# 基于数字图像的大容量信息隐藏算法

# High Capacity Information Hiding Algorithm in Digital Images

谢建全　著

科学出版社

# 基于数字图像的大容量信息隐藏算法

# High Capacity Information Hiding Algorithm in Digital Images

谢建全 著

科学出版社

北京

## 内 容 简 介

本书是作者多年来在信息安全领域研究成果的总结，主要围绕如何提高信息隐藏容量，以满足隐秘通信和篡改认证等应用所需的嵌入容量这个目标展开。全书共 8 章，第 1 章介绍了国内外信息隐藏的相关理论、技术和应用现状；第 2 章讨论了影响隐藏容量的不可感知性评价和改进方法；第 3 章讨论了图像的加密与置乱在信息隐藏中提高隐秘数据的不可感知性、安全性、抗剪切攻击性和隐蔽信道容量等方面的作用；第 4～8 章着重讨论了在图像空间域和变换域提高信息隐藏容量的技术和方法，并给出了基于空间域、变换域和游程长度的多种大容量信息隐藏算法。

本书可供信息隐藏、保密通信、版权保护、数字指纹、多媒体内容篡改认证等领域的科技人员阅读，也可作为高等院校信息安全、通信工程和计算机科学与应用等专业的研究生和高年级本科生的教材和参考书。

**图书在版编目(CIP)数据**

基于数字图像的大容量信息隐藏算法/谢建全著. —北京：科学出版社，2014.7

ISBN 978-7-03-041395-6

Ⅰ. ①基… Ⅱ. ①谢… Ⅲ. ①信息系统—安全技术—算法—研究 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2014）第 156051 号

策划编辑：陈 静 / 责任编辑：陈 静 邢宝钦 / 责任校对：彭 涛
责任印制：阎 磊 / 封面设计：迷底书装

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

新科印刷有限公司印刷
科学出版社发行 各地新华书店经销

*

2014 年 7 月第 一 版 开本：720×1 000 1/16
2014 年 7 月第一次印刷 印张：10 3/4
字数：214 200

**定价：50.00 元**

（如有印装质量问题，我社负责调换）

# 前　言

互联网络和信息科学的飞速发展，为信息的传输和处理带来了极大方便，但是网络在给人们带来便利的同时也暴露出越来越严重的安全问题。为了保证信息的安全，人们广泛使用加密技术对要保护的信息进行加密，然而一段有意义的信息通过加密处理后，会转换成看起来没有意义的乱码信息。这种加密后的乱码信息呈现出明显的乱码特性，明确地提示攻击者密文是重要信息，容易引起攻击者的好奇和注意，从而造成攻击者明确知晓攻击的目标。即使加密的强度足以使得攻击者无法破解出明文，但攻击者仍有足够的手段来对其进行破坏，干扰通信的进行，并且信息加密后的乱码特性使得攻击者很容易发现这些加密后的信息，因此加密作为一种安全传输的手段存在明显的不足。

信息隐藏(information hiding)是一种具有伪装特点的新兴信息安全技术，它从另外一个角度来保证信息传输的安全，从而引起了人们的极大关注。它通过隐藏信息的“存在性”来保证信息的安全传输，能解决密码学在应用上容易引起攻击的问题。信息隐藏主要应用在包括隐秘通信、版权保护、数字指纹、多媒体内容篡改认证等军事和民用领域，有重要的理论和应用研究价值。在过去的十多年中，信息隐藏的一大分支数字水印取得了快速的发展，但在隐秘通信和篡改认证方面取得的研究成果相对较少。其主要原因是缺乏对安全性和感知质量客观准确的评价手段，隐藏算法的嵌入容量、安全性、感知失真之间的固有约束存在着一定的难度，尤其是多数隐藏算法的嵌入容量还远未达到隐秘通信的容量要求。因此，本书的主要工作就是围绕如何提高信息隐藏容量，以满足隐秘通信和篡改认证等应用所需的嵌入容量这个目标展开的，内容涉及信息隐藏的不可感知性评估、数字图像的加密与置乱、大容量的图像信息隐藏算法等方面。本书共分 8 章，具体安排如下。

第 1 章为绪论。介绍本书形成的背景和意义，给出了国内外相关理论、技术和应用现状，讨论了目前主流算法的特点和不足。

第 2 章介绍了常用的视觉不可感知性评价方法，并讨论了它们的不足之处。根据人眼视觉特性提出了一种衡量信息隐藏算法不可感知性的视觉失真感知函数，并对视觉失真感知函数与峰值信噪比等传统指标进行视觉感知质量方面的对比评价。

第 3 章概述了隐秘信息预处理的要求，给出了传统的数据加密方法因为复杂

度高而不适合对有大量冗余信息的图像、音频和视频等多媒体数据进行预处理的观点，指出了混沌加密在信息隐藏中提高隐秘数据的不可感知性、安全性、抗剪切攻击性和隐蔽信道容量等方面的作用。针对目前用于信息隐藏预处理的混沌序列加密和混沌置乱两类方法，探讨了用它们直接进行隐秘数据预处理中存在的安全问题，给出了产生混沌序列和图像混沌置乱的新算法。

第 4 章分析了图像在空间域的位平面分解特性，提出了基于空间域的大容量算法。利用人类视觉系统的亮度掩蔽效应，提出了一种基于彩色图像空间域的自适应信息隐藏算法，该算法根据像素点的每个颜色分量判断信息的隐藏位置，在满足不可感知性的前提下，能最大限度地利用可利用的隐藏空间。针对空间域算法隐藏容量大但安全性差的特点，提出了一种具有鲁棒性且较安全的空间信息隐藏算法。本章还利用空间域信息隐藏算法嵌入容量大的特点，提出了一种用于图像内容像素级篡改认证的脆弱水印算法，不仅能准确地识别图像被篡改的像素点，还能容忍图像传输过程中出现的个别认证信息位的传输错误。

第 5 章分析了 DCT 系数的分布特性，通过对载体图像进行频谱均匀化处理，获得更多的可用于隐藏信息的 DCT 系数，从而提高算法的可嵌入容量。根据这一思想提出了在频谱均匀化的基础上进行隐藏的大容量隐藏算法。根据 JPEG 压缩不变性，提出了对不超过预设品质因子的有损压缩有强鲁棒性的大容量隐藏算法。

第 6 章分析了二值图像的特点，并根据二值图像每个像素点非白即黑的特点，提出了 2×2 分块的二值图像大容量算法。该算法自适应地确定了可嵌入隐藏信息的比特数，嵌入位置可通过密钥控制。

第 7 章针对半色调这种特殊的二值图像，利用半色调处理技术提出了一种能在半色调图像中嵌入与载体图像同样大小的水印图像的隐藏算法，信息的嵌入过程与半色调处理过程同步进行。在提取过程中，只要将标准半色调图像直接叠加到含水印图像上，就能看到水印图像，可应用于所有基于半色调技术的图片的认证和防伪。

第 8 章分析了自然图像游程长度的分布特点和多数信息隐藏算法对游程长度的统计特性的影响，指出了这种影响与算法的安全性的关系。利用人类视觉特性，提出了一种基于游程长度的大容量隐藏算法，可应用于隐秘通信等对隐藏容量和安全性有较高要求的场合。

本书的出版得到湖南省教育科学“十二五”规划课题“数字教学资源共享与版权保护机制及技术研究”（XJK011BXJ008）、湖南省科技计划项目“基于机器视觉的产品瑕疵检测技术研究”（2012GK3064）和湖南省高等学校重点建设学科——湖南财政经济学院计算机应用技术学科的资助。

感谢作者所在工作单位湖南财政经济学院各级领导、老师对本书撰写的关心和支持，感谢所有关心、支持、帮助过作者的领导、老师、同事和朋友。书中引用了大量的文献资料，在此向原作者表示深深的谢意。

由于作者学识、水平有限，书中不足之处在所难免，恳请同行专家和广大读者不吝指正！

谢建全

于长沙湖南财政经济学院

2014年3月

# 目　录

# 第1章 绪 论

网络的推广和普及为信息的传输和处理带来了极大方便，但是网络在给人们带来便利的同时也暴露出越来越严重的安全问题。为了保证信息的安全，人们广泛使用加密技术对要保护的信息进行加密，然而一段有意义的信息通过加密处理后，会转换成看起来没有意义的乱码信息，它明确地提示攻击者密文是重要信息，容易引起攻击者的好奇和注意，从而造成攻击者明确知晓攻击的目标。即使加密的强度足以使攻击者无法破解出明文，但攻击者仍有足够的手段来对其进行破坏，干扰通信的进行。

具有伪装特点的新兴信息安全技术——信息隐藏(information hiding)技术则是从另外一个角度来保证信息传输的安全，它通过将所要传送的信息嵌入到可以公开传输的多媒体信息中，利用人类感觉器官的局限性，使人觉察不到秘密信息的存在，从而实现秘密信息的安全传输，有效地解决了密码术容易引起攻击者注意的安全问题。密码技术隐藏信息的“内容”，而信息隐藏技术则隐藏信息的“存在性”，它们之间不是互相矛盾、互相竞争的关系，运用恰当策略、相互融合会得到更好的应用。信息隐藏的应用包括版权保护、数字指纹、多媒体内容篡改认证、隐秘通信等军事和民用领域，因此有着重要的理论和应用价值。

## 1.1 信息隐藏的基本概念

信息隐藏是一种防止秘密信息在存储和传输过程中受到敌手的攻击和破坏而采用的一种安全保障技术，其历史可以追溯到古希腊。随着数字技术的发展，信息隐藏被赋予新的含义。它研究的是如何利用人类感觉器官在感知上的局限性和多媒体数字信号本身存在的冗余，以数字媒体或数字文件为载体，将秘密信息隐藏在一个宿主信号中而不为人们所感知，从而达到保护信息安全的目的。

### 1.1.1 信息隐藏的基本框架

目前通常将信息隐藏看成一个通信过程[1]，通用信息隐藏模型框图如图 1-1 所示[2]。

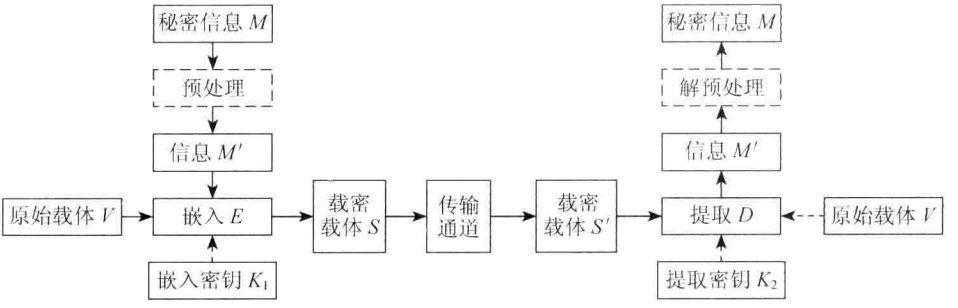


图 1-1　通用信息隐藏模型框图

(1) 秘密信息：是指要进行隐藏的信息，它可以是文本、图像、视频或声音等二进制数据。

(2) 原始载体：有时也称为载体介质或宿主数据，它可以是文本、图像、视频或音频信息。由于图像数据的空间冗余和视觉冗余较大，具有大量的冗余空间以隐藏更多的信息，更适宜于信息隐藏，所以从目前所做的信息隐藏算法来看，以图像或视频的比较多，尤其是大容量信息隐藏算法多以数字图像作为载体。用作载体的图像称为原始图像。

(3) 嵌入：是指将秘密信息嵌入隐秘载体的过程。

(4) 载密载体：它是嵌入过程的输出，是指已经进行数据嵌入的某种介质。为满足不可感知的要求，载密载体与原始载体在主观感觉上应该是没有区别的。

(5) 隐藏密钥：有时也称为伪装密钥，它是在隐藏过程中用来控制嵌入过程和嵌入位置的一些额外的秘密数据，在恢复要嵌入的信息时，通常要用到它或与它相关的一些信息。并不是所有的隐藏算法都要用到隐藏密钥。

(6) 恢复或提取：它是嵌入过程的逆过程，是指利用相关密钥，从伪装后的载体介质中得到所嵌入的信息。

(7) 预处理：是对信息加密、置乱或特性调制的过程[3-5]，在信息隐藏中它不是必需的，但它可以有效地改善信息隐藏算法的性能。其作用有两个：一是加密等操作使隐藏数据呈现噪声特性，可以在隐藏算法被攻破后，攻击者得到的仍然是一些无意义的数据，无法判断其得到的数据是否为隐藏的秘密信息，从而提高隐藏信息的安全性；二是对需隐藏的信息 $M$ 进行纠错编码[6]，因为在存在攻击的情况下，隐藏数据的检测发生错误是必然的[7]，使用纠错编码可以在信息 $M'$ 存在误差时，仍然能够得到正确的隐藏信息，从而提高系统的鲁棒性。

信息隐藏的目的是在收发双方之间建立一个隐蔽的通信，使攻击者无法知道这个通信事件的存在。信息隐藏的隐藏与提取过程如下。

首先，将等待秘密发送的信息 $M$ 经过加密或其他预处理后得到信息 $M'$；然

后，通过嵌入算法和嵌入密钥 $K_1$ 将信息 $M'$ 嵌入到载体 $V$ 中，得到嵌入有信息 $M'$ 的载密载体 $S$，$S$ 在传输通道中传输，接收方收到传输过来的载密载体 $S'$，接收方在收到信息 $S'$ 后通过提取算法和提取密钥 $K_2$，将载密载体 $S'$ 中的信息 $M'$ 提取出来；最后，通过解预处理得到信息 $M$。在传输过程中，如果未受到任何干扰或攻击，则 $S$ 与 $S'$ 完全相同，否则它们之间就存在差异。

### 1.1.2 信息隐藏的技术性能要求

信息隐藏的技术性能要求有不可感知性、鲁棒性、隐藏容量和安全性等多个方面[8-10]，并视其应用场合不同而有所不同。

(1)不可感知性，又称为透明性、不可见性，指的是隐藏信息的嵌入操作不应使载体发生可感知的改变，也不能使载体在质量上发生可以感觉到的失真，即除了个别特殊应用场合会采用可见水印，隐秘载体 $S$ 和原载体 $V$ 应充分接近。例如，若载体 $V$ 为一幅图像，则肉眼应无法区分载密图像 $S$ 与原图像 $V$ 之间的差异。不可感知性是信息隐藏最基本的指标，如果这一指标不能满足，则在通信过程中携带秘密信息的载体就会引起第三方的怀疑，从而失去了隐藏的意义。

(2)鲁棒性，又称为健壮性，指的是加入载体中的隐藏信息必须能够承受施加于载体的变换操作(如常规信号处理、重采样、有损压缩、旋转、缩放、裁剪等)。即使在载密载体 $S$ 受到一定的扰动的情况下，隐藏信息仍然能保持一定的完整性，并能以一定的正确概率被检测到。对于版权保护等应用，存在攻击是不可避免的[11]，并且攻击者一定是主动的，它们有可能通过某种处理手段来去掉或破坏被嵌入信息，因此一般情况下有一定的鲁棒性要求。不过在某些特殊情况下，鲁棒性毫无用处甚至被极力避免，例如，用于真伪鉴别的水印就应该是脆弱的或者半脆弱的[12]，而不应是鲁棒的。

(3)隐藏容量，又称为嵌入信息量，是指在给定的载秘载体中能够隐藏于载体数据中的不被人类感觉器官感知的最大二进制秘密数据的位数，通常以嵌入的秘密信息大小与载体信息大小之比来表示。如果以数字图像为载体信号，那么一般以每个像素中所能嵌入的最大比特数来表示。对于一个具体的隐藏算法，要具有实用性，必须有足够的嵌入容量。目前研究容量的方法分别从两个不同角度对隐蔽信道容量进行定义：一种是不管具体的信息嵌入、提取算法和隐藏信息的鲁棒性，仅针对载体数据本身的特点研究载体作为隐蔽信道的容量，例如，文献[13]给出了在以图像作为掩护媒体的隐秘通信中，一幅图像(信道)能够传输的秘密信息量的上界，而不管秘密信息如何被提取；另一种是针对具体的信息嵌入、提取算法并考虑隐藏信息的鲁棒性问题来研究容量，即把针对具体的隐藏算法在载体信号中所能嵌入的最大数据量称为容量。

(4)安全性，指的是信息隐藏系统难以伪造或者加工，攻击者不能阅读和修改

隐藏的信息。理想情况下是指攻击者不能检测到载体中是否包含隐藏信息。具体来说，安全性包括存在安全性和内容安全性[14]。存在安全性是指在任何时候，攻击者判断载密载体中是否包含隐藏信息的正确性都不高于随机的猜测。当前的隐写分析[15]主要是从存在安全性的角度实施攻击。内容安全性是指嵌入信息内容的安全性，具体包括信息嵌入的位置和信息内容，针对内容安全性的攻击称为“提取攻击”。Cachin 提出了数据隐藏的信息论模型[16]，并引入了概念“$\varepsilon$-安全”。如果载体信号和载密信号的概率分布的相关熵小于$\varepsilon$，那么就称数据隐藏系统是$\varepsilon$-安全的。如果$\varepsilon$=0，那么数据隐藏系统是绝对安全的，即 0-安全。Mittelholzer 从信息论的角度出发，提出了数据隐藏算法[17]，并以互信息来描述数据隐藏算法的安全性与鲁棒性。当前学术界对信息隐藏算法的安全性基本达成了这样一个共识：在信息隐藏算法和加密体制公开的前提下，算法的安全性仅依靠于密钥的使用，这与密码学中 Kerckhoffs 加密原则完全一致。

除了以上的一些基本技术性能要求，在实际应用中，根据具体情况可能还有盲检测性、通用性、嵌入与检测效率、水印修改与多重水印、虚检率等性能要求。

对于一个具体的隐藏算法，不可感知性、隐藏容量和鲁棒性三个指标常是相互制约的[18]，并且在一定条件下可以相互转化。例如，隐藏容量的增加往往需要增加对原始载体信息的修改，可能会使不可感知性下降；对嵌入的信息加大其嵌入强度，可提高其鲁棒性[19]，但往往大强度的信号调制会导致不可感知性的下降；在转化方面，增加密文信号的冗余可以提高鲁棒性，而这是以牺牲隐藏容量为代价的。实践中往往需要根据具体应用模式在这三者之间寻求适当的平衡点。对于数字水印技术，往往追求强鲁棒性，因为数字水印保护的是载体本身，在受到攻击后水印应该仍旧存在；而对于隐秘通信系统，在保证不可感知的前提下，更加强调隐藏容量，因为隐秘通信保护的是秘密信息，只有在隐藏容量达到一定规模时，隐秘通信才有实际意义。

## 1.2　隐藏技术分类

对信息隐藏技术进行分类的方法有多种，而分类方法的不同导致了分类的不同，它们之间既有联系又有区别。常用的分类方法有按使用密钥方式的分类方法、按提取过程是否需要原始载体的分类方法和按载体信息类型的分类方法等。

1. 按使用的密钥方式分类

按使用的密钥方式可分为无密钥隐藏系统和有密钥隐藏系统两大类，而根据密钥体制的不同，有密钥隐藏系统又分为私钥信息隐藏系统和公钥信息隐藏系统两类。

1)无密钥信息隐藏系统

无密钥信息隐藏系统在数据嵌入和提取的过程中不使用密钥，因此不需要预先交换密钥。秘密信息的嵌入和提取的过程描述如下。

$E$：$V\times M\rightarrow S$ 为嵌入变换，对所有的 $m\in M$，$v\in V$，$s\in S$，有 $s=E(c, m)$。

$D$：$S'\rightarrow M'$ 为提取变换，对所有的 $s'\in S'$，$m\in M'$，有 $m'=D(s')$。

这里 $V$ 是所有可能的原始载体的集合，$M$ 是所有可能秘密信息的集合，$S$ 是所有可能的载密载体的集合。在实用的信息隐藏系统中，集合 $C$ 应选择有意义的但表面上无关紧要的信息(如所有有意义的数字图像的集合)，这样通信双方在交换秘密信息的过程中才不至于引起攻击者的怀疑。

在无密钥信息隐藏系统中，嵌入与提取过程无密钥控制，因此收发双方所使用的嵌入和提取算法是不能公开的。因为在无密钥信息隐藏系统中，除函数 $E$ 和 $D$ 之外不需要其他信息，所以系统的安全性完全取决于隐秘算法本身的安全性。但这违反了 Kerckhoffs 加密原则，因而并不十分安全。不过无密钥系统也并不是毫无安全性可言，当嵌入的信息是经过加密处理的并且其特性与没有隐藏信息的载体特性相同时，攻击者虽然能提取出隐藏的信息，但他无法确定提取出的信息是隐藏的信息还是原始载体信息的一部分，即无法判断载密载体 $S'$ 中是否隐藏有秘密信息，从而得不到任何证据(甚至是猜测)能表明该系统发生过通信，此时整个算法仍然是安全的。因此在很多应用中，无密钥信息隐藏系统仍是首选，这是因为通信双方不需要共享一个隐藏密钥。

2)私钥信息隐藏系统

私钥信息隐藏系统对信息的发送与接收使用相同的密钥，即图 1-1 中当 $K_1=K_2$ 的情况，因此私钥信息隐藏系统也称为对称密钥信息隐藏系统。对称密钥信息隐藏系统和对称加密系统相类似，发送方选择一个隐秘载体 $v$ 并利用密钥 $k$ 将秘密信息 $m$ 嵌入 $v$ 中，并且隐秘载体 $v$ 和隐秘对象 $s$ 之间是知觉相似的。此处密钥 $k$ 既可以用于在嵌入操作之前对秘密信息进行加密处理，也可以作为参数控制嵌入过程，或者同时使用。

如果接收方知道嵌入过程中所使用的密钥 $k$，则他就可采用与嵌入相反的逆向操作提取秘密信息。其他任何不知密钥 $k$ 的人都不能提取出秘密信息 $m$。

秘密信息的嵌入和提取的过程描述如下。

$E$：$V\times M\times K\rightarrow S$ 为嵌入变换，对所有的 $m\in M$，$s\in S$，$k\in K$，有 $s=E(v, m, k)$。

$D$：$S'\times K\rightarrow M'$ 为提取变换，对所有的 $s'\in S'$，$m\in M'$，$k\in K$，有 $m'=D(s', k)$。

私钥信息隐藏系统的安全性信赖于私有密钥 $k$，因此私钥信息隐藏系统需要某些密钥的交换，即需要假设通信各方能够通过安全信道传送密钥，但这种额外秘密信息的传输与隐秘通信的原始意图是不相符的。

3)公钥信息隐藏系统

基于公钥密码系统的公钥信息隐藏系统是 1996 年 Anderson 在第一届信息隐藏国际会议上提出的[20]，他的方案中，信息在预处理过程中用公钥密码系统进行加密处理，再将密文嵌入载体中，不过多数学者认为这不是真正的公钥信息隐藏系统。国外有些学者已经在非对称水印方面进行了一些有益的探索[21,22]，但切实可行的真正意义的公钥信息隐藏系统还有待进一步研究，特别是在公开检测算法和密钥的时候，任何人都可以方便地检测水印，但却无法根据检测算法和密钥去除已嵌入信息的公钥信息隐藏系统。

2. 按提取过程是否需要原始载体分类

按提取信息的过程中是否需要原始载体信息可分为盲的隐藏技术(秘密信息提取时不需要原始载体信息)和非盲的隐藏技术两种。

通常在检测或者提取隐藏信息时，如果有原始的载体数据作为参照，那么能够极大地提高检测的准确性，这不仅是针对像噪声一样的失真，也是针对数据的几何失真，尤其是在隐秘载体经受到几何类攻击的时候，原始的载体数据在检测过程中的重要性更为显著。但是，在大多数的应用场合却不能取得原始的载体数据，如数据监控和跟踪。在隐秘通信的应用背景下，必须构造盲信息隐藏算法，否则基于信息隐藏的隐秘通信是没有实用价值的。在其他一些应用中，例如，在视频水印应用中，由于要处理的数据数量很大，使用原始载体数据也是行不通的。

非盲的信息隐藏系统比盲的隐藏系统设计起来容易一些，鲁棒性相对更好，隐藏容量相对更大，但盲的隐藏技术有更为广阔的应用领域。因此，目前的研究大都针对得不到原始载体的应用场合，即盲的隐藏技术。

3. 按载体信息类型分类

按载体信息类型可分为基于彩色或灰度图像、文本、视频、音频的信息隐藏技术。

基于图像的信息隐藏是在数字化图像中人眼无法感知的部分嵌入秘密信息的，通常是对部分图像数据(空域)或描述图像的参数(变换域)进行一定的修改或替换，这种修改或替换操作主要是利用人类的视觉感知特性实现的。由于图像具有较大的冗余空间，同时也是互联网上传递最为频繁的一种多媒体信息形式，所以图像成为信息隐藏的首选载体。可以查到的有关信息隐藏的文献中以图像作为载体的占到了 80%以上，同时它还是以视频为载体的信息隐藏技术的基础。

基于音频的信息隐藏是在数字化音频中人耳无法感知的部分嵌入秘密信息[23]的，通常是对部分音频数据(空域)或描述音频信号的参数(变换域)进行一定的修改或替换。音频信号在单位时间内的采样数据量相对图像比较少，加上人类听觉系统

(Human Auditory System，HAS)比人类视觉系统(Human Visual System，HVS)更为敏感[24]，因此以音频为载体的信息隐藏更加具有挑战性，目前这方面的文献较少。

文档类的信息隐藏技术依据文档类型分为软复制和硬复制两种，以软复制文档为载体时，大都通过对格式文本文件适当微调一些排版特征来隐藏信息，典型的方法有行移编码、字移编码和特征编码；硬复制文档则可以视为一类特殊类型的图像，只是这种图像中可供信息隐藏利用的冗余信息比较少。

视频的信息隐藏技术[25,26]为在数字化视频中嵌入秘密信息，视频序列是由一系列连续的、等时间间隔的静止图像组成的，因此视频的信息隐藏技术和数字图像的信息隐藏技术有很多相似之处，有些用于图像的隐藏算法甚至可以直接应用于视频信息隐藏中，但视频的信息隐藏也有很多自己独特的特点。

## 1.3 基于图像的信息隐藏基本算法

从嵌入域的角度看，常用的基于图像的信息隐藏算法可以分为空间域信息隐藏算法、变换域信息隐藏算法和修改调色板的信息隐藏算法等多种。

### 1.3.1 空间域信息隐藏算法

空间域信息隐藏算法通过改变载体图像某些像素的灰度值来隐藏信息，其典型代表为最低有效位(Least Significant Bit，LSB)算法。最早的一篇数字水印论文 *Electronic Watermark* 是1993年在数字图像计算、技术和应用(Digital Image Computing: Techniques and Applications，DICTA)会议上由Tirkel等发表的，文中嵌入信息的方法就是基于修改图像LSB的方法。

LSB位平面替换嵌入公式可描述为

$$s_{i,j}=\begin{cases} v_{i,j}+w_{i,j}, & v_{i,j}\text{为偶数} \\ v_{i,j}-1+w_{i,j}, & v_{i,j}\text{为奇数} \end{cases} \tag{1-1}$$

式中，$v_{i,j}$为载体图像在坐标为$(i,j)$处的像素值，对于8级灰度图像$v_{i,j}$的值域为$\{0,1,2,\cdots,255\}$；$w_{i,j}$为嵌入到坐标为$(i,j)$处的像素上的二进制数据，它的值域为$\{0,1\}$；$s_{i,j}$为载密图像在坐标为$(i,j)$处的像素值。

实际上，式(1-1)相当于在嵌入之前先将原始载体图像中需要嵌入信息的像素的LSB清零，然后用待隐藏的二值信息直接替换原有的LSB位平面。在实际应用中，LSB信息隐藏基本算法嵌入信息的过程主要分为两步。

(1)在密钥的控制下按“某种规则”在载体图像中选择$l(m)$个隐藏信息的像素点($l(m)$为待隐藏的信息的长度)。