中国科学技术大学

博士学位论文

3D 隐写模型与方法研究

作者姓名：　　周 航

学科专业：　　网络空间安全

导师姓名：俞能海 教授　张卫明 教授

完成时间：　　二〇二〇年六月

University of Science and Technology of China

A dissertation for doctor's degree

Research on Models and Methods of 3D Steganography

Author's Name:	Hang Zhou
Speciality:	Cyberspace Security
Supervisor:	Prof. Nenghai Yu Prof. Weiming Zhang
Finished Time:	June, 2020

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文，是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外，论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名：_____　　签字日期：_____

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一，学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权，即：学校有权按有关规定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，可以将学位论文编入《中国学位论文全文数据库》等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、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。

保密的学位论文在解密后也遵守此规定。

□ 公开　□ 保密（____ 年）

作者签名：_____　　导师签名：_____

签字日期：_____　　签字日期：_____

摘　要

近年来，随着信息技术和互联网的高速发展，大量敏感数据，包括军事、政治、商业等国家、企业或个人的重要数据在网络上传输，数字信息的安全问题正逐步受到重视。因此，为了保障数字信息的安全，亟需采取必要的保护措施。数字隐写术是信息隐藏中的一类方法，是隐蔽通信或隐蔽存储的一种重要形式。其主要目标是将秘密信息隐藏在某个数字载体（如图像、视频、音频、3D 模型、文本等）之中并传送给接收方，而不引起第三方的注意。面对复杂多样的隐写分析者，如何进一步提升隐写的安全性，从而创造更为安全的隐蔽通信手段成为了当前隐写技术研究的重要内容。然而，相比于图像隐写，3D 隐写的研究尚处于初等阶段，仍有很多关键的科学问题需要分析和解决。本文研究的 3D（3D 网格、3D 贴图、深度图像等）隐写是基于新型载体的隐写术，丰富了隐写数据类型，有望提供更安全的隐蔽通信方式，是隐写术的重要发展趋势之一。因此，研究有效的 3D 隐写方法具有重要的意义和价值。

本文围绕 3D 隐写的三个关键问题开展研究：3D 网格隐写研究、3D 纹理图像贴图隐写研究和 3D 深度图像隐写研究。这三个方面的研究内容相辅相成，旨在实现高安全性的 3D 隐写方法。现将这三个方面的主要工作与创新点简要阐述如下：

1. **3D 网格模型隐写方法**

   - **3D 网格模型隐写安全性分析**

     现阶段 3D 网格隐写分析主要借助基于坐标点信息或边信息的相关性强弱设计特征，分类效果不够明显。由于 3D 网格模型隐写会破坏坐标点邻域相关性，本文通过分析三角面邻域相关性，提出基于三角面邻域法向量张量投票模型的特征来提升 3D 隐写分析性能，形成了新的 3D 网格隐写安全评测方法。

   - **基于最小化失真框架的 3D 网格模型隐写**

     现阶段的 3D 网格隐写没有考虑不同坐标点隐写后对隐写分析特征的敏感性，直接根据消息比特嵌入消息，因此，隐写安全性较低。本文通过分析不同子隐写分析特征对隐写扰动的检测能力，定义了坐标点的失真函数，并采用校验网格编码实施自适应 3D 网格隐写，有效提升 3D 网格载密模型的安全性。

2. **3D 纹理合成隐写方法**

- **纹理图像合成隐写安全性分析**

  针对已有典型的纹理合成图像的隐写方法，发现其原始纹理图像抽样获取候选图像块的方法有漏洞。本文提出了一种有效的攻击方法，通过合成后的大幅纹理图像重构出原始纹理图像，并提取嵌入的秘密消息。本文还提出了另一种有效的检测方法，采用纹理缝补技术重构每一图像块的边界区域，并从中判断重构区域的最优性。最优性作为统计量，有效提升了隐写分析性能，形成了新的纹理图像隐写安全评测方法。

- **基于 3D 纹理贴图的隐写方法**

  针对纹理合成隐写算法的漏洞，本文改进了已有的算法，使得攻击者无法准确估计出合成块的尺寸因而无法实施攻击。本文设计了一种基于密钥控制的边界区域填充的纹理合成隐写，提升了隐写安全性。本文进一步将纹理图像隐写与 3D 网格模型结合，设计 3D 纹理贴图隐写方法，实现了多域联合隐写，扩展了隐写容量。

3. **3D 深度图像隐写方法**

   深度图像通常存储为同一路径下的两个单独文件（彩色图像和深度），在使用中必须同时传输或加载，而且存在深度文件容易丢失的问题。深度图像隐写的任务是在彩色图像中藏深度文件，需要保证合成图像视觉质量，以及原始彩色图像和深度信息的重构。本文提出了基于图像合成的深度图像隐写算法，设计了基于卷积深度网络的图像合成方法，用两个编码器分别抽取高维彩色图像和深度图像的特征，通过特征级联之后，再经过另一编码器编码得到合成的彩色图像，实现隐写术的一种特殊应用，即多模态集成通信。

关键词：三维模型，多边形网格，纹理图像，深度图像，隐写，隐写分析

ABSTRACT

In recent years, with the development of information technology, large amount of sensitive data including military, political, financial and commercial data are circulating on the Internet, thus, the security of these digital information is receiving unprecedented attention within countries, enterprises, or individuals. In order to ensure the security of digital information, necessary protective measures should be considered. Digital steganography is a type of information hiding method utilized for covert communication and covert storage. Its main goal is to hide the secret information in digital carriers (such as images, videos, audios, 3D models, text, etc.) and transmit them to the receiver without being observed by a detector. In the face of complex and diversified steganalysts, how to enhance the security of steganography has become an important problem of current steganography research. However, compared with image steganography, 3D steganography still remains in the preliminary research stage and many key problems deserve investigation. As new data carriers, the 3D steganography model (3D meshes, 3D textures, depth images, etc.) studied in this project has created a more secure way of covert communication, which has better resistance against potential steganalysis. Therefore, it is meaningful and valuable to study effective methods of 3D steganography.

To improve the security of 3D steganography, three key problems need to be solved: 3D mesh steganography, 3D texture steganography and RGBD image steganography. Focusing on these three key issues, this dissertation investigates corresponding 3D steganography methods. The main innovations of this dissertation are listed as follows:

1. **Research on 3D mesh steganography**

   - **Security analysis of 3D mesh steganography**

     The state-of-the-art mesh steganalysis methods extract features from vertices and edges, which are not effective in discriminating cover meshes and stego meshes. The dissertation proposed normal voting tensor based features to boost 3D mesh steganalysis, which forms a new security evaluation method for 3D mesh steganography.

   - **3D mesh adaptive steganography**

     The majority of existing 3D mesh steganography methods modulate vertex coordinates to embed messages in a nonadaptive way. The dissertation took

account of complexity of local regions as joint distortion of a triple unit (vertice) and coding method such as syndrome trellis codes to adaptively embed messages, which owns stronger security.

2. **Research on 3D texture steganography**

   - **Security analysis of texture steganography**

     The dissertation proposed a method to attack classic texture image synthesis based steganography methods. We find that the mirror operation over the image boundary is flawed and is easy to attack. The attack can not only detect the stego-images but can also extract the hidden messages. The dissertation proposed another solution to improve the texture image steganalysis. By exploiting the observation that steganography destroys optimization of matching extent between the synthetic patch and optimal candidate patch, we reconstruct the two patches from an overlapped region to extract the existence of optimality, to boost texture steganalysis, which forms a new security evaluation method for texture steganography.

   - **3D texture mapping based steganography**

     The dissertation proposed a security-enhanced texture synthesis based steganographic method by padding redundant regions carrying no message around the periphery of the synthesized image and generating additional candidate patches to increase capacity. To reach the goal of multi-domain steganography, the stego texture images are mapped to the stego 3D meshes, and they are considered as textured 3D meshes.

3. **Research on 3D depth image steganography**

   RGBD images are usually stored as two separate files in the same file path and utilized by users simultaneously. There are cases that the depth file may be lost during transferring or loading. Therefore, the dissertation proposed a novel algorithm for RGBD image steganography based on convolutional deep networks, using two encoders to extract features and a encoder to encode the cascaded features into synthesized images. The method is a special application of steganography, that is, multi-modal integrated communication.

Key Words: 3D, Polygonal mesh, Texture, Depth image, Steganography, Steganalysis

目 录

图目录

表目录

第 1 章　绪论

本章介绍了数字隐写术的研究背景与意义、研究现状和发展趋势。其中1.1节介绍了信息隐藏的概念和应用；1.2节介绍了数字隐写术的研究现状与发展趋势；1.3节分析了数字隐写术的研究难点以及需要解决的关键问题，提炼了本文的创新点；1.4节概述了本学位论文的体系结构安排。

1.1　研究背景和意义

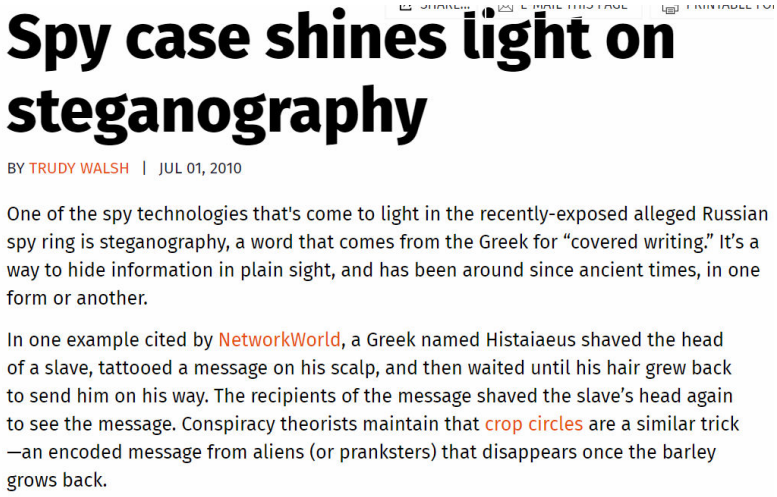
信息隐藏（Information Hiding）是将秘密消息隐藏在载体中，以不被察觉的方式传输秘密消息。信息隐藏技术利用了数字载体的冗余和人类感官特性，在不影响感知的前提下，将秘密消息嵌入到载体的冗余空间中，从而回避第三方的攻击。信息隐藏包括数字隐写术（Steganography）、数字水印（Digital Watermarking）和数字指纹（Digital Fingerprinting）等，隐写术主要用于隐蔽通信，数字水印和数字指纹则较多应用于版权保护等场景。自 1996 年首届国际信息隐藏会议在英国剑桥大学召开起，信息隐藏技术便作为信息安全的重要课题吸引了国际学术界的目光。近年来，信息隐藏的研究增长迅速，国内学术界对于信息隐藏的研究也快速发展，全国信息隐藏研讨会已举办 15 届，国内外的重要期刊会议中也不乏中国学者的身影。作为信息隐藏技术中的重要分支，数字隐写技术是当前信息隐藏领域中的热点问题之一。

隐写术是一类信息隐藏方法，是隐蔽通信或隐蔽存储的一种重要形式[1–5]。这个词来源于拉丁文 steganographia，它结合了希腊词 steganós（$\sigma\tau\varepsilon\gamma\alpha\upsilon\acute{o}\varsigma$），意为“遮盖或隐藏”，以及-graphia（$\gamma\rho\alpha\varphi\acute{\eta}$），意为“书写”。该术语的首次记录使用是在 1499 年，出现在约翰内斯·特里米缪斯（Johannes Trithemius）撰写的专著《隐写术》（*Steganographia*）上。此书是一本关于密码学和隐写术的书籍，却伪装成了一本关于魔术的书。数字隐写术是信息安全领域中一个非常重要的研究方向，其主要建立在图像处理、密码学、机器学习、计算机视觉等学科基础上，并为这些学科的研究提供一个综合的应用平台。数字隐写术作为信息隐藏中的重要技术，自二十世纪九十年代末以来，一直受到了国防安全部门和学术界的重视。早期研究载体主要为静态图像，因其常见、易得且编码方法多、冗余空间充足等性质。

隐写的主要目标是将秘密消息隐藏在某个数字载体之中并传送给接收方，而不引起第三方的注意。与传统加密技术将明文转换为密文后传输密文不同，隐写利用数字媒体（如图像、视频、音频、3D 模型、文本等）的冗余性，修改局部载

体以隐藏秘密消息。隐写术主要有两种应用场景：数据隐蔽通信和多模态集成通信。数据隐蔽通信是指隐写者通过将秘密消息嵌入数字载体，使其看起来与普通的数字媒体无异，从而掩盖秘密消息的存在，不引起监控者的注意。多模态集成通信是隐写术的一种特殊应用，采用隐写算法实现高维信息的自重构或自嵌入，例如彩色图像灰度化、深度图像彩色化等高维数据低维化过程，并需保证载体的可自重构性。

隐写古来有之。例如，隐蔽信息通过隐形墨水藏于纸张上，藏头诗中隐藏的特殊文字。由于隐写技术上的特殊性，隐写往往被用于情报或安全部门的隐蔽通信。随着隐写技术的发展和应用，近年来，互联网上出现了一批免费使用的隐写工具。例如，早在“911 事件”发生半年之前，美国新闻就曾报道了恐怖分子通过某些公开网站的数字图像隐蔽传输有关恐怖袭击的重要信息。美国 CIA 前雇员、“棱镜”曝光者爱德华·斯诺登的女友米尔斯上传一系列配有隐晦标题的照片，曾引发过有关图像隐蔽通信的广泛关注和讨论。2010 年，美国 FBI 在破获一起重大间谍案中发现，俄罗斯特工主要采用信息隐藏技术秘密传递情报，信息中暴露了俄罗斯特工在纽约郊区火车站的秘密集会活动，导致 10 名间谍被抓获，新闻报道如图1.1所示。由此可见，研究秘密消息存在性检测、提取和还原为主要目的的隐写分析技术，对维护国家安全和社会稳定具有重要的现实意义。



Spy case shines light on steganography

BY TRUDY WALSH | JUL 01, 2010

One of the spy technologies that's come to light in the recently-exposed alleged Russian spy ring is steganography, a word that comes from the Greek for “covered writing.” It's a way to hide information in plain sight, and has been around since ancient times, in one form or another.

In one example cited by NetworkWorld, a Greek named Histaiaeus shaved the head of a slave, tattooed a message on his scalp, and then waited until his hair grew back to send him on his way. The recipients of the message shaved the slave's head again to see the message. Conspiracy theorists maintain that crop circles are a similar trick —an encoded message from aliens (or pranksters) that disappears once the barley grows back.

图 1.1　2010 年美俄间谍案新闻报道

传统隐写主要的研究载体是图像、视频、音频等常见的多媒体数据，本文关注的是随着虚拟现实、实时仿真、交叉三维设计技术发展产生的 3D 模型数据的隐写技术。这种新型的 3D 模型作为许多重要应用的底层支撑技术，是计算机图形学本身的一个基础性研究课题。随着计算机图形学的发展和大数据时代计算性能的提高，3D 模型有了大量的应用，包括 3D 渲染、3D 计算和虚拟现实等，3D 模型的隐写和隐写分析的研究也与日俱增，近几年得到了重视。研究 3D 模型的隐写技术满足了复杂多样社交环境下多媒体数据隐写安全性的迫切需求，对于

创造更为安全的隐蔽通信手段也有重要的影响。

1）复杂多样社交环境下的隐写技术研究有助于保障信息通信的安全性

随着信息技术和互联网的发展，网络成为了最便利、最常用的信息传输渠道，每天有数以亿计的数字多媒体信息在网络上传输，占据了通信流量相当大一部分。由于大量敏感数据，包括军事、政治、金融、商业等国家、企业或个人的信息流通于网络，数字信息的安全问题正受到前所未有的重视。为了确保数字信息的安全，需要采取必要的保护措施。传统的手段是采用加密技术，而加密技术的本质是采用特殊的编码方式编码秘密消息，形成不可识别的密文，使攻击者无法破译，从而达到安全传输的目的。但是这也带来了更大的潜在隐患，因为将秘密消息转化成一段看似没有任何意义的乱码的行为本身就告诉了攻击者秘密消息的存在，容易引来攻击者的怀疑，甚至遭受攻击和破坏。

近年来，信息隐藏的研究增长迅速，大量信息隐藏应用被设计开发，而作为信息隐藏技术中的重要分支，数字隐写技术逐渐成为了信息安全领域的热点问题。随着隐写技术的发展，新的隐写理论和隐写算法不断涌现，网络上更是出现了很多可以免费下载使用的隐写工具。隐写术的发展为隐蔽通信带来了便利，但同时也给犯罪组织提供了从事非法活动的有力手段。有新闻报道，一些著名网站，如 eBay 和 Amazon 等已经成为恐怖分子传播秘密信息的隐蔽渠道。基地组织和哈马斯组织等国际恐怖组织已将欧美一些科学家早期关于隐写的研究应用于实践。因此，为了避免隐写技术被不正当利用所带来的危害，隐写分析技术的研究也在不断的推进，这也给数字隐写的设计带来了更大的挑战。如何进一步提升隐写的安全性，使其在特殊需求部门的隐蔽通信中发挥关键作用，成为了当前的研究重点。面对复杂多样的隐写分析者，如何进一步提升隐写的安全性，从而创造更为安全的隐蔽通信手段成为了当前隐写技术研究的重要内容。

本文研究的 3D（3D 网格、3D 贴图、深度图像等）作为新型隐写载体创造了更为安全的隐蔽通信方式，从而对潜在的隐写分析有了更好的抗检测性。

2）大数据环境下亟需新型载体隐写技术

随着云计算的不断普及，大数据环境下的信息安全问题越来越严峻，隐私保护需求越来越强烈。近年来，隐私数据的泄露和滥用的事件屡见不鲜，更是加剧了人们对信息安全的担忧。作为信息安全中重要的研究内容之一，隐写术在保护秘密信息内容的同时隐藏秘密信息存在的事实本身，也越来越被人们所关注，和密码学一起被并称为间谍秘籍家族的一对堂兄弟。

在科学研究方面，随着网络和多媒体技术的发展，当前涌现了越来越多的新型多媒体。作为合适的隐蔽通信载体，新型多媒体隐写技术的研究也随之展开。随着大数据的兴起和云计算的推广，用户对云数据安全性及隐私性的强烈需求推动了云环境下数字隐写技术的发展。面向隐私保护的数字隐写技术不仅是新

兴研究热点，而且是云环境下受隐私保护应用需求强烈驱动的研究点，是信息隐藏、密码学和信号处理等多学科交叉的研究点。

本文研究的 3D 隐写方法将有效推动数字隐写技术的发展，为其他数字多媒体隐写技术的研究推波助澜，从中挖掘大数据中的宝贵价值。

1.2　国内外研究现状

数字隐写术作为信息隐藏中的重要技术，近年来一直受到了国防安全部门和学术界的重视。随着计算机图形学的发展和大数据时代计算性能的提高，3D 模型有了大量的应用，包括 3D 渲染、3D 计算和虚拟现实等，3D 模型的隐写和隐写分析在近几年得到重视且相关研究也与日俱增。传统数字图像隐写术的研究状况可以参考综述文献[1]。

1.2.1　自然图像隐写

自然图像隐写研究主要为空域图像隐写和 JPEG 图像隐写。

空域隐写算法主要研究如何改变图像的像素值来嵌入秘密消息。空域隐写算法包括最低位（Least Significant Bit，简称 LSB）替换和载体系数加减 1 嵌入等。这一类的隐写算法按照固定的嵌入模式隐藏秘密消息，其主要目的是为了尽可能多地嵌入消息以及尽可能好地保持视觉效果，但是较少地考虑统计变化的影响，因此，隐写分析算法通过分析自然图像的统计特征能够检测特定的隐写算法。这一类算法统称为非自适应隐写。现阶段的空域图像隐写算法的研究主要为自适应隐写，分为最小化失真的隐写和基于模型的隐写。最小化失真隐写模型研究的关键为定义修改单个载体元素产生的失真，在消息嵌入过程中同时最小化总体的失真，以达到载体图像和载密图像不可区分的目的。HUGO[6] 算法根据自然图像隐写分析算法 SPAM[7] 的特征向量偏差来定义失真，其中，修改像素后给特征向量带来较小偏差的像素被赋予较小的失真。WOW[8] 和 S-UNIWARD[9] 算法根据单组方向滤波器进行多方向像素残差预测，其中，在任意方向上都较难预测的像素被赋予较小的失真。这二者的不同在于，S-UNIWARD[9] 定义失真的方式更加简洁，也可应用到其他图像域上。这两种算法在对抗空域富模型（Spatial Rich Model，简称 SRM）的隐写分析[10] 上都有较强的安全性。基于最小化失真的空域隐写算法多为启发式设计的方法，这些算法的安全性常常取决于失真定义的合理性。基于模型的隐写包括 MG[11]、MVG[12]、MiPOD[13] 等，一般情况下采用特定的模型描述载体图像和载密图像，通过最小化载体和载密图像的 KL 散度（Kullback-Leibler Divergence，简称 KLD）来达到载体和载密之间的不可区分

性。通过对基于模型的隐写算法进行数学建模，隐写过程中载体修改点选择的问题被转化为数学优化问题，因此，这类方法的安全性取决于载体模型设计的合理性。相比于其他算法，S-UNIWARD 算法的复杂度更高，但安全性也更高。

JPEG 图像隐写算法主要是研究 DCT 域或 DWT 域中如何嵌入秘密消息。近年来，不断有新的 JPEG 图像的自适应隐写算法被提出，包括 J-UNIWARAD[9]、UED[14] 及其改进算法 UERD[15]、HDS[16] 和 RBV[17] 等。这些算法的核心都是设计合理的失真函数，然后采用自适应隐写编码最小化嵌入秘密消息后的总体失真。目前，自适应编码所采用的模型主要为 Filler 等人提出的校验网格编码（Syndrome Trellis Codes，简称 STC）[18]。STC 编码是一种可以接近最优消息嵌入的编码方法，隐写方仅需定义失真函数，STC 编码即可根据每个像素的失真值获取合适的待修改位置，并保证嵌入秘密消息后的总失真接近理论最小值。接收方只需要知道秘密消息长度而无需知道原始载体，就能提取嵌入的秘密消息。

1.2.2　3D 网格模型隐写

由点、线和面依据特定的拓扑关系组合而成的多边形面片构成了 3D 模型的基本骨架结构，其中面片通常由三角形、四边形或其他简单凸多边形组成。由于三角形网格是目前主流网格，本文只考虑三角形网格的隐写算法设计。3D 网格模型的空间描述包括几何特性和连接结构。根据消息嵌入的位置，3D 网格隐写术主要可分为四类：两态调制隐写、最低位隐写、置换隐写和变换域隐写。

在 3D 信息隐藏的早期研究阶段，研究人员将水印和隐写术视为相同的技术，并提出了一批嵌入秘密消息的算法。两态调制隐写通常等分邻近的两个坐标点之间的线段，标记为 0 和 1 两个状态。根据秘密消息的值对应的状态来相应地修改第三个点的坐标。François 和 Benoit[19] 提出采用量化索引调制技术来调制某个三角面片顶点的坐标值，以嵌入消息 0 或 1。Wang 和 Cheng[20] 提出基于层级 k-维树和高级跳跃策略的快速路径搜索方法，并提出在嵌入区域的多层分段嵌入秘密消息以实现更高容量的隐写。Chao 等人[21] 提出了一种大容量的可逆隐写方法，首先旋转和放缩 3D 模型，校准至主成分分析（Principle Components Analysis，简称 PCA）变换得到的主轴、次轴和垂直主轴与次轴的方向上，然后将每一个轴上的点根据坐标位置等间隔划分并聚类，最后通过空间调制嵌入消息。Itier 和 Puech[22] 提出了一种基于静态算术编码和哈密顿图的嵌入方法，但是嵌入产生的修改幅度较大。由于 Itier 和 Puech 提出的隐写算法会导致载密 3D 网格在球坐标系下的方位角和仰角坐标分量有较为明显的修改，容易受到隐写分析的检测。为了抵抗隐写分析，Li 等人[23] 提出仅在距离分量上嵌入秘密消息。

最低位隐写是将消息比特藏于最低有效位的方法。Yang 等人[24] 提出了一种

估计坐标点曲率，并依据曲率大小自适应修改部分坐标点的最低有效位以嵌入秘密消息的方法。Li 等人[25] 提出了在失真约束下基于密钥调制的 3D 网格隐写算法。

置换隐写通过扰动集合中元素的顺序嵌入秘密消息。由于 3D 网格包含具有可重排顶点和三角面的集合，这为置换隐写提供了秘密消息嵌入的空间。每一种元素的排列顺序可以单一地映射为某个整数，因此，可以通过更改集合中元素的顺序实现秘密消息的嵌入。然而，大量元素在使用置换隐写算法时计算复杂度很高，因此，近年来研究者们权衡嵌入容量和时间复杂度以降低算法复杂度。Bogomjakov 等人[26] 提出了一种改进的置换隐写算法，通过秘密消息分段编码排列值，并扰动排列值对应位置的坐标元素以嵌入秘密消息。Huang 等人[27] 改进了编码方式，在相同嵌入效率下提升了嵌入容量。Tu 等人[28–30] 分别提出了基于二叉树、左斜二叉树和最大期望树的编码方法，更进一步提升了嵌入容量。

变换域隐写算法预先通过某种映射变换顶点坐标值，然后在变换域中隐写。Cho 等人[31] 提出了在球坐标系下将顶点坐标与球心坐标的距离作为度量值，分段聚类后进行均值调制嵌入秘密消息的算法。Kanai 等人[32] 提出基于小波变换域和多分辨率表征下的秘密消息嵌入算法。变换域隐写算法具有鲁棒性强和嵌入容量低的特点。

迄今为止，3D 网格模型的隐写技术的研究仍处于起步阶段，大多是通过调制嵌入秘密信息，没有考虑到拓扑关系对载体失真的影响。因此，3D 网格隐写具有非常广阔的开拓空间，值得我们探究高安全性的的隐写算法。

1.2.3　纹理图像隐写

纹理图像是一类特殊的图像，具有近似的周期性变化。不同于自然图像中有一定比例的平滑区域，纹理图像几乎不含平滑区域。一般而言，图像中平滑区域相比于复杂区域像素间的相关性更强。由于隐写会破坏邻域像素间的相关性，设计基于邻域残差特征的隐写分析方法能有效检测自然图像隐写。对于纹理图像来说，像素邻域相关性较弱，隐写前后的相关性变化程度不明显，难以用传统的隐写分析特征进行检测。

纹理合成是由一小块样本纹理图像依据马尔科夫模型生成大幅纹理图像[33–36] 的过程，纹理合成隐写即在纹理合成的过程中嵌入秘密消息，最终生成的大幅纹理图像是与秘密消息有关的。Otrori 和 Kuriyama[36,37] 最先提出在纹理合成过程实现数据嵌入，通过在样本图像中选择若干彩色点，然后使用局部二值模式（Local Binary Patterns，简称 LBP）来映射二值数据和彩色点之间的关系，再根据秘密消息内容预先确定若干位置的彩色点，最后从样本图像中寻找合适内容合成大

幅纹理图。Wu 和 Wang[38] 指出 Otrori 和 Kuriyama 的方案有容量低和嵌入信息提取错误率高的局限，并提出新的解决方案以实现大容量无误码的信息隐藏。该方法在样本图像中逐点移动获得多个候选块，将每一个候选块分为内核和外围两部分，比较每一个候选块的外围与其他候选块外围之间的匹配程度，由大到小建立索引表，该索引表直接与二进制数据相映射。在纹理合成时用候选块来填充大幅图像的空白部分，具体选取哪个候选取决于秘密消息，最终可得到一幅由秘密消息决定的纹理图像。最近，Qian 等人[39] 提出一种抗 JPEG 压缩的纹理合成隐写算法。由于纹理合成图像的特殊性，目前还没有一般性的纹理图像隐写分析方法，这使得不法分子以纹理图像作为携带秘密消息的载体有了可趁之机。通过实验发现，Wu 和 Wang 的方法[38] 存在安全漏洞，本文提出了针对性的攻击方法，并形成了新的纹理图像隐写安全评测方法。

与纹理图像合成技术息息相关的研究热点是 3D 纹理合成技术。3D 纹理合成是大规模场景绘制技术的一个研究分支，是虚拟现实、实时仿真以及交叉三维设计等许多重要应用的底层支撑技术，是计算机图形学本身的一个基础性研究课题。随着游戏编程、GIS 系统、飞行模拟系统和 VR 系统的大步发展，3D 纹理合成技术的研究显得尤为重要。早期的 3D 纹理映射方法主要研究如何合理地将二维纹理图像“贴”到 3D 模型上同时不引起较大的失真。Wei 和 Levoy[40] 提出采用 3D 网格平面化和邻域像素构造方法生成每个坐标点的像素值，以获取纹理映射后的 3D 模型。Turk[41] 认为纹理映射的方法会破坏纹理的模式，因此，Turk 提出过程纹理合成从而避免纹理映射带来的失真。最近，Waechter 等人[42] 提出了大规模场景图像的 3D 重构技术，不同角度下拍摄的图像经过预处理之后，通过马尔科夫随机场能量最优化问题选择最优的图像块映射到 3D 模型上，然后通过泊松编辑技术调整颜色信息，保证块之间的亮度一致性，最终实现纹理映射。

长远来看，如何有机地结合纹理映射和平面纹理合成隐写，并且应用到 3D 纹理合成隐写中，是 3D 隐写未来的研究趋势。

1.2.4　深度图像隐写

深度图像（RGB-D）由普通的彩色图像和图像深度地图构成。在 3D 计算机图形中，深度地图是与视点场景对象表面距离有关的图像。深度地图类似于灰度图，只是它的每个像素值是传感器距离物体的实际距离。通常彩色图像和深度地图是配准的，因此，像素点之间具有一一对应关系。在计算机视觉系统中，三维场景信息为图像分割、目标检测和物体跟踪等各类计算机视觉应用提供了更多的可能性，而深度图像作为一种普遍的三维场景信息表达方式得到了广泛的应用。

深度图像的广泛应用使得我们不得不考虑深度图像内存占用的问题。众所周知，深度图像通常存储为同一路径下的两个单独文件，在使用中必须同时传输或加载，存在深度文件容易丢失的问题。深度图像隐写的任务是在彩色图像中藏深度文件，需要保证合成图像视觉质量，以及原始彩色图像和深度信息的重构。由于深度图像的彩色图像和深度具有一定的关联性，因此，将图像深度视为待嵌入秘密消息，并与原彩色图像融合得到三通道的彩色图像可实现深度地图的隐藏。由于彩色图像相较于深度图像而言使用更为普遍，通过伪装深度图像为彩色图像，实现深度秘密消息的隐写。

1.3　论文的研究内容与创新点

3D 网格模型隐写算法目前在安全性上还有待提升。纹理图像具备结构的近似重复性，在隐写上具备自然图像不具备的优势。从眼下看，纹理图像的隐写方法还较为初步，理论基础还不够，而且没有尝试应用到 3D 模型上，因此，纹理图像隐写还有极大的研究和提升空间。深度图像目前尚无隐写算法，其研究处于起步阶段。本文围绕 3D 模型隐写现有技术的不足与劣势，展开相关的研究，主要工作和创新点着眼于如下三个方面：

第一，当前的 3D 网格模型的隐写方法依然比较初级，也没有丰富的理论基础，存在着不少缺陷和改进的空间。本文希望深入研究和探索 3D 网格隐写和隐写分析之间的因果联系，提升了 3D 网格隐写分析的性能，构建了更好的安全性验证框架，能够更准确地验证所提出的隐写算法是否有效。其次，本文优化和设计了新的 3D 网格隐写方法，将隐写编码应用于 3D 网格模型上嵌入消息以最小化模型的失真，提高了隐写算法的抗检测能力。

第二，上述纹理合成图的隐写分析研究现状表明，针对载密纹理合成图像的隐写分析研究比较少，使用当前性能最优的自然图像隐写分析检测器检测纹理载密图像性能较差，因此，本文需要进一步探究如何设计一种有效的隐写分析方法。本文在已有研究的基础上，发现已有典型的纹理合成隐写算法存在安全漏洞，并提出如下攻击方法：由于生成的载密纹理图像完整地保存了原始样本图像的所有分块，攻击者可通过分析载密图像中块与块之间的缝合关系重建原始样本纹理图案，从而重建候选块索引和提取秘密消息。同时，随着 3D 网格模型的应用日益广泛，3D 网格的纹理合成技术和大规模场景图像 3D 重构技术发展迅速。本文设计 3D 纹理贴图隐写方法，实现了多域联合隐写，扩展了隐写容量。

第三，深度图像作为 3D 数据的一种表现形式，是目前许多 3D 数据获取设备（TOF 相机、Kinect 和激光扫描等）获取到的原始数据表现形式。然而，针对于深度图像隐写的研究少之又少，亟需进一步探索。本文提出了深度图像的自嵌

入模型，通过设计深度卷积网络将深度通道嵌入到彩色图像中，实现了深度图像到彩色图像的变换，达到了多模态集成通信的功能。

通过提升 3D 网格模型隐写算法，实现纹理合成隐写和 3D 网格纹理映射的协同工作，以及设计深度图像隐写算法，本文将实现广义上多种 3D 多媒体数据的隐写算法，为大数据环境下数据的隐蔽通信提供有力的技术支持。

1.4　论文的结构安排

本论文的结构框架如图1.2所示。

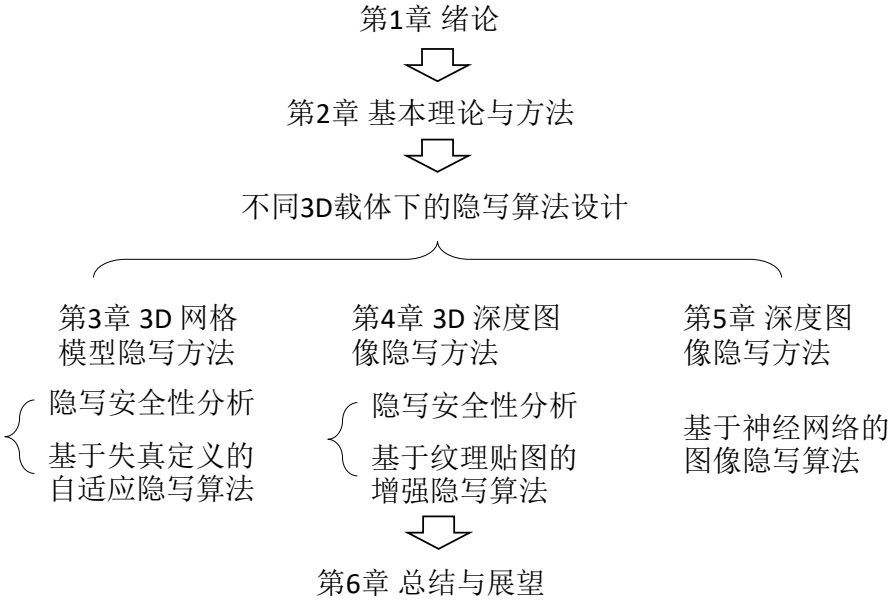


图 1.2　本学位论文体系结构

本学位论文围绕 3D 模型隐写方法，着重开展三个研究内容。学位论文共分为六章，论文体系安排与各研究点之间的关联如图 1.2所示。本学位论文各章节的主要内容与关联性如下所述：

第 1 章绪论。介绍论文的研究背景和研究现状，分析论文的创新点和组织结构。

第 2 章基本理论与方法。铺垫了背景知识。介绍了隐蔽通信基本模型，隐写与隐写分析的基本评价指标和三种 3D 数据（3D 网格、纹理图像和深度图像）的格式。

第 3 章 3D 网格模型隐写方法。本章首先设计了基于三角面邻域法向量张量特征，展开讨论这种特征对 3D 网格隐写的检测性能的影响，提升了 3D 隐写分析性能，形成了新的 3D 网格隐写安全评测方法。随后，设计了 3D 网格基于失真定义的自适应隐写算法，分析并验证了坐标点法向量偏移作为失真代价的有效性，提升了已有隐写算法的安全性，为 3D 网格自适应隐写奠定了方法基础。

第 4 章 3D 纹理贴图隐写方法。通过纹理图像隐写分析，介绍了纹理合成隐写算法的安全性，设计了增强的纹理合成隐写算法模型以及给出 3D 纹理贴图隐写的实例。本章首先设计了基于镜像对称的隐写分析算法和基于纹理合成区域最优性匹配特征的隐写分析算法，并分别讨论检测性能。随后，基于图像边界区域纹理随机填充设计了增强的隐写算法来抵御已有的隐写分析。最后，本文在 MeshLab 平台上实施了 3D 纹理贴图，证实了基于 3D 纹理贴图的隐写算法的实用性。

第 5 章深度图像隐写方法。介绍了基于图像深度通道自嵌入至彩色图像的深度图像隐写算法，设计了隐写编码器和解码器，考虑了合成图像和重构图像分别与原彩色图像之间的损失，加入了抗 JPEG 压缩的 JPEG 压缩模拟器，而且将峰值信噪比作为评价指标。实验结果表明，本文提出的深度图像隐写算法具有较好的隐写性能。

第 6 章总结与展望。总结本论文的主要研究工作，并给出了可能的改进点和未来的研究方向。

第 2 章　基本理论与方法

本章将主要讨论信息隐藏信息论理论模型，包括基于隐蔽通信的隐写与隐写分析框架及其基本理论与主流方法。同时，简要地介绍了 3D 数据格式和使用场景。2.1节介绍了隐蔽通信基本模型；2.2节回顾了当前隐写术和隐写分析性能的基本评价准则；2.3、2.4和2.5节分别介绍了 3D 网格、纹理图像和深度图像的基本形式。本章内容是后续章节内容的方法基础。

2.1　隐蔽通信基本模型

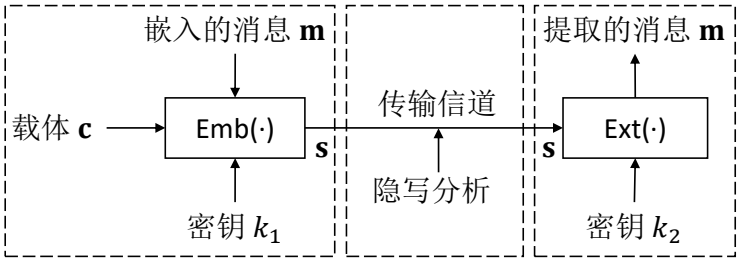


图 2.1　数字隐蔽通信和隐写分析示意图

现代的隐写模型都是基于 Simmons 提出的囚犯问题[43] 设计的，该问题中 Alice 与 Bob 需要在 Wendy 的监视下进行隐蔽通信。通过图2.1 所示的隐写系统可以达到该目的，其中 Alice 享有密钥 k_1，Bob 享有密钥 k_2，$\mathbf{c}$ 是一个被 Wendy 认可的载体。一般情况下，在私钥隐写系统中，$k_1 = k_2$。隐写过程如下：Alice 将待传递消息 $\mathbf{m}$ 使用密钥 k_1 加密后，通过隐写嵌入步骤 $\mathrm{Emb}(\cdot)$ 将其嵌入载体 $\mathbf{c}$ 得到载密 $\mathbf{s}$，然后在 Wendy 监视下的信道中将 $\mathbf{s}$ 传输给 Bob：

$$\mathrm{Emb}(\mathbf{c}, \mathbf{m}, k_1) = \mathbf{s}. \tag{2.1}$$

Bob 接收到 $\mathbf{s}$ 后利用提取步骤 $\mathrm{Ext}(\cdot)$ 和密钥 k_2 得到消息 $\mathbf{m}$，完成一次隐蔽通信：

$$\mathrm{Ext}(\mathbf{s}, k_2) = \mathbf{m}. \tag{2.2}$$

2.2　评价指标

为了合理地评估各种隐写和隐写分析方法的性能，有必要定义一些通用的评价标准。

2.2.1　隐写评价指标

安全性、容量和鲁棒性用于评估隐写算法的性能。

安全性。如果秘密消息的存在只能以不高于随机猜测的概率来估计，则隐写算法可以被认为在隐写分析系统中是完全安全的。安全性的定义将在下一节中进一步讨论。

容量。为了实现传达秘密消息的高效性，隐写术提供的隐藏能力应尽可能高，可以通过绝对度量，即秘密消息的大小或相对有效载荷（也称为嵌入率），例如比特每顶点（bit per vertex，简称 bpv）进行评估。

鲁棒性。尽管大多数隐写方法并不追求鲁棒性，但在某些实际应用中，由于网络流量、带宽和智能设备处理能力的限制，通信信道是有损耗的，从而导致传输媒体的性能下降，并进一步影响秘密消息的正确提，因此，有时候有必要考虑隐写算法的鲁棒性。

2.2.2　隐写分析评价指标与典型的分类器

隐写分析的主要目的是确定载体是否嵌入了秘密消息。如果使用某种隐写分析方法来检测可疑的载体，则会有四种可能的结果：

- 真阳性（True Positive，简称 TP），表示载密被正确地分类为载密。
- 假阴性（False Negative，简称 FN），表示载体被错误地分类为载密。
- 真阴性（True Negative，简称 TN），表示载体被正确地分类为载体。
- 假阳性（False Positive，简称 FP），表示载密被错误地分类为载体。

混淆矩阵。载体和载密数据混合而成的隐写分析结果可以构成 2×2 混淆矩阵[44]，并且有以下几个评估指标：

$$\begin{aligned}
\text{召回率} &= \frac{\mathrm{TPs}}{\mathrm{TPs}+\mathrm{FNs}},\\
\text{假正率} &= \frac{\mathrm{FPs}}{\mathrm{TNs}+\mathrm{FPs}},\\
\text{准确率（Accuracy）} &= \frac{\mathrm{TPs}+\mathrm{TNs}}{\mathrm{TPs}+\mathrm{FNs}+\mathrm{TNs}+\mathrm{FPs}},\\
\text{查准率（Precision）} &= \frac{\mathrm{TPs}}{\mathrm{TPs}+\mathrm{FPs}}.
\end{aligned} \tag{2.3}$$

受试者操作特征曲线（Receiver Operating Characteristic Curve，简称 ROC）。隐写分析器的性能可以通过 ROC 曲线[44] 可视化，其中在纵轴上绘制了真阳率，

在横轴上绘制了假阳率。曲线下面积（Area Under Curve，简称 AUC）越大，隐写分析性能越好。

下面，我们介绍几种典型的监督分类器，用于训练从载体提取的特征向量。

支持向量机（Support Vector Machine，简称 SVM）。支持向量机是一种监督式机器学习模型，用于解决分类问题。以下为两种常用的分类器：

- 基于软件包 LIBSVM[45] 的高斯 SVM。
- 基于软件包 LIBLINEAR[46] 的线性 SVM。

然而，随着特征空间维数和训练样本的增加，SVM 的复杂度和内存需求也迅速增加。为了能够处理高维隐写分析特征，在实验中一般使用集成分类器进行分类。

集成分类器。集成分类器[47] 是 SVM 的替代工具，用于隐写分析检测器的构建。检测器是由多个 Fisher 线性判决器（Fisher Linear Discriminant，简称 FLDs）构成的分类器。默认情况下，集成分类器在相同先验条件下最小化总分类错误率：

$$P_{\mathrm{E}} = \min_{P_{\mathrm{FA}}} \frac{1}{2}(P_{\mathrm{FA}} + P_{\mathrm{MD}}), \tag{2.4}$$

其中 P_{FA} 和 P_{MD} 分别是虚警率和漏警率。最终的安全性 $\overline{P}_{\mathrm{E}}$ 由多次试验中错误率取均值得到。

2.3　3D 网格模型基本形式

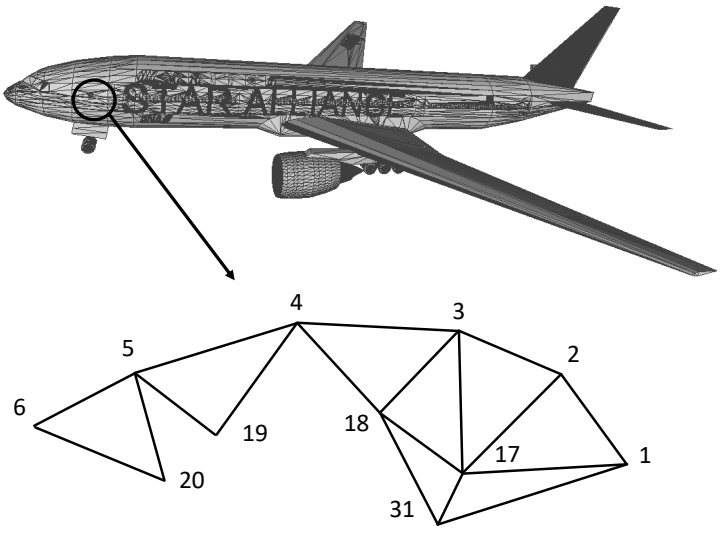


图 2.2　3D 网格及其局部形状

表 2.1　图2.2对应的三角面索引的数据结构

顶点坐标列表				三角面索引列表	
顶点索引	*x* 轴	*y* 轴	*z* 轴	三角面索引	每个面的元素
1	x_1	y_1	z_1	1	(17,1,2)
2	x_2	y_2	z_2	2	(3,2,17)
3	x_3	y_3	z_3	3	(4,3,18)
4	x_4	y_4	z_4	4	(5,4,19)
5	x_5	y_5	z_5	5	(6,5,20)
6	x_6	y_6	z_6	...	...
...	...	...	...	16	(31,17,1)
17	x_{17}	y_{17}	z_{17}	17	(18,17,31)
18	x_{18}	y_{18}	z_{18}	...	...
...	...	...	...	...	...
31	x_{31}	y_{31}	y_{31}	...	...
...	...	...	...	...	...

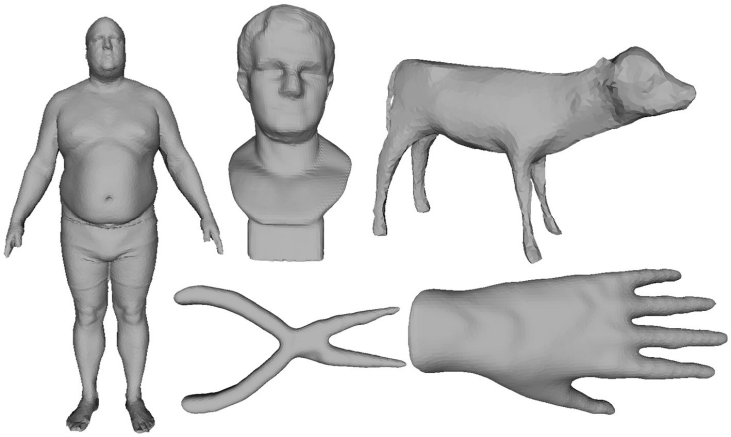
网格是多边形小平面的集合，目标是构成真实 3D 对象的适当近似。它具有三个不同的组合元素：顶点，边和面。网格还可以通过几何信息和连接信息来描述：几何信息描述了其所有顶点的 3D 位置（坐标），而连接信息提供了邻接关系。在数学上，可以将包含 V 个顶点和 F 个面的 3D 多边形网格 $\mathcal{M}$ 建模为信号 $\mathcal{M}=\{\mathcal{V},\mathcal{E},\mathcal{F}\}$，其中

$$\begin{aligned}\mathcal{V}&=\{v_i\}_{i=1,2,\ldots,V},\\ \mathcal{F}&=\{f_i\}_{i=1,2,\ldots,F},\ f_i\in\mathcal{V}\times\mathcal{V}\times\mathcal{V},\\ \mathcal{E}&=\{e_i\}_{i=1,2,\ldots,E},\ e_i\in\mathcal{V}\times\mathcal{V},\end{aligned}\tag{2.5}$$

其中，在笛卡尔坐标系中，$\mathcal{E}$ 是边集，而 $\mathcal{F}$ 是三角面集。三角形网格到 $\mathbb{R}^3$ 中的几何嵌入是通过将 3D 位置 $\mathbf{p}_i$ 与 $\mathcal{V}$ 中的每个顶点 v_i 相关联得到：

$$\begin{aligned}\mathcal{P}&=\{\mathbf{p}_1,\ldots,\mathbf{p}_V\},\\ \mathbf{p}_i&:=\mathbf{p}(v_i)=[x(v_i),y(v_i),z(v_i)]^T\in\mathbb{R}^3.\end{aligned}\tag{2.6}$$

网格通常按一定的顺序排列顶点和面。尽管面列表包含冗余信息，但它可以促进给定网格上的几何和拓扑运算。图2.2为 3D 网格示例，表2.1为相应的文件格式。面通常由三角形（对应于三角形网格），四边形（对应于四边形网格）或其他简单的凸多边形（对应于多边形网格）组成。由于三角形网格是当前主流 3D 网格，因此，本文仅考虑三角形网格。



(a) 普林斯顿分割数据集（PSB）

(b) 普林斯顿网格（PMN）

图 2.3　3D 网格数据示意图

普林斯顿分割数据集（Princeton Segmentation Benchmark，简称 PSB）。如图2.3(a) 所示，PSB[1]是一个含有 354 个 3D 网格[48] 用于分割任务的数据集。260 对载体载密 3D 网格对用于分类器的训练，剩余 94 对载体载密 3D 网格用于测试。

普林斯顿网格（Princeton Modelnet，简称 PMN）。如图2.3(b) 所示，PMN[2]包含 12311 个共 40 类的 3D 网格数据，用于计算机视觉、计算机图形学、机器人技术和认知科学。50% 的 3D 网格用于训练，剩余的 3D 网格用于测试。

2.4　纹理图像基本形式

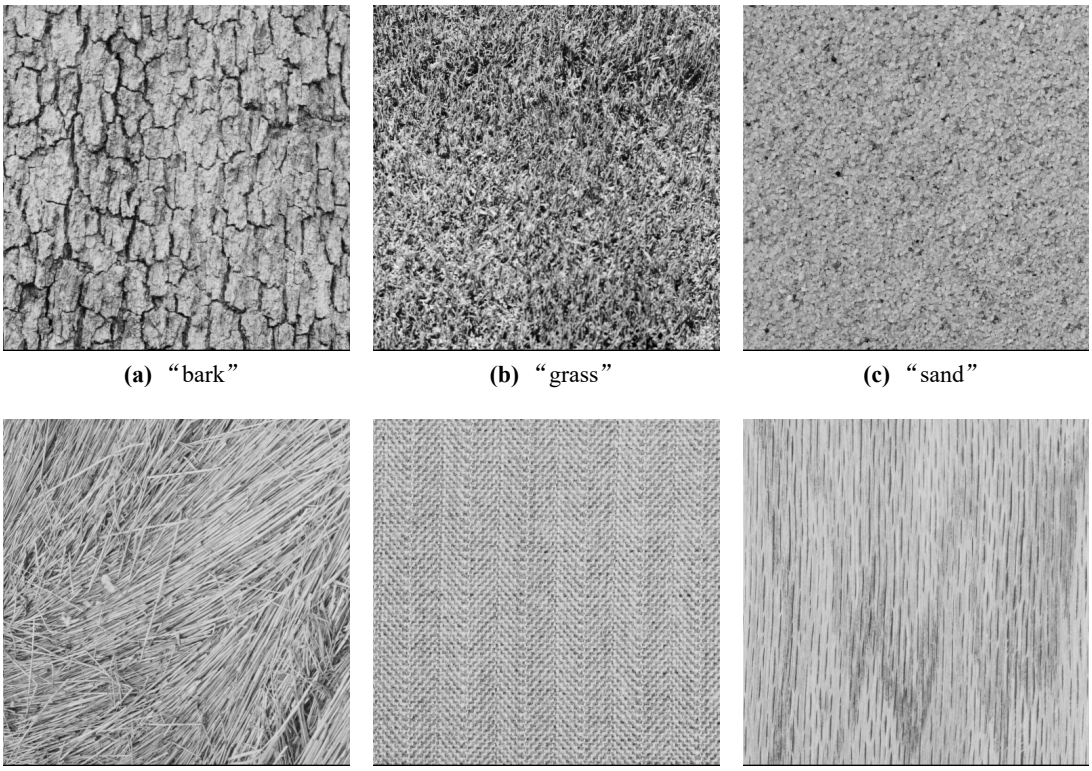
如图2.4所示，纹理是物体表面上的线条或花纹。纹理图像广泛存在于大自然，是人类视觉系统最常接收和处理的图像信号。纹理图像含有纹理基元和纹理颜色等的图像信息，能够给予人类丰富的信息用于图像分析和理解，因此，纹理

[1]http://segeval.cs.princeton.edu/

[2]http://modelnet.cs.princeton.edu/

图像广泛应用于物体检测和场景识别中。纹理图像含有复杂多样的图像信息，许多抽象的信息难以用直观的语言描述。随着对纹理图像研究的不断深入，研究者尝试将纹理图像与人类视觉感知相结合，使计算机能够学习人类的视觉感知能力感知纹理图像所含有的信息。探索人类视觉感知纹理图像的研究工作主要集中在纹理感知属性和纹理感知语义这两个方面。纹理感知属性是人们对纹理图像的主观认知，通常是较为抽象的图像信息，例如纹理粗糙度、纹理方向性、纹理光泽度和纹理密度等。而纹理感知语义则是人们对纹理图像的描述，主要包括气泡状、网格状、螺旋的和蜂巢状等，都是比较具象的描述词。在计算机视觉领域，人们使用感知相似性来衡量不同的纹理图像之间的差异。

Brodatz 纹理图像库。如图2.4所示，实验中，采用 Brodatz Textures[3], 包含大小为 640 × 640 的 112 张灰度纹理图像。



(a)“bark”　**(b)**“grass”　**(c)**“sand”

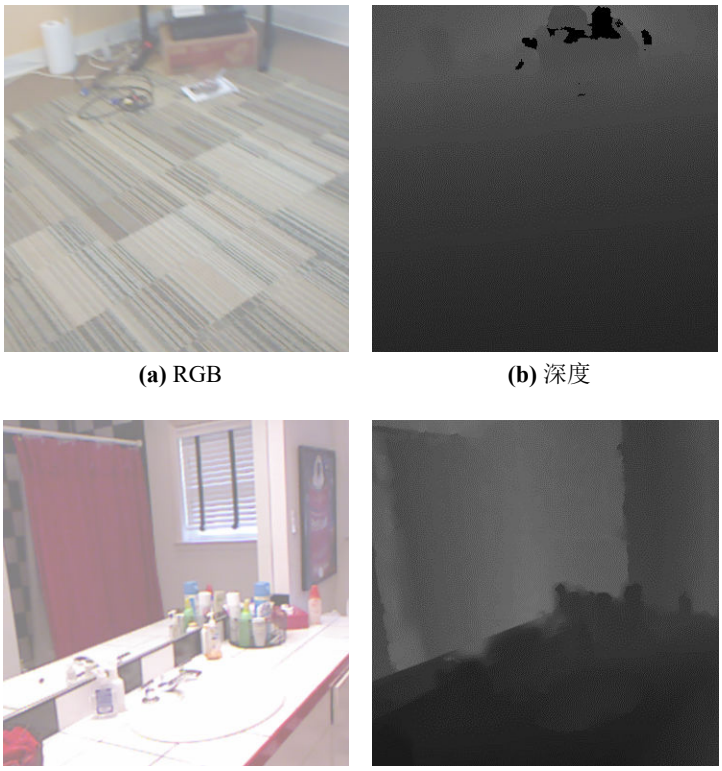
(d)“straw”　**(e)**“weave”　**(f)**“wood grain”

图 2.4　纹理图像示意图

2.5　深度图像基本形式

三维重建（3D Reconstruction）一直是计算机图形学和计算机视觉领域的一个热点课题。早期的三维重建技术通常以二维图像作为输入重建出场景中的三

[3]http://www.ux.uis.no/~tranden/brodatz.html



(a) RGB　　**(b)** 深度

(c) RGB　　**(d)** 深度

图 2.5　RGB-D Scenes Dataset 示意图

维模型。然而，受限于输入的数据，重建出的三维模型通常不够完整，而且真实感较低。随着各种面向普通消费者的深度相机（Depth Camera）的出现，基于深度相机的三维扫描和重建技术得到了飞速发展。以微软的 Kinect，华硕的 XTion 以及英特尔的 RealSense 等为代表的深度相机造价低廉，体积适当，操作方便，并且易于研究者和工程师开发算法。三维重建技术也是增强现实（Augmented Reality，简称 AR）技术的基础，经过扫描重建后的三维模型可以直接应用到 AR 或 VR 场景中。下文将简要介绍基于深度相机的三维重建技术的基本原理及其应用。

三维重建。三维重建通过输入数据建立 3D 模型。在面向消费者层面的深度相机出现之前，三维重建技术的输入数据通常只有 RGB 图像。通过对物体的不同角度拍摄的 RGB 图像使用相关的计算机图形学和视觉技术，便可重建出该物体的三维模型。然而早期的三维重建技术得到的模型精度往往较低，且技术的适用范围有限。消费者层面的深度相机的出现为三维重建技术提供了深度图像（Depth Image）数据，大大降低了重建难度，使得三维重建技术可以应用到几乎任何现实场景中。由于基于深度相机的三维重建技术所需数据是 RGB 图像和深度图像，因此，这类技术通常也被称为基于 RGBD 数据的三维重建技术。

深度值和三维数据。对于现实场景中的点，深度相机扫描得到的每一帧数据不仅包括了场景中的点的彩色 RGB 图像，还包括每个点到深度相机所在的垂直

(a) RGB　　**(b)** 深度

(c) RGB　　**(d)** 深度

图 2.6　NYU Depth Dataset V2 示意图

平面的距离值。这个距离值被称为深度值（Depth），如图2.5所示，这些深度值共同组成了这一帧的深度图像。也就是说，深度图像可以看做是一副灰度图像，其中图像中每个点的灰度值代表了这个点的深度值。

深度图像场景数据集（RGB-D Scenes Dataset）。如图2.5所示，深度图像场景数据集[4]由 Lai 和 Bo 等人[49] 提出，包含从深度视频中重建的 14 个新场景，其中包含家具和桌面物品。

NYU 深度数据集 V2（NYU Depth Dataset V2）。如图2.6所示，NYU 深度数据集 V2[5]由 Microsoft Kinect 的 RGB 和深度摄像机获取的多种室内场景视频序列组成[50]，包含 1449 个密集标记的 RGB 和深度图像，来自 3 个城市共 464 个新场景，以及 407024 个未标记帧。

2.6　本章小结

本章介绍了隐蔽通信基本模型、评价指标和 3D 基本数据。后续章节设计的各种 3D 隐写模型需要用到这些基本技术。

[4]https://rgbd-dataset.cs.washington.edu/

[5]https://cs.nyu.edu/∼silberman/datasets/nyu_depth_v2.html

第 3 章　3D 网格模型隐写方法

本章将主要讨论 3D 网格模型隐写方法，包括 3D 网格隐写安全性分析和基于最小化失真框架的 3D 网格隐写算法设计。3.1节介绍了 3D 网格隐写与隐写分析的研究进展；3.2节介绍了基于三角面法向量张量投票的 3D 网格隐写分析算法；3.3节介绍了基于最小化失真框架的 3D 网格模型隐写；3.4节为本章小结。

3.1　引言

早期隐写术的研究对象主要为图像和音视频，因为在互联网上这些载体的传输是相对频繁的。近年来，硬件技术的提升促进了 3D 产业的发展，具备 3D 渲染能力的硬件不再是遥不可及的商品，而是更多地应用于 CAM/CAD 行业中，并带动了庞大的用户端应用的开发，例如虚拟现实、视觉特效、3D 打印、动画电影和视频游戏等。作为新一代的数字媒体，3D 网格频繁地在网络上生产、使用和分发，因此，3D 网格是适用于隐蔽传输的媒体载体。

近年来，很多 3D 网格隐写算法被研究者相继提出。总的来说，根据消息嵌入的位置，3D 网格隐写算法分为四类：两态调制隐写、最低位隐写、置换隐写和变换域隐写。在 3D 信息隐藏的早期研究阶段，研究人员将水印和隐写术视为相同的技术，并提出了一批嵌入信息的算法。

第一类是两态调制隐写。两态调制隐写通常等分邻近的两个坐标点之间的线段，标记为 0 和 1 两个状态。根据秘密消息的值对应的状态来相应地修改第三个点的坐标。Cayre 和 Macq[19] 提出采用量化索引调制技术来调制某个三角面片顶点的坐标值，以嵌入消息 0 或 1。Wang 和 Cheng[20] 提出基于层级 k-维树和高级跳跃策略的快速路径搜索方法，并提出在嵌入区域的多层分段嵌入消息以实现更高的容量。Wang 等人[51] 提出抗置换攻击的嵌入算法，将坐标点变换到由主成分分析构建的空间，并通过相邻点之间的坐标调制以嵌入消息。Chao 等人[21] 提出了一种大容量的可逆隐写方法，首先旋转和放缩 3D 模型，校准至主成分分析变换得到的主轴、次轴和垂直主轴与次轴的方向上，然后将每一个轴上的点根据坐标位置等间隔划分并聚类，最后通过空间调制嵌入消息。Itier[22] 等人提出了一种基于静态算术编码和哈密顿图的嵌入方法，但是嵌入产生的修改幅度较大。由于 Itier 等人[22] 提出的隐写算法得到的载密网格在球坐标系下的方位角和仰角坐标分量有较为明显的修改，容易受到隐写分析的检测，因此，为了抵抗隐写分析，Li 等人[23] 提出仅在距离分量上嵌入消息。

第二类是最低位隐写。最低位隐写是首先将消息藏于最低有效位的隐写方

法。Yang[24] 等人提出了一种估计坐标点曲率，并依据曲率大小自适应修改部分坐标点的最低位以嵌入秘密消息的 3D 网格隐写方法。Li 等人[25] 提出了在失真约束下基于密钥调制的 3D 网格隐写算法。

第三类是置换隐写。置换隐写通过扰动集合中元素的顺序嵌入秘密消息。由于 3D 网格包含具有可重排顶点和三角面的集合，这为置换隐写提供了消息嵌入的空间。每一种元素的排列顺序可以单一地映射为某个整数，因此，通过更改集合中元素的顺序可嵌入秘密消息。然而，当载体元素较多时，使用置换隐写算法的计算复杂度很高，因此，近年来研究者们通过权衡嵌入容量和时间复杂度以降低置换隐写算法的复杂度。Bogomjakov 等人[26] 提出了一种改进的置换隐写算法，通过秘密消息分段编码排列值，并扰动排列值对应位置的坐标元素以嵌入消息。Huang 等人[27] 改进了编码方式，在相同的嵌入效率下提升了嵌入容量。Tu 等人[28–30] 分别提出了基于二叉树、左斜二叉树和最大期望树的编码方法，进一步提升了嵌入容量。由于置换隐写会导致存储结构上相邻坐标点的邻域相关性下降，容易受到针对性隐写分析的检测，因此，Wang 等人[52] 提出在坐标点的一环近邻域编码嵌入消息以抵抗检测。置换隐写的嵌入容量与载体长度相关，当载体顶点数达到 5000 时，最大的嵌入率达到了 11 bpv。

第四类是变换域隐写。变换域隐写算法预先通过某种映射变换顶点坐标值，然后在变换域中隐写。Cho 等人[31] 提出了在球坐标系下将顶点坐标与球心坐标的距离作为度量值，分段聚类后进行均值调制嵌入秘密消息的算法。Bors 和 Luo[53] 改进了此方法，增加了表面平滑性的约束。Kanai 等人[32] 提出基于小波变换域和多分辨率表征下的秘密消息嵌入算法。变换域隐写算法具有鲁棒性强和嵌入容量低的特点。

3D 隐写分析的研究随之而来。3D 隐写分析可分为通用型隐写分析和专用型隐写分析。通用型隐写分析主要检测基于坐标点修改的隐写算法，包括两态调制隐写、最低位隐写和变换域隐写算法的检测。

通用型隐写分析由标准化（基于 PCA 的旋转和缩放）、特征提取和分类器的训练构成。其中，3D 网格特征由原始 3D 网格特征与一环邻域均匀拉普拉斯平滑后的 3D 网格特征的距离表示。Yang 和 Ivrissimtzis[54] 提出了基于笛卡尔坐标系下和拉普拉斯坐标系下的坐标分量变化特征、坐标向量长度变化特征和坐标点的价小于 6、等于 6 和大于 6 的坐标向量长度变化特征。同时，他们提出了相邻三角面之间基于二面角角度偏移的特征和三角面法向量方向偏移的特征。特征降维包含抽取均值、方差、偏度和峰度四个统计特征，以及直方图相邻 bin 的插值构成另外四个统计特征。最后，所有特征经过对数变换，以提取更为有效的特征。这 208 维特征简称为 YANG208。Li 和 Bors[55] 有效约简了 Yang 和 Ivrissimtzis[54] 提出的 YANG208 特征，摒弃了若干判决能力较弱的特征，提出了基于局部特征

集合（Local Feature Set，简称 LFS）的有效特征，共含有 52 维，简称为 LFS52，并保持了隐写分析原有的性能。同时，Kim 等人[56] 在 LFS52 特征的基础上，提出了坐标顶点法向量方向偏移特征、高斯曲率值变化特征和最小主曲率和最大主曲率的曲率比值变化特征，包含 64 维特征，简称为 LFS64。进一步地，Li 和 Bors[57] 在 LFS52 基础上提出了球坐标系下坐标分量值变化特征，简称为 LFS76。Li 等人[58] 在 LFS76 特征的基础上，提出了基于边长变化特征和边长分量变化特征，简称为 ELFS124。Li 和 Bors[59] 提出在 3D 网格原始模型与其分别进行上采样得到的高分辨率网格和下采样得到的低分辨率网格经小波分解后的系数变化和边长变化的特征，简称为 WFS228。Li 等人[60,61] 通过特征选择来解决载体来源失配问题（Cover Source Mismatch，简称 CSM）。

专用型隐写分析主要检测特定隐写算法，包括针对基于 PCA 旋转变换的隐写和置换隐写的检测。Wang 等人[52] 发现置换隐写导致存储结构上相邻坐标点不具有近邻特性，因此，他们提出基于存储结构上相邻坐标点在空域中的距离度量值作为特征，以实现隐写检测。

本文对已有的 3D 隐写和隐写分析算法做了分类，并绘制了分类系统，如图3.1所示。表3.1展示了 3D 隐写分析算法中的基本元素。

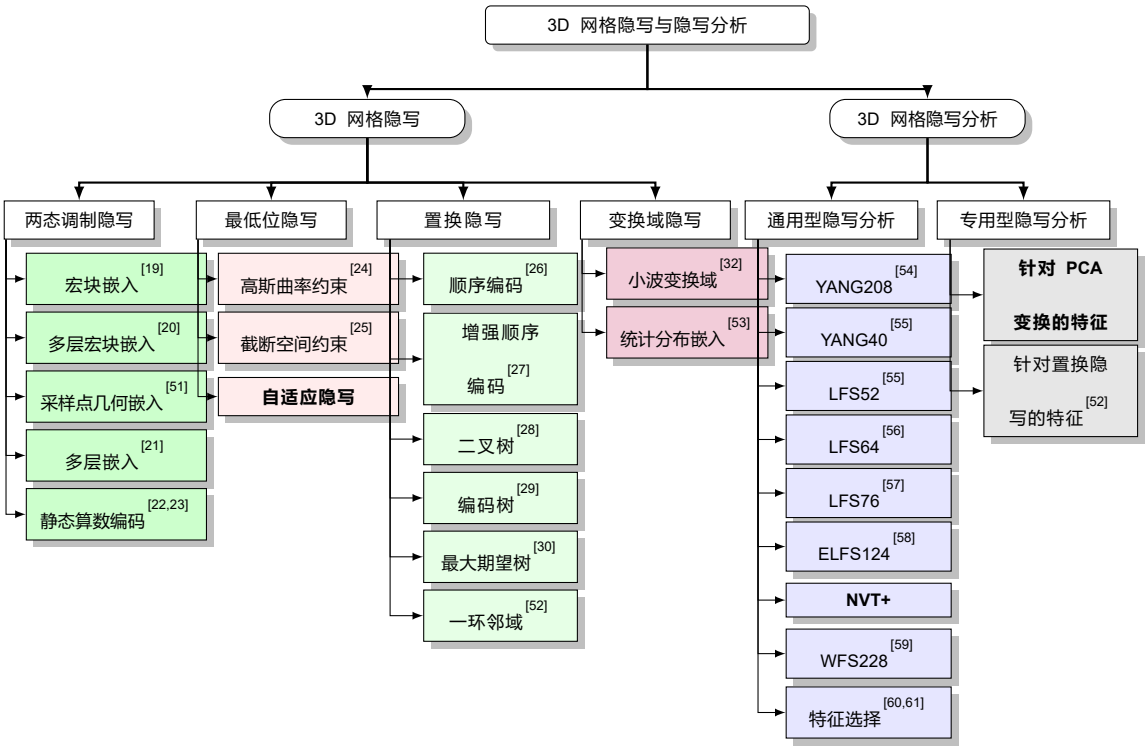


图 3.1　3D 网格隐写和隐写分析分类系统

表 3.1　3D 网格隐写分析特征中的基本元素

特征	维度	YANG 208	YANG 40	LFS 52	LFS 64	LFS 76	ELFS 124	**NVT+** 100	WFS 228
坐标和不同价下的欧式距离	24	✓							
二面角角度	2	✓	✓	✓	✓	✓	✓	✓	
坐标及其欧式距离	8		✓	✓	✓	✓	✓	✓	
顶点法向量	1			✓	✓	✓	✓	✓	
高斯曲率	1			✓	✓	✓	✓	✓	
曲率比	1			✓	✓	✓	✓	✓	
边法向量	1				✓			✓	
平均曲率	1				✓			✓	
总曲率	1				✓			✓	
球坐标	3					✓	✓		
球坐标系下的边向量	3					✓	✓		
边向量	12						✓		✓
法向量投票张量特征根	9							✓	
小波系数和边向量	45								✓

3.2　3D 网格模型隐写安全性分析

如前所述，正常的 3D 网格模型相邻元素之间具有强相关性，即邻域残差的直方图呈现较陡的状态。由于隐写算法会破坏相邻元素之间的相关性，并造成载密 3D 网格邻域元素相关性下降，因此目前的隐写分析方面的研究主要集中于通过分析三维空间中相邻元素间的关联度设计残差特征，并进一步训练隐写分析分类器实现二分类。早期的工作主要将空间坐标点或三角面的边长作为元素，以此元素特征之间的相关性设计特征，包括坐标点法向量残差特征、三角面法向量残差特征和相邻二面角夹角残差特征等。然而，这些残差特征在区分载体和载密 3D 网格时不够有效，因此，基于这些特征训练的隐写分析器检测准确率较低。

猜想，是否存在一种代表邻域的元素，能够更敏感地察觉 3D 坐标点隐写扰动造成的影响？由于坐标点或三角面代表的元素涵盖区域面积不够大，本文考虑三角面一环邻域区域作为单位元素设计隐写分析特征。通过分析三角面邻域相关性，本文提出了基于三角面邻域法向量张量投票模型的特征以提升 3D 网格隐写分析性能。

3.2.1　通用型隐写分析框架

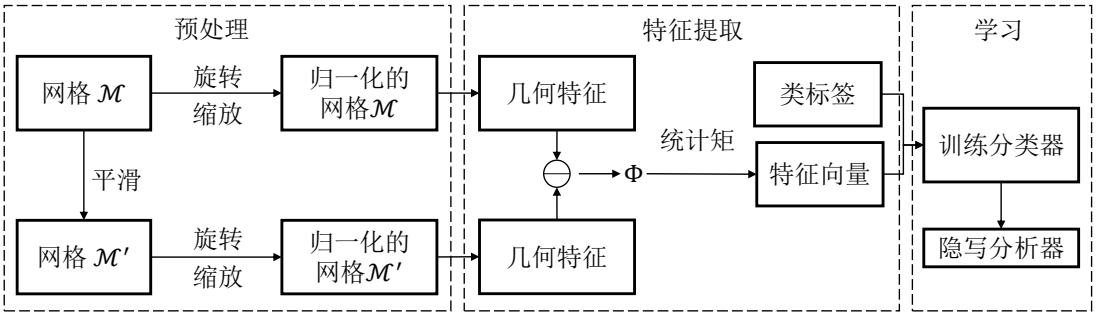


图 3.2　基于统计残差特征学习和分类器分类的 3D 网格隐写分析框架

图3.2为基于统计残差特征学习和分类器分类的通用型 3D 网格隐写分析框架，包括校准（旋转和缩放）、平滑、特征提取和特征映射。在特征提取之前，顶点坐标需要归一化：将 3D 网格原先的坐标旋转至主成分分析获得的三个主轴方向，并缩放至单位立方体内。

受图像隐写分析启发，载密图像与其平滑后的图像之间的差异大于载体图像与其平滑后的图像之间的差异[62,63]。由于隐写过程对 3D 网格也造成了同样的影响，因此，3D 网格的隐写分析也遵循同样的原则。

[0]本节内容已于 2019 年发表在 3D 计算机图形可视化领域 CCF A 类，SCI 一区国际期刊 IEEE Transactions on Visualization and Computer Graphics 上（“Feature-Preserving Tensor Voting Model for Mesh Steganalysis”，2019）。

3D 网格的平滑过程定义如下：对原始网格 $\mathcal{M}$ 实施一次迭代的均匀拉普拉斯算子平滑处理，使得每个顶点坐标 $\mathbf{p}_i$ 是其一环邻域坐标的均值，并得到平滑后的网格 $\mathcal{M}'$[64]：

$$\mathbf{p}_i \leftarrow \mathbf{p}_i + \frac{\tau}{\sum_{v_j \in \mathcal{N}_1(v_i)} w_{ij}} \sum_{v_j \in \mathcal{N}_1(v_i)} w_{ij}(\mathbf{p}_j - \mathbf{p}_i), \tag{3.1}$$

其中 τ 是标量因子，w_{ij} 是权重项：

$$w_{ij} = \begin{cases} 1 & \text{if } \mathbf{v}_j \in \mathcal{N}(\mathbf{v}_i) \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

τ 的选择会影响隐写分析的性能，因此，Li 等人[65] 分析了不同 τ 值对 3D 网格的平滑和特征提取的影响情况。

需要与之区分的是 3D 网格坐标的拉普拉斯变换。坐标点 v_i 的一环邻域 $N(v_i)$ 定义为：

$$\mathcal{N}(v_i) = \{v_j | (v_i, v_j) \in E, 1 \le i, j \le N\}. \tag{3.3}$$

拉普拉斯变换定义为

$$\mathbf{L} = \mathbf{M} \times \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ \vdots & \vdots & \vdots \\ x_N & y_N & z_N \end{bmatrix}, \tag{3.4}$$

其中 **M** 为基尔霍夫矩阵：

$$M_{ij} = \begin{cases} |\mathcal{N}(v_i)| & \text{if} \quad i = j \\ -1 & \text{if} \quad v_j \in \mathcal{N}(v_i) \\ 0 & \text{otherwise.} \end{cases} \tag{3.5}$$

对于坐标 v_i，拉普拉斯坐标为 **L** 的中相应的第 i 行。

通常，实验中采用集成分类器[47] 训练隐写分析器。设计一个有效的隐写分析器的核心是特征设计，因此，接下来将介绍本文提出的隐写分析特征。

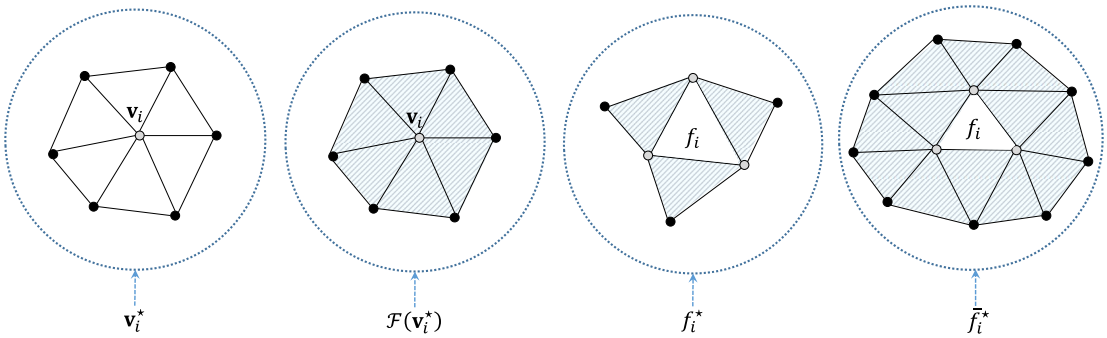
3.2.2　网格离散曲面邻域

首先定义“邻域”。如图3.3所示，定义 4 种邻域区域：坐标点的点邻域区域、坐标点的面邻域区域、三角面与边相邻的面邻域区域和三角面与顶点相邻的面邻域区域。由于三角面的法向量特征在之前的隐写分析算法中已验证为较为有

效的特征，因此，本文将邻域三角面法向量之间的差异程度作为隐写分析特征。为此引入张量的概念。

张量是一个用于表示在一些矢量、标量和其他张量之间的线性关系的多线性函数，这些线性关系的基本例子有内积、外积、线性映射以及笛卡儿积。在同构的意义下，第零阶张量为标量，第一阶张量为矢量，第二阶张量为矩阵。从几何角度讲，张量是一个真正的几何量，因为它不随参照系的坐标变换（基向量变化）而变化。由于基向量可以有丰富的组合，因此，张量能表示非常丰富的物理量。

在曲面的参数化表示中，曲面局部区域的一阶表示由点的坐标及其法向量给出，而二阶表示包含坐标曲率及其方向。为了更好地描述坐标点一阶差分的几何信息及其奇异性，Medioni 等人[66] 设计了二阶对称张量提取方向信息及其置信度。直观地看，张量的形状定义了坐标点邻域的特性：孤立的点，曲线上的点还是曲面上的点。为了检测曲面特征，Medioni 等人采用三角网格顶点法向量的张量投票协方差矩阵。通常，特征是指曲面上具有至少一个较大主曲率的区域，特征边是指极大或极小主曲率沿相应主曲率方向的极值点连线，这种基于定点法向量的张量能够有效识别特征边。通过检测载体和载密上特征边的变化情况，可以实现有效的隐写分析。从数学角度上分析，张量投票模型能够提取局部区域的复杂程度特征，即对于面点、边点和角点赋予不同的特征值。本文将面点视为平滑区域，边点视为小扰动区域，角点视为复杂区域，并依据这三个特征值构建隐写分析特征。



(a) 点 v_i 的点邻域集合 $\mathcal{N}_1(v_i)$ **(b)** 点 v_i 的面邻域 $\mathcal{N}(v_i)$ **(c)** 与三角面 f_i 的边相邻的面邻域 $\mathcal{N}_1(f_i)$ **(d)** 与三角面 f_i 的顶点相邻的面邻域 $\mathcal{N}_2(f_i)$

图 3.3　四种邻域的示意图

3.2.3　法向投票张量

根据以上章节中对张量和坐标点邻域的介绍，依据不同邻域表示，本文设计了两种基于法向量投票的张量。

1）基于三角面法向量的坐标点邻域

Sun 等人[67] 提出了基于邻域三角面单位法向量的顶点法向量投票张量。定义三角面 f_i 法向量 $\mathbf{n}(f_i)$ 的协方差矩阵 $\mathbf{C}(f_i)$ 以表达法向量方向信息：

$$\mathbf{C}(f_i) = \mathbf{n}(f_i) \cdot \mathbf{n}(f_i)^T. \tag{3.6}$$

因此，顶点 v_i 邻域的三角面法向量投票张量 $\mathbf{T}_i$ 为点邻域三角面协方差的加权之和，并且定义如下：

$$\mathbf{T}_i = \sum_{f_j \in \mathcal{N}_1(v_i)} \mu_{ij} \mathbf{n}(f_j) \cdot \mathbf{n}(f_j)^T, \tag{3.7}$$

其中，权重 μ_{ij} 由邻域面积比和三角面重心 $\mathbf{c}(f_j)$ 至坐标点 v_i 的距离构成：

$$\mu_{ij} = \frac{A(f_j)}{\max\left(A(\mathcal{N}_1(v_i))\right)} \exp\left(-\frac{\|\mathbf{c}(f_j) - \mathbf{p}_i\|_2}{1/3}\right). \tag{3.8}$$

2）基于三角面法向量的三角面邻域

面邻域的法向量投票模型定义为面邻域三角面协方差的加权之和[68]：

$$\mathbf{T}_i = \sum_{f_j \in \mathcal{N}(f_i)} \mu_{ij} \mathbf{n}(f_j) \cdot \mathbf{n}(f_j)^T. \tag{3.9}$$

本文定义了两种 $\mathcal{N}(f_i)$：与边相邻的邻域和以顶点相邻的邻域，且权重 μ_{ij} 均设为 1。

3.2.4　隐写分析特征设计

由于张量是对称且半正定的矩阵，因此，可以用矩阵的特征向量和特征根表示张量的特性。二阶对称张量 $\mathbf{T}$ 特征值分解如下:

$$\mathbf{T} = \lambda_1 \mathbf{e}_1 \mathbf{e}_1^T + \lambda_2 \mathbf{e}_2 \mathbf{e}_2^T + \lambda_3 \mathbf{e}_3 \mathbf{e}_3^T, \tag{3.10}$$

分解得到三个特征根 λ_1，λ_2，λ_3，并且有 $\lambda_1 > \lambda_2 > \lambda_3 \geq 0$。

特征根更容易体现邻域关联性。对于一个无噪 3D 网格，平坦区域只有一个占主导的特征值，边缘区域有两个占主导的特征值，而拐角区域的三个特征值都比较接近，均占主导。例如，考虑一个立方体模型，有以下结论：$\{\lambda_1 = 1, \lambda_2 = \lambda_3 = 0\}$（面），$\{\lambda_1 = \lambda_2 = \sqrt{2}/2, \lambda_3 = 0\}$（边缘）和 $\{\lambda_1 = \lambda_2 = \lambda_3 = \sqrt{3}/3\}$（拐点）。

如上所述，特征根可以反映法向量投票张量的形状。因此，特征根能有效表示局部表面的形状，如图3.4 所示。在隐写分析特征的设计上，本文将原始网格与平滑后的网格各个局部区域张量的特征根之差的绝对值作为隐写分析特征。

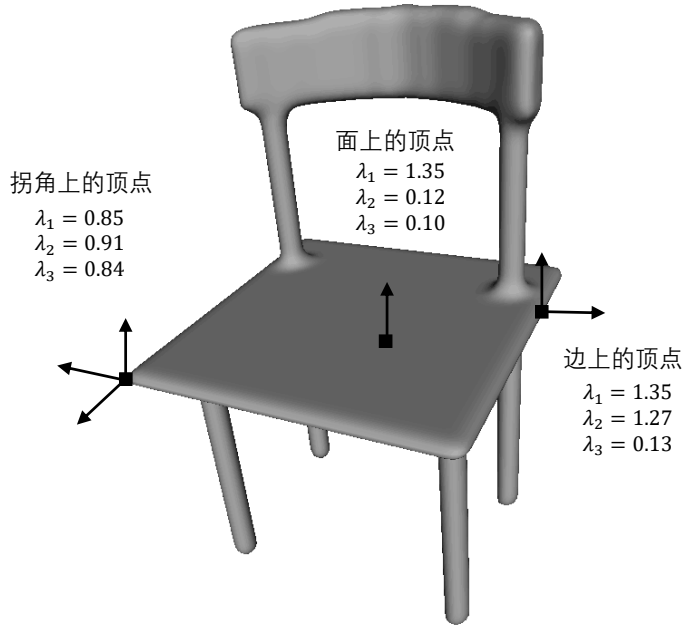


图 3.4　不同特征（拐角，边和面）的法向量投票张量的特征值

上一节提出的三种张量模型均能分别提取三个特征根的差，因此，共构成 9 维特征。

这里，残差特征定义如下：

$$\begin{aligned} \phi_1(i) &= |\lambda_1 - \lambda_1'|, \\ \phi_2(i) &= |\lambda_2 - \lambda_2'|, \\ \phi_3(i) &= |\lambda_3 - \lambda_3'|. \end{aligned} \tag{3.11}$$

提取统计矩之后，最终的隐写分析特征构成 $9 \times 4 = 36$ 个，并简称为法向量投票张量算法（Normal Voting Tensor，简称 NVT）。本文将 NVT 特征和 LFS64 特征[57] 进行结合，组成了 100 维的新特征 NVT+。

3.2.5　MMD 安全性能评价

隐写隐写算法安全性能采用最大平均差异（Maximum Mean Discrepancy，简称 MMD）来衡量[2]，该距离可以度量从载体和载密中提取到的特征之间的差异，从而直观地反映隐写后载密的安全性。该距离与隐写分析的检测错误率对应，MMD 距离越小表示隐写的安全性越高，MMD 距离越大则表示隐写安全性越低。本文通过以下仿真实验验证 NVT 特征能有效检测隐写引起的修改失真：

1. 在嵌入率分别为 $\eta = 2, 5, 10$ bpv 下，采用 Chao 等人提出的多层嵌入算法[21] 修改网格的顶点坐标实施隐写。验证数据集为 PSB 数据集。

表 3.2　MMD 距离测试结果

嵌入率	隐写分析算法	MMD 距离
2 bpv	LFS64	.0396
	ELFS124	.0305
	NVT+	**.0816**
5 bpv	LFS64	.0503
	ELFS124	.0361
	NVT+	**.1008**
10 bpv	LFS64	.1026
	ELFS124	.0603
	NVT+	**.1706**

2. 对每个 3D 网格分别计算 LFS64[56]，ELFS124[58] 和 NVT+ 的隐写分析特征向量，得到载体网格和载密网格特征对。

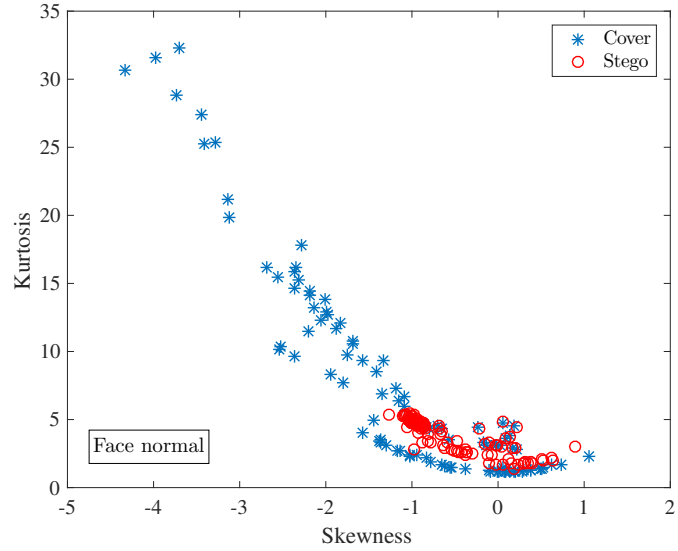
3. 计算 MMD 距离。独立计算 MMD 值 30 次并取均值，最后比较 MMD 距离。

表3.2给出了 MMD 的统计结果。一般来说，MMD 能够有效衡量载体和载密在特征空间的距离。因此，MMD 越大，隐写分析特征的判决能力越好。从统计结果来看，NVT+ 的 MMD 大于其他两种方法的 MMD，表明本文提出的 NVT+ 具有更好的判决性能。

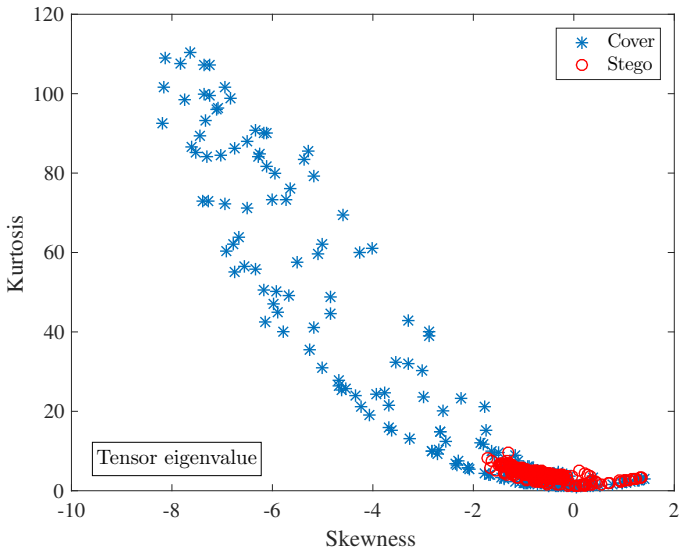
3.2.6　隐写分析特征的可视化

本文将隐写分析特征投影到指定的二维空间，观察其样本分布，以比较法向量投票张量特征和已有特征的隐写分析性能，如图3.5所示。载密 3D 网格由 Chao 等人提出的多层嵌入算法[21] 生成，数据集为 PSB。

首先，分别得到三角面法向量投票张量特征和三角面法向量的特征。其中，张量的特征选取模型 ξ_1 的特征根 λ_1，选取三角面法向量的特征作为对比特征的原因是三角面法向量的偏移度特征是目前最有效的隐写分析特征[69]。对数映射后，两种隐写分析方法均会计算偏度和峰度特征。如图3.5所示，载体 3D 网格标为蓝色星号，载密 3D 网格标为红色圆圈。图3.5(a) 展示了基于三角面法向量特征的样本分布，图3.5(b) 展示了基于法向量投票张量特征的样本分布。对于线性分类器来说，图3.5(a) 比图3.5(b) 更难划分载体样本和载密样本，表明法向量投票张量特征更容易区分载体 3D 网格和载密 3D 网格。



(a) 三角面法向量的偏移度特征



(b) 张量投票特征（λ_1 的变化值）

图 3.5　PSB 数据集下，对 Chao 隐写算法得到的载体和载密对隐写分析时偏度和峰度的分布

3.2.7　子分类器的选择

本文采用 Chao 等人[21] 和 Zhou 等人[69] 提出的隐写方法来验证 NVT 算法的有效性。对隐写分析特征向量的各个子模型独立地进行性能评估，以比较各个隐写分析特征的判决能力。

具体方法描述如下。首先，采用 Chao 和 VND 隐写方法，在相同嵌入率下进行隐写得到载密 3D 网格。由于基学习器 FLD 训练过程简单高效，因此，本文采用 FLD 评估各个隐写分析特征的判决能力。对于任一训练集中的特征 $m = 1, 2, 3, ..., N^{trn}$，载体和载密特征分别记作 $\mathbf{x}^{(m)}$ 和 $\bar{\mathbf{x}}^{(m)}$。训练分类器时，采

用袋外错误率（Out-Of-Bag error，简称 OOB error）[10] 以找到随机森林中最优的特征选择个数：

$$E_{\mathrm{OOB}}^{(L)}=\frac{1}{2N^{trn}}\sum_{m=1}^{N^{trn}}\left(B^{(L)}(\mathbf{x}^{(m)})+1-B^{(L)}(\overline{\mathbf{x}}^{(m)})\right). \tag{3.12}$$

其中，袋外错误率也称为测试误差的无偏估计[70]。

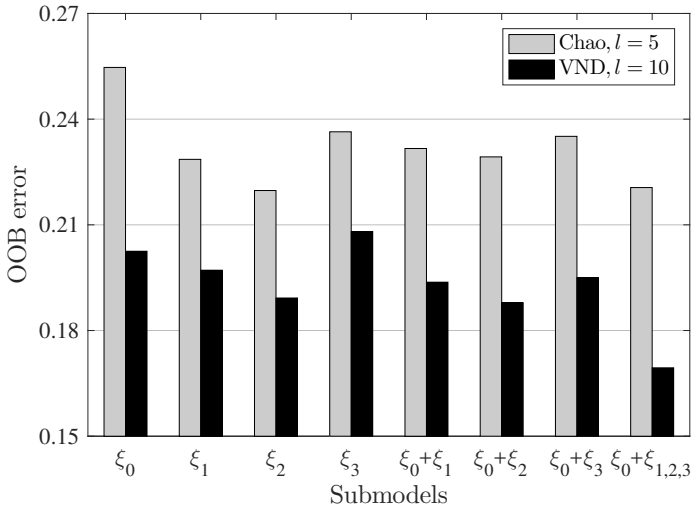


图 3.6　PSB 数据集下，对 Chao 进行隐写分析的袋外平均错误率

在实验中，本文采用嵌入率为 5 bpv 下的 Chao 隐写算法[21] 和嵌入率为 10 bpv 的 VND[69] 隐写算法得到载密 3D 网格，并计算不同子特征模型的袋外错误率。图3.6为每个子模型的袋外错误率，其中 ξ_0 为 LFS64 隐写分析特征，ξ_1 为基于顶点邻域构造的 NVT 隐写分析特征，ξ_2 为基于边连接的三角形邻域构造的 NVT 隐写分析特征，以及 ξ_3 为基于顶点连接的三角形邻域构造的 NVT 隐写分析特征。这三个特征各自的袋外错误率均低于 ξ_0 的袋外错误率。由于 NVT 特征设计的方式不同于其他特征（NVT 特征从邻域面提取，其他特征从单个顶点、单个边或单个面提取），因此，这些特征能够彼此互补以提升隐写分析性能。本文将 ξ_1,ξ_2,ξ_3 特征与 LFS64 特征 ξ_0 进行融合，构成 100 维特征，此时隐写分析性能实现进一步的提升。

3.2.8　不同数据库的隐写分析性能表现

在实验中，本文分别采用 PSB 和 PMN 数据集分析隐写分析性能。

本节比较本文提出的 NVT+ 隐写分析特征与目前最新的 5 种隐写分析特征（YANG208[54]，LFS52[55]，LFS64[56]，LFS76[57] 和 ELFS124[58]）的性能。隐写算法采用 Chao[21]，VND[69] 和 Li[25]。

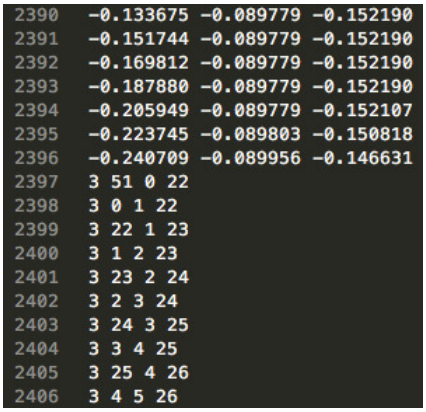


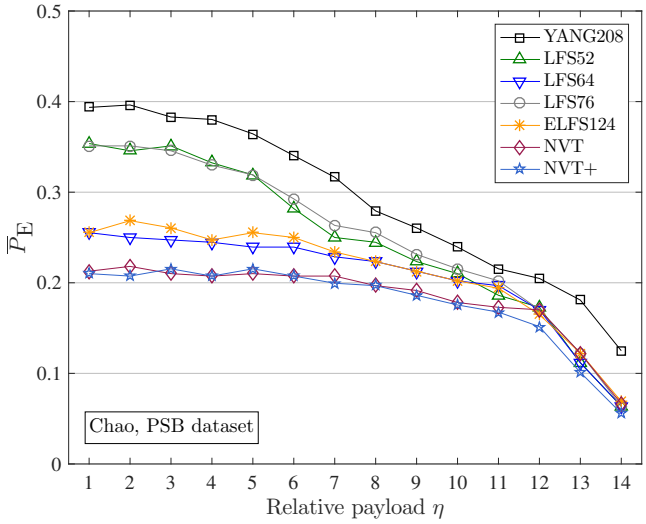
图 3.7　3D 网格中顶点的存储结构

需要注意的是，实验中未考虑针对置换隐写算法[26–30,52]的隐写分析，因为通用型隐写分析特征无法检测 3D 网格几何上没有修改的隐写算法。然而，置换隐写算法通过结构顺序中坐标扰动实现消息嵌入，容易被专用型隐写分析特征检测出来。由于结构顺序中相邻的坐标点通常是一个三角面上的两个点，而置换隐写后的 3D 网格在结构顺序中，相邻的坐标点在几何距离上通常离得较远。如图3.7所示，这是一个正常的 3D 网格的结构示意图，其中第 2397 行和第 2398 行有两个公共顶点，第 2398 行和第 2399 行有两个公共顶点，即相邻坐标点共享共同的顶点；而载密 3D 网格中，相邻的坐标点几乎没有相同的顶点。

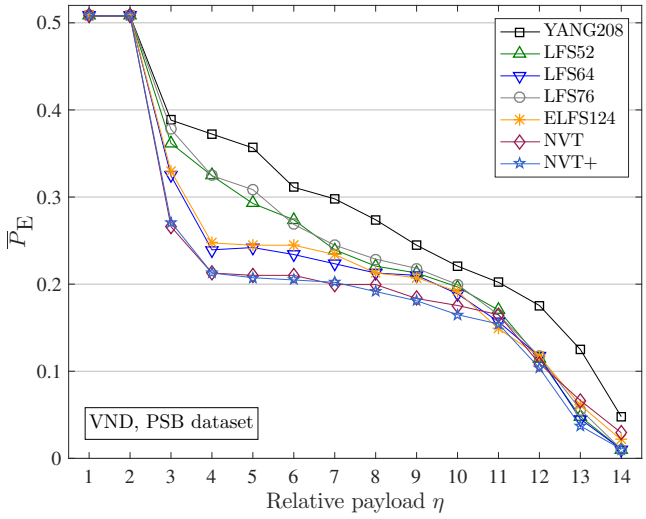
图3.8为 PSB 数据集的实验结果。检测错误率 $\overline{P}_{\mathrm{E}}$ 随嵌入率的增大而减小。与 LFS64 和 ELFS124 相比，NVT+ 最高能提升 5% 的检测准确率。当嵌入率增加时，提升幅度减小。对于任意一种隐写算法，当嵌入率较大（$\gamma > 10$ bpv）时，NVT+ 的检测错误率优势并不明显。对于 VND 隐写算法，在小嵌入率（$\gamma = 1,2$ bpv）时，顶点的修改量太小，导致目前所有的隐写分析方法均无法检测，因此，检测错误率接近 50%。

图3.9为 PMN 数据集上的隐写分析实验。除了嵌入率较小时所有的隐写分析方法均无法区分载体 3D 网格和载密 3D 网格之外，本文提出的 NVT+ 方法始终优于已有的隐写分析方法。嵌入率越低，NVT+ 的隐写分析性能越明显，其中，检测准确率的提升最高可达 22%。

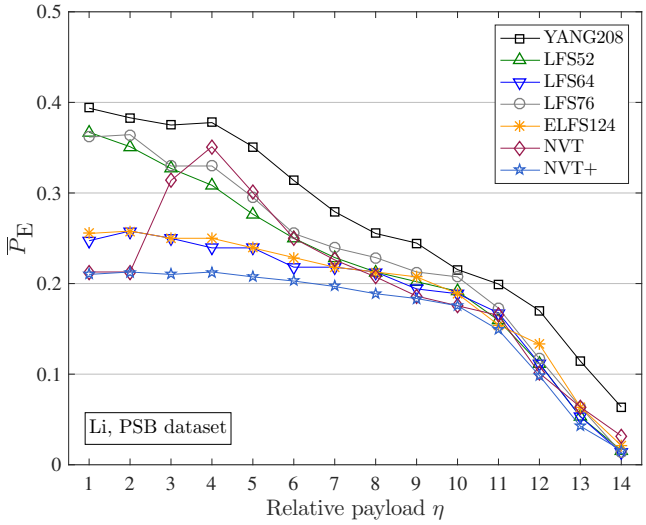
相比于 PSB 数据集，PMN 数据集在检测准确率上有更明显的性能提升，原因在于数据类型的不同。PSB 数据集中的 3D 网格均是自然物体通过扫描重建得到的，而 PMN 数据集中的 3D 网格是由 CAD 技术制成的。因此，来自 PSB 数据集的 3D 网格具有更加多样化的局部形状。通过提取诸如 NVT 的邻域特征，与自然物体相比，隐写分析器能够更容易地从 CAD 制成的 3D 网格中检测到固定模式，因此，这两个数据集上的性能会有不同程度的提升。



(a) Chao 隐写算法[21]



(b) VND 隐写算法[69]



(c) Li 隐写算法[25]

图 3.8　七种隐写分析特征在 PSB 数据集上的平均检测错误率对比

本文还对隐写分析方法的复杂度进行了分析。如表3.3所示，由于 NVT+ 方法在搜索邻域三角面时复杂度较大，因此，总体而言隐写分析复杂度较大。

3.2.9　统计显著性检验

本节通过假设检验方法中的 z 检验方法，检验 NVT+ 算法安全性提升的显著性。假设表示如下：

$$\boldsymbol{H}_0 : \mu_1 = \mu_2; \qquad \boldsymbol{H}_1 : \mu_1 \neq \mu_2,$$

其中，μ_1 和 μ_2 分别为原始特征和 NVT+ 特征测试误差的平均值。当 $\mu_1 = \mu_2$ 时，这两个特征之间没有显着差异。

z 的计算公式为

$$z = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{\sigma_1}{n_1} + \frac{\sigma_2}{n_2}}},$$

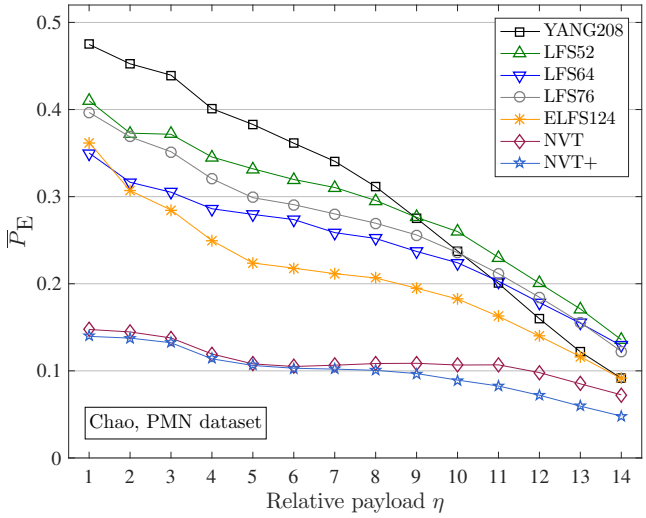
其中 n_1 和 n_2 是测试样本的数量，σ_1 和 σ_2 分别是原始特征检测错误率和 NVT+ 特征检测错误率的标准差。

根据 z 值查表可得到相应的 p 值。p 值较低时，表示原假设 $\boldsymbol{H}_0$ 成立的可能性较低。如果 p 值大于某个阈值，则假设 $\boldsymbol{H}_0$ 被否定，说明隐写分析性能的提升在统计意义上是显著的。

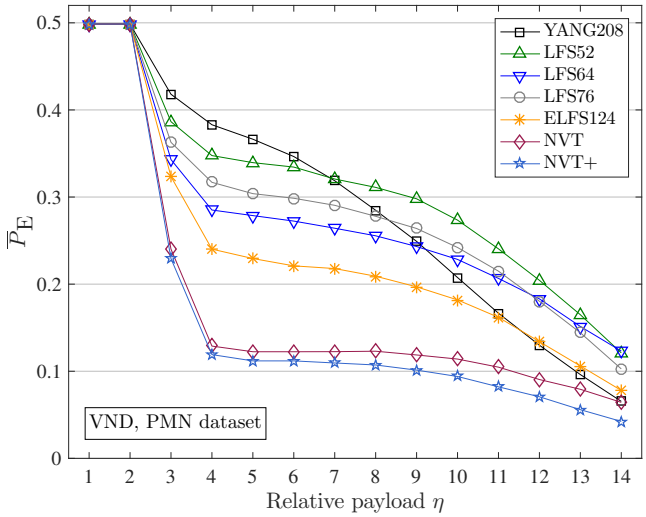
在实验中，显著性水平 z 值设置为 5%。由于经过了多个独立事后统计检验，因此，本文使用邦费罗尼校正（Bonferroni Correction）[71] 来调整阈值。邦费罗尼校正法被称为“最简单粗暴有效”的校正方法，它拒绝了所有的假阳性结果发生的可能性，通过对 p 值的阈值校正来实现消除假阳性以说明具有高度统计意义的虚警率。由于做了 30 次假设，因此，更新的 p 值为 $0.05/30 = 0.0017$，此时相应的分位数 $z_{0.0017} = 2.93$。经过多种不同隐写算法和不同嵌入率下的实验验证，统计量 z 的值远大于相应的分位数 $z_{0.0017}$，因此，NVT+ 隐写分析性能的提升是显著的。

3.2.10　专用隐写分析器的设计

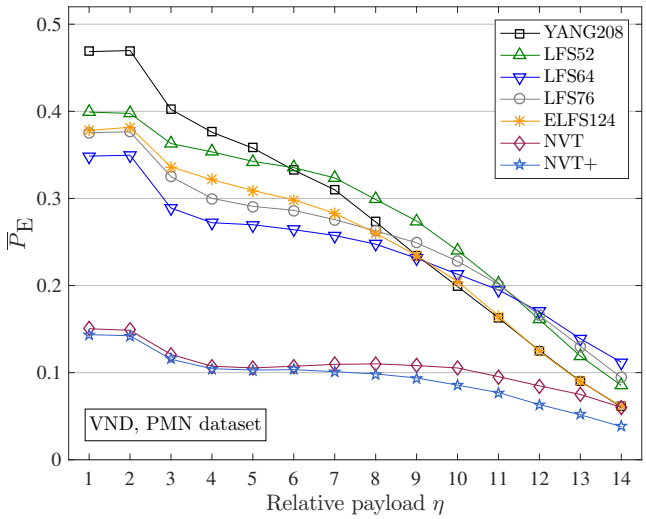
Chao 等人提出的隐写算法[21] 经过 PCA 旋转变换的预处理造成载体 3D 网格和载密 3D 网格的方向位置发生变化，即 3D 载密网格通过 PCA 计算得到的第一和第二主轴的方向分别接近 x 轴和 y 轴方向，因此，这种带有特殊行为的隐写容易引起检测者的怀疑。由于载密 3D 网格经过了人为的旋转处理，因此，再次经过 PCA 变换后几乎没有旋转，即旋转矩阵接近于单位矩阵 $\mathbf{I}$。



(a) Chao 隐写算法[21]



(b) VND 隐写算法[69]



(c) Li 隐写算法[25]

图 3.9　七种隐写分析特征在 PMN 数据集上的平均检测错误率对比

在大多数情况下，载体 3D 网格的旋转矩阵与单位矩阵距离较远。据此，本文设计了一种专用隐写分析检测器，通过一维特征衡量旋转矩阵的变化以实施隐写分析。特征定义为旋转矩阵与单位矩阵的 ℓ_1 距离：

$$f_m = ||\mathbf{T} - \mathbf{I}||_1. \tag{3.13}$$

余弦距离（$\sum_{j=1}^{3} \arccos(\mathbf{T}_j, \mathbf{I}_j)$）和 ℓ_2 距离（$||\mathbf{T} - \mathbf{I}||_2$）也可作为特征，但性能差于 ℓ_1 距离。

本文采用 SVM 的五重交叉验证检测 Chao 等人提出的隐写算法。每个测试重复 10 次，取均值以评估最终性能。具体参数设置为：高斯内核 $k(x, y) = \exp(-\gamma_k \|x - y\|_2^2)$, $\gamma_k > 0$ 的软边距支持向量机，惩罚参数 $C = 5$ 和内核参数 $\gamma_k = 0.5$。

实验结果表明，径向基函数（Radial Basis Function，简称 RBF）支持向量机具有较好的隐写分析检测性能。如图3.10 所示，Chao 方法的平均检测错误率在 PSB 和 PMN 数据集上分别为 0.265 和 0.124，并且不受嵌入率变化的影响，几乎为固定常数；相比而言，VND 方法的检测错误率为 0.5。因此，Chao 算法有缺陷，容易泄漏 3D 网格的空间状态。

表 3.3　五种隐写分析算法复杂度比较

时间（秒）	训练	特征提取	分类
YANG208 [54]	1.99	17.1	17.8
LFS52 [55]	1.27	82.1	7.20
LFS64 [56]	2.19	84.3	9.70
LFS76 [57]	1.94	106	7.13
ELFS124 [58]	2.07	107	16.8
NVT+	2.22	1689	9.45

3.3　基于最小化失真框架的 3D 网格模型隐写

迄今为止，3D 网格模型隐写技术的研究仍然处于起步阶段，目前已有的算法基本通过调制嵌入秘密消息，未考虑拓扑关系对载体的影响。如前所述，在现阶段的 3D 网格模型隐写中的大容量隐写算法研究分支上，研究方法主要为调制

[0]本节内容已于 2019 年 6 月发表在多媒体领域 CCF B 类，SCI 一区国际期刊 IEEE Transactions on Multimedia 上（“Distortion Design for Secure Adaptive 3-D Mesh Steganography”，2019）。

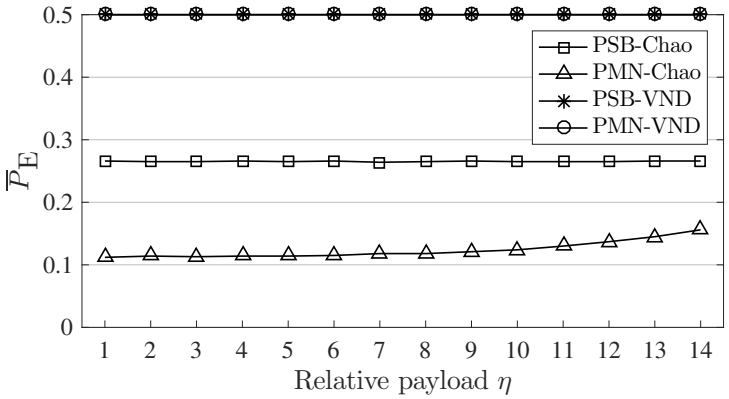


图 3.10　专用隐写分析器检测 Chao 和 VND 的隐写算法的平均检测错误率

坐标点嵌入消息。随着编码理论的发展，一种称之为 STC 的矩阵编码技术广泛应用于自适应隐写中。给定嵌入失真 ρ 和嵌入率，STC 可以接近嵌入效率上界。

在自适应隐写中，最小化嵌入失真隐写是研究热点，可以分解成两个核心问题：第一个问题是如何定义不同载体元素修改造成的嵌入失真，第二个问题是如何使得总体失真最小化。对于第二个问题，采用具有优良编码性能的 STC 码。对于第一个问题，在图像隐写中已经有大量成熟的算法，但是在 3D 网格隐写中尚未有相关的算法。因此，如何定义坐标点的失真，有效地提升隐写算法安全性，是本节研究的主要问题。由于载密网格的坐标点发生了偏移，总体曲面的平滑性有了一定的下降，而目前 3D 网格的隐写分析特征主要来源于检测坐标点或曲面的平滑性，因此，在设计坐标点的失真时，有必要考虑坐标点或曲面的曲率等特征。

然而，3D 网格与灰度图像的差异表明本文不能直接移植失真定义的方式进行自适应隐写。具体原因有以下 3 点：

- 3D 网格的坐标点由小数表示，而灰度图像每个像素点为 8 比特整数。
- 3D 网格坐标点由 xyz 三个分量构成三维数据，而灰度图像只有一维数据。
- 3D 网格的坐标点具有约束条件，即面的拓扑结构，而灰度图像的像素之间没有约束。

因此，这三点原因直接反映 3D 网格模型数据在处理方面更为复杂。

3.3.1　自适应隐写的最小化失真模型

现阶段的自适应隐写可以分为两种框架：最小化失真模型的框架和基于模型的框架。其中，基于模型的框架通过数学建模，将载体和载密图像转化为概率分布的数学模型，使载体修改点选择的问题转化为数学优化问题，通过最小化二

者概率分布的距离，来指导载体的修改，实现秘密消息的嵌入。基于模型的框架具有明确的理论体系，但这类方法的安全性取决于对载体所建立的模型是否合理。然而由于自然载体很难准确地用数学模型刻画，因此，这类方法的安全性受到了一定程度的制约，且算法的复杂度较高。

当前更为有效的方式是基于最小化失真模型的框架，该框架下的算法需要预先对载体元素定义一个失真，这个失真的大小反映了元素被修改时的代价，即对图像某种统计特征的影响。影响越小，则修改代价越小，对应的失真也越小。在定义了所有载体元素的失真后，再选择失真较小的一些元素实施隐写修改，在嵌入秘密消息的同时最小化载体的总失真，因此，该框架被称为最小化失真模型框架，该模型的数学描述如下。

为表达方便，将载体以一维序列表示为 $\mathbf{c}=(c_1,c_2,c_3,...,c_n)$，其中 c_i 为整数。对元素 c_i 的修改操作记为 I_i。本文只讨论隐写中二元嵌入的情况。二元嵌入表示对元素只有不修改和修改这两种操作，因此，有 $|I_i|=2$，且 $I_i=\{c_i,\bar{c}_i\}$。最小化失真隐写模型中，失真是通过载体 $\mathbf{c}$ 修改为载密 $\mathbf{s}=(s_1,s_2,s_3,...,s_n)$ 引入的，载体的总失真可以简记为 $D(\mathbf{c},\mathbf{s})=D(\mathbf{s})$。在隐写算法中，载体 $\mathbf{c}$ 的元素以一定的概率变为 $\mathbf{s}$，记该概率为 $\pi(\mathbf{s})$（包括不修改和修改的概率），则对某个元素 c_i 而言，其承载的信息量可以表示为该点的消息熵。因此，对于整段载体而言，当载体的平均失真为 $E_\pi(D)$ 时，其最多可以承担的消息比特为 $H(\pi)$，且有：

$$H(\pi)=-\sum\pi(\mathbf{s})\log\pi(\mathbf{s}), \tag{3.14}$$

$$E_\pi(D)=\sum\pi(\mathbf{s})D(\mathbf{s}). \tag{3.15}$$

对于一段长度为 L 的载体，隐写者可以通过如下优化问题来最小化总的嵌入失真：

$$\begin{aligned}&\min_{\pi}E_\pi(D)\\&\text{subject to } H(\pi)=L.\end{aligned} \tag{3.16}$$

遵循最大熵原则，在最小化失真模型中，最优的概率分布与失真的对应关系遵循吉布斯分布（Gibbs Distribution）[72]，有如下对应形式：

$$\pi_\lambda(\mathbf{s})=\frac{1}{Z(\lambda)}\exp\left(-\lambda D(\mathbf{s})\right), \tag{3.17}$$

这里 $Z(\lambda)$ 是归一化参数，定义如下：

$$Z(\lambda)=\sum\exp\left(-\lambda D(\mathbf{s})\right), \tag{3.18}$$

其中 λ 是一个嵌入率相关的尺度因子，有 $\lambda>0$。在实际的隐写过程中，λ 是随 $H(\pi)$ 单调递减的，即总消息长度增加时，求得的 λ 结果会相应地减少。对于一个给定的消息长度 L，可以通过二元查找确定 λ 的取值。

当每个像素的修改操作相互独立时，由 **c** 修改为 **s** 引入的失真可以看作是加性的，有 $D(\mathbf{s}) = \sum_i^n \rho_i(s_i)$，这里 $\rho_i(s_i)$ 表示将 c_i 改为 s_i 时的修改代价。因此，公式 (3.17) 可以写成单个元素的形式：

$$\pi_{(s_i)} = \frac{\exp\left(-\lambda\rho_i(s_i)\right)}{\sum_{s_i \in I_i} \exp\left(-\lambda\rho_i(s_i)\right)}, 1 \leq i \leq n. \tag{3.19}$$

当 λ 在 $(0, +\inf)$ 内变化时，可以得到一条 $H(\pi)$ 和 $E_\pi(D)$ 之间的关系曲线，称为率失真曲线[72]，该曲线是隐写过程中最小化失真能够达到的理论界。在实际隐写中，隐写编码可以在率失真曲线下用定义好的失真执行消息嵌入，其中当前最先进的隐写编码 STC[18] 能够逼近率失真曲线的理论界。此时，嵌入和提取的过程分别表示为：

$$\mathrm{Emb}_{\mathrm{STC}}(\mathbf{c}, \mathbf{p}, \mathbf{m}) = \arg \min_{\mathbf{s} \in coset(\mathbf{m})} D(\mathbf{c}, \mathbf{s}), \tag{3.20}$$

$$\mathrm{Ext}_{\mathrm{STC}}(\mathbf{s}) = \mathbf{s}\mathbf{H}_{\mathrm{STC}}^T = \mathbf{m}, \tag{3.21}$$

其中 $\mathbf{p} = (\rho_1, \rho_2, \ldots, \rho_N)$ 为失真向量，$coset(\mathbf{m})$ 是校验子 **m** 的陪集，$\mathbf{H}_{\mathrm{STC}} \in \{0,1\}^{R \times N}$ 是发送方和接收方共享的校验矩阵。STC 算法具体细节见参考文献[18]。

3.3.2　3D 网格结构分解

3D 网格模型的非压缩表达形式中，通常每个顶点坐标为 32 位 IEEE 754 单精度标准格式，而且有效精度数为 23 位（约 7 位十进制数字[21]）。顶点坐标分量的小数表示也可转换为二进制表示[73]，例如 x 分量表示为：$\mathbf{b}_{i,x} = [b_{i,x}^1, b_{i,x}^2, ..., b_{i,x}^L]^T$，其中位平面有 $L = 31$ 层。因此，第 l 层位平面上的 x 分量表示为 $\mathbf{c}_x^l = [b_{1,x}^l, b_{2,x}^l, ..., b_{N,x}^l]^T$。记 r^l 为第 l 层位平面的残差，位平面 $v_{i,x}$ 的二进制比特由下式迭代得到：

$$\begin{aligned} b_{i,x}^l &= \lfloor 2r^{l+1} \rfloor, \\ r^l &= 2r^{l+1} - \lfloor 2r^{l+1} \rfloor. \end{aligned} \tag{3.22}$$

其中，迭代起始条件为 $r^{L+1} = v_{i,x}$，有 $l = L$。

3.3.3　从隐写分析特征到隐写算法的设计

本节将分析不同隐写分析特征对 3D 载体和载密对的检测性能。

正如“木桶理论”所揭示的，木桶的容量取决于最短的木板。同样地，对于集成分类器检测隐写算法而言，隐写的安全性能主要取决于最有效的隐写分析特征。由于无法直接得到哪个隐写分析子特征是最有效的分类特征，因此，很难

通过隐写分析特征构造失真函数并给予每个 3D 坐标修改代价 ρ_i，从而设计隐写算法。假设赋予每个载体元素相同的修改代价，并采用 STC 编码嵌入消息得到载体载密对。在此基础上，便可公平地比较哪些隐写分析特征能够有效区分载体载密网格。本文采用 Jessica 和 Soukal[74] 提出的基于常数失真的矩阵嵌入隐写方法进行隐写得到载密 3D 网格。Filler 等人[18] 提到，矩阵嵌入方法旨在最小化修改元素的数量。随后，单独训练每个隐写分析子特征模型分类器，并对分类结果排序，找到最优的隐写分析分类子特征。

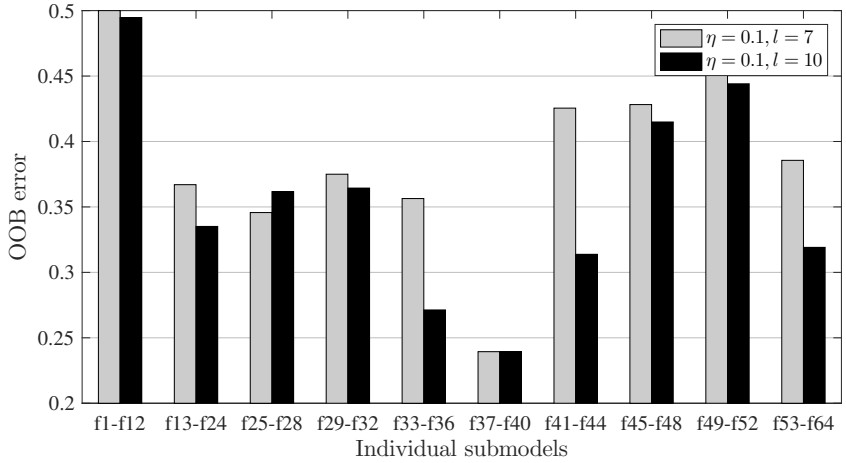


图 3.11　采用矩阵嵌入算法的袋外检测错误率

在实验中，隐写分析与第3.2.7节的过程类似，具体方法如下。首先，采用矩阵嵌入隐写方法，在相同嵌入率下隐写得到载密 3D 网格。然后，抽取隐写分析特征。然后，采用 Fisher 线性判决器来评估各个隐写分析特征的判决能力。最后，得到的分类结果能够间接地指导隐写算法中失真函数的设计。

如图3.11所示，嵌入率为 0.1 bpv，对第 7 层和第 10 层采用常数失真隐写算法得到载密 3D 网格，并计算不同子特征模型的袋外错误率，以观察不同嵌入层位置下最优的隐写分析子模型仍否是最优的。实验证明，子特征“f37-f40”（即三角面法向量偏移度）在两种嵌入强度下，始终是最优的隐写分析特征，因此，需要针对这种特征设计隐写失真函数来抵御它的检测。图3.11还表明，高层位平面的隐写更容易被隐写分析方法检测到。据此分析，下一节将介绍如何设计失真函数。

3.3.4　失真函数构造

本节主要介绍了两种失真函数的设计。

1）基于坐标点法向量的失真函数

如图3.11所示，本文分析了不同隐写分析子特征作用于载体和载密 3D 模型

上的检测错误率之后，发现基于顶点法向量的隐写分析特征（f37-f40）对载体和载密的分类性能最好，即隐写前后坐标点法向量的偏移量最为明显。因此，为了对抗基于坐标点法向量的隐写分析，需要设计基于坐标点法向量的隐写分析特征的失真函数。

为了计算顶点法向量在拉普拉斯平滑后的变化情况，本文采用 Nelson 等人[75]定义的多边形近似的顶点法向量（包含该顶点的面的法向量的加权总和）指导失真函数的定义。定义顶点法向量为

$$\overrightarrow{N}_{v_i} = \sum_{F_j \in F_{v_i}} \frac{S_j^{(i)} \cdot \overrightarrow{N}_{F_j'}}{||e_{(v_i, v'_{F_j})}|| \cdot ||e_{(v_i, v''_{F_j})}||}, \tag{3.23}$$

其中，F_{v_i} 是包含顶点 v_i 的三角面集合，顶点 v'_{F_j} 和顶点 v''_{F_j} 是顶点 v_i 在 F_j 中相邻的两个顶点，$e_{(v_1,v_2)}$ 是连接顶点 v_1 和顶点 v_2 的边，$S_j^{(i)}$ 是包含顶点 v_i 的三角形面积，如图3.12所示。三角形面积定义为

$$S_j^{(i)} = \sqrt{q_j^{(i)} \left(q_j^{(i)} - e_j^{(i)}\right) \left(q_j^{(i)} - e_{j+1}^{(i)}\right) \left(q_j^{(i)} - p_j^{(i)}\right)}, \tag{3.24}$$

其中，半周长定义为

$$q_j^{(i)} = \left(e_j^{(i)} + e_{j+1}^{(i)} + p_j^{(i)}\right)/2. \tag{3.25}$$

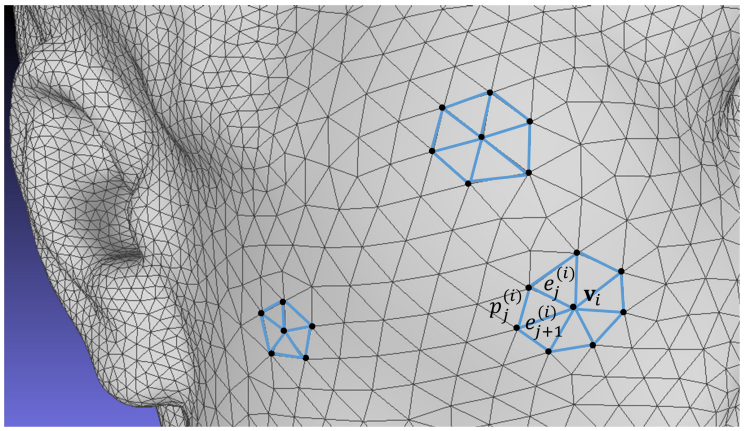


图 3.12　笛卡尔坐标系下，三角面片的一环邻域示意图

接下来，本文设计基于顶点法向量构造失真函数，以对抗目标隐写分析特征的检测。失真（代价）函数 ρ_i 定义为载体 3D 网格和拉普拉斯平滑后的 3D 网格之间顶点法向量的 ℓ_2 范数绝对值的倒数，并具有如下形式：

$$\rho_i = \frac{1}{\mathrm{g}(||\overrightarrow{N}_{v_i} - \overrightarrow{N}_{v_i'}||_2 + 1) + \sigma}. \qquad 1 \le i \le N \tag{3.26}$$

其中，$\mathrm{g}(x)$ 是某一用于提高隐写性能的单调映射函数，参数 σ 为偏置项。

在失真函数中，坐标点的嵌入失真代价由顶点法向量决定。对于拉普拉斯平滑前后变化不大（变化前后的顶点法向量的二范数距离较小）的顶点，局部区域

比较平滑，定义较大的失真；反之，对于复杂的局部区域，则定义较小的失真。为方便起见，本方法简称为顶点法向量失真算法（Vertex Normal Distortion，简称 VND）。

2）基于高斯曲率的失真函数

为了辩证地说明失真函数设计的重要性，本文还设计了一种次优的隐写失真函数。一般来说，曲率能够有效地反映 3D 网格模型曲面的平滑程度。已有文献表明，3D 网格顶点的离散高斯曲率与该局部区域中连接到顶点的三角面的夹角有关。如图3.12所示，局部顶点的锐度由亏损角度 $\Delta(v_i)$ 近似：

$$\Delta(v_i) = 2\pi - \sum_{j=1}^{E} \theta_j^{(i)}, \tag{3.27}$$

其中，E 是坐标点的相邻三角形的数量，$\theta_j^{(i)}$ 是第 i 个顶点上的两个连续边 $e_j^{(i)}$ 和 $e_{j+1}^{(i)}$ 之间的夹角，表示为

$$\theta_j^{(i)} = \arccos\left[\frac{\left(e_j^{(i)}\right)^2 + \left(e_{j+1}^{(i)}\right)^2 - \left(p_j^{(i)}\right)^2}{2e_j^{(i)}e_{j+1}^{(i)}}\right], \qquad 1 \le j \le E \tag{3.28}$$

其中，$p_j^{(i)}$ 是该角度的对边，且有 $e_1^{(i)} = e_{E+1}^{(i)}$，$1 \le i \le N$。

假设曲率在顶点周围均匀分布，则离散高斯曲率定义为

$$K(\mathbf{v}_i) = \frac{\Delta(\mathbf{v}_i)}{\sum_{j=1}^{E} S_j^{(i)}/3}. \tag{3.29}$$

直观地讲，如果失真函数足够精细，那么复杂区域中能够嵌入相对更多的秘密消息，此时隐写分析器更加难以对局部区域建模或预测残差。也就是说，在设计失真函数时，可以增大复杂区域的修改概率，即赋予较小的代价值。据此，本文设计了如下基于离散高斯曲率的失真函数：

$$\rho_i' = \frac{1}{|K(\mathbf{v}_i)|^{\alpha} + \sigma}, \qquad 1 \le i \le N \tag{3.30}$$

其中 α 是超参数。为方便起见，本方法称为高斯曲率失真算法（Gaussian Curvature Distortion，简称 GCD）。

3.3.5　嵌入策略

为了合理地实施 3D 网格的隐写，本文借鉴了图像隐写中的 LSB 嵌入技术，并将顶点坐标转换为多个位平面以嵌入秘密消息。鉴于将数据嵌入至较低位平面对整体顶点坐标的影响更小，考虑先将秘密消息嵌入至较低的位平面上，然后

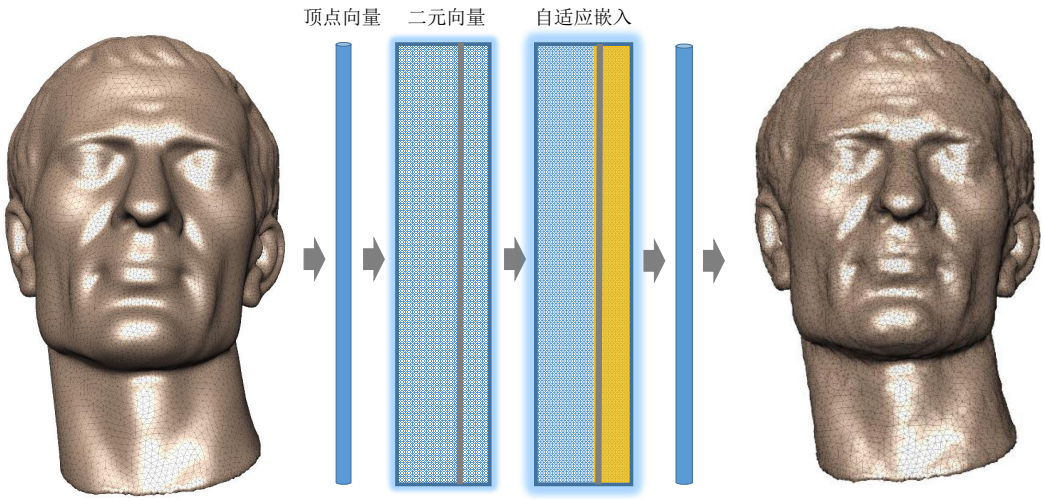


图 3.13　本文自适应隐写方法对“雕塑”模型实施隐写的示意图

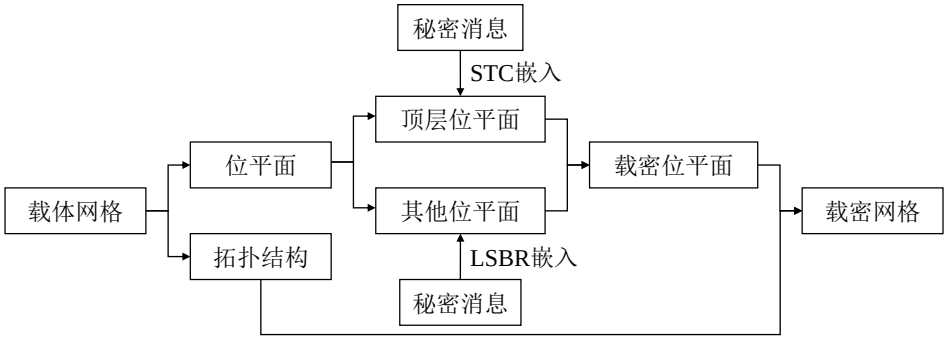


图 3.14　本文自适应隐写方法的流程图

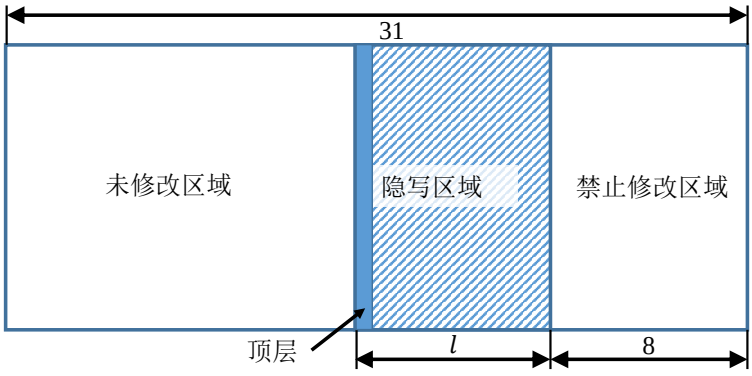


图 3.15　3D 网格未修改区域、隐写区域和禁止修改区域的示意图

再迭代地嵌入到较高的位平面上。由于本文的方法直接在位平面上嵌入秘密消息，因此，能够避免无效区域的修改。图3.13是 3D 隐写的示意图，图3.14是本方法的流程框图。

如图3.15所示，3D 网格上的操作区域由未修改区域、隐写区域和禁止修改区域构成。禁止修改区域包含全为 0 的 8 个位平面，因为一旦对其做了修改，容易被专用型隐写分析检测器检测到。由于较低位平面的修改幅度小于较高位平

Input: 含 N 个坐标点的载体 3D 网格 **X**; 总嵌入消息比特数为 m 比特，嵌入率为 $\eta = m/N$。

Output: 载密 3D 网格 **Y**。

1 获得载体坐标序列 $\mathcal{V} = \{\mathbf{v}_i\}_{i=0}^{N}$ 的位平面（x，y 和 z 轴分量）;
2 计算最高消息嵌入平面的层 l;
3 采用失真函数公式(3.26)获得每个坐标的失真 $\rho_i, i = 1, 2, \ldots, N$;
4 采用失真分配策略赋予每个位平面 $\mathbf{c}_x^l$，$\mathbf{c}_y^l$ 和 $\mathbf{c}_z^l$ 对应的失真向量;
5 根据已有的失真向量，采用 STC 编码将 m_l 的消息嵌入到载体位平面中，并得到载密 3D 网格坐标的位平面 $\mathbf{s}_x^l$，$\mathbf{s}_y^l$ 和 $\mathbf{s}_z^l$;
6 **for** $j = l - 1$ **to** 1 **do**
7 　采用 LSBR 嵌入算法，将 N 比特长的消息嵌入到载体位平面上，并得到载密位平面 $\mathbf{s}_x^j$，$\mathbf{s}_y^j$ 和 $\mathbf{s}_z^j$;
8 **end**
9 重构并输出载密 3D 网格的顶点坐标序列 $\mathcal{V}_s$;
10 整合顶点序列 $\mathcal{V}_s$ 和其他 3D 网格结构，最终得到载密 3D 网格 **Y**。

算法 3.1: 最小化失真框架的 3D 网格模型隐写算法

面的修改幅度，因此，本文优先考虑将消息嵌入较低层。隐写区域和未修改区域按实际消息长度分段进行消息嵌入。

根据待嵌入的消息比特数 m 和顶点个数 N 计算可嵌入的位平面数 l，并计算最高层待嵌入消息长度 $m' = m - N\lceil \frac{m}{N} \rceil$。在隐写区域中，对最高层采用上述失真函数实施 STC 编码嵌入；而在其余位平面上，采用最低位平面替换（Least Significant Bit Replacement，简称 LSBR）算法嵌入消息。

如前所述，在加性失真模型中，假定对元素的修改是独立的，因此，总代价最小化等价于使各个已修改元素的代价的总和最小。在加性失真规则下，采用一种最简单的失真分配算法，即对坐标三元组的元素（x 轴，y 轴和 z 轴分量）分别赋予相同的代价值：

$$\begin{aligned} \rho^{(i)}(x) &= \rho_i, \\ \rho^{(i)}(y) &= \rho_i, \\ \rho^{(i)}(z) &= \rho_i. \end{aligned} \tag{3.31}$$

因此，3D 网格坐标的每个分量各自单独采用 STC 编码嵌入消息，并不相互影响。得到载密位平面 s_x^j, s_y^j, s_z^j，并整合载密位平面得到载密坐标序列 V'，然后与面集合 F 编码成载密 3D 网格模型 Y。

为了阐明本文提出的 3D 隐写算法，本文提供了如算法 3.1 所示的伪代码。

表 3.4　单层嵌入下不同映射函数 g(x) 的平均检测错误率

模型	函数 g(x)	平均检测错误率 $\overline{P}_{\mathrm{E}}$
线性函数	x	.4388 ± .0203
平方根函数	$\sqrt{x}$	.4415 ± .0209
指数函数	$\exp(x)$	.4016 ± .0176
对数函数	$\ln(x+1)$	.4468 ± .0205

3.3.6　映射函数 g(x) 的确定

公式(3.26)中的映射函数 g(x) 有两个重要属性：

- g(x) 的值域为 $[0,+\infty)$。由于代价值不能小于 0，因此，g(x) 的值必须为非负数。

- g(x) 单调递增。在 VND 的规则中，由公式(3.26)计算得到较大的值对应于隐写分析特征敏感的坐标点；而值越小，则这些坐标点更适合修改。因此，g(x) 单调递增。

因此，本文考虑了几种单调函数以设计最优的隐写失真函数：线性模型、指数模型、对数模型和平方根模型。如表3.4所示，对数模型对应的隐写分析平均检测错误率 $\overline{P}_{\mathrm{E}}$ 相较于其他模型更高，因此，对数模型作为公式(3.26)中的单调函数：

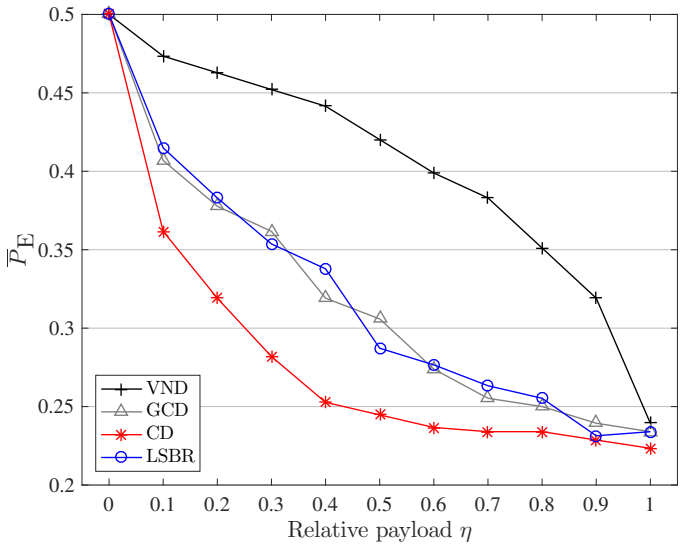
$$\rho_i = \frac{1}{\ln(||\overrightarrow{N}_{\mathbf{v}_i} - \overrightarrow{N}_{\mathbf{v}_i'}||_2 + 1) + \sigma}. \qquad i = 1, 2, \ldots, N \tag{3.32}$$

3.3.7　单层位平面隐写的性能比较

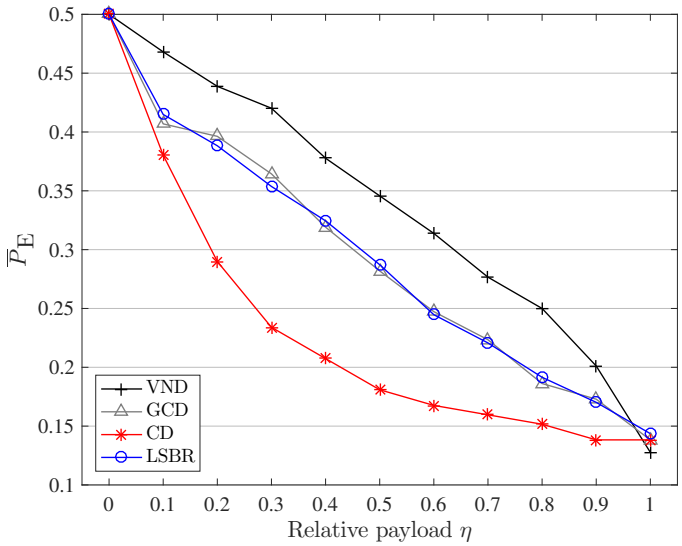
为了验证 VND 方法的有效性，本文采用不同的隐写方法，分别在单个位平面上嵌入秘密消息得到载密 3D 网格，然后采用常用的隐写分析算法比较隐写安全性。图3.16(a) 和图3.16(b) 分别为第 7 层和第 12 层平面上采用不同隐写失真函数进行隐写，由 LFS64 隐写分析器检测的隐写安全性实验。隐写算法分别为基于高斯曲率的自适应算法（GCD）、常数失真隐写算法（Constant Distortion，简称 CD）和 LSB 替换算法（LSBR）。公式(3.29)的尺度因子 α 已经过最优搜索，并在 $\alpha = 1$ 时达到最优。

图中，所有曲线两端的平均检测错误率几乎相同。这是因为在左端点上，嵌入率过低导致所有隐写算法的平均检测错误率均接近 50%。在右端点上，满嵌入率时所有自适应隐写算法均退化为非自适应隐写算法，即直接根据消息比特

值替换载体比特值。值得注意的是，单层隐写（第 $l = 7$ 层）时，VND 相较于 LSBR 算法的抗检测性的最大提升为 17%。单层隐写的实验结果表明，本文提出的 VND 算法有安全性的提升。这两个图的曲线有相似的变化趋势，而且在更高比特平面上采用 VND 隐写算法的抗检测能力的提升略弱于低比特平面上抗检测能力的提升。



(a) 单层位平面嵌入 $l = 7$



(b) 单层位平面嵌入 $l = 12$

图 3.16　LFS64 隐写分析特征的检测错误率

3.3.8　不同数据库的抗检测性能比较

早期的 3D 网格隐写方法[19,20,76]通过简单的顶点调制来嵌入秘密消息，消息嵌入容量较低，因此，不考虑安全性能的比较。近年来，有了一批大容量隐写算法[21,23,25]。下文将比较本文提出的 VND 算法与已有隐写算法的性能。

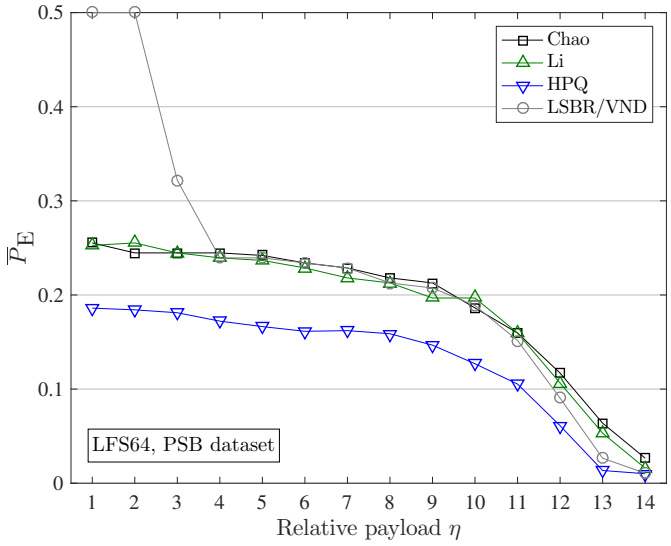
为了评估采用 LSBR 和 VND 算法的嵌入策略在多大程度上能够提升隐写算法的安全性，图3.17和图3.18分别给出了在 PSB 和 PMN 数据集上相比于采用 Chao[21]，Li[25] 和 HPQ[23] 隐写算法的抗隐写分析检测的结果。隐写分析方法采用 LFS64 和 LFS76。实验结果表明，顶层位平面上满嵌入时，LSBR 和 VND 算法的性能是相同的。这四个曲线图说明，LSBR 和 VND 算法的隐写安全性随着嵌入率的提高而明显下降，而 Chao、Li 和 HPQ 隐写算法安全性的降低则是缓慢的，并且在小嵌入率下安全性较低。当嵌入率大于 13 bpv 时，Chao 算法的安全性超过了 LSBR 和 VND 算法的安全性。这是由于 Chao 算法需要预处理 3D 网格，通过 PCA 旋转 3D 网格，主成分方向的分量具有了最大的方差，而其他维度分量的方差较小。因此，隐写修改对 3D 网格在隐写分析特征上影响较低，抗检测性更好。然而，Chao 算法在预处理后会泄漏位置信息，容易受到专用隐写分析器的检测，如前文第3.2.10节所述。图3.17和图3.18中平均检测错误率 $\overline{P}_{\mathrm{E}}$ 的数值结果在表3.5和表3.6中给出。

表 3.5　PSB 数据集下，VND 隐写算法抵抗隐写分析检测器的安全性结果

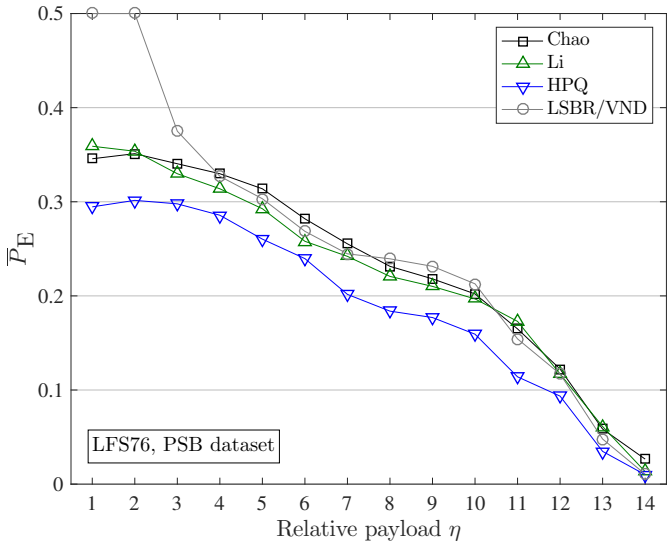
检测器	隐写方法	1	2	3	4	5	6	7
LFS64	Chao	.2553 ± .0229	.2447 ± .0235	.2447 ± .0224	.2447 ± .0224	.2420 ± .0210	.2340 ± .0239	.2287 ± .0227
	Li	.2527 ± .0248	.2553 ± .0228	.2447 ± .0219	.2394 ± .0199	.2367 ± .0202	.2287 ± .0212	.2181 ± .0249
	HPQ	.1860 ± .0211	.1842 ± .0212	.1811 ± .0214	.1722 ± .0231	.1664 ± .0231	.1614 ± .0228	.1621 ± .0217
	LSBR/VND	.5080 ± .0358	.5080 ± .0358	.3218 ± .0231	.2394 ± .0214	.2394 ± .0196	.2340 ± .0174	.2287 ± .0230
LFS76	Chao	.3457 ± .0220	.3511 ± .0212	.3404 ± .0226	.3298 ± .0198	.3138 ± .0189	.2819 ± .0239	.2553 ± .0233
	Li	.3590 ± .0222	.3537 ± .0246	.3298 ± .0190	.3138 ± .0169	.2926 ± .0227	.2580 ± .0229	.2420 ± .0255
	HPQ	.2946 ± .0315	.3015 ± .0318	.2978 ± .0241	.2857 ± .0174	.2603 ± .0111	.2396 ± .0184	.2016 ± .0201
	LSBR/VND	.5080 ± .0358	.5080 ± .0358	.3617 ± .0200	.3245 ± .0163	.2872 ± .0174	.2686 ± .0199	.2247 ± .0238
检测器	隐写方法	8	9	10	11	12	13	14
LFS64	Chao	.2181 ± .0213	.2128 ± .0218	.1862 ± .0223	.1596 ± .0183	.1170 ± .0197	.0638 ± .0163	.0266 ± .0092
	Li	.2128 ± .0193	.1968 ± .0201	.1968 ± .0252	.1596 ± .0158	.1064 ± .0169	.0532 ± .0147	.0160 ± .0078
	HPQ	.1588 ± .0221	.1467 ± .0211	.1269 ± .0202	.1053 ± .0121	.0611 ± .0111	.0135 ± .0142	.0101 ± .0015
	LSBR/VND	.2128 ± .0227	.2074 ± .0203	.1888 ± .0231	.1516 ± .0136	.0904 ± .0135	.0266 ± .0160	.0106 ± .0048
LFS76	Chao	.2314 ± .0256	.2181 ± .0255	.2021 ± .0216	.1649 ± .0204	.1223 ± .0202	.0585 ± .0173	.0266 ± .0127
	Li	.2207 ± .0214	.2101 ± .0274	.1968 ± .0210	.1729 ± .0179	.1170 ± .0179	.0612 ± .0156	.0133 ± .0064
	HPQ	.1838 ± .0261	.1770 ± .0174	.1593 ± .0174	.1140 ± .0141	.0935 ± .0148	.0348 ± .0157	.0100 ± .0041
	LSBR/VND	.2394 ± .0254	.2314 ± .0192	.2128 ± .0198	.1543 ± .0172	.0904 ± .0188	.0319 ± .0117	.0106 ± .0047

图3.19和图3.20分别是 PSB 和 PMN 数据集上隐写算法的对比实验。如图所示，本文提出的 VND 的隐写安全性比其他算法更优，而且曲线趋势与图3.16相同。唯一不同之处是 VND 隐写方法相比于单层嵌入的隐写算法提升更弱。

本文还对多种隐写方法的复杂度进行了分析。实验环境为：Windows 10，MATLAB R2017b，服务器 Intel Xeon CPU E7-4820，32 GB RAM。如图3.22所示，复杂度排序为 HPQ>VND>Chao≈Li。实验结果表明，HPQ 算法的复杂度最高，这是由于该算法中查找汉密尔顿路径的步骤较为耗时。Chao 算法和 VND 算



(a) LFS64 隐写分析特征



(b) LFS76 隐写分析特征

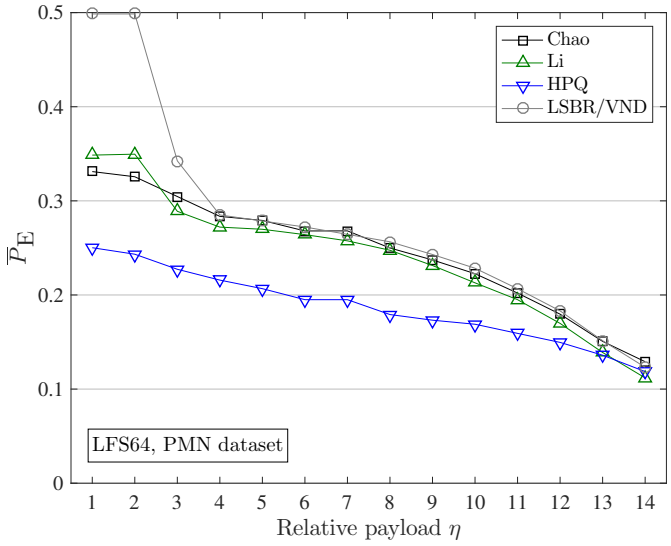
图 3.17　PSB 数据集下，不同整数倍嵌入率的平均检测率

法在整数嵌入率下复杂度接近，在非整数嵌入率下,VND 算法复杂度稍高些，这是由计算每个坐标点的代价值所产生的计算量。

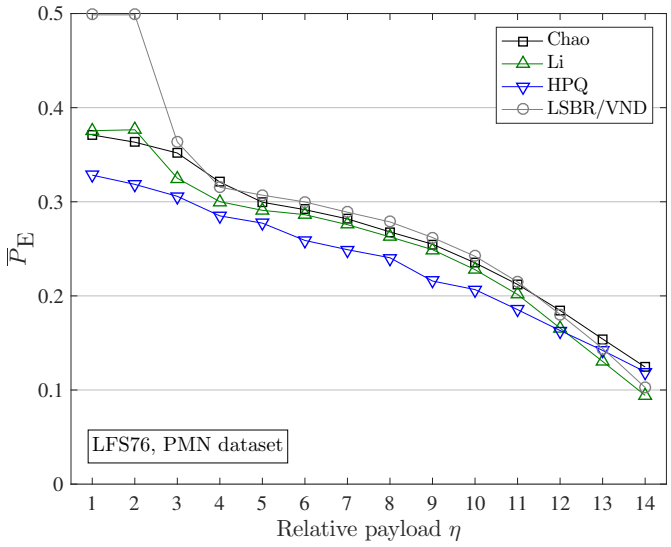
统计显著性检验。本节采用与第3.2.9节相同的 z 检验以证明 VND 算法的显著性。假设定义为：

$$\boldsymbol{H}_0 : \mu_1 = \mu_2; \qquad \boldsymbol{H}_1 : \mu_1 \neq \mu_2,$$

其中 μ_1 和 μ_2 分别为 VND 算法经过隐写分析特征检测和 LSBR 算法经过隐写分析特征检测的平均检测错误率。$\mu_1 = \mu_2$ 表示两者的均值之间没有显著的差异。z



(a) LFS64 隐写分析特征



(b) LFS76 隐写分析特征

图 3.18　PMN 数据集下，不同整数倍嵌入率的平均检测率

值定义为：

$$z = \frac{|\mu_1 - \mu_2|}{\sqrt{\frac{\sigma_1}{n_1} + \frac{\sigma_2}{n_2}}},$$

其中 n_1 和 n_2 分别为测试样本数量，σ_1 和 σ_2 为各自的方差。

根据 z 值可查表得到 p 值。p 值较低表示原假设 $\boldsymbol{H}_0$ 成立的可能性较低。如果 p 值大于某个阈值，则假设 $\boldsymbol{H}_0$ 被否定，并且说明性能的提升在统计意义上是显著的。实验中，显着性水平 z 设置为 5%。

图3.19中，$\overline{P}_E$ 的实验结果对应表3.7和表3.8；图3.20中，$\overline{P}_E$ 的实验结果对应表3.9和表3.10。粗体表示 VND 隐写算法相比于 LSBR 隐写算法性能的提升是显

表 3.6　PMN 数据集下，VND 隐写算法抵抗隐写分析检测器的安全性结果

检测器	隐写方法	1	2	3	4	5	6	7
LFS64	Chao	.3311 ± .0052	.3256 ± .0052	.3046 ± .0058	.2835 ± .0055	.2792 ± .0049	.2680 ± .0058	.2681 ± .0056
	Li	.3486 ± .0058	.3496 ± .0056	.2889 ± .0056	.2721 ± .0057	.2698 ± .0057	.2641 ± .0056	.2575 ± .0054
	HPQ	.2502 ± .0081	.2433 ± .0079	.2273 ± .0035	.2158 ± .0061	.2067 ± .0039	.1950 ± .0041	.1950 ± .0048
	LSBR/VND	.4986 ± .0083	.4986 ± .0083	.3425 ± .0041	.2850 ± .0053	.2786 ± .0040	.2722 ± .0044	.2644 ± .0050
LFS76	Chao	.3710 ± .0050	.3633 ± .0053	.3518 ± .0052	.3209 ± .0047	.2995 ± .0043	.2916 ± .0052	.2818 ± .0052
	Li	.3755 ± .0048	.3765 ± .0050	.3250 ± .0049	.3001 ± .0051	.2909 ± .0050	.2863 ± .0065	.2757 ± .0071
	HPQ	.3283 ± .0082	.3185 ± .0082	.3058 ± .0037	.2850 ± .0035	.2773 ± .0043	.2589 ± .0052	.2491 ± .0060
	LSBR/VND	.4986 ± .0082	.4986 ± .0082	.3635 ± .0037	.3155 ± .0035	.3070 ± .0043	.2998 ± .0052	.2889 ± .0060
检测器	隐写方法	8	9	10	11	12	13	14
LFS64	Chao	.2499 ± .0061	.2372 ± .0055	.2226 ± .0069	.2020 ± .0067	.1796 ± .0075	.1507 ± .0067	.1291 ± .0064
	Li	.2475 ± .0060	.2313 ± .0060	.2129 ± .0059	.1950 ± .0051	.1698 ± .0051	.1389 ± .0045	.1119 ± .0034
	HPQ	.1792 ± .0042	.1732 ± .0055	.1689 ± .0051	.1592 ± .0053	.1496 ± .0045	.1360 ± .0040	.1186 ± .0031
	LSBR/VND	.2565 ± .0051	.2430 ± .0068	.2284 ± .0057	.2066 ± .0058	.1831 ± .0042	.1514 ± .0041	.1232 ± .0036
LFS76	Chao	.2680 ± .0063	.2549 ± .0068	.2351 ± .0076	.2122 ± .0062	.1845 ± .0064	.1542 ± .0061	.1244 ± .0056
	Li	.2627 ± .0062	.2491 ± .0078	.2279 ± .0071	.2015 ± .0056	.1658 ± .0042	.1303 ± .0033	.0943 ± .0038
	HPQ	.2405 ± .0064	.2158 ± .0065	.2067 ± .0065	.1854 ± .0054	.1632 ± .0046	.1421 ± .0036	.1193 ± .0037
	LSBR/VND	.2786 ± .0074	.2620 ± .0069	.2421 ± .0067	.2149 ± .0059	.1804 ± .0042	.1442 ± .0032	.1027 ± .0034

表 3.7　PSB 数据集下，嵌入第 7 层时 VND 隐写算法抵抗隐写分析检测器的安全性结果

检测器	隐写方法	0	0.1	0.2	0.3	0.4	0.5
LFS64	LSBR	.2287 ± .0197	.2314 ± .0212	.2314 ± .0208	.2314 ± .0251	.2261 ± .0247	.2287 ± .0262
	VND	.2340 ± .0201	.2340 ± .0201	.2314 ± .0197	.2287 ± .0243	.2287 ± .0240	.2314 ± .0230
LFS76	LSBR	.2660 ± .0245	.2713 ± .0203	.2633 ± .0253	.2606 ± .0224	.2553 ± .0191	.2553 ± .0262
	VND	.2713 ± .0215	.2660 ± .0197	.2660 ± .0238	.2606 ± .0221	**.2686 ± .0240**	.2606 ± .0217
检测器	隐写方法	0.6	0.7	0.8	0.9	1.0	
LFS64	LSBR	.2340 ± .0213	.2261 ± .0189	.2287 ± .0241	.2234 ± .0223	.2234 ± .0195	
	VND	.2340 ± .0182	.2287 ± .0218	.2287 ± .0269	.2314 ± .0243	.2340 ± .0266	
LFS76	LSBR	.2500 ± .0252	.2500 ± .0223	.2500 ± .0227	.2527 ± .0227	.2394 ± .0255	
	VND	.2606 ± .0237	.2580 ± .0238	**.2660 ± .0272**	.2553 ± .0254	.2500 ± .0232	

表 3.8　PSB 数据集下，嵌入第 12 层时 VND 隐写算法抵抗隐写分析检测器的安全性结果

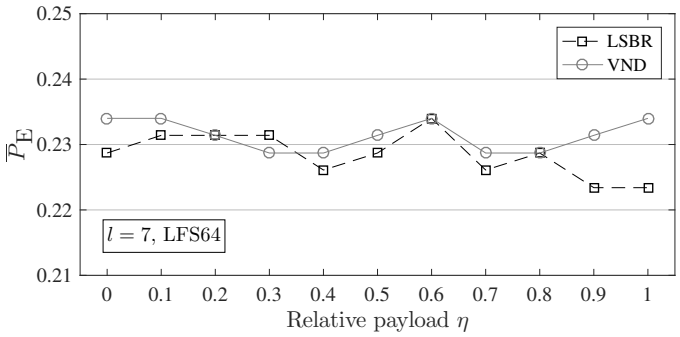
检测器	隐写方法	0	0.1	0.2	0.3	0.4	0.5
LFS64	LSBR	.1516 ± .0233	.1489 ± .0203	.1436 ± .0157	.1356 ± .0221	.1277 ± .0169	.1277 ± .0154
	VND	.1463 ± .0156	.1436 ± .0187	.1463 ± .0164	**.1516 ± .0191**	**.1436 ± .0198**	**.1383 ± .0183**
LFS76	LSBR	.1516 ± .0217	.1569 ± .0246	.1543 ± .0191	.1436 ± .0241	.1383 ± .0207	.1330 ± .0187
	VND	.1602 ± .0176	.1569 ± .0202	.1543 ± .0223	**.1569 ± .0260**	**.1489 ± .0197**	**.1436 ± .0228**
检测器	隐写方法	0.6	0.7	0.8	0.9	1.0	
LFS64	LSBR	.1223 ± .0205	.1117 ± .0170	.1170 ± .0196	.1064 ± .0175	.1117 ± .0157	
	VND	.1303 ± .0171	**.1277 ± .0185**	.1223 ± .0128	**.1223 ± .0199**	.1117 ± .0171	
LFS76	LSBR	.1277 ± .0194	.1277 ± .0171	.1170 ± .0192	.1170 ± .0181	.1223 ± .0189	
	VND	**.1383 ± .0211**	.1330 ± .0238	**.1383 ± .0192**	**.1330 ± .0170**	.1170 ± .0177	

表 3.9　PMN 数据集下，嵌入第 7 层时 VND 隐写算法抵抗隐写分析检测器的安全性结果

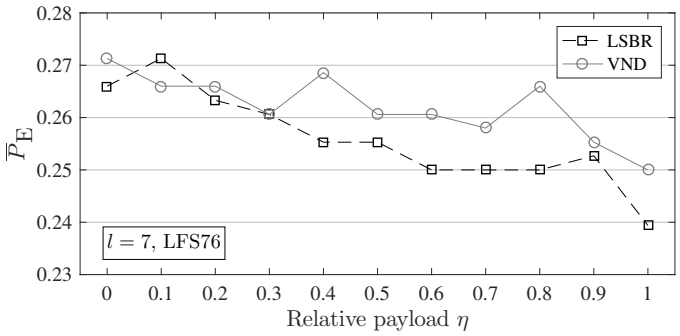
检测器	隐写方法	0	0.1	0.2	0.3	0.4	0.5
LFS64	LSBR	.2820 ± .0052	.2761 ± .0045	.2731 ± .0058	.2705 ± .0048	.2689 ± .0048	.2677 ± .0043
	VND	.2824 ± .0045	**.2833 ± .0049**	**.2786 ± .0042**	**.2739 ± .0053**	**.2724 ± .0043**	**.2721 ± .0043**
LFS76	LSBR	.3076 ± .0053	.3021 ± .0051	.3000 ± .0067	.2975 ± .0054	.2959 ± .0065	.2954 ± .0049
	VND	.3077 ± .0049	.3044 ± .0046	**.3043 ± .0047**	**.3038 ± .0050**	**.3010 ± .0054**	**.2995 ± .0056**
检测器	隐写方法	0.6	0.7	0.8	0.9	1.0	
LFS64	LSBR	.2674 ± .0055	.2660 ± .0050	.2654 ± .0055	.2644 ± .0041	.2639 ± .0041	
	VND	**.2710 ± .0047**	**.2698 ± .0053**	**.2695 ± .0033**	**.2687 ± .0051**	.2632 ± .0049	
LFS76	LSBR	.2919 ± .0058	.2888 ± .0052	.2869 ± .0060	.2860 ± .0043	.2913 ± .0058	
	VND	**.2969 ± .0055**	**.2978 ± .0055**	**.2948 ± .0054**	**.2909 ± .0054**	.2904 ± .0055	

表 3.10　PMN 数据集下，嵌入第 12 层时 VND 隐写算法抵抗隐写分析检测器的安全性结果

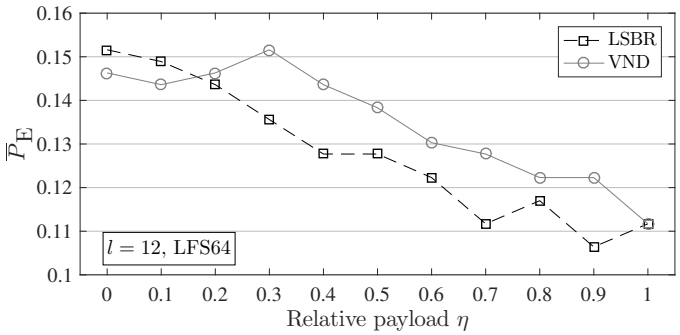
检测器	隐写方法	0	0.1	0.2	0.3	0.4	0.5
LFS64	LSBR	.2054 ± .0040	.1978 ± .0041	.1949 ± .0046	.1913 ± .0050	.1892 ± .0042	.1885 ± .0051
	VND	.2036 ± .0045	**.2008 ± .0046**	**.1988 ± .0048**	**.1966 ± .0042**	**.1964 ± .0045**	**.1944 ± .0046**
LFS76	LSBR	.2060 ± .0046	.2000 ± .0045	.1969 ± .0043	.1929 ± .0033	.1939 ± .0045	.1888 ± .0044
	VND	.2051 ± .0035	.2008 ± .0041	**.2010 ± .0049**	**.1973 ± .0042**	**.1989 ± .0048**	**.1939 ± .0044**
检测器	隐写方法	0.6	0.7	0.8	0.9	1.0	
LFS64	LSBR	.1885 ± .0045	.1851 ± .0048	.1832 ± .0048	.1847 ± .0045	.1840 ± .0053	
	VND	**.1944 ± .0044**	**.1916 ± .0046**	**.1869 ± .0043**	.1870 ± .0053	.1821 ± .0053	
LFS76	LSBR	.1862 ± .0041	.1835 ± .0040	.1830 ± .0045	.1802 ± .0050	.1794 ± .0042	
	VND	**.1941 ± .0047**	**.1895 ± .0042**	**.1888 ± .0043**	**.1862 ± .0045**	.1796 ± .0048	



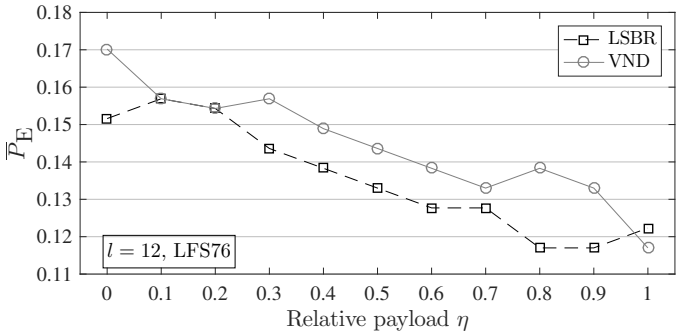
(a) 最高嵌入层为第 7 层，隐写分析器为 LFS64



(b) 最高嵌入层为第 7 层，隐写分析器为 LFS76



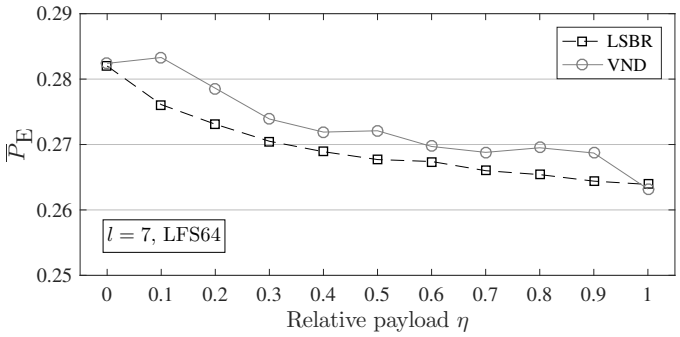
(c) 最高嵌入层为第 12 层，隐写分析器为 LFS64



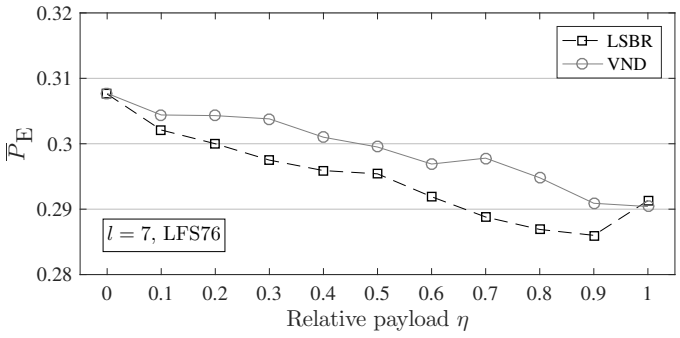
(d) 最高嵌入层为第 12 层，隐写分析器为 LFS76

图 3.19　PSB 数据集下，隐写算法为 VND 和 LSBR 方法的安全性对比

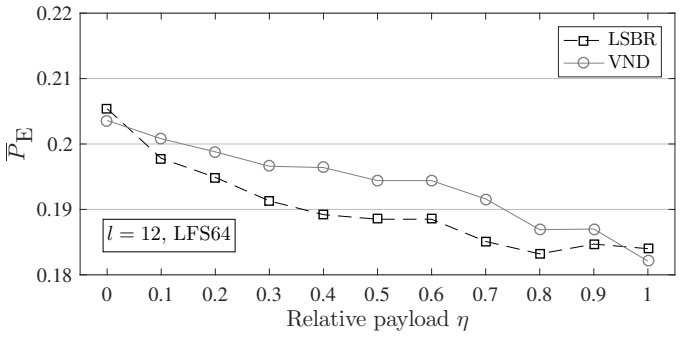
著的。隐写分析方法采用 LFS64 和 LFS76。实验结果表明，除了单层嵌入率接近 0 bpv 或接近 1 bpv 的隐写结果外，z 值始终大于相应的分位数 $z_{0.05/2}$，表明 VND



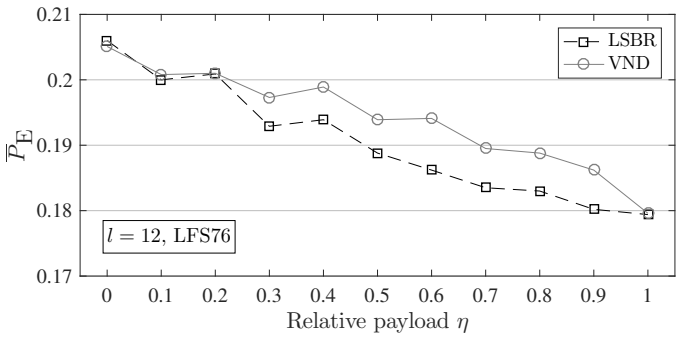
(a) 最高嵌入层为第 7 层，隐写分析器为 LFS64



(b) 最高嵌入层为第 7 层，隐写分析器为 LFS76



(c) 最高嵌入层为第 12 层，隐写分析器为 LFS64



(d) 最高嵌入层为第 12 层，隐写分析器为 LFS76

图 3.20　PMN 数据集下，隐写算法为 VND 和 LSBR 方法的安全性对比

算法的隐写安全性有显著提升。由于 PSB 数据集样本数较少，导致平均检测错误率 $\overline{P}_{\mathrm{E}}$ 发生波动（即标准差较大），因此，无法体现 VND 隐写算法是否有提升。

图3.21是 3D 网格模型隐写前后的可视化结果，从左至右分别为载体网格、嵌入 9 层秘密消息的载密网格、嵌入 12 层秘密消息的载密网格和嵌入 15 层秘密消息的载密网格。隐写强度通过载体和载密 3D 网格坐标的欧式距离衡量。3D 网格中消息嵌入量越大，修改幅度越明显。

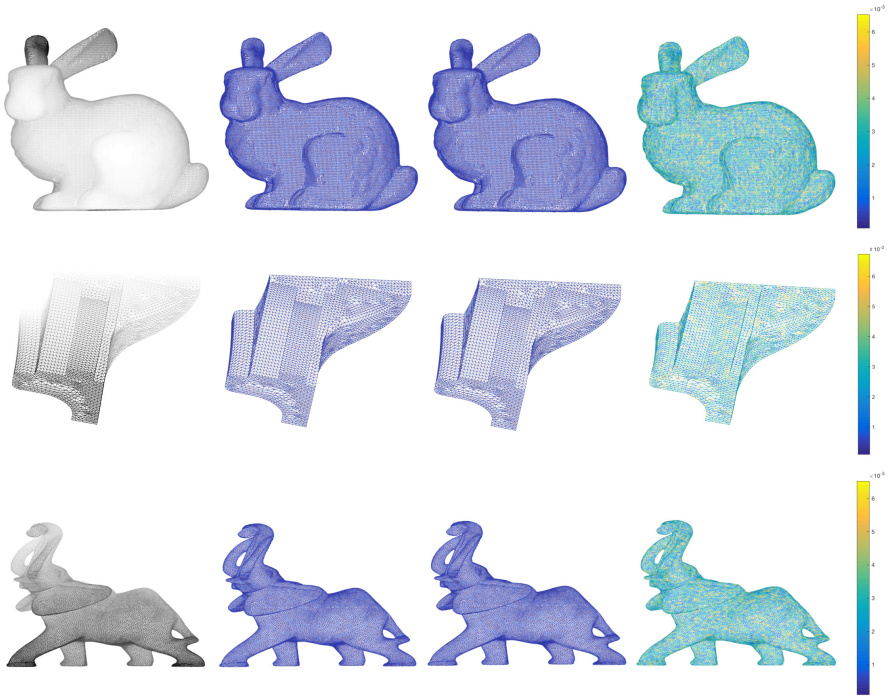


图 3.21　常用 3D 网格模型隐写前后的可视化图示

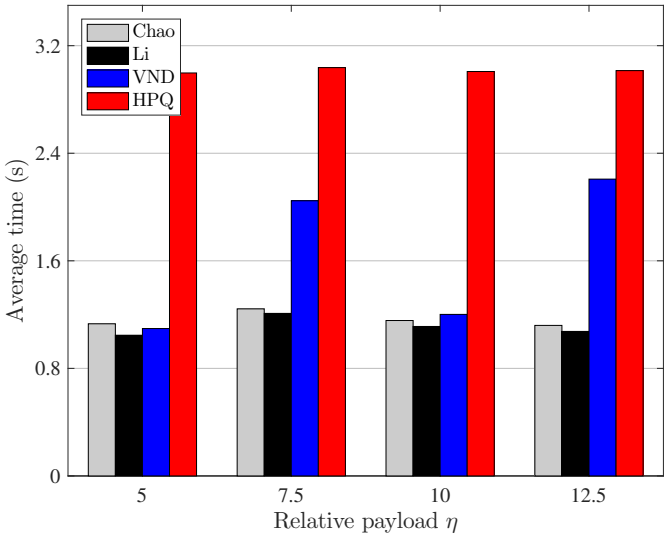


图 3.22　PMN 数据集下，四种隐写算法运算复杂度对比

3.3.9　带噪 3D 网格实验

本节分析带噪 3D 网格的隐写安全性。实验条件设置如下：在 PMN 数据集上，LFS64 隐写分析方法作为检测器，载体数据为带噪 3D 网格，由零均值和不同标准差下的高斯噪声模拟产生，标准差选取为 $std \in \{0.00001, 0.0001, 0.001, 0.01\}$。如图3.23所示，带噪 3D 网格比无噪 3D 网格具有更高的隐写安全性。噪声强度越大，3D 网格越适合隐写。当标准差为 0.01 时，隐写算法能达到 50% 的平均检测率，此时无法被 LFS64 隐写分析方法检测。

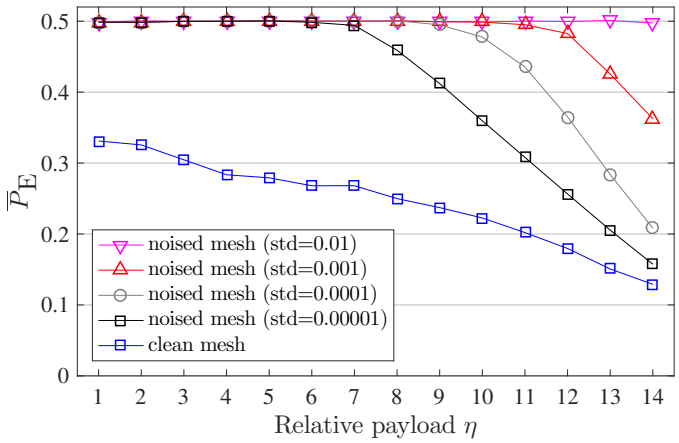


图 3.23　PMN 数据集上，不同强度高斯带噪网格的隐写安全性对比

3.4　本章小结

本章提出了基于法向量投票张量特征的 3D 网格隐写分析方法，该方法能够有效地检测 3D 网格上的隐写扰动，从而提升隐写分析性能。同时，为了对抗隐写分析的检测，本章提出基于坐标点法向量偏移量的失真函数，实现对高维隐写分析特征提取的干扰，加强了 3D 网格隐写算法的安全性。本章在多个数据集上实施了实验，验证了算法的有效性。表3.11总结了不同隐写算法在失真、嵌入率、安全性和鲁棒性的对比结果。

本章主要贡献包括：

- 根据载体 3D 网格模型和载密 3D 网格模型在法向量投票张量的差异性，提出了基于法向量投票张量的隐写分析特征，并且有效地提升了隐写分析的性能；

- 根据已有 3D 网格隐写分析特征中最有效的特征，针对该特征设计了基于坐标点法向量偏移量的失真函数，并且采用自适应隐写框架实施 3D 网格

表 3.11　3D 网格隐写算法之间的比较

类别	方法	失真	嵌入率	安全性	鲁棒性
两态调制隐写	宏块嵌入[19]	较大	1	较弱	脆弱
	多层宏块嵌入[20]	一般	6	较弱	脆弱
	采样点几何嵌入[51]	一般	3	较弱	脆弱
	多层嵌入[21]	较小	69	一般	非常脆弱
	静态算数编码[22,23]	较小	8	较强	脆弱
LSB 隐写	高斯曲率约束[24]	较小	69	一般	非常脆弱
	截断空间约束[25]	较小	90	一般	非常脆弱
	自适应隐写	较小	69	较强	非常脆弱
置换隐写	顺序编码[26]	无	$\frac{1}{V}\sum_{i=1}^{V}\lfloor\log_2 i\rfloor$	一般	非常脆弱
	增强顺序编码[27]	无	大于[26]	一般	非常脆弱
	二叉树[28]	无	[26]+0.69	一般	非常脆弱
	编码树[29]	无	[26]+0.69	一般	非常脆弱
	最大期望树[30]	无	大于[28,29]	一般	非常脆弱
	一环邻域[52]	无	较小 (<[26])	较强	非常脆弱
变换域隐写	小波变换域[32]	较大	较小	较弱	脆弱
	统计分布嵌入[31,53]	一般	0.016	较弱	鲁棒

自适应隐写算法，有效地提升了隐写算法的安全性。

为了方便读者研究和对比本章中提出的方法，实验代码已放在如下的网站上。其中 3D 网格隐写算法：https://github.com/RyanHangZhou/3D-Mesh-Steganography，以及 3D 网格隐写分析算法：https://github.com/RyanHangZhou/3D-Mesh-Steganalysis。

第 4 章　3D 纹理合成隐写方法

本章将主要讨论 3D 纹理合成隐写方法，包括纹理合成隐写安全性分析和基于 3D 纹理贴图的 3D 纹理隐写算法设计。4.1节介绍了纹理隐写的研究进展；4.2节提出了基于镜像重构攻击和纹理缝合区域统计最优性特征的纹理图像隐写分析算法；4.3节提出了基于 3D 纹理贴图的隐写方法；4.4节为本章小结。

4.1　引言

计算机图形学中的纹理既包括通常意义上物体表面的纹理，即使物体表面呈现凹凸不平的沟纹，同时也包括物体光滑表面上的彩色图案。这两种类型的纹理生成方法完全一致，这也是计算机图形学中把他们统称为纹理的原因所在。所以，纹理映射就是在物体的表面上绘制彩色的图案。近年来，合成纹理图像的需求随着计算机图形学的发展而大大提高。计算机图形学的应用主要包括在线游戏、特效电影、3D 道路和虚拟现实等。尽管当前主流的图像隐写算法使用自然图像作为载体图像以嵌入秘密消息，但是纹理图像作为一种特殊图像，可作为秘密消息嵌入的载体。

基于纹理合成的隐写算法首次由 Otori 和 Kuriyama[36,37] 提出，通过结合数据编码和基于像素点的纹理合成实现隐写。秘密消息编码为纹理图像中采样的彩色点状模式，并将它们直接填充至空白图像上，而其余像素采用基于像素的纹理合成方法实现填充，因此，隐写嵌入容量由点状模式的数量决定。Wu 和 Wang[38] 提出了一种基于可逆纹理合成的隐写方法，该方法对较小的纹理图像重采样，然后合成具有相似局部外观和任意大小的新纹理图像。该算法的核心思想是通过选择源图像生成的候选图像单元以编码消息，在这过程中实现消息的嵌入。Qian 等人[39] 提出了一种抗 JPEG 压缩的鲁棒纹理图像隐写算法，然而隐写嵌入率较低。

由于载体图像和载密图像均为局部高复杂图像，不适合采用自然图像的隐写分析器检测隐写算法的安全性，因此，目前还没有专用于纹理图像隐写的隐写分析方法。

4.2　纹理图像合成隐写安全性分析

[0]本节内容已于 2017 年发表在图像处理领域 CCF A 类，SCI 一区国际期刊 IEEE Transactions on Image Processing 上（“Comments on “Steganography Using Reversible Texture Synthesis””，2017）。

纹理图像合成技术的发展使得隐写者有了新的隐写载体，同时纹理图像具有全局复杂性和近似周期性使得当前自然图像隐写分析方法难以对载体和载密合成纹理图像进行检测，这对评估隐写的安全性带来了极大的挑战。

4.2.1　纹理图像合成隐写算法

Wu 和 Wang 提出了基于块合成的纹理合成隐写算法[38]，其过程描述如下。纹理合成技术可由一小块样本纹理图像依据马尔科夫模型生成大幅纹理图像，纹理合成隐写即在纹理合成的过程中实施信息隐藏，最终生成的大幅纹理图像是与秘密消息有关的。该方法在样本图像中逐点移动获得多个候选块，将每一个候选块分为内核和外围两部分，比较每一个候选块的外围与其他候选块外围之间的匹配程度，由大到小建立索引表，该索引表直接与二进制数据相映射。在纹理合成时用候选块来填充大幅图像的空白部分，具体选取哪个候选取决于秘密消息，最终可得到一幅由秘密消息决定的纹理图像。

用 **A** 表示源图像，**S** 表示合成图像，**m** 表示嵌入的秘密消息。纹理单元结构是隐写者每次嵌入秘密信息的单元，大小为 $P_w \times P_h$。如图4.1(a) 所示，纹理单元结构包含大小为 $K_w \times K_h$ 的中央内核区域和深度为 P_d 的边界区域。**A** 的大小为 $S_w \times S_h$，**S** 的大小为 $T_w \times T_h$。

可逆图像合成的过程描述如下。首先，将源图像 **A** 划分为相同大小的非重叠内核块，共有 SP 个：

$$SP = n_w \times n_h = \frac{S_w}{K_w} \times \frac{S_h}{K_h}. \tag{4.1}$$

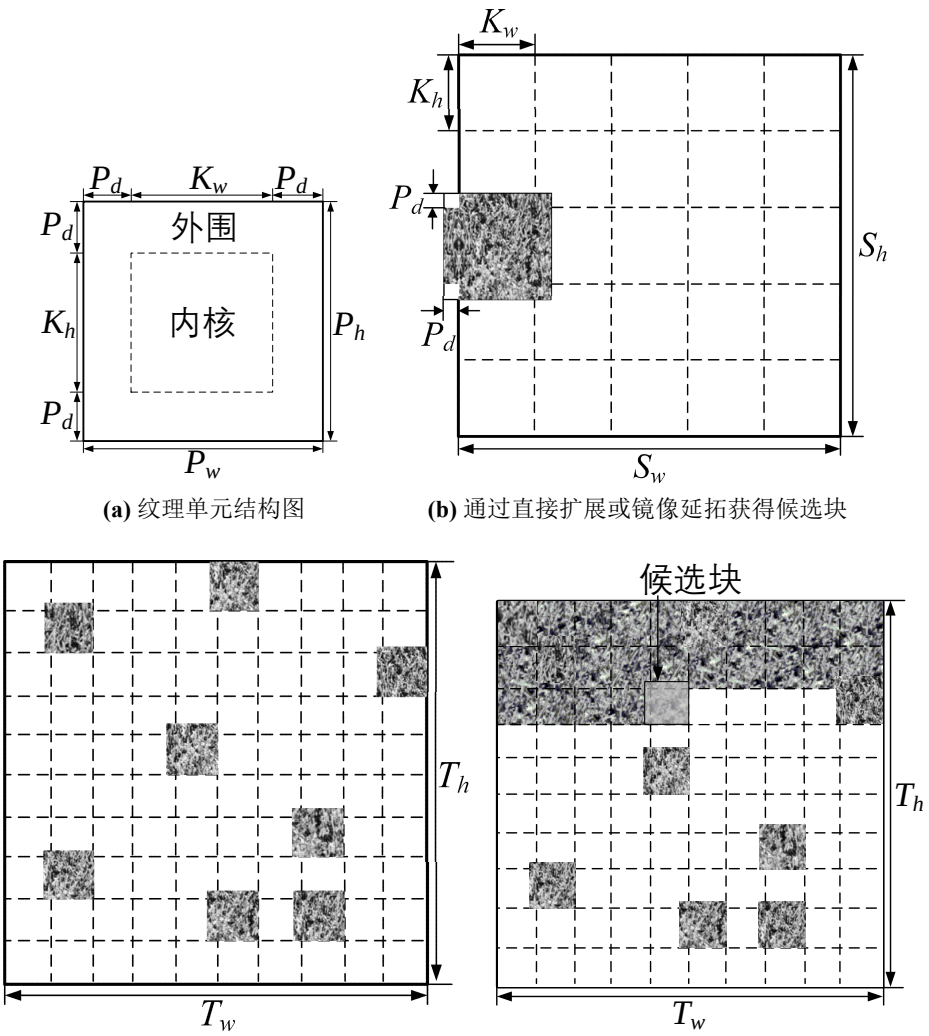
如图4.1(b) 所示，以深度为 P_d 内核为中心的核区域上直接扩展或镜像延拓得到候选块。值得注意的是，源图像 **A** 边界上的扩展区域由镜像操作得到。为了合成具有指定大小的图像，根据密钥置乱源图像所有分块，然后填充到待合成的图像上，如图4.1(c) 所示。按照之字形顺序，在源图像 **A** 上使用步径为 1 的滑动窗口构建候选区域，然后根据秘密消息选取相应的图像单元填充到合成图像 **S** 中。候选区域共有 CP 个：

$$CP = (S_w - P_w + 1) \times (S_h - P_h + 1). \tag{4.2}$$

合成图像 **S** 中的纹理单元结构的数量为

$$TP_n = T_{pw} \times T_{ph} = \left\lfloor \frac{(T_w - P_w)}{(P_w - P_d)} + 1 \right\rfloor \times \left\lfloor \frac{(T_h - P_h)}{(P_h - P_d)} + 1 \right\rfloor. \tag{4.3}$$

如图4.1(d) 所示，通过之字形模式同时嵌入消息和填充图像。由于候选纹理单元块迭代填充到 **S** 中空白区域的过程中存在重叠区域（OverLapped Region，简



(a) 纹理单元结构图　　**(b)** 通过直接扩展或镜像延拓获得候选块

(c) 原始图像分割后随机填充至合成图像中　　**(d)** 锯齿状图像单元填补的同时嵌入消息

图 4.1　纹理合成隐写示意图

称 OLR），因此，通过计算候选块和已填充块之间重叠区域的均方误差可判断两个图像块适合缝合的程度。均方误差越小，候选块与合成区域越相似，缝合后边界区域更为连续。由于每一个候选块均可获得一个对应的均方误差，因此，本文排序均方误差，并编码候选块。构建完排序表之后，n 比特的秘密消息转换为十进制数，然后将对应的候选纹理单元作为待合成的图像单元。Wu 和 Wang 采用 Efros 和 Freeman 提出的图像缝合技术[33] 来减少图像合成产生的不连续性，具体算法描述如下。

图像缝合旨在在两个图像块之间找到一条缝合线，并保证两边的图像缝合后视觉失真最小。如图4.2所示，$\mathbf{B}_l$ 和 $\mathbf{B}_r$ 分别表示待合成的左图和右图，它们分别沿垂直方向重叠。记 **D** 为两个图像块之间的感知距离，例如均方误差，$\mathbf{q} = \{q_j | j = 1, 2, 3, ..., K_h\}$ 为竖直方向上的接缝线。此时，满足最小均方误差时的最

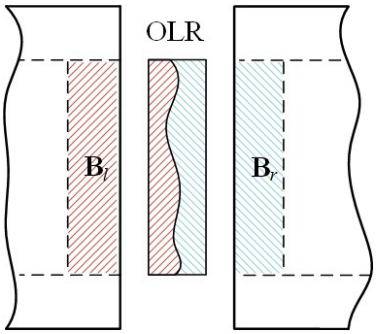


图 4.2　图像缝合示意图

优缝合线 $\hat{\mathbf{q}}$ 可由动态规划算法求解以下最短路径问题得到：

$$\begin{aligned}\hat{\mathbf{q}} &= \arg\min_{\mathbf{q}} \sum_{j=1}^{K_w} D(q_j, j)^2 \\ &\text{subject to } |q_j - q_{j-1}| \leq 1.\end{aligned} \tag{4.4}$$

水平方向上的缝合线可通过相似方式求解。

通过实验发现，Wu 和 Wang 的隐写方法有漏洞：攻击者分析合成图像中的每一个图像单元以判断该图像单元是否来自于原始图像的边缘。如果来自边缘，则将该图像单元填充至边缘上相应的位置重构图像边界，迭代多次能够重构出原图。这是由于在于原始图像中，边缘图像单元的获取由镜像延拓得到，而非边缘图像单元由直接扩展得到。只要能够区分这两类图像单元，攻击者就能够重构出原始图像，然后进行消息的提取。

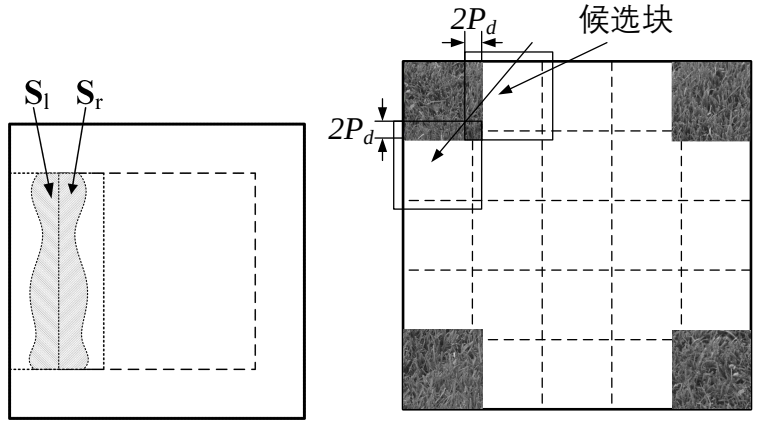
4.2.2　镜像重构攻击

本节提出了一种通过分解合成纹理图像 **S** 来恢复源图像 **A** 的方法。记 $\mathbf{A}'$ 为恢复的源图像，一旦重构了 $\mathbf{A}'$，便可模拟图像 **S** 的合成过程。在此合成过程中，可以分析 **S** 是否为载密图像，并从载密图像中提取隐藏的秘密消息。

1）源图像重构

Wu 和 Wang 在源图像上的镜像操作导致合成图像有漏洞，据此现象可以从合成图像中逆向地重构出源图像。由于只有图像的边界区域会实施镜像操作，因此，源图像边界区域与图像内部区域边界的镜像程度是不同的。通过分析合成图像 **S** 中所有的合成单元边界的镜像程度，然后排序，最后可以重构出来自源图像 **A** 的四个角块和边界的图像块。

由于合成图像的重叠区域来自不同的图像块，因此，如何从两个图像块中选取最终的像素取决于图像的缝合技术。如图4.3(a) 所示，当合成区域为源纹理图像 **A** 的左边界时，记内核外围的左边区域为 $\mathbf{S}_\mathrm{l}$，右边区域为 $\mathbf{S}_\mathrm{r}$，对 $\mathbf{S}_\mathrm{l}$ 镜像操作得到 $\mathbf{S}_\mathrm{l}'$。根据镜像对称原理，$\mathbf{S}_\mathrm{l}'$ 中纹理的形状接近 $\mathbf{S}_\mathrm{r}$，而源纹理图像 **A** 的内部、



(a) S_l 由 S_r 镜像而得　　**(b)** 重构原图的过程

图 4.3　纹理图像隐写分析示意图

上边界、下边界或右边界相同位置的纹理相似性较低，因此，攻击者能够从合成图像中找出源图像的左边界。其中，重叠区域相似性 w_p 描述如下。

由于从合成单元中难以估计原先合成时的缝合线，因此，直接比较并统计 $\mathbf{S}_\mathrm{l}'$ 和 $\mathbf{S}_\mathrm{r}$ 相同的像素值来估计 w_p。越靠近镜像轴的像素，来自对称区域像素的可信度越高，因此，如果能够赋予每个像素合适的权重，那么相似性评估更为准确。在实验中，对于每个重叠区域，本文将缝合线左侧的像素标记为 0，缝合线右侧的像素标记为 1，统计了 100 张合成图像的合成边界区域像素点来自于内核的概率分布，估算得权重 $h(i)$，其中 i 是像素在重叠区域中的位置，$1 \leq i \leq P_d$。

表 4.1 图像缝合区域不同位置 i 对应的可信度权重 h

i	1	2	3	4	5	6	7	8
权重 h	1	1.66	2.37	3.07	3.77	4.43	4.96	5.34

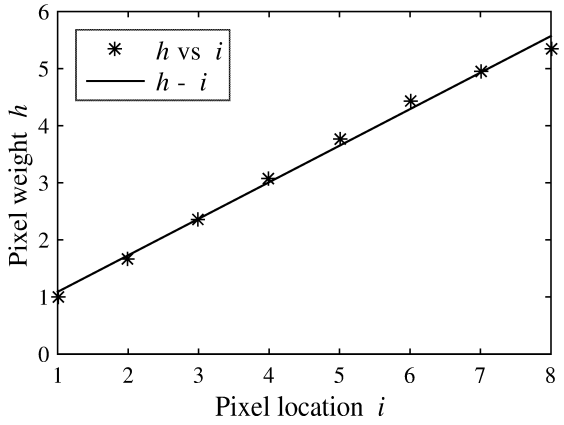


图 4.4　图像缝合区域（i，h）分布散点图

表4.1为图像缝合区域不同 i 时权重 $h(i)$ 的统计值，并于图4.4中给出分布的散点图。实验结果表明，$h(i)$ 随 i 单调递增。本文采用线性回归模型刻画 $h(i)$ 与

i 的关系，并拟合数据：

$$h(i) = 0.64i + 0.45. \tag{4.5}$$

拟合的线性函数能够对任一 i 值估计最优的权重 $h(i)$。

相似性 w_p 越大，表示缝合区域由内核镜像而得的可能性越大。如图4.3(b) 所示，由于原图四个角的图像块各有两条边是由镜像延拓得到，因此，这四个角的纹理块的相似性最为明显，需要首先依据 w_p 的排序找到这四个角的纹理块。w_p 定义为

$$w_p = \frac{1}{LP_d}\sum_{i=1}^{L}\sum_{j=1}^{P_d} h(j)I(\mathrm{S_l'}(i,j) = \mathrm{S_r}(i,j)), \tag{4.6}$$

其中，L 是重叠区域的高度，I 为指示函数，S_l' 与 S_l 呈镜像关系。

源图像重构过程描述如下。根据上述实验分析，合成图像 **S** 中的每个合成单元均可计算得到 w_p 值。由于边界镜像操作，源纹理图像 **A** 左边界上合成单元的 w_p 值明显大于其他区域的 w_p 值。降序排序所有纹理图像单元的 w_p 值，并将最大值对应的纹理单元内核填充至源图像指定的边界区域。

本文迭代地将估计的图像块粘贴到空白待恢复的源图像 **A**′ 上以重构源图像，直到所有的图像块拼合结束，这个过程类似求解拼图游戏。重构过程的第一步为估计源图像中的四个角区域上的图像块。如图4.3(b) 所示，这四个图像块各自存在着两个各不相同的镜像区域，不会造成其他图像块的混淆现象。第二步为填充图像边界，采用从左到右和从上至下的过程填充。为了填充左上角图像块下方的空白区域，在候选图像块中，找出最优匹配值对应的图像块并粘贴至此区域，在计算 w_p 时，重叠区域的宽度为 $2P_d$，因此，本文设计了新的估计方式：

$$w_p = \frac{1}{2LP_d}\sum_{i=1}^{L}\sum_{j=1}^{2P_d} h(j)I(\mathrm{S_l'}(i,j) = \mathrm{S_r}(i,j)). \tag{4.7}$$

一旦源图像 **A**′ 的外围边界填充完毕，迭代填充内部区域直到填满。

本算法的假设为攻击者已知内核区域大小和 P_d 的值。已知合成图像 **S** 的大小 $T_h \times T_w$，可以求解二元一次方程估算得到多组 K_h、K_w 和 P_d。对于任意一种情况，需要计算每个合成图像块的 w_p 值，并选取最大值对应的一组尺寸。当尺寸匹配时，镜像现象不仅存在，而且高概率是能重构的. 在重构源图像的过程中，还需要记录源图像中每个合成单元在合成图像 **S** 中的位置，以便于后期消息的提取。

2）秘密消息提取

消息提取的过程与消息嵌入的过程相似。从重构的原始图像中生成候选图像单元集合，然后按照纹理合成隐写的过程计算均方误差并排序，与原合成图像中图像块的均方误差相同的图像单元所对应的索引值即为嵌入的秘密消息。

重构源图像 $\mathbf{A}'$ 后，采用 Wu 和 Wang 的隐写算法[38] 从 $\mathbf{A}'$ 中构造候选纹理单元，并通过这些候选纹理单元再现图像 **S** 的合成过程。首先，根据上节重构源图像过程中记录的源图像中每个合成单元在合成图像 **S** 中的位置，将扩展或镜像生成的每个源图像块从 $\mathbf{A}'$ 粘贴至到新的合成图像 $\mathbf{S}'$ 上 **S** 上。然后，以之字形模式逐步填充候选图像块，每一次纹理单元合成时计算当前图像单元 $\mathbf{B}_{\mathrm{C}}$ 与候选图像单元之间重叠区域的均方误差，并得到一组降序排列的均方误差 **v** 序列。另一方面，用合成单元 $\mathbf{B}_{\mathrm{C}}$ 计算 **S** 中合成单元之间重叠区域的均方误差 v。v 在 **v** 序列中的位置即为编码的信息。随后，将从每个合成单元中提取的消息级联在一起，即可解码嵌入的秘密消息 **m**，并用 $\mathbf{m}'$ 表示。如果 $\mathbf{m}'$ 为全零序列，则合成图像 **S** 未嵌入消息；否则 **S** 是载密图像，且嵌入的消息为 $\mathbf{m}'$。

然而，上述方法存在秘密消息无法正确提取的情况。若候选图像单元与扩展的无信息合成单元相同，则消息提取时无法区分这两个图像单元，从而导致提取错误。

4.2.3　重构攻击实验结果与评估

表 4.2 重构攻击隐写分析结果

图像正确重构率	漏警率 P_{MA}	虚警率 P_{FA}	消息正确提取率
96.77%	0	5.71%	94.66%

在实验中，本文采用 Brodatz Textures 数据集，由于样本数偏少，需要进行数据增强。隐写嵌入率定义为比特每个图像块（bits per patch，简称 bpp）。根据嵌入率的不同（1∼12 bpp），共生成 2088 张载体图像以及相同数量的载密图像用于隐写分析。其中，内核参数为 $K_w = K_h = 32$，缝合区域深度为 $P_d = 8$，以及合成图像参数为 $T_w = T_h = 488$。

在隐写分析过程中，未知 K_w、K_h 和 P_d 的值，因此，本文需要估计这三个参数。候选参数值为：$\{(K_w, K_h, P_d)|(32, 32, 8), (18, 18, 4), (16, 16, 12), (43, 43, 16)\}$。通过实验发现，本方法能以 98.12% 高的概率准确估计出正确的参数。

表4.2为隐写分析实验结果。实验结果表明，原始纹理图像正确恢复的概率高达 96.77%，漏警率为 0，虚警率为 5.71%，有 94.66% 的图像能够正确提取秘密消息。然而，存在无法从载密图像中正确提取秘密消息的情况，主要有以下两种原因：其一是 w_p 区分度不够明显，导致原始纹理图像重构失败；其二是虽然原始图像重构正确，但是某些图像并非来源于分割图像而是来源于候选图像集合，导致消息提取错误。

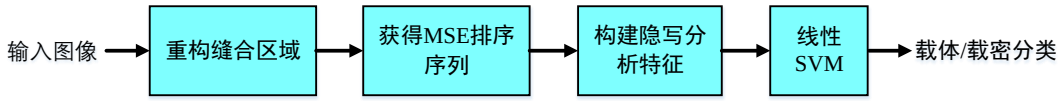


图 4.5　纹理图像隐写分析流程图

4.2.4　统计最优性特征构造

本文提出了另一种检测纹理图像隐写的隐写分析方法，称为基于参数估计的隐写分析方法。由于纹理图像合成的隐写过程会破坏待合成单元和最优候选单元的匹配性，因此，本文通过重构纹理合成的过程并检测纹理合成最优性的匹配程度来判断纹理合成图像是否经过隐写。图4.5为基于最优性特征提取的纹理图像隐写分析流程图，共包含 4 个步骤：重构缝合区域、获得均方误差排序序列、构建隐写分析特征和线性 SVM 分类。指定任意一缝合区域，重构左侧原始图像块 B_l' 以及右侧原始图像块 B_r'，同时重构出近似的候选纹理单元集合 $\mathcal{B}'$。重新合成 B_l' 和 B_r' 并估计均方误差在候选纹理单元与当前图像单元缝合的均方误差集合的排序，并把排序值作为隐写分析特征。采用线性支持向量机作为分类器分类载体纹理图像和载密纹理图像。

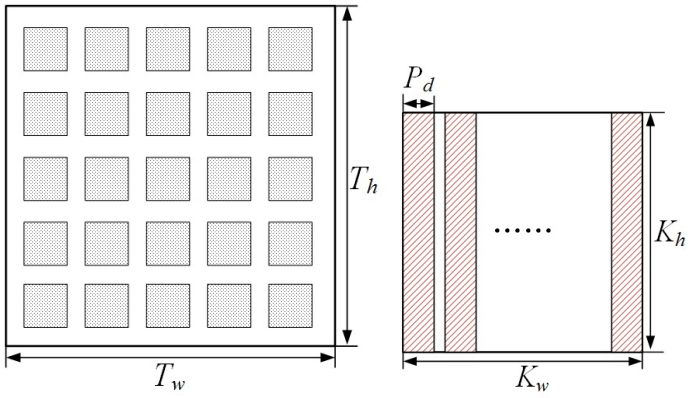
具体方法描述如下。

1）重构缝合区域

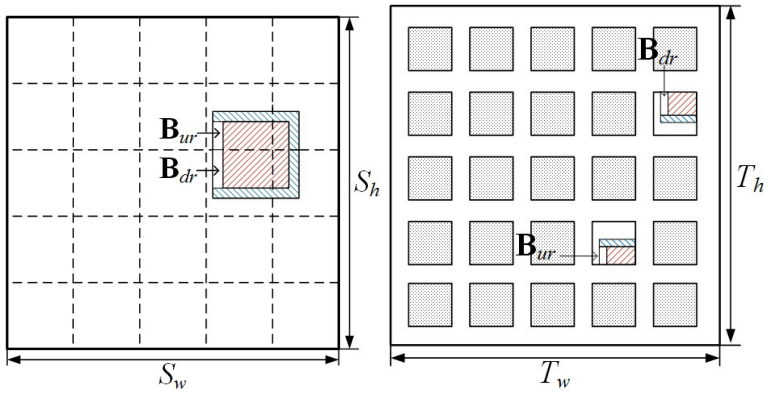
事实上，设计这样一种基于重构缝合区域的隐写分析方法的初衷是为了还原隐写者进行隐写的一个过程。由于这个过程不可逆，因此，本文需要模拟一个近似版本的纹理合成隐写过程，并将待合成区域的最优性程度作为特征。其中，构建集合 $\mathcal{B}'$ 是为了近似隐写过程中的候选纹理单元集合 $\mathcal{B}$。如图4.6(b) 所示，$K_h \times P_d$ 大小的滑动窗口在载密纹理合成图像中的核区域上进行卷积，得到一组候选纹理单元集合 $\mathcal{B}$。如图4.6(c) 所示，在合成的过程中，多数合成图像块来源于多个分割的核区域。因此经过纹理合成后，原始纹理单元被分散至不相邻的核区域中，如图4.6(d) 所示。

那么，如何重构左侧原始图像块 B_l' 以及右侧原始图像块 B_r' 呢？实验证明，纹理缝合区域的可能情况分为 5 类，如图4.7(a) 所示。其中，第三种缝合区域适合于 B_l' 和 B_r' 的重构。如前所述，在纹理合成过程中，缝合区域被分为了两段，例如 B_{ur} 和 B_{dr} 位于不同区域。为了在合成图像中找到 B_{ur} 和 B_{dr}，本文提出在合成图像中的核区域中进行全局搜索，首先找到 B_{ur} 的右上角区域 R^u 和 B_{dr} 的右下角区域 R^d，然后进行扩展重构出原始纹理单元，如图4.7(b) 所示。一旦 $\mathbf{R}^u$

[0]本节内容已于 2018 年发表在图像处理领域 CCF C 类，SCI 二区国际期刊 Journal of Visual Communication and Image Representation 上（“Targeted Attack and Security Enhancement on Texture Synthesis Based Steganography”，2018）。



(a) 纹理合成图像示意图　　**(b)** 核区域滑动获得候选区域



(c) 某一待合成候选块处于 4 个核区域上　　**(d)** 合成图中 B_{ur} 和 B_{dr} 不相邻

图 4.6　基于重构图像块最优性检测的隐写分析方案示意图

和 $\mathbf{R}^d$ 在核区域中搜索到，则此时在核区域上的偏移量为

$$\begin{aligned}\mathbf{v}^u &= \left\{(\Delta i,\Delta j)\middle|\sum_{i=1}^{C_w}\sum_{j=1}^{C_h+C_d}|R^u_{ij}-K_{i+\Delta i,j+\Delta j}|=0\right\},\\ \mathbf{v}^d &= \left\{(\Delta i,\Delta j)\middle|\sum_{i=1}^{C_w}\sum_{j=1}^{C_h+C_d}|R^d_{ij}-K_{i+\Delta i,j+\Delta j}|=0\right\},\end{aligned} \tag{4.8}$$

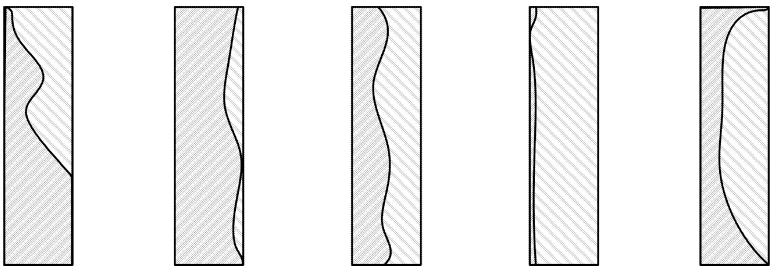
其中，K 表示核区域，R 为搜索区域。

2）获得 MSE 序列

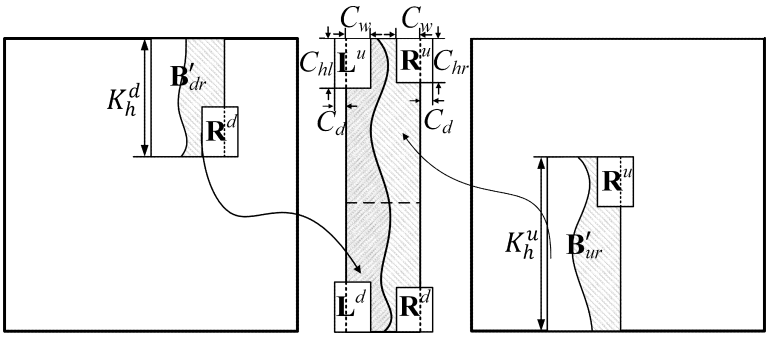
重构得到 B'_l 和 B'_r 后，B'_r 分别与集合 $\mathcal{B}'$ 中所有候选纹理单元进行纹理合成得到均方误差，并进行降序排列。然后，本文将 B'_l 和 B'_r 均方误差在均方误差序列的排序索引作为特征。

3）构建隐写分析特征

记 $R=\{r_i|r=1,2,3,...,N\}$ 为载体或载密图像的最优性排序值集合。由于集合 R 中存在漏检率和误检率，因此，本文提取最优性的鲁棒特征，即 R 的均值、中值、方差和峰度作为隐写分析特征，并记作 $v_r=[\mu_r,m_r,\delta_r,k_r]^T$。若未知



(a) 纹理区域中缝合线可能出现的 5 种示意图



(b) 纹理缝合区域原始区域 B'_l 的重构示意图

图 4.7　纹理区域特征提取示意图

参数 P_w，P_h 和 P_d，则需通过下式求解线性方程组的整数解：

$$\begin{aligned}(P_w - P_d) \times T_{pw} + P_d = T_w,\\ (P_h - P_d) \times T_{ph} + P_d = T_h.\end{aligned} \tag{4.9}$$

其中，求得 $\{P_w, P_h, P_d\}$ 的 t 组解。唯一的一组正确解此时匹配的参数对应的内核全部来自源图像，不含有重叠区域，如图4.6(c,d) 所示。相比之下，不匹配的参数对应的内核部分包含重叠区域。因此，本文提出的隐写分析方法能有效地检测载体和载密纹理图像。

4.2.5　隐写分析实验结果与评估

本节评估本文提出的 ReSid 隐写分析方法隐写方法 CASO 的有效性。

数据集。采用 CASO 隐写方法生成载密图像。由于 Brodatz 数据库纹理图像数据量较少，因此，本文通过缩放和裁剪技术进行数据增强，最终生成 10000 张图像（128×128）作为源图像[2]。为了对齐实验设置，本文仅在灰度纹理图像上进行实验。根据不同隐写嵌入率（γ 从 1 bpp 到 13 bpp）得到不同载体和载密纹理图像对，其中参数设置为：$T_{pw} = T_{ph} = 488$，$P_d = 8$，$P_d = 8$ 和 $P_w = P_h = 48$，此时 $n_C = 6,561$。

[2]纹理数据集下载地址: http://home.ustc.edu.cn/∼zh2991/

分类器训练。本文采用支持向量机训练载体纹理图像和某一嵌入率下的载密纹理图像对，其中，支持向量机为含高斯核函数 $k(x,y)=\exp(-\gamma\|x-y\|_2^2)$，$\gamma>0$ 的软边距支持向量机。惩罚参数 $C=5$，核参数 $\gamma=0.5$。

本文提出的 ReSid 方法与空域图像隐写分析方法 SPAM[7]、SRM[10] 和 maxSRM[77] 进行比较。这几种方法采用集成分类器进行分类器训练。在实验中，采用参数搜索方式估算得到若干组参数对 $\{P_w,P_h,P_d\}$：

$$\mathcal{T}=\{(P_w,P_h,P_d)\mid(15,15,4),(15,26,4),...,(108,108,32)\},\tag{4.10}$$

其中 $\|\mathcal{T}\|=150$。实验结果表明，正确估计参数的概率高达 97%。

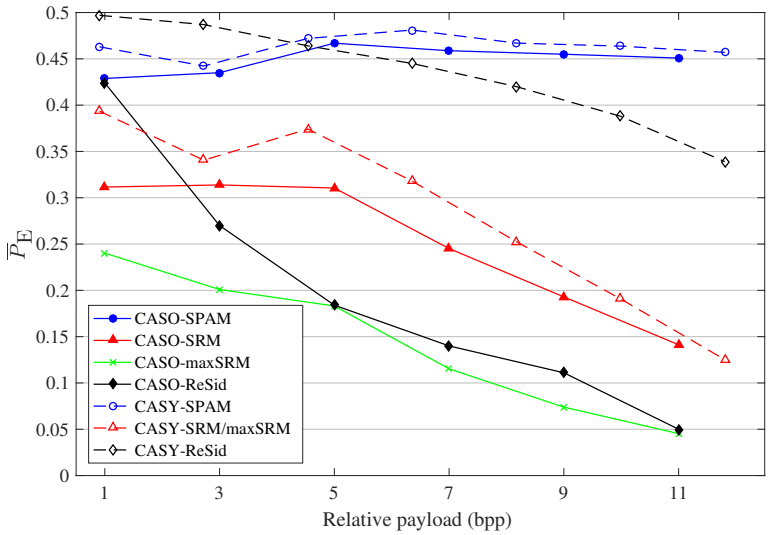


图 4.8　针对 CASO 隐写方法，ReSid 与 SPAM，SRM/maxSRM 平均检测错误率对比

在参数估计准确的前提下，进一步实施隐写分析实验。如图4.8所示，本文提出的隐写分析器 ReSid 采用 SVM 分类器的分类准确率明显高于 SPAM、SRM 和 maxSRM。在低隐写嵌入率下，ReSid 检测性能不如 SRM 特征，是由于 SRM 特征含有高维特征（34671 维），相较于 ReSid 的 4 维特征更容易检测载体和载密之间微弱的差异。SPAM 隐写分析特征主要采用二阶马尔可夫抽取残差特征，实验结果表明，这种特征难以捕捉载体和载密之间的差异，因此，在不同隐写嵌入率下，SPAM 检测错误率始终较高，约为 45%。与 SRM 隐写分析特征相比，本文提出的 ReSid 平均有 5.6% 的提升。

由于 ReSid 检测方法已将参数对 $\{P_w,P_h,P_d\}$ 作为先验知识，因此，为了公平比较隐写分析性能，本文将 SRM 替换为 maxSRM，并定义以下边信息显著图：核区域权重为 0，合成区域权重为 1。如图4.8所示，相较于 SRM 隐写分析特征，maxSRM 隐写分析特征具备修改区域的位置信息，因此检测准确率更高。在检测准确率的对比上，本文提出的 ReSid 特征在大嵌入率下与 maxSRM 接近，在

小嵌入率下次于 maxSRM。在计算复杂度的对比上，maxSRM 的平均计算复杂度约为 ReSid 的 1500 倍，表明 ReSid 是一种快速且有效的隐写分析特征。因此，本文提出的 ReSid 隐写分析算法为纹理图像隐写安全提供了全新的评测方法。

4.3　基于 3D 纹理贴图的隐写方法

4.3.1　增强型纹理合成隐写算法设计

本节改进了纹理合成图像隐写算法，提升了纹理隐写算法的抗检测性能。本文发现，一旦攻击者无法准确估计纹理单元的大小，ReSid 隐写分析方法的攻击性能会失效。因此，本文设计了一种基于密钥控制的边界区域填充纹理合成隐写。如图4.9所示，载密纹理图像的四条填充边的宽度由密钥控制，且填充区域不进行隐写。

1）合成任意大小的隐写纹理图像

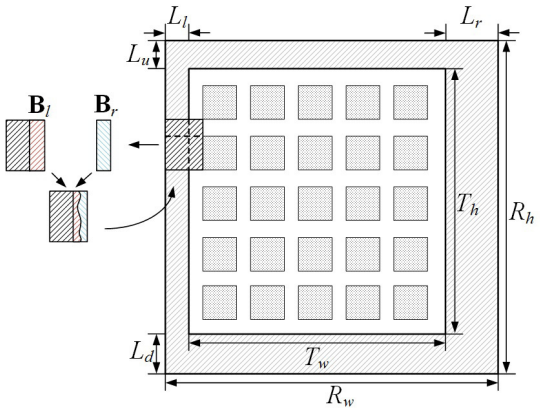


图 4.9　任意大小的合成图像 **R** 由原始合成图像 **S** 和边界冗余纹理构成

合成图像边界的冗余区域有助于提升合成纹理图像的安全性，因为冗余区域导致攻击者难以估计载密纹理图像中内核深度的大小，导致难以进一步执行隐写分析。因此，本文提出在原载密图像的边界填充冗余纹理的安全纹理图像隐写方法。记期望合成的纹理图像 **R**（稍大于 **S**）大小为 $R_w \times R_h$，则扩展宽度 $L = (R_w - T_w) + (R_h - T_h)$。如图4.9所示，记原合成图像左侧、右侧、上侧和下侧的冗余宽度分别为 L_l、L_r、L_u 和 L_d。

本文采用马尔可夫随机场实现纹理合成。假设待合成区域纹理的概率分布与整张图像的其余部分无关。记 $\mathbf{B}_s \in \mathcal{B}$ 为待合成的图像块，依据 $\mathbf{B}_s$ 邻域纹理建模当前待合成区域的纹理。记 $w(\mathbf{B}_s) \subset S$ 为 $\mathbf{B}_s$ 的邻域，为了合成图像块 $\mathbf{B}_s$，首先构造条件概率分布 $P(\mathbf{B}_s|w(\mathbf{B}_s))$ 的近似值，然后从中进行采样实现纹理区域的

合成。假设 $\mathbf{B}_s$ 独立于 $\mathbf{B}_s$ 的 $S\backslash w(B_s)$，此时最为匹配的图像块 $\mathbf{B}_s^*$ 由下式求得：

$$\mathbf{B}_s^* = \arg\min_{w} D(w(\mathbf{B}_s), w). \tag{4.11}$$

并且将 $\mathbf{B}_s^*$ 填充至图像 $\mathbf{R}$ 上。通过同样的方法迭代填充其他边界区域，直到图像 $\mathbf{R}$ 填充完全。

2）扩充容量

CASO 算法的最大嵌入率 γ_{max} 取决于源图像的大小和内核区域的深度，即

$$\gamma_{max} = \lfloor \log_2 n_C \rfloor. \tag{4.12}$$

为了扩大嵌入容量，本文提出增加候选纹理单元 n_C 的数量。同时，必须保证新增候选纹理单元的视觉质量，因此，本文对现有候选图像块 $\mathcal{B}$ 进行数据增以强增加候选纹理单元数量。

具体方法描述如下。由于具有相似纹理的图像经过纹理合成后仍然具有较好纹理质量，因此，本文聚类 $\mathcal{B}$ 中的纹理图像单元以构建纹理图像单元集合 $\mathcal{B}_s$。记 n_D 为子集 $R_{s_i} \subset \mathcal{B}$ 中表示聚类程度的元素数，子集 R_{s_i} 表示为

$$R_{s_i} = \{B_{i\cdot n_D+1}, B_{i\cdot n_D+2}, ..., B_{(i+1)n_D}\}, \quad i = 1, 2, ..., \left\lfloor \frac{n_C}{n_D} \right\rfloor. \tag{4.13}$$

分别对每个子集 R_{s_i} 中的任意两个纹理图像单元进行纹理合成，并得到新的候选纹理单元数 n_S：

$$n_S = n_C + \left\lfloor \frac{n_C}{n_D} \right\rfloor \binom{n_D}{2}. \tag{4.14}$$

此时，最大嵌入率为

$$\gamma_{max} = \lfloor \log_2 n_S \rfloor, \tag{4.15}$$

其上界为

$$\begin{aligned} \left\lfloor \lim_{n_D \to n_C} \log_2 n_S \right\rfloor &\le \left\lfloor \lim_{n_D \to n_C} \log_2 \left(n_C + \frac{n_C}{n_D} \binom{n_D}{2} \right) \right\rfloor \\ &= \log_2 [n_C(n_C+1)] - 1. \end{aligned} \tag{4.16}$$

候选纹理单元数 n_S 受到聚类度 n_D 的约束：

$$2^\gamma \le n_S \le n_C + \frac{n_C}{n_D} \binom{n_D}{2}. \tag{4.17}$$

因此，通过上式可以计算得到最大的聚类度 n_D^*：

$$\begin{aligned} n_D^* &= \left\lceil \frac{2^{\gamma+1}}{n_C} - 1 \right\rceil \\ &= \left\lceil \frac{2^{\gamma+1}}{(S_w - P_w + 1)(S_h - P_h + 1)} - 1 \right\rceil. \end{aligned} \tag{4.18}$$

增强的载密纹理图像 **R** 的总容量 C 为

$$C = \left(n_T - \frac{S_w \times S_h}{K_w \times K_h} \right) \gamma. \tag{4.19}$$

与 CASO 方法相比，增大的容量 ΔC 为

$$\Delta C = \left(n_T - \frac{S_w \times S_h}{K_w \times K_h} \right) \left(\lfloor \log_2 n_S \rfloor - \lfloor \log_2 n_C \rfloor \right). \tag{4.20}$$

不可忽视的是，纹理填充扩充的图像宽度 L 占用了额外的图像面积 ΔS：

$$\Delta S = R_w \times R_h - T_w \times T_h. \tag{4.21}$$

为了公平比较隐写嵌入率，需要校准嵌入率 $\hat{\gamma}$：

$$\hat{\gamma} = \frac{S_w \times S_h}{R_w \times R_h} \cdot \gamma. \tag{4.22}$$

Wu 和 Wang[38] 指出，大嵌入率下的载密纹理图像质量与小嵌入率下的载密纹理图像质量接近，没有明显差异。由于增强的载密纹理图像的外围是由缝合程度最优的纹理块填充的，因此，本文提出的增强的纹理隐写算法可以保证得到视觉质量较好的载密纹理图像。为方便起见，本方法简称为候选合成方法（CAndidate SYnthesis，简称 CASY）。

4.3.2　安全性分析

本节讨论攻击者成功估计参数 $\{P_w, P_h, P_d\}$ 的概率。一旦成功估计，攻击者可以采用上述提出的 ReSid 隐写分析方法检测 CASY 隐写算法。攻击者试图裁掉图像外围的冗余宽度 L_0 以进一步执行隐写分析，实际裁掉宽度 $L \geq L_0$。在攻击过程中，L 分为 4 段，并分别在图像的四条边界上裁去相应的宽度。只有满足 $L = L_0$，且四条边裁去正确的宽度时，攻击者才准确地裁出原始载密图像 **R**。因此，从 **S** 中正确估计 **R** 的概率为

$$P_s(L) = \frac{1}{1 + 4 + 4^2 + ... + 4^L} = \frac{3}{4^{L+1} - 1}. \tag{4.23}$$

对于任意候选裁剪图像 **R′**，攻击者可以估计出 t_i 组候选参数 $\{P_w, P_h, P_d\}$。因此，正确估计参数的概率为

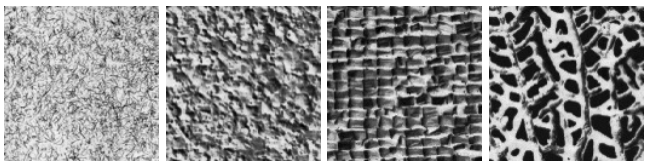
$$P_b(L) = \frac{1}{\sum\limits_{i=1}^{\frac{1}{P_s(L)}} t_i} = \frac{1}{\sum\limits_{i=1}^{\frac{4^{L+1}-1}{3}} t_i}, \tag{4.24}$$

其中 t_i 是第 i 个候选裁剪图像的候选参数个数。

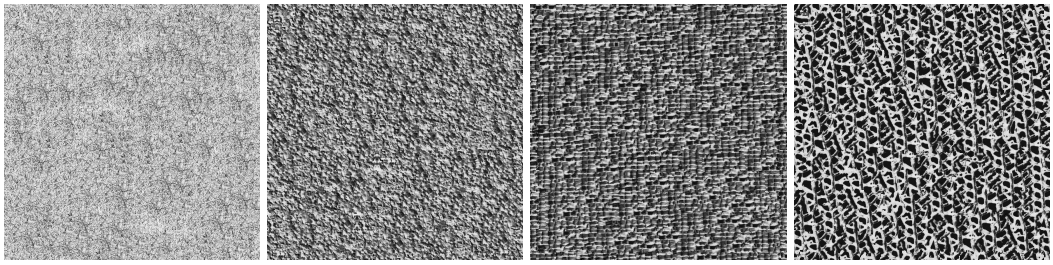
这里举例说明攻破 CASY 隐写算法的概率。假设 $L = L_0 = 16$，并且每条冗余边界的宽度为 4 个像素（远小于 P_d）。此时，正确定位原图的概率为 $P_s(16) \approx 2 \times 10^{-10}$。由于不同的裁剪图像对应不同的候选参数个数 $t_i \geq 1$，因此，正确估计参数 $\{P_w, P_h, P_d\}$ 的概率 $P_b(16) < P_s(16) \approx 2 \times 10^{-10}$。

4.3.3　隐写分析实验与评估

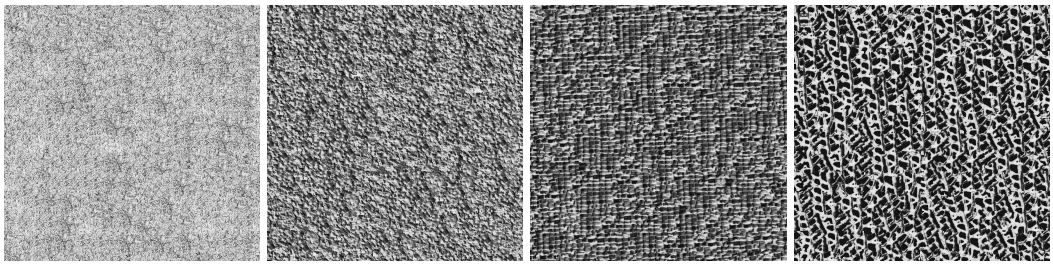
本节采用 ReSid 检测本文提出的隐写方法 CASY，以验证隐写算法的安全性。



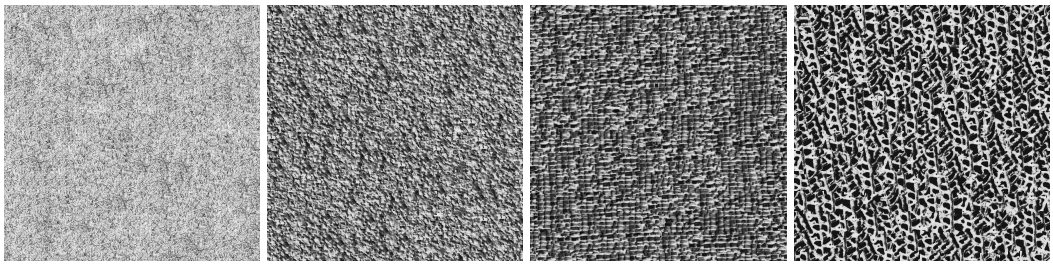
(a) 源图像



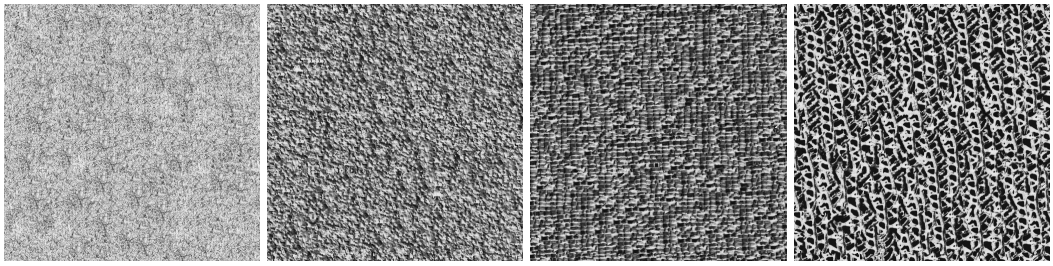
(b) 不含秘密消息的合成纹理图像



(c) 载密图像（5 bpp）



(d) 载密图像（10 bpp）



(e) 载密图像（15 bpp）

图 4.10　源纹理图像和采用 CASY 方法得到的载密纹理图像示意图

图4.10展示了 CASY 算法生成的载体和载密纹理图像的视觉质量。源图像[3]大

小为 512×512，$L_0 = 16$。要使最大嵌入率为 $\gamma_{max} = 13$ bpp，根据公式 (4.18)得到聚类度 $n_D^* = 2$，根据公式 (4.14)可得候选纹理单元数量 $n_S = 9841$。此时，扩增的嵌入量 $\Delta C = 128$ 比特。由于 CASY 隐写方法可以指定合成图像的尺寸，因此，相较于 CASO 方法，CASY 方法具有更强的隐蔽性。

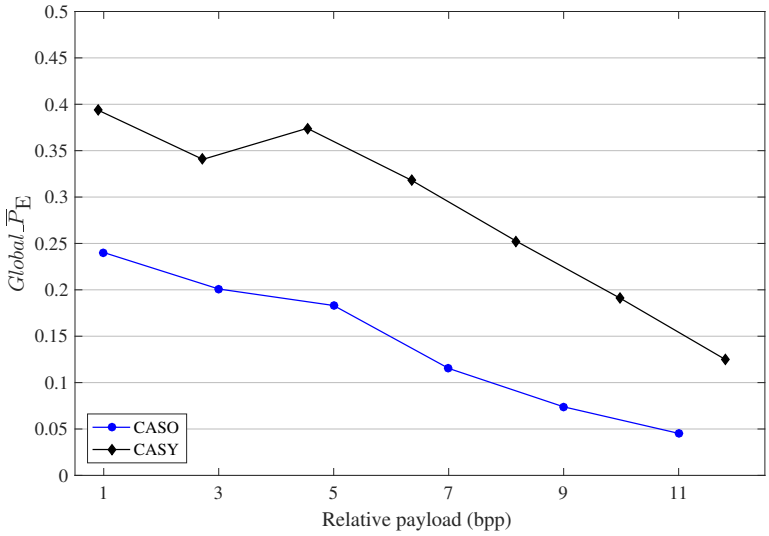


图 4.11　CASY 与 CASO 全局检测错误率对比

如图4.11所示，采用隐写分析方法 ReSid、SRM 和 maxSRM 检测本文提出的 CASY 隐写方法和 Chao 等人提出的 CASO 方法。为了对齐隐写嵌入率，采用公式 (4.22)校准实际嵌入率 $\hat{\gamma} = 0.908\gamma$。实际上，隐写算法的安全性取决于多种隐写分析检测结果中最高的检测准确率，也就是说，隐写算法的安全性是由多种隐写分析算法检测结果的一种集成。因此，本文引入了一种新的隐写安全性的度量指标 $Global\_P_{\mathrm{E}}$[78]：

$$Global\_P_{\mathrm{E}} = \min_{i \in \mathbf{F}} P_{\mathrm{E}}^{i}, \tag{4.25}$$

其中 **F** 为隐写分析算法的集合，P_{E}^{i} 是第 i 个隐写分析算法的检测错误率。

由于 ReSid 无法直接检测 CASY 隐写算法，因此，本文粗略估计 **S** 的大小以进行隐写分析。以 $T_w = T_h = 489$ 为例，选择 **R** 的中心区域作为 **S**，此时 $\{P_w, P_h, P_d\}$ 和 L 均没有正确估计。实验结果表明，在不同隐写分析方法的检测下，本文提出的 CASY 隐写算法优于 CASO，平均检测错误率至少提升 10%，这是由于 CASY 算法对图像边界区域采用了最优的邻域填充。SRM 和 ReSid 分别从两个不同角度来检测隐写算法，其中，SRM 特征是基于局部区域残差的设计的统计特征，ReSid 特征是利用相邻合缝合区域之间的最优性设计的统计特征。本文提出的 CASY 隐写算法使得攻击者无法正确估计参数 $\{P_w, P_h, P_d\}$，阻碍隐

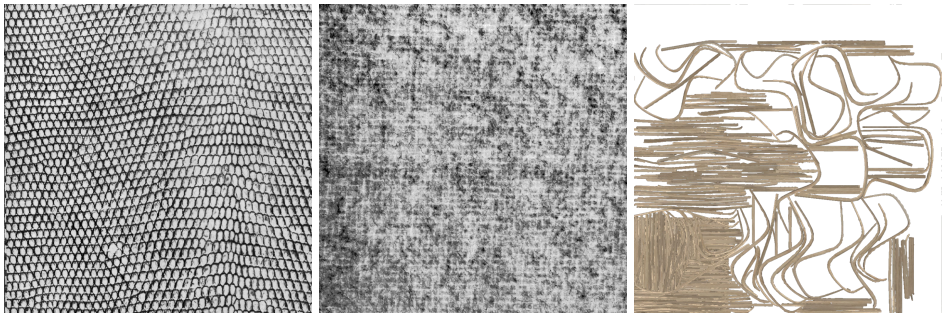
[3]从数据集中随机选了四张纹理图用于隐写效果比较，分别为“1.bmp”、“4.bmp”、“3110.bmp”和“8762.bmp”。

写分析者获得边信息矩阵，使 maxSRM 退化为 SRM。因此，与 CASO 隐写方法相比，CASY 具备更强的抗检测性。

4.3.4　3D 纹理贴图实验

本文将改进的纹理图像隐写算法与 3D 网格模型结合，设计了 3D 纹理贴图隐写方法。由于 MeshLab 3D 处理工具自带纹理贴图处理，因此，通过执行相关软件功能将纹理合成隐写后的图像贴图至 3D 网格模型上，实现多载体隐写方案。实验结果如图4.12所示。

(a) 带纹理贴图的 3D 模型



(b) 纹理图像

图 4.12　带纹理贴图的 3D 模型及其对应的纹理图像

4.4　本章小结

本章提出了两种针对纹理合成隐写算法的隐写分析方法，用作新的纹理图像隐写安全评测方法。这两种方法均通过分析纹理图像的结构特征匹配纹理单元实现隐写分析。同时，为了对抗隐写分析的检测，本章提出在纹理图像边界区

域添加冗余纹理的方法阻碍隐写分析方法对纹理图像单元尺寸的估计，从而阻碍隐写分析。同时，本文将载密纹理图像映射至 3D 网格上，实现多载体隐写的功能。

本章主要贡献包括：

- 设计了基于纹理图像合成隐写在纹理单元缝合过程中产生特性的两种隐写分析方法。第一种方法通过分析纹理镜像对称特征，从而重构原始纹理块，并实现隐写分析。第二种方法通过提取合成区域的最优合成程度作为隐写分析特征，以实现快速有效的隐写分析；
- 设计了基于图像边界荣誉纹理单元填充的增强纹理图像隐写算法，提高了纹理隐写算法的抗检测性。同时，利用 MeshLab 工具箱，实现了实际有效的载密图像 3D 纹理贴图，达到了多载体隐写的目的。

为了方便读者研究和对比本章中提出的方法，实验代码已放在如下的网站上。其中基于镜像攻击的纹理图像隐写分析算法：https://github.com/RyanHangZhou/Texture-Attack，以及基于重构最优性检测的纹理图像隐写分析算法：https://github.com/RyanHangZhou/Texture-Steganalysis。

第 5 章　3D 深度图像隐写方法

本章将主要讨论 3D 深度图像隐写方法，包括基于卷积神经网络的图像隐写算法设计和实验结果分析。5.1节介绍了深度图像深度估计的研究进展；5.2节介绍了基于卷积神经网络的图像隐写网络结构设计、目标损失函数设计和训练策略；5.3节分析了实验结果；5.4节为本章小结。

5.1　引言

多模态集成通信是隐写术的一种特殊应用，它采用隐写算法实现高维信息的自重构或自嵌入，例如彩色图像灰度化和深度图像彩色化等高维数据低维化过程，并且需要保证载体的可自重构性。

深度图像作为 3D 数据的一种表现形式，是目前许多 3D 数据获取设备（TOF 相机、Kinect 和激光扫描等）获取到的原始数据表现形式。深度图像的广泛应用使得我们不得不考虑深度图像内存占用的问题。众所周知，深度图像通常存储为同一路径下的两个单独文件，分别为彩色图像（RGB 图像）和深度，并且具有相同的命名。彩色图像的每个通道由 8 比特数据构成，而深度是由 10 比特数据构成，信息量更为庞大。在使用中必须同时传输或加载，存在深度文件容易丢失的问题。因此，如何在彩色图像中藏深度文件，并同时保证合成图像视觉质量尽可能没有变化，且能够重构原始彩色图像和深度信息，是本文亟需解决的问题。

深度图像存储和使用的不便捷是本章提出 3D 深度图像隐写算法的动机之一。在经典的计算机视觉任务中，已有大量从给定的图像数据集中恢复深度的研究工作，包括三个分支：运动恢复结构（Structure From Motion，简称 SFM）、光场恢复结构和阴影恢复结构。近年来，随着机器学习和深度学习的发展，研究者更多地投入到单张图像恢复深度的研究上。他们将深度恢复的任务视为 RGB 图像深度估计的回归问题，并且分为监督学习和无监督学习的深度估计研究。在监督学习的任务中，训练样本已知深度信息，而在无监督学习的任务中，RGB 图像隐式地给出了深度信息。无监督学习任务中最常见的方法训练集需要提供立体的图像对，或其他形式的多视图[79,80]。这类方法的学习目标与监督学习的任务相同：在测试阶段，对于任意一张输入 RGB 图像，深度估计模型能够估计这张图像的深度。

单目图像深度估计的任务是将单张图像输入至神经网络并输出预测的深度。监督学习的方法直接从 RGB 图像和其对应的深度中训练深度估计网络，而无监督学习的方法是间接地利用给定的数据预测深度，比如训练集为立体图像对。

Saxena 等人[81] 首次提出利用监督学习和马尔可夫随机场的方法训练深度估计模型。随后，有大量的工作[82–85] 基于此方法做了改进。Liu 等人[86] 提出基于卷积神经网络（Convolutional Neural Network，简称 CNN）和条件随机场（Conditional Random Field，简称 CRF）[87,88] 的方法，端到端训练深度估计模型。近年来，也有许多研究者采用自编码器[89–94] 训练深度估计模型，这类模型能够采用网络层数较深的网络，例如采用 ResNet[95] 提升深度估计的性能。Eigen 等人[96] 提出基于多尺度的深度预测方法，能够克服编码器模型中分辨率下降的情况，并因此改善深度估计。还有一些通过设计不同的损失函数以改进深度回归性能的深度估计方法，例如 Laina 等人[92] 提出基于逆向 Huber 损失[97] 的方法以降低 ℓ_2 范数的平滑效果。

近年来，学术界涌现了一批基于无监督学习利用场景的几何信息进行深度估计的方法。Garg 等人[90] 提出利用可微分逆向变形技术和立体图像对进行深度特征学习。Godard 等人[98] 利用了一种几何线索，即在损失函数中增加了左右图的一致性约束以改进深度估计的性能。Zhou 等人[99] 提出了基于场景的光流约束和 GeoNet[80] 的深度估计算法。最近，Wang 等人[79] 提出了直接视觉测距法和深度归一化的方法，明显地提升了深度估计性能。

深度估计算法的研究还有另一分支，称为*对焦与离焦的深度测量*。对焦与离焦估计得到的深度是不同的，分为以下两种情况：相机参数在深度估计时可以更改，和相机参数在深度估计时不可更改。与上述基于运动估计的方法不同，这些方法利用镜片光学几何结构和光线估计深度。Zhuo 等人[100] 提出了基于图像边缘位置上估计空域离焦模糊变化量的方法。还有一些方法基于编码孔径[101–103] 改进深度估计的性能。Suwajanakorn 等人[104]、Tang 等人[105] 和 Surh 等人[106] 均提出了基于焦点栈（多张图像同一场景下，不同焦距）估计不同模糊模型下深度的方法，包括基于环差滤波器的方法[106]，这些方法首先重建全焦点图像，然后优化深度。Srinivasan 等人[107] 提出了花卉图像的光场数据集，并且使用真实的光场图像渲染聚焦图像，然后采用回归模型估计深度，具备迁移到其他全焦点图像深度估计的优势。

5.2　深度图像隐写算法

如前所述，在计算机视觉领域，单目深度估计是一个热门的研究话题，其任务是从单张图像中估计深度信息。这个过程表示为：

$$D = F(I), \tag{5.1}$$

其中 F 是相当复杂的函数，即从二维空间估计三维空间的信息。这个估计任务是困难的，因为即使在人的双眼定位自然世界的物体的情况下依然会有定位不准的问题出现，所以传统的深度估计在单目深度估计上效果并不好。

近年来涌现了一组基于深度网络估计图像深度的解决方案，包括基于多尺度卷积神经网络方法、全卷积网络方法和双目法估计深度。这些算法相较于基于人工特征的深度估计方法有了较为明显的性能提升，但是与基准的深度相比，仍然有较大的差距。不同于从单张图像上进行深度估计，如果能够通过一定的方式将深度信息隐藏于图像中，同时保证合成图像质量的前提下，无需从原图中估计深度，而是从合成图像中恢复深度便可以实现所需要的功能。由于深度与原图像在空间域中有强相关性，因此，彩色图像与深度经过合成之后仍能较好地保留原图像的视觉质量。由于两者仍然存在一定的差异性，因此，恢复深度相比于估计深度具有更好的效果。

5.2.1　算法框架

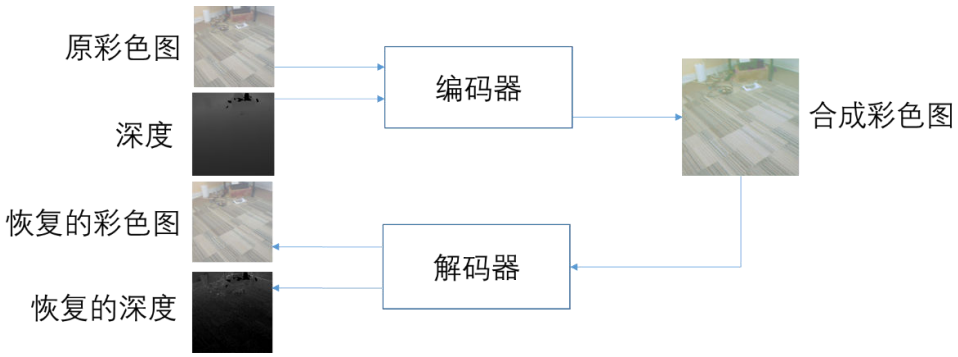


图 5.1　深度图像隐写示意图

基于以上分析，本文提出了基于图像合成的深度图像隐写算法。如图5.1 所示，本文设计了基于卷积深度网络的图像编解码方法，用编码器分别抽取高维彩色图像和深度地图的特征，通过特征级联之后经过另一编码器编码得到合成的彩色图像，称为图像隐藏网络。记彩色图子编码器为 $\mathbb{E}_c$，深度地图子编码器为 $\mathbb{E}_d$，主编码器为 $\mathbb{E}$。记深度图像中的彩色图为 I_o，深度地图为 D_o，合成彩色图为 I_e。为了保证合成图像与原彩色图像的不可检测性，本文设计了基于生成对抗网络的方法约束合成彩色图的质量，使其具备较高的视觉质量。与图像隐藏网络相比，图像提取网络 $\mathbb{D}$ 可视为从合成的彩色图像 I_o 中可逆地提取原始彩色图像 I_d 和深度地图 D_d。

图像隐写的过程表示为

$$I_e = \mathbb{E}([\mathcal{E}_c(I_o); \mathbb{E}_d(D_o)]). \tag{5.2}$$

图像提取的过程表示为

$$[I_d; D_d] = \mathbb{D}(I_e). \tag{5.3}$$

直观地看，纹理区域嵌入秘密消息相比于平滑区域嵌入秘密消息更不容易识别，这也是传统自适应隐写算法设计的基本理念。为了使深度网络更精细地嵌入信息，本文采用对抗学习指导如何合理地在 RGB 图像上嵌入深度地图。

5.2.2　网络结构

1）图像隐藏网络 $\mathbb{E}$

本文将隐藏网络视为一种特殊的编码器，并用作图像合成。遵循方法[108] 中使用的自编码器网络架构，采用批量标准化（Batch Normalization，简称 BN）[109] 稳定训练过程。图像隐藏网络 $\mathbb{E}$ 描述如下：在编码器部分，首先采用一个卷积层和两个残差模块，然后经过两个下采样模块对输入图像进行编码得到特征图。其中，下采样模块包含两个连续的卷积层，步径分别为 2 和 1，然后连接四个残差模块。解码器采用对称的网络结构，采用两个上采样模块将特征映射到与原图像分辨率大小相同的特征上。每个上采样模块由一个最近邻上采样层和两个卷积层构成。然后，连接两个残差模块。最后，采用一个卷积层重构原始图像。其中，所有卷积层的卷积核大小均为 3×3。

2）图像提取网络 $\mathbb{D}$

图像提取网络 $\mathbb{D}$ 由一个卷积层、八个残差模块和两个卷积层构成。为了约束神经网络输出的范围，本文在网络后端增加了一个 tanh 激活层。虽然提取网络 $\mathbb{D}$ 不涉及任何降采样或上采样的操作，但是实验证明这样的网络结构足以进行有效的信息提取。

3）生成对抗网络

Goodfellow 等人[110] 首次提出生成对抗网络（Generative Adversarial Networks，简称 GAN）框架，从随机噪声中通过对抗学习生成逼真的图像。在训练过程中，生成网络 G 用于生成逼真的伪造图像以欺骗判决网络 D，而判决网络 D 用于区分真实图像和 G 生成的伪造图像。GAN 网络的关键元素是对抗损失，而对抗损失在许多图像翻译任务中已证实能够辅助生成具备视觉真实感的图像[111–114]。目前有两种常用的判决器网络：基于全局的判决网络和基于块的判决网络（PatchGAN）。给定输入图像，基于全局的判决网络仅能预测一个标签以表示输入图像是否为真实图像，而基于块的判决网络根据滑动窗口分别对多个区域进行预测。本文采用 PatchGAN 作为判决网络，其主要结构由一个卷积层，步径为 2 的下采样卷积层（以扩大每个局部区域的感受野）和两个卷积层构成。

4）JPEG 压缩模拟网络

通常，用户产生的图像在社交平台的传播过程中，不可避免地会经过图像压缩。图像压缩的目的是为了减少图像在传输过程中产生的负荷。为了降低图像压缩对载密图像提取原 RGB 图像和深度地图的影响，本文在设计编解码网络的同时，加入了一个 JPEG 压缩模拟器，如图5.2所示。不直接将 JPEG 压缩器接到隐写网络中的原因是由于 JPEG 压缩过程不可导，因此，如果直接将 JPEG 压缩模块级联在隐写网络后方，那么神经网络无法进行训练。

为了提高载密图像抗 JPEG 压缩的鲁棒性，本文设计了一种基于深度网络的 JPEG 压缩模拟网络 J 以近似真实 JPEG 压缩的过程。受文献[115] 的启发，在图像隐写网络训练过程中，级联 JPEG 压缩模拟网络并进行训练，以达到隐写算法抗真实 JPEG 压缩的效果。真实 JPEG 压缩的过程简介如下：输入图像被分成若干个 8×8 大小的区域，然后对每个区域进行离散余弦变换（Discrete Cosine Transform，简称 DCT）得到代表不同频率分量的频率系数。最后，根据已有的量化表进行有损量化得到用于霍夫曼编码的 DCT 系数。由于量化对图像质量产生了不可逆的有损压缩，因此，无法使用神经网络进行端到端的学习以实现梯度的反向传播。

图5.2为 JPEG 模拟压缩网络的结构。为了实现网络端到端的训练，本文将上述的量化步骤替换为一个控制 DCT 系数保留数量的门函数矩阵，并用该模板与余弦变换后的图像进行相乘得到量化后的系数，这本质上与量化功能相同。在实现过程中，采用 8×8 大小的卷积核，步径为 8 进行卷积得到 DCT 系数，用于学习 DCT 基向量。随后，采用门函数矩阵进行特征激活。最后，被激活后的特征经过一个转置卷积层进行逆 DCT 变换，并得到模拟 JPEG 压缩的图像。在训练过程中，仅保留前 k 个低频 DCT 系数。相比文献[115] 中采用固定的 k，本文随机选择范围为 $[32, 64]$ 内的 k 值，保证对不同 JPEG 质量因子压缩鲁棒。

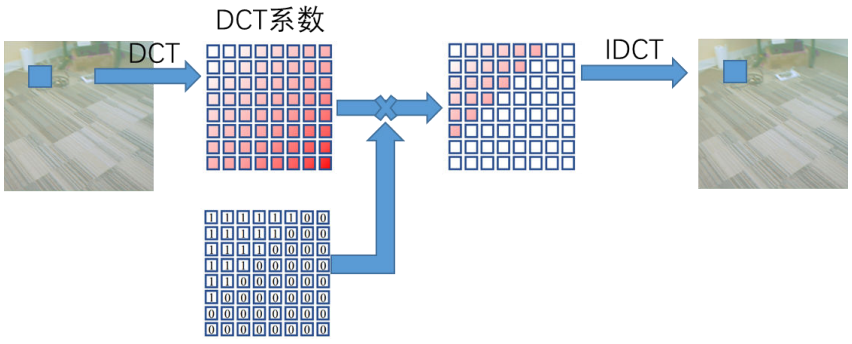


图 5.2　模拟 JPEG 压缩示意图

5.2.3　目标损失函数

1）生成网络的损失函数

均方误差损失 $\mathcal{L}_I$。为了保证合成图与恢复图的视觉质量，直接在原 RGB 图像和合成图像之间，以及原 RGB 图像和重构的 RGB 图像之间使用均方误差损失：

$$\begin{aligned}\mathcal{L}_I(I_o, I_e) &= \|I_o - I_e\|^2, \\ \mathcal{L}_I(I_o, I_d, D_o, D_d) &= \|I_o - I_d\|^2 + \|D_o - D_d\|^2.\end{aligned} \tag{5.4}$$

一致损失 $\mathcal{L}_{conf}$。与文献[108]相同，本文采用一致损失以保证合成的载密图像 I_e 在网络训练初期大致与输入图像 I_o 相近，这有利于缩减网络收敛的时间：

$$\mathcal{L}_{conf}(I_o, I_e) = \|\max(|I_o - I_e| - \tau, 0)\|_1. \tag{5.5}$$

其中，τ 设置为 70。

对比度损失 $\mathcal{L}_{cont}$。对比度损失是为了保证在特征层上原图像与合成图像之间的约束。与文献[108]相同中，本文采用 VGG[116] 网络约束特征层的输出：

$$\mathcal{L}_{cont}(I_o, I_e) = \|VGG_l(I_o) - VGG_l(I_e)\|^2, \tag{5.6}$$

其中，$VGG_l(\cdot)$ 表示 VGG 网络在第 l 层的输出特征，实验中选用“conv4_1”作为输出的层。对比度损失（也称为感知损失）[117] 能有效提高合成图像的质量。

局部结构损失 $\mathcal{L}_{str}$。局部结构损失能够约束像素在局部区域的变化程度：

$$\mathcal{L}_{str}(I_o, I_e) = \|Var(I_o) - Var(I_e)\|_1, \tag{5.7}$$

其中，$Var(\cdot)$ 表示图像的局部标准差。因此，此约束能够保证合成图像的平滑性。

对抗损失 $\mathcal{L}_{gen}$。GAN 网络用于约束合成图像与原图像的近似程度，使合成图像具备视觉真实感。生成网络中的对抗损失由交叉熵损失构成：

$$\mathcal{L}_{gen} = \mathbb{E}[\log_{x \in I_o}(\mathcal{R}(x))]. \tag{5.8}$$

因此，生成器的损失函数由均方误差损失、一致损失、对比度损失、局部结构损失和对抗损失共同构成：

$$\mathcal{L}_G = \mathcal{L}_I(I_o, I_e) + \mathcal{L}_I(I_o, I_e, D_o, D_d) + \alpha\mathcal{L}_{conf} + \beta\mathcal{L}_{cont} + \gamma\mathcal{L}_{str} + \eta\mathcal{L}_{gen}. \tag{5.9}$$

2）判决网络的损失函数

对抗损失损失 $\mathcal{L}_{dis}$。如上所述，GAN 网络损失包含生成网络对抗损失和判决网络对抗损失。为了提高判决网络的分辨能力，本文采用了交叉熵损失：

$$\mathcal{L}_{dis} = \mathbb{E}[\log_{x \in I_o}(\mathcal{R}(x))] - \mathbb{E}[\log_{y \in I_d}(1 - \mathcal{R}(y))]. \tag{5.10}$$

因此，判决器的损失函数由判决网络的交叉熵损失构成：

$$\mathcal{L}_D = \mathcal{L}_{dis}. \tag{5.11}$$

5.2.4　训练策略

网络训练过程考虑了两种训练策略：逐步训练和混合训练。以下是这两种策略的动机和细节。

逐步训练。训练深度图像隐写的任务具有一定的挑战性，因为有些损失函数之间优化的目标是相悖的，因此，如果直接使用端到端训练网络，网络不容易收敛。而且，训练抗 JPEG 压缩的隐写网络更为复杂。为了减轻网络训练的难度，本文采用分段训练策略进行网络训练。第一步，仅训练隐写网络 $\mathbb{E}$ 和提取网络 $\mathbb{D}$，它们用于深度地图的有效嵌入和提取。第二步，加入判决网络 $\mathcal{L}_{gen}$ 和 $\mathcal{L}_{dis}$ 的训练，以约束载密图像与原 RGB 图像的不可区分。第三步，若考虑抗 JPEG 压缩，则加入模拟 JPEG 压缩网络模块进行训练。通过上述三个步骤的训练，网络能够更快收敛，并得到较好的隐写结果。

混合训练。在训练抗 JPEG 压缩的网络时，本文采用 JPEG 压缩模拟网络模拟 JPEG 压缩的过程。然而，通过实验发现，训练好的模型在模拟 JPEG 压缩的输出上有较好的鲁棒隐写效果，而在真实 JPEG 压缩的输出结果上隐写鲁棒性较差，有明显的过拟合效应。因此，在训练网络时，每一批训练图像包括 2 张 JPEG 压缩得到的图像、4 张模拟 JPEG 压缩得到的图像和 2 张压缩前的图像。采用该策略能够有效降低网络的过拟合效应。

5.3　实验结果

5.2节主要介绍了基于深度卷积神经网络的深度图像隐写和提取算法的细节。为了验证本算法的有效性，本节将先介绍数据集设置与实验细节，然后再给出与现有基准方法的详细对比结果。

5.3.1　实验环境配置和细节

本文采用 NYU 深度数据集 V2 训练深度图像隐写网络模型。从数据集中随机采样 16000 张图像作为训练集，每张图像缩放至 256×256 大小。训练时批处理大小为 8，迭代 40 万次，并且采用逐步训练策略。

优化器采用的是 Adam[118] 优化算法，第一步的初始学习率是 $1e-4$，在 20 万次迭代后衰减到 $1e-6$。；第二步和第三步的学习率均初始化为 $1e-5$，并且在 10 万次迭代后衰减为 $1e-7$。对于判决网络，初始学习率设为 $2e-4$。损失函数之间的权重设为 $\alpha = 0.5, \beta = 1e-7, \gamma = 5, \eta = 1$。

5.3.2　与基准方法的对比

如前所述，本文提出的深度图像隐写系统有如下三个目标：

- 载密图像与原 RGB 图像在视觉上没有明显的失真。
- 提取的 RGB 图像与原 RGB 图像没有明显的失真；提取的深度地图与输入的深度地图没有明显的失真。
- 当考虑 JPEG 压缩时，加入模拟 JPEG 压缩模拟网络后训练的隐写网络进行深度图像隐写时对 JPEG 压缩鲁棒。

5.3.2.1　无损隐写质量评估

1）定量评估

采用峰值信噪比（PSNR）评估图像质量。如图5.3 所示，隐写后的图像以及重构得到的 RGB 图像和深度地图从视觉上看几乎没有明显的失真。

如表5.1所示，在不考虑 JPEG 压缩时，训练好的隐写模型经过测试样本的测试后，载密图像的平均 PSNR 值为 42.45dB，恢复的 RGB 图像平均 PSNR 值为 41.56dB，恢复的深度地图平均 PSNR 值为 47.16dB。而目前性能最优的深度估计算法[119] 估计的深度 PSNR 最高不超过 39dB，因此，相比而言，本文采用以图藏图的技术能实现更优的深度重构。

表 5.1 不抗 JPEG 压缩的隐写前后图像 PSNR 值

载密图像 I_o	提取的 RGB 图像 I_d	提取的深度 D_d
42.45dB	41.56dB	47.16dB

2）定性评估

图5.3给出了三组不同样本的深度图像隐写结果。从视觉上看，载密图像、提取的 RGB 图像和深度地图均没有明显的噪声，具有良好的视觉结果，证明了本文提出的深度图像隐写算法的有效性。

5.3.2.2　鲁棒隐写质量评估

1）定量评估

如表5.2所示，在考虑 JPEG 压缩的情况下，训练好的隐写模型经过测试样本的测试后，载密图像的平均 PSNR 值为 18.52dB，而经过模拟压缩之后重构的深度 PSNR 值为 38.02dB，经过不同质量因子下的 JPEG 压缩后的 PSNR 值始终高

(a) 原 RGB 图像 I_o

(b) 原深度地图 D_o

(c) 隐写后的载密图像 I_e

(d) 重构的 RGB 图像 I_d

(e) 重构的深度地图 D_d

图 5.3　不抗 JPEG 压缩的隐写前后图像示意图

于 30dB。若不加入 JPEG 模拟压缩模块，则经过 JPEG 压缩之后恢复的深度地图的 PSNR 值只有 10dB 左右，因此，证明了本文提出的深度图像鲁棒隐写算法的有效性。

表 5.2 抗 JPEG 压缩的隐写前后图像 PSNR 值

载密 I_o	提取的深度 D_d				提取的 RGB 图像 I_d		
	模拟压缩	QF=75	QF=95	QF=100	QF=75	QF=95	QF=100
18.52dB	38.02dB	31.64dB	35.02dB	35.02dB	27.12dB	28.77dB	29.01dB

2）定性评估

图5.4和图5.5给出了三组不同样本的深度图像抗 JPEG 压缩的隐写结果。从视觉上看，经过 JPEG 压缩之后提取的 RGB 图像和深度地图仍然具有良好的视觉结果。

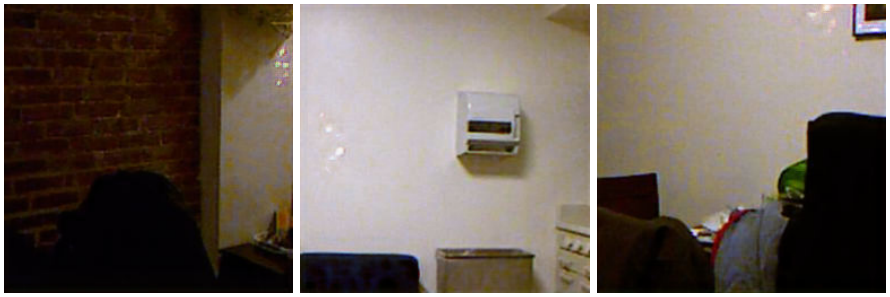
5.4　本章小结

本章提出了基于图像合成的深度图像隐写算法，该方法作为多模态集成通信的一种特殊应用，能够实现高维信息的自重构或自嵌入，达到隐蔽通信的用途。在网络设计上，本文采用深度卷积网络进行隐写和信息提取，以及采用对抗生成网络约束载密图像与原始图像的不可区分性。本章分别在无损隐写和鲁棒隐写上进行了实验，验证了算法的有效性。

本章主要贡献包括：

- 设计了基于深度卷积网络图像合成的深度图像隐写算法，挖掘了 RGB 图像和深度地图之间的相关性，并据此设计了隐写网络、提取网络和生成对抗网络，实现了有效的隐写嵌入和图像提取的实验效果；
- 设计了模拟 JPEG 压缩网络，能够有效减少 JPEG 压缩对 RGB 图像和深度地图的重构产生的失真。

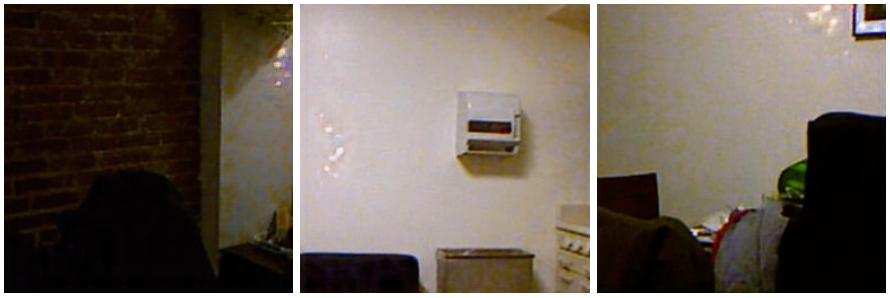
(a) 原 RGB 图像 I_o



(b) 模拟 JPEG 压缩后重构的 RGB 图像

(c) 质量因子为 75 时 JPEG 压缩后重构的 RGB 图像

(d) 质量因子为 95 时 JPEG 压缩后重构的 RGB 图像

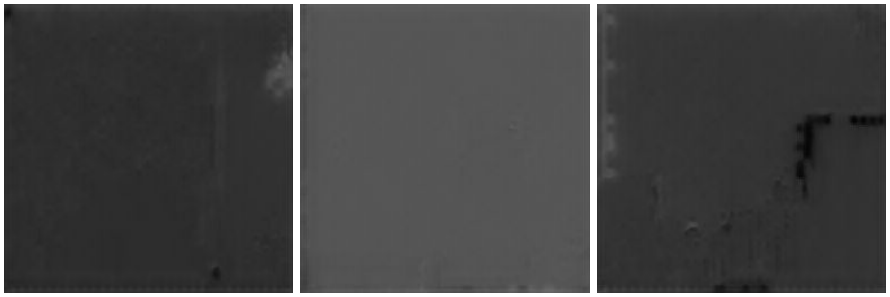


(e) 质量因子为 100 时 JPEG 压缩后重构的 RGB 图像

图 5.4　抗 JPEG 压缩的隐写前后图像示意图

(f) 原深度地图 D_o。

(g) 模拟 JPEG 压缩后重构的深度地图



(h) 质量因子为 75 时 JPEG 压缩后重构的深度地图

(i) 质量因子为 95 时 JPEG 压缩后重构的深度地图

(j) 质量因子为 100 时 JPEG 压缩后重构的深度地图

图 5.5　抗 JPEG 压缩的隐写前后图像示意图

第 6 章　总结与展望

6.1　工作总结

3D 隐写模型与方法的研究面临着三个关键科学问题：3D 网格隐写研究、3D 纹理图像贴图隐写研究和 3D 深度图像隐写研究。这三个方面的研究内容相辅相成，旨在实现高安全性的 3D 隐写方法。现将这三个方面的主要工作与创新点阐述如下：

1）3D 网格模型隐写安全性分析

现阶段 3D 网格隐写分析主要根据坐标点信息或边信息的相关性强弱设计的隐写分析特征，分类效果不够明显。由于 3D 网格模型隐写会破坏坐标点邻域的相关性，本文通过分析三角面邻域相关性，提出基于三角面邻域法向量张量投票模型的特征以提升 3D 网格隐写分析性能，形成了新的 3D 网格隐写安全评测方法。

2）基于最小化失真框架的 3D 网格模型隐写

现阶段的自适应隐写基本采用 Filler 等人提出的 STC 编码嵌入秘密消息。STC 编码是一种能够接近最优嵌入的编码，隐写者只需定义好失真函数，STC 编码即可根据失真选择出合适的修改模式嵌入秘密消息；对于接收方而言，只要知道消息的长度，无需知道失真矩阵就能正确提取秘密消息。该框架解决了隐写算法设计中的编码问题，因此，隐写设计的重点就落在了失真函数的合理定义上。本文依据坐标点之间的位置、曲率、顶点法向量等特性定义失真函数，并借助 STC 编码嵌入消息，提升了 3D 网格隐写算法的安全性。

3）纹理图像合成隐写安全性分析

纹理图像合成技术的发展使得隐写者有了新的隐写载体，同时由于纹理图像本身具有的全局复杂性和近似周期性使得隐写分析者难以对载密纹理图像进行隐写分析。针对已有的纹理合成图像的隐写方法，本文发现其基于纹理图像抽样获取候选纹理单元的方法有漏洞，容易受到隐写分析的检测。本文提出另一种隐写分析方法，采用纹理缝补技术重构合成图像中每一缝合区域的原始图像块，并从中判断重构区域的最优性，有效提升了隐写分析性能，形成了新的纹理图像隐写安全评测方法。

4）基于 3D 纹理贴图的隐写方法

针对纹理合成隐写算法的漏洞，本文改进了已有的算法，使得攻击者无法准确估计出合成块的尺寸因而无法实施攻击。本文设计了一种基于密钥控制的边界区域填充的纹理合成隐写，提升了隐写安全性。本文进一步将纹理图像隐写与

3D 网格模型结合，设计 3D 纹理贴图隐写方法，实现了多域联合隐写，扩展了隐写容量。

5）3D 深度图像隐写理论与方法

深度图像作为 3D 数据的一种表现形式，是目前许多 3D 数据获取设备获取到的原始数据。深度图像通常存储为同一路径下的两个单独文件，在使用中必须同时传输或加载，存在深度文件容易丢失的问题。深度图像隐写的任务是在彩色图像中隐藏深度文件，不仅需要保证合成图像视觉质量，而且需要保证重构的彩色图像和深度信息的质量。本文提出了基于图像合成的深度图像隐写算法，采用两个编码器分别抽取彩色图像和深度图像的高维特征，通过特征级联之后再经过另一编码器编码得到合成的彩色图像，实现隐写术的一种特殊应用，即多模态集成通信。

6.2　未来工作展望

本文虽然提出了 3D 数据的多种隐写方法，但面对快速发展的隐写分析和深度学习技术，3D 模型隐写的相关研究仍有很多值得开拓的空间。这里对本文的改进空间和可能的发展方向做出简要阐述。

6.2.1　3D 网格隐写算法

实现更高的隐写安全性是 3D 网格隐写的目标，因此，本文以下提出改进方法。

1）融合扰动隐写和置换隐写算法

联合置换隐写和 LSB 隐写是提升隐写安全性的一种方法。实验证明，当网格的顶点数为 5000 时，置换隐写最大嵌入率达到 11bpv，可视为大容量隐写。随着嵌入率的增加，抗通用隐写分析和置换隐写分析的安全性也随之下降。因此，如何在两个域中最优地分配消息长度，是设计更优 3D 网格隐写算法的关键。

2）设计非加性失真函数模型

图像自适应隐写算法的最新研究表明，利用相邻元素之间的相关性提升隐写算法的安全性，称为非加性失真模型[120,121]。本文在 3D 网格模型的 xyz 轴上平均分配消息长度，没有考虑三个分量上嵌入消息之后的相互影响。如何对坐标点设计联合失真，并利用 DeJoin[122] 算法分配消息长度，最后利用 STC 编码[18] 嵌入消息，是一种实现更高安全隐写算法的可能方式。

3）针对置换隐写分析设计增强置换隐写算法

Wang 等人[52] 提出了一种基于邻域嵌入的置换隐写算法，该方法利用消息

比特序列中 $\lfloor \log_2 i \rfloor$ 比特代表的信息，从当前顶点领域的 i 个未被选用过的顶点中选择顶点以嵌入秘密消息。文献[73] 中已证明 $1 \leq i \leq 11$，并在大多数情况下 $i = 6$[73]，即平均嵌入率为 2bpv，因此，此隐写方法嵌入率较低。此外，Wang 等人[52] 提出的方法缺乏严格的隐写分析实验，因此，有望设计一种基于多环邻域的置换隐写算法提高嵌入率。另一种解决方案是将顶点列表均匀划分为多段并分段嵌入秘密消息。

4）设计 3D 网格批隐写算法

批隐写和池化隐写分析问题是隐写领域中的公开问题[123]，是一类批数据的隐写和隐写分析问题。对于图像隐写而言，安全隐写容量与载体长度的平方根成正比[124]。因此，探究 3D 网格的安全容量与顶点数量之间是否存在上述关系则是一个具有挑战性的问题。

6.2.2　3D 网格隐写分析算法

1）设计 3D 通用隐写分析富模型

由于低嵌入率下的两态调制隐写和最低位隐写算法得到的载密网格模型不容易被目前最优的隐写分析算法检测到，因此，隐写分析算法存在较大的改进空间。Fridrich 和 Kodovskỳ 提出的富模型特征[10] 是基于多个线性和非线性高通滤波器和高维量化噪声残差特征设计的，能有效检测载密图像。受其启发，可以利用更多的 3D 网格平滑技术提取更为丰富的残差特征。这些技术包括早期经典的平滑方法，例如去噪和抹平[125]，以及最新的曲面平滑技术，例如各向异性扩散流[126]、双边滤波[127]、非线性平滑[128,129] 和基于神经网络的滤波方法[130]。

设计更多的特征也可能提升隐写分析性能，比如张量能够体现局部区域向量的某些特性。实验结果表明，顶点法向量，边法向量，边向量的张量都能够反映局部平滑程度。另一种改进的角度是考虑 n 环邻域特征（$n > 1$）。当邻域元素更多时，隐写分析特征更容易检测隐写扰动。

此外，当前用于降维的统计矩可能会过度地丢弃有效的隐写分析特征。本文发现，目前的隐写分析特征维数只有三种情况（顶点数、边数或三角面数），因此，可以单独训练这三个子分类器并投票表决集成分类，这也可能提升隐写分析的性能。

除上述几点外，3D 网格特征提取的复杂度明显高于图像的特征提取，因此，还需考虑 3D 网格隐写分析时工程开发的高效性，例如采用并行处理或更为高效的数据结构以解决相邻顶点搜索的问题。

2）设计基于深度学习的隐写分析方法

迄今为止，现有的隐写分析特征都是人工设计的特征，而这些人工特征设

计较为复杂，不容易在短时间内设计出来。近年来，深度学习在多种机器学习分类问题上展现了卓越的性能。深度神经网络（Deep Neural Networks，简称 DNN）从大量的训练数据中学习模型和分类测试数据，例如卷积神经网络[131]和图卷积网络（Graph Convolutional Networks，简称 GCN）[132]等。3D 网格本身存在的拓扑属性与 GCN 或 MeshNet[133]一致，因此，改编 MeshNet 网络结构，设计端到端学习的神经网络，并使用反向传播算法训练网络，是提高 3D 网格隐写分析性能的一种解决方案。

3）设计针对置换隐写的隐写分析方法

为了检测置换隐写算法，Wang 等人[52]提出了基于结构元素列表邻域相关性的 3D 网格隐写分析方法。然而，该研究没有提供定量结果，有待进一步的研究。此外，顶点列表 $\mathcal{P}$ 中相邻两个顶点的距离并不足以作为有效的隐写分析特征，因为拓扑结构中相邻顶点的距离更能反应隐写造成的失真：

$$D(\mathcal{P}) = \frac{1}{n}\sum_{i=1}^{n}\frac{1}{|\mathcal{N}_1(v_i)|}\sum_{v_j\in\mathcal{N}(v_i)} d(\mathbf{p}_i, \mathbf{p}_j). \tag{6.1}$$

4）载源失配问题

当训练集和测试集数据来源于不同数据集时，会造成测试集检测错误率增高的现象，称之为载源失配问题。为了削弱此现象，可以扩大 3D 网格训练集的多样性，或在多个不同源上各自训练检测器并在测试阶段选择最靠近源数据的检测器进行测试。

6.2.3　3D 纹理贴图

多模态集成通信是隐写术的一种特殊应用，采用隐写算法实现高维信息的自嵌入。“以图藏图”[108]的技术属于多模态集成通信，也是隐写术的一种特殊应用。考虑“以网格藏图”的应用场景，将纹理图像隐藏于 3D 网格中，实现多模态通信。

参考文献

[1] Li B, He J, Huang J, et al. A survey on image steganography and steganalysis[J]. Journal of Information Hiding and Multimedia Signal Processing. 2011, 2 (2): 142–172.

[2] Pevný T, Fridrich J J. Benchmarking for steganography[C]//Solanki K, Sullivan K, Madhow U, Information Hiding, 10th International Workshop, IH 2008, Santa Barbara, CA, USA, May 19-21, 2008, Revised Selected Papers: volume 5284. [S.l.]: Springer, 2008: 251–267.

[3] Petitcolas F A, Anderson R J, Kuhn M G. Information hiding-a survey[J]. Proceedings of the IEEE. 1999, 87 (7): 1062–1078.

[4] 王朔中, 张新鹏, 张开文. 数字密写和密写分析: 互联网时代的信息战技术[M]. 北京: 清华大学出版社有限公司, 2005.

[5] 赵险峰, 张弘. 隐写学原理与技术[M]. 北京: 科学出版社, 2018.

[6] Pevný T, Filler T, Bas P. Using high-dimensional image models to perform highly undetectable steganography[C]//Böhme R, Fong P W L, Safavi-Naini R, Information Hiding - 12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010, Revised Selected Papers: volume 6387. [S.l.]: Springer, 2010: 161–177.

[7] Pevný T, Bas P, Fridrich J J. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Trans. Information Forensics and Security. 2010, 5 (2): 215–224.

[8] Holub V, Fridrich J J. Designing steganographic distortion using directional filters[C]//2012 IEEE International Workshop on Information Forensics and Security, WIFS 2012, Costa Adeje, Tenerife, Spain, December 2-5, 2012. [S.l.]: IEEE, 2012: 234–239.

[9] Holub V, Fridrich J J. Digital image steganography using universal distortion[C]//Puech W, Chaumont M, Dittmann J, et al., ACM Information Hiding and Multimedia Security Workshop, IH&MMSec '13, Montpellier, France, June 17-19, 2013. [S.l.]: ACM, 2013: 59–68.

[10] Fridrich J J, Kodovský J. Rich models for steganalysis of digital images[J]. IEEE Trans. Information Forensics and Security. 2012, 7 (3): 868–882.

[11] Fridrich J J, Kodovský J. Multivariate gaussian model for designing additive distortion for steganography[C]//IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2013, Vancouver, BC, Canada, May 26-

31, 2013. [S.l.]: IEEE, 2013: 2949–2953.

[12] Sedighi V, Fridrich J J, Cogranne R. Content-adaptive pentary steganography using the multivariate generalized gaussian cover model[C]//Alattar A M, Memon N D, Heitzenrater C, Media Watermarking, Security, and Forensics 2015, San Francisco, CA, USA, February 9-11, 2015, Proceedings: volume 9409. [S.l.]: SPIE, 2015: 94090H.

[13] Sedighi V, Cogranne R, Fridrich J J. Content-adaptive steganography by minimizing statistical detectability[J]. IEEE Trans. Information Forensics and Security. 2016, 11 (2): 221–234.

[14] Guo L, Ni J, Shi Y. Uniform embedding for efficient JPEG steganography[J]. IEEE Trans. Information Forensics and Security. 2014, 9 (5): 814–825.

[15] Guo L, Ni J, Su W, et al. Using statistical image model for JPEG steganography: Uniform embedding revisited[J]. IEEE Trans. Information Forensics and Security. 2015, 10 (12): 2669–2680.

[16] Wang Z, Zhang X, Yin Z. Hybrid distortion function for JPEG steganography[J]. J. Electronic Imaging. 2016, 25 (5): 050501.

[17] Wei Q, Yin Z, Wang Z, et al. Distortion function based on residual blocks for JPEG steganography[J]. Multim. Tools Appl. 2018, 77 (14): 17875–17888.

[18] Filler T, Judas J, Fridrich J J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. IEEE Trans. Information Forensics and Security. 2011, 6 (3-2): 920–935.

[19] Cayre F, Macq B. Data hiding on 3-d triangle meshes[J]. IEEE Trans. Signal Process. 2003, 51 (4): 939–949.

[20] Wang C M, Cheng Y M. An efficient information hiding algorithm for polygon models[C]//Wiley Online Library, Computer Graphics Forum: volume 24. [S.l.]: Wiley Online Library, 2005: 591–600.

[21] Chao M, Lin C, Yu C, et al. A high capacity 3d steganography algorithm[J]. IEEE Trans. Vis. Comput. Graph. 2009, 15 (2): 274–284.

[22] Itier V, Puech W. High capacity data hiding for 3d point clouds based on static arithmetic coding[J]. Multim. Tools Appl. 2017, 76 (24): 26421–26445.

[23] Li Z, Beugnon S, Puech W, et al. Rethinking the high capacity 3d steganography: Increasing its resistance to steganalysis[C]//2017 IEEE International Conference on Image Processing, ICIP 2017, Beijing, China, September 17-20, 2017. [S.l.]: IEEE, 2017: 510–414.

[24] Yang Y, Peyerimhoff N, Ivrissimtzis I P. Linear correlations between spatial and

normal noise in triangle meshes[J]. IEEE Trans. Vis. Comput. Graph. 2013, 19 (1): 45–55.

[25] Li N, Hu J, Sun R, et al. A high-capacity 3d steganography algorithm with adjustable distortion[J]. IEEE Access. 2017, 5: 24457–24466.

[26] Bogomjakov A, Gotsman C, Isenburg M. Distortion-free steganography for polygonal meshes[J]. Comput. Graph. Forum. 2008, 27 (2): 637–642.

[27] Huang N, Li M, Wang C. Toward optimal embedding capacity for permutation steganography[J]. IEEE Signal Process. Lett. 2009, 16 (9): 802–805.

[28] Tu S, Tai W, Isenburg M, et al. An improved data hiding approach for polygon meshes[J]. The Visual Computer. 2010, 26 (9): 1177–1181.

[29] Tu S, Hsu H, Tai W. Permutation steganography for polygonal meshes based on coding tree[J]. International Journal of Virtual Reality. 2010, 9 (4): 55–60.

[30] Tu S, Tai W. A high-capacity data-hiding approach for polygonal meshes using maximum expected level tree[J]. Comput. Graph. 2012, 36 (6): 767–775.

[31] Cho J, Prost R, Jung H. An oblivious watermarking for 3-d polygonal meshes using distribution of vertex norms[J]. IEEE Trans. Signal Process. 2007, 55 (1): 142–155.

[32] Kanai S, Date H, Kishinami T, et al. Digital watermarking for 3d polygons using multiresolution wavelet decomposition[C]//International Workshop on Geometric Modeling: Fundamentals and Applicattion: volume 5. [S.l.], 1998: 296–307.

[33] Efros A A, Freeman W T. Image quilting for texture synthesis and transfer[C]//Pocock L, Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH 2001, Los Angeles, California, USA, August 12-17, 2001. [S.l.]: ACM, 2001: 341–346.

[34] Kwatra V, Essa I A, Bobick A F, et al. Texture optimization for example-based synthesis[J]. ACM Trans. Graph. 2005, 24 (3): 795–802.

[35] Dong F, Ye X. Multiscaled texture synthesis using multisized pixel neighborhoods[J]. IEEE Computer Graphics and Applications. 2007, 27 (3): 41–47.

[36] Otori H, Kuriyama S. Data-embeddable texture synthesis[C]//Butz A, Fisher B D, Krüger A, et al., Smart Graphics, 7th International Symposium, SG 2007, Kyoto, Japan, June 25-27, 2007, Proceedings: volume 4569. [S.l.]: Springer, 2007: 146–157.

[37] Otori H, Kuriyama S. Texture synthesis for mobile data communications[J]. IEEE Computer Graphics and Applications. 2009, 29 (6): 74–81.

[38] Wu K, Wang C. Steganography using reversible texture synthesis[J]. IEEE Trans.

Image Process. 2015, 24 (1): 130–139.

[39] Robust steganography using texture synthesis[C]//Qian Z, Zhou H, Zhang W, et al.: volume 1. [S.l.], 2017.

[40] Wei L, Levoy M. Texture synthesis over arbitrary manifold surfaces[C]//Pocock L, Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH 2001, Los Angeles, California, USA, August 12-17, 2001. [S.l.]: ACM, 2001: 355–360.

[41] Turk G. Texture synthesis on surfaces[C]//Pocock L, Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH 2001, Los Angeles, California, USA, August 12-17, 2001. [S.l.]: ACM, 2001: 347–354.

[42] Waechter M, Moehrle N, Goesele M. Let there be color! large-scale texturing of 3d reconstructions[C]//Fleet D J, Pajdla T, Schiele B, et al., Computer Vision - ECCV 2014 - 13th European Conference, Zurich, Switzerland, September 6-12, 2014, Proceedings, Part V: volume 8693. [S.l.]: Springer, 2014: 836–850.

[43] Simmons G J. The prisoners' problem and the subliminal channel[C]//Chaum D, Advances in Cryptology, Proceedings of CRYPTO '83, Santa Barbara, California, USA, August 21-24, 1983. [S.l.]: Plenum Press, New York, 1983: 51–67.

[44] Fawcett T. Roc graphs: Notes and practical considerations for researchers[J]. Machine Learning. 2004, 31 (1): 1–38.

[45] Chang C, Lin C. LIBSVM: A library for support vector machines[J]. ACM Trans. Intell. Syst. Technol. 2011, 2 (3): 27:1–27:27.

[46] Fan R, Chang K, Hsieh C, et al. LIBLINEAR: A library for large linear classification[J]. J. Mach. Learn. Res. 2008, 9: 1871–1874.

[47] Kodovský J, Fridrich J J, Holub V. Ensemble classifiers for steganalysis of digital media[J]. IEEE Trans. Information Forensics and Security. 2012, 7 (2): 432–444.

[48] Chen X, Golovinskiy A, Funkhouser T A. A benchmark for 3d mesh segmentation[J]. ACM Trans. Graph. 2009, 28 (3): 73.

[49] Lai K, Bo L, Fox D. Unsupervised feature learning for 3d scene labeling[C]//2014 IEEE International Conference on Robotics and Automation, ICRA 2014, Hong Kong, China, May 31 - June 7, 2014. [S.l.]: IEEE, 2014: 3050–3057.

[50] Silberman N, Hoiem D, Kohli P, et al. Indoor segmentation and support inference from RGBD images[C]//Fitzgibbon A W, Lazebnik S, Perona P, et al., Computer Vision - ECCV 2012 - 12th European Conference on Computer Vision, Florence, Italy, October 7-13, 2012, Proceedings, Part V: volume 7576. [S.l.]: Springer,

2012: 746–760.

[51] Wang C, Wang P. Steganography on point-sampled geometry[J]. Comput. Graph. 2006, 30 (2): 244–254.

[52] Wang Y, Kong L, Qian Z, et al. Breaking permutation-based mesh steganography and security improvement[J]. IEEE Access. 2019, 7: 183300–183310.

[53] Bors A G, Luo M. Optimized 3d watermarking for minimal surface distortion[J]. IEEE Trans. Image Process. 2013, 22 (5): 1822–1835.

[54] Yang Y, Ivrissimtzis I P. Mesh discriminative features for 3d steganalysis[J]. ACM Trans. Multim. Comput. Commun. Appl. 2014, 10 (3): 27:1–27:13.

[55] Li Z, Bors A G. 3d mesh steganalysis using local shape features[C]//2016 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2016, Shanghai, China, March 20-25, 2016. [S.l.]: IEEE, 2016: 2144–2148.

[56] Kim D, Jang H, Choi H, et al. Improved 3d mesh steganalysis using homogeneous kernel map[C]//Kim K, Joukov N, Information Science and Applications 2017 - ICISA 2017, Macau, China, 20-23 March 2017: volume 424. [S.l.]: Springer, 2017: 358–365.

[57] Li Z, Bors A G. Steganalysis of 3d objects using statistics of local feature sets[J]. Inf. Sci. 2017, 415: 85–99.

[58] Li Z, Gong D, Liu F, et al. 3d steganalysis using the extended local feature set[C]//2018 IEEE International Conference on Image Processing, ICIP 2018, Athens, Greece, October 7-10, 2018. [S.l.]: IEEE, 2018: 1683–1687.

[59] Li Z, Bors A G. Steganalysis of meshes based on 3d wavelet multiresolution analysis[J]. Inf. Sci. 2020, 522: 164–179.

[60] Li Z, Bors A G. Selection of robust features for the cover source mismatch problem in 3d steganalysis[C]//23rd International Conference on Pattern Recognition, ICPR 2016, Cancún, Mexico, December 4-8, 2016. [S.l.]: IEEE, 2016: 4256–4261.

[61] Li Z, Bors A G. Selection of robust and relevant features for 3-d steganalysis[J]. IEEE Trans. Cybern. 2020, 50 (5): 1989–2001.

[62] Fridrich J J, Goljan M, Hogea D. Steganalysis of JPEG images: Breaking the F5 algorithm[C]//Petitcolas F A P, Information Hiding, 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7-9, 2002, Revised Papers: volume 2578. [S.l.]: Springer, 2002: 310–323.

[63] Kodovský J, Fridrich J J. Calibration revisited[C]//Felten E W, Dittmann J, Fridrich J J, et al., Multimedia and Security Workshop, MM&Sec 2009, Prince-

ton, NJ, USA, September 07 - 08, 2009. [S.l.]: ACM, 2009: 63–74.

[64] Taubin G. A signal processing approach to fair surface design[C]//Mair S G, Cook R, Proceedings of the 22nd Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH 1995, Los Angeles, CA, USA, August 6-11, 1995. [S.l.]: ACM, 1995: 351–358.

[65] Li Z, Liu F, Bors A G. 3d steganalysis using laplacian smoothing at various levels[C]//Sun X, Pan Z, Bertino E, Cloud Computing and Security - 4th International Conference, ICCCS 2018, Haikou, China, June 8-10, 2018, Revised Selected Papers, Part VI: volume 11068. [S.l.]: Springer, 2018: 223–232.

[66] Medioni G, Tang C K, Lee M S. Tensor voting: Theory and applications[J]. Proceedings of RFIA, Paris, France. 2000, 3.

[67] Sun Y, Paik J K, Koschan A F, et al. Triangle mesh-based edge detection and its application to surface segmentation and adaptive surface smoothing[C]//Proceedings of the 2002 International Conference on Image Processing, ICIP 2002, Rochester, New York, USA, September 22-25, 2002. [S.l.]: IEEE, 2002: 825–828.

[68] Yadav S K, Reitebuch U, Polthier K. Mesh denoising based on normal voting tensor and binary optimization[J]. IEEE Trans. Vis. Comput. Graph. 2018, 24 (8): 2366–2379.

[69] Zhou H, Chen K, Zhang W, et al. Distortion design for secure adaptive 3-d mesh steganography[J]. IEEE Trans. Multimedia. 2019, 21 (6): 1384–1398.

[70] Breiman L. Bagging predictors[J]. Mach. Learn. 1996, 24 (2): 123–140.

[71] Weisstein E W. Bonferroni correction[M]//[S.l.]: [s.n.], 2004.

[72] Filler T, Fridrich J J. Gibbs construction in steganography[J]. IEEE Trans. Information Forensics and Security. 2010, 5 (4): 705–720.

[73] Jiang R, Zhou H, Zhang W, et al. Reversible data hiding in encrypted three-dimensional mesh models[J]. IEEE Trans. Multimedia. 2018, 20 (1): 55–67.

[74] Fridrich J J, Soukal D. Matrix embedding for large payloads[J]. IEEE Trans. Information Forensics and Security. 2006, 1 (3): 390–395.

[75] Max N. Weights for computing vertex normals from facet normals[J]. J. Graphics, GPU, & Game Tools. 1999, 4 (2): 1–6.

[76] Cheng Y, Wang C. A high-capacity steganographic approach for 3d polygonal meshes[J]. The Visual Computer. 2006, 22 (9-11): 845–855.

[77] Denemark T, Sedighi V, Holub V, et al. Selection-channel-aware rich model for steganalysis of digital images[C]//2014 IEEE International Workshop on Infor-

mation Forensics and Security, WIFS 2014, Atlanta, GA, USA, December 3-5, 2014. [S.l.]: IEEE, 2014: 48–53.

[78] Yao Y, Zhang W, Yu N, et al. Defining embedding distortion for motion vector-based video steganography[J]. Multim. Tools Appl. 2015, 74 (24): 11163–11186.

[79] Wang C, Buenaposada J M, Zhu R, et al. Learning depth from monocular videos using direct methods[C]//2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018. [S.l.]: IEEE Computer Society, 2018: 2022–2030.

[80] Yin Z, Shi J. Geonet: Unsupervised learning of dense depth, optical flow and camera pose[C]//2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018. [S.l.]: IEEE Computer Society, 2018: 1983–1992.

[81] Saxena A, Chung S H, Ng A Y. Learning depth from single monocular images[C]//Advances in Neural Information Processing Systems 18 [Neural Information Processing Systems, NIPS 2005, December 5-8, 2005, Vancouver, British Columbia, Canada]. [S.l.], 2005: 1161–1168.

[82] Saxena A, Sun M, Ng A Y. Make3d: Learning 3d scene structure from a single still image[J]. IEEE Trans. Pattern Anal. Mach. Intell. 2009, 31 (5): 824–840.

[83] Ladicky L, Shi J, Pollefeys M. Pulling things out of perspective[C]//2014 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2014, Columbus, OH, USA, June 23-28, 2014. [S.l.]: IEEE Computer Society, 2014: 89–96.

[84] Ranftl R, Vineet V, Chen Q, et al. Dense monocular depth estimation in complex dynamic scenes[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016. [S.l.]: IEEE Computer Society, 2016: 4058–4066.

[85] Furukawa R, Sagawa R, Kawasaki H. Depth estimation using structured light flow - analysis of projected pattern flow on an object's surface[C]//IEEE International Conference on Computer Vision, ICCV 2017, Venice, Italy, October 22-29, 2017. [S.l.]: IEEE Computer Society, 2017: 4650–4658.

[86] Liu F, Shen C, Lin G, et al. Learning depth from single monocular images using deep convolutional neural fields[J]. IEEE Trans. Pattern Anal. Mach. Intell. 2016, 38 (10): 2024–2039.

[87] Cao Y, Wu Z, Shen C. Estimating depth from monocular images as classification using deep fully convolutional residual networks[J]. IEEE Trans. Circuits Syst. Video Techn. 2018, 28 (11): 3174–3182.

[88] Xu D, Ricci E, Ouyang W, et al. Multi-scale continuous crfs as sequential deep networks for monocular depth estimation[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 161–169.

[89] Eigen D, Fergus R. Predicting depth, surface normals and semantic labels with a common multi-scale convolutional architecture[C]//2015 IEEE International Conference on Computer Vision, ICCV 2015, Santiago, Chile, December 7-13, 2015. [S.l.]: IEEE Computer Society, 2015: 2650–2658.

[90] Garg R, Kumar B G V, Carneiro G, et al. Unsupervised CNN for single view depth estimation: Geometry to the rescue[C]//Leibe B, Matas J, Sebe N, et al., Computer Vision - ECCV 2016 - 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part VIII: volume 9912. [S.l.]: Springer, 2016: 740–756.

[91] Kuznietsov Y, Stückler J, Leibe B. Semi-supervised deep learning for monocular depth map prediction[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 2215–2223.

[92] Laina I, Rupprecht C, Belagiannis V, et al. Deeper depth prediction with fully convolutional residual networks[C]//Fourth International Conference on 3D Vision, 3DV 2016, Stanford, CA, USA, October 25-28, 2016. [S.l.]: IEEE Computer Society, 2016: 239–248.

[93] Xie J, Girshick R B, Farhadi A. Deep3d: Fully automatic 2d-to-3d video conversion with deep convolutional neural networks[C]//Leibe B, Matas J, Sebe N, et al., Computer Vision - ECCV 2016 - 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part IV: volume 9908. [S.l.]: Springer, 2016: 842–857.

[94] Fu H, Gong M, Wang C, et al. Deep ordinal regression network for monocular depth estimation[C]//2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018. [S.l.]: IEEE Computer Society, 2018: 2002–2011.

[95] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016, Las Vegas, NV, USA, June 27-30, 2016. [S.l.]: IEEE Computer Society, 2016: 770–778.

[96] Eigen D, Puhrsch C, Fergus R. Depth map prediction from a single image us-

ing a multi-scale deep network[C]//Ghahramani Z, Welling M, Cortes C, et al., Advances in Neural Information Processing Systems 27: Annual Conference on Neural Information Processing Systems 2014, December 8-13 2014, Montreal, Quebec, Canada. [S.l.], 2014: 2366–2374.

[97] Owen A B. A robust hybrid of lasso and ridge regression[J]. Contemporary Mathematics. 2007, 443 (7): 59-72.

[98] Godard C, Aodha O M, Brostow G J. Unsupervised monocular depth estimation with left-right consistency[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 6602–6611.

[99] Zhou T, Brown M, Snavely N, et al. Unsupervised learning of depth and ego-motion from video[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 6612–6619.

[100] Zhuo S, Sim T. Defocus map estimation from a single image[J]. Pattern Recognit. 2011, 44 (9): 1852–1858.

[101] Levin A, Fergus R, Durand F, et al. Image and depth from a conventional camera with a coded aperture[J]. ACM Trans. Graph. 2007, 26 (3): 70.

[102] Veeraraghavan A, Raskar R, Agrawal A K, et al. Dappled photography: mask enhanced cameras for heterodyned light fields and coded aperture refocusing[J]. ACM Trans. Graph. 2007, 26 (3): 69.

[103] Sellent A, Favaro P. Which side of the focal plane are you on?[C]//2014 IEEE International Conference on Computational Photography, ICCP 2014, Santa Clara, CA, USA, May 2-4, 2014. [S.l.]: IEEE Computer Society, 2014: 1–8.

[104] Suwajanakorn S, Hernández C, Seitz S M. Depth from focus with your mobile phone[C]//IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2015, Boston, MA, USA, June 7-12, 2015. [S.l.]: IEEE Computer Society, 2015: 3497–3506.

[105] Tang H, Cohen S, Price B L, et al. Depth from defocus in the wild[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 4773–4781.

[106] Surh J, Jeon H, Park Y, et al. Noise robust depth from focus using a ring difference filter[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer

Society, 2017: 2444–2453.

[107] Srinivasan P P, Garg R, Wadhwa N, et al. Aperture supervision for monocular depth estimation[C]//2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018. [S.l.]: IEEE Computer Society, 2018: 6393–6401.

[108] Xia M, Liu X, Wong T. Invertible grayscale[J]. ACM Trans. Graph. 2018, 37 (6): 246:1–246:10.

[109] Ioffe S, Szegedy C. Batch normalization: Accelerating deep network training by reducing internal covariate shift[C]//Bach F R, Blei D M, Proceedings of the 32nd International Conference on Machine Learning, ICML 2015, Lille, France, 6-11 July 2015: volume 37. [S.l.]: JMLR.org, 2015: 448–456.

[110] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]//Ghahramani Z, Welling M, Cortes C, et al., Advances in Neural Information Processing Systems 27: Annual Conference on Neural Information Processing Systems 2014, December 8-13 2014, Montreal, Quebec, Canada. [S.l.], 2014: 2672–2680.

[111] Isola P, Zhu J, Zhou T, et al. Image-to-image translation with conditional adversarial networks[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017. [S.l.]: IEEE Computer Society, 2017: 5967–5976.

[112] Zhu J, Zhang R, Pathak D, et al. Toward multimodal image-to-image translation[C]//Guyon I, von Luxburg U, Bengio S, et al., Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA. [S.l.], 2017: 465–476.

[113] Zhu J, Park T, Isola P, et al. Unpaired image-to-image translation using cycle-consistent adversarial networks[C]//IEEE International Conference on Computer Vision, ICCV 2017, Venice, Italy, October 22-29, 2017. [S.l.]: IEEE Computer Society, 2017: 2242–2251.

[114] Wang T, Liu M, Zhu J, et al. High-resolution image synthesis and semantic manipulation with conditional gans[C]//2018 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2018, Salt Lake City, UT, USA, June 18-22, 2018. [S.l.]: IEEE Computer Society, 2018: 8798–8807.

[115] Zhu J, Kaplan R, Johnson J, et al. Hidden: Hiding data with deep networks[C]//Ferrari V, Hebert M, Sminchisescu C, et al., Computer Vision - ECCV

2018 - 15th European Conference, Munich, Germany, September 8-14, 2018, Proceedings, Part XV: volume 11219. [S.l.]: Springer, 2018: 682–697.

[116] Simonyan K, Zisserman A. Very deep convolutional networks for large-scale image recognition[C]//Bengio Y, LeCun Y, 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings. [S.l.], 2015.

[117] Johnson J, Alahi A, Fei-Fei L. Perceptual losses for real-time style transfer and super-resolution[C]//Leibe B, Matas J, Sebe N, et al., Computer Vision - ECCV 2016 - 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part II: volume 9906. [S.l.]: Springer, 2016: 694–711.

[118] Kingma D P, Ba J. Adam: A method for stochastic optimization[C]//Bengio Y, LeCun Y, 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings. [S.l.], 2015.

[119] Gur S, Wolf L. Single image depth estimation trained via depth from defocus cues[C]//IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2019, Long Beach, CA, USA, June 16-20, 2019. [S.l.]: Computer Vision Foundation / IEEE, 2019: 7683–7692.

[120] Li B, Wang M, Li X, et al. A strategy of clustering modification directions in spatial image steganography[J]. IEEE Trans. Information Forensics and Security. 2015, 10 (9): 1905–1917.

[121] Denemark T, Fridrich J J. Improving steganographic security by synchronizing the selection channel[C]//Alattar A M, Fridrich J J, Smith N M, et al., Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, IH&MMSec 2015, Portland, OR, USA, June 17 - 19, 2015. [S.l.]: ACM, 2015: 5–14.

[122] Zhang W, Zhang Z, Zhang L, et al. Decomposing joint distortion for adaptive steganography[J]. IEEE Trans. Circuits Syst. Video Techn. 2017, 27 (10): 2274–2280.

[123] Ker A D. Batch steganography and pooled steganalysis[C]//Camenisch J, Collberg C S, Johnson N F, et al., Information Hiding, 8th International Workshop, IH 2006, Alexandria, VA, USA, July 10-12, 2006. Revised Selcted Papers: volume 4437. [S.l.]: Springer, 2006: 265–281.

[124] Ker A D. A capacity result for batch steganography[J]. IEEE Signal Process. Lett. 2007, 14 (8): 525–528.

[125] Botsch M, Kobbelt L, Pauly M, et al. Polygon Mesh Processing[M]. [S.l.]: A K Peters, 2010.

[126] Bajaj C L, Xu G. Anisotropic diffusion of surfaces and functions on surfaces[J]. ACM Trans. Graph. 2003, 22 (1): 4–32.

[127] Fleishman S, Drori I, Cohen-Or D. Bilateral mesh denoising[J]. ACM Trans. Graph. 2003, 22 (3): 950–953.

[128] Schneider R, Kobbelt L. Geometric fairing of irregular meshes for free-form surface design[J]. Comput. Aided Geom. Des. 2001, 18 (4): 359–379.

[129] Eigensatz M, Sumner R W, Pauly M. Curvature-domain shape processing[J]. Comput. Graph. Forum. 2008, 27 (2): 241–250.

[130] Zhao W, Liu X, Zhao Y, et al. Normalnet: Learning based guided normal filtering for mesh denoising[J]. CoRR. 2019, abs/1903.04015.

[131] Krizhevsky A, Sutskever I, Hinton G E. Imagenet classification with deep convolutional neural networks[C]//Bartlett P L, Pereira F C N, Burges C J C, et al., Advances in Neural Information Processing Systems 25: 26th Annual Conference on Neural Information Processing Systems 2012. Proceedings of a meeting held December 3-6, 2012, Lake Tahoe, Nevada, United States. [S.l.], 2012: 1106–1114.

[132] Hamilton W L, Ying Z, Leskovec J. Inductive representation learning on large graphs[C]//Guyon I, von Luxburg U, Bengio S, et al., Advances in Neural Information Processing Systems 30: Annual Conference on Neural Information Processing Systems 2017, 4-9 December 2017, Long Beach, CA, USA. [S.l.], 2017: 1024–1034.

[133] Feng Y, Feng Y, You H, et al. Meshnet: Mesh neural network for 3d shape representation[C]//The Thirty-Third AAAI Conference on Artificial Intelligence, AAAI 2019, The Thirty-First Innovative Applications of Artificial Intelligence Conference, IAAI 2019, The Ninth AAAI Symposium on Educational Advances in Artificial Intelligence, EAAI 2019, Honolulu, Hawaii, USA, January 27 - February 1, 2019. [S.l.]: AAAI Press, 2019: 8279–8286.

致　谢

气候逐渐温热，窗外栀子含苞待放，突然意识到，已是毕业季了。

求学生涯终究即将结束。回首过往，满眼都是自己青春年少的影子。经历过满腔热血、迷惘、无助、喜悦和感动，无数次质疑过自己，却无数次释怀。都说，一棵树，从发芽、成长到开花结果，离不开大自然的孕育。而这一路上的艰难险阻，也正是因为在父母师长亲朋好友的无私帮助之下，我才撑着坚持至今。刘禹锡在《浪淘沙》中言道：“千淘万漉虽辛苦，吹尽狂沙始到金”。从一名没有任何学术功底的学生，到有机会从事领域内一流研究的科研工作者，读博求学之路，有太多人需要感谢。

首先感谢我的导师俞能海教授。俞老师高瞻远瞩的学术视野，令我收益颇丰。二零一七年转博之后，博士课题定为以三维模型为载体的隐写研究，他多次与我提及保护三维数据的重要性，而近年来三维数据在深度学习领域的研究呈井喷式发展正是验证了他的一番大胆猜想。同时，他有着拼搏的工作精神，孜孜不倦，夜里甚至周末也往往能在办公室见到身影。他有着丰富的人生阅历，常教导我们“思路决定出路，眼界决定境界”，因此，每次与他的交谈是短暂的，却又醍醐灌顶。他积极乐观的人生态度和豁达宽广的胸襟是我学习的榜样。谨此向敬爱的俞老师及其家人表示最衷心的祝福和谢意。

感谢我的导师张卫明教授。张老师平易近人，知识渊博，处处为学生着想，是极为难得的好导师。第一次见到他时，我立刻被老师的学术魅力所折服。做学问最关键的是勤读论文勤思考，在每周的组会上，他帮助学生“打通任督二脉”，教会怎么发现问题、怎么解决问题，并总能抛出研究痛点、难点和新的研究点。他身兼数职，从逐字逐行帮我校读论文，到我行将毕业时出谋划策，已是我生活上的导师。求学期间曾数度出现健康问题，屡屡得到老师深切的关心。他严谨求是的治学风格和淡泊名利的生活态度深刻影响着我，使我在学习和生活上都收获颇多。谨此向敬爱的张老师及其家人表示最衷心的祝福和谢意。

特别感谢复旦大学的钱振兴老师。钱老师对我而言，有知遇之恩。正是他将我引入了研究的殿堂，让我有了更高的追求。仍记得一个阳光明媚的午后，他怀着满腔热情把信息隐藏领域的脉络向我娓娓道来。我的第一个研究课题是“JPEG图像的密文域可逆隐藏”，历经三个月失败的实验验证，随后凭借不懈的坚持和他的鼓励，在本科毕业答辩前夕我实现了代码，并与老师合作投出了我生涯第一篇期刊论文。非常感谢钱老师一直以来对我的赏识。

特别感谢陈可江同学。我和你认识八年，本科期间已是共同组队参加过多项大赛的朋友。在科大求学期间，不仅是室友，而且也是实验室同个导师的学生。

你尽管饱经风雨，在学习工作生活上积极乐观的人生态度、坚持不懈的意志力和严密的思辨力深深地影响与激励着我。我们是最好的兄弟，希望你今后的人生能够美满幸福。

感谢 Ant Finance 的王太峰研究员。在微软亚洲研究院实习期间，您作为我的导师，悉心地指导了我的学术研究，教会了我许多新的知识，让我的视野变得开阔。感谢陈冬冬师兄，你积极乐观的生活态度和开阔的思维深深地影响了我，并且在科研和求职路上给予了我巨大的帮助。感谢 Wormpex 的华刚老师，与您在一九年 ICCV 会场的交谈令我受益匪浅。感谢香港城市大学的廖菁老师，您在研究上的洞见令我印象深刻。感谢姚远志师兄，不仅带我入门视频隐写，而且帮助我在科研之路上更清晰地定位自身。感谢周文柏师兄，在生活上帮助我如何更好地待人接物。

感谢中国科学院电磁空间重点实验室的胡红钢教授、林宪正教授、刘斌副教授、李卫海副教授、王冬老师在实验室生活中的指导与帮助，感谢张方志老师、华孝枝老师和罗瑜老师为实验室同学们的辛苦付出。感谢谭勇老师、张玉颖老师等在科研与教学方面的悉心指导。

感谢同窗多年的室友阮玉平和陈培新，感谢求学期间曾给予我关心和帮助的师兄师姐们：查宏越、侯冬冬、张卓、杨培韬、王辉、郑书新、李震宇等，感谢共同奋斗的兄弟姐妹们：卞寰宇、方涵、秦川、刘泓谷、李伟祥、刘嘉阳、崔灏、董潇逸、刘昆麟、张杰、李岁缠、Mohsin Shah、董晓娟、李莉、左鑫、胡欢欢、杨宽、王垚飞、沈豪、于心智、耿霖峰、张逸为、吴媛欣、刘雨佳、马泽华、管玺权、孙杉、李梦涵、程宇翔、张奎、林佳滢、王锋、赵汉卿等，与大家共处的这几年，我过得很开心，感谢你们对我的支持。

最后，我要特别感谢我的家人，感谢父母周恩龙和干翠菊，感谢你们廿多年来茹苦含辛将我和弟弟拉扯长大。没有你们从小对我的教育和一直以来无微不至的关怀，我无法走到今天。求学期间没能陪伴你们左右，我始终倍感惭愧。在今后的工作和生活中，我一定不会辜负你们的期望。

谨以此文献给所有曾经关心和帮助过我的人。

周航

2020 年 7 月 3 日

在读期间发表的学术论文与取得的研究成果

已发表论文

1. **Zhou Hang**, Chen Kejiang, Zhang Weiming, Yu Nenghai. Comments on "Steganography Using Reversible Texture Synthesis"[J]. IEEE Transactions on Image Processing (TIP), 2017, 26(4): 1623-1625. (CCF A，SCI 一区，IF 6.79)

2. **Zhou Hang**, Chen Kejiang, Zhang Weiming, Qin Chuan, Yu Nenghai. Feature-Preserving Tensor Voting Model for Mesh Steganalysis[J]. IEEE Transactions on Visualization and Computer Graphics (TVCG), 2019. (CCF A，SCI 一区，IF 3.780)

3. **Zhou Hang**, Chen Kejiang, Zhang Weiming, Yao Yuanzhi, Yu Nenghai. Distortion Design for Secure Adaptive 3D Mesh Steganography[J]. IEEE Transactions on Multimedia (TMM), 2018, 21(6): 1384-1398. (CCF B，SCI 一区，IF 5.452)

4. **Zhou Hang**, Chen Dongdong, Liao Jing, Zhang Weiming, Chen Kejiang, Dong Xiaoyi, Liu Kunlin, Hua Gang, Yu Nenghai. LG-GAN: Label Guided Adversarial Network for Flexible Targeted Attack of Point Cloud-based Deep Networks[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020. (CCF A)

5. **Zhou Hang**, Chen Kejiang, Zhang Weiming, Fang Han, Zhou Wenbo, Yu Nenghai. DUP-Net: Denoiser and Upsampler Network for 3D Adversarial Point Clouds Defense[C]. Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). 2019: 1961-1970. (CCF A)

6. **Zhou Hang**, Chen Kejiang, Zhang Weiming, Qian Zhenxing, Yu Nenghai. Targeted Attack and Security Enhancement on Texture Synthesis Based Steganography[J]. Journal of Visual Communication and Image Representation (JVCIR), 2018, 54: 100-107. (CCF C，SCI 三区，IF 2.259)

7. Li Weixiang, Zhang Weiming, Li Li, **Zhou Hang**, Yu Nenghai. Designing Near-Optimal Steganographic Codes in Practice Based on Polar Codes[J]. IEEE Transactions on Communications (TCOM), 2020. (CCF B，SCI 一区，IF 5.69)

8. Chen Kejiang, **Zhou Hang**, Zhou Wenbo, Zhang Weiming, Yu Nenghai. Defining Cost Functions for Adaptive JPEG Steganography at the Microscale[J]. IEEE Transactions on Information Forensics and Security (TIFS), 2018, 14(4): 1052-1066. (CCF A，SCI 一区，IF 6.211)

9. Fang Han, Zhang Weiming, **Zhou Hang**, Cui Hao, Yu Nenghai. Screen-Shooting Resilient Watermarking[J]. IEEE Transactions on Information Forensics and Security (TIFS), 2018, 14(6): 1403-1418. (CCF A，SCI 一区，IF 6.211)

10. Qian Zhenxing, **Zhou Hang**, Zhang Xinpeng, Zhang Weiming. Separable Reversible Data Hiding in Encrypted JPEG Bitstreams[J]. IEEE Transactions on Dependable and Secure Computing (TDSC), 2016, 15(6): 1055-1067. (CCF A，SCI 二区，IF 6.404)

11. Dong Xiaoyi, Chen Dongdong, **Zhou Hang**, Hua Gang, Zhang Weiming, Yu Nenghai. Self-Robust 3D Point Recognition via Gather-vector Guidance[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020. (CCF A)

12. Jiang Ruiqi, **Zhou Hang**, Zhang Weiming, Yu Nenghai. Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models[J]. IEEE Transactions on Multimedia (TMM), 2017, 20(1): 55-67. (CCF B，SCI 一区，IF 5.452)

13. Chen Kejiang, **Zhou Hang**, Li Weixiang, Yang Kuan, Zhang Weiming, Yu Nenghai. Derivative-based Steganographic Distortion and Its Non-additive Extensions for Audio[J]. IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2019. (CCF B，SCI 二区，IF 4.046)

14. Fang Han, Zhang Weiming, Ma Zehua, **Zhou Hang**, Sun Shan, Cui Hao, Yu Nenghai. A Camera Shooting Resilient Watermarking Scheme for Underpainting Documents[J]. IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2019. (CCF B，SCI 二区，IF 4.046)

15. Li Weixiang, Chen Kejiang, Zhang Weiming, **Zhou Hang**, Wang Yaofei, Yu Nenghai. JPEG Steganography with Estimated Side-information[J]. IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2019. (CCF B，SCI 二区，IF 4.046)

16. Yao Yuanzhi, Zhang Weiming, Wang Hui, **Zhou Hang**, Yu Nenghai. Content-Adaptive Reversible Visible Watermarking in Encrypted Images[J]. Signal Processing, 2019, 164: 386-401. (CCF C，SCI 二区，IF：4.086)

17. Chen Kejiang, Chen Yuefeng, **Zhou Hang**, Mao Xiaofeng, Li Yuhong, He Yuan, Xue Hui, Zhang Weiming, Yu Nenghai. Self-supervised Adversarial Training[C]. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2020. (CCF B)

18. Zhou Wenbo, Li Weixiang, Chen Kejiang, **Zhou Hang**, Zhang Weiming, Yu Nenghai. Controversial 'Pixel' Prior Rule for JPEG Adaptive Steganography[J]. IET Image Processing, 2018, 13(1): 24-33. (CCF C，SCI 三区，IF 2.004)

19. Fang Han, **Zhou Hang**, Ma Zehua, Zhang Weiming, Yu Nenghai. A Robust Image Watermarking Scheme in DCT Domain Based on Adaptive Texture Direction Quantization[J]. Multimedia Tools and Applications (MTA), 2019, 78(7): 8075-8089. (CCF C，SCI 四区，IF 2.101)

20. Shah Mohsin, Zhang Weiming, Hu Honggang, **Zhou Hang**, Mahmood Toqeer. Homomorphic Encryption-Based Reversible Data Hiding for 3D Mesh Models[J]. Arabian Journal for Science and Engineering (AJSE), 2018, 43(12): 8145-8157. (SCI 四区，IF 1.518)

21. Qian Zhenxing, **Zhou Hang**, Zhang Weiming, Zhang Xinpeng. Robust Steganography Using Texture Synthesis[M]. Advances in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2017: 25-33. (EI)

22. Xu Jiajia, **Zhou Hang**, Zhang Weiming, Jiang Ruiqi, Ma Guoli, Yu Nenghai. Second Order Predicting-Error Sorting for Reversible Data Hiding[C]. International Workshop on Digital Watermarking (IWDW), 2016: 407-420. (EI)

23. Chen Kejiang, Zhang Weiming, **Zhou Hang**, Yu Nenghai, Feng Guorui. Defining Cost Functions for Adaptive Steganography at the Microscale[C]. IEEE International Workshop on Information Forensics and Security (WIFS), 2016: 1-6. (EI)

已投稿论文

1. **Zhou Hang**, Zhang Weiming, Chen Kejiang, Li Weixiang, Yu Nenghai. Three-Dimensional Mesh Steganography and Steganalysis: A Review[J]. IEEE Transactions on Visualization and Computer Graphics (TVCG), 2020. (CCF A，SCI 一区，IF 3.780)

2. Chen Kejiang, **Zhou Hang**, Hou Dongdong, Zhang Weiming, Yu Nenghai. Reversible Data Hiding in JPEG Images under Multi-distortion Metric[J]. IEEE Transactions on Circuits and Systems for Video Technology (TCSVT), 2020. (CCF B，SCI 二区，IF 4.046)

3. Guan Xiquan, Zhang Weiming, **Zhou Hang**, Zhang Jie, Yu Nenghai. Reversible Watermarking in Deep Neural Network for Integrity Authentication[C]. ACM Multimedia (MM). 2020. (CCF A)

4. Chen Kejiang, Chen Yuefeng, **Zhou Hang**, Qin Chuan, Mao Xiaofeng, He Yuan, Zhang Weiming, Yu Nenghai. Two-Stream Convolutional Neural Networks for Adversarial Example Detection[C]. ACM Multimedia (MM). 2020. (CCF A)

5. Qin Chuan, Zhang Weiming, **Zhou Hang**, Liu Jiayang, He Yuan, Yu Nenghai. Robust Defense Against Adversarial Steganography by Exploiting Differences Between CNN and Handcrafted Features[J]. IEEE Transactions on Multimedia (TMM). (CCF B，SCI 一区，IF 5.452)

6. Bian Huanyu, Zhang Weiming, Cui Hao, Liu Kunlin, **Zhou Hang**, Chen Dongdong, Yu Nenghai. Color Decomposition based Adversarial Examples for Screen Devices[C]. ACM Multimedia (MM). 2020. (CCF A)

7. Bian Huanyu, Chen Dongdong, Zhang Kui, **Zhou Hang**, Dong Xiaoyi, Zhang Weiming, Yu Nenghai. Adversarial Defense via Self-orthogonal Randomization Super-networks[C]. European Conference on Computer Vision (ECCV). 2020. (CCF B)

8. Liu Kunlin, Chen Dongdong, Liao Jing, Zhang Weiming, **Zhou Hang**, Zhang Jie, Zhou Wenbo, Nenghai Yu. JPEG Robust Invertible Grayscale[J]. IEEE Transactions on Visualization and Computer Graphics (TVCG). 2020. (CCF A，SCI 一区，IF 3.780)

已申请专利

1. 张卫明，俞能海，**周航**，陈可江. 3D 网格模型隐写方法.
   申请号：201910146687.2.

2. 张卫明，俞能海，陈可江，**周航**，董潇逸. 一种基于 PDF 文件的图文相关鲁棒隐写方法及系统.
   申请号：201910129282.8.

在读期间参与科研项目

1. 国家自然科学基金重点项目课题“应对大数据分析的情景融合个性化隐写理论与方法”，项目编号：U1636201，起止时间：2017.01-2020.12.

   主要贡献：基于纹理图像、3D 网格的隐写安全性分析和隐写模型进行相关学术科研工作，发表论文 4 篇。

2. 国家自然科学基金面上项目课题“面向隐蔽存储应用的可逆隐写理论与方法研究”，项目编号：61572452，起止时间：2016.01-2019.12.

   主要贡献：基于 3D 网格的密文域可逆隐藏模型进行相关学术科研工作，发表论文 1 篇。

3. 中科院战略性先导专项课题“数字媒体安全防护关键技术”，项目编号：XDA06030601，起止时间：2012.01-2016.12.

   主要贡献：负责基于真实场景下 JPEG 图像隐写算法的部分开发任务。

4. 国家 863 项目，媒体安全技术，科技部，起止时间：2014.01-2017.12.

   主要贡献：负责 MPEG4 格式视频自适应隐写工程开发任务。

5. 中国科学技术大学青年创新基金专项课题“3D 隐写模型与方法研究”，项目编号：WK6030000136，起止时间：2019.01-2020.12.

   主要贡献：项目负责人，负责项目管理以及 3D 隐写算法研究。

6. 中国科学技术大学青年创新基金专项课题“信息隐藏编码与算法研究”，项目编号：WK6030000135，起止时间：2019.01-2020.12.

   主要贡献：基于 3D 网格的隐写模型进行相关学术科研工作，发表论文 1 篇。

求学期间主要获奖情况

1. 中科院院长奖优秀奖，2020 年。
2. 中国互联网发展基金会网络安全专项基金网络安全奖学金，2018 年。
3. 中国科学技术大学博士生国家奖学金，2019 年。
4. IJCAI——阿里巴巴天池对抗攻防竞赛防御赛道第四名，获奖人：卞寰宇，周航，周文柏，2019 年。
5. 中国科学技术大学优秀毕业生，2020 年。
6. 中电仪器奖学金，2016 年。