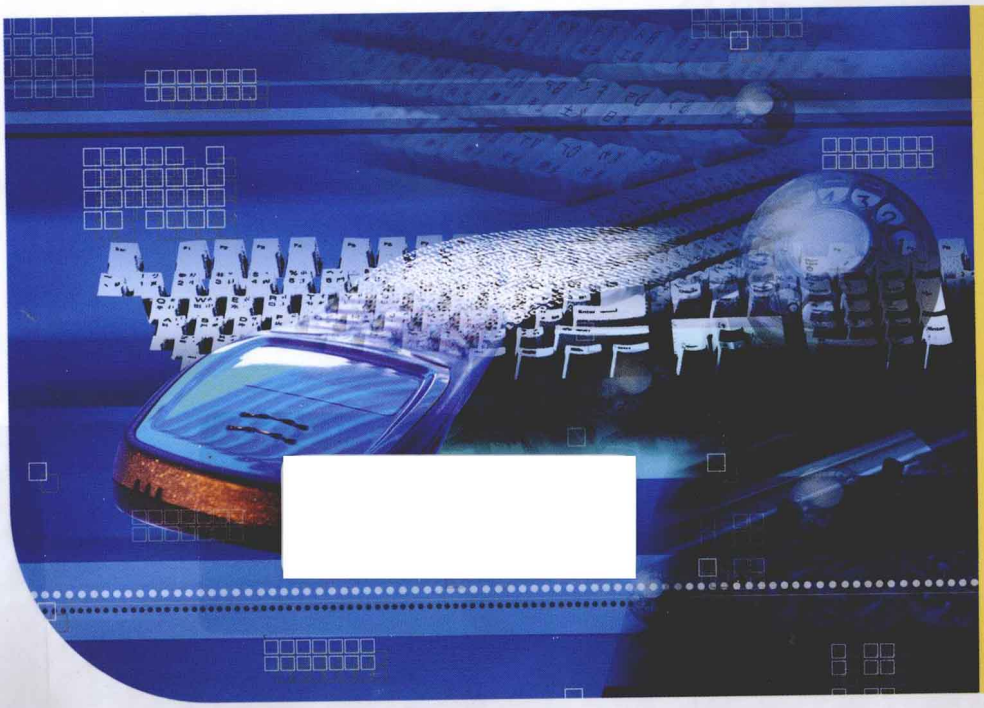
信息安全专业系列教材

信息安全新技术

XINXI ANQUAN XINJISHU

（第2版）

杨义先　马春光　钮心忻　孙建国⊙编著



北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

信息安全新技术

（第 2 版）

编　著　杨义先　马春光
钮心忻　孙建国

北京邮电大学出版社
www. buptpress. com

内 容 简 介

本书对国内外网络信息安全方面有代表性的最新技术作了系统而详细的总结。全书共10章，分别对信息隐藏技术、数字水印技术、多媒体信息伪装技术、入侵检测技术、电子支付技术、网络安全协议、智能卡安全技术、公钥基础设施(PKI)、物联网安全和无线网络安全技术等进行了充分的论述。

本书内容翔实，叙述通俗易懂。可作为通信与电子系统、信号与信息处理、密码学、信息安全、计算机应用等专业的研究生、本科生和大专生相关课程的教学参考书。也可作为从事国家网络信息安全工作人员提高业务水平的实用工具书。同时，本书也可作为国内网络安全、计算机安全和信息安全领域相关人员的技术培训教材。

图书在版编目(CIP)数据

信息安全新技术/杨义先等编著. --2版. --北京：北京邮电大学出版社，2013.1
ISBN 978-7-5635-3357-2

Ⅰ.①信… Ⅱ.①杨… Ⅲ.①计算机网络—安全技术—高等学校—教材 Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2012)第299273号

书　　名：信息安全新技术(第2版)
著作责任者：杨义先　马春光　钮心忻　孙建国　编著
责任编辑：张珊珊
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路10号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京联兴华印刷厂
开　　本：720 mm×1 000 mm　1/16
印　　张：15.5
字　　数：294千字
印　　数：1—3 000册
版　　次：2002年3月第1版　2013年1月第2版　2013年1月第1次印刷

ISBN 978-7-5635-3357-2　　定　价：32.00元

· 如有印装质量问题，请与北京邮电大学出版社发行部联系 ·

目　录

试读结束，需要全本PDF请购买 www.ertongbook.com

第1章 信息隐藏技术

几千年的历史已经证明：密码是保护信息机密性最有效的手段之一。通过使用密码技术，人们将明文加密成他人看不懂的密文，从而阻止了信息的泄露。但是，在如今开放的因特网上，谁也看不懂的密文无疑成了“此地无银三百两”的标签。“黑客”完全可以通过跟踪密文来“稳、准、狠”地破坏合法通信。为了对付这类“黑客”，人们采用以柔克刚的思路重新启用了古老的信息隐藏技术，并对这种技术进行了现代化的改进，从而达到了迷惑“黑客”的目的。当然，毋庸讳言，信息隐藏技术在国内外重新受到青睐的另一个重要原因是相关用户希望通过此项技术来回避密码管制的政策风险。

1.1 信息隐藏的历史沿革

随着多媒体技术和 Internet 的迅猛发展，互联网上的数字媒体应用正在呈爆炸式的增长，越来越多的知识产品以电子介质的方式在网上传播。数字信号处理和网络传输技术可以对数字媒体（数字声音、文本、图像和视频）的原版进行无限制的任意编辑、修改、复制和散布，造成数字媒体的知识产权保护和信息安全的问题日益突出，并已成为数字世界的一个非常重要和紧迫的议题。因此，如何防止知识产品被非法复制及传播，也是目前亟需解决的问题。传统的信息安全技术无法解决这些新问题。因此，国际上近几年来开始提出并尝试一种新的关于信息安全的概念，开发设计不同于传统密码学的技术，即将机密资料信息秘密地隐藏于一般的文件中，然后再通过网络传递。由于非法拦截者从网络上拦截下来的伪装后的机密资料并不像传统加密过的文件一样看起来是一堆会激发非法拦截者破解机密资料动机的乱码，而是看起来和其他非机密性的一般资料无异，因而十分容易逃过非法拦截者的破解。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中，免于被天敌发现而遭受攻击。这一点是传统加解密系统所欠缺的，也是信息隐藏基本的思想。

顾名思义，所谓信息隐藏，就是将秘密信息秘密地隐藏于另一非机密的文件内容之中。其形式可为任何一种数字媒体，如图像、声音、视频或一般的文档等。信息隐藏的首要目标是隐藏的技术要好，也就是使加入隐藏信息后的媒体目标的降

质尽可能小,使人无法看到和听到隐藏的数据,达到令人难以察觉的目的。信息隐藏还必须考虑隐藏的信息在经历各种环境、操作之后而免遭破坏的能力。比如,信息隐藏必须对非恶意操作(如图像压缩和信号变换等)具有相当的免疫力。信息隐藏的数据量与隐藏的免疫力始终是相互矛盾的,不存在一种完全满足这两种要求的隐藏方法。通常只能根据需求的不同有所侧重,采取某种妥协,使一方得以较好的满足,而使另一方作些让步。从这一点看,实现真正有效的信息隐藏的难度较大,很具有挑战性。

信息隐藏技术和密码技术的区别在于:密码仅仅隐藏了信息的内容,而信息伪装不但隐藏了信息的内容而且隐藏了信息的存在。信息隐藏技术提供了一种有别于加密的安全模式,其安全性来自于对第三方感知上的麻痹性。在这一过程中载体信息的作用实际上包括两个方面:①提供传递信息的信道;②为隐藏信息的传递提供伪装。随着计算机网络和多媒体技术的发展,信息隐藏技术的应用也在不断扩展,载体信息的作用也在发生着变化。例如:用于版权保护的数字水印技术,这时的载体信息是具有某种商业价值的信息,而秘密信息则是一些具有特殊意义的标识或控制信息。应该注意到,密码技术和信息隐藏技术并不是互相矛盾、互相竞争的技术,而是互补的。它们的区别在于应用的场合不同、要求不同,但可能在实际应用中需要互相配合。例如:将秘密信息加密之后再隐藏,这是保证信息安全的更好的办法,也是更符合实际要求的方法。

数字化的信息隐藏技术的确是一门全新的技术,但是它的思想其实来自于古老的隐写术。大约在公元前 440 年,隐写术就已经被应用了。当时,一位剃头匠将一条机密消息写在一位奴隶的光头上,然后等到奴隶的头发长起来之后,将奴隶送到另一个部落,从而实现了这两个部落之间的秘密通信。类似的方法,在 20 世纪初期仍然被德国间谍所使用。实际上,隐写术自古以来就一直被人们广泛地使用。隐写术的经典手法有很多,此处仅列举一些典型例子:

- 使用不可见墨水给报纸上的某些字母作上标记来向外发送消息。
- 在一个录音带的某些位置加一些不易察觉的回声等。
- 将消息写在木板上然后用石灰水把它刷白。
- 将信函隐藏在信使的鞋底里或妇女的耳饰中。
- 由信鸽携带便条传送消息。
- 通过改变字母笔画的高度或在掩蔽文体的字母上面或下面挖出非常小的小孔(或用无形的墨水印制作非常小的斑点)来隐藏正文。
- 在纸上打印各种小像素点组成的块来对诸如日期、打印机标识符、用户标识符等信息进行编码。
- 将秘密消息隐藏"在大小不超过一个句号或小墨水点的空间里"(1857 年)。

- 将消息隐藏在微缩胶片中(1870 年)。
- 把在显微镜下可见的图像隐藏在耳朵、鼻孔以及手指甲里(1905 年);或者先将间谍之间要传送的消息经过若干照相缩影步骤后缩小到微粒状,然后粘在无关紧要的杂志等文字材料中的句号或逗号上(第一次世界大战期间)。
- 在印刷旅行支票时使用特殊紫外线荧光墨水。
- 制作特殊的雕塑或绘画作品,使得从不同角度看会显出不同的映象。
- 藏头诗,或者歧义性的对联、文章等文学作品。
- 在乐谱中隐藏信息(简单地将字母表中的字母映射到音符)。
- 我国古代还有一种很有趣的信息隐藏方法,即消息的发送者和接收者各有一张完全相同的带有许多小孔的掩蔽纸张,而这些小孔的位置是被随机选择并戳穿的,发送者将掩蔽纸张放在一张纸上,将秘密消息写在小孔位置上,移去掩蔽纸张,然后根据纸张上留下的字和空格编写一段掩饰性的文章。接收者只要把掩蔽纸张覆盖在该纸张上就可立即读出秘密消息。直到 16 世纪早期,意大利数学家 Cardan 又重新发现了这种方法,该方法现在被称作卡登格子隐藏法。
- 利用掩蔽材料的预定位置上某些误差和风格特性来隐藏消息。比如,利用字的标准体和斜体来进行编码,从而实现信息隐藏;将版权信息和序列号隐藏在行间距和文档的其他格式特性之中;通过对文档的各行提升或降低三百分之一英寸来表示 0 或 1 等等。

信息隐藏研究虽然可以追溯到古老的隐写术,但在国际上正式提出数字化信息隐藏研究则是在 1992 年。国际上的第一届信息隐藏研究会于 1996 年在剑桥大学举行,这次会议推动了信息隐藏的理论和技术研究。台湾"国立大学"通信和多媒体实验室也做了大量的工作。1998 年在美国俄勒冈州召开了第二届信息隐藏研究会,1999 年 9 月 29 日至 10 月 1 日在德国 Dresden 召开了第三届信息隐藏研讨会。最近,IEEE ICIP、EUSIPCO 的会议中也都研讨了信息隐藏。中国也在 1999 年 12 月 11 日,由北京电子技术应用研究所组织,召开了第一届信息隐藏学术研讨会,2000 年 6 月 17 日至 18 日召开了第二届信息隐藏学术研讨会。2000 年 1 月 15 日至 16 日,国家 863 计划智能计算机专家组、中国科学院自动化研究所和北京邮电大学信息安全中心成功举办了数字水印技术研讨会。2001 年 9 月,全国第三届信息隐藏学术研讨会又在西安召开。如今,信息隐藏已经成为当前国际上的研究热点。

信息隐藏技术作为一种新兴的信息安全技术已经被许多应用领域所采用。越

试读结束,需要全本PDF请购买 www.ertongbook.com

来越多的数字视频、声频信号及图像被“贴”上了不可见的标签,这些标签往往携带隐藏了的版权标识或序列号来防止非法复制。军事系统广泛地采用信息安全技术,不只用加密隐藏消息内容,还用信息隐藏技术来隐藏消息的发送者、接收者甚至消息本身。类似的技术还用在移动电话系统及其他的电子媒介系统中。

信息隐藏术也正日益受到研究机构和业界的关注。主要动力来自人们对版权问题的关注。随着音像、图像和其他产品的数字化,数字产品的盗版更加容易,这引起了音乐、电影、书籍和软件发行商的极大关注。因此引发了信息隐藏术的重要分支领域“数字水印”和“数字指纹”的研究。前者可以作为版权争端的法律凭证,用来指控盗版者;后者则可以用来追查盗版者。

数字水印技术为电子数据的版权保护等需要提供了一个潜在的有效手段,因而引起了国际学术界与企业界的广泛关注,是目前国际学术界研究的一个前沿热门方向。数字水印是携带所有者版权信息的一组辨别数据。数字水印被永久地嵌入到多媒体数据中用于版权保护并检查数据是否被破坏。数字水印技术作为在开放的网络环境下保护版权的新型技术,它可以确立版权所有者,识别购买者或者提供关于数字内容的其他附加信息,并将这些信息以人眼不可见的形式嵌入在数字图像、数字音频和视频序列中,用于确认所有权和跟踪行为。另外,它在证据篡改鉴定、数据的分级访问、数据的跟踪和检测、商业和视频广播、互联网数字媒体的服务付费、电子商务的认证鉴定等方面也具有十分广阔的应用前景。自从 1993 年,尤其是 1995 年或 1996 年以来引起了工业界的浓厚兴趣,日益成为国际上非常活跃的研究领域。

尽管版权保护是发展数字水印技术的原动力,但人们发现数字水印还具有其他的一些重要应用,如版权保护、真伪鉴别、隐蔽通信、标识隐含等。这些研究预示着商业上的巨大应用前景。例如:数字水印技术在 DVD 的发行中的应用也有很大的市场潜力。DVD 联盟建议提出一个版权保护方案来加强复制管理,因为现有的 DVD 播放器允许 Vedio 的无限制拷贝不利于版权保护。该建议提出 home vedio 将不作标记,电视广播制品将标识为“一次拷贝”,商业音像制品标识为“禁止拷贝”,播放器将根据这些标记作出相应的动作。

目前,国外研究信息伪装的学术机构有麻省理工学院的媒体实验室、IBM 等一些机构和一些大学。研究的重点在如何将信息隐藏到图像、声音和文字之中。目前对于信息隐藏应用在数字产品的著作权保护方面(或称为数字水印)的研究较多。瑞士洛桑联邦工技院信号处理实验室和通信研究所、美国的 NEC 研究所等都作出了不少成就。除了学术界的研究之外,也有一些公司开发出一些软件如:Fraunhofer's SYSCOP、HIGHWATER FBI、Digimarc Corporation、DICE's Argent Digital Watermark 等,提供有关数字产品著作权保护的服务。国内研究信息伪装

的科研院所有北京邮电大学信息安全中心、中国科学院自动化研究所模式识别国家重点实验室、北方工业大学、清华大学、北京理工大学、北京电子技术应用研究所、国家信息安全测评认证中心等单位。

基于信息隐藏技术而建立起来的一个安全的信息隐藏系统可以用如下的非正式定义来描述：一个安全的信息隐藏系统应该是任何了解系统但不知道密钥的敌手不能得到任何有关已发生的通信的证据(甚至怀疑的范围)。它将遵守一个核心准则：被广泛使用的信息隐藏程序步骤应该公开发布，就像商用的密码算法和协议那样。所以人们可以期望版权标记系统的设计者会公开发布他们使用的系统机制和原理，并且系统的安全性仅依赖于其使用密钥的保密性。

一个理想的信息隐藏系统应该具有以下特性(以载体为静止图像为例)：

(1) 隐蔽性。这是信息伪装的基本要求，经过一系列隐藏处理的图像没有明显的降质，隐藏的信息无法看见或听见。

(2) 安全性。隐藏的信息内容应是安全的，应经过某种加密后再隐藏，同时隐藏的具体位置也应是安全的，至少不会因格式变换而遭到破坏。

(3) 对称性。通常，隐藏信息的隐藏和提取过程具有对称性，包括编码、加密方式，以减少存取难度。

(4) 可纠错性。为了保证隐藏信息的完整性，使其在经过各种操作和变换后仍能很好地恢复，通常采取纠错编码方法。

需要指出的是，对信息隐藏技术的不同应用，各自有着进一步不同的具体要求，并非都满足上述要求。信息隐藏技术包含的内容范围十分广泛，可以作如下分类(如图 1.1 所示)。

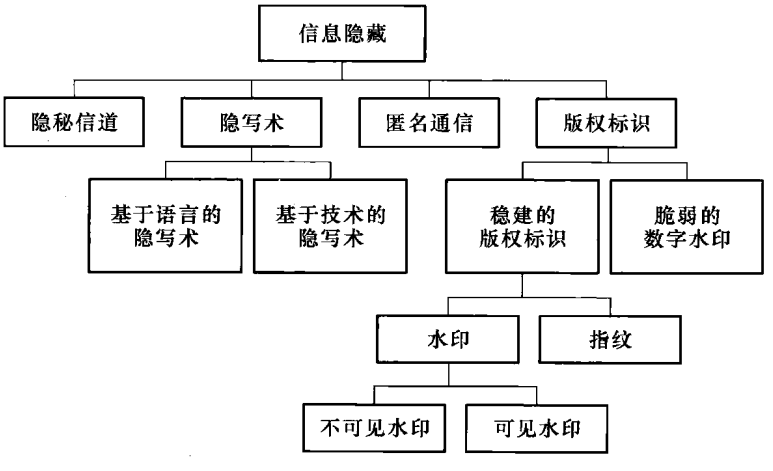


图 1.1 信息隐藏技术的分类

(1) 隐写术:一般指那些进行秘密通信的技术的总称,通常把秘密信息嵌入或隐藏在其他不易受怀疑的数据中。伪装方法通常依赖于第三方不知道隐蔽通信的存在的假设,而且主要用于互相信任的双方的点到点秘密通信。因此,隐写术一般稳健性较弱。例如:在数据改动后隐藏的信息不能被恢复。

(2) 数字水印:数字水印就是向被保护的数字对象(如静止图像、视频、音频等)嵌入某些能证明版权归属或跟踪侵权行为的信息,可以是作者的序列号、公司标志、有意义的文本等等。同隐写术相反,水印中的隐藏信息具有能抵抗攻击的稳健性。即使知道隐藏信息的存在,对攻击者而言,要毁掉嵌入的水印仍很困难(理想的情况是不可能),虽然水印算法的原理是公开的。在密码学中,这就是众所周知的 Kerkhoffs 原理:加密系统在攻击者已知加密原理和算法但不知道相应的密钥的仍是安全的。稳健性的要求使得水印算法中在宿主数据中嵌入的信息要比隐写术中要少。水印技术和隐写术更多的时候是互补的技术而不是互相竞争的。

(3) 数据隐藏和数据嵌入:通常用在不同的上下文环境中,它们一般指隐写术,或者指介于隐写术和水印之间的应用,在这些应用中嵌入数据的存在是公开的,但没必要保护它们。例如:嵌入的数据是辅助的信息和服务,它们可以是公开得到的,与版权保护和控制存取等功能无关。

(4) 指纹和标签:指水印的特定用途。有关数字产品的创作者和购买者的信息作为水印而嵌入,每个水印都是一系列编码中的唯一的一个编码,即水印中的信息可以唯一地确定每一个数字产品的拷贝,因此,它们被称为指纹或者标签。

1.2 信息隐藏的基本手段

信息隐藏(或称为信息伪装)的手段非常多,从隐藏信息的载体来看,有以下几种。

(1) 在文本中隐藏信息

利用语言的自然冗余性,将信息直接编码到文本内容中去;或者将信息直接编码到文本格式中去(比如,调整字间距或行间距);如果载体文本以固定格式(像 HTML、LATEX 或 Postscript 文件)的形式传输,则信息可以嵌入到格式中而不是消息内容本身,秘密信息可以存储在行间距或列间距中,如果两行之间的距离小于某个门限值,就表示隐藏的信息是"0",否则隐藏的信息是"1"(类似的方法也可用于传输 ASCII 码文本的信息:偶尔的附加空格字符可以用来构成秘密信息);将信息编码隐藏在字处理系统的断行处。

在文本消息中能否存在安全和健壮的信息隐藏仍然是一个悬而未决的问题。一个攻击者只需简单地重新调整文本的格式,就可以破坏掉所有嵌入在文本格式

中的信息。另外，文本消息可以以各种不同的格式进行存储(像 HTML、TEX's DVI、Postscript、PDF，或者 RTF)，从一种格式转化到另一种格式对嵌入的消息也有很大的损害。

(2) 利用阈下信道隐藏信息

比如，利用 ElGamal 型数字签名方案(其实别的数字签名方案也行)，按如下方式，可以实现隐藏信息的通信。为了生成 ElGamal 密钥，用户首先选择一个素数 p，选择 Z_p^* 的一个生成元 g 和一个随机数 $x < p$。然后用户计算 $y = g^x \bmod p$，于是公钥为三元组$\langle y, g, p\rangle$，私钥为 x。为了对消息 M 签名，用户首先选择一个随机数 k，且使 k 与$(p-1)$互素，计算 $a = g^k \bmod p$，并从方程：$M \equiv xa + kb \bmod (p-1)$求解 b。签名就是$\langle a, b\rangle$。为验证该签名，验证方程：$y^a\ a^b \equiv g^M \bmod p$。为了在数字签名中隐藏附加的秘密信息，接收者必须获得发送者的私钥 x。为了将秘密消息 M' 与某些无关紧要的消息 M 一起发送，M'在基本的 ElGamal 方案(也就是，发送者计算 $a = g^{M'} \bmod p$ 并从方程 $M \equiv xa + M'b \bmod (p-1)$求解 b)中扮演随机数 k 的角色，签名仍然是$\langle a, b\rangle$并像上述那样进行验证。如果接收者已获得 x，则可以利用扩展的欧几里德算法重构 M'(给予更强的条件)。

(3) 利用操作系统中的隐蔽信道来隐藏信息

在一个操作系统里，运行在高安全级别的进程 A 能够向一个磁盘写数据，而运行在低安全级别的另一个进程 B 能够访问其文件表(即由前一个进程创建的所有文件的名字和大小)，虽然它没有访问数据本身。这种情形可以导致一个隐蔽信道：进程 A 通过选择合适的文件名和大小来向 B 发送信息。一个 IP 包的时间戳可以用来传输 1 比特数据(偶时间增量发送的包代表逻辑 0，奇时间增量发送的包代表逻辑 1)。以太网物理层的碰撞检测系统可以被修改，因特网控制消息可以被利用等等。

(4) 在可执行文件中隐藏数据

可执行文件以这样的方式包含许多冗余信息，如可以安排独立的一串指令，或者选择一个指令子集解决特定的问题。代码迷乱技术最初主要用来保护软件产品的不正当再处理，它能用来在可执行文件中存储额外的信息。这种技术试图把一个程序 P 变换成一个功能等价的程序 P'，而 P'更难以反向编程，在信息伪装应用中，秘密信息隐藏在所用的一系列变换中。如果 $P \rightarrow P'$是源程序 P 到目标程序 P'的一个变换，并满足两个条件：如果 P 未能终止或以一个错误信息终止，则 P'可以终止也可以不终止，否则 P'终止并产生与 P 一样的输出。Collberg 等人列出了许多可用来迷乱 Java 代码的技术，它们中有“分支插入”变换和“循环条件插入”变换。第一个变换通过写两个功能等价的代码块引入一个额外的分支，而代码块根据分支条件来选择。第二个变换扩展循环条件使得循环执行总时间不受影响。

(5) 在视频通信系统中隐藏信息

在一个综合业务数字网(ISDN)视频会议系统里,可以嵌入一个 GSM 电话对话(带宽高达 8 kbit/s)而不会使视频信号严重降质,从而形成了一个秘密通信。

但是,到目前为止,研究最成熟的信息隐藏载体是图像。所以,下面重点介绍如何将机密信息隐藏进图像中去。

1.2.1 信息隐藏的替换方法

基本的信息隐藏替换系统,就是试图用秘密信息比特替换掉伪装载体中不重要的部分,以达到对秘密信息进行编码的目的。如果接收者知道秘密信息嵌入的位置,他就能提取出秘密信息。由于在嵌入过程中仅对不重要的部分进行修改,发送者可以假定这种修改不会引起被动攻击者的注意。目前,比较常用的替换方法有以下几种。

(1) 最低比特位替换

每一幅图像都可以由其位平面来唯一地表示。而位平面中的最低几位比特对人的视觉系统很不敏感,将这些比特替换成机密消息的相应比特就是一种很具有迷惑性的信息隐藏手法。利用此方法在伪装载体中能隐藏数量惊人的信息,即使对载体有影响,也几乎察觉不到。在这类信息隐藏方法中主要使用无损图像格式,并且数据能直接处理和恢复。在这些系统中,除了应用替换手段外,还可采用压缩和加密技术,以提供更好的隐藏数据的安全性。最低比特位替换方法的主要缺点是对伪装载体稍微更改的抵抗力相当脆弱。克服此脆弱性的一种方法是采用伪随机数发生器以相当随机的方式来扩展秘密信息,如果通信双方使用同一个伪装密钥作随机数发生器的种子,那么它们能生成一个随机序列,并且把它们和索引一起按适当的方式生成隐藏信息位置来进行信息传送。从而,可以伪随机地决定两个嵌入位的距离。由于接收者能获得种子和随机数发生器的信息,因此能获得整个元素的索引序列。

(2) 伪随机置换

把秘密信息比特随机地分散在整个载体中。由于不能保证随后的消息位按某种顺序嵌入,因此这种技术进一步增加了攻击的复杂度。发信方使用一个伪随机数发生器创建一个索引序列 $j_1,\cdots,j_{l(m)}$,并将第 k 个消息比特隐藏在索引为 j_k 的载体元素中。注意由于对伪随机数发生器的输出不加任何限制,一个索引值在序列中可能出现多次,称这种情况为碰撞。如果一个碰撞发生,发信方将可能在一个载体元素中插入多个消息比特,因而破坏了这些信息。如果与载体元素的个数相比,消息比特较少的话,发生碰撞的概率能够被忽略,并且被破坏的比特能使用纠错编码进行重构。当然这仅仅适合很短的秘密信息。例如,如果载体是一个 600×600 像

素的图像并且在嵌入过程中选择 200 个像素，那么至少发生一次碰撞的概率大约是 5%。另一方面，如果进行信息传输时使用了 600 个像素，则至少发生一次碰撞的概率增大到 40%左右。因此，只有对非常短的消息，才能忽略碰撞的概率。可以采取一些额外的办法来解决碰撞问题，比如，发信方可以在一个集合 B 中记录所有已经使用过的载体元素。如果在嵌入过程中，一个载体元素以前没有使用过，就把它的索引加入集合 B，并且使用这个元素。但是，如果载体元素索引已经包含在集合 B 中，那么就放弃这个元素并伪随机地选择另一个元素。

(3) 图像降级

图像降级是替换系统中的特殊情况，其中图像既是秘密信息又是载体。给定一个同样尺寸的伪装载体和秘密图像，发送者把伪装载体图像灰度(或彩色)值的 4 个最低比特替换成秘密图像的 4 个最高比特。接收者从隐藏后的图像中把 4 个最低比特提取出来，从而获得秘密图像的 4 个最高比特位。在许多情况下载体的降质视觉上是不易察觉的，并且对传送一个秘密图像的粗略近似而言，4 比特足够了。

(4) 载体区域和奇偶校验位

称任何一个非空子集$\{c_1,\cdots,c_{\ell(c)}\}$为一个载体区域。通过把载体分成几个不相接的区域，从而可以在一个载体区域中(而不是单个元素中)储存 1 比特信息。一个区域 I 的奇偶校验位能通过公式 $p(I)=\sum_{j\in I}LSB(c_j)\bmod 2$ 计算出来。在嵌入过程中，首先选择 $\ell(m)$个不相接区域 $I_i(1\leqslant i\leqslant \ell(m))$，每一个区域在奇偶校验位 $p(I_i)$上嵌入一个信息比特 m_i。如果一个载体区域的奇偶验校位与 m_i 不匹配，则将 I_i 中所有值的最低一个比特位进行反转，结果导致 $p(I_i)=m_i$。在译码过程中，计算出所有区域的奇偶校验位，排列起来就可重构消息。另外，使用伪装密钥作为种子，能伪随机地构造载体区域。

(5) 基于调色板的图像

在基于调色板的图像中，仅用特定色彩空间的一个颜色子集来对图像着色。每一个基于调色板的图像由两部分组成：一部分是调色板，它定义了 N 种颜色索引对(i,c_i)列表，它为一个颜色向量 c_i 指配一个索引 i；另一部分是实际图像数据，它保存每一个像素的调色板索引，而不是保存实际的颜色值。如果整个图像仅使用一小部分颜色值，这种方法大大地减少了文件的尺寸。一般地，在基于调色板的图像中有两种方法对信息进行编码：或操作调色板，或操作图像数据。颜色向量的 LSB 也能用于信息传输。另外，因为调色板不需以任何方式排序，在以调色板保存颜色时，可选择对信息进行编码。因为有 $N!$ 个不同方式对调色板进行排序，所以有足够的能力对一个短信息进行编码。然而，所有使用调色板顺序保存信息的方法都不具有健壮性，任何攻击者都能简单地以不同方式排序调色板而毁坏秘密信息(甚至在视觉上可以不修改图像)。另外，还可以在图像数据中对信息进行编码。

试读结束，需要全本PDF请购买 www.ertongbook.com