公司成立于1995年，是最早从事数字水印软件开发的企业之一，其产品主要面向多媒体版权保护、认证和电子商务等领域，产品包括：

## ■ PictureMarc

PictureMarc是与Adobe Photoshop、Corel DRAW、Corel PHOTO PAINT、Micrografx Wedbtricity、Micrografx Graphics Suite和Micrografx Picture Publisher等图像处理和图形绘制软件捆绑销售的数字水印插件。PictureMarc可以在图像中加入著作权ID、发行权ID和复制权ID。

## ■ ReadMarc

ReadMarc是与PictureMarc配套使用的数字水印阅读器，是一个可以自由下载的免费软件，可在Windows 95/NT和Macintosh PowerPC平台上运行。

## ■ BatchMarc Pro

BatchMarc Pro是专门用于批量添加图像水印的软件。

## ■ Digimarc Watermarking SDK

Digimarc Watermarking SDK是一个数字水印软件开发包，提供C/C++调用界面，可以实现图像水印的嵌入、检测和阅读。

## ■ Marc Centre

Marc Centre是一个基于Internet的水印认证服务系统，可以管理大规模的著作权ID数据库，并提供各种在线服务。

## ■ Marc Spider

Marc Spider是一个水印Agent，它可以根据用户的著作权管理信息，自动地在Internet上搜索数字作品的非法拷贝，然后以报表形式将相关网址提供给用户。

## 2、Signum技术公司

[http://www.signumtech.com/index\\_ns.html](http://www.signumtech.com/index_ns.html)

这家英国公司成立于1997年，所开发的SureSign系列数字水印产品主要面向数字摄影、多媒体、网络发行、电子商务和医学影像等领域。Signum 水印产品包括两个系列：SureSign Fingerprints和SureSign Fingerprint Detection。其中，SureSign Fingerprints系列为水印嵌入软件，SureSign Fingerprint Detection系列为免费的水印检测软件。

SureSign Fingerprints系列包括为Photoshop开发的数字水印插件SureSign Writer、批量水印书写软件SureSign Pro和水印开发包SureSign SDK。

SureSign Fingerprint Detection系列包括为Photoshop开发的水印检测插件SureSign Detector和为Netscape Navigator开发的水印检测插件CyberSleuth。

SureSign水印产品允许用户嵌入作者标识和作品标识两种水印信息。在图像类型方面，SureSign没有特殊的要求，支持真彩色、灰度和索引色图像。在存储格式方面，SureSign支持压缩比小于30的JPEG格式。SureSign还可以从打印作品的扫描图像中读取水印。

### 3、Aliroo有限公司 (<http://www.aliroo.com>)

该公司成立于1993年12月，主要开发各种基于密码学的网络安全产品和数字水印软件。Aliroo公司与Digimarc公司达成了一系列技术协议，其开发的数字水印软件ScarLet可以直接使用Digimarc公司的认证服务。

ScarLet提供了所谓"descarring"功能，在确认用户密码后，可以消除水印并恢复原图。这种功能在数字水印产品中是不多见的。

## 4、Alpha技术公司

(<http://www.generation.net/~pitas/>)

Alpha公司是专门从事计算机图形学、图像处理、计算机视觉等专业软件开发的企业，其开发的数字水印产品EIKONAmark在技术上有很多特色，非常适于数字图像的版权保护。

EIKONAmark比较好地解决了多次图像水印问题，可以添加50个以上不同的水印。当然，每个水印都会在一定程度上损害图像的质量。EIKONAmark还允许将添加了水印的图像保存为高压缩比的JPEG格式，解码时也不需要原始图像。

## 5、MediaSec 技术公司

(<http://www.mediasec.com>)

该公司是一家专业的信息隐藏技术公司，其开发的 SysCop 系列产品主要面向数字水印、隐蔽标识和隐蔽通信。SysCop 系列产品最突出的特点是允许在图像（PPM/PGM/PBM、GIF、TIFF 和 JPEG 格式）和视频信号（MPEG I 和 MPEG II）中灵活地隐藏各种长度的信息。

SysCop系列包括水印开发包SysCop API、水印嵌入工具 SysCop Writer、水印批量处理工具SysCop Batch和水印阅读工具SysCop Reader，这些产品可以在Unix（SUN Solaris、HP-Ux、SGI IRIX）和Windows（NT 3.51、NT4.0、95/98）环境下运行。

## 二、供研究用的软件

Internet上有许多为验证算法而编写的数字水印软件，其中一些体现了非常宝贵的设计思想，具有较高的参考价值。以下罗列的是其中较为典型的几个软件：

## 1、S-Tools

(<ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/s-tools4.zip>)

S-Tools是一个时（空）域数字水印软件，支持.wav格式的音频文件和.gif、.bmp等格式的图像文件。S-Tools处理24位真彩色图像的速度很快，对于索引色图像，根据用户的选择，可以还原成真彩色图像处理或通过削减颜色数量添加水印。

## 2、 Hide and Seek

(4.1版

[:ftp://ftp.csua.berkeley.edu/pub/cypherpunk/steganography/hdsk41b.zip](ftp://ftp.csua.berkeley.edu/pub/cypherpunk/steganography/hdsk41b.zip) )

(5.0版:

<http://www.rugeley.demon.co.uk/security/hdsk50.zip>)

(ver1.0 for Windows95版:

<http://www.cypher.net/products/>)

Hide and Seek是时（空）域数字水印软件，它对图像的限制较多，只能处理256色图像，图像尺寸被限制为 $320 \times 320$ 、 $320 \times 400$ 、 $320 \times 480$ 、 $640 \times 400$ 、 $1024 \times 768$ 。

### 3、Hide4PGP

([http://www.rugeley.demon.co.uk/security/hi  
de4pgp.zip](http://www.rugeley.demon.co.uk/security/hi<br/>de4pgp.zip))

Hide4PGP是一个典型的使用LSB算法的数字水印软件，用于在8位或24位BMP图像中嵌入水印。对于24位真彩色图像，可选的隐藏位数为1、2、4、8几种。对于8位索引色图像，Hide4PGP引入的噪声很明显。

## 4、StegDOS

(<ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/stegodos.zip>)

StegDOS是早期的运行在DOS下的水印软件，使用的也是LSB方法，效果比较差。

## 5、 White Noise Storm

(<ftp://ftp.csua.berkeley.edu/pub/cypherpunks/steganography/wns210.zip>)

White Noise Storm是典型的基于扩展频谱技术的数字水印软件，隐藏效果非常好，但数据量偏小。

## 6、Mandelsteg

(<ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/>)

Mandelsteg是一个提供源代码的时  
(空)域数字水印软件。

## 7、Jsteg,Jpeg

(<ftp://ftp.funet.fi/pub/crypt/steganography>)

Jsteg Jpeg是专门针对JPEG图像格式开发的数字水印软件，水印隐藏在DCT变换域上。从处理后的图像上很难看出隐藏数据的痕迹，但对比添加水印前后的DCT谱，可以发现嵌入水印后图像的DCT变换系数有明显的阶梯效应。

## 8、UnZign

(<http://altern.org/watermark/>)

UnZign是早期的（1997年）数字水印测试工具。

## 9、StirMark

([http://www.cl.cam.ac.uk/~fapp2/watermarking/image\\_watermarking/stirmark](http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/stirmark))

StirMark是一个在数字水印研究领域中有名的测试工具，由剑桥大学开发，其版本更新速度很快。StirMark可以从多方面测试水印算法的鲁棒性，用于测试的攻击手段包括线性滤波、非线性滤波、剪切/拼接攻击、同步性破坏攻击等。许多公开发表的数字水印方面的论文都以StirMark的攻击结果作为衡量水印算法好坏的标准。

# 第十二节

# 研究动态

从公开发表的文献看，国际上在数字水印方面的研究刚开始不久，但由于有大公司的介入和美国军方及财政部的支持，该技术研究的发展速度非常快。1998年以来，《IEEE 图像处理》、《IEEE 会报》、《IEEE 通信选题》、《IEEE 消费电子学》等许多国际重要期刊都组织了数字水印的技术专刊或专题新闻报道。

在美国，以麻省理工学院媒体实验室为代表的一批研究机构和企业已经申请了数字水印方面的专利。1998年，美国政府报告中出现了第一份有关图像数据隐藏的AD报告。目前，已支持或开展数字水印研究的机构既有政府部门，也有大学和知名企业，它们包括美国财政部、美国版权工作组、美国空军研究院、美国陆军研究实验室、德国国家信

息技术研究中心、日本NTT信息与通信系统研究中心、麻省理工学院、伊利诺斯大学、明尼苏达大学、剑桥大学、瑞士洛桑联邦工学院、西班牙Vigo 大学、IBM公司Watson研究中心、微软公司剑桥研究院、朗讯公司贝尔实验室、CA公司、Sony公司、NEC研究所以及荷兰飞利浦公司等。

1996年5月30日~6月1日，在英国剑桥牛顿研究所召开了第一届国际信息隐藏学术研讨会，至今已举办了三届。SPIE和IEEE的一些重要国际会议也开辟了相关的专题。

我国学术界对数字水印技术的反应也非常快，已经有相当一批有实力的科研机构投入到这一领域的研究中来。为了促进数字水印及其他信息隐藏技术的研究和应用，1999年12月，我国信息安全领域的何德全院士、周仲义院士、蔡吉人院士与有关应用研究单位联合发起召开了我国第一届信息隐藏学术研讨会。2000年1月，由国家“863”智能机专家组和中科院自动化所模式识别国家重点实

实验室组织召开了数字水印学术研讨会，来自国家自然科学基金委员会、国家信息安全测评认证中心、中国科学院、北京邮电大学、国防科技大学、清华大学、北方工业大学、上海交通大学、天津大学、中国科技大学、北京大学、北京理工大学、中山大学、北京电子技术应用研究所等单位的专家学者和研究人员深入讨论了数字水印的关键技术，报告了各自的研究成果。从这次会议反应的情况上看，我国相关学术领域的研究与世界水平相差不远，而且有自己独特的研究思路。

目前，已支持或开展数字水印研究的机构既有政府部门，也有大学和知名企业，它们包括美国财政部、美国版权工作组、美国空军研究院、美国陆军研究实验室、德国国家信息技术研究中心、日本NTT信息与通信系统研究中心、麻省理工学院、伊利诺斯大学、明尼苏达大学、剑桥大学、瑞士洛桑联邦工学院、西班牙 Vigo 大学、IBM 公司 Watson 研究中心、微软公司剑桥研究院、朗讯公司贝尔实验室、CA 公司、Sony 公司、NEC 研究所以及荷兰飞利浦公司等。

# 第十三节

# 研究展望

- ❑ 第二代的数字水印技术：基于内容特征
- ❑ 算法理论分析
- ❑ 非对称（公钥）数字水印系统
- ❑ 多水印问题
- ❑ 安全有效的应用框架
- ❑ 针对实际应用提出适合的算法和应用系统框架
- ❑ 数字水印与基于内容的图象检索

谢谢！

