# 信息隐藏算法及应用

Information Hiding Algorithms and Applications

柏森 朱桂斌 曹玉强 编著

國防工業出版社
National Defense Industry Press

# 信息隐藏算法及应用

柏森　朱桂斌　曹玉强　编著



国防工业出版社
·北京·

# 内 容 简 介

信息隐藏是一种重要的信息安全技术。本书全面介绍了信息隐藏及其对抗技术的基本概念、分类、经典算法及其在隐密通信、篡改认证、电子印章等方面的应用。全书共分10章，第1章概要介绍了信息隐藏的基本概念、主要分支、主要特性。第2章介绍了信息隐藏相关的基础知识。第3、4、5章分别介绍了以图像、视频和音频为载体的信息隐藏算法。第6章介绍了其他媒体中的一些信息隐藏算法。第7、8、9章分别介绍了图像、视频和音频中的隐密分析算法。第10章主要介绍了信息隐藏的一些应用方法和应用系统。

本书可作为计算机应用、通信与信息系统、信号与信息处理、信息安全与密码学专业的研究生和高年级本科生教材，也可供从事信息安全研究及应用的学者、技术人员参考。

**图书在版编目(CIP)数据**

信息隐藏算法及应用/柏森，朱桂斌，曹玉强编著. —北京：国防工业出版社，2015.7

ISBN 978-7-118-10176-8

Ⅰ.①信… Ⅱ.①柏…②朱…③曹… 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(2015)第151147号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号 邮政编码100048)

天利华印刷装订有限公司印刷

新华书店经售

*

**开本** 787×1092 1/16 **印张** 14½ **字数** 352千字

2015年7月第1版第1次印刷 **印数** 1—2000册 **定价** 35.00元

**(本书如有印装错误，我社负责调换)**

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

# 前　言

自20世纪90年代初以来，信息隐藏作为信息安全的新领域引起了国际学术界的普遍重视，其主要内容包括隐密术(Steganography)和数字水印技术(Digital Watermarking)。受安全通信、版权保护及篡改认证等应用需求的驱动，信息隐藏发展异常迅猛，信息隐藏的载体多种多样，信息隐藏的方法层出不穷，与信息隐藏对抗的信息隐藏检测技术(即隐密分析技术，steganalysis)方兴未艾，信息隐藏的应用丰富多彩。本书在内容的选择上把握重经典、重启发、重对抗、重适用的原则。即在算法的选择上重点选择了有代表性的经典信息隐藏算法，也选择了部分不是很先进、甚至有瑕疵的算法，但这些算法对启发学生的思考、开拓学生思路有帮助和借鉴作用；突出了信息隐藏的对抗技术——隐密分析算法的选取，同时在内容组织及编著上既注重了方便老师教学，又注重方便学生自学。在算法的介绍上，采用了两种方式：一种是详细具体的算法步骤及性能介绍，便于学生学习时编程实现，以增强对算法精要的深刻理解和认识；另一种是算法原理框图式简介，以便于学生学习时发挥主观能动性，去领悟创新算法。

本书是在作者多年来从事该领域的科研、教学工作实践基础上完成的。全书共分为10章：第1章信息隐藏概论，主要介绍信息隐藏的基本概念、主要分支、主要特性及应用，明确信息隐藏技术与数字水印技术的关系，阐述信息隐藏技术与信息加密技术的区别。第2章信息隐藏相关基础知识，主要介绍与信息隐藏技术紧密相关的人类视觉和听觉系统的掩蔽特性、常用的信息隐藏攻击方法和性能测试软件。第3章图像信息隐藏算法，主要介绍在图像空域进行信息隐藏的经典LSB(Least Significant Bit)算法及其改进算法、在图像变换域进行信息隐藏的经典算法以及其他一些图像信息隐藏算法。第4章视频信息隐藏算法，介绍视频信息隐藏的特点及几个简单的信息隐藏算法。第5章音频信息隐藏算法，主要介绍了在空间域、变换域和压缩域的音频信息隐藏算法。第6章其他载体中的信息隐藏算法，介绍文本、流媒体、信道协议、加密媒体等信息隐藏载体中的信息隐藏方法。第7章图像隐密分析算法，介绍图像LSB隐藏、调色板隐藏、JPEG隐藏的隐密分析算法及几种抗隐密分析的图像信息隐藏算法设计方法。第8章视频隐密分析算法，阐述视频隐密分析的特点，介绍针对具体隐藏算法的隐密分析方法和通用型的隐密分析算法。第9章音频隐密分析算法，主要介绍音频空间域及扩频隐藏的隐密分析方法。第10章信息隐藏的应用与实现，主要介绍基于信息隐藏的隐密通信、篡改认证和电子印章的实现技术及系统开发方面的知识。

本书由柏森统稿。第1、2、3、7章由柏森编写；第4、8章由朱桂斌编写；第5、9章及第2.4节由曹玉强编写；第6章主要由柏森编写，其中6.4节由闫兵编写，6.5节由阳溢编写；第7.4节由季晓勇编写；第10章由朱桂斌和柏森共同编写。本书在编写过程中，得到了重庆通信学院训练部教务科和教保科的大力支持，在此表示深深的谢意！特别感谢上海大学张新鹏教授

提供了第7章部分小节的电子文档！重庆通信学院图像通信实验室研究生刘博文、刘程浩、江铁、郭雨、唐鉴波、郭辉等同学为本书的完成也付出了辛勤的劳动，在此一并表示感谢！

感谢国家自然科学基金（No. 61272043）、重庆市基础与前沿研究计划项目（cstc2013jjB40009）、重庆市科技研发基地能力提升项目（cstc2014pt-sy40003）及重庆市研究生教育教学改革项目（yjg110346、yjg110320、yjg133110）对该书出版的资助。

由于作者水平有限，书中不足和疏漏之处在所难免，敬请同行专家和读者不吝指教，我们将不胜感激。

作 者

2015年7月于林园

# 目　录

# 第1章　信息隐藏概论

本章主要介绍信息隐藏的基本概念、主要分支、主要特性及应用，明确信息隐藏与数字水印的关系，阐述信息隐藏与信息加密的区别。

## 1.1　信息隐藏的基本概念

### 1.1.1　信息隐藏的概念

**信息隐藏**，对应的英文术语是 information hiding 或 data hiding，是利用人类感觉器官的不敏感性（感觉冗余），以及多媒体数字信号本身存在的冗余（数据特性冗余），将有意义的信息（如秘密消息、软件序列号或版权信息等）隐藏于一个载体信息中，不被人的感知系统察觉到，而且不影响载体信息的感知效果和使用价值。这里的“载体信息”可以是数字图像、音频和视频等。在信息隐藏的文献中，所谓的图像信息隐藏、音频信息隐藏及视频信息隐藏分别指的是在图像、音频和视频中隐藏信息，而不是对图像、音频和视频信息进行隐藏。自从 20 世纪 90 年代世界各国开始研究信息隐藏技术以来，已有相当数量的研究成果问世，是信息安全领域研究的热点之一。

信息隐藏最重要的特点在于它不仅隐藏了信息的内容，而且隐藏了信息的存在，因而在信息安全存储和信息安全传输领域体现出重要的应用价值[1]。

### 1.1.2　信息隐藏与数字水印的关系

本书取名《信息隐藏算法及应用》，而众所周知，信息隐藏技术中一个非常重要的分支是数字水印技术。就技术实质而言，数字水印技术中应用的也是隐藏算法。因此，本书取名时没有突出数字水印，这里将两者的关系阐述于后。

**数字水印**（Digital Watermarking）技术是将一些标识信息（序列号、作者信息、公司商标等）直接嵌入数字作品（包括图像、音频、视频、文档、软件等）中，以便保护数字产品的版权，证明产品的真实可靠性，跟踪盗版或者提供产品附加信息，传送隐密信息等。

数字水印是信息隐藏技术的一个重要研究方向，也可看成信息隐藏技术的一个分支。二者的区别在于：①从保护对象看，信息隐藏保护的是嵌入的信息本身，而数字水印保护的是载体信息，即数字作品本身；②从视觉感知看，信息隐藏一定是不可感知的，而数字水印不一定要求不可感知；③从嵌入性能看，信息隐藏强调的是不可感知性（又称为隐蔽性）和隐藏容量；数字水印强调的是鲁棒性，即抵抗各种有意或无意对数字作品进行攻击的能力。

数字水印有很多特性，其中最重要的 4 个特性是保真度、鲁棒性、容量和安全性，更详细的特性介绍可参看文献[2]。

**1. 保真度（Fidelity）**

保真度是衡量数字作品在被处理前后的相似性，也称为不可感知性。数字作品在嵌入水

印信息之后在感知上要达到一定的要求,这个要求并不一定是水印的不可见或者可见,要根据水印的应用场合来确定。

**2. 鲁棒性(Robustness)**

鲁棒性指的是数字作品在经过信号处理操作后,仍能够检测到水印的能力。常规的信号处理包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。数字水印主要用于版权保护,其中易损水印(Fragile Watermarking),主要用于完整性保护,这种水印同样是在数字作品的内容数据中嵌入不可见的信息。当内容发生改变时,这些水印信息会发生相应的改变,从而可以鉴定原始数据是否被篡改。

**3. 容量(Capacity)**

容量也称嵌入率、加载率或者有效载荷,指的是在一个数字作品中最多可以嵌入水印的比特数。嵌入的水印信息必须足以表示多媒体内容的创建者或所有者的标志信息,或购买者的序列号,这样有利于解决版权纠纷,保护数字产权合法拥有者的权益。

**4. 安全性(Security)**

安全性是指它抵御敌手攻击的能力。敌手攻击是指为了阻碍水印用途的专门处理,包括未经授权的删除、未经授权的嵌入和未经授权的检测。未经授权的删除和嵌入被称为主动攻击,因为这些攻击修改了数字作品。未经授权的检测不修改数字作品,因此被称为被动攻击。

### 1.1.3 信息隐藏与信息加密的区别

**隐密术**(Steganography)或称**隐写术**,是指将信息隐藏于载体信息的技术,是信息隐藏的重要分支之一,也是信息隐藏中的重要技术之一。信息隐藏与信息加密的区别,实质上就是隐密术与加密术的区别。

隐密术与加密术的根本区别是:密码加密是将信息的语义隐藏起来,看上去为随机的乱码(图1.1.1(a))。对手得到加密信息后,从感知器官上已经知道其中有秘密信息存在,只是不知道秘密信息的含义而已。而隐密术是将秘密信息本身的存在性隐藏起来,对手得到含有秘密信息的载体(文本、图像、音频、视频等)后,从感觉器官上并不知道有秘密信息存在(图1.1.1(b)),因而也就降低了信息被攻击的可能性。为了增强攻击的难度,也可将加密术与隐密术结合起来,即先用加密术进行加密,再用隐密术进行隐藏(图1.1.1(c))。更重要的是:加密术的问题可通过信息论来阐述,而隐密术的很多核心问题已无法用信息论来解释。

采用密码技术开发出来的密码系统,对秘密信息的处理是将其转换为密文。显然,这些杂乱无章的密文,会引起攻击者的注意并激发他们破解秘密信息的热情。现在,计算技术的飞速发展使得对密码破译的能力越来越强,因此,常规密码的安全性受到了很大的威胁。单单通过增加密钥的长度,来增强加密系统的机密等级已经不再是唯一可行的方法。而经过隐密术隐藏的机密信息看起来与一般的非机密资料没有两样,它们隐匿于千千万万的信息之中,很难引起攻击者的注意,因而十分容易逃过攻击者的破解。其道理如同生物学上的保护色,巧妙地将自己伪装隐藏于环境之中,免于被天敌发现而遭受攻击。这一点是传统密码系统所欠缺的,也是隐密术区别于加密术的最根本的特性。

其实,通过对隐密术与加密术的英文字面含义的分析,也可以看出它们的分别。信息隐密术 steganography 这个词来源于希腊文,它是由 steganos 和 graphein 两个希腊字合成的,意为"covered writing"即"隐写"。而加密术(Cryptography)也来自希腊文,意为"secret writing"即

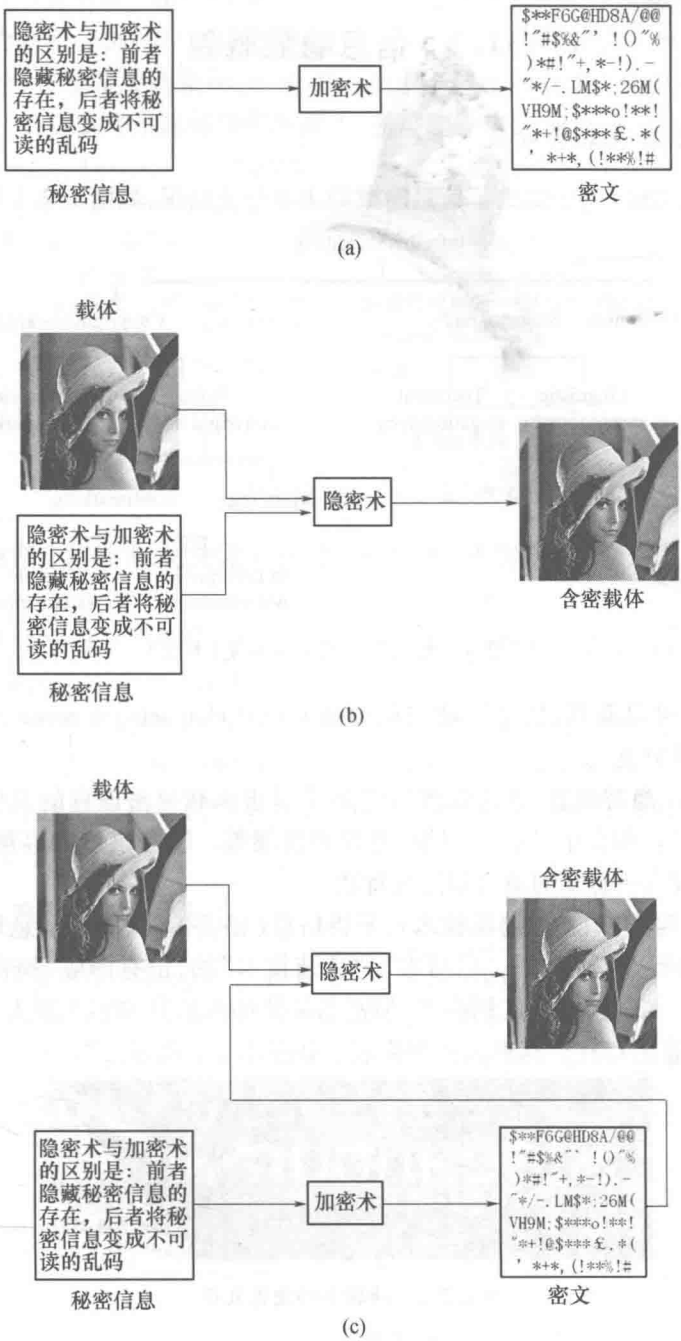


图 1.1.1　加密术与隐密术的比较

(a) 加密术示意图；(b) 隐密术示意图；(c) 加密术与隐密术结合示意图。

“密写”。经密码加密的文字，看起来可能是一堆不可读的码字，这样反而会激发密码信息截获者破译密码的兴趣。因此，以信息隐藏方式实现的隐密通信的最大优点是：除通信双方以外的任何第三方并不知道秘密通信存在的事实，使得秘密信息通信从“看不懂”变为“看不见”，以减少被攻击的可能性。

## 1.2 信息隐藏概貌

### 1.2.1 信息隐藏主要分支

Petitcolas 等在文献[1]中给出了信息隐藏的主要分支情况，如图 1.2.1 所示。

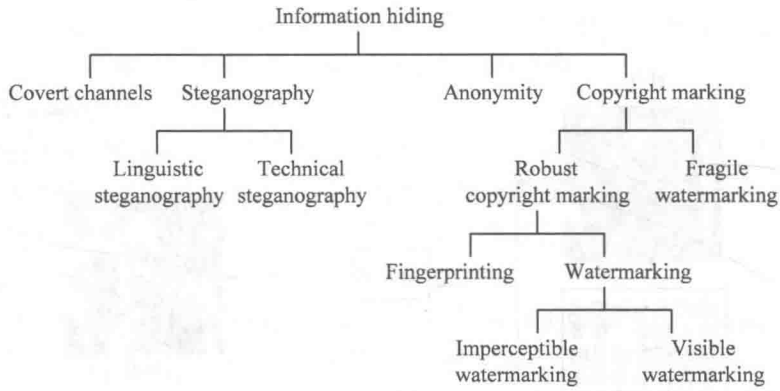


图 1.2.1 信息隐藏的主要分支(英文)

从图 1.2.1 中可以看到，信息隐藏主要包括 Covert channels、Steganography、Anonymity 和 Copyright marking 等分支。

Covert channels(**隐密信道，隐蔽信道**)：它实质是指承载秘密信息的其他信息(可称为掩护信息或掩护媒体)。如文字、图形、图像、音频和视频等。隐密信道的容量实质就是掩护信息中可隐藏的、不被人所感知的最大信息比特数。

Steganography(**隐密术，信息隐藏技术**)：是将信息(秘密信息、版权信息等)隐藏在其他信息之中的技术。有译成“隐密术”、“隐写术”、“伪装技术”的，也有译成“掩密术”、“隐蔽术”、“隐密学”的，等等。与加密术的区别在于：加密术是使秘密信息内容不被人看懂和理解；而隐密术是隐藏秘密信息的存在。其形象的图像表示如图 1.2.2 所示。

图 1.2.2 隐密术的图像表示

Anonymity(**匿名**)：信息隐藏中的匿名技术就是设法隐藏消息的来源，即隐藏消息的发送者和接收者。例如：收发信者通过一套邮件转发器或路由器，就能够实现掩盖信息的痕迹的目的，条件是只要这些中介环节相互不串谋。因此，剩下的是对这些手段的信赖。需要注意的是，不同的情况取决于谁要“被匿名”，是发信者，还是收信者，或者两者皆要。网上浏览等将问题集中于收信者的匿名，而电子邮件用户关心的是发信者的匿名。

Copyright marking(**版权标志**)：是利用信息隐藏技术在数字作品(包括文本、图像、音频、视频等)中嵌入表明该作品受版权保护的标记。其作用是向公众昭示作品受版权保护，或以资证明作品归属其所有人等。

在密码学中，有加密术就有密码破译技术，同样，在信息隐藏中，有隐密术就应该有揭示信息隐藏的技术，称为隐密分析技术（Steganalysis）。图 1.2.1 没有列出来，但近年的发展表明，该技术随着信息隐藏技术发展而发展，形成了一个不可忽视的分支。因此这里将其列出，如图 1.2.3所示。其中的虚线表示随着研究的深入，还可能继续发展出新的分支。

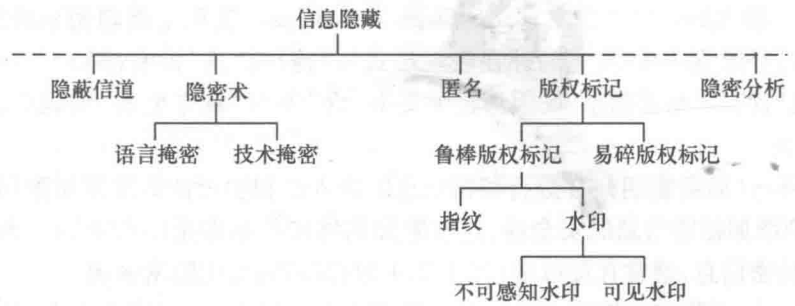


图 1.2.3　信息隐藏的主要分支（中文）

Steganalysis（**隐密分析技术，揭密术**）：是对各种媒体（或信息）进行分析，揭示其中是否含有秘密信息的技术。

此外，上述分支还可进一步细分，这里就不一一介绍，可参考文献[1]。与图 1.2.1 对应的信息隐藏主要分支的中文术语如图 1.2.3 所示。

因为信息隐藏是正在发展的新兴技术，还可能进一步发展，因此在信息隐藏的第一次分支时，两端用虚线表示，表明存在潜在的发展空间，还可能形成新的分支，这是尤新刚在第三届信息隐藏全国学术研讨会上提出来的[3]。例如，隐密分析技术是 2004 年前后才发展起来的分支。

### 1.2.2　信息隐藏系统构成

第一届国际信息隐藏学术研讨会中，Pfitzman 对隐密术的系统构成做了介绍，给出了隐密术的一般系统构成，如图 1.2.4 所示[4]。其中的数据类型（ < datatype > ）可以是任何的“文本”、“音频”、“图像”及“视频”等信息，现给出对应的中文术语及解释，在解释中使用“信息”代替 < datatype > 。有时，为使表述更贴切，也用“媒体”或“载体”代替 < datatype > 。

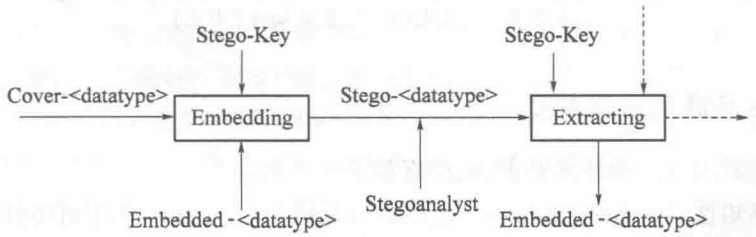


图 1.2.4　隐密术的一般系统构成（英文）

（1）Embedded- < datatype > （**秘密信息**）：英文原意为被嵌入信息，这里可理解为秘密信息或版权信息等，是指隐藏在公开信息中的秘密信息，也即发信者想要发送给收信者而不想让第三者知道的信息。

（2）Cover- < datatype > （**掩护信息，掩护媒体**）：指承载秘密信息的载体信息，是用来隐藏秘密信息的，是 Stego- < datatype > 的原始形式，在隐藏秘密信息的过程中可对它进行选择，如

载体选为视频、图像、音频和文本，则分别称为掩护视频、掩护图像、掩护音频和掩护文档。有时也统称为“掩护媒体”。

(3) Stego- < datatype > (**含密信息，含密媒体**)：该术语的中文翻译最多，有“载密信息”、“隐密信息”、“伪装信息”等。“隐密信息”与“掩护信息”一字之别，不易区分，“伪装信息”及“载密信息”又不能很好体现其真实含义。Stego- < datatype > 实质上指隐密系统的输出信息，此时秘密信息已经隐藏在其中，它的外在表现形式与“掩护信息”没有感知上的差别，为了体现和突出其中已含有了秘密信息，又因为在中文里“含”字有“藏在里面”的意思，因此主张用“含密信息”一词。

(4) Stego-Key(**隐密密钥**)：在进行秘密信息的嵌入过程中可能需要使用附加的秘密数据(Secret Data)来增加秘密信息的安全性，这些附加的秘密数据即是隐密密钥。为了提取掩护信息中嵌入的秘密信息，通常在提取端(图 1.2.4 的右端)需要用隐密密钥。

(5) Stegoanalyst(**隐密分析者或攻击者**)：隐密术中的隐密分析者(攻击者)的目的是检测出隐密事实的存在甚至破译出秘密信息，其侧重点是检测出隐密事实的存在。攻击者分为主动攻击者和被动攻击者，被动攻击者的目的是检测出隐密事实的存在，而主动攻击者不仅要检测出隐密事实的存在，还要破坏秘密信息，甚至在该载体中嵌入自己的信息，以欺骗秘密信息的接收者。

因此，基于上述考虑，隐密术系统的一般构成，中文表述如图 1.2.5 所示。在这个系统构成图中，右端向下的虚线箭头表示在从“含密信息”中提取秘密信息时，可能需要原始的掩护信息，这样的嵌入算法通常称为“**非盲的信息隐藏算法**”，或“**非盲的隐密方案**”、“**非盲的提取**”；否则称为“**盲的信息隐藏算法**”、“**盲提取算法**”等。向右的虚线箭头表示，非秘密的接收者所见到或听到的与掩护信息视觉或听觉一致的含密信息。

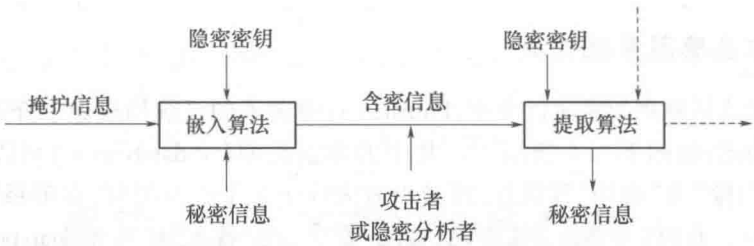


图 1.2.5　隐密术的一般系统构成(中文)

### 1.2.3　信息隐藏主要特性

根据信息隐藏的目的和技术要求，它应有如下一些特性[5]：

(1) **不可感知性**(Imperceptibility)。包括不可见性(Invisibility)和不可听性(Inaudibility)，指利用人类视觉系统或听觉系统属性，经过一系列隐密术处理，掩护信息必须没有明显的降质现象，而隐藏其中的秘密信息无法被人看到或听见，也即人的视觉或听觉觉察不出掩护信息与含密信息的差别。不可感知性也称为**透明性**或**隐蔽性**，这是信息隐藏技术最根本的特性和要求。

(2) **不可检测性**(Undetectability)。指含密信息与掩护信息具有一致的数据特性，如具有一致的统计噪声分布等，使非法拦截者即使通过数据特性的数学分析也无法判断是否有隐藏信息。