

抗几何攻击 数字水印技术

**DIGITAL WATERMARKING
ALGORITHMS ROBUST
TO GEOMETRICAL ATTACKS**

李京兵 著

知识产权出版社

TP309.7/21

2007

本书的出版得到海
科学基金[80635]和海南省教育厅项目[Hjkj200714]的资助

抗几何攻击数字水印技术

**Digital Watermarking Algorithms
Robust to Geometrical Attacks**

李京兵 著

知识产权出版社

内容提要:

数字水印是保护数字媒体版权的有效手段之一,作为国内第一本关于抗几何攻击数字水印技术的专著,本书主要包括以下内容:数字水印的基本知识、数字水印常用的数学变换和人眼的视觉系统理论、抗几何攻击的数字水印算法研究、抗局部非线性几何攻击研究、二值文本图像鲁棒数字水印算法研究,并提出了一种基于互联网的鲁棒水印系统工作原理和性能指标。

本书既可以作为计算机科学与技术、电子工程、系统科学、信息技术等相关专业高年级本科生、研究生和研究人员的科研用书,也可作为相关课程的补充教材。同时,本书还可以作为安全系统、基于内容的文本检索、图像处理和模式识别系统等研究开发人员和工程技术人员参考资料。

责任编辑:马 岳

装帧设计:臧 磊

图书在版编目(CIP)数据

抗几何攻击数字水印技术/李京兵 著. — 北京:知识产权出版社,2007.9

ISBN 978-7-80198-982-6

I. 抗… II. 李… III. 电子计算机—密码术 IV. TP309.7

中国版本图书馆 CIP 数据核字(2007)第 122221 号

抗几何攻击数字水印技术

Kang Jihe Gongji Shuzi Shuiyin Jishu

李京兵 著

出版发行: 知识产权出版社

社 址: 北京市海淀区马甸南村 1 号

网 址: <http://www.ipph.com>

发行电话: 010-82000893 82000860 转 8101

印 刷: 知识产权出版社电子制作中心

责编电话: 010-82000860 转 8325

开 本: 880mm×1230mm 1/32

版 次: 2007 年 12 月第一版

字 数: 150 千字

邮 编: 100088

邮 箱: zscq-bjb@126.com

传 真: 010-82000893

经 销: 新华书店及相关销售网点

责编邮箱: mayue@cnipr.com

印 张: 6.5

印 次: 2008 年 4 月第二次印刷

定 价: 22.00 元

ISBN 978-7-80198-982-6/T·254 (2036)

版权所有 侵权必究

如有印装质量问题,本社负责调换。

前 言

近年来，随着互联网和多媒体技术的迅猛发展，各种形式的多媒体作品包括图像、视频、音频得以利用网络途径向外发布或下载，这给人们的工作和生活带来了极大的方便，但同时也带来了一些负面的影响，那就是对原始作品的知识产权的侵犯变得容易。有些人不经过作者的同意，就对原作品进行拷贝、复制、修改。因此，当前如何在网络中实施有效的版权保护和解决信息安全的问题，就成为一个日益重要的课题。在这种情况下，人们提出了数字水印的概念。数字水印是进行数字媒体版权保护的有效手段之一。它将水印嵌入到数字媒体中，然后通过对水印的检测来确定媒体的版权所有，并且可以跟踪数字媒体的使用情况。

数字水印是一门新兴学科，其研究涉及信息学、密码学、数学、计算机科学、模式识别等多种学科。数字水印技术自1993年提出以来，发展已有十多年了，人们研究出多种水印算法，但目前数字水印仍然是一个未成熟的领域，还有许多难题没有解决，离实际应用阶段还有一段距离。特别是在抗几何攻击、抗局部非线性几何攻击和文本水印、多水印等方面还有许多瓶颈问题没有解决。本书就是针对这些问题，特别是抗几何攻击的

数字水印算法提出了自己的算法，并成功申请了四项国家发明专利。因此，写这本书的目的的一方面是使更多的人了解这一领域，满足国内外从事数字水印的研究、开发和应用的有关人员的需求；另一方面也是总结整理近几年的学习和工作成果，并与读者相互学习和讨论，共同促进数字水印技术的发展。

本书作为国内第一部关于抗几何攻击数字水印的专著，提出了基于变换域抗几何攻击的一些新算法，这些算法将数字水印、图像特征、第三方概念和密码学有机地结合在一起，有效地解决了数字水印发展所遇到的一些难题。

本书共分7章。第1章作为绪论，较为详细地介绍了数字水印的背景知识、数字水印和鲁棒数字水印研究的历史与现状；第2章介绍了数字水印算法所需要的理论基础和人类视觉系统理论；第3章内容为抗几何攻击的数字水印算法研究；第4章内容为抗局部非线性几何攻击的数字水印算法研究；第5章介绍了二值文本图像鲁棒数字水印算法研究；第6章提出了一种基于互联网的鲁棒水印系统原理及指标；第7章进行了数字水印技术的展望。

本书的出版得到海南大学学术著作出版基金、海南省自然科学基金[80635]海南省教育厅项目[Hjkj200714]的资助

由于作者水平有限，书中不妥之处在所难免，敬请各位读者批评指正。

李东兵

2007年6月

摘 要

本书以静止图像作为研究对象，根据图像处理理论和水印技术的特性，通过统计、分析大量的实验数据，在变换域中找到抗几何攻击的图像特征向量，再利用图像的特征向量进行水印的嵌入和提取；这些基于图像特征的算法具有抗几何攻击能力，它们将图像的特征向量与密码学进行了有机结合。本书提出的水印算法在抗几何攻击、抗非线性局部几何攻击，二值文本水印、多水印的嵌入等方面，都有一定的突破，并据此成功申请了四项国家发明专利（都已公布，两项已授权）。这些算法基于变换域。本书使用了全局离散余弦变换（DCT）、离散傅里叶变换（DFT）、离散小波变换（DWT），以及它们的结合体——小波余弦变换（DWT-DCT）。文章最后提出了一个新的水印系统模型和一套衡量实用水印系统的性能指标。创造性的工作如下：

（1）提出了一种基于全局 DCT 抗几何攻击和常规攻击的数字水印算法。

该算法基于全局 DCT 变换，在变换域中求出一个图像的视觉特征向量，利用该特征向量来进行水印的嵌入与提取。该算法将图像的视觉特征向量、第三方概念和加密技术、零水印

技术有机地结合。实验证明该算法具有理想的抗几何和抗常规攻击能力。与常规的水印嵌入和提取算法相比,该算法嵌入和提取水印的速度快,并且水印的提取不需原始图像,故有较高的实用价值。

(2)提出了一种基于 DWT-DCT 抗几何攻击的数字水印算法。

该算法是利用 DWT-DCT 变换,先对数字图像进行 DWT 变换,然后再对逼近子图进行全局 DCT 变换,从 DCT 低频系数中求出特征向量。该算法将主流变换 DCT 和下一代压缩标准所使用的小波变换 DWT 有机地结合起来,实验证明该算法有较强的抗几何攻击能力。

(3)提出了一种基于 DFT 抗局部非线性几何攻击(RBA)的水印算法。

该水印算法基于 DFT 变换的相位特性。通过提取图像的相位特征,来进行水印的嵌入与提取。通过实验验证,在抗局部非线性几何攻击方面,该算法的鲁棒性要优于 Adobe 公司的 Photoshop 6.0 中使用的商业水印软件 Digimarc,并且与基于傅里叶-梅林(Fourier-Mellin)变换的算法相比,该算法嵌入和提取水印的速度快,有较强的实用性。

(4)提出了一种基于 DWT 抗几何攻击的二值文本图像鲁棒水印算法。

该方法是基于小波变换,在逼近子图中进行水印的嵌入与提取。与常规的通过调整行间距和调整字间距的文档结构微调法相比,该方法嵌入水印的容量大,抗剪切等几何攻击能力强。

(5)提出一个基于互联网的鲁棒水印系统模型及一套衡量

指标。

该水印系统基于变换域，通过在变换域提取图像的特征以及利用互联网上的第三方概念，来实现水印的嵌入与提取。使用该模型的水印系统可以较好地解决数字水印的不可见性和鲁棒性之间的矛盾，并且可以解决多水印的嵌入与提取等数字水印技术的难题。为了更好地描述一个基于互联网的实用水印系统的性能，本书将自动控制理论中的稳、快、准系统指标用于水印系统，用来衡量一个实用水印系统的优劣。

总之，本书突破了传统的数字水印嵌入思想，创造性地提出了利用数字图像的特征向量来进行水印的嵌入与提取，并将特征向量、第三方概念、密码学和零水印技术有机地结合成一体，较好地解决了水印的抗几何攻击、非线性局部几何攻击、二值文本水印、多水印的嵌入等难题。

Abstract

Nowadays, with the rapid development of Internet and multimedia technologies, all kinds of multimedia work (digital image, video and music, etc.) can be found on Internet. Undoubtedly, it brings conveniences to our working and daily lives, but comes along with the problem of intellectual property protection. Some dishonest person might revise and distort multimedia works on the Internet without authorized permission from the original authors. So, how to safeguard information and intellectual properties on Internet now is an urgent subject.

Under this circumstance, the concept of digital watermarking, which could effectively protect the copyright of digital multimedia, came into shape in 1993. The basic idea is to embed watermarking into original multimedia works. When facing piratical cases, we can extract and compare watermarks of involved works.

For more than a decade, lots of watermarking algorithms have been presented, but none of them are perfect. Most algorithms become instable under geometrical attacks, particularly under local random bending attack (RBA). Topics such as document-watermarking and

multiple watermarks are also facing their bottlenecks.

In my thesis, still images are taken as main research object. By utilizing the theory of image processing and character of watermarking, a feature vector robust to geometrical distortion is acquired, which can be used to embed and extract watermarking. These feature vector-based watermarking algorithms merge the character of image with encryption, and are resistant to geometric attacks.

My algorithms are based on transformation domains (DCT, DWT, DFT, DWT-DCT and so on). In the end of my thesis, a set of innovative and practical watermarking scheme and performance-measuring norm is proposed.

The innovations of this thesis are as follows:

(1) Proposing a DCT-based watermarking algorithm robust to geometric and common attacks.

Considering that most of the watermarking algorithms are not robust to geometric distortion, a novel algorithm is presented. It based on whole DCT. An image feature vector is acquired in DCT domain, and watermarking can be embedded and extracted by using it. The algorithm links up watermarking with image's visual character perfectly. Simulation result shows this algorithm is robust to geometric and common attacks. And it functions more effectively than the others.

(2) Presenting a DWT-DCT based robust watermarking algorithm.

This algorithm grounded on DWT and DCT. The approaching

subband image is attained by using the DWT, and then the whole DCT is used for the approaching subband image. A feature vector is found from coefficients of transform domain. Results prove that the algorithm is robust to geometric attacks.

(3) Creating a DFT-based algorithm robust to local nonlinear geometric attacks.

This algorithm found on phase character of DFT. The phase character is utilized to embed and detect watermarks. This algorithm integrates phase feature with encrypting technology. Results show that this method is more robust to local nonlinear attacks than the commerce watermarking software – DIGIMARC, adopting in Adobe Photoshop. Comparing with other algorithms based on Fourier-Mellin, this algorithm is speedy.

(4) Devising a DWT-based watermarking algorithm for binary images.

This method is based upon DWT. In the approaching subband image, we embed and extract watermarks. Comparing with the common document watermarking methods, which usually changing the line space or word space to embed watermarks, this algorithm can hide more information, and remain unconverted to geometric distortions. The algorithm fuses the distillates of the first generation and the second generation watermarking techniques.

(5) Advancing an Internet based robust watermarking system model, and bringing forward performance-measuring norm of the watermarking system.

The presented model is based on transform domain, in which we find a feature vector. This system can effectively solve not only the conflicts of invisibility and robustness, but also the conflicts of invisibility and multiple watermarks.

In order to measure watermarking system's performance, a quantitative index, by means of the concepts of Robustness, Speediness and Exactness, are proposed. This kind of index is formerly used only in the field of automatic control theory.

In short, some creative and practical algorithms are detailed in this thesis. Results show that these proposed algorithms are robust to geometric and local nonlinear. They can effectively solve the problem of document watermarking, multiple watermarks, and they can also protect the copyrights of those un-watermarked multimedia works, which had already been uploaded onto the Internet.

目 录

1 绪论	1
1.1 背景	1
1.1.1 数字水印技术	4
1.1.2 数字水印的主要用途	5
1.1.3 数字水印的工作过程	6
1.1.4 数字水印的分类	9
1.2 数字水印技术研究的历史与现状	10
1.2.1 抗几何攻击数字水印的研究现状	14
1.2.2 抗局部非线性几何攻击研究现状	23
1.2.3 二值文本水印算法研究现状	25
1.2.4 多水印的嵌入与提取技术	29
1.3 常规数字水印系统的性能指标	30
1.4 数字水印攻击类型	32
1.5 数字水印所要研究的主要问题	34
1.6 本书主要研究工作及内容安排	35
1.6.1 研究工作	35
1.6.2 各章内容安排	36

2	数字水印常用的数学变换和人类视觉系统理论	38
2.1	傅里叶变换	39
2.1.1	连续傅里叶变换	39
2.1.2	离散傅里叶变换	41
2.2	余弦变换	43
2.3	小波变换	46
2.3.1	从傅里叶变换到小波变换	46
2.3.2	小波分析基本理论	48
2.3.3	小波的多分辨分析与 Mallat 算法	52
2.3.4	图像的小波变换	57
2.4	水印图像质量的定量描述	59
2.5	人类视觉系统理论	61
2.5.1	人眼的生理结构	61
2.5.2	人类视觉系统感知模型	64
2.5.3	人眼的视觉特性在水印技术中的应用	65
2.6	本章小结	70
3	抗几何攻击鲁棒数字水印算法研究	72
3.1	引言	72
3.2	一种基于 DCT 抗几何攻击的水印算法	73
3.2.1	水印的嵌入与提取算法	73
3.2.2	实验结果	81
3.3	一种基于 DWT-DCT 可抗几何攻击的水印算法	91
3.3.1	水印的嵌入与提取算法	92
3.3.2	实验结果	101
3.4	本章小结	108

4	抗局部非线性几何攻击的水印算法研究	110
4.1	引言	110
4.2	图像的离散傅里叶变换 (DFT)	111
4.3	一种基于图像相位特征的水印算法	112
4.3.1	相位特征的选取方法	112
4.3.2	一种基于图像相位特征抗局部非线性几何攻击的水印算法	115
4.4	实验结果	117
4.5	本章结论	128
5	二值文本图像鲁棒数字水印算法研究	129
5.1	引言	129
5.2	一种基于 DWT 二值文本图像数字水印算法	131
5.2.1	数字水印的嵌入和提取算法	131
5.2.2	实验结果	137
5.3	一种基于 DFT 可抗局部几何攻击的二值文本图像多水印算法	142
5.3.1	水印的嵌入与提取算法	142
5.3.2	实验结果	148
5.4	本章小结	156
6	一种基于互联网的鲁棒水印系统原理及指标	158
6.1	一种基于互联网和图像特征的鲁棒水印系统	158
6.1.1	常规的水印系统模型及难以解决的问题	158
6.1.2	基于互联网和图像特征的鲁棒水印系统模型	159

6.2 一种基于互联网和图像特征的鲁棒水印系统的性能指标	162
6.3 本章小结	164
7 结论与展望	165
7.1 全书工作总结	165
7.2 未来展望	168
参考文献	170
附录	186
附录 A 数字水印常用英汉名词对照	186
附录 B 简写符号对照表	203
附录 C 水印研究相关网址	205

1

绪 论

1.1 背 景

近年来，互联网技术发展迅猛。1996 年全球互联网用户不到 4000 万，1998 年就达到了 1 个亿，2000 年超过 2 个亿，到 2005 年年底，全球在线的互联网用户达到了 10 个亿。与此同时，数字图像、音频、视频等数字媒体发展快速，人们可以通过互联网发布自己的多媒体作品（包括图像、音频、视频、动画等），传递重要的信息。另外，通过互联网进行数字媒体的拷贝、下载、发布变得非常方便。这一方面给人们的生活和工作提供了便利，提高了工作效率，但另一方面也为数字媒体的盗版提供了方便。一些人在没有获得数字媒体所有者授权的情况下，随意拷贝和传播有版权保护的数字媒体出版物，并从中牟取巨大的非法利益。比如，有些数字媒体作品还没有公开发行，或刚发行，人们就可在互联网上免费下载、拷贝，这大大侵犯了数字媒体作品版权所有人和制作人的利益，抑止了该产