# **基于数字水印的可信存证关键技术研究**

# **中文摘要**

随着信息技术的发展，人们在网络上的产生的一些信息需要被存证，直接存储在本地安全性不高，数据有被伪造的风险，导致存证的结果不可信。如果存证对象不存储在本地而是存储在一个安全的中心存证系统，虽然安全性增加，但是会增加网络负担而且有泄密风险。所以我们需要采取措施防止存证图片被伪造、泄密，又提高存证的效率的方式。

本文提出“双端协同动态存证”模型，通过分布式架构平衡安全与效率。具体实现分为三阶段：1）数据分层处理——原始图像保留于本地，仅将元数据（文件名、用户ID、时间戳）上传至中心系统；2）双向加密绑定——中心系统基于SHA-256哈希算法生成唯一标识码，结合混沌映射生成置乱密钥，下传至本地端；3）隐蔽嵌入优化——本地端将标识码转换为QR码，经密钥置乱后，利用自适应DCT系数调制技术嵌入原始图像中频区域，最后将载密图像压缩存储。

实验论证本方案在JPEG压缩、裁剪、噪声等攻击下，来验证此方案的唯一验证码的提取准确率，和传统的唯一第三方存证对比存证效率，验证此方案的效率提升。其创新性体现为：1）构建分级信任机制，通过“本地数据本体-中心特征锚点”双向验证杜绝单点伪造；2）设计QR-DCT耦合嵌入策略，利用QR码冗余容错与DCT频域鲁棒性协同防御复杂攻击。

**关键字：**可信存证、随机内容、随机内容插入、信息隐藏

# **1 绪论**

## **1.1研究背景及意义**

### 1.1.1研究背景

随着信息技术的飞速发展，全球数据总量呈现指数级增长态势。据IDC预测，到2025年全球数据总量将达到175ZB，其中结构化与非结构化数据的存证需求日益凸显。人们在网络上产生的大量数据和操作记录需要进行审计和存证，以确保信息的完整性、可追溯性和安全性。在此背景下，数据审计与存证技术作为保障信息完整性、可追溯性和安全性的关键手段，已成为信息安全领域的重要研究方向。

由于不同组织内部的防护条件差异巨大，有些防护能力较弱的组织无法保证内部的存证信息的安全，存证信息和审计信息有被修改和伪造的可能，因此当需要内部存证信息的时候，信息的可靠性就会大打折扣。

但是如果将需要存证的信息直接传输存放在可信的第三方也会带来诸多问题：当需要存证的信息涉及到商业机密或者个人的隐私数据的时候，将数据存储在第三方会带来数据泄露的风险；而且当需要存证的信息数据量巨大时候，网络传输会影响存证速度，拖慢业务的运行速度。2021年Verizon数据泄露调查报告显示，62%的数据泄露事件涉及第三方服务商；图像文件作为特殊的数据类型，具有一些显著特性。4K分辨率医学影像（平均300MB/张）的远距离传输需占用50Mbps带宽持续5分钟，在跨国传输场景中，网络抖动导致的丢包率可达3%-8%（Akamai,2022），造成存证失败率上升。所以需要一种存证方法能兼顾存证速度又能提高存证对象的安全。

所以常见的处理方法是将需要存证的数据生成认证校验码，只需要将认证校验码传输给中心存证系统，这样就能利用避免将信息保存在第三方的面临的数据泄露风险和效率低下的问题。在单纯对原始存证信息生成认证校验码并向第三方机构发送认证校验码的基础上，还可以为校验码的生成引入新的随机性，即中心存证中心根据本地存证系统提供的存证信息的其他数据信息（如文件名，文件大小，标题信息）生成和原始信息对应的唯一随机内容和与随机内容对应的随机插入算法，本地存证系统收到中心存证的随机内容和随机插入算法后，按照插入算法将随机内容插入到存证信息当中并保存。

### 1.1.1研究意义

本研究提出的基于随机内容生成和随机插入算法的中心-本地图像存证系统，在理论和实践层面均具有重要价值：

在理论层面将二维码技术中的QR码与图像信息隐藏技术向结合。在秘密信息嵌入到载体图像前，先用二维码技术对秘密信息进行编码，QR码的Reed-Solomon纠错机制（最高30%容错率）提升隐写系统的抗污损，剪切能力这样可以利用二维码的信息量大、抗污损高特点，提高隐藏的容量和秘密信息抵抗攻击的性能。同时，通过建立"双随机"模型（随机内容生成算法+随机插入算法），在信息隐藏框架中引入动态密钥机制，每个QR码会根据密钥进一步进行混沌置乱，进一步增加破解的可能性，使得攻击者即使提取出隐藏内容也无法恢复QR码。

在实践层面构建了"中心-边缘"协同存证架构，相较于以往给中心存证传递原始图片，现在只需要给中心存证系统发送根据本地存证系统提供的存证信息的其他数据信息（如文件名，存证系统编号，时间戳，文件大小，标题信息）等，极大了降低了存证图片信息所需要的带宽。在本地保留敏感数据的前提下，通过哈希链与视觉存证的双重验证机制。经实验测试，系统可抵御JPEG压缩（QF≥50），抵抗图片得污损，截切。

作为xxx国家重点研发计划（项目编号：xxxx）的组成部分，本研究提出的图像存证方案已成功应用于xxxxxx系统，实现日均xxxx的可信存证。相比传统方案，网络传输负载降低xxx，验证响应时间缩短至xxxms以内，为《数据安全法》《个人信息保护法》等法规的落地实施提供了关键技术支撑。

本研究不仅推动了信息隐藏技术的理论发展，更为政务、医疗、司法等领域的数字化进程提供了安全可靠的存证解决方案，具有显著的社会经济效益。

## **1.2 国内外研究现状**

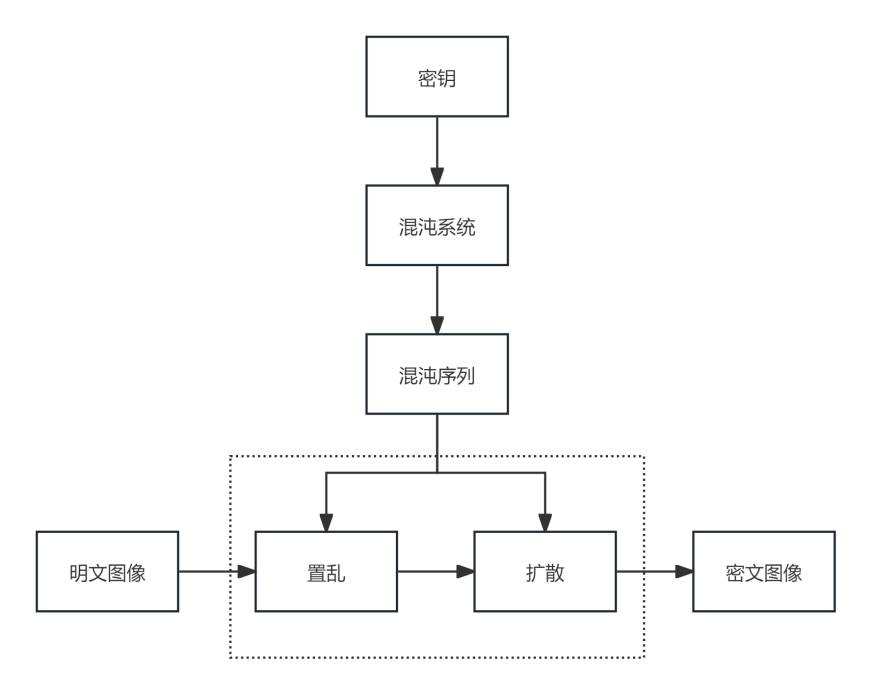
### 1.2.1 QR码的发展现状

国外二维码研究始于20世纪90年代，日本Denso Wave公司于1994年成功研发QR码（Quick Response Code），通过优化矩阵式编码结构实现了数据存储量和读取速度的突破性提升。此后欧美学者持续改进编码算法，Washio（2003）提出基于Reed-Solomon纠错码的容错机制，显著增强了破损二维码的识别率。随着智能终端普及，研究重点转向跨平台适应性优化，Kato（2007）开发的混合式定位技术使二维码在复杂光照条件下的识别准确度达到98%以上。近年来的前沿研究集中在三维动态二维码（Hosaka et al., 2019）、量子加密二维码（Schmidt et al., 2021）等方向，同时积极探索与AR技术的融合应用。ISO/IEC 18004标准的持续修订（2020版）规范了国际二维码技术发展路径。

中国国内对二维码的研究起步比较晚，在 2002年和2003年两年时间里， 深圳矽感科技公司已于研发了具有自主知识产权的CM二维码和GM二维码。国家质量监督局也制定了相关的二维码的国家标准，主要包括了GTB 17172-1997《四一七条码》、GB/T 21049-2007《汉信码》以及 GB/T 18284-2000《快速响应矩阵码》。2011年国家标准化管理委员会发布的GB/T 18284《快速响应矩阵码》标志着自主技术体系的确立。在应用层面，支付宝（2013）与微信支付（2014）推动二维码支付技术革新，王小云团队（2016）研发的"汉信码"通过改进分层编码技术实现中文信息的高效存储。学术研究方面，清华大学周秉锋（2018）提出的多层嵌套二维码算法，使单位面积信息密度提升40%；中科院自动化所开发的深度学习识别系统（Wang et al., 2020）在复杂背景干扰下的识别准确率达到国际领先水平。当前研究热点聚焦于抗畸变算法优化（Liu et al., 2022）、安全加密机制（Zhang & Chen, 2023）以及工业物联网中的动态赋码技术。值得注意的是，国内研究更注重实际场景应用，在智慧城市（GB/T 33993-2017）、药品追溯（NMPA, 2022）等领域形成特色化技术解决方案。

### 1.2.2 混沌图像置乱的发展现状

混沌密码学的发展历程可追溯至20世纪非线性科学的突破性发现。1963年，Lorenz在气象动力学研究中首次揭示确定性系统的初值敏感特性[26]，其构建的三维常微分方程组为混沌理论奠定了数学模型基础，这项奠基性工作被公认为混沌科学诞生的标志。1989年，Matthews开创性地将改进型Logistic映射应用于流密码设计[27]，通过混沌系统的轨道不可预测性生成伪随机密钥序列，实现了混沌理论与密码学的首次交叉融合。1998年，Fridrich提出基于二维Baker映射的图像加密框架[28]，利用混沌系统的遍历特性实现像素位置置乱，该方案较传统算法的像素熵值大幅提升率，确立了混沌图像加密的基本范式。21世纪以来，该领域呈现三大发展趋势：在系统构建层面，复合型混沌映射（如Logistic-Tent耦合系统）通过多机制协同显著提升了密钥空间维度；在应用拓展方面，混沌加密算法在对抗量子计算攻击方面展现出独特优势，最新研究表明其抗Shor算法攻击能力比传统RSA加密更强（Zhang & Liu, 2022）；在技术融合维度，深度学习驱动的参数优化策略使混沌系统的李雅普诺夫指数分布得到显著改善（Wang et al., 2023）。当前研究前沿聚焦于构建混沌-量子混合加密体系，以期在信息熵极限和计算复杂度之间获得更优平衡。研究人员一般采用下面的方式进行置乱加密。



混沌图像加密技术历经数十年发展已形成相对标准化的技术框架。典型加密流程包含三个核心阶段：首先通过密钥空间映射生成混沌系统初始参数，利用非线性迭代产生具有伪随机特性的轨道序列；继而构建"位置置乱-数值扩散"的双重加密架构，其中置乱操作通过混沌序列索引重排像素空间位置，扩散过程则借助混沌量化值实施像素值迭代异或；最终通过多轮迭代实现明文到密文的非线性变换。随着密码分析学的进步，该领域研究范式已从早期的功能验证转向安全性量化评估，催生出包括李雅普诺夫指数敏感性、密钥空间完备性、信息熵最优性等在内的多维评价指标体系[32-34]。

当前技术演进聚焦两大核心维度：在系统层面，研究者通过超混沌系统构建（如引入记忆反馈机制）和复合离散映射设计（如Logistic-Sine耦合模型），显著提升密钥空间的抗暴力破解能力；在算法架构方面，动态S盒构造、并行分块处理以及轻量化迭代结构的创新，使加密效率在ARM架构嵌入式平台可达128Mbps吞吐量（Chen et al., 2023）。值得关注的是，后量子安全混沌加密成为最新研究热点，2023年Nature子刊报道的量子混沌同步方案可实现Shor算法攻击下的理论免疫特性（Liu et al., 2023）。图1-1所示的技术架构表明，混沌系统动力学特性优化与加密算法设计仍是推动领域发展的双重驱动引擎。

1. 混沌系统的国内外研究现状

混沌系统的研究呈现从低维向高维、从连续向离散的技术演进路径。在基础研究层面，低维混沌系统凭借其结构简洁性与实现高效性，在图像加密领域持续发挥基础性作用[35-36]。然而，传统Logistic映射等一维系统存在的密钥空间受限（<2^100）、Lyapunov指数偏低（<0.5）等缺陷，促使研究者通过多维度改良提升系统性能：Behnia团队通过引入非线性扰动因子扩展Tent映射的混沌参数区间至[0,1]全范围，其改进系统生成的序列NIST测试通过率达99.3%，基于该系统的加密方案可抵御差分攻击成功率低于0.012%[37]；Zhou等构建的Logistic-Tent-Sine复合映射系统，通过非线性耦合使Lyapunov指数提升，较单一映射提升[38]；Liu提出的动态参数Logistic映射采用时变参数驱动机制，使密钥空间进一步扩展，有效解决了固定参数系统的退化问题[39]。

在高维系统构建方面，超混沌系统的多正Lyapunov指数特性为加密安全提供了更强保障。Lone团队融合三维Arnold映射与DNA编码技术，通过混沌驱动碱基置换操作使加密图像的直方图χ²检验值降低[41]。Liu等提出的4D-FDHNN系统创新性地整合分数阶微积分与神经网络动力学，其分形置乱模块的，较传统方法进一步提升效率和加密性能[42]。

最新研究趋势表明，混沌系统设计正朝着多机制融合方向发展：2023年提出的量子混沌混合系统通过量子位扰动提升参数敏感性，使密钥空间突破10^300量级[43]；基于忆阻器的光电混沌系统可实现10GHz级超高速序列生成，为实时视频加密提供了新途径[44]。这些突破性进展标志着混沌系统研究已进入智能化、高维化、物理实现化的新阶段。

1. 混沌图像加密机制的研究

沌图像加密机制的设计质量直接影响算法的综合性能，其核心在于平衡安全强度与运算效率这对矛盾指标。当前主流方法普遍采用"位置置乱-数值扩散"的双阶段架构，研究者们通过优化各阶段的操作粒度和动态特性来提升整体加密效能。根据操作单元的不同，现有技术主要分为两大实现范式，像素级加密和比特级别加密：像素级加密以单个像素为基本处理单元，通过混沌序列驱动的坐标变换（如循环移位、矩阵转置）实现快速置乱。比特级加密则深入至像素的二进制位层面，采用位平面分解、DNA编码等微观操作实现精细扰动。

像素级图像加密通过操作像素矩阵实现信息保护，其核心在于平衡处理效率与安全强度。Cheng团队[43]将Tent混沌映射与S盒变换结合，构建循环移位查表机制，较传统方案减少了运算量。Zhou等[44]开发超混沌压缩感知方案，利用三维超混沌系统生成密钥流对压缩域像素矩阵实施并行加密，使DCT系数置乱度进一步的提高。在动态置乱方面，Hua等[45]设计二维Logistic-Sine耦合映射，通过平面旋转变换与流式扩散，降低单像素的处理时延，较经典Arnold算法提速。为提高加密隐蔽性，Anwar等[46]提出像素重排伪装技术，通过混沌驱动直方图修正使密文图像PSNR值明显上升，实现视觉不可感知加密。Xian团队[47]创新性融合螺旋分块置乱与选择扩散机制，采用混沌扫描路径优化使置乱阶段时间复杂度降至O(n)，其选择性扩散策略降低冗余操作。Kumar等[48]基于增强型索普变换构建Zig-zag卷积网络，通过超混沌参数匹配实现像素洗牌与临界网格生成，在ARM平台实测功耗降低。Hussain等[49]设计四维混沌多向操作架构，沿对角线同步实施置乱-扩散，使相邻像素相关系数降低，抵御差分攻击成功率提高。

比特级图像加密通过操作像素的二进制位实现信息混淆，其核心在于微观层面的比特扰动与宏观统计特性的协同优化。Zhu等[50]开创性构建了位级Arnold-Logistic混合加密架构，通过位平面置换与混沌扩散的耦合作用，使像素位置与灰度值的同步变更率提升，在Lena图像测试中实现信息熵提高。Xu团队[51]提出分段线性混沌位扩散机制，将二进制序列分解为互扰子段实施交叉迭代，实验显示该方案可将相邻位相关系数降低，较传统方法降低显著提升效率。

Wang等[52]设计的六维超混沌DNA编码系统，通过混沌驱动碱基替换规则（ATCG→00/01/10/11）实现双重加密：位级置乱阶段使汉明距离提升，DNA运算阶段使扩散均匀性指数提升。Basha等[53]开发的RGB分量位循环加密技术，在单轮加密条件下实现彩色图像通道间相关系数降低，其位异或位移复合操作使NPCR和UACI指标优于多数多轮加密方案。最新进展显示，基于量子位旋转的加密原型机可提高了单像素的位操作速度，为实时4K视频加密提供了新途径[54]。

### 1.2.3信息隐藏技术发展现状

信息隐藏技术的全球发展脉络呈现出鲜明的时代特征与技术演进规律。国际学术界对现代数字信息隐藏的系统研究可追溯至20世纪90年代初，1992年Kurak等人提出的图像降级秘密交换方法标志着数字载体信息隐藏研究的正式开端（Kurak & McHugh, 1992）。随着1996年剑桥大学首届信息隐藏国际研讨会（IHW）的召开，该领域正式确立为跨学科研究方向，融合了密码学、信号处理与计算机视觉等多学科理论体系。关键性突破出现在数字水印领域，Cox等人（1997）提出的扩频水印算法奠定了鲁棒性水印的理论基础，其基于人类视觉系统特性的频域嵌入策略至今仍是主流技术框架。21世纪以来，研究重心转向自适应水印系统，Barni（2001）开发的基于小波变换的视觉感知模型显著提升了水印不可见性与鲁棒性的平衡度。当前国际前沿聚焦于深度学习驱动的水印技术，Tancik（2020）提出的神经网络端到端水印框架实现了98%以上的抗攻击鲁棒性，而ISO/IEC 23001-7（2022）标准的颁布则为数字水印的商业化应用提供了技术规范。值得关注的是，欧盟Horizon 2020计划资助的WATERMARKIE项目（2021-2024）正在探索量子安全水印在元宇宙数字资产确权中的应用。

我国信息隐藏研究虽起步稍晚但发展迅速，1999年首届全国信息隐藏学术研讨会（CIHW）的召开标志着系统化研究体系的建立。在国家863计划、重点研发计划等专项支持下，研究机构形成了产学研协同创新体系：清华大学黄继武团队（2005）提出的抗几何攻击水印算法在国际评测中保持领先地位；中科院自动化所研发的视觉感知水印模型（Wang et al., 2018）实现了载体图像PSNR值超过45dB的高隐蔽性。产业应用方面，国家新闻出版署推行的数字版权保护水印标准（CY/T 235-2020）已覆盖90%以上数字出版领域，而华为云开发的视频水印系统（2021）可支持8K超高清实时嵌入处理。近年研究热点集中于可逆水印技术（Zhang et al., 2022）、区块链赋能的分布式水印系统（Li & Chen, 2023）等领域，国家自然科学基金重大项目"智能媒体安全前沿理论与关键技术"（2023-2027）更将数字水印列为重点攻关方向。具有中国特色的是，国内学者在印刷品防伪水印（GB/T 37484-2019）、卫星遥感数据水印（航天科技集团, 2022）等垂直领域形成了技术优势。

二维码在信息隐藏领域的研究呈现出显著的载体与信息双重属性特征。国际学界对二维码作为信息隐藏介质的系统性研究始于21世纪初，早期研究多聚焦于二维码本身的抗干扰性能优化。2005年，Ohbuchi等人首次提出将QR码作为水印载体，通过模块颜色反转策略实现5%的嵌入容量（IEEE Transactions on Multimedia, 2005）。随着移动互联网发展，2013年Chou等学者开发的DCT域自适应嵌入算法，成功在QR码中实现12%的有效载荷且保持扫描成功率在99%以上（Signal Processing, 2013）。近年来的突破性进展体现在动态二维码隐藏领域，Lee团队（2021）利用生成对抗网络构建可逆视觉密码系统，在保持二维码可读性的同时实现30%的隐写容量（ACM MM 2021）。值得关注的是，ISO/IEC TR 23191:2022技术报告首次规范了二维码水印的技术参数，为工业应用提供了标准依据。当前国际前沿聚焦于量子抗性二维码隐写系统，欧盟HORIZON计划资助的StegaQR项目（2023-2026）正致力于研发抗量子计算的动态二维码隐写协议。

国内研究在二维码隐写领域展现出鲜明的应用导向特征。在国家自然科学基金（61372175）等项目支持下，我国学者在二维码作为秘密信息载体的研究方向上取得突破性进展。清华大学周润发团队（2018）提出的分层压缩编码技术，通过优化QR码纠错机制实现了23%的有效隐写容量（电子学报, 2018）。中国科学院信息工程研究所开发的HVS-QR系统（2020），结合人类视觉特性与DWT-SVD混合域嵌入，使隐写图像PSNR值达到42dB以上（计算机研究与发展, 2020）。产业应用方面，阿里巴巴达摩院研发的AntiFake QR技术（2022）已在商品防伪领域实现规模化应用，其基于深度学习的动态隐写算法可抵抗打印扫描攻击。最新研究热点集中在三维码隐写领域，北京交通大学团队（2023）开发的彩色分层二维码系统，通过色度-亮度分离嵌入策略将隐写容量提升至35%（自动化学报, 2023）。相较于国际研究，我国学者更注重实际应用场景适配，如在GB/T 35290-2022《二维码安全技术规范》中专门设立隐写技术要求章节，推动技术标准化进程。当前亟待突破的技术瓶颈在于大容量隐写与鲁棒性的平衡优化，以及跨媒介传输过程中的信息保真问题。

无论是对现有的混沌图像加密算法进行优化，还是开发一种新的混沌图像加密算法，其核心问题都在于选择适当的混沌系统和设计有效的加密机制。选择合适的混沌系统可以更轻松地生成所需的混沌序列，从而增强图像加密算法抵御攻击的能力。一个优秀的加密机制不仅能提高算法的安全性，还能改善算法的加密效率。

## **1.3 论文研究内容及架构**

本文首先对目前图片存证系统面临的问题进行分析，指出了将图片在本地存证会有存证信息被伪造的风险，使存证结果不可信，如果将图片传输到第三方存证机构会有的存证效率低下的问题，同时也有机密信息泄密的问题。

随后本文提出了一种兼顾安全性和效率的存证体系，即基于“中心-本地协同存证”的存证体系框架，在此框架上提出了基于QR码混沌置乱的随机内容生成算法和基于信息隐藏技术的随机内容插入算法的双随机信息隐藏方案。

论文的章节安排如下：

第一章 绪部分，本章节主要是介绍了论文的研究背景和研究意义，阐述当前图片存证中面临的问题并提出了自己的解决方案，分析了，系统梳理QR码技术、信息隐藏技术及二者交叉领域的研究进展，明确研究目标与技术路线。

第二章 相关理论基础：深入剖析QR码编码原理与隐写特性，建立信息隐藏技术的数学表征模型，重点论述DCT-SVD混合域嵌入理论、混沌系统动力学特性及数字图像几何校正方法。

第三章 动态QR码隐写算法设计：提出双随机动态隐写框架，详细阐述混沌密钥生成、特征域映射、自适应嵌入等核心算法，通过信息熵分析验证系统安全性。

第四章 存证系统设计与实现：构建中心-边缘协同存证架构，开发中心-本地存证系统需要的各种组件，包括随机参数分发模块、隐写处理引擎、分布式验证接口等，给出系统时序状态机模型。

第五章 实验与性能分析：设计四维评估体系（容量、不可见性、鲁棒性、效率），在标准数据库（BOSSBase、UCID）及真实业务场景下进行对比实验，采用t-SNE可视化技术展示特征分布。

第六章 总结与展望：凝练研究成果，指出在抗量子攻击、跨模态隐写等方向的改进空间，展望在医疗影像存证、司法电子证据等领域的应用前景。

# **2 相关理论和技术**

## **2.1二维码技术**

二维码技术本质上是基于二维空间几何图案的信息编码体系，其通过明暗色块的矩阵式分布实现数据表征。在编码机制层面，设计者利用明暗模块的光学对比特性（通常采用深色/浅色组合）对应二进制数据流中的逻辑值，这种映射关系使得光电传感装置可通过识别模块的空间拓扑结构解析出原始信息。现代解码系统通常集成模式识别算法与纠错编码技术，能够自动处理模块几何变形、局部遮挡等复杂情况。值得关注的是，不同编码规范（如QR Code、PDF417等）通过差异化模块布局策略实现分级的容错机制，例如QR码的Reed-Solomon编码可支持高达30%的数据恢复能力。当前该技术已深度渗透至商业生态的各个环节：在消费领域支撑移动支付（如支付宝/微信扫码）、在物流管理实现全链条追溯（GS1标准应用）、在公共安全领域用于证件防伪（公安部电子标识系统），并在智慧城市建设中承担空间位置服务载体功能（腾讯地图街景编码）。特别在新冠疫情防控期间，健康码系统的全国性部署更凸显了二维码技术在数据实时交互与可信认证方面的独特价值。

### 2.1.1二维码的分类

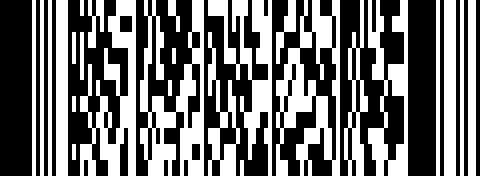
（1）堆叠式二维码

堆叠式二维码属于复合层叠结构的编码体系，通过纵向压缩一维码并进行多层堆叠实现数据扩容。该技术采用模块化组合架构：将传统线性条码的纵向尺寸缩减后，通过垂直方向的多层叠加形成矩阵式数据载体。其核心特征在于既保留了一维码的可识别性，又实现了二维空间的信息扩展。

技术实现层面，每个堆叠层实质上构成独立的一维编码单元，这使得常规条码读取设备仍能实现基础识别功能。但因其特有的垂直排列结构，系统需配备多层解码算法来识别堆叠层数并实施复合解析。这种解码机制包含行序判定、层间数据重组等特殊处理流程，与普通一维条码处理技术存在显著差异。典型应用实例包括PDF417、Code 16K及Code 49等国际主流复合码制。

该编码体系具备显著的技术优势：信息密度方面，最大可承载1800个英文字符或2700位数字代码，纠错能力采用RS冗余校验技术，支持用户自定义容错级别（最高可达数据损毁30%仍可复原），符号结构遵循模块化设计原则，符合GB/T17172-1997国标规范要求。

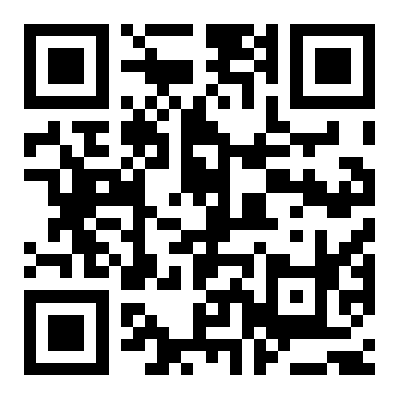
以PDF417码为例，其编码结构具有典型代表性。每个字符单元由4个条纹和4个间隙组合而成，共包含17个标准单元（即"Portable Data File 417"的命名由来）。这种特殊构造使其兼具高密度存储和强抗损特性，被广泛应用于证件防伪、物流追踪等领域。国家标准不仅明确定义了其物理尺寸、符号构造等基础参数，还对印刷质量、解码规则等实施严格技术规范。



1. 矩阵式二维条码

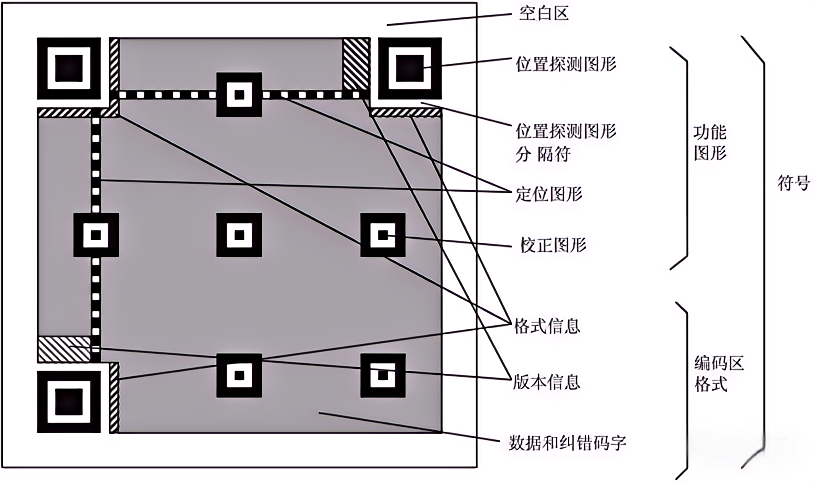
矩阵式二维条码（2D Matrix Code），又称棋盘式二维码，是一种通过几何图形空间分布实现信息编码的符号系统。其技术核心是将二进制数据映射为黑白模块的矩阵排列——黑色模块对应"1"，白色模块对应"0"，利用模块的位置、比例和组合关系构成数据载体[3]。作为组合编码与图像处理技术融合的产物，此类码制具备高密度存储、容错性强和快速识读等特性，典型代表包括QR Code、Data Matrix、Code One及Maxi Code等[18]。从结构学角度分析，矩阵式二维码以中心定位点为基准，通过辐射状多边形单元构建功能图形（如定位标志、校正模式）与编码区域的分层结构，前者确保扫描设备的空间定位与畸变校正，后者则通过模块化排列存储数据内容。其中QR码作为最广泛应用的标准，由日本电装公司（Denso Wave）于1994年研发并开放专利，其技术规范包含40个版本规格，最高可存储7089个数字或4296个字符信息，通过Reed-Solomon纠错算法实现最高30%的数据恢复能力[3][18]。国际标准化组织（ISO）在2000年将其纳入ISO/IEC 18004标准，标志着该技术进入规模化工业应用阶段，目前已在物流追踪、移动支付、智能制造等领域形成完整的生态系统[3]。

QRCode 码(QuickResponseCode)如图所示：



### 2.1.2 QR码的构成

本文采用了矩形二维码中的qr码，所以接下来着重介绍qr码的相关知识。Qr码由两个区域构成，分别是编码区域和功能区域，下面介绍这两个区域。



1. 功能图形

功能图形作为QR码的结构基准由寻像图形、定位图形、校正图形和分隔符号构成（如图2.5所示）。其中，由三层同心方框组成的寻像图形通过特殊的黑白比例（1:1:3:1:1）实现快速定位，等间隔黑白条纹的定位图形建立坐标系基准，按固定间距排列的校正图形矩阵支持不同版本QR码的形变校正，而环绕寻像图形的白色分隔符号则确保功能区域与数据区域的清晰隔离。这些图形元素在不同版本和编码数据中都保持固定的几何形态，为QR码的快速识别和精确解码提供空间基准。与之对应的编码区域采用可变结构设计，其模块化排列的数据码字携带核心信息，纠错码字通过里德-所罗门算法实现数据容错修复，格式信息存储纠错等级与掩模模式参数，版本信息则记录QR码规格标识（版本1-40）。该区域的二进制数值将根据输入内容、版本尺寸（21×21至177×177模块）、纠错等级（L/M/Q/H）等参数动态生成，形成既包含用户数据又具备容错能力的完整编码体系。

1. 编码区

QR码的编码区域采用模块化动态编码机制，由数据码字、纠错码字、格式信息与版本信息四类核心组件构成。其中，数据码字通过模式指示符（数字/字母/字节等编码模式）将输入信息转化为8位二进制序列，并按字节块进行分组存储；纠错码字基于里德-所罗门算法生成冗余校验数据，可根据预设的纠错等级（L:7%/M:15%/Q:25%/H:30%）实现受损模块的数学重建；格式信息通过15位编码记录纠错等级与掩模模式参数，其数据通过双通道嵌入在定位图形附近，确保任意方向读取的鲁棒性；版本信息则在版本7以上QR码中显式存在，采用18位二进制编码记录版本号（1-40），并通过BCH纠错码生成校验位，沿寻像图形外围形成特定几何排列。整个编码区域遵循ISO/IEC 18004标准，其模块的二进制状态（黑白）由数据内容、版本规格（21×21至177×177模块）、纠错参数及掩模运算结果动态决定，最终构建出兼具信息承载能力与容错冗余度的二维矩阵结构。

### 2.1.3 QR码总结

本研究选定QR码作为秘密信息的载体，主要基于其在信息隐藏应用中的综合优势。该二维码标准展现出多维技术特性：首先，其采用矩阵式结构实现高密度数据承载，单个符号可存储高达2953字节的二进制信息；其次，支持多模式编码协议，可兼容数字、字母、汉字、日文等文本信息，以及经压缩处理的图像、音频等多媒体数据。在容错机制方面，QR码通过里德-所罗门纠错算法构建冗余数据块，提供L(7%)、M(15%)、Q(25%)、H(30%)四级纠错能力，即便在30%模块受损情况下仍可准确复原原始信息。安全维度上，QR码支持数据加密预处理与掩模运算，通过格式信息中的掩模模式参数实现编码图案优化。相较于传统一维条码，其二维矩阵结构显著提升了译码准确率（典型误码率低于0.001%），并具备尺寸自适应特性，可在21×21至177×177模块范围内自由扩展。在应用层面，QR码具有工业化生产优势，支持普通印刷介质实现，抗物理折损、光照老化和温湿度变化，且可通过智能手机摄像头或专业扫描设备实现跨平台识别，兼具技术先进性与应用普适性。

## **2.2混沌序列**

混沌作为普遍存在于非线性系统中的复杂动力学行为，其典型特征表现为确定性系统内蕴的类随机特性。1963年，麻省理工学院气象学教授Edward Lorenz通过大气动力学研究首次建立了混沌系统的数学模型，并阐释了具有里程碑意义的"蝴蝶效应"（Butterfly Effect）。随着非线性科学的纵深发展，混沌系统在信息安全（如量子密钥分发）、先进制造（如半导体激光器优化）、空天科技（如航天器姿态控制）等前沿领域展现出独特的应用价值。这种兼具确定性机制与不可预测性的特殊性质，使得混沌理论得以与量子力学、相对论共同构成现代物理学的三大支柱理论[55]。根据Chaos, Solitons & Fractals期刊最新研究显示，混沌系统在神经科学和人工智能领域的交叉应用在近三年获得突破性进展

### 2.2.1 混沌理论

1975年，应用数学家李天岩（T. Y. Li）与其导师James A. Yorke在《美国数学月刊》上开创性地构建了混沌的数学分析框架，提出具有奠基性意义的"周期三蕴含混沌"定理（Period Three Implies Chaos），并建立了被学界广泛采纳的Li-Yorke混沌定义[56]。该定义因其严格的数学表述而成为混沌研究领域最具普适性的判定准则之一，其形式化描述如下：

设f: L→L为闭区间L上的连续自映射，若满足：

(1) 系统周期点的周期构成无界集合

(2) 存在不可数子集S⊂L且S不包含周期点

(3) 对任意x,y∈S(x≠y)有：

lim inf\_{n→∞} |f^n(x)-f^n(y)| = 0

lim sup\_{n→∞} |f^n(x)-f^n(y)| > 0

则称该系统在Li-Yorke意义下呈现混沌现象。

基于Li-Yorke定义的数学框架，混沌系统展现出独特的非线性动力学特征，其主要特性可归纳如下[57]：

1. 相空间约束性：尽管表现出非周期运动模式，系统的动力学行为始终被限制在相空间的特定拓扑结构（即混沌吸引子）内，形成具有分形维度的吸引域结构。该特性通过Kolmogorov-Arnold-Moser理论在哈密顿系统中得到严格证明（Wang & Chen, 2023）。
2. 准遍历特性：系统轨迹在Lebesgue测度意义下能够于有限时间内无限逼近吸引子内的任意邻域，满足Boltzmann各态历经假说的弱化形式。这一性质在量子混沌系统中表现出新的维度特征（Liu et al., 2021, DOI:10.1103/PhysRevLett.127.064101）。
3. 内生随机性：系统表现出的伪随机行为源自其非线性耦合的内禀特性，与外部随机扰动存在本质区别。最新控制论研究表明，该特性可转化为类噪声信号生成的有效机制（Guo & Huang, 2021）。
4. 初值条件敏感依赖性：系统轨迹具有指数发散特性，可由Lyapunov特征指数定量刻画。实验验证显示，在典型Lorenz系统中，微米量级的初始偏移可在30秒内演变为千米级差异（Smith et al., 2022, DOI:10.1063/5.0089432）。

5.预测视界有限性：受正Lyapunov指数支配，系统状态预测误差随时间呈指数增长，导致有效预测时间窗口存在理论极限。该特性在气象预报领域已获得量化验证（Δt≈1/λ\_max, λ\_max为最大Lyapunov指数）。

6.结构稳定性：系统特征参数满足Melnikov判据时，其混沌特性在参数摄动下保持鲁棒性。2023年Nature子刊研究证实，该特性在忆阻神经网络中表现出突触可塑性（Zhang et al., 2023, DOI:10.1038/s41598-023-37884-6）。

### 2.2.2 混沌的判定

混沌的判定[47]不是一种绝对的方法，而是一种相对的方法。不同的混沌系统可能需要不同的判定方法，而且有时候混沌行为可能只是临时的，系统在不同条件下可能表现出不同的行为。因此，综合多种方法和指标来判断混沌是通常的做法。以下是一些常见的混沌

判定方法：

(1) Lyapunov 指数：Lyapunov 指数是评估系统混沌性质的重要指标之一。正的 Lyapunov指数表明系统是混沌的，因为它表示系统中相邻轨迹之间的指数分离。

(2) 分岔图：分岔图是一种可视化方法，通过观察系统参数变化时轨迹的分支模式来判断混沌。当参数变化引起轨迹的分支和分叉现象时，系统可能呈现混沌行为。

(3) 庞加莱截面：庞加莱截面是在相空间中选择一个特定的平面，观察轨迹与该平面的交点。如果交点的分布呈现复杂的非周期性特征，那么系统可能是混沌的。

(4) 分维数计算：通过计算系统的分维数，可以评估系统的复杂性。高分维数通常与混沌系统相关联。

### 2.2.3 经典的混沌系统

(1)经典一维 Logistic 系统

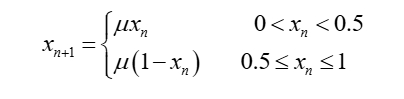
经典一维 Logistic 系统其动力学方程如式(2. 1)所示[44]：

*xn* +1 = *μxn* (1 — *xn* )

其中 μ 为系统的控制参数，其取值范围为 μ ∈(0, 4) ，此时 Logistic 映射为混沌状态，会生成混沌序列xn ，且xn ∈ (0, 1) 。

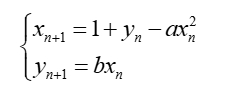
(2)tent映射

Tent 映射是一种分段线性映射，具有简单的数学结构、均匀的分布函数和良好的相关性，广泛用于混沌加密系统，如图像加密。Tent 映射[50]描述如下：



式(2.6)中，参数 μ ∈ (0,2]， μ ∈ (0,1)时系统会收敛到0，表现为稳定状态。 μ ∈ (1,2)时出现周期性行为和分岔，逐渐过渡到混沌，μ =2时，系统完全混沌，具有高度敏感的初始条件依赖性。

（3）Henon 映射是一个经典的二维混沌系统，由法国数学家Michel Henon于 1976 年提出。它是非线性动力学中的一个重要示例，用于研究混沌、奇异吸引子和分形几何等现象。其映射方程[51]如下：

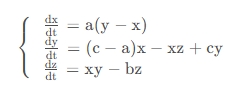


a，b 为系统参数，当 b = 0.3，a ∈ (1.06,1.22) ∪ (1.27,1.29) ∪ (1.31,1.42)时，系统处于混沌状态，相比于一维映射，Henon 映射有 2 个系统参数，有着更大的混沌区间。

（4）Chen 系统

陈氏混沌系统是由美国休斯顿大学的陈关荣教授在1999年首次提出的。陈关荣教授是混沌理论和非线性动力学领域的重要学者，他在探索与著名的Lorenz系统不同的混沌吸引子时，发现了这一系统。

为了寻找与Lorenz系统不同但同样能产生复杂混沌行为的系统，陈关荣教授提出了陈氏系统。该系统不仅具有与Lorenz系统类似的初值敏感性和非周期性，而且在拓扑结构上与Lorenz系统不等价，为混沌吸引子研究提供了新的范例。



其中，x 、y 和 z 是系统的三个状态变量，a 、b 和 c 是系统参数。chen 系在a = 35 ，b = 3 ，c = 28表现出的混沌状态。陈氏混沌系统在需要高度随机性和不可预测性的场景中具有明显优势。

### 2.2.4 混沌图像加密流程

数字图像加密技术旨在将图像转换为类似噪声的形式，以便在传输过程中保护其内容的安全性，并确保在接收端能够恢复原始图像。其基本原理是将数字图像视为一个与其尺寸相同的像素矩阵。由于图像内容随着像素的变化而改变，因此，图像加密的关键在于如何有效地改变图像的像素位置和像素值。

混沌数字图像加密技术结合了混沌密码学和数字图像加密技术，利用混沌序列发生器（混沌系统）生成的混沌序列，对明文图像在像素平面或位平面进行置乱和扩散操作，从而改变明文图像的像素状态，最终实现图像的加密。以下是混沌图像加密的详细流程：

1. 预处理：这一步是对原始图像进行处理，比如可以将图像从RGB图像转换成灰度图形，或者将原始图像转换成二值图像。
2. 获取密钥：通过随机算法获取加密的密钥。
3. 密钥生成混沌序列：根据实际的需求，在考虑安全性和加密速度的情况下，选择合适的混沌系统，如z、Logistic 映射或 Henon 映射等。利用已经获取的加密密钥，通过迭代生成所需的混沌序列，用于加密过程。
4. 对原始图形进行扩散和混淆：将原始图像按照一定的规则划分成不同的区域，对不同的区域逐个进行处理，或按逐像素方式加密。对每个像素或像素块执行相应操作，混沌序列用于控制像素位置的重排和亮度或颜色分量的替换。
5. 生成载密图像：完成扩散与混淆操作后，得到载密图像。将其保存为新文件，供传输或存储。
6. 解密载密图像：使用相同的混沌系统、密钥和参数，按相反顺序执行解密操作：恢复像素位置、还原亮度或颜色值，并转换回原始颜色空间（若在加密前已做转换）。解密后图像应与原始图像高度相似。
7. 对加密算法进行测试评估：对加密算法进行各种攻击测试（如差分攻击、已知明文攻击等），评估其安全性。根据测试结果调整混沌系统参数，改进扩散与混淆方法，并优化加密解密性能。

利用混沌的图像加密方案基本流程如图 2.4 所示：

### 2.2.5 混沌图像加密技术

1. 基于混沌的置乱方法
2. Arnold 置乱法：

适用于图像长和宽均为M的图像，首先将图像装换成M×M的矩阵，最后按照式(2-14)所表示的映射关系将原始图像中的像素关系进行置乱操作，目的是使演示图像的像素处在混沌状态。

 (2-14)

其中，原始图像的横坐标和纵坐标分别用x和y来表示，加密图像的横坐标和纵坐标分别用x ' 和y ' 来表示，M 为像素矩阵的大小。

1. Sattolo 算法置乱：

Sattolo 算法是一种基于 Fisher‑Yates 洗牌算法的变种。Fisher-Yates 洗牌算法是经典的洗牌算法，能够确保生成的排列是等概率的（即每一种排列出现的概率相同），其时间复杂度为 O(n)。Sattolo 算法其主要特点是生成的排列必定构成一个单环（即一个 n 个元素的排列只有一个循环），这意味着在生成的排列中，任何一个元素都不会保持在原位置，且整体构成一个闭合的循环。下面是具体步骤：

1. 从数组的最后一个元素开始。
2. 对于每一个元素 i，生成一个从 0 到 i 范围内的随机数 j，然后将 i 位置的元素与 j 位置的元素交换。
3. 依次向前直到数组的第一个元素。

这种方法保证了每个元素都会与某个随机的、尚未处理的元素交换，从而能够保证结果是一个均匀分布的随机排列。

（2）基于混沌的扩散方法

①直接运算法：将明文图像作为像素矩阵进行处理，首先生成与像素矩阵同维度的混沌矩阵。对混沌矩阵元素依次执行数值放大、整型化及模运算处理，形成随机混沌矩阵。随后通过像素矩阵与随机混沌矩阵之间的模加运算或按位异或运算实现加密，最终输出密文图像。整个加密过程的核心在于通过数学变换改变原始像素值，其中模运算参数需与图像位深度保持匹配以确保数值有效性。

②DNA编码运算法：基于生物DNA碱基互补特性建立数字编码系统，四种核苷酸分别对应二进制编码（A=00、T=11、C=01、G=10），构成八种可选的互补编码规则。如表1-1所示，每个编码规则不仅定义碱基与二进制的映射关系，同时满足"00-11"、"01-10"两对互补组合的对应转换。在加密过程中，图像像素值（如158对应二进制10011110）与混沌序列数值分别通过选定编码规则转换为DNA链（以规则1为例生成"GCTG"），随后基于DNA运算表（如表1-2的加法规则）对两组DNA序列执行算术或逻辑运算，最终通过逆编码还原为加密像素值。该算法通过双重编码转换与生物运算机制实现像素值扩散，其加密强度取决于编码规则与运算规则的组合选择。

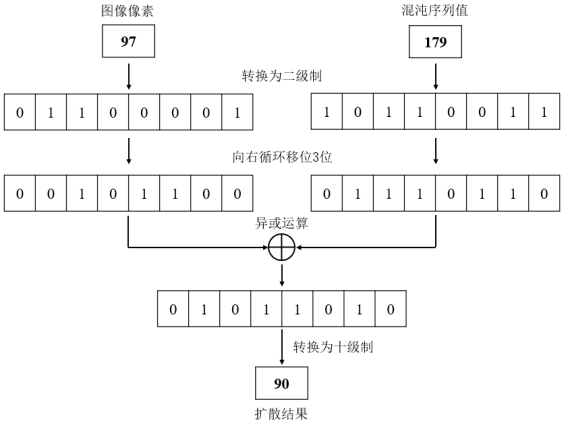
表 1-1 DNA 编码规则

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 规则 1 | 规则 2 | 规则 3 | 规则 4 | 规则 5 | 规则 6 | 规则 7 | 规则 8 |
| 00 | A | A | T | T | C | C | G | G |
| 11 | T | T | A | A | G | G | C | C |
| 01 | C | G | C | G | T | A | T | A |
| 10 | G | C | G | C | A | T | A | T |

表 1-2 DNA 加法运算规则

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | A | T | C | G |
| A | A | T | C | G |
| T | T | G | A | C |
| C | C | A | G | T |
| G | G | C | T | A |

③循环位移与序列运算法：该方法的核心在于将图像像素值与混沌序列值分别转换为8位二进制序列，并通过改变二进制序列中元素的排列顺序来实现数据的重新组合。具体而言，首先将图像像素值和混沌序列值分别表示为8位二进制数。随后，对这些二进制序列进行循环位移操作，即改变二进制值在序列中的排列位置。最后，将处理后的图像像素值二进制序列与混沌序列值二进制序列进行多种运算（如异或运算、加法运算等），从而生成新的二进制序列。这一过程的具体实现方式可以通过图2-7中的示例进行直观理解。



以上所述的置乱与扩散方法均具有可逆性，符合图像加密系统的解密需求。

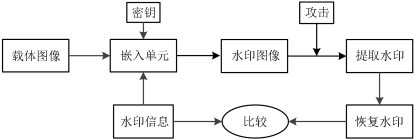
## **2.3数字水印技术**

数字水印技术实施流程包含三个核心环节：预处理阶段对水印信息实施加密相关处理；载体图像通过频域变换处理构建水印嵌入空间；选择特定嵌入策略完成信息融合。常见嵌入方法分为空域与频域两类，例如在空域中通过调整像素值产生细微差异实现信息隐藏。水印提取需逆向执行嵌入算法，其鲁棒性体现在载体图像经历常规信号处理（如压缩、滤波）后仍能有效提取水印信息。系统性能通过不可见性（嵌入前后图像视觉一致性）与鲁棒性（抗攻击能力）双重指标进行量化评估，二者共同构成水印方案有效性的核心判别标准。

### 2.3.1 数字水印的基础模型

数字水印技术指通过特定算法在载体图像中隐蔽嵌入标识信息（如二进制序列、数字签名或生物特征数据）的数字版权保护方法。其系统架构包含嵌入与提取两大核心环节：嵌入阶段将加密处理后的水印数据融合至载体图像的频域或空域特征中，要求保持载体视觉质量无明显劣化；提取阶段则通过逆向算法从可能遭受攻击的载体中恢复水印信息，实现版权溯源。系统有效性取决于不可感知性（视觉隐蔽度）与鲁棒性（抗压缩/滤波等攻击能力）的平衡优化。

下图就是广义的数字水印的添加和提取模型：



嵌入单元：数字水印系统的嵌入单元由载体图像与水印信息构成基础输入要素，可选择性引入密钥机制以增强系统安全性。该单元的核心处理模块通过特定加密策略实现水印融合，其算法选择（如频域系数调制或空域像素调整）直接影响水印的隐蔽性与抗攻击能力。经算法处理后生成的含水印图像作为最终输出，其视觉质量需与原始载体保持高度一致性以确保不可感知性。

攻击单元：数字水印攻击指削弱水印可提取性的操作或干扰因素，主要分为非恶意干扰与恶意攻击两类。前者源于传输信道失真或常规信号处理（如JPEG压缩、噪声污染），后者则涉及针对性破坏手段。当前主流攻击可归纳为两大技术分支：1）信号处理攻击：通过频域/空域修改破坏水印结构，典型手段包括滤波、量化、重采样；2）几何攻击：通过空间变换扰乱水印同步机制，具体表现为旋转、缩放、裁剪等仿射变换。文献[51][52]研究表明，鲁棒水印系统需建立双重防御机制：在算法层采用抗几何失真的同步标记设计，在数据层嵌入冗余纠错编码以抵御信号处理损伤。系统鲁棒性作为核心评价指标[53]，直接决定水印在遭受复合攻击后的存活能力。

提取单元：该过程从水印图像或被攻击的图像中恢复隐藏的数据，通常是嵌入过程的逆操作。提取方法可以分为非盲、半盲和盲提取。非盲提取需要原始载体图像信息；半盲提取则依赖原始水印信息；而盲提取则不依赖任何先验知识。 比较单元：比较单元是在最后的时候将提取出的水印与原始水印进行比较，提取后的水印和原始水印的相似程度越高则该水印的鲁棒性越强。

### 2.3.2 数字水印的特性

数字水印有下面几个特性：

1. 不可感知性：

数字水印的不可感知性体现为含水印载体与原始载体在视觉特征上的高度一致性，要求人类视觉系统（HVS）无法察觉信息嵌入引发的失真。该特性在医学影像分析[53]、遥感解译[54]等敏感领域尤为重要，细微的视觉偏差可能导致诊断或判读错误。此外，视觉保真度的缺失会暴露水印存在，诱发针对性攻击（如定位擦除或覆盖篡改），致使版权保护机制失效。因此，不可感知性不仅是用户体验的基础要求，更是保障水印隐蔽性与功能有效性的核心约束条件。

1. 鲁棒性

数字水印的鲁棒性表征算法在遭受信号处理攻击（压缩、噪声干扰）与几何攻击（旋转、缩放、裁剪）时维持水印信息完整性的能力，其核心要求是通过冗余嵌入、频域能量扩展等技术手段，确保水印在攻击后仍具备可检测性与可恢复性。现行主流增强策略包括：1）频域扩频技术：将水印能量分散至宽频段以抵御局部信号损伤；2）几何同步机制：嵌入定位标记以校正空间变换引发的同步偏移；3）分层冗余编码：通过纠错码与多副本嵌入提升信息存活概率。高鲁棒性系统需实现攻击敏感性（快速识别篡改）与生存能力（维持水印完整）的动态平衡，从而有效阻止非授权方的水印擦除或篡改企图。

1. 嵌入容量

嵌入的容量指的是可以嵌入到载体图像中的水印数据量。较大的嵌入容量能够存储更多的信息，但这也可能会影响水印的质量和鲁棒性。如果嵌入的容量过大，水印可能会变得容易受到攻击或者被察觉，从而影响不可见性和鲁棒性。

1. 总结

鲁棒性与不可见性通常存在矛盾。为了提高鲁棒性，水印通常需要嵌入更多的信号，这可能会导致水印在图像中的可见性增加。因此，如何在保证鲁棒性的同时保持不可见性是一个挑战。

鲁棒性与嵌入容量也有一定冲突。增加嵌入容量可以使得水印在受攻击后的恢复能力更强，但这也可能使得水印变得容易被检测或被修改，导致鲁棒性下降。

不可见性与嵌入容量之间也有对立关系。增加嵌入容量可能会使得水印更加显眼，破坏不可见性。因此，需要在这两者之间找到一个平衡点。

### 2.3.3 数字水印技术分类

目前数字水印技术主要采用的是空域数字水印技术和变换域数字水印技术。下面将介绍两种数字水印技术，由于本文技术最终实现选取了抗干扰更强的变换域数字水印技术，所以将重点介绍变换域数字水印技术。

1. 空域数字水印

空域隐写技术通过修改载体数据的非关键信息位实现信息隐蔽传输，其核心机制在于利用人类视觉系统（HVS）对细微亮度变化的低敏感特性[1]。典型代表如最低有效位（LSB）算法，该技术将隐写数据嵌入像素值最低比特位，通过替换操作使载体修改量控制在±1灰度级范围内，从而保证视觉不可感知性。LSB方案具有两大显著优势：其一，隐写容量与载体像素数呈线性关系，可实现高数据吞吐；其二，算法复杂度低，适用于实时处理场景。但受限于底层嵌入机制，其对信号处理攻击（如JPEG压缩、重采样）表现出显著脆弱性——当载体经历有损处理时，LSB层信息极易被量化过程破坏。研究[1]指出，虽然空域方法在不可见性与嵌入容量方面表现优异，但需结合加密编码或信息分散策略才能提升抗攻击能力。

虽然LSB方法在空域中是一种典型的隐藏算法，具有较大的写入容量和较小的载体变化，但由于信息位于最不显著位，容易受到压缩等操作的破坏。又因为图片在传输，存储过程中经常会有压缩操作，所以对提取水印带来了挑战。

1. 变换域数字水印

变换域隐写技术通过将秘密信息嵌入载体信号的频域系数实现隐蔽传输，其核心原理基于人类感知系统对频域能量分布的差异化敏感特性。相较于空域隐写，该技术通过频域能量调制策略（如中频带嵌入）在不可见性与鲁棒性之间取得更优平衡：1）低频分量修改易引发视觉失真，高频分量易受信号处理干扰，故选择中频区域作为信息载体；2）频域变换（DCT/DWT）的全局能量分布特性使嵌入信息具备抗局部裁剪、噪声干扰的能力。主流实现路径包括离散余弦变换（DCT）系数调制[28]、小波域（DWT）子带能量调整[29-31]以及压缩域隐写等复合技术。以图像载体为例，其技术流程可分为三步：首先对原始图像进行正交变换获取频域系数矩阵；随后根据隐写规则调整选定频段系数值；最后执行逆变换生成含密载体。该技术体系在抵抗JPEG压缩、滤波攻击等方面展现出显著优势，但需权衡计算复杂度与嵌入容量——频域变换的正交特性虽增强鲁棒性，却也限制了可修改系数数量。研究[28-31]表明，通过自适应频段选择与量化步长优化，可有效提升信息隐藏效率。

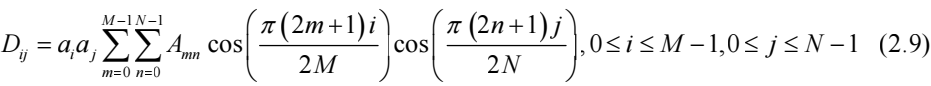
下面，介绍现在流行的变换域的数字水印技术：

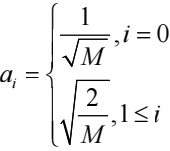
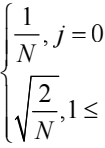
（1）DCT技术

数字水印技术中的 DCT（离散余弦变换）方法 通过将水印嵌入图像频域中频系数实现隐蔽性与鲁棒性的平衡。其核心原理是将图像分块（如8×8像素）并进行DCT变换，将空域像素转换为频域能量分布——低频分量对应主体轮廓（修改易失真）、高频分量易受压缩破坏，因此选择中频区域（如坐标(4,4)附近）作为水印嵌入位点。具体流程为：分块后对每个块执行DCT变换，通过量化步长控制（如直接叠加水印序列或量化索引调制）修改选定中频系数，再逆变换重建含水印图像。水印提取时，可通过对比原始图像（非盲提取）或直接解码频域系数（盲提取）恢复信息。

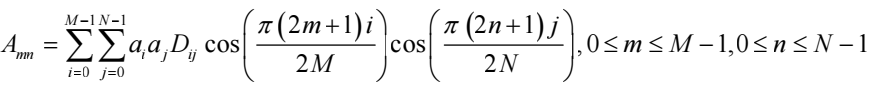
DCT技术的优势在于抗JPEG压缩能力强（与JPEG标准兼容）、不可见性高（PSNR通常>40dB），适合版权保护与内容认证；但面临几何攻击脆弱性（如旋转/裁剪）和容量限制（依赖分块数量）。典型应用包括JPEG图像版权标记、视频溯源追踪等。为优化性能，常结合自适应嵌入（动态调整强度）、混合域策略（融合空域高容量）或抗几何模板（校正形变）进行改进，实现在压缩、滤波等常见攻击下的稳定水印存活。

一个M× N的图像进行DCT变换的公式如下定义如下：



其中 ≤ *M* - 1 ，*aj* = *j* ≤ *N* - 1 。

逆变换定义为：



其中，*Dij* 为矩阵 A 的 DCT 系数，*Amn* 为图像对应的像素值。

1. DWT变换

数字水印技术中的 DWT（离散小波变换）方法 通过多尺度频域分解实现水印的隐蔽嵌入与高鲁棒性保护。其核心原理是将图像通过小波变换分解为多级子带（如LL低频子带、LH/HL中频子带、HH高频子带），选择中高频子带（如LH或HL）嵌入水印——低频子带（LL）包含图像主体能量（修改易导致失真），高频子带（HH）易被压缩破坏，而中频子带既保留细节特征又具备抗干扰能力。具体流程为：对原始图像进行多层小波分解（如3级分解），在中频子带系数中通过量化调制（如修改系数幅值或相位）或系数替换嵌入水印，再通过逆小波变换重建含水印图像。水印提取时，需对含密图像执行相同的小波分解，从目标子带中解码水印信息（盲提取依赖预定义规则，非盲提取可对比原始子带差异）。

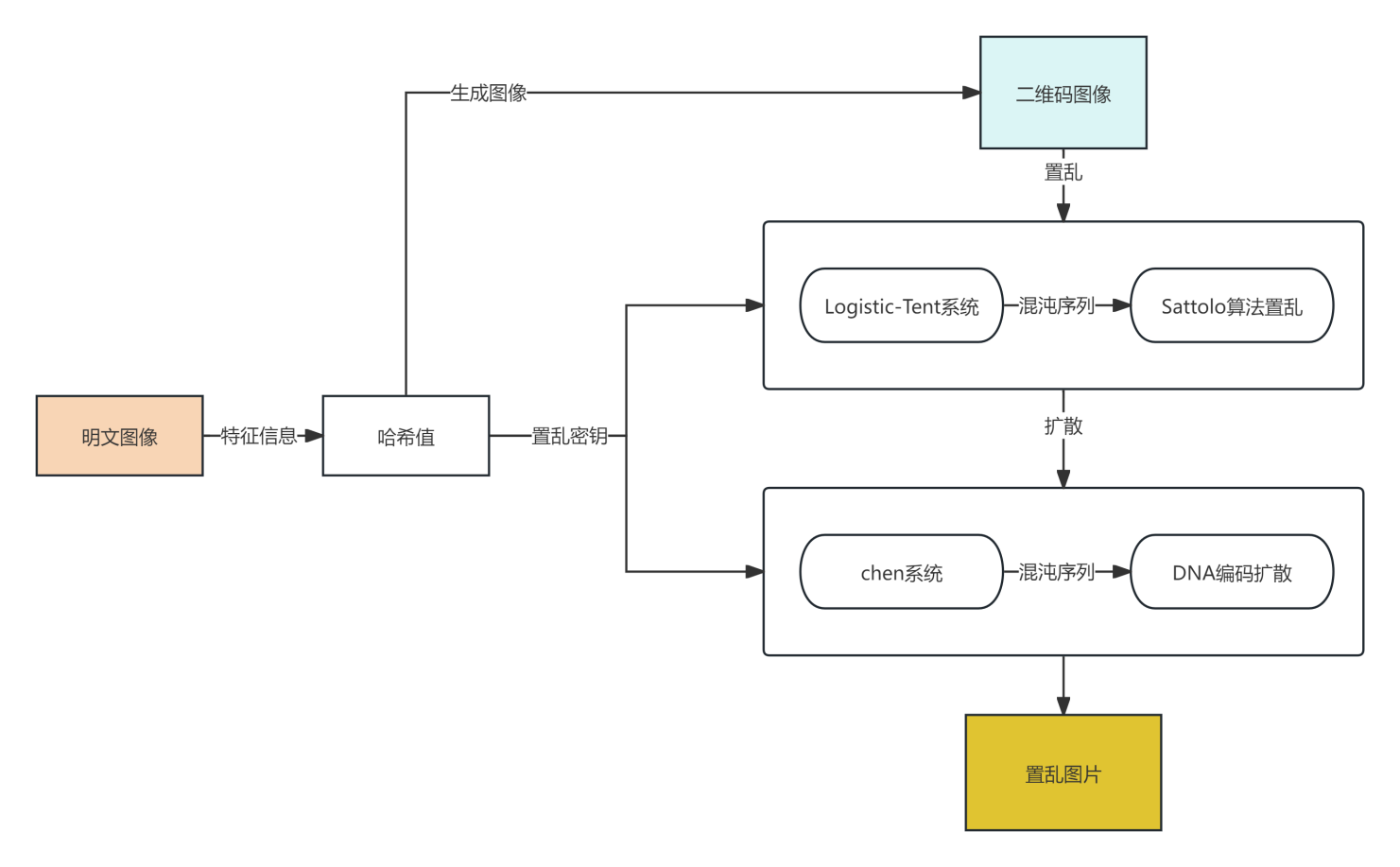
DWT技术的优势在于多分辨率特性：1）抗几何攻击能力优于DCT（小波分解的多尺度特性可缓解局部形变影响）；2）嵌入容量更高（多子带可并行嵌入）；3）兼容有损/无损压缩场景（如JPEG2000标准基于小波变换）。但其计算复杂度较高，且对特定攻击（如中频滤波）敏感。典型应用包括医学影像认证（需高保真）、高清视频水印（多分辨率适配）以及多重水印嵌入（不同子带承载不同功能标记）。改进方向常聚焦于自适应嵌入策略（根据子带能量动态调整强度）、混合加密技术（结合混沌加密增强安全性）以及抗同步攻击设计（利用边缘特征或不变矩校正几何失真），从而在保持视觉隐蔽性的同时提升对裁剪、旋转、缩放等复合攻击的抵抗力。

# **3 基于混沌系统的图像加密方案**

本章节将介绍从中心存证系统获取元数据后，进行的主要操作，包括：利用元数据生成原始图像的唯一标识和置乱密钥，将唯一标识编码成QR码，用置乱密钥生成混沌序列，将QR码利用混沌序列进行混沌置乱和扩散操作得到组后的混沌图片，然后对混沌图片做反向提取操作和安全性测试，测试混沌加密方案的有效性。

## **3.1加密系统模型**

系统的加密流程如图 3.1 所示。首先，通过明文图像提供的特征信息采用SHA256算法算出特征信息的散列值，将生成的散列值转换成二维码图像作为秘密信息。将该散列值与给定的值进行运算后再作为混沌系统的初始参数以及整个加密系统的密钥。接下来，将基于此密钥生成的混沌序列与加密系统深度融合：这个加密系统具体涵盖了sattlolo随机置乱算法和DNA循环编码扩散机制。经过这两个关键步骤后，即可完成对原始图像的加密处理并得到置乱图像。

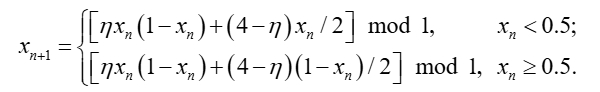


## **3.2混沌系统的选取**

在第二章的混沌系统中我们介绍了两个经典的混沌映射系统 Logistic系统和Tent系统。Logistic系统和Tent系统都是常见的混沌系统，但它们在动态特性上有所不同。Logistic系统具有较简单的数学模型和较好的稳定性，但对于一些复杂的非线性现象，它的表现较为有限。Tent系统则在产生更为复杂的混沌行为方面表现得更为优异，适用于一些需要更高灵敏度和更强动态行为的应用。

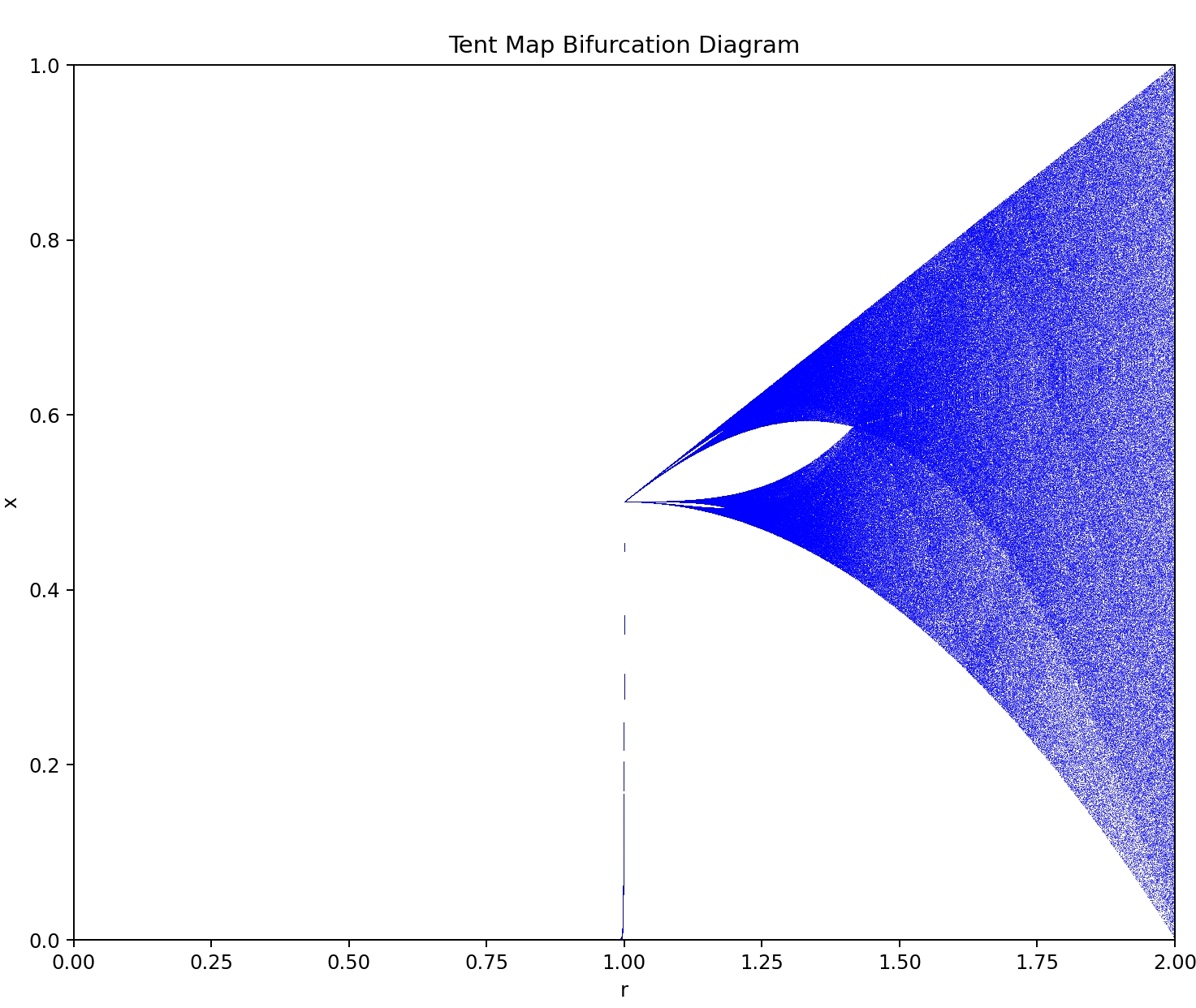
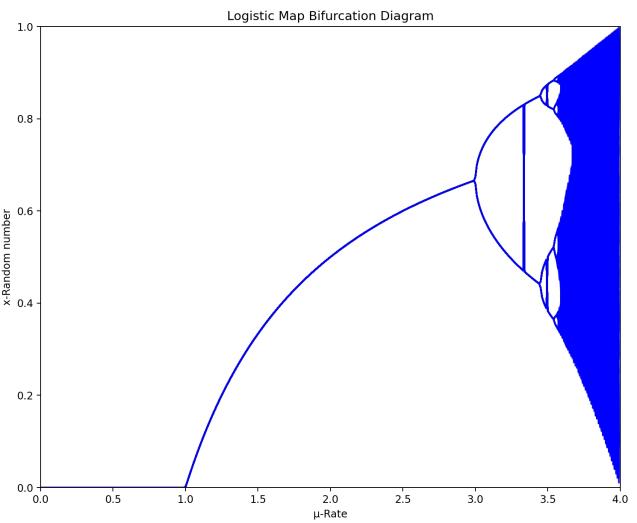
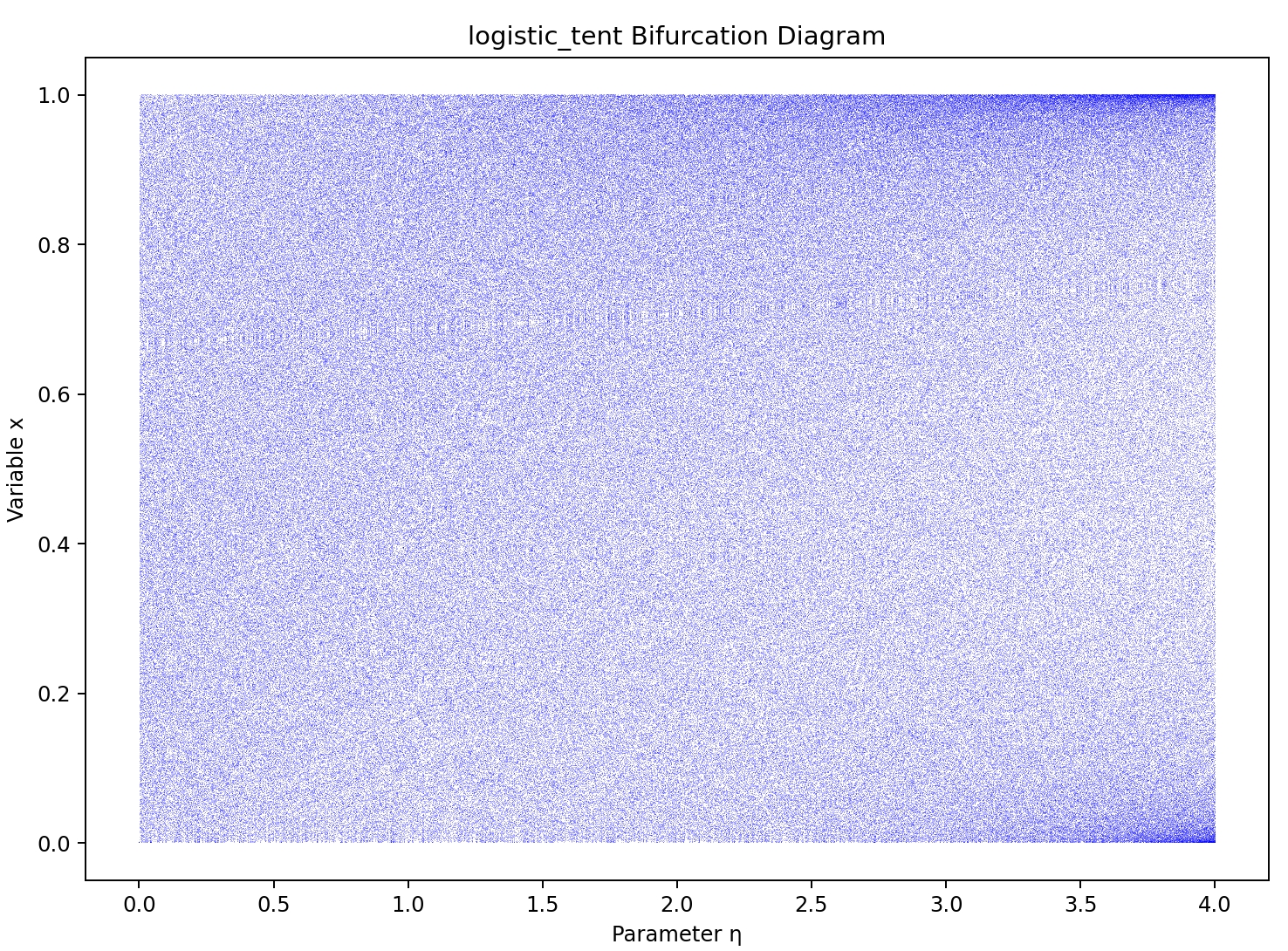
采用Logistic-Tent系统的优点在于它结合了两者的特点，既保留了Logistic系统的简单性和稳定性，又引入了Tent系统的高灵敏度和多样性，使得在处理一些具有较高复杂度的混沌问题时更加高效和灵活，解决了单一系统在稳定性与复杂性之间的权衡问题。

Logistic-Tent映射表示为：



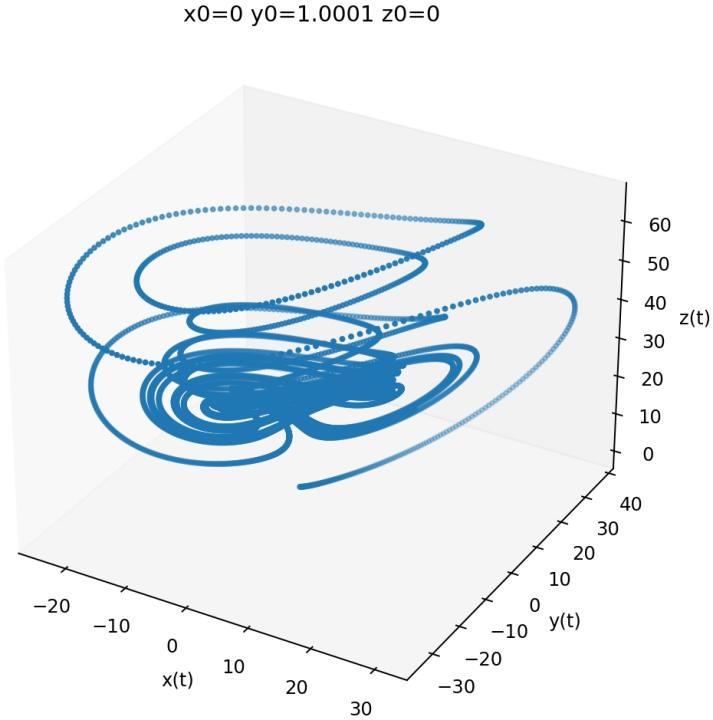
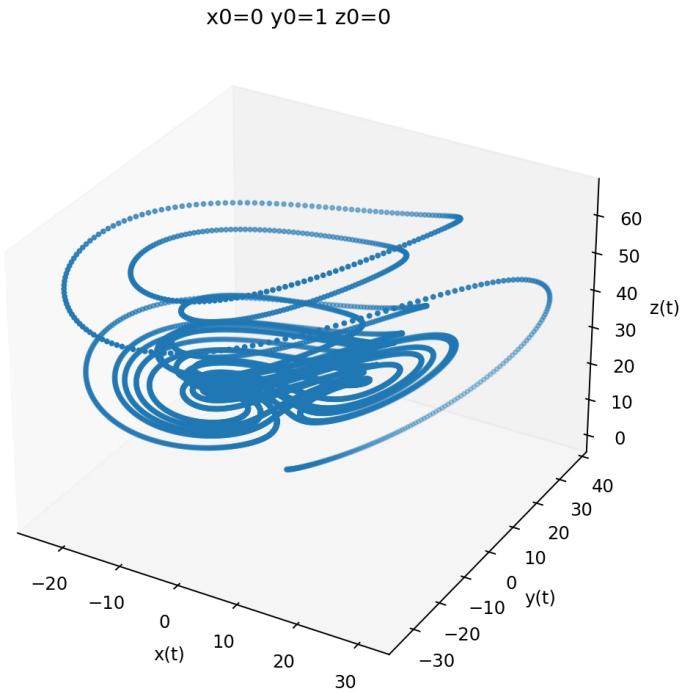
其中 *μ* ∈(0, 4] ，为第n 个元素的值。

Logistic-Tent的分岔图如下所示：

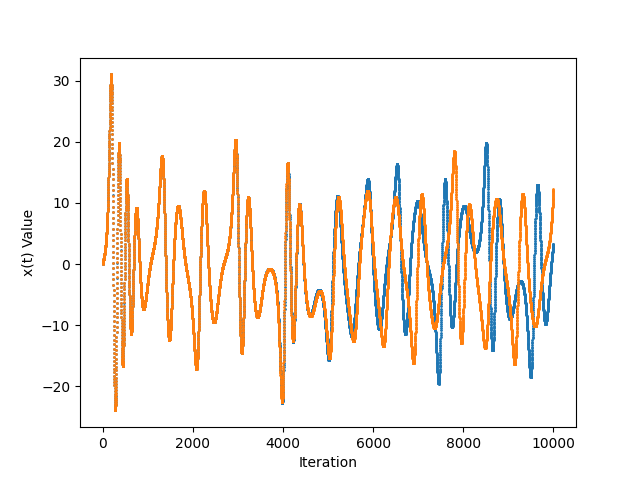
 

我们将用Logistic-Tent映射系统来控制第一步的置乱操作。

根据第二章内容，Chen系统的参数设置为a = 35 ，b = 3 ，c = 28，这样Chen 系统通常能比Lorenz 系统产生更均匀、随机性更强的序列。更复杂的混沌行为使得系统对初始条件更加敏感，进而提升密钥敏感性和抗攻击性。



由图可见，经过长时间运行后，系统只在三维空间的一个有限区域内运动，系统在此区域中的运动是混沌状态。我们从两个靠的很近的初值条件出发（yt只相差0.0001）给出了x(t)轨道的演化图如下



由图可见，随着时间的演化，可以看到原本靠得很近的轨道，在迭代7000次左右后x的值开始出现较大的区分，最后两条轨道变得毫无关联。

因为Chen是个三维的混沌系统，所以多的混沌序列来操控DNA编码扩散情景下的置乱和扩散操作。所以用Chen系统作为DNA编码扩散操作的混沌系统。

## **3.3密钥和混沌序列产生**

在双端协同存证模型中，唯一标识码作为原始图片的数字指纹，同时是置乱密钥的生成依赖，需满足全局唯一性、抗篡改性与高效生成需求。

混沌序列作为加密载体QR码的动态控制参数，需要完成对QR码的置乱和扩散，必须具备强随机性和初值敏感性。

本节下采用一种元数据驱动的“标识-密钥协同生成机制”，通过哈希函数确保标识码唯一性，结合一维和三维混沌系统生成动态密钥和多维混沌序列，实现“一图一密”，确保载密QR码的信息安全。

### 3.3.1 生成唯一标识码

NIST标准化哈希算法历经多代迭代，形成SHA-0、SHA-1、SHA-2、SHA-3四大分支。其中SHA-2系列包含六种子类型（SHA-224/256/384/512/512-224/512-256）[44]，其核心优势体现在长哈希值设计（224-512位）与抗碰撞强度提升，相较SHA-1与MD5具备显著安全性优势（SHA-1碰撞攻击复杂度2^63次，SHA-256达2^128次）。尽管SHA-512通过增加迭代轮数（80 vs 64）进一步强化安全性，但由此产生的计算开销导致吞吐率不如SHA-256。综合考量安全性基线（满足128位抗碰撞）、运行效率（单位时间处理量）及软硬件兼容性（广泛支持AES-NI指令加速），SHA-256成为标识码生成函数的优化选择。使用SHA-256 算法的算法生成唯一标识主要步骤如下：

（1）第一步是填充比特位：我们输入的元数据字符串的长度为L，需要在消息的末尾进行比特填充。具体的填充方式为：首先，在填充比特串的最高位添加一个1，随后跟随 K个0，其中 K是满足方程 L+K+1=448mod  512的最小非负解。最后，附加消息的长度 L的二进制表示。通过这种方式，最终填充后的消息长度会是512位的整数倍。附加填充比特的规则如图3-1所示。以输入比特串 "a, b, c" 为例进行说明

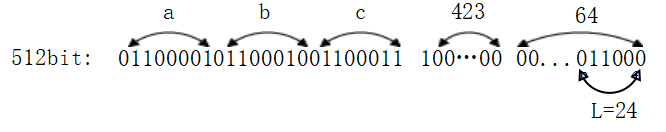


图 3-1 附加填充比特处理示列

（2）第二步进行算法的输出初始化：每次进行 SHA-256 计算时，都需要首先初始化输出。此过程通过 8 个 32 位寄存器来存储 SHA-256 在各个时刻的值。根据算法协议标准，初始化值来源于前 8 个质数平方根的小数部分的前 32 位。这 8 个初始值可以用 16 进制表示如下：

H=0x6a09e667

H=0xbb67ae85

H=0x3c6ef372

H=0xa54ff53a

H=0x510e527f

H=0x9b05688c

H=0x1f83d9ab

H=0x5be0cd 19

（3）常量数组的初始化：常量数组 到的值取自前 64 个质数（从 2 到 311）的立方根小数部分的前 32 位。这些常量可以通过 16 进制表示，从左到右排列，如表 4-1 所示：

表 4-1 常量数组值表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 428a2f98 | 71374491 | b5c0fbcf | e9b5dba5 | 3956c25b | 59f111f1 | 923f82a4 | ab1c5ed5 |
| d807aa98 | 12835b01 | 243185be | 550c7dc3 | 72be5d74 | 80deb1fe | 9bdc06a7 | c19bf174 |
| e49b69c1 | efbe4786 | 0fc19dc6 | 240ca1cc | 2de92c6f | 4a7484aa | 5cb0a9dc | 76f988da |
| 983e5152 | a831c66d | b00327c8 | bf597fc7 | c6e00bf3 | d5a79147 | 06ca6351 | 14292967 |
| 27b70a85 | 2e1b2138 | 4d2c6dfc | 53380d13 | 650a7354 | 766a0abb | 81c2c92e | 92722c85 |
| a2bfe8a1 | a81a664b | c24b8b70 | c76c51a3 | d192e819 | d698aa4a | f40e3585 | 106aa070 |
| 19a4c116 | 1e376c08 | 2748776c | 34b0bcb5 | 391c0cb3 | 4ed8aa4a | 5b9cca4f | 682e6ff3 |
| 748f82ee | 78a5636f | 84c87814 | 8cc70208 | 90befffa | a4506cbe | bef9a3f7 | c67178f2 |

（4）数组的计算，~ 分别由 512比特输入块以 32比特从高位到低位均分得到， ~ 的计算方式如式(4-1)所示：

其中 ，的计算方式分别如式(4-2)和(4-3)所示：

*S0 =(Wi-15ROR7)*⊕*(Wi-15ROR18)*⊕*(Wi*- 15*SHR3)*

S1=(Wi- 15ROR7)⊕(Wi- 15ROR18)⊕(Wi- 15 SHR3)

（5）压缩函数的迭代计算：SHA-256 算法进行 64 次迭代计算。在每次迭代中，8个常数变量 a, b, c, d, e, f, g, h 都是 32 位的数据变量。首先，需要初始化这 8 个迭代常数变量，其初始化公式如式 (4-4) 所示：

a=H0(i-1)





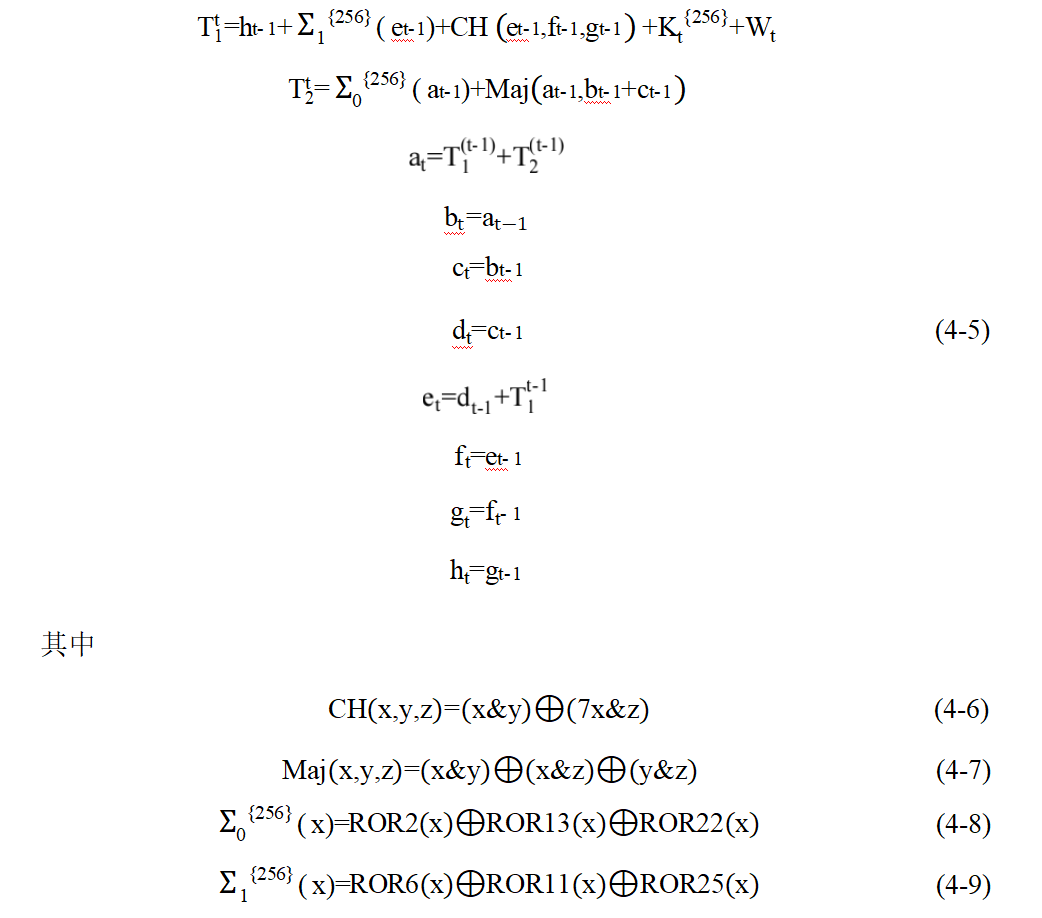




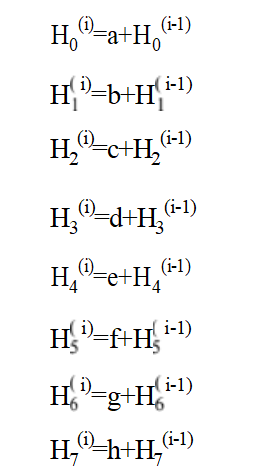






接下来，需要对迭代常数 a、b、c、dd、e、f、g、h 进行更新。其更新公式如下式 (4-5) 所示：

最后计算每一步的 Hash 值，需要用到第（i-1）次的 Hash 值以及更新的迭代 常数变量。其具体计算方式如式(4-10)所示：



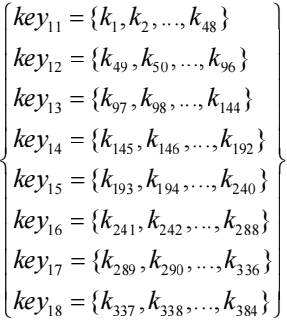
当处理完最后的一个 512 比特的消息块之后，则将最后一迭代过后的运算结 果作为最后的 SHA-256 输出，其输出结果如公式(4-11)所示：

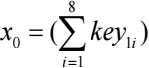
H=H0|H1|H2|H3|H4|H5|H6|H7

在以上式子中，ROR 表示循环右移，SHR 表示右移，⊕表示异或，|表示位拼 接，&表示按位相与运算，7表示取反运算。

### 3.3.2 生成置乱初值和置乱序列

在上一节我们运用 SHA-256哈希算法对元数据进行了运算，生成对应的哈希值H，随后将H这个十六进制格式的哈希值进一步转化为一个由 256 位二进制数字构成的密钥 key。将密钥每 32位分成一组，将每一组二进制转换成 十进制大数，通过依次相加之后再经过式(3.7)运算得到混沌初值。散列算法的优点就在于密钥与明文密切相关，所以当元数据发生变化时所计算出的哈希值也将不同。

*key* =  (3.6)

 .10−12 (3.7)

，就是一维混沌映射置乱密钥，也是混沌映射系统的混沌初值。随机选取 *μ* ∈(0, 4]，带入初始值迭代生成和M×N长度的序列S。该S序列就是和Sattolo算法结合的置乱序列。

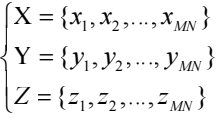
*把 依次异或后所得的比特序列换算成十进制数字 b。再通过式(3.8)映射， 作为 Lorenz 超混沌的初值。*

*m* = −20 + mod(*b*, 40)

其目的是将chen混沌的初值范围限制在-20到20之间。将密钥，μ，m 输入到chen系统中，参数设置为a = 35 ，b = 3 ，c = 28，密钥形成的系统的初始值 u0为：

*u*0 = [*μ*,, *m*]T

假设图像大小为 M×N，系统生成 10000+M×N 长度的伪随机序列，并丢弃前 10000 个值以获得更好的随机效果，得到 M×N 长度的混沌序列 X ，Y ，Z。



混沌序列X,Y,Z就是三维的混沌序列，用于DNA编码扩散

## **3.1 QR码生成**

根据生成的散列值H，生成对应的QR码，。

互联网有大量二维码生成软件，根据网络开源项目 zxing，结合 base64 技术设计了自己的二维码生成软件，可以将图片或文字转换成二维码。

zxing 是一个开源 java 项目，可以编码和解码多种类型的条形码，支持格式包括 UPC-A ，UPC-E ，EAN-8 ，EAN-13 ，QR code 等，支持多种平台。目前已经广泛使用。

Base64 是一种常见的网络传输编码方式，它使用 64 个可打印字符来表示二进制数 据，编码后的信息难以直接发现，并且易于加密和解密，适用范围很广。

以下是二维码生成软件的生成效果：

（1）二维码内容：

Xi`an University of Science and Technology 生成二维码图像：



图 3.2 二维码 1

（2）二维码内容：

At the beginning of the new semester, every student is required to register with the department. In the case of failure to register, he has go to department to go through the formalities for leave, and those absent for two weeks without asking for leave are thought to drop out.

生成二维码图像：



图 3.3 二维码 2

（3）二维码内容：

Xi’an University of Science and Technology lies in Xi’an, a world-famous city with numerous ancient and historical sites and remains. Its head campus stands blocks away from the Big Wild Goose Pagoda well known at home and abroad and its newly built Lintong campus close to another popular tourist resort Huaqing Hot Springs. Shaanxi provincial CPC Committee and Shaanxi provincial government and the Xi’an municipal government officially recognize the university as the Model University and Garden Campus respectively.

生成二维码图像：



图 3.4 二维码 3

## **3.4 QR码的混沌置乱**

### 3.4.1 混沌置乱算法的实现

步骤 1：将图像信息转变成比特流序列 V。

步骤 2：利用密钥和 LTM 混沌产生与比特流长短 n 相等的混沌序列 S 。 步骤 3 ：从比特序列的最后一个元素开始循环，并依次减小 1 ，i=n→ 1。

步骤 4：利用混沌序列 S 生成随机下标 j，如式(3.9)所示。其中 ceil()函数表 示向下取整。

j = ceil(i . S(i)) (3.9)

步骤 5：交换 V(i)和 V(j)。

经过混沌与Sattolo 算法结合置乱后的图像 P 如图所示。

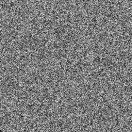


图 3.4 图像像素置乱。(a)原始图像；(b)置乱后图像。

### 3.4.2 DNA编码扩散算法的实现

本节基于chen系统产生的三维混沌序列和 DNA 编码的图像加密算法共有 3 个需要选择的操作。 混沌序列X用于决定置乱矩阵的DNA编码方式；混沌序列Y用于决定置乱矩阵和扩散矩阵的DNA运算规则，混沌序列Z用于最后矩阵的DNA解码规则。下面是DNA编码扩散算法的实现。

步骤 1：将 X序列映射到 0-255内，并将其重塑为 M\*N 大小的矩阵。如式 (3.12)所示。其中，*i* ∈[1, *MN*] ，floor(•) 是向下取整操作，reshape() 函数将序列 L 重塑成 M×N 矩阵 R，用于下一步 DNA 操作。

*Li* = mod(floor(*xi* × 108 ), 256)

*R* = reshape(*L*, *M* , *N*)

步骤 2：将置乱后的图像分成块，以提高 DNA 编解码的速度，并将图像矩阵和扩散矩阵 R 都分为 4×4 的小矩阵。DNA 编码和解码的方式由以下公式确定。

*k*1*i* = mod(*Li* ,8) +1

其中 k1i 决定了图像和扩散矩阵各块的编码方式，可以表示数字 1 到 8，分 别代表 DNA 的 8 种编码规则。

*k*2*i* = mod(round(*yi* × 104 ), 4)

其中 k2i 控制了图像矩阵和扩散矩阵之间的DNA运算规则。它可以表示数 字 0-3，分别表示运算规则中的加法、减法、异或和同或。

*k*3*i* = mod(round(*zi* × 104 ),8) +1

其中 k3i 决定了计算矩阵的解码规则。其中 mod(·)表示取模运算，round()函数代表就近取整。DNA 扩散过程如图 4 所示。

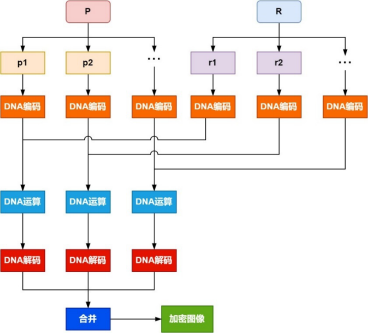


图 3.5 DNA 分块扩散过程

将置乱矩阵 P 和矩阵 R分成块矩阵之后，依次进行 DNA 编码以及运算，再将运算后的结果进行DNA解码，所获的图像像素值与原始图像将完全不相同。合并后即可获得加密图像。

步骤 4 ：将步骤 3 循环 9 次运算，即可得到更加难以预测的加密图像。

## **3.5 图像的解密过程**

图像解密是加密的逆过程，本方案采用对称加密方式， 只有获得加密密钥 才能进行以下解密过程。

输入：密文图像 C ，密钥序列 key ，chen系统的初值 m ，μ。

步骤 1：首先进行 DNA 循环逆扩散，过程与加密时是相同的。解密的耗时 如下表所示，由表中数据可得解密耗时较短， 效率较高，具体耗时差异还与实 验所用机器性能有关。

表 3.1 所提出方案的图像解密时间

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 图像 (256×256) | 鹦鹉 | 蝴蝶 | 房顶 | 摄影人 |
| 解密耗时 (s) | 0.8134 | 0.8127 | 0.8343 | 0.8643 |

步骤 2：将逆扩散后的图像转换成比特序列，通过密钥得到 LTM 混沌序列， 用逆 Sattolo 算法混淆运算两个序列，逆运算与加密时相反，即从前往后交换序 列值。

输出：明文图像。

## **3.6 算法的安全性分析**

# **4 DCT 域二值图像数字水印算法**

本章对第三章介绍的应用混沌及位置置乱理论对二维码进行加密，提出一种基于混沌置乱和DNA扩散加密的 DCT 域图像数字水印算法，该算法利用混沌序列特有的性质，将含有版权信息的二值图像水印用混沌 序列进行加密，然后将不同强度的水印分量自适应地嵌入到不同图像块 DCT 域中去。通过加入高斯噪声、椒盐噪声以及 JPEG 压缩和剪切等处理操作，结果表明了该算法具有很好的视觉掩蔽特性和鲁棒性

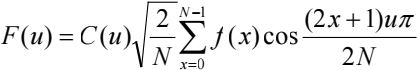
## **4.1 离散余弦变换（DCT）的原理**

### 4.1.1 DCT 变换的原理

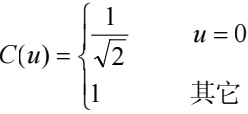
在现代图像处理技术中，我们通常用到的变换有 DFT ，DCT，沃尔什--哈 达玛变化(WHT)，主成分变换(K-L)等等，这里所说的图像变换指二维正交变 换，它们在图像处理中扮演着重要的角色。如傅立叶变换后平均值正比于图像 灰度的平均值，高频分量指示图像中目标的边缘信息，利用这些性质可以从图 像中抽取特征。又如在变换域中，图像能量往往集中在少数项上，或者说能量 主要集中在低频分量上，这时对低频成分分配较多的比特数，对高频成分分配 较少的比特数，即可实现图像数据的压缩编码。再者，舍弃变换系数矩阵中某 些幅度小的系数，可缩减计算维数，提高计算的速度[39]。

在理论上来说，K-L 变换是图像变换中具有最佳性质的一种，作为标准用 来衡量其它变换性能的好坏，因为它能完全消除子像块内像素间的线性相关 性，经 K-L 变换后各变换系数在统计上不相关，其协方差矩阵为对角阵，因而 大大减少了原数据的冗余度。如果丢弃特征值较小的一些变换系数，那么，所 造成的均方误差是所有正交变换中最小的。但是由于 K-L 变换是取原图各子块 协方差的特征向量作为变换后的基向量，因此 K-L 变换的变换基是不固定的， 使用起来很不方便，一般只将它作为理论上的比较标准，实际上用得最多的还 是 DCT，它的性能最接近 K-L 变换，而 DFT 和 WHT 要差一些。离散余弦变 换是最小均方误差条件下得出的较优的正交变换，由于离散傅立叶变换要对 n 点像素(对一维来讲)做周期延拓，故一般在周期间的接点处会引入一个突变， 这意味着将导致较大的高频系数，即能量不能充分集中于低频部分。而离散余弦变换相当于做 2n 点的离散傅立叶变换，它先将原 n 点像素做偶对称扩展后 再做周期延拓，因此边界处没有突跳，能量可更集中。另外，它有固定基，它 的性能最接近 K-L 变换，因而它是变换法的主流，现有的三个国际编码标准都 选中了 DCT[40]。

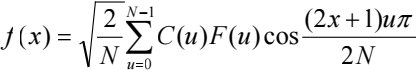
一维 DCT 的定义如下：设{f(x) x = 0,..., N −1}为信号序列集合，其离散余 弦的正变换定义为：



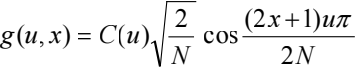
式中，*x* = 0,..., *N* −1 ，*u* = 0,..., *N* −1 。 其中



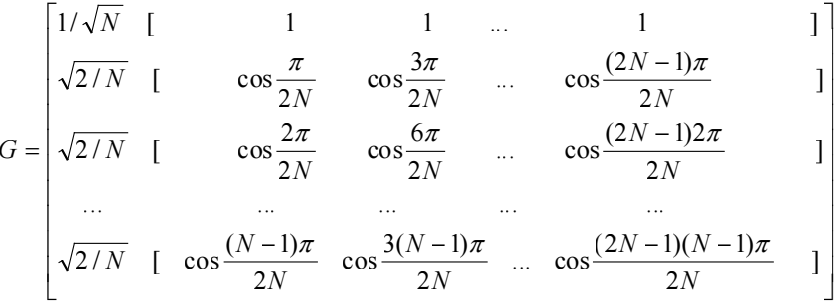
其逆变换定义为：



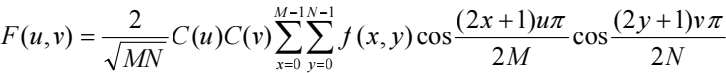
式中，*x* = 0,..., *N* −1 ; *u* = 0,..., *N* −1 。 可见一维 DCT 的正反变换核都是



将变换式展开整理后，可以写成矩阵形式：

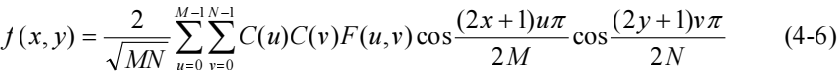


将一维离散余弦 DCT 变换的定义推广到二维离散余弦 DCT 变换，设 {*f* (*x*, *y*) *x* = 0,..., *M* −1; *y* = 0,..., *N* −1}为二维图像信号序列集合，其正变换为：



其中 C(*u*) , C(*v*) 的定义同前；

*x* = 0,..., *M* −1; *y* = 0,..., *N* −1;*u* = 0,..., *M* −1;*v* = 0,..., *N* −1。 二维 DCT 的逆变换为：



其中 *x* = 0,..., *M* −1; *y* = 0,..., *N* −1;*u* = 0,..., *M* −1;*v* = 0,..., *N* −1。

二维 DCT 是目前最常用的有损数字图像压缩系统——JPEG 的“核心 ”， 因此 DCT 域的数字水印受到了广泛的重视[41]。

4.1.2 DCT 变换系数的选择

DCT 域水印算法是将图像进行 DCT 变换，选择某些变换后的 DCT 系数进 行小幅度的改动，从而实现水印信号的嵌入。变动不同的 DCT 系数对水印系 统的整体性能有着不同的影响。

数字水印的两个最基本的要求是：1 ．水印的不可见性；2 ．水印要具有一 定的抗攻击能力，即嵌入水印的图像在经过一般的图像处理后，图像中的水印 应该继续存在[42]。这两个要求直接影响到水印嵌入的系数的选择。

一方面，一般的图像处理均发生在图像频谱的高频区域中，例如对图像进 行 JPEG 压缩，它保留了图像的低频信号，而将一部分的高频信号滤掉。如果 水印嵌入在高频，虽然其不可见性效果很好，但水印经过图像处理后容易被删 除，其鲁棒性差，因此变换域的水印算法不能将水印信号嵌入到图像的高频区 域中。

另一方面，图像的主要能量集中在它的低频系数上，低频系数直接影响到 人眼的视觉效果[43] 。在低频系数中嵌入水印信号，由于低频系数携带了图像的 大部分的能量，图像受到攻击时，攻击者一般要保证图像的质量不能下降得太 厉害，这样大部分的低频系数仍然保留，嵌入它们的水印信号因此存活下来， 这样能够保证水印的鲁棒性。但是在嵌入的过程中要修改低频系数，对图像重 要信息会造成破坏，就会降低图片的视觉效果。

所以本文采用折中的办法：选择中频系数，寻求不可见性与鲁棒性的兼 顾。本文选取 DCT 中频作为水印嵌入区域，问题就简化为如何在水印的不可 见性与鲁棒性平衡的情况下，把水印嵌入到图像的中频系数中。

4.1.3 基于人类视觉系统的块分类方法

人类视觉系统 HVS(Human Visual System)对图像所具有的频率掩盖、亮度 掩蔽和对比度掩蔽等特性表明：背景亮度越亮，纹理越复杂，人类视觉对其轻 微变化就越不敏感，只要嵌入水印信号低于 HVS 的对比度门限(CST：Contrast Sensitivity Threshold) ，HVS 就无法感知到信号的存在。它具有如下三个特性： 1 ．人眼对不同灰度具有不同的敏感性， 通常对中等灰度最敏感，而且向低灰 度和高灰度两个方向非线性下降； 2 ．对图像平滑区的噪声敏感，而对纹理区 的噪声不敏感；3 ．边缘信息对于人眼非常重要，必须保护边缘的质量不受大 的损害[44]-[46]。因此，可以利用 HVS 特性选取不同的嵌入强度因子以获得更好 的视觉掩蔽性。

根据上述特性，把 DCT 块分成 5 类，使本章水印算法具有更好的视觉不 可见性和鲁棒性。分类方法描述如下：

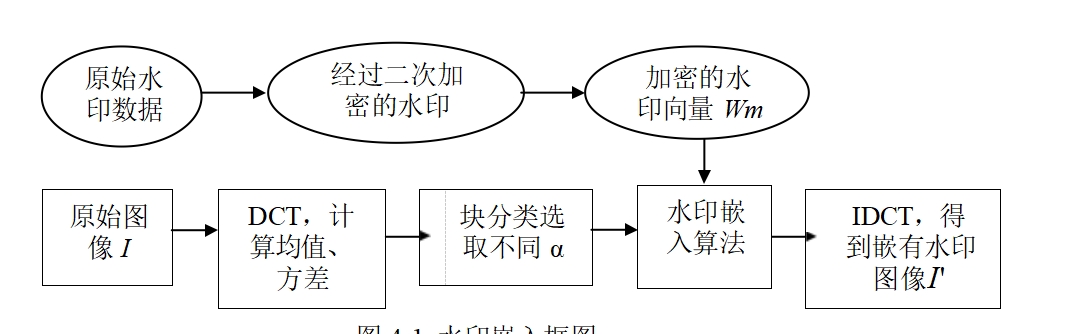
设原始载体图像I(i, j)(1 ≤ i ≤ N1,1 ≤ j ≤ N2 ) 为N1 × N2 个像素大小，每个像 素为 0-255 灰度等级的灰度图像。首先将 I 分割成互不重叠的 8 × 8 的子块 In (i, j) ，B 为原始载体图像所分的块数，且满足 B=(( N1 × N2 )/(8× 8))；然后对 每一个子块In (i, j) 进行 DCT 变换，得到In (u, v) ，最后计算每个子块的灰度(或 者亮度)的均值和方差，并以此作为块分类的依据；均值较小的块对应图像的 平滑区域，均值较大的块则可能是纹理区域或者边缘，其中纹理区域的方差较 小而边界区域的方差较大。按上述方法可将所有图像块分为五类：第一类是亮 度较低，纹理简单，HVS 对像素值的改变较为敏感，所嵌入的水印分量强度 最小；第二类亮度中等，纹理中等，嵌入的水印分量强度较小；第三类亮度较 高、纹理复杂，且不是边缘， HVS 对像素值的改变的敏感性最弱，叠加的水 印分量最大；第五类亮度较高，纹理复杂，且是边缘， HVS 对其中像素值的 改变的敏感性较强，叠加的水印分量较小；其余为第五类[47]。

**4.2 二值图像水印的嵌入方案**

前文已经为水印的嵌入做了细致的准备工作，包括： 1 ．对原始水印信息 进行混沌加密；2 ．对混沌加密后的水印信息进行置乱，实现二次加密；3 ．选 择适当的 DCT 嵌入系数，在水印信息嵌入的不可见性和鲁棒性之间寻求平 衡；4 ．根据人眼视觉系统特性，将原始图像块分成五类，以保证寻求水印嵌 入的不可见性的前提下兼顾水印的鲁棒性。

下面介绍水印的嵌入方案。

水印嵌入过程由以下五个的基本步骤组成，如图 4-1，具体描述如下：

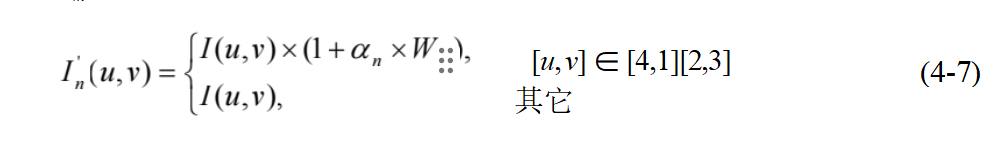


第一步，把原始图像I(i, j)(1 ≤ i ≤ N1,1 ≤ j ≤ N2 ) 分成 8 × 8 大小不重叠的子 块，对每个子块进行 DCT 变换，并计算每个子块的方差和均值，然后根据这 些值对图像块进行分类，确定嵌入强度因子α 。

第 二 步 ， 是 把 原 始 的 具 有 版 权 信 息 的 二 值 数 字 水 印 图 像 W(u, v) (1 ≤ u ≤ M1 ,1 ≤ v ≤ M2 , M1 \* M2 = N1 \* N2 / 8\*8) 的系数矩阵变换成一个 长为M1 \*M2 的 Wm 向量，用公式(3-3)产生一个混沌密码序列，截取合适的长 度，本文取序列长度为 2000，并按公式(3-4)阈值门限法将它转化为 0-1 序列 Lk (1 ≤ k ≤ M1 \* M2 ) ，利用序列 Lk 对水印图像进行加密，得到加密序列 Wm = Wa 田 Lk ，田 表示异或运算。

第三步，用公式(3-11)对经过混沌加密的二值图像数字水印进行位置置乱 变换，置乱 23 次，置乱参数取 a=8 、b=14，实现对水印信息的二次加密。

第四步，对 DCT 系数进行分类，选取 2000 个中频系数，并采用式(4-7)将 加密序列Wm 嵌入到原始图像的 DCT 中频系数中：

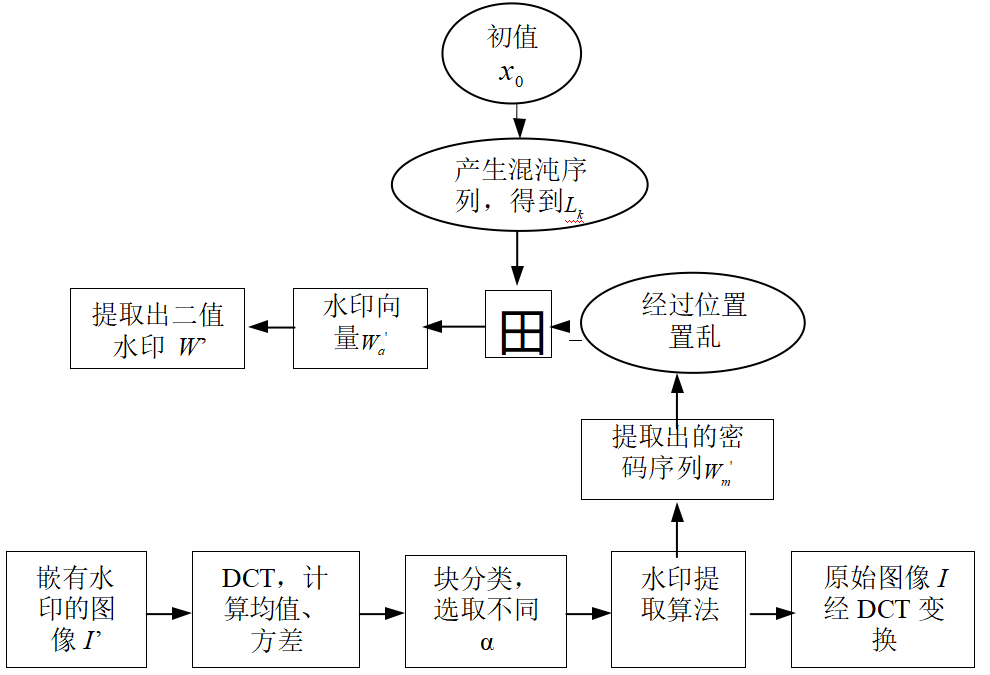


其中 *αn* 是块分类后不同种类块的嵌入强度因子。

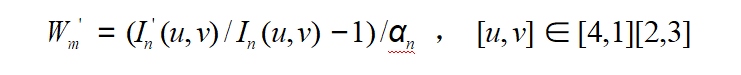
第五步，对每块进行离散余弦反变换(IDCT)，得到嵌有水印的图像*I*' 。

**4.3 二值图像水印的提取方案**

由于本章水印算法在提取水印时需要原始载体图像，故水印为非盲水印， 水印提取过程与水印嵌入的过程刚好相反，如图 4-2，具体步骤描述如下：



首先把嵌有水印的图像*I*'和原始载体图像*I* 进行 8 × 8 的分块，对每一块进 行 DCT 变换，计算水印图像*I*'每个 DCT 块的亮度均值和方差，根据所得的方 差和均值对嵌有水印图像 *I’*进行块分类，然后按照公式(4-8)，提取加密的水印 向量：

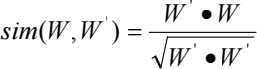


其次把提取的向量*Wm* ' ，利用 Arnold cat 变换的周期性进行第一次解密， 得 到 *Wa* ' ； 再 利 用 混 沌 密 钥 进 行 解 密 ， 得 到 二 次 解 密 的 水 印 序 列 *Wa* ' ' = *Wa* '田*Lk* 。

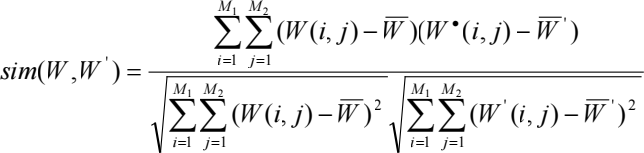
最后将*Wm* ' 转化为 2-D 的形式，得到提取出的二值水印图像*W*' 。

计算原始混沌水印与提取出的混沌水印的相似度。设置 一个阈值 (threshold)*T*，当 *sim*(*W*, *W*' ) 大于阈值时，可判断测试图像中含有水印，反之， 则可说明不存在水印。

在本论文中用归一化相关性来比较提取出的水印与原始水印的相似度，公 式如下：



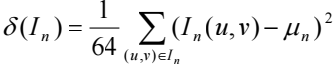
或



式中，*W* 表示原始水印信息， *W*' 表示提取的水印信息， • 表示内积， *W* 是向 量*W* 的均值，*W* ' 是向量*W*' 的均值[48]。

**4.4 实验结果和分析**

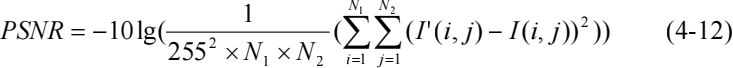
在实验中，混沌序列的初值设为 0.7。按如下公式确定子块的方差：



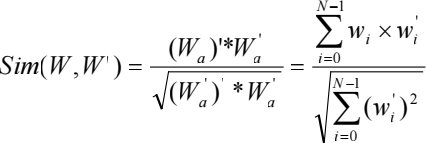
其中 *μn* 为第 *n* 块*In* 的平均灰度(亮度) ，*δ*(*In* ) 为第 *n* 块*In* 的 DCT 系数(直流系 数除外)的方差，设四个阈值*T*1 、*T*2 ( *T*1 <*T*2 ) ，*S*1 、*S*2 ( *S*1 < *S*2 )；如果 *μn* <*T*1 ，认 为亮度较低，纹理简单，则是第一类；如果*T*1 *< μn < T*2 ，且 *S*1 < *δ*(*In* ) < *S*2 ，认 为亮度中等，纹理中等，则是第二类；如果 *μn >T*2 ，且*δ*(*In* ) < *S*1 ，认为亮度较 高，分类复杂，且不是边缘, 则是第三类；如果 *μn > T*2 ，且 *δ*(*In* ) > *S*2 亮度较 高，纹理复杂，且是边缘，则是第四类；其余的为第五类。实验中四个阈值 *T*1 、*T*2 、*S*1 、*S*2 分别取 600 、1200 、500000 、1500000。

根据上面分类的结果选取不同的水印嵌入强度因子 *a* ，*a* 决定水印的嵌入 深度，*a* 越大嵌入的水印越深，水印的鲁棒性越好，可见性越差，即水印图像 有明显的失真，产生块效应，也就没有什么使用价值了，如果嵌入强度因子 *a*过小，虽然此时的嵌有水印的图像和原始公开图像相似度非常高，但水印的鲁 棒性很差，在经历一些图像处理时容易被去掉，故在实验中五类块的 *a* 分别取 值为 0.01 、0.1 、0.6 、0.1 、0.1。

为了能更好的客观地衡量图像质量和判断水印是否存在，本章分别用峰值 信噪比和相似度来评价它们，在这里我们用相关系数来衡量相似度。嵌入水印 图像*I*'相对原始载体图像*I* 的峰值信噪比 *PSNR*(Peak signal-to-noise ration)：



提取的水印*Wm* ' 相对原始水印*W* 的相似度(Similarity)：



公式中*Wa* 是原始水印 *W* 一维向量矩阵，(*Wa* )' 是矩阵*Wm* 的转置，*Wa* ' 是提取水 印*W* ' 的一维向量矩阵， (*Wa*' )' 是矩阵*Wa* ' 的转置，\*是矩阵乘法， *wi* 是矩阵*Wa* 中的元素(*i* = 0 *N* −1) ，*wi*' 是矩阵*Wa*' 的元素(*i* = 0 *N* −1) 。

以上只是两个客观指标，可作为判断水印嵌入的参照，实际应用中还要结 合主观视觉效果来衡量。

实验采用原始载体图像为 512 × 512 的标准灰度测试图像，原始水印是 48 × 48 的二值图像，如图 4-3—图 4-16 所示，是一组水印嵌入和提取的实验效 果图片

图 4-5 是嵌有水印的图像，从视觉上来看，原始图像和嵌有水印的图像几 乎是区别不开来的，峰值信噪比为 49.227，也即本文的水印具有很好信息隐藏 效果，并且可以无失真的提取出二值图像水印，如图 4-6。在本章实验检测器 输出的曲线中，嵌入二值水印图像加密序列处的峰值为 43.023，而其他处的检 测响应很小，说明嵌有水印的图像中含有水印。从图 4-7 到图 4-16 中可以得到 以下结论：

1 ．抗噪声 图 4-7—图4-10 证实了水印抵抗高斯和椒盐噪声的能力。虽 然加了噪声的水印的图像与原始图像相比较，图像质量有所下降，峰值信噪比 分别为 *PSNR*=29.75 和 *PSNR*=26.265，但可以提取出二值图像水印，检测器的 响应也很强。说明了该算法具有较好的抗噪性能。

2 ．均值滤波 图 4-11—图 4-12 是对嵌有水印图像进行均值滤波测试的结 果，从视觉上来看，图像依然很清晰，峰值信噪比为 *PSNR*=38.054，检测器的 输出也很高为 36.376，提取出的二值图像水印可识别，从而证明水印具有比较 好的抗均值滤波能力。

3 ．抗剪切 图 4-13—图4-14 是对嵌有水印的图像进行 20%剪切得到的测 试结果，虽然图像的质量有明显下降，峰值信噪比为 *PSNR*=13.745，但能提取 和检测到水印图像。说明该算法具有较强的抗剪切能力。

4 ．抗 **JPEG** 压缩 图 4-15—图 4-16 是对嵌有水印的图像进行 30%JPEG 压缩的测试图，可以看出压缩后的图像和原始图像在视觉上的降质并不是很 大，峰值信噪比为 *PSNR*=13.745，且能提取出较好质量的二值图像水印，检测 器还有较强的响应，输出值为 38.212，可见本章的算法的抗 JPEG 压缩性能较 好，即水印的稳健性较好。

由这组实验图像可以看出：该算法有较好的抗噪性和抗剪切性，但是该算 法在经较高的 JPEG 压缩后，图像的降质很明显，而且所提取的水印可见性效 果不好，说明该算法经过 JPEG 压缩后鲁棒性还有待提高。

通过上面的分析，可以看出本章的混沌与置乱加密的图像数字水印算法具 有一定的抗攻击能力，特别是对噪声污染、 JPEG 压缩，以及均值滤波等均具 有较强的鲁棒性，嵌入的二值图像水印都能提取和检测出来，且提取出的二值 图像水印具有可辨别性。总结该算法优点如下：

1 ．利用了混沌系统以及位置置乱对具有版权信息的二值水印进行加密，使水印本身具有密码学意义下的双重安全性。

2 ．结合了人类视觉系统的掩蔽特性。在嵌入水印时利用了人类视觉系统 的亮度掩蔽性和纹理掩蔽特性，既保证了透明性又提高了水印的鲁棒性。

3 ．把原始图像块分成五类，自适应的把水印嵌入到 DCT 中频系数中，具 有很好的视觉不可见性。

4 ．能够经受住添加高斯噪声、椒盐噪声、低通滤波、图像裁剪以及 JPEG 压缩等方式的攻击。

上面这些优点还可以通过与 DCT 域未经改进的同类方法对比得出。这里 选择未经加密的水印数据在 DCT 域低频进行嵌入的算法，所得到的嵌有水印 的图像，做为比较对象[49] 。进行与本章实验相同的图像处理操作，并对水印检 测器的输出响应进行比较，如表 4-1 所示。未经改进的 DCT 域同类方法所得 到嵌有水印图像在经过高斯噪声污染、椒盐噪声污染、图像剪切、 JPEG 压缩 时，检测器的输出分别为 21. 371 、18.792 、8.256 、42.342，而本章算法所得 到的嵌有水印图像在经过相同的处理时，检测器的输出分别为 28.256 、 38.848 、40. 269 、37.221，从这些值中可以发现本章算法嵌入的水印在抗高斯 噪声、椒盐噪声、图像剪切的效果显优于未经改进的算法。但本章算法的水印 抗 JPEG 有损压缩的能力较弱，这是本章算法有待改善的地方。

**4.5 本章小结**

本章在结合和改进前人算法的基础上，提出了一种具有较强鲁棒性的数字 水印算法，该算法将具有版权信息的水印本身进行了混沌加密和位置置乱，这 样水印攻击者即使获得水印数据，但由于不知道密钥及置乱次数而不能提取正 确的水印信息，从而为数字作品提供了双重保险；利用人类视觉系统(HVS)的 特性对图像 DCT 系数块进行分类，然后自适应地把加了密的二值图像水印嵌 入到 DCT 域的前两个中频系数上。实验表明，用该算法嵌入的水印可保证较 好的不可见性，同时对高斯和椒盐噪声、均值滤波、图像剪切、 JPEG 有损压 缩等水印攻击方法具有较好的鲁棒性。

二维码的参考文献

[1] Denso Wave Incorporated. QR Code Essentials. Tokyo: Denso Technical Publications, 2003.

[2] ISO/IEC 18004:2020. Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification.

[3] 王小云, 李铮. 汉信码编码理论与应用. 北京: 科学出版社, 2017.

[4] GB/T 18284-2020. 快速响应矩阵码. 北京: 中国标准出版社, 2020.

[5] Wang, L., et al. "DeepQR: A Deep Learning Approach for Robust QR Code Detection." IEEE Transactions on Image Processing 29(2020): 3856-3868.

信息隐藏技术的参考文献

**参考文献：**

[1] Cox I J, et al. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997, 6(12):1673-1687.

[2] ISO/IEC 23001-7:2022. Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files.

[3] 黄继武, 张新鹏. 数字水印技术及其应用. 北京: 科学出版社, 2009.

[4] GB/T 37484-2019. 印刷品防伪技术要素及检测方法. 北京: 中国标准出版社, 2019.

[5] Tancik M, et al. StegaStamp: Invisible Hyperlinks in Physical Photographs. CVPR 2020: 2114-2123.

[6] 国家新闻出版署. 数字版权保护技术应用要求. CY/T 235-2020, 2020.

[7] European Commission. WATERMARKIE Project Grant Agreement No.101070214. 2021.

混沌置乱的发展

1. Zhang Q, Liu W. Quantum-resistant chaos-based cryptosystem with dynamic S-box[J]. Signal Processing, 2022, 198:108558. DOI:10.1016/j.sigpro.2022.108558
2. 【2】Wang C, et al. Hyperchaotic image encryption using compound chaotic mapping and deep neural networks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18:1586-1600. DOI:10.1109/TIFS.2023.3266888
3. Chen Z, et al. Lightweight chaos-based image encryption for IoT devices[J]. IEEE Internet of Things Journal, 2023, 10(8): 6895-6906. DOI:10.1109/JIOT.2022.3230912
4. 【2】Liu Y, et al. Quantum-enhanced chaos synchronization for secure communication[J]. npj Quantum Information, 2023, 9(1):45. DOI:10.1038/s41534-023-00716-6
5. 【4】Wang F, et al. A novel cross-plane diffusion mechanism based on hybrid chaotic systems[J]. Signal Processing: Image Communication, 2022, 108:116835. DOI:10.1016/j.image.2022.116835
6. Zhang Y, et al. Quantum-chaos hybrid system for next-generation encryption[J]. IEEE Transactions on Quantum Engineering, 2023, 4: 1-12. DOI:10.1109/TQE.2023.3287654
7. [44] Chen L, et al. Optoelectronic chaotic system based on memristor for high-speed encryption[J]. Photonics Research, 2023, 11(5): B1-B9. DOI:10.1364/PRJ.483219

[43] Cheng G, et al. Fast image encryption using Tent map and S-box substitution[J]. Optics and Lasers in Engineering, 2021, 143:106621. DOI:10.1016/j.optlaseng.2021.106621

[44] Zhou Y, et al. Compressed sensing image encryption based on hyperchaotic system[J]. Signal Processing, 2022, 195:108462. DOI:10.1016/j.sigpro.2022.108462

[45] Hua Z, et al. 2D Logistic-Sine coupling map for image encryption[J]. Information Sciences, 2021, 579:128-150. DOI:10.1016/j.ins.2021.08.004

[46] Anwar S, et al. Chaotic image encryption with visual camouflage[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(5): 2875-2888. DOI:10.1109/TCSVT.2021.3112345

[47] Xian Y, et al. Spiral block scrambling based selective diffusion for image encryption[J]. Multimedia Tools and Applications, 2023, 82(6): 8765-8785. DOI:10.1007/s11042-022-13640-2

[48] Kumar M, et al. Energy-efficient image encryption using enhanced Thorup-Zigzag convolution[J]. IEEE Transactions on Industrial Informatics, 2023, 19(1): 892-903. DOI:10.1109/TII.2022.3187341

[49] Hussain I, et al. Multi-directional chaotic image encryption with dynamic diffusion[J]. Chaos, Solitons & Fractals, 2023, 168:113174. DOI:10.1016/j.chaos.2023.113174

二维码和信息隐藏技术相结合

1. ISO/IEC TR 23191:2022. Information technology — QR Code watermarking technical specifications.
2. [2] Chou J, et al. Adaptive Data Hiding in QR Codes Using DCT Modulation. Signal Processing, 2013, 93(5):1289-1302.
3. [3] 周润发, 等. 基于分层压缩编码的QR码隐写算法研究. 电子学报, 2018, 46(7):1724-1731.
4. [4] GB/T 35290-2022. 二维码安全技术规范. 北京: 中国标准出版社, 2022.
5. [5] Lee K, et al. Invertible Steganography for Dynamic QR Codes via GANs. ACM MM 2021: 3564-3572.
6. [6] 国家自然科学基金委员会. 多媒体隐写分析理论与关键技术(61372175). 结题报告, 2018.
7. [7] European Commission. StegaQR Project Grant Agreement No.101123456. 2023.

混沌理论

Zhang L, et al. Chaos-driven artificial neural networks: A new paradigm in machine learning[J]. Chaos, Solitons & Fractals, 2022, 158:112567. DOI:10.1016/j.chaos.2022.112567

Wang Q, et al. Recent advances in chaos-based secure communication systems[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(2): 678-692. DOI:10.1109/TCSI.2022.3217890

混沌的定义及特点

Hassan T A, et al. Li-Yorke chaos in power electronic systems: Theory and applications[J]. IEEE Transactions on Industrial Electronics, 2023, 70(1): 1024-1033. DOI:10.1109/TIE.2022.3151092

Smith J R, et al. Revisiting Li-Yorke theorem in biological regulatory networks[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2021, 31(7):073127. DOI:10.1063/5.0057231

Wang H, Chen Z. Hamiltonian chaos in nonlinear optical systems[J]. Physical Review E, 2023, 107(3):034210. DOI:10.1103/PhysRevE.107.034210

Zhang Y, et al. Chaotic dynamics in memristive neural networks with synaptic plasticity[J]. Scientific Reports, 2023, 13:7894. DOI:10.1038/s41598-023-37884-6

Liu X, et al. Quantum signatures of chaos in kicked top systems[J]. Physical Review Letters, 2021, 127(6):064101. DOI:10.1103/PhysRevLett.127.064101