JOURNAL OF IMAGE AND GRAPHICS

主办：中国科学院空天信息创新研究院
中国图象图形学学会
北京应用物理与计算数学研究所

中国图象图形学报

2022
01
VOL.27

ISSN1006-8961
CN11-3758/TB

数字图像/视频内容安全

中国图象图形学报

刊名题字：宋健 | 月刊（1996年创刊）

主管单位 中国科学院
主办单位 中国科学院空天信息创新研究院
中国图象图形学学会
北京应用物理与计算数学研究所

主　　编 吴一戎
编辑出版 《中国图象图形学报》编辑出版委员会
通信地址 北京市海淀区北四环西路19号
邮　　编 100190
电子信箱 jig@aircas.ac.cn
电　　话 010-58887035
网　　址 www.cjig.cn

广告发布登记号 京朝工商广登字20170218号
总 发 行 北京报刊发行局
订　　购 全国各地邮局
海外发行 中国国际图书贸易集团有限公司
（邮政信箱：北京399信箱　邮编：100048）
印刷装订 北京科信印刷有限公司

第27卷第1期（总第309期）
2022年1月16日

中国精品科技期刊
中国国际影响力优秀学术期刊
中国科技核心期刊
中文核心期刊

Journal of Image and Graphics

Title inscription: Song Jian | Monthly, Started in 1996

Superintended by Chinese Academy of Sciences
Sponsored by Aerospace Information Research Institute, CAS
China Society of Image and Graphics
Institute of Applied Physics and Computational Mathematics

Editor-in-Chief Wu Yirong
Editor, Publisher Editorial and Publishing Board of Journal of Image and Graphics
Address No. 19, North 4th Ring Road West, Haidian District, Beijing, P. R. China
Zip code 100190
E-mail jig@aircas.ac.cn
Telephone 010-58887035
Website www.cjig.cn

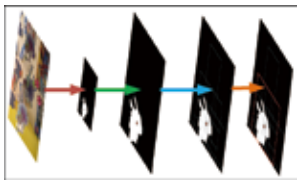
Distributed by Beijing Bureau for Distribution of Newspapers and Journals
Domestic All Local Post Offices in China
Overseas China International Book Trading Corporation (P.O.Box 399, Beijing 100048,P.R.China))
Printed by Beijing Kexin Printing Co., Ltd.

CN 11-3758/TB
ISSN 1006-8961
CODEN ZTTXFZ

国外发行代号 M1406
国内邮发代号 82-831
国内定价 60.00元

2022年1月 第27卷 第1期（总第309期）
中国图象图形学报
Zhongguo Tuxiang Tuxing Xuebao

目次



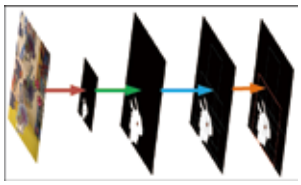
检测小篡改区域的U型网络(第0176页)

结合半张量积压缩感知的可验证图像加密(第0215页)

实离散分数Krawtchouk变换及其在数字图像水印中的应用(第0252页)

Volume 27, Number 1
Published January 16, 2022

CONTENTS
JOURNAL OF IMAGE AND GRAPHICS



U-Net for detecting the small forgery region(P0176)

Semi-tensor product compression sensing integrated to verifiable image encryption method(P0215)

Real discrete fractional Krawtchouk transform with an application to image watermarking(P0252)

E-mail: jig@aircas.ac.cn
Website: www.cjig.cn
Tel: 010-58887035

中图法分类号:TP37　　**文献标识码**: A　　**文章编号**: 1006-8961(2022)01-0150-13

论文引用格式: Zhou H, Chen K J, Zhang W M and Yu N H. 2022. 3D mesh steganography and steganalysis: review and prospect. Journal of Image and Graphics,27(01):0150-0162(周航,陈可江,张卫明,俞能海. 2022. 3D 网格隐写与隐写分析回顾与展望. 中国图象图形学报,27(01):0150-0162)[DOI:10.11834/jig.210371]

3D 网格隐写与隐写分析回顾与展望

周航[1,2],陈可江[1,3],张卫明[1,3*],俞能海[1,3]

1. 中国科学技术大学信息科学技术学院, 合肥　230027; 2. 西蒙弗雷泽大学计算机科学学院, 加拿大 温哥华　V5A1S6;
3. 中国科学院电磁空间信息重点实验室, 合肥　230027

摘　要:　在计算机图形学中,3D 形状可有多种表示形式,包括网格、体素、多视角图像、点云、参数曲面和隐式曲面等。3D 网格是常见的表示形式之一,其构成 3D 物体的顶点、边缘和面的集合,通常用于表示数字 3D 物体的曲面和容积特性。在过去的 20 年中,基于 3D 网格载体的虚拟现实、实时仿真和交叉 3 维设计已经在工业,医疗和娱乐等场景得到广泛应用,以 3D 网格为载体的水印技术、隐写和隐写分析技术也受到研究者的关注。相比于图像与音视频等载体的隐写,3D 网格具备嵌入方式灵活与载体形式多变等其自身的优势。本文回顾了 3D 网格隐写和隐写分析的发展,并对现有研究工作进行了系统的总结和分类。根据嵌入方式和嵌入位置将隐写算法分成 4 类:两态调制隐写、最低位隐写、置换隐写和变换域隐写;根据特征提取角度将隐写分析算法分为 2 类:通用型隐写分析和专用型隐写分析。随后,介绍了每个类别的技术,综合安全性、鲁棒性、容量以及运算效率分析了各类算法的优劣性,总结当前的发展水平,并提供了不同嵌入率下两种数据集上隐写分析算法之间的性能比较。最后讨论了 3D 隐写和隐写分析现有技术的局限性,并探讨了潜在的研究方向,旨在为后续学者进一步推动 3D 隐写和隐写分析技术提供指导。

关键词:3 维模型;多边形网格;信息隐藏;隐写;隐写分析;综述

3D mesh steganography and steganalysis: review and prospect

Zhou Hang[1,2], Chen Kejiang[1,3], Zhang Weiming[1,3*], Yu Nenghai[1,3]

1. School of Cyberspace Information, University of Science and Technology of China, Hefei　230027, China;
2. School of Computer Science, Simon Fraser University, Vancouver　V5A1S6, Canada;
3. Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Hefei　230027, China

Abstract: Three-dimensional (3D) meshes have been mainly used to illustrate virtual surfaces and volumes. 3D meshes have implemented in industrial, medical, and entertainment applications over the past decade, which are of great practical significance for 3D mesh steganography and steganalysis. The application of 3D geometry as host object has been focused over the past few years based on image, audio files and videos processing method in early steganography and steganalysis. Cost effective 3D hardware stimulates the widespread use of 3D meshes in the evolving of the computer aided design (CAD) industry to real-world end-user applications such as virtual reality (VR), web integration, Facebook support, video games, 3D printing and animated movies. Hence, the development of computer graphics has facilitated the production,

收稿日期:2021-05-19;**修回日期**:2021-09-10;**预印本日期**:2021-09-17

*通信作者:张卫明　zhangwm@ustc.edu.cn

基金项目:国家自然科学基金项目(62002334,62106386,62072421,62121002);中国博士后科学基金项目(2021M693091);中央高校基本科研业务费专项资金资助(WK2100000018)

Supported by: National Natural Science Foundation of China (62002334, 62106386, 62072421, 62121002); China Postdoctoral Science Foundation (2021M693091); Fundamental Research Funds for the Central Universities (WK2100000018)

application and distribution of the emerging generation of 3D geometry digital media. Moreover, the flexible data structure of 3D geometry provides enough space to host security information, making it ideal for use a cover object for steganography. A 3D mesh consists of a set of triangular faces, which is to form an approximation of a real 3D object. A 3D mesh has 3 different synthesized factors: vertices, edges, and faces; a mesh can also be taken as the integration of geometry connectivity, where the geometry provides the 3D positions of all its vertices, and connectivity, which provides the information hidden between different adjacent vertices. A systematic overview of 3D mesh steganography and steganalysis has been issued related to computer graphics and security. The objective projects in the context of the types of steganographic and steganalytic methods have been reviewed in literature. Quantitative evaluation has been conducted from the perspective of security assessment simultaneously. The target of this task is to demonstrate the evaluation procedures in the 3D mesh steganography and steganalysis methods as a whole. It is essential to recognize a growing number of efforts on how to improve the anti-steganalysis efforts in the case of steganographer side and how to improve the steganalysis ability in the case of the steganalyzer side. Some standard evaluation metrics, an overall summary, and an understanding of relevant research results have been evaluated based on the previous analyses. Unlike image steganography which embeds data by modifying pixel values, 3D mesh steganography modifies vertex coordinates or vertex order to embed data. In the latest literature analysis of 3D steganography and steganalysis of Girdhar and Kumar's work, steganography is divided into three categories (geometrical domain, topological domain and representation domain), which reflects the robustness of the algorithms to attacks, and steganalysis is briefly introduced. The entire communities of 3D steganography and steganalysis have to be further promoted. For instance, the geometrical domain can still be divided into two-state domain and the least significant bit (LSB) domain. In addition, the concepts of "steganography" and "watermarking" can be used interchangeably. Watermarking seeks robustness, protects copyright ownership and reduces the counterfeiting of digital multimedia, while steganography seeks un-detectability used for covert communication. They focus has been primarily on analyzing the robustness of the existing methods, while the undetectability of steganography is a more important property because of its practical requirement: covert communication. A more comprehensive survey, a clear taxonomy and several criteria for evaluating robustness and un-detectability has been offered. Conversely, hidden data has been used into reversible data hiding and steganography. For the structure of 3D data, the 3D mesh and RGBD image have been mainly concentrated. 3D meshes as carriers and steganographic techniques have been considered. The steganographic techniques into several domains (two-state domain, LSB domain, permutation domain and transform domain) in a subdivision way have been divided with no small embedding capacities. This demonstration has evolved common digital attacks including affine transform attack, vertex reordering attack, noise addition attack, smoothing attack and simplification attack. In addition, 3D mesh steganalysis has been divided into two aspects (general steganalysis and specific steganalysis). For overall steganalysis, there are YANG208 features, local feature set (LFS) 52 features, LFS64 features, LFS76 features, LFS124 features, normal voting tensor (NVT) + features and 3D wavelet feature set (WFS) 228 features respectively. Current methods have revealed strong weaknesses and strengths from which we can learn for future work. In order to evaluate the performance of various steganographic and steganalytic methods clearly, it is important to identify standards for users friendly. Meanwhile, the steganographic performance based on three general requirements (i. e. , security, capacity and robustness) has been evaluated. Ensemble learning is an effective way to produce a variety of base classifiers, from which a new classifier with a better performance can be derived, and ensemble classifier is used to evaluate steganalysis performance, a common tool for steganalysis. The datasets proposed are suitable for the princeton segmentation benchmark and the Princeton ModelNet, where the former has 354 objects and the latter has 12 311 mesh objects with 40 categories. Some promising future research directions and challenges in improving the performance of 3D mesh steganography and steganalysis have been highlighted. 3D mesh steganography research has been summarized as following: 1) combining the permutation domain and LSB domain; 2) designing spatial steganographic models; 3) designing steganalysis-resistant permutation steganographic methods; 4) designing 3D mesh batch steganography methods and 5) designing 3D-printing-material-based robust steganography methods. Open issues of 3D mesh steganalysis has been summarized as bellows: 1) rich steganalytic features designation for universal blind steganalysis; 2) designing deep-learning-based steganalysis methods; 3) designing a finer distance metric to improve the steganalysis of permutation steganography and 4) cover source mismatch problem.

Key words: 3D model; polygonal mesh; information hiding; steganography; steganalysis; survey

0 引 言

隐写术是一类信息隐藏方法,其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,是隐蔽通信或隐蔽存储的一种重要形式(Pevny 和 Fridrich,2008)。与传统加密技术将明文转换为密文后传输密文不同,隐写利用数字媒体的冗余性,修改局部载体以隐藏秘密消息。数字隐写术作为信息隐藏中的重要技术,自20 世纪 90 年代末以来,持续受到国防安全部门和学术界的重视。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。已有国际恐怖组织将欧美一些科学家早期关于隐写的研究应用于实践。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。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地推进,这也给数字隐写的设计带来了更大的挑战。

传统隐写主要的研究载体是图像、视频和音频等常见的多媒体数据,而本文关注的是随着虚拟现实、实时仿真和交互式 3 维设计技术发展产生的 3D 模型的隐写技术。这类 3D 模型作为许多重要应用的底层支撑技术,是计算机图形学的一个基础性研究课题。早期计算机图形学旨在解决如何在计算机中表示 3 维几何图形,以及如何利用计算机进行图形的生成、处理和显示的相关原理与算法,产生令人赏心悦目的真实感图像。经过 40 年的发展,广义的计算机图形学的研究非常广泛,如图形交互技术、光栅图形生成算法、曲线曲面造型、实体造型、真实感图形计算与显示算法,以及计算机动画、自然景物仿真和虚拟现实等。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 模型的隐写和隐写分析的研究也与日俱增,近几年得到了重视。2D 图像隐写通过修改像素值的方式嵌入秘密消息,与之不同的是,3D 网格隐写通过修改顶点坐标或顶点存储顺序嵌入消息。相比于像素调制,顶点坐标调制在 x,y,z 这 3 个坐标分量上均可实现调制,因此在设计 3D 网格隐写算法时相比于图像隐写更为复杂。

研究 3D 模型的隐写技术满足了复杂多样的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。首先,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。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则成为当前隐写技术研究的重要内容。其次,大数据环境下亟需新型载体隐写技术。随着网络和多媒体技术的发展,当前涌现了大量新型多媒体。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。

本文对现有的 3D 网格隐写和隐写分析方法进行了较为全面的总结和分析。根据消息嵌入的位置将 3D 网格隐写算法分为两态调制隐写、最低有效位(least significant bit, LSB)隐写、置换隐写和变换域隐写 4 类,以及将 3D 网格隐写分析算法分为通用型隐写分析和专用型隐写分析 2 类。为更好地描述与分析,首先简要介绍隐蔽通信基本模型;然后评估隐写算法安全性的数据集及评价指标;接着,分别介绍每类 3D 网格隐写算法和隐写分析算法的基本思想、代表性改进方案以及优缺点总结等,并对典型方法在数据集上总结和分析性能;最后,对 3D 网格隐写和隐写分析方法的未来发展方向进行了初步展望。

1 隐蔽通信基本模型

现代的隐写模型都是基于囚犯问题(Simmons,1984)设计的,该问题中 Alice 与 Bob 需要在 Wendy 的监视下实现隐蔽通信。通过图 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,$\boldsymbol{c}$ 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 $\boldsymbol{m}$ 使用密钥 k_1 加密后,通过隐写嵌入步骤 $Emb(\cdot)$ 将其嵌入载体 $\boldsymbol{c}$ 得到载密 $\boldsymbol{s}$,然后在 Wendy 监视下的信道中将 $\boldsymbol{s}$ 传输给 Bob,即

$$Emb(\boldsymbol{c},\boldsymbol{m},k_1)=\boldsymbol{s} \tag{1}$$

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

$$Ext(\boldsymbol{s},k_2)=\boldsymbol{m} \tag{2}$$

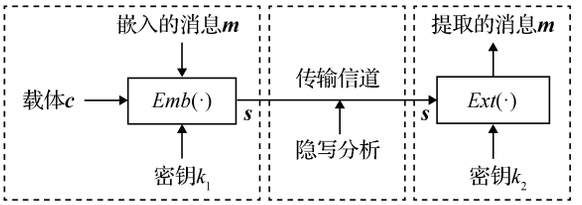


图 1　数字隐蔽通信和隐写分析示意图

Fig. 1　Diagram of digital covert communication and steganalysis

2　数据库及评价指标介绍

3D 网格是多边形小平面的集合，是真实 3D 物体的适当近似。随着 3 维表面重建和密集即时定位与地图构建（simultaneous localization and mapping，SLAM）的兴起，利用点云—网格生成算法，对海量的 3 维点云数据预处理得到 3D 网格。通常，根据不同的拓扑需求和算法需求，会选择不同的 3D 网格数据结构。最常见的数据结构为面数据结构，由网格所有面的集合构成，而对于每一个面则使用组成面多边形的点来表示。3D 网格包含 3 种不同的组成元素：顶点、边和面。3D 网格也可由几何信息和连接信息描述，其中几何信息描述了顶点的 3D 位置（坐标），连接信息提供了邻接关系。

3D 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，但能够加速网格上的几何和拓扑运算。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。

2.1　数据库

普林斯顿分割集（Princeton segmentation benchmark）包含 354 个网格（Chen 等，2009），主要用于 3D 网格分割任务。其中，260 对载体—载密网格对用于训练分类器，剩余 94 对作为测试样本。

普林斯顿网格（Princeton ModelNet）包含 12 311 个 40 类网格数据。其中，50% 的网格用于分类器训练，剩余网格作为测试样本。

2.2　评价指标

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性能。

1）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。

2）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，可通过相对有效载荷（也称为嵌入率），即比特每顶点（bit per vertex，bpv）评估。

3）鲁棒性。尽管大多数隐写方法并不追求鲁棒性，但在实际应用中，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，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取，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 4 种可能的结果：

1）真阳性（*TP*）：载密被正确分类为载密；

2）假阴性（*FN*）：载体被错误分类为载密；

3）真阴性（*TN*）：载体被正确分类为载体；

4）假阳性（*FP*）：载密被错误分类为载体。

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，评估指标包括

$$R = \frac{TP}{TP + FN} \tag{3}$$

$$FPO = \frac{FP}{TN + FP} \tag{4}$$

$$ACC = \frac{TP + TN}{TP + FN + TN + FP} \tag{5}$$

$$PR = \frac{TP}{TP + FP} \tag{6}$$

式中，*R* 为召回率，*FPO* 为假正率，*ACC* 为准确率，*PR* 为查准率。

支持向量机（support vector machine，SVM）是一种监督式机器学习模型，用于解决分类问题。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。为了能够处理高维特征，在实验中一般使用集成分类器分类。

集成分类器（Kodovský 等，2012）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）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，即

$$P_{\mathrm{E}} = \min_{P_{\mathrm{FA}}} \frac{1}{2}(P_{\mathrm{FA}} + P_{\mathrm{MD}}) \tag{7}$$

式中，P_{FA} 和 P_{MD} 分别是虚警率和漏警率。最终安全性 $\bar{P}_{\mathrm{E}}$ 由多次实验错误率取平均得到。

3 3D 网格隐写

根据秘密消息嵌入方式，3D 网格隐写算法可分为 4 类：两态调制隐写、最低位隐写、置换隐写和变换域隐写。在 3D 网格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信息的算法。

以下为几种典型数字攻击（Zhou 等，2021b）：

1）仿射变换（包括平移、旋转和缩放）。通过移动 3D 网格或者相机拍摄位置得到变换矩阵，也可通过齐次变换矩阵表示变换过程。

2）顶点重新排序。重新排序不会改变网格拓扑结构，只改变存储顶点的布局，并赋予新的索引。

3）加噪。扫描得到的 3D 模型通常是带噪模型，由扫描设备和数字化过程产生。

4）平滑。过滤掉高频信号。

5）简化。降低网格处理的复杂度。

3.1 两态调制隐写

两态调制隐写等分邻近两个坐标点之间的线段，标记为 01 两个状态。根据秘密消息的值对应的状态来相应地修改第 3 个点的坐标。

早期的 3D 网格隐写算法常采用两态调制隐写作为基础算法。Cayre 和 Macq（2003）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（2005）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 和 Wang（2006）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嵌入消息。Chao 等人（2009）提出了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（2017）提出了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。由于通过此方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（2017a）提出仅在距离分量上嵌入消息。

以上两态调制隐写算法中，Chao 等人（2009）算法隐写的容量相对较大，Li 等人（2017a）的隐写算法具有较明显的抗隐写分析检测性能。这类方法基于统计位移嵌入消息，对加性噪声攻击、拉普拉斯平滑攻击和网格简化攻击具有鲁棒性。值得一提的是，已经有一些隐写分析方法能够检测某些隐写算法。此外，嵌入过程中的优化算法阻碍了水印嵌入的速度。由于顶点数量有限，因此嵌入容量仍然很小。此外，由于修改幅度明显，因此这类方法无法抵御隐写分析。

3.2 最低位隐写

最低位隐写首先将消息编码至最低有效位平面，并随着嵌入量向更高位平面嵌入信息。

Yang 等人（2013）提出了估计坐标点曲率，并依据曲率大小自适应修改部分坐标点的最低位以嵌入消息的 3D 网格隐写方法。Li 等人（2017b）提出了在失真约束下基于密钥调制的 3D 网格隐写算法。Zhou 等人（2019）提出了基于自适应于顶点复杂度的网格顶点的失真函数，并采用校验栅格编码（syndrome trellis code，STC）（Filler 等，2011）嵌入秘密消息，实现更高安全性的隐写性能。

最低位隐写算法通常为大容量抗检测算法，其性能由相同嵌入率下的抗检测性能评估。以上最低位隐写算法中，Zhou 等人（2019）提出的隐写算法具备最强的抗检测性能。这类算法无法抵御加性噪声攻击、拉普拉斯平滑攻击和网格简化攻击，但对隐写分析有一定的抗检测性。

3.3 置换隐写

置换隐写基础原理是通过秘密消息的值扰动坐标或拓扑结构集合中元素的顺序实现消息嵌入。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，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（2008）提出了改进的置换隐写算

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(2009)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(2010a)、Tu 和 Tai(2012)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(2019)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 5 000 时,最大的嵌入率能够达到 11 bpv。

以上置换隐写算法中,Tu 和 Tai(2012)的算法隐写容量相比较而言最大,Wang 等人(2019)的隐写算法具有一定的抗隐写分析检测性能。这类算法具有较大的秘密信息嵌入容量,而且对基于坐标修改的攻击(仿射变换攻击、加噪攻击和平滑攻击)具有完全的鲁棒性。

3.4　变换域隐写

变换域隐写算法基础原理是预先经过某种映射变换顶点坐标值,然后在变换域中嵌入秘密消息。

Cho 等人(2007)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,分段聚类后均值调制嵌入秘密消息的算法。Bors 和 Luo(2013)改进了此方法,增加了表面平滑性的约束。Kanai 等人(1998)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。

变换域隐写算法主要评价其鲁棒性。Cho 等人(2007)以及 Bors 和 Luo(2013)提出的方法均具有较强的抗攻击性能。这类算法由于嵌入位置与坐标无关,因此对绝大多数攻击算法均具备一定的鲁棒性,但其主要缺点为低嵌入容量。

3.5　算法比较

本节比较了不同的隐写方法的性能。表 1 比较了不同隐写算法的失真和安全性。若某一隐写算法能有效抵抗所有隐写分析的检测,则视该隐写算法是安全的;否则不安全。对嵌入容量没有进行具体比较,是因为不同隐写算法对于容量上下限的评估不同。对于两态调制隐写和最低位隐写,大多数方法都有严格的容量上限,即不能嵌入超过上限的消息量。而置换隐写方法的上限是估计值,可以逼近但达不到,因此上限不是紧致的。表 2 是不同隐写算法鲁棒性的比较,其中数字攻击包括仿射变换、顶点重新排序、加噪、平滑和简化攻击等。

表 1　3D 网格隐写算法失真和容量的比较

Table 1　Comparison of steganographic methods in terms of distortion and security

类别	方法	失真	安全性
两态调制隐写	Cayre 和 Macq(2003)	较大	×
	Wang 和 Cheng(2005)	中等	×
	Wang 和 Wang(2006)	中等	×
	Chao 等人(2009)	中等	×
	Itier 和 Puech(2017)	中等	×
	Li 等人(2017b)	中等	√
最低位隐写	Yang 等人(2013)	较小	×
	Li 等人(2017a)	较小	×
	Zhou 等人(2019)	较小	√
置换隐写	Bogomjakov 等人(2008)	无	×
	Huang 等人(2009)	无	×
	Tu 等人(2010a)	无	×
	Tu 和 Tai(2012)	无	×
	Wang 等人(2019)	无	√
变换域隐写	Cho 等人(2007)	中等	×
	Bors 和 Luo(2013)	中等	×
	Kanai 等人(1998)	较大	×

注:“√”表示隐写算法抗所有隐写分析的检测,“×”表示隐写算法至少受某种检测攻击。

4　3D 网格隐写分析

3D 网格隐写分析与图像隐写分析相似,均通过提取邻域元素之间的相关性特征作为分类的依据。两者的不同在于图像像素的相关性通常在图像卷积基础上计算得到,而 3D 网格坐标邻域相关性通常由网格卷积作为预处理步骤。如前所述,3D 网格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 3 维空间中相邻元素间的关联度设计残

表 2　3D 网格隐写算法鲁棒性比较

Table 2　Comparison of steganographic methods in terms of robustness

类别	方法	仿射变换攻击	顶点重新排序攻击	加噪攻击	平滑攻击	简化攻击
两态调制隐写	Cayre 和 Macq(2003)	√	√	×	×	×
	Wang 和 Cheng(2005)	√	√	×	×	×
	Wang 和 Wang(2006)	√	√	×	×	×
	Chao 等人(2009)	√	√	×	×	×
	Itier 和 Puech(2017)	√	√	×	×	×
	Li 等人(2017b)	√	√	×	×	×
最低位隐写	Yang 等人(2013)	×	√	×	×	×
	Li 等人(2017a)	√	×	×	×	
	Zhou 等人(2019)	×	×	×	×	×
置换隐写	Bogomjakov 等人(2008)	√	×	√	√	×
	Huang 等人(2009)	√	×	√	√	×
	Tu 等人(2010a)	√	×	√	√	×
	Tu 和 Tai(2012)	√	×	√	√	×
	Wang 等人(2019)	√	×	√	√	×
变换域隐写	Cho 等人(2007)	√	√	√	√	√
	Bors 和 Luo(2013)	√	√	√	√	√
	Kanai 等人(1998)	√	√	×	×	×

注:“√”表示隐写算法对该攻击鲁棒,“×”表示隐写算法容易受到攻击。

差特征,并进一步训练隐写分析分类器实现二分类。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。

4.1　通用型隐写分析

通用型隐写分析由标准化(基于主成分分析(principal component analysis, PCA)的旋转和缩放)、特征提取和分类器的训练构成,如图 2 所示。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。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 3 个主轴方向,并缩放至单位立方体内。

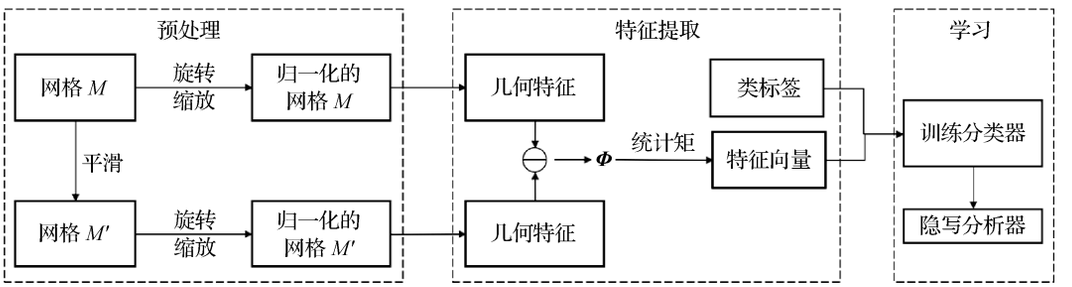


图 2　基于统计残差特征学习的 3D 网格隐写分析框架图

Fig. 2　3D mesh steganalysis framework based on learning from statistics of residual features and classification

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(Fridrich 等,2002;Kodovsky 和 Fridrich,2009)。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,分别对原始信号和平滑后信号计算残差特征,即图 2 中“⊖”,并且计算统计矩进行降低处理。表 3 根据隐写分析特征设计角度比较了不同隐写分析特征和特征维数。

表 3　3D 网格隐写分析方法的基本特征元素

Table 3　Basic feature elements of all 3D mesh steganalytic methods

标号	隐写分析特征	维数	YANG208	YANG40	LFS52	LFS64	LFS76	LFS124	NVT +	WFS228
1	不同价下坐标、坐标范数	24	√							
2	三角面法向量	1	√	√	√	√	√	√	√	
3	二面角夹角	1	√	√	√	√	√	√	√	
4	坐标、坐标范数	8		√	√	√	√	√	√	
5	顶点法向量	1			√	√	√	√	√	
6	高斯曲率	1			√	√	√	√	√	
7	曲率比	1			√	√	√	√	√	
8	边法向量	1				√			√	
9	平均曲率	1				√			√	
10	总曲率	1				√			√	
11	球坐标系下坐标	3					√	√		
12	球坐标系下边夹角	3					√	√		
13	边向量	12						√		√
14	法向量投票张量的特征根	9							√	
15	多分辨率下边向量和小波系数	45								√

注:“√”表示隐写算法抗所有隐写分析的检测。

4.1.1　Yang208 特征

Yang 和 Ivrissimtzis(2014)首次提出了检测载体载密 3D 网格的隐写分析特征,包括基于笛卡儿坐标系下和拉普拉斯坐标系下的坐标分量变化、坐标向量长度变化和坐标点的价小于 6、等于 6 和大于 6 的坐标向量长度变化特征(不抽取 3D 网格边界特征)。其中,拉普拉斯坐标由笛卡儿坐标乘以 3D 网格的 Kirchhoff 矩阵(Bollobás,1998)得到。

同时,他们还提出了相邻三角面间基于二面角角度偏移和三角面法向量方向偏移夹角的特征。特征降维包含抽取均值、方差、偏度和峰度 4 个统计特征,以及直方图相邻 bin 的插值构成另外 4 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。

尽管 YANG208 计算成本较低、特征数量较多,但其检测准确率比其他隐写分析特征弱,表明部分隐写分析特征不起作用。此外,YANG208 特征对不同嵌入率下的载体载密对的检测准确率波动明显,表明其检测隐写算法不够鲁棒。

4.1.2　Yang40 特征

Li 和 Bors(2016a)有效约简了 YANG208,摒弃了若干判决能力较弱的检测子,保留了以下 6 个特征:笛卡儿坐标系和拉普拉斯坐标系下坐标分量的绝对值。此外,笛卡儿坐标系和拉氏坐标系下各个顶点坐标与网格中心的欧氏距离,以及二面角夹角偏移量为作者设计的另两个隐写分析特征。

从以上 10 个特征向量中,分别计算统计特征(均值、方差、偏度和峰度),最终得到 40 维隐写分析特征。与 YANG208 相比,YANG40 特征在特征维数下降的情况下仍能保持较好的隐写分析性能。

4.1.3　LFS52 特征

Li 和 Bors(2016a)提出了基于局部特征集合

(local feature set, LFS)的有效特征,共含有 52 维,简称为 LFS52。第 1 个特征为顶点法向量的偏移量。由于网格表面局部形状曲率能表达网格表面光滑度,因此提出了基于曲率的隐写分析特征。由于最小主曲率和最大主曲率能够反映局部曲面顶点的弯曲程度,因此第 2 个特征为高斯曲率(Rugis 和 Klette,2006)偏移量特征,其中高斯曲率为最小和最大主曲率的乘积。曲率比是最小主曲率与最大主曲率之比,并将曲率比偏移量作为第 3 个特征。

与基于坐标和三角面法线的隐写特征相比,基于顶点法向量和曲率的特征有更强的检测能力。

4.1.4 LFS64 特征

Kim 等人(2017)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以及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。

该方法性能明显优于 LFS52 特征,是由于增加了边法向量、中值曲率和总曲率特征。

4.1.5 LFS76 特征

Li 和 Bors(2017)在 LFS52 基础上进一步提出了球坐标系下坐标分量值变化特征,简称为 LFS76。其中,球坐标系下坐标点与原点的欧氏距离、方位角和仰角的偏移量为新的 3 维特征。球坐标系下三角面的边长分量的偏移量为另外 3 维特征。

通过实验发现,就针对检测隐写算法的隐写分析性能而言,LFS76 特征性能并不优于 LFS64 特征,说明这 6 维新的特征并不能有效检测隐写扰动。

4.1.6 ELFS124 特征

Li 和 Bors(2020a)在 LFS76 特征的基础上,提出了基于边长变化和边长分量变化特征,简称为 ELFS124。笛卡儿坐标系和拉氏坐标系下分别计算 3 种特征:三角面边向量偏移量(模长的差、差的模长和向量差的向量夹角),最后形成了新的 12 维特征。

LFS124 的计算复杂度非常低,而且隐写分析性能有了明显的提升,这说明三角面边向量容易受到隐写扰动的影响。

4.1.7 法向量投票张量(normal voting tensor, NVT)+特征

Zhou 等人(2021a)提出代表邻域的元素,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,他们采用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,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。

Zhou 等人(2021a)设计了三角面法向量的张量投票模型,并通过对张量矩阵特征值分解得到 3 个特征根。特征根的偏移量即为最后的隐写分析特征。将该特征与 LFS76 特征级联得到 100 维的 NVT+隐写分析特征。由于特征值能够反映局部 3D 表面形状的凸起程度,例如尖角、尖锐的边缘或平面,因此 NVT+能够更为有效地检测隐写算法。

NVT+明显地提升了隐写算法的检测性能,同时表明三角面法向量是一个相当有效的隐写分析检测指标。其唯一的缺点是,由于搜索相邻三角面非常耗时,因此该算法的复杂度非常高。

4.1.8 WFS228 特征

Li 和 Bors(2020b)提出在 3D 网格原始模型与其分别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 WFS(3D wavelet feature set)228。

通过采用 3D 懒小波分解(Lounsbery 等,1997)和蝴蝶方案(Dyn 等,1990)得到的小波系数向量,可用于表示不同分辨率下的 3D 网格特征。由于与小波变换相关的水印嵌入方法基本上是通过修改小波系数和 3D 网格的边来实现秘密消息的嵌入,因此这种方式得到的特征能有效地检测 3D 网格隐写算法。此外,可通过分析原模型更大的顶点邻域,得到高分辨率的 3D 网格模型,这种高分辨率模型相比于原网格模型对隐写扰动更敏感。

该算法提出了基于边向量和小波系数向量的 3 种不同分辨率下的隐写分析特征。WF228 特征隐写分析性能优于 LFS76 特征,但劣于 NVT+特征。该算法复杂度也较高,是因为需要搜寻近邻的坐标点。

4.1.9 特征筛选

Li 和 Bors(2016b)、Li 等人(2018)通过特征选择来解决载体来源失配问题(cover source mismatch, CSM)。

Li 和 Bors(2016b)首先对原始 3D 网格进行了简化和加噪处理,并对预处理后的 3D 网格隐写。然后,采用皮尔逊相关系数等技术分析载体和载密网格的差异程度,最后选择有效的隐写分析特征。

4.2　专用型隐写分析

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。

4.2.1　针对基于 PCA 旋转变换隐写的隐写分析

Zhou 等人(2019)指出一系列基于 PCA 变换预处理隐写算法的安全漏洞：预处理后的载密模型和未经过预处理的载体模型是容易受到针对性隐写分析方法检测的。对于任意一测试模型，通过分析其旋转至 PCA 主轴和次轴构建的空间的旋转矩阵，能高效地检测其为载体或载密。

4.2.2　针对置换隐写的隐写分析

Wang 等人(2019)发现置换隐写容易导致 3D 模型存储结构上相邻坐标点失去近邻特性，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。

此方法在检测不同置换隐写算法时是通用的，并不需要任何先验知识，比如具体的隐写方法或者固定的嵌入率。

4.3　算法比较

如图 3 所示，本节分析了不同隐写分析方法的实验结果。实验中采用了两种数据集：普林斯顿分割集和普林斯顿网格。训练过程中，分别对训练集的载体和载密网格提取隐写分析特征，并用集成分类器训练特征。测试过程中，预测测试集的载体和载密网格的分类结果。

本文实验评估了 Chao 等人(2009)大容量 3D 网格隐写算法的性能。嵌入率等间隔取 2 ～ 14 bpv 之间的整数，评价指标为平均检测错误率。结果表明，隐写分析方法性能从高到低排序为：NVT + 、WFS228、LFS124、LFS76、LFS64、LFS52、YANG208。

此外，普林斯顿网格数据集上的平均检测错误率低于普林斯顿分割集上的结果。出现差异的原因在于数据集类型不同：前者是计算机辅助设计(computer-aided design，CAD)技术人工制作而成；而后者是对自然物体扫描重建而得的模型。结果表明，3D 模型表面越平整，越不适合秘密消息的嵌入。

5　结　语

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值得开拓的空间。

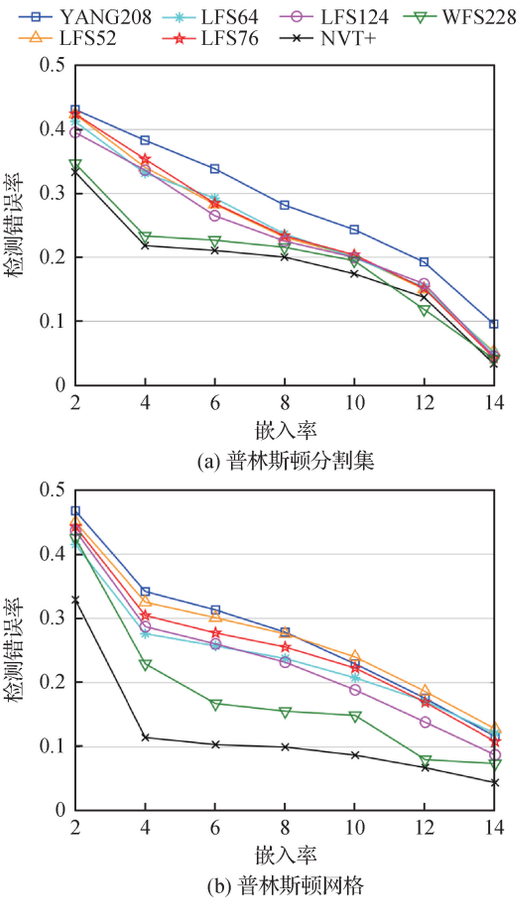


图 3　3D 网格隐写分析性能比较

Fig. 3　3D mesh steganalysis performance comparison

((a) Princeton segmentation benchmark; (b) Princeton ModelNet)

5.1　3D 模型隐写

实现更高的隐写安全性是 3D 网格隐写的目标，本文提出以下改进的方向：

1)融合扰动隐写和置换隐写算法。联合置换隐写和最低有效位隐写是提升隐写安全性的方法。实验表明，当网格的顶点数达到 5 000 时，置换隐写最大嵌入率达到11 bpv，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(Li 等，2015；Denemark 和 Fridrich，2015)。如何对坐标点设计联合失真，并利用 DeJoin(Zhang 等，2017)算法在 x，y，z 分量上分配消息长度，最后利用校验栅格编码(Filler 和 Fridrich，2011)嵌入消息，是实现高安全隐写算法的方式。

3)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(Ker,2006),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(Ker,2007)。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。

5.2 3D模型隐写分析

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Kodovský(2012)提出的富模型特征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(Botsch等,2010),以及最新的曲面平滑技术,例如各向异性扩散流(Bajaj和Xu,2003)、双边滤波(Fleishman等,2003)、非线性平滑(Eigensatz等,2008)和基于神经网络的滤波方法。

2)设计基于深度学习的隐写分析方法。迄今为止,3D网格隐写分析都是基于人工设计的特征实现的检测,而人工特征设计较为复杂,不易于短时间内设计得到。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(convolutional neural network, CNN)(Krizhevsky等,2012)和图卷积网络(graph convolutional network, GCN)(Hamilton等,2017)等。因此,设计针对3D隐写分析的端到端学习的神经网络,是实现更有效的隐写分析性能的解决方案。

参考文献(References)

Bajaj C L and Xu G L. 2003. Anisotropic diffusion of surfaces and functions on surfaces. ACM Transactions on Graphics, 22(1): 4-32 [DOI: 10.1145/588272.588276]

Bogomjakov A, Gotsman C and Isenburg M. 2008. Distortion-free steganography for polygonal meshes. Computer Graphics Forum, 27(2): 637-642 [DOI: 10.1111/j.1467-8659.2008.01161.x]

Bollobás B. 1998. Modern Graph Theory. New York: Springer-Verlag [DOI: 10.1007/978-1-4612-0619-4]

Bors A G and Luo M. 2013. Optimized 3D watermarking for minimal surface distortion. IEEE Transactions on Image Processing, 22(5): 1822-1835 [DOI: 10.1109/TIP.2012.2236345]

Botsch M, Kobbelt L, Pauly M, Alliez P and Lévy B. 2010. Smoothing//Polygon Mesh Processing. CRC Press: 61-74 [DOI: 10.1201/b10688-6]

Cayre F and Macq B. 2003. Data hiding on 3-D triangle meshes. IEEE Transactions on Signal Processing, 51(4): 939-949 [DOI: 10.1109/tsp.2003.809380]

Chao M W, Lin C H, Yu C W and Lee T Y. 2009. A high capacity 3D steganography algorithm. IEEE Transactions on Visualization and Computer Graphics, 15(2): 274-284 [DOI: 10.1109/tvcg.2008.94]

Chen X B, Golovinskiy A and Funkhouser T. 2009. A benchmark for 3D mesh segmentation. ACM Transactions on Graphics, 28(3): #73 [DOI: 10.1145/1531326.1531379]

Cho J W, Prost R and Jung H Y. 2007. An oblivious watermarking for 3-D polygonal meshes using distribution of vertex norms. IEEE Transactions on Signal Processing, 55(1): 142-155 [DOI: 10.1109/tsp.2006.882111]

Denemark T and Fridrich J. 2015. Improving steganographic security by synchronizing the selection channel//Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. Portland, USA: ACM: 5-14 [DOI: 10.1145/2756601.2756620]

Dyn N, Levine D and Gregory J A. 1990. A butterfly subdivision scheme for surface interpolation with tension control. ACM Transactions on Graphics, 9(2): 160-169 [DOI: 10.1145/78956.78958]

Eigensatz M, Sumner R W and Pauly M. 2008. Curvature-domain shape processing. Computer Graphics Forum, 27(2): 241-250 [DOI: 10.1111/j.1467-8659.2008.01121.x]

Filler T, Judas J and Fridrich J. 2011. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security, 6(3): 920-935 [DOI: 10.1109/tifs.2011.2134094]

Fleishman S, Drori I and Cohen-Or D. 2003. Bilateral mesh denoising//ACM SIGGRAPH. San Diego, USA: ACM: 950-953 [DOI: 10.1145/1201775.882368]

Fridrich J J, Goljan M and Hogea D. 2002. Steganalysis of JPEG images: breaking the F5 algorithm//Proceedings of the 5th International Workshop on Information Hiding. Noordwijkerhout, the Netherlands: Springer: 310-323 [DOI: 10.1007/3-540-36415-3_20]

Fridrich J and Kodovský J. 2012. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3): 868-882 [DOI: 10.1109/tifs.2012.2190402]

Girdhar A and Kumar V. 2018. Comprehensive survey of 3D image steganography techniques. IET Image Processing, 12(1): 1-10 [DOI: 10.1049/iet-ipr.2017.0162]

Hamilton W L, Ying R and Leskovec J. 2017. Inductive representation learning on large graphs//Proceedings of the 31st International Con-

ference on Neural Information Processing Systems. Long Beach, USA: Curran Associates Inc. : 1025-1035

Huang N C, Li M T and Wang C M. 2009. Toward optimal embedding capacity for permutation steganography. IEEE Signal Processing Letters, 16(9): 802-805 [DOI: 10.1109/lsp.2009.2024794]

Itier V and Puech W. 2017. High capacity data hiding for 3D point clouds based on static arithmetic coding. Multimedia Tools and Applications, 76(24): 26421-26445 [DOI: 10.1007/s11042-016-4163-y]

Kanai S, Date H and Kishinami T. 1998. Digital watermarking for 3D polygons using multiresolution wavelet decomposition//Proceedings of the 6th International Workshop on Geometric Modeling: Fundamentals and Application. Tokyo, Japan: [s. n.]: 296-307

Ker A D. 2006. Batch steganography and pooled steganalysis//Proceedings of the 8th International Workshop on Information Hiding. Alexandria, USA: Springer: 265-281 [DOI: 10.1007/978-3-540-74124-4_18]

Ker A D. 2007. A capacity result for batch steganography. IEEE Signal Processing Letters, 14(8): 525-528 [DOI: 10.1109/lsp.2006.891319]

Kim D, Jang H U, Choi H Y, Son J, Yu I J and Lee H K. 2017. Improved 3D mesh steganalysis using homogeneous kernel map//Proceedings of International Conference on Information Science and Applications. Singapore, Singapore: Springer: 358-365 [DOI: 10.1007/978-981-10-4154-9_42]

Kodovský J and Fridrich J. 2009. Calibration revisited//Proceedings of the 11th ACM workshop on Multimedia and Security. Princeton, USA: ACM: 63-74 [DOI: 10.1145/1597817.1597830]

Kodovský J, Fridrich J and Holub V. 2012. Ensemble classifiers for steganalysis of digital media. IEEE Transactions on Information Forensics and Security, 7(2): 432-444 [DOI: 10.1109/tifs.2011.2175919]

Krizhevsky A, Sutskever I and Hinton G E. 2012. ImageNet classification with deep convolutional neural networks//Proceedings of the 25th International Conference on Neural Information Processing Systems. Lake Tahoe, USA: Curran Associates Inc. : 1097-1105

Li B, Wang M, Li X L, Tan S Q and Huang J W. 2015. A strategy of clustering modification directions in spatial image steganography. IEEE Transactions on Information Forensics and Security, 10(9): 1905-1917 [DOI: 10.1109/tifs.2015.2434600]

Li N N, Hu J B, Sun R M, Wang S F and Luo Z X. 2017b. A high-capacity 3D steganography algorithm with adjustable distortion. IEEE Access, 5: 24457-24466 [DOI: 10.1109/access.2017.2767072]

Li Z Y, Beugnon S, Puech W and Bors A G. 2017a. Rethinking the high capacity 3D steganography: increasing its resistance to steganalysis//Proceedings of 2017 IEEE International Conference on Image Processing. Beijing, China: IEEE: 510-514 [DOI: 10.1109/icip.2017.8296333]

Li Z Y and Bors A G. 2016a. 3D mesh steganalysis using local shape features//Proceedings of 2016 IEEE International Conference on Acoustics, Speech and Signal Processing. Shanghai, China: IEEE: 2144-2148 [DOI: 10.1109/icassp.2016.7472056]

Li Z Y and Bors A G. 2016b. Selection of robust features for the cover source mismatch problem in 3D steganalysis//Proceedings of the 23rd International Conference on Pattern Recognition. Cancun, Mexico: IEEE: 4256-4261 [DOI: 10.1109/icpr.2016.7900302]

Li Z Y and Bors A G. 2017. Steganalysis of 3D objects using statistics of local feature sets. Information Sciences, 415/416: 85-99 [DOI: 10.1016/j.ins.2017.06.011]

Li Z Y and Bors A G. 2020a. Selection of robust and relevant features for 3-D steganalysis. IEEE Transactions on Cybernetics, 50(5): 1989-2001 [DOI: 10.1109/tcyb.2018.2883082]

Li Z Y and Bors A G. 2020b. Steganalysis of meshes based on 3D wavelet multiresolution analysis. Information Sciences, 522: 164-179 [DOI: 10.1016/j.ins.2020.02.061]

Li Z Y, Gong D F, Liu F L and Bors A G. 2018. 3D steganalysis using the extended local feature set//Proceedings of the 25th IEEE International Conference on Image Processing. Athens, Greece: IEEE: 1683-1687 [DOI: 10.1109/icip.2018.8451643]

Lounsbery M, DeRose T D and Warren J. 1997. Multiresolution analysis for surfaces of arbitrary topological type. ACM Transactions on Graphics, 16(1): 34-73 [DOI: 10.1145/237748.237750]

Pevný T and Fridrich J. 2008. Benchmarking for steganography//Proceedings of the 10th International Workshop on Information Hiding. Santa Barbara, USA: Springer: 251-267 [DOI: 10.1007/978-3-540-88961-8_18]

Rugis J and Klette R. 2006. A scale invariant surface curvature estimator//Proceedings of the 1st Pacific-Rim Symposium on Image and Video Technology. Hsinchu, China: Springer: 138-147 [DOI: 10.1007/11949534_14]

Simmons G J. 1984. The prisoners' problem and the subliminal channel//Advances in Cryptology. Boston, USA: Springer: 51-67 [DOI: 10.1007/978-1-4684-4730-9_5]

Tu S C, Hsu H and Tai W K. 2010a. Permutation steganography for polygonal meshes based on coding tree. International Journal of Virtual Reality, 9(4): 55-60 [DOI: 10.20870/ijvr.2010.9.4.2790]

Tu S C and Tai W K. 2012. A high-capacity data-hiding approach for polygonal meshes using maximum expected level tree. Computers and Graphics, 36(6): 767-775 [DOI: 10.1016/j.cag.2012.06.002]

Tu S C, Tai W K, Isenburg M and Chang C C. 2010b. An improved data hiding approach for polygon meshes. The Visual Computer, 26(9): 1177-1181 [DOI: 10.1007/s00371-009-0398-1]

Wang C M and Cheng Y M. 2005. An efficient information hiding algorithm for polygon models. Computer Graphics Forum, 24(3): 591-600 [DOI: 10.1111/j.1467-8659.2005.00884.x]

Wang C M and Wang P C. 2006. Steganography on point-sampled geom-

etry. Computers and Graphics, 30(2): 244-254 [DOI: 10.1016/j.cag.2006.01.030]

Wang Y M, Kong L S, Qian Z X, Feng G R, Zhang X P and Zheng J M. 2019. Breaking permutation-based mesh steganography and security improvement. IEEE Access, 7: 183300-183310 [DOI: 10.1109/access.2019.2960455]

Yang Y and Ivrissimtzis I. 2014. Mesh discriminative features for 3D steganalysis. ACM Transactions on Multimedia Computing, Communications, and Applications, 10(3): #27 [DOI: 10.1145/2535555]

Yang Y, Peyerimhoff N and Ivrissimtzis I. 2013. Linear correlations between spatial and normal noise in triangle meshes. IEEE Transactions on Visualization and Computer Graphics, 19(1): 45-55 [DOI: 10.1109/tvcg.2012.106]

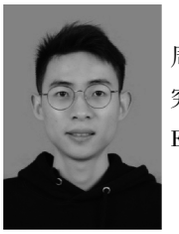
Zhang W M, Zhang Z, Zhang L L, Li H Y and Yu N H. 2017. Decomposing joint distortion for adaptive steganography. IEEE Transactions on Circuits and Systems for Video Technology, 27(10): 2274-2280 [DOI: 10.1109/tcsvt.2016.2587388]

Zhou H, Chen K J, Zhang W M, Qin C and Yu N H. 2021a. Feature-preserving tensor voting model for mesh steganalysis. IEEE Transactions on Visualization and Computer Graphics, 27(1): 57-67 [DOI: 10.1109/tvcg.2019.2929041]

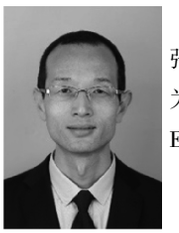
Zhou H, Chen K J, Zhang W M, Yao Y Z and Yu N H. 2019. Distortion design for secure adaptive 3-D mesh steganography. IEEE Transactions on Multimedia, 21(6): 1384-1398 [DOI: 10.1109/tmm.2018.2882088]

Zhou H, Zhang W M, Chen K J, Li W X and Yu N H. 2021b. Three-dimensional mesh steganography and steganalysis: a review. IEEE Transactions on Visualization and Computer Graphics: #3075136 [DOI: 10.1109/TVCG.2021.3075136]

作者简介



周航,1992 年生,男,博士后研究员,主要研究方向为 3D 视觉和多媒体安全。
E-mail: zhouhang2991@gmail.com



张卫明,通信作者,男,教授,主要研究方向为多媒体安全、信息隐藏、人工智能安全。
E-mail:zhangwm@ustc.edu.cn

陈可江,男,博士后研究员,主要研究方向为信息隐藏和人工智能安全。E-mail: chenkj@ustc.edu.cn
俞能海,男,教授,主要研究方向为图像处理与视频分析、媒体内容安全、网络通信与安全。E-mail: ynh@ustc.edu.cn