

**本科毕业设计（论文）**

题目：基于水印和混沌系统的图像篡改

检测与自恢复

学 院： 计算机科学与工程学院

专业班级： 计算机科学与技术2017级1班

姓 名： 夏晓帆

学 号： 201701060329

指导教师： 孙承爱

完成日期： 2021年6月6日

教务处制

**BACHELOR'S DEGREE THESIS OF SHANDONG UNIVERSITY**

**OF SCIENCE AND TECHNOLOGY**

**Image Tampering Detection and Self-Recovery Based on Watermarking and Chaotic System Algorithm**

College： College of Computer Science and Engineering

Subject： Computer Science and Technology

Name： Xia Xiaofan

Directed by： Sun Chengai Professor

**QINGDAO CHINA**

学术声明：

**郑 重 声 明**

本人呈交的毕业论文，是在导师的指导下，独立进行研究工作所取得的成果，所有数据、图片资料真实可靠。尽我所知，除文中已经注明引用的内容外，本设计（论文）的研究成果不包含他人享有著作权的内容。对本设计（论文）所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确的方式标明。本设计（论文）的知识产权归属于培养单位。



本人签名： 日期：

摘 要

在当前数字网络多媒体通信技术和无线网络通信技术等快速发展的时代环境下，随着各种各样编辑软件技术的出现和开发，确保原始数字图像信息内容的完整性以及有效真实性等变得愈发重要。基于上述背景与需求，本文提出一种基于水印和混沌系统的图像篡改检测与自恢复，对于篡改区域它可以自动有效识别，借助隐藏于图像中的信息实现最终图像的近似恢复。

本文将图像划分为非重叠块，通过像素值自适应优化算法来提取每个块的有效信息，以混沌系统为技术依托产生伪随机链，借助伪随机链实现子块之间的关系映射，基于映射关系，将每个块提取出来的有效信息嵌入到对应映射块中。在嵌入过程中，提出改进的平滑功能对有效信息进行嵌入，这样可以使嵌入信息更贴合原始图像，同时也能尽最大程度地减少图像像素的改变。在对图像进行篡改检测时，使用了四层级的分层篡改检测算法，借助四层级篡改检测方案，对图像进行四层级的篡改检测。对于图像恢复，在传统一级恢复的基础上，使用自适应二次恢复策略即权值自适应算法，借助相邻块的内圈像素值进行恢复，从而达到更好的恢复效果。

通过实验的研究结果可以看出，本文提出的解决方案可以检测到拼贴攻击以及大面积的普通剪切攻击，同时图像恢复的效果十分理想，能够保证图像篡改检测率与理论值的一致性。总体而言，本文提出的方法更为通用和实用。

**关键词：**混沌系统；像素值自适应优化算法；平滑功能；分层篡改检测；权值自适应算法

**ABSTRACT**

In the current environment of the rapid development of digital network multimedia communication technology, with the emergence and development of various editing software technologies, to ensure the security of information content, the integrity, reliability, authenticity and effectiveness of the original image information content is becoming more and more important. Therefore, we propose image tamper detection and self-recovery based on watermarking and chaos system algorithms that can effectively identify the modulated area and achieve approximate restoration of the original image by utilizing the hidden information of the image.

In this paper, the image is divided into  non-overlapping blocks, the effective information of each block is extracted through the pixel value adaptive optimization algorithm, the pseudo-random chain is generated based on the chaotic system, and the relationship between the sub-blocks is realized by the pseudo-random chain. Mapping, based on the mapping relationship, embeds the effective information extracted from each block into the corresponding mapping block. In the embedding process, an improved smoothing function is proposed to embed the effective information, which can make the embedded information more fit the original image, and at the same time minimize the change of image pixels. When performing tamper detection on images, a four-level hierarchical tamper detection algorithm is used. With the help of a four-level tamper detection scheme, a four-level tamper detection is performed on the image. For image restoration, on the basis of the traditional primary restoration, an adaptive secondary restoration strategy, that is, the weight adaptive algorithm, is used to restore the inner circle pixel values of  adjacent blocks, so as to achieve a better restoration effect.

Through the experimental research results, it can be seen that the solution proposed in this paper can detect collage attacks and large-area common cutting attacks, and the effect of image restoration is very satisfactory, which can ensure the consistency of the detection rate of image tampering with the theoretical value. In general, the method proposed in this article is more versatile and practical.

**KEY WORDS:** Chaotic system, pixel value adaptive optimization algorithm, smoothing function, layered tampering detection, weight adaptive algorithm

**目 录**

**[第1章 绪论 1](#_Toc25620)**

[1.1 研究背景 1](#_Toc7266)

[1.2 国内外研究现状 2](#_Toc17846)

[1.3研究的目的与意义 4](#_Toc9839)

[1.4 本文的主要工作 5](#_Toc13269)

[1.5 论文结构 6](#_Toc27621)

**[第2章 相关技术综述 7](#_Toc5659)**

[2.1 数字水印技术 7](#_Toc1717)

[2.1.1 数字水印技术发展过程 7](#_Toc29669)

[2.1.2 数字水印技术概述 8](#_Toc2379)

[2.1.3 数字水印基本特征 8](#_Toc9317)

[2.1.4 数字水印技术分类 9](#_Toc10916)

[2.2 混沌系统 10](#_Toc5361)

[2.2.1 混沌的基本特征 10](#_Toc5087)

[2.2.2 混沌系统的应用 11](#_Toc32450)

[2.2.3 典型混沌系统 11](#_Toc25477)

[2.3 本章小结 12](#_Toc28587)

**[第3章 自恢复水印算法设计 13](#_Toc23514)**

[3.1 块映射 13](#_Toc26005)

[3.1.1 Logistic一维混沌映射 13](#_Toc7417)

[3.1.2 双伪随机链映射机制 14](#_Toc31423)

[3.1.3 块映射方案 15](#_Toc4231)

[3.2 水印生成 17](#_Toc20753)

[3.3 水印嵌入 19](#_Toc7230)

[3.4 分层篡改检测 21](#_Toc7433)

[3.5 图像恢复 23](#_Toc6565)

[3.6 本章小结 26](#_Toc29959)

**[第4章 实验结果及分析 27](#_Toc17582)**

[4.1 PSNR 27](#_Toc28677)

[4.2 拼贴攻击检测 29](#_Toc8205)

[4.2.1 第一类拼贴攻击检测 29](#_Toc14076)

[4.2.2 第二类拼贴攻击检测 32](#_Toc1416)

[4.3 大面积的普通剪切攻击检测 35](#_Toc1671)

[4.4 实验结果对比与分析 37](#_Toc2453)

[4.5 本章小结 38](#_Toc19071)

**[第5章 总结与展望 39](#_Toc21747)**

[5.1 总结 39](#_Toc2988)

[5.2 展望 40](#_Toc27699)

**[参考文献 42](#_Toc26554)**

**[致谢 44](#_Toc23616)**

# **第1章 绪论**

## 1.1 研究背景

在我国当今社会经济发展的整个过程中，信息已经逐渐成为最重要的社会资源之一，网络则更是已经逐渐成为了不能缺少和不能被替代的一个部分。与此同时，随着移动多媒体和其他移动通信通讯技术的不断普遍化快速发展，随着移动数字化和移动电信通讯设备的快速化发展，例如数字智能手机、数码相机、平板电脑等等，人们可以通过更为便捷的方式来获取各式各样的数字图像信息，数字图像信息的交换与传输也变得更为容易，人们可以借助各种类型的数字移动设备，将图像数字信息以及媒体信息等传送到不同终端，数字信息的传播范围和传输途径愈发广泛。除此之外，数字图像也已经被十分广泛地应用于各行各业中，它在给人们带来极大便利的同时，在信息交流的深度和广度方面，也都得到了相应的扩展。

人们日常生活中，在方方面面享受图像信息数字化所带来便利的同时，随之而来的副作用也越来越明显，涉及到不同领域以及不同类型与图像处理相关的软件数量不断增多，与此同时随着市场的需求，图像处理软件的功能也变得越发强大，使用趋向普遍化，这使得人们对于多媒体数据，可以毫不费力地进行各种各样的篡改，比如进行各种修改、再加工与再发布等。当某些带有恶意的个人和团队对数字形式的图像信息进行利益化的利用时，如果未事先征得所有者的同意，在这种情况下，信息极有可能遭到恶意攻击甚至篡改伪造，从而导致发生版权纠纷等复杂问题，因此在日常生活中，我们在享受着媒体信息数字化所带来便利的同时，对于知识产权以及信息泄露等问题都是不可忽略的，对于个人或者集体的利益而言，图像数字信息的安全及其保密性更是息息相关，同时也已经成为信息世界中的一个非常重要且迫切的议题。

一般会从版权和完整性这两个方面出发进行信息的保护，通过密码技术来实现保护信息的安全性与完整性，从密码技术这一方面来说，它主要是为了从更为特殊的角度，对加密信息的编码方式进行更为深入的探究，目的是为了使传输内容以密码形式掩饰原始内容，从而使得原始内容不会被轻易识别。由于信息技术的飞速发展，对于这种最为原始且基础的密码技术而言，一些非常规操作者已经可以借助使用运算的方式，对非法取得的已经被加密过的信息进行相应解密。因此，对于传统的数字签名技术，如果其中的内容被篡改，就无法再逆向恢复篡改前的信息内容，也就是说它只能对信息的完整性进行保护。

正是因为目前传统信息加密技术方法中，普遍存在以上所阐述的泄密问题，随着加密技术的不断发展，才可能会逐渐产生加密信息中的信息隐藏技术。近几十年信息安全隐藏分析技术一直是研究的重要热点之一，同时在电子信息安全技术领域内，它也是非常重要的一个分支[5~67]。它研究的主要内容是，在公共信息中进行秘密信息的隐藏，以公共信道为媒介，通过它进行隐藏信息的传输，信息接收者接收到对应的信号后，对其进行相应的提取与验证操作。信息隐藏技术与传统加密方法这两者最大的区别在于载体的公开性，对于信息隐藏技术而言，其欺骗性导致不易引起篡改攻击者的注意，与此同时也增加了破解的难度。

近几年随着技术的不断改进，信息隐藏技术也得到了飞速的发展，在篡改检测中得到了广泛的应用，篡改检测的主要内容是，对载体攻击性的检测以及对攻击区域的定位[8]。由于医学、法庭等领域的特殊性，因此在这些领域有着更为广泛的应用，它们的特殊性在于其载体信息都是被视为保护相应权益的有效证据，必须保证载体信息的真实性，从而需要通过篡改检测验证材料的有效性。

从以上可以看出，对于数字内容安全性而言，其真实性以及完整性等是非常重要的，它可以实现篡改图像的检测恢复等，并且近几年来越发吸引研究人员的注意。

## 1.2 国内外研究现状

互联网信息技术、多媒体以及现代数字通信技术的快速化发展，使得信息隐藏技术愈发吸引国内外学者进行更加深入的研究，现在将对其国内外的研究现状进行相应的总结。

于1994年举办了ICIP会议，在这次的会议上，R.G.van.Schyndel等人发表了一篇首次提出有关数字水印概念的学术论文：“A Digital Watermark”[5]。1996年，顺利举办了有关国际信息隐藏的学术会议，本次学术会议在英国的剑桥举办，此次学术会议的举办代表了一门新的有关信息隐藏学科的成立，也在理论方面为信息隐藏技术奠定了基础。从此各种相关的文章相继面世，在信息隐藏方面的深入探究也愈发变多。

从1998年开始以后的几年中，有关数字水印的国际会议又先后举办了几场，例如SPIE Security、IEEE ICIP等，同时有关数字水印的国际期刊也陆续问世[9]。一些比较著名的大学、相对知名的企业、以及世界各国的研究组织等都对其投入了非常大的重视程度，例如位于欧洲电信联盟、德国的Erlangen-Nuremberg大学以及微软公司等。始于上世纪的90年代末，出于市场的需要，水印产品在营销发酵下，才在市场上开始真正的面市。市场上出现的第一款产品是进行商用的软件，其中用到了数字水印技术，由Digimarc公司研发出这款产品，随后，市面上又出现了Photoshop等软件，这类软件主要是用于进行图像的相关编辑操作，数字水印则是作为插件集成的形式用来方便人们使用。

初始于上世纪的90年代末，国内对于这一方面的探究才逐步开始，于1999年举办了有关信息隐藏的相应学术研讨会，此次研讨会在我国国内的北京电子技术应用研究所举行。从这次研讨会之后，在拥有国家政策的支持下，越来越多的院校专注于数字水印的研究，由此也营造出了浓厚的科研氛围，在此推动下，国内的数字水印技术深入探究也取得突破性发展。

在2001年9月举办了有关数字信息隐藏的第三次全国性质学术研讨会，此次会议在西安顺利召开，其关注点在于对学术术语制定标准。在2002年8月24日举办了全国第四届国际数字信息技术隐藏领域学术专题研讨会，此次学术研讨会的成功举办，从各方面而言都推进了国内水印隐藏技术的科学研究与应用发展。从国家这一层面来说，由于其效能，因此加大了与信息安全等相关产业发展的重视力度。于2003年，在有关创新基金方面所提出的对应保护项目指南中，对与数字信息相关的知识产权以及与个人相关数码产品方面的保护做出了非常明确的指示，目的是为了防止信息数据的虚假伪造，保护产权合法性，国家对于这些方面都将予以非常重要的技术支持并推动其完整性发展[9]。

现在虽然在国内，数字水印的技术应用领域相比国外而言，还是仍然处于较为初级的发展阶段，但是，我国国内已经逐渐出现了许多与专业生产数字水印相关产品技术有关的公司，也或许正是因为这些数字水印专业公司的广泛存在与成功创办，使得在数字水印相关技术应用方面的深入研究，不再是浅层次地停留在理论研究的层面，而是逐步实现面向技术应用产业化和面向商业化，正是如此，才能在有效保证国内外水印信息技术产业发展与兴旺的同时，还在技术安全性和应用有效性两个方面为国内的水印信息安全技术产业发展提供出了相应的政策保障与技术支持。

## 1.3研究的目的与意义

随着我国现代工业网络通信技术的不断普及，计算机网络技术也由此开始得到了迅猛的进步发展，与数字信息、视频、音频等多媒体数据相关的应用与传播，也变得越来越广泛与便捷。然而在这些信息技术已经得到逐步发展情况的同时，在多媒体以及数字信息管理方面，其中发生的非法信息篡改和恶意传播，对于我们当今社会的安全管理方面已经带来了一个不可让人忽略的严重安全问题，如果非法的恶意篡改发生在刑事法庭上的证据、文献、医疗、国家安全等各个方面，对于未来社会上的影响以及其他经济损失而言都已经是不可估量的，因此不管我们是从整个国家安全层面角度出发还是从整个社会利益层面角度出发，保证个人信息安全等这个问题已经变得越来越重要，同时，对于如何认证这些多媒体信息源的真伪以及及时进行一些相应的安全保护，对于当今社会中的我们而言也是一个非常需要尽快解决的关键性问题，而且，在当今信息安全领域，这也已经成为研究的热点问题之一。

在上述技术背景下，由此才逐渐产生网络图像安全认证检测技术，针对上面所说的这些问题，此认证技术的主要目的其实就是通过鉴别和验证检测网络图像的完整性和真实性[10]。目前通过下面的两种认证方法，都已经可以实现图像信息认证技术：第一种方法是以数字签名为认证媒介，另一外两种方法是以数字水印以及图像处理技术为认证媒介，进行数字图像信息认证。于第一种而言，仅仅是在原始图像内采取最简单的内容附加，即进行数字签名信息的基础添加，通过进行数字签名信息以及存在于图像内附加数字信息的计算，实现图像相应的认证操作以及实现数据的匹配，通过上述操作完成图像的篡改检测，这种方法的实现相对而言是比较方便的并且计算量也比较小，但是由于需要额外添加相应的签名信息，因此这种方法不可能进行盲认证。对于另一种方法，则完全克服了第一种方法使用中的一些缺点，另一种方法也就是将图像信息全部隐藏于原始的图像，在这个隐藏过程中，不必再需要图像附加额外的图像签名或者信息。对上面两种方法进行分析对比，鉴于这种方法中的优点，越来越多的数字水印研究技术工作者对基于数字水印图像认证技术的各个方面，不断进行更深一步的研究和更深一个层次的扩展，从中发现取得的研究成果对于数字图像水印认证以及数字水印应用技术的进一步研究发展而言，有非常重要且具有关键性的促进作用。

数字水印隐藏技术在当今社会中的广泛使用，对于许多学术研究工作者而言，使得向多媒体信息中正确嵌入不可见隐藏信息已经成为了一种可能，其主要作用目的也就是，在原始化的多媒体信息中正确进行秘密信息的隐藏，并且为了保证所有数字水印产品的知识版权及其真实性和可靠性，由于嵌入数字水印后的原始多媒体信息数据并没有明显的增量降质优化表现，所以其对隐藏数据信息的正确嵌入并不直接影响其实际使用价值。因此对于数字水印信息技术的深入研究而言，具有非常高的实际意义与价值，并且也可以为国内此领域研究提供相应的素材。

## 1.4 本文的主要工作

通过认真查阅与数字水印信息技术发展相关的专业论文和获取相应的学术研究成果，对国内外相关学者已经成功实现的数字水印信息相关处理算法进行深入的研究了解和分析研究，本文通过结合已经成功实现了篡改定位算法方面相关的经验，并且结合可以对已经篡改的区域进行图像恢复的图像认证算法方面取得的研究经验，对数字隐藏技术进行进一步的研究，实现相应的篡改检测以及自恢复。

本文主要完成了以下几个方面的工作：

（1）深入理解学习和充分了解混沌系统，通过实现混沌映射来获取块映射序列。先将整个图像按照既定大小划分为许多非重叠的块，以块为计算单位，进行整个图像的混沌置乱操作，通过混沌置乱操作可以得到不同子块映射序列，从而确保隐藏信息与原始图像块之间嵌入位置关系的随机性，同时也可以保证嵌入隐藏信息后图像的质量。

（2）使用像素值自适应优化算法提取恢复信息，同时对现有的平滑功能进行改进优化，使嵌入信息后的像素与原像素更加切合。提取信息时使用像素值自适应优化算法，嵌入过程中使用改进的平滑功能，使得改进后的值仍可以近似地表示图像信息，同时也实现了对原始图像最小程度的改变。

（3）对图像的分层篡改检测算法进行深入研究，研读图像分层篡改检测算法并且对其进行分析，借助分层篡改检测算法来实现对图像更为细致的篡改检测。

（4）深入学习与图像恢复有关的算法，借助权值自适应算法实现第二层级的篡改恢复。传统二级恢复的基础上，在一定区域内，借助原始有效块与一级恢复有效块设置对应的权重，从而可以达到更好的效果。

（5）利用MATLAB R2017b实现相应算法，进行仿真实验测试。

## 1.5 论文结构

第1章 绪论。介绍了本文的研究背景，国内外研究的现状，研究完成的目的与意义以及本文完成的主要工作。

第2章 相关技术综述。介绍了本文涉及的相关技术“数字水印技术”以及“混沌系统”。

第3章 自恢复水印算法设计。介绍了双伪随机链形成机制，详细描述了如何进行块映射、水印的生成与嵌入、篡改检测以及原始图像恢复，并且对算法的实现步骤进行了详细说明。

第4章 实验结果及分析。对实验的结果进行展示，同时对实验结果进行详细的对比分析。

第5章 总结与展望。对各章内容要点进行简要分析总括，并详细分析各种算法的具体利弊。

# 第2章 相关技术综述

## 2.1 数字水印技术

### 2.1.1 数字水印技术发展过程

700年前就已经有人工造纸术，其中所涉及的水印知识，在那个时代就已经被广泛地应用于识别商标，作为区分纸张的规格、重量以及质量等判断标准[7]。但是随着当今社会计算机技术以及网络等发展，与版权、知识窃取等相关问题，又逐渐成为当今社会的一个焦点，在上述问题的推动下，数字水印由此诞生。

1961年，在一个美国公司的Enlil Hembrooke进行了专利的申请，他所申请的专利与水印相关，这项专利核心技术研究的主要内容是，将可以标识某一个艺术品的数字信息码嵌入到相应作品中，借助嵌入的识别码信息，从而来证明其艺术所有权。

始于1994年Tirkel等人写的一篇文章，才真正开始有了与数字水印技术发展相关的理论实践论述。同一年，Van Schyndel发表了一篇明确讲述相关于水印的一些关键性技术概念的论文，学术文章的题目为“A digital watermark”，在这样一篇文章中还指出有关于鲁棒水印相关性检测的使用方法，这无疑是一篇与水印相关且非常关键的学术文章。数字水印相关实际价值的新一轮大规模飞速发展始于上世纪90年代，从那个时候开始，就已经逐步成为水印研究界的焦点[7]。

在1996年5月举办了国际上第一届有关隐藏学术的研讨会，此次研讨会举办地点是英国的剑桥牛顿研究所，这次会议之后，产生了与数字水印相关并且涉及信息隐藏性质的学科。

在国际浓厚的研究背景下，此领域内，中国也已经有一批非常有实力的科研机构进行深入的研究。在2000年由研究水印方向相应专家们联合发起召开了有关数字水印的学术研讨会，这次会议上对数字水印方面涉及到的一些关键性技术，研究专家们对此进行了深入探讨。现在数字水印方面的研究已更加深入，相应的研究成果也较为丰硕，在国内外的期刊上也已经发表了相当数量的论文。

当代信息社会中，数字水印应用相关的研究软件不断涌现，例如当代的Photoshop、WbStego等，其中早在Photoshop中就已经加入了数字水印的应用功能；WbStego支持对于BMP、文本等文件信息的隐藏。

### 2.1.2 数字水印技术概述

新兴的数字水印处理技术基本设计思想是向原始媒体文件中嵌入数字信息的同时保证不影响原始文件的正常传输使用，即将具有某些特殊意义的秘密信息嵌入水印到数字图像、视频等多媒体文件中，同时还能不影响文件的常规使用等操作，由于其具有隐藏性所以还能不被轻易察觉，从而可以有效保护相关产品知识版权，也可以及时证实相关产品的真实性等。其中，对于嵌入到数据文件中的秘密信息，人们把它被称为数字水印，它有多种表现形式，既可以是随机序列，也可以是图像、文字等具有某些特殊含义的信息[11]，通常秘密信息都需要进行适当合理的变换，然后再嵌入到数字产品中。

在各种类型的工作场所中，数字水印已经得到了广泛的商业应用，同时也已经开始可以用来实现不同的工作目标，虽然每个目标不同，但是数字水印的工作机制是有着共通性的，本质都比较相似，通常都认为是包含水印的生成、嵌入以及检测或认证这三个大部分[7]，其框架图如图2.1所示。根据不同的水印图像生成算法来自动生成相应的原始水印图像信息，按照所设计的不同嵌入方式，将水印嵌入到最初始的图像中，由此则形成水印图像。传输水印图像的过程中，可能会受到不同方式和类型的攻击，在接收到疑似篡改的图像之后，利用设计好的篡改检测算法对水印信息进行相应的提取同时进一步认证图像的真实性。

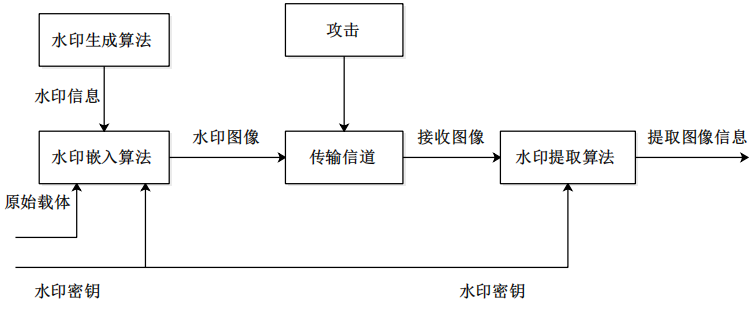


图2.1 水印机制框架图

### 2.1.3 数字水印基本特征

数字水印有许多特征，其中最主要的特征是包括鲁棒性、透明性和安全性等[7~8910]，根据将要应用场所的不同，构建水印系统时，所考虑的特征也不尽相同。

（1）鲁棒性

指在数字图像信息中嵌入的水印数据，在经过一系列不同方式的攻击以及传输处理等非常规操作后，仍然可以存留的能力，也可以理解为对于各类恶意篡改的防御程度，它要求嵌入图像的水印信息在经过不同类型的图像变换后，对于隐藏于图像内的水印信息仍然可以完整得到。

（2）透明性

指在经过水印机制后，不会使原始载体产生较大的变化，即尽最大可能的减小嵌入隐藏数据后的信息与原始信息的差距，同时也保证失真的程度尽可能减小，水印的嵌入过程尽最大可能的不引起注意。

（3）安全性

防止因为信息样式的变化而遭受一些非必要的影响，将信息嵌入到原始数据的中间部分，而非文件头等极其容易被发现的地方。

### 2.1.4 数字水印技术分类

可以从多种技术角度对数字水印技术应用进行不同的分类，同时从多种技术角度分析出发，也可以同时得到既有联系又有一定区别的不同分类分析结果[7~8910]。

（1）水印可见性分类

根据水印的具备可见性将水印大致划分两类为具备可见性的水印以及不具备可见性的水印。其中不可见水印是将信息隐藏在数字作品中，仅仅靠肉眼是无法观察到的，它可以隐藏包括版权等其它信息，是为抵抗非法使用者而做的准备，此类水印的应用范围也愈发广泛。可见水印则通过比较直接的方式对版权所有者进行标明，通常会有较为明显的标志性信息，会明显地引起载体信息的变化，虽然不会严重影响载体信息本来的样貌，但还是会降低载体信息的质量，从而导致水印安全性能比较差。因此，不可见水印成为更多水印技术研究者的选择。

（2）根据抗攻击性能分类

依据水印算法的抗攻击性能，可以把水印划分三类为半脆弱性水印、脆弱性水印以及鲁棒性水印。脆弱性数字水印很容易随着图像信息的修改而受到破坏，即使是非常细小的水印信息改变，也可能会直接影响数字水印的完整提取验证检测，为此，脆弱性数字水印主要广泛地应用于数字水印产品内容完整性的提取验证检测方面。半脆弱性水印一般来说，不会受到一些常见错误操作的影响，比如微弱的噪声以及各种常见的水印编码操作等，这种类型的水印比起前一种在鲁棒性方面有稍微的增进。鲁棒性水印具有非常强的抗干扰的能力，可以抵抗各种类型的恶意攻击，通常作为产品版权标志，在经过各种恶意攻击以及篡改处理之后，仍可以被提取出来。

（3）根据水印的检测过程分类

根据水印的检测操作过程将水印的种类依次细致地分为非盲水印和盲水印两种。非盲水印因为它们具有私有的特性，因此在进行检测的时候需要与初始信息相结合，它有较好的鲁棒性，但是需要较高的存储以及维护的成本，同时信息泄露的可能性很高。盲水印具有一定的公有化特性，任何时候进行不同的检测，只需要直接用到特定的密钥信息即可，不会直接使用户用到初始化的信息，因此其检测成本以及技术风险都可以大大降低，实用性也会更好，也是现在大多数水印算法中，所采取的主要检测方式。

## 2.2 混沌系统

混沌中的动力系统与一般认为具有高度确定性的流体动力系统之间可能有一定的的非线性测量差异，混沌中的动力系统一般指它是一种复杂且线性无法完全确定的非线性测量动力系统[12]，其运动时的混沌轨迹是不规则、无法预测且不可重复的，但同时又不会离开某一特定区域。

### 2.2.1 混沌的基本特征

虽然混沌动力系统的物理运动非常复杂，但是每个混沌动力系统都会具有其独特的运动特征，混沌动力系统的主要运动特征描述如下[12~131415]：

（1）内在随机性

混沌系统随机性的表现与外部随机噪声完全无关，它是一种噪声表现源于系统内部自发发生变化时，内部所产生的不规则性与随机性。对于某个系统而言，由于外界的干扰，可能会出现或者不出现某种状态，这是由外界因素引起的，但是其自身不会出现这种随机性。而对于混沌系统，它的随机性是在内部作用下引起的，与初始值的敏感性相关联，即使是有确定的方程，其内部状态还是随机的，不具有任何的周期性和规律性。

（2）初始值敏感性

对于混沌而言初始条件即使是发生了极其细微的调整，但是它在经过混沌系统的运算扩大后，最后的混沌状态非常不同。对于混沌系统而言，各种类型的混沌状态对于初始条件都带有非常强烈的依附性和敏锐性，即使最初始的两个值相差极小，但是经过多次迭代变化，其运行轨迹还是千差万别。

（3）不可预测非周期性

由于混沌系统对初始值的高度依赖性与对数值的敏感性，运动状态的稳定性也非常的差，从而使得人们无法对混沌的运动状态进行正确的预测。

（4）局部不稳定性

混沌系统在受到来自外界的扰动时，是不会改变系统原有性能的，但是系统运动的行为非常强烈地依赖于初始条件。

### 2.2.2 混沌系统的应用

混沌系统在现代信息安全相关技术领域中的广泛应用主要如下，信息安全技术涉及关系到信息的保密性、可控性、完整性以及技术可用性，密码学技术是现代信息安全的技术核心，而混沌密码系统由于能够具有良好的伪随机性、状态的不可预测性以及安全局部不稳定性等与密码学要求相似的特性，因此混沌序列被广泛应用于密码学方面[15]。

于上世纪80年代在密码学的计算方面最先提出了混沌序列在其中的广泛应用，从此开始了一定的发展[12]。1990年后它开始逐步兴起，主要在两个学术研究方向进行重点应用，一个方向是主要基于在保密系统相关领域内的模拟加密混沌，另一个则是基于数字计算机局部传输精度下的加密数字混沌系统。

混沌不仅是一种非线性普遍存在的数学现象，而且其数学行为随机且复杂，却又必然存在其内在数学规律性，具有非常丰富的物理时空空间动态，因此混沌已经发展成为一种新颖的数学优化计算技术并且已经受到了非常广泛且深入的科学研究。

### 2.2.3 典型混沌系统

（1）Tent一维混沌映射

Tent映射是一种分段线性映射，其函数表达式如公式（2.1）所示：

 （2.1）

在上是混沌的，但是Tent映射具有概率密度函数如公式（2.2）所示：

 （2.2）

所以对Tent表达式进行进一步的改进，其计算公式如（2.3）所示：

 （2.3）

（2）Arnold二维混沌映射

Arnold变换的映射表达的形式是非常简单而且具有周期性的，使用起来非常方便，表达公式如（2.4）所示：

 （2.4）

由于混沌系统是灵活多变的，是不固定的，因此以Arnold变换为基础，对其数学公式进行拓展，其表达形式如公式（2.5）所示：

 （2.5）

数字量化即改变的取值，将的取值从实数范围改变到正整数范围，如果初始值出自于正整数则相关函数具备相应的周期性，但是如果初始值是任意选择的则函数将处于混沌的状态。

## 2.3 本章小结

在数字水印技术方面，从发展过程、技术概述、基本特征以及分类四个方面进行了详细的介绍。在混沌系统方面，从基本特征、应用以及典型的混沌系统三个方面进行了深入阐述。

# 第3章 自恢复水印算法设计

本文提出的自恢复水印方案由块映射、水印生成、水印嵌入、分层篡改检测以及图像恢复五个部分构成，图3.1展示了水印生成和嵌入过程的流程图，图3.2展示了篡改后图像恢复的流程图。

图3.1 水印生成和嵌入流程图



图3.2 篡改后图像恢复流程图

## 3.1 块映射

### 3.1.1 Logistic一维混沌映射

Logistic一维混沌映射在所有的混沌模型中极具有典型性，逻辑映射又是动态系统、混沌等多样性系统最基础的模型，这个系统具有非常复杂的动力学行为，由于它的简便、随机性，它被非常广泛地应用于水印嵌入技术[16]，其数学表达公式如（3.1）所示：

 （3.1）

其中是混沌序列的迭代次数，是逻辑映射系统的控制参数。

对于任意的，当时[18,19]，混沌映射都具有混沌的基本特征，也就是说，在Logistic混沌映射的作用下，由初始混沌条件生成的序列是非特定周期的、不完全收敛的，而除上述初始条件之外，生成的混沌序列必将收敛于某一特定的周期值，它构成了算法中需要的伪随机链。

当时，该映射的概率分布函数如公式（3.2）所示：

 （3.2）

如图3.3所示，呈现了与Logistic映射相对应的分岔图[26]。

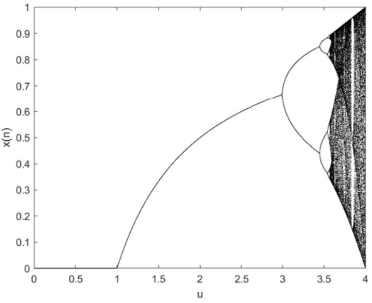


图3.3 Logistic映射分岔图

### 3.1.2 双伪随机链映射机制

在Logistic一维混沌映射的基础上，双伪随机链是两个具有不同的混沌序列，并且它具有以下特征[25]：

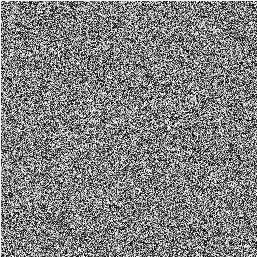
（1）双伪随机链之间的两个映射函数关系必须是一对一的，而且不会相互重复，不会同时发生一对多或者多对一的映射情况。

（2）双伪随机链的映射关系都是非常独特的，它们全部由初始参数所决定，而且对初始参数非常的敏感，同时也非常依赖于初始参数，初始参数不同，生成的序列也不相同，从而确保映射序列的独立性。

（3）双伪随机链的相邻元素彼此相距较远。

图3.4用于检测伪随机链的安全性，置乱图的初始参数为并且。图3.4（a）是一个大小为的8位灰度Lena图像，图3.4（b）是根据Logistic一维混沌序列进行置乱后的图像。

例如，原始像素向量为[102，64，93，53，72，100，100]，原始像素的索引向量为[1，2，3，4，5，6，7]，通过伪随机链得到的映射索引向量是[5，2，7，1，3，4，6]，因此，可以得到重新排序后的像素向量为[72，64，100，102，93，53，100]。从图3.4中可以看出，在加扰之后，两幅图像几乎没有相似性，从而证明了伪随机链的随机性和安全性。

（a）原始图像 （b）加扰图像

图3.4 伪随机链的安全性

### 3.1.3 块映射方案

映射序列可以表示为，该映射序列意味着块A的恢复信息隐藏在块B中，块B的恢复信息隐藏在块C中，块C的恢复信息隐藏在块D中，以此类推。通过以上表述可以看出，对于一个映射序列而言，其最重要的部分是在一个非常大的篡改率的情况下，确保恢复信息的存在，借助恢复信息，对图像进行相应的恢复。但是通过研读现有的映射方法，发现其中存在以下问题，利用一维变换算法构建块映射关系函数时[1,4]，在这个方法中，尽管序列是随机的，但是同一列中的其余元素都是相等的，因此，在遇到对列进行篡改时的性能非常差；为了保证序列的随机性，采用Arnold变换算法[20]，但由于这个算法是具有周期性的，因此并不安全；在一些映射方法中，基于Arnold变换算法加入了重映射机制[21]，即对于映射到原始块周围的块进行重新映射，这样做虽然水印图像的安全性获得了提高，但是，当拐角篡改率超过25%的情况下，将会失去25%的水印，重新映射的机制就无效了，同时会严重影响图像的质量。

为了解决以上提出的这些问题，本文采用双伪随机链的映射方式来生成相应的块映射序列。假设是一个大小为的8位灰度图像，其中。将图像进行无重叠分割，最终每个无重叠图像块的大小为，具体划分形式如公式（3.3）所示：

 （3.3）

将不同的初始值带入公式（3.1）中，通过计算可以产生两个不同的伪随机块索引序列，把这两个不同的伪随机块索引序列标记为和，将伪随机链中的块数据嵌入到对应映射块的高5位，将伪随机链中的块数据嵌入到对应映射块的中间5位，映射序列的值如公式（3.4）、公式（3.5）以及公式（3.6）所示：

 （3.4）

 （3.5）

 （3.6）

公式（3.4）、公式（3.5）以及公式（3.6）的含义为，块的恢复信息嵌入到块的高5位，块的恢复信息嵌入到块的中间5位，、和分别是中的元素，而且、和代表大小为2×2图像块的块标签，它们的块映射关系如图3.5所示。

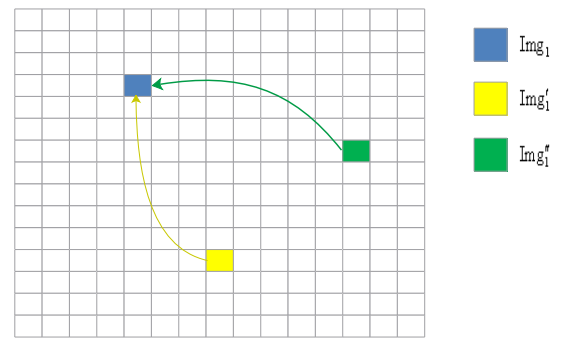


图3.5 块映射样例

## 3.2 水印生成

在基于DWT和DCT的以及图像块水印生成的过程中[21]，这些方法可以获得更多的嵌入信息，同时也可以使得嵌入图像的质量更高。但是，在这种情况下，对于块的影响还是比较显著的，对于较小篡改率的检测会出现很明显的错误，而且虚警错误率会很高。

为了解决以上提出的这些问题，将图像分割为的非重叠块，但是，按照这样的方式对图像进行分割，导致能够嵌入图像块中的信息变得非常有限，最大嵌入容量仅仅为12位。为此，参考当前使用划分图像块相关论文中恢复信息的生成，然而在参考这些论文的过程中，发现了以下问题：当恢复信息是基于图像块高5位平均值生成时[1,4]，这对于平滑图像块篡改的恢复效果更好，但是，此方法对于纹理块的篡改恢复效果非常差；也有的方法中提出了一种变长恢复信息构造方案[22]，对于纹理和平滑块，分别使用不同的位数进行图像相应块的恢复，尽管它可以更好地表示纹理信息，但会影响嵌入的信息位，从而导致在篡改检测方面变得更加困难。

为了更好地解决以上提出的问题，本文使用种像素值自适应优化算法，使嵌入的值能够更好且更相似地表达图像块信息，整个流程如图3.6所示。

图3.6 水印产生过程图

通过映射序列和，将块和块的恢复信息嵌入到块中，块和块的四个像素表示为和，由以及的高5位组成恢复信息，由于获取块恢复信息的方法与获取块恢复信息的方法相同，因此，将获取块恢复信息的方法作为示例，进行相应的介绍。

块恢复信息的最大值和最小值可以通过公式（3.7）和公式（3.8）得到：

 （3.7）

 （3.8）

代表恢复信息，那么，并且。为了使嵌入值能够更好地反映图像块的实际值，使用公式（3.9）来获得图像块的最佳嵌入值：

 （3.9）

块高5位恢复信息可以通过公式（3.10）计算得到：

 （3.10）

同样的块的高5位恢复信息可以通过公式（3.11）计算得到：

 （3.11）

通过上述方法，可以得到10位的恢复信息和，同时，可以通过公式（3.12）和公式（3.13）计算产生2位的认证信息和，下面公式中是异或操作，是取反操作：

 （3.12）

 （3.13）

最后，可以通过公式（3.14）计算得到嵌入到块中的水印值，其中是二进制字符按位方式进行拼接的运算符：

 （3.14）

为了方便表示，由表示。

## 3.3 水印嵌入

水印嵌入的详细过程如图3.7所示。

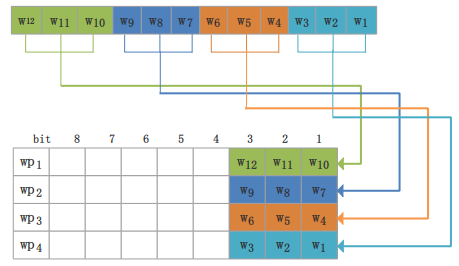


图3.7 水印嵌入过程图

步骤一：将大小为的图像进行分块处理操作，其分割后成为个数是的非重叠图像块，其中每个非重叠图像块的大小表示为，并且每个图像块。

步骤二：使用两个不同的初始值，生成两条无关的伪随机链和，相关的生成方法参照3.1部分。

步骤三：参照3.2部分使用的方法，计算将要嵌入的恢复信息和认证信息，并且最终得到整个水印信息。

步骤四：将嵌入到对应的图像块中，但是如果将恢复信息直接嵌入到原始图像的低3位，那么图像的质量将会受到非常大的影响。现有的平滑功能对于提高嵌入信息后图像的质量有很大帮助，但是仍然有弊端，因此，本文对现有的平滑功能进行修改[1]，修改后的平滑功能如公式（3.15）和公式（3.16）所示：

 （3.15）

 （3.16）

在公式（3.15）和公式（3.16）中，是将要被嵌入的值，是原始图像的值，是和原始图像低3位的差值，是由平滑功能生成的将要被嵌入到图像中的嵌入值。

公式（3.15）和公式（3.16）的原理是，在不影响将要嵌入低3位值的情况下，从嵌入的像素值中添加或者减去8，但是它将会减少嵌入图像值和原始图像值之间的差值。例如，，那么，使用公式（3.16），可以得到嵌入值，原始像素值和嵌入像素值的差值变为，比最初的差值6小，因此，在没有改变的情况下得到了更好的嵌入像素值。

## 3.4 分层篡改检测

首先，对将要进行篡改检测的图像进行分块，把它划分为的非重叠块，详细的篡改检测方案如下：

步骤一：使用与3.3节中同样的初始值，生成两条无关的伪随机链和。

步骤二：使用公式（3.17）从当前块的这四个像素中提取12位水印信息。

 （3.17）

使用公式（3.18）对进行定义：

 （3.18）

步骤三：第一层级篡改检测。

通过第3.2节，可以非常容易地得出，如果某个图像块没有被恶意篡改，那么将会分别满足公式（3.12）和公式（3.13）两个公式，因此可以对进行数据计算并与进行数据的比较，同时对进行数据计算，并与进行数据的比较。如果两个运算中任何一个比较的结果不完全的相等，那么当前块将被标记为无效块。

步骤四：第二层级篡改检测。

如果当前块在第一层级篡改检测中被检测为有效块，则继续进行第二层级篡改检测，使用公式（3.19）和（3.20）对进行解码并得到恢复信息。

 （3.19）

 （3.20）

通过3.2节，可以很容易地看出，有效块的和将满足公式（3.10）和公式（3.11）。因此，如果并且，那么当前块为有效块，否则当前块为无效块[17]。

步骤五：第三层级篡改检测。

如果当前块在第二层级篡改检测中被标记为有效块，则继续进行第三层级篡改检测。

对当前块的相邻块进行检测，的相邻块如图3.8所示，相邻块被划分为4个三元组，它们是,如果其中任何一个三元组是无效的，那么当前块就被标记为无效块[1]。

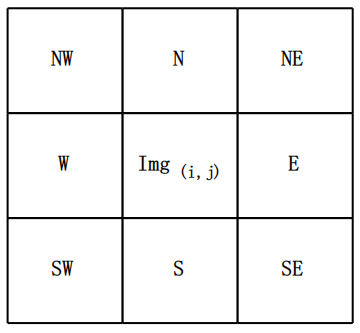


图3.8 当前块的四个三元组

步骤六：第四层级篡改检测。

如果当前块在第三层级篡改检测中被标记为有效块，则继续进行第四层级篡改检测。

如果当前块的相邻块中，有4个以上的无效块，那么当前块就被标记为无效块[17]，如图3.9所示。

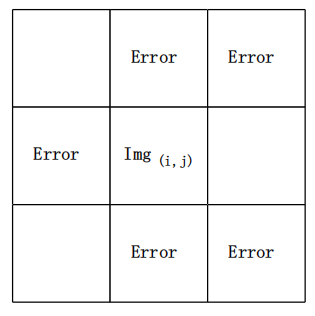


图3.9 当前块的相邻块

## 3.5 图像恢复

当完成上述的四层级图像篡改检测后，接下来要对被标记为无效块的部分进行恢复操作。为了使恢复图像具有更高的质量，本文设计了一种优化二次恢复方案。假设被标记的无效块是，则通过可以得知它的恢复信息隐藏在块和块中。

第一层级篡改恢复的详细步骤如下：

步骤一：如果是有效块，那么直接跳到步骤二。如果是无效块，那么直接跳到步骤三。

步骤二：从块的低三位中提取水印信息，并且通过公式（3.21）来得到恢复值，然后直接跳到步骤四。

 （3.21）

步骤三：如果是无效块，那么就被标记为无效块。如果是有效块，那么从块的低三位中提取水印信息，并且通过公式（3.22）来得到恢复值，然后直接跳到步骤四。

 （3.22）

步骤四：使用恢复当前无效块。

如果块和块都是无效块，那么就不能通过提取恢复信息的方法来恢复当前的篡改块，当碰到高篡改率时更容易发生块和块都是无效块的这种情况，因此第二层级篡改恢复策略的设计对于图像恢复是非常重要的，本文设计了一种权值自适应算法来进行第二层级的篡改恢复。

第二层级篡改恢复的详细步骤如下：

步骤一：在的相邻块中，其中代表原始有效块的数量，代表原始有效块的像素权重，代表原始有效块的像素值。代表第一层级恢复有效块的数量，代表第一层级恢复有效块的像素权重，代表第一层级恢复有效块的像素值。代表未恢复块的数量，未恢复块对应的像素权重为0。是原始像素块权重与恢复像素块权重的比值，它的值通常是1.5或者是2[17]，通过公式（3.23）和公式（3.24）可以计算出和：

 （3.23）

对方程（3.23）进行求解，可以得到和如公式（3.24）所示：

 （3.24）

当前无效块的像素值可以通过公式（3.25）计算的到：

 （3.25）

可以通过以下的步骤证明：

假设是和的最大值，是和的最小值，同时能够很容易地得到，那么通过公式（3.25）可以得到公式（3.26），从而可以证明。

 （3.26）

使用同样的方法，也可以证明，如公式（3.27）所示：

 （3.27）

因此，从而可以保证修改后的像素值不溢出。

恢复步骤流程图如图3.10所示，棕色块代表篡改后的恢复块，紫色块代表原始有效块，蓝色代表无效块。从下图中可以看出，，设置，通过上述公式，可以计算得到原始块的权重和恢复块的权重是，最后可以通过公式（3.25）计算。

步骤二：使用恢复无效块。

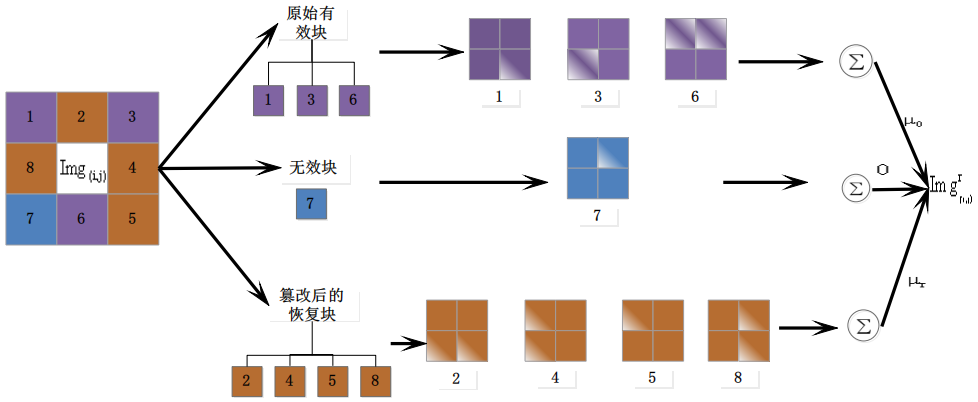


图3.10 恢复步骤过程图

## 3.6 本章小结

首先对Logistic一维混沌映射进行分析，介绍双伪随机链映射机制，以及如何由映射系统生成双伪随机链，对块映射方案进行了详细的描述。然后介绍水印生成过程，使用像素值自适应优化算法生成水印信息。紧接着在水印嵌入部分，提出了一种改进的平滑功能来提高嵌入图像的质量。随后，在图像篡改检测过程中，使用四层级篡改检测方案。最后，在图像恢复的过程中，在传统一级恢复的基础上，使用权值自适应算法，借助自适应二次恢复策略，对图像进行二层级篡改恢复。

# 第4章 实验结果及分析

对篡改检测中提出方案的性能进行了一系列分析和仿真，攻击的种类包括拼贴攻击以及大面积的普通剪切攻击。同时还将性能与现有的基于块的方法[1,3]进行了比较，本实验中使用到的数据集是从国外某数字图像处理著名实验室的数据集网站下载，所有仿真环境均为MATLAB R2017b。

## 4.1 PSNR

PSNR（Peak Signal to Noise Ratio）即图像的峰值信噪比，在图像信号处理技术领域，经常可以使用测量峰值信噪比来将其作为图像质量优化检测中的标准，它不仅可以用来测量与原始图像之间的抖动偏离水平程度，同时它也是一种对水印图像抖动失真水平程度和图像噪声失真水平程度进行综合衡量的一个重要标准[23,24]，如果两幅图像之间的PSNR比值越大，则也就表明两幅图像之间更加相似，同时也表明图像的失真程度越小，其中它以30dB为基准，PSNR为30dB以下的图像质量较差，其计算方法如公式（4.1）和公式（4.2）所示：

 （4.1）

 （4.2）

表示均方差，表示某图像点所有颜色的最大像素取值，例如8位原始处理像素图像的取值为255，与分别代表原始图像和重构图像相对应像素点的像素值。

表4.1显示了使用优化后平滑功能对于嵌入水印的影响，PSNR值越大表明图像质量越高，从表中可以看出，使用优化后平滑功能嵌入信息后图像的质量都高于未使用优化后平滑功能嵌入信息的图像。由于本文使用了改进的平滑功能，因此整体上得到的水印图像质量更高，并且比理论值37.9dB[24]高约2.80dB。

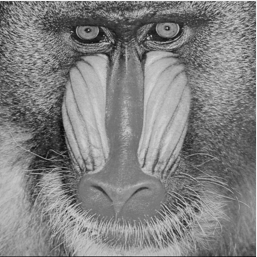
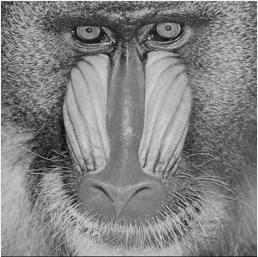
表4.1 未使用平滑功能和使用平滑功能的PSNR比较（dB）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 图像 | Lena | Baboon | Barbara | Peppers | Cameraman |
| 未使用优化后平滑功能 | 38.2001dB | 38.3030dB | 38.3023dB | 38.3441dB | 38.1844dB |
| 使用优化后平滑功能 | 40.7215dB | 40.7084dB | 40.6967dB | 40.7496dB | 40.7465dB |

图4.1是本文使用优化后平滑功能嵌入水印和未嵌入水印前后图像效果的对比，的8灰度Lena图像、的8位灰度Baboon图像、的8位灰度Barbara图像、的8位灰度Peppers图像和的8位灰度Cameraman图像用于进行检测后的模拟，图4.1的（a1）-（e1）是原始图像，图4.1的（a2）-（e2）是本文使用优化后平滑功能进行水印嵌入后的图像。

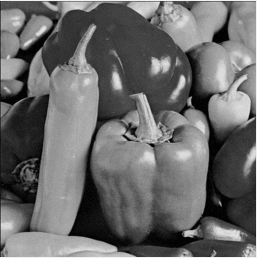
（a1）Lena原始图像 （a2）Lena嵌入水印后图像

（b1）Baboon原始图像 （b2）Baboon嵌入水印后图像

（c1）Barbara原始图像 （c2）Barbara嵌入水印后图像

（d1）Peppers原始图像 （d2）Peppers嵌入水印后图像

（e1）Cameraman原始图像 （e2）Cameraman嵌入水印后图像

图4.1 使用优化后平滑功能前后效果对比图

通过仿真实验测试，可以得出仅仅通过肉眼，是无法观察到原始图像与使用优化后平滑功能嵌入水印后图像之间的区别。

## 4.2 拼贴攻击检测

进行两种拼贴攻击检测，第一种是将当前图像的某一块拼贴到同一图像的不同位置，第二种是将当前图像的某一块拼贴到另一个图像的某一位置。

### 4.2.1 第一类拼贴攻击检测

256×256的8位灰度Lena图像用于模拟第一类拼贴攻击，拼贴攻击操作是将图像中坐标（48,42）至（211,125）的块粘贴到坐标（48,134）至（211,217）的图像块中，理论上篡改率为，图4.2（a1）-（d1）是本次模拟的结果。

图4.2（a1）它的PSNR值是40.7215dB，图4.2（b1）检测是图4.2（a1）在受到第一类拼贴攻击后的检测结果，图4.2（c1）是篡改检测结果。如该图所示，本文中的方法可以检测到第一种拼贴攻击，并且篡改检测率是22%，这与理论值是一致的。图4.2（d1）是基于图4.2（b1）图像自动恢复的结果，其PSNR为32.3479dB。

256×256的8位灰度Baboon图像用于模拟第一类拼贴攻击，拼贴攻击操作是将图像中坐标（40,40）至（210,110）的块粘贴到坐标（40,130）至（210,200）的图像块中，理论上篡改率为，图4.2（a2）-（d2）是本次模拟的结果。

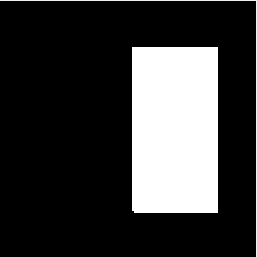
图4.2（a2）它的PSNR值是40.7084dB，图4.2（b2）检测是图4.2（a2）在受到第一类拼贴攻击后的检测结果，图4.2（c2）是篡改检测结果。如该图所示，本文中的方法可以检测到第一种拼贴攻击，并且篡改检测率是19%，这与理论值是一致的。图4.2（d2）是基于图4.2（b2）图像自动恢复的结果，其PSNR为32.8510dB。

256×256的8位灰度Peppers图像用于模拟第一类拼贴攻击，拼贴攻击操作是将图像中坐标（116,27）至（166,97）的块粘贴到坐标（30,27）至（80,97）的图像块中，理论上篡改率为，图4.2（a3）-（d3）是本次模拟的结果。

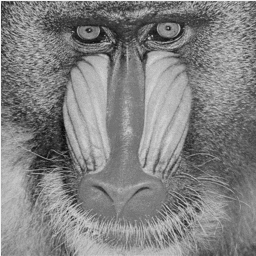
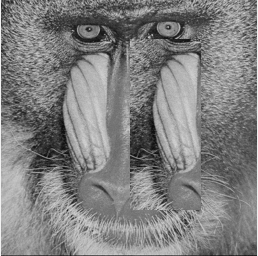
图4.2（a3）它的PSNR值是40.7496dB，图4.2（b3）检测是图4.2（a3）在受到第一类拼贴攻击后的检测结果，图4.2（c3）是篡改检测结果。如该图所示，本文中的方法可以检测到第一种拼贴攻击，并且篡改检测率是6%，这与理论值是一致的。图4.2（d3）是基于图4.2（b3）图像自动恢复的结果，其PSNR为36.7945dB。

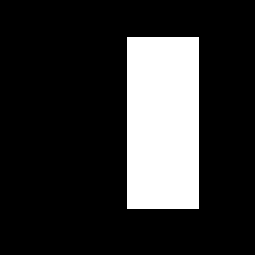
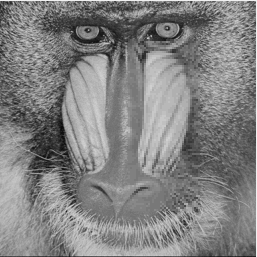
（a1）本文中Lena水印图像 （b1）基于（a1）受到第一类拼贴攻击

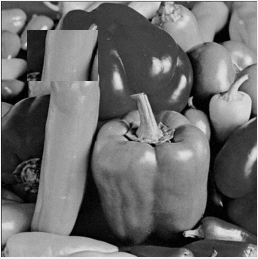
（c1）对（b1）篡改检测结果 （d1）对（b1）的恢复结果

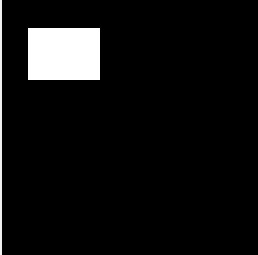
（a2）本文中Baboon水印图像 （b2）基于（a2）受到第一类拼贴攻击

（c2）对（b2）篡改检测结果 （d2）对（b2）的恢复结果

（a3）本文中Peppers水印图像 （b3）基于（a3）受到第一类拼贴攻击

（c3）对（b3）篡改检测结果 （d3）对（b3）的恢复结果

图4.2 第一类拼贴攻击检测结果对比图

通过所列出的数据和相关图形可以看出，本文中的方法，在经过分层篡改检测后，可以自动检测到第一种拼贴攻击，在经过图像两层级的恢复之后，可以对受到攻击的图像进行恢复且恢复效果非常理想，并且可以保证篡改检测率与理论值的一致性。

### 4.2.2 第二类拼贴攻击检测

256×256的8位灰度Lena图像和256×256的8位灰度Baboon图像用于模拟第二类拼贴攻击，拼贴攻击操作是将Lena图像中坐标（48,42）至（211,125）的块粘贴到Baboon图像坐标（48,134）至（211,217）的图像块中，理论上篡改率为，图4.3（a1）-（d1）是本次模拟的结果。

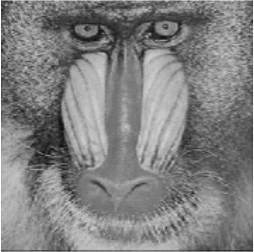
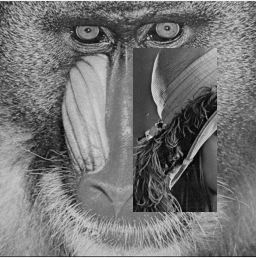
图4.3（a1）它的PSNR值是40.7084dB，图4.3（b1）检测是图4.3（a1）在受到第二类拼贴攻击后的检测结果，图4.3（c1）是篡改检测结果。如该图所示，本文中的方法可以检测到第二种拼贴攻击，并且篡改检测率是22%，这与理论值是一致的。图4.3（d1）是基于图4.3（b1）图像自动恢复的结果，其PSNR为32.3508dB。

256×256的8位灰度Baboon图像和256×256的8位灰度Peppers图像用于模拟第二类拼贴攻击，拼贴攻击操作是将Baboon图像中坐标（40,40）至（210,110）的块粘贴到Peppers图像坐标（40,130）至（210,200）的图像块中，理论上篡改率为，图4.3（a2）-（d2）是本次模拟的结果。

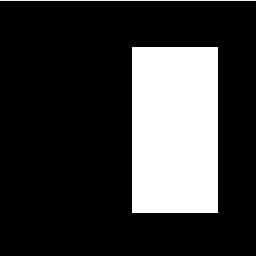
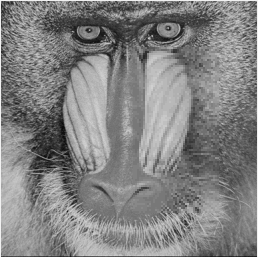
图4.3（a2）它的PSNR值是40.7496dB，图4.3（b2）检测是图4.3（a2）在受到第二类拼贴攻击后的检测结果，图4.3（c2）是篡改检测结果。如该图所示，本文中的方法可以检测到第二种拼贴攻击，并且篡改检测率是19%，这与理论值是一致的。图4.3（d2）是基于图4.3（b2）图像自动恢复的结果，其PSNR为34.5026dB。

256×256的8位灰度Peppers图像和256×256的8位灰度Cameraman图像用于模拟第二类拼贴攻击，拼贴攻击操作是将Peppers图像中坐标（116,27）至（166,97）的块粘贴到Cameraman图像坐标（30,27）至（80,97）的图像块中，理论上篡改率为，图4.3（a3）-（d3）是本次模拟的结果。

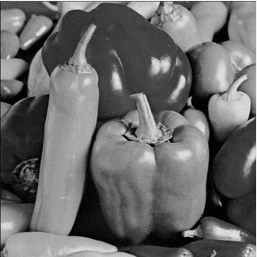
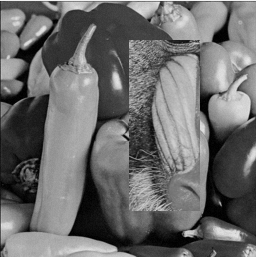
图4.3（a3）它的PSNR值是40.7465dB，图4.3（b3）检测是图4.3（a3）在受到第二类拼贴攻击后的检测结果，图4.3（c3）是篡改检测结果。如该图所示，本文中的方法可以检测到第二种拼贴攻击，并且篡改检测率是6%，这与理论值是一致的。图4.2（d3）是基于图4.3（b3）图像自动恢复的结果，其PSNR为38.6506dB。

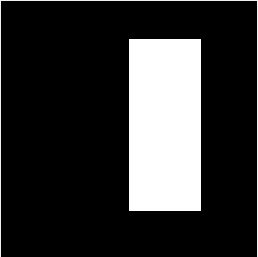
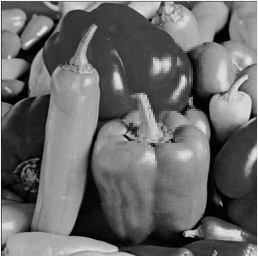
（a1）本文中Baboon水印图像 （b1）基于（a1）受到第二类拼贴攻击

（c1）对（b1）篡改检测结果 （d1）对（b1）的恢复结果

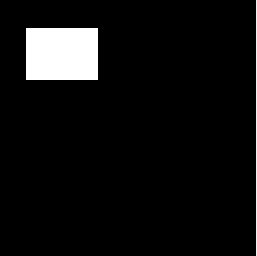
（a2）本文中Peppers水印图像 （b2）基于（a2）受到第二类拼贴攻击

（c2）对（b2）篡改检测结果 （d2）对（b2）的恢复结果

（a3）本文中Cameraman水印图像（b3）基于（a3）受到第二类拼贴攻击

（c3）对（b3）篡改检测结果 （d3）对（b3）的恢复结果

图4.3 第二类拼贴攻击检测结果对比图

通过所列出的数据和相关图形可以看出，本文中的方法，在经过分层篡改检测后，可以自动检测到第二种拼贴攻击，在经过图像两层级的恢复之后，可以对受到攻击的图像进行恢复且恢复效果非常理想，并且可以保证篡改检测率与理论值的一致性。

## 4.3 大面积的普通剪切攻击检测

测试本文方案在遇到较大面积的普通剪切攻击时的性能，仿真图像是256×256的8位灰度Lena图像，它的水印图像PSNR值是40.7215dB。

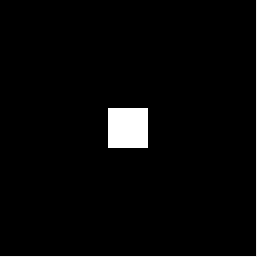
图4.4（a1）Lena的水印图像，图4.4（b1）检测是图4.4（a1）在受到40×40普通剪切攻击后的检测结果，图4.4（c1）是篡改检测结果。如该图所示，本文中的方法可以检测到大面积的普通剪切攻击，其PSNR为37.4552dB。

图4.4（a2）Lena的水印图像，图4.4（b2）检测是图4.4（a2）在受到85×256普通剪切攻击后的检测结果，图4.4（c2）是篡改检测结果。如该图所示，本文中的方法可以检测到大面积的普通剪切攻击，其PSNR为33.3355dB。

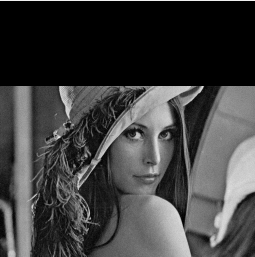
图4.4（a3）Lena的水印图像，图4.4（b3）检测是图4.4（a3）在受到230×230普通剪切攻击后的检测结果，图4.4（c3）是篡改检测结果。如该图所示，本文中的方法可以检测到大面积的普通剪切攻击，其PSNR为22.9952dB。

（a1）本文中Lena水印图像 （b1）基于（a1）受到大面积普通剪切攻击

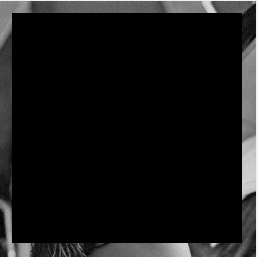
（c1）对（b1）篡改检测结果 （d1）对（b1）的恢复结果

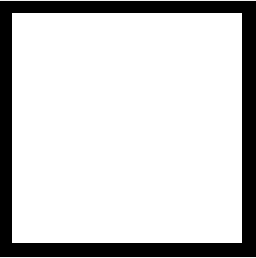
（a2）本文中Lena水印图像 （b2）基于（a2）受到大面积普通剪切攻击

（c2）对（b2）篡改检测结果 （d2）对（b2）的恢复结果

（a3）本文中Lena水印图像 （b3）基于（a3）受到大面积普通剪切攻击

（c3）对（b3）篡改检测结果 （d3）对（b3）的恢复结果

图4.4 大面积普通剪切攻击检测结果对比图

## 4.4 实验结果对比与分析

仿真图像是256×256的8位灰度Lena图像，本次模拟过程中，对水印图像从0％到95％的篡改程度进行模拟，将本文方案的测试结果与Lee[1]和Lin[3]中的测试结果进行对比，结果如表4.2所示，对比分析图如图4.5所示。

表4.2 大面积普通剪切攻击恢复图像的PSNR（dB）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 篡改大小 | 篡改率 | Lee[1] | Lin[3] | 本文方案 |
| 40×40 | 2.4% | 39.48dB | 39.96dB | 37.4552dB |
| 80×80 | 9.7% | 35.17dB | 36.24dB | 34.2605dB |
| 256×64 | 25% | 33.45dB | 31.60dB | 33.2825dB |
| 85×256 | 34% | 33.01dB | 27.37dB | 33.3355dB |
| 164×164 | 40% | 27.97dB | 23.97dB | 28.2122dB |
| 200×200 | 61% | 25.20dB | 19.47dB | 26.0016dB |
| 206×206 | 65% | 24.57dB | - | 25.6803dB |
| 214×214 | 70% | 24.16dB | - | 24.9984dB |
| 222×222 | 75% | 23.43dB | - | 24.1802dB |
| 230×230 | 80% | 22.55dB | - | 22.9952dB |
| 236×236 | 85% | 21.28dB | - | 21.8904dB |
| 244×244 | 90% | 19.86dB | - | 19.9727dB |
| 250×250 | 95% | 18.05dB | - | 17.8143dB |

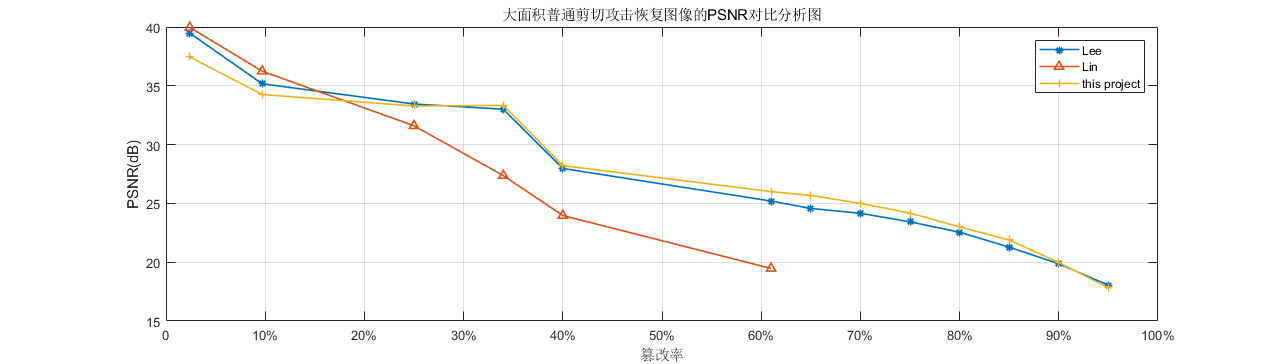


图4.5 大面积普通剪切攻击恢复图像的PSNR(dB) 对比分析图

通过表4.2以及图4.5中的数据，可以看出，与Lee[1]和Lin[3]中的方法相比，本文使用方案在篡改率为40%-90%的时候有更好的篡改性能。

双伪随机链的映射具有更好的遍历性，并且在遇到篡改时，具有更好的效果。相反，Lin和Lee的映射序列不是随机的，例如，Lee映射序列的每一列的其余部分相等，这导致在极低篡改率的时候，图像恢复具有较好的结果，但是在极高的篡改率时，图像恢复的结果却不是很理想。

因此，总体而言，本文提出的方法更为通用和实用。

## 4.5 本章小结

首先对测试参数PSNR进行了详细介绍，然后对改进的平滑功能算法进行测试，紧接着进行第一类拼贴攻击、第二类拼贴攻击以及大面积的普通剪切攻击，这三种攻击检测，最后，对大面积普通剪切攻击的实验结果与Lee[1]和Lin[3]中的实验结果进行详细的对比分析，攻击检测的结果表明了本文提出方法的通用性以及实用性。

# 第5章 总结与展望

## 5.1 总结

本文主要是为了验证数字图像的完整性，确定数字图像的篡改区域，并提出了一种基于水印和混沌系统的图像篡改检测与自恢复方案。

本文首先从数字水印相关技术的一些发展形成过程，数字水印相关技术的一些基本原理，数字水印相关技术的一些基本特征以及技术分类等几个方面对数字水印相关技术发展进行相应的理论了解和深入性的学习，接着从混沌系统的定义、混沌的基本特征、混沌系统的应用以及典型混沌系统等方面对混沌系统进行了系统的学习。在深入了解现在已经存在的研究方法的基础上，实现了在使用者面临拼贴攻击以及大面积的普通图像剪切攻击时，准确地直接进行被篡改图像位置定位，同时它可以保证已经恢复的图像具有较高的图像质量。

具体过程如下：

（1）对Logistic映射知识进行了学习。首先对图像分块进行深入了解，了解了图像分块理论知识来源。然后对Logistic映射知识进行了学习，明白了Logistic映射原理，在此基础上，借助Logistic映射与图像分块，从而由映射系统生成双伪随机链，通过伪随机链来构造图像子块之间的映射关系。

（2）对恢复信息和认证信息的提取和嵌入知识进行了学习。现有的数字图像恢复相关论文中，都讲述了不同的提取和嵌入恢复信息以及认证信息。在浏览相关论文的同时，发现基于DWT和DCT的以及图像块的水印生成过程中[21]，这些方法可以得到更多的嵌入信息，同时也可以使得嵌入图像的质量更高。但是，在这种情况下，对于块的影响还是比较显著的，对于较小篡改率的检测会出现很明显的错误，而且虚警错误率会很高。为此，本文将图像划分为的非重叠块，但是这样图像块中可以嵌入的信息是非常有限的，为此查阅了以进行图像分块的相关论文，发现出现了以下问题：恢复信息是基于图像块平均值的高5位生成的[1,4]，这对于平滑图像块篡改的恢复效果更好，但是，此方法对于纹理块的篡改恢复效果非常差；也有的方法中提出了一种变长恢复信息构造方案[22]，对于纹理和平滑块，分别使用不同的位数进行图像相应块的恢复，尽管它可以更好地表示纹理信息，但它会影响嵌入的信息位，因此，在篡改检测方面会变得更加的困难。再针对以上问题，本文使用了一种像素值自适应优化算法，它可以使嵌入的值能够更好地表达图像块信息。

（3）对现有的平滑功能进行了解，并且加以优化。现有的平滑功能对于提高嵌入信息后图像的质量有很大帮助，但是仍然有弊端，对于某些特殊情况在应用平滑功能的时候是无效的，因此，本文对现有的平滑功能进行改进，使所有情况都可以有针对性地借助平滑功能对嵌入信息进行优化，从而提高图像的质量。

（4）对篡改检测算法进行深入地了解。研读相关论文时，发现分层篡改检测算法使篡改检测有更高的精确度，为此，本文也结合分层篡改检测算法对图像进行篡改检测。

（5）对图像恢复进行学习。深入了解图像在受到攻击后恢复的应用方法，发现恢复像素仅为相邻块片面取平均，忽略了与原始像素的像素差，为此使用权值自适应算法，该算法对传统的二级恢复进行了改进，在相邻块恢复中，它可以区分原始有效块与一级恢复有效块，从而达到更好的恢复效果。

## 5.2 展望

随着计算机网络、互联网技术的飞速发展，图像、视频等多媒体技术的完整性、安全性与真实性无疑会成为当今社会的一个聚焦点。直到现在，科学研究人员已经提出了许多基于图像干扰检测和复原的水印方面的算法，比如用于进行版权保护的水印算法，比如在法庭等需要保护相关证据等领域的水印算法，但是随着技术的发展人们对于水印技术的需求也越来越高，对于水印图像篡改该检测和恢复技术的研究仍待提高。本文对图像的恶意篡改检测和复原方面深入分析与研究，取得了一定程度上的改善与进步，但是仍然存在许多不足之处需要进行进一步的研究与完善：

（1）提高水印容量

本文对图像进行2×2划分块，仅能嵌入12位信息，如何大量嵌入水印信息并保证水印的隐藏性仍待提高。

（2）优化算法效率

在理论研究中，为了提高算法的精确度，算法流程总是很复杂，但是在实际应用中，大量的运算会严重影响到运行的效率，为此，如何进行算法优化，提高算法的效率从而尽最大程度地减少算法执行的时间是需要考虑的问题。

（3）提高图像篡改区域定位精度

本文是以块为单位对图像进行划分，并进行水印嵌入、篡改检测与图像恢复。虽然子块尺寸越小，定位精度越高，但是子块划分越小，需要水印信息就会增多，所以需要设计出一种更加优化的算法，以达到在缩小子块尺寸的同时，也可以达到抑制水印信息增加。

参考文献

1. Tien-You Lee,Shinfeng D. Lin. Dual watermark for image tamper detection and recovery[J]. Pergamon,2008,41(11).
2. Wei-Liang Tai,Zi-Jun Liao. Image self-recovery with watermark self-embedding[J]. Signal Processing: Image Communication,2018,65.
3. Phen Lan Lin,Chung-Kai Hsieh,Po-Whei Huang. A hierarchical digital watermarking method for image tamper detection and recovery[J]. Pattern Recognition,2005,38(12).
4. Chengyou Wang,Heng Zhang,Xiao Zhou. A Self-Recovery Fragile Image Watermarking with Variable Watermark Capacity[J]. Applied Sciences,2018,8(4).
5. 王建文. 灰度图像的信息隐藏、篡改检测及恢复[D].北京工业大学,2013.
6. 沈嘉琪. 基于脆弱水印的图像篡改检测与修复算法研究[D].华中科技大学,2017.
7. 杨群亭. 基于数字水印的图像篡改检测与版权保护技术研究[D].南开大学,2012.
8. 李躲. 基于图像块自适应分类的篡改区域定位和恢复水印算法研究[D].江西理工大学,2018.
9. 石兆军. 基于半脆弱数字水印的图像内容认证及恢复研究[D].电子科技大学,2010.
10. 宋强. 基于自嵌入数字水印的图像认证技术研究[D].北京工业大学,2010.
11. 何延强. 用于图像认证及恢复的水印算法研究[D].北京交通大学,2014.
12. 李南. 基于超混沌的图像篡改定位零水印算法研究[D].辽宁工程技术大学,2017.
13. 张继明. 基于混沌的数字图像篡改检测及修复技术[D].大连理工大学,2014.
14. 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.
15. 何希平. 基于混沌的图像信息安全算法研究[D].重庆大学,2006.
16. Geoff Boeing,Ockie Bosch. Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction[J]. Systems,2016,4(4).
17. Yewen Li,Wei Song,Xiaobing Zhao,Juan Wang,Lizhi Zhao. A Novel Image Tamper Detection and Self-Recovery Algorithm Based on Watermarking and Chaotic System[J]. Mathematics,2019,7(10).
18. M Lawnik. Generalized logistic map and its application in chaos based cryptography[J]. Journal of Physics: Conference Series,2017,936(1).
19. Arroyo D , Alvarez G , Fernandez V . On the inadequacy of the logistic map for cryptographic applications[J]. Universidad De Salamanca, 2008, 06(5):773-782.
20. 丁玮,闫伟齐,齐东旭.基于Arnold变换的数字图像置乱技术[J].计算机辅助设计与图形学学报,2001(04):338-341.
21. Wei-Liang Tai,Zi-Jun Liao. Image self-recovery with watermark self-embedding[J]. Signal Processing: Image Communication,2018,65.
22. 张儒. 结合图像修复的变长自嵌入水印算法研究[D].西南交通大学,2013.
23. 佟雨兵,张其善,祁云平.基于PSNR与SSIM联合的图像质量评价模型[J].中国图象图形学报,2006(12):1758-1763.
24. K. Sreenivas,V. Kamkshi Prasad. Fragile watermarking schemes for image authentication: a survey[J]. International Journal of Machine Learning and Cybernetics,2018,9(7).
25. Wei Song,Jian-jun Hou,Zhao-hong Li,Liang Huang. Chaotic system and QR factorization based robust digital image watermarking algorithm[J]. Journal of Central South University of Technology,2011,18(1).
26. 曾祥秋,叶瑞松.基于改进的Logistic映射的混沌图像加密算法[J/OL].计算机工程:1-18[2021-06-15].https://doi.org/10.19678/j.issn.1000-3428.0059928.

致谢

我的四年大学本科生活，随着时间飞快的流逝即将结束。静下心来仔细回想自己大学四年间的学习、生活、工作经历，心中思绪万千，收到来自许多老师以及同学们的关心和帮助，在这里，我要向他们献上我最诚挚的感谢。

首先感谢我的导师——孙承爱老师，对我而言，孙承爱老师是我本科期间最重要的老师之一，从本科入学成为我的人生导师起，对我的生活、学习以及工作都给予了非常大的帮助，在我最迷惘的时候给予我支持，在我不知道如何选择的时候指引我前进，使我对于自己的未来有更加明确的目标和方向。从本科期间孙老师的数据库设计课程中，我就感觉到她是一位对于教学方面非常认真、对于学生非常负责的老师，孙老师对于学生要求很严格，不管是作业还是课程设计每一次对我们都会提出非常严格的要求，同时对于每次犯的错误老师也还是会用耐心的态度对我们进行指导。本论文和毕业设计都是在孙承爱老师精心指导下完成的，孙老师为我的毕业设计提供了许多非常有价值的建议，同时对于我的错误也及时进行指正，为我答疑解惑，给我提供思路和方向，内心真的非常感激老师，在编写论文阶段，孙老师一次次地帮助我，进行论文的修改和审核，教我克服了一个个困难，最终完成本论文。孙承爱老师对我的教导和关心使我深受感动，在此，我要向我的导师孙老师致以最诚挚的谢意！

同时，我也非常感谢我身边同学给予我的帮助，感谢四年来，身边能有这些朋友们的陪伴，日常生活中的方方面面，他们对于我的帮助我都受益良多。在论文撰写时，我们互相帮助，一起翻阅资料，互相探讨问题，及时指正错误，使我不仅提升了自己，还提高了自己的思维能力，同时还收获了更深层的友谊，这些都是我未来前行路上的财富。

感谢我大学中碰到的所有任课老师，是他们给予我知识的财富，不遗余力地将知识教授给我们，使我这四年来，收获到了更加深入且专业的计算机方面的知识，感谢老师们的关怀，使我顺利完成了大学学习任务并实现了自我的提高，让我在求学路上更进一层。

最后，感谢山东科技大学计算机科学与工程学院，是入学时对我的接纳，才有现在更好的我。

我会带着这些一路向前，未来的我，会继续坚持不懈地努力，定不负青春韶华，向着更美好的生活前进。