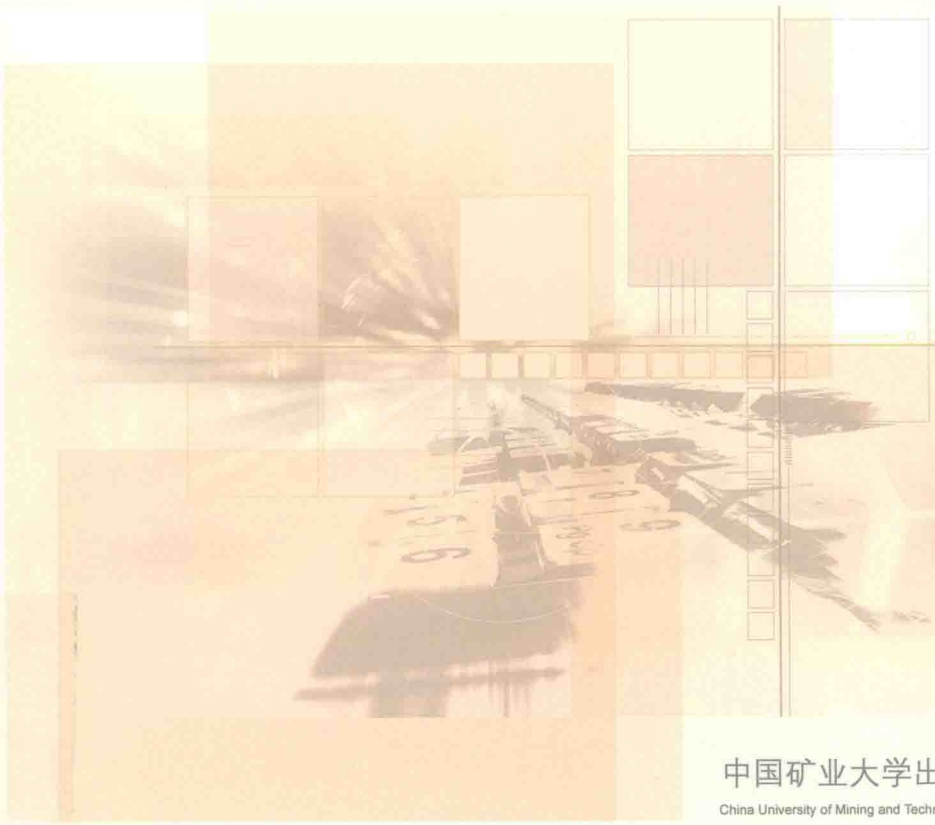
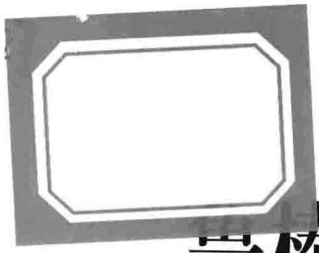
ROBUST PUBLIC-KEY IMAGE WATERMARKING

鲁棒性公钥图像数字水印技术

胡延军 高 莉 马小平 著



中国矿业大学出版社
China University of Mining and Technology Press



鲁棒性公钥图像数字水印技术

胡延军　高　莉　马小平　著

中国矿业大学出版社

内 容 提 要

本书介绍了鲁棒性公钥图像数字水印技术的理论模型、典型算法及其应用。全书共分8章，分别介绍了数字水印发展背景及现状、鲁棒性公钥图像数字水印模型、针对算法的鲁棒性及容量计算框架、基于弱信号检测原理的算法、基于扩展最佳正弦伪随机序列的算法以及在实际工程中的应用。同时对典型的数字水印算法及攻击算法、常用的水印信号嵌入位置进行了介绍。本书可作为信息安全、计算机科学与技术、通信与信息系统等专业的大学生和研究生的学习参考书，也可作为理工类大学教师的教学参考用书。

图书在版编目(CIP)数据

鲁棒性公钥图像数字水印技术 / 胡延军，高莉，马小平著. —徐州：中国矿业大学出版社，2013.7

ISBN 978-7-5646-1758-5

Ⅰ.①鲁… Ⅱ.①胡… ②高… ③马… Ⅲ.①电子计算机—密码术 Ⅳ.①TP309.7

中国版本图书馆CIP数据核字(2012)第310606号

书　　名　鲁棒性公钥图像数字水印技术
著　　者　胡延军　高　莉　马小平
责任编辑　仓小金
出版发行　中国矿业大学出版社有限责任公司
（江苏省徐州市解放南路　邮编 221008）
营销热线　(0516)83885307　83884995
出版服务　(0516)83885767　83884920
网　　址　http://www.cumtp.com　**E-mail**:cumtpvip@cumtp.com
印　　刷　徐州中矿大印发科技有限公司
开　　本　787×960　1/16　**印张** 9.25　**字数** 176千字
版次印次　2013年7月第1版　2013年7月第1次印刷
定　　价　28.00元

前　言

数字水印是实现数字作品版权保护的有效技术办法，是信息隐藏技术研究领域的重要分支和研究方向。数字水印技术已经发展成有着庞大分支的一门技术，也有很多丰富成果。鲁棒性公钥图像数字水印技术是其中的一种技术。

鲁棒性数字水印技术是我们在研究鲁棒性图像数字水印技术的探索。现有的鲁棒性图像数字水印技术的研究中，一般有意或者无意的弱化了攻击者的能力，在考虑攻击者对算法攻击的时候，认为攻击者是不清楚算法的所有细节，特别是水印信号的嵌入细节。这样，水印信号存在与否的判断就像黑箱判决，输入一个图像，然后算法输出一个水印信号是否存在的结论，让人难以信服；如果为了水印验证过程更加具有说服力，就必须公开算法细节进行验证，但这样造成的后果是水印信号存在与否只能公开验证一次。这种缺点就限制了数字水印算法在某些场合的应用。参考密码学的发展历程，是从不能公开算法细节的古典密码算法发展到一切算法细节都可以公开的公钥加密算法。我们的思考是“鲁棒性数字水印算法在设计时，能否假设攻击者能力是：对于水印的攻击者知道除了称为密钥以外的水印算法的所有细节，算法的一切细节都可以公开，即满足密码学中 Kerckhoffs 假设。”对于在这种假设基础上的鲁棒性图像数字水印技术，我们称为鲁棒性公钥图像数字水印技术。

鲁棒性公钥图像数字水印技术是比较难实现的技术。对比与密

码学中公钥加密算法，公钥加密算法只要实现明文的细微变化就会导致密文的雪崩式变化；而鲁棒性公钥图像数字水印技术不仅要实现水印的细微变化导致可用水印的巨大变化，并且还能还原或者解码出水印信息，这两个要求在某种角度上考虑是矛盾的。

我们试图通过本书，介绍鲁棒性公钥图像数字水印技术的相关研究成果，目的是让读者通过此书对其产生浓厚的兴趣；同时也期望能起“抛砖引玉”的作用，希望能吸引更多的水印研究工作者展开这方面的研究。

在本书写作过程中，研究生杨磊对第2章中水印位置的选择提供了较多的素材。作者们感谢中国矿业大学校青年基金对课题研究的支持。

由于时间仓促，加之水平所限，疏漏和不足之处在所难免，敬请读者批评指正。

目　录

1 概　述

数字水印技术是一门学科交叉、应用前景强的技术。研究数字水印的学者已经遍布通信与信息系统、信号与信息处理、信息安全、密码学、信息与计算机科学、应用数学、控制理论与控制工程等领域。

本章对数字水印技术进行了简单介绍，首先对数字水印技术的产生背景、发展、特性以及概念等进行了介绍，然后讨论了数字水印技术的分类方法，并列举了具有代表意义的水印算法。由于数字水印技术的理论基础和模型还不是非常成熟，因此，本章对数字水印相关理论进展也进行了描述。最后，本书对鲁棒性公钥图像数字水印技术的研究出发点进行了阐述，并对本书的内容和结构进行了介绍。

1.1 数字水印技术概述

1.1.1 发展背景

计算机技术和计算机网络技术的发展使得信息的发布和传输实现了“网络化”和“数字化”。因特网(Internet)的发展，使得数字作品具有非常容易进行复制和传播的特点。随着因特网的日益普及，多媒体信息的交流已达到了前所未有的深度和广度，其发布形式也愈加丰富。计算机网络已经成为发布信息的重要媒介，这使得

数据的交换和传输变成了一个相对简单且快捷的过程。随之而来的副作用是:由于数据文件或作品的数字化存在形式,使有恶意的个人和团体有可能在没有得到作品所有者的许可下,拷贝和传播有版权的内容,例如,对数字影视作品的盗版;而一些具有特殊意义的数字信息,如涉及司法诉讼、政府机要等信息,则可能会遭到恶意攻击和篡改伪造等等。如何在网络环境中实施有效的版权保护和信息安全手段,已经不仅仅是 一个法律上的问题,还是一个技术上的问题,这引起了国内外专家学者和相关部门的广泛关注[1-12]。

应用多媒体信息安全中的多媒体信息加密技术,或将密码学中的认证和鉴别的算法及其方案应用到数字数据上,并不能很好地解决版权保护问题。这是因为:对某个数字作品在分发前进行加密,同时给被授权人密钥,这样固然可以保证经过加密后的多媒体数据只有被授权持有解密密钥的人才可以存取数据,但是这样的方案却无法实现向更多的人展示自己的作品。而且数据一旦被解开,就完全置于解密人的控制之下,原创作者无法追踪作品的复制和二次传播[17,18]。因此,迫切需要一种多媒体信息加密技术的替代技术或是对密码学进行补充的技术,它应该甚至能在内容被解密后也能够继续保护内容。数字水印技术(digital watermarking)就是在这样的背景情况下被提出的。数字水印技术 是一种可以在开放网络环境下保护版权和认证来源及完整性的技术,创作者 的创作信息和个人标志通过数字水印系统以人所不可感知的水印形式嵌入在多媒体中,人们一般无法从表面上感知水印,只有专用的检测器或计算机软件才可以检测出隐藏的数字水印。

1.1.2 数字水印技术的应用

最初提出数字水印的目的是为了保护版权,然而随着数字水印技术的发 展,人们发现了更多更广的应用,有许多是当初人们所没有预料到的。一般认为数字水印具有以下主要作用[19-21]:

① 版权保护：利用算法在数字作品中嵌入版权信息，嵌入数字产品上的版权信息能够证明版权所有人的版权主张；

② 版权跟踪：利用数字指纹技术实现版权跟踪，数字指纹是水印的一种应用方式，可以追踪合法拷贝的来源；

③ 拷贝保护：水印与数字设备的结合使用可以实现拷贝保护的功能，这种情况下，数字设备提取数字产品水印中的拷贝权限比特，决定拷贝次数或者是否合法；

④ 发行监控：数字产品的网络发行或者电视播放，结合 PC 对产品的 ID 识别以及电视机对播放节目的识别与监控，可以实现对数字产品的发行统计，播放监控；

⑤ 数据认证：脆弱性水印能够完成对数字产品的完整性认证，可以判断产品是否被篡改和定位产品被篡改的位置；

⑥ 信息隐藏：水印技术可以实现隐秘通信。

1.1.3 数字水印技术的创建

文献[1]认为最早发表的有关数字版权保护思想的文献是 Muzak 公司的 Emil Hembrooke 于 1954 年写的 *Identification of Sound and Like Signals*。在这篇文章中，作者首先提出了类似于在纸中加水印一样在原始的音乐作品中加入版权所有者的信息的思想。同年，Emil Hembrooke 为带有水印的音乐作品申请了一项专利。在这项专利中，通过间歇性地应用中心频率为 1 kHz 的窄带陷波器，认证码就被插入到音乐中。该频率上能量的缺失表征使用了陷波滤波器，而缺失的持续时间通常被编码为点或长划，此认证码使用了莫尔斯电码。此系统被 Muzak 公司用到了 1984 年前后[15]。1961 年美国专利局这样描述了该项发明[22]："此发明使对音乐作品进行确证成为可能，从而制定出了一个防止盗版的有效途径，这也可以比作纸币中的水印。"

文献[2]则认为关于数字水印技术研究的最早论述应是 Tirkel

等人在1993年发表的文章 *Electronic Watermark*[23]，该文中首次使用了“water mark”这一术语。这一命名标志着数字水印技术作为一门正式研究学科的诞生。后来二词合二为一就成为“watermark”，而现在一般都使用“digital watermarking”一词来表示“数字水印技术”。随后 Tirkel 等人发表的另一篇文章 *A Digital Watermark*，当时 Tirkel 等人已经意识到数字水印的重要性，并且提出了可能的应用，包括图像标记，增强版权保护，防止伪造及控制存取图像数据等。他们针对灰度图像提出了两种向图像最低有效位中添加水印的方案。其中一种向图像的最低有效位叠加一个 m 序列，并使用自相关函数对其进行监测。另外，文献[2]还认为 Tirkel 还是第一个认识到可以将扩频技术应用到数字水印中的人，它提出可以使用扩频技术向静止图像中添加水印的思想。

1.1.4 数字水印技术的发展

数字水印技术自1993年被提出以来，由于其在信息安全和经济上的重要地位，发展较为迅速。世界各国的科研机构、大学和商业集团都积极地参与或投资支持此方面的研究。如美国财政部、美国版权工作组、美国洛斯阿莫斯国家实验室、美国海陆空研究实验室、欧洲电信联盟、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、南加利福尼亚大学、剑桥大学、瑞士洛桑联邦工学院、微软公司、朗讯贝尔实验室等都在进行这方面的研究工作。IBM 公司、日立公司、NEC 公司、Pioneer 电子公司和 Sony 公司等五家公司还宣布联合研究基于信息隐藏的电子水印技术。

国际学术界陆续发表了许多关于数字水印技术方面的文章，几个有影响的国际会议（例如 IEEE，SPIE 等）及一些国际权威学术期刊（例如 Signal Processing 等）相继出版了有关数字水印技术的专题。1996年5月，国际第一届信息隐藏学术讨论会[24]（Interna-

tional Information Hiding Workshop, IHW) 在英国剑桥牛顿研究所召开,至今该研讨会已举办了多届。在 1999 年第三届信息隐藏国际学术研讨会上,数字水印成为主旋律,全部 33 篇文章中有 18 篇是关于数字水印的研究。1998 年的国际图像处理大会(ICIP)上,还开辟了两个关于数字水印技术的专题讨论。由 Martin Kutter 创建的 Watermarking World 已成为一个关于数字水印技术的著名网上论坛。

在 20 世纪 90 年代末期一些公司开始正式销售数字水印产品。在图像水印方面,美国 Digimarc 公司[25]率先推出了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 公司的 Photoshop 和 Corel Draw 图像处理软件中。该公司还推出了媒体桥(Mediabridge)技术,利用这项技术用户只要将含有 Digimarc 水印信息的图片放在网络摄像机(web camera)前,媒体桥技术就可以直接将用户带到与图像内容相关联的网络站点。AlpVision 公司[26]推出的 LavelIt 软件,能够在任何扫描的图片中隐藏若干字符,这些字符标记可 以作为原始文件出处的证明,也就是说,任何电子图片,无论是用于 Word 文 档、出版物,还是电子邮件或者网页,都可以借助于隐藏的标记知道它的原始出处。AlpVision 的 SafePaper 是专为打印文档设计的安全产品,它将水印信息隐藏到纸的背面,以此来证明该文档的真伪。SafePaper 可用于证明一份文件是否为指定的公司或组织所打印,如医疗处方、法律文书、契约等,还可以将一些重要或秘密的信息,如商标、专利、名字、金额等,隐藏到数字水印中。欧洲电子产业界和有关大学协作开发了采用数字水印技术来监视复制音像软件的监视系统,以防止数字广播业者的不正当复制的行为。该开发计划名称为 TALISMAN(Tracing Authors' Rights by Labeling Image Service and Monitoring Access Networks)[27]。此开发计划作为欧洲电子产业界等组织的欧共体项目于 1995 年 9 月开始进行,1998 年 8 月结束,法国、比利时、德

国西班牙、意大利和瑞士等在内的11个通信与广播业者、研究单位和大学参加。

随着数字水印技术信息交流的加快和水印技术的迅速发展，国内一些研究单位也已逐步从技术跟踪转向深入系统研究。各大研究所和高校纷纷投入数字水印技术的研究且取得较好成绩。我国于1999年12月11日，由北京电子技术应用研究所组织，召开了第一届信息隐藏学术研讨会(CIHW)，至今已成功举办了多届，很大程度地推进了国内水印技术的研究与发展。同时，国家对信息安全产业的健康发展也非常的重视，我国863计划、973项目(国家重点基础研究发展规划)和国家自然科学基金对数字水印的研究均有资金支持，2006年的《科技型中小企业技术创新基金若干重点项目指南》中[28]还明确指出了“本年度重点支持数字水印及相关处理设备”。在国家政策支持下，已经有相应的公司研制了相关软件产品并进行了实施。如：国泰信安公司就已实施了不少数字水印技术相关工程及项目[29]。

1.1.5 数字水印技术概念

数字水印技术可以从水印技术的作用和过程两个方面进行定义：

从数字水印技术所起的作用上而言：数字水印技术是利用作品中普遍存在的冗余数据与随机性，把版权信息嵌入在数字作品本身中，从而起到保护数字产品版权或完整性的一种技术[2]。

从数字水印技术的过程而言：数字水印技术，是指在数字化的数据内容中嵌入不明显的记号；这些被嵌入的记号通常是不可见或不可察的，但是通过一些计算操作可以检测或者提取出；水印与源数据(如图像、音频、视频数据)紧密结合并隐藏其中，成为源数据不可分离的一部分，并可以经历一些不破坏源数据使用价值或商用价值的操作而存活下来[7]。

1.1.6 数字水印技术特性

不同的应用场合对数字水印的要求不尽相同，一般认为数字水印技术应具有如下特点[1,2]：

① 可证明性：数字水印技术应能为受到版权保护的信息产品的归属提供完全可靠的证据。数字水印技术能够将所有者的有关信息（如注册的用户号码、产品标志或有意义的文字等）嵌入到被保护的对象中，并在需要的时候将这些信息提取出来。数字水印技术可以用来判别对象是否受到保护，并能够监视被保护数据的传播、真伪鉴别以及非法拷贝控制等。这实际上也是发展数字水印技术的基本动力。

② 不可感知性：不可感知性是指视觉或听觉上的不可感知性，即指载体数据因嵌入水印信号导致的变换对于观察者的视觉或听觉系统来讲应该是不可察觉的，最理想的情况是嵌入水印信号后的载体与原始载体在感觉上是一模一样的。不可感知性这是绝大多数数字水印技术所应达到的要求。

③ 鲁棒性（稳健性）：鲁棒性是指嵌入到被保护作品中的水印信号应该能够承受大量的物理和几何失真，包括有意的（如恶意攻击）或无意的（如图像压缩、滤波、打印、扫描与复印、噪声污染、尺寸变换等等）。显然在经过这些操作后，鲁棒的数字水印算法应仍能从含水印载体中提取出嵌入的水印信号或证明水印信号的存在。一个鲁棒的数字水印算法应做到若攻击者试图删除水印信号将会导致含水印信号载体的价值彻底破坏。

由于水印信号特性的要求对应用的依赖型很强，恰当的评价准则和具体的应用有关。许多文献中讨论的数字水印算法可能不具备上述所有特点，或者只具备部分上述特点。

1.2 数字水印技术的分类

随着数字水印技术的发展，数字水印技术的分类方法繁多[12,18,30-36]：

（1）按水印发展来分，可分为第一代数字水印技术和第二代数字水印技术。第一代数字水印技术是指水印信号往往是嵌入到一些变换域系数或采样点上，而第二代数字水印技术则是将水印信号嵌入到对被保护数字作品的感知部分。

（2）按嵌入的水印信号形式来分，可以分为一维数字水印技术和多维数字水印技术。嵌入到作品中的水印信号是一维信号的数字水印技术称为一维数字水印技术。如果水印信号是多维的数字水印技术称为多维数字水印技术。

（3）按特性来分，可分为脆弱性数字水印技术和鲁棒性数字水印技术。

脆弱性数字水印技术是指在原始真实信号中嵌入某种标记信息，通过鉴别这些标志信息的改动，达到对原始数据完整性检验的目的。因此，脆弱性水印技术应随着宿主信号的变动而做出相应的改变。鲁棒性水印技术则是能保证在宿主信号可能发生的各种失真变换下以及各种恶意攻击下，技术都具备很高的的抵抗能力。

（4）按载体分类，可分为图像数字水印技术、视频数字水印技术、音频数字水印技术和文档数字水印技术。随着数字技术的发展，会有更多类的数字媒体出现，同时也会产生更多相应的数字水印技术。

（5）从水印的嵌入域来分，可分为空间域（时空域）数字水印技术、变换域数字水印技术。时（空）域数字水印技术是直接在信号空间上叠加水印信息，具有较大的信息嵌入量，但鲁棒性较弱。变换域数字水印技术则分别是在 DCT、DFT 等频域、时/频变换域和小

波变换域上隐藏水印。变换域数字水印技术能较好的利用人类关键特性，具有较强的鲁棒性。

(6) 根据不同的用途划分，可分为证件防伪数字水印技术、版权标识数字水印技术、篡改提示水印技术等。证件防伪水印技术是一类比较特殊的水印。因为其要求检测的快速性，一般要求技术不能太复杂，而且要能抗打印扫描过程引起的几何失真和像素值失真。篡改提示水印技术是一种脆弱水印技术，其目的是标识宿主信号的完整性和真实性。

(7) 按内容划分，可以分为有意义数字水印技术和无意义数字水印技术。有意义数字水印技术是指水印信号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；无意义数字水印技术则只对应于一个序列号。对于无意义水印技术来说，如果解码后的水印信号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。

(8) 从外观上分类，可分为可见(可觉察)和不可见(不可觉察)数字水印技术。可见数字水印技术最常见的是有线电视上在播出节目上标上半透明标志(Logo)，其主要目的在于明确标识版权，防止非法使用。而不可见数字水印技术将水印隐藏，感官上无法察觉，目的是为了将来起诉非法使用者，作为起诉的证据，以增加起诉非法使用者的成功率，保护原创造者和所有者的版权。

(9) 根据所采用的用户密钥的不同分类，可以分为公钥数字水印技术、非公钥(私钥)数字水印技术。两个概念类似密码学中的公钥密码技术和私钥密码技术。私钥数字水印技术在加载水印和检测水印过程中采用同一密钥，因此，只有水印信号嵌入者才能检测水印，证明版权。而公钥数字水印技术则在水印的加载和检测过程中采用不同的密钥，由所有者用一个仅有其本人知道的密钥加载水印信号，加载了水印信号的载体可由任何知道公开密钥的人来进行检测。

1.3 水印技术的相关理论进展

1.3.1 水印算法结构

一般的数字水印算法的体系结构如图 1-1 所示[37]：

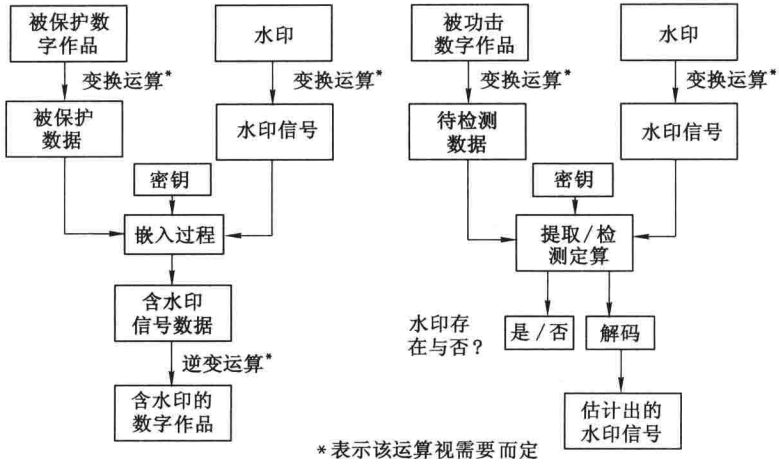


图 1-1 一般水印算法的体系结构

在嵌入水印过程中，被保护数字作品和要被嵌入的水印信号，在必要的时候需变换到合适的变换域中。在水印嵌入器中，利用密钥 K 将水印信号嵌入到被保护数字作品中。密钥 K 通过类似在数字媒体中随机产生嵌入位置等动作来保证算法的安全性。比较常见的方法是先将水印信号进行合适的扩频，然后再加载在被保护数字媒体信号上。被保护含水印作品在进行上述操作后，再进行逆变换转换为含水印的适合传输的数字作品。

在水印提取过程中，接收到可能被攻击的数字作品进行必要的转换。然后将其送入到水印检测器中（一般情况下，不需要原始的数字作品输入到水印检测器中）。而水印检测器一般设计为和水印信号相匹配的滤波器。滤波器一般具体设计为一个具有某个门限