－吉林财经大学资助出版图书－

基于隐藏容量的
数字图像信息隐藏算法

韩佳伶◎著

Digital Image Information Hiding Algorithms Based on Hiding Capacity

科学出版社

吉林财经大学资助出版图书

基于隐藏容量的数字图像信息隐藏算法

韩佳伶 著

科学出版社

北京

内 容 简 介

本书主要对数字图像信息隐藏算法进行系统的研究，针对信息隐藏算法中提高隐藏容量的关键问题，提出解决方案并进行仿真实验和分析。主要研究工作如下：在宿主图像分析中，分析人类视觉系统对图像的掩蔽特性，分别对宿主图像中两类不敏感区域进行筛选，并提出结合两类不敏感区域的综合区域筛选方法，利用阈值确定掩蔽区的数量，决定嵌入容量的大小。为了更大限度地去除冗余，合理有效地利用载体图像的空间，嵌入有用信息，提出在秘密图像信息嵌入之前，利用图像像素间的相关性构建编码器来进行预测，通过消除像素之间的冗余度达到压缩的目的。

本书可供从事计算机技术与工程、信息技术等领域，以及关注信息传输安全、多媒体版权保护的工程技术人员和教学科研人员参考，也适合高等院校信息隐藏研究、图像处理等相关专业的硕士生与博士生阅读。

图书在版编目（CIP）数据

基于隐藏容量的数字图像信息隐藏算法/韩佳伶著. —北京：科学出版社，2017.10

ISBN 978-7-03-054738-5

Ⅰ. ①基… Ⅱ. ①韩… Ⅲ. ①计算机保密–数据保密–算法–研究 Ⅳ. ①TP309.2

中国版本图书馆 CIP 数据核字（2017）第 246371 号

责任编辑：王喜军 / 责任校对：王 瑞
责任印制：吴兆东 / 封面设计：壹选文化

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http：//www.sciencep.com

北京虎彩则铭印刷科技有限公司印刷
科学出版社发行 各地新华书店经销

*

2017 年 10 月第 一 版 开本：720 × 1000 1/16
2017 年 10 月第一次印刷 印张：8 1/4
字数：164 000

定价：68.00 元

（如有印装质量问题，我社负责调换）

前　言

计算机技术的快速发展和网络应用的迅速普及，使人们的生活和工作变得更加方便，为数字化信息的传播开辟了新的道路。大量的数字文件作为通信、沟通的主要载体，在网络上传输和共享。随之而来出现了一系列的安全问题，人们对通信的安全保密性提出了更高的要求。传统的保密通信通过对通信内容加密成密文来达到保密信息的目的，但容易引起监听者的注意。信息隐藏技术在这种情况下应运而生，它将要传输的秘密信息隐藏到不容易引起监听者注意的宿主信息中，并把隐藏后的信息作为传输对象，使其在传输过程中不易被发现。作为信息隐藏的宿主，图像的冗余空间相对较大，是目前使用最多的隐藏载体。信息隐藏技术应用的不同目的，要求它应分别具备不可感知性、安全性、不可检测性、鲁棒性、高嵌入容量等不同特性。对一般的信息隐藏系统而言，不可感知性、鲁棒性和嵌入容量三个指标之间通常是互相制约的。

本书是作者多年来科研成果的总结。全书共分 7 章，主要内容是数字图像处理、信息隐藏的理论研究和应用研究，针对信息隐藏算法中提高隐藏容量的关键问题，提出解决方案，并对提出的算法进行仿真实验和分析，取得了令人满意的结果。具体研究内容如下。

（1）主要介绍信息隐藏的定义和技术要求，以及信息隐藏技术的两大分支——隐写术和数字水印技术。另外，简要描述信息隐藏的发展历史，在此基础上提出本书的主要研究内容和组织结构。

（2）主要介绍针对数字图像的信息隐藏算法。从不同的角度对现有图像信息

隐藏算法进行分类、比较。对不同类型隐藏算法的基本原理、使用特点和适用场合进行对比，并结合国内外研究现状进行分析。

（3）在宿主图像分析的基础上，提出新的信息隐藏算法。在介绍人类视觉系统特点的基础上，根据人类视觉系统对高亮区和纹理复杂区不敏感的特性，对宿主图像分别从亮度和纹理度两方面进行分析，计算宿主图像中将视觉不敏感区域作为掩蔽区。提出空间域多位面替换嵌入算法，将伪随机排序后的秘密信息根据选择出的掩蔽区嵌入图像的多个位面中，在保证不可感知性的前提下，增加隐藏系统的嵌入容量。

（4）提出基于隐藏信息压缩的信息隐藏算法。在嵌入秘密图像信息之前，首先对信息进行编码处理，降低编码的比特率，更大限度地嵌入有用信息，去除冗余，合理有效地利用载体图像的空间，以节省空间来嵌入更多的信息量。算法结合冗余信息对秘密图像进行压缩编码，减少组成图像的数据。分析和比较两类预测编码技术的压缩效果，提出将灰度图像作为秘密信息，将图像的预测编码参数作为隐藏信息嵌入宿主图像中；并通过仿真实验，给出算法的效果和对比结果。

（5）提出一种新型的基于遗传算法的彩色图像隐藏算法。该算法利用遗传算法分析水印对原始图像的影响、嵌入后不同通道抵抗攻击的能力，为每个通道选择最优的嵌入权值。通过使用遗传算法，提高隐藏系统的不可察觉性，同时提高嵌入水印的鲁棒性和安全性。遗传算法的使用能够实现水印的不可见性与鲁棒性较好的折中。同时提出基于神经网络的水印复原算法，相当于对水印算法的重要补充，提高水印系统的鲁棒性。

（6）在现有预测误差扩展算法的基础上，引入梯度预测算法增加预测的准确性，提出一种基于图像梯度预测的可逆图像隐藏算法，扩大隐藏信息容量。隐藏方案可实现优化现有嵌入规则，降低对宿主图像的修改，增加图像的不可感知性。

本书是在吉林财经大学的资助和支持下完成的。值此专著完成之际，诚挚地感谢吉林财经大学给予的支持，感谢吉林大学赵晓晖教授的热情帮助和指点。

由于作者水平有限，加之信息安全领域纵深宽广，书中难免会有不足之处，恳请广大读者批评指正。

目　录

第1章 绪 论

1.1 引 言

随着社会的快速发展和科技的日益进步，计算机技术的快速发展和网络的迅速普及给人们的生活和工作带来了极大的方便，也给数字化信息的传播开辟了新的道路。越来越多的企业、机关和个人通过网络互相通信和交流，数字文件作为通信、沟通的主要载体，大量的数字信息在网络上传输和共享，但随之而来也出现了一系列的安全问题。数字信息具有容易复制、容易更改和容易传播等特点，对信息版权的拥有者造成了一定的困扰。数字信息很容易被复制，对版权的认证造成了混淆。数字信息很容易被更改，信息的真实性受到了威胁。数字信息很容易被传播，重要信息或秘密信息很容易被泄露。更严重的是，数字信息可能被恶意利用甚至被用来从事非法活动，影响国家政治稳定、经济发展，对国家安全造成威胁。

因此，数字信息的安全问题已经引起了人们的广泛关注，信息技术的高速发展不仅给人类社会带来了巨大的进步，同时改变着人们对信息安全重要性的认识，从而对通信安全提出了更高的要求。传统的保密通信通过对通信内容加密成密文来达到保密信息的目的，通常使用密钥系统（DES）或是公钥系统（RSA），没有获得加密密钥的接收者无法获得明文。这种方法的缺点是，它使监听者很明确地看出哪些信息是要传输的通信信息，容易引起监听者的注意，从而获取和破解那些他们感兴趣的信息。另外，随着分布式计算技术的发展和普及，计算机的计算技术不断提高，破解密钥的速度越来越快。1997 年，美国程序员 Verser 在互联网上万名志愿者的帮助下，历时 96 天成功破解了 DES 密码。1999 年，电子边境基

金会破解 DES 仅用了 22 小时。加密信息在被破解后便完全透明，因此加密技术面临着严重的挑战和危机。

信息隐藏（information hiding）技术[1-3]在这种情况下应运而生。信息隐藏将要传输的秘密信息隐藏到不容易引起监听者注意的宿主信息中，并把隐藏后的信息作为传输的对象，其中宿主信息可以是文本[4, 5]、音频[6, 7]、视频[8-10]和图像[11-15]等。该技术加密了保护内容并使通信过程隐蔽进行，增加了安全性。与传统密钥加密方式的原理不同，加密方法是通过将信息伪装达到保密的目的，信息隐藏是把整个信息隐藏到其他载体内部，让人完全感觉不到信息的存在，降低了被截取和破解的概率。两种方式可以同时使用，先把秘密信息加密，把加密后的信息隐藏到宿主中，增加了隐藏的安全性。作为信息隐藏的宿主，由于图像的冗余空间相对较大，因此是目前使用最多的隐藏载体。

1.2　信息隐藏的定义

信息隐藏又称为数据隐藏，主要利用多媒体信息自身存在的冗余，以及人类视觉或听觉的不敏感，把要传输的秘密信息隐藏在公开传输的载体信号（文本、图像、音频或视频等）中，隐藏后的信息不容易被人发现，在传输的过程中能够免于被攻击或破坏。

信息隐藏过程包括秘密信息的嵌入和提取（或检测）过程，系统流程一般如图 1.1 所示。

图 1.1 中的重要步骤的定义如下。

秘密信息：要隐藏的消息，可以是情报或版权信息等。

原始载体：用来隐藏秘密信息的容器，也称宿主，可以是文本、图像、音频、视频或其他形式的多媒体数据。在嵌入秘密信息前称为原始载体，嵌入后称为含密载体。

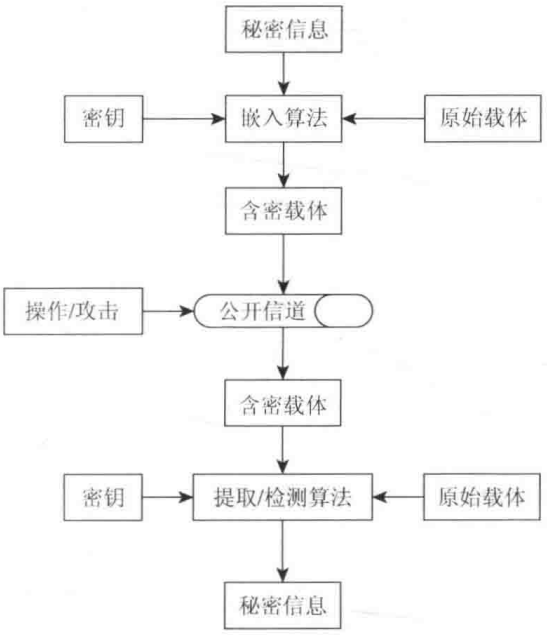

图 1.1 隐藏系统流程

嵌入算法：把秘密信息隐藏到原始载体的过程。

含密载体：嵌入秘密信息后的原始载体，此时原始载体的信息已被改变，但在主观上是无法察觉的。

密钥：在嵌入的过程中用来控制嵌入的位置或嵌入强度等信息的秘密数据，对整个隐藏过程进行加密保护。在接收端，需要使用对应的密钥信息才能获取隐藏的秘密信息。该密钥的组成虽然无法与现代分组加密强度相比，但对于信息隐藏系统也是增加了一重保护。密钥的形成是由嵌入算法决定的，并不是所有的算法都需要密钥。

操作/攻击：含密载体在传输的过程中可能会遇到无意的信号处理操作或恶意的攻击，这些都有可能对含密载体的数据造成改变，破坏载体中的秘密信息。

提取/检测算法：在接收端获取秘密信息的过程，多为嵌入过程的逆过程。根据提取/检测过程是否需要原始载体的参与分为全盲提取/检测、半盲提取/检测和非盲提取/检测。全盲提取/检测比非盲提取/检测更加具有普遍性和适用

性，是目前的隐藏算法主要的研究方向。

1.3　信息隐藏技术的要求

信息隐藏技术与传统的加密技术不同，它的目的不在于控制信息的存取，而在于保证信息的隐蔽，在传输过程中不被发现。根据信息隐藏技术应用的不同目的，可分为以下具体要求。

（1）不可感知性。不可感知性也称隐蔽性、透明性。它是指向宿主载体嵌入秘密信息后对宿主的改变和失真较小，不容易引起人类的感知和察觉，嵌入信息后的隐体与原始载体相差不大。它包括两方面的感知：一方面是人类感官的感知，如听觉和视觉；另一方面是统计意义上的感知。在评价该指标时，一般同时使用这两方面来判断，可以称为主观感知评价和客观感知评价。主观感知评价是人用自己的视觉或听觉来判断：嵌入后隐体与原始载体是否一致，哪里发生了变化，相似程度有多少。客观感知评价是利用统计指标计算两者之间的误差，如峰值信噪比、结构相似性等。这是信息隐藏系统最基本的指标，如果嵌入秘密信息后的数据被攻击者所感知，就能针对性地提取或破坏秘密信息，未能达到隐藏的目的。

一种可见水印的信息隐藏技术例外，它把信息以可视的方式加载在宿主图像上，这是一种主动保护，用以保护并提示载体信息不可被传播或篡改，以可见性良好、不影响载体信息、难以去除为主要特征。

（2）安全性。安全性是指信息隐藏技术要具备较强的抗攻击和抗干扰能力，当面临人为的恶意攻击时能够保证嵌入的隐秘对象不被损坏。Mittelholzer[16]基于信息论的角度提出了信息隐藏和数字水印算法。Cachin[17]则提出“ε安全”的信息隐藏信息论模型，认为如果原始载体和含密载体的概率分布相关熵小于ε，则可以说该隐藏系统是安全的，如果$\varepsilon=0$则认为系统是绝对安全的。

与传统的加密方式类似，为了使信息隐藏得更加隐秘，信息隐藏技术有时也需要密钥的参与。在信息隐藏嵌入算法和提取算法公开的前提下，算法的安全性完全依赖于密钥的使用，对隐藏信息的保护即是对密钥的保护，这与密码学中的加密第一原则一致，因此如何产生密钥和发放密钥也是需要考虑的问题。

（3）不可检测性。不可检测性是指在信息传输时，使隐藏分析者无法检测出隐藏对象中是否藏有秘密信息。这就要求载体信息与秘密信息具有一致性。

与信息隐藏相对应的对抗技术为隐写分析[18, 19]。目前对隐写分析技术的研究主要集中在检测技术上，检测到载体含有隐藏信息后便可对含密载体进行破坏或破解，破解技术涉及嵌入算法，具有较大难度，但检测后对信息的破坏比较容易实现，对图像载体进行剪切、旋转、改变格式等攻击操作都可能会达到破坏的效果，会造成无法准确提取信息。类似于密码分析技术和密码设计两者之间的互相促进，隐写分析技术的发展是对信息隐藏算法的检验[20]，为隐写技术的安全性提供了理论依据，对设计出安全的隐写算法具有指导作用。

（4）鲁棒性。鲁棒性是指在经历了多种信号处理操作后，依然能从传输载体中提取出秘密信息的能力[21-23]。载体在传输过程中，有可能会受到一些无意的（如压缩、滤波、图像打印与扫描、噪声、尺寸改变等）或是恶意的信号处理操作，这些操作必然对载体造成一定的改变。如何在这些改变中依然保持秘密信息的准确是鲁棒性所强调的。对于隐藏系统想要实现完全的鲁棒性，即经受这些信号处理操作后还保持完全的秘密信息是很难实现的。鲁棒信息隐藏技术[24-26]应能做到若要去除嵌入的秘密信息，将会对整个载体进行破坏，使载体失去使用价值。

（5）嵌入容量。嵌入容量是指在保证宿主质量的前提下，能够隐藏信息的最大数据量。一般用数据嵌入量（单位为 bit）或是数据嵌入率（单位为 bit/B）来评价。由于在测评时，宿主的大小各不相同，仅用数据嵌入量来测量系统的嵌入容量并不能完全表达系统的容量特征。因此，更多使用的是数据嵌入率[27-30]，数据

嵌入率等于隐藏信息的长度/宿主的长度。如果载体不被影响，理想的状态是在载体中尽可能多地嵌入信息[31-33]。但事实上，嵌入的隐藏信息越多对载体的影响越大，鲁棒性也越差。因此，一般的处理方式都是在嵌入容量、鲁棒性以及不可感知性之间进行折中。

除了上述的几种主要技术性能要求外，信息隐藏还有其他的一些性能指标，包括是否盲提取（检测）[34, 35]、嵌入算法的效率[36, 37]和复杂度、是否多重嵌入[38-40]等。根据不同的应用需要对隐藏系统具有不同的要求。

对一般的信息隐藏系统而言，不可感知性、鲁棒性和嵌入容量三个指标之间通常是互相制约的。例如，要想增加系统的不可感知性，往往是尽量降低对原始载体的修改，而嵌入信息的容量却需要通过修改载体数据来实现，两者是互相矛盾的。同时，若要提高系统的鲁棒性，需要增加嵌入强度，加大信号调制，但这样容易导致不可感知性降低。有时，鲁棒性的提高也需要增加冗余，它以牺牲嵌入容量为代价。因此，若要追求全部性能的最优化几乎是无法实现的，在实际应用中往往是在其中寻找一个折中的平衡点，根据具体的应用需要，有目的地侧重。例如，数字水印系统会更加重视系统的鲁棒性，而隐写术更加强调嵌入容量。

1.4　信息隐藏技术的分支

信息隐藏技术是一门新兴的交叉学科，它涉及密码学、模式识别、数学、图像处理和通信等领域。根据信息隐藏的应用目的不同，可分为不同的领域分支。其中，最重要的两大分支分别是隐写术与数字水印技术。

1. 隐写术

隐写术（steganography）来源于希腊语，意为隐藏与书写，主要是指把秘密信息隐藏在其他信息中传输出去，属于保密通信技术。从应用来看，隐写术可分

为两个研究方向：防检测保护和防修改保护。防检测保护是保护嵌入秘密信息的载体不被人或计算机察觉，即强调嵌入信息后的载体与原始载体之间的不可感知性，使攻击者察觉不到这个通信传输的存在；防修改保护主要强调对秘密信息的保护，攻击者若要去除秘密信息，需要对隐秘后载体做大量的破坏才能实现，而这样载体将失去本身的应用价值。

隐写术主要用于秘密通信，保护隐藏在载体中的秘密信息。通常把隐写术与密码术结合起来，加上密码后相当于对信息又多了一层保护，增加了系统的安全性。隐写术最开始主要集中在军事应用上。特别是在现代战争中，隐蔽通信、间谍活动等都是利用信息隐藏技术实现的。随着网络技术的普及和全球经济一体化，人们对一些重要的商业机密的重视程度等同于军事机密，信息隐藏技术的研究和应用开始向个人、商业信息的保护以及电子商务交易数据的传递和保护发展[41-46]。

2. 数字水印技术

数字水印技术的思想和隐写术一样，都是将秘密信息隐藏到载体信息中。但两者的使用目的不同[47-51]，因此实现起来侧重点也不一样。隐写术强调要保护的对象是秘密信息，载体仅仅是为了容纳秘密信息所用，因此可以使用任意不同的载体。而数字水印技术强调要保护的对象是载体的版权，嵌入的秘密信息即数字水印的作用是用来证明载体的归属权、购买者或其他相关信息。数字水印技术的应用包含以下几个方面。

1）版权认证

数字产品具有容易复制、传播等特点，对数字产品的篡改和侵权也很容易实现，因此数字产品的版权保护成为了当今的热点问题，这正是推动数字水印技术发展的动力。数字水印技术把具有代表性的版权所有者信息，如作者、发行者、使用者等版权相关信息按照一定的嵌入算法，以不可见水印的形式嵌入数字产品中，当产品被盗用或是出现版权纠纷时，可以通过从盗版或侵权作品中提取出水

印信息来验证产品的版权所属，保护作者的合法利益。

一般来说，版权认证仅要求把版权信息作为隐藏信息嵌入载体中。因此，该应用并不在意嵌入容量的大小。由于版权信息要作为证明永久存在，因此要求该隐藏系统要具有强鲁棒性，嵌入的信息不能被攻击者去除。

2）交易跟踪

作品的所有者可以在每个产品的合法复制中加入不同的数字水印，作为每个复制的唯一标识，可以是购买者的 ID 或序列号等，该应用也称为“数字指纹”。版权所有者把作品分发给购买者前，将购买者的身份信息与加入的数字指纹信息同时保存到数据库中，当作品被非授权使用或滥用时，所有者从侵权作品中提取出数字水印，与数据库中的数字指纹进行比对来确定购买者的身份，继而跟踪出作品的传播出处，确定来源信息，找到为盗版者提供作品的购买者。

3）完整性验证

随着计算机技术的发展，对数字产品进行篡改越来越容易，一些作品被用于医学、商业和法庭时，要求保证作品的真实性，需要确定作品是否被修改过，是否是伪造的，有没有经过特殊处理。该应用主要是针对数字产品的完整性进行验证，也称真伪验证。该技术通过脆弱水印或半脆弱水印实现，对数字产品做极小的改动都能造成水印的破坏，用脆弱水印的完整来证明产品的完整，以此来证明图像的真伪。

在该应用中，将一些与作品相关的信息嵌入作品中，验证时通过分析作品中的水印与作品的关系，确定作品是否被修改过，甚至可以确定修改的位置，更优的算法能够对更改的内容进行大致修复。

4）复制保护

数字水印技术可以禁止非法用户复制数据，以防止大量盗版的出现，有效地保护版权。例如，将数字水印嵌入 DVD 数据中，DVD 防复制系统通过检测 DVD