****

**毕业设计（论文）开题报告**

**题 目：基于轮廓波变换的图像压缩加密系统的实现**

**院 （系） 计算机科学与技术学院**

**专    业         信息安全**

**学    生           郦乐宁**

**学    号       100410316**

**班    号         1004201**

**指导教师      张 淼  讲 师**

**开题报告日期 2013年12月2日**

**哈尔滨工业大学教务处制**

说      明

一、开题报告应包括下列主要内容：

1．课题来源及研究的目的和意义；

2．国内外在该方向的研究现状及分析；

3．主要研究内容；

4．研究方案及进度安排，预期达到的目标；

5．为完成课题已具备和所需的条件和经费；

6．预计研究过程中可能遇到的困难和问题，以及解决的措施；

7．主要参考文献。

二、对开题报告的要求

1．开题报告的字数应在3000字以上；

2．阅读的主要参考文献应在10篇以上，其中外文资料应不少于三分之一。本学科的基础和专业课教材一般不应列为参考资料。

3．参考文献按在开题报告中出现的次序列出；

4．参考文献书写顺序：序号 作者.文章名.学术刊物名.年，卷（期）：引用起止页。

三、如学生首次开题报告未通过，需在一周内再进行一次。

四、开题报告由指导教师填写意见、签字后，统一交所在院（系）保存，以备检查。

指导教师评语：

指导教师签字：                            检查日期：

目 录

[1 课题来源及研究的目的和意义 1](#_Toc375050285)

[1.1课题来源 1](#_Toc375050286)

[1.2研究目的和意义 1](#_Toc375050287)

[2 国内外在该方向的研究现状及分析 2](#_Toc375050288)

[3 主要研究内容 2](#_Toc375050289)

[3.1 轮廓波变换简介 3](#_Toc375050290)

[3.1.1 基于高频 Contourlet 变换的图像压缩 3](#_Toc375050291)

[3.1.2 基于小波变换的 Contourlet 变换的图像压缩 6](#_Toc375050292)

[3.2 混沌系统简介 9](#_Toc375050293)

[4研究方案及进度安排，预期达到的目标； 9](#_Toc375050294)

[4.1研究方案 9](#_Toc375050295)

[4.1.1 原始图像预处理模块 9](#_Toc375050296)

[4.1.2 压缩变换模块 10](#_Toc375050297)

[4.1.4 简单流程 11](#_Toc375050298)

[4.2 进度安排以及各阶段预期达到的目标 12](#_Toc375050299)

[5 为完成课题已具备的的条件 12](#_Toc375050300)

[6 研究过程中可能遇到的问题和解决方案 12](#_Toc375050301)

[7 主要参考文献 13](#_Toc375050302)

# 1 课题来源及研究的目的和意义

## 1.1课题来源

随着网络的快速发展,数据量越来越大，而我们的带宽却没有跟上网络的发展，经常会出现高质量的图像刷新缓慢的问题，我们急迫地需求将图像进行压缩以缩短我们的等待时间，并且也需要对大量的图像进行加密以保证安全可靠。

## 1.2研究目的和意义

随着互联网和通信技术的发展,人们会进行大量的图像数据的传输。由于通信传输和接受设备的充分发展,通过无线电和一般的通信网络获取数据已经变得越来越容易。因此,图像信息安全已经成为一个关键而迫切的问题,。数字图像加密技术已经成为一项非常实用而又亟待快速发展的关键技术。保护图像信息安全最经济有效的方法是采用密码技术。但是,一方面现有的加密算法大多数是为保护文本信息而设计的,另一方面已有加密算法的抗破译能力不强。而基于混沌的图像加密算法具有以上加密算法不具备的特性。

同时，由于网络流量的急剧增大，对传输的文件进行压缩以减轻网络负载、提高传输效率也变得非常重要。通过压缩，文件变得更小，但不影响信息的完整性，这样既节省了流量，又为传输节省了时间。压缩是一种非常重要的技术。因此，将加密和压缩结合起来是一个非常重要的研究方向，有很大的实用价值。

综上所述，同时具有混沌加密和压缩功能的算法具有很高的研究价值和实用价值。

# 2 国内外在该方向的研究现状及分析

对加密与压缩结合目前来说主要有三大研究方向。

一个方向是将压缩合并到加密中，Wong和Yuen提出了一个算法，该算法在Baptista型混沌密码系统中嵌入压缩[1]。这种方法以加密系统的结构为基础。

第二个方向是将加密嵌入到压缩算法中。基于这个思想，许多基于密钥控制的熵编码方法被提出[2-7]。在这些方法中，将加密嵌入到熵编码中，如算数编码和Huffman编码。其基本思想是通过使用密钥去控制熵编码使用的统计模型，这样一个熵编码器很容易被转变成一个密码系统。将加密嵌入进算数编码主要是使用密钥来控制区间的分配[3-7]。文献[2]基于多Huffman表将密码嵌入进Huffman编码中。然而，由于这些方法都是基于压缩的，加密被作为一个附加的属性而不是主要考虑的对象，因此其安全性不是很令人满意。例如文献[2]只是根据密钥对Huffman树的左右子树进行交换，没有改变树的结构，码长保持不变，其压缩性能没有损失，但是这种方法有一个已知明文攻击的漏洞。[6]也遭受了已知明文攻击。

第三个研究方向是基于特定的图像压缩算法提出加密与压缩联合算法。与前两个方向不同的是，这些算法将压缩和加密同等考虑，没有将一个根植于另一个中。

而在本次设计中，我打算将压错和加密并行地执行，两者之间没有互相影响。首先将图像进行预处理。然后将图像进行轮廓波变换，再量化。将量化后的数据进行混沌加密，最后进行huffman编码。这样的好处使得图像能够在传输的过程中减少了延迟，保护了用户的隐私。

基于混沌[8]的图像加密技术[9]年来才发展起来的一种密码技术。它是把待加密的图像信息看成是按照某种编码方式编成的二进制数据流，利用混沌信号来对图像数据流进行加密[10]。混沌现象[12]美国气象学家Lorenz早在1963年在研究模拟天气预报时发现的。当时他是把大气的动态方程简化成了三阶非线性方程[11]后来被称之为Lorenz方程，应用当时的计算技术，结果发现这个确定性方程的动力学演化具有类似随机的性质，发现了著名的Lorenz吸引子，因而推断出长期的天气预报是不可能的结论(即著名的“蝴蝶效应”)。后来，美国生物学家Robert.May在研究生物的种群变换的Logistic方程[15]也发现了这个确定性的动力学系统的演化具有混沌的特征，即对初始条件极端敏感。

混沌理论关于非线性系统在一定参数条件下展现分岔、周期运动与非周期运动相互纠缠，以至于通向某种非周期有序运动的理论。在耗散系统和保守系统中，混沌运动有不同表现，前者有吸引子，后者无（也称含混吸引子）[12]。从20世纪80年代中期到20世纪末，混沌理论迅速吸引了数学、物理、工程、生态学、经济学、气象学、情报学等诸多领域学者有关注，引发了全球混沌热。自然科学中讲的浑沌运动指，确定性系统中展示的一种貌似随机的行为或性态。确定性是指方程不含随机项的系统，也称动力系统。典型的模型有logistic迭代系统，洛伦兹微分方程系统，若斯功吸引子，杜芬方程等。为浑沌理论做出重要贡献的学者有庞加莱、洛伦兹、上田宛亮、费根堡姆、约克、李天岩、斯美尔、芒德勃罗、郝柏林等。混沌理论向前可追溯到19世纪庞加莱等人对天体力学的研究，他提出了同宿轨道、异宿轨道的概念，他也被称为浑沌学之父。

近年来，混沌现象的应用研究已越来越受到人们的重视，其中混沌保密技术[12]研究已经成为国内外的热门课题。混沌系统用于数据加密最早由英国数学家Matthews提出，从此人们开始了混沌密码的研究。混沌信号具有的非周期性、类噪声的特性，使得它具有天然的隐蔽性；对初始条件和微小扰动的高度敏感性，又使混沌具有长期的不可预测性。混沌信号的隐蔽性和不可预见性使得混沌适宜保密通信。在基于混沌理论的密码技术加密算法体制中，密钥的设计和所参与的运算机制，使其具有位错误扩散用，即两个长度完全相同的密钥，只要存在一位的差异，两个密钥的非线性变换的结果是截然不同的。它实现了不同的密钥将导致加密或解密的非线性变换结果的全局性差异，从而保证了用户密钥使用唯一的属性。1990 年以来，国际著名刊物IEEE Trans. Circuits Syst. I 先后出版了四期混沌方面的专辑[13-16]，Proceedings of the IEEE 也于2002 年5 月出版了混沌学在电子与通信工程中应用的专辑[17]，显示了混沌通信研究的重大进展。然而，时至今日，仍然有不少重要或关键的问题尚未解决。例如，文献[18-20]提出并讨论了许多重要问题，其中包括混沌的基本特性以及系统安全性等方面的问题。这些文献着重于混沌的数学基础和加密系统分析等方面的探讨。

20 世纪 80 年代后期发展起来的小波变换，其本质是多分辨率或多尺度地分析信号，故特别适用于分析非平稳信号，而且它具有等 Q 分解信号的特性，非常符合人的视觉系统对频率感知的对数特性。小波域静态图像编码方案的成功主要归功于[21]：(1)采纳了计算量较小的可分离二维小波变换算法；(2)利用了小波变换多尺度本质所固有的“零树”结构特征。1992 年，Shapiro 提出嵌入式零树小波编码(Embedded Zerotree Wavelet Coding，EZW)[22]。其基本思想是，将小波变换系数的编码分解为对标志系数特征的系数重要性图的编码和对重要系数的幅度编码两部分，利用不同尺度间小波系数存在较强的相关性，将多数的零系数组织成一种树结构，从而提高了总体编码效率。Said 和 Pearlman 在 Shapiro 算法的基础上提出了层树分集(Set Partitioning in Hierarchical Trees, SPIHT)图像编码算法[24]。在实际应用当中，多棵零树连续出现的概率很高，以至于给它们分配特定的符号是值得的，Said和 Pearlman 实现了这一点，这是其性能比 EZW 算法好的主要原因。David Taubman 提出的最优截断嵌入块编码 (Embedded Block Coding with Optimized Truncation，EBCOT)[25]是一种基于熵编码的方案，其基本思想是将每一个子带划分为多个子块，对这些子块使用相同的算法进行完全独立的编码，生成可分离的位流。该算法充分利用相邻系数的相关性(显著性统计近似满足 Markov性)构造良好的上下文，使后续的算术编码得到高效实现。此算法具有较高的压缩比、容易控制位率以及低存储器要求等性质。 另外，由 Shannon 信息论知，对于无记忆信源，矢量量化不仅总是优于标量量化，对于给定码率，维数任意大的矢量量化可以任意接近率失真下界[26]。鉴于小波变换具有良好的表示特性而矢量量化具有出色的压缩能力，许多专家学者陆续提出了一系列小波域矢量量化图像编码方案，并取得了较好的压缩效果[27-28]。 应该说，对类似于图像扫描线的一维分段平滑信号，小波变换已经成为一种比较理想的信号分析处理工具，这是因为小波变换能够在一定程度上为一维分段平滑信号提供有效的最佳表示（包括快速变换和“树”形结构），即小波变换在分析点状瞬态特征的奇异性时是最优的。然而，自然图像并不是一维分段平滑扫描线的简单堆砌。相反，图像内物理对象的平滑边界常常使得平滑轮廓曲线处存在大量的间断点（即边缘），也就是说，自然图像通常含有携带大量重要视觉特征信息的内在几何结构。作为一维小波的分离扩展，二维小波能够很好地分离出边缘处的间断点，但却无法刻画轮廓曲线的平滑度，即小波变换在表示图像结构的直线/曲线奇异性时不是最优的[29]。此外，可分离的二维小波也仅仅能够捕获有限的方向信息（方向信息是多维信号重要的、唯一的特征）。可分离二维小波的上述不足将导致进行图像低比特率压缩时，在图像边缘附近产生严重的“振铃”现象（特别是对于 Barbara 之类纹理图像）。 为了避免小波变换的不足，更加有效地表示和处理图像的高维空间数据，一门崭新的信号分析工具—多尺度几何分析（Multiscale Geometric Analysis, MGA）引起了学术界的关注。目前，人们提出的多尺度几何分析方法主要有：Emmanuel J Candes 和 David Donoho 提出的脊波变换（Ridgelet transform）[30]（1998 年）、单尺度脊波变换（Monoscale ridgelet transform）[31]（1999 年）和Curvelet 变换[29]（1999 年）；2000 年，E Le Pennec 和 Stephane Mallat 提出的Bandelet 变换[32]；以及 Do 和 Vetterli 于 2002 年提出的 Contourlet 变换[33]，等等。其中最有代表性的是 Contourlet变换（即轮廓波变换），它是一种全新的高维信号奇异性分析工具。与小波变换相比，Contourlet 变换不仅具有良好的方向性和各向异性，而且能够高效率捕获图像几何结构（将图像边缘信息捕获到不同尺度、不同频率的子带中），这使得研制开发新型图像编码方案成为可能[34-35]。 虽然新的多尺度几何分析能弥补小波变换在处理高维信号的不足，但其始终是一个非常前沿的研究领域，理论和算法都处于发展初期，有些问题还需要进一步的研究完善[36]。例如，Contourlet 变换的系数统计特性还很难描述、它还存在冗余等问题。因此，研究新的信号分析工具以及如何将其运用到实际的图像压缩编码算法中是极其必要的。

而将 Contourlet 变换应用到图像压缩方面的研究刚刚起步，只有 R.Eslami和 H.Radha 等人提出的 Contourlet 图像编码算法[37]，以及随后 A.N.Belbachir和 P.Goebel 提出的改进算法[38]。但基于 Contourlet 的压缩算法没有考虑Contourlet 变换后各子带间的相关性；并且 Contourlet 变换具有 4/3 的冗余度，在低码率情况下，Contourlet 编码算法的率失真特性与小波变换编码相比提高并不显著。因而其理论框架和实际图像压缩应还有待于进一步的探索和完善。

# 3 主要研究内容

本次毕设课题可分成三个部分-压缩加密、解压解密、测试评估。其中压缩加密可分成图像预处理模块、轮廓波变换量化模块、密钥产生模块、加密模块、编码模块。而解压解密部分是压缩加密的逆过程，测试评估是对具体的加解密前后的图像进行如压缩比、速率等参数的评测。

压缩加密过程如图3-1：

密钥产生模块

加密模块

图像预处理模块

轮廓波变换

原始图像

量化

编码后图像

编码模块

图3-1 压缩加密过程图

解密解压过程如图3-2：

解密模块

编码后图像

解码译码

后处理

解密密钥产生模块

原始图像

图3-2 解密解压过程图

如图，在整个研究过程中，主要涉及的难点和重点内容是小波变换的量化、压缩、解压过程，以及混沌加解密过程和最终的编码译码过程，下面就这几部分内容简单介绍下。

## 3.1 轮廓波变换

采用 Contoulet 变换进行的图像压缩大致有基于高频 Contourlet变换的图像压缩方案和基于 WBCT 的图像压缩方案两类。

### 3.1.1 基于高频 Contourlet 变换的图像压缩

将 Contourlet 变换应用到图像压缩过程中，最直接的方法就是在小波变换图像压缩方案中用 Contourlet 变换替代所有的小波变换，但是这样是缺乏谋略的。这是因为Contourlet 变换第一步需要进行拉普拉斯金字塔分解，它比 Mallat 分解后具有较多的冗余。也就是说，每一次拉普拉斯金字塔分解比 Mallat 分解多出了 1/4 的冗余信息。边长为a × a的图像如果进行 n 次 Mallat 小波分解，其子带系数总是a × a；而如果进行 n 次拉普拉斯金字塔分解，系数总数量为，式(3-1)所示：

多出的系数总数量为，式(3-2)所示:

以512 × 512的图像为例，根据 Mallat 算法，无论经过多少次分解，子带的系数总数始终是512 × 512，Contourlet 变换则不是。如果进行拉普拉斯金字塔变换5 次，变换系数的总数就要多出 253952 个，而 Mallat 算法的系数总数 262144，多出近一倍的数据量。对于压缩而言是不能容忍的，因此必须在变换的方面做替换。塔式变换，无论是 Mallat 小波变换还是拉普拉斯金字塔变换，都存在着一个对低频子带的下采样操作，这一操作使得分解层数越高，得到的低频子带系数越少，相应低频子带系数中的方向信息越少。Nabil 和 Maichael 的研究表明，对于一定大小的图像，大多数的方向信息都存在于 2~3 次分解变换的高频子带中。据此，他们提出了基于高频的 Contourlet 变换的图像压缩方案。图 3-3 是基于高频Contourlet 变换的部分示意图。

WVT

3

LL LL子带

低频 子带 小波变换

WVT

3

子带 高频子带

3个

LP

低频

子带 小波变换高频子带3个

原始 高频

LP

图像 子带 次高频方向

DFB

16

高频 细节子带16个

子带

DFB

16

图3-3 基于高频 Contourlet 变换的图像压缩方案示意图

首先，对原始图像进行 2 次拉普拉斯金字塔分解(LP)，然后对第二次拉普拉分解得到的低频子带进行小波分解(WVT)，并且对两次拉普拉斯金字塔分解后的高频进行方向滤波分解。这样，在方向信息较少的低频子带中采用 Mallat 分解，从而减少了变换系数的总数，在一定程度上缓和了 Contourlet 变换带来的细节与冗余数据量过大的矛盾。如图 3-4 为对测试图 zoneplate 进行 2 次 LP 分解和一次小波分解的示意图。

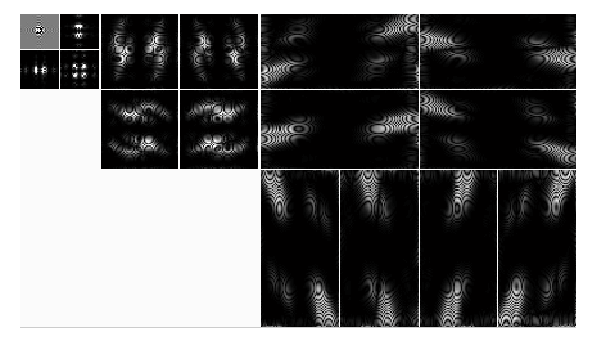


图3-4 基于高频 Contourlet 变换的分解示例

### 3.1.2 基于小波变换的 Contourlet 变换的图像压缩

基于高频 Contourlet 图像压缩方案由于子带尺寸的问题，无法使用现在已

经比较成熟的一些编码，比如 SPIHT 算法。所以，Contourlet 变换在图像中的应用存在局限性。为了解决这个问题，Eslami 和 Radha 提出了基于小波变换的Contourlet 变换(Wavelet based Contourlet Transform，WBCT)的类 SPIHT 编码算法WBCT 的基本思想是用小波变换的 Mallat 塔式分解代替 Contourlet 变换的拉普拉斯金字塔分解，然后使用方向滤波器分别对 Mallat 分解中的非 LL 子带进行卷积处理。其原理如图 3-5 所示。图中进行了 3 次 Mallat 小波分解：第一次小波分解的高频(LH、HL 和 HH)子带方向分解数(层方向数)是 4，共16 × 3个方向子带，第二、三次小波分解的层方向数均是 3，共8 × 3 × 2个方向子带，LL 子带层方向数为 0(不做方向滤波分解)。

Mallat

原始图像

高频

小波 子带滤波

变换 分解

图 3-5 WBCT 原理示意图

图 3-6 所示是对 zoneplate 图 2 级小波分解，并对高频进行方向滤波，给出的层方向数分别是 3，2，0 的 WBCT 两次分解示意图。

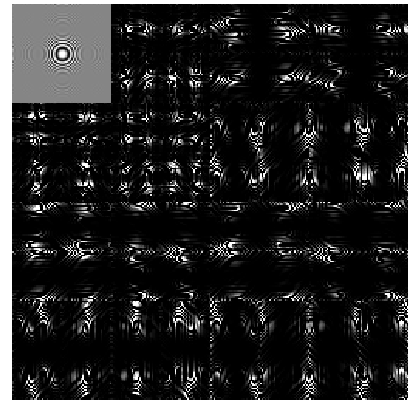


图 3-6 层方向数为 3，2，0 的 WBCT 两次分解示例

从 WBCT 变化的示例中可以看出，子带的排列是横向和纵向分开的(这里的横向和纵向是指变换后子带的长和宽的关系，长大于宽的子带为横向子带，反之就是纵向子带，与子带本身代表的方向数无关)。如果按照这样的数据结构方式进行 SPIHT 编码，因为相邻的方向子带系数之间的相关性问题，编码效率就不够高，于是，还需要调整子带之间数据结构放置的问题，以便于进行高效率的编码。图 3-7 给出了两种情况：当 Mallat 分解的两级小波与对应子带之间分解的方向数相同时，如图 3.5(a)所示，寻找系数之间的对应关系；当 Mallat 分解的两级小波与对应子带之间分解的方向数不同时，图 3-7(b)所示，寻找系数之间的对应关系，其中第一次分解的方向数是 3，第二次分解的方向数是 2。

（a）子带方向数不同时系数对应关系 （b）子带方向数相同时系数对应的关系

图 3-7 基于 WBCT 的类 SPIHT 图像压缩算法系数树形关系说明图

如果方向子带的排列顺序如图 3-8 左图(方向数为 3，共有 8 个方向子带)，阴影部分的是纵向子带，同样，标称的子带为同一个上一级小波子带的对应高频子带分解而来。因此，将他们排列为如图 3-8 右图所示，符合 SPIHT 算法编码的要求。

2

3

4

5

1

1 2 3 4 5

12345

1 2 3 4 5

图 3-8 基于 WBCT 的类 SPIHT 图像压缩算法子带排列变换说明图

## 3.2 混沌系统

混沌是非线性确定系统的一个复杂现象, 将两个十分相近的初值代入同一个混沌函数进行迭代运算, 经过多次迭代后, 两个混沌数值序列变得毫不相关。混沌系统因具有这种对初始条件的敏感依赖性和高度不可预测性, 近二三十年来已被广泛应用于保密通信的研究。

混沌用于掩盖明文和密文之间的关系，使密钥和密文之间的统计关系变得尽可能复杂，从而导致攻击者无法从密文推理得到密钥。扩散则是将明文冗余度分散到密文中多位的值。

一般混沌密码的实践主要有-混沌流密码、混沌分组密码、基于混沌的图像加密和基于混沌的Hash函数，从总体来说，混沌密码学主要有三个重要的设计思路：(1)使用混沌系统生成伪随机密钥流，该密钥流直接用于掩盖明文；(2)使用明文和/或密钥作为初始条件和/或控制参数，通过迭代/反向迭代多次的方法得到密文。第一种思路对应序列密码，第二种思路对应分组密码；(3)利用混沌来构造公开密钥密码，该项研究还处在初期阶段。

解密密钥

加密密钥

混沌信号发生器

混沌信号发生器

混沌信号序列流

混沌信号序列流

密文序列流

明文序列流

明文序列流

发送端 接收端

图3-9 混沌加密原理

### 3.2.1 Logistic 映射的主要特性

一维Logistic 映射是一个简单的混沌映射，20 世纪50年代，有好几位生态学家就利用过这个简单的差分方程，来描述种群的变化：Xn+1 = μ \* Xn \* ( 1 - Xn ) μ∈[0,4] X∈[0,1]式中，Xn 表示当年的种群数，Xn+1 便是下年的种群数，μ 为增长参数。显然这个方程只有一个二次项非线性部分。可以利用Logistic 映射的混沌区产生伪随机性很好的伪随机数序列，理论上讲，在混沌区的伪随机序列可以是无周期的， 但是，数值在计算机中表示的位数是有限的，所以有限位精度数值的迭代运算是有周期的。Logistic 映射的控制参数μ 应该介于[0，4]之间，初始条件的X 初值X0 应该介于[0，1]之间。为了观察这个迭代过程输出的数值序列的分布情况和局部细节，首先选取X0=0.5，μ 值遍历于[0,4]之间，迭代512 次；其次再选取X0=0.5，μ 分别取[3,4]范围，再迭代388 次，如图3-10，其中横轴表示μ 的取值范围，纵轴表示X 的取值范围。

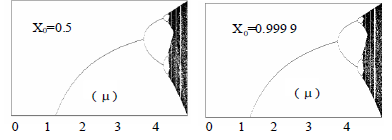


图3-10 初值X0=0.5 和X0=0.999 9 时Logistic 映射迭代(抛弃前512 次迭代数)从图1 中可以看出，在μ 取值很接近4 的时候，X 的取值趋向于分散在整个(0,1)范围内。 这说明当μ 取值在4 附近的时候，X 伪随机数序列的取值区间范围较大，μ 的这个取值范围比较适合于用来产生较好的伪随机数序列。再结合图3-11，还有其它的一些迭代图，研究者们进一步得出如下结论：

(1)当μ >=3 时，X 值一分为二，对应周期为2 的解，随着参数进一步增加，周期数不断加倍，X 迭代值周而复始地在有限个周期轨道之间重复，从而进入2n(n=1,2,3,…) 的倍周期分岔(Bifurcation)区，进而进入多片混沌区。

(2)当μ=4 时，X 取值进入单片混沌区，周期为任意整数的解都存在，且不稳定。当μ 逐渐小于4 时，出现混沌区的倒分岔行为。

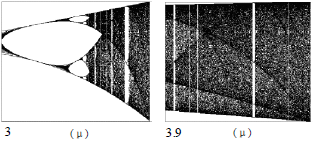
(3)混沌区有些空白的窗口，最大的窗口是周期3 窗口。 它出现在μ=3.828 的地方。周期3 窗口附近还有7,9,…等周期窗口， 在混沌的2 带区则有2×3,2×5,2×7…等周期窗口；在2n 带区中有2n ×3,2n×5,2n ×7…等周期窗口。

图3-11 初值X0=0.5，μ 取[3,4]和[3.9,4]范围时的迭代(无抛弃数)

在混沌密码方法的实现中, 主要要考虑混沌信号的序列流如何得到, 为了得到混沌序列流, 首先我们设计了下面的方法: 选取一个迭代的初始值X 0 和参数b, 让Logist ic 公式迭代M 次, 得到X 1, 取出X 1 的第2、4、6位组成一个整数并与256 求余得到X 􀀁1, 用X􀀁1与明文做异或运算得到该明文的密文c。然后在对Logistic 公式进行迭代进行对第二个明文的加密, 以此类推直至整个明文加密完毕。

### 3.2.2对初值与控参的敏感性

如果μ 的取值定下来，讨论X 的初值选取对迭代序列的影响。考虑不同的迭代初值对以后的生成结果有什么影响，从而保证不同的用户能够通过不同的初值参数产生不同的伪随机数序列。当初值选取差别很大的时候，显然运算结果将会有很大差别的，但是如果X 的初值选取得很接近的时候，比如X0 分别选取0.1+DBL\_EPSILON(2.2204460492503131e-016)和0.1，它们的初值相差微小，当μ 选取4，分别进行150 次迭代运算，两个序列差值的图形(就是用第一个序列某一次运算的迭代值减去另一个序列相同运算次数产生的迭代值)如图3-12 所示。

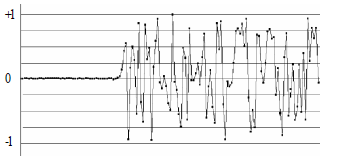


图3-12 固定μ 值，初值X 有微小差别时，两个迭代序列的差值

其中横轴表示迭代次数，纵轴表示2 个序列迭代值之间的差值。可以形象地看出，两个伪随机数序列最初相差很小，迭代值非常接近，但是随着迭代次数增加，差距逐渐变大，然后变得越来越毫无规律。同理，对于固定X 值而让μ 值有一个微小差异，混沌迭代序列差值的特性和上面的结果非常类似。因此，当应用Logistic 一维映射来产生伪随机数序列的时候，任意的μ 或X 初值的微小差异，都会导致一定次数迭代运算以后的结果产生很大差别，特别是当使用的两套μ参数和X 初值均不相同的时候，生成的两个序列之间很难寻找到明显的相关性。可以认为用这种方法产生的混沌伪随机数序列具备有较好的伪随机性。

### 3.2.3 离散分布和密度分布

伪随机数序列在取值范围内的分布特征也是一个衡量其伪随机性时要考虑的方面。看一下一维Logistic 映射生成的伪随机序列的离散分布和密度分布，迭代次数为100 000 次，输出是双精度浮点数取整后的字节输出值，参数 μ=0.4，初值 X=0.1，结果如图3-13 所示。

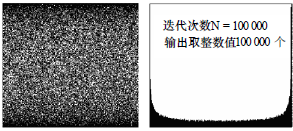


图3-13 字节输出方式的离散分布和密度分布(X0=0.1, μ=4)

由图3-13 可以看出Logistic 映射的迭代序列在完全混沌区的离散分布和密度分布并不是均匀的，可以考虑采用按比特输出的如下2 种改进的方法：

1. 如果Logistic 映射迭代序列整数化后的奇偶性分布是均匀的，则可以采用每次根据迭代值整数化后的奇偶性来输出0 或1 比特的方法来产生伪随机数序列，公式如下：
2. 如果Logistic 映射迭代序列关于X=0.5 的分布是对称的，则可以采用每次根据迭代值是否大于或小于0.5 域值来输出0 或1 比特的方法来产生伪随机数序列，公式如下：

采用方法(2)的结果如图3-14 所示。其中，迭代运算160 000次，输出10 000 个16 比特整数。从图3-14 可以看出这种改进的伪随机数序列生成方法至少应该有相对较好的离散分布和密度分布。方法(1)的迭代结果同方法(2)相近，这里不再作图说明，可以在上述两个方法基础上继续改进，以期达到更好的效果。

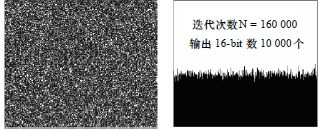


图3-14 比特输出方式的离散分布和密度分布(X0=0.1,μ=4)

### 3.2.4 结论

混沌系统的类密码学特性，比如初值和控参敏感性、伪随机性、确定性等使得基于混沌系统的密码设计成为近十几年来密码学新研究领域的热点之一，已经有了不少的进展和研究积累。通过调整Logistic 映射的迭代输出方式，可以改不论从视觉效果，还是从图像置乱程度来看，改进猫映射均优先于传统猫映射。

表1 两种猫映射加密图像的相关系数比较

|  |  |  |  |
| --- | --- | --- | --- |
|  | 原始图像 | 传统猫映射加密图像 | 改进猫映射加密图像 |
| 水平方向 | 0.9605 | 0.3982 | 0.1868 |
| 垂直方向 | 0.9483 | 0.0724 | 0.0969 |
| 对角线方向 | 0.9239 | 0.0352 | 0.0105 |

# 4研究方案及进度安排，预期达到的目标；

## 4.1研究方案

课题的主要研究方案重心如在研究内容中所述一样-图像预处理、压缩、加密、编码，然后能够将整个过程还原回来。本次研究的主要着重点在于将图像用Contoulet变换压缩和加压缩完后的进行加密，反之也能进行。研究方案设计如下。

### 4.1.1 原始图像预处理模块

这个模块重点在于BMP图像的处理。BMP(全称Bitmap)是Window操作系统中的标准图像文件格式，可以分成两类：设备相关位图（DDB)和设备无关位图（DIB）。它采用位映射存储格式，除了图像深度可选以外，不采用其他任何压缩，因此，BMP文件所占用的空间很大。BMP文件的图像深度可选lbit、4bit、8bit及24bit。BMP文件存储数据时，图像的扫描方式是按从左到右、从下到上的顺序。

典型的BMP图像文件由四部分组成： (1)位图头文件数据结构，它包含BMP图像文件的类型、显示内容等信息； (2)位图信息数据结构，它包含有BMP图像的宽、高、压缩方法，以及定义颜色等信息； (3)调色板，这个部分是可选的，有些位图需要调色板，有些位图，比如真彩色图（24位的BMP）就不需要调色板； (4)位图数据，这部分的内容根据BMP位图使用的位数不同而不同，在24位图中直接使用RGB，而其他的小于24位的使用调色板中颜色索引值。

具体的数据结构在此不赘述，图像预处理的流程图如图4-1：

读入BITMAPINFOHEADER结构

跳过BITMAPFILEHEADER结构

读方式打开图像

后续处理

读入位图数据

读入颜色表

图4-1 图像预处理流程图

### 4.1.2 压缩变换模块

离散余弦变换

对一幅N × N图像进行基于小波变换的压缩过程是：首先将原始图像通过水平和垂直滤波，分解为水平、垂直、对角和低频 4 个子带，其中低频部分可以继续进一步分解。简单来说，对N × N图像，小波变换可以先按列将图像分解成两部分，低频子图像 N × N2和高频子图像 N × N2，然后按行将每个子图像分解成低频部分和高频部分，也可以先按行后列分解。如图 2.3 所示为图像二级小波分解过程示意图，其中 L 表示低频，H 表示高频，下角 1 和 2 表示一级和二级分解。

原

HH2

HL2

LL2

HL1

HL1

LL1

L H

图

LJ2

HH1

LH1

HH1

LH1

图 4-2 图像的小波分解过程示意图(L 表示低频，H 表示高频)

轮廓波变换

Minh N.DO 和Martin Vetterli提出的contourlet变换, 也称塔型方向滤波器组PDFB (Pyramid Directional Filter Bank) 是一种多分辨率、局域的、多方向的图像表示方法, contourlet变换基的支撑区间具有随尺度而长宽比变化的“长条形结构”, 因此相比于小波分析, 轮廓波变换能更“稀疏”地表示图像。contourlet变换的基本思想是首先用一个类似小波的多尺度分解捕捉边缘奇异点, 再根据方向信息将位置相近的奇异点汇集成轮廓段。其算法实现主要是由拉普拉斯金字塔分解(LP) 和方向滤波器组(DFB ) 两个部分组成, 具体实现过程见图1 ( a)。LP 用来实现多尺度分解, 每一级分解得到一个低通子带和高通子带, 然后将高通子带采用方向性滤波器组进行分解, 进一步将图像分解到不同的频带。采用这种理想的滤波器, 轮廓波变换将高频子带分解为一个个“楔状” 区域, 见图1 (b )。

:

:

带通方向子带

带通方向子带

1. Contourlet变换滤波器组结构图

W1

W2

(b) Contourlet频域分解图

图4-3 Contourlet 变换原理图

量化

量化是一种降低整数精度的过程,因此就减少了存储整数所需的位数。在图像编码中,DCT本身并不减少数据,因为64个样值仍然得到64个系数。只是在经过量化后,特别是按人眼的生理特征对低频分量和高频分量设置不同的量化,会使大多数高频分量的系数变为零。一般说来,人眼对低频分量比较敏感,而对高频分量不太敏感,低频图像的干扰比高频图像的干扰更易察觉。信噪比测量时要根据视觉敏感度进行加权,高频方向比低频图像分量可以容许更大噪声。因此,为节省码率,低频信号进行更精细量化,高频信号进行粗量化。

变换系数经量化函数量化,得到编码前的输入码流。表2为量化矩阵。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2048 | 2979 | 3277 | 2048 | 1356 | 819 | 643 | 537 |
| 2731 | 2731 | 2341 | 1725 | 1260 | 565 | 546 | 596 |
| 2341 | 2521 | 2048 | 1365 | 819 | 575 | 475 | 585 |
| 2341 | 1982 | 1489 | 1130 | 643 | 377 | 410 | 529 |
| 1820 | 1489 | 886 | 585 | 482 | 301 | 318 | 426 |
| 1365 | 936 | 596 | 512 | 405 | 315 | 290 | 356 |
| 669 | 512 | 420 | 377 | 318 | 271 | 273 | 324 |
| 455 | 356 | 345 | 334 | 293 | 328 | 318 | 331 |

表2量化矩阵

算术编码

量化器的输出是一个包含少数非零和大量的零系数的稀疏矩阵。在嫡编码之前必须进行重排序(把非零系数集中起来)并对零系数进行有效的表示。典型合适的扫描顺序是从左上角开始的219一Zag扫描。用219一Zag序列的方法为量化后的DCT系数排序。对量化后的值进行之字扫描后的矩阵,右下角的部分接近O,把这个矩阵中的值重新排列游程,可以使游程中0值的长度增加,以此进一步提高压缩率。表3为量化系数的扫描顺序。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 5 | 6 | 14 | 15 | 27 | 28 |
| 2 | 4 | 7 | 13 | 16 | 26 | 29 | 42 |
| 3 | 8 | 12 | 17 | 25 | 30 | 41 | 43 |
| 9 | 11 | 18 | 24 | 31 | 40 | 44 | 53 |
| 10 | 19 | 23 | 32 | 39 | 45 | 52 | 54 |
| 20 | 22 | 33 | 38 | 46 | 51 | 55 | 60 |
| 21 | 34 | 37 | 47 | 50 | 56 | 59 | 61 |
| 35 | 36 | 48 | 49 | 57 | 58 | 62 | 63 |

表3扫描规则

在算术编码中,输入符号被表示成(0,1)的一个实数区间[L,H),根据概率统计模型中与符号Si对应的累计概率区间,将编码区间缩小为原来的一部分,算术编码的核运算为:

公式(4-1)中,L代表编码区间的低限值,H代表编码区间的高限值,R代表编码区间的宽度值,51表示概率统计模型中与符号对应的累计频率值,便是概率统计模型中与符号51对应的累计频率值,S表示概率统计模型中所有符号的总频率值。设L,H和R的有效位数为b,初始化时H为，L为0。在编码过程中,由于编码方程中的参数不断的更新,L和H的值会不断地接近。当L和H的最高有效位相同时,因为这个最高位在以后的编码过程中保持不变,所以可把它移出,作为输出编码流,同时把L和H左移一位。扫描后的系数经算术编码得到压缩图像,解码是编码的逆过程。

### 4.1.3 混沌加密模块

在混沌密码方法的实现中, 主要要考虑混沌信号的序列流如何得到, 为了得到混沌序列流, 首先我们设计了下面的方法: 选取一个迭代的初始值X（0）和参数u, 让Logistic 公式迭代M 次, 得到X（1）, 取出X（1）的第2、4、6位组成一个整数并与256 求余得到X（1）, 用X（1）与明文做异或运算得到该明文的密文c。然后在对Logistic 公式进行迭代进行对第二个明文的加密, 以此类推直至整个明文加密完毕。

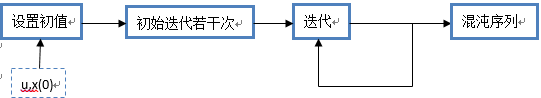


图4-4 混沌序列产生图

### 4.1.4编码模块

（1）将原始图像bmp格式做预处理，将图像的全部信息都读入内存。

（2）将图像做基于小波变换的Contourlet变换的压缩。

（3）将变换之后的数据进行量化。

（4）量化后的数据进行混沌加密。

（5）将加密后数据再进行Huffman编码。

（6）将这个过程逆向还原。

## 4.2 进度安排以及各阶段预期达到的目标

2月底，正式完成开题，确定研究方向。

3月，对算法进行全面学习，并尝试编写一些测试程序，对之前零散的学习进行整合编写，进行主体代码的编写调试。

4月，视情况，如代码实现完成则进一步进行晚上调试，否则尽快完成主体编写同时进行测试调试。

5月，调试、测试、完善，同时完成文档的大部分，准备答辩。

6月初，完成整个程序与论文，对整个毕设进行总结，整理材料完成答辩

# 5 为完成课题已具备的的条件

现已经具备PC一台

现已具备学校的电子数据库来查找文献、学习现有的成果

本课题暂时不需要其他经费

# 6 研究过程中可能遇到的问题和解决方案

1. 自己对于图像的格式、操作等的不熟悉；需要学习一下常见图像的格式构成以及读写等具体操作。
2. 轮廓波变换与加密的理论与实践；自己掌握的知识远远不足，需要勤读论文，多了解一些具体的实例，并加以小程序等的实践，具体掌握并加以思考创新。
3. 对于参考文献的搜索方法还没有熟悉，对论文的格式要严格控制。

# 主要参考文献

[1] K.W. Wong, C.H.Yuen. Embedding Compression in Chaos-based Cryptography, IEEE Transactions on Circuits and Systems II: Express Briefs. 2008, 55 (11): 1193-1197.

[2] C.P. Wu, C.C.J. Kuo, Design of Integrated Multimedia Compression and Encryption Systems, IEEE Transactions on Multimedia. 2005, 7 (5): 828-839..

[3] H. Kim, J.Wen, J.D. Villasenor. Secure Arithmetic Coding, IEEE Transactions n Signal Processing. 2007, 55 (5): 2263-2272.

[4] M. Grangetto, E. Magli, G. Olmo. Multimedia Selective Encryption by Means of Randomized Arithmetic Coding, IEEE Transactions on Multimedia. 2006, 8 (5): 905-917.

[5] X. Liu, P. Farrell, and C. Boyd. A Unified Code, [Cryptography and Coding](http://link.springer.com/book/10.1007/3-540-46665-7) Lecture Notes in Computer Science. 1999, 1746: 84-93.

[6] J.Wen, H. Kim, and J. Villasenor. Binary Arithmetic Coding with Keybased Interval Splitting. IEEE Signal Process. Lett. 2006, 13(2): 69-72.

[7] Jianeng Tang, Xiaodan Zhang, Li Zhao, Cairong Zou. A Novel Arithmetic Coding on Data Compression and Encryption with Asymptotic Deterministic Randomness, 2010 International Conference on Computer Application and System Modeling. 2010: 210-214.

[8] 黄佳庆，程文青．信息论基础．电子工业出版社，2010：10-30.

[9] 段钢编．加密与解密．电子工业出版社，2008：152-207.

[10] 陈滨．混沌波形的相关性:相空间轨迹与混沌序列自相关特性．西安电子科学技术大学出版，2011：33-53.

[11] 刘宗华．混沌动力学基础及其应用．高等教育出版社，2006：57-111.

[12] 廖晓峰等．混沌密码学原理及其应用背景．科学出版社，2009：53-107.

[13] Chua. L O. Special issue on chaos [J]. IEEE Trans. Circuits Syst.I, 1993, 40(10, 11).

[14] Kennedy M, Ogorzalerk M. Special issue on chaos synchronization and control [J]. IEEE Trans. Circuits Syst.I, 1997, 44(10).

[15] Kennedy M, Kolumbán G. Special issue on noncoherent chaotic communication [J]. IEEE Trans. Circuits Syst. I, 2000, 47(12).

[16] Kocarev L, Maggio G, Ogorzalerk M. Special issue on applications of chaos in modern communication systems [J]. IEEE Trans. Circuits Syst.I, 2001, 48(12).

[17] Martin Hasler, Gianluca Mazzini. Special issue on applications of nonlinear dynamics to electronic and information engineering [J]. Proceedings of the IEEE, 2002, 90(5).

[18] Brown R, Chua L O. Clarifying chaos: examples and counter examples [J]. Int. J. Bifur. Chaos, 1996, 6(2): 219-249.

[19] Dachselt F, Schwarz W. Chaos and cryptography [J]. IEEE Trans. Circuits Syst. I, 2001, 48(12): 1498-1509.

[20] Kocarev L. Chaos-based cryptography: A brief overview [J]. IEEE Circuit and system Magazine, 2001, 1(3): 6-21.

[21] S.I. Park, M. J. T. Smith, and R. M. Mersereau. Improved structures of maximally image analysis. IEEE Trans. on Image Processing, 2004, 13(11): 1424-1431.

[22] J.M. Shapiro. Embedded image coding using zerotrees of wavelet coefficients. IEEE Trans. on Signal Processing, 1993, 41(12): 3445-3462

[23] 邓绍江等．基于Logistic映射混沌加密算法的设计与实现．重庆大学学报，2004，27(4)：61-62.

[24] A. Said, W.A. Pearlman. A new, fast, and efficient image codec based on set partitioning in hierarchical trees. IEEE Transactions on Circuits and Systems for Video Technology, 1996, 6(3): 243-250

[25] D. taubman. High Performance Scalable Image Compression with EBCOT. Proc. IEEE Int. Conference Image Processing, 1999, 3:343-348

[26] Basel, Karger. Image and video compression: the principles behind the technology. Telemedicine and Teledermatology, 2003, 32: 17-23

[27] D. Mukherjee, S.K. Mitra. Vector SPIHT for embedded wavelet video and image coding. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(3): 231-246

[28] X. Li, E Salari. Embedded Image Compression Using a Classified Multistage VQ in Wavelet Domain. IEEE International conference on Acoustics, Speech, and Signal Processing, 2005, 2: 381-384

[29] J. L. Starck, E. J. Candes, D. L. Donoho. The curvelet transform for image denoising. IEEE Trans Image Processing, 2002, 11(6): 670-684

[30] E.J. Candes. Ridgelets: Theory and Applications [D]. USA: Department of Statistics, Stanford University, 1998

[31] E.J. Candes. Monoscale Ridgelets for the Representation of Image with Edges[R]. Department of Statistics,Stanford University,1999

[32] E.L.Pennec, S. Mallat. Sparse geometric image representation with bandelets. IEEE Transactions on Image Processing, 2005, 14(4): 423-438

[33] M.N. Do, M. Vetterli. Contourlets. In: J Stoeckler, G. V. Welland. Beyond Wavelets[C]. USA: Academic Press, 2002, 1-27

[34] M. N. Do, M. Vetterli. The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans. on Image Processing, 2005, 14(12): 2091-2106

[35] 倪伟，郭宝龙等．图像多尺度几何分析新进展: Contourlet．计算机科学, 2006, 33(2): 234~237

[36] 焦李成，谭山．图像的多尺度几何分析：回顾和展望．电子学报，2003, 31(12):1975~1981

[37] D.D. –Y. Po, M.N. Do. Directional multiscale statistical modeling of images. In: Proceedings of SPIE Conference on Wavelets: Applications in Signal and Image Processing X, San Diego, USA, 2003, 69-79.

[38] 梁栋，沈敏，高清维等．一种基于Contourlet递归Cycle Spinning的图像去噪方法．电子学报，2005, 33(11): 2044~2046.