基于混沌神经网络的医学体数据水印技术

韩宝如 著

科学出版社

基于混沌神经网络的医学体数据水印技术

韩宝如 著

科学出版社
北京

内 容 简 介

本书主要包括以下内容：绪论、相关理论、基于 Legendre 混沌神经网络的抗几何攻击的水印算法、基于 Chebyshev 混沌神经网络的大容量水印算法、基于 Legendre 混沌神经网络的多重变换域水印算法。全书总结了作者多年来在这一领域的研究成果和国内外同行的有关工作，围绕医学体数据水印技术，详细地描述了基于混沌神经网络的医学体数据水印技术的具体实现过程，为数字水印的应用开拓了新方向。

本书可作为高等院校信息与通信工程、计算机科学与技术等专业高年级本科生和研究生的教材或参考书，也可供从事信息安全和数字版权管理的相关人员阅读。

图书在版编目 (CIP) 数据

基于混沌神经网络的医学体数据水印技术 / 韩宝如著. — 北京：科学出版社，2019.8

ISBN 978-7-03-057574-6

Ⅰ. ①基… Ⅱ. ①韩… Ⅲ. ①电子计算机－密码术－研究 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字 (2018) 第 117523 号

责任编辑：任 静 / 责任校对：郑金红

责任印制：张克忠 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京九州逐驰传媒文化有限公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 8 月第 一 版 开本：720×1000 B5

2019 年 8 月第一次印刷 印张：8

字数：151 000

定价：60.00 元

（如有印装质量问题，我社负责调换）

前　言

医院信息化建设给医学信息的存储和传输带来了便利，它使患者的电子病历和医学图像等医疗信息能便捷地在医院各个诊断部门之间通过网络快速传输。利用互联网可实现远程医疗，但是通过网络传输患者的医学图像时，可能会泄露患者的个人信息。患者的个人隐私，如磁共振成像、超声成像和计算机断层扫描成像等医学图像上的患者信息及患者的电子病历等数据的泄露问题随着互联网的普及变得越来越严重。数字水印技术的使用，可以使远程医疗诊断和远程手术所需要的相关患者资料在互联网上传输时受到保护，并避免患者的资料被篡改，从而起到鉴别内容真伪、保护版权等作用。

数字水印技术作为信息隐藏技术的一个重要分支，是近年来国际学术界兴起的一个前沿研究领域，其研究涉及信息学、密码学、数学、计算机科学等多种学科。数字水印技术自 1993 年被提出以来，已有二十多年的历史，出现了各种算法，但目前数字水印仍然是一个不成熟的研究领域，还存在许多难题，特别是在抗几何攻击、大容量嵌入等方面还有许多瓶颈问题没有得到解决。本书针对这些问题，在研究相关数字水印算法和分析医学图像特殊性的基础上，提出基于混沌神经网络的医学体数据水印算法。读者可在此基础上举一反三。

本书作为国内关于基于混沌神经网络的医学体数据水印技术的专著，提出一些新算法，其内容不但涵盖混沌神经网络和感知哈希，还覆盖更加可视化的三维体数据。这些算法将混沌神经网络、三维离散变换、感知哈希和零水印有机地结合在一起，有效地解决了医学图像水印发展所遇到的一些难题。

本书是作者从事医学图像水印研究的系统总结。全书共分 5 章：第 1 章介绍数字水印的背景和研究意义，以及医学图像水印算法在国内外的研究现状，从各个方面对医学图像数字水印进行详细介绍；第 2 章介绍基于混沌神经网络的医学体数据水印算法所需要的数学理论基础；第 3 章介绍基于 Legendre 混沌神经网络的抗几何攻击的水印算法；第 4 章介绍基于 Chebyshev 混沌神经网络的大容量水印算法；第 5 章介绍基于 Legendre 混沌神经网络的多重变换域水印算法。

本书可以作为专业课程的指导书，也可以作为课程设计和毕业设计指导书，还可以作为数字水印研发人员的入门参考书。

本书撰写过程中参考了国内外发表的大量文献以及网站资料（这些资料在本书

中已尽量列出，若有遗漏深表歉意），在此对本书所引用文献的作者深表感谢。

本书主要内容是作者在海南大学读博期间完成的，为此，感谢导师李京兵教授，以及学习期间给予作者鼓励与帮助的老师、同学和朋友们。

本书得到了重庆医科大学医学信息学院领导和同事的大力支持，在此一并向他们表示诚挚的感谢。

本书得到了海南省自然科学基金(项目编号：617165)和重庆医科大学医学信息学院科研启动基金的资助。

由于作者水平有限，书中难免有不足之处，欢迎读者批评指正。作者联系方式：baoruhan@cqmu.edu.cn。

作　者

2018年1月

目　录

前言

第 1 章　绪论 …… 1
1.1　背景及研究意义 …… 1
1.2　医学图像数字水印算法的研究现状 …… 4
1.3　医学数字水印概况 …… 9
1.3.1　数字水印基本概念 …… 9
1.3.2　医学图像的特点 …… 14
1.3.3　医学图像数字水印的特点 …… 16
1.3.4　医学图像数字水印的优点 …… 16
1.3.5　医学图像数字水印的种类 …… 17
1.3.6　医学图像数字水印的性能 …… 18
1.3.7　医学图像数字水印的评价 …… 19
1.4　本章小结 …… 21

第 2 章　相关理论 …… 22
2.1　混沌神经网络 …… 22
2.1.1　混沌基本理论 …… 22
2.1.2　混沌神经网络建模 …… 26
2.2　离散变换 …… 30
2.2.1　离散傅里叶变换 …… 30
2.2.2　离散余弦变换 …… 32
2.2.3　离散小波变换 …… 34
2.3　图像感知哈希 …… 37
2.4　本章小结 …… 40

第 3 章　基于 Legendre 混沌神经网络的抗几何攻击的水印算法 …… 41
3.1　引言 …… 41
3.2　Legendre 混沌神经网络 …… 42
3.3　三维离散傅里叶变换 …… 43

3.4 基于三维离散傅里叶变换的差异感知哈希算法……44
3.5 抗几何攻击的水印嵌入与提取算法……50
3.5.1 抗几何攻击的水印嵌入算法……50
3.5.2 抗几何攻击的水印提取算法……52
3.6 实验与分析……53
3.6.1 不可见性……55
3.6.2 鲁棒性……56
3.6.3 安全性……63
3.7 讨论……66
3.8 本章小结……70
第 4 章 基于 Chebyshev 混沌神经网络的大容量水印算法……71
4.1 引言……71
4.2 Chebyshev 混沌神经网络……71
4.3 分块三维离散余弦变换……73
4.4 基于分块三维离散余弦变换的均值感知哈希算法……74
4.5 大容量水印嵌入与提取算法……78
4.5.1 大容量水印嵌入算法……78
4.5.2 大容量水印提取算法……79
4.6 实验与分析……80
4.6.1 不可见性……81
4.6.2 鲁棒性……82
4.6.3 安全性……87
4.7 讨论……89
4.8 本章小结……93
第 5 章 基于 Legendre 混沌神经网络的多重变换域水印算法……94
5.1 引言……94
5.2 Legendre 混沌神经网络……94
5.3 三维离散小波变换……94
5.4 基于多重变换域的距离感知哈希算法……95
5.5 多重变换域水印嵌入与提取算法……98
5.5.1 多重变换域水印嵌入算法……98
5.5.2 多重变换域水印提取算法……99

5.6　实验与分析……100
5.6.1　不可见性……101
5.6.2　鲁棒性……102
5.6.3　安全性……108
5.7　本章小结……108
参考文献……109

第1章 绪 论

1.1 背景及研究意义

互联网在各个领域快速发展，并已广泛应用到远程医疗、网上银行、网上购物等。远程医疗是互联网的一个重要应用[1]。在远程医疗中，医疗专家利用互联网传递或接收医学数据。由于信息和通信技术的进步，医学图像可以很容易地通过网络传输进行共享、使用和处理[2,3]。当前医疗卫生行业的主要问题之一就是不能将高质量的医疗服务提供给所有的人。当前，实现公平医疗面临的主要困难是医疗资源分布不均匀[4]。计算机信息处理和通信技术的飞速发展为公平医疗提供了有效的途径。远程医疗是医疗技术和信息技术的结合，涉及医学、计算机信息处理和通信技术[5,6]。远程医疗分为远程影像学、远程诊断及会诊、远程手术和远程护理等医疗活动[1,6,7]，它给医疗服务带来了革命性的变革。我国是一个人口众多和国土广阔的大国，由于地区经济发展水平不同，医疗资源分布不均匀，各地医疗水平差别大，严重影响了医疗卫生行业的发展。因此，在我国发展远程医疗非常必要。在一系列远程医疗应用中，医学图像可以通过互联网发送给医生。一位医生可以将医学图像传送给另一位医生，以听取另一位医生的意见。因为最重要的是依据医学图像做出正确的判断，所以医学图像需要特殊的安全性和保密性，需要根据医学图像所提供的信息进行关键的诊断。利用互联网可实现远程医疗，但是通过网络传输患者的医学图像时，可能会泄露患者的个人信息。患者的个人隐私，如患者的磁共振成像(magnetic resonance imaging，MRI)、超声成像、计算机断层扫描(computed tomography，CT)成像等医学图像上的个人信息、患者的电子病历等数据的泄露问题随着互联网的普及变得越来越严重[8-10]。因此，医疗卫生行业需要更多的、可靠的医疗信息安全技术。

《中共中央国务院关于深化医药卫生体制改革的意见》中明确提出以医院管理和电子病历为重点，推进医疗信息化建设，利用网络信息技术，促进城市医院与社区卫生服务机构的合作。医疗信息化基础是基于数字信息化的，在当今医疗卫生行业中，数字信息化的作用越来越重要，各医院也进行了医疗信息化建设。传

统的诊断系统已被电子诊断系统取代。医学图像是由各种医疗设备产生的，可以将人体内的器官用图像来表示，其中的一个例子是超声图像。事实上，在大多数医院，医生诊断病情依靠的是电子和数字医学数据(如磁共振成像、超声成像、计算机断层扫描成像和 X 射线图像)，这将导致在世界各地不同的医疗中心和医院不断产生大量的电子数据(医学图像)。医学图像往往被转换成数字形式，由原来的胶片方式存储发展成数字医学图像方式存储，使它更容易被存储和分布。为了以后的诊断，医学图像被存储在患者的历史数据库中，电子病历也逐渐替代了纸质病历[11]。由于把患者的不同信息存储在单独的文件中会增加失配和诊断错误的风险，把电子病历嵌入医学图像有助于医院信息系统节省内存和降低诊断病历不匹配的风险。医院信息化建设的应用给医学信息的存储和传输带来了便利。它使患者的电子病历、医学图像等医疗信息能便捷地在医院各个诊断部门之间快速传输。另外，在标准的制定上，医学数字成像和通信(digital imaging and communications in medicine，DICOM)标准的推出与实现，进一步促进了医院间的医学影像信息的交流。医院之间的医学图像交换需要高效、可靠的信息安全技术。然而，医学图像在网络上传输时，容易遭受电子病历篡改、医学图像篡改、非法攻击和患者信息泄露等信息安全问题[12]。这容易产生患者隐私泄露、误诊和版权纠纷等难题。特别是作为医生诊断病情依据的医学图像，一旦被篡改，不但会对患者的病情造成误诊，耽误治疗的最好时机，也不能成为医疗事故鉴定的证据。这要求所有患者的电子病历、医学图像以及与医疗相关的信息必须是完整、保密和安全的[13-15]。因此，医疗信息安全问题已经成为亟待解决的难题。

目前，医疗信息安全主要是利用传统的密码加密及认证方式来实现对医学图像及相关信息的保护[16]。随着医疗信息化的快速发展，该加密方式的缺点也越来越显而易见，已经不能完全地起到保护作用。首先，医疗信息系统每天生成巨大数量的医学图像及相关信息，如果医疗信息安全采用密码加密方式保护，工作量越来越大，需要运算速度快的计算机系统。其次，密码加密方式只能在传输信道实现，计算机破解密钥的运算能力越来越强，医疗数据容易被破解。再次，对医疗信息进行加密可能会引起他人的注意，使其更容易被拦截破解。最后，传统的密码认证方式中的数字签名或消息认证码是存储在文件中与原始医疗信息一起传递的，需要额外的传递信道。并且当医学图像文件由一种格式转换为另一种格式，如由 DICOM 标准图像格式转化为 Tiff 格式时，会丢失掉存储在文件中的认证信息。这些缺陷严重影响了传统的密码加密及认证方式在医疗信息安全中的应用。因此急切需要一种可靠的方法来实现对医疗信息的保护。

医学图像数字水印可以有效地解决以上难题[8,17-20]，为医疗信息提供安全可

靠的保护。最初数字水印是用于互联网上的数字多媒体的版权保护的，现在可以利用数字水印的不可见性、鲁棒性等特点，把患者的个人信息隐藏在其医学图像中，以保证它在互联网上的安全传输[21-24]。医学图像水印的使用，可以使远程医疗诊断和远程手术所需要的相关患者资料在互联网上传输时，保护患者的隐私，并避免患者的资料被篡改[25,26]。

从现在的研究成果来看，医学图像数字水印的主要研究对象是二维医学图像，针对三维医学体数据数字水印的研究较少[20,27,28]。随着医疗成像设备的发展，在医院实际使用的大多数医学图像都是三维医学体数据，如磁共振成像、超声成像和计算机断层扫描成像等，因此医学体数据数字水印的研究具有十分重要的意义[2,29,30]。它能够有效地起到保护医疗信息的作用，能够积极有效地解决医院信息化管理中存在的占用存储空间大、医疗信息易失配和网络传输中患者个人信息被泄露及医学图像被篡改等难题[31-33]。同时，对医学体数据数字水印的研究也会促进医疗信息产业的发展，由此产生明显的经济效益和社会效益。

对于医学体数据数字水印，也有两个基本要求：第一是水印算法的鲁棒性，由于医学体数据容量较大，在进行远程传输或存储时，希望在不影响医生诊断的前提下，对这些医学体数据进行有损压缩，甚至对于一些非感兴趣区域(region of non interest，RONI)进行裁剪，不希望当这些数据经过常规的图像处理或几何变换后，隐藏在其中的患者信息丢失，所以在医学体数据中，希望水印有较强的鲁棒性；第二是希望嵌入较大容量的数字水印，对于一个医学体数据，都希望其能嵌入较多的信息，如患者的个人信息、电子病历、不同医生的诊断信息，医生希望这些信息都能够隐藏在患者的医学体数据中。但这些用传统数字水印算法难以实现。Kutter 等曾经提出第二代数字水印的思路，就是将水印嵌入图像的特征向量中，或者将数字水印和图像的特征向量相关联[34]。但由于医学图像的特殊性，嵌入的水印不能影响医学图像的视觉质量和内容，否则会影响医生的诊断结果。考虑到医学图像的特殊性，针对目前医疗信息安全中存在的问题，本书在研究相关数字水印算法和分析医学图像特殊性的基础上，提出基于混沌神经网络的医学体数据数字水印算法。该水印算法把混沌神经网络、三维离散变换、感知哈希和零水印结合在一起，实现对医学体数据全方位的保护。众所周知，零水印算法使用医学体数据特征向量进行零水印的构造，不对医学体数据做任何修改，使医学体数据具有良好的透明性，水印的提取无须原始医学体数据，不会影响医生对医学体数据的诊断，利用混沌神经网络置乱增强了水印信息的安全性，因此可以十分有效地保护医疗信息。

1.2　医学图像数字水印算法的研究现状

目前，医学图像是由各式各样的数字成像设备产生的，如磁共振成像、超声成像和计算机断层扫描成像等。复制、编辑和传送这些医学数字图像，比处理模拟图像容易得多。通常的医学图像存储在电子病历系统等。然而，这些系统收集的医疗信息用于不同的目的，如患者护理、临床研究和保险理赔等[17]，所以这些信息需要保密和验证。此外，医学图像的体量巨大，因此需要巨大的存储容量。不断发展的医学数字成像和通信标准提供了指南，确保医学图像的认证、完整性和保密性[12,35-37]。DICOM 标准已经认可像素数据压缩使用联合图像专家小组(joint photographic experts group，JPEG)、JPEG2000 压缩标准等。有时，保险公司和医疗专家等出于各种目的，可能想改变这些医学图像的基本内容，毫无疑问，为了应对此类威胁，对医学图像的保护成为一个迫切的需求。数字水印可以作为一种解决方案。

目前大部分医学图像数字水印算法以二维图像为主，根据所嵌入容量的要求和鲁棒程度来选择不同的水印算法[38]，一般嵌入的水印容量越大，不可见性越差，但鲁棒性会越好。鲁棒性和不可见性是一对矛盾。医学图像的特殊性在于其嵌入的水印不能影响医生的诊断，不能明显改变医学图像的内容，特别是不能改变图像的感兴趣区域(region of interest，ROI)，也就是含有重要病理信息的病灶区[8]。通常的医学图像水印算法都是在医学图像的 RONI 嵌入水印[17,39]，如图 1-1 所示。然而，RONI 大都是黑色的，限制了水印的容量。所以大多数时候都是花费大量的精力和时间，选择医学图像的 ROI，以便嵌入高容量的水印，如果选错区域，就会影响医生的诊断。

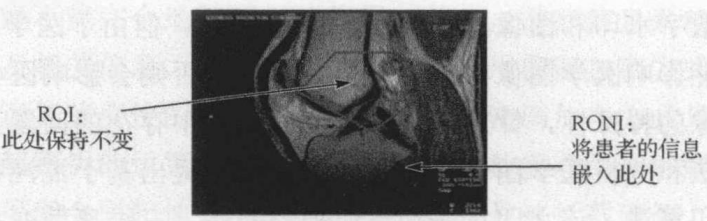

图 1-1　医学图像 ROI 和 RONI

目前，医学图像数字水印算法研究已经成为数字水印领域的研究热点，吸引了越来越多的国内外学者[26,39-43]。

在国际上，对医学图像数字水印算法的研究已经取得了不少进展[28,44,45]。其中，Giakoumaki 等将小波变换应用到医学图像数字水印中，并提出了一种改进的

算法。该算法利用 Haar 小波变换对原始图像进行三级分解，将 BCH 码的水印信息嵌入图像的第二级和第三级水平细节系数，水印信息分别由医生的数字签名和患者的个人数据构成，水印图像的平均峰值信噪比(peak signal to noise ratio，PSNR)值是 46dB[46]。

Memom 等提出了一种基于最低有效位(least significant bit，LSB)的脆弱水印算法。该脆弱水印算法把医学图像(计算机断层扫描胸部图像)分割为 ROI 和 RONI。水印由医院标识和患者的信息组成。算法令宿主图像的所有 LSB 为 0，生成的水印嵌入 RONI LSB 置乱的像素上，其水印图像的 PSNR 值大于 55dB[47]。

Wakatani 提出了一种医学图像数字水印算法。为了不影响诊断，避免在 ROI 嵌入水印，嵌入的水印用渐进编码算法压缩。嵌入水印过程中，原始图像使用离散小波变换(discrete wavelet transform，DWT)进行变换，小波函数使用 Haar 函数。水印提取是逆向的嵌入过程。该算法的主要缺点是非水印区域容易被复制攻击[39]。

Lim 等提出了一个基于网络的图像认证方法，他们使用了计算机断层扫描图像。该方法主要基于对医学图像完整性和真实性的验证。在这种方法中，水印通过使用医学图像最重要的 7 个位平面，作为哈希函数输入。此哈希函数生成 0 或 1 二进制值密钥，然后嵌入图像 LSB 平面，得到嵌入水印后的医学图像[48]。

Giakoumaki 等提出了一种基于小波变换的多水印算法。该算法提供了解决医疗数据的管理和分配问题的方法，如数据保密、归档和检索，并记录完整。该算法对医学图像进行四级小波变换，在不同频带嵌入多个水印。其实验是利用超声医学图像做的。该算法对医疗过程的隐私性有很好的保护作用并对数据的认证也有作用[46]。

Golpira 和 Danyali 提出了一种可逆盲水印。在水印嵌入过程中，该算法采用整数小波变换(integer wavelet transform，IWT)把医学图像分解成四个子带，通过选择两个阈值，根据水印数据所需的容量嵌入水印。利用逆整数小波变换(inverse integer wavelet transform，IIWT)得到嵌入水印后的图像。提取过程正好相反[49]。

Memom 等提出了一种医学图像的脆弱和鲁棒水印算法。该算法把两种不同的水印(鲁棒水印和脆弱水印)分别嵌入医学图像。嵌入过程是从医学图像分割为 ROI 和 RONI 开始的。含电子病历、医生识别码和 ROI 的 LSB 平面的鲁棒水印采用用户密钥产生的伪随机序列进行置乱。该算法把脆弱水印嵌入医学图像 ROI 部分空间域[50]，如将水印加在图像的 LSB 上[51,52]，Acharya 等将电子病历嵌入图像的 LSB 上[53]。

Trichili 等提出了一种水印算法，它采用伪随机二进制密钥进行加密，在医学图像上加虚拟边框，并把加密的水印嵌入 LSB 的每个像素上，这并不影响医学图像包含的数据，能够使医学图像以安全的方式传输[54]。

Engin 等研究了基于离散小波变换的数字水印技术，用于对监测心血管疾病的心电图的信号进行完整性验证，在不同的噪声条件下，利用不同的小波函数对提出的技术进行了评估，表明 Daubechies 小波函数的性能优于双正交小波函数[44]。

Kumar 等提出了一种新的基于离散小波变换域的扩频水印算法。该算法把敏感的医学信息，如医生的签名/识别码或患者身份码嵌入放射图像，达到身份认证的目的。该算法具有较高的水印容量[55]。

Mostafa 等提出了一种新的基于离散小波包变换(discrete wavelet packet transform，DWPT)的医学图像水印算法，该水印算法可以对患者的信息提供有效的保护，而且该水印算法在医学图像中嵌入电子病历信息以节省存储空间和传输开销，保证共享数据的安全。该水印算法是盲水印，电子病历可以从医学图像提取，且不需要原始图像[56]。

Singh 等研究了基于离散小波变换和奇异值分解的双重水印算法。为了医学图像的应用和传输，文本和图像水印被嵌入放射医学图像中。该算法结合了两种变换的优点，并消除了两者的缺点。实验结果表明，该算法具有良好的鲁棒性且不影响图像质量[57]。

在区域算法的基础上，Al-Haj 提出了一个基于频域和空间域的多水印算法。一方面，保密性和真实性由医学图像 RONI 嵌入鲁棒水印来确保，使用基于离散小波变换和奇异值分解的盲水印算法。另一方面，完整性由医学图像 ROI 嵌入脆弱水印来确保，使用基于空间域的可逆水印算法。该水印算法提出的完整性检测是在分块图像上实现的，只能进行篡改区域的局部检测[58]。

Singh 等提出了一种新的以扩频为基础的基于小波变换域的、安全的多重数字图像水印算法，利用选择性离散小波变换系数进行嵌入。该算法基于扩频技术。嵌入过程中，医学图像进行二级小波分解，图像及文本水印分别嵌入选择的离散小波变换的第一级和第二级系数中。与其他算法相比，该算法具有良好的鲁棒性和不可见性[59]。

Badshah 等对超声医学图像 ROI 无损压缩使用不同的水印，该算法使用 LZW 无损压缩确保图像的感知特性和诊断特性不变[60]。

Divecha 和 Jani 提出了一种新的安全的医学图像数字水印算法。为了提高图像的安全性，图像被分割成块。相邻像素的相关性较高，相邻像素之间的差作为

一个数据嵌入空间，即差分直方图的全局峰值用于嵌入水印。嵌入过程的多个迭代增加了数据隐藏容量[61]。

Nyeem 等提出了一种医学图像数字水印，利用医学图像 RONI 的 LSB 嵌入水印，避免了对医学图像 RONI 的分割[62]。

Anusudha 等介绍了一种用于医学图像版权保护及认证的混合水印和加密技术，在小波域嵌入水印，利用遗传算法的优点，提出了一种改进的图像复合算法对水印图像进行加密[63]。

Garcia-Hernandez 等提出了两种水印算法，即扩展的基于离散余弦变换(discrete cosine transform，DCT)和大容量数据隐藏水印算法。嵌入水印后的图像可以保证适合计算机辅助诊断系统，其主要结果是病灶分割和分类[64]。

Cedillo-Hernandez 等提出了一种强鲁棒性的水印算法，同时保持高质量的水印图像，生成的水印嵌入原始医学图像的离散傅里叶变换(discrete Fourier transform，DFT)的中间频率。在检测过程中，水印使用比特正确率进行检测[65]。

Mohananthini 和 Yamuna 提出了一种基于离散小波变换与奇异值分解的医学图像数字多水印算法。该水印算法将三个水印嵌入不同的颜色图像中，如第一水印是患者识别，第二水印是患者的诊断信息，第三水印是医生签名图像[66]。

Parah 等提出了两种不同的基于变换域的医学图像水印算法，采用基于 8×8 块的离散余弦变换。该算法不仅能抵抗单独攻击，也能抵抗混合攻击[33]。

在国内，与医学图像有关的数字水印研究也取得了一些进展，学者也发表了不少文章[67,68]。其中，Wu 等提出了一种基于分块的医学图像数字水印方法，实现了信息隐藏和图像认证。该方法把图像分为 256×256 像素，只能识别出篡改的块，不能确定篡改的确切位置。水印图像的平均 PSNR 值是 48.2dB[69]。

Piao 等提出了基于整数小波变换的脆弱水印算法。最高有效位和图像信息作为水印，转换成一个哈希值，嵌入图像整数小波变换 LL 子带的 $M\times M$ 块的 LSB 上。对于医学图像，这种算法也取得了很高的 PSNR 值[70]。

Huang 等根据差分块直方图的基本原理对医学图像的高容量可逆水印进行了详细的研究，该算法将有利于医学图像认证和医生与患者的信息保密。该算法运算复杂度低，嵌入容量小，对辅助信息的需求量小，具有较高的安全性和实用性[71]。

Chao 等对医学图像进行离散余弦变换，把与电子病历有关的数据作为水印信息嵌入量化的离散余弦变换系数上[26]。

高琳把数字水印应用到医学图像版权保护上，提出了两种水印算法。一种是可逆水印算法，该算法基于整数变换和能量选择。另一种是大容量频域水印算法，该算法基于冗余小波变换和子采样方法[72]。

Wu 等提出了一种基于离散余弦变换和扩频通信的医学体数据水印，该水印能抵抗几何攻击，需要利用原始医学体数据提取水印，是非盲水印[27]。

陈凌剑利用整数小波变换对医学图像进行变换，把水印嵌入每个矩形的高频系数上，这是脆弱水印，能检测篡改位置，但是嵌入的水印影响医学图像的质量[73]。

Sun 和 Bo 把主成分分析和离散小波变换结合起来，提出了一种盲水印算法并应用到彩色医学图像中。利用小波变换对图像的主成分进行变换，在小波变换的低频子带上嵌入水印，该水印不需要原始医学图像，具有不可见性和较差的抗攻击能力[74]。

Sun 等提出的水印算法利用独立主成分分析对牙齿的医学图像进行特征提取，在医学图像中嵌入患者信息的 ASCII 码[75]。

刘岩和张春田利用小波变换对医学图像进行变换和选择，把水印嵌入医学图像 ROI 的小波系数上，可以增强水印的鲁棒性，但是降低了水印的容量[76]。

Gao 等提出了一种使用冗余离散小波变换(redundant discrete wavelet transform，RDWT)和子样本的医学图像可逆水印。为了满足感知质量的高要求，该算法通过修改 RDWT 系数嵌入水印[68]。

对于三维医学体数据，刘旺等在三维离散余弦变换的基础上，提出了一种医学体数据水印的算法，该算法利用三维离散余弦变换嵌入水印，具有抵抗加噪、滤波攻击的能力，但其抵抗旋转攻击的能力较差[77]。

Li 等提出了一种基于离散余弦变换的零水印算法。该算法避免了寻找医学图像 ROI 的复杂过程，并结合了图像的视觉特征向量与加密技术。该水印算法具有较强的鲁棒性和不可见性，能抵抗旋转、缩放、平移、裁剪等攻击，是盲水印提取。此外，与现有的医学图像数字水印技术相比，它可以嵌入更多的数据，具有更低的复杂度，在临床应用上更具有实用性[78]。

Han 和 Li 提出了一种新的医学体数据鲁棒水印算法，该算法把三维离散小波变换、三维傅里叶变换和 Hermite 混沌神经网络结合起来，采用 Hermite 混沌神经网络置乱，具有很高的安全性和鲁棒性[79]。

隋淼提出了新的医学图像水印算法，该算法采用 Arnold 置乱增加了安全性，在变换域上提取鲁棒特征向量，不仅能应用于二维医学图像，也能应用到三维医学体数据中[29]。

刘瑶利提出了基于 Logistic Map 置乱的水印算法用于三维医学体数据。该算法采用 Logistic Map 置乱增加了安全性，在变换域上提取鲁棒特征向量，具有良好的鲁棒性，能抵抗各种攻击[80]。

Lu 等提出了一种医学图像的多水印算法。该水印算法能有效地把图像特征信息嵌入原来的图像中，与此同时，把私有标签的信息也一并嵌入原来图像作为水印图像。水印嵌入 ROI 小波变换的低频带[81]。

Han 和 Li 提出了一种基于 Legendre 混沌神经网络和感知哈希的医学体数据零水印算法。该算法在三维离散余弦变换域上，利用感知哈希构造零水印，使用 Legendre 混沌神经网络对水印图像进行置乱[82]。

Han 等将三维离散傅里叶变换应用到医学体数据数字水印中。该算法首先对医学体数据进行三维离散傅里叶变换，选择低频系数进行三维离散傅里叶逆变换，然后利用差异哈希构造零水印[83]。

1.3 医学数字水印概况

1.3.1 数字水印基本概念

1) 定义

作为隐藏技术研究的一个方向，数字水印通常被用来隐藏数字多媒体中的专有信息，如数字图像、数字音乐或数字视频[84-86]。它把具有特定含义的标志信息——水印嵌入数字图像、数字音乐或数字视频等数字载体中，并且原载体的使用不能被影响，这些具有特定含义的标志信息——水印可以通过相应的算法检测和提取，能起到保护作者版权的作用，并且可以当作鉴定或侵权的证据，因此成为数字多媒体保护和防伪的有效工具。如果能够达到特定的要求，数字水印可以更有效。然而，一个成功的数字水印方案需要满足不同的应用。毫无疑问，目前作为多学科交叉技术的数字水印是信息安全技术领域的一个研究热点[38]。

从基本原理来说，数字水印主要包括：水印的选择、水印的嵌入、水印的提取和水印的检测四个步骤。

(1) 水印的选择。水印是根据具体的应用类型来选择的。原始数据和原始数据之间不应该有任何差异。相同的所有者可以有不同的水印。例如，一个公司有不同种类的产品，每一个产品都有独一无二的水印。

(2) 水印的嵌入。水印的嵌入过程如图 1-2 所示，图中原始图像被嵌入水印。而密钥、原始图像和水印信息作为输入，嵌入过程中生成的水印图像作为输出。

水印嵌入后要求原始图像和水印图像之间的区别不能被人眼分辨出来。水印的嵌入不能对原始图像的质量产生影响。但是对于可见水印，嵌入的水印是在原