信息隐藏技术及其应用

刘勋　张步达　温志贤　何向阳

信息作为人们宝贵的财富，贯穿在当今人类的一切活动当中，而信息隐藏(Information Hiding)是一门具有渊源历史背景的新兴学科，涉及感知科学、信息论、密码学等多个学科领域，涵盖信号处理、扩频通信等多种专业技术的研究方向。在以因特网为代表的全球性信息化迅猛发展的今天，由于对保护知识产权的不断增长的需求以及受到使用密码加密技术的限制这两方面的原因，世界各国对信息隐藏技术的研究与应用兴趣正在迅速增长。

一、信息隐藏技术的基本原理

信息隐藏不同于传统的密码学技术。密码技术主要是研究如何将机密信息（明文）进行特殊的编码，以形成不可识别的密码形式(密文)进行传递；而信息隐藏则主要研究如何将某一机密信息秘密隐藏于另一公开的信息中，然后通过公开信息的传输来传递机密信息。对加密通信而言，可能的监测者或非法拦截者可通过截取密文，并对其进行破译，或将密文进行破坏后再发送，从而影响机密信息的安全；但对信息隐藏而言，可能的监测者或非法拦截者则难以从公开信息中判断机密信息是否存在，难以截获机密信息，从而能保证机密信息的安全。多媒体技术的广泛应用，为信息隐藏技术的发展提供了更加广阔的领域。

一个信息隐藏系统的一般化模型如图 1 所示。该系统中主要包括一个嵌入过程和一个提取过程，其中嵌入过程是信息隐藏者利用嵌入密钥（在隐藏过程中可能需要的附加秘密数据，通常在提取过程中使用与嵌入过程中相同或相关的密钥才能重新提取出被嵌入的消息)，将嵌入对象(希望能被秘密保存的信息)添加到掩体对象(用于隐藏被嵌入信息的非保密载体)中，从而生成隐藏对象(嵌入过程的输出，是被嵌入对象隐藏在掩体对象中之后得出的结果)。隐藏对象在传输过程中有可能被隐藏分析者截获并进行处理。提取过程是利用提取密钥从接收到的、可能经过修改的隐藏对象中恢复嵌入对象，在提取过程中有可能需要掩体对象，也可能不需要。该模型中的“对象”可以是“消息”“图像”“文本”或“声音”等。在有些特殊情况下，为了提高保密性需要预先对隐藏信息进行预处理(例如加密)，相应地在提取过程后要对得到的嵌入对象进行后处理（如解密)，以便恢复出原始信息。

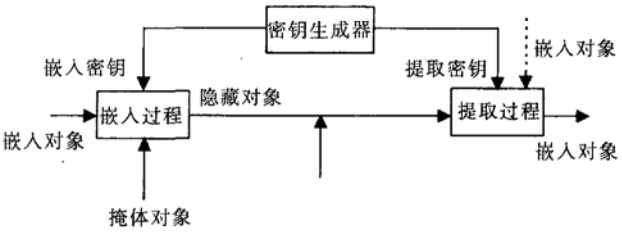

图 1　信息隐藏系统的一般模型

在信息隐藏系统模型的隐藏对象传输信道上存在一个隐藏分析者，隐藏分析者可对隐藏对象进行攻击，以便从中获取相关信息，一般地，攻击有被动攻击与主动攻击，对不同的信息隐藏系统其攻击的目的也不尽相同。被动攻击的主要目的有检测出隐藏对象、查明被嵌入对象以及向第三方证明消息被嵌入，甚至可以指出是什么消息；主动攻击的主要目的是在不对隐藏对象作大的改动的前提下，从隐写对象中删除被嵌入对象或删除所有可能被嵌入对象而不考虑掩体对象。

信息隐藏技术主要由下述两部分组成：(1)信息嵌入算法(嵌入过程中使用的算法)，它利用密钥来实现秘密信息的隐藏；(2) 隐蔽信息检测 /提取算法(检测器)，它利用密钥从隐蔽载体中检测/恢复出秘密信息。在密钥未知的前提下，隐藏分析者很难从隐秘载体中得到或删除，甚至发现秘密信息。信息隐藏技术中常用的算法有时空域嵌入/提取算法和变换域嵌入/提取算法，有兴趣的读者可阅读相关对算法描述的文章。

二、信息隐藏技术的特点

信息隐藏不同于传统的加密，因为其目的不在于限制正常的资料存取，而在于保证隐藏数据不被侵犯和发现。因此，信息隐藏技术必须考虑正常的信息操作所造成的威胁，即要使机密资料对正常的数据操作技术具有免疫能力。这种免疫力的关键是要使隐藏信息部分不易被正常的数据操作 (如通常的信号变换操作或数据压缩)所破坏。根据信息隐藏的目的和技术要求，该技术存在以下特性：

稳健性 也叫鲁棒性，指不因对象的某种改动而导致隐藏信息丢失的能力。这里所谓“改动”包括传输过程中的信道噪音、滤波操作、重采样、有损编码压缩、数/模(D/A)或模/数(A/D)转换等处理或变形。

不可检测性 指隐蔽载体与原始载体具有一致的特性。如具有一致的统计噪声分布等，以便使非法拦截者无法判断是否有隐蔽信息。

透明性 利用人类视觉系统或人类听觉系统属性，经过一系列隐藏处理，使目标数据没有明显的降质现象，而隐藏的数据却无法人为地看见或听见。

安全性 指隐藏算法有较强的抗攻击能力，即它必须能够承受一定程度的人为攻击，而使隐藏信息不会被破坏。

自恢复性 由于经过一些操作或变换后，可能会使原信息产生较大的破坏，如果只从留下的片段数据，仍能恢复隐藏信号，而且恢复过程不需要宿主信号，这就是所谓的自恢复性。

三、信息隐藏技术的应用

信息隐藏学是一门新兴的交叉学科，在计算机、通讯、保密学等领域有着广阔的应用前景。目前信息隐藏技术在信息安全的各个领域中所发挥的作用可系统地总结为以下几个方面：

数据的不可抵赖性 在网上交易中，交易双方的任何一方不能抵赖自己曾经做出的行为，也不能否认曾经接收到对方的信息，这是交易系统中的一个重要环节。这可以使用信息隐藏技术中数字水印技术，在交易体系的任何一方发送或接收信息时，将各自的特征标记以数字水印的形式加入到传递的信息中，这种水印应是不能被除去的，以达到确认其行为的目的。

数据的保密 在因特网上传输一些数据要防止非授权用户截获并使用，这是网络安全的一个重要内容。随着经济的全球化，这一点不仅将涉及政治、军事，还将涉及到商业、金融和个人隐私。而通过使用信息隐藏技术则可保护在网上交流的信息，如电子商务中的敏感信息、谈判双方的秘密协议和合同、网上银行交易中的敏感数据信息、重要文件的数字签名和个人隐私等。另外，还可以通过信息隐藏技术的另一种方法——隐写术的应用，可以使人们更加安全有效地进行秘密信息的传递，这一技术的应用有着显而易见的实用价值。

数字作品的版权保护 版权保护是信息隐藏技术中的水印技术所试图解决的一个重要问题。随着网络和数字技术的快速普及，通过网络向人们提供的数字服务也会越来越多，如电影、音乐、数字图书馆、数字图书出版、数字电视、数字新闻等具有知识产权的数字作品，这些数字作品具有易修改、易复制的特点，当今就已经成为迫切需要解决的实际问题。数字水印技术可以成为解决此难题的一种方案：服务提供商在向用户发放作品的同时，将双方的信息代码以水印的形式隐藏在作品中，这种水印从理论上讲应该是不被破坏的。当发现数字作品在非法传播时，可以通过提取出的水印代码追查非法散播者。这样一种在图片和音乐上不引起可感知退化，且难以被侵权者删除的方式是进行版权保护非常有效的技术手段。另外，数字水印技术还有许多非对抗的应用，如在音轨上加入购买信息的标记，当用户在车上收听收音机中的一首歌曲时就可以通过一个简单的按键来定购需要的CD。因此，信息隐藏技术已经引起了音乐、电影、书籍等出版者的广泛关注。

信息防伪与数据的完整性 商务活动中的各种票据的防伪也是信息隐藏技术可以用武之地。在数字票据中隐藏的水印经过打印后仍然存在，还可以通过再扫描成数字形式，提取防伪水印，证实票据的真实性；对于数据完整性的验证是要确认数据在网上传输或存储过程中并没有被窜改。通过使用脆弱水印技术保护的媒体一旦被窜改就会破坏水印，从而很容易被识别。

另外，信息隐藏技术在军事、广播通信等特殊方面也有着广泛的应用。其中流星爆发通信是一种从军事领域而来的隐写技术，它利用流星进入大气层产生的电离轨迹所提供的短暂无线电信道在移动站和基站间发送数据包，这些信道的短暂性使得敌方难以使用无线电定位移动站。此外，还可以利用一些软件以一种一般用户不可见，但可以轻易地被改造后的电视接收器重构的方式在视频屏幕内容中隐藏信息。利用扩频技术将信息嵌入视频信号或CPU的总线活动中也是使用软件实现隐蔽广播的一种方式。

总之，经过许多研究者多年的不懈努力，对信息隐藏技术的研究已经取得了很大进展，目前，国际上先进的信息隐藏技术已能使隐藏有嵌入对象的信息不但能经受人的感觉检测和仪器设备的检测，而且

重要的无源器件光纤光栅

岳丛建

光纤光栅在调Q、锁模、单频、多波长等各种光纤激光器中有重要的应用价值。光栅的物理原理是光纤的光敏性,即光致折变效应。利用光纤在紫外光照射下产生的光致折变效应，在纤芯上形成周期性的折射率调制分布，从而对入射光波中相位匹配的频率产生相干反射,可以在典型的0.1到几十纳米的带宽($\Delta\lambda$)内产生反射,反射率可以达到100%。光纤光栅的这一重要的波长选择特性使之成为光纤器件中一种最重要的无源器件,受到普遍关注。光纤光栅由最简单和最基本的均匀周期光纤布喇格光栅,发展到多种不同结构、不同特点的光纤光栅。

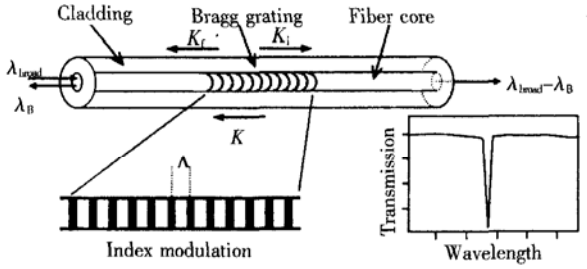

图1 均匀周期光纤布拉格光栅结构及光谱特性示意图

均匀周期光纤布拉格光栅

均匀周期光纤布拉格光栅一般简称为光纤布拉格光栅,是最早发展的光纤光栅,而且应用最广泛。其纤芯中折射率呈固定的周期性调制分布，当光经过时对满足布拉格相位匹配条件的光产生很强的反射，对不满足布拉格条件的光由于各个光栅面反射的光相位不匹配只有很微弱部分被反射回来，例如一个光栅长度为1mm、折射率调制深度达10^{-3}的中心波长在1.5μm附近的光栅,对不满足布拉格条件的光的反射只有约0.05%。光纤布拉格光栅的结构与光谱特性如图1所示。

啁啾光纤光栅

啁啾光纤光栅是光纤通信领域最感兴趣的有应用需要的光纤光栅类型之一，这种光栅的周期不是常数而是沿轴向呈线性变化的(如图2所示),因此能够产生宽带反射,带宽最大可超过100nm,远远大于均匀周期光栅的带宽。线性啁啾光纤光栅能产生大而稳定的色散,可用于光纤WDM通信系统的色散补偿,亦可用于宽带反射滤波器、温度不敏感光纤光栅传感及光学傅立叶变换等。

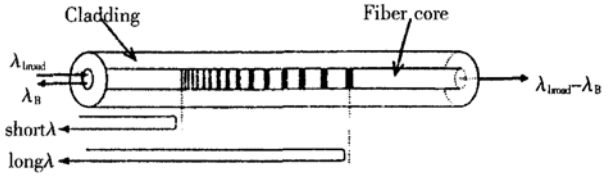

图2 啁啾光纤光栅结构及光谱特性示意图

闪耀光纤布拉格光栅

在光栅制作过程中，当紫外侧写光束与光纤轴不严格垂直、而有一个小角度时，形成所谓闪耀光栅。闪耀布拉格光栅的波矢方向不是与光纤轴线方向相一致的,而是与其成一固定的角度。它不但引起反向导波模耦合，而且还将基阶模耦合至包层模中损耗掉。利用闪耀光栅的包层模耦合形成的宽带损耗特性,可将其用于铒光纤放大器的增益平坦。当光栅法线与光纤轴向倾角较小时，还可以将闪耀光栅用作空间模式耦合器，它可以将一种导波模耦合至另一种导波模中。

相移光纤光栅

所谓相移光栅是在均匀周期光纤光栅的某些点

还能抵抗各种人为地蓄意攻击。但总的来说,信息隐藏技术尚未发展到完善得可实用的阶段，仍有不少技术性问题需要解决。同时,水印验证体系的建立、法律的保护等也是信息隐藏技术在迈向实用化过程中不可缺少的应用因素。另外,信息隐藏技术发展到今天,还没有找到自己的理论依据,没有形成理论体系。目前,随着技术的不断提高,对理论指导的期待已经越来越迫切，特别是在一些关键问题难以解决的时候,这个矛盾更加突出。而目前使用密码加密仍是网络上主要的信息安全传输手段，信息隐藏技术在理论研究、技术成熟度和实用性方面都无法与之相比,但它潜在的价值是无法估量的,特别是在迫切需要解决的版权保护等方面，可以说是根本无法被代替的，相信其必将在未来的信息安全体系及相关领域中发挥重要作用。

(甘肃天水师范学院数理与信息科学学院 741000)