2003年上海大学博士学位论文 8

数字图像和音频中隐藏信息的检测和主动攻击

作　者：张开文
专　业：通信与信息系统
导　师：王朔中

上海大学出版社
·上海·

2003 年上海大学博士学位论文

数字图像和音频中隐藏信息的检测和主动攻击

作　者：张开文
专　业：通信与信息系统
导　师：王朔中

上海大学出版社
· 上海 ·

Shanghai University Doctoral Dissertation (2003)

Detection and Active Attack against Hidden Information in Digital Images and Audio Signals

Candidate: Zhang Kaiwen
Major: Communication and Information System
Supervisor: Prof. Wang Shuozhong

Shanghai University Press
• Shanghai •

上 海 大 学

本论文经答辩委员会全体委员审查，确认符合上海大学博士学位论文质量要求。

答辩委员会名单：

主任：	余松煜	教授，上海交通大学图像所	200030
委员：	王治钢	研究员，上海航天局 809 研究所	200031
	翁默颖	教授，华东师范大学电子系	200062
	张立明	教授，复旦大学电子信息工程系	200433
	顾亚平	研究员，中科院东海站	200017
	蒋昌俊	教授，同济大学计算机系	200437
	张兆扬	教授，上海大学通信学院	200072
导师：	王朔中	教授，上海大学通信学院	200072

评阅人名单：

余松煜	教授，上海交通大学图像所	200030
张兆扬	教授，上海大学通信学院	200072
翁默颖	教授，华东师范大学电子系	200062

评议人名单：

王治钢	研究员，上海航天局 809 研究所	200031
梁庆林	教授，北京大学电子学系	100871
黄继武	教授，中山大学信息学院	510275
吴亚明	研究员，中科院上海微系统所	200021
严壮志	教授，上海大学通信学院	200072

答辩委员会对论文的评语

张开文的博士论文围绕信息安全这一重要问题，研究对数字媒体中隐藏信息的检测和攻击，是当前信息学科的前沿课题. 研究工作在国家自然科学基金和上海市重点学科建设项目资助下进行，选题具有先进性和重要的学术意义，而且结合其本职工作具有积极的现实意义. 该论文围绕对抗敌对隐蔽通信的盲分析和主动攻击这一主题，取得了以下具有创新性的成果.

1. 针对图象中的信息隐藏，提出了以加权均方误差（WMSE）作为图象失真度指标. 由于 WMSE 利用象素间的相关性，反映了人的视觉特性，与常用的 PSNR 和 MSE 相比能更准确地反映信息隐藏算法在隐蔽性方面的性能优劣，是研究隐蔽通信及其分析的一种有效工具.

2. 论文研究了对感官无法分辨的两幅图象或两个音频信号之间判断哪一个含有隐蔽数据的问题，提出了互为补充的三个统计判据，利用这些判据成功地检测出含有秘密信息的图象和音频信号. 该方法适用于多种不同的嵌入算法，对样本的大小和嵌入数据是否经过扰码并无限制，提供了一种有实用价值的隐蔽信息盲检测手段.

3. 论文针对常用的 DCT/QIM 嵌入算法提出基于直方图和变换系数能量分布的盲分析和主动攻击方案，不仅能判断隐蔽信息的存在性，还能在不引入进一步失真的前提下破坏隐蔽数据. 该算法作为一种主动卫士能阻断一类可能存在的敌对隐蔽通信，对

于网络环境下的信息安全有重要的意义.

论文作者具备信息学科的扎实基础，在信号处理、信号分析、信息隐藏等方面有较广的知识面，独立从事科研工作的能力强. 本论文论点正确，论据充分，有创新性. 论文层次分明，条理清晰，实验方法合理，实验结果可信. 在答辩中叙述清楚，能正确回答提出的问题.

答辩委员会表决结果

经答辩委员会表决，全票同意通过张开文同学的博士学位论文答辩，建议授予工学博士学位.

答辩委员会主席：余松煜

2003 年 9 月 6 日

摘　要

随着通信、信号处理和计算机网络技术的发展，特别是Internet 在世界范围内的无缝连接，信息隐藏技术得到日益重视和迅速的发展. 科研成果层出不穷，许多企业也相继开发出用于版权保护的数字水印产品. 一些特殊的群体已经利用大众媒体将一些重要的信息隐藏在网络多媒体数据中秘密传输，形成了所谓的“潜信道”. 这一研究领域的兴起，给信息安全注入了新的活力.

针对不同宿主信号的特点和不同的用途，信息隐藏技术千变万化. 这种变化不仅仅是算法上的变化，更重要的是借助了密码学中的密钥，将现代密码技术与信息隐藏技术相结合，大大增强了隐藏信息的安全性，使攻击者难以发现秘密通信信道，更难以获取可进一步分析研究的素材.

论文的研究工作是国家自然科学基金项目“数字音频中高度稳健的数据隐藏技术”、上海市重点学科建设项目“互联网环境下的多媒体编码与信号处理技术”以及上海市博士点基金项目“基于图像统计特性和密码术的数字水印新技术研究”的一部分，侧重于对数字音频信号和静止图象中数据隐藏进行盲检测分析和主动攻击的研究.

信息隐藏及其攻击是当代信息战的重要内容，对于网络时代的信息安全具有特别重要的意义. 作为一项特殊的工作，如何开展隐藏信息的盲检测分析研究和主动攻击，本课题做了一些有益的尝试. 论文首先概述信息隐藏及其攻击技术以及国内外的研

究现状，然后针对以隐蔽通信为目的的信息隐藏技术为研究对象，深入探讨了信息隐藏对宿主信号的修改实质，针对某些常用的信息隐藏方法提出相应的分析和攻击策略. 主要研究成果和创新点有以下三个方面：

1. 作为检测隐蔽信息存在性的基础，对信息隐藏重要指标之一的隐蔽性度量进行研究. 通过分析常规均方误差存在的不足和针对人的视觉效应，提出了加权均方误差(WMSE)度量图像失真度. 理论分析和实验表明，这一方法用于衡量信息嵌入和某些图像处理所导致的图像失真时，比一般 MSE 方法更接近主观评价的结果，可以作为评价信息隐藏嵌入算法隐蔽性能的一个有效工具.

2. 在数字水印或隐蔽通信存在性的盲检测方面，本文基于数据时(空)域局部相关特性提出了 3 个性能互补的统计判别准则，用于对视听觉无差异的两个样本进行检验，以辨别其中哪一个可能携带隐蔽信息，取得了满意的判别准确率.

3. 针对变换域中的量化索引调制(QIM)信息隐藏方法的基本特征，提出了有力的攻击方法，不仅成功地删除了嵌入的信息，而且对嵌入所引起的宿主信号失真实现了一定程度的补偿. 这一方法可成为对敌对隐蔽通信进行主动攻击的有效手段之一.

论文最后对现代密码技术与信息隐藏技术的有机结合以提高安全性等问题作了简要的论述，对有关领域进一步研究进行了展望.

关键词 信息隐藏 潜信道 检测和密写分析 失真和隐蔽度量 主动攻击

Abstract

With the development of communications, signal processing and computer networks, especially the seamless connection of the Internet, information hiding has attracted much attention in recent years. Digital watermarking for copyright protection has been studied intensely, and many products have been developed. In the mean time, hidden communication through subliminal channels is also being investigated, which transmits secret information within multimedia data in public networks. This emerging technological field is closely related to the important issue of information security.

This thesis investigates information hiding techniques aimed at hidden communication. A general discussion on the background is first given. A literature survey on the related research and recent development is then presented. The very nature of modification to the host data due to information hiding is explored, leading to effective analysis of, and attacks against, some commonly used data embedding schemes. The main contributions and innovative results of this work include:

1. As a basis for detection of subliminal channels, an important measure representing invisibility of the hidden information in still images is studied. After analyzing the drawbacks of the conventional mean square error (*MSE*) method, an improved metric, the weighted mean square error (*WMSE*) is proposed. Theoretical and

experimental studies show that, when used to measure image distortion caused by data embedding and image processing, WMSE is closer to the human visual assessment than the original MSE. The *WMSE* metric is particularly useful in evaluation of data hiding algorithm in terms of invisibility.

2. For blind detection of the existence of a watermark or secret communication, this thesis proposes three criteria based upon analysis of local statistic properties in the data for making decision as to which of the two given versions of the same multimedia material (digital audio or image) carries secret data. These three criteria are mutually complementary. Experimental results are presented showing the effectiveness of the method.

3. An effective attack scheme is proposed against a commonly adopted data embedding technique, quantization index modulation (*QIM*). The described scheme not only removes the embedded information, but also, to some extent, compensates for the distortion in the host media due to embedding. This technique can be used as an active warden to prevent hostile hidden communication.

In the final part, the thesis briefly discusses the benefits of combining modern encryption with steganographic techniques in enhancing security of information systems, and gives a perspective view to the future development of the field.

The work was supported by Natural Science Foundation of China, Key Disciplinary Development Program of Shanghai, and Doctoral Programs Foundation of Shanghai.

Key words information hiding, subliminal channel, detection and steganalysis, distortion-metric, active attack

目　录

第一章 绪 论

随着通信、信号处理和计算机网络技术的发展，特别是Internet 世界范围内的无缝连接，人们已经步入了数字化的信息社会. 数字化的信息社会给人们的工作和生活带来了无限的便利：大量信息能够迅速、便捷、安全地传输与交流，宝贵的信息资源得以共享并最大地发挥其功用；电子政务极大地提高了政府和社会公共事业部门的办公效率，促进了正规化和标准化建设，特别是将人们从文山会海中解放了出来；电子商务推动了网络经济的发展，网上信息服务、电子购物与贸易、电子银行与金融服务等将成为全新的技术服务手段和方法；珍贵资料的保存、历史档案的查询等，所有这一切都与信息的数字化和网络化密切相关. 然而，信息的数字化和网络的无缝连接，也给信息的安全、管理、合理和合法运用等提出了挑战.

与模拟信息不同，数字信息可以永远的储存、精确的重复复制、篡改后可以不留有痕迹等. 因此，识别信息的真伪、判别信息的来源以及保护数字多媒体信息的版权、保护核心信息的安全等，成为数字时代迫切需要解决的主要问题之一.

作为信息隐藏的一种应用，数字水印(digital watermarking)技术应运而生[1~3]. 数字水印技术的主要功能是为了保护知识产权[4~7]. 其中心思想是知识产权拥有者将一些自定义的数字信息鲁棒地隐藏在需要保护的多媒体信号诸如图像、三维图形、视频、

音乐(音频)、文本以及超文本文件中[2~7]. 携带秘密信息的原始信号称之为宿主信号，秘密信息称之为水印信息，而嵌有产权信息后的信号称为混合信号. 水印信息既可以是具有实际意义的文字、图像或语音，也可以是版权所有者自定义的数字串及其他形式，甚至可以是只进行是否是检验者拥有权的一种假设检验[8,9]. 这种用于知识产权保护的数字水印技术通常应兼有不可见性和鲁棒性.

信息化社会中的另一个非常重要的方面就是信息的安全问题. 信息安全在信息时代关系到国家安全、经济的发展和个人利益等许多方面. 虽然信息安全是一个系统工程，需要一个完整的保障体系，涉及到立法[10]、管理和使用等诸多方面，但理论研究与应用技术支持是不可或缺的最重要一环，先进的安全技术是信息安全的根本保证.

保障敏感信息安全的传统方法主要是加密. 虽然加密后的数据为一种无序、随机状态，但这将会引起一些特殊团体和个人的攻击[11,12]. 这种易于遭受攻击的特征实际上就已经带来了某种程度的安全隐患. 在一个密码系统中，密码体系的安全性依赖于密钥的安全[12]. 随着破译技术的进步和计算能力的提高，密码的安全遇到强有力的挑战. 密码系统为了保障其安全，所使用的密钥越来越长，给实际的使用带来了不便. 技术的进步和特殊应用的需求，使得古老的信息隐蔽术焕发了生机——一种新的秘密通信技术即隐蔽通信正在崛起.

利用公开、有实际意义的多媒体数据传递秘密信息，作为一种新的隐蔽通信手段和途经正得到迅速发展[13,14]. 这种隐蔽通讯技术与传统的密码技术相比具有实质意义上的区别. 密码只掩蔽了通信的真实内容，而隐蔽通信不仅可以隐蔽通信的内容，

更是掩盖了通信信道的存在. 这种在一个有意义的信号中传输另一个隐含的秘密信息技术称之为隐蔽通信技术或“潜信道(subliminal channel)”技术.

数字水印和隐蔽通信技术可以统归为信息隐藏(information hiding)技术[15]. 在信息隐藏技术中被隐藏的信息可以是文字、密码、图像、图形或声音，而作为隐藏信息载体的宿主信号可以是一般的文本文件、图像、视频和音频等等.

1.1 数字水印与隐蔽通信

信息隐藏技术集密码学、通信理论、编码理论、数字信号处理技术和人的感知等多学科理论与技术于一身，是多项技术相融合的新兴领域. 它利用信号自身的多余度和人类感觉器官对数字信号的感觉冗余，将一个消息(称为秘密信息)隐藏在另一个消息(宿主信号)中. 由于隐藏了秘密消息的混合信号依然表现出完全原宿主信号的外部特征，故并不影响宿主信号的使用价值，也难以引起攻击者的怀疑.

信息之所以能够隐藏在多媒体数据中是因为：

(1) 多媒体信息本身存在很大的冗余性. 从信息论的角度看，未压缩的多媒体信息的编码效率较低. 无论是文字、图像或图形以及音频，数据间均具有不同程度的相关性. 这种相关性是压缩编码的理论基础，也是信息隐藏的理论依据. 如果数据间没有相关性，就不能压缩，也就不能再携带其他 的额外信息. 一个性能好的加密机的输出数据之间应当不存在冗余，因此密码数据中一般不能再藏有其他 额外的信息，否则，密码数据自身将遭到破坏，使其译码发生错误.

(2) 人的视觉系统(human visual system–HVS)和听觉系统

(human auditory system–HAS)存在的冗余[16,17]. 从人的生理和心理特征上看，并非多媒体数据中的所有信息都是同等重要、同等对待的. 一些信息的损伤或忽略并不影响人们对信息的接受和正常理解，甚至人们难以察觉到这些数据的存在. 如在图像数据中，人眼对灰度的分辨能力只有几十个灰度级，对边缘附近的信息不敏感等，而在音频信号中，人耳可以用 24 个相互重叠的滤波器组来近似[18]，存在着高频掩盖低频、高能量掩蔽低能量等特征. 利用这些特点就能将秘密信息隐藏起来而又不被发觉.

事实上，信息隐藏的历史古老而又悠久[19]. 人类从未间断对信息隐藏的研究和运用. 我国古代的藏头露尾诗、古希腊人的蜡板藏书和德国间谍使用的隐形墨水等都是典型的例子. 而如今互联网和数字多媒体技术的广泛应用，为信息隐藏技术的发展和使用提供了更加广阔的领域.

数字信息隐藏技术出现于 20 世纪 90 年代中期. 近十年来的研究和运用有了长足进步和发展，至今方兴未艾. 其中用于知识产权保护的数字水印技术运用的最广泛. 而作为隐蔽通信的有效手段，在网络四通八达的今天，在一些特殊场合已经被一些特殊的群体所采用.

数字水印、秘密通信的信息隐藏技术、密码学均属于信息安全的范畴. 它们之间的关系如图 1.1 所示.

信息隐藏和密码学(cryptography)都是为了达到通信保密之目的，然而两者有着明显的区别. 密码技术是通过一定的数学模型，将要传递的秘密信息转换成随机乱码，以对通信双方之外的第三者隐藏其信息的真实内容(又称为明文). 它不隐藏秘密信息通信的存在性. 总体而言，这种保密手段虽然坚固，但也存在着两方面的隐患：一是对于秘密信息的拦截者来说，如果获取了