信息安全技术与教材系列丛书

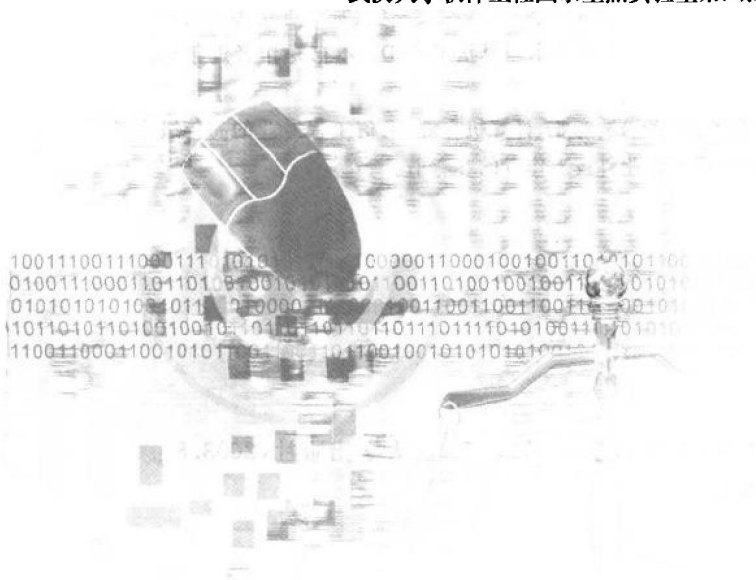
网络多媒体信息安全保密技术

王丽娜 / 著

全国优秀出版社
武汉大学出版社

信 息 安 全 技 术 与 教 材 系 列 丛 书

国家自然科学基金重大研究计划（编号：90104005，90204011）
湖北省自然科学基金（编号：2002AB0039）
武汉大学软件工程国家重点实验室第四批开放基金



网络多媒体信息安全保密技术

王丽娜 / 著

全国优秀出版社
武汉大学出版社

内 容 简 介

本书是一部关于计算机网络安全的专著。全书共分 13 章。主要内容包括适合多媒体信息的混沌加密算法、基于全距特征排列的全距置换方法、(t,n)门限秘密共享体制、等级系统中的访问控制、门限数字签名体制、数据的保密传输、VPN 原型系统、入侵检测系统、基于进化神经网络的入侵检测方法、入侵容忍技术、基于混沌特性的小波数字水印算法 C-SVD。本书是作者近年来的科研成果。

本书可作为高等院校的信息安全专业、密码学专业、计算机专业、通信工程专业的高年级本科生或研究生的教材，也可作为科研院所相关专业科技工作者的参考书。

图书在版编目(CIP)数据

网络多媒体信息安全保密技术/王丽娜著. —武汉：武汉大学出版社，2003.8
信息安全技术与教材系列丛书
ISBN 7-307-03924-9

Ⅰ.网… Ⅱ.王… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2003)第 021169 号

责任编辑：黄金文　　责任校对：王　建　　版式设计：支　笛

出版发行：武汉大学出版社　(430072　武昌　珞珈山)
(电子邮件：wdp4@whu.edu.cn　网址：www.wdp.whu.edu.cn)
印刷：湖北省通山县印刷厂
开本：787×980　1/16　　印张：11.75　　字数：238 千字
版次：2003 年 8 月第 1 版　　2003 年 8 月第 1 次印刷
ISBN 7-307-03924-9/TP・140　　定价：18.00 元

信息安全技术与教材系列丛书

编　委　会

序 言

21世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以Internet为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。到2003年，全国设立信息安全本科专业的高等院校增加到20多所。2003年经国务院学位办批准武汉大学建立信息安全博士点。

为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天，这套丛

书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以使丛书能够进一步修改完善。

中国工程院院士，武汉大学兼职教授

沈昌祥

2003 年 7 月 28 日

前 言

网络技术在全世界迅速发展，Internet 已成为全世界的信息资源中心。网络安全问题越来越成为网络用户关注的焦点。对网络中的重要的多媒体信息进行快速、有效的加密，保证信息的秘密性、完整性和真实性；对数字作品嵌入水印进行版权永久性保护；对网络系统进行入侵检测以保证网络多媒体信息系统的安全可靠、平稳运行，具有十分重要的理论意义与实际应用价值，这已成为国际前沿研究领域。

全书共分 13 章。第一章介绍网络多媒体信息安全保密研究的重要意义。第二章介绍安全与保密的数学理论基础。第三章设计一种适合多媒体信息的快速有效的混沌加密算法，分析混沌加密的效率及安全性。实现对文本、图像、声音等多媒体信息的加密。提出基于混沌理论的用户身份“指纹”认证算法构造及安全性分析，构造身份认证双方的混沌同步控制器。第四章提出全距特征排列的概念，对全距特征排列的性质、计数进行研究，并在此基础上讨论全距置换与全距特征排列之间的映射关系，基于全距特征排列给出了全距置换的一种有效的构造方法。第五章阐述(t,n)门限秘密共享体制，包括基于 RSA 数字签名防欺诈的(t,n)门限秘密共享体制；两种基于 RSA 加解密算法防欺诈的(t,n)门限体制；Asmuth-Bloom 体制的扩展；多个组织间的门限秘密共享体制；(t,n)门限秘密共享体制的安全性讨论。第六章阐述等级系统中的访问控制方案。第七章阐述门限数字签名体制。第八章阐述数据的保密传输。第九章对所提出、设计的基于混沌理论的身份认证算法、基于混沌理论的数字签名算法、混沌加密算法，进行综合集成，设计并实现 VPN 原型系统，以解决 VPN 安全的关键技术问题。第十章介绍入侵检测技术。第十一章将神经网络与遗传算法相结合，提出基于进化神经网络的入侵检测方法，进行数据库系统及网络系统的入侵检测。第十二章讨论入侵容忍技术。第十三章基于混沌特性提出一种小波混沌数字水印算法，采用数字水印技术可以有效保护多媒体信息（如图像、音频、视频）的版权。本书第一、二、三、九、十、十一、十二、十三章由王丽娜写作，第四、五、六、七、八章由费如纯和王丽娜共同写作。

本书在写作过程中得到于戈教授、张焕国教授、冯夏庭教授的支持与帮助，在此表示衷心感谢。

本书得到国家自然科学基金重大研究计划(编号:90104005,90204011)、湖北省自然科学基金(编号:2002ABO039),武汉大学软件工程国家重点实验室第四批开放基金项目的支持。在此表示感谢。

由于学术水平有限,书中难免出现错误,敬请批评指正。

作　者

2002 年 8 月

目 录

第一章 绪 论

1.1 网络多媒体信息安全保密研究的重要意义

自从1956年第一个计算机网络建立以来,网络技术得到了极其迅速的发展。今天,各种通信网络,如用于数据传输的分组交换网络(PSDN),用于话音通信的公共业务电信网络(PSTN),综合业务网络(ISN),(陆地或卫星)移动通信网络等,使我们的生活方式和工作方式发生了巨大的变化。我们正在步入一个崭新的信息社会。随着信息化社会的发展,信息在社会中的地位和作用越来越重要,每个人的生活都与信息的产生、存储、处理和传递密切相关,信息的安全与保密问题成了人人都关心的事情,这时的安全、保密学脱去了神秘的面纱,成为大家感兴趣并为更多人服务的科学。信息空间的侦察与反侦察,截获与反截获,破译与反破译的斗争愈演愈烈。近年来,在网上所进行的各种犯罪活动出现了逐年上升的趋势,由此所造成的经济损失是十分巨大的。在网络上的电子商业活动日益频繁,电子资金传送的金额数量也在快速增加。资源共享和信息安全历来是一对矛盾。据美国联邦调查局统计,美国每年因信息和网络安全问题所造成的损失高达75亿美元。1994年4月16日,美国《金融时报》报道:据权威机构统计,平均每20秒就发生一起入侵Internet计算机的事件。由上述情况看出,信息时代网络安全面对严峻的挑战,安全对策显得尤为重要。网络安全是计算机安全在网络环境下的扩展和延伸。网络信息系统的安全保密问题已成为影响社会稳定和国家安危的战略性问题。

网络技术的发展,为银行、政府机关、商业、企业及私人通信提供了相当便利的条件,大大加快了信息发布和传播的速度,各种各样的电子商务纷纷在网上展开。通过计算机网络,人们可以不出家门就买到所需的东西。但是网络的发展也带来了一系列问题。例如,攻击者可以通过各种技术手段非法接收甚至修改一些他本来无权使用的秘密信息,非法用户冒充合法用户操纵计算机终端获取一些机密情报,非法信息进入计算机系统,存储和传输中的合法信息遭到破坏等。

无论是个人还是集体,网络中的安全问题成为人们关注的焦点,失去安全就意味着财产得不到保障,因此如何保证用户的合法利益不受侵犯成为电子商务能否发展下去的关键。如何防止信息在开放的网络中传输时被窃听呢?一种简单可行的办法就是对要传输的信息进行加密。经过加密的信息在网络中传输时即使被网络黑客截

获,其信息也不会暴露,因为被截获的信息对黑客来说没有任何意义。

密码形成新的学科是在20世纪70年代。它的理论基础之一应该首推1949年Shannon的一篇文章——《保密通信的信息理论》,这篇文章过了30年才显示出它的价值。这篇论文和1976年Diffie W. 与Hellman M. 发表的《密码学的新方向》[1]一文以及1977年美国公布实施的《数据加密标准(DES)》[2],标志着保密学理论与技术划时代的革命性变革。这主要表现在以下几个方面:第一,传统密码体制的主要功能是信息的保密,而双钥(公钥)密码体制的出现,不但赋予了通信的保密性,而且还提供了消息的认证性。第二,这种新的双钥密码体制无需先交换密钥就可通过不安全信道安全传递信息,大大简化了密钥分配的工作量。双钥密码体制和DES适应了通信网的需要,为保密学技术应用于商业领域开辟了广阔的天地。第三,双钥密码体制的出现和DES的设计充分体现了Shannon信息保密理论所阐述的设计密码的思想,使密码的分析和设计提高到新的水平[3]。当今密码学和信息安全保密技术已逐步得到广泛的重视,相应的保安软、硬件已逐渐形成一个新的产业,其中包括认证、加密、访问控制、防火墙、抗病毒等方面的产品。信息安全保密技术在军事系统、政府机构、金融系统、医疗保健、通信网络、教育系统、制造业等方面开始得到广泛应用。中国不能没有自己的密码系统,中国也必须有自己的加密标准[4]。

多媒体信息的出现极大地丰富了计算机信息的表现能力,它已经成为计算机信息中的一个重要部分,因此对多媒体信息的安全保密工作变得越来越重要。多媒体信息具有信息量大及易复制的特点,因此早期的加/解密算法在多媒体信息安全保密方面已经显得力不从心。

密码学采用加密算法(如:DES,RSA,…)加密信息后得到密文,任何人不用合法的密钥解密都无法得到或使用明文信息。但是,一旦将密文解密得到明文信息,信息再无法受到保护。而在电子商务中提到的多媒体作品版权恰恰需要得到永久的保护,显然,传统的加密算法已经不足以实现版权保护功能。为了保证创作者的合法权益不受侵害,采用了一种全新的概念——数字水印(Digital Watermark)技术来实现多媒体信息的版权保护。数字水印技术很好地解决了这一问题。数字水印技术以信息隐藏学为基础。它是指在数字化的多媒体信息中嵌入不易察觉的信号,在需要的时候可通过特定的算法,将此隐藏的信号提出以用来确认身份的技术。它的核心是信息隐藏技术。数字水印技术是借助人类的视觉、听觉器官所具有的某种不敏感性,在不影响作品内容的前提下,将水印信息保存到多媒体作品当中。由于水印信息并不影响作品的宏观内容,因而水印信息将永久地保存在多媒体作品当中,任何人若试图从作品中剔除水印都不得不大幅度破坏原作品,以致到面目全非的地步,从而保护了作者的合法版权。

现代网络多媒体信息系统,如:数字图书馆、数字博物馆等,这些系统存储的都是精品、宝贵信息和财富。如果遭到入侵,那么会造成很大损失。因此网络信息安全不但是发挥信息革命带来的高效率、高效益的有力保证,而且是对抗霸权、抵御信息侵

略的重要屏障,信息安全保障是21世纪世界各国奋力攀登的制高点。自主性、创新性是建立我国网络信息安全体系的第一位要求。

Internet技术在全世界迅速发展,Internet已成为全世界的信息资源中心。当Intranet连接到Internet时,安全问题越来越成为网络用户关注的焦点。对Internet网络中的重要信息进行加密,保证信息的秘密性、完整性和真实性。随着Internet中图像和视频信息的快速增长,对数字信息进行版权永久性保护有着迫切的需求。研究网络的安全性和可靠性,能保证网络多媒体信息系统的安全可靠、平稳运行。入侵检测是网络系统安全的重要组成部分。对此进行研究,具有十分重要的理论意义与实际应用价值,并已成为国际上亟待解决的重大前沿课题[5~7,19,20,155,156]。

1.2 网络信息安全与保密研究的主要内容

国内外许多专家在网络信息安全与保密研究方面做出了重要贡献[8,9,21,149,150,151,152,153]。美国公布了DES、RSA加密标准及DSA[10]数字签名标准。Rubin阐述了Web安全策略。Oppliger阐述了IP安全协议、认证头部协议及密钥管理协议。在信息编码与密码学理论方面,西安电子科技大学、中国科学院软件研究所、北京邮电大学、上海交通大学、清华大学、中国科学院计算技术研究所等单位的专家学者进行了深入的研究,都取得了可喜的成果。

1.2.1 多媒体信息保密方法

(1)已有的加密方法大都使用DES或3-DES或RSA,但是DES算法存在着一定的脆弱性和一定的局限性,面临着挑战。同时这些算法也不适合对大容量信息的高效快速加密。因而需要设计新的加密算法,突破原有的DES思想设计模式。混沌密码学是设计新的加密算法的一种有效途径。混沌是发生在一个确定性系统中的伪随机运动[11],混沌理论用于处理随机的和不可预测的现象,而加密的效果就是要对没有密钥的用户来说密文是随机的和不可预测的。最近,基于混沌理论的密码学[12~15]成为很活跃的研究领域。这并不奇怪,因为古典密码学的核心即流密码学的密钥生成器就是一个离散混沌(或者说是伪混沌的)动力系统。混沌安全通信的安全性取决于混沌系统对它们的参数及初始条件的敏感性。

网络多媒体信息系统中需要传递的多媒体信息的信息量会很大,多媒体技术的关键特性主要表现在信息媒体的多样性和处理信息的集成性、实时性、交互性和协同性上,并要求安全、快速、实时传递[16]。随着网络技术的不断发展,网络传输速度有了很大的提高,于是各种类型的多媒体信息出现在网上。多媒体信息的出现弥补了单调的文本信息的不足,使得网络信息更加丰富精彩[17]。多媒体信息丰富的表现力当然是以膨胀的数据量为代价的,因此多媒体数据信息加重了网络负载。针对多媒体信息数据量较大这一特点[18],对多媒体信息加密所采用的加密算法就要求有较高