福建工程学院
Fujian University of Technology

毕业设计（论文）

题　　目：基于 EMD 的可逆信息隐藏方法

学　　生：杜言

指导老师：陈宇　副教授

院　　系：信息科学与工程学院

专　　业：软件工程

班　　级：软工 1502 班

学　　号：3151906228

2019 年 6 月

:

福建工程学院本科毕业设计（论文）作者承诺保证书

本人郑重承诺： 本篇毕业设计（论文）的内容真实、可靠。如果存在弄虚作假、抄袭的情况，本人愿承担全部责任。

学生签名:

年　　月　　日

福建工程学院本科毕业设计（论文）指导教师承诺保证书

本人郑重承诺：我已按有关规定对本篇毕业设计(论文)的选题与内容进行了指导和审核，且提交的毕业设计（论文）终稿与上传至“大学生论文管理系统”检测的电子文档相吻合，未发现弄虚作假、抄袭的现象，本人愿承担指导教师的相关责任。

指导教师签名:

年　　月　　日

基于 EMD 的可逆信息隐藏方法

摘 要

在社会信息化迅猛发展的今天，信息已经包含人生活的方方面面；在此大背景下，信息安全愈发重要。同时，计算机网络和多媒体技术的飞速发展于广泛应用在给人们生活带来巨大便利的同时，也带来了诸多安全问题；在此时代背景下，图像隐藏技术愈发成为了一个值得研究的方向。

图像隐藏技术是密码学很有前景的发展方向，不同于传统的信息加密技术，它具有没有载体，直接将第三方不可读的加密信息传输给接收方的特点；图像隐藏技术采用图像等媒体作为载体，转移观察者的注意力，从而达到信息传输的效果。图像隐藏技术主要是运用人眼对于颜色细微的变化不敏感的生理特性，在人眼不可判别的范围内，对图像进行处理，进而实现信息藏入的效果。

本次毕业设计的题目是《基于 EMD 的可逆信息隐藏方法》，主要的内容方向是受到张新鹏教授提出的 EMD 信息隐藏算法的启发，并对其方法进行了扩充，提出的一种改进算法。不同于 EMD 算法，本算法利用了参考矩阵在任意一个3×3 的矩阵数字分布的特点来藏入两个五进制数，从而获得两张隐写图。而后，通过两张隐写图的相互配合，提取出藏入的密字，并且能够还原出原始图。本算法采用多载体分享隐藏信息，并可将载体图片无损还原为原始图片的可逆信息隐藏。除此之外，本算法在峰值信噪比（PSNR）的值上较类似的可逆信息隐藏方法有一定提高。

关键字：信息安全，隐写术，图像信息隐藏，多载体，可逆性

Reversible information hiding method based on EMD

Abstract

Nowadays, with the rapid development of social information, information has already covered all aspects of human life; in this context, information security is becoming more and more important. At the same time, the rapid development of computer networks and multimedia technologies has been widely used to bring great convenience to people's lives. At the same time, it has brought various security problems. In this era, image hiding technology has become a research direction.

Image hiding technology is a promising development direction of cryptography. Different from traditional information encryption technology, there is no carrier, and the third-party unreadable ciphertext is directly transmitted to the receiver. Image hiding technology uses images and other media as carriers. Observe the direction of the observer to achieve the effect of information transmission. The image hiding technology mainly uses the physiological characteristics of the human eye that are insensitive to subtle changes in color, and processes the image within a range that is unrecognizable to the human eye, thereby realizing the effect of information hiding.

The title of this graduation project is "Reversible Information Hiding Method Based on EMD". The main content direction is inspired by the EMD information hiding algorithm proposed by Professor Zhang Xinpeng, and its method is extended, and an improved algorithm is proposed. Different from the EMD algorithm, the algorithm uses the characteristics of the reference matrix in any one of the matrix digital distribution to hide two hexadecimal numbers, thus obtaining two steganographic maps. Then, through the cooperation of the two pictures, the hidden secret characters are extracted, and the original picture can be restored. The algorithm uses multiple carriers to share hidden information, and can reduce the carrier image to the reversible information hiding of the original image. In addition, the algorithm has a certain improvement in the value of the peak signal-to-noise ratio (PSNR) compared to the similar reversible information hiding method.

Key words: information security, steganography, image information hiding, multi-carrier, reversibility

目　　录

第 1 章 绪论

1.1 研究背景

随着计算机网络的高速建设及多媒体技术的广泛应用，极大地方便了人们的日常生活，也极大地提高了人们的生活质量，人们开始越发离不开各种以多媒体形式涌来的信息。同时，伴随各种多媒体信息朝我们而来的还有各种信息安全隐患，其中最常见也最有代表性的就是陌生邮箱发来的邮件中的图片往往带有病毒，而往往因为当前大多数的反恶意软件解决方案在抵抗该方面基本都束手无策，即使提供了保护也微不足道，可以说任何能够秘密携带有效载荷的载体都可能带来潜在的威胁。近年以来，随着社会信息化的高速发展，以及物联网海量设备的出现、大数据时代的到来，无论是应对现在还是面向未来，网络信息安全愈发成为不可忽视的一部分。随着人们对于网络信息安全愈发关注，网络信息安全成为当前热门的研究课题[1][2]。

信息加密技术和信息隐藏技术是信息安全领域的两个重要组成部分。信息加密技术仅仅将密文通过一定方式加密，以第三方不可见的方式传送给接收方，从而起到保护密文内容的作用。其缺点显而易见：虽然密文的内容不可见，但密文存在的载体本身是可以被发现的；一旦遭受到恶意的攻击，密文信息将传递失败。而信息隐藏技术利用数字载体的冗余性以及人类视觉系统对信息变化的不敏感性，将编码或加密后的秘密信息嵌入到普通多媒体数据中，实现传递密文的目的。此举不仅可以起到对于密文内容的隐藏，同时也可以瞒天过海般地将密文存在的本身藏于载体之中，让观察者无从得知密文的存在[1]。

隐写术是信息隐藏技术的一个重要分支，同时，数字图像仍是当今世界信息传递的主要媒介之一，所以，图像信息隐藏成为信息隐藏技术一个很合适的入手与实现方向。

1.2 当前多媒体加密研究现状

当前图像和视频加密主要分为两种：第一种是利用传统的加密算法，比如 RSA, IDEA 等算法用于加密图像或视频，但是有很重要的缺点，比如计算复杂度大，尤其对视频的码流有影响。另外如果在传输过程中不小心收到噪声干扰，则无法解密。而对于图像来说，如果解密的图像能辨认，用于评价图像视觉质量的 PSNR 值较好，我们还是能接受的，这点和传统的密码有一定的区别，所以基本不用此方法。

第二是利用各种伪随机序列，比如由各种混沌系统生成的序列，对图像的每个位平面进行异或、平移等等操作，以实现加密，优点是计算复杂度较低，安全性也还可以。不过需要选择好的伪随机序列生成器和好的加密操作才行。而对视频的加密比较复杂，主要是视频的数据量大，还根据用途不同，所选择的加密方法也不一样，因此加密方法的选择要在安全性、计算复杂度、码流控制等方面进行折中，不同场合选择不同的方法。比如利用

选择性加密，或者部分加密等。

1.3 本研究目的与意义

信息安全本身就是攻防两端互相抗衡、相互竞争、共同进步的领域。无论是在研究攻击还是研究防御都可以给本领域带来进步，本次研究只为找出更好的图像可逆隐写算法。因为绝大多数隐写算法在密字提取后，载体图片都无法无损地恢复为原图片；而在某些领域，如医疗行业和在线内容分发系统等，图像隐写的可逆性是极有必要的，因为这些领域处理要传递与个人隐私、商业机密相关的重要信息外，对于原图片仍有用途，所以具有可逆性的图像隐写技术的研究很有必要。

1.4 论文结构

第 1 章：介绍本文的研究背景，本文的研究目的与可逆性图像隐写的研究意义。

第 2 章：对于图像隐写经典算法的介绍与分析，主要有 LSB 算法和本算法借鉴的 EMD 算法

第 3 章：介绍本文将提出的基于 EMD 的可逆信息隐藏方法，并阐述其算法思路；另外，因为算法比较抽象，所以将通过一组实例模拟算法实现过程，让算法更容易理解。最后，将会根据实验结果阐述算法的优势。

第 4 章：对论文的总结并对图像隐写技术及其相关领域的展望。

第 2 章 信息隐写算法介绍

图像隐写算法分为两个步骤：藏入和提取。藏入就是将信息藏入载体图片，而提取是将信息从载体图片中提取出。

2.1 LSB 算法介绍与分析

在过去的文献中，有大量的信息隐藏技术被提出[3-7]。其中，在图像隐写技术中非常常见的算法有 LSB(least-significant-bit)[8,9]，因为其经典并且原理简单易于理解，所以经常在文章被引用，并被扩展或改进。LSB 主要运用人眼对于颜色细微的变化不敏感的生理特性，在人眼不可判别的范围内，对图像进行处理，从而实现信息藏入的效果。而现在，由于人对于图片的清晰度、分辨率、色域的要求越来越高，所以现代图片的存储空间越来越大，冗余度也便越来越高。而 LSB 算法仅仅是对图像像素的最低的 L 位（一般 L 为 1，即为最低有效位；同时，L 不会超过 3）进行修改，并藏入二进制密文，如果秘密信息与最低比特位相同，则不改动；如果秘密信息与最低比特位不同，则使用秘密信息值代替最低比特位。而因为像素的变化值相较于像素整体的强度范围变化极小，所以人眼并不会发觉异常，从而起到藏入信息的作用。同时因为一个像素至少可以藏入一个密字，所以综上，LSB 算法具有容量大、嵌入速度快、对载体图像质量影响小的特点。

同时正是由于 LSB 算法实现简单，所以在检测攻击中也很容易被破解，比如提取出隐写图片像素的最低有效位；从而导致密文信息将传递失败，甚至是信息泄露给第三方。于是很多对 LSB 的改进和扩展算法被提出，无论是有学者提出的使用最佳中间有效位替换(optimal moderately-significant-bit replacement)的方法改进[8]，其解决在传输过程中一些软件为节省空间，提高传输速率或加快图像处理速度，会丢弃最低有效位使图像变为每像素 7 位而不是 8 位，从而使隐写失效的问题。还是中通过将传统 LSB 方法和 OPAP(optimal pixel adjustment process)相结合[9]，从而用较低的额外计算复杂度获得增强的图像质量，都展现出更好的性能。

2.2 EMD 算法介绍与分析

接下来介绍 EMD(exploiting modification direction)算法[10]。EMD 算法正如其名，它充分利用了矩阵由维度产生的方向。在该方法中，使用不同方向的修改来表示不同的秘密数据，从而产生更高的嵌入效率。具体来说，该算法的主要思想是：每 n 个像素将作为一个(2n+1)进制的密字的载体，用于信息隐藏；同时，每个像素点的变化最多只是加一减一。换句话说：对于这 n 个像素我们有(2n+1)种可能的变化情况，这(2n+1)种情况可以映射表示为(2n+1)个可能为密字的数字。而这正好对应的公式

$$f(g_1,g_2,...,g_n)=[\sum_{i=1}^{n}(g_i \bullet i)]\bmod(2n+1) \qquad \text{公式 (1)}$$

所产生的的 n 维矩阵（在这里以及下面将公式产生的矩阵成为魔法矩阵）的性质。在这里不妨以 n=2 为例，其简单有代表性。在二维的魔法矩阵中任意一个3×3 的矩阵中均可以在“+形区域”（如下图 2-1 所示）中均可找到“0 1 2 3 4”这 5 个数字。由于 EMD 算法所需隐藏的密字均为五进制数，也就与“+形区域”中的数字 “0 1 2 3 4”相对应。算法的主要步骤是：以公式

$$f(g_1,g_2)=(g_1+g_2 \bullet 2)\%5 \qquad \text{公式(2)}$$

构造出一个 256×256 的魔法矩阵，由于作为载体的图像是灰度范围为 0-255 的图片，所以在载体图片中，每一个像素对所对应的两个灰度值可看成坐标均可以映射到魔法矩阵的一个点上，以该点作为中心点，在“+形区域”中寻找所需藏入的五进制密字对应的值，并以该值所在的坐标作为隐写图像素对的灰度值，如此，藏入过程得以实现。而提取过程只需根据传来的隐写图，将像素对所对应的两个灰度值所形成的坐标映射到魔法矩阵中，找到其在魔法矩阵中对应的值作为密字，将当前找到的密字放入密字序列即可。不同于传统LSB 的修改最低有效位较为固定的特点，EMD 利用多种方向对像素进行修改，使得对于像素的修改更加没有规律可循。同时，LSB 算法检测方只需对载体图片进行处理就可得到密字信息，而 EMD 还需要公式构造的魔法矩阵，这样即使检测方对于载体图片进行处理，如果不知道构造公式，也无法获得密字。

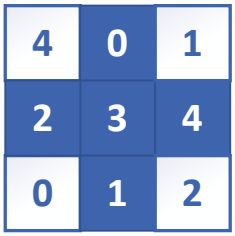


图 2-1 +形区域

由于原 EMD 算法不具有可逆性，接下来将介绍本文提出的方法，在 EMD 算法的基础上进行一定的扩展，使得其具有可逆性。

第 3 章 基于 EMD 的可逆信息隐藏方法

3.1 算法介绍

本算法借鉴了 EMD 算法，并对其进行了一定的扩展，使用多载体的思想对信息进行隐藏，使得信息更加安全的同时，也使其拥有了载体图片恢复成原始图片的可逆的性质。具体来说：设魔法矩阵的维度为 2。另外，使用 EMD 中的魔法矩阵的“+形区域”的性质，还发现并使用了在“×形区域”（如下图 3-1 所示）中均可找到“0 1 2 3 4”这 5 个数字的性质。依次在“+形区域”和“×形区域”中查找密字，从而实现藏入过程

图 3-1 x 形区域

3.2 算法思想

藏入过程：

Step1:根据公式 （2）构造一个大小为256×256的魔法矩阵。

Step2:将载体图片从左上方开始，依次以像素对的形式隐藏密字，将像素对的灰度值作为坐标映射到魔法矩阵中，步骤如下：

设 i 为藏入操作的步骤的次序。在第 i 步，先将原图的第 i 个像素对的像素值作为坐标映射到魔法矩阵中，得到在魔法矩阵中对应的值。并在以在魔法矩阵中映射的点为中心的3×3矩阵中，以映射点为基准的“＋形区域”（如上图所示）中寻找需要藏入的第2×i个密字，并以该点的坐标值作为第一张隐写图像素对的灰度值。同理，在以映射点为基准的“×形区域”（如上图 3-1 所示）中寻找需要藏入的第2×i+1个密字，并以该点的坐标值作为第二张隐写图像素对的灰度值。

分别将第一张图的第 i 个像素对和第二张图的第 i 的像素对映射在魔法矩阵中的点分别定义为起点和终点，在这里我们设两点形成一个由起点指向终点的矢量。这便形成了矢量长度平方值为 0、1、2、5 这 4 种共 25 个矢量（分别如下图 3-2、3-3、3-4、3-5 所示）。

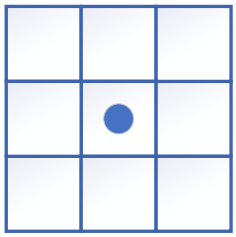


图 3-2 长度平方值 D=0（共 1 种情况）

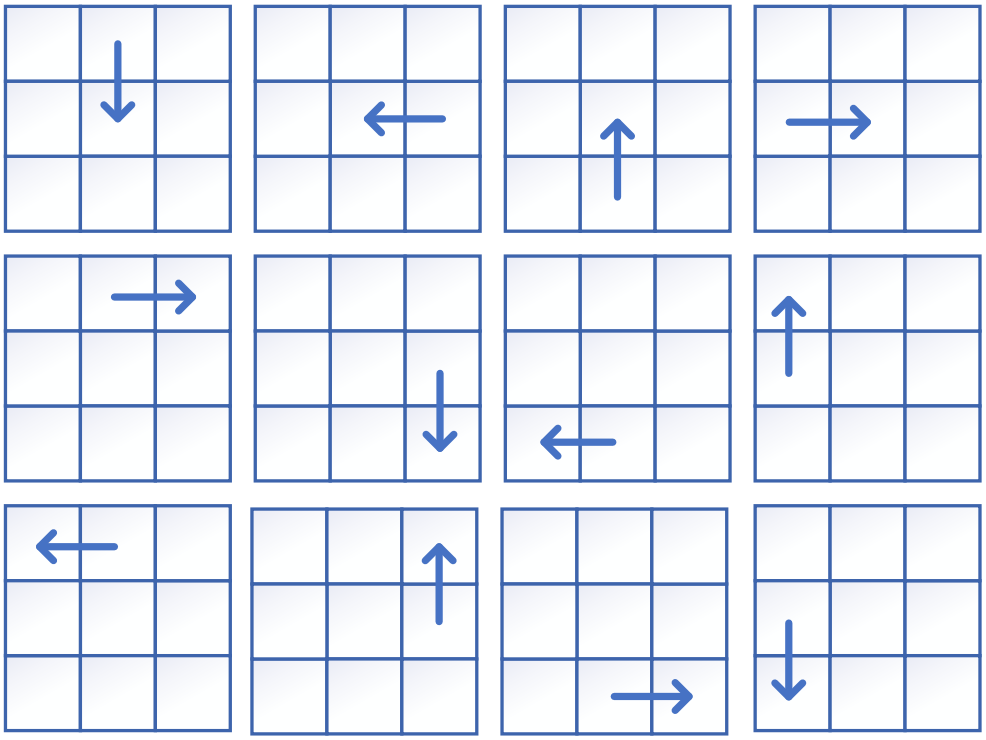


图 3-3 长度平方值 D=1（共 12 种情况）

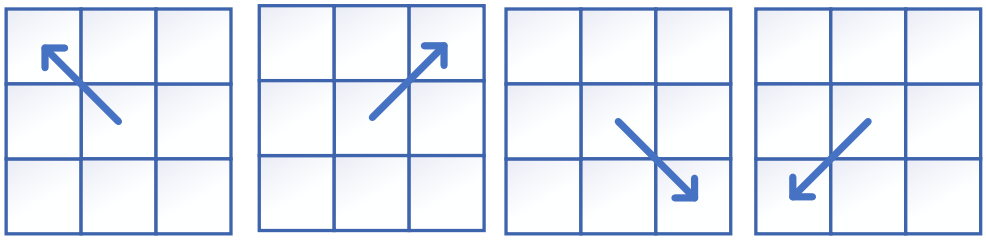
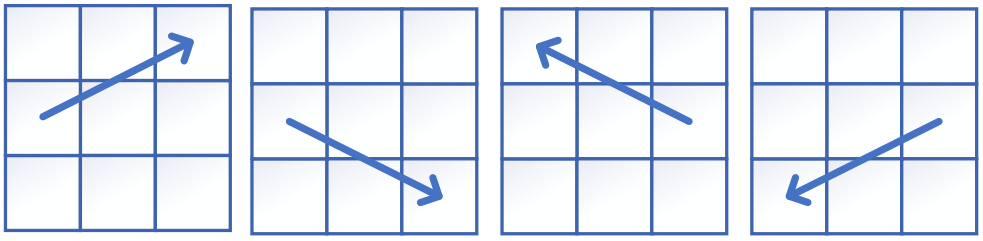


图 3-4 长度平方值 D=2（共 4 种情况）



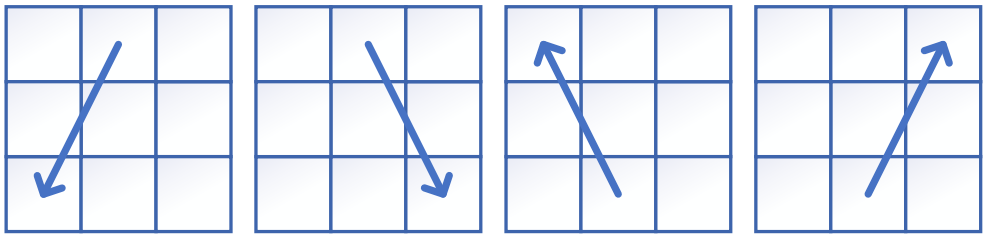


图 3-5 长度平方值 D=5（共 8 种情况）

因为考虑到后面的提取过程中，需要根据两点确定3×3矩阵的中心点的位置。但如下图 3-6 所示，其中每一组长度为 1 且同方向的矢量，在不知道中心点将会产生歧义冲突，无法确定其中心点的位置。所以需要进行消除歧义操作。接下来对通过自定义的方式对产生歧义的 3 中矢量进行歧义消除，为了操作方便，不妨假定终点为中心点的矢量无需进行转换，而其他两种需要进行转化。同时，假定关于中点顺时针的矢量起点沿着矢量的反方向移动 1（如下图 3-7 所示），关于中点逆时针的矢量起点移动到终点相对于中点对称的位置（如下图 3-8 所示）。

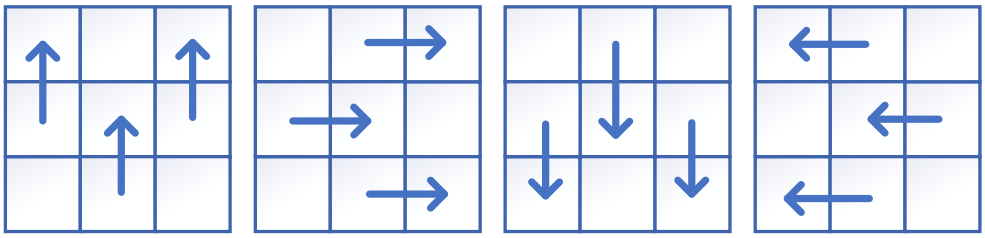


图 3-6 无法判断中心点的冲突矩阵

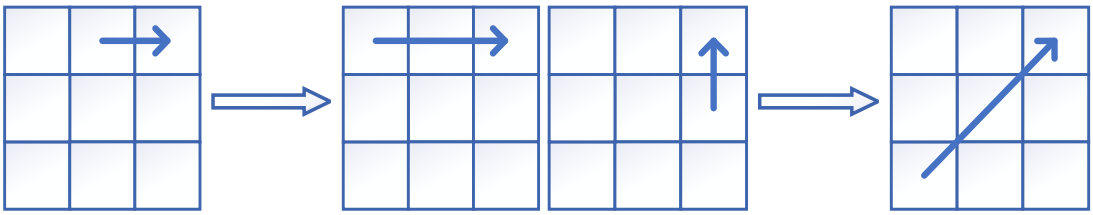


图 3-7 长度为 1 且顺时针方向转换方式　　图 3-8 长度为 1 且逆时针方向转换方式

于是，便得到这样的判定与消除歧义的规则：

1. 若矢量不经过中心点，矢量长度的平方值为 1，且相对于中心点顺时针指向，则要将起点沿着矢量的反方向移动 1。
2. 若矢量不经过中心点，矢量长度的平方值为 1，且相对于中心点逆时针指向，则要将起点移动到终点相对于中点对称的位置。
3. 若为其他情况，则不作变化。

在经过消除歧义后，形成的矢量共有 25 种情况，可以按照矢量长度平方值（不妨设为 D）分为 6 类（如下图 3-9 所示）

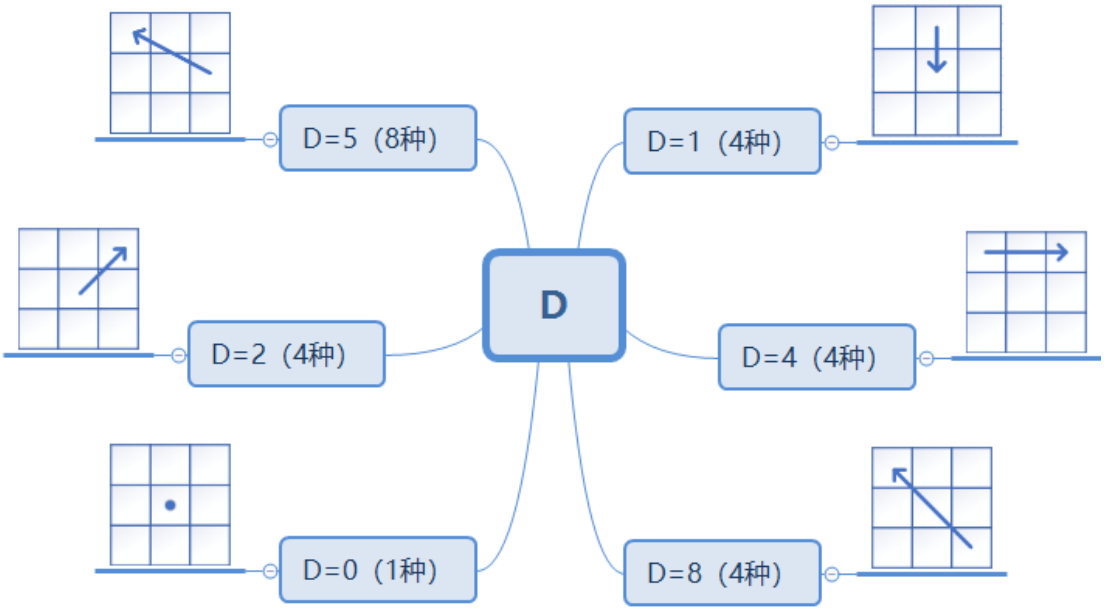


图 3-9 歧义消除后 6 种情况思维导图

具体 25 种情况，按分类显示如下图 3-10、图 3-11、图 3-12、图 3-13、图 3-14、图 3-15 所示：

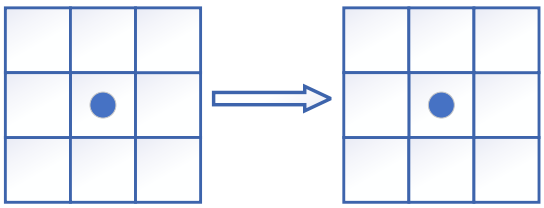


图 3-10 D=0（1 种）

矢量长度平方值为 0，所以未产生歧义，于是起始点无需作任何变化。

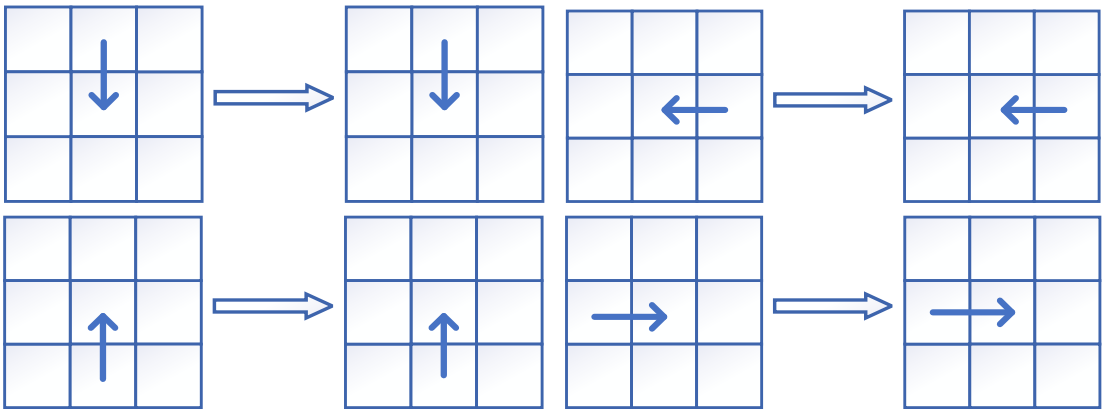


图 3-11 D=1（4 种）

矢量长度平方值为 1，其经过中心点；所以未产生歧义，于是起始点无需作任何变化。

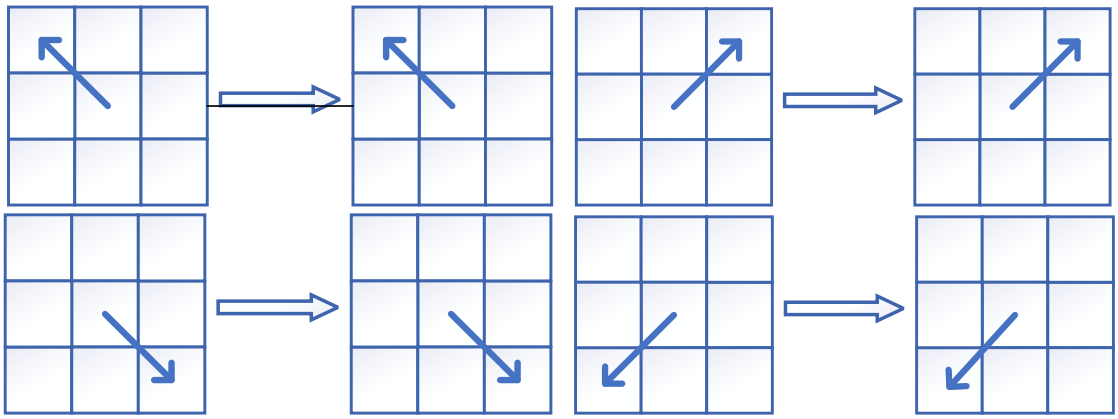


图 3-12　D=2（4 种）

矢量长度平方值为 2，所以未产生歧义，于是起始点无需作任何变化。

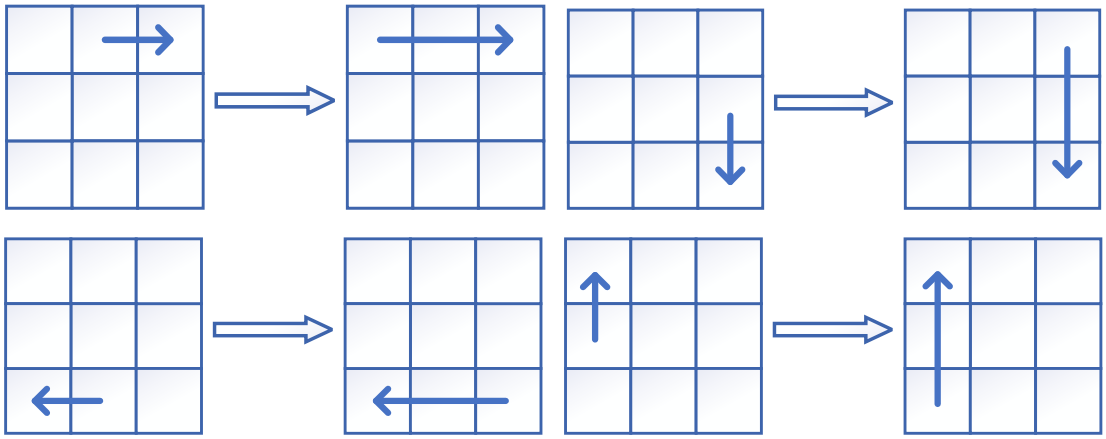
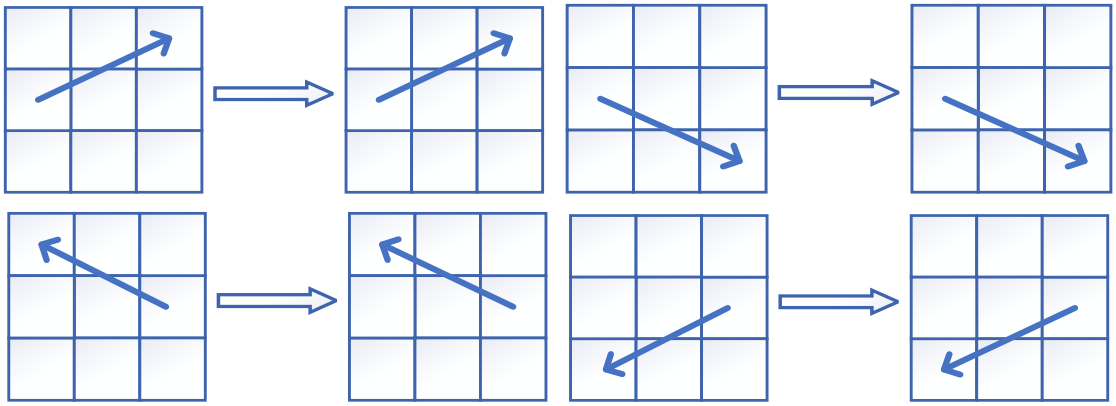


图 3-13 D=4（4 种）

矢量长度平方值为 1，未经过中心点，且相对中心点呈顺时针方向，所以产生歧义，需要将起始点变为终点关于未变化中点相对称的位置。



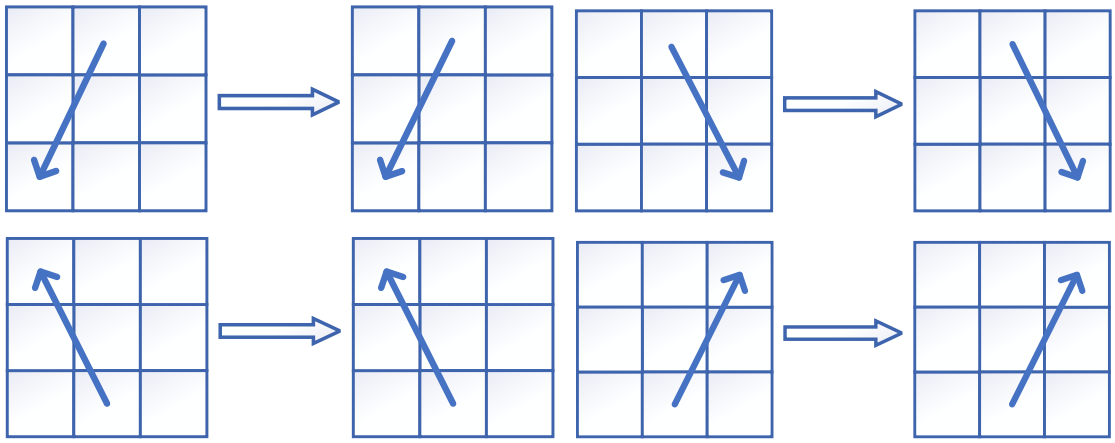


图 3-14 D=5（8 种）

矢量长度平方值为 5，所以未产生歧义，于是起始点无需作任何变化。

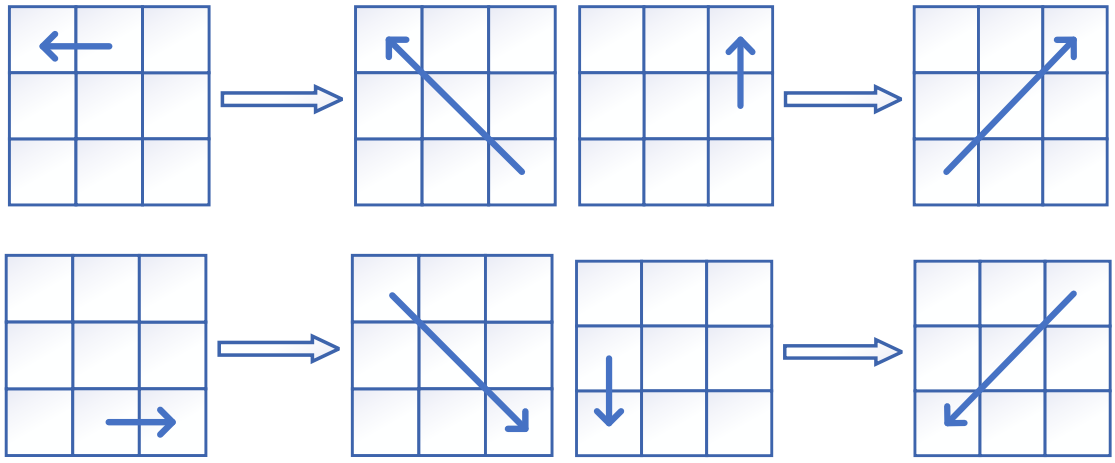


图 3-15 D=9（4 种）

矢量长度平方值为 1，未经过中心点，且相对中心点呈逆时针方向，所以产生歧义，需要将起始点变为终点关于中心点对称的位置。

再完成第 i 步后，随即进行第i+1步，以下过程依次类推。

Step3:在完成循环后，隐写图 1 和隐写图 2 完成。

提取过程：

Step1:将得到得隐写图 1 和隐写图 2 从左上方开始，从左到右，从上到下轮流取出一个像素对，并将像素对灰度值对应的坐标映射到魔法矩阵中。将隐写图 1 和隐写图 2 的像素对在魔法矩阵中对应的点分别称为起点和终点。根据矢量与中心点的数学性质对前面的歧义消除逆向处理，得到3×3矩阵的中点坐标和两个像素对中隐藏的两个密字。将中点的坐标作为原图的像素值，同时将五进制的密字拼接。

Step2:获得原图片，并将获得的五进制串，通过一定方法转化为二进制密字。

3.3 算法实现详解

根据 EMD 方法构造的256×256的魔法矩阵（如下图 3-16 所示）。不妨设载体图片为[6 1 7 8 6 7 6 4 6 2]，要藏入的五进制密字为[3 0 1 0 4 3 3 1 4 0]，接下来模拟本算法：

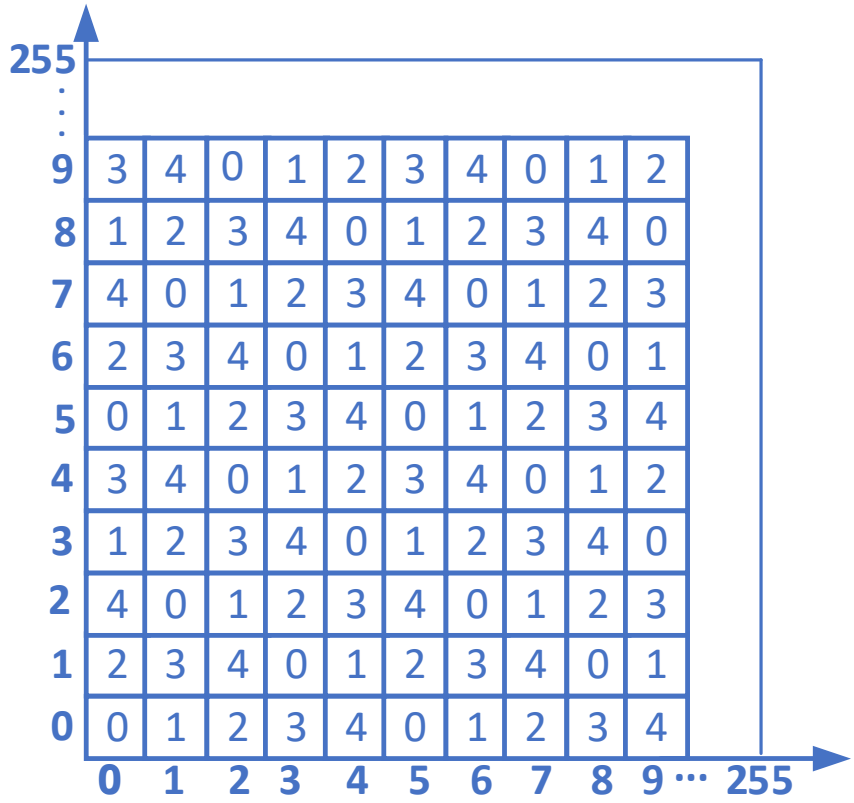


图 3-16 魔法矩阵示意图

藏入过程：

第一次藏入：当前像素对为(6, 1)，在魔法矩阵中对应的数字为 3 ，在3×3矩阵中第一个密字 3 在“+形区域”所对应的坐标为(6,1)，第二个密字 0 在“×形区域”所对应的坐标为(5, 0)，由于矢量长度平方值为 2，所以不需要进行歧义消除，于是直接将这两个坐标作为隐写图该像素对的灰度值。

第二次藏入：当前像素对为(7, 8)，在魔法矩阵中对应的数字为 3，在3×3矩阵中第一个密字 1 在“+形区域”所对应的坐标为(7, 7)，第二个密字 0 在“×形区域”所对应的坐标为(6, 7)，由于矢量长度平方值为 1，且相对于中心点为顺时针方向，所以需要进行歧义消除，需要将起点坐标修改为(8, 7)，同时将这两个坐标作为隐写图该像素对的灰度值。

第三次藏入：当前像素对为(6, 7)，在魔法矩阵中对应的数字为 0，在3×3矩阵中第一个密字 4 在“+形区域”所对应的坐标为(5, 7)，第二个密字 3 在“×形区域”所对应的坐标为(7, 8)，由于矢量长度平方值为 5，所以不需要进行歧义消除，于是直接将这两个坐标作为隐写图该像素对的灰度值。

第四次藏入:当前像素对为(6, 4),在魔法矩阵中对应的数字为 4 ，在3×3矩阵中第一个密字 3 在“+形区域”所对应的坐标为(5, 4),第二个密字 1 在“×形区域”所对应的坐标为(5, 3)，由于矢量长度平方值为 1，且相对于中心点为逆时针方向，所以需要进行歧义消除，需要将起点坐标修改为(7, 5)，同时将这两个坐标作为隐写图该像素对的灰度值。

第五次藏入:当前像素对为(6, 2),在魔法矩阵中对应的数字为 0，在3×3矩阵中第一个密字 4 在“+形区域”所对应的坐标为(5, 2),第二个密字 0 在“×形区域”所对应的坐标为(6, 2)，由于矢量长度平方值为 1，但矢量经过中心点，所以不需要进行歧义消除，此时直接将两个坐标作为隐写图该像素对的灰度值。

于是得到的两张隐写图的对应部分为:[6 1 8 7 5 7 7 5 5 2]和[5 0 6 7 7 8 5 3 6 2]。

提取过程：

第一次提取：起点坐标为(6, 1)，终点坐标为(5, 0)，矢量长度平方值为 2，此时起点坐标仍是原来起点的坐标，依据矢量与中点的几何性质得到中点坐标为(6, 1)。以中点的坐标作为原图片中像素对的灰度值，同时分别将获得的起点和终点在魔法矩阵中对应的值 3 和 0 作为密字加入密字序列,此时密字序列为[3 0]。

第二次提取：起点坐标为(8, 7)，终点坐标为(6, 7)，矢量长度平方值为 4，此时起点坐标不是原来起点的坐标，需要进行还原，原起点坐标为(7, 7),依据矢量与中点的几何性质得到中点坐标为(7, 8)。以中点的坐标作为原图片中像素对的灰度值，同时分别将获得的起点和终点在魔法矩阵中对应的值作为密字 1 和 0 加入密字序列,此时密字序列为[3 0 1 0]。

第三次提取：起点坐标为(5, 7)，终点坐标为(7, 8)，矢量长度平方值为 5，此时起点坐标仍是原来起点的坐标，依据矢量与中点的几何性质得到中点坐标为(6, 7)。以中点的坐标作为原图片中像素对的灰度值，同时分别将获得的起点和终点在魔法矩阵中对应的值作为密字加入密字 4 和 3 序列,此时密字序列为[3 0 1 0 4 3]。

第四次提取：起点坐标为(7, 5)，终点坐标为(5, 3)，矢量长度平方值为 8，此时起点坐标不是原来起点的坐标，需要进行还原，原起点坐标为(5, 4),依据矢量与中点的几何性质得到中点坐标为(6, 4)。以中点的坐标作为原图片中像素对的灰度值，同时分别将获得的起点和终点在魔法矩阵中对应的值作为密字 3 和 1 加入密字序列,此时密字序列为[3 0 1 0 4 3 3 1]。

第五次提取：起点坐标为(5, 2)，终点坐标为(6, 2)，矢量长度平方值为 1，但矢量经过中心点，此时起点坐标仍是原来起点的坐标，依据矢量与中点的几何性质得到中点坐标为(6, 2)。以中点的坐标作为原图片中像素对的灰度值，同时分别将获得的起点和终点在魔法矩阵中对应的值 4 和 0 作为密字加入密字序列,此时密字序列为[3 0 1 0 0 4 3 1 4 0]。

于是得到原图片[6 1 7 8 6 7 6 4 6 2],密字[3 0 1 0 4 3 3 1 4 0]。

藏入查找与歧义消除示图如下图 3-17、图 3-18、图 3-19、图 3-20、图 3-21 所示：

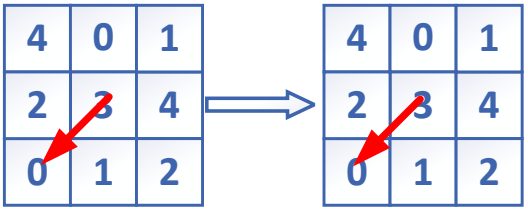


图 3-17 第一次藏入与消歧

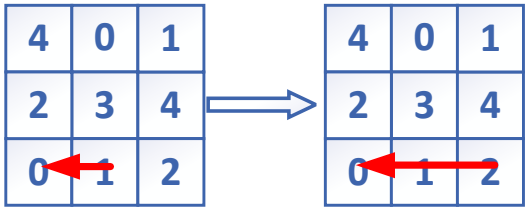


图 3-18 第二次藏入与消歧

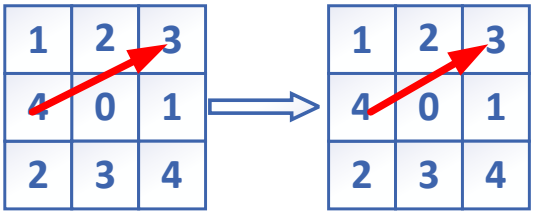


图 3-19 第三次藏入与消歧

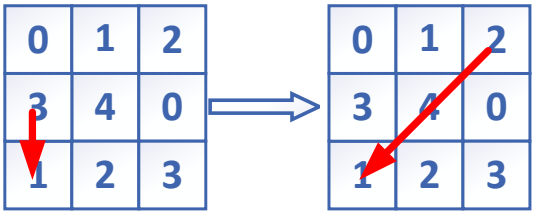


图 3-20 第四次藏入与消歧

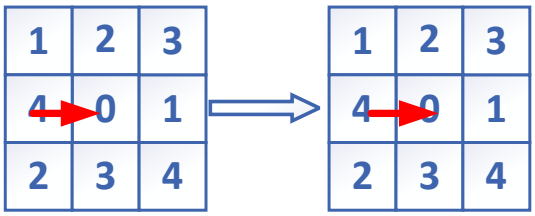


图 3-21 第五次藏入与消歧

在实现模拟完成之后，以下三张图分别为 Lena 原图、第一张隐写图、和第二张隐写图（如下图 3-22、图 3-23、图 3-24 所示），可以发现这三张图以人眼观察很难找出不同。

图 3-22 Lena 原图

图 3-23 第一张隐写图

图 3-24 第二张隐写图

3.4 算法优势

图像的视觉质量是评价秘密数据传输方法的一个非常重要的衡量指标，也就是说，具有更高视觉质量的隐秘图像更容易欺骗无意识的观察者。由于图像的视觉质量对人眼的观察是主观的，并不能完全代表其视觉质量，所以我们使用峰值信噪比（PSNR）作为评估隐秘图像视觉质量的度量。PSNR（Peak Signal to Noise Ratio）是一种广泛使用且易于实现的、

用于评估两个图像之间的相似性的方法。PSNR 的定义如下：

$$PSNR = 10 \times \lg(\frac{MAX_I^2}{MSE}) \quad \text{公式(3)}$$

其中 MAX 一般为图像的灰度值，在这里为 255；另外 MSE(Mean Squarer Error)为均方误差，其定义为：

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j)-K(i,j)\right\|^2 \quad \text{公式(4)}$$

PSNR 常常被用来评价隐写图与原图片之间的差别，一般 PSNR 值较大，则说明隐写图与原图越相似；同理，PSNR 值越小，说明明隐写图与原图差距越明显。而通常，当 PSNR 值大于 30dB 时，人眼不能区分隐秘图像和原始图像之间的失真。

经过实验进行对算法进行实现，并对 PSNR 进行计算，可得：隐写图 1 的 PSNR 的平均值在 50 左右，隐写图 2 的 PSNR 的平均值在 49 左右。两者 PSNR 的平均值也在 50 左右，也就是说，隐秘图像有更多机会欺骗无意识的观察者以达到秘密数据传递的目的。同时较原生的 EMD 算法，虽然 PSNR 值要稍微小一些，但实现了可逆的功能，同时 PSNR 值仍远远超过人眼难以区分是否失真的 PSNR 值 30dB，也算是值得。

如果说图像视觉质量是影响图像是否可以通过检测的关键因素，值得算法设计者不断改进与优化外；那么数据隐藏能力是算法在同一张图像中可以隐藏信息量大小的能力，这也是算法设计者提高算法性能的主要目标。往往一种算法的数据隐藏能力越强，在同一张图片种可以藏入越多的信息；同时，藏入越多的信息往往会导致图像的视觉质量下降，而这两者的矛盾，也是研究者需要折衷考虑。

本算法通过 MatLab 模拟环境计算出多张标准测试图像的 PSNR 和数据隐藏能力的值，与原生 EMD 算法比较如下表 3-1 所示：

表 3-1 本算法与 EMD 性能比较表

方法 / 图片	EMD		本方法		
	PSNR	Capacity	Stego1's PSNR	Stego2's PSNR	Capacity
Baboon	52.11	1	50.65	49.11	1.16
Barbara	52.11	1	50.66	49.10	1.16
Lena	52.12	1	50.65	49.09	1.16
Pepper	52.12	1	50.64	49.10	1.16
Average	52.11	1	50.65	49.10	1.16

为了实现原图像的可逆性，较原生 EMD 算法，PSNR 值下降了 4%，也在可接受的范围，同时数据隐藏能力有不小的增幅。同时，本算法使用五进制的密字进行隐写，相较大多数使用二进制密字进行隐写的算法，在数据隐藏能力方面要好不少。

第 4 章 总结与展望

4.1 总结

本算法对 EMD 算法进行改进，除了 EMD 算法用到的在魔法矩阵的3×3 矩形的“+形区域”内进行密字查找外，还在添加了在“×形区域”内进行查找，并进行歧义消除，另外还采用多载体技术，从而实现原始图片的可逆恢复。

其中，采用多载体藏入的方法，利用分享的技术，一次采用两张图片进行隐藏，增大了可藏入的数据量；同时，在两张图片中轮流进行隐藏，因为无法根据其中任意一张图片获取全部信息或一整段的信息；这在同时减小了数据被第三方破译的风险。

另外，虽然图像隐写算法更普遍关注的是密字的藏入和提取，但原图的获取更多的是依据实际需求来，在某些方面，比如前面说到的医学领域和在线内容分发系统仍有必要的。或者说，可逆的性质至少给算法使用者多了一种选择。

4.2 相关技术的展望

如今，图像信息隐藏技术已经在业界得到了广泛地应用。比如，在当前国内不少企业中已经有通过该技术对机密图片进行处理，防止员工外泄机密。而在医学界，对于病人的医学影像的传输往往不会直接附上病人的个人信息，而是将这些隐私内容通过信息隐藏技术藏在传输的医学隐藏影像中。

而放眼未来，尤其是在当今深度学习大红大紫、并被广泛应用的今天，图像信息隐藏技术甚至是范围更广的信息隐藏技术，都将在这场由深度学习引发的技术革命中焕发出新的生机。以 Google Research 为例，其在 NIPS 2017 上发表了一篇论文[12]，主要的内容就是将深度学习应用到图像隐写中，实现在一张图像中隐写另一张图像。这种在图像中藏入图片的方法虽然看起来并没有纯文字描述来的直接，甚至可以说：同样空间大小的文字和图片，文字的信息熵要比图片高不少，而图像在直观性、直接性、难以篡改等方面仍较图片有优势，所以这种技术仍有较大的价值。同时，面对视觉攻击(Visual attack)或统计分析攻击(Statistical attack)[13]等检测手段，隐写图像有一定概率会被拦截，而导致传送失败。面对视觉攻击这总更多依靠人眼或一些固定的处理手段，通过提高 PSNR 值或优化算法尚且可以解决，而面对相对机器执行也更客观的统计分析攻击，将其交给机器学习算法解决，是一个良好的思路。

参考文献

[1]殷娇娇. 多载体图像隐写研究[D]. 湖南大学, 2018.

[2] Jordan S, Merrill W, Shwadhin S. Personality, attitudes, and intentions: Predicting initialadoption of information security behavior. Computers and Security, 2015, 49:177–191

[3]A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark, Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86–90.

[4] W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.

[5] T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.

[6] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.

[7] K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD- and VQ-based image hiding scheme, Pattern Recognition Lett. 22 (9) (2001) 1051–1058.

[8]Chan C. K. and Cheng L. M., "Hiding data in images by simple LSB substitution," Pattern Recognition, Vol. 37, No. 3, 2004.

[9] Wang R. Z., Lin C. F. and Lin J. C., “Hiding Data in Images by Optimal Moderately significant-bit replacement,” IEE Electronics Letters, Vol. 36, No. 25, 2000.

[10]Zhang X, Wang S: Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters 2006, 10(11):781-783. 10.1109/LCOMM.2006.060863

[11] Chang C. C., Kieu T. D. and Chou Y. C., “Reversible data hiding scheme using two steganographic images,” in Proceedings of IEEE Region 10 International Conference (TENCON), Taipei, Taiwan, 2007.

[12]Baluja, S. (2017): Hiding images in plain sight: Deep steganography. Advances in Neural Information Processing Systems, pp. 2066-2076.

[13]A. Westfeld, “F5: a steganographic algorithm,” in Proc. 4th Int. Workshop Information Hiding 2001, Lecture Notes in Computer Science, vol. 2137,

pp. 289-302.

致谢

时光荏苒，白驹过隙，转眼大学四年就过去了。从高中毕业到大学毕业，在这四年里，我从一个对于计算机知识甚少的学生，在学习和实践中逐渐成为了一名对于计算机科学领域有一定理解，并有志继续进行研究准毕业生。在这四年的成长中我想感谢在我这段路程中陪伴我的每一个人。

首先想要感谢的是每一位教过我的福建工程学院的老师们，是你们循循善诱，将我引进了计算机科学及软件工程的殿堂。其中，我还想特别感谢一下我的毕业论文指导老师陈宇老师，给我推荐了这样一个富有现实意义和研究价值的课题。另外，陈宇老师不厌其烦地给我指导和提出建议，甚至我在夜里 11 点打扰都能够及时的给我解惑，这使我对图像信息隐藏算法有了更深入的了解。

其次，想要感谢专业的同学以及我在大学时结识的志同道合的朋友们，是你们在生活和学习上对我予以帮助，陪伴我度过美好的闲暇时光。

然后，还想感谢我的家人，感谢谢家人的养育之恩，也感谢远在家乡的他们时不时对我的关心，愿意在我心情不好的时候听我的倾诉。

最后，想要感谢每一位论文评审的转交老师，感谢您在百忙之中能够评阅这篇文章。