文章编号:1005－0523(2006)01－0082－05

数字图像安全技术研究进展

黄晓生

(华东交通大学 土木建筑学院,江西 南昌 330013)

摘要:随着数字技术和因特网的飞速发展,图像数据的安全性越来越受到社会的普遍重视.全面分析了数字图像安全需求以及为达到各安全需求的各种安全措施,重点对数字图像加密以及数字图像水印技术的研究现状以发展进行了分析,并对存在的问题以及该领域未来可能的研究方向和研究重点进行了展望.

关 键 词:信息安全;密码学;图像加密;数字水印

中图分类号:TP391　　**文献标识码**:A

1 引言

随着数字技术和因特网的飞速发展,图像数据的安全性越来越受到社会的普遍重视.网络背景下的数字图像,其安全性需求包含以下四个方面:1)保密性:即图像的内容不允许被未授权用户、或实体访问或利用.2)完整性:即图像在存储或传输过程中保持不被非法修改、破坏或丢失,并且能够判别出图像是否已被改变.3)鉴别性:指能保证图像的真实性,即能证实接收到的图像就是来自所要求的源方,包括对等实体鉴别和数据来源鉴别.4)不可抵赖性:指接收方可以证明发送方确实发送了其接收到的图像,或者发送方不能否认其曾发送过图像.为了达到以上需求,人们提出了许多相应的安全措施[1],这些措施,从总体上可以分成两大类:一类是基于现代密码学思想和一种新手段的图像加密方法,另一类是基于信息隐藏与伪装思想的方法,包括将需要保密图像隐藏于另一不需要保护的图像中的图像隐藏和以版权保护为主要目的的数字水印技术.

本文对以上这两类数字图像安全技术进行了分析比较,简要归纳了各类技术算法的优缺点并指出其今后的发展方向.

2 现代密码学与数字水印技术

2.1 现代密码学

现代密码学的理论基础主要包括 Shannon 的保密系统信息理论[2]和 Simmons 的认证系统信息理论[3],密码系统的设计则遵循 Kerckhoffs 假设.

从理论上讲,数字图像信息也可以应用现代密码体制来进行加密,但由于:(1)数字图像数据量一般都比较大,应用一般现有的密码技术直接加密的话,需要很长的加密时间,因而其加密效率不高;(2)数字图像一般以二维数组的数据格式存储,应用现有的加密算法来加密数字图像需要先将数字图像数据重排,这也需要一定的图像预处理时间,也降低了加密效率;(3)与文本信息不同,数字图像信息是允许一定的图像失真度的,这种图像失真只要控制在人的视觉不能觉察到时是完全可以接受的.有时为了初略浏览,甚至视觉上觉察到一定的失真也是完全可以的.因此,对于数字图像信息加密,还需要设计适合数字图像数据特点的图像加密算法[9].

基于密码学概念的图像加密技术就是将待传输的图像看作明文,通过各种加密算法,如 DES,RSA 等,在密钥控制下,达到图像数据保密通信.这种加密机制的设计思想是加密算法可以公开,通信保密完全依赖于密钥的保密性.

2.2 数字水印技术

数字水印是一种有效的数字产品版权保护和数据安全维护技术,它将具有特定意义的标记(水印),利用数字嵌入方法隐藏在数字图像、声音、文档、图书、视频等的数字产品中,用以证明创作者对其作品的所有权,并作为鉴定、起诉非

收稿日期:2005－05－20

作者简介:黄晓生(1972－),男,江西省于都人,博士研究生,讲师,研究计算机辅助设计,图形图像处理,信息安全.

法侵权的证据,同时通过对水印的检测和分析来保证数字信息的完整可靠性,从而成为知识产权保护和数字多媒体防伪的有效手段.图 1 为基于通信模型的水印系统基本模型[5].

水印系统主要包括两部分:水印嵌入器和水印检测器.水印嵌入器的工作过程为:首先根据某个水印密钥 k 生成一组信息模板 W_m,然后将它们组合起来对信息 m 进行编码,然后再对信息模板进行缩放或其他变换以产生最终的附加模板 W_a.接下来把 W_a 加到载体作品 C_0 上,便产生了水印作品 C_w.这类水印嵌入器叫做盲嵌入器,如果水印嵌入和原始载体作品有关,则称为含辅助信息的嵌入器.在嵌入附加模板后,假设水印作品 C_w 还经历了某些处理过程,其结果相当于在作品中加入了噪声 n,从而形成 C_{wn}.水印的检测则首先从接收到的作品 C_{wn}中减去原始载体作品 C_0 得到带噪声的水印模型 W_n,然后在水印解码器中使用水印密钥对其进行解码.因为嵌入时加入载体作品在检测是被完全减去,附加模板 W_a 和 W_n 的唯一差别是由噪声引起的.如果在水印检测时不用知道原始载体作品 C_0 的信息,则称为盲检测器.

水印算法识别被嵌入到保护对象中的所有者的有关信息(如注册的用户号码、产品标志或有意义的文字等)并能在需要的时候将其提取出来,用来判别对象是否受到保护,并能够监视被保护数据的传播、真伪鉴别以及非法拷贝控制等.

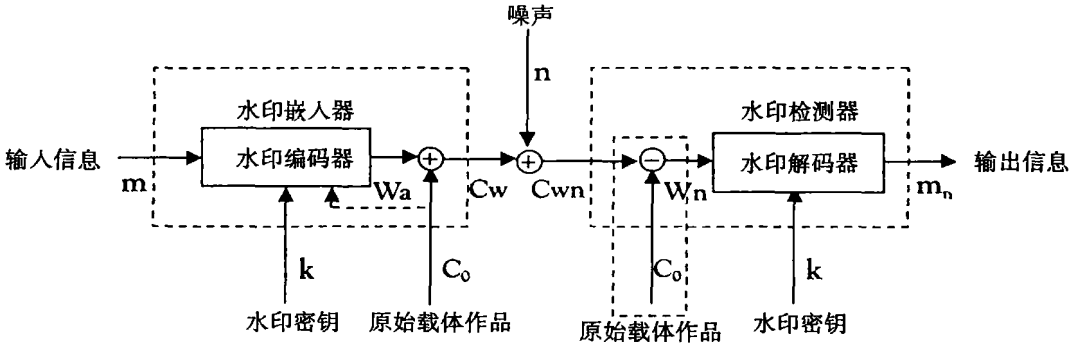

图 1　水印系统基本模型

3　图像加密技术

近年图像加密技术得到了快速发展,除了基于密码学的图像加密技术以外,考虑到图像信息的一些特征,近年来针对数字图像特点,人们研究了许多图像加密算法.

早期的数字图像加密算法主要有以下几类:1)基于置乱的图像加密技术[6],2)基于伪随机序列的加密技术[7].3)基于 SCAN 语言的加密技术[8],4)基于"密钥图像"的加密技术[9],5)基于四叉树编码及 SCAN 语言的加密技术[10],6)基于图像的矢量量化(VQ)压缩编码技术及商业密码加密技术[4]等.文献[11,12]对这些算法进行了较好的综述,并指出这些加密算法总体来说保密性不高或者加密效率不高,而且其加密算法大多不能公开,不符合现代密码体制的要求,在实际应用中应该加以适当的改进.

除以上几类加密技术外,近年来,图像加密技术的发展主要有以下几方面:

1) 基于混沌思想的图像加密技术.由于混沌动力学的发展,人们逐渐认识到混沌系统是一种天然的密码系统,因此基于混沌的图像加密技术的研究成了一个研究热点和方向,这个领域也出现了大量的研究成果[13,14,15,16].这些算法的基本思想是首先通过某种混沌映射如 Logistic、Rossler、Lorenz 映射等生成具有较高随机性和长周期的密钥序列,再对图像进行加密.由于一维映射生成的混沌序列经过简单的变换加密是一种平凡的加密系统,安全性难以保障[17,18],因此,基于混沌系统的数字图像加密算法正逐步由低维向高维混沌系统甚至超混沌系统的图像加密算法方向发展.

2) 改进的基于密码学的数字图像加密算法.文献[19]提出利用 Fibonacci 数列良好的均匀性,对标准 DES 算法的初始置换表 IP 表进行改进,再用于图像加密,具有良好的雪崩效应和抗攻击能力.文献[20]探讨了基于椭圆曲线加密体制进行图像加密的算法,具有一定的实用性.但这类算法对数字图像完全加密的方法虽然安全性较高,但还是存在要改变数据的格式,计算复杂性较高的缺点.因此对图像采取有选择性的部分加密方法就成了目前的一个研究方向[21].

3) 基于新的变换方法的图像置乱加密算法.早期的基于置乱的图像加密算法多采用 Arnold 变换或幻方变换来对图像像素进行置乱,算法的安全性不高,因此人们便探讨了许多新的变换方法来对图像进行置乱以提高算法的安全性[22,23],这些方法计算效率较好,适用于对安全性要求不太高的场合.

4)新的理论和工具在图像加密中的应用研究.文献[24]利用混沌系统产生二进序列来设定神经网络的权值和阀值,对每个像素进行加密运算,这种方法计算复杂度大,无失真且安全性高,但计算效率低.文献[25]利用不对称分数傅立叶的特性,对图像 x,y 方向分别实话不同级次的一维分数傅

立叶变换来对图像进行加密，从实验结果看，具有较好的效果.文献[26]则利用混沌映射的随机性以及不可预测性，产生混沌序列矩阵对小波变换矩阵系数进行调整，再对系数进行置乱处理，然后利用信息隐藏技术对密钥进行隐藏，这种方法加密强度高，安全性好，计算效率也较高，具有较好的实用性.

4 图像水印技术

根据应用领域的不同，图像水印可以分成两大类：鲁棒水印和脆弱水印.鲁棒水印主要用于版权保护.

1) 鲁棒水印.鲁棒水印的基础研究主要集中在鲁棒水印算法、水印容量等方面.在水印算法方面，90 年代中期，采用通信理论模型，将原始图像和有意无意的攻击看作噪声，特别是将扩频通信理论引入后，水印的鲁棒性大大提高，随后提出结合感知模型、自适应的鲁棒水印算法，在此基础上，提出了更精确的带边信息(side information)的水印模型.最近，提出矢量量化的方法，预言能取得更鲁棒的算法[27].文献[28]提出的基于奇异值分解的鲁棒水印算法，通过理论分析和实验证明具有很好的鲁棒性[29,30,31].

在不同鲁棒性算法中，水印容量分析相当重要，结合信息论、通信理论，分析容量范围，成为了当前研究热点.文献[32]利用直接扩频技术把被隐藏信息转换为嵌入信号并将它嵌入选定的静止图像的 DCT 系数中，对水印信号容量进行计算，文献[33]提出了一种利用噪声可见性函数对水印嵌入功率进行自适应限定的水印容量分析方法，这些方法对水印系统的设计具有一定的指导意义.

目前另一个主要方向是对鲁棒水印算法的攻击和反攻击的研究，如共谋攻击、混淆攻击(IBM 攻击)、拷贝攻击、抗几何攻击和同步攻击等.传统的误警概率和位错误率引入到数字水印模型中，有利于衡量水印算法和具体的应用相结合.采用更精确的噪声模型，尤其是针对量化噪声，具有很大的现实意义，因为大量的水印工作需要结合基于量化的有损压缩.

2) 脆弱水印.与鲁棒性水印不同的是脆弱性水印主要用于确定图像在传输或分发过程中是否被非法编辑、修改、破坏或恶意篡改过，因此主要用于图像的内容认证，人们称这种系统为图像认证系统[34].

当前图像脆弱性水印的研究主要从完全脆弱水印、半脆弱水印、图像可视内容的真伪鉴别与自嵌入式水印四个层次进行研究[35].在完全脆弱水印的层次上，如何有效地抵抗“伪认证的攻击”是一个急需解决的问题；在半脆弱水印的层次上，目前已有能够抵抗 JPEG 压缩的脆弱性水印算法，尚无抵抗 JPEG2000 的脆弱性水印算法，而实际中用户一般不知道采用的压缩标准是那种，因此设计一种与压缩标准无关的半脆弱性水印算法也是非常必要的；在图像可视内容真伪鉴别的层次上，如何对图像的可视内容进行定义是一个关键的问题而且也是一个比较难的问题；而在自嵌入式水印层次上，最重要的功能就是对篡改定位并且恢复，如何能够有效地恢复被篡改的部分也是一个非常有意义的方向.

也有少数学者[36,37]考虑把脆弱性水印与鲁棒性水印结合在一起.虽然也是用于内容认证，但与传统的数字签名不同.传统的数字签名技术是为通信领域的信息传送进行篡改检测，而脆弱性数字水印技术则为网络环境下的多媒体的内容保护提供了一个有效的解决方案.

5 总结与展望

如何在网络背景下解决图像的安全性问题，成了目前的一个研究热点.近年虽然在这些领域均取得了很大的进展，但图像的安全性性问题还没有得到完满的解决，目前在以下几个方面还需要努力：

1) 对于图像加密技术，在寻找符合现代密码体制的加密方法的同时，选择合适的内容，对图像进行部分加密，将可获得高效加密的同时获得良好的保密性.

2) 对消息认证码以及数字签名技术考虑与图像内容相结合以获得具有较高抗攻击的能力.

3) 数字水印是解决版权保护的有效技术手段，如何在网络中检测水印，由此打击非法分布和非法传播是一个重要的课题.

4) 以前的水印算法几乎全是独立的，没有根据具体的应用要求设计，根据现有的应用和可能的应用制定相应的具体要求，并据此选择、设计水印算法，将现有的大量水印算法分类比较，具有很大的现实意义.

5) 很多系统基于网络，网络只是尽最大可能的传送，无法保证服务质量，并且一般传输都要结合压缩编码，研究基于网络特性的水印是一个挑战.

6) 对于脆弱水印的研究还远未成熟，尚有许多问题待于解决，尤其在将技术推向标准化方面多做一些工作，包括水印嵌入算法和检测算法的理论研究、水印的构造模型、水印能量和容量的理论估计、算法的评价等等，尚缺乏对脆弱性水印系统进行公正的比较和评价方法，水印系统的脆弱之处无法进行全面测试与衡量[38].

参考文献：

[1] 阙喜戎，孙 锐，龚向阳，王 纯.信息安全原理及应用[M].清华大学出版社，2003.

[2] C. E. Shannon, Communication theory of secrecy systems[J]. Bell Syst. Tech. J., Vol.28, pp. 656—715, Oct, 1949.

[3] G. J. Simmons, Ed., Contemporary cryptology—the science of information integrity[M]. New York: IEEE Press, 1992.

[4] Chang C C, et al, A new encryption algorithm for image cryptosystems[J]. The Journal of Systems and Software, 2001, 58(7): 83—91.

[5] 王炳锡，陈琦，邓峰森.数字水印技术[M].西安：西安电

子科技大学出版社.2003.

[6] 丁　伟,齐东旭.数字图像变换及信息隐藏与伪装技术[J].计算机学报,1998,21(9):838－843.

[7] Schwartz C. A new graphical method for encryption of computer data[J].Cryptology, 1991,15(1): 43－46.

[8] Bourbakis N, Alexopoulos C., Picture data encryption using SCAN patterns[J].Pattern Recognition, 1992,25(6):567－581.

[9] Kuo C J. Novel image encryption technique and its application in progressive transmission[J].J. Electron. Imaging, 1993,2(4):345－351.

[10] Chang H K, Liou J I.. An image encryption scheme based on quadtree compression scheme[A]. Proceedings of the International Computer Symposium[C].Taiwan:2001,230－237.

[11] 张浩然,图像加密技术综述[J].计算机研究与发展,2002,(10):1317－1324.

[12] 李昌刚,韩正之,图像加密技术新进展[J].信息与控制,2003,(4):4:339－343.

[13] 陈永强,孙华宁.基于二维混沌映射的数字图像加密算法[J].武汉工业学院学报,2004, 23(4):45－48.

[14] 王　英,郑德邻,鞠　磊.基于 Lorenz 混沌系统的数字图像加密算法[J].北京科技大学学报,2004, 26(6):678－682.

[15] 于为中,马红光,王令欢,等.基于一维混沌映射的图像加密算法[J].计算机应用,2005,25(1):141－143

[16] 彭　飞,丘水生,龙　敏.一种基于混合混沌动力系统的图像加密算法[J].计算机应用,2005, 25(3):543－556.

[17] Short K M, Unmasking a modulated chaotic communications scheme[J].Int. J. Bifurcation Chaos, 1996, 6(2):367

[18] Yang T, Yang L B, Yang C M, Breaking chaotic switching using generalized synchronization: Examples[J].IEEE Trans Circuits Sys. I, 1998, 45(10):1062

[19] 钟文琦,刘　雪,商艳红,等.一种改进 DES 的数字图像加密方法[J].北方工业大学学报,2005, 17(1):10－14.

[20] 蒋金山,曾德炉.基于椭圆曲线公钥密码体制的数字图像加密技术[J].微型机与应用,2004,(5):50－52.

[21] 廉士国,李忠新,王执铨.两种基于部分加密的图像和视频加密方案[J].计算机工程,2004,30(7):18－20.

[22] 王成儒,王凤英,胡正平.截断 Baker 变换及其在数字图像加密中的应用[J].计算机工程,2004, 30(18):103－105.

[23] 陆红强,赵建林,范　琦,等.基于像素置乱技术的多重双随机相位加密法[J].光子学报,2005,34(7):1069－1073.

[24] 丁　群,陆哲明,孙晓军.混沌神经网络密码的图像加密[J].电子学报,2004,32(4):677－679.

[25] 何俊发,李　俊,王红霞,等.不对称离散分数傅里叶变换实现数字图像的加密交换[J].2005,31(3):409－411.

[26] 尹显东,姚　军,唐　丹,等.基于小波变换域的图像加密技术研究[J].信息与电子工程,2005,3(1):1－5.

[27] 石　磊,钟　铭、洪　帆.抵抗几何变换的基于量化的水印技术[J].计算机辅助设计与图形学学报,2004,16(6):850－855.

[28] 周　波,陈　健.一种基于奇异值分解的稳健数字水印算法[J].计算机工程,2004,30(15):120－121

[29] 易开祥,石教英,孙　鑫.数字水印技术研究进展[J].中国图象图形学报,2001,6(2):111－117.

[30] 常　敏,卢　超,蒋　明,等.数字图像水印综述[J].计算机应用研究,2003,(10):1－4.

[31] 杨　忠,李万社,刘　艳,等.数字水印技术综述[J].安康师专学报,2004,12(10):80－84.

[32] 杜　江,喻建平,谢维信,等.信息隐藏的理论容量测度研究[J].信号处理,1999,15(10):601－604.

[33] 张　帆,张鸿宾.数字图像水印容量分析[J].计算机工程与应用,2004,14:11－15.

[34] N. Memon, S. Shende, and P. Wong, On the security of the Yueng－Mintzer Authentication Watermark[C]. Final Program and Proceedings of the IS&T PICS 99, pp. 301－306, Savanna, Geogia, April 1999.

[35] J. Fridrich, Methods for Tamper Detection in Digital Images[A].Multimedia and Security Workshop at ACM Multimedia 99, Orlando, FL, USA, Oct, 1999.

[36] C.S. Lu, H. M. Liao and C. J. Sze, Combined Watermarking for Image Authentication and Protection[A].Proc.1st IEEE Int. Conf. on Multimedia and Expo, New York City, NY, USA, Jul. 30～Aug. 2, 2000.

[37] C.S. Lu, S.K. Huang, C. J. Sze, and H. M. Liao, Cocktail Watermarking for Digital Image Protection [J]. IEEE Trans. on Multimedia, Vol. 2, No. 4, pp. 209－224, 2000.

[38] J. J. Quisquater, B. Macq, M. Joye, N. Degand and A. Bernard, Practical Solution to Authentication of Images with a Secure Camera[A].SPIE International Conference on Storage and Retrieval for Image and Video Databases, vol. 3022, pp. 290－297, San Jose, USA, Feb. 1997.

A Brief Review on Security of Digital Image

HUANG XIAO-sheng

(School of Civil Engineering and Architecture, East China Jiaotong University, Nanchang 330013, China)

Abstract: Effective digital image security is an increasing important issue in a networked environment. An overall analysis of the requirement of image security, which is met by security mechanisms and measures, is made. We especially review the digital image encryption techniques and the digital image watermarking techniques, and point out the remaining problems of the image security measures and propose some research directions and key issues in the field in future.

Key words: information security; cryptology; image encryption; digital watermarking

(上接第 74 页)

实时、历史数据和实时、历史趋势曲线成组显示,通过选择不同的测点组,操作员可浏览在任意测点的当前数据的状态和曲线以及一段时间内任意时间段的历史数据和历史曲线,为用户检错、纠错提供了方便.

5) 报表生成模块

系统提供定时报表打印、报警打印、历史数据记录报表,报表内容可动态设定.

6) 数据记录模块

系统完成数据定时存到数据记录文件、定时生成数据记录文件、定时删除数据记录文件等功能.

6 结束语

本文介绍一个与 RSView32 结合的 LonWorks 组态监控系统,系统与 LNS DDE Server 相连,以 DDE 方式访问网络,是一个集控制系统的功能组态、实时监控、远程监控和实时报警功能于一体的组态平台.由于组态软件 RSView32 具有较强的功能,使 LonWorks 技术在监控中应用得到进一步发展和完善,它的应用将会越来越广泛.

参考文献:

[1] 阳宪惠.现场总线技术及其应用.北京[M].北京:清华大学出版社,2003,6.

[2] 黄天戍,汤 滢,陈 健.DDE 技术在 LON 总线中的应用[J].电子技术,2001,(10):24－25

[3] ECHELON Corporation. LNS DDE Server User's Guide.Version 2.11,2002

[4] 张明光. RSView32 工控组态软件功能分析和应用举例[J].自动化仪表,2002,(6):53－55.

[5] 谢 昕,尹 燕.基于 DDE 的 RSView32 与 Delphi 数据通讯的实现[J].华东交通大学学报,2004,(5):26－28.

[6] 刘 磊. LonWorks FCS 的组态监控平台设计与应用[J].基础自动化,2001,(4):22－25.

Application of RSView32 in LonWorks configuration supervisory

SU Hong-bo, YUAN Ke-feng

(School of Information Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper Introduces the functions of the LNS DDE Server, and combining with the RSView32 configuration software, designed the LonWorks supervisory system.

Key words: LNS; LNS DDE Server; Rsview32; configuration software; supervisory system