



中国矿业大学
CHINA UNIVERSITY OF MINING AND TECHNOLOGY

本科生毕业设计（论文）

抗几何失真的鲁棒数字水印的研究与实现
Research on Robust Digital Watermarking
Resilient to Geometric Distortion

作 者：丁锦扬
导 师：韩丽霞

中国矿业大学
2020 年 6 月

中国矿业大学

本科生毕业设计（论文）

抗几何失真的鲁棒数字水印的研究与实现
Research on Robust Digital Watermarking
Resilient to Geometric Distortion

作者 丁锦扬 学号 08163324
导师 韩丽霞 职称 讲师
学院 计算机科学与技术学院 专业 信息安全

二〇二〇年六月

毕业论文原创性声明

本人郑重声明：所呈交的毕业论文《抗几何失真的鲁棒数字水印的研究与实现》，是本人在指导教师指导下，在中国矿业大学攻读学位期间进行的研究工作所取得的成果。据我所知，除文中已经标明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。本人完全意识到本声明的法律结果由本人承担。

作者签名：

年 月 日

致谢

逝者如斯夫，不舍昼夜。四年的本科生涯即将画上句号，值此毕业论文几易其稿，不断完善，最终形成之际，回顾这四年的求学经历，心中思绪万千。

首先感谢我的毕业设计指导老师——韩丽霞老师。在这几个月的时间里，韩老师给了我很多关心与指导。在程序编写时，韩老师耐心地与我讨论在过程中遇到的问题，并为我理清思路。在初稿形成时，韩老师也非常细致地帮我逐字逐句修改论文，指出了不少问题，不辞辛劳地多次与我沟通交流，让我得以顺利完成论文的撰写。

感谢我的研究生导师——张卫明老师。张老师在百忙之中抽出时间与我交流选题，并提出了对我非常有帮助的建议。张老师严谨的治学态度、严密的学术思维也使我受益匪浅。

感谢张立江老师，带领我踏入信息安全领域，在学习、竞赛、生涯规划上给了我很大鼓励与帮助。

感谢研究生课题组的马泽华师兄。毕业设计的一切内容对我来说都是新的尝试，在此期间，我遇到了很多困难与挑战，师兄都非常耐心地为我的答疑解惑。

感谢即将成为我母校的中国矿业大学，这个承载着我四年青春奋斗拼搏的地方。在这里，我遇见了许多良师益友，他们在成长路上给了我很大帮助。矿大也给予了我优良的学习、生活环境与平台，使我能与梦想中的瀚海星云如此接近。在今后的旅途中，我将一直秉持“开拓创新，严谨治学”的校训，不断奋进拼搏。

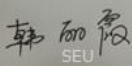
感谢父母一直以来对我的关心与支持，让远在千里之外的我感受到家庭的温暖，能够以饱满的热情投入到学习中。

感谢特殊时期所有奋战在一线的“最美逆行者”。

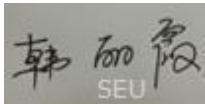
感谢自己的一路坚持与努力。

求知的道路依然漫长，让我们永远坚持走向上的路，追求正义和智慧。

中国矿业大学本科毕业设计（论文）任务书

| | | | |
|--|------------|------|----------|
| 设计（论文）题目： <u>抗几何失真的鲁棒数字水印的研究与实现</u> | | | |
| 学院 | 计算机科学与技术学院 | 专业年级 | 信息安全 |
| 学生姓名 | 丁锦扬 | 学号 | 08163324 |
| <p>1、设计（论文）的主要内容</p> <p>针对数字水印难以抵抗几何攻击的实际问题进行研究，设计抗几何失真的鲁棒数字水印方案。主要研究内容包括：</p> <p>(1) 设计一种数字水印方案，从嵌入策略和水印结构两方面保证水印算法对常见图像处理和几何失真的鲁棒性；</p> <p>(2) 对常见标准测试图测试数字水印方案的有效性，并优化水印方案；</p> <p>(3) 对数字水印方案的测试结果进行分析和总结。</p> | | | |
| <p>2、设计（论文）的基本要求</p> <p>(1) 通过查阅相关文献和资料，掌握常见数字水印算法和数字图像处理相关的基础知识；</p> <p>(2) 熟悉数字水印领域中比较常见的对几何失真鲁棒的数字水印方案；</p> <p>(3) 设计具有鲁棒性的数字水印方案，并实现该水印方案；</p> <p>(4) 对设计的数字水印方案，在常见标准测试图进行测试，并进行优化；</p> <p>(5) 根据测试结果,对该水印方案及测试结果进行分析和总结；</p> <p>(6) 撰写毕业论文,完成毕业答辩。</p> <div style="text-align: right; margin-top: 100px;"><p>指导教师签字： </p></div> | | | |

中国矿业大学毕业（设计）论文指导教师评阅书

| | | | |
|--|--------------------|---|----------|
| 学生姓名 | 丁锦扬 | 学号 | 08163324 |
| 设计（论文）题目 | 抗几何失真的鲁棒数字水印的研究与实现 | | |
| <p>指导教师评语（①基础理论及基本技能的掌握；②独立解决实际问题的能力；③研究内容的理论依据和技术方法；④取得的主要成果及创新点；⑤工作态度及工作量；⑥总体评价及建议成绩；⑦存在问题；⑧是否同意答辩等）：</p> <p>该生掌握了常见数字水印算法和数字图像处理相关的基础知识，熟悉比较常见的对几何失真鲁棒的数字水印方案，基础理论知识扎实。根据 ULPM 映射表将水印嵌入到载体图像的 DFT 幅度谱中，水印提取算法通过与跟踪模式做互相关运算来定位水印。对标准测试图数据库中 8 幅具有代表性的图像测试结果表明，提出的水印方案具有良好的不可见性、计算效率。</p> <p>该生在毕业设计期间，工作态度非常认真，对遇到的难点进行积极有效的讨论，能够利用所学的知识独立解决问题，体现了一定的科研能力。论文工作量比较充实，撰写的论文符合本科生毕业论文规范，建议成绩优秀。</p> <p>同意答辩。</p> | | | |
| 成 绩： 97 | | 指导教师签字：  | |
| 2020 年 6 月 10 日 | | | |

中国矿业大学毕业设计（论文）评阅教师评阅书

| | | | |
|---|--------------------|---|----------|
| 学生姓名 | 丁锦扬 | 学号 | 08163324 |
| 设计（论文）题目 | 抗几何失真的鲁棒数字水印的研究与实现 | | |
| <p>评阅教师评语（①选题的意义；②基础理论及基本技能的掌握；③综合运用所学知识解决实际问题的能力；④工作量的大小；⑤取得的主要成果及创新点；⑥写作的规范程度；⑦总体评价及建议成绩；⑧存在问题；⑨是否同意答辩等）：</p> <p>论文选题具有应用与理论价值。论文实现了基于均匀对数极坐标映射(ULPM)鲁棒盲水印框架。水印嵌入后，在空域进行失真补偿，提升了不可见性。使用了纠错编码、扩频技术提高了水印的鲁棒性。编程实现了具有水印嵌入、水印提取、图像模拟攻击、水印性能测试的实验系统。论文反映出作者掌握了信息安全的基础理论知识，具有较强的解决实际问题的能力。工作量适中，论文结构清晰，写作规范。总体评价优秀。</p> <p>同意答辩。</p> | | | |
| 成绩： 90 | | 评阅教师签字：  | |
| 2020 年 6 月 7 日 | | | |

中国矿业大学毕业设计答辩及综合成绩

| 答 辩 情 况 | | | | | |
|---|---------|------------------|----------------------------|----------------------------|------------------|
| 提 出 问 题 | 回 答 问 题 | | | | |
| | 正 确 | 基 本 正 确 | 有 一 般 性 错 误 | 有 原 则 性 错 误 | 没 有 回 答 |
| 水印嵌入的容量是多少？ | √ | | | | |
| 水印嵌入与提取的计算复杂性如何？ | √ | | | | |
| 攻击者是否能够删除水印？ | √ | | | | |
| 对嵌入水印的图像进行失真补偿对水印质量的影响是多大？ | √ | | | | |
| 等比例缩放，是否考虑不等比例的缩放？ | √ | | | | |
| <p>答辩委员会评语及建议成绩：</p> <p>论文围绕鲁棒数字水印展开研究，选题有较好的实用价值，作者综合运用了数字水印和密码技术，设计并开发了一个抗几何失真的鲁棒数字水印软件，具备了水印嵌入、水印提取、抗攻击测试等功能，工作量饱满。设计的软件在答辩演示中能够正常运行，功能设计合理，达到了设计方案中的要求，在设计思路 and 具体实现上，作者创新性地提出在空域进行失真补偿，使用纠错编码、扩频技术提高水印的鲁棒性，具备较强的本专业工程项目管理能力。答辩过程中思路清晰，对老师题提出的问题能够充分回答，阐述问题正确、逻辑性强。论文总体结构合理、逻辑清楚、格式规范。很好地达到了毕业设计的要求。</p> <p>成绩： 96</p> <p>答辩委员会主任签字：曹天杰</p> <p>2020 年 6 月 10 日</p> | | | | | |
| 成绩评定： | | | | | |
| 成绩组成 | 指导教师 | 评阅教师 | 答辩成绩 | 其他 | 总评 |
| 成绩比例 | 30% | 20% | 50% | 0% | 优秀 |
| 评分 | 97 | 90 | 96 | 0 | |
| <p>学院领导签字：林学国</p> <p>2020 年 6 月 10 日</p> | | | | | |

摘 要

随着互联网的迅速发展,数字多媒体信息已成为人们生活中不可或缺的组成部分,随之而来的版权问题日益凸显。数字水印技术将一段特定的信息即水印嵌入到载体信息中,为版权所有者提供所有权证明,是解决版权问题的一种重要方法。

本课题实现了基于均匀对数极坐标映射(ULPM)的鲁棒盲水印框架,并完善了其细节,优化了算法流程和参数取值。用于嵌入的水印由两部分组成:消息序列和跟踪序列。水印嵌入算法根据 ULPM 映射表将水印嵌入到载体图像的 DFT 幅度谱中。水印提取算法通过互相关运算来定位水印,从而提取出其携带的消息。水印嵌入端与水印提取端只需要共享一个密钥,就能实现水印的盲提取。在嵌入水印后,基于人类视觉系统的掩蔽特性在空域进行失真补偿,以提升其不可见性;使用纠错编码、扩频技术,以满足其鲁棒性。在此基础上,设计并实现了一个水印综合评估系统,从标准测试图数据库中选取了 8 幅具有代表性的图像作为测试图像集。实验结果表明,提出的水印方案具有良好的不可见性、计算效率。对质量因数为 20 以上的 JPEG 压缩、滤波器大小为 3×3 的高斯滤波等简单攻击,任意角度的旋转、缩放因子为 0.75~1.40 的等比例缩放、比例为 45%以上的裁剪等几何攻击具有良好的鲁棒性。

该论文有图 23 幅,表 12 个,参考文献 31 篇。

关键词: 信息隐藏; 数字水印; 几何攻击; 均匀对数极坐标映射; 失真补偿

Abstract

With the rapid development of the Internet, digital multimedia information has become an indispensable part of people's lives, and the copyright issues are becoming increasingly prominent. As an important method to solve the copyright problem, digital watermarking technology embeds a specific piece of information named watermark into the carrier information, which can provide proof of ownership for the copyright owner.

The robust blind watermarking based on uniform log-polar mapping (ULPM) is implemented, the details are improved, and the algorithm flow and parameter values are optimized. The watermark used for embedding consists of two parts: informative sequence and tracking sequence. The watermark embedding algorithm embeds the watermark into the DFT amplitude spectrum of the carrier image according to the ULPM mapping table. The watermark extraction algorithm locates the watermark by performing cross-correlation operation, and the message is extracted. The watermark embedding end and the watermark extraction end only need to share one key to realize the blind extraction of the watermark. In order to improve the invisibility, distortion compensation is performed in the spatial domain based on the masking characteristics of the human visual system after embedding the watermark, while error correction coding and spread spectrum technology are used to improve the robustness of the watermark. Based on these, a watermark comprehensive evaluation system is designed and implemented. Eight representative images are selected from the standard test images database as the test image set. The experimental results demonstrate that the proposed watermarking scheme has good invisibility and computational efficiency. And the watermark is robust to common signal processing such as JPEG compression with a quality factor of 20 or higher, Gaussian filtering with a filter size of 3×3 , and so on. It is also robust to common geometrical attacks such as rotation at any angle, proportional scaling with a scaling factor of 0.75 to 1.40, and cropping with a ratio of more than 45%.

The thesis has 23 figures, 12 tables, and 31 references.

Keywords: information hiding; digital watermarking; geometric attacks; uniform log-polar mapping; distortion compensation

目 录

| | |
|---------------------------|-----------|
| 摘要..... | i |
| 目录..... | iii |
| 1 绪论..... | 1 |
| 1.1 研究背景及意义..... | 1 |
| 1.2 国内外研究现状..... | 2 |
| 1.3 研究内容和创新点..... | 3 |
| 1.4 论文组织结构..... | 4 |
| 2 相关概念与技术 | 5 |
| 2.1 数字水印技术的基本理论..... | 5 |
| 2.2 傅里叶变换与图像频域..... | 12 |
| 2.3 对数极坐标映射..... | 13 |
| 2.4 互相关与互相关定理..... | 14 |
| 2.5 本章小结..... | 15 |
| 3 水印嵌入算法 | 17 |
| 3.1 水印生成..... | 18 |
| 3.2 零延拓..... | 18 |
| 3.3 在傅里叶幅度谱中应用 ULPM | 19 |
| 3.4 嵌入水印..... | 21 |
| 3.5 空域失真补偿..... | 22 |
| 3.6 纠错方案..... | 23 |
| 3.7 本章小结..... | 24 |
| 4 水印提取算法 | 25 |
| 4.1 水印重同步..... | 25 |
| 4.2 解扩频和解码..... | 28 |
| 4.3 本章小结..... | 28 |
| 5 系统测试与优化 | 29 |
| 5.1 测试环境及测试图像集..... | 29 |
| 5.2 数字水印性能评估模型..... | 30 |
| 5.3 零延拓对水印的优化..... | 33 |

| | |
|-----------------------|-----------|
| 5.4 基准频率的取值..... | 33 |
| 5.5 空域失真补偿对水印的优化..... | 34 |
| 5.6 嵌入强度的取值..... | 36 |
| 5.7 优化后水印的性能..... | 36 |
| 5.8 本章小结..... | 40 |
| 6 总结与展望 | 41 |
| 6.1 全文总结..... | 41 |
| 6.2 未来展望..... | 42 |
| 参考文献 | 43 |
| 翻译部分 | 45 |

Contents

| | |
|--|-----------|
| Abstract..... | ii |
| Contents | v |
| 1 Introduction..... | 1 |
| 1.1 Research Background and Significance..... | 1 |
| 1.2 Research Status at Home and Abroad | 2 |
| 1.3 Research Contents and Innovations | 3 |
| 1.4 The Organizational Structure of the Thesis | 4 |
| 2 Related Concepts and Technologies | 5 |
| 2.1 The Basic Theory of Digital Watermarking | 5 |
| 2.2 Fourier Transform and Image Frequency Domain..... | 12 |
| 2.3 Log-Polar Mapping..... | 13 |
| 2.4 Cross-correlation and Cross-correlation Theorem..... | 14 |
| 2.5 Chapter Summary | 15 |
| 3 Watermark Embedding..... | 17 |
| 3.1 Watermark Generation | 18 |
| 3.2 Padding with Zeros | 18 |
| 3.3 Applying ULPM to the Fourier Magnitude Spectrum | 19 |
| 3.4 Embedding the Watermark..... | 21 |
| 3.5 Spatial Distortion Compensation | 22 |
| 3.6 Error Correction Scheme | 23 |
| 3.7 Chapter Summary | 24 |
| 4 Watermark Extracting | 25 |
| 4.1 Watermark Resynchronization | 25 |
| 4.2 Despreading and Decoding | 28 |
| 4.3 Chapter Summary | 28 |
| 5 Testing and Optimization..... | 29 |
| 5.1 Test Environment and Image Set | 29 |
| 5.2 Performance Evaluation Model of Digital Watermarking | 30 |
| 5.3 Optimization by Padding with Zeros | 33 |

| | |
|--|-----------|
| 5.4 The Value of the Base Frequency..... | 33 |
| 5.5 Optimization by Spatial Distorstion Compensation | 34 |
| 5.6 The Value of the Embedding Strength | 36 |
| 5.7 Performance of Optimized Watermarking Scheme..... | 36 |
| 5.8 Chapter Summary | 40 |
| 6 Conclusions and Prospects | 41 |
| 6.1 Conclusions..... | 41 |
| 6.2 Prospects | 42 |
| References | 43 |
| Translation..... | 45 |

1 绪论

1 Introduction

1.1 研究背景及意义(Research Background and Significance)

随着互联网的普及与多媒体技术的高速发展,数字多媒体信息的存储、传播越来越便捷,并已成为人们生活、工作中一个不可或缺的组成部分。然而,这些信息极易被无限制地恶意篡改、非法复制与散布,版权和隐私问题日益凸显,在图像、音频、视频等多媒体信息上尤为严重。例如,盗版者只需通过非常简单的复制粘贴操作,就可以获得高质量甚至是与原版一模一样的复制品,从而牟取暴利。这些非法行为不仅严重侵害了版权所有者的利益,也给网络空间安全造成了极大的影响。如有涉密信息(国家机密、法庭证据、商业机密等)遭到非法泄露或篡改,极有可能对个人或社会带来极其严重的损失,甚至会对国家安全造成威胁。如何既享受互联网与信息技术带来的红利,又有效保护多媒体信息的版权,逐渐被提上日程。

数字水印技术(digital watermarking)就是针对这个问题的常见解决方案之一。它的基本思想是将特定的信号(如序列号、图像等),即水印(watermark)以某种特定的方式嵌入到数字载体信号的某个特定的域中。水印一般是不易被人们所感知的,即不会影响原始数字信息的内容和使用。若有人试图拷贝已被嵌入水印的信息时,水印信息也会一并被拷贝。在需要时,只有通过特定的方法才能提取或检测出之前嵌入的水印,从而起到所有权证明的作用。然而,水印在嵌入到数字载体后,可能会遭受各种无意或有意的攻击。无意的攻击包括存储及传输过程中的信号处理给信息带来的损失、噪声,而有意的攻击则可能来源于恶意用户想方设法去除水印。数字水印主要的研究目的之一是使得信息载体中的水印不能轻易被去除^[1]。

目前,图像数字水印技术主要是将水印嵌入到图像的空域或频域中,从综合性能来看,空域水印计算速度一般较快,但抵抗各种攻击能力较差,因此应用场合比较受限;而频域水印抗干扰能力强,对常见信号处理及其他攻击都有较强的免疫力,占据了重要地位。

一个好的数字水印方案应当是鲁棒的,即拥有对各种攻击的抵抗能力。常见的攻击有简单攻击(简单图像处理)、几何攻击、混淆攻击、擦除攻击等。在众多水印攻击方法中,几何攻击(geometric attacks)是最有效的方法之一,这种攻击一般通过旋转、缩放、平移、裁剪(rotation, scaling, translation, and cropping, RSTC)等几何变换方法,破坏水印信号与载体信号之间原有的同步性,使得水印提取端

难以恢复水印。现有的数字水印技术大多数只具有对一般信号处理攻击的鲁棒性，对能抵抗几何攻击的数字水印的研究仍是目前数字水印研究中最困难的课题之一[2]。

1.2 国内外研究现状(Research Status at Home and Abroad)

近几十年来，学者们提出了许多能抵抗几何攻击的图像数字水印方案，大致可以将它们分为两类：第一类是基于几何失真校正的方法，第二类是基于几何不变性(不变量)的方法。

基于几何失真校正的方法的基本思路是：在提取水印前先检测图像所经历几何变换的系数，然后对图像进行相应的反变换，那么水印信号和载体信号就可以恢复同步。刘九芬等^[3]在提取水印时将原图作为参考，利用图像配准技术恢复待检图像的几何变形。还有一种思路是在嵌入水印的同时嵌入一个模板，它可以跟踪并记录下图像在存储、传输过程所经历的几何变换。Braudaway 等^[4]提出了基于参考点最佳匹配的方法，在原图和包含水印的图像中分别选取多个参考点，然后枚举出所有可能的变换，找到它们的最佳匹配。Lu 等^[5]使用基于尺度交互模型的滤波器提取原始图像中的特征点，通过计算水印与嵌入区域的统计相关性将水印自适应地嵌入到特征点所定位的局部区域中。这些方法的共同之处是最终得到了图像所经历的几何变形系数，在提取时一般需要原始图像或辅助模板，否则将导致无法定位水印，其适用范围也较小，通常难以抵抗比较复杂的几何攻击，如局部扭曲、剪切等。

基于不变性的方法的基本思路是：将水印嵌入在几何变换不变域中，这样，即使图像遭受了几何变换，水印信息也还能正确恢复。O'Ruanaidh 等^[6]构建了几何变换不变量的相关理论，为抵抗 RSTC 攻击做铺垫。该算法①首先计算图像的 DFT(离散傅里叶变换)幅度谱，这一操作使得水印可以抵抗平移变换。②接着对 DFT 幅度谱做 LPM(对数极坐标映射)，这一过程可将原图像上的缩放和旋转变换简化为平移变换。③最后再取 DFT 幅度谱，经历 DFT-LPM-DFT 这一系列变换后得到的这个域具有 RST 不变性，水印的嵌入与提取也是在这个域中进行的。然而，该算法运算量较大，而且在该域嵌入水印之后，将其反变换回来时经历了 ILPM(LPM 的反变换)，严重降低了图像质量，所以并不能满足实际需求。基于此，文献[7-10]提出了相关的改进。Lin 等^[7]在 DFT 幅度谱做 LPM，再沿着对数极半径轴 $\log(r)$ 方向将 DFT 系数求和，从而得到一个一维序列，在这个序列上嵌入和提取水印，具有较好的鲁棒性，但水印容量仅为 1 比特。Kim 等^[8]则提出对图像先进行 LPM，再做 DFT，在其幅度谱上嵌入水印，该算法在感知重要的频带上嵌入水印，并且保持了较好的图像质量。Zheng 等^[9]结合相位相关，通过避免计算 ILPM 来保持图像质量。LPM 的好处是将较为复杂的旋转、缩放变换简

化为平移变换,从而使定位水印变得更快、更简单,但它也存在着局限性,它引入了对数运算,而 LPM 前后信号都是离散的,所以可能带来数据量压缩,从而严重影响图像质量。Kang 等^[10]通过控制对数的底数,提出了基于 ULPM(Uniform Log-Polar Mapping, 均匀对数极坐标映射)的水印方案,通过 ULPM 映射表将水印嵌入到图像的 DFT 系数中,既充分利用了 LPM 简化水印模型,又避免了 LPM 所带来的局限性,能抵抗 RSTC 变换、一般打印扫描等攻击,具有较为出色的鲁棒性。由于 DFT 幅度谱具有平移不变性等良好特性,而 LPM 又能简化旋转、缩放变换,所以很多水印方案都是利用它们的组合。除此之外,还有基于图像归一化的算法^[11-13],通过一些处理将图像变换为预定义的标准形式,在标准形式中嵌入或提取水印;基于几何不变性图像特征点的算法^[14-16],在图像感知相对重要的区域嵌入水印,并用特征点标记出嵌入区域;基于奇异值分解(SVD)的算法^[17,18],利用了奇异值对微小的失真的鲁棒性这个重要特性。

与第一种方法相比较,基于几何不变量的方法充分利用了图像自身的属性,在提取时所需要的信息较少,能较好地实现水印的盲提取,且在鲁棒性、算法复杂性上都有很大进步,今后可能成为数字水印技术的主流研究方向。

1.3 研究内容和创新点(Research Contents and Innovations)

本课题系统地研究了数字水印技术的基本理论、相关方法与手段、常见攻击方式及性能评价标准,旨在设计一种不可见性良好、计算效率高、能有效抵抗几何攻击的水印方案。研究的主要内容包括:

- 1) 再现了文献[10]提出的基于 ULPM 的水印嵌入算法、水印提取算法,并完善了其流程细节;
- 2) 为测试水印方案的鲁棒性,实现了图像模拟攻击程序,可以对包含水印的图像进行各种常见简单攻击、几何攻击以及两者的组合;
- 3) 为评估水印的综合性能,对常用于评估水印性能的关键指标进行了建模,设计并实现了能够自动输出对水印综合评价的水印性能评估系统;
- 4) 结合模型测试结果,对水印算法流程做出了优化,如:①读取图像后,首先进行零延拓,以提升其频域的计算分辨率,尽可能防止水印嵌入时水印位就直接丢失的现象;②结合人类视觉系统的掩蔽特性,引入空域失真补偿方法,提升水印的不可见性;③水印重同步前,对跟踪区域做两个方向上的标准化操作,以弱化强背景对提取水印带来的影响。此外,还对算法流程中涉及到的重要参数的取值做了测试、对比、分析,以最终获得接近最优的综合性能。

1.4 论文组织结构(The Organizational Structure of the Thesis)

本文共分为 6 章，余下各个章节的内容安排如下：

第 2 章：相关概念与技术。这一章属于基础章节，介绍了数字水印技术的重要概念。并引出了与本课题设计实现的数字水印系统高度相关的傅里叶频域、对数极坐标变换、互相关的基础理论。

第 3 章：水印嵌入算法。先给出了本课题实现的水印嵌入算法的过程示意图，再对过程中涉及到的处理方法进行详细说明。

第 4 章：水印提取算法。与第 3 章类似，先给出了水印提取算法的过程示意图，再对过程涉及的处理方法进行详细说明。

第 5 章：系统测试与优化。为量化评估数字水印方案的综合性能，基于计算效率、不可见性、鲁棒性提出了综合评估模型，以表格的形式给出了水印各方面的测试结果，以便于对水印方案进行测试、对比、优化。从而直观展现零延拓、空域失真补偿对水印的优化效果。并针对水印方案涉及的几个重要参数如基准频率、嵌入强度的不同取值对水印的影响进行了测试，以最终实现水印不可见性、鲁棒性以及效率之间的良好折衷。

第 6 章：总结与展望。对研究内容、所做工作以及创新点进行总结，对未来进一步研究做了展望。

2 相关概念与技术

2 Related Concepts and Technologies

文献[10]提出了一种基于 ULPM 的水印方案，用于嵌入的水印由消息序列与跟踪序列两部分构成，水印嵌入算法通过 ULPM 映射表将水印嵌入到图像的 DFT 幅度谱中，提取算法通过互相关定位水印。这个方案既简化了提取时跟踪定位水印的过程，又避免了 LPM 所带来的不必要的失真，具有较为出色的不可见性、鲁棒性、计算效率。

本文再现了文献[10]提出的水印框架，完善了流程细节，并对算法流程和参数做了优化。因此有必要对数字水印技术、傅里叶变换、对数极坐标映射、互相关等基本理论知识进行介绍。

2.1 数字水印技术的基本理论(The Basic Theory of Digital Watermarking)

2.1.1 数字水印系统模型

数字水印技术通常是指将特定的序列号、图像等表示数据(即水印信息)嵌入到载体信息中，这个过程可视为在强背景(信息载体)上加入弱信号(水印)^[1]。数字水印技术之所以能够实现，主要是因为人类视觉系统(human visual system, HVS)具有一些掩蔽特性，比如，①HVS 对图像高频分量上的噪声较不敏感；②图像纹理越复杂，HVS 就越无法感受到噪声的存在；③HVS 对图像很亮或很暗的区域上的噪声较不敏感^[19,20]。

通用的数字水印系统主要由水印嵌入端(用于将水印嵌入到原始信息中)、水印提取或检测端(用于从包含水印的信息中提取或检测水印)两个部分组成。

A. 水印嵌入系统

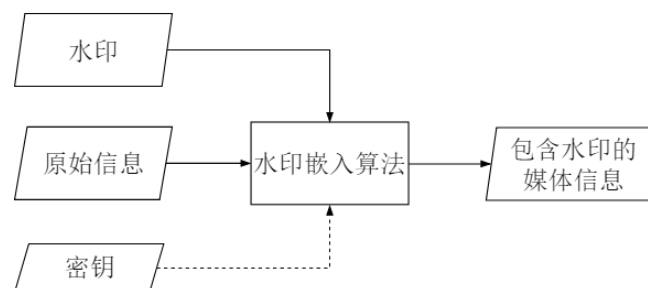


图 2-1 水印嵌入系统

Figure 2-1 Simplified model of watermark embedding system

图 2-1 给出了水印嵌入系统的框架模型。水印嵌入算法将输入的水印嵌入到原始信息中，有时也会引入密钥，以实现水印提取者身份认证的目的。

常用的嵌入公式有两种,加性准则和乘性准则,分别如公式(2-1)、(2-2)所示。

$$I_w(x, y) = I(x, y) + \alpha W(x, y) \quad (2-1)$$

$$I_w(x, y) = I(x, y)[1 + \alpha W(x, y)] \quad (2-2)$$

其中, I 和 I_w 分别为嵌入水印前后图像的像素强度(灰度)值矩阵, α 表示水印嵌入强度, W 表示水印信号。一般来说,增大嵌入强度 α 可以增强水印的鲁棒性,但相应的,水印给原始图像带来的失真会更大。

数字水印的嵌入有时也要对载体信号以及水印信号本身进行分析和处理,对水印嵌入位置、嵌入方式进行选择,以寻求不易察觉、安全可靠、鲁棒性好等诸多因素的良好折衷^[2]。

B. 水印提取或检测系统

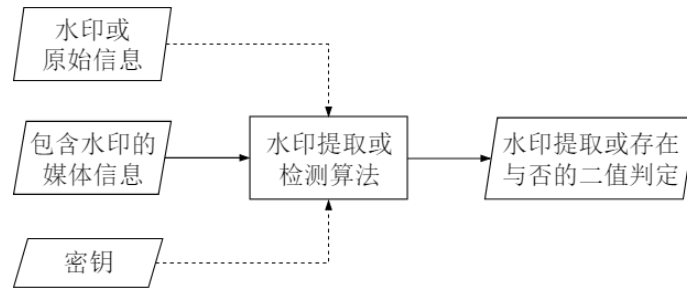


图 2-2 水印提取或检测系统

Figure 2-2 Simplified model of watermark extraction or detection system

图 2-2 给出了水印提取或检测系统的框架模型。水印提取或检测算法从输入的包含水印的媒体信息中提取水印,其中密钥为可选项。若提取或检测水印时不需要原始水印和原始载体,则将这个过程称为盲提取,将能够盲提取的水印技术称为盲水印(blind watermark),反之为非盲水印(non-blind watermark)。非盲水印具有很大局限性,很多场合都不适用。

在不同应用场合,水印提取或检测的目标不尽相同,有时仅需要通过相似度判断媒体信息中是否存在着某水印,有时还需准确提取出水印携带的完整消息。

2.1.2 数字水印的特性

面对不同目的与需求,对数字水印的要求也不尽相同。为了更好地实现版权保护、内容认证、票据防伪等目的,一般情况下,数字水印应至少具有以下基本特性^[2,21]。

1) 不可见性(invisibility): 也称为隐蔽性、透明性、保真性。嵌入水印给载体信息带来的失真对于观察者来说是难以察觉的,甚至是没有任何区别的。有时还应保证使用统计手段恢复水印信息在计算上不可行。

2) 鲁棒性(robustness): 也称为健壮性。在经历各种攻击后, 水印仍能保持其完整性, 提取算法仍能正确提取水印信息, 直到载体信息发生了十分严重的失真而丧失其使用价值。

3) 安全性: 水印的嵌入过程应是秘密、安全的, 非授权用户不能通过统计方法检测到水印,

4) 所有权唯一性: 也称为可证明性。媒体所携带的水印信息应能被确定地、唯一地鉴别, 从而为版权所有者提供完全的、安全可靠的所有权归属证明。

5) 计算有效性: 水印嵌入算法、检测算法应该易于用软、硬件实现, 从而适应各种应用场合。此外, 水印算法计算应该足够快。

在众多水印的特性中, 不可见性与鲁棒性是数字水印最基本、最重要的两个特性。它们构成了一对基本矛盾, 无法同时取得最优, 水印方案往往是取得两者的良好折衷。

2.1.3 数字水印的常见攻击方式

鲁棒性良好的水印应该具有抵抗各种攻击行为的能力。通常只考虑不会让载体数据发生严重失真的攻击方法, 因为当载体数据严重失真时, 其自身也丧失了使用价值。按照原理的不同可大致将攻击分为四类^[22, 23], 分别描述如下。

A. 简单攻击



(a)原图

(b) 引入 AWGN



(c)中值滤波

(d) 质量因数为 50 的 JPEG 压缩

图 2-3 常见图像简单攻击

Figure 2-3 Images before and after common simple attacks

简单攻击(simple attacks)又称为波形攻击, 指在存储或传输过程中可能引入的各种噪声(如 AWGN、椒盐噪声)、滤波(如中值滤波、高斯滤波)、压缩处理(如 JPEG、MPEG)、数模转换等。这种攻击试图削弱水印, 使水印无法正确提取。

可通过提高水印嵌入强度、使用信息冗余、扩频编码等方法来增强对这种攻击的抵抗能力。信息冗余是一种很有效的方法, 比如多次嵌入相同的消息, 提取时使用大多数投票原则; 使用纠错编码, 在提取时能自动纠正可能发生的错误; 使用扩频编码, 以减少信息的出错概率, 提高对噪声的免疫能力。

图 2-3 给出了常见简单攻击效果图, 其中, (a)为原图, (b)为引入 AWGN(加性高斯白噪声)后得到的图, (c)为中值滤波后得到的图, (d)为质量因数为 50 的 JPEG 压缩后得到的图。

B. 几何攻击

几何攻击(geometric attacks)也称为同步攻击, 这种攻击一般不会对图像质量带来明显的影响, 而是通过几何变换, 如旋转、缩放、平移、裁剪等, 使水印信号与载体信号失去同步^[24]。

设图像变换前后分别为 I_0 和 I_1 , 原图尺寸为 $M \times N$ 。

旋转(rotation)变换:

$$I_1(x, y) = I_0(x\cos\theta_0 - y\sin\theta_0, x\sin\theta_0 + y\cos\theta_0) \quad (2-3)$$

其中, θ_0 是旋转角度。由于图像是正放的矩阵, 对一幅图像旋转以后(除去旋转角度为 90° 的整数倍的情况), 一般要在原始图像信息周围补 0。

缩放(scaling)变换:

$$I_1(x, y) = I_0(\sigma_1 x, \sigma_2 y) \quad (2-4)$$

其中 σ_1 和 σ_2 分别为图像水平方向和竖直方向的缩放比例。

由于像素图是二维离散信号, 图像旋转和缩放变换时存在插值操作, 都有可能对图像造成不可逆的失真^[25]。

平移(translation)变换:

$$I_1(x, y) = I_0(x + x_0, y + y_0) \quad (2-5)$$

其中, (x_0, y_0) 为图像沿两个方向的平移量。为了使得平移前后图像尺寸相同且没有其他元素填充, 一般采用循环平移:

$$I_1(x, y) = I_0[(x + x_0) \bmod M, (y + y_0) \bmod N] \quad (2-6)$$

将旋转、缩放、平移这三种变换结合在一起, 可得到 RST 组合攻击的数学表示如公式(2-7)所示。

$$I_1(x, y) = I_0[\sigma_1(x\cos\theta_0 - y\sin\theta_0) - x_0, \sigma_2(x\sin\theta_0 + y\cos\theta_0) - y_0] \quad (2-7)$$

除 RST 外, 裁剪(cropping)也是现实中一种常用的攻击方式。例如, 攻击者只对图像的一部分感兴趣, 那么他可以通过裁剪变换, 只保留感兴趣的区域, 将其他区域直接丢弃。

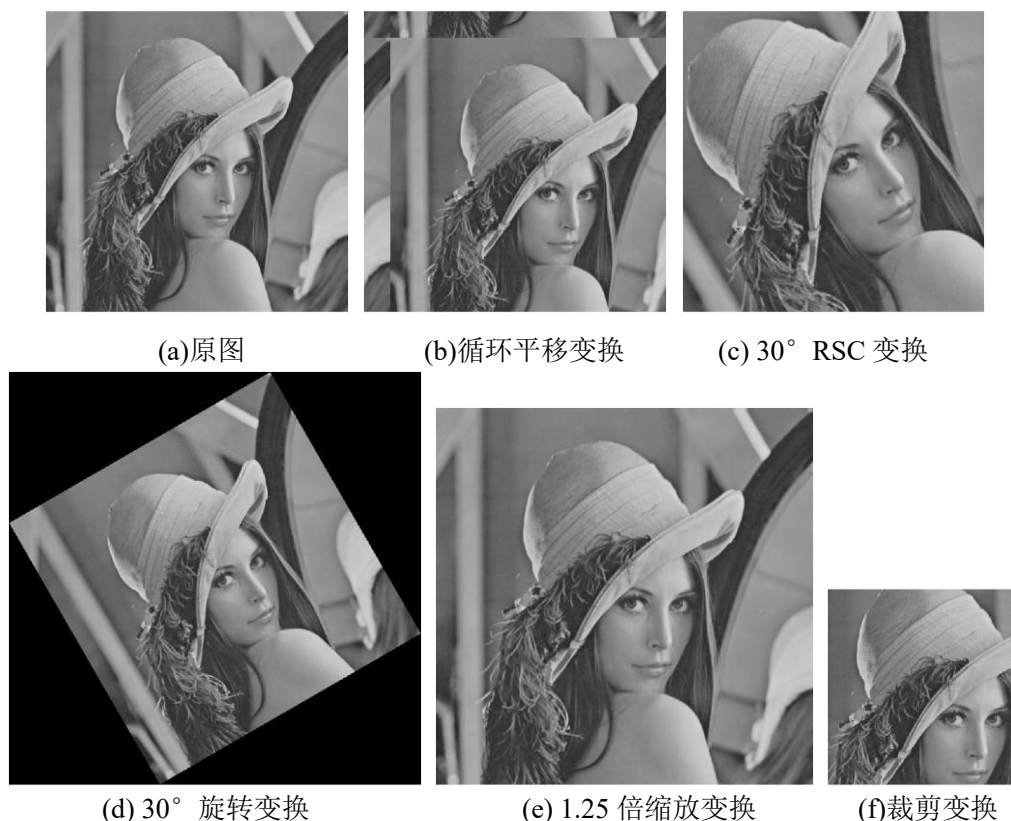


图 2-4 常见图像几何攻击效果图

Figure 2-4 Images before and after common geometric attacks

现实中, 图像可能经过上述几种变换方式的组合攻击。例如, 自动裁剪缩放的旋转(rotation with auto-cropping and scaling, RSC)是指先将图像旋转一定角度, 然后通过裁剪去除周围的三角形 0 填充(原始图像中的一些信息也会被截掉), 最后再缩放至原图尺寸。

图 2-4 给出了图像常见几何攻击示意图。其中, (a)为原图, (b)为循环平移变换后得到的图, (c)为旋转角度为 30° 的 RSC 变换后得到的图, (d)为旋转 30° 变换后得到的图, (e)为 1.25 倍等比例缩放变换后得到的图, (f)为比例为 30% 的裁剪变换后得到的图。

多数水印方案中, 提取或检测端必须事先掌握水印嵌入的精确位置信息, 才能正确提取出水印, 而几何变换使其成为难题。

针对几何攻击的防御思路主要有两种。①在提取水印前先检测出图像遭受的攻击, 并做逆向恢复, 再提取水印。若无任何预知信息, 或许只能通过穷举的方法, 计算量非常巨大, 因此不可行。比较可行的方法是在嵌入水印时, 加入一些

特征参考点，水印提取时，通过这些参考点的变化，计算出几何变换参数。②将水印嵌入到几何不变域中，在几何攻击后仍能正确提取水印。

C. 混淆攻击

混淆攻击(ambiguity attacks)也称为 IBM 攻击，其基本思路是在包含水印的媒体信息中再嵌入一个或多个附加水印，使水印失去唯一性。

D. 擦除攻击

擦除攻击(removal attacks)通过分析包含水印的媒体信息，利用平均、拼接等手段去除水印，从而得到不含水印或难以确定水印的媒体信息。如将多个含水印拷贝取平均值，或在每个拷贝仅取一小部分数据，将它重新整合成一个完整的载体数据。

2.1.4 数字水印的性能评价

数字水印最重要的两个特性是不可见性和鲁棒性，它们是一对基本矛盾。评价水印一般也是从这两个特性入手。

对不可见性与鲁棒性的评估，实际上都可以视为相似程度评估：使用原始图像与嵌入水印图像之间的相似程度来衡量水印的不可见性，使用从嵌入水印图像(可能已遭到有意或无意的攻击)中提取出的水印信号与嵌入时使用的原始水印之间的相似度来衡量水印的鲁棒性。

A. 不可见性评估

嵌入的水印不应该给原图像带来过大的失真，以保证嵌入水印后图像仍具有使用价值。

一般使用嵌入水印的信息媒体与原始信息媒体之间的偏离误差来评估水印的隐蔽程度。如对所有像素误差的平方取平均值的均方误差(mean square error, MSE)；还有峰值信噪比(peak signal-to-noise rate, PSNR)，它是目前最被广泛使用的不可见性评价指标。它们的定义分别如公式(2-8)、(2-9)所示。

$$MSE(f, g) = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N [f(x, y) - g(x, y)]^2 \quad (2-8)$$

$$\begin{aligned} PSNR(f, g) &= 10 \log_{10} \frac{\max I^2}{MSE(f, g)} \\ &= 10 \log_{10} \frac{MN \max I^2}{\sum_{x=1}^M \sum_{y=1}^N [f(x, y) - g(x, y)]^2} \end{aligned} \quad (2-9)$$

其中， M 、 N 分别为图像的行数、列数， $f(x, y)$ 、 $g(x, y)$ 分别表示嵌入前后图像中坐标为 (x, y) 的像素强度值， $\max I$ 表示像素强度值的最大可能数值，若每个像素强度需要使用 b 比特表示，那么 $\max I = 2^b - 1$ 。

由公式(2-8)、(2-9)可知，MSE 和 PSNR 呈反比的关系，当两幅图像越接近时，MSE 越接近 0，PSNR 则越接近无穷大。

不过，MSE、PSNR 等传统的图像失真评价指标存在缺陷，因此并不适用于评估水印的不可见性^[26]。Wang 等^[27]基于 HVS 的掩蔽特性提出了基于结构相似度(structural similar index, SSIM)的评价模型，其更符合 HVS 对图像品质的理解与判断，能够较好的反映图像的失真情况。与传统的误差求和方法不同，SSIM 是将任何图像失真建模为三个视觉感知重要因素的组合，它的定义如公式(2-10)所示：

$$SSIM(f, g) = [l(x, y)]^\alpha [c(x, y)]^\beta [s(x, y)]^\gamma \quad (2-10)$$

$$\begin{cases} l(f, g) = \frac{2\mu_f\mu_g + C_1}{\mu_f^2 + \mu_g^2 + C_1} \\ c(f, g) = \frac{2\sigma_f\sigma_g + C_2}{\sigma_f^2 + \sigma_g^2 + C_2} \\ s(f, g) = \frac{\sigma_{fg} + C_3}{\sigma_f\sigma_g + C_3} \end{cases}$$

其中， $l(x, y)$ 、 $c(x, y)$ 、 $s(x, y)$ 分别衡量了图像的亮度(luminance)失真、对比度(contrast)失真、结构(structure)失真， α 、 β 、 γ 是用于调整三者相对重要性的参数， μ_f 、 σ_f 和 μ_g 、 σ_g 分别为 $f(x, y)$ 和 $g(x, y)$ 的均值和标准差， σ_{fg} 为它们的协方差。 C_1 、 C_2 、 C_3 均为常数，用以维持三者的稳定。

SSIM 的值越大，则两幅图像的相似性越高，当两幅图像完全相同时取得最大值 1。

B. 鲁棒性评估

鲁棒性主要用于衡量水印对各种攻击的抵抗能力。

对水印鲁棒性的评估，使用最多的是归一化相关系数(normalized correlation coefficient, NC)，它的定义如公式(2-11)所示。它通过计算原始水印与提取出水印的相似度，并将其与人为规定的阈值作比较来判断水印的存在性。

$$NC(W, W') = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i, j)W'(i, j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W(i, j)^2} \sqrt{\sum_{i=1}^M \sum_{j=1}^N W'(i, j)^2}} \quad (2-11)$$

其中， M 和 N 对应水印的尺寸， W 为原始水印， W' 为从嵌入水印媒体中提取出的水印。

NC 通常用于评估嵌入的水印是图像时算法的鲁棒性。使用它判断图像中是否含有水印时，阈值的大小对最终检测结果影响非常大。实际使用中，需要多次

调试，以获得虚警率(false alarm rate)、漏警率(missing alarm rate)之间一个较好的折衷。

对于嵌入的水印是比特序列的水印算法，一般使用错误比特率(bit error rate, BER)即提取出的错误比特占水印比特总数的比值来评估水印的鲁棒性。

2.2 傅里叶变换与图像频域(Fourier Transform and Image Frequency Domain)

傅里叶变换(Fourier transform)可将信号从时域或空域(空间域)变换至频域，广泛应用于信号处理中。其基本思想是任何信号都可以视为有限个或无穷多个正弦信号的叠加，从而将不同频率(不同波长)、不同相位的信号分量提取出来。

图像可视为二维离散信号。二维离散傅里叶变换(2-D DFT)及其反变换 2-D IDFT 的定义如公式(2-12)、(2-13)所示：

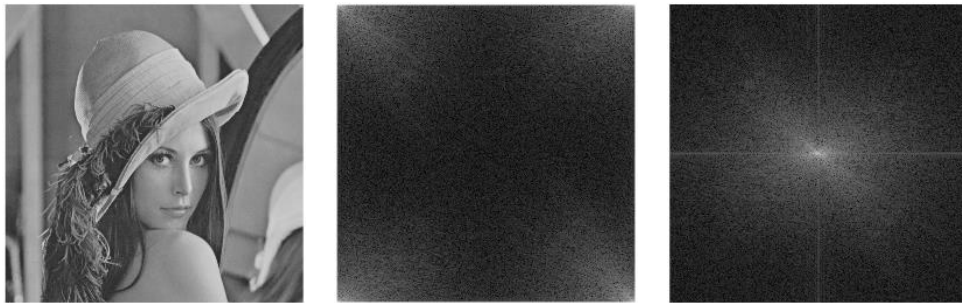
$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(ux/M + vy/N)} \quad (2-12)$$

$$f(x, y) = \frac{1}{MN} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{j2\pi(ux/M + vy/N)} \quad (2-13)$$

其中， M 和 N 为图像的行数和列数， e 为欧拉数， j 为虚数单位。

实际计算中，常通过快速傅里叶变换(fast Fourier transform, FFT)及其反变换 IFFT 来快速计算 DFT 及 IDFT，将复杂度由按 DFT 定义计算时所需要的 $O(n^2)$ 降至 $O(n \log n)$ 。

实际处理中，常用中心化(将一三象限、二四象限互换)操作，将图像的直流(direct current, DC)分量移动至中心。这样，越靠近中心频率越低，对应低频分量；越远离中心频率越高，对应高频分量；低频与高频分量之间则为中频分量。图 2-5 给出了 Lena 图以及它的傅里叶幅度谱中心化前后的示意图。



(a) Lena 图 (b) DFT 幅度谱(中心化前) (c) DFT 幅度谱(中心化后)

图 2-5 Lena 图及它的 DFT 幅度谱中心化前后示意图

Figure 2-5 Lena and its DFT amplitude spectrum before and after centralization

DFT 幅度谱具有以下重要特性^[6,25]。

- 1) 平移不变性：图像在空域中平移，其 DFT 幅度谱不变。
- 2) 旋转一致性：图像在空域中旋转，其 DFT 幅度谱也会旋转相同角度。
- 3) 缩放反比性：图像在空域中的尺度变换，对应 DFT 幅度谱中缩放系数取倒数的尺度变换。

- 4) 对称性：DFT 幅度谱是呈中心对称的。

将一幅图像 $I_0(x, y)$ 在空域中经过 RST 变换得到 $I_1(x, y)$ ，那么有它们以下数学关系：

$$I_1(x, y) = I_0[\sigma_1(x\cos\theta_0 - y\sin\theta_0) - x_0, \sigma_2(x\sin\theta_0 + y\cos\theta_0) - y_0] \quad (2-14)$$

其中， θ_0 为旋转角， σ_1 和 σ_2 分别为水平方向和竖直方向上的缩放因子， (x_0, y_0) 为平移量。若缩放为等比例，令 $\sigma_1 = \sigma_2 = \sigma$ ，则上式变为：

$$I_1(x, y) = I_0[\sigma(x\cos\theta_0 - y\sin\theta_0) - x_0, \sigma(x\sin\theta_0 + y\cos\theta_0) - y_0] \quad (2-15)$$

设它们经过 2D-DFT 后分别得到 $F_0(u, v)$ 和 $F_1(u, v)$ ，根据 DFT 的平移不变性、旋转一致性、缩放反比性，它们在傅里叶幅度谱上有以下数学关系：

$$|F_1(u, v)| = \sigma^{-2} |F_0[\sigma^{-1}(x\cos\theta_0 - y\sin\theta_0), \sigma^{-1}(x\sin\theta_0 + y\cos\theta_0)]| \quad (2-16)$$

2.3 对数极坐标映射(Log-Polar Mapping)

如图 2-6 所示，对数极坐标映射(LPM)是将图像等二维信号，从笛卡尔坐标转换至对数极坐标的过程^[9]。设一像素在笛卡尔坐标系中坐标为 (x, y) ，在对数极坐标系中坐标为 (r, θ) ，则有以下数学关系^[28]：

$$\begin{cases} r = \log\sqrt{(x - x_c)^2 + (y - y_c)^2} \\ \theta = \arctan\frac{y - y_c}{x - x_c} \end{cases} \quad (2-17)$$

其中， (x_c, y_c) 是中心点坐标。

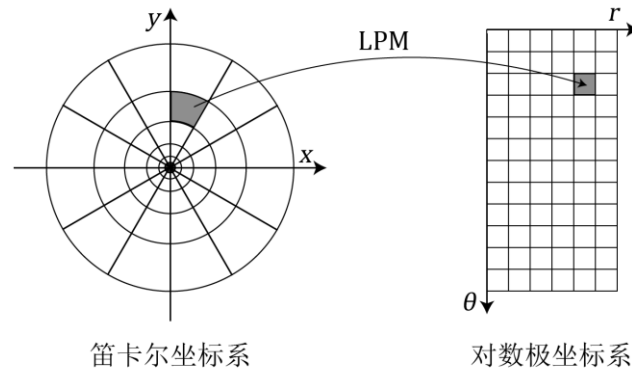


图 2-6 对数极坐标映射示意图

Figure 2-6 Schematic diagram of log-polar mapping (LPM)

若对图像的处理仅存在旋转和缩放变换, 设笛卡尔坐标系中图像 $I_0(x, y)$ 经过角度为 θ_0 的旋转, 缩放因子为 σ 的缩放变换得到 $I_1(x, y)$, 那么有^[28]:

$$I_1(x, y) = I_0[\sigma(x\cos\theta_0 - y\sin\theta_0), \sigma(x\sin\theta_0 + y\cos\theta_0)] \quad (2-18)$$

由对数的运算性质 $\log(ab) = \log a + \log b$, 在对数极坐标系中 $I_0(r, \theta)$ 和 $I_1(r, \theta)$ 对应关系为:

$$I_1(r, \theta) = I_0[r + \log\sigma, (\theta + \theta_0) \bmod 360] \quad (2-19)$$

这样, 笛卡尔坐标系中的旋转、缩放变换就简化为对数极坐标系中的平移变换: ①旋转对应于对数极坐标系中沿角度轴循环平移; ②缩放对应于对数极坐标系中沿对数半径轴平移。

这种处理方法为后续的匹配、追踪提供了很大便利。

但是, 这种方法并不是完美的。由于①位图是离散信号, ②对数极坐标映射后结果也是离散的, ③对数运算将一个较大范围映射到较小范围, 是一个多对一映射, 所以必然会引入数据量的压缩, 嵌入水印时有些水印位(尤其是接近中心区域的水印位)在嵌入时可能就已经直接丢失。此外, 执行反变换时, 数据会遭受很严重的失真。

设对数的底数为 a , 那么对数极坐标系中沿对数半径轴的两相邻网格线对应笛卡尔坐标系中相邻圆圈的间距为 $a^i - a^{i-1}$, 两相邻间距之商为 $(a^{i+1} - a^i) / (a^i - a^{i-1}) = a$ 。由于 $a > 1$, 所以间距是不均匀的, 导致对数极坐标中的一个点对应的笛卡尔坐标系中点的数量有很大差距。可以通过控制底数 a 的值, 取略大于1且近似为1的值, 使两相邻间距之商近似为1, 那么间距就近似均匀了。

2.4 互相关与互相关定理(Cross-correlation and Cross-correlation Theorem)

互相关(cross-correlation)可以衡量两个信号之间的相关程度(或相似性)^[29], 常用于模式匹配、目标追踪。例如需要在一副完整图像(匹配矩阵)中寻找其的一部分(模式矩阵)所在位置时, 可以计算它们的互相关, 其峰值出现的位置即为模式矩阵在匹配矩阵中最可能的位置, 这个过程如图 2-7 所示。二维互相关运算的定义^[25]如公式(2-20)所示:

$$r(f, g) = f(x, y) \otimes g(x, y) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m, n)g(x+m, y+n) \quad (2-20)$$

其中, \otimes 表示互相关运算符。

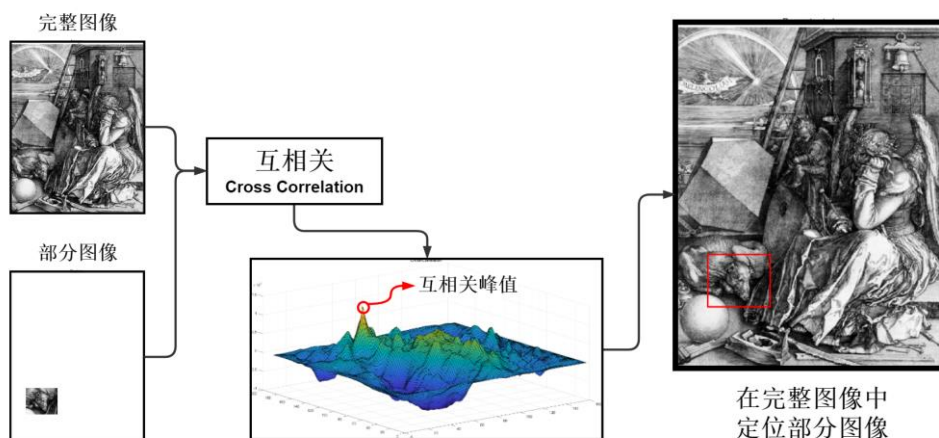


图 2-7 利用互相关匹配图像

Figure 2-7 Schematic diagram of matching images using cross-correlation

若通过互相关定义直接计算，需要沿两个轴滑动模式矩阵，使其穷尽搜索匹配矩阵的每行每列，需要很长时间。一种更快的计算方法是使用互相关定理^[25]：

$$r'(f, g) = f(x, y) \otimes g(x, y) = \text{IDFT}[F(u, v)G^*(u, v)] \quad (2-21)$$

其中， $F(u, v)$ 和 $G(u, v)$ 分别为 $f(x, y)$ 的 DFT 和 $g(x, y)$ 的 DFT， $G^*(u, v)$ 表示 $G(u, v)$ 的复共轭， $\text{IDFT}(\cdot)$ 表示离散傅里叶反变换。

2.5 本章小结(Chapter Summary)

首先介绍了数字水印技术的重要概念，包括数字水印的一般模型、特性、常见攻击方法、性能评价指标；然后引出了与本课题设计实现的数字水印系统高度相关的傅里叶频域、对数极坐标变换、互相关的基础理论。为后续章节的水印嵌入与提取算法、评估模型设计与实现提供理论支持。

3 水印嵌入算法

3 Watermark Embedding

本文方案中，水印嵌入端的输入为原始图像 I_o 、密钥 key 、消息 m ，输出为包含水印的图像 I_w 。算法示意图如图 3-1 所示。

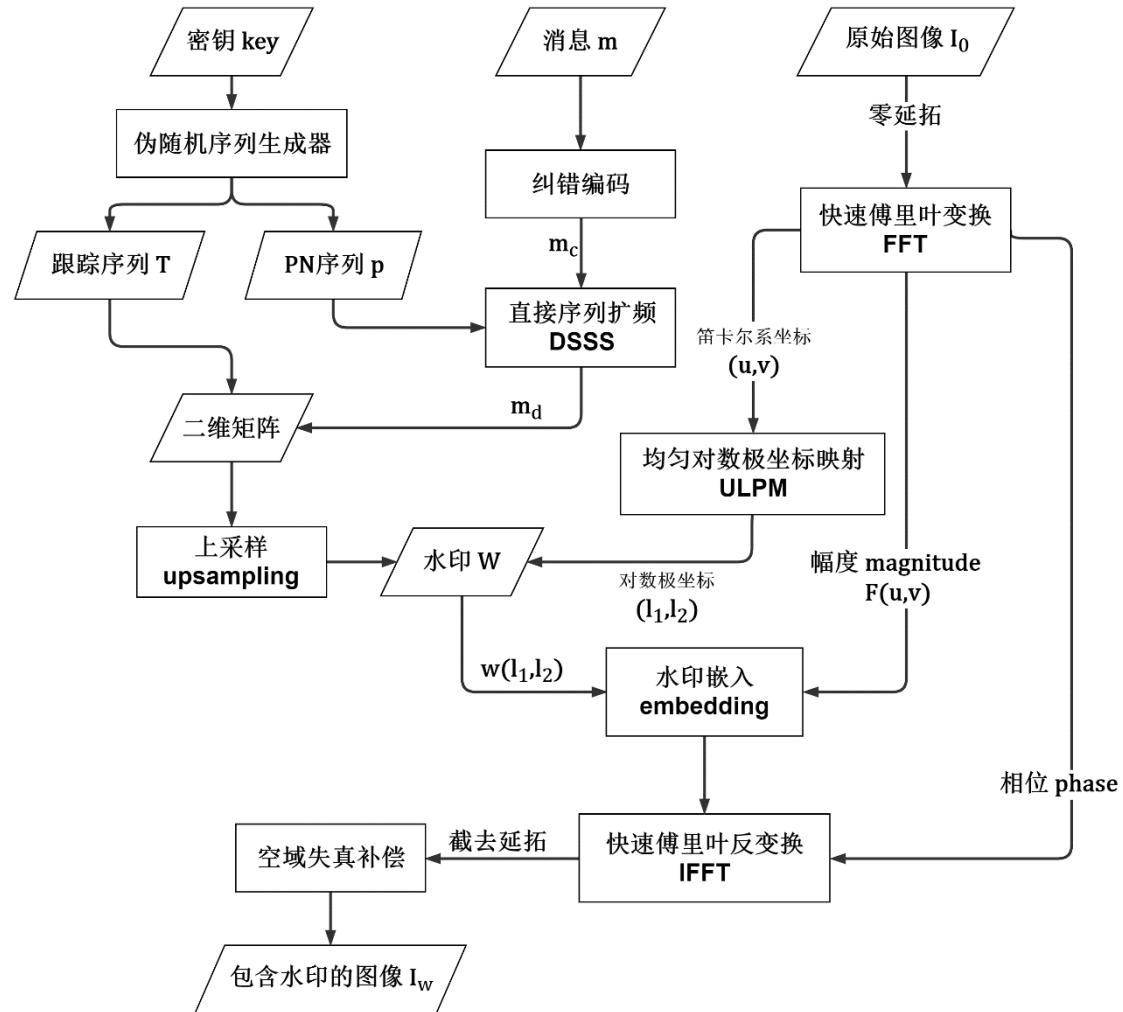


图 3-1 基于 ULPM 的水印嵌入算法

Figure 3-1 ULPM-based watermark embedding algorithm

为了扩大水印的适用范围，考虑到原始图像可能是灰度图(只有一个通道)或真彩图(有 R、G、B 三个通道)，嵌入系统在读取原始图像后，首先判断其类型：若原图为灰度图，不需要特别的处理；若原图为真彩图，则在其 YCbCr 色彩空间的 Y 通道中嵌入水印，嵌入水印后仍为真彩图；提取系统同理，若为真彩图，则在其 YCbCr 色彩空间的 Y 通道中提取水印。由于水印是嵌入在 Y 通道的，包含水印的真彩图灰度化后也能提取水印。

3.1 水印生成(Watermark Generation)

本文方案中，水印的行数和列数分别为 $M = 64$ 和 $N = 360$ ，对数极坐标系的尺寸也设计为与水印一致。

首先，使用密钥 key 作为伪随机序列生成算法的输入，生成一个长度为 N_T 的跟踪序列 T 和一个长度为 $N_p = 64$ 的伪随机噪声(pseudo-random noise, PN)序列 p 。它们都是仅由+1 和-1 两种元素组成的平衡序列。使用纠错码对长度为 L 的消息 m 编码得到长度为 L_c 比特的消息的纠错编码 m_c ，然后使用 p 序列对其每一比特 m_{ci} 进行扩频调制，使用的扩频调制方法是直接序列扩频，比特 1 被调制为 p 序列的正相序列，即一位 1 被编码成扩频序列 $+1 \times p$ ；比特 0 被调制为 p 序列的反相序列，即一位 0 被编码成 $-1 \times p$ 。得到一个一维序列 m_d ，将其整形重构为高度为 $N/2$ 的矩阵，得到有效载荷(消息)矩阵 W_1 。然后，将跟踪序列 T 也整形重构为高度为 $N/2$ 的矩阵，得到跟踪模式矩阵 W_2 。最后将这两个矩阵串连起来，进行二倍上采样(upsampling)得到最终的水印 W 。二倍上采样的目的是通过提升水印的解析能力来提高水印的鲁棒性，在实现中直接重复每行、重复每列。

需要注意的是，这里的 T 、 p 的尺寸 N_T 、 N_p 以及纠错码的码长都经过了特别的设计，使得最终 W 的尺寸为 $M \times N$ 。

图 3-2 给出了水印示意图，图中，①黑色区域代表-1，白色区域代表+1，②有效载荷矩阵 W_1 位于左侧区域，跟踪模式矩阵 W_2 则位于右侧区域。水印中的跟踪模式区域用红色实线矩形圈出(本文只是为了直观呈现特意将其圈出，实际水印中并没有这个红色矩形)。

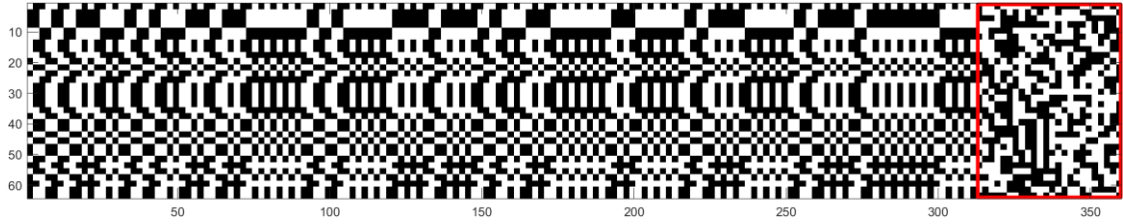


图 3-2 水印示意图

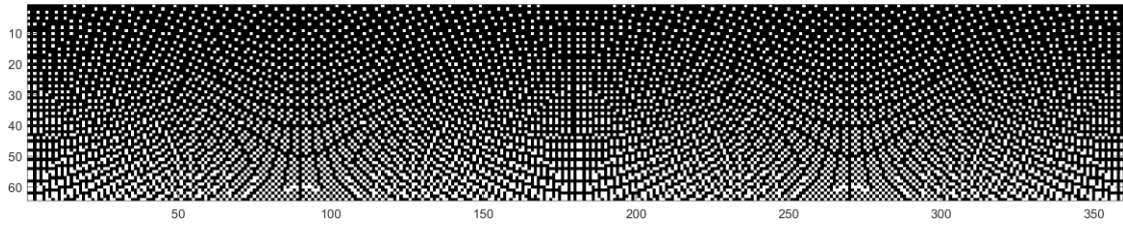
Figure 3-2 Schematic diagram of the watermark

3.2 零延拓(Padding with Zeros)

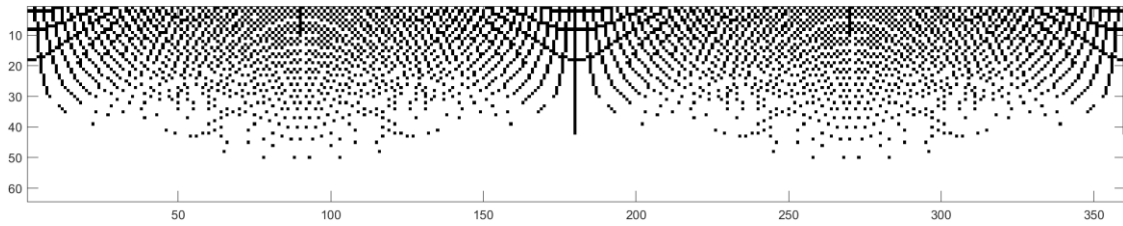
在 2.3 节中提到，使用对数极坐标变换导致有些水印位尤其是接近中心的水印位(即位于低频的水印位)在嵌入时就直接丢失，当原图尺寸过小时这种现象尤其明显，给水印算法带来了很大问题。为了弥补这个问题，增加一参数 p_{size} ，其取值为 2^m ，其中 m 为整数，一般取 $m \geq 10$ 。在嵌入水印前首先将原图像零延拓成尺寸为 $p_{size} \times p_{size}$ 的矩阵。在提取水印前也进行同样操作。

一方面,当数据样点为2的整数幂时,FFT是最高效的;另一方面,空域零延拓虽然并不能真正提升信号的频域分辨率(因为其并没有增加信号的信息量),但是它相当于在频域进行插值,从而提高频域的计算分辨率,使信号在频域上的解析能力更强。

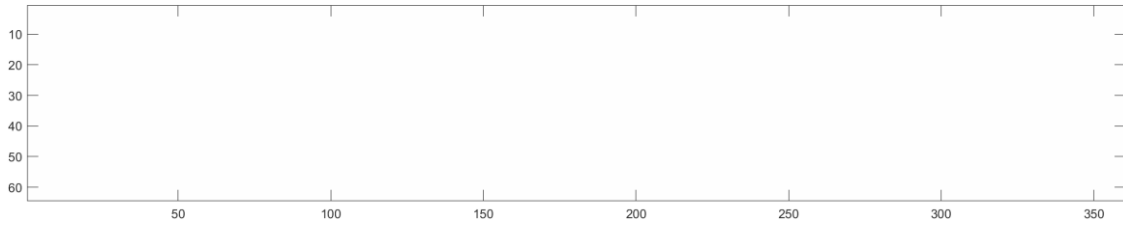
图3-3展示了 $R = 0.20$,尺寸为 512×512 的图像不进行零延拓、进行零延拓且 $p_{size} = 1024$ 、进行零延拓且 $p_{size} = 2048$ 的水印在对数极坐标系中的直接丢失情况示意图,图中黑色区域表示直接损失的水印位。可以看出,当 $p_{size} = 2048$ 时,已经不会出现水印位在嵌入时直接丢失的情况。



(a) 不延拓时水印丢失情况



(b) $p_{size} = 1024$ 时水印丢失情况



(c) $p_{size} = 2048$ 时水印丢失情况

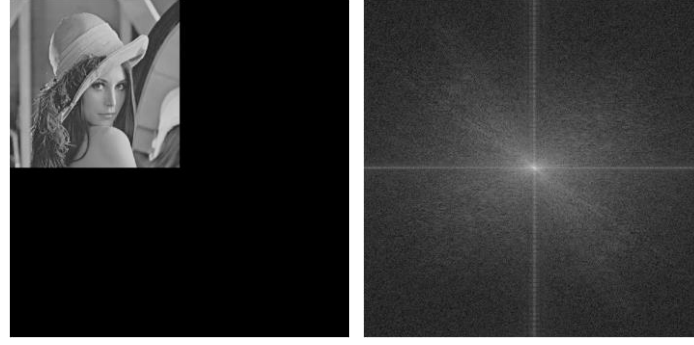
图3-3 水印位丢失

Figure 3-3 Schematic diagram of watermark loss

3.3 在傅里叶幅度谱中应用 ULPM(Applying ULPM to the Fourier Magnitude Spectrum)

为避免混淆,本文中 DFT 幅度谱的笛卡尔坐标系坐标和对数极坐标系中坐标的一般形式分别为 (u, v) 、 (l_1, l_2) , 其中, l_1 对应对数半径轴, l_2 对应角度轴。

对零延拓后的原图像进行 2-D DFT 并中心化(即交换一三象限、二四象限),将直流分量移动到中心,把这个中心作为笛卡尔坐标系的中心。例如, 512×512 的 Lena 零延拓到 1024×1024 大小的空域图像以及它的 DFT 幅度谱如图3-4所示。



(a)零延拓后的 Lena 图 (b)图(a)的 DFT 幅度谱

图 3-4 图像零延拓及它的 DFT 幅度谱

Figure 3-4 Image padding with zeros and its DFT magnitude spectrum

如图 3-5 所示，水印最终是嵌入到位于傅里叶幅度谱(即 DFT 系数) $F_m(u, v)$ 的以 DC 分量位置(点 C)为中心的圆环形区域上。考虑到图像的尺寸可以是任意的，本课题中使用归一化的半径 r 来描述傅里叶幅度谱中一点到中心点 C 的相对距离，它是 0 到 1 之间的数。例如，点 P 所在圆环上任一点的半径都为 1。

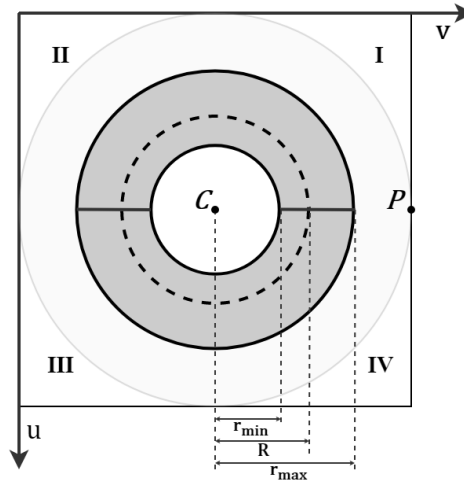


图 3-5 水印嵌入圆环区域

Figure 3-5 Schematic diagram of the ring area where the watermark is embedded

设原图尺寸为 $X \times X$ ，若 X 为偶数，则点 C 的坐标为 $(X/2 + 1, X/2 + 1)$ ；若 X 为奇数，则点 C 的坐标为 $[(X + 1)/2, (X + 1)/2]$ 。

设 R 为归一化的基准半径(即基准频率)，它决定了在傅里叶幅度谱上嵌入水印的大致区域。 R 越大，对应区域频率越高。通过 R 来定义嵌入水印圆环形区域的内径 r_{\min} 、外径 r_{\max} ：

$$\begin{aligned} r_{\min} &= R \times a^{-M/2} \\ r_{\max} &= R \times a^{M/2} \end{aligned} \quad (3-1)$$

令外径与内径的比值为 b ，即 $b = r_{\max}/r_{\min}$ ，本文中取 $b = 2$ 。令对数的底数 $a = b^{1/M} = 2^{1/M} \approx 1$ ，那么对数极半径轴的间距是近似均匀的。

ULPM 将圆环形区域映射到尺寸为 $M \times N$ 的对数极坐标 (l_1, l_2) 中, 如公式(3-2)所示:

$$\begin{aligned} l_1 &= \text{floor}\left(\log_a \frac{r}{R}\right) + \frac{M}{2} \\ l_2 &= \text{floor}\left(\frac{N \times \theta}{\pi}\right) \end{aligned} \quad (3-2)$$

其中, $\text{floor}(\cdot)$ 表示向下取整运算。

通过将 r 的取值范围 $R \times a^{-M/2} < r < R \times a^{M/2}$ 、 θ 的取值范围 $-90 < \theta < 90$ 代入这两个式子, 不难验证 $0 \leq l_1 < M, 0 \leq l_2 < N$, 这样, 就构造了从幅度谱圆环形区域到对数极坐标系的映射。将这个映射表存储起来, 方便之后嵌入水印时使用。

这是一个多对一映射, 即①笛卡尔坐标系中的一个点仅对应于对数极坐标系的一个点, ②对数极坐标系上一个点可能对应于笛卡尔坐标系上的多个点。

在实现过程中, 仅需先构造傅里叶幅度谱第一、二象限的映射表, 之后再利用傅里叶幅度谱的中心对称性构造第三、四象限映射表。

3.4 嵌入水印(Embedding the Watermark)

将对数极坐标 (l_1, l_2) 上的每个水印位, 通过前面构造好的映射表嵌入到图像的傅里叶幅度谱系数(即 DFT 系数)中。由于 ULPM 是一个多对一映射, 所以一个水印位可能嵌入到多个 DFT 系数中。嵌入使用的是乘性准则, 如公式(3-3)所示:

$$F'_m(u, v) = F_m(u, v) \times [1 + \alpha \times \mathbf{W}(l_1, l_2)] \quad (3-3)$$

其中, $F_m(u, v)$ 、 $F'_m(u, v)$ 分别为嵌入前后的 DFT 系数, α 表示嵌入强度。

由于水印实际上是嵌入到傅里叶幅度谱中的, 避免了对图像带来不必要的失真。如图 3-6 所示, 可以通过将嵌入前后图像的 DFT 幅度谱相减观察到嵌入区域, 其中纯黑色区域表示嵌入前后傅里叶幅度谱无变化的区域。

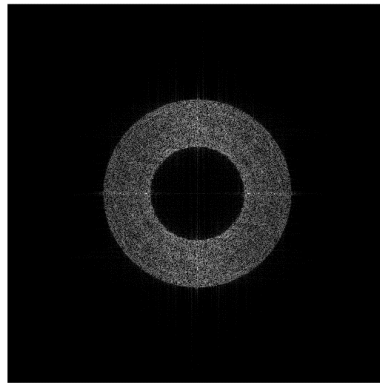


图 3-6 $R = 0.35$ 时的水印嵌入区域

Figure 3-6 Diagram of watermark embedding area when $R = 0.35$

3.5 空域失真补偿(Spatial Distortion Compensation)

在频域嵌入水印的缺点是，嵌入水印的能量不能自适应地分布在图像空域中，而是简单地分布在整幅图像上，在图像光滑区域可能会出现易被人眼所感知的网格状失真。且嵌入强度越大，这种失真越明显。

人们所观看到的影像依赖于人眼对影像信息的捕获和大脑对信息的分析处理^[30]。人类视觉系统结构很复杂，目前的研究尚无一个全面的理论认识，不过心理物理学在此方面已经有一些研究进展。

最小可察觉差(Just-noticeable difference, JND)表示某一感官所能察觉的刺激的最小改变量。若失真低于 JND 函数值，则无法被 HVS 所感知^[19,31]。

根据这一概念原理，本文对文献[19]提出的基于 HVS 的水印模型进行了简化，设计了一个失真补偿方案，以达到在略微降低水印鲁棒性的情况下大幅提高水印的不可见性的目的。

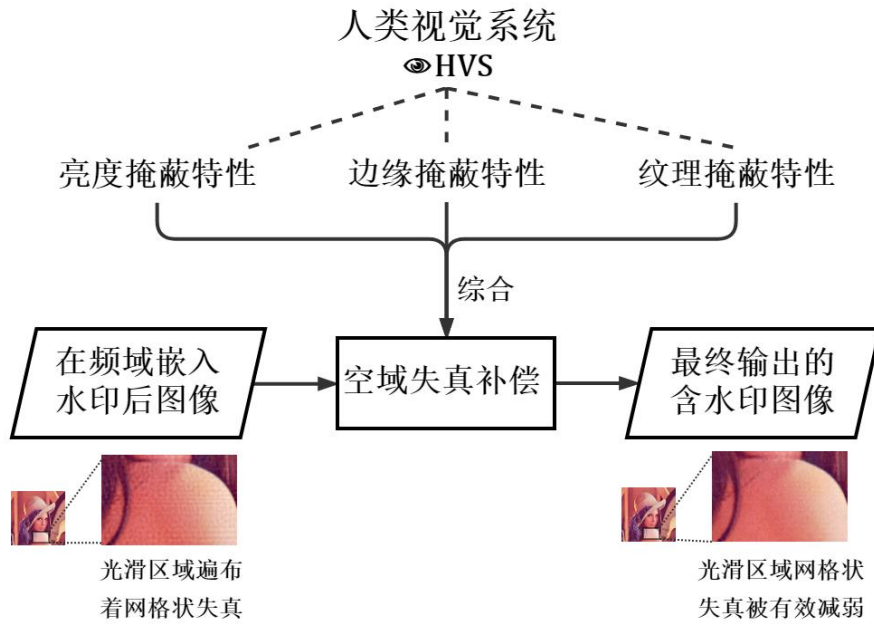


图 3-7 空域失真补偿示意图

Figure 3-7 Schematic diagram of spatial distortion compensation

如图 3-7 所示，该模型利用图像的三个决定 HVS 感知的关键因素——亮度、边缘、纹理的掩蔽特性以减轻图像的失真。分别是：①HVS 对高光或阴影区域的噪声较不敏感；②HVS 对图像边缘区域上噪声较不敏感；③HVS 对平滑背景上噪声的敏感度远高于对复杂纹理背景上噪声的敏感度。

在傅里叶幅度谱中嵌入水印后，在空域中对图像进行失真补偿。首先计算图像中每个像素的“掩蔽值”（用以描摹的 JND）：

$$M(x, y) = (2.8l^2 - 2.8l + 1)[E(x, y)T(x, y)]^\beta \quad (3-4)$$

其中, $l = L(x, y)$ 。 $L(x, y)$ 、 $E(x, y)$ 和 $T(x, y)$ 分别是局部平均亮度、局部平均梯度(用于衡量边缘)和局部标准方差(用于衡量纹理), 它们都是经过归一化的数值, 以确保量纲尺度是一致的。 $2.8l^2 - 2.8l + 1$ 是一个中间低、两边高的二次函数, 用以描述 HVS 的亮度掩蔽特性。 β 为空域失真补偿系数, 用于调整结构、纹理的相对重要性, β 越大, 则补偿后的图像越平滑。

在程序实现中, 综合考虑计算复杂度与失真补偿效果, 对图像进行滤波, 将滤波器尺寸为 5×5 的中值滤波的结果作为局部平均亮度 $L(x, y)$, 滤波器尺寸为 3×3 的 Laplacian 滤波的结果作为局部平均梯度 $E(x, y)$, 滤波器尺寸为 5×5 的移动方差滤波的结果作为局部标准方差 $T(x, y)$ 。

根据 HVS 掩蔽特性, 图像做如下调整: 对于图像上的每个像素, 首先计算原始图像与嵌入水印后图像在这一像素上的强度值之差的绝对值, 与掩蔽值做比较: ①若差异小于掩蔽值, 则认为此像素上水印不会被 HVS 发现, 保留嵌入水印后的结果; ②否则, 对该像素进行补偿(直接将原图该点像素值加上或减去归一化的掩蔽值), 以降低噪声的影响。失真补偿的公式如下:

$$I_w(x, y) = \begin{cases} I_w(x, y), & \text{if } |I_w(x, y) - I(x, y)| < M_n(x, y); \\ I(x, y) + M_n(x, y), & \text{if } I_w(x, y) - I(x, y) > M_n(x, y); \\ I(x, y) - M_n(x, y), & \text{otherwise.} \end{cases} \quad (3-5)$$

其中, $I(x, y)$ 、 $I_w(x, y)$ 分别表示嵌入前后图像中坐标为 (x, y) 的像素的强度值, $M_n(x, y)$ 为 $M(x, y)$ 归一化后的值。

3.6 纠错方案(Error Correction Scheme)

综合考虑信息传输过程出错比特的分散性(即提取水印时, 错误比特一般不是集中出现的, 而是分散出现的), 结合测试分析结果, 权衡码长、消息长度、纠错能力以及水印尺寸后提出此纠错方案:

- 1) 总消息长度为 43 比特, 总码长为 78 比特;
- 2) 消息的前 36 比特使用(63,36) BCH 编码, 码长为 63, 最多可纠正 5 比特错误;
- 3) 消息的后 7 比特使用(15,7)BCH 编码, 码长为 15, 最多可纠正 2 比特错误;
- 4) 总计最多能纠正 7 比特错误(要求消息的前 36 比特最多出现 5 比特错误, 消息的后 7 比特最多出现 2 比特错误)。

纠错方案的编码、解码过程示意图如图 3-8 所示。

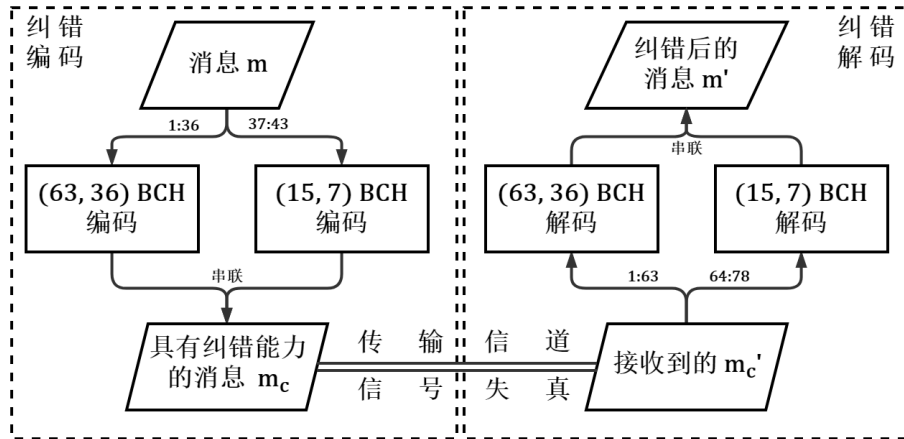


图 3-8 纠错方案示意图

Figure 3-8 Schematic diagram of error correction scheme

3.7 本章小结(Chapter Summary)

详细介绍了本课题的水印嵌入算法。先给出了水印嵌入算法的过程示意图，再对过程中涉及到的处理方法进行详细说明。水印嵌入算法的输入是原始图像、消息、密钥，输出是包含水印的图像。嵌入的水印由两部分组成，分别是消息序列(携带消息)、跟踪序列(用于提取时重同步水印)，消息是经过纠错编码、PN 序列直接序列扩频的，以满足对鲁棒性的需求。为了防止接近中心的水印位直接丢失，先对图像做零延拓。然后根据 ULPM 映射表将水印嵌入到图像的 DFT 幅度谱中。在嵌入水印后，利用 HVS 的掩蔽特性在空域进行失真补偿，以提升水印的不可见性。

4 水印提取算法

4 Watermark Extracting

本文方案中，水印提取端的输入为包含水印的图像 I_w 和密钥 key ，输出为提取出的消息 m' 。算法示意图如图 4-1 所示。

水印提取端与嵌入端唯一共享的信息是密钥 key 。水印提取端仅需要这个密钥，就可以实现水印盲提取。

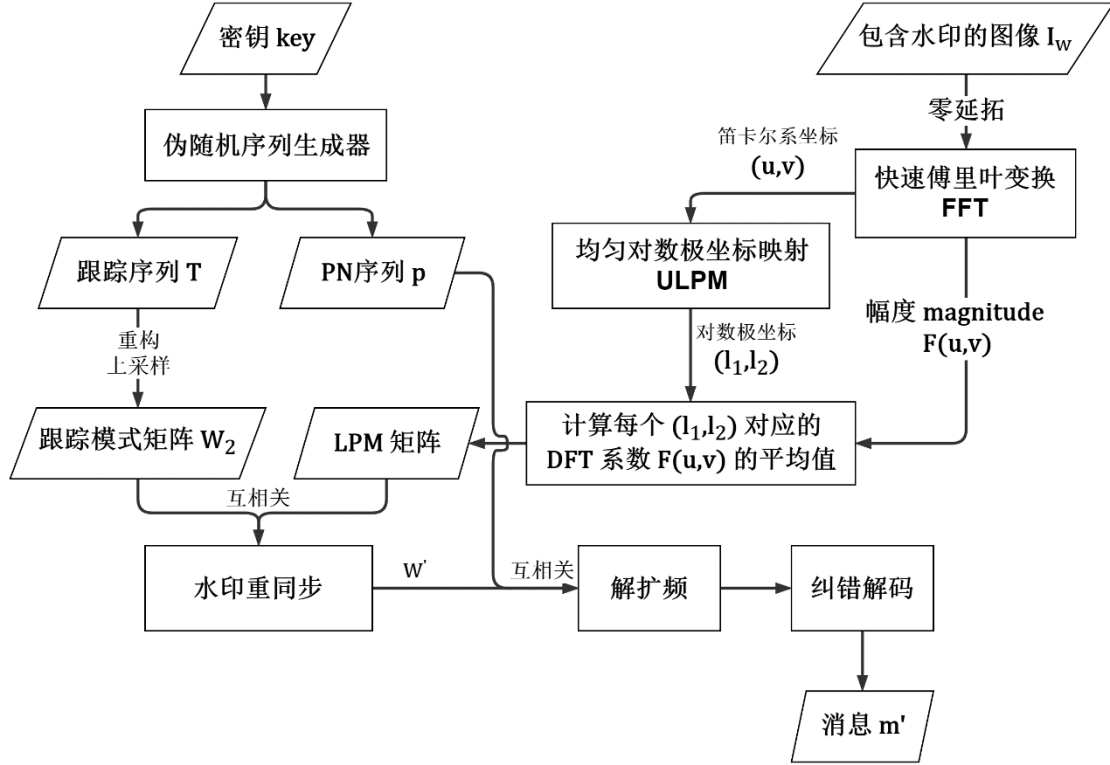


图 4-1 基于 ULPM 的水印提取算法

Figure 4-1 ULPM-based watermark extracting algorithm

与水印嵌入端相同，水印提取端也要对输入的图像进行零延拓，以提升其计算分辨率；也要在 DFT 幅度谱中应用 ULPM，从而在对数极坐标系中定位水印。上文已给出了零延拓、ULPM 的作用与过程，这一章就不再赘述。

4.1 水印重同步(Watermark Resynchronization)

和水印嵌入端相同，提取端首先使用伪随机序列生成算法得到跟踪模式 T 和 PN 序列 p 。由于输入 key 是相同的，所以 T 和 p 与嵌入端相同。

水印嵌入时，圆环形区域为：

$$R \times a^{-M/2} \leq r < R \times a^{M/2} \quad (4-1)$$

由于图像可能已经遭受了缩放攻击，对应其傅里叶频谱在对数极坐标上沿对数极半径轴 l_1 平移，所以要扩展跟踪区域。水印提取时，圆环区域为：

$$R \times a^{-\lambda M} \leq r < R \times a^{\lambda M} \quad (4-2)$$

其中， λ 是唯一控制跟踪区域大小的参数。为了顺利提取水印，跟踪区域要比嵌入区域更大，即需满足 $\lambda > 1/2$ 。图 4-2 展示了水印嵌入时的圆环区域与水印提取时的圆环区域(跟踪区域)的对比，图中深灰色表示水印嵌入区域，浅灰色表示跟踪区域。 λ 越大，跟踪区域越大，但同时获得 ULPM 映射表的时间更长，错误跟踪率也越高。综合考虑各种因素，选取 $\lambda = 1$ ，这样，对数极坐标的尺寸也从原来的 M 扩展到 $M' = 2 \times M$ 。由于区域发生了扩展，所以这时的 ULPM 映射表会比嵌入时大很多。

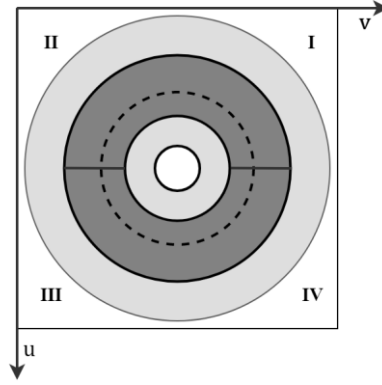


图 4-2 水印嵌入时与水印提取时的圆环区域的对比示意图

Figure 4-2 Comparison of ring area when watermark is embedded and watermark is extracted

从 DFT 幅度谱中提取水印时，由于 ULPM 是一个多对一映射，所以对数极坐标系中的每个元素可能对应 DFT 幅度谱上多个元素。在这里，计算 (l_1, l_2) 对应的所有 DFT 系数 $F_m(u, v)$ 的平均值，将结果存入一个尺寸为 $M' \times N$ 矩阵中，称它为 LPM 矩阵。

水印嵌入相当于在原始图像这个强背景上加入弱信号，为了有效提取水印，期望背景强度较为均一，而实际上，如图 3-4(a)所示，其沿两个方向都是不够均一的：

- 1) 对于一般图像而言，从低频到高频，即 DFT 幅度谱圆环从内到外，能量分布的大致趋势是从高到低的，所以沿 l_1 方向是不够均一的；
- 2) 由于图像空域具有一定方向特征，DFT 幅度谱会有一些从中心延展出的高强度分支，所以沿 l_2 方向也是不够均一的。

为了尽可能降低背景对水印提取造成的影响，使背景能量分布较为均一，将 LPM 矩阵进行两个方向上的标准化操作：先将每列化为标准分数(z-score, 均值为 0，标准差为 1)，再将每行化为标准分数。

为了直观说明，图 4-3 给出了LPM矩阵标准化效果对比图。可以看出，当进行了两个方向上的标准化操作后，能量分布较为均一，背景带来的影响就被大幅削弱了。

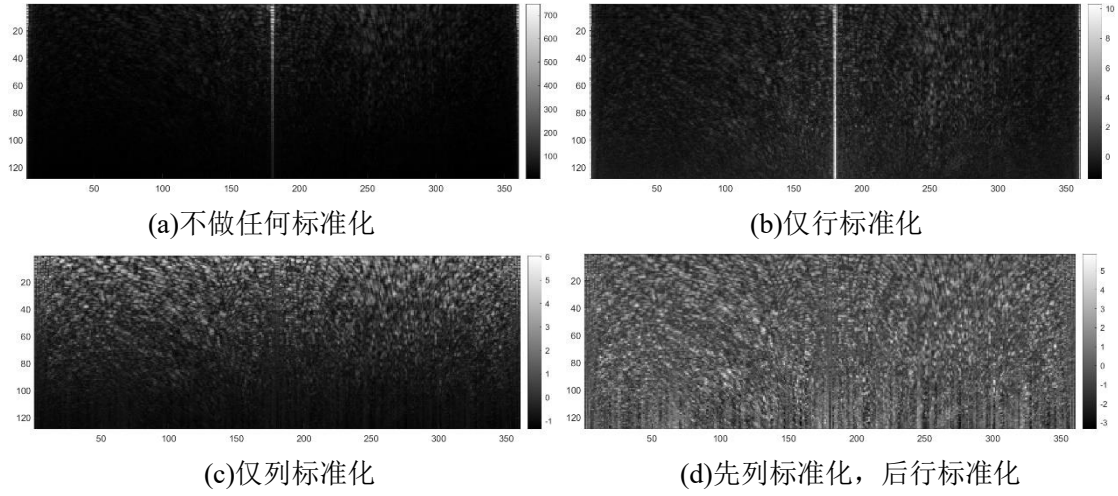


图 4-3 LPM矩阵标准化效果对比图

Figure 4-3 Comparison of the standardization effect of LPM matrix

由于图像可能已遭受旋转攻击，对应其傅里叶频谱在对数极坐标上沿角度轴 l_2 循环移位。为了避免循环移位操作带来不必要的麻烦，在程序实现中，串联三个相同的LPM矩阵，形成一个更大的矩阵 $LPM' = [LPM \ LPM \ LPM]$ 。

为了定位LPM'中的水印，将跟踪序列 T 重构并上采样，得到与嵌入时跟踪模式 W_2 完全相同的跟踪模式矩阵 W_2' ，将它与LPM'利用互相关定理做互相关运算。例如，受到旋转 30° 攻击时，互相关运算结果曲面图如图 4-4 所示。出现峰值的位置即为 W_2' 在匹配矩阵LPM'中最有可能出现的位置，它的左侧区域即为消息矩阵 W_1' ，对应嵌入算法中的 W_1 。因为做了矩阵串联重复，所以峰值会出现多个，任取一个就好。

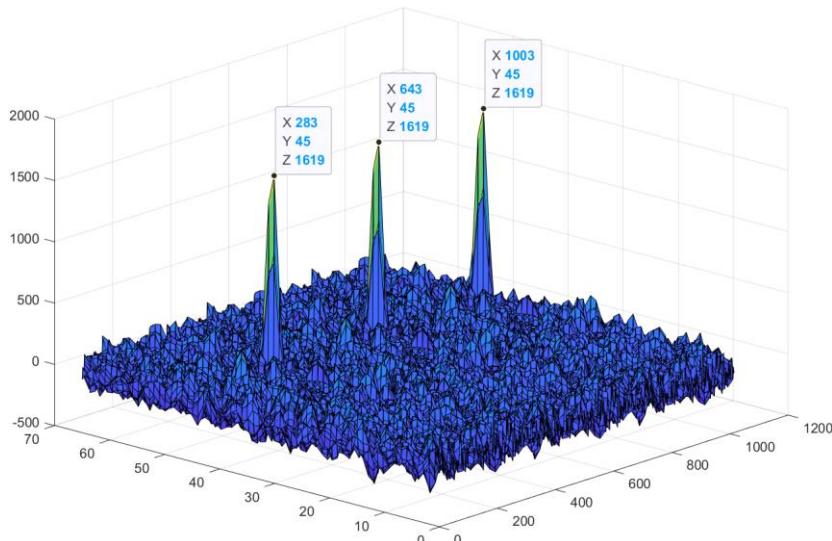


图 4-4 重同步互相关结果曲面图

Figure 4-4 Surface graph of cross-correlation results during resynchronization

4.2 解扩频和解码(Despreading and Decoding)

在嵌入系统中, 消息进行了纠错编码, 使水印方案具有一定纠错能力, 再使用扩频技术进一步提高其鲁棒性, 接着将这一维序列整形重构为二维矩阵, 再进行二倍上采样。从这个过程不难推出, 纠错编码的消息 m_c 的每一位经过扩频后占据 W_1 的四列。故在解扩频时, 先将由 key 生成的 p 变换成相同的形式, 即先重构为 32×2 大小, 再做二倍上采样, 得到 64×4 的矩阵 p_{mat} 。和重同步时做法类似, 为了降低背景对水印提取效果的影响, 将提取出的矩阵 W_1' 做标准化操作。然后, 使用 p_{mat} 与水印的逐四列做点积, 若结果大于 0, 则纠错编码消息 m'_c 的该位为 1, 否则为 0。可以用数学语言描述如下:

$$m'_c(i) = \begin{cases} 1, & \text{if } \sum_{k=1}^4 \sum_{j=1}^{64} \{p_{mat}(j, k) \times W_1'[j, 4(i-1) + k]\} > 0; \\ 0, & \text{otherwise.} \end{cases} \quad (4-3)$$

使用此方法能得到消息的原因是, p 是仅由+1 和-1 构成的序列, 而 $(+1) \times (+1) = (-1) \times (-1) = 1$, $(+1) \times (-1) = -1$, 若提取出的序列与 p 相位相同, 则点积的结果是正数, 而 p 与 $-p$ 做点积的结果是负数。

随后, 对 m'_c 进行纠错码解码, 从而得到提取出消息 m' , 水印提取算法完成。最后, 可将其与原始消息 m 作比较, 以得到比特误码率 BER。

4.3 本章小结(Chapter Summary)

详细介绍了本课题的水印提取算法。先给出了水印提取算法的过程示意图, 再对过程中涉及到的处理方法进行详细说明。水印提取算法的输入是包含水印的图像、密钥, 输出是提取出的消息。水印提取端仅需与嵌入端共享一个密钥就能实现水印盲提取。由于图像可能经过缩放, 所以跟踪区域比嵌入区域要大。由于ULPM 是一个多对一映射, 所以对数极坐标系上的一个点可能对应笛卡尔坐标系上多个点, 这里对笛卡尔坐标系上多个 DFT 系数取平均值, 得到 LPM 矩阵。为了降低强背景对水印提取结果的影响, 对 LPM 做两个方向的标准化操作。使用跟踪模式与 LPM 矩阵做互相关, 以找到水印在 LPM 矩阵中的位置。经过解扩频、纠错解码, 最终得到水印携带的消息。

5 系统测试与优化

5 Testing and Optimization

本文对常用于评估水印性能的关键指标进行了建模,使程序能够自动输出对水印的测试结果、综合评分,从而方便测试、对比、优化。程序的优化主要有两方面:①分析测试结果,调整算法中关键参数的取值;②吸取现有文献中的优化策略,从而改进算法。

对于水印算法中涉及到的关键参数的取值,本文的总体思路是控制变量,先进行大范围测试(取值间隔较大),再根据测试结果选择可能取得最优值的区间进行进一步细分测试(取值间隔较小),从而获得可能取值中接近最优的取值,实现水印不可见性、鲁棒性以及效率之间的良好折衷。

5.1 测试环境及测试图像集(Test Environment and Image Set)

本文中,用于运行测试程序的环境如表 5-1 所示。

表 5-1 本文测试环境

Table 5-1 Test environment

| 项目 | 配置 |
|------|--|
| 操作系统 | Windows 10 x64 专业版 |
| 处理器 | Intel(R) Core(TM) i5-6300HQ CPU @ 2.30GHz 2.30 GHz |
| 内存 | 16.0 GB |
| 软件环境 | MATLAB R2020a 64-bit |

从互联网上公开的标准测试图数据库中选取了 8 幅具有一定代表性的图像作为测试图像集,如图 5-1 所示,分别为①Lena(512×512,真彩)、②Pirate(512×512,灰度)、③Peppers(512×512,真彩)、④Baboon(512×512,真彩)、⑤Miramar NAS(512×512,真彩)、⑥Point Loma(512×512,真彩)、⑦Woolen cloth(1024×1024,灰度)、⑧Plastic bubbles(1024×1024,灰度)。



图 5-1 测试图像集

Figure 5-1 Test image set

5.2 数字水印性能评估模型(Performance Evaluation Model of Digital Watermarking)

不可见性、鲁棒性是数字水印两个最基本、最重要的指标，此外，在数字水印的实际应用中，水印嵌入算法、水印提取算法的计算效率也非常重要。本课题为量化评估数字水印方案的综合性能，提出了评估模型，以便于后续对水印方案进行测试、优化。提出的模型综合考虑了上述三个方面，最后输出综合评分。效率、不可见性、鲁棒性满分分别为 x 、 y 、 z ，可根据实际需求调整它们的占比。评估满分为 $x + y + z = 100$ 分，得分越高，则认为水印的综合性能越好。图 5-2 给出了提出的综合性能评估模型示意图。

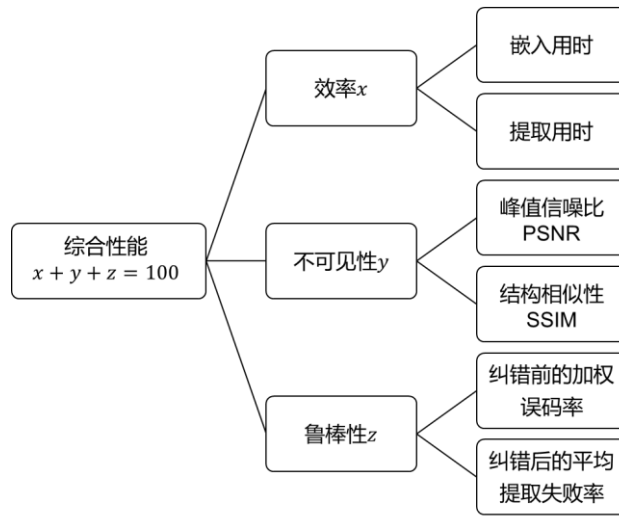


图 5-2 综合性能评估模型

Figure 5-2 Proposed comprehensive performance evaluation model

5.2.1 水印计算效率评估

对水印嵌入、提取算法的计算效率进行评估，总分为 x 。使用两个指标：嵌入水印平均用时 t_{embed} (0.50 x 分)、提取水印平均用时 t_{extract} (0.50 x 分)。计分方法如公式(5-1)、(5-2)所示。

$$S_{t_{\text{embed}}} = \begin{cases} 0.50x, & \text{if } t_{\text{embed}} < 0.3 \text{ s;} \\ 0, & \text{if } t_{\text{embed}} > 1.0 \text{ s;} \\ 0.50x \times (1.0 - t_{\text{embed}})/0.7, & \text{otherwise.} \end{cases} \quad (5-1)$$

$$S_{t_{\text{extract}}} = \begin{cases} 0.50x, & \text{if } t_{\text{extract}} < 0.3 \text{ s;} \\ 0, & \text{if } t_{\text{extract}} > 1.0 \text{ s;} \\ 0.50x \times (1.0 - t_{\text{extract}})/0.7, & \text{otherwise.} \end{cases} \quad (5-2)$$

若嵌入或提取时间大于 1 秒，则认为其效率过低，计 0 分；若时间小于 0.3 秒，则认为效率优秀，计满分；若时间介于 0.3 秒和 1 秒之间，则按线性函数计分。

5.2.2 水印不可见性评估

对嵌入水印给原图带来的失真和人类视觉系统实际能感受到的失真进行评估，总分为 y 。使用峰值信噪比PSNR(0.48 y 分)、结构相似性SSIM(0.52 y 分)两个指标，在这里设置SSIM的权重较高、PSNR权重较低的原因是PSNR并不适用于评估水印的不可见性，SSIM更符合 HVS 对图像品质、图像失真的判断，能够较好的反映图像失真。计分方法如公式(5-3)、(5-4)所示。

$$S_{\text{PSNR}} = \begin{cases} 0.48y, & \text{if } \overline{\text{PSNR}} \geq 45; \\ 0.48y \times \overline{\text{PSNR}}/45, & \text{otherwise.} \end{cases} \quad (5-3)$$

$$S_{\text{SSIM}} = 0.52y \times \overline{\text{SSIM}}^8 \quad (5-4)$$

其中， $\overline{\text{PSNR}}$ 、 $\overline{\text{SSIM}}$ 分别表示在多幅图像嵌入水印前后的峰值信噪比的平均值、结构相似性的平均值。

对于 $\overline{\text{PSNR}}$ ，若它的值不小于 45，则认为隐蔽性好，记为满分；否则按线性函数计分。

$\overline{\text{SSIM}}$ 是介于[0,1]之间的数，且它的变化非常微小。为了放大变化，计算它的 n 次方(其中 $n > 1$)，使得接近 1 区域的斜率很大，本文取 $n = 8$ 。为了直观说明，图 5-3 给出了 $y = x^8$ 在 $0 \leq x \leq 1$ 上的取值情况。

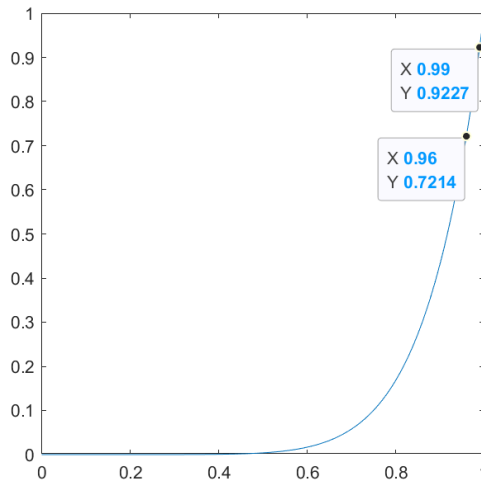


图 5-3 $y = x^8$ 在 $0 \leq x \leq 1$ 上的取值情况

Figure 5-3 $y = x^8$ on $0 \leq x \leq 1$

5.2.3 水印鲁棒性评估

对水印抵抗常见简单攻击、常见几何攻击的能力进行评估，总分为 z 。使用两个指标：纠错前加权误码率(0.60 z 分)、纠错后平均提取失败比率(0.40 z 分)，它们均为本文自定义的指标。该模型考虑到提取失败有两种情况：①水印重同步失败；②水印重同步成功，但错误比特数大于纠错码的纠错能力。

提出的模型模拟了常见的简单攻击、几何攻击以及组合攻击。设 k 为攻击类型， i 为图像编号， j 为参数取值编号。则定义的攻击类型与相应的权重 $z_t(k)$ 列举如下(所有攻击权重之和为 100)：

- 1) JPEG: JPEG 压缩，压缩因数为 10、15、20、30、40、50、60、70、80、90、100，权重 $z_t(1) = 8$ ；
 - 2) AWGN: 加性高斯白噪声，均值 μ 为 0，标准差 σ 为 0.02、0.01、0.001、0.0001，权重 $z_t(2) = 8$ ；
 - 3) MEDIAN: 中值滤波，滤波器尺寸为 3×3 、 5×5 ，权重 $z_t(3) = 8$ ；
 - 4) GAUSS: 高斯滤波，滤波器尺寸同 MEDIAN，权重 $z_t(4) = 6$ ；
 - 5) SHARP: 高提升滤波，滤波器尺寸同 MEDIAN，权重 $z_t(5) = 3$ ；
 - 6) ROT: 旋转(不自动裁剪)，角度为-2、-1、-0.75、-0.5、-0.25、0.25、0.5、0.75、1、2、5、10、15、30、45、90，权重 $z_t(6) = 10$ ；
 - 7) RSC: 旋转(自动裁剪并缩放至原图大小)，角度同 ROT，权重 $z_t(7) = 12$ ；
 - 8) SCALE: 缩放，比例为 0.75、0.90、1.10、1.25、1.40，权重 $z_t(8) = 10$ ；
 - 9) CROP: 裁剪，百分比为 40、45、50、60、75，权重 $z_t(9) = 15$ ；
 - 10) RSC-JPEG50: RSC 后 JPEG-50 压缩，角度同 ROT，权重 $z_t(10) = 20$ 。
- 权重从两方面考虑：①该攻击参数列表的长度、②抵御该攻击的难度。

定义以下对误码率BER的计分规则：

- 1) 若 $BER > 0.33$ ，视为失去同步，计分 $z_e(i, j, k) = 0$ ；
- 2) 若 $0.07 < BER \leq 0.33$ ，视为效果不佳，计分 $z_e(i, j, k) = 1 - 3 \times BER$ ；
- 3) 若 $BER \leq 0.07$ ，视为正常可接受范围，计分 $1 - BER$ 。

在这些基础上，计分方法如公式(5-5)、(5-6)所示。

$$S_{\text{robust}_1} = 0.60z \times \frac{1}{100} \sum_{k=1}^{10} z_t(k) \frac{\sum_{i=1}^{n_{\text{im}}} \sum_{j=1}^{n_{\text{para}}(k)} z_e(i, j, k)}{n_{\text{im}} \times n_{\text{para}}(k)} \quad (5-5)$$

$$S_{\text{robust}_2} = 0.40z \times \left(\frac{n_{\text{fail}}}{n_{\text{im}} \times \sum_{k=1}^{10} n_{\text{para}}(k)} - 1 \right)^8 \quad (5-6)$$

其中, n_{im} 代表测试图像数量, $n_{para}(k)$ 代表每种攻击参数取值列表的长度, n_{fail} 表示对所有图像、所有攻击的所有参数取值进行测试, 纠错码解码后仍无法得到正确消息的出现次数。

通过调整 x 、 y 、 z 可改变模型中水印效率、不可见性、鲁棒性的相对重要性, 本文取 $x = 10$, $y = 50$, $z = 40$ 。

最后, 将所有分数相加, 得到水印的综合评分如公式(5-7)所示。

$$S = S_{t_embed} + S_{t_extract} + S_{PSNR} + S_{SSIM} + S_{robust_1} + S_{robust_2} \quad (5-7)$$

水印测试系统依次完成水印嵌入、图像模拟攻击、水印提取三个过程, 并将各方面的测试结果输出至 Excel (.xlsx) 文件中, 方便对比。

5.3 零延拓对水印的优化(Optimization by Padding with Zeros)

若原图像尺寸较小, 则有些水印位尤其是位于低频的水印位, 在嵌入时就直接丢失了。因此, 读取图像后, 应先进行零延拓, 这样可以提升其频域的计算分辨率, 减少丢失水印位数量。

表 5-2 展示了当 $R = 0.35$ 时, 零延拓及 p_{size} 的不同取值对水印性能的影响。其中, 斜杠(/)表示不进行延拓。

表 5-2 不同 p_{size} 下水印综合性能测试结果

Table 5-2 Test results under different p_{size}

| p_{size} | 平均嵌入用时 | 平均提取用时 | 平均 PSNR | 平均 SSIM | 效率得分 | 不可见性得分 | 鲁棒性得分 | 总分 |
|------------|--------|--------|---------|---------|-------|--------|-------|-------|
| / | 0.09 | 0.11 | 43.3960 | 0.9903 | 10.00 | 46.78 | 25.31 | 82.08 |
| 1024 | 0.13 | 0.13 | 39.5356 | 0.9857 | 10.00 | 42.93 | 37.37 | 90.30 |
| 2048 | 0.41 | 0.26 | 39.9540 | 0.9876 | 8.44 | 43.62 | 39.22 | 91.28 |
| 4096 | 1.60 | 0.77 | 40.0004 | 0.9879 | 0.00 | 43.70 | 39.22 | 82.92 |

测试结果表明, ①零延拓操作会给图像带来一定的图像质量损失; ②当 p_{size} 增大, 算法处理的数据量也增大, 导致水印嵌入和提取时间变长; ③零延拓能提升水印的鲁棒性, p_{size} 取值为 2048、4096 时, 水印的鲁棒性几乎没有变化; ④ p_{size} 取 2048 时, 水印的整体性能达到最佳。

综合考虑各方面因素, 本文取 $p_{size} = 2048$ 。

5.4 基准频率的取值(The Value of the Base Frequency)

基准频率 R 决定了在傅里叶幅度谱上嵌入水印的大致频率范围。 R 越大, 嵌入水印区域频率越高。

表 5-3 展示了当 $p_{size} = 2048$ 时, R 取不同值时水印的综合性能。

表 5-3 在不同归一化的基准频率 R 下的水印综合性能Table 5-3 Test results under different base frequency R

| R | 平均嵌入用时 | 平均提取用时 | 平均 PSNR | 平均 SSIM | 效率得分 | 不可见性得分 | 鲁棒性得分 | 总分 |
|-------|--------|--------|---------|---------|------|--------|-------|-------|
| 0.200 | 0.41 | 0.23 | 39.3757 | 0.9890 | 9.21 | 43.44 | 36.00 | 88.65 |
| 0.225 | 0.40 | 0.22 | 39.5204 | 0.9882 | 9.26 | 43.40 | 36.74 | 89.39 |
| 0.250 | 0.39 | 0.23 | 39.4857 | 0.9876 | 9.38 | 43.25 | 37.74 | 90.38 |
| 0.275 | 0.39 | 0.23 | 39.6111 | 0.9872 | 9.36 | 43.27 | 38.13 | 90.76 |
| 0.300 | 0.39 | 0.24 | 39.7185 | 0.9871 | 9.35 | 43.33 | 38.53 | 91.21 |
| 0.325 | 0.38 | 0.24 | 39.7877 | 0.9873 | 9.40 | 43.43 | 38.57 | 91.41 |
| 0.350 | 0.39 | 0.24 | 39.9540 | 0.9876 | 9.38 | 43.62 | 39.22 | 92.21 |
| 0.375 | 0.40 | 0.25 | 40.0764 | 0.9878 | 9.29 | 43.74 | 39.27 | 92.30 |
| 0.400 | 0.42 | 0.25 | 40.1566 | 0.9881 | 9.14 | 43.85 | 38.91 | 91.90 |
| 0.425 | 0.39 | 0.26 | 40.3677 | 0.9884 | 9.35 | 44.08 | 38.77 | 92.38 |
| 0.450 | 0.39 | 0.27 | 40.4942 | 0.9888 | 9.33 | 44.24 | 38.41 | 91.99 |

测试结果表明，①嵌入水印的频率范围，也即 R 的取值对水印不可见性的影响是微小的；②当 R 取约 0.375 左右时，其鲁棒性达到最优。

综合考虑各方面因素，本文取 $R = 0.375$ 。

5.5 空域失真补偿对水印的优化(Optimization by Spatial Distortion Compensation)

本课题使用的水印算法中，在频域嵌入水印后，在空域做失真补偿。空域失真补偿利用了 HVS 的几个掩蔽特性，在对鲁棒性影响不大的情况下减轻图像的失真。

表 5-4 展示了当 $p_{size} = 2048$ 、 $R = 0.375$ 时，空域失真补偿系数 β 的取值对水印性能的影响的测试结果。其中斜杠(/)表示不进行空域失真补偿。

表 5-4 在不同失真补偿系数 β 下水印的综合性能Table 5-4 Test results under different distortion compensation coefficient β

| β | 平均嵌入用时 | 平均提取用时 | 平均 PSNR | 平均 SSIM | 效率得分 | 不可见性得分 | 鲁棒性得分 | 总分 |
|---------|--------|--------|---------|---------|------|--------|-------|-------|
| / | 0.40 | 0.25 | 40.0764 | 0.9878 | 9.28 | 43.74 | 39.27 | 92.28 |
| 0.1 | 0.50 | 0.27 | 40.0927 | 0.9882 | 8.54 | 43.83 | 39.27 | 91.63 |
| 0.2 | 0.68 | 0.32 | 40.1182 | 0.9885 | 7.15 | 43.90 | 39.26 | 90.31 |
| 0.3 | 0.64 | 0.31 | 40.2590 | 0.9896 | 7.53 | 44.23 | 39.21 | 90.96 |
| 0.4 | 0.64 | 0.30 | 40.7756 | 0.9915 | 7.54 | 44.99 | 38.86 | 91.38 |
| 0.5 | 0.88 | 0.30 | 41.8736 | 0.9937 | 5.86 | 46.27 | 37.99 | 90.13 |
| 0.6 | 0.63 | 0.30 | 43.3274 | 0.9956 | 7.63 | 47.78 | 35.49 | 90.91 |

结果表明，空域失真补偿能有效提升水印的不可见性。但如果 β 取值太大，会对水印鲁棒性带来严重冲击。为了在只是轻微降低水印鲁棒性的情况下，获得

水印不可见性的较大提升，取 $\beta = 0.3$ 。总分对比不进行补偿时降低的主要原因是空域失真补偿使得水印嵌入算法运行时间更长。

为了直观说明空域失真补偿对水印的优化，图 5-4 展示了原图像、以 $\alpha = 0.4$ 的强度嵌入水印未进行空域失真补偿的图像、以 $\alpha = 0.4$ 的强度嵌入水印并进行了空域失真补偿的图像的对比，将其局部放大，对比效果更加明显。



(a) Lena 图像原图



(b) 包含水印未进行失真补偿的图像



(c) 包含水印并进行了失真补偿的图像

图 5-4 空域失真补偿对比图

Figure 5-4 Comparison of spatial distortion compensation

5.6 嵌入强度的取值(The Value of the Embedding Strength)

一般来说, 嵌入强度 α 越高, 水印抵抗攻击的能力越强, 水印的不可见性越弱。水印方案通常是获得鲁棒性与不可见性之间的良好折衷。

对于需要跟踪重同步的数字水印方法而言, 水印提取或检测算法面临的一个很严重的问题就是重同步失败, 提升跟踪模式的嵌入强度有利于改善这个问题。而且, 在本文水印方案中, 跟踪模式位于加水印图像的高频区域, 根据人类视觉系统的频率掩蔽特性, 其不容易被人眼所感知。令跟踪模式补偿系数为 $\gamma = 1.5$, 则跟踪模式部分的实际嵌入强度为 $\alpha \times \gamma$ 。

表 5-5 展示了当 $p_{size} = 2048$ 、 $R = 0.375$ 、 $\beta = 0.30$ 、 $\gamma = 1.5$ 时, 嵌入强度 α 对水印综合性能的影响。

表 5-5 在不同嵌入强度 α 下水印的综合性能

Table 5-5 Test results under different embedding strength α

| α | 平均嵌入用时 | 平均提取用时 | 平均 PSNR | 平均 SSIM | 效率得分 | 不可见性得分 | 鲁棒性得分 | 总分 |
|----------|--------|--------|---------|---------|------|--------|-------|-------|
| 0.20 | 0.50 | 0.24 | 43.5880 | 0.9947 | 8.55 | 47.80 | 37.91 | 94.27 |
| 0.25 | 0.76 | 0.24 | 41.6850 | 0.9921 | 6.70 | 45.79 | 38.97 | 91.47 |
| 0.30 | 0.72 | 0.24 | 40.1397 | 0.9890 | 6.98 | 44.01 | 39.53 | 90.52 |
| 0.35 | 0.55 | 0.24 | 38.8425 | 0.9855 | 8.22 | 42.39 | 39.76 | 90.37 |
| 0.40 | 0.70 | 0.24 | 37.7277 | 0.9818 | 7.17 | 40.87 | 39.83 | 87.87 |
| 0.45 | 0.57 | 0.24 | 36.7529 | 0.9778 | 8.05 | 39.44 | 39.88 | 87.37 |
| 0.50 | 0.80 | 0.24 | 35.8886 | 0.9735 | 6.43 | 38.07 | 39.92 | 84.42 |
| 0.55 | 0.70 | 0.25 | 35.1147 | 0.9691 | 7.16 | 36.77 | 39.96 | 83.89 |
| 0.60 | 0.69 | 0.24 | 34.4152 | 0.9645 | 7.23 | 35.53 | 39.96 | 82.72 |

从测试结果可以看出, 嵌入强度 α 对水印鲁棒性的提升具有边际收益递减的特点, 即提升 α 对水印鲁棒性的提升效果是递减的。综合考虑鲁棒性和不可见性, 这里选取 $\alpha = 0.30$ 。

5.7 优化后水印的性能(Performance of Optimized Watermarking Scheme)

根据前面的测试, 本文对几个关键参数都获得了较优的取值, 使得数字水印方案最终有较好的综合性能。结合测试中各种攻击后提取出水印的错误比特率, 可得出以下结论:

1) 归一化基准频率 R 的选择在很大程度上会影响水印的鲁棒性。 R 越大, 抵抗裁剪攻击的能力越强, 抵抗 JPEG 压缩攻击的能力越弱。当 $R = 0.375$ 左右时, 取得鲁棒性与不可见性之间较好的折衷。

2) 嵌入强度 α 越大, 对原图视觉效果影响越大, 抵抗裁剪攻击的能力显著增强, 抵抗其他攻击的能力略有增强。当 $\alpha = 0.30$ 左右时, 取得鲁棒性、不可见性之间较好的折衷。

3) 空域失真补偿系数 β 越大, 嵌入水印后图像与原图像视觉差异越小, 但鲁棒性会减弱。当 $\beta = 0.3$ 左右时, 取得鲁棒性、不可见性之间较好的折衷。

表 5-6 水印的最终性能

Table 5-6 Final performance of the proposed watermarking scheme

| | | | |
|---------|---------|--------|-------|
| 平均嵌入用时 | 0.48 | 效率得分 | 8.71 |
| 平均提取用时 | 0.25 | 不可见性得分 | 44.01 |
| 平均 PSNR | 40.1397 | 鲁棒性得分 | 39.53 |
| 平均 SSIM | 0.9890 | 总分 | 92.25 |

综合前面的测试结果及分析, 选取零延拓尺寸 $p_{size} = 2048$, 归一化基准频率 $R = 0.375$ 、空域失真补偿系数 $\beta = 0.30$ 、跟踪模式补偿系数 $\gamma = 1.5$ 。表 5-6 呈现最终水印的性能。

5.7.1 对简单攻击的鲁棒性

本课题使用的纠错方案是自定义方案, 其总消息长度为 42 比特, 总码长为 78 比特, 在符合一定条件时最多能纠正 7 比特错误。图像仿真攻击程序中预设的简单攻击有 JPEG 压缩(JPEG)、加性高斯白噪声(AWGN)、中值滤波(MEDIAN)、高斯滤波(GAUSS)、高提升滤波(HLF), 详细参数见 5.2.3 节。

表 5-7 对简单攻击的测试结果

Table 5-7 Test results for simple attacks

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|-------------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| JPEG_10 | 36 | N | 4 | Y | 15 | N | 0 | Y | 0 | Y | 13 | N | 8 | N | 0 | Y |
| JPEG_15 | 1 | Y | 0 | Y | 10 | N | 0 | Y | 0 | Y | 2 | Y | 1 | Y | 0 | Y |
| JPEG_20 | 0 | Y | 1 | Y | 1 | Y | 0 | Y | 0 | Y | 2 | Y | 0 | Y | 0 | Y |
| JPEG_30~100 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| AWGN_0.02 | 2 | Y | 3 | Y | 0 | Y | 0 | Y | 0 | Y | 2 | Y | 4 | Y | 0 | Y |
| AWGN_0.01 | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 1 | Y | 1 | Y | 0 | Y |
| AWGN_0.001 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| AWGN_0.0001 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| MEDIAN_3×3 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| MEDIAN_5×5 | 2 | Y | 5 | Y | 7 | N | 0 | Y | 0 | Y | 2 | Y | 4 | Y | 0 | Y |
| GAUSS_3×3 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| GAUSS_5×5 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y |
| HLF_3×3~5×5 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |

对简单攻击的测试结果如表 5-7 所示。其中，err 列为错误比特数，?列表示是否能正确提取出水印信息，即纠错解码后是否和原始水印完全相同，Y 代表成功，N 代表失败，表格中使用加粗字体标出以强调。

从测试结果可以看出，①当 JPEG 压缩的质量因数大于等于 20 时，可以正确提取出消息，甚至有些图像在 JPEG 压缩质量因数为 10 时，还能正确提取出水印消息；②当加性高斯白噪声的标准差小于等于 0.02 时，可以正确提取出消息；③水印能抵抗滤波器尺寸为 3×3 、 5×5 的高斯滤波和高提升滤波攻击；④水印能抵抗滤波器尺寸为 3×3 的中值滤波攻击。

5.7.2 对几何攻击的鲁棒性

表 5-8 对旋转(不自动裁剪)的鲁棒性

Table 5-8 Robustness to rotation without cropping

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|--------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 旋转角度 | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| -2° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -1° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.75° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.5° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.25° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 0.25° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 0.5° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 0.75° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 1~90° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |

表 5-9 对旋转(自动裁剪并缩放至原图大小)的鲁棒性

Table 5-9 Robustness to rotation with auto-cropping and scaling (RSC)

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|--------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 旋转角度 | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| -2~-1° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.75° | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.5° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.25° | 0 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 0.25° | 1 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 1 | Y | 0 | Y | 0 | Y |
| 0.5° | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |
| 0.75° | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 0 | Y | 0 | Y |
| 1° | 1 | Y | 0 | Y | 2 | Y | 0 | Y | 1 | Y | 2 | Y | 0 | Y | 0 | Y |
| 2° | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |
| 5~30° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 45° | 0 | Y | 1 | Y | 1 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y |
| 90° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |

表 5-10 对等比例缩放的鲁棒性

Table 5-10 Robustness to scaling

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|-----------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 缩放因子 | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| 0.75~1.40 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |

表 5-11 对裁剪的鲁棒性

Table 5-11 Robustness to cropping

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 裁剪比例 | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| 40% | 5 | Y | 6 | Y | 8 | N | 4 | Y | 2 | Y | 3 | Y | 1 | Y | 1 | Y |
| 45% | 1 | Y | 3 | Y | 3 | Y | 2 | Y | 2 | Y | 1 | Y | 1 | Y | 0 | Y |
| 50% | 3 | Y | 2 | Y | 1 | Y | 2 | Y | 2 | Y | 1 | Y | 0 | Y | 0 | Y |
| 60% | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 75% | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |

图像仿真攻击程序中预设的几何攻击有旋转、RSC、等比例缩放、裁剪，详细参数见 5.2.3 节。对这些攻击的鲁棒性测试结果分别如表 5-8、5-9、5-10、5-11 所示。

从测试结果可以看出，①水印能抵抗任意角度的 ROT(不自动裁剪)、RSC(自动裁剪并缩放至原图大小)旋转攻击，其中，RSC_45°是所有 RSC 中最为严重的攻击，因为它会给图像带来最严重的裁剪和最严重的缩放；②水印能抵抗缩放因子为 0.75 ~ 1.40 的等比例缩放攻击；④水印能抵抗裁剪比例为 45%(水平、竖直均只保留 45%)以上的裁剪攻击，这意味着当图像的内容仅剩原来的四分之一时，消息仍能正确提取。

5.7.3 对组合攻击的鲁棒性

表 5-12 对 RSC 与 JPEG50 组合攻击的鲁棒性

Table 5-12 Robustness to the combination attack of RSC and JPEG-50 Compression

| | 1 | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
|--------|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 旋转角度 | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? | err | ? |
| -2~-1° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.75 | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.5 | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| -0.25 | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 0.25 | 1 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 1 | Y | 0 | Y | 0 | Y |
| 0.5 | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |
| 0.75 | 1 | Y | 1 | Y | 1 | Y | 1 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |
| 1 | 1 | Y | 0 | Y | 2 | Y | 0 | Y | 1 | Y | 2 | Y | 0 | Y | 0 | Y |
| 2 | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y |
| 5°~30° | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |
| 45 | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 1 | Y | 0 | Y | 0 | Y | 0 | Y |
| 90 | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y | 0 | Y |

本课题提出的水印方案对简单攻击、几何攻击都具有良好的鲁棒性。JPEG 压缩是图像存储、传播中最普遍使用的压缩算法，RSC 可视为旋转、缩放、裁剪的组合，所以这里只对 RSC 变换后再进行质量因数为 50 的 JPEG 压缩的鲁棒性进行测试。测试结果如表 5-12 所示。

从结果可以看出，水印方案对简单攻击与几何攻击的组合攻击依然具有良好的鲁棒性。

5.8 本章小结(Chapter Summary)

为了方便对水印方案进行测试、对比、优化，基于计算效率、不可见性、鲁棒性三个方面，提出了水印综合性能评估模型，量化了数字水印方案的综合性能。以表格的形式给出了测试结果，并对结果进行分析、总结。直观展现了零延拓、空域失真补偿以及一些重要参数的不同取值对水印的优化效果，以最终实现水印不可见性、鲁棒性以及效率之间的良好折衷。给出了水印的最终性能、抗攻击测试结果。

6 总结与展望

6 Conclusions and Prospects

6.1 全文总结(Conclusions)

本课题首先对数字水印技术的研究背景做了简要概括,分析了图像数字水印算法在抵抗几何变换方面的研究现状,从而引出了本文研究的意义与目的。接着对数字水印技术的基本理论、常用处理方法手段进行了总结描述。在此基础上深入研究了文献[10]提出的基于 ULPM 的水印方案,再现了其基本框架,并完善了流程细节,在此基础上对其进行了优化。

为了方便测试、对比、优化,设计了一个初步的水印综合评估模型。编程实现了水印嵌入系统、图像模拟攻击系统、水印提取系统,并在此基础上实现了一个水印综合性能测试系统,它可以依次进行水印嵌入、图像攻击、水印提取操作,并基于本文提出的水印评估模型对水印各方面性能进行评分,将水印提取结果、一些关键指标(如平均嵌入/提取时间、PSNR、SSIM 等)以及最终评分输出至 Excel(.xlsx)文件中。

水印由两部分组成,分别是消息序列(携带消息)、跟踪序列(用于提取时重同步水印),消息是经过纠错编码、PN 序列扩频的,以满足对鲁棒性的需求。水印嵌入算法根据 ULPM 映射表将水印嵌入到载体图像的 DFT 幅度谱中,水印提取算法面临的一个很严重的问题就是重同步失败,为了弥补这个问题,提升跟踪序列的嵌入强度。在嵌入水印后,利用 HVS 掩蔽特性在空域进行失真补偿,在只是轻微降低鲁棒性的情况下,获得不可见性的较大提升

水印提取端与水印嵌入端唯一共享的信息是密钥 key ,可通过其生成与嵌入端相同的跟踪序列与 PN 序列,从而实现水印的盲提取。由于图像可能经过缩放,所以跟踪区域比嵌入区域要大。由于 ULPM 是一个多对一映射,所以对数极坐标上一个点可能对应笛卡尔坐标系上多个点,这里对笛卡尔坐标系上的多个 DFT 系数取平均值,得到 LPM 矩阵。为了降低强背景对水印提取结果的影响,对 LPM 做两个方向的标准化操作。使用跟踪模式与 LPM 矩阵做互相关,以找到水印在 LPM 矩阵中的位置。经过解扩频、纠错解码,最终获得水印携带的消息。

实验测试与分析表明,提出的水印方案具有良好的不可见性、计算效率,对质量因数为 20 以上的 JPEG 压缩、 5×5 高斯滤波、 3×3 中值滤波等简单攻击,任意角度的旋转、缩放因子为 0.75~1.45 的等比例缩放、比例为 45%以上的裁剪等几何攻击有良好的鲁棒性。

6.2 未来展望(Prospects)

由于本人从事此领域研究时间不长, 学术水平有限, 难免出现纰漏。

本课题的工作也还有许多值得改进的地方, 比如可加入几何不变性图像特征点或图像标准化方法, 以抵抗长宽比改变攻击、更大范围的缩放攻击、更苛刻的裁剪攻击。

所使用的空域失真补偿方法只考虑了嵌入水印前后空域中局部的差距, 对整体性的考虑还不够, 未来会对这一部分进一步深入研究; 所提出的评估测试模型也可能比较粗糙, 尚处于初步阶段, 下一步将对其进行打磨。

因为测试的攻击类型较多、每种攻击类型的参数列表也比较长, 所以测试用时较长。未来考虑引入并行计算, 从而减少测试时间; 对参数取值的测试过程中, 每次只变化一个参数, 忽略了整体性, 下一步可以多参数变化对水印的性能进行测试, 寻找最优的参数组合, 从而进一步提升水印综合性能。

参考文献

- [1] 黄继武, 谭铁牛. 图像隐形水印综述[J]. 自动化学报, 2000(05): 645-655.
- [2] 楼偶俊, 祁瑞华, 邬俊, 唐双童. 数字水印技术及其应用[M]. 清华大学出版社, 2018.
- [3] 刘九芬, 王振武, 黄达人. 抗几何攻击的小波变换域图像水印算法[J]. 浙江大学学报(工学版), 2003, 37(4): 386-392.
- [4] Braudaway G W, Mintzer F. Automatic recovery of invisible image watermarks from geometrically distorted images[J]. Proceedings of Spie the International Society for Optical Engineering, 2000, 9(4): 477-483.
- [5] Lu W, Lu H, Chung F L. Feature based watermarking using watermark template match[J]. Applied Mathematics and Computation, 2006, 177(1): 377-386.
- [6] O'Ruanaidh J J K, Pun T. Rotation, scale and translation invariant digital image watermarking[C]//Proceedings of International Conference on Image Processing. IEEE, 1997: 536-539.
- [7] Lin C Y, Wu M, Bloom J A, et al. Rotation, scale, and translation resilient watermarking for images[J]. IEEE Transactions on image processing, 2001, 10(5): 767-782.
- [8] Kim B S, Choi J G, Park C H, et al. Robust digital image watermarking method against geometrical attacks[J]. Real-Time Imaging, 2003, 9(2): 139-149.
- [9] Zheng D, Zhao J, El Saddik A. RST-invariant digital image watermarking based on log-polar mapping and phase correlation[J]. IEEE transactions on circuits and systems for video technology, 2003, 13(8): 753-765.
- [10] Kang X, Huang J, Zeng W. Efficient general print-scanning resilient data hiding based on uniform log-polar mapping[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(1): 1-12.
- [11] Song Q, Zhu G, Luo H. Geometrically robust image watermarking based on image normalization[C]//2005 International Symposium on Intelligent Signal Processing and Communication Systems. IEEE, 2005: 333-336.
- [12] Singh S P, Bhatnagar G. A robust watermarking scheme based on image normalization[C]//2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA). IEEE, 2018: 140-144.
- [13] Yang K, Wang W, Yuan Z, et al. Strong robust zero watermarking algorithm based on NSCT transform and image normalization[C]//2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). IEEE, 2018: 236-240.
- [14] Kutter M, Bhattacharjee S K, Ebrahimi T. Towards second generation watermarking schemes[C]//Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348). IEEE, 1999: 320-323.

- [15] 牛盼盼, 杨思宇, 王丽, 杨红颖, 李丽, 王向阳. 基于稳健特征点的平稳小波域数字水印算法[J]. 通信学报, 2019, 40(11): 187-198.
- [16] 张梦轩, 王曙光, 赵勇. 一种基于 SURF 特征点校正的二维码图像水印算法[J]. 计算机与数字工程, 2017, 45(12): 2498-2502.
- [17] 周波, 陈健. 基于奇异值分解的, 抗几何失真的数字水印算法[J]. 中国图象图形学报, 2004, 9(4): 506-512.
- [18] 任克强, 梁亮亮, 喻玲娟. SVD 与 HVS 相结合的小波域数字图像鲁棒水印[J]. 电子测量与仪器学报, 2017, 31(06): 869-875.
- [19] Qi H, Zheng D, Zhao J. Human visual system based adaptive digital image watermarking[J]. Signal Processing, 2008, 88(1): 174-188.
- [20] 黄继武. 一种自适应图象水印算法[J]. 自动化学报, 1999, 25(4): 476-482.
- [21] 陈磊. 基于混沌的图像加密与数字水印算法的安全性研究[D]. 北京邮电大学, 2018.
- [22] 靳强. 基于 DWT 的彩色图像数字水印算法研究[D]. 西安电子科技大学, 2014.
- [23] 王志雄, 王慧琴, 李人厚. 数字水印应用中的攻击和对策综述[J]. 通信学报, 2002, 023(11): 74-79.
- [24] 李雷达. 数字水印抗几何攻击理论及应用研究[D]. 西安: 西安电子科技大学, 2009.
- [25] Gonzalez R C, Woods R E, Masters B R. Digital Image Processing, 4th Edition[M]. Pearson, 2017.
- [26] 尤新刚, 郭云彪, 周琳娜. 峰值信噪比不宜用来评价信息隐藏技[C].//中国电子学会.全国第三届信息隐藏学术研讨会论文集. 2001: 51-56.
- [27] Wang Z, Bovik A C, Sheikh H R, et al. Image Quality Assessment: From Error Visibility to Structural Similarity[J]. IEEE Trans Image Process, 2004, 13(4).
- [28] 冉洪成. 基于对数极坐标的图像匹配综述[J]. 现代计算机, 2020(04): 65-69.
- [29] Lewis J P. Fast Normalized Cross-Correlation[J]. Circuits Systems & Signal Processing, 1995, 82(2): 144-156.
- [30] 鲍敏, 黄昌兵, 王莉, 等. 视觉信息加工及其脑机制[J]. 科技导报, 2017, 35(19): 15-20.
- [31] 杨曦晨. 基于 HVS 的主客观图像质量评价方法研究[D]. 南京理工大学, 2018.