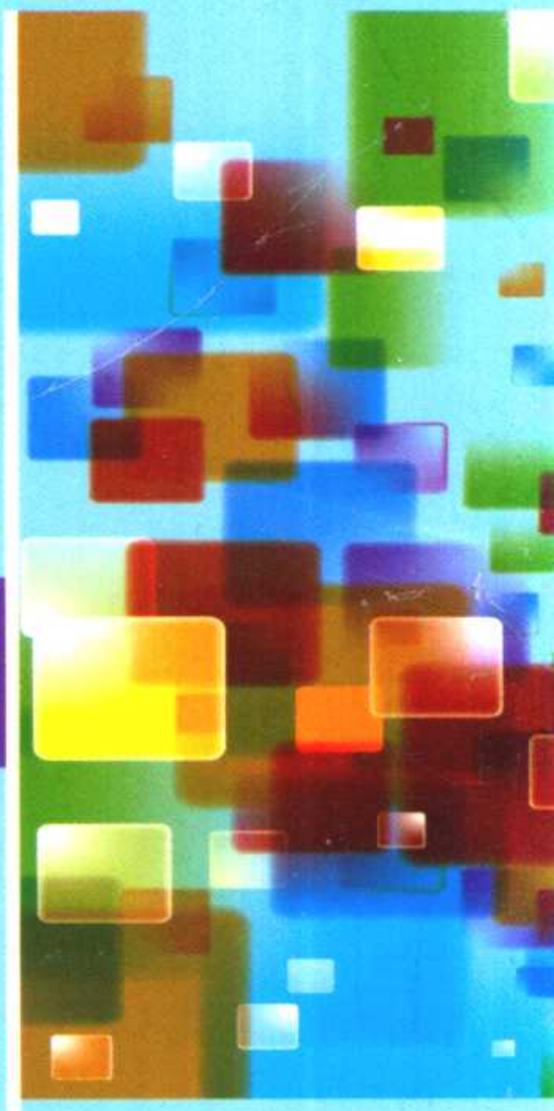
刘　丽　著

安全水印关键技术与应用

Anquan shuiyin guanjian jishu yu yingyong



电子科技大学出版社

安全水印关键技术与应用

刘　丽　著

电子科技大学出版社

图书在版编目(CIP)数据

安全水印关键技术与应用 / 刘丽著. —成都:电子科技大学出版社,2015.5
ISBN 978-7-5647-2985-1

Ⅰ.①安… Ⅱ.①刘… 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(2015)第 096754 号

安全水印关键技术与应用

刘 丽 著

出 版:电子科技大学出版社(成都市一环路东一段 159 号电子信息产业大厦 邮编:610051)
策划编辑:谭炜麟
责任编辑:谭炜麟
主 页:www.uestcp.com.cn
电子邮箱:uestcp@uestcp.com.cn
发 行:新华书店经销
印 刷:郑州宏达印务有限公司
成品尺寸:145mm×210mm 印张 7 字数 152 千字
版 次:2015 年 5 月第一版
印 次:2015 年 5 月第一次印刷
书 号:ISBN 978-7-5647-2985-1
定 价:20.00 元

前　言

数字水印通常被看成是信息安全领域的一项重要技术，近年来，水印的安全性越来越受到众多学者的关注。作为水印领域的一个新兴课题，水印的安全性已经成为一个亟待解决的问题，它给水印系统的设计带来了新的挑战。本书采用的技术与研究内容在现在及将来都有着较为广泛的应用前景，它不仅为水印理论转化为行业应用提供了新的思路，同时能够与电视广播网相结合，解决电视广播网在安全方面的瓶颈问题，为该技术在行业的应用带来了新的应用前景。因此，研究这种体系的安全水印系统有着较强的应用背景和现实意义。

本书总结了作者在完成河南省科技攻关项目、河南省教育厅科技攻关项目的过程中，在多媒体哈希、不同应用中安全视频水印算法、安全视频水印协议的设计等方面取得的研究成果。主要内容包括：对水印安全性中的一些重要问题展开研究，并将其与密码学研究进行对比；探讨水印安全性分析的框架；通过分析线性共谋攻击的数学模型，建立了有效抵抗线性共谋攻击的视频水印设计规则，并根据该规则提出能够有效抵抗线性共谋攻击的视频水印方案；基于三维离散小波变换提出新的安全视频哈希算法；借助于密码分析的思想，提出一个对多媒体哈希进行安全性分析的理论框架，该框架用 Shannon 理论中的唯一解距离度量提出哈希算法的安全级别，并在此过程中解决了提出的多媒体哈希算法的单向性证明问题，为进一步研究多媒体哈

希算法的安全性打下了良好的理论基础;考虑到版权保护应用中,存在敌手编辑一个水印放在作品中并声称他拥有版权,或者他将合法水印嵌入自己的作品中(拷贝攻击)这两个有关安全性攻击的问题,利用鲁棒水印技术提出一种具有多重保护目的的安全视频水印算法;考虑到广播监视应用中可能产生的欺诈行为,针对该应用中对水印提取的实时性要求较高的情况,本书利用通信分集技术提出一种适用于广播监视的空域安全视频水印算法;利用提出的框架以及现有的理论框架对算法的安全性进行了定量分析;分别基于同态公钥密码技术和安全嵌入技术提出两个应用于广播监视的安全视频水印协议,以解决水印协议中常见的消费者权利问题和非绑定问题,从而避免广播监视应用中广告商或广播电台的欺诈行为。

本书在撰写过程中得到了西南交通大学信息科学与技术学院彭代渊教授的指导;西南交通大学机械工程学院张祖涛副教授认真地审阅了全书,并提出了许多宝贵意见;电子科技大学出版社大力支持了本书的出版工作。此外,由于书中所含的专业知识和技术领域众多,并在撰写过程中引用了大量的国内外相关领域的最新成果和资料,许多朋友都为此书付出了辛勤的劳动,在此一并表示衷心感谢。

随着技术的进步和需求的变化,安全水印技术还会不断地发展,我们希望得到各位读者的支持,也期待与大家共同探讨安全水印技术的发展动向。由于我们水平有限,书中错误在所难免,欢迎读者批评指正。

刘　丽

2015 年 3 月

目　录

第1章 引 言

说起水印，人们自然会想到纸币中的水印，它可以起到防止伪造的作用。最早的水印就是指纸张中的水印。纸张的水印可以表明纸张的生产厂商和商标，也可以用于对纸张的式样、质量和强度的标识，还可以作为确定纸张的生产日期和鉴别的依据。在现代，纸张的水印被广泛应用于货币、证券和票据以及各种需要标识的纸张中，起到标识和防伪的作用。

伴随着信息产业的飞速发展和信息商品化意识深入人心，数字化信息产品面临新的严峻挑战——非法侵权盗版和恶意篡改。今天无论是独特创意的数字化作品，还是巨额投资而成的数字电影视盘，现代盗版者仅需轻点几下鼠标就可获得与原版完全一样的复制品，并以此谋取暴利。而一些具有特殊意义的信息，如涉及司法诉讼、政府机要等信息，则会遭到恶意攻击和篡改伪造。这一系列数字化技术本身特性所带来的负面效应，已成为信息产业健康持续发展的一大障碍。

现有版权保护系统多采用密码学技术对数字产品进行加密，只有合法用户（或付费用户）才拥有密钥，这样可以保证数字产品内容的安全传送，并且可以作为存取控制和征收费用的手段。但是，仅采用密码学技术存在一个重要问题，所加密的数字内容在解密之后，没有有效的手段来保证其不被非法拷贝、再次

传播和盗用;此外,数字形式的多媒体产品由于可以方便地完成复制并在网络环境下广泛散发,大范围的侵权拷贝行为受到了音像、出版、影视和软件等行业的高度关注。为了防止这种情况的发生,人们提出了数字水印技术。与纸币水印类似,这是一种将特制的不可见的标记,利用数字内嵌的方法隐藏在数字图像、声音、文档、图书、视频等数字产品中,用以证明原创作者对其作品的所有权,并作为鉴定、起诉非法侵权的证据,同时通过对水印的探测和分析保证数字信息的完整可靠性,从而成为知识产权保护和数字多媒体防伪的有效手段。[1,2]

1.1 研究背景

数字水印通常被看作是一项与安全有关的技术,然而许多研究者并不真正清楚水印安全指的是什么。在水印技术发展初期,水印的安全是指嵌入和提取过程由密钥控制。他们声称即使算法是公开的,但只要密钥不公开,那么该水印系统就是安全的。在密码术中攻破该密码系统意味着得到明文,而数字水印则不同,如未经授权的用户企图去除、检测(估计)、嵌入水印信号。作为水印领域的一个新兴课题,近几年来水印安全已经成为一个亟待解决的问题,它给水印系统的设计带来了新的挑战。

1.安全性

在许多水印应用中有必要相信那些通过水印信道传输的信息。当指纹水印被用来追踪那些恶意打破许可协议的用户时,版权拥有者主要想依靠那些提取的水印信息。因此,在这种情

况下，那些恶意用户想通过制作带伪造水印的多媒体内容是不可能的，从而避免清白的消费者遭陷害。另外，在作品分发系统中，指纹水印能够用来鉴别信息泄漏源，因此他们有可能遭受到攻击，所以在设计该系统的时候应尽可能地抵抗未经授权的去除攻击，即使攻击者能够成功检测或读取水印信息也不会有所影响；然而，当数字水印被用来进行隐蔽通信的时候，就不允许攻击者检测或读取水印信息。在这种情况下，水印信道被当作一个隐蔽的通信信道，而这个信道只有通信双方才知道。因此在隐蔽通信应用中，只要不知道密钥，就不能检测到水印；另外，从认证的角度看，水印信息未经授权的去除并不是真的很重要；在一个完全不同的机制中，我们可以利用水印在作品中插入有用信息，如注释水印、错误恢复水印。在这种情况下，改变水印很可能会去除相关的有用信息或相关服务。

总之，一些利用水印技术的应用环境是值得仔细研究的。根据不同的有针对性的应用，消费者不能利用同样的水印技术，而应该采用对该应用有针对性的水印技术。一般来讲，消费者越是干扰水印，他们的行为越是恶劣，水印所需要的安全规格也就越高。因此，当遇到两种情况的时候，安全问题就自然而然的产生了：一种情况是多媒体内容提供商在其提供的作品中加入水印，并期望嵌入的水印能够提供一些服务。如拷贝控制应用中，如果未经许可就不能拷贝多媒体内容；在多媒体内容分发系统中，追踪鉴别泄漏信息的叛徒等。另一种情况是消费者主动向水印系统窜扰，采用恶劣的方法击败保护系统。换言之，安全性的讨论本来就是在相信恶劣条件下进行的，在研究水印系统的时候，这是一个值得考虑的关键性问题。特别是在有关知识

产权保护的应用中，应该能够鉴别哪些操作危险哪些不危险。不过值得提醒的是，许多利用鲁棒水印技术的应用系统中根本没有考虑安全规格问题。

2. 区分鲁棒性和安全性

在鲁棒数字水印技术中常见的两个主要概念是鲁棒性和安全性，而这两个概念已经被混淆好长时间了。一个显而易见的不同点是安全性中需要假设一个恶劣的环境，而鲁棒性则不需要。鲁棒性针对的是常规信号处理的攻击。一个最典型的例子就是：为了存储和传输的方便而对视频进行压缩不能被看作是对安全性的威胁，尽管有损压缩降低了水印提取的正确率。关键点在于消费者不是有意去除水印的。简要地说，鲁棒性是一般消费者所关心的问题，而安全性则是部分试图攻击系统的黑客所关心的问题。另外一个区别是通常安全性攻击的目的是获取一些被保护系统的相关信息。对一幅图像进行 JPEG 压缩的消费者与那些集结大量含水印作品以检查是否有信息泄漏的恶意攻击者是有明显区别的，后者可以检测、去除或者编辑水印信息。可以说鲁棒性攻击比安全性攻击更具一般性。鲁棒性与安全性的第三个区别是鲁棒性仅与水印去除有关，而安全性不仅与未经授权的去除有关，还与未经授权的检测、嵌入和编辑有关。概括地说，鲁棒性指的是在经过常规的信号处理操作后，仍能够检测到水印的能力；而安全性是指它抵御敌手攻击（敌手攻击是指专门为了阻碍水印用途的处理）的能力。

依据所研究的攻击是属于鲁棒性问题还是安全性问题，水印攻击的分类如图 1-1 所示。[3,4] 针对鲁棒性的攻击被分为同步攻击和非同步攻击。同步攻击指的是一般的信号处理，如滤波、有损压缩和去噪等那些有可能直接阻碍检测器检测水印信号的

攻击。非同步攻击指的是那些所有扰乱信号采样位置的操作。这种攻击没有真正的去除水印信号，但是由于检测器无法提取出水印，所以它仍然被看成是水印去除攻击。针对安全性的攻击被分为协议攻击和密码攻击。协议攻击试图生成一个伪数据源、伪水印化数据来混淆含有真正水印的数字作品的版权，使水印检测的结果错误或出现偏差。例如，在版权保护应用中，如果媒体作品中发现载有一个以上的水印，就称为死锁攻击，这种情况下没有人能够声称他拥有作品的版权。密码攻击的目的是获得一些有关水印信号的信息，如密钥或所用的伪随机序列。蛮力攻击是搜索所有可能的密钥，直到搜索到真正的密钥为止。在数字水印的很多领域，攻击者可以通过网络访问到水印检测器，在这种情况下，即使攻击者不知道水印的嵌入方法，仍可以利用检测器返回的信息来破坏水印，使检测器无法检测出有效的水印，这种攻击称为 Oracle 攻击。统计攻击主要指的是共谋攻击，即集合一些含水印的作品，然后组合分析他们以获得不含水印的版本。最后是被大多数人所熟知的拷贝攻击，它是敌手将水印从一个作品拷贝到另一个作品的攻击方法。

图 1-1 依据其属于鲁棒性问题还是安全性问题对水印攻击分类

3. 现实生活中的安全性

众所周知，一个完全安全的系统是不存在的。如果一个有动机的攻击者在没有时间、金钱以及计算量限制的条件下，那么他就能够成功击败一个保护系统（如蛮力攻击），数字水印领域也是如此。那么这是否意味着安全是无用的呢？回答是否定的。例如，在 DVD 分发应用中的拷贝保护：当版权拥有者发放一个新的影片时，他们知道大部分的销售额都将在头几个月完成。因此，他们都希望拷贝保护机制能够持续几个月，这几个月后是否有盗版行为发生，版权拥有者就不关心了。如果这个保护机制持续的时间足够长，那么那些渴望得到新发布影片的消费者就等不到盗版出现在网络上，而自己去购买正版影片了。还有很重要的一点是，攻击者能够攻破一个系统并不意味着他能够有效地做到这一点。总之，在现实生活中重要的是攻破一个系统的代价（如复杂度、时间和金钱花费等）应该高于合法应用该系统的代价。

回到现实中，金钱花费是不得不考虑的。谁将付费引进这个安全保护系统呢？这是一个很关键的问题，也是有关各方面的分歧所在。我们考虑三个典型的实体：多媒体作品拥有者，电子消费品制造商和消费者协会。多媒体作品拥有者一旦将他们的作品公布于众，就想保护他们的多媒体作品，但是他们大部分都不愿意承担这个保护系统的所有花费。从制造商的角度看，越安全意味着需要越多的硬件、软件和更昂贵的设备，从而使销售额下降，利润减少。当然，消费者并不真正热心于给那些安全机制缴费。这种利益冲突将他们带进了一条死胡同。例如在那些已经几乎被遗弃的 DVD 光盘中利用数字水印技术，当遇到危

急情况时,保护技术的效率应该与经济利益相折中。如果风险处理得当,一些不安全的技术也是值得青睐的。[5]尽管信用卡网络利用了不安全的磁条技术,但是风险管理工具仍然能够将欺诈率保持在交易量的0.1%以下。

4.共谋攻击

共谋攻击是一个很著名的攻击机制,它主要是指一些恶意消费者聚集他们各自的有关保护系统的相关信息,以获得未被保护的作品。它最早出现在密码技术中——建立一个协议,在不同的个体中分配秘密信息,如秘密共享(也被称为门限密码)、会议密钥等。秘密共享的主要思想是:当符合要求的若干参与者合作时,利用他们所保管的片段采用一定的算法可以恢复原始的秘密信息K,而不符合要求的若干参与者合作则恢复不了秘密信息K。任何的秘密共享,必定牵涉多人的团体,以及多人共享的秘密。银行保险柜账户即是秘密共享的一个很好的例证,只有在同时得到消费者密钥和银行管理员的密钥时,才能够访问该账号。一个人要想进入一个绝密实验室必须要有通行卡,并且只有当一个安全警卫的通行卡和一名实验室研究人员的通行卡同时出具时才允许进入该实验室。又由于实验室里有许多警卫和研究员,这导致了通行卡被分成两组,从这两组中任意各抽取一张通行卡就可以进入该实验室。从更广泛的角度来看,秘密共享分离个体之间的信息,以至于任意少于m个参与者都不能恢复原始的秘密信息K。在这个框架下,c个共谋者试图伪造一个秘密信息,甚至想在$c<m$的情况下重构秘密信息。秘密共享可以被看作是一种密钥预分配技术,其中被重构的秘密信息是静态的,且对所有的组该秘密信息都是相同的。而会

议密钥则不同，它允许有会话密钥，即使用一个单独的密钥对一次单独的会话加密。一般来说，一个会话密钥只在一个具体的通信中使用，即在会话开始前建立会话密钥，然后使用这个共享的会话密钥进行通信，会话密钥只使用于通信期间，下次通信再重新启用一个新的会话密钥。在这种机制中，共谋者的目标是产生一些新的密钥，以便他们不用付费的参与会话。

在数字水印中，共谋攻击最早出现在操作跟踪应用中。[6]在这种应用中，版权拥有者想将他们的作品分发给大量的消费者，但是又担心他们的版权，从而想追踪作品的泄漏源。为此，他们不分配给消费者完全一样的作品，而是分配略有差别的作品给每个消费者。这样每个消费者都拥有一个独一无二的副本，每个副本都含有一个自己的可以追踪泄漏源的水印标识。因此，如果一个消费者把他的副本随意地放在网上，版权拥有者就能够利用其中的水印标识追查到作品泄漏者的身份。在这种情况下，几个用户(共谋者)或者结合几个含水印作品直接估计出原始的不含水印作品，或者估计出水印信号的一些特性以达到删除或陷害其他无罪用户的目的，如图 1-2 所示。已有一些文献对此提出了解决的方案。但是，当考虑视频作品时，对共谋攻击的研究则更具挑战性。

综上所述，今后我们在设计鲁棒水印系统的时候，应该仔细研究该技术的应用环境，该环境下可能遇到的攻击，不能只考虑增强鲁棒性，还应考虑如何增强安全性。而且，不能一味地为了增强系统的性能，也要结合现实生活中的各种实际情况(如复杂度、金钱等)来设计水印系统。