图形图像

数字水印算法

Digital Watermarking Algorithms for Image and Graphic

王 勋 金剑秋 章志勇 著

科学技术文献出版社

图形图像数字水印算法

王　勋　金剑秋　章志勇　著

科学技术文献出版社

图书在版编目(CIP)数据

图形图像数字水印算法 / 王勋，金剑秋，章志勇著. —北京：科学技术文献出版社，2010.11

ISBN 978-7-5023-6775-6

Ⅰ. ①图… Ⅱ. ①王…②金…③章… Ⅲ. ①电子计算机—密码术—研究生—教学参考资料 Ⅳ. ① TP309.7

中国版本图书馆 CIP 数据核字(2010)第 214343 号

出　版　者	科学技术文献出版社
地　　址	北京市复兴路 15 号(中央电视台西侧)/100038
图书编务部电话	(010)51501739
图书发行部电话	(010)51501729,(010)68511035(传真)
邮购部电话	(010)51501729
网　　址	http://www.stdph.com
	E-mail: stdph@istic.ac.cn
责任编辑	科　文
发　行　者	科学技术文献出版社
排　　版	杭州朝曦图文设计有限公司
印　刷　者	杭州杭新印务有限公司
版(印)次	2010 年 11 月第 1 版第 1 次印刷
开　　本	787×960　1/16
字　　数	216 千字
印　　张	13.25
定　　价	28.00 元

前　言

随着计算机技术的发展、媒体的数字化和互联网的迅速普及，数字多媒体信息（图像、文本、音频、视频、三维模型）的存储、复制与传播变得非常方便，但这也带来了两个方面的问题：一是数字媒体的完美复制和无代价分发带来的版权保护问题；二是数字媒体在传输过程中可能遭受各种有意无意的篡改，如何保证媒体内容的真实性和完整性是另一个亟待解决的问题。

密码技术是信息安全技术领域的主要传统技术之一，其保护方式都是控制文件的存取，即将文件加密成密文，使非法用户不能解读。但是，传统的加密方法对多媒体版权和内容的保护及完整性认证具有一定的局限性。首先，随着计算机处理能力的快速提高，这种通过不断增加密钥长度来提高系统密级的方法变得越来越不安全；其次，加密方法只能保护在通信信道中的安全，一旦被解密，则完全失去了保护性；此外，密码学中的完整性认证是通过数字签名方式实现的，它并不是直接嵌到多媒体信息之中，因此无法察觉信息在经过加密系统之后的再次传播与内容的改变。

针对上述领域应用问题和研究背景，研究人员尝试用各种信号处理方法对音像数据进行隐藏加密，并将该技术用于制作多媒体的“数字水印”。这样，数字水印技术作为加密技术的补充，在多媒体信息的版权保护与完整性认证方面得到迅猛发展。数字水印技术通过在被保护的数字对象中嵌入某些秘密信息－水印（Watermark）来证明版权归属或跟踪侵权行为。它通过一定的算法将一些标志性信息直接嵌到多媒体内容当中，但不影响原内容的价值和使用，并且不能被人的感知系统察觉，也很难被清除。它旨在解决多媒体信息内容的版权保护问题（鲁棒水印），以及多媒体信息内容的真实性与完整性认证问题（脆弱和半脆弱水印）。与加密技术不同，数字水印技术并不能阻止盗版活动的发生，但它可以判别对象是否受到保护，监视被保护数据的传播、真伪鉴别和非法拷贝，解决版权纠纷并为法庭提供证据。

从1994年Van Schyndel等人在ICIP国际会议上发表*A Digital Watermarking*开始，数字水印技术受到了国际上众多著名研究机构的广泛关注，如IBM、三菱电机、NEC等。从最初的数字图像水印研究，到现在已经扩展到音频、视频、数字地图和三维模型等水印算法的研究。经过这十余年的发展，数字水印技术已经形成了从基本概念、相关理论基础到实用算法、技术标准和安全交易模型等一系列较为成熟的学科框架。但在水印的安全性、鲁棒性、抗攻击能力，以及计算复杂性等问题上仍有许多亟待解决的问题，数字水印技术的研究仍然十分活跃。

我们在多个基金的资助下，从2000年开始展开了水印算法相关课题的研究，在鲁棒图像水印算法、半脆弱图像水印算法、栅格地图水印算法、矢量地图水印算法和三维模型水印算法等方面取得了一定的研究成果，并在半脆弱图像水印算法的基础上，给出完整的基于互联网的安全交易模型，同时综述了数字水印技术的历史发展、最新成果以及存在的问题。本书第一章简要介绍了数字水印技术的基本概念、相关理论基础及主要应用，阐述了水印攻击方法及系统评价标准。第二章在介绍图像鲁棒数字水印的相关算法基础上，给出了一个基于成分分离的鲁棒图像水印算法。第三章主要讨论用于完整性认证的图像半脆弱水印算法，并给出了一种基于半脆弱水印的安全交易模型。第四章介绍栅格地图水印算法，在综述前人工作的基础上，给出了互补栅格地图水印算法和基于小波变换的遥感图像盲水印算法。第五章围绕矢量地图水印算法，详细给出了基于双重嵌入机制的鲁棒矢量地图水印算法、基于DCT域的矢量地图盲水印方法、基于B样条的等高线地图水印算法和二维矢量地图特征的零水印算法。第六章讲述三维网格模型水印算法，讨论三维模型水印与其他载体水印的不同之处与难点，并具体给出在球面参数化基础上，利用球面小波变换的网格模型水印算法，以及利用Nielson仿射不变量的三维模型盲水印算法。由于作者水平有限，再加上数字水印文献众多，内容涉及信号处理、数学、通信等多个学科，书中许多看法观点是我们在这个领域的一己之见，难免有失偏颇，欢迎广大读者批评指正。

可以说，本书是我们在该领域几年来研究工作的小结，也是浙江工商大学信息处理与可视计算重点实验室近些年来集体工作的结晶。全书的理论和算法成果实现得到了浙江省重大科技专项“面向GIS应用的通用城市空间数据处理平台开发与安全研究(2006C13098)”、“地理

空间数据共享利用的若干关键技术研究与应用(2009C11034)”等项目经费的支持。本书第1、3、4、5章由浙江工商大学王勋教授撰写，第2章由王勋教授、章志勇副教授共同撰写，第6章由王勋教授、金剑秋副教授共同撰写。全书由王勋教授负责整体结构设计、内容安排和全部审校工作，并最后审定。本书的最终完成还要特别感谢浙江大学的鲍虎军教授与林海教授、浙江工商大学的凌云教授等的指导与帮助，感谢黄定军、孙海涛、林传峰等研究生在数字图像采集和程序实现中所付出的辛勤劳动。

本书得以正式出版，并以较快的速度与读者见面，这与参与撰写的老师及出版社编辑的辛勤工作是分不开的，在此一并表示诚挚的感谢！

非常感谢在本书完成过程中给予帮助的人们，我们也感谢为修正和充实本书提供宝贵意见的各位同仁。

由于著者水平有限，书中不妥之处在所难免，恳求读者批评指正。

作　者

2010年9月6日于浙江工商大学

目 录

第一章 绪 论

1.1 研究背景

计算机技术的发展在方便人们处理信息的同时，也给信息的安全提出更加严峻的考验：计算机使人们能够非常方便地编辑、修改、存储和传播数字媒体信息，但一些个人或团体受利益驱动，在未经所有者许可的条件下擅自篡改数字媒体内容；或者在传输过程中，遭受各种有意无意的篡改攻击，使得人们对数字媒体的完整性和内容的真实性产生质疑。如果篡改的内容涉及到国家安全、法庭举证、历史文献等重要媒体数据，将会造成不良的社会影响甚至导致重大的政治、经济损失。因此，如何在互联网环境下，对数字媒体内容的真实性、完整性实施有效认证具有重要的研究意义和应用价值[1-6]。

随着互联网的迅速普及，基于 web 服务的各种应用日益增长，使得多媒体信息的交流达到前所未有的广度和深度，其发布与传播的形式也愈加丰富。今天，数码相机、录像机、扫描仪和打印机等硬件数字处理设备和功能强大的软件，已被广泛地应用于创作、处理和共享数字媒体（图像、图形、音频和视频等）；互联网已经成为信息发布的重要媒介，为数字媒体信息的分发和交换提供了广阔而便捷的渠道。然而，数字媒体信息这种近乎完美的复制和几乎无代价的分发，带来了一个严重的版权保护问题。如何既能充分利用现代计算机技术带来的便利，又能实现有效的版权保护成为一个急需解决的现实问题[7-9]。

综上所述，数字媒体产品安全保护已经成为一个迫在眉睫的问题，通常的保护包含两个方面的内容：一是数字媒体内容的真实性、完整性认证，二是数字媒体版权保护。现阶段，解决数字媒体以上两方面问题的主要方法有：信息加密、数字签名和信息隐藏。

加密技术将明文消息变换成旁人无法理解的密文消息，从而达到控制数据访问。或者通过设置密码，使得数据在传输时变得不可读，从

而可以为处于从发送到接收过程中的数据提供有效的保护。数字签名是用“0”、“1”字符串来代替书写签名或印章，具有书写签名或印章同样的法律作用。它可以分为通用签名和仲裁签名两种方式。数字签名技术已经用于检验短数字信息的真实可靠性[10]，并已形成了数字签名标准(Digital Signature Standard, DSS)[11]。它通过使用私用密钥对每个消息进行签名，而公共的检测算法用来检查消息的内容是否符合相应的签名。但这种签名在数字图像、视频或音频中的应用并不方便也不实际，因为在原始数据中需要加入大量的签名。另外，随着电脑软硬件技术的迅速发展以及基于网络的具有并行计算能力的破解技术的日渐成熟，这些传统系统的安全性已经受到质疑。同时，一旦信息被非法破密，就没有任何直接证据来证明信息被非法复制和转发。再者，对于少数人来说，加密具有挑战性，因为人们很难防止一个加密文件在解密时被“剪掉”。因此，需要寻求一种不同于传统技术的更加有效的手段，来保障数字媒体的安全传输和保护数字产品的版权。

数字水印技术作为加密技术的一种有效补充，一方面弥补了密码技术的缺陷，因为它可以为解密后的数据提供进一步的保护；另一方面，数字水印技术也弥补了数字签名技术的缺陷，因为它可以在原始数据中一次性嵌入大量的秘密信息。人们可以设计某种水印，它在解密、再加密、压缩、数模转化以及文件格式变化等操作下保持完好。数字水印可分为脆弱水印和鲁棒水印，其分别被应用于真实性认证和版权保护。此外，数字水印技术还被广泛地应用于广播监控、交易跟踪、真伪鉴别、拷贝控制等。

1.1.1 信息论基础

1. 信息熵

根据贝尔实验室的著名科学家 Claude E. Shannon 的研究，一个具有符号集的信息源 $S=\{s_1, s_2, s_3, \cdots, s_n\}$ 的熵(Entropy)η 定义为：

$$\eta = H(S) = \sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i} = -\sum_{i-1}^{n} p_i \log_2 p_i \tag{1.1}$$

其中 p_i 是 S 中符号 s_i 出现的概率。

$\log_2 \frac{1}{p_i}$ 表明了包含在 s_i 中的信息量(即自信息量)，它与对 s_i 进行编码所需的位数相等。例如，如果在一分稿件中出现字符 n 的概率为 1/32，则这个字符包含信息量是 5 位。换句话说，需要使用 15 位对字

符串 *nnn* 编码。

因此，熵是对一个系统的无序性(Disorder)的度量。熵越大，系统越无序。一般来说，当我们希望系统更有序时，我们会给系统增加负熵。如，对一叠纸牌进行排序(假设采用冒泡排序)，对于每一次交换或不交换的决策，我们将为纸牌增加 1 位的信息量，并且为这叠纸牌传送了 1 位的负熵。

熵定义包含了这样的思想：两次决策意味着在以 2 为底的对数中传输两次负熵。一个 2 位的向量可以有 2^2 种状态，而对数将把这个值转换成 2 位的负熵。两次决策会引起两倍的熵的改变。

现在，假设希望通过网络来传送这些交换决策，那么必须发送 2 位来表示两次决策。如果我们有一个两次决策系统，那么，所有这样的传送所需的平均位数也是 2 位。如果我们愿意，可以把 2 位系统中可能的状态数看作 4 个输出结果，每个结果具有 1/4 的概率。所以平均来说，传送每个结果所需发送的位数为 $4\times(1/4)\times\log((1/(1/4)))=2$ 位，即要传送两次决策的结果，我们需要传送 2 位。

但是如果某个结果的概率高于其他的结果，则我们发送的平均位数将会有所不同。假设我们的四个状态中某个状态的概率为 1/2，而其他三个状态发生的概率分别为 1/6。为了对平均发送位数模型进行扩展，我们不得不借助于 2 的非整数次幂来表示概率。然后使用对数来计算需要多少位来传送信息内容。根据式(1.1)，需要传送 $(1/2)\times\log_2(2)+3\times(1/6)\times\log_2(6)=1.7925$ 位，比 2 位要少。这反映出如果能够对我们的四个状态进行编码，并且使出现概率最高的一个状态用较少的位数来传送，那么就可以实现用更少的位来传送平均值。

熵定义旨在从数据流中识别出经常出现的符号作为压缩流中的候选短码字，也就是说使用变长编码方案进行熵编码，即给频繁出现的符号分配能够快速传输的码字，而给不经常出现的符号分配较长的码字。如，在英语中 E 频繁出现，所以应该给 E 赋予比其他字母(如 Q)更短的码字。

2. 互信息

信源产生的随机变量包括 2 个符号 $S=\{s_1,s_2,s_3,\cdots,s_n\}$ 和 $T=\{t_1,t_2,t_3,\cdots,t_n\}$，则接收到该序列后所获得的平均信息量称为联合熵，定义为：

$$H(S\cdot T)=-\sum_i\sum_j r_{ij}\log_2 r_{ij} \tag{1.2}$$

式中，r_{ij} 是符号 s_i 和 t_j 同时发生时的联合概率。

假设 S 和 T 相互独立，则联合概率 $r_{ij}=p_iq_j$，(1.2)式可定义为：

$$H(S\cdot T)=H(S)+H(T) \tag{1.3}$$

假设 S 和 T 是相关的，则联合概率 $r_{ij}=p_iP_{ji}=q_jP_{ij}$，其中 $P_{ji}=P(t_j/s_i)$ 和 $P_{ij}=P(s_i/t_j)$ 为条件概率。

在给定 S 的条件下，T 所具有的熵称为条件熵，即

$$H(T/S)=<-\log_2 P_{ji}>=-\sum_{i=1}^{n}\sum_{j=1}^{m}r_{ij}\log_2(r_{ij}/p_i) \tag{1.4}$$

上式中在对 $-\log_2 P_{ji}$ 进行统计平均时，由于要对 s_i 和 t_j 进行两次平均，所以用的是联合概率 r_{ij}。利用(1.2)式和 1.4 式以及联合概率与条件概率之间的关系，可以得到联合熵与条件熵存在下述关系：

$$H(S\cdot T)=H(S)+H(T/S)=H(T)+H(S/T) \tag{1.5}$$

上式表明，如果 S 和 T 之间存在着一定的关联，那么当 S 发生，在解除 S 的不肯定性的同时，也解除了一部分 T 的不肯定性。但此时 T 还残余有部分的不肯定性，这就是 1.5 式中 $H(T/S)$ 的含义。我们把无条件熵和条件熵之差定义为互信息，即

$$I(S;T)=H(T)-H(T/S) \tag{1.6}$$

$$I(T;S)=H(S)-H(S/T) \tag{1.7}$$

显然，$I(S;T)=I(T;S)\geqslant 0$。

两个事件的相关性越小，互信息越小，残余的不确定性便越大。当两事件相互独立时，S 的出现，丝毫不能解除 T 的不肯定性。在这种情况下，联合熵变为 2 个独立熵之和(见 1.3 式)，从而达到它的最大值。图 1.1 给出了无条件熵、条件熵和互信息之间关系的示意。

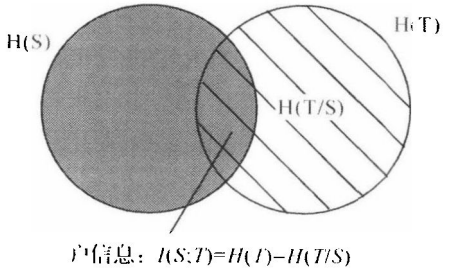

图 1.1　无条件熵、条件熵和互信息之间的关系

1.1.2 信息加密技术

信息加密技术是信息安全领域的核心技术，是在编码与破译的矛盾中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术。随着计算机网络不断渗透到各个领域，加密技术的应用也随之扩大，如数字签名、身份鉴别等都是由加密技术派生出来的新技术和应用。

密码学(Cryptology)是研究编制密码和破译密码的技术科学。它包括密码编码学(Cryptography)和密码分析学(Cryptanalysis)两个相互对立又相互促进的分支。密码编码学是研究编制密码使消息保密的技术科学。密码分析学是研究如何破译密码获得原始消息的技术科学。在密码学中，通常把待加密的消息称为明文(Plaintext)，加密后的消息称为密文(Cipheretext)。加密(Encryption)就是从明文得到密文的过程；而合法地由密文恢复出明文的过程称为解密(Decryption)。加密和解密所采用的算法分别称为加密算法(Encryption Algorithm)和解密算法(Decryption Algorithm)。加密和解密算法统称为密码算法。各种密码算法进行明密变换所依据的法则称为密码体制。实现这种变换过程需要输入的参数称为密钥(Key)。根据密码算法所使用的加密密钥和解密密钥是否相同、能否由加密过程推导出解密过程(或者由解密过程推导出加密过程)，可将密码体制分为对称密码体制和非对称密码体制。如果一个加密系统的加密密钥和解密密钥相同，或者虽然不相同，但是由其中的任意一个可以很容易地推导出另一个，则该系统所采用的就是对称密码体制。对称密码体制的优点是具有很高的保密强度，可以经受较高级破译力量的分析和攻击。但它的密钥必须通过安全可靠的途径传递，密钥管理成为影响系统安全的关键性因素，使它难以满足系统的开放性要求。如果一个加密系统的加密和解密的过程分开，加密和解密分别用两个不同的密钥实现，并且不可能由加密密钥推导出解密密钥(或者不可能由解密密钥推导出加密密钥)，则该系统所采用的就是非对称密码体制。采用非对称密码体制的每个用户都有一对选定的密钥，其中一个是可以公开的，另一个由用户自己保存。非对称密码体制的主要优点是可以适应开放性的使用环境，密钥管理问题相对简单，可以方便安全地实现数字签名和验证。

在密码学研究中，人们习惯根据英文的开头两个字母 A 和 B，把通信的双方分别称为 Alice 和 Bob。根据 Eavesdropper(偷听者)的第一

个字母 E，把企图偷听 Alice 和 Bob 之间通信的人称为 Eve；也称 Eve 为被动攻击者。根据 Malicious(怀恶意的)的第一个字母 M，把可能篡改和仿造消息的恶意窃听者称为 Mallet；也称 Mallet 为主动攻击者。被动攻击的隐蔽性很强，而主动攻击的破坏性大。如图 1.2 是密码通信系统结构示意图。

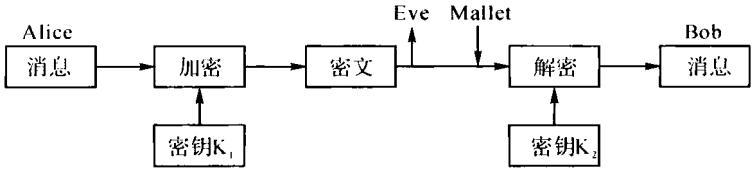

图 1.2　密码通信系统模型

传统的加密算法一般是基于文本数据设计的，它把一段有意义的数据流(即明文)转换成看起来没有意义的数据(即密文)，如 DES(数据加密标准，Data Encryption Standard)。该技术通过将明文加密成密文，使得在网络传递过程中非法拦截者无法从中获得信息，从而达到保密的目的。

虽然也可以把多媒体数据作为文本数据流一样看待，使用传统的加密算法进行加密，但是多媒体数据流的特性与文本数据有很大不同。在传统加密方法中，为保证安全性，一般主要依靠密钥以非常复杂的方式控制替换过程，对于数据量极为庞大的多媒体数据流而言，难以实现快速的加、解密算法，也就无法满足多媒体应用中的实时性等要求。考虑到数字图像所特有的大数据量与自相关性，必须针对多媒体信息的特点，研究适合多媒体信息的加密技术。近年来，在这方面的研究取得了一些成果，主要针对视频数据和图像数据[12-17]。

传统的加密方法一直被认为是通信领域的主要信息安全手段而受到极大重视，但近年来人们逐步认识到其对多媒体内容的保护和完整性认证具有一定的局限性。首先，加密方法只用在通信的信道中，密文数据因其不可理解性妨碍了多媒体信息的传播；其次，多媒体信息经过加密后容易引起攻击者的好奇和注意，并有被破解的可能；而一旦被破解，其内容完全透明，版权所有者就失去了对盗版的任何控制权；另外，密码学中的完整性认证是通过数字签名方式实现的，它并不是直接嵌到多媒体信息之中，因此无法察觉信息在经过解密之后的再次传播中内容的改变，最后，多媒体内容的完整性认证往往需要容忍一定程度的

失真，而密码学中的认证不允许被保护的内容有任何一个比特的改变。因此，基于加密技术的多媒体版权保护和完整性认证有其严重的缺陷，亟待寻求一种新的技术来弥补其不足。

1.1.3 信息隐藏技术

1. 信息隐藏概述

信息隐藏(Information Hiding)是指将机密信息秘密地隐藏于另一非机密的信息中散发出去，用以跟踪侵权行为并提供法律保护的证据，其形式可以为任何一种数字媒体，如文本、图像、图形、音频和视频等。它除了要求隐藏算法要好，隐藏的信息令人难以察觉外，还要求有高的机密信息安全性，即当作为机密信息载体的非机密信息被非法截获后，任何非法的破解动作都会导致机密信息的破坏。

一般而言，现代信息隐藏学开端于 1996 年 5 月在英国剑桥大学召开的第一届国际信息隐藏研讨会[18]，在这之后，信息隐藏技术在数字媒体这个崭新的领域获到广泛研究和应用。在信息隐藏学中，待隐藏的信息为秘密信息(Secret Message)，它可以是版权信息或其他秘密数据，比如说一个序列号；而公开信息则称为载体信息(Cover Message)，如视频、音频片段。而信息隐藏过程一般由密钥来控制，通过嵌入算法(Embedding Algorithm)将秘密信息隐藏到公开信息中，而隐蔽载体(隐藏有秘密信息的公开信息)则通过信道(Communication Channel)传递，最后检测器(Detector)利用密钥从隐蔽载体中提取/检测出秘密信息，其隐藏与提取过程可表示为如图 1.3 所示：

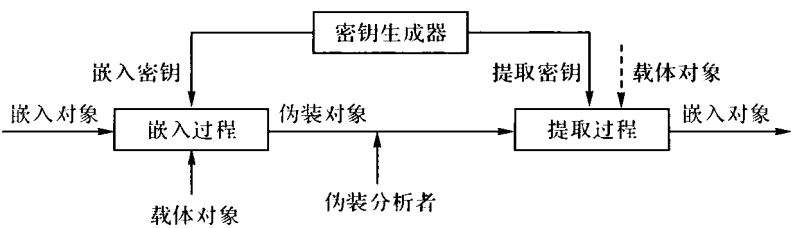

图 1.3 信息隐藏系统模型

上图中的“对象”可以是“消息”、“音频”、“视频”、“图像”、“文本”等。嵌入对象是信息隐藏嵌入过程的输入之一，指需要被隐藏在其他载体之中的对象。嵌入对象将在提取过程中被恢复出来，但由于隐藏对象在传输过程中有可能受到伪装分析者的攻击，提取过程往往只能