计 算 机 研 究 与 发 展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202221040
61(6): 1536−1544, 2024

基于顶点划分和坐标标准化的密文域3维网格模型可逆信息隐藏

吕皖丽[1] 唐 运[1] 殷赵霞[2] 罗 斌[1]
[1](智能计算与信号处理教育部重点实验室(安徽大学) 合肥 230601)
[2](华东师范大学通信与电子工程学院 上海 200241)
(lwl@ahu.edu.cn)

Reversible Data Hiding for 3D Mesh Model in Encrypted Domain Based on Vertex Partition and Coordinate Standardization

Lü Wanli[1], Tang Yun[1], Yin Zhaoxia[2], and Luo Bin[1]
[1] (*Key Laboratory of Intelligent Computing and Signal Processing* (*Anhui University*), *Ministry of Education*, *Hefei* 230601)
[2] (*School of Communication & Electronic Engineering*, *East China Normal University*, *Shanghai* 200241)

Abstract Reversible data hiding in encrypted domain enables the secure and confidential embedding of additional information in encrypted multimedia, ensuring the privacy and integrity of both the carrier and the embedded data during transmission. The authorized recipients can extract the data without any loss and recover the media successfully. In the realm of digital media, 3D mesh models, being a relatively nascent form, possesses a distinctive file structure markedly different from that of conventional image media. Consequently, limited research has been conducted in this domain. Augmenting the embedding capacity of 3D mesh models in the encrypted domain poses an enduring challenge. The direct application of multiple most significant bit prediction algorithm from the image domain to 3D mesh models is impeded by disparities in data storage formats, thus encumbering the predictive performance of algorithms. To effectively tackle this issue, we propose the adoption of coordinate standardization to eliminate the influence of the sign bit and ameliorate the prediction algorithm's overall performance. In order to further mitigate the inclusion of redundant auxiliary information, we introduce the integration of the selection of embedding set vertices into our experiments, which effectively generates additional payload space. The experimental results affirm that our purposed methodology attains the maximum embedding capacity while guaranteeing lossless and separable recovery of both the model and the embedded information, surpassing the capabilities of existing techniques.

Key words 3D mesh model; reversible data hiding; encrypted domain; prediction error; embedding capacity

摘 要 密文可逆信息隐藏技术可以在加密载体中利用冗余空间额外嵌入信息,在传输过程中保障载体和信息的隐私安全,载体接收者还可以实现无损地提取信息和恢复载体.3维网格模型作为新型的数字媒体,其文件结构与传统的图像等数字媒体存在着不同,并且在该领域的研究相对较少.如何提升模型的嵌入容量是目前需要解决的问题.将图像领域多个高有效位预测算法直接迁移到3维模型中应用时,由于数据的存储格式与图像媒体不同,使得算法的预测性能受到了限制.因此,提出了将顶点坐标值标准化处理,消除符号位带来的影响,提升了预测算法的性能.为了进一步减少无用的辅助信息,嵌入集顶点的筛选被加入实验中,成功地为有效载荷腾出空间.实验表明,提出的方法与现有方法相比,在保证无损和可

收稿日期: 2022-12-30; **修回日期**: 2023-08-16
基金项目: 国家自然科学基金项目(62172001,61872003); 安徽省高等学校科学研究项目(2022AH50120)
This work was supported by the National Natural Science Foundation of China (62172001,61872003) and the Research Project of Anhui Provincial Department of Education (2022AH50120).
通信作者: 殷赵霞(zxyin@cee.ecnu.edu.cn)

分离地恢复模型与所嵌入的信息的同时，获得了最高的嵌入容量.

关键词 3 维网格模型；可逆信息隐藏；密文域；预测误差；嵌入容量

中图法分类号 TP309

信息隐藏技术[1]通过将额外数据嵌入到多媒体载体中，可以提取额外数据从而实现载体的版权认证和隐私保护. 信息隐藏技术根据应用场景可分为 3 类：隐写与隐写分析[2−3]、数字水印[4−5]和可逆信息隐藏[6−7]. 隐写技术用于隐蔽通信，使得人眼视觉系统和隐写分析技术无法感知和捕获额外数据的存在. 数字水印技术分为鲁棒水印和脆弱水印，分别被应用于版权保护和数据完整性验证. 可逆信息隐藏不仅可以正确地提取额外数据还可以无损地恢复原始载体，保证了原始载体的完整性，这在医疗、军事等对多媒体数据的完整性和正确性有着严苛要求的领域具有重要意义. 随着大数据技术和云计算的发展，数据的传递和存取变得更加方便和快捷. 与此同时，数据的安全和隐私保护问题迫在眉睫[8]，与添加头文件等方法不同，密文域可逆信息隐藏算法[9−12]将额外数据巧妙地嵌入到载体中，使得嵌入的数据更加隐蔽和安全，并保持了数据和载体的完整性，因此越来越受到研究者们的关注.

3 维网格模型在医疗、电影和建筑行业都有着广泛的应用[13−14]. 设计和制作 3 维模型需要消耗大量的费用和人力，因此将模型数据加密后再经过云端进行传输和存取可以保护模型所有者的版权和隐私. 为了方便云端管理者对加密的模型进行管理和分配，研究基于 3 维网格的密文可逆信息隐藏算法是具有重要意义的. 如图 1 所示，原始模型在经过加密后很好地保护了模型的数据和内容，这在云安全、医疗数据和司法取证等方面都具有重要意义. 密文域可逆信息隐藏算法对不同的应用方都有重要的评价指标[15]. 在信息嵌入时，算法的嵌入能力决定了嵌入信息长度. 嵌入容量越大所带来的信息嵌入能力也越强，这对信息隐藏者而言是至关重要的. 因此嵌入容量是算法的重要评价指标之一. 在信息提取和模型恢复时，信息提取或模型恢复一旦出现错误，模型接收者就无法准确地获得信息或模型，那么信息的隐藏也就失去了意义. 因此，信息和模型的无损恢复和提取是重要的评价指标之一. 载密模型恢复与嵌入信息提取能否可分离地独立操作，影响了算法的应用场景. 对于模型所有者，并不希望信息接收者在提取信息时获得到关于模型的相关信息，实现可分离地提取信息和恢复模型是具有重要意义的. 因此，方法的可分离性也是重要指标之一.

文献 [16] 首次提出了密文域 3 维网格可逆信息隐藏算法. 然而该算法中信息提取存在误码率的情况. 文献 [17–18] 在文献 [16] 的工作基础上设计了新的预测方法，通过 MSB（most significant bit, MSB）预测的方法，不仅做到了可分离提取信息，还提升了嵌入容量. 文献 [19] 根据不同顶点的嵌入能力，为网格顶点设计了标签机制，自适应地调整嵌入信息的长度，进一步提升了嵌入容量，然而文献 [19] 对顶点的划分方法单一，没有充分利用 3 维网格模型的结构信息. 文献 [20] 改进了的顶点的划分方式，进一步提升了嵌入容量. 然而，该工作在应用多 MSB 预测方法到 3 维网格模型上时，没有做到更加合适的改进，使得预测值偏差较大，模型嵌入容量仍存在着改进的空间. 文献 [21–22] 提出了利用同态加密算法进行额外信息嵌入的方法. 然而，使用的加密方法所需要的计算复杂度较高，并且模型的嵌入容量较低. 文献 [23] 提出了空间划分和空间编码的方法，利用顶点坐标

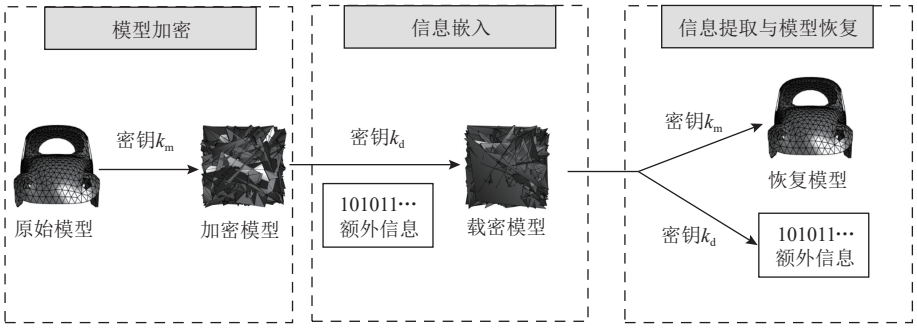

Fig. 1 Framework for 3D mesh reversible data hiding algorithm in encrypted domain

图 1 密文域 3 维网格可逆信息隐藏算法框架

值与子空间边界顶点坐标值的比值进行加密和信息嵌入. 然而该方法会因为阈值的错误设置而导致信息提取错误.

现有的方法对3维网格信息嵌入方式进行了深入的研究，但是由于对3维网格的文件结构和数据存储的研究和利用还不够深入，在顶点的划分和嵌入数据的处理上存在不足，导致3维网格模型的嵌入容量较低. 本文提出了一种基于多MSB预测算法的密文域3维网格算法，主要贡献有2点：

1)提出了一种顶点坐标标准化方法，减少由于顶点坐标MSB是符号位给多MSB预测算法带来预测影响. 数据标准化处理可以有效地提升预测算法在3维模型中的性能，提升顶点的嵌入长度，有效地增加模型的嵌入容量.

2)现有方法忽略了嵌入顶点集的处理，存在闲置顶点和冗余标签数据. 闲置顶点既没有做到有效地嵌入额外信息，也没有发挥预测能力，反而增加了辅助信息的长度，占据了有效载荷的空间. 对该部分的顶点处理，可以有效地减少辅助信息的长度，增加有效载荷.

1 相关工作

本节介绍了3维网格模型的数据格式和目前基于3维网格模型的密文域可逆信息隐藏算法.

1.1 3维网格模型结构

3维模型中最为常见的是3维网格模型.3维网格模型由多个多边形组成[24]. 本文将围绕应用最广的3维网格模型展开研究. 模型中包含了顶点集合和面集合. 顶点集合中包含了顶点在直角坐标系中的坐标位置，面集合中记录了每个面包含的顶点信息. 点和面的关系可以表示为：

$$\begin{aligned} &V=\{v_i,|0<i<\alpha\},\\ &v_i=\{v_{i,x},v_{i,y},v_{i,z}\},\\ &F=\{f_j|0<j<\beta\},\\ &f_j=\{v_{j,1},v_{j,2},v_{j,3}\}, \end{aligned} \tag{1}$$

其中V表示顶点集合，v_i表示顶点，α表示顶点的个数，x,y,z分别代表坐标轴的3个方向，F表示面的集合，f_j表示面，β代表面的个数.

1.2 密文域3维网格模型可逆信息隐藏

文献[16]首次提出了将秘密信息嵌入在多个MSB的密文域3维网格模型可逆信息隐藏算法中. 然而，该方法嵌入容量上限较低且在提取过程中存在错误提取，需要结合纠错码使用. 文献[17]提出了基于MSB的预测方法，腾出了更多的嵌入空间，成功实现了嵌入信息无损和可分离地提取. 文献[18]将预测方法扩展到了多MSB预测，进一步实现了容量的提升. 然而，该方法对于所有顶点的预测采用了同一嵌入长度，没有做到自适应性. 文献[19]通过增加标签机制，记录模型中每一个顶点变长的嵌入能力，大大地提升了嵌入容量. 然而，文献[19]的方法在顶点的划分时，没有充分考虑顶点间的拓扑关系，对点的划分不够合理. 文献[20]结合面集合和顶点集合，对预测顶点进行了筛选处理，提升了嵌入顶点的利用率，在嵌入容量上又取得了进一步的提升. 文献[21]利用同态加密的特性，提出了2层嵌入的方法. 第1层的信息嵌入由信息发送方嵌入，利用直方图平移技术实现了数据的嵌入. 在加密的模型上，利用Paillier密码系统的自盲性，云服务器负责人可以实现第2层额外信息的嵌入. 然而该方法的嵌入容量较低且计算复杂度高. 文献[22]提出了一种基于同态加密且没有文件扩展的嵌入方式，但是该方法舍弃了浮点数值尾数中的多个低位，使得原始模型只能进行重建而无法获得无损的恢复. 文献[23]提出了一种将顶点划分在多个子空间，并利用顶点与子空间边界顶点数值比例进行加密和数值嵌入，实现了顶点接近100%的利用率. 但该方法的嵌入容量较低且在数据提取过程中存在错误选择阈值时会造成大量的数据提取错误.

2 方 法

本文方法共有3方参与者，分别是模型拥有者、信息隐藏者和模型接收者. 图2给出了方法的流程图：首先，模型拥有者需要对模型进行预处理操作，从而腾出空间用于嵌入额外信息，模型拥有者对模型进行流密码加密，再进行模型的传输，保护模型的隐私安全；然后信息隐藏者对加密的模型嵌入额外信息；最后模型接收者根据自己手中的密钥解密出信息或模型.

2.1 数据拥有者

预处理阶段是为了找出模型中的冗余空间，计算信息的嵌入位置. 该部分执行3步操作：1)模型顶点划分；2)坐标标准化；3)多MSB预测.

1)模型顶点划分

在3维网格中，同一个面上的顶点的空间坐标相近，因此可以使用相邻的顶点进行坐标值的预测. 在文献[16–18]的方法中，顶点是从面集合中的每个面

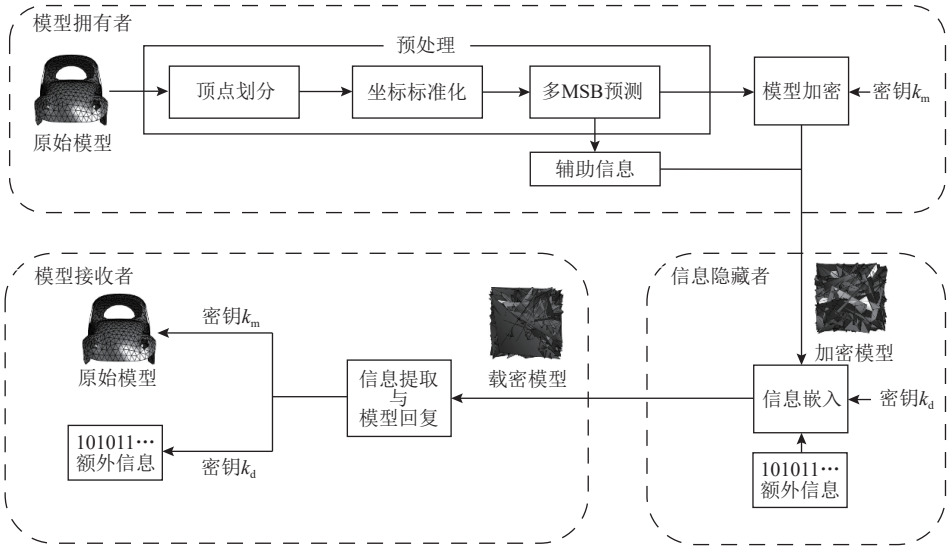

Fig. 2 Flowchart of our proposed method

图 2 所提方法的流程图

中抽取 1 个点纳入嵌入集. 文献 [19] 按照顶点集合中顶点序号的奇偶性划分嵌入集和预测集. 例如, 所有的偶数顶点用于嵌入, 所有的奇数顶点用于预测. 文献 [20] 发现由于 3 维网格复杂的拓扑关系, 同一个顶点会存在多个面上, 并与多个顶点具有关联. 因此, 仅使用奇偶划分嵌入集和预测集忽略了 3 维模型的拓扑结构. 因此, 文献 [20] 根据奇偶初始化的顶点进行了再筛选处理, 使用面集合信息将预测集中的顶点纳入到嵌入集中, 提升嵌入顶点的利用率. 然而, 该方法忽略了嵌入集中存在着一类特殊顶点, 这类顶点在初始化时不存在用来预测它们的相关点, 不仅没有嵌入信息, 反而占用了标签信息, 增加了辅助信息长度, 减少了有效载荷. 我们进一步改进了文献 [20] 的划分方法. 首先利用奇偶性, 初始化嵌入集和预测集. 这里以偶数顶点为预测集、奇数顶点为嵌入集为例. 然后, 顺序遍历预测集中的顶点, 将预测集顶点相邻偶数点数目不大于奇数点数目 2 倍且偶数点数目大于 2 的顶点纳入到嵌入集中. 这样做既保证了具有更好的预测能力的顶点不被错误筛选, 又保证了加入嵌入集的顶点可以被正确预测. 最后, 将嵌入集中的不具有相邻顶点的嵌入顶点划为预测集. 这样, 既避免了顶点的无效使用, 又减少了辅助信息的长度.

2)坐标标准化

3 维网格模型在计算机中的存储为 32 b 浮点小数, 但在实际应用中并不需要这么高的精密度[25]. 将浮点小数变换成整数有利于下一步的多 MSB 预测和流密码加密. 首先将顶点坐标值扩大m倍, 变换公式为:

$$v' = \lfloor v \times 10^m \rfloor, m \in \{1,2,\cdots,33\}, \tag{2}$$

其中v为初始网格顶点值, v'为可扩大后的坐标值, m是顶点值扩大的倍数. 变换后的坐标值的长度l与m的对应关系如式(3)所示, 其中, m的大小与保留的精度和嵌入容量之间具有关联, 后面在实验部分会进一步讨论和分析.

$$l = \begin{cases} 8, & 1 \leqslant m \leqslant 2, \\ 16, & 3 \leqslant m \leqslant 4, \\ 32, & 5 \leqslant m \leqslant 9, \\ 64, & 10 \leqslant m \leqslant 33. \end{cases} \tag{3}$$

在文献 [16–20] 中, 顶点值的预测直接采用了灰度图像的预测方法[26]. 灰度图像的数值在 0~255, 而 3 维模型的顶点坐标值存在着正负. MSB 的符号位限制了预测方法在 3 维网格模型中的使用. 为了使该方法更好地发挥预测效果. 我们应消除符号位带来的影响, 将负数变换成正数时需要记录变换顶点的坐标位置, 这会增加辅助信息的长度. 因此, 我们使所有的坐标采用统一的映射函数进行数值标准化:

$$v'' = \left\lfloor \frac{v' - 10^m}{2} \right\rfloor, m \in \{1,2,\cdots,33\}. \tag{4}$$

模型接收者在恢复模型时只需要执行逆运算就可以获得恢复模型v''的浮点表示.

3)多 MSB 预测

每个嵌入点使用它相邻的顶点进行预测并计算出顶点的可嵌入长度. 顶点坐标具有 3 个维度, 在预测时, 3 个维度分别预测, 最后取其中的最小可嵌入长度作为该顶点的可嵌入长度并记录为辅助信息.

如图 3 所示, 嵌入顶点使用了 3 个相邻顶点作为预测顶点. 预测顶点在预测每一位时, 选取 0 和 1 中出现次数最多的作为预测值, 若出现次数相同则任选其一(为保证可逆性可设置固定选取值). 以图 3 为例, 该顶点在 x, y, z 这 3 个方向上分别具有的可嵌入位长度为 4, 3, 5, 所以选取其中最小的嵌入长度 3 作为该顶点的可嵌入长度并记录该顶点的标签信息. 然后, 模型拥有者对模型预处理后使用密钥 k_m 对模型进行流密码加密, 并将被加密的模型和辅助信息发送给信息隐藏者.

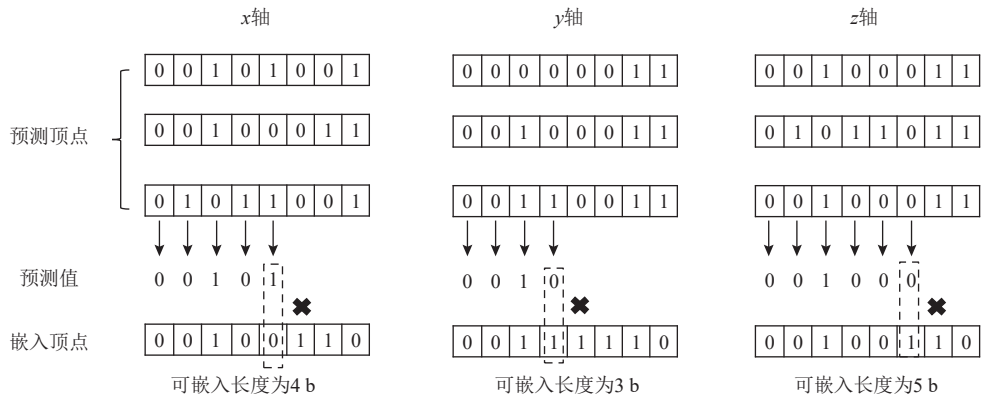

Fig. 3 Multi-MSB prediction method

图 3 多 MSB 预测方法

2.2 信息隐藏者

信息隐藏者在接收到被加密的模型后, 在标签信息的帮助下进行额外信息的嵌入. 如图 4 所示, 首先将模型的坐标值转换成二进制表示, 根据标签辅助信息, 再将二进制比特流分为可嵌入数据和不可嵌入数据. 为了模型接收者可以准确提取信息或恢复模型, 信息隐藏者将可嵌入的比特流放在前方, 不可嵌入的比特流放在后方. 标签信息的长度占据了腾出的信息嵌入空间, 为了减少辅助信息的长度, 本文采用算术编码将辅助信息进行压缩. 不同模型的顶点数目不同, 压缩后的辅助信息长度也不同. 为了确保辅助信息长度可以被准确地记录, 我们将根据不同模型的可嵌入顶点数目和坐标标准化的十进制长度自适应地改变存储辅助信息长度的位数, 其计算公式为 $\lg(\lg(l))\times 3\times n_e$, 其中 l 为坐标值的十进制长度, n_e 为模型中可嵌入顶点的数目. 信息隐藏者在剩余的可嵌入比特流中嵌入被密钥 k_d 加密的额外信息. 最后, 含有额外信息的比特流重构生成一个新的 3 维网格模型.

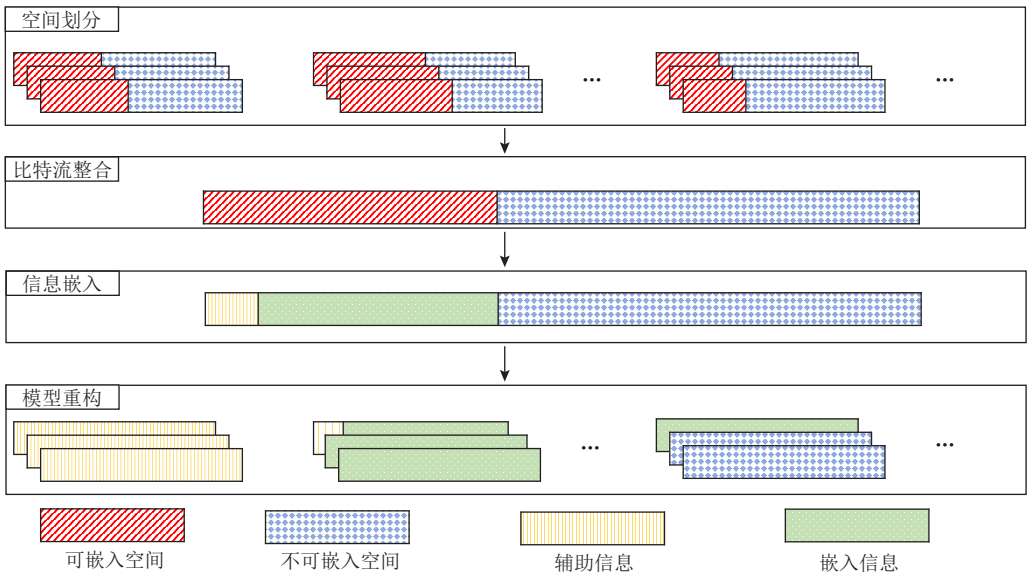

Fig. 4 Process of information embedding

图 4 信息嵌入过程

2.3 模型接收者

模型接收者根据自己手中的密钥可以解密出对应的数据. 此时存在着 3 种情况：

1)模型接收者只拥有嵌入信息的密钥. 模型接收者对模型重复同样的预处理过程. 在获得二进制比特流后，提取位于前方的辅助信息. 根据标签信息，将被加密的嵌入信息全部提取后使用密钥k_{d}解密出嵌入的信息.

2)模型接收者只拥有模型的密钥. 模型接收者在模型进行预处理的过程中获得二进制比特流后，提取位于前方的辅助信息. 在标签的帮助下，结合后方未被修改的二进制比特流重构 3 维网格模型的二进制比特流后使用密钥k_{m}解密. 此时嵌入顶点的高位数值是存在错误的. 数据接收者利用未被修改的顶点坐标值预测并恢复嵌入顶点坐标值的错误高位，获得正确的原始模型.

3)数据接收者同时拥有嵌入信息和模型的密钥. 此时数据接收者只需要采取前 2 种情况同样的处理就可以同时获得正确的嵌入信息和原始模型. 但是要注意的是，嵌入信息的提取需要在模型解密前完成.

3 实验与分析

在实验部分，本文首先介绍使用的评价指标，接着对所提方法进行了视觉质量评估、可逆性分析、嵌入容量分析、消融实验和对比分析. 本文实验在 WIN10 系统下使用 MATLAB 语言编写并运行在 MATLAB R2021a 上. 实验使用了图 5 中的 4 张标准测试模型. 为了测试算法的通用性，我们测试了 Princeton benchmark[27] 中 380 张模型的平均嵌入容量并与现有的算法进行平均嵌入率的比较.

3.1 评价指标

信噪比(signal-noise-ratio, *SNR*)用来评价模型之间的几何失真，其计算公式为

$$SNR = 10\times\lg\frac{\sum_{i=1}^{n}[(v_{i,x}-\bar{v}_x)^2+(v_{i,y}-\bar{v}_y)^2+(v_{i,z}-\bar{v}_z)^2]}{\sum_{i=1}^{n}[(v'''_{i,x}-v_{i,x})^2+(v'''_{i,y}-v_{i,y})^2+(v'''_{i,z}-v_{i,z})^2]}, \tag{5}$$

其中v_x,v_y,v_z是原始坐标值，$\bar{v}_x,\bar{v}_y,\bar{v}_z$是原始坐标的平均值，$v'''_{i,x},v'''_{i,y},v'''_{i,z}$是恢复后的模型坐标值. *SNR* 值越大，说明模型结构越相似.

Hausdorff 距离定义度量空间中任意 2 个集合之间的距离. 若存在 2 个集合$A=\{a_i|i=1,2,\cdots,n\}$和$B=\{b_i|i=1,2,\cdots,n\}$，则A和B这 2 个集合之间的 Hausdorff 距离计算公式为

$$D(A,B)=\max(d(A,B),d(B,A)), \tag{6}$$

$$d(A,B)=\max_{a\in A}\min_{b\in B}\|a-b\|,$$

$$d(B,A)=\max_{b\in B}\min_{a\in A}\|b-a\|.$$

Hausdorff 距离越小，说明模型越接近.

嵌入率(embedding rate, *ER*)是指模型中每个顶点的有效嵌入位数，单位为位每顶点(bit per vertex, bpv)，是衡量算法嵌入容量的重要指标. 其计算公式为：

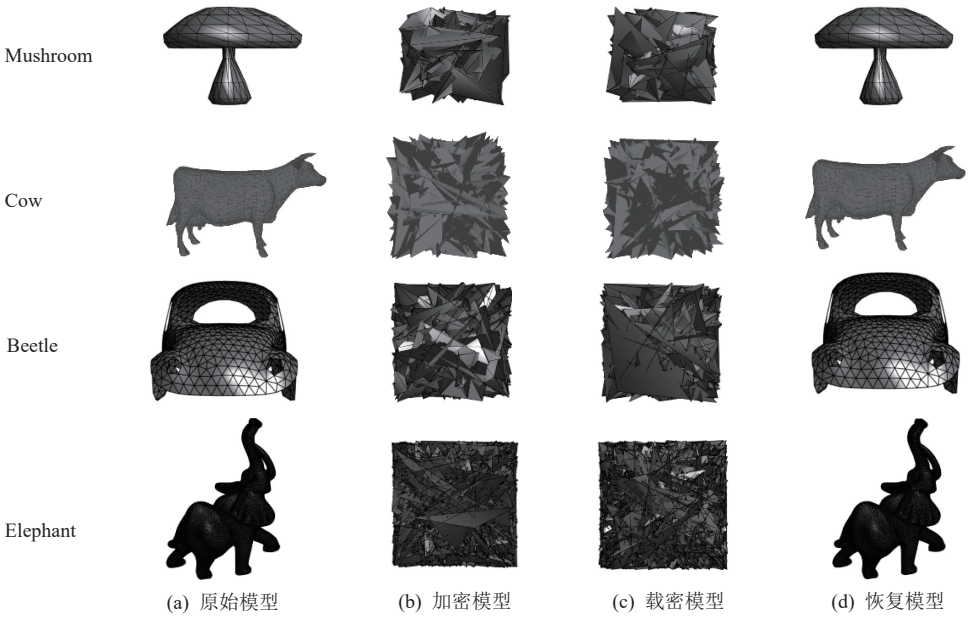

Fig. 5 The visual quality of test model

图 5 测试模型的视觉质量

$$ER=\frac{l_{\mathrm{p}}-l_{\mathrm{ai}}}{n},\tag{7}$$

其中l_{p}是嵌入信息的总长度，l_{ai}是辅助信息的总长度，n是顶点的总数目.

3.2 视觉质量和可逆性

由图 5 可知，本文的加密模型和载密模型很好地保护了模型在网络上传输时的隐私，恢复模型与原始模型在人眼视觉上也几乎不存在差别. 为了更好地评估方法的视觉质量和可逆性，我们选取了 4 张测试模型，在预处理阶段对模型取不同m值进行数值映射时模型的 *SNR* 和 Hausdorff 距离数值变化如图 6 所示，本文测试模型的 *SNR* 值随m值的增大而增加，当m=5 时，所测试的 4 个模型的 *SNR* 值都接近 100 dB；Hausdorff 距离随m值的增大而逐渐变小，在m=5 时，所测试的模型的 Hausdorff 距离几乎接近于 0. *SNR* 和 Hausdorff 距离的变化曲线表明了，m值越大，本文测试方法对模型造成的影响越小，恢复模型的质量越高.

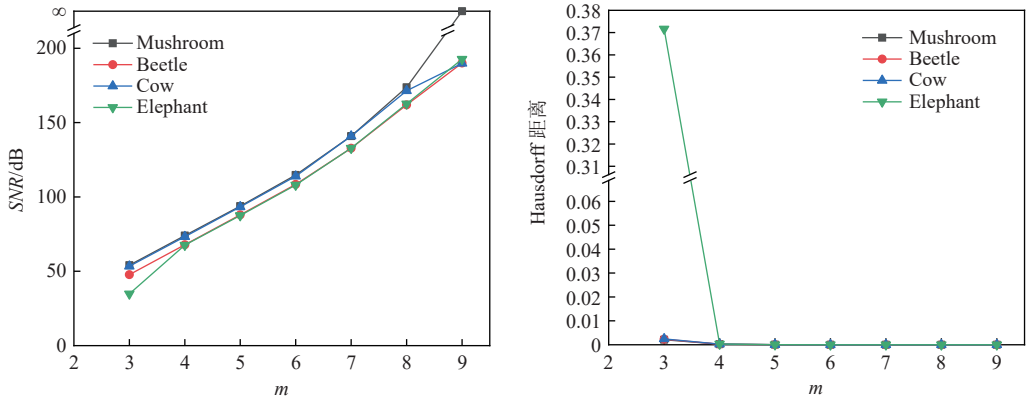

Fig. 6 Result of *SNR* and Hausdorff distance varying with m values

图 6 *SNR* 和 Hausdorff 距离随着m值变化结果

3.3 嵌入容量

参数m的取值大小不仅影响模型的恢复质量，也影响模型的 *ER*. 图 7 展示了 4 张测试模型在不同m取值下嵌入容量的变化. 由图 7 可知，随着m值变化，嵌入容量也在变化. 当m<3 时，模型顶点的坐标值被存储为 8 b，损失了过多的精度，因此不考虑使用，在图 7 中无显示. 当m=3 时，模型精度被保存为 16 b；当m=4 时，增加了 MSB，使得模型的可嵌入空间减少. 当m=5 时，模型精度在计算机中被存储为 32 b，数据冗余极大地增加，*ER* 也获得提升；随着m值变大，更多的低位数据被保留，使得嵌入空间减少，造成 *ER* 下降.

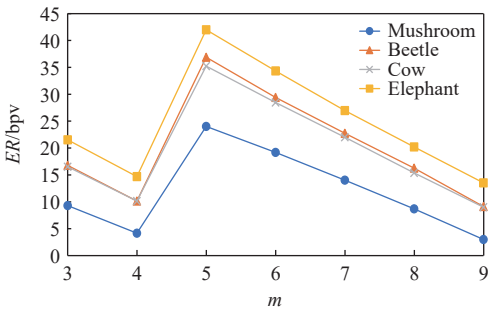

Fig. 7 *ER* of 4 tested models under different m values

图 7 4 张测试模型在不同m值下的 *ER*

3.4 消融实验

为了验证本文方法对于嵌入容量的提升，我们对预处理中的嵌入集顶点过滤和坐标标准化进行了消融实验. 从表 1 可以看出，嵌入集顶点过滤方法可以有效地去除无用的嵌入顶点，继而减少多余的辅助信息，节省出更多的有效载荷. 表 1 中的 Mushroom 模型由于嵌入顶点都存在相邻预测顶点，因此顶点划分未获得优化效果. 坐标标准化成功地消除了符号位给多 MSB 预测方法带来的负面影响，进一步提升了多 MSB 预测算法在 3 维网格模型中的预测能力，成功地提升了模型的 *ER*.

Table 1 Ablation Experiment of Coordinate Standardization and Vertex Partitioning

表 1 坐标标准化和顶点划分的消融实验

测试模型	*ER*/bpv			
	IWDW 2022[20]	坐标标准化	顶点划分	坐标标准化+顶点划分
Mushroom	22.53	24.01	22.53	24.01
Cow	32.04	35.14	32.11	35.22
Beetle	31.75	36.5	31.96	36.87
Elephant	38.93	41.05	39.36	41.98

3.5 对比分析

我们在*ER*、加密方法、可分离提取和数据误码方面与目前最新的方法进行了对比分析并将结果展示在了表2中.

Table 2 Comparison of Features with Existing Methods

表2 与现有方法特征的对比

方法	*ER* /bpv	加密方式	可分离性	信息准确提取	模型完全恢复
TMM2017[16]	0.34	流加密	×	×	×
AJSE2018[21]	6	同态加密	√	√	√
ICIP2021[22]	16	同态加密	√	√	√
TMM2021[23]	7.68	流加密	√	×	√
CognitComput2022[17]	1.06	流加密	√	√	√
PRCV2021[18]	14.25	流加密	√	√	√
SIGPRO2022[19]	25.65	流加密	√	√	√
IWDW2022[20]	33.15	流加密	√	√	√
本文	36.52	流加密	√	√	√

1)*ER*方面. 文献[16]的方法是加密后腾出空间的方法，由于加密后熵值增加，冗余空间小，模型*ER*较低；文献[21–22]利用了同态加密特性进行了加密，但是嵌入容量同样有限；文献[23]的方法尽管顶点可用率较高但每个顶点的*ER*较低；文献[17–20]由于对于多MSB预测方法迁移到3维模型中没有进一步改进，预测的性能没有达到最优；本文方法优化了顶点的划分方法并且进一步提升了多MSB预测算法在3维网格中的预测效率，取得了目前最高的*ER*.

2)加密方式方面. 本文方法采用了该领域广泛使用的流密码加密，与同态加密相比能够极大程度减少计算复杂度.

3)信息提取和模型恢复方面. 文献[16]由于平滑函数计算结果导致信息提取和模型恢复存在误码；文献[22]对浮点数表示的尾数进行部分舍弃导致了原始模型无法被无损地恢复；文献[23]一旦对关键参数的阈值选择错误就会存在大量的错误信息；而本文方法在信息提取和模型恢复都可以做到零误差.

4 总 结

本文面向3维网格模型提出了一种高容量密文域可逆信息隐藏算法. 首先针对3维网格顶点坐标值符号位对预测效果的限制问题，提出了标准化处理，提升了预测效率；其次通过对嵌入顶点的筛选，减少无用顶点的标签信息，从而缩短了辅助信息的长度. 这2种方法的成功结合提高了3维网格模型密文域可逆信息隐藏算法的有效载荷. 实验结果表明，在保证算法可分离性、信息无误提取以及模型完全恢复的同时，能够获得最高嵌入率.

由于辅助信息占据了总嵌入容量的空间，在未来，我们将研究如何优化辅助信息的表示方法，进一步压缩辅助信息的长度和提升算法的有效嵌入率.

作者贡献声明：吕皖丽负责设计实验方案、指导代码撰写、处理与分析实验数据，以及修改论文；唐运负责实现实验和撰写论文；殷赵霞提供论文选题和结构，以及修改论文；罗斌指导论文撰写和修改论文.

参 考 文 献

[1] Zhang Xinpeng, Yin Zhaoxia. Data hiding in multimedia[J]. Chinese Journal of Nature, 2017, 39(2): 87−95 (in Chinese)
(张新鹏, 殷赵霞. 多媒体信息隐藏技术[J]. 自然杂志, 2017, 39(2): 87−95)

[2] Zhou Hang, Chen Kejiang, Zhang Weiming, et al. 3D mesh steganography and steganalysis: Review and prospect[J]. Journal of Image and Graphics, 2022, 27(1): 150−162 (in Chinese)
(周航, 陈可江, 张卫明, 等. 3D网格隐写与隐写分析回顾与展望[J]. 中国图象图形学报, 2022, 27(1): 150−162)

[3] Chen Junfu, Fu Zhangjie, Zhang Weiming, et a1. Review of image steganalysis based on deep learning[J]. Journal of Software, 2021, 32(2): 551−578 (in Chinese)
(陈君夫, 付章杰, 张卫明, 等. 基于深度学习的图像隐写分析综述[J]. 软件学报, 2021, 32(2): 551−578)

[4] Su Wengui, Shen Yulong, Wang Xiang. Two-layer reversible watermarking algorithm using difference expansion[J]. Journal of Computer Research and Developmen, 2019, 56(7): 1498−1505 (in Chinese)
(苏文桂, 沈玉龙, 王祥. 双层差值扩展可逆数字水印算法[J]. 计算机研究与发展, 2019, 56(7): 1498−1505)

[5] Gong Daofu, Liu Fenlin, Luo Xiangyang. A variable payload self embedding fragile watermarking algorithm for image[J]. Journal of Computer Research and Development, 2014, 5l(11): 2505−2512 (in Chinese)
(巩道福, 刘粉林, 罗向阳. 一种变容量的自嵌入图像易碎水印算法[J]. 计算机研究与发展, 2014, 5l(11): 2505−2512)

[6] Shi Yunqing, Li Xiaolong, Zhang Xinpeng, et al. Reversible data hiding: advances in the past two decades[J]. IEEE Access, 2016, 4: 3210−3237

[7] Ou Bo, Yin Zhaoxia, Xiang Shijun. Overview of reversible data hiding in plaintext image[J]. Journal of Image and Graphics, 2022, 27(1): 111−124 (in Chinese)
(欧博, 殷赵霞, 项世军. 明文图像可逆信息隐藏综述[J]. 中国图象图形学报, 2022, 27(1): 111−124)

[8] Luo Yating, He Hongjie, Chen Fan, et al. Security analysis of image encryption for redundant transfer based on non-zero-bit number

feature[J]. Journal of Computer Research and Development, 2022, 59(11): 2606−2617 (in Chinese)
(罗雅婷, 和红杰, 陈帆, 等. 基于非 0 比特个数特征的冗余转移图像加密安全性分析[J]. 计算机研究与发展, 2022, 59(11): 2606−2617)

[9] She Xiaomeng, Du Yang, Ma Wenjing, et al. Reversible data hiding in encrypted images based on pixel prediction and block labeling[J]. Journal of Computer Research and Development, 2022, 59(9): 2089−2100 (in Chinese)
(佘晓萌, 杜洋, 马文静, 等. 基于像素预测和块标记的图像密文可逆信息隐藏[J]. 计算机研究与发展, 2022, 59(9): 2089−2100)

[10] Yang Yaolin, He Hongjie, Chen Fan, et al. Reversible data hiding of image encryption based on prediction error adaptive coding[J]. Journal of Computer Research and Development, 2021, 58(6): 1340−1350 (in Chinese)
(杨尧林, 和红杰, 陈帆, 等. 基于预测误差自适应编码的图像加密可逆数据隐藏[J]. 计算机研究与发展, 2021, 58(6): 1340−1350)

[11] Wu Youqing, Ma Wenjing, Yin Zhaoxia, et al. Reversible data hiding in encrypted images based on bit-plane com-pression of prediction error[J]. Journal on Communications, 2022, 43(8): 219−230 (in Chinese)
(吴友情, 马文静, 殷赵霞, 等. 基于预测误差位平面压缩的密文图像可逆信息隐藏[J]. 通信学报, 2022, 43(8): 219−230)

[12] Puteaux P, Ong S, Wong K, et a1. A survey of reversible data hiding in encrypted images the first 12 years[J]. Journal of Visual Communication and image Representation, 2021, 77: 103085

[13] Pucci J U, Christophe B R, Sisti J A, et al. Three-dimensional printing: Technologies, applications, and limitations in neurosurgery[J]. Biotechnology Advances, 2017, 35(5): 521−529

[14] Ni Jiahua, Ling Haonan, Zhang Shiming, et al. Three-dimensional printing of metals for biomedical applications[J]. Materials Today Bio, 2019, 3: 100024

[15] Yu Mingji, Yao Heng, Qin Chuan, et al. A comprehensive analysis method for reversible data hiding in stream-cipher-encrypted images[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2022, 32(10): 7241−7254

[16] Jiang Ruiqi, Zhou Hang, Yu Nenghai. Reversible data hiding in encrypted three-dimensional mesh models[J]. IEEE Transactions on Multimedia, 2017, 20(1): 55−67

[17] Xu Na, Tang Jin, Luo Bin, et al. Separable reversible data hiding based on integer mapping and MSB prediction for encrypted 3D mesh models[J]. Cognitive Computation, 2022, 14(3): 1172−1181

[18] Yin Zhaoxia, Xu Na, Wang Feng, et al. Separable reversible data hiding based on integer mapping and multi-MSB prediction for encrypted 3D mesh models[C]//Proc of the 4th Chinese Conf on Pattern Recognition and Computer Vision. Berlin: Springer, 2021: 336–348

[19] Lv Wanli. Cheng Lulu, Yin Zhaoxia. High-capacity reversible data hiding in encrypted 3D mesh models based on multi-MSB prediction[J]. Signal Processing, 2022, 201: 108686

[20] Tang Yun, Cheng Lulu, Lv Wanli, et al. High capacity reversible data hiding for encrypted 3D mesh models based on topology[C]//Proc of the 21st Int Workshop on Digital Watermarking. Berlin: Springer, 2022: 205−218

[21] Shah M, Zhang Weiming, Hu Honggang, et al. Homomorphic encryption-based reversible data hiding for 3D mesh models[J]. Arabian Journal for Science and Engineering, 2018, 43(12): 8145−8157

[22] Jansen van Rensburg B, Pauline P, Puech W, et al. Homomorphic two tier reversible data hiding in encrypted 3D objects[C]//Proc of the 28th IEEE Int Conf on Image Processing. Piscataway, NJ: IEEE, 2021: 3068−3072

[23] Tsai Y. Separable reversible data hiding for encrypted three-dimensional models based on spatial subdivision and space encoding[J]. IEEE Transactions on Multimedia, 2020, 23: 2286−2296

[24] Modigari N, Valarmathi M, Jani A. Watermarking techniques for three-dimensional (3D) mesh models: A survey[J]. Multimedia Systems, 2022, 28(2): 623−641

[25] Deering M. Geometry compression[C]//Proc of the 22nd Annual Conf on Computer Graphics and Interactive Techniques. New York: ACM, 1995: 13−20

[26] Yin Zhaoxia, Xiang Youzhi, Zhang Xinpeng. Reversible data hiding in encrypted images based on muhi MSB prediction and Huffman coding[J]. IEEE Transactions on Muhimedia, 2020, 22(4): 874−884

[27] Philip S, Patrick M, Michael K, et al. The Princeton shape benchmark[C]//Proc of the 6th Shape Modeling Applications. Piscataway, NJ: IEEE, 2004: 167−178

Lü Wanli, born in 1974. PhD, associate professor. Her main research interests include image processing, digital watermarking, and information security.
吕皖丽, 1974 年生. 博士, 副教授. 主要研究方向为图像处理、数值水印、信息安全.

Tang Yun, born in 1999. Master candidate. His main research interest includes reversible data hiding in 3D mesh models in encrypted domain.
唐　运, 1999 年生. 硕士研究生. 主要研究方向为密文域 3 维网格模型可逆信息隐藏.

Yin Zhaoxia, born in 1983. PhD, professor. Her main research interests include data hiding, privacy&security of multimedia and artificial intelligence.
殷赵霞, 1983 年生. 博士, 教授. 主要研究方向为信息隐藏、人工智能安全和多媒体内容保护.

Luo Bin, born in 1963. PhD, professor. His main research interests include patterns recognition and digital image processing.
罗　斌, 1963 年生. 博士, 教授. 主要研究方向为模式识别、数字图像处理.