数字水印的应用、性质及性能评测*)

张鸿宾　张　帆
(北京工业大学计算机学院　北京100044)

A Review of Watermarking Applications, their Properties and Benchmarking

ZHANG Hong-Bin　ZHANG Fan
(Computer Institute of Beijing Polytechnic University, Beijing 100044)

Abstract The last ten years have seen rapidly growing in the field of digital watermarks. Meanwhile, a large number of attacks appears as fast as new algorithms are proposed, which emphasizes the limits and weaknesses of those algorithms. The tools, methodologies and benchmarking of assessing the current algorithms are almost non-existent. This paper reviews a number of applications of digital watermarking and their properties, describes and classifies a number of attacks on digital watermarks, and analyzes the Stirmark, Checkmark, Optimark benchmarking systems. At end, we give some comment on the watermarking research.

Keywords Digital watermark, Attacks on digital watermarks, Evaluation, Benchmarking

近年来，随着数字化技术的进步和互联网的迅速发展，数字多媒体(图像、视频、音频和三维计算机图形等)的应用取得了惊人的进步。数字媒体易于编辑、修改、复制和传播的优点在推动信息化社会前进的同时，也使它的知识产权保护和完整性、真实性的认证等问题成为人们关注的焦点。由于缺乏知识产权保护和认证的有效手段，也妨碍了数字媒体在许多方面更进一步的应用。从20世纪90年代初开始，国际上一些大学、研究机构和公司等都投入了大量的人力和财力，启动了不少科研计划和项目，进行多媒体安全技术的研究和开发，提出了以数字水印和信息隐藏技术为工具的多媒体数据版权保护的方法，并迅速成为一个热点的研究领域。通过近十年的发展，目前数字水印和信息隐藏已经成为一个单独的研究领域，吸引了国内外大量的研究和实际工作者[1~7]。

数字水印的早期研究是由多媒体版权保护的需要推动的。研究方向主要集中在鲁棒水印上，即利用人的视听觉特性，有控制地在多媒体数据中引入一定量的畸变，以嵌入不易感知的版权等信息。鲁棒水印要能够经受常用的信号处理运算及抵抗各种旨在破坏和去除水印的攻击。十年来人们在鲁棒水印问题上发表了许多理论研究成果，提出了大量的水印算法和实施技巧。这些研究以及人们在视听觉感知模型和计算机信息安全等问题上的进展，为今后数字水印技术的发展奠定了很好的基础。

然而，随着研究的深入，人们也提出了各种攻击数字水印的方法，其数量几乎和水印算法一样多。大量的攻击算法以及这些算法的组合攻击，暴露了目前大多数以版权保护为目标的鲁棒水印的弱点，需要人们研究更加鲁棒的抗攻击的水印算法。另外，人们也认识到目前迫切需要一种能测试水印算法性能的基准和工具。虽然不少论文的作者都声称自己的算法"能够抵抗一般的信号处理和各种攻击"，但他们的结论往往是基于自己的有限实验、自己的图像或音视频数据以及自己的测试方法而得出的，缺乏可比和可重复性，性能的测试也不够完全和充分。由于缺少水印性能评测的基准和工具，人们不能评价水印算法是否达到了用户(软硬件制造商、版权所有人等)的要求。不能期望他们目前会在自己的产品或作品上采用这种未经充分测试的尚未成熟的技术。

以上两个问题解决的好坏，将在很大程度上影响今后水印技术的应用。本文将重点归纳、分析攻击水印的各种方法及其对抗措施，分析几个在试用或正在建设中的水印测试基准和平台，并对今后水印应用的前景提出一些看法。

1　数字水印的应用

早期的数字水印是以版权保护为目标的。随着研究的发展，人们发现除了版权保护之外，水印和信息隐藏还有许多其它可能的应用。这些应用的前景甚至比版权保护的还要看好[8]。不同的应用场合对水印的性质提出了不同的要求。只有区别不同性质的水印，才有可能确定相应的评价基准。本节将介绍数字水印的一些主要应用。下一节分析在不同的应用中水印应该具备的性质。目前提出的水印的主要应用领域有：

1)电视和电台广播的监视和监听　有这种要求的主要是购买了电视、电台广告时间的客户以及音像作品的版权人。购买了广告时间的人关心他们的广告是否播出了，音像的版权人也关心他们的利益是否受到了损害。1997年日本两家电视台暴露出来的重复收费而有的广告未播的丑闻使人们感到了这种系统的必要性[9]。利用水印的监视/听系统已经存在一些年了。其基本原理则来自一些较早的专利[10~14]。

2)版权的标识　利用数字水印技术可以把类似"©Date by Owner"的版权提示信息嵌入在数字媒体中。目前这种版权提示对版权保护已不再是必需的，但仍然是推荐使用的。在Adobe公司的著名Photoshop图像处理软件中就采用了Digimarc公司的这种水印技术。

3)版权的证明　数字媒体的产权所有人不仅希望利用水印来标识版权，而且希望当有版权争议时可以利用水印来解决争端。版权的证明是一个困难的问题。除了鲁棒性等问题之外，盗版者还可以插入另一个水印而声称版权是他们的[15]。

*)本课题得到国家自然科学基金、北京市自然科学基金、北京市教委科技发展计划和863计划的资助。

当有一个版权注册中心时，这个问题要容易解决些。

4）认证　数字技术的进步使得窜改媒体的内容变得非常容易，而且不易察觉。媒体完整性的认证在法律、医学、金融、保险、刑侦以及大众传媒等行业有着非常重要的意义。Friedman 提出的“可信赖照相机”[16,17]，是把图像的数字签名存放在文件的头部。这种数字签名在格式转换或被攻击时很容易丢失。而利用水印技术的认证方法，则是将数据完整性的信息直接嵌入媒体中。对媒体的任何窜改也会作用在水印上，因而可以检测有无窜改，有的还可以定位窜改。有些算法允许对图像等进行一定程度的压缩，但不允许有更大的变化。

5）交易水印或称指纹　在版权保护和版权标识中，同一个版权水印要嵌在同一作品的不同拷贝里。而在多媒体数据的销售中，可以把销售出去的每份拷贝都加入购买者或产品序列号等信息，这种水印称为指纹（交易水印）。指纹的用途是当发现有盗版行为时，可以为追踪盗版源头提供一种调查的手段。交易水印目前已经被 Divx 公司用在他们的产品中。

6）拷贝控制　上述用于版权标识和证明、监视/听的水印以及交易水印和认证水印等都不具有防止拷贝的功能。它们的功能是威胁盗版者并提供有力的调查工具。如果在音像的录制设备中装有检测水印的电路，那么就可以实现拷贝控制的功能。目前 DVD 业和数字音乐销售业都在从事这方面的工作[18,19]。实际上，利用水印来控制视频或音频设备的专利可以分别追溯到1989和1953年[20,21]。

7）隐蔽通信　这是一种将重要信息隐藏在无关紧要的媒体中进行通信的方法。更确切地说，是一种数据隐藏的方法。Simmons1984年用“囚犯问题（The Prisoner's Problem）”从理论上描述了这个问题[22]。其背景是当时美苏削减战略导弹核查中的问题。

8）数字水印的其它应用　除了上面提到的一些应用之外，数字水印还有其它一些已经发现或尚未发现的应用。例如：图像和音/视频数据的注释，将音频信号嵌入视频中的多语言广播，图像和视频的检索，视频数据发送错误的校正等。这些新的应用领域同样吸引了企业和学术界的注意。

2　数字水印的性质

谈到数字水印的性质时，人们常使用鲁棒性、抗攻击性、保真性、嵌入和检测水印的速度、水印容量、负荷、错检率、漏检率等。这些性质和水印的应用场合密切相关。不同应用的水印有不同的性质要求。不可能也没有必要要求一种水印同时具有上述的性质。必须针对应用场合在各种性质间进行折衷和取舍。下面，我们根据不同的应用场合，分析水印的各种性质。

1）鲁棒性　是指水印经受各种常用的信号处理运算的能力。如 A/D、D/A 转换、有损压缩以及几何变换等。对一种运算鲁棒的水印可能对另一种运算脆弱。在实际应用中要区别情况，对水印的鲁棒性提出适当的要求。

例如，在电视、电台的广播监视/听中，要求水印能经受发送和接受过程中的处理和畸变就可以了，如有损压缩、模拟发送和少量的水平和垂直位移等。其它的畸变在这个过程中没有发生，自然不要求它能抵抗了。

再如隐蔽通信中对水印的鲁棒性没有特别的要求，只要隐藏得不易察觉、隐藏的数据量大就可以了。而对认证水印，一般要求它是易损的，以便检测窜改。

对鲁棒性要求高的场合是版权的标识和证明、指纹和拷贝控制等。这时的水印要能经受盗版人的各种信号处理手段。

2）抗攻击性　指水印系统抵抗恶意攻击的性能。攻击的目的是要清除水印，或使得水印不能检测，或使得水印的功能失效，同时尽量保持原媒体的质量。针对不同的应用，攻击的类型也不相同。当攻击的方法是信号处理的方法时，抗攻击性和鲁棒性的含义是相同的。我们将在下一节详细分析各种攻击算法。

抗攻击性对版权水印、指纹水印和拷贝控制等是非常关键的。但对认证水印和数据隐藏来说则关系不大。

3）保真性　要求嵌入水印后媒体音视质量的变化不易被观察者所察觉（不少文献使用不可感知来描述这种性质。不可感知当然是最理想了。但若真的不可感知，则基于感知的有损压缩将会完全清除这种水印）。音、视的质量可以用客观评测，如信噪比等，也可用专家的主观感受来评价。

在水印系统中，保真性和鲁棒性、水印容量间往往要作折衷的选择。如以中等的感知质量换取更好的鲁棒性。

4）水印的容量和负荷　这两个术语目前尚无一致的明确定义。水印容量一般指可以在载体中嵌入多少的信息量。而负荷则表示在一定量的载体（或单位载体）数据中可以嵌入的位数。水印的容量或负荷和水印的鲁棒性、保真性之间互相影响。水印算法应该根据具体情况在三者间作出折衷。

5）误检率　是指在没有水印的媒体中检测出有水印的概率。本质上有两种不同的误检率。一是对同一个媒体数据嵌入不同水印时的情况，另一种情况是同一种水印嵌入了不同的载体。大多数的应用属于第二种情况，而指纹水印则属于第一种。不同的应用场合要求的误检率和漏检率（有水印但没有检测出来）也不相同。

6）水印密钥空间的安全性　在水印的嵌入和检测时一般都要用密钥对水印信息进行编码。和密码学一样，密钥空间要足够大才能保证安全。

7）水印嵌入和检测的时间　有些应用如音/视频的广播监视/听要求实时，而版权水印则对时间无特殊要求。

8）不对称水印　目前绝大多数的水印算法在嵌入和检测水印时使用的是同一密钥。把这个密钥放在每个水印检测器上（如家用多媒体播放机），会给盗版人很大的便利。在这种情况下，我们希望的是不对称的水印系统。即嵌入水印时使用的是私钥，查看水印时用的是公钥。用公钥可以查看，但不能修改水印。目前人们还不知道能否找到鲁棒的不对称水印系统。

3　数字水印的嵌入和检测

数字水印嵌入和检测的一般框架如图1所示。图中 S_0 是原媒体或称为宿主媒体。W 是要嵌入的信息，即水印。嵌入过程要保证 S_1 和 S_0 感知上相同或相似。S_1-S_0 表示由于水印嵌入而引起的畸变。而 S_2-S_1 表示由于攻击而引入的噪声。

目前在空间（时间）域和变换域上都提出了许多水印算法，从水印嵌入的方法上看这些算法主要可以分为两种类型[23]。第一类水印嵌入方法是把水印信息（或经过编码、调制或放大缩小的）W 加到宿主信号上去，即 $S_1=S_0+f(S_0,W)$，其中 $f(S_0,W)$ 是 S_0 和 W 的一个函数。相加运算可以在空间（时间）或变换域或特定的特征上进行。相加性的广谱水印（Additive Spread Spectrum）是这类方法的代表。这类水印的检测一般通过相关运算来进行。虽然可以从 S_1 或 S_2 中直接提取水印 W，但若能利用 S_0，则水印检测的性能将会提高。

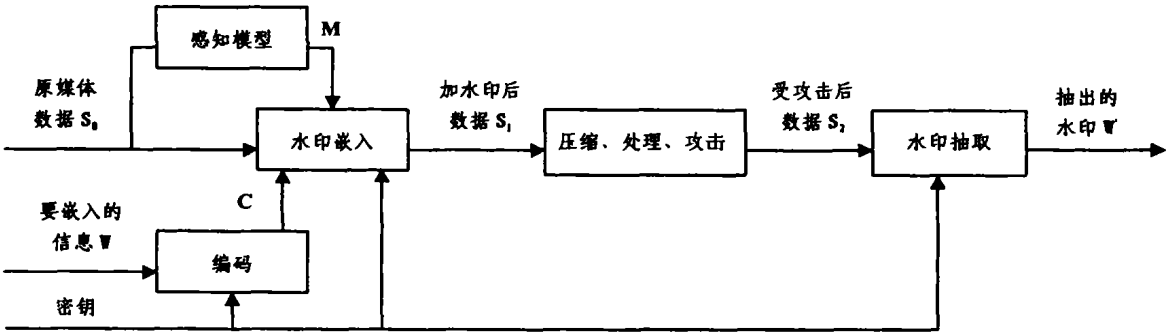

图1 水印系统的一般框架

第二类水印方法是将原信号空间划分为一些子集，通过函数 g(·)将它们映射到水印取值的空间，例如二值水印时的{0,1}。为了嵌入一个水印位 b，嵌入水印后的信号 S_1 应该满足：它映射到 b，即 $b=g(S_1)$，而且 S_1 和 S_0 间的感知畸变越小越好，即：

$$S_1=\arg\min_{S\ s.t.\ g(S)=b} D(S_0,S)$$

式中 D(·,·)是 S 和 S_0 间的感知距离。和第一类水印嵌入方法时不同，第二类水印的提取不需要 S_0，因为水印位 b 可以完全由 S_1 确定。许多盲检测的水印算法都属于这种类型。这类水印的嵌入容量比第一类的一般要大许多，但鲁棒性有一定的限制。

第二类嵌入方法的一个简单例子是奇偶嵌入。即将承担水印信息的像素值改为离它最近的偶数来嵌入水印"0"，或改为离它最近的奇数来嵌入水印"1"。水印抽取时只要检验该像素值的奇偶就可以了。

除了奇偶嵌入外，第二类水印的基本方法还有根据查找表嵌入，或根据像素值间的关系来嵌入"0"或"1"等。例如，将原像素值 P_1 和 P_2 分别修改为他们最近的值 P_1' 和 P_2'，通过满足 $P_1'>P_2'$ 来嵌入"1"，满足 $P_1'<=P_2'$ 来嵌入"0"[24]，扩展这些基本的方法，可以得到更复杂的嵌入方式。但是，随着嵌入单位的扩大，水印的鲁棒性得到了增强，而容量则会减少。为了增大水印的容量，MIT 的 Chen 提出了 QIM(Quantization Index Modulation)的方法[25]。Chen 的方法可以看作是第一类和第二类水印方法的一种组合。

4 攻击水印的方法

在人们提出各种水印算法的同时，也出现了大量攻击水印的方法。所谓攻击就是要破坏水印的检测或使水印的功能产生歧义而失效。研究攻击水印的方法主要有两个目的。一是改进水印算法的性能，研究更好的水印算法；二是为水印的评测提供一些基准和手段。从攻击的原理上看，目前攻击水印的方法大体上可以分为以下几类：旨在清除水印的攻击，旨在破坏水印检测同步的攻击，基于水印或原宿主数据估计的攻击，协议级和系统实施级上的攻击等。还有些攻击方法是这些基本方法的组合。下面分析几种主要的基本攻击方法[26~30]。

1）*旨在清除水印的一类攻击* 试图从嵌入水印的媒体中完全清除水印信息，而不必破解具体的水印算法和密钥。这类攻击包括去噪处理、量化、重新调制和共谋(Collusion)攻击等。这些方法不一定总能完全去除水印，但却能对水印信息造成相当程度的破坏。

水印的嵌入可以看作是向原数据中加入了噪声。当有水印和原数据的统计模型时，可以设计最优的去噪或量化算法，以便尽可能地破坏水印而又保持攻击后数据的一定保真性。

共谋攻击常用在指纹水印等场合。这时同一宿主(Host)媒体中嵌入了不同的水印。如果能获得一定数量的不同拷贝(比如10个)，则简单的平均运算即可有效地破坏水印。还可以从每个拷贝中剪切一部分拼接起来而清除水印。

2）*旨在破坏相关检测同步的几何攻击* 和旨在清除水印的攻击不同，几何攻击不去清除水印，而是破坏水印相关检测时的同步从而使水印检测不出来。而相当一部分水印算法正是基于这种相关检测的。早期的两个水印评测工具 Unzign[31] 和 Stirmark[32] 正是凭借组合的几何攻击方法攻破了当时几乎所有的图像水印算法。

Unzign 中引入了局部像素的跳动(Jitter)，即随机删掉或复制某些行或列。这种简单的方法对攻击空间域的水印非常有效。而 Stirmark 则组合了整体和局部的几何变换攻击。为了抵抗整体的几何攻击，人们提出了采用嵌入附加的基准模板的方法，或采用自相关函数具有特殊性质的周期水印，或采用具有变换不变性质的变换域(如 Fourier-Melline 变换)的方法等。

目前的研究状况是，人们可以找到对付整体仿射变换攻击的方法，而对付像 Stirmark 中的局部随机几何畸变则要困难得多。

3）*基于估计的攻击* 其原理是，当知道原宿主数据和水印的统计性质时，即使没有水印密钥的信息也可以利用一些最优化方法，如最大似然估计(ML)、最大后验估计(MAP)和最小均方误差估计(MMSE)等，去估计或至少部分地估计水印或原来未加水印的数据[33~37]。估计出的水印或原数据可以用来移去水印、破坏水印的同步模式、或用作调制攻击和拷贝攻击等。调制攻击是从加水印的数据中减去水印估计的某一倍数，这样可以在很大程度上破坏水印的相关检测。如果再辅助使用对水印估计的视觉掩蔽加权、添加非高斯分布噪声以及在感知次要分量上添加大量噪声等手段，会对相关检测造成更大的破坏。

拷贝攻击是把估计出的水印拷贝到另一个没有水印的目标数据中。拷贝过程中要对水印和目标数据作些调整以满足不易察觉的要求。这些调整可以根据人的视听觉系统特性(HVS/HAS)进行，如对比度和纹理屏蔽等。拷贝攻击主要用在相加性水印的场合。

抵抗基于估计的攻击的方法是使水印满足功率谱条件，即使水印的功率谱和原宿主数据的功率谱成正比[34]，有时也称为调节水印功率谱的形状。Voloshynovskiy 和 Pun 等从图像去噪的角度分析了水印的估计问题。在假定原图像是非平稳高斯过程或广义平稳高斯过程，水印(即噪声)为平稳高斯

过程的条件下，导出了水印最能抵抗基于估计攻击的地方。实验表明，这两种不同方法得出的结果是基本吻合的。

4）*当水印检测装置可以利用时的* Oracle *攻击*　当攻击者可以利用水印检测装置来得到媒体中的水印检测值或只是有、无的响应时，他可以采用类似机器学习中的 Oracle 模型，采取试探的方法学习水印的存在区域，从而在一个合理的时间限制内以相当高的概率来清除水印。

5）*协议*（Protocol）*层次上的攻击*　协议层次上的攻击旨在攻击水印应用的协议和概念。Craver 等提出的“可颠倒水印”即属于这种攻击类型[15]。这种攻击的出发点是，若媒体数据中存在两个以上的水印时，一般的水印系统中没有区别哪个水印是先加入的机制。假定原始媒体数据是 d，版权人 a 在 d 中嵌入了版权水印 w_a，得到了加水印后的数据 $d+w_a$。而攻击者 b 在得到 $d+w_a$ 后，从中减去他的水印 w_b 而形成了 $d+w_a-w_b$，并声称拥有该数据的版权。这时的版权归属将成为一个有歧义的问题。上节的拷贝攻击也属于这种协议层次上的攻击。

虽然也用一些技术上的方法来防止“可颠倒攻击”，但解决这个问题的根本方法可能是建立“注册中心”和采用时间邮戳等技术。

6）*系统实施层次上的攻击*　仅考虑水印嵌入和检测过程的攻击是不够的。许多安全上的漏洞可能来自系统实施层次上的问题。例如，在拷贝控制的应用中，攻击者完全可以不去攻击水印，而是改动自己的录制设备的水印检测器的输出。而这样的改动比攻击水印要容易得多。

5　数字水印的评测基准和系统

十年来人们发表了大量的水印算法，但同时也提出了各种攻击水印的方法。这些方法暴露了目前水印算法的弱点。有不少论文的作者都声称自己的算法“可以经受常用的信号处理和抵抗各种攻击”，但他们的结论只是用自己的测试方法、在自己的数据上进行有限的实验而得出的，不具有可比性和可重复性。这些水印算法还没有经过充分可靠的安全测试。不可能期望人们把版权保护这样的利害攸关问题建立在一个不成熟的技术上。目前迫切需要建立数字水印的评测方法、评测基准和评测系统。凭借这样的测试系统，研究人员可以充分检验自己的算法，改进算法的弱点，和其它方法进行比较。水印的用户可以检验水印算法是否满足了他们的要求，而企业界也可以借此来评估水印的可靠性以及采用时可能出现的风险。

粗略地讲，一个水印评测系统的输入是水印的嵌入和检测（或信息位抽取）程序，输出则是它的性能指标和表征各种性能的图表等。为了能全面、充分、准确地评测一个水印算法，需要结合具体的应用场合，选择适当的评价指标和评测方法。评测系统中需要包含有各种攻击方法和各种实验数据及参数。如：

1. 各种攻击程序的集合：$A=\{A_i|i=1,\cdots,N_A\}$

2. 各种性质和内容的有代表性的图像（或音频、视频）试验数据的集合：$I=\{I_i|i=1,\cdots,N_I\}$

3. 密钥的集合：$K=\{K_i|i=1,\cdots,N_K\}$

4. 要嵌入的信息的集合：$M=\{M_i|i=1,\cdots,N_M\}$

5. 音/视质量规格的参数集：$Q=\{Q_i|i=1,\cdots,N_Q\}$

6. 对各种性能加权的参数集合：$P=\{P_i|i=1,\cdots,N_P\}$

下面我们分析几个已经提出或正在建设中的水印评测系统。

1）Stirmark *评测系统*　是较早的一个著名水印评测系统，经过不断的改进和扩充，目前已到了版本3.1，2002年4月又公布了版本4。它的工作方式是将一组攻击加到一组加水印的图像上。然后用待测的水印算法去检测或提取水印信息。如果水印检测或提取正确，则赋予该试验的分值为1，否则分值为零。对各种试验成功的百分比即为该水印算法的性能指标。

Stirmark 中包含的攻击主要有：信号增强、JPEG 压缩、缩放、旋转、剪切（Cropping）、切变（Shearing）、线性变换、几何变换和随机几何变换等。Stirmark 出现后，几乎可以攻破当时所有著名的水印算法。它的有力工具是采用了组合的随机几何畸变。

Stirmark 的成功之处在于它暴露了水印算法对局部几何畸变的弱点，促进了人们寻求更鲁棒算法的研究。然而，作为一个水印系统的测试工具来说，Stirmark（版本3.1）还远不够充分和全面。主要的问题有：

（1）在确定图像质量的评定及算法可靠性的等级时，没有根据不同的应用场合确定不同的等级标准。

（2）没有考虑水印的误检（False Alarm，False Positive 即没有水印时却检测出有水印）概率。这样当两种算法的漏检率相同而误检率不同时，Stirmark 给两个算法打的分相同。这显然不够合理。

（3）没有把水印有无的检测和提取水印时的位错率这两种事情区别开来处理。

（4）Stirmark 只利用一个密钥来检验水印的性能是不充分的。因为水印检测是和密钥有关的，所以应当用不同的密钥来检验水印算法的性能。

（5）没有考虑水印嵌入和检测的时间开销。

（6）在计算某个水印算法的总体评价时，Stirmark 对各种攻击和各个图像是等权平均的，这不太符合实际情况。实际上对不同的应用场合，某些攻击比另外的攻击可能会更重要，更常出现。

（7）在评测水印算法时除了嵌入和检测性能外，还要考虑水印的容量和水印抵抗某类攻击（如压缩）的极限点。

（8）与用户之间的接口还需要进一步完善。

上述这些问题的存在并不奇怪。因为早期的 Stirmark 是作为攻击水印算法的工具出现的，其目的并不是要全面地评测水印算法。目前 Stirmark 的作者正在进一步扩充和完善它的功能。版本4的性能和用户接口已经有了很大的改进，而欧盟也启动了有组织的大规模的研制水印评测系统的计划——Certimark。

2）Certimark *计划*　为了研制正式的全面的水印评测系统，欧盟于2000年5月启动了 Certimark（Certification for Watermarking Techniques）计划[38]。有15家大学、科研机构和企业参加了这一计划。Certimark 计划的研究目标为：

（1）设计、研制和公布完善的水印技术评测基准和工具，为水印技术的提供者和使用者提供一个参考工具。

（2）为水印技术提供一个认证过程。

（3）研究图像及 Internet 上传输的低位率视频的水印技术中的关键问题。

Certimark 的目的是为水印技术建立一种国际承认的认证工具。这样，消费者可以评价一个水印算法是否满足他们的需要，水印技术的开发者可以在一个公开的统一评测基准上进行竞争，并增强水印技术使用者的信心。

Certimark 计划采用客户机-服务器结构。水印的嵌入、攻击、检测、图像质量的主/客观评价和评测结果等功能采用模块结构，并设计灵活的、对用户友好和易于使用的接口。目前已有β版在 Certimark 组织内部使用。

3)Checkmark 评测系统　在 Certimark 计划的支持下，瑞士日内瓦大学的 S. Pereira 和 T. Pun 等人于2001年5月开发出一个名为 Checkmark1.0的水印评测系统供人们比较和使用[39]。Checkmark 的主要特点有：

(1)在保留 Stirmark 的攻击方法的同时，新增加了基于以下几种方法的攻击：小波压缩(JPEG2000)，投影变换，几何扭曲，拷贝，去噪以及去噪后的重新调制，清除对准模板，清除非线性线，拼贴等。

(2)在图像质量评价中引入了加权峰值信噪比(PSNR)和 Watson 的图像质量度量。

(3)采用应用驱动的评测方式，可以避免和具体应用无关的一些不必要测试。

(4)以灵活的 XML 格式输出，并自动生成 HTML 格式。

(5)以加权平均的方式计算总的性能得分。

(6)可以单独使用其中的各个攻击试验。

目前 Checkmark 还有一些功能不够完全，研制作者正在进一步完善和改进该系统。

4)Optimark 水印评测系统　是在 Certimark 计划支持下，由希腊 Thessaloniki 大学的 I. Pitas 等人开发出的另一个水印评测系统[40]。和 Stirmark 以及 Checkmark 相比，Optimark 在水印评测的全面性上做得更好、更细致一些。

小结和展望　本文介绍了数字水印的一些主要应用及其性质，分析了攻击水印的一些主要方法及其对抗措施，对目前的几个水印评测工具 Stirmark、Certimark 、Checkmark 和 Optimark 的功能作了介绍和分析。下面对当前数字水印的研究现状提出几点看法。

1)数字水印的研究只有短短的十年时间，它将和密码学的发展过程一样，在攻击和反攻击的相互作用中不断发展。

2)大量攻击算法的出现，暴露了目前水印技术的弱点和局限性。然而怀疑甚至放弃水印的研究是没有道理的。事实上，对许多实际问题来说水印技术是可行的，没有绝对安全的系统。就象门锁的防盗作用一样，尽管它的防盗功能有限，可是仍然被人们普遍地使用着。这里面有一个"防君子(或技术不高的君子或小人)不防小人"的问题。

3)多媒体的版权保护不仅仅是一个水印问题。同时，对于不同的应用，必须综合考虑水印的鲁棒性、容量和媒体质量等问题的折衷。

4)数字水印的研究是由版权保护的需要而推动的。但随着研究的开展人们发现，水印技术在认证等其它问题上可能会有更好的应用。应当注意开发水印技术的新应用领域。

5)要继续深入研究目前尚未很好解决的问题，如不对称水印，水印容量和高鲁棒性的水印等问题。

6)要有好的开放的水印测试平台，使水印技术能通过评测而取得人们的承认，增强使用这一新技术的信心。

参 考 文 献

1 Proceedings of the IEEE,1998,86(6)
2 Proceedings of the IEEE,1999,87(7)
3 The First Information Hiding Workshop,LNCS,Isaac Newton Institute,Cambridge,England,vol. 1174
4 The Second Information Hiding Workshop,LNCS,vol,Springer-Verlag,April,Berlin,Germany,1998,1525
5 The Third Information Hiding Workshop,LNCS,Dresden,Germany,1999,1768: 318～332
6 The Fourth Information Hiding Workshop,Holiday Inn University Center,25-27 Pittsburgh,PA,USA,April 2001
7 The Fifth Information Hiding Workshop,Noordwilkerhout,The Netherland,Oct. 2002
8 Eurasip Journal on Applied Signal Processing,2002(2)
9 Kilburn D,Dirty linen. Data secret. Adweek,1997
10 Hembrooke E F. Identification of sound and line signals. U. S. Patent,(3004104),1961
11 Abbey C R,Pursel H H. Data Channel monitor. U. S. Patent,(3415947),1968
12 Ohsawa T,Karita M. Automatic telecasting or radio broadcasting monitoring system. U. S. Patent,(3760275),1973
13 Crosby M G. Communication including submerged identification signal. U. S. Patent,(3845391),1974
14 Solar C M. Automatic monitor for programs broadcast. U. S. Patent,(4025851),1977
15 Craver S,Memon N Yeo B L,Yeung M. Resolving rightful ownerships with invisible watermarking techniques: Limitation, attacks,and implications. IEEE Trans. on Selected Areas of Communications,1998,16(4): 573～586
16 Friedman G L. The trustworthy camera: restoring credibility to the photographic image. IEEE Trans. on Consumer Electronics,1993,39(4): 905～910
17 Friedman G L. Digital camera with apparatus for authentication of images produced from an image file. U. S. Patent,(5499294),1996
18 Bloom J A,Cox I J,Kalker T,Linnartz J-P,Miller M L,Traw B. Copy protection for DVD vidio. Proceedings of the IEEE,1999,87(7): 1267～1276
19 Bell A E. The dynamic digital disk. IEEE Spectrum,1999,36(10): 28～35
20 Branghton R S,Laumeister W C. Interactive video method and apparatus. U. S. Patent,(4807031),1989
21 Tomberlin W M,Mackenzie L G,Bennett P K. System for transmitting and receiving coded entertainment programs. U. S. Patent,(2630525),1953
22 Simmons G L. The prisoners' problems and the subliminal channel. Proc. CRYPTO'83,Plenum Press,1984: 51～67
23 M W,Yu H,Gelman A. Multi-level data hiding for digital image and video. Proc. of SPIE Vol. 3845,Photonics East Conf. On Multimedia Systems and Applications,Boston,MA,1999
24 Koch E,Zhao J. Towards robust and hidden image copyright labeling. IEEE Workshop on Nonlinear Signal and Image Processing,1995,452～455
25 Chen B. Design and analysis of digital watermarking,information embedding and data hiding system:[Ph. D. Thesis]. MIT,2000
26 Kutter M,Petitcolas F A P. A fair benchmark for image watermarking systems. 11th Int. Symp. Electronic Imaging,San Jose,CA: IS&T and SPIE,Jan. 1999,3657: 219～455
27 Petitcolas F,Anderson R,Kuhn M. Attacks on copyright marking systems. Second Workshop on Information Hiding,Portland,Oregon,USA,April,LNCS,1998,1525: 218～238
28 Anderson R,Petitcolas F. On the limits of steganography. IEEE J. of Selected Areas in Communication,1998,16(4): 474～481
29 Petitcolas F,Anderson R. Evaluation of copyright marking system. Proc. of IEEE Multimedia Systems'99,Florence,Italy,1999,1: 574～579
30 Voloshynovskiy S,Pereira S,Pun T,Eggers J,Su J K. Attacks on digital watermarks: classification,estimation-based attacks,and benchmarks. IEEE Communications Magazine,Aug. 2001. 118～126
31 Http://altern.org/watermark
32 Http://www.cl.cam.ac.uk/～fappl/watermarking/stirmark
33 Voloshynovskiy S,Pereira S,Iquise V,Pun T. Attack modeling: Towards a second-generation benchmark. Signal Processing,Special Issue: Information Theoretic Issues in Digital Watermarking,2001,81(6): 1177～1214
34 Kutter M,Voloshynovskiy S,Herrigel A. The Watermark Copy Attack. Proceedings of SPIE: Security and Watermarking of Multimedia Contents II,San Jose,CA,2000,3971: 371～380
35 Voloshynovskiy S,et al. Generalized watermark attack based on watermark estimation and perpetual demodulation. SPIE Proc. San Jose,CA,2000,3971: 358～370
36 Su J K,Girod B. Power-spectrum condition for energy-efficient watermarking. In: Proc. IEEE ICIP'99,Oct. 1999
37 Su J K,Eggers I J,Girod B. Analysis of digital watermarks subjected to optimum linear filtering and additive noise. Signal Processing,2001,81(6): 1141～1175
38 Http://cui.unige.ch/～ vision/certimark. Http://www.certimark.org
39 Http://watermarking.unige.ch/checkmark
40 Http://poseidon.csd.auth.gr/LAB_RESEARCH/watrmarking/Benchmarking/index.html