

◎ 宋 伟 / 著

SHUZI TUXIANG
SHUYIYIN SUANFA
JI YINGYONG

数字图像水印

算法及应用

中央民族大学出版社
China Minzu University Press

数字图像水印算法及应用

SHUZI TUXIANG SHUIYIN SUANFA JI YINGYONG

◎ 宋 伟 / 著



中央民族大学出版社
China Minzu University Press

图书在版编目 (CIP) 数据

数字图像水印算法及应用/宋伟著. —北京: 中央民族大学出版社, 2018.7 重印
ISBN 978-7-5660-0542-7

I. ①数… II. ①宋… III. ①电子计算机—密码术
IV. ①TP309.7

中国版本图书馆 CIP 数据核字 (2013) 第 258723 号

数字图像水印算法及应用

著 者	宋 伟
责任编辑	满福玺
封面设计	布拉格
出 版 者	中央民族大学出版社
	北京市海淀区中关村南大街 27 号 邮编: 100081
	电话: 68472815 (发行部) 传真: 68932751 (发行部)
	68932218 (总编室) 68932447 (办公室)
发 行 者	全国各地新华书店
印 刷 厂	北京建宏印刷有限公司
开 本	880×1230 (毫米) 1/32 印张: 6.25
字 数	130 千字
版 次	2018 年 7 月第 2 次印刷
书 号	ISBN 978-7-5660-0542-7
定 价	28.00 元

版权所有 翻印必究

序

数字技术的发展使得人们在享受数字化带来便利的同时,也深陷安全隐患之中。数字图像,作为多媒体形式的主要内容,其获取、修改、传输越来越容易,随之而来的数字图像的真实性、完整性验证以及数字版权带来的归属确认等问题一定程度上制约了信息化技术的发展。出于保护多媒体产品,特别是数字图像知识产权不断增长的需求,出于使用传统的密码技术受到限制而又必须进行隐秘通信的特殊需求,信息隐藏技术得到了迅速发展。本课题就信息技术领域中的一大研究热点问题,即信息隐藏中的数字水印技术进行研究。

本著作在查阅了大量资料的基础上,对图像认证技术、鲁棒性数字水印技术、零水印技术和可逆信息隐藏技术四个方面进行了研究,提出了新的算法和模型。取得的成果总结如下:

1. 针对图像认证技术中定位精度和安全性之间矛盾这一关键问题,提出了新的基于混沌系统的图像认证水印算法。基于猫映射构成的循环结构,将不相关的图像块由于水印的嵌入变得相关,解决了传统的一一对应块相关算法定位精度不高的问题。选取对初值极端敏感的 Logistic 混沌系统构造伪随机循环链,利用奇异

值分解构造基于图像内容的水印,在保持块独立算法高定位精度的同时,提高了算法的安全性;同时证明矩阵行或列互换时奇异值不发生改变,从而指出利用奇异值直接生成水印,在水印检测时发生漏检,导致篡改定位精度不高的问题。

2. 为有效解决数字图像版权保护问题,提出了两类具有良好数学基础的鲁棒性水印算法。将优化理论中具有良好学习能力和泛化能力的支持向量机和数字水印算法相结合,完成了一种基于优化理论的鲁棒性数字水印算法,利用支持向量机的回归理论建立图像像素间关系的理论模型,通过该模型利用周围像素预测目标像素值,从而通过修改目标像素值嵌入水印。将分解理论中的QR分解引入数字水印技术中,通过分析QR分解后 Q 矩阵中系数的不变特性,从而通过修改 Q 矩阵第一列系数嵌入水印。两类算法均为盲水印算法,且能够有效地抵抗一系列常规的图像攻击,具有很好的鲁棒性。

3. 针对传统水印算法通过修改原始宿主图像内容嵌入水印,对图像造成不可修复性损失的问题,提出了基于奇异值分解的零水印算法。利用奇异值分解的稳定性,通过验证奇异值对算法鲁棒性的影响,选取第一个奇异值构造图像信息,并利用具有意义的二值图像作为水印图像,将其与图像信息进行运算作为保存在第三方的版权认证信息,有效地解决了传统零水印算法可视性效果不佳的问题。同时对水印容量和算法安全性进行了深入的分析。

4. 在可逆信息隐藏技术方面,针对基于差值扩展技术中差值

扩展对图像像素值修改幅度过大的问题,引入了改进型对数函数,进一步缩小了差值扩展后的像素值和原始像素值之间的距离,从而有效地提高了嵌入数据后图像的质量。同时,针对传统可逆信息隐藏算法单一嵌入容量和单一嵌入方向的问题,利用图像块间的均值关系,设计了图像块类型判定准则和图像块嵌入方向判定准则,实现了多嵌入容量和多嵌入方向的目标,在增加数据嵌入容量的同时,有效地提高了嵌入数据后图像的质量。

该研究是属于图像处理、信息安全、数学等领域的交叉学科,研究成果解决了数字水印技术中存在的一些关键问题,丰富和完善了数字水印技术,对数字多媒体信息特别是数字图像的版权保护起到了积极的推动作用。

本著作的出版得到中央民族大学“985”建设经费的支持,这里一并表示感谢!

目 录

第 1 章 绪论	1
1.1 引言	1
1.2 研究背景与研究动机	2
1.3 国内外研究现状	7
1.4 本书的研究内容及其框架结构	25
1.5 本书的研究情况	27
1.6 本书章节安排	30
第 2 章 相关工作综述	32
2.1 引言	32
2.2 数字水印的基本框架结构	32
2.3 数字图像水印的基本要求	39
2.4 本章小结	44
第 3 章 混沌系统的图像认证水印算法的研究	45
3.1 引言	45
3.2 图像认证水印算法的结构研究	45

3.3 花托自同构混沌系统和 Logistic 混沌系统·····	49
3.4 基于猫映射构成的循环结构的图像认证 水印算法·····	51
3.5 基于奇异值分解和 Logistic 系统的图像认证 水印算法·····	59
3.6 本章小结·····	70
 第 4 章 优化理论和分解理论的鲁棒性数字水印 算法的研究·····	72
4.1 引言·····	72
4.2 基于优化理论的鲁棒性数字水印算法·····	72
4.3 基于分解理论的鲁棒性数字水印算法 的研究·····	87
4.4 本章小结·····	103
 第 5 章 基于奇异值分解的零水印算法的研究·····	105
5.1 引言·····	105
5.2 零水印基本算法研究·····	106
5.3 基于 SVD 的数字图像零水印算法的流程·····	109
5.4 本章小结·····	125
 第 6 章 可逆数字图像信息隐藏算法的研究·····	126

6.1 引言	126
6.2 可逆信息隐藏算法的基本框架	126
6.3 可逆信息隐藏基本算法研究	127
6.4 基于对数函数的可逆信息隐藏算法	138
6.5 基于块分类和差值扩展的可逆信息隐藏算法	152
6.6 本章小结	169
 第7章 全书总结及其展望	 171
7.1 全书总结	171
7.2 工作展望	174
 参考文献	 177

第1章 绪 论

1.1 引言

自 20 世纪 90 年来以来,网络技术的发展产生了多种新型多媒体形式,诸如文字、图像、声音、多媒体数据等,而计算机的普及使得这些多媒体形式能够迅速地传播到世界各地。但是,网络的平民化在给人们带来信息获取的便利性和信息传输的快捷性的同时,也给人们带来了安全上的诸多问题。网络的开放和共享使得版权侵犯、信息篡改的现象时常发生,给人们的生活和社会造成了重大的影响和经济损失。作为信息隐藏(Information Hiding or Data Hiding)领域关键技术之一的数字水印技术(Digital Watermarking)凭借其有效检测数字图像完整性和有效进行数字版权保护等诸多特性引起很多研究者的关注。本著作通过对现有的数字图像水印技术进行分析从而展开研究。本章主要介绍本书的研究背景与研究动机,通过分析现有技术中存在的一些关键问题,给出了研究内容及其框架结构,努力使研究内容系统化、整体化。最后对所取得的成果进行简要的概述,并对本书的章节进行了安排。

1.2 研究背景与研究动机

中国互联网络信息中心 (CNNIC) 在 2009 年 7 月份发布的《第 24 次中国互联网络发展状况调查统计报告》中指出:截至 2009 年 6 月底,中国网民规模达到 3.38 亿人 (图 1-1),较 2008 年底增长 13.4%,上网普及率达到 25.5%。网民规模持续扩大,互联网普及率平稳上升^[1]。

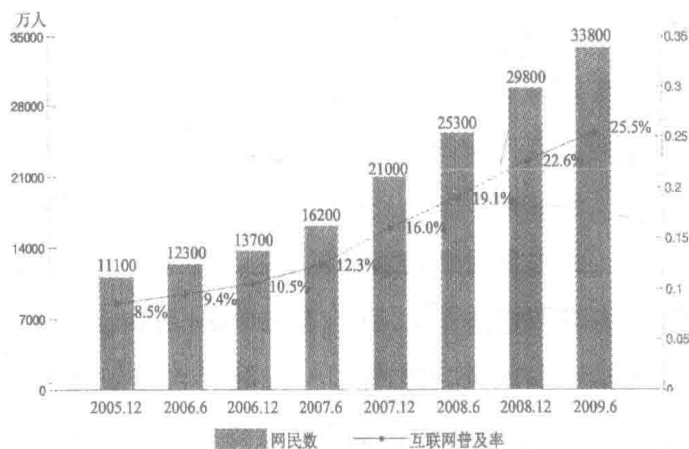


图 1-1 中国大陆网民规模与互联网普及率

Fig.1-1 The Scale of Chinese Mainland Netizens and Popularizing Rate of Internet

网民规模的扩大和网络普及率的上升表明:社会经济的发展使得人们的生活水平不断提高,对物质的需要达到一定满足后,社会交流和信息获取成了精神生活的重要成分。而网络作为媒体和交流工具,填补了人们在日常生活中信息和社会交流的空缺。网站作为网络的主要存在形式,是人们交流和学习的主要途径,

其数量也正以极快的速度增长。截至2009年6月,中国的网站数,即域名注册者在中国境内的网站数(包括在境内接入和境外接入)达到306万个(图1-2),较2008年末增长6.4%^[1]。

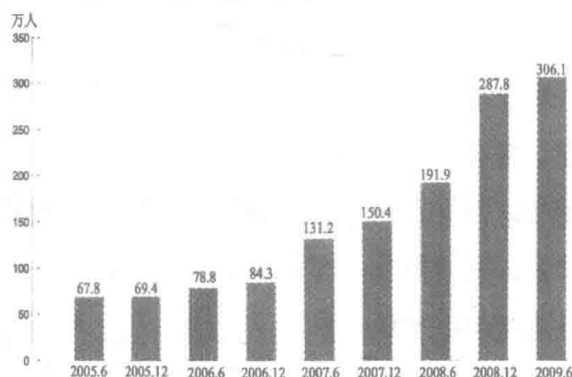


图1-2 我国大陆网站规模变化

Fig 1-2 Scale of Chinese Mainland's Websites

网站的多媒体内容多为图像、音频、视频。据不完全统计,多媒体中的图像占据高达98%的份额(表1-1),图像作为信息含量最为丰富,且是信息传递的一个有利载体,广泛应用在新闻报道、智能信息收集等网络环境中^[2-4]。

表1-1 中国互联网网页内容分类情况(按多媒体形式)

Tab.1-1 Content classification of website in Chinese internet

(according to the type of multimedia)

年份	图像	音频	视频	全国网页总数
2005年	98.75%	1.13%	0.11%	约24亿个
2004年	98.91%	0.75%	0.34%	约6.507亿个
2003年	97.9%	0.5%	1.6%	约3.118亿个

然而在现实生活中，随着各种高质量和高精度的图像处理设备，如高像素数码相机、高分辨率的打印机、扫描仪、复印机的出现，以及大量的图像编辑软件如 Adobe PhotoShop、Microsoft Paint、PaintShop Pro 的普遍应用，使得数字图像的获取，修改变得更加容易。这些编辑软件可以实现图像的各种编辑和处理，如图像效果处理、图像剪辑、拼接、合成等。虽然人们可以方便地从网上得到图像，但这些图像是否被篡改，是否真实和完整，却很难被用户确定。正如美国《PC》所说“只怕日后，照片再也不能符合‘眼见为实’这一说了”。

同时网络爱好者或者政府部门常常把自己的作品或者有重要意义的图像放在网站，供人们使用或者学习，但如果有不法分子对其进行篡改或者恶意占有这些作品，网络的快速传播使得这些篡改后不真实的作品以讹传讹，必定会造成不良后果。另外，在法庭或者交通管理中拍摄的痕迹物证图片、交通违章肇事图片等有重要证据意义的图片，如果不能得到可信的来源，那么别有用心的图片提供者可以通过现有的图像处理软件对犯罪现场证据图像中的部分场景或人物进行操作和篡改，如将人物进行替换或者移除，将号码擦除等，使得看似真实的图片无法提供真实的证据。这表明了数字图像的完整性在犯罪调查、安全监控、医疗保健、法律证据、数字金融文档领域等一些非网络应用中扮演着越来越重要的角色。图像的不完整性和不真实性给大众带来了信任危机。

除此之外，在 2009 年 11 月中旬，25 家美国图书馆参加的全

球最大“虚拟图书馆”正式启动,使得人们在网络上能够建成“人类知识的源泉”,从而可以分享庞大的藏书与资料,任何人只需一台电脑,都可随时随地免费阅览藏书。然而这些可读的主要是著作权过期的书籍,更多的图书馆仍未参与其中。究其原因,书籍的电子化版权归宿认证使得这项造福人类的计划受到一定程度的影响。在书籍电子化的著作权规则尚未完善之前,更多的图书馆担心大量的图书参与其中,将会引起较为麻烦的版权归属纠纷。

由此可以看到,社会的信息化虽然给我们带来了巨大的好处,为我们的生活带来了便利,但这种技术带来的各种各样的安全隐患也不容忽视。对于网上信息的可靠程度,网络消息的来源和去向,信息的保密性、真实性、完整性,通信对象的可信赖性,个人隐私的保护,以及辛勤劳动所创造的数字制品的版权等,都在引起越来越多人的注意。同时,侵权盗版活动的日益猖獗,知识产权保护问题和个人信息的保密成为数字制品发行业务首先考虑的问题。如何合理地鉴别数字图像的完整性,如何有效地保护数字产品的版权问题也日益成为人们关注的焦点。

信息隐藏通过把秘密信息永久地隐藏在可公开的媒体信息里,达到证实该媒体信息的所有权归属和数据完整性或传递秘密信息的目的,从而为数字信息的安全(Information Security)问题提供一种新的解决方法^[5-6]。信息隐藏中的数字水印作为一种有别于传统的密码技术的新技术,一定程度上有效地维护了数字作品

的版权,保护了信息的真实性和完整性,也使得用户的隐私,知识产权和财产更加安全。信息隐藏与传统的加密技术区别^[7]在于,加密技术旨在隐藏所传输信息的内容,使得网络的攻击者无法得到真正的明文,从而达到保护数据的目的,加密数据在信息解密之后将不再受到保护;而信息隐藏技术是利用人在视觉、听觉系统分辨率上的局限,以多媒体数字产品为载体,将有价值的秘密信息隐藏在其中,从而掩盖秘密信息的存在,和传统的密码技术相比,信息隐藏为数字媒体提供更进一步的保护,因为含隐藏信息的载体和原始载体变化不大,这样不易引起攻击者的注意。在实际的应用中两者相互结合,相互补充。

数字图像的完整性和版权的保护在信息化战争中将会发挥着越来越重要的作用。本书旨在解决数字图像的完整性和版权归宿确认方面的若干关键问题,将以灰度图像为研究对象,通过对数字图像水印算法深入的研究,分析现有的技术特点,提出新的理论和算法,在图像完整性鉴定和篡改准确定位的图像认证方面、在鲁棒性数字水印方面取得进展,同时提出新的零水印算法和可逆信息隐藏算法。充分利用数字水印算法的特点,促进水印技术的发展,加快其实用化的步伐,引领电子商务、票务防伪、医学、法学图像的完整性认证和数字化版权归属鉴定等领域的健康发展。数字图像水印算法的研究已成为信息安全领域中的一个新兴且极其重要的研究方向,同时也是研究图像内容安全的关键技术,对其进行研究必将具有重要的理论和现实意义。

1.3 国内外研究现状

信息隐藏作为一门横跨信号处理、通信、计算机、数学、生理学等学科的交叉学科,吸引了国内外来自不同专业的研究人员的关注。20世纪90年代初期,R.G.Schynedel等人^[8]在IEEE国际图像处理会议(ICIP'94)首次明确提出了“数字水印”概念,随后信息隐藏技术的研究便如火如荼地进行开来,有关数字水印方面的论文数量也逐年上升^[9]。在我国20世纪末,由何德全院士、周仲义院士、蔡吉人院士等信息安全领域的著名人士与有关应用研究单位联合发起召开了我国第一届信息隐藏学术研讨会,我国的信息隐藏技术也取得一定的进步^[10]。本书针对数字水印算法中的四个重要方面,即图像认证、鲁棒性数字水印、零水印算法和可逆信息隐藏存在的关键问题,详细分析了国内外的研究现状,从而引出本课题研究的主要内容以及技术难题。

1.3.1 精确定位篡改区域的图像认证技术

数字产品的完整性和真实性决定了它的应用价值。随着电子政务、电子商务技术的发展,随着网上办公、网上交易逐年递增,电子文件、电子票据的真实性、完整性、不可否认性和保密性必须得到保证。作为数字水印算法的重要分支,图像认证技术凭借其能够准确的定位篡改区域引起数字水印和图像处理学术界的浓厚兴趣。它和传统的基于密码学的数字签名^[11](Data Signature Algorithm,DSA)技术有共同点但也有本质的区别。作为一种对多

媒体信息进行论证的有效手段,数字签名在 ISO7498-2 标准中定义为:“附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据和变换允许数据单元的接收者用于确认数据单元来源和数据单元的完整性,并保护数据,防止被人(例如接收者)进行伪造。”美国电子签名标准(DSS, FIPS186-2)对数字签名作了如下解释:“利用一套规则和一个参数对数据计算所得的结果,用此结果能够确认签名者的身份和数据的完整性。”而图像认证技术是指在保证一定视觉质量前提下,将数字水印嵌入到多媒体数据中,当多媒体内容受到怀疑时,提取该水印来鉴别多媒体内容的真伪,并指出篡改位置,甚至攻击类型等^[12]。其共同点为:二者都是对接收到的信息的完整性和可信性进行认证;区别有如下两点:(一)前者是基于密码技术,即将明文加密成密文,使信息不可理解,隐藏了信息的内容,同时认证信息独立于原始图像而存在;后者是将认证信息隐藏在图像中,隐藏了信息的存在,不许额外存储或发送。(二)前者是对数据级的认证,即通过签名判断信息是否真实、完整;而后者更侧重于图像内容的完整性认证,是从多媒体数据所表示的语义内容的角度验证图像的完整性,即除了能够鉴别真实性和完整性以外,还能够较为准确地定位篡改区域,甚至能够得到有效的近似恢复^[13]。根据图像认证的目的,可将用于图像认证的水印算法分为对篡改完全敏感的脆弱水印^[14-28]和能够抵抗一定处理,诸如 JPEG 压缩的半脆弱技术^[29-31],这里我们主要针对脆弱性数字水印算法进行分析研究。