

学校代码: 10252  
学 号: 167720595

上海理工大学硕士学位论文

# 基于 LDPC 码的加密图像可逆信息隐藏 研究

姓 名	张威
系 别	光电信息与计算机工程学院
专 业	仪器仪表工程
研究方向	精密测试技术与装置
指导教师	秦川 教授

学位论文完成日期 2018 年 12 月

REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES  
BASED ON LDPC CODE

by  
Zhang Wei

A Thesis Submitted to University of Shanghai for Science & Technology in  
Partial Fulfillment of the Requirements for  
the Degree of Master


Under the Supervision of  
Professor Qin Chuan

University of Shanghai for Science & Technology  
December 2018

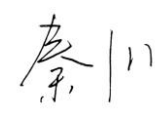
## 学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，同意学位论文保留并向国家有关部门或机构送交论文的复印件和电子版。允许论文被查阅和借阅。本人授权上海理工大学可以将本学位论文的全部内容或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于      保 密 \_\_\_\_ 年    ☐  
                                 不保密                    ☒

学位论文作者签名：

2019 年 2 月 27 日


指导教师签名：

2019 年 2 月 27 日

## 声 明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已注明引用的内容外，本论文不包含任何其他个人或集体已经公开发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。

本声明的法律责任由本人承担。

学位论文作者签名：

2019 年 2 月 27 日

## 摘 要

随着云计算等技术的快速发展,人们的生活得到了极大的丰富,人与人之间的交流也变得日益密切。微信等应用程序的使用使得人们从过去的单一的文字交流发展到现在的语音、图像和视频等多媒体交流方式,人们的生活得到了极大的便利。虽然人们的交流方式和生活方式得到了很大程度的改善,但是,在这繁荣发展的背后也存在着很大的安全隐患,最主要的就是隐私信息泄露的问题。过去由于发展水平的原因,人们更多的注重保护文字信息的安全,但随着科技的发展和多媒体技术的应用,图像等多媒体信息的安全性也受到了人们高度的重视。在军事、医疗等安全性要求较高的领域,多媒体信息的安全性就显得尤为重要。如今人脸识别、虹膜识别等技术的广泛使用,给图像信息的保护工作带来了更大的挑战。如何在保护图像信息的同时又能隐藏秘密信息的问题引起了很多学者的研究兴趣。为了更好地提高图像与秘密信息的安全性,在本文中我们提出了两种基于 LDPC 码的加密图像的可逆信息隐藏算法。这两种方法既可以保护原始图像的信息安全,又能很好的隐藏秘密信息达到信息保护的效果。

在第一种方法中,我们首先利用图像块的二进制流密码异或和块置乱的方法对原始图像进行加密操作。然后将加密图像发送给信息嵌入者,接着信息嵌入者根据一个阈值将加密的图像块分成平滑区和复杂区,并收集平滑区中像素的最低有效位(LSB),利用 LDPC 矩阵对这些比特进行压缩,最后将秘密信息嵌入到被压缩的位置上从而组成新的比特流并将它们放回原来的位置。这样如果接收者只有加密密钥,他可以直接解密图像但无法提取秘密信息。如果接收者只有信息嵌入的密钥,他可以直接提取秘密信息但是不能获得图像的信息。如果接收者既有加密密钥又有信息嵌入的密钥,那么他既可以准确的提取秘密信息,又可以无损地恢复原始图像。

在第二种方法中,我们先根据特定的类似流密码和块置乱的方法加密原始图像,从而得到加密图像。信息嵌入者在得到加密图像后利用阈值将图像块分成两个部分,即平滑区和复杂区。不同于第一种方法的是,在这里我们把平滑区中的部分像素的最高有效位(MSB)直接用秘密信息替换,完成第一次秘密信息嵌入的过程,然后剩余的部分像素的最低有效位(LSB)采用 LDPC 矩阵压缩的办法再次嵌入秘密信息,从而完成第二次秘密信息的嵌入。通过这两个信息嵌入的步骤,我们可以很大程度地提高信息的嵌入量。这样接收者在获得图像后,如果只有加密

密钥，那么他可以直接解密图像。如果只有信息嵌入密钥，他就可以直接提取秘密信息。如果既有加密密钥又有信息嵌入的密钥，那么他既可以准确地提取秘密信息，又可以正确地恢复原始图像。我们的方法在一定程度上提高了信息的嵌入量和直接解密时图像的解密质量。

**关键词：**图像加密 信息嵌入 图像解密 图像恢复

## ABSTRACT

With the development of cloud computing and other technologies, people's lives have been greatly enriched, and the communication between people has become increasingly close. With the use of applications such as WeChat, people have developed from text communication to multi-media communication such as voice, image and video. Although ways of communication and lifestyle have been greatly improved, there are also some security risks. The most important one is the leakage of privacy. In the past, because of the level of development, people paid more attention to protecting the security of text information. However, with the development of technology and the application of multimedia technology, the security of multimedia information such as images has been proposed. In the field of military and medical, the security of multimedia information is particularly important. Nowadays, face recognition, iris recognition and other technologies are widely used, which bring greater challenges to the protection of image information. How to protect image information while hiding secret information has attracted many researchers. In order to improve the security of image and secret information, we propose two reversible information hiding algorithms for encrypted image based on LDPC code. These two methods can not only protect the information security of the original image, but also hide secret information to achieve the result of information protection.

In the first method, we first encrypt the original image by using binary XOR and block scrambling. Then the data hider divides the encrypted image blocks into smooth region and complex region according to a threshold and collects the least significant bits (LSB) of the pixels in the smooth region. Then these bits are compressed by LDPC matrix, and the additional bits are embedded into the compressed room to generate a new bit stream. In this way, if the receiver only has the encryption key, he can decrypt the image directly but can not extract the additional information. If the receiver only has the data hiding key, he can extract the additional information directly. If the receiver has both the encryption key and the data hiding key, he can extract the additional information correctly and recover the original image without any error.

In the second method, we encrypt the original image according to stream-cipher

and block permutation to generate the encrypted image. After getting the encrypted image, the data hider divides the encrypted blocks into smooth region and complex region according to the threshold. Unlike with the first method, we directly replace the most significant bits (MSB) of some pixels in the smooth region with additional information to complete the first step. Then the least significant bits (LSB) of other pixels are embedded again by LDPC matrix compression to complete the second step. In this way, the receiver can decrypt the marked image directly if he only has the encryption key. If he only the data hiding key, he can extract the additional information directly without any error. If he has both encryption key and data hiding key, he can not only extract additional information accurately, but also recover the original image. Our schemes improve the embedding capacity and the image quality of decrypted image.

**Key Word: image encryption, data hiding, image decryption, image recovery**



# 目 录

第一章 引言 .....	1
1.1 背景介绍 .....	1
1.2 本文方法框架 .....	2
1.3 本文结构安排 .....	4
第二章 国内外的研究现状 .....	6
2.1 相关文献介绍 .....	6
2.1.1 明文图像的可逆信息隐藏 .....	6
2.1.2 加密图像的可逆信息隐藏 .....	7
2.2 目前存在的问题 .....	10
第三章 基于自适应嵌入机制的加密图像可逆信息隐藏 .....	11
3.1 图像加密 .....	11
3.2 信息嵌入 .....	15
3.3 信息提取与图像恢复 .....	17
3.4 实验结果 .....	18
3.5 本章小结 .....	26
第四章 基于混合嵌入机制的加密图像的可逆信息隐藏 .....	27
4.1 图像加密 .....	27
4.2 信息嵌入 .....	28
4.3 信息提取和图像恢复 .....	30
4.4 实验结果 .....	32
4.5 本章小结 .....	40
第五章 总结与展望 .....	41
5.1 工作总结 .....	41
5.2 未来展望 .....	42
参考文献 .....	43
在读期间公开发表的论文 .....	48
致 谢 .....	49

# 第一章 引言

## 1.1 背景介绍

当今社会的发展中，人们之间的交流日益密切，图像，视频，语音等已经成为日常交流中重要组成部分，尤其图像，更是成为人们生产生活中不可或缺的部分。然而现如今信息泄露的情况时有发生，给人们的生活，社会的发展带来了不好的影响。人们因此越来越重视个人隐私信息的安全，尤其是在军事、医疗等领域。为了更好地保护图像信息以及个人的隐私信息，加密图像的可逆信息隐藏算法应运而生。它既可以保护图像的原始信息不被泄露又可以保护嵌入的秘密信息不被窃取。例如病人在医院拍完 CT 图片以后，医院为了保护病人的隐私，可以先将病人的医疗图像加密然后再上传到医院的数据库中。接着数据库管理员为了更好地管理这些上传的加密图像，可以将病人的信息包括姓名、性别、年龄、发病情况等信息嵌入到加密图像中，从而方便数据库的后期管理。病人再次来到医院，医生就可以直接从数据库中下载病人的图像资料，并根据密钥来恢复原始图像和提取嵌入的秘密信息，从而获得病人的图像和文字资料。当设计师在完成自己的设计图之后在上传云端前，如果担心图像会被别人窃取，可以先对原始的图像进行加密操作，然后将加密图像上传至云端。云端的管理员在收到加密图像后可以在加密图像中嵌入作者的信息，一是为了方便后期的管理，二是可以保护作者的知识产权。以后设计者再从云端下载设计图的时候，就可以根据自己手中的密钥恢复原始的设计图的图像。这样既保护了图像的信息，又在很大程度上保护了设计师的版权。这些都是加密图像的可逆信息隐藏算法的优点，在保护人们信息安全的同时也给生活带来极大的便利。

图像的信息隐藏可以说是从明文域的信息隐藏慢慢发展到密文域的可逆信息隐藏。明文域的可逆信息隐藏忽略了原始图像的安全性，重在保护嵌入的秘密信息。但加密图像的可逆信息隐藏可以很好地保证原始图像不被泄露，很大程度的弥补了明文域的缺点。众所周知，明文图像因为存在相邻像素的相关性，所以人们可以利用这些特性来进行信息隐藏的操作，在一定程度上方便了人们隐藏信息。并且可以很好的恢复图像。但是，当原始图像加密以后，像素之间的相关性就会被打乱，图像的不确定性就会增加，图像的熵信息会变大，这在一定程度上增加了信息隐藏的难度和后期图像恢复的难度。这样一来，人们无法直接使用明文图

像信息嵌入的方法在密文图像中使用。这就需要研究人员去研究可以用在密文图像上的信息隐藏的方法。

## 1.2 本文方法框架

LDPC 码 (Low Density Parity Check Code), 即低密度奇偶校验码, 最早是由 Gallager 博士在 1963 年提出。LDPC 码其实是一类具有稀疏校验矩阵的线性分组码, 它的稀疏性在于其校验矩阵只含有非常少量的非零元素, 即校验矩阵中的 1 的个数要远小于 0 的个数。正是因为存在这种稀疏性, 译码复杂度和最小码距都只随码长线性增加。要想经过 LDPC 码得到发送序列, 则需要通过一个生成矩阵将图像的信息序列映射成发送序列。值得注意的是, 对于生成矩阵, 都会有一个完全等效地奇偶校验矩阵存在。

在本文中, 为压缩加密图像的比特序列, 数据嵌入者通过设置位节点和校验节点的数目得到对应的 LDPC 校验矩阵  $\mathbf{A}$ 。校验矩阵  $\mathbf{A}$  的大小可由信息嵌入时的密钥控制。假设需要压缩的图像的信息向量为  $f = [f(1), f(2), \dots, f(g)]^T$ , 则根据校验矩阵  $\mathbf{A}$ , 我们可以压缩这些信息序列。

$$e = \mathbf{A} \cdot f, \quad (1.1)$$

校验矩阵  $\mathbf{A}$  的大小为  $(g-\alpha) \times g$ , 则它对应了  $g$  个位节点和  $(g-\alpha)$  个校验节点。经过式(1.1), 原始长度为  $g$  的序列就被压缩成长度为  $(g-\alpha)$  的向量  $e = [e(1), e(2), \dots, e(g-\alpha)]$ 。校验矩阵  $\mathbf{A}$  的构造方法有多种, 包括例如 Gallager 构造一类码和有限几何代码等。在本文中, 我们利用两部分来构造校验矩阵  $\mathbf{A}$ , 包括一个单位矩阵  $\mathbf{I}$  和一个伪随机的二进制矩阵  $\mathbf{Z}$ 。

$$\mathbf{A} = [\mathbf{I}, \mathbf{Z}], \quad (1.2)$$

由此, 我们可以得到压缩比为

$$r = (g - \alpha) / g, \quad (1.3)$$

这样空余出的  $\alpha$  个比特位就可以用于嵌入秘密信息。当接收者在收到嵌入有秘密信息的序列后, 需要对其进行解码操作。假设原始图像的信息序列为  $x = [x(1), x(2), \dots, x(g)]^T$ , 我们可以得到

$$f = x \oplus K, \quad (1.4)$$

$K$  为加密过程中的密钥。根据式(1.1) 和式(1.4), 接收者可以得到

$$e \oplus \mathbf{A} \cdot K = \mathbf{A} \cdot x, \quad (1.5)$$

因为序列  $e$ , 密钥  $K$  以及矩阵  $\mathbf{A}$  都是已知的, 所以接收者可以将式(1.5)的左半部分进一步表示为

$$y = [y(1), y(2), \dots, y(g - \alpha)]^T = e \oplus \mathbf{A} \cdot K, \quad (1.6)$$

即

$$y = [y(1), y(2), \dots, y(g - \alpha)]^T = \mathbf{A} \cdot x, \quad (1.7)$$

在式(1.7)中,  $y$  和  $\mathbf{A}$  都是已知的。通过把  $x$  看做  $g$  个位节点, 把  $y$  看做  $(g - \alpha)$  个 LDPC 码的校验结点, 接收者可以进一步利用原始图像的平滑性等辅助信息来解码恢复原始图像的比特信息  $x$ 。

为了进一步提高信息的嵌入量和图像的解密以及恢复质量, 在本文中我们提出了新的加密图像可逆信息隐藏的框架, 如图 1.1 所示。在本文的方法中, 我们设计了一款新的图像加密方法, 在保留一定像素信息的同时又保证了图像加密的安全性。我们会在后面的安全性分析中证明我们加密方法的安全性。在第一种框架中, 图像拥有者将原始图像分成许多个不重叠的图像块, 然后利用特殊的密码流和块置乱的方法将这些图像块加密。信息嵌入者拿到加密图像之后, 将加密的图像块分成平滑区和复杂区。通过信息嵌入的密钥, 将平滑区的像素的最低有效位进行压缩, 然后将秘密信息嵌入到压缩了的剩余空间中, 从而完成秘密信息的嵌入过程。在接收端, 有三种情况可能发生。如果接收者只有加密密钥, 那么他就可以直接解密图像。如果接收者只有信息嵌入的密钥, 他就可以直接提取秘密信息。如果接收者既有加密密钥又有信息嵌入的密钥, 那么他就能提取秘密信息, 同时无损的恢复原始图像。在第二种框架中, 信息嵌入者充分利用了相邻像素的相关性。首先, 图像拥有者将原始图像分成不重叠的图像块, 并将这些图像块加密形成最终的加密图像。信息嵌入者在拿到加密图像后, 将图像块分成平滑区和复杂区, 通过两个步骤将秘密信息嵌入到加密图像中。第一步: 将平滑区的部分像素的最高有效位(MSB)直接用秘密信息替换, 第二步: 将余下的像素的最低有效位(LSB)压缩嵌入秘密信息。当完成这两步, 秘密信息就被嵌入到加密图像中。同样, 当接收者只有加密密钥的情况下, 加密图像可以被直接解密但无法提取秘密信息。当接收者只有信息嵌入的密钥, 他可以准确的提取秘密信息。当接收者既有加密密钥, 又有信息嵌入的密钥, 他既可以成功的提取秘密信息, 又可以无损

的恢复原始图像。

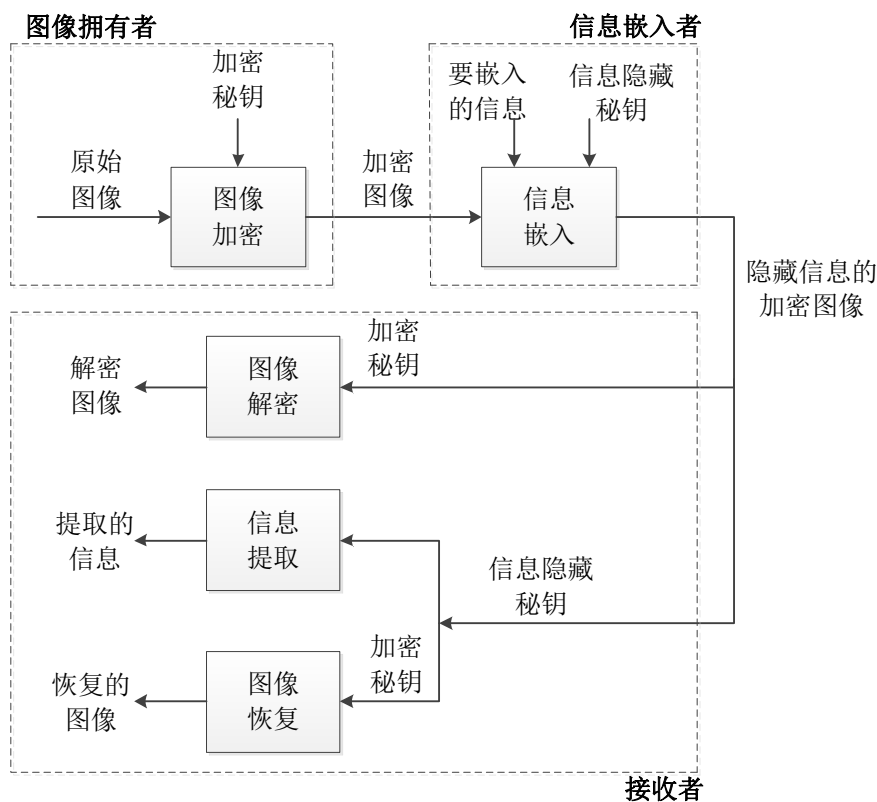


图 1.1 加密图像的可逆信息隐藏框架

### 1.3 本文结构安排

基于加密图像的可逆信息隐藏的四个重要性能指标,即加密图像的安全性,秘密信息的嵌入量,图像的直接解密质量和图像的恢复质量,本文做了以下的工作:

第一章 引言。介绍了加密图像的可逆信息隐藏的背景以及其发展的意义,同时简单介绍了本文方法的研究框架。

第二章 国内外的研究现状。介绍了加密图像的可逆信息隐藏的相关文献,简要描述了目前存在的问题。

第三章 基于自适应嵌入机制的加密图像可逆信息隐藏。详细介绍了基于自适应嵌入机制的加密图像可逆信息隐藏算法的原理,包括图像的加密,信息的嵌入,图像的解密和图像的恢复,并给出了相应的实验结果。

第四章 基于混合嵌入机制的加密图像的可逆信息隐藏。详细介绍了另一种我们提

出的算法，即基于混合嵌入机制的加密图像的可逆信息隐藏算法。在这一算法中我们创新的使用了最高有效位(MSB)来进行信息的隐藏。同时，我们分析了加密方法的安全性以及本章算法的复杂度。最后，我们给出了本章方法的实验结果。

第五章 总结与展望。回顾自己研究生阶段所做的关于加密图像的可逆信息隐藏的研究工作，总结了全文的工作内容，并对加密图像的可逆信息隐藏未来的发展进行了展望。

在本文的最后，写了致谢部分并且展示了本人在研究生阶段公开发表的学术论文。

## 第二章 国内外的研究现状

### 2.1 相关文献介绍

信息隐藏，就是将秘密信息通过一定的方法嵌入到多媒体载体中，这种载体可以是文字、图像或者视频等。信息隐藏的主要目的是利用特殊的编码方法，实现对秘密信息的隐藏，从而达到版权保护、篡改修复的目的<sup>[1-3]</sup>。但是由于传统的信息隐藏会导致原始图像永久性失真，因此为了更好的恢复原始图像，人们提出了可逆信息隐藏算法，这是一种从载体中提取嵌入信息，并且准确将载体图像恢复到原始状态的技术<sup>[4]</sup>。根据载体图像是否需要被加密，可逆信息隐藏又可以被分为密文域和明文域两个类别。虽然明文图像的可逆信息隐藏技术可以在嵌入秘密信息之后无损地恢复原始图像，但是，嵌入秘密信息的载体图像在传输的过程中会存在原始图像信息泄露的可能，这在一些保密性要求较高的领域是不能使用的。因此，为了避免原始图像信息泄露的危险，加密图像的可逆信息隐藏技术被提出来，即在信息隐藏之前就将原始图像进行加密。这种技术进一步保护了原始图像和嵌入信息的安全，同时可以做到原始图像的无损恢复和秘密信息的准确提取，实现隐蔽通信、信息保护的目的。近年来，在加密图像的可逆信息隐藏领域，越来越多的国内外的研究人员致力于提高秘密信息的嵌入量，图像的直接解密质量以及图像的恢复质量。

#### 2.1.1 明文图像的可逆信息隐藏

明文图像的可逆信息隐藏是一种既可以准确地从载体中提取秘密信息，又可以无损地恢复载体图像的技术<sup>[5-6]</sup>。作为信息隐藏的重要组成部分，明文图像的可逆信息隐藏算法可以主要分为三种类型：无损压缩算法<sup>[4]</sup>，差值扩展算法<sup>[7-9]</sup>和直方图平移算法<sup>[10-13]</sup>。

(1) 无损压缩算法。无损压缩算法是一种通过压缩载体图像来生成用于嵌入秘密信息空间的技术。Celik 等人提出了一种无损（可逆）信息嵌入技术，该技术能够在提取嵌入信息的时候准确地恢复原始载体图像。通过利用无损压缩算法压缩易受嵌入失真影响的部分来得到可以用来嵌入秘密信息的空间，从而将信息嵌入其中完成信息隐藏的工作。该方法的优势在于较大的信息隐藏量和较小的载体图像失真<sup>[4]</sup>。

(2) 差值扩展算法。Tian 等人首次提出一种基于像素值差值扩展的可逆信息隐藏的算法, 该算法通过计算相邻像素的差值, 并选择一些差值进行差值扩展, 同时把秘密信息嵌入到差值扩展后的最低位, 完成信息嵌入的工作。原始图像信息等额外信息也会被嵌入到这些差值中, 以帮助后期图像的有效恢复<sup>[7]</sup>。除了直接像素之间的差值扩展方法, 人们还提出了预测误差扩展技术。传统的预测误差扩展技术是利用预测算子对图像中的像素值进行预测, 然后扩展预测误差完成水印嵌入。Ou 等人改进了传统的预测误差扩展技术, 充分利用预测误差之间的相关性, 将相邻两个预测误差共同考虑, 从而获得更好的性能<sup>[9]</sup>。

(3) 直方图平移算法。利用基于直方图平移的可逆信息隐藏可以有效地实现较高的信息嵌入量和较低图像失真的目的。国外 Ni 等人提出利用图像直方图的零点或者最小点, 对像素灰度值进行微小的修改从而将数据嵌入到图像中的方法<sup>[10]</sup>。通过该方法, 标记图像与原始图像之间的峰值信噪比(PSNR)在 48dB 以上, 有较高的视觉质量。此外, 国内 Li 等人基于直方图平移技术的优势, 提出构建一个基于直方图平移的可逆信息隐藏的通用框架。通过该框架, 用户可以简单地定义直方图平移和嵌入函数, 从而得到一个可逆信息隐藏的算法<sup>[11]</sup>。另外, 根据该框架, 人们可以通过进一步研究直方图的平移性质和嵌入函数, 设计出更有效的可逆信息隐藏算法。

### 2.1.2 加密图像的可逆信息隐藏

随着现在科学技术的迅速发展, 云存储的计算能力相当成功, 人们可以在网上存储和处理大量的个人数据, 例如图像和视频。然而, 为了保护隐私, 用户数据在上传到网上之前需要进行加密。因此, 为了方便数据的管理和检索, 如何实现加密图像中的可逆信息隐藏极大地引起了大家的研究兴趣<sup>[14]</sup>。根据秘密信息嵌入的时机与图像的加密方法, 加密图像的可逆信息隐藏算法大致可分为三种类型: (1)加密后隐藏秘密信息, (2)加密前预留信息隐藏空间, (3)同态加密算法。

(1) 加密后隐藏秘密信息。根据图像的直接解密、信息的提取和图像的恢复的操作是否能够在接收者端分别进行, 加密后隐藏秘密信息的框架又可以分为不可分离(联合)框架<sup>[15-19]</sup>和可分离框架<sup>[20-24]</sup>。国内的张新鹏老师提出一种新的加密图像的可逆信息隐藏的算法, 首先使用流密码对原始图像进行加密, 然后通过翻转每个块中的一半像素的三个最低有效位(LSB)嵌入一个信息比特。直接解密后, 基于像素的空间相关性, 可以实现信息提取和图像恢复<sup>[15]</sup>。为了降低较小块下的比特提取的误码率, 在数据提取和图像恢复过程中, 有人改进了计算块平滑度的平滑函数, 并基于恢复块和未恢复块之间的相邻块边界处的像素相关性来提高图像



的恢复质量<sup>[16]</sup>。通过选择要翻转的部分像素,在信息隐藏过程中对每个块进行较小的修改,可以大大提高图像的直接解密质量<sup>[18]</sup>。Qian 等人提出了一种新的联合框架,首先利用流密码方法对原始图像进行加密,然后信息嵌入者利用循环平移和数据交换的算法将秘密信息嵌入到加密图像中<sup>[19]</sup>。这种算法提高了秘密信息的隐藏量,同时该算法可用于医疗图像,扩大了其应用范围。在不可分离的框架中,接收端的用户只能同时完成秘密信息的提取与图像的恢复,这在一定程度上束缚了接收端在不同情况下的权限范围。

不同于不可分离(联合)框架,可分离框架丰富了接收者的权限。为了实现加密图像的可逆信息隐藏的可分离性,Zhang 等人利用压缩了的加密图像的最低有效位的方法来创建可用于嵌入秘密信息的空间。详细来说,首先利用标准的流密码方式加密原始图像,然后将加密图像发送给信息嵌入者。信息嵌入者将加密图像中的像素分成很多的组,每个组的像素个数都是一样的,然后将每个组的像素的最低有效位(LSB)收集起来得到一串比特流,最后利用 LDPC 矩阵将每一组的比特流压缩,这样就可以将秘密信息添加到每一组的比特流中,并将这些比特流放回原始的位置,实现信息的隐藏。这种加密图像的可逆信息隐藏算法的可分离性体现在,如果接收者只有加密密钥,他可以直接解密加密图像得到一个近似原始图像的直接解密图像。如果接收者只有信息嵌入的密钥,他可以直接准确的提取秘密信息但无法获得原始的图像信息。如果接收者既有加密密钥,又有信息嵌入的密钥,他既可以准确地提取秘密信息,又可以无损的恢复原始图像<sup>[21]</sup>。这样,接收者可以分别实现信息的提取、图像的解密和图像的恢复。加密图像的可逆信息隐藏的可分离框架极大的丰富了接收者的权限,用户可以根据不同的情况或者不同的需要,分配给不同的接收者不同的密钥,大大提高了加密图像可逆信息隐藏方面的工作效率和应用范围。基于这种可分离的思想,基于渐进恢复的可分离的加密图像的可逆信息隐藏的算法被提了出来,其中信息嵌入者将加密后的图像分割成三个部分,并在这三个部分中嵌入不同数量的附加比特。在接收端,可以使用渐进机制来恢复原始图像<sup>[22]</sup>,所谓的渐进机制就是首先恢复根据参考像素恢复第一部分的像素值,然后参考第一部分已恢复的像素值来恢复第二部分的原始像素值,接着根据前两部分已恢复的像素来帮助恢复第三部分的像素值,最后将这三部分组合就得到了原始的图像。

基于低密度奇偶校验(LDPC)码<sup>[25-26]</sup>,Zhang 和 Qian 等人分别提出了新的加密图像可逆信息隐藏的可分离框架。首先,他们都是先利用流密码方法对原始图像进行加密,然后信息嵌入者利用基于 Slepian-Wolf 模型的低密度奇偶校验(LDPC)矩阵对部分加密数据进行压缩,从而为秘密信息的空余出可用于嵌入的空间,接

着, 秘密信息和被压缩的数据就可以被可逆地嵌入到加密图像中<sup>[31-32]</sup>。此外, Wu 等人在一篇论文中提出了两种加密图像的可逆信息隐藏的框架, 即不可分离的框架和可分离的框架。在其不可分离的框架中, 一些加密像素被伪随机选择嵌入秘密信息, 并且保证其四邻域像素不被修改。通过翻转像素组的最低有效位(LSB), 每个比特被嵌入到一个像素组中。然后, 借助于四邻域像素的估计值, 实现信息的提取和图像的恢复。在可分离框架中, 通过最高有效位(MSB)替换, 将每个信息比特隐藏到每个选定的加密像素中, 从而可以实现可分离的信息提取和图像恢复<sup>[27]</sup>。然而, 该方案中的直接解密图像的质量并不理想。

(2)加密前预留信息隐藏空间。不同于前文提过的加密图像的可逆信息隐藏的框架<sup>[15-27]</sup>, 还有一些研究人员提出了加密前为嵌入信息预留空间的框架<sup>[28-32]</sup>。Ma 等人提出在图像加密之前, 原始图像被分割成两部分, 并且用一种传统的明文域的可逆信息隐藏的方法将一部分的比特信息隐藏在另一部分中。这样, 第一部分像素的最低有效位(LSB)就被空余出来, 然后图像加密之后通过最低有效位(LSB)替换的方法将秘密信息嵌入<sup>[28]</sup>。此外, 在加密前基于采样的像素对未采样像素进行预测也是一种为信息嵌入预留空间的办法。利用具有集中直方图分布的调整和加密后的预测误差嵌入秘密信息。将加密的、采样的像素与标记的、加密的预测误差相结合, 可以产生最终嵌入有秘密信息的加密图像<sup>[29-30]</sup>。利用稀疏表示的方法来压缩图像块, 并在图像加密之前对残差进行编码和自嵌入, 从而为加密的图像创建更大的隐藏信息的空间<sup>[32]</sup>。加密前预留信息隐藏空间虽然可以提高秘密信息的嵌入量, 但是这在一定程度上增加了图像拥有者端的算法复杂度。

(3)同态加密算法。同态加密算法让第三方如云端的管理员可以直接在密文域的图像上进行算术操作, 其得到的结果等同于在明文域中进行相应的算术操作。这样可以保证图像的原始信息在不被泄露的情况下, 完成秘密信息的嵌入。比较经典的同态加密算法有 Paillier 同态加密算法等。Chen 等人利用能量传递方程将原始图像的每个像素分成三个分量, 并用 Paillier 同态加密算法对每个分量进行加密<sup>[34]</sup>。基于同态的性质, 通过对加密信号的处理, 可以嵌入秘密信息。采用像素值排序(PVO)策略对同态加密后的每个块中的信息进行隐藏<sup>[35]</sup>, 并且加法同态保证了 PVO 在加密域中的性能接近于明文域的性能。同态加密算法虽然可以在保证图像信息安全的前提下大大提高秘密信息的嵌入量, 但是其算法复杂度比较高, 对数学能力的要求较高。

今年, 同样有很多优秀的研究人员发表了诸多论文<sup>[36-44]</sup>, 这些文献都在一定程度上提高了秘密信息的嵌入量以及图像的恢复质量。例如, 国外有人提出利用最高有效位(MSB)预测的方法来提高信息的嵌入量, 达到高嵌入量的水平<sup>[43]</sup>。除了

我们提到的加密图像的可逆信息隐藏的框架，近几年来很多国内外研究人员提出了其他优秀的秘密信息隐藏的方案，例如提高秘密信息嵌入量的方案<sup>[46-55]</sup>，减小载体图像和隐秘图像差异性的方案<sup>[56-61]</sup>。

## 2.2 目前存在的问题

加密图像的可逆信息隐藏近几年来发展迅速，相关的学者们发表了很多优秀的文献，但是这里依然存在着一些需要解决的问题。一般来说，对于加密图像的可逆信息隐藏算法，我们一般可以分为这样四个指标：

- (1) 加密图像的安全性。
- (2) 秘密信息的嵌入量。
- (3) 图像的直接解密质量。
- (4) 图像的恢复质量。

这四个指标都是衡量加密图像可逆信息隐藏算法的重要性能。一般我们判断一个加密图像可逆信息隐藏的算法好与不好时都从这四个指标出发。但是，这四个性能指标之间也存在着关系，例如一般情况下，当图像的秘密信息的嵌入量变大时，原始图像的失真就会比较大，因此图像的直接解密质量和恢复质量都会有所下降。如何能同时优化这些性能指标是加密图像的可逆信息隐藏领域研究的关键。同时，如何处理好这四个指标的平衡关系也是现在的研究者们需要解决的问题。

## 第三章 基于自适应嵌入机制的加密图像可逆信息隐藏

在本章节中，我们提出了一个新的加密图像的可逆信息隐藏框架。这个框架包括图像加密，信息嵌入，信息提取和图像恢复。图像拥有者首先根据加密密钥将原始图像分成许多个不重叠的块，同时将这些图像块加密。随后，信息隐藏者将这些加密后的图像块分成平滑区和复杂区两个部分，通过压缩平滑区像素的最低有效位(LSB)创建一个冗余空间，并将秘密信息嵌入到这个空间中。然后将这个嵌入有秘密信息的加密图像传送给接收方。如果接收者只有加密密钥，他就可以直接解密图像得到高质量的解密图像。如果接收者只有信息嵌入的密钥，他就可以直接提取秘密信息，但无法得到原始图像信息。如果接收者既有加密密钥，又有信息嵌入的密钥，他就可以提取秘密信息，并且根据图像像素的相关性无损地恢复图像。

### 3.1 图像加密

在这一部分中，我们认为图像拥有者有一个未经压缩的大小为  $M \times N$  的原始图像  $\mathbf{I}_0$ ，并且像素值的范围是  $[0, 255]$ 。首先，原始图像  $\mathbf{I}_0$  被分成许多个不重叠的图像块，每块的大小为  $2 \times 2$ ，这样一共就有  $M \times N / 4$  个图像块。如图 3.1，将每个图像块  $\mathbf{B}_{i,j}$  的四个像素分别表示为两个三角形像素  $B_{i,j}^{(0,0)}$  和  $B_{i,j}^{(1,1)}$ ，一个圆形像素  $B_{i,j}^{(0,1)}$ ，一个方形像素  $B_{i,j}^{(1,0)}$ 。值得注意的是，图像块  $\mathbf{B}_{i,j}$  的索引  $i$  和  $j$  的取值范围是  $(1 \leq i \leq M/2$  和  $1 \leq j \leq N/2)$ 。每个图像块的四个像素都可以表示成 8 比特： $b_{i,j}^{(x,y,0)}$ ,  $b_{i,j}^{(x,y,1)}$ , ...,  $b_{i,j}^{(x,y,7)}$ ，这里  $(x,y) \in \{(0,0), (0,1), (1,0), (1,1)\}$ 。

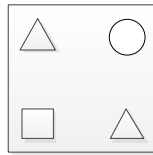


图 3.1 加密图像的可逆信息隐藏框架

$$b_{i,j}^{(x,y,s)} = \left\lfloor \frac{B_{i,j}^{(x,y)}}{2^s} \right\rfloor \bmod 2, \quad s = 0, 1, \dots, 7, \quad (3.1)$$

$$B_{i,j}^{(x,y)} = \sum_{s=0}^7 [2^s \times b_{i,j}^{(x,y,s)}]. \quad (3.2)$$

为了保护原始图像的信息，图像拥有者利用加密密钥来加密每个图像块  $\mathbf{B}_{i,j}$ 。加密部分可以分为两个部分：特殊的流密码加密和块置乱。首先，对于每个图像块  $\mathbf{B}_{i,j}$  中  $\Phi_1 \cup \Phi_2$  部分的比特  $b_{i,j}^{(x,y,s)}$ ，我们可以根据加密密钥随机生成一个伪随机的二进制序列  $r_{i,j}^{(x,y,s)}$ ，然后利用此序列加密这些比特信息。

$$b'_{i,j}^{(x,y,s)} = b_{i,j}^{(x,y,s)} \oplus r_{i,j}^{(x,y,s)}, \quad (x,y,s) \in \Phi_1 \cup \Phi_2, \quad (3.3)$$

$$\Phi_1 = \{(x,y,s) \mid (x,y) \in \{(1,0),(0,1)\} \text{ and } s = 0,1,\dots,7\}, \quad (3.4)$$

$$\Phi_2 = \{(x,y,s) \mid (x,y) \in \{(0,0),(1,1)\} \text{ and } s = 0,1,\dots,u-1\}, \quad (3.5)$$

这里  $u$  表示被用来完成后面信息嵌入工作的最低有效位(LSB)的数量。在本篇论文中，我们设定  $u$  不大于 3。然后，当  $(x,y,s)$  属于  $\Phi_3$  的时候，另一个伪随机的二进制序列  $\rho_{i,j}$  也会根据密钥随机生成。

$$\begin{cases} b'_{i,j}^{(x,y,s)} = \overline{b_{i,j}^{(x,y,s)}}, & \text{if } \rho_{i,j} = 1, \\ b'_{i,j}^{(x,y,s)} = b_{i,j}^{(x,y,s)}, & \text{if } \rho_{i,j} = 0, \end{cases} \quad (x,y,s) \in \Phi_3, \quad (3.6)$$

$$\Phi_3 = \{(x,y,s) \mid (x,y) \in \{(0,0),(1,1)\} \text{ and } s = u, u+1, \dots, 7\}, \quad (3.7)$$

在这里  $b'_{i,j}^{(x,y,s)}$  表示通过二进制序列加密后的结果。这样我们就可以初步的得到一个加密的图像块  $\mathbf{B}'_{i,j}$ 。

$$B'_{i,j}^{(x,y)} = \sum_{s=0}^7 [2^s \times b'_{i,j}^{(x,y,s)}], \quad (3.8)$$

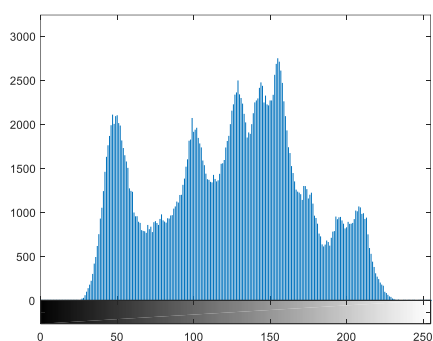
为了进一步的提高图像加密的安全性，我们根据加密密钥置乱  $M \times N/4$  个图像块得到最终的加密图像  $\mathbf{I}_e$ 。

图 3.2 给我们展示一个大小为  $512 \times 512$  的未压缩的 Lena 图像的案例。图 3.2(a) 显示的是原始图像。图 3.2(b-c) 分别表示经过密码流加密的初步加密结果图和最终的加密效果图。图 3.2(d) 表示和原始图像非常相似的直接解密图像。图 3.3 分别表示 Lena 图像加密前和加密后的图像直方图。从图中我们可以看到经过加密以后的图像直方图与原始图像相比发生了很大的变化。在图 3.4 中，我们展示了 Lena 图

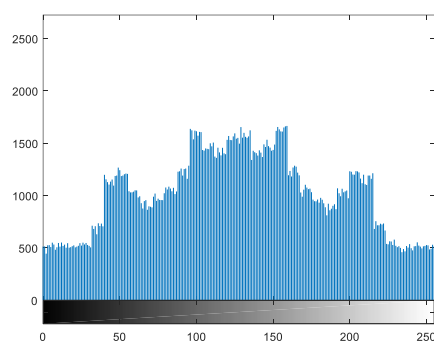
像像素值的分布情况，X 轴，Y 轴和 Z 轴分别表示横坐标，纵坐标和图像的像素值。图 3.4(a)显示的是原始图像的像素值的分布情况。图 3.4(b-c)分别表示初步加密图像和最终加密图像的像素值的分布情况。值得注意的是，原始图像的像素值的分布是连续的，而加密后像素值分布却是分散一致的。此外，在块置乱的过程中，会有 $(MN/4)!$ 种可能性。总的来说， $(MN/4)!$ 是一个非常大的数值而且加密前和加密后像素值的分布情况也是不相同的，所以在没有加密密钥的情况下不可能将这些图像块准确的放回原始的位置上去。综上所述，我们设计的加密方法是十分安全的。



图 3.2 对于 Lena 图像的加密样例

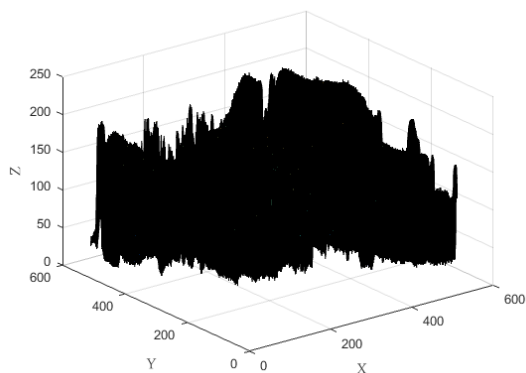


(a) 原始图像直方图

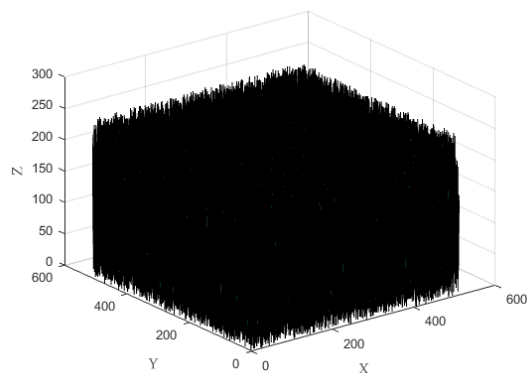


(b) 加密图像直方图

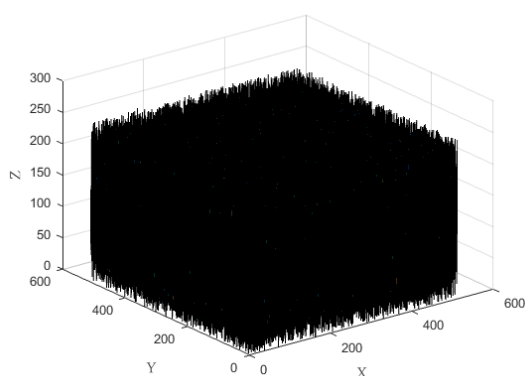
图 3.3 Lena 图像加密前和加密后的直方图结果



(a) 原始图像像素值分布图



(b) 初步加密图像像素值分布图



(c) 最终加密图像像素值分布图

图 3.4 Lena 图像的像素值分布情况图

### 3.2 信息嵌入

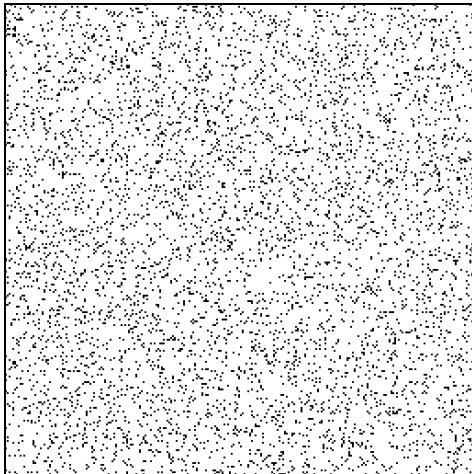
信息嵌入者拿到加密图像  $\mathbf{I}_e$  之后,他就可以将秘密信息嵌入到加密图像  $\mathbf{I}_e$  中。首先,信息嵌入者同样先把加密图像分成  $M \times N/4$  个不重叠的图像块  $\mathbf{C}_{i,j}$ 。将每个图像块的四个像素从上到下,从左到右分别表示成  $C_{ij}^{(0,0)}$ ,  $C_{ij}^{(0,1)}$ ,  $C_{ij}^{(1,0)}$ ,  $C_{ij}^{(1,1)}$ 。然后信息嵌入者计算每个加密图像块  $\mathbf{C}_{i,j}$  的左上角像素和右下角像素的差值  $\delta_{i,j}$ 。

$$\delta_{i,j} = \left| 2^u \cdot \left\lfloor C_{i,j}^{(0,0)} / 2^u \right\rfloor - 2^u \cdot \left\lfloor C_{i,j}^{(1,1)} / 2^u \right\rfloor \right|. \quad (3.9)$$

从式(3.9)中可以看出  $\delta_{i,j}$  值取决于图像块  $\mathbf{C}_{i,j}$  的  $(8-u)$  个最高有效位(MSB),同时,它也能反映出图像块  $\mathbf{C}_{i,j}$  的复杂性。 $\delta_{i,j}$  值越大,则表明图像块  $\mathbf{C}_{i,j}$  的像素分布的复杂程度更高。这时,信息嵌入者利用一个阈值  $T$  将这些图像块分成平滑区  $\Omega_1$  和复杂区  $\Omega_2$  两个部分。

$$\begin{cases} \mathbf{C}_{i,j} \in \Omega_1, & \text{if } \delta_{i,j} \leq T, \\ \mathbf{C}_{i,j} \in \Omega_2, & \text{if } \delta_{i,j} > T. \end{cases} \quad (3.10)$$

图 3.5 显示了加密图像 Lena 的块分类结果,包括置乱前和置乱后的结果。其中,白色区域和黑色区域分别表示平滑区  $\Omega_1$  和复杂区  $\Omega_2$ 。图 3.5(a)和(c)分别表示在阈值  $T = 20$  和  $T = 10$  的情况下加密图像的块分类结果。图 3.5(b)和(d)分别是相应(a)和(c)图像的逆置乱后的块分类结果图,这两幅图也证明了我们块分类方法的有效性。

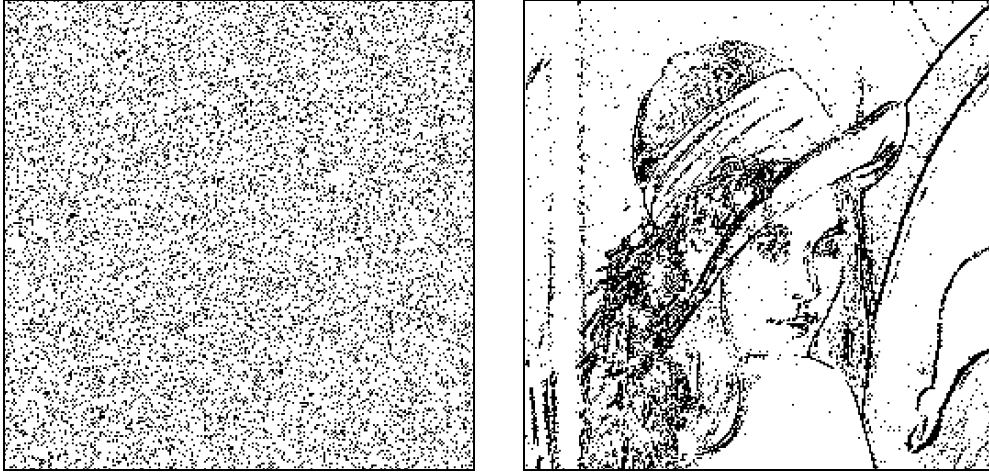


(a) 平滑块置乱后结果图( $T = 20$ )



(b) 平滑块未置乱结果图( $T = 20$ )




 (c) 平滑块置乱后结果图( $T = 10$ )

 (d) 平滑块未置乱结果图( $T = 10$ )

图 3.5 Lena 图像的块分类结果图

将属于平滑区 $\Omega_1$ 的块的个数表示成 $\gamma$  ( $\gamma \leq M \times N/4$ )。根据信息嵌入的密钥, 信息嵌入者将平滑区 $\Omega_1$ 的像素随机分成许多组, 每组包含有 $p$ 个像素。需要注意的是, 平滑区中的每个像素块的四个像素都会被选入同一个组中。因此,  $p$ 的数值是四的整数倍。在每个像素组中, 收集 $p$ 个像素的 $u$ 个最低有效位(LSB), 并将它们表示为 $\mathbf{V}_k = \{v(k, 1), v(k, 2), \dots, v(k, l)\}$ , 这里 $l = u \cdot p$ 。这时信息嵌入者可以根据信息嵌入的密钥生成一个二进制矩阵 $\mathbf{G}$ , 它的大小为 $(l - \alpha) \times l$ , 并且由两部分组成:

$$\mathbf{G} = [\mathbf{E}_{l-\alpha}, \mathbf{Q}], \quad (3.11)$$

$\mathbf{E}$ 是一个大小为 $(l - \alpha) \times (l - \alpha)$ 的单位阵,  $\mathbf{Q}$ 是一个大小为 $(l - \alpha) \times \alpha$ 的伪随机二进制矩阵。这里的 $\alpha$ 是正整数的嵌入参数。然后, 信息嵌入者将每个组的 $l$ 个比特压缩成 $(l - \alpha)$ 个比特

$$\begin{bmatrix} z(k, 1) \\ z(k, 2) \\ \vdots \\ z(k, l - \alpha) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} v(k, 1) \\ v(k, 2) \\ \vdots \\ v(k, l) \end{bmatrix}, \quad (3.12)$$

式(3.12)的运算是二进制的。这样每个组就有 $\alpha$ 个比特被压缩空余出来嵌入秘密信息。将嵌入秘密信息的 $\alpha$ 个比特与 $z(k, 1), z(k, 2), \dots, z(k, l - \alpha)$ 组合成新的像素组, 并将新的 $l$ 个比特放回原来的位置。因为复杂区 $\Omega_2$ 的像素值和平滑区 $\Omega_1$ 的 $(8 - u)$ 个最高有效位(MSB)在嵌入过程中都是没有改变的, 所以直接解密的图像质量是非常好

的。

### 3.3 信息提取与图像恢复

在本章过程中会有三种情况发生，(1)接收者只有信息嵌入的密钥，(2)接收者只有加密密钥，(3)接收者既有信息嵌入的密钥，又有加密密钥。

如果接收者只有信息嵌入的密钥，他就可以从嵌入有秘密信息的加密图像  $\mathbf{I}_w$  中直接准确的提取嵌入的秘密信息。首先，他先将收到的图像分成  $M \times N/4$  个不重叠的块，每个块的大小为  $2 \times 2$ 。根据阈值  $T$  将这些图像块分成平滑区  $\Omega_1$  和复杂区  $\Omega_2$ 。然后，将平滑区  $\Omega_1$  中的像素比特分成许多的组，并从每组中提取出嵌入的  $\alpha$  个秘密信息。

如果接收者只有加密密钥，他就可以直接解密图像得到一个近似于原始图像的解密图像  $\mathbf{I}_d$ 。首先，接收者将图像分成  $M \times N/4$  个不重叠的块，并根据阈值  $T$  将这些块分成平滑区  $\Omega_1$  和复杂区  $\Omega_2$ 。然后，根据密钥  $r_{i,j}^{(x,y,s)}$  和  $\rho_{i,j}$  可以解密相应的比特位，然后将  $M \times N/4$  个不重叠的块逆置乱放回原始的位置，这样一个直接解密的图像就形成了。因为复杂区  $\Omega_2$  的像素值没有发生任何改变，所以我们直接解密图像的质量是非常好的。

如果接收者既有信息嵌入的密钥，又有加密密钥，他就可以准确的提取秘密信息和无损的恢复原始图像。正如上文中所写，接收者可以根据信息嵌入的密钥将秘密信息从图像中提取出来。接着，接收者要恢复平滑区  $\Omega_1$  中像素的  $u$  个最低有效位(LSB)。首先，根据信息嵌入的密钥，接收者可以得到一个大小为  $\alpha \times l$  的二进制矩阵  $\mathbf{H}$ ：

$$\mathbf{H} = [\mathbf{Q}', \mathbf{E}_\alpha], \quad (3.13)$$

矩阵  $\mathbf{H}$  由  $\mathbf{Q}$  的转置矩阵和一个大小为  $\alpha \times \alpha$  的单位阵  $\mathbf{E}_\alpha$  组成。接着，我们定义一个集合  $\Theta_k$ ：

$$\Theta_k = \{\Lambda_k^{(1)}, \Lambda_k^{(2)}, \dots, \Lambda_k^{(2^\alpha)}\}, \quad (3.14)$$

$$\Lambda_k^{(t)} = [z(k, 1), z(k, 2), \dots, z(k, l - \alpha), 0, 0, \dots, 0] + \Gamma_t \cdot \mathbf{H}, \quad t = 1, 2, \dots, 2^\alpha, \quad (3.15)$$

$\Gamma_t$  是一个大小为  $1 \times \alpha$  的二进制矩阵。因此，根据式(3.12)向量  $\mathbf{V}_k = [v(k, 1), v(k, 2), \dots, v(k, l)]$  一定是集合  $\Theta_k$  中的一种。对于每一个像素组，我们都可以利用加密密钥恢复

每个像素的高位比特信息，得到一个解密图像  $\mathbf{I}_d$ 。很显然， $(8-u)$ 个最高有效位的比特信息是与原始图像  $\mathbf{I}_o$  相同的。这样，相邻像素的 $(8-u)$ 个最高有效位就可以用来预测需要恢复的像素值。

$$D_k^{(t)} = \sum_{(x,y) \in \mathfrak{R}_k} \left| \beta_{x,y}^{(t)} - \hat{\beta}_{x,y} \right|, \quad t = 1, 2, \dots, 2^\alpha, \quad (3.16)$$

$$\hat{\beta}_{x,y} = 2^u \times (\lambda_1 \cdot \hat{\beta}_{x,y} + \lambda_2 \cdot \tilde{\beta}_{x,y}) + 2^{u-1}, \quad (3.17)$$

$$\hat{\beta}_{x,y} = \frac{\lfloor \beta_{x-1,y}^{(t)} / 2^u \rfloor + \lfloor \beta_{x+1,y}^{(t)} / 2^u \rfloor + \lfloor \beta_{x,y-1}^{(t)} / 2^u \rfloor + \lfloor \beta_{x,y+1}^{(t)} / 2^u \rfloor}{4}, \quad (3.18)$$

$$\tilde{\beta}_{x,y} = \frac{\lfloor \beta_{x-1,y-1}^{(t)} / 2^u \rfloor + \lfloor \beta_{x+1,y-1}^{(t)} / 2^u \rfloor + \lfloor \beta_{x-1,y+1}^{(t)} / 2^u \rfloor + \lfloor \beta_{x+1,y+1}^{(t)} / 2^u \rfloor}{4}, \quad (3.19)$$

$\beta_{x,y}^{(t)}$ 表示直接解密图像中的像素， $\lambda_1$ 和 $\lambda_2$ 是两个权重( $\lambda_1 + \lambda_2 \equiv 1$ )。由于自然图像的平滑特性，我们把拥有最小值的向量  $\mathbf{\Lambda}_k^{(t)}$ 认为是原始图像的信息。

$$t^* = \arg \min_t D_k^{(t)}, \quad t = 1, 2, \dots, 2^\alpha. \quad (3.20)$$

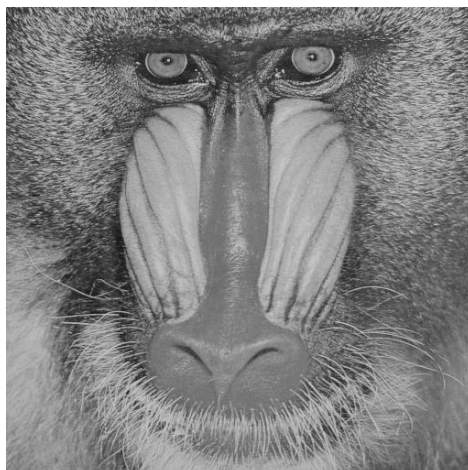
我们将所有的像素组都采用上面的方法进行恢复，因为复杂区 $\Omega_2$ 的像素没有嵌入秘密信息，所以这些像素可以通过加密密钥直接正确恢复。最后将平滑区 $\Omega_1$ 的恢复像素值与复杂区 $\Omega_2$ 的解密像素值合并就可以得到恢复的原始图像  $\mathbf{I}_o$ 。

在本章方法中，只有平滑区 $\Omega_1$ 的像素被用来嵌入秘密信息，同时，更加精确的预测算法也被用来在恢复过程中计算原始像素值。因此，本章方法的直接解密质量是非常好的，但因为有了精准的像素预测算法，所以信息的嵌入量以及原始图像的恢复质量都是令人满意的。

### 3.4 实验结果



(a) Lena



(b) Baboon



(c) Airplane



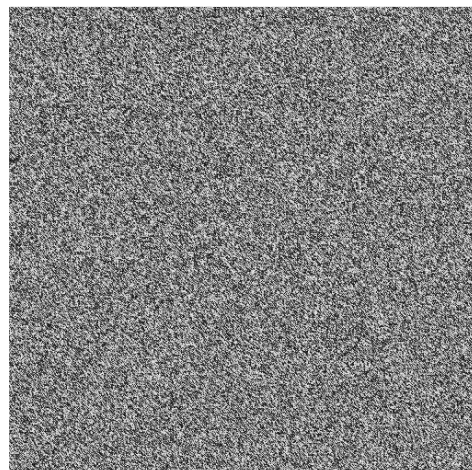
(d) Man

图 3.6 四幅测试图像

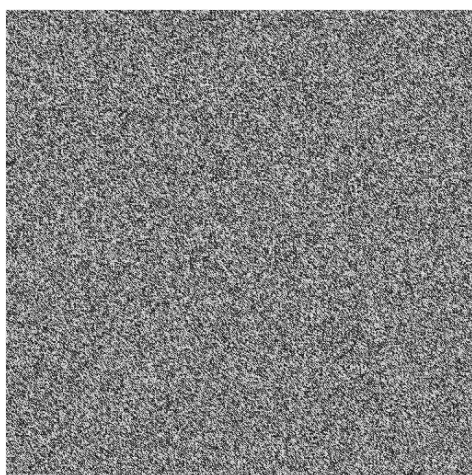
在实验部分，我们使用四幅图像来完成本章方法的实验，包括 Lena，Baboon，Airplane 和 Man，如图 3.6 所示。这四张测试图像都是大小为  $512 \times 512$  的未压缩的原始图像。后面的实验结果都是基于这四张图像来进行的。



(a) 原始图像



(b) 加密图像



(c) 嵌入秘密信息的加密图像



(d) 解密图像

图 3.7 Airplane 图像的四种结果图



图 3.8 Man 图像的四种结果图

图 3.7 和图 3.8 显示的是在  $T = 40$ ,  $u = 3$ ,  $p = 240$ ,  $\alpha = 5$ ,  $\lambda_1 = 0.9$  and  $\lambda_2 = 0.1$  的情况下, 我们利用测试图像 Airplane 和 Man 的实验结果。图 3.7 和图 3.8 的子图像(a-d)显示的分别是原始图像, 加密图像, 嵌有秘密信息的加密图像和直接解密图像。在图 3.7 中, 秘密信息的嵌入量为 0.020bpp, 直接解密的图像的峰值信噪比是 41.4 dB。在图 3.8 中, 秘密信息的嵌入量为 0.020bpp, 直接解密的图像的峰值信噪比是 41.2 dB。这里我们可以定义嵌入量的表达式, 即信息的嵌入量可以表示为:

$$\tau = \frac{4 \cdot \alpha \cdot \gamma}{p \cdot M \cdot N}. \quad (3.21)$$

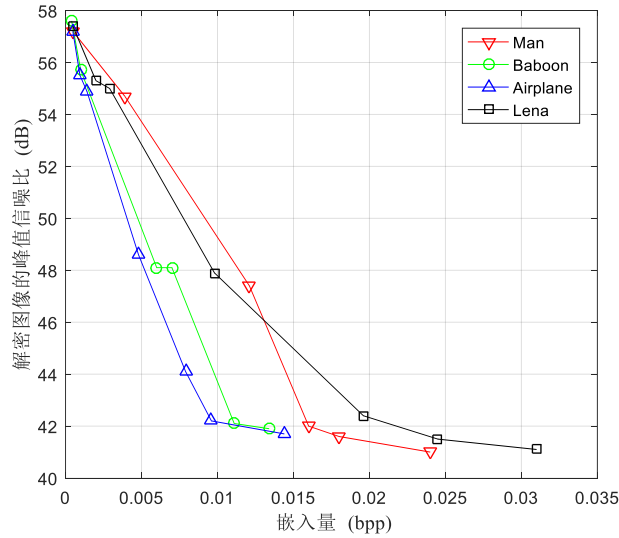


图 3.9 解密图像在不同嵌入量时的 PSNR

图 3.9 给出了直接解密图像的在不同嵌入量的情况下峰值信噪比的曲线图。这里我们采用了四幅测试图像，分别是 Lena, Baboon, Airplane 和 Man。如图 3.9 所示，峰值信噪比的最大值是 57.8 dB，最小值也大于 41 dB。表 3.1 列出了 Lena 和 Baboon 图在不同阈值  $T$  的情况下，平滑块的百分比，信息的嵌入量以及解密图像的峰值信噪比的实验结果。在表 3.1 中，我们可以看到当阈值  $T$  的值变小的时候，属于平滑区  $\Omega_1$  的块就会减少，这样信息的嵌入量也会相应的减少。此外，当两幅图像的阈值  $T$  都一样的情况下，平滑图像(如 Lena)的信息的嵌入量也会大于复杂图像(如 Baboon)的嵌入量。表 3.2 给出了基于我们提出的框架下秘密信息的嵌入量，直接解密质量和图像的恢复质量的表现情况。在不同的参数下，信息的嵌入量，图像的解密和恢复质量会发生一定的变化。当参数  $u$  比较小时，图像的解密质量会比较高。同时，较高的  $\alpha$  也会让信息的嵌入量变大。如表 3.2 所示，符号“ $+\infty$ ”表示恢复图像的峰值信噪比的值是无穷大，表明原始图像可以被无损的恢复。我们可以从表 3.2 中看出，当秘密信息的嵌入量不是特别大的时候，本文的方法可以完全正确的恢复原始图像。在图 3.10 中，横坐标表示嵌入率，纵坐标表示峰值信噪比(PSNR)的值。我们将本文方法的图像解密质量与文献[15, 17, 21, 22]的方法进行了比较，分别利用了图像 Lena, Baboon, Airplane 和 Man。图 3.10 展示了秘密信息的嵌入量与直接解密图像质量的关系对比情况，从中可看出在相同的嵌入量的情况下，本文方法的直接解密图像的峰值信噪比高于其他四种文献方法。此外，我们还采用了图像的结构相似性(SSIM)<sup>[42]</sup>，综合考虑了亮度、对比度和结构等信息，对直接解密图像的视觉质量进行了测量。SSIM 的计算方法如式 3.22 与式 3.23。

$$\Phi(\mathbf{X}, \mathbf{Y}) = \frac{1}{K} \cdot \sum_{i=1}^K \varphi(\mathbf{x}^{(i)}, \mathbf{y}^{(i)}), \quad (3.22)$$

$$\varphi(\mathbf{x}^{(i)}, \mathbf{y}^{(i)}) = \frac{(2\mu_x^{(i)}\mu_y^{(i)} + C_1) \cdot (2\sigma_{xy}^{(i)} + C_2)}{\{[\mu_x^{(i)}]^2 + [\mu_y^{(i)}]^2 + C_1\} \cdot \{[\sigma_x^{(i)}]^2 + [\sigma_y^{(i)}]^2 + C_2\}}, \quad (3.23)$$

这里的  $\mathbf{X}$  和  $\mathbf{Y}$  分别原始图像和用于评价的修饰过的图像,  $\mathbf{x}^{(i)}$  和  $\mathbf{y}^{(i)}$  表示  $\mathbf{X}$  和  $\mathbf{Y}$  中的第  $i$  个块,  $K$  是块的个数,  $\mu_x^{(i)}$  和  $\mu_y^{(i)}$  是  $\mathbf{x}^{(i)}$  和  $\mathbf{y}^{(i)}$  的均值,  $\sigma_x^{(i)}$  和  $\sigma_y^{(i)}$  是  $\mathbf{x}^{(i)}$  和  $\mathbf{y}^{(i)}$  的标准偏差,  $C_1$  和  $C_2$  是一个趋近于零的常数。SSIM 的值属于  $[0,1]$ , SSIM 的值越大, 则说明待评价的图像质量越高。图 3.11 中, 横坐标表示嵌入率, 纵坐标表示结构相似性(SSIM)的值。我们依然使用图像 Lena, Baboon, Airplane 和 Man 来显示本章方法在直接解密图像的图像质量方面的优越性。如图 3.11 所示, 相比于文献[15, 17, 21, 22], 本章的方法在图像的结构相似性(SSIM)方面的实验结果也是非常好的。

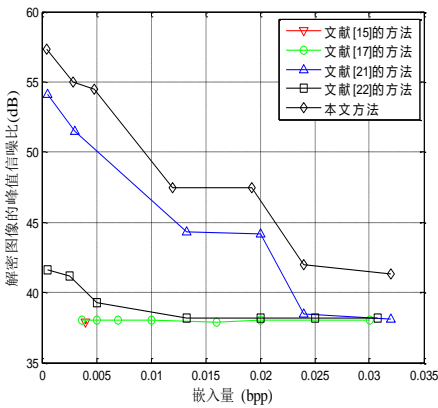
表 3.1 不同阈值时平滑块的百分比, 嵌入量和解密图像的峰值信噪比

阈值	Lena			Baboon		
	平滑块的	嵌入量	解密图	平滑块的	嵌入量	解密图
	百分比		像的峰	百分比		像的峰
	$(4\gamma/MN)$		值信噪	$(4\gamma/MN)$		值信噪
			比			比
$T = 5$	46.01%	0.0096	44.5	21.42%	0.0044	47.8
$T = 10$	82.74%	0.0172	41.9	52.07%	0.0108	43.9
$T = 20$	91.18%	0.0190	41.5	68.14%	0.0140	42.8
$T = 40$	97.93%	0.0204	41.2	89.11%	0.0186	41.6
$T = 60$	99.11%	0.0206	41.1	94.79%	0.0197	41.3
$T = 80$	99.71%	0.0207	41.1	98.50%	0.0205	41.1
$T = 100$	99.86%	0.0208	41.1	99.42%	0.0207	41.2

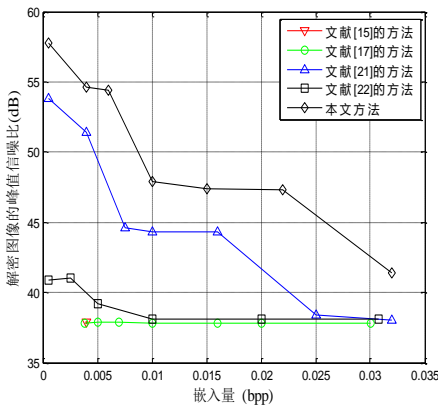


表 3.2 不同参数下的嵌入量，直接解密质量和图像的恢复质量

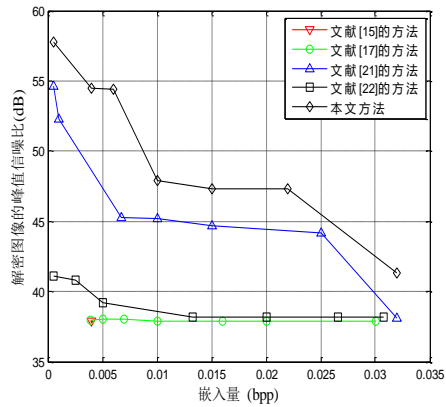
图像	$u$	$p$	$\alpha = 1$	$\alpha = 2$	$\alpha = 3$
Airplane	1	1200	0.0008, 57.5, $+\infty$	0.0016, 55.8, $+\infty$	0.0024, 54.9, $+\infty$
	2	400	0.0024, 50.4, $+\infty$	0.0048, 48.3, $+\infty$	0.0072, 47.8, $+\infty$
	3	160	0.0060, 44.2, $+\infty$	0.0120, 42.6, $+\infty$	0.0180, 41.9, $+\infty$
Man	1	1200	0.0008, 57.7, $+\infty$	0.0016, 55.7, $+\infty$	0.0024, 54.7, $+\infty$
	2	400	0.0024, 50.0, $+\infty$	0.0049, 48.2, $+\infty$	0.0073, 47.7, $+\infty$
	3	160	0.0061, 44.1, $+\infty$	0.0121, 42.2, $+\infty$	0.0182, 41.6, 74.2
Lena	1	1200	0.0008, 57.4, $+\infty$	0.0016, 55.4, $+\infty$	0.0024, 54.9, $+\infty$
	2	400	0.0024, 50.2, $+\infty$	0.0049, 48.5, $+\infty$	0.0073, 47.8, $+\infty$
	3	120	0.0082, 44.1, $+\infty$	0.0163, 41.9, $+\infty$	0.0245, 41.7, $+\infty$
Baboon	1	4800	0.0002, 57.0, $+\infty$	0.0004, 56.1, $+\infty$	0.0005, 55.0, 71.5
	2	1400	0.0006, 50.8, $+\infty$	0.0013, 49.2, $+\infty$	0.0019, 48.3, $+\infty$
	3	400	0.0022, 44.5, $+\infty$	0.0045, 42.6, $+\infty$	0.0067, 41.8, 69.5



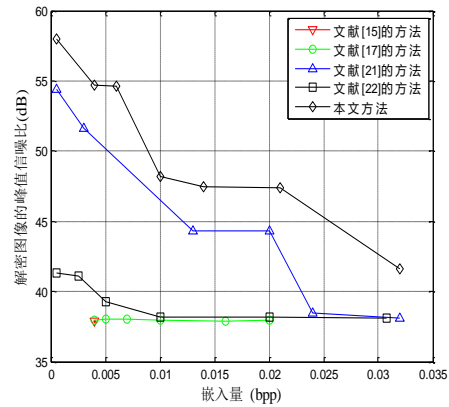
(a) Airplane



(b) Man

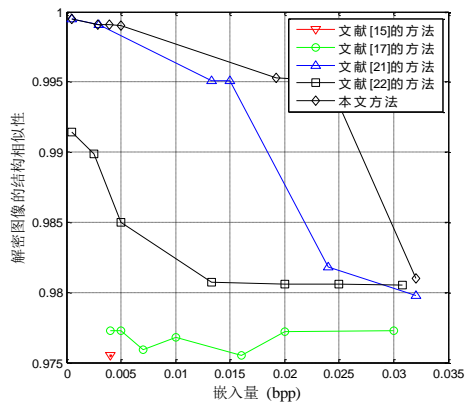


(c) Lena

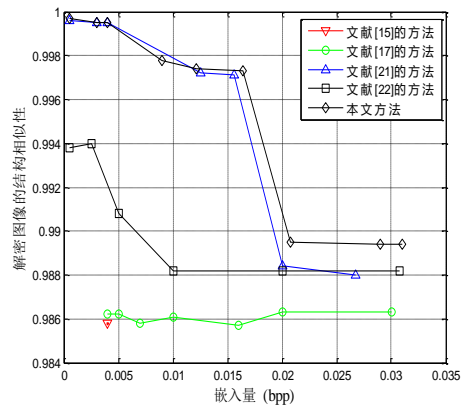


(d) Baboon

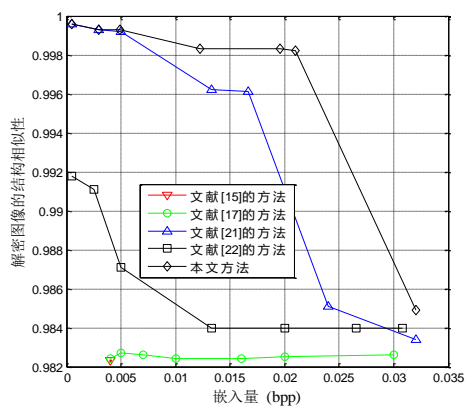
图 3.10 不同嵌入量下直接解密图像 PSNR 比较



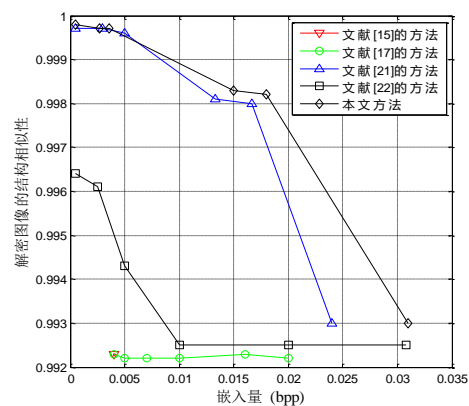
(a) Airplane



(b) Man



(c) Lena



(d) Baboon

图 3.11 不同嵌入量下直接解密图像 SSIM 比较

### 3.5 本章小结

在本章中，我们提出了一个新的加密图像的可逆信息隐藏的框架，包括图像加密，信息隐藏，信息提取和图像恢复。在图像加密阶段，原始图像中所有未重叠的块被特殊的流密码和后续的块置乱加密，从而保护图像的原始信息不被泄露。在信息隐藏的阶段，信息嵌入者将这些加密的图像块分成平滑区和复杂区，通过压缩平滑区像素的最低有效位(LSB)来嵌入秘密信息。当嵌入有秘密信息的加密图像发送到接收端时，如果接收者只有加密密钥时，他就可以直接解密图像得到一个近似于原始图像的直接解密图像，但不能提取秘密信息。如果接收者只有信息嵌入的密钥，他就可以准确地直接提取秘密信息，但无法获得原始图像的信息。当接收者既有加密密钥，又有信息嵌入的密钥时，他既可以提取秘密信息，又可以无损地恢复原始图像。因为在嵌入过程中，复杂区的像素值没有发生任何改变，所以本文的方法提高了直接解密图像的图像质量。

## 第四章 基于混合嵌入机制的加密图像的可逆信息隐藏

在第四章中，我们提出另一种新的加密图像的可逆信息隐藏框架，如图 1.1 所示，包括图像的加密，信息的嵌入，信息的提取和图像的恢复。图像拥有者首先将原始图像分成  $2 \times 2$  大小的不重叠的块，然后利用特殊的流密码和块置乱的方法加密这些图像块。信息嵌入者在拿到加密图像后，根据阈值  $T$  将图像块分成平滑区和复杂区。在平滑区中，我们用秘密信息替换部分像素的最高有效位(MSB)，实现信息的第一步嵌入。然后，再压缩剩余的部分像素的最低有效位(LSB)创建一个空余空间来第二步嵌入秘密信息。经过这两个信息嵌入的过程，一个嵌入有秘密信息的加密图像就形成了。当接收者只有加密密钥时，他就可以根据密钥直接解密图像。如果接收者只有信息嵌入的密钥，他就可以直接提取秘密信息，但不能解密图像。如果接收者既有加密密钥，又有信息嵌入的密钥，他既可以准确的提取秘密信息，又可以无损的恢复原始图像。

### 4.1 图像加密

原始未压缩的灰度图像  $\mathbf{I}$  的大小是  $M \times N$ ，并且可以每个像素都可以被表示成 8 比特。图像拥有者首先将原始图像  $\mathbf{I}$  分成  $2 \times 2$  大小的不重叠的图像块，这样总共有  $M \times N / 4$  个图像块。然后将这些图像块表示成  $\mathbf{B}_{i,j}$  ( $1 \leq i \leq M/2$  和  $1 \leq j \leq N/2$ )，每个块中的四个像素表示为  $B_{i,j}^{(0,0)}$ ,  $B_{i,j}^{(0,1)}$ ,  $B_{i,j}^{(1,0)}$  和  $B_{i,j}^{(1,1)}$ 。如图 4.1 所示，像素  $B_{i,j}^{(0,0)}$  和  $B_{i,j}^{(1,1)}$  用“○”来表示， $B_{i,j}^{(0,1)}$  和  $B_{i,j}^{(1,0)}$  用“□”来表示。

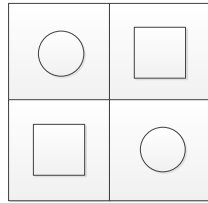


图 4.1 每个块中的四个像素

将每个块中四个像素值分解成 8 比特

$$b_{i,j}^{(x,y,u)} = \left\lfloor \frac{B_{i,j}^{(x,y)}}{2^u} \right\rfloor \bmod 2, \quad u = 0, 1, \dots, 7, \quad (4.1)$$

这里的 $(i, j)$ 是块的索引, 并且 $(x, y) \in \{(0,0), (0,1), (1,0), (1,1)\}$ 。在每一个块中, 图像拥有者根据加密密钥, 利用伪随机的流密码加密方形像素的 8 个比特和圆形像素的  $p$  个比特

$$b'_{i,j}(x,y,u) = b_{i,j}(x,y,u) \oplus f_{i,j}(x,y,u), \quad (x,y,u) \in \Psi_1 \cup \Psi_2, \quad (4.2)$$

$$\Psi_1 = \{(x,y,u) \mid (x,y) \in \{(1,0), (0,1)\} \text{ and } u = 0, 1, 2, \dots, 7\}, \quad (4.3)$$

$$\Psi_2 = \{(x,y,u) \mid (x,y) \in \{(0,0), (1,1)\} \text{ and } u = 0, 1, 2, \dots, p-1\}, \quad (4.4)$$

这里的  $p$  表示最低有效位(LSB)的个数, 并且是一个小于 4 的正整数。然后, 图像拥有者需要去加密每个块中的圆形像素余下的 $(8-p)$ 个比特。另一个不同伪随机的二进制序列  $A_{i,j}$  由加密密钥生成。

$$\begin{cases} b'_{i,j}(x,y,u) = \overline{b_{i,j}(x,y,u)}, & \text{if } A_{i,j} = 1, \\ b'_{i,j}(x,y,u) = b_{i,j}(x,y,u), & \text{if } A_{i,j} = 0, \end{cases} \quad (x,y,u) \in \Psi_3, \quad (4.5)$$

$$\Psi_3 = \{(x,y,u) \mid (x,y) \in \{(0,0), (1,1)\} \text{ and } u = p, p+1, p+2, \dots, 7\}. \quad (4.6)$$

最后, 流密码加密的像素值可以根据式(4.7)得到

$$B_{i,j}^{(x,y)} = \sum_{u=0}^7 [2^u \times b'_{i,j}(x,y,u)]. \quad (4.7)$$

当所有的像素都加密完成, 图像拥有者根据加密密钥将图像块伪随机置乱, 形成最终的加密图像  $\mathbf{I}_e$ 。

## 4.2 信息嵌入

在这一节中, 秘密信息被分成两步嵌入到加密图像中。

第一步: 加密图像  $\mathbf{I}_e$  被分成许多个不重叠的块, 每个块的大小是  $2 \times 2$ , 并用  $\mathbf{E}_{i,j}$  表示。在每个加密的图像块  $\mathbf{E}_{i,j}$  中, 四个像素从上到下, 从左到右被分别表示为  $E_{i,j}^{(0,0)}$ ,  $E_{i,j}^{(0,1)}$ ,  $E_{i,j}^{(1,0)}$  和  $E_{i,j}^{(1,1)}$ 。然后, 信息嵌入者计算每个图像块的两个圆形像素的绝对差作为块的平滑度值:

$$d_{i,j} = \left| 2^p \cdot \lfloor E_{i,j}^{(0,0)} / 2^p \rfloor - 2^p \cdot \lfloor E_{i,j}^{(1,1)} / 2^p \rfloor \right|, \quad (4.8)$$

这里  $d_{ij}$  表示相对应块的平滑度值。 $d_{ij}$  的值越高说明图像越复杂。为了更好地区分这些块，我们设定一个阈值  $T$ 。根据阈值，信息嵌入者将这些块分成平滑区和复杂区。

$$\begin{cases} \mathbf{E}_{i,j} \in \mathbf{R}_1, & \text{if } d_{i,j} \leq T, \\ \mathbf{E}_{i,j} \in \mathbf{R}_2, & \text{if } d_{i,j} > T, \end{cases} \quad (4.9)$$

这里的  $\mathbf{R}_1$  和  $\mathbf{R}_2$  分别表示平滑区和复杂区。在平滑区  $\mathbf{R}_1$  中，信息嵌入者收集每个块的两个方形像素  $E_{ij}^{(0,1)}$  和  $E_{ij}^{(1,0)}$  形成一个像素组  $\mathbf{G}_e$ 。在这个像素组里的像素的最高有效位(MSB)被秘密信息  $b_e$  替换

$$E'_{i,j}(x,y) = (E_{i,j}(x,y) \bmod 128) + b_e \times 128, \quad (x,y) \in \Psi_4, \quad (4.10)$$

$$\Psi_4 = \{(x,y) \mid (x,y) \in \{(0,1), (1,0)\}\}. \quad (4.11)$$

当像素组  $\mathbf{G}_e$  中所有像素都被嵌入秘密信息后，信息嵌入者把他们放回原始位置。因为考虑到原始图像的像素的空间相关性，所以我们把信息嵌入到平滑区  $\mathbf{R}_1$ 。这样，第一步秘密信息的嵌入就完成了。在这一步中，我们把秘密信息嵌入通过最高有效位(MSB)替换的方式嵌入到平滑区  $\mathbf{R}_1$  的图像块中，因此，如果阈值  $T$  变大，则将会有更多的块分到平滑区，也就意味着会有更多的秘密信息嵌入到加密图像中。

第二步：信息嵌入者直接收集每个块中的两个圆形像素( $E_{ij}^{(0,0)}, E_{ij}^{(1,1)}$ )的  $p$  个最低有效位 (LSB)，并将它们平均分成不同的组，每个组有  $q$  个像素。在这一步中，可以被用来嵌入秘密信息的像素个数是  $M \times N/2$ 。在每个组中，将这些像素表示为  $v(k, 1), v(k, 2), \dots, v(k, p \cdot q)$ ， $k$  表示组的索引。根据信息嵌入的密钥，信息嵌入者可以生成一个大小为  $(p \cdot q - s) \times p \cdot q$  的二进制矩阵。

$$\mathbf{M} = [\mathbf{I}_{p \cdot q - s}, \mathbf{Q}], \quad (4.12)$$

这里的矩阵  $\mathbf{I}$  是一个大小为  $(p \cdot q - s) \times (p \cdot q - s)$  的单位矩阵，矩阵  $\mathbf{Q}$  是一个大小为  $(p \cdot q - s) \times s$  的伪随机的二进制矩阵。在每组中，我们根据式(4.13)压缩收集的比特。

$$\begin{bmatrix} v'(k, 1) \\ v'(k, 2) \\ \vdots \\ v'(k, p \cdot q - s) \end{bmatrix} = \mathbf{M} \cdot \begin{bmatrix} v(k, 1) \\ v(k, 2) \\ \vdots \\ v(k, p \cdot q) \end{bmatrix}. \quad (4.13)$$

经过式(4.13)的计算, 原始向量 $[v(k, 1), v(k, 2), \dots, v(k, p \cdot q)]$ 被压缩成 $[v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q - s)]$ , 这样  $p \cdot q$  个比特就被压缩成 $(p \cdot q - s)$ 个比特。信息嵌入者接着将秘密信息嵌入到每一组的 $[v'(k, p \cdot q - s + 1), v'(k, p \cdot q - s + 2), \dots, v'(k, p \cdot q)]$ 中。重新合并 $[v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q - s)]$  和 $[v'(k, p \cdot q - s + 1), v'(k, p \cdot q - s + 2), \dots, v'(k, p \cdot q)]$ 形成新的向量 $[v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q)]$ 。最后将向量 $[v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q)]$ 替换原始的向量 $[v(k, 1), v(k, 2), \dots, v(k, p \cdot q)]$ , 并放回原位置, 这样就完成了第二步的信息嵌入。最终经过这两步, 一个嵌入秘密信息的加密图像  $\mathbf{I}_m$  就形成了。

### 4.3 信息提取和图像恢复

如果接收者只有加密密钥, 他就可以直接解密图像。如果接收者只有信息嵌入的密钥, 他就可以提取秘密信息但无法得到原始图像的信息。如果接收者既有加密密钥, 又有信息嵌入的密钥, 他既可以准确地提取秘密信息, 又可以无损的恢复原始图像。在本章的方法中, 阈值  $T$  是一个预定义的值, 并且被图像拥有者, 信息嵌入者和接收者所知道。

如果接收者只有加密密钥, 他就可以直接解密得到一个近似于原始图像的解密图像。首先, 接收者先将收到的图像  $\mathbf{I}_m$  分成  $M \times N/4$  个大小为  $2 \times 2$  的图像块, 并根据阈值  $T$  将这些图像块分成平滑区  $\mathbf{R}_1$  和复杂区  $\mathbf{R}_2$ 。将每个像素表达成 8 比特, 并根据密钥利用异或操作解密这些像素, 如 4.1 单元所描述的。然后, 将  $M \times N/4$  个图像块逆置乱回原来的位置。为了更好的提高直接解密图像的质量, 接收者还需要恢复平滑区  $\mathbf{R}_1$  中每个方形像素的最高有效位(MSB)。因为圆形像素的 $(8-p)$ 个最高有效位(MSB)解密后是没有发生改变的, 所以接收者可以根据这些没有改变的比特信息得到一个参考像素值。

$$\hat{p}_{m,n} = \frac{\lfloor p_{m-1,n} / 2^p \rfloor + \lfloor p_{m+1,n} / 2^p \rfloor + \lfloor p_{m,n-1} / 2^p \rfloor + \lfloor p_{m,n+1} / 2^p \rfloor}{4} \cdot 2^p + 2^{p-1}, \quad (4.14)$$

其中参考像素值来自于周围相邻的像素值, 并且 $(m,n)$ 表示像素的位置( $1 \leq m \leq M$  和  $1 \leq n \leq N$ )。对于平滑区  $\mathbf{R}_1$  的方形像素来说, 接收者就可以根据参考像素值计算得到原始的像素值,

$$p'_{m,n} = \begin{cases} 128 + \text{mod}(p_{m,n}, 128), & \text{if } |128 + \text{mod}(p_{m,n}, 128) - \hat{p}_{m,n}| < |\text{mod}(p_{m,n}, 128) - \hat{p}_{m,n}|, \\ \text{mod}(p_{m,n}, 128), & \text{otherwise.} \end{cases} \quad (4.15)$$

根据式(4.15), 接收者进一步恢复了平滑区  $\mathbf{R}_1$  中方形像素的最高有效位(MSB)。因为信息嵌入者将秘密信息嵌入到平滑区部分像素的最高有效位, 所以像素比特恢复的结果是很好的。

如果接收者只有信息嵌入的密钥, 他就可以直接准确地提取秘密信息。首先, 接收者将收到的图像分成大小为  $2 \times 2$  的不重叠的块, 并根据阈值  $T$  将这些块分成平滑区  $\mathbf{R}_1$  和复杂区  $\mathbf{R}_2$ 。嵌入到平滑区  $\mathbf{R}_1$  的方形像素的秘密信息可以被直接提取出来。接着, 接收者收集每个块中圆形像素的  $p$  个最低有效位(LSB), 并将这些比特分成  $k$  组。每组中, 根据信息嵌入的密钥, 接收者可以提取  $s$  个嵌入的信息。这样, 接收者就可以提取出完整的秘密信息。

如果接收者既有加密密钥, 又有信息嵌入的密钥, 他既可以提取秘密信息, 又可以无损的恢复原始图像。首先, 接收者将收到的图像分成  $M \times N/4$  个大小为  $2 \times 2$  的不重叠的块, 同时, 根据信息嵌入的密钥可以得到参数  $p, q$  和  $s$  的值。将这些不重叠的块根据阈值  $T$  分成平滑区  $\mathbf{R}_1$  和复杂区  $\mathbf{R}_2$ 。这样被嵌入的秘密信息就可以像前文提到的那样被提取出来。然后, 接收者根据加密密钥可以直接解密图像得到解密图像  $\mathbf{I}_d$ 。在解密图像  $\mathbf{I}_d$  中, 只有每个块中的圆形像素的  $p$  个最低有效位(LSB)需要恢复。在每组中, 接收者可以根据公式(4.13)得到一个向量  $[v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q - s)]$ 。则每一组的原始比特向量  $[v(k, 1), v(k, 2), \dots, v(k, p \cdot q)]$  一定是式(4.16)中的一个。

$$\Theta = [v'(k, 1), v'(k, 2), \dots, v'(k, p \cdot q - s), 0, 0, \dots, 0] + \Gamma \cdot \mathbf{H}, \quad (4.16)$$

$$\mathbf{H} = [\mathbf{Q}', \mathbf{I}_s], \quad (4.17)$$

这里的  $\Gamma$  是一个大小为  $1 \times s$  的二进制矩阵,  $\mathbf{H}$  是一个大小为  $s \times pq$  的矩阵, 它由一个大小为  $s \times s$  的单位矩阵和  $\mathbf{Q}$  的转置矩阵构成。为了恢复原始比特向量  $[v(k, 1), v(k, 2), \dots, v(k, p \cdot q)]$ , 就会有  $2^s$  种可能性。接收者将每种可能的向量  $\Theta$  中的元素放回到原始的位置并解密得到解密的像素组  $O_k$ , 然后根据式(4.18-4.19)在每组中计算解密像素值和参考像素值之间总的误差。这里  $r_{m,n}$  表示解密的像素值。

$$\tilde{p}_{m,n} = \frac{p_{m-1,n} + p_{m+1,n} + p_{m,n-1} + p_{m,n+1}}{4}, \quad (4.18)$$

$$D = \sum_{(m,n) \in O_k} |r_{m,n} - \tilde{p}_{m,n}|. \quad (4.19)$$

这样  $2^s$  个  $D$  值就对应  $2^s$  个解密的像素组  $O_k$ 。因为考虑到自然图像的相邻像素相关



性，所以我们将有最小值  $D$  的那一组解密的像素值作为原始图像的像素值，并将他们放回原位置。每一组都把有最小值  $D$  的一组解密像素值作为原始像素值。当所有的像素组都恢复以后，原始图像就成功恢复了。

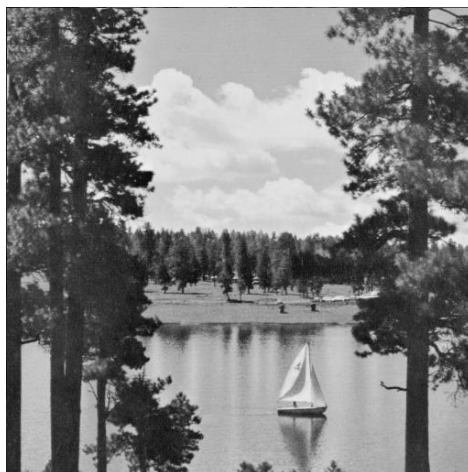
在本章的方法中，我们先利用圆形像素的 $(8-p)$ 个最高有效位(MSB)来帮助恢复方形像素的最高有效位(MSB)，然后利用已恢复的方形像素来帮助恢复圆形像素的  $p$  个最低有效位(LSB)，从而实现原始图像的最终无损恢复。虽然我们使用了最高有效位(MSB)来完成秘密信息的嵌入，但是我们充分利用了相邻像素的相关性来帮助恢复原始图像，图像的恢复质量和信息的嵌入量都得到了提高。同时，参数  $p, q$  和  $s$  可以作为额外信息传输给接收方。

#### 4.4 实验结果

在实验部分，我们使用四幅图像来进行数据的测试，包括 Airplane, Lake, Lena 和 Crowd，如图 4.2 所示。这四张测试图像都是大小为  $512 \times 512$  的未压缩的灰度图像。每张图像中的像素值的取值范围都是  $[0, 255]$ ，即每个像素值都可以用 8 比特来表示，如式 4.1 所示。基于这四张测试图像，我们进行了接下来的实验，包括图像加密安全性的分析和与其他文献比较的实验。



(a) Airplane

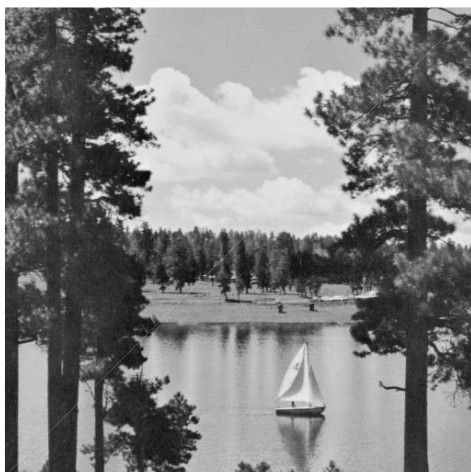


(b) Lake

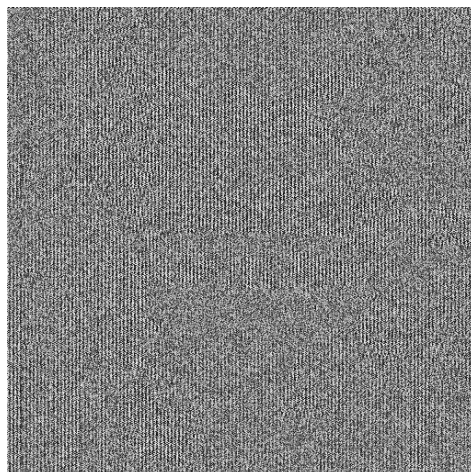


图 4.2 四幅测试图像

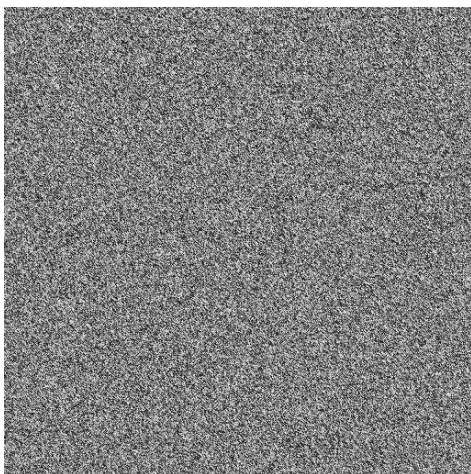
对于加密图像的可逆信息隐藏来说，加密的安全性是一个重要的性能。本章方法的加密算法包括特殊的流密码加密和块置乱。在流密码加密算法之后，我们会随机的置乱  $M \times N/4$  个不重叠的块。在置乱的过程中，会有最多  $(M \times N/4)!$  种置乱后的形式。值得注意的是， $(M \times N/4)!$  是一个很大的数值，所以不可能将已置乱的图像块都准确地放回原始的位置。为了更好地说明我们加密方法的安全性，我们利用 Lake 图作为我们的实验图。图 4.3(a-d) 分别展示了原始图像，流密码加密的初步图像，最终的加密图像和直接解密图像。从图 4.4 (a-b) 中，我们可以看到原始图像和最终加密图像的直方图，但是这个图像的直方图是完全不一样的，加密后的图像的直方图发生了很大的变化。在图 4.4(c-d) 中，X 轴和 Y 轴表示图像中相对应像素的位置，Z 轴则表示像素值。此外，原始图像的像素值分布情况和加密图像的像素值分布情况都在图 4.4(c-d) 中显示出来，很明显，经过加密后的图像的像素值分布情况更规则，更平均，与原始图像的分布图有很大的区别。综上所述，本章方法的加密算法是非常安全的。



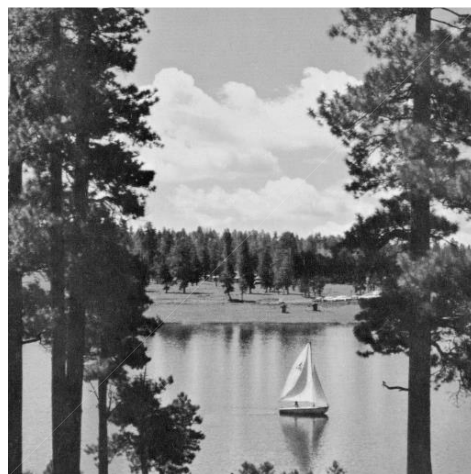
(a) 原始图像



(b) 初步加密图像

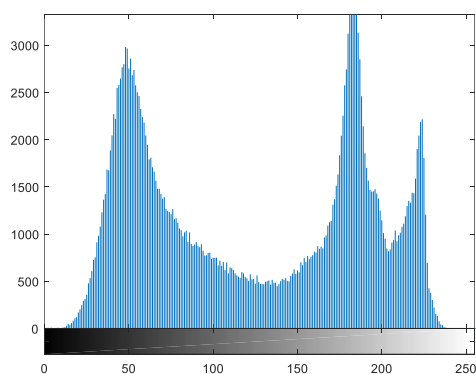


(c) 最终加密图像

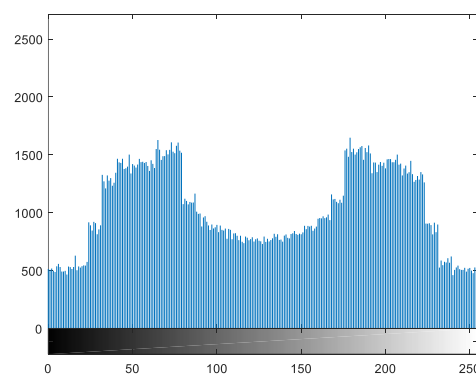


(d) 解密图像

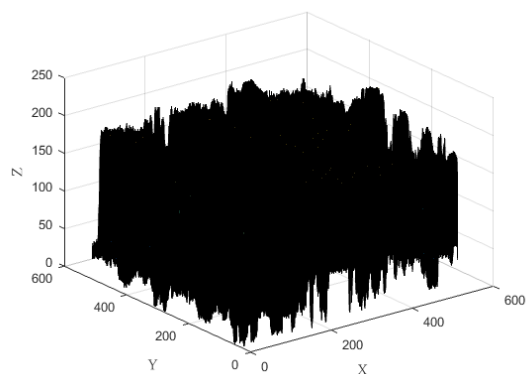
图 4.3 对于 Lake 图像的加密样例



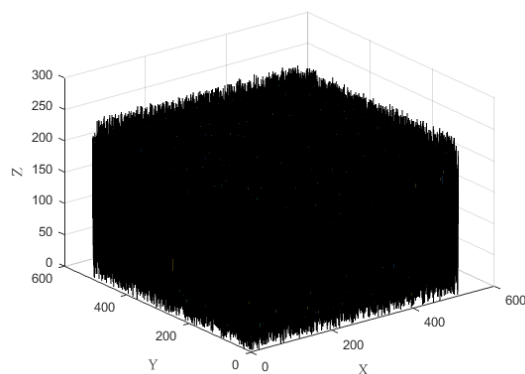
(a) 原始图像直方图



(b) 加密图像直方图



(c) 原始图像像素值分布图



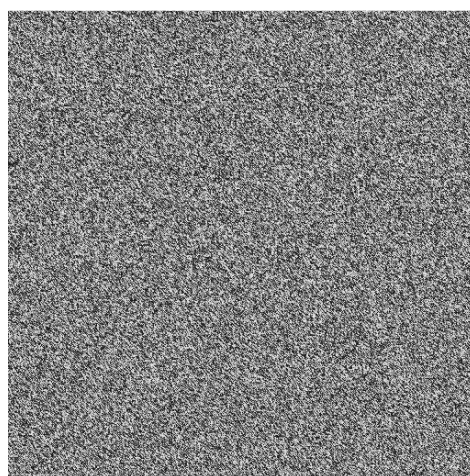
(d) 加密图像像素值分布图

图 4.4 对于 Lake 图像的加密样例

在这一节中，我们使用的测试图像的大小都是  $512 \times 512$ ，并且阈值  $T=1$ 。在图 4.5 中，我们用图像 Airplane 来显示实验结果，这里的参数  $q, p$  和  $s$  分别是 1600, 1 和 1。图 4.5(a)展示了图像 Airplane 的原始图像。图 4.5(b-c)分别显示了加密图像和嵌入量为 0.1171 bpp 的加密图像。图 4.5(d)则显示的是直接解密图像，它的峰值信噪比为 57.4 dB。



(a) 原始图像



(b) 初步加密图像



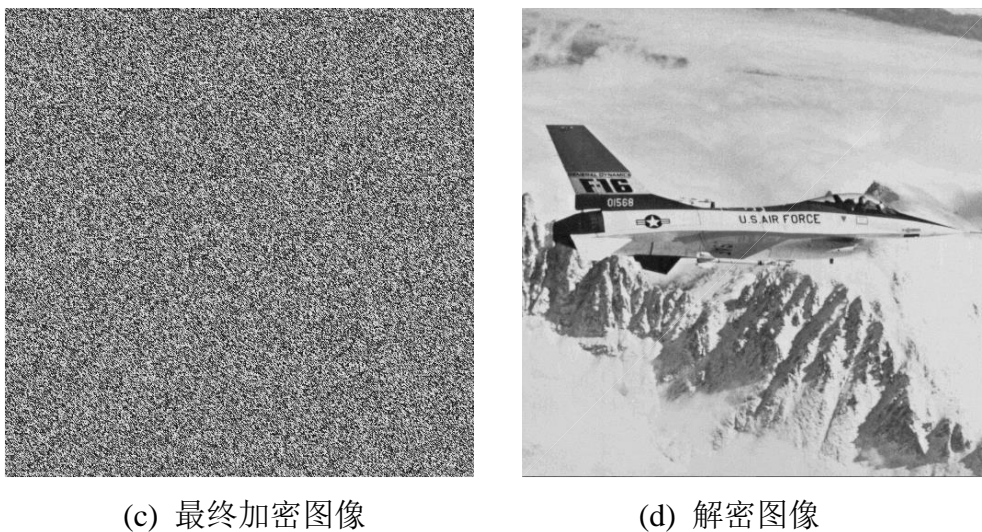


图 4.5 对于 Lake 图像的加密样例

四幅图像 Airplane, Lake, Lena 和 Crowd 在不同嵌入量情况下的实验结果显示在图 4.6 上。他们既拥有比较大的信息嵌入量，也有比较好的直接解密图像质量。本章方法更适合平滑的图像，因为本章方法充分使用了图像中平滑区的特性。

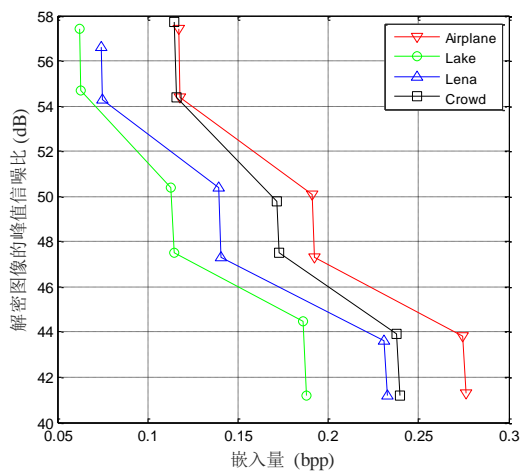
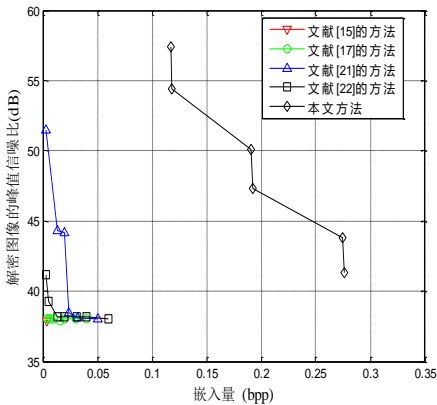


图 4.6 解密图像在不同嵌入量时的 PSNR

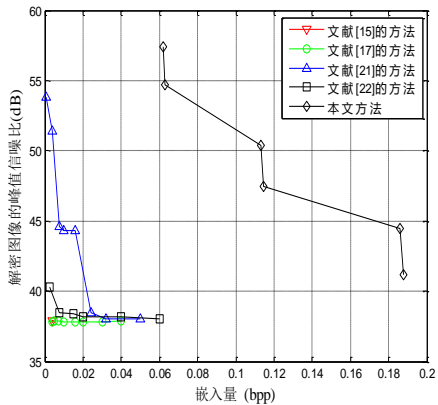
表 4.1 不同参数下的嵌入量，直接解密质量和图像的恢复质量

图像	$q$	$p$	$s = 1$	$s = 2$	$s = 3$
Airplane	1600	1	0.1171, 57.4, $+\infty$	0.1174, 55.3, $+\infty$	0.1177, 54.8, $+\infty$
	1000	2	0.1908, 50.1, $+\infty$	0.1913, 48.3, $+\infty$	0.1918, 47.6, $+\infty$
	800	3	0.2745, 43.8, $+\infty$	0.2751, 41.9, $+\infty$	0.2757, 41.7, $+\infty$
Lake	2000	1	0.0620, 57.4, $+\infty$	0.0622, 55.0, $+\infty$	0.0624, 54.5, 66.2
	1000	2	0.1131, 50.4, $+\infty$	0.1136, 48.6, $+\infty$	0.1141, 47.7, $+\infty$
	800	3	0.1860, 44.5, $+\infty$	0.1866, 42.5, $+\infty$	0.1872, 41.4, $+\infty$
Lena	1600	1	0.0741, 56.6, $+\infty$	0.0744, 55.4, $+\infty$	0.0747, 54.8, $+\infty$
	1000	2	0.1394, 50.4, $+\infty$	0.1399, 48.6, $+\infty$	0.1404, 47.8, $+\infty$
	800	3	0.2307, 43.6, $+\infty$	0.2313, 42.2, $+\infty$	0.2319, 41.5, $+\infty$
Crowd	1600	1	0.1148, 57.7, $+\infty$	0.1151, 55.5, $+\infty$	0.1154, 54.7, $+\infty$
	1000	2	0.1716, 49.8, $+\infty$	0.1721, 48.4, $+\infty$	0.1726, 47.8, $+\infty$
	800	3	0.2377, 43.9, $+\infty$	0.2383, 41.9, $+\infty$	0.2389, 41.5, $+\infty$

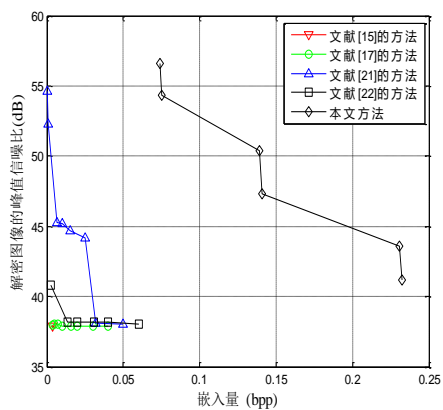
表 4.1 详细的阐明了四幅图像 Airplane, Lake, Lena 和 Crowd 在不同参数下的实验结果。从中我们可以看出，当参数  $p$  的值变大时，则信息的嵌入量也会相应的变大。但是，如果更多的最低有效位(LSB)的被用来嵌入秘密信息，则图像的加密质量会相应的下降。用户可以根据自己的需求来调整参数，达到自己的要求。如表 4.1 所示，图像的恢复质量都是很好的，大多数的原始图像都可以无损的恢复。



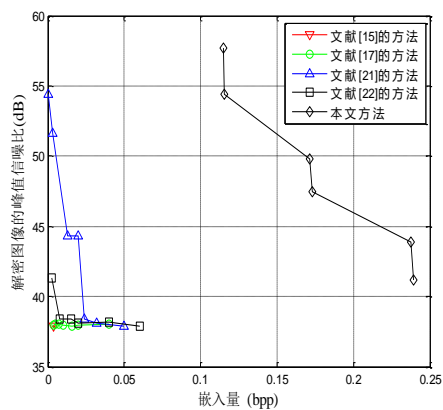
(a) Airplane



(b) Lake

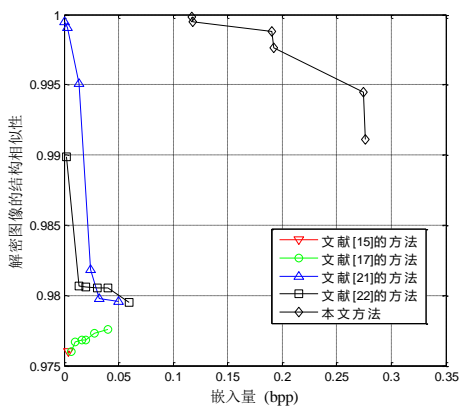


(c) Lena

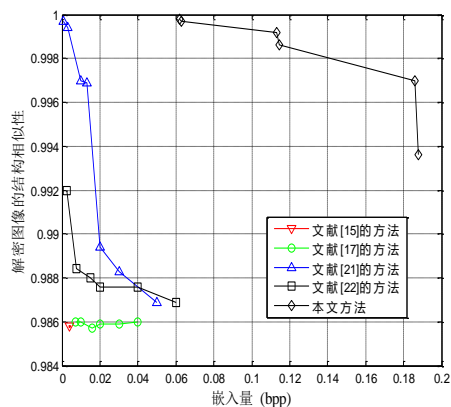


(d) Crowd

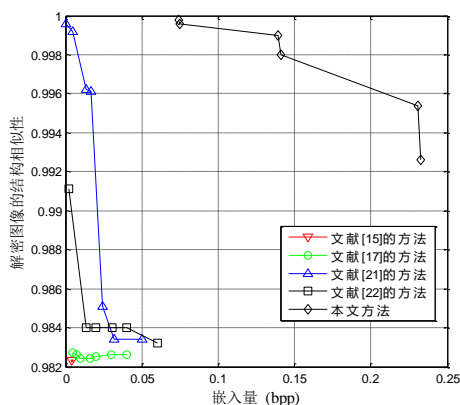
图 4.7 不同嵌入量下直接解密图像 PSNR 比较



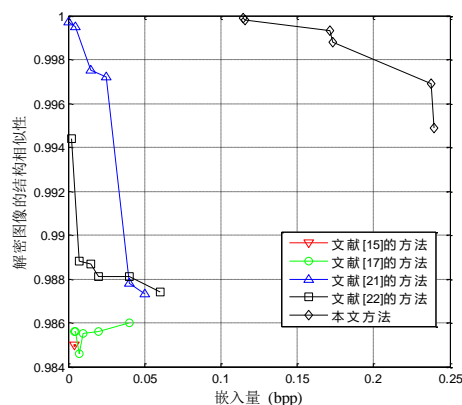
(a) Airplane



(b) Lake



(c) Lena



(d) Crowd

图 4.8 不同嵌入量下直接解密图像 SSIM 比较

图 4.7 与图 4.8 展示了本章方法与文献[15, 17, 21, 22]的比较结果。其中文献[17]的参数  $p=1$ 。图 4.7 从峰值信噪比(PSNR)方面阐述了直接解密图像在不同嵌入量下的对比结果。本章的方法不管是直接解密的图像质量还是信息的嵌入量都高于其他四个文献的方法。图 4.8 则从图像的结构相似性(SSIM)角度表达了直接解密图像在不同嵌入量情况下的对比结果。同样，本章的方法在直接解密图像的质量和信息的嵌入量都高于其他四个文献的方法。在实验部分中，我们设定的阈值  $T$  为 1。如果需要更高的嵌入量，可以将阈值  $T$  设置为更高的数值。

本章方法的计算复杂度主要在信息嵌入的过程包括两步信息嵌入的算法和图像恢复过程中的迭代算法。如果更多的信息要被嵌入到加密图像中，那么本章方法的实际运行时间将会受到影响。在本章的方法中，加密方法，信息嵌入方法和解密方法都有比较低的复杂度。我们将参数  $q$ ,  $p$  和  $s$  分别设定为 1600, 1 和 1，并使用 Lena 图像作为实验图像。我们可以得出每个部分的程序的执行时间，图像的加密，信息的隐藏，图像的解密和图像的恢复的执行时间分别是 0.819 秒，2.570 秒, 0.824 秒和 1.863 秒，这充分说明了本章方法的实时性能 and 在实际应用中的可行性。

本章方法与第三章方法的不同之处主要在秘密信息的嵌入过程和后期的图像恢复过程。在第三章的方法中，信息嵌入者只利用了平滑区的最低有效位(LSB)来完成信息的嵌入，即利用 LDPC 矩阵来压缩平滑区像素的低位比特，并将秘密信息嵌入到被压缩的位置中。这种方法在一定程度上提高了图像的直接解密质量和恢复质量。在本章的方法中，我们采用最高有效位(MSB)和最低有效位(LSB)相配合的方式来进行秘密信息的嵌入。与第三章方法不同的是，本章我们主要利用平



滑区的最高有效位(MSB)来嵌入秘密信息。详细来说,我们将秘密信息与平滑区部分像素的最高有效位(MSB)直接替换从而完成第一次隐藏秘密信息的工作,此外,我们再次利用剩余像素的最低有效位(LSB)的 LDPC 矩阵压缩的方法完成第二步的信息嵌入。在后期的图像恢复过程中,最高有效位(MSB)可以在周围像素的帮助下先恢复,已恢复的像素可以进一步帮助恢复剩余像素的低位比特值。因为本章方法采用了最高有效位(MSB)直接替换的方法,所以本章方法的秘密信息嵌入量有很大的提高。

## 4.5 本章小结

在本章的工作中,我们提出了一个新的加密图像的可逆信息隐藏的方案,在方案中,我们充分利用相邻像素的互相帮助来提高信息的隐藏量和图像的直接解密质量。在图像加密阶段,图像拥有者将原始图像分成不重叠的块,并使用流密码和块置换的方法对原始图像进行加密。当信息嵌入者得到加密图像时,可以在不知道原始图像内容的情况下将秘密信息嵌入到加密图像中。详细来说,信息嵌入者首先将加密的图像块划分为平滑区域和复杂区域,并将秘密信息直接嵌入到平滑区域的方形像素的最高有效位(MSB)中。然后,在所有的块中收集圆形像素的最低有效位(LSB),并利用 LDPC 矩阵压缩这些比特信息,为再次嵌入秘密信息腾出空间。最后生成带有秘密信息的加密图像。如果接收者只有加密密钥,他可以将图像分割成块,并直接用加密密钥解密得到解密图像。如果接收者只有信息嵌入的密钥,则可以根据阈值  $T$  将加密块分为平滑区域和复杂区域,然后通过信息嵌入的密钥提取嵌入的数据。如果接收者同时拥有加密密钥和信息嵌入的密钥,则可以直接提取嵌入数据并无损地恢复原始图像。我们提出的方案具有良好的解密图像质量和较高的嵌入率。

## 第五章 总结与展望

在本文的工作中，我们研究了两种加密图像的可逆信息隐藏的算法，并在第三章和第四章分别对这两种方法进行了详细的阐述。本章中我们对加密图像的可逆信息隐藏的算法进行总结，并对展望未来的发展。

### 5.1 工作总结

本人研究生期间主要的研究方向是加密图像的可逆信息隐藏。这是一个最近几年被提出来的研究课题，主要为了保护原始图像的信息安全和秘密信息的安全。正如现在人们之间的交往日益密切，交流的方式也趋于多样化，包括图像，视频，音频等。随着这种多媒体交流的日益广泛，很多的信息泄露的问题也随之暴露出来，如客户的隐私信息泄露，传输的图像资料被窃取以及上传云端的多媒体资料被篡改等等。信息安全的问题已经给人们敲响了警钟，如何更好的保护人们的隐私成为很多研究人员的研究热点。尤其是在军事、医疗等对于信息安全性要求较高的地方，信息安全至关重要。为了进一步保护人们的图像信息以及秘密信息的安全，有人提出了加密图像的可逆信息隐藏的算法。这套算法主要包括四个部分，分别是图像的加密，信息的嵌入，信息的提取以及图像的恢复。

在第三章中，我们详细阐述了第一种加密图像的可逆信息隐藏算法。该方法通过特殊的加密手段对原始图像进行加密，同时保留了原始图像的部分冗余。信息嵌入者根据这些冗余把图像块分成平滑区和复杂区两个部分。在平滑区部分的像素被分成许多的组，每组像素的个数是相同的。在每组中，收集像素的最低有效位(LSB)组成一串比特流，并利用 LDPC 矩阵对其进行压缩，得到少于原始比特流个数的新比特流，最后将秘密信息嵌入到被压缩的比特流的后面完成信息嵌入工作。在接收端，如果接收者只有加密密钥，他就可以直接解密图像。如果接收者只有信息嵌入的密钥，他可以直接提取秘密信息但无法获取原始图像信息。如果接收者既有加密密钥又有信息嵌入的密钥，他既可以准确的提取秘密信息，又可以无损的恢复原始图像。由于我们没有在复杂区嵌入秘密信息，所以该方法的直接解密质量是很好的。

在第四章中，我们详细阐述了第二种加密图像可逆信息隐藏的算法。与第一种方法不同，我们在第二种方法中，使用了像素的最高有效位(MSB)，并且在嵌入的过程中我们采用分步嵌入的方法，充分利用了相邻像素的相关性，即相邻像素

相互帮助来恢复原始像素值。第四章的方法也是可分离的框架，给予了接收者更多的权限。实验结果表明，该方法在信息的嵌入量、图像的直接解密质量以及图像的恢复质量方面都优于另外四篇比较文献。

## 5.2 未来展望

加密图像的可逆信息隐藏是保护原始图像和秘密信息的有效途径，本文中的方法还有可以进步的地方。对于加密图像的可逆信息隐藏的算法研究，主要在三个方面，包括图像加密的安全性，秘密信息的嵌入量以及图像的解密和恢复质量。一个好的加密图像的可逆信息隐藏的框架要有较高的加密安全性，较大的秘密信息嵌入量和较好的图像解密和恢复质量。如何提高这四个指标的性能是现在研究人员的主要研究方向。此外，除了图像，我们还可以考虑将秘密信息嵌入到音频，视频等其他载体中，提高信息隐藏在多媒体领域的应用范围。相信未来加密图像的可逆信息隐藏会为人们的生产生活提供更多的帮助。

## 参考文献

- [1] C. Qin, P. Ji, X. P. Zhang, J. Dong, and J. W. Wang. Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy[J]. Signal Processing, 2017, (138): 280–293.
- [2] C. Qin, H. L. Wang, X. P. Zhang, and X. M. Sun. Self-embedding fragile watermarking based on reference-data interleaving and adaptive selection of embedding mode[J]. Information Sciences, 2016, (373): 233–250.
- [3] C. Qin, X. Q. Chen, D. P. Ye, and J. W. Wang, and X. M. Sun. A novel image hashing scheme with perceptual robustness using block truncation coding[J]. Information Sciences, 2016, (361-362): 84–99.
- [4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber. Lossless generalized-LSB data embedding[J]. IEEE Transactions on Image Processing, 2005, 14(2): 253–266.
- [5] C. Qin, C. C. Chang, and T. J. Hsu. Reversible data hiding scheme based on exploiting modification direction with two steganographic images[J]. Multimedia Tools and Applications, 2015, 74(15): 5861–5872.
- [6] Y. Q. Shi, X. L. Li, X. P. Zhang, H. T. Wu, and B. Ma. Reversible data hiding: Advances in the past two decades[J]. IEEE Access, 2016, (4): 3210–3237.
- [7] J. Tian. Reversible data embedding using a difference expansion[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890–896.
- [8] D. M. Thodi and J. J. Rodriguez. Expansion embedding techniques for reversible watermarking[J]. IEEE Transactions on Image Processing, 2007, 16(3): 721–730.
- [9] B. Ou, X. L. Li, Y. Zhao, R. R. Ni, and Y. Q. Shi. Pairwise prediction-error expansion for efficient reversible data hiding[J]. IEEE Transactions on Image Processing, 2013, 22(12): 5010–5021.
- [10] Z. C. Ni, Y. Q. Shi, N. Ansari, and W. Su. Reversible data hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology. 2006, 16(3): 354–362.
- [11] X. L. Li, B. Li, B. Yang, and T. Y. Zeng. General framework to histogram-shifting-based reversible data hiding[J]. IEEE Transactions on Image Processing, 2013, 22(6): 2181–2191.
- [12] C. Qin, C. C. Chang, Y. H. Huang, and L. T. Liao. An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2013, 23(7): 1109–1118.

- [13] X. L. Li, W. M. Zhang, X. L. Gui, and B. Yang. Efficient reversible data hiding based on multiple histograms modification[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 2016–2027.
- [14] W. Puech, M. Chaumont, and O. Strauss. A Reversible Data Hiding Method for Encrypted Images[C]. Proceedings of SPIE 6819. 2008: 1–9.
- [15] X. P. Zhang. Reversible data hiding in encrypted image[J]. IEEE Signal Processing Letters, 2011, 18(4): 255–258.
- [16] W. Hong, T. S. Chen, and H. Y. Wu. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199–202.
- [17] X. Liao and C. W. Shu. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels[J]. Journal of Visual Communication and Image Representation, 2015, (28): 21–27.
- [18] C. Qin and X. P. Zhang. Effective reversible data hiding in encrypted image with privacy protection for image content[J]. Journal of Visual Communication and Image Representation, 2015, (31): 154–164.
- [19] Z. X. Qian, S. Dai, F. Jiang, and X. P. Zhang. Improved joint reversible data hiding in encrypted images[J]. Journal of Visual Communication and Image Representation, 2016, (40): 732–738.
- [20] Z. X. Qian, X. P. Zhang, Y. L. Ren, and G. R. Feng. Block cipher based separable reversible data hiding in encrypted images[J]. Multimedia Tools and Applications, 2016, 75(21): 13749–13763.
- [21] X. P. Zhang. Separable reversible data hiding in encrypted image[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 526–532.
- [22] Z. X. Qian, X. P. Zhang, and G. R. Feng. Reversible data hiding in encrypted images based on progressive recovery[J]. IEEE Signal Processing Letters, 2016, 23(11): 1672–1676.
- [23] P. Puteaux, D. Trinel, and W. Puech. High-capacity data hiding in encrypted images using MSB prediction[C]. Proceedings of the 2016 Sixth International Conference on Image Processing Theory, Tools and Applications, Oulu, Finland, 2016: 1–6.
- [24] P. Singh and B. Raman. Reversible data hiding for rightful ownership assertion of images in encrypted domain over cloud[J]. AEU - International Journal of Electronics and Communications, 2017, (76): 18–35.
- [25] X. P. Zhang, Z. X. Qian, G. R. Feng, and Y. L. Ren. Efficient reversible data hiding in encrypted images[J]. Journal of Visual Communication and Image Representation, 2014, 25(2): 322–328.
- [26] Z. X. Qian and X. P. Zhang. Reversible data hiding in encrypted images with distributed source encoding[J]. IEEE Transactions on Circuits and Systems for

- Video Technology, 2016, 26(4): 636–646.
- [27] X. T. Wu and W. Sun. High-capacity reversible data hiding in encrypted images by prediction error[J]. *Signal Processing*, 2014, (104): 387–400.
- [28] K. D. Ma, W. M. Zhang, X. F. Zhao, N. H. Yu, and F. H. Li. Reversible data hiding in encrypted images by reserving room before encryption[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(3): 553–562.
- [29] W. M. Zhang, K. D. Ma, and N. H. Yu. Reversibility improved data hiding in encrypted images[J]. *Signal Processing*, 2014, (94): 118–127.
- [30] D. W. Xu and R. D. Wang. Separable and error-free reversible data hiding in encrypted images[J]. *Signal Processing*, 2016, (123): 9–21.
- [31] F. J. Huang, J. W. Huang, and Y. Q. Shi. New framework for reversible data hiding in encrypted domain[J]. *IEEE Transactions on Information Forensics and Security*, 2016, 11(12): 2777–2789.
- [32] X. C. Cao, L. Du, X. X. Wei, D. Meng, and X. J. Guo. High capacity reversible data hiding in encrypted images by patch-level sparse representation[J]. *IEEE Transactions on Cybernetics*, 2016, 46(5): 1132–1143.
- [33] Y. C. Chen, C. W. Shiu, and G. Horng. Encrypted signal-based reversible data hiding with public key cryptosystem[J]. *Journal of Visual Communication and Image Representation*, 2014, 25(5): 1164–1170.
- [34] X. T. Wu, B. Chen, and J. Weng. Reversible data hiding for encrypted signals by homomorphic encryption and signal energy transfer[J]. *Journal of Visual Communication and Image Representation*, 2016, (41): 58–64.
- [35] D. Xiao, Y. P. Xiang, H. Y. Zheng, and Y. Wang. Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism[J]. *Journal of Visual Communication and Image Representation*, 2017, (45): 1–10.
- [36] 袁源, 和红杰, 陈帆. 减少相邻位平面间冗余度的加密图像可逆信息隐藏[J]. *中国图象图形学报*, 2019, 24(01): 13–22.
- [37] C. Qin, Z. H. He, X. Y. Luo, and J. Dong. Reversible data hiding in encrypted image with separable capability and high embedding capacity[J]. *Information Sciences*, 2018, (465): 285–304.
- [38] 鄢舒, 陈帆, 和红杰. 异或-置乱框架下邻域预测加密域可逆信息隐藏[J]. *计算机研究与发展*, 2018, 55(06): 1211–1221.
- [39] X. T. Wu, J. Weng, and W. Q. Yan. Adopting secret sharing for reversible data hiding in encrypted images[J]. *Signal Processing*, 2018, (143): 269–281.
- [40] S. Yi and Y. C. Zhou. Parametric reversible data hiding in encrypted images using adaptive bit-level data embedding and checkerboard based prediction[J]. *Signal Processing*, 2018, (150): 171–182.
- [41] Z. J. Tang, Q. F. Lu, H. Lao, C.Q. Yu, and X. Q. Zhang. Error-free reversible

- data hiding with high capacity in encrypted image[J]. *Optik*, 2018, (157): 750–760.
- [42] S. Yi, Y. C. Zhou, and Z. Y. Hua. Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion[J]. *Signal Processing: Image Communication*, 2018, (64): 78–88.
- [43] P. Puteaux and W. Puech. An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(7): 1670–1681.
- [44] 陈艳, 俞春强, 侯晓杰, 张显全, 唐振军, 何南. 基于曲面插值的加密图像可逆信息隐藏算法[J]. *应用科学学报*, 2018, 36(02): 220-236.
- [45] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli. Image quality assessment: from error visibility to structural similarity[J]. *IEEE Transactions on Image Processing*, 2004, 13(4): 600–612.
- [46] 刘宇, 杨百龙, 赵文强, 袁志华. 基于矩阵编码的大容量密文域可逆信息隐藏算法[J]. *计算机工程*, 2018, 44(10): 215–220.
- [47] 何志红, 秦川, 周青. 大容量的密文域图像可逆信息隐藏算法[J]. *应用科学学报*, 2018, 36(04): 611-627.
- [48] 邓敏. 基于加密图像的高容量可逆信息隐藏算法研究[D]. 西南交通大学, 2018.
- [49] C. C. Wang, Y. F. Chang, C. C. Chang, J. Jan, and C. Lin. A high capacity data hiding scheme for binary images based on block patterns[J]. *Journal of Systems and Software*. 2014, 93(2): 152–162.
- [50] S. Y. Shen and L. H. Huang. A data hiding scheme using pixel value differencing and improving exploiting modification directions[J]. *Computers and Security*. 2015, 48(1): 131–141.
- [51] W. C. Kuo, S. H. Kuo, C. C. Wang, and L. Wu. High capacity data hiding scheme based on multi-bit encoding function[J]. *Optik-International Journal for Light and Electron Optics*. 2016, 127(4): 1762–1769.
- [52] W. L. Xu, C. C. Chang, T. Chen, and L. Wang. An improved least-significant—bit substitution method using the modulo three strategy[J]. *Displays*. 2016. 42(1): 36–42.
- [53] Y. J. Liu, C. C. Chang, and T. Nguyen. High capacity turtle shell—based data hiding[J]. *Iet Image Processing*. 2016, 10(2): 130–137.
- [54] A. Malik, G. Sikka, and H. Verma. A high payload data hiding scheme based on modified AMBTC technique[J]. *Multimedia Tools and Applications*. 2016: 1–17.
- [55] Ranjani J. Jennifer. Data hiding using pseudo magic squares for embedding high payload in digital images[J]. *Multimedia Tools and Applications*. 2016: 1–15.
- [56] C. Wang, N. Wu, C. Tsai, and M. Hwang. A high quality steganographic method with pixel-value differencing and modulus function[J]. *Journal of Systems and*

- Software. 2008, 81(1): 150–158.
- [57] W. E. Hong, T. S. Chen, and C. Shiu. Reversible data hiding for high quality images using modification of prediction errors[J]. Journal of Systems and Software. 2009, 82(11): 1833–1842.
- [58] H. T. Wu, J. Dugelay, and Y. Q. Shi. Reversible image data hiding with contrast enhancement[J]. IEEE Signal Processing Letters. 2015, 22(1): 81–85.
- [59] K. Jung and K. Yoo. Steganographic method based on interpolation and LSB substitution of digital images[J]. Multimedia Tools and Applications. 2015, 74(6): 2143–2155.
- [60] T. Quach. Extracting hidden messages in steganographic image[J]. Digital Investigation. 2014, (11): S40–S45.
- [61] C. Yang, S. Hsu, and C. Kim. Improving stego image quality in image interpolation based data hiding[J]. Computer Standards and Interfaces. 2016, 50(1): 209–215.



## 在读期间公开发表的论文

### 一、论文

1. **Wei Zhang**, Ping Kong, Heng Yao, Yu-Chen Hu, Fang Cao. Real-Time Reversible Data Hiding in Encrypted Images Based on Hybrid Embedding Mechanism[J]. Journal of Real-Time Image Processing. DOI: <https://doi.org/10.1007/s11554-018-0811-y>.
2. Chuan Qin, **Wei Zhang**, Fang Cao, Xinpeng Zhang, Chin-Chen Chang. Separable Reversible Data Hiding in Encrypted Images via Adaptive Embedding Strategy with Block Selection[J]. Signal Processing, 2018, (153): 109-122.
3. **Wei Zhang**, Qing Zhou, Zhenjun Tang, Heng Yao, and Chuan Qin. A Reversible Data Hiding Scheme in Encrypted Image with LSB Compression and MSB Replacement[C]. The 2018 2nd International Conference on Security with Intelligent Computing and Big-data Services (SICBS). (录用).

## 致 谢

自己三年的研究生生活即将结束，十分荣幸可以在上海理工大学学习的时候遇到几个知心的朋友。他们让我的研究生生活变得更加丰富多彩，变得更加有意义。我要感谢我的导师秦川教授。在硕士就读期间给予了我很多的帮助，在研究的道路上对我精心教导，让我在这三年中学到了很多的知识，也收获了不少做研究的经验，这对我来说是一笔巨大的财富。感谢实验室的小伙伴们，大家一起学习，吃饭，运动，给原本枯燥的学习带来了很多的乐趣。

最后，再次感谢那些帮助过我的人，谢谢。