基于面元素重排的三维网格模型数据隐藏算法

文猛，张释如
（西安科技大学，西安 710054）

摘要：目的 为了解决目前三维数据隐藏算法不能兼顾无失真和盲提取的问题，提出一种新的完全无失真的三维网格模型数据隐藏盲算法。**方法** 首先使用混沌逻辑映射选择嵌入与提取模式，保证数据的安全性。然后利用面元素重排，完全不会造成三维模型失真的性质，通过不同嵌入模式规则对三角面元素进行重排，以嵌入秘密数据。接收端则可根据相应的提取模式规则提取秘密数据。**结果** 仿真结果与分析表明，该算法不会对三维模型造成任何失真，嵌入容量为每顶点 2 比特，且能抵抗仿射变换攻击、噪声攻击和平滑攻击等。**结论** 这种三维数据隐藏盲算法无失真，容量大、安全性高、鲁棒性强，适用于三维载体不容修改的情形，如军事、医学、秘密通信和版权保护等。

关键词：三维网格模型；面元素重排；数据隐藏；盲提取；无失真
中图分类号：TP309.2 **文献标识码：**A **文章编号：**1001-3563(2022)21-0162-07
DOI：10.19554/j.cnki.1001-3563.2022.21.021

Data Hiding Algorithm for 3D Mesh Model Based on Face Elements Rearrangement

WEN Meng, *ZHANG Shi-ru*
(Xi'an University of Science and Technology, Xi'an 710054, China)

ABSTRACT: The work aims to propose a new blind algorithm for data hiding of 3D mesh models with complete distortion-free to solve the problem that the current 3D data hiding cannot take into account both distortion-free and blind extraction. First, chaotic logical mapping was used to select embedding and extracting modes to ensure the security of data. Then, the face elements rearrangement that would not cause distortion of the 3D model was adopted. The secret data was embedded by rearranging the triangular face elements through different embedding mode rules. The receiver could extract the secret data according to the corresponding extraction mode rules. Simulation results and analysis indicated that the algorithm did not cause any distortion to the 3D model, the embedding capacity was two bits per vertex, and it could resist affine transformation attacks, noise attacks and smoothing attacks. This blind 3D data hiding algorithm has no distortion, large capacity, high security and strong robustness, and is suitable for situations where the 3D carrier cannot be modified, such as military, medical, secret communication and copyright protection.

KEY WORDS: 3D mesh model; face elements rearrangement; data hiding; blind extraction; distortion-free

近年来数据隐藏在信号处理领域得到了广泛的应用，如所有权保护、指纹识别、身份认证和秘密通信等[1]。随着三维技术的飞速发展，以三维模型为载体的数据隐藏吸引了研究者的注意。传统的三维数据

收稿日期：2022–01–12
基金项目：陕西省科技厅技术创新引导专项基金（2020TG–005）
作者简介：文猛（1996—），男，硕士生，主攻三维数据隐藏。
通信作者：张释如（1965—），女，博士，教授，主要研究方向为图像处理、三维人脸建模。

隐藏技术通过改变载体模型完成嵌入，导致载体永久失真。在医学、军事和法律取证等领域，或在某些特殊情况下，由于载体的机密性或重要性，为了避免其永久损坏[2]，三维数据隐藏不仅要能嵌入与正确提取秘密数据，还要保证载体不被修改[3]。

为了解决这个问题，Honsinger 等[4]提出可逆数据隐藏的概念，即嵌入与提取方法是可逆的，隐写模型可以通过提取秘密数据之后恢复原始载体模型。基于此，Tian 等[5]提出一种差分扩展的可逆方法，Ni 等[6]提出一种直方图移位的可逆方法，这 2 种方法都是针对二维图像像素值的，不能在三维模型中使用。Jhou 等[7]和 Wu 等[8]用顶点坐标值替换像素值，分别将直方图移位和差分扩展应用到三维模型中，实现了三维可逆数据隐藏。文献[9-10]对上述工作进一步优化，提高了可逆数据隐藏的容量和鲁棒性。另一方面，Wen 等[11]提出零水印的概念，即不需要修改原始图像嵌入秘密数据。他们使用高阶累积量构造零水印，但只适用于二维图像。杜顺等[12]提出一种基于形状直径函数的算法，将零水印扩展到三维网格模型。在此基础上，文献[13-14]对算法进行了改进，提高了零水印的鲁棒性。

目前，保证三维数据隐藏中载体不被修改的手段有 2 种：可逆数据隐藏和零水印。可逆数据隐藏能够在提取出秘密数据后恢复原始载体，零水印则强调不对载体进行任何修改，而是利用载体的某些重要特征来构造水印，但是这 2 种方法都有一定的弊端，可逆数据隐藏嵌入秘密数据后会使载体失真，传输过程容易引起怀疑，安全性较低，且要恢复载体就必须先提取秘密数据，碰到顶点坐标值精度损失的情况还会提取失败，鲁棒性差；零水印用模型的某些特征生成秘密数据，用户不能自定义秘密数据大小和类型，且过于依赖知识产权（Intellectual Property Rights, IPR）信息数据库[11]，不能进行自主盲提取。针对上述问题，文中提出一种基于面元素重排的三维网格模型数据隐藏算法。根据混沌逻辑映射生成的嵌入与提取模式的对称性，联合秘密数据，可以不依赖 IPR 信息数据库独立进行盲提取；无需修改顶点坐标，而是重排面元素嵌入秘密数据，兼具高安全性和大嵌入容量，且不会对载体造成任何失真。

1　无失真数据隐藏的前提

1.1　三维网格模型

三维网格模型指物体在空间中由若干个多边形连接而成，当多边形足够多足够小时，就可以完美表示物体。基础三维网格模型由点和面（大多是三角面）2 种元素构成。按一定的顺序（记作顶点的索引）排列顶点，使用顶点索引便可构成面，最后形成网格。目前主流的三维文件格式（OFF、PLY、OBJ、VRML、X3D 等）都是基于这种数据结构[15]。如图 1 展示的是 Bunny 三维网格模型及其局部网格情况，表 1 展示了局部网格对应的数据。

表 1　局部网格文件信息
Tab.1 Local mesh file information

顶点信息				三角面信息	
顶点索引	X 轴	Y 轴	Z 轴	面索引	面元素
1	$v_{1,x}$	$v_{1,y}$	$v_{1,z}$	1	(1, 2, 3)
2	$v_{2,x}$	$v_{2,y}$	$v_{2,z}$	2	(2, 3, 4)
3	$v_{3,x}$	$v_{3,y}$	$v_{3,z}$	3	(3, 4, 5)
4	$v_{4,x}$	$v_{4,y}$	$v_{4,z}$	4	(3, 5, 6)
5	$v_{5,x}$	$v_{5,y}$	$v_{5,z}$	…	…
6	$v_{6,x}$	$v_{6,y}$	$v_{6,z}$	…	…
…	…	…	…	…	…

注：$v_{1,x}$、$v_{1,y}$、$v_{1,z}$ 分别为索引为 1 的顶点的 X、Y、Z 轴坐标值，以此类推。

1.2　三角面元素重排方法

传统三维数据隐藏算法通过修改三维模型顶点坐标嵌入秘密数据，易对模型造成永久失真，破坏模型，因此提出一种面元素重排的方法嵌入秘密数据。

网格中组成三角面的 3 个顶点索引称为面元素，参见表 1。一个三角面在空间中分两面：光照面和阴影面。依靠法线判断，法线从阴影面指向光照面，法线与面元素的关系符合右手法则，如图 2 所示，当握住拳头大拇指指向法线方向时，面元素沿着指尖的方向顺序排列。

每个三角面中的 3 个面元素有 6 种排列方式，由于三角面在空间中的光照面朝向是确定的，为了避免三维模型失真，将三角面的排列顺序减少为 3 种。在三维网格文件中，数据是以一种方式排列的，如表 1 所示，第 1 个面的面元素是 1、2、3。若用其他 2 种方式表示该面元素，三维模型虽在数据保存方面有所变化，但在视觉上完全无失真。由于只是面元素的顺序交换，所以文件大小也不会改变。文中正是利用该特点，通过重排面元素的排列顺序来嵌入数据。

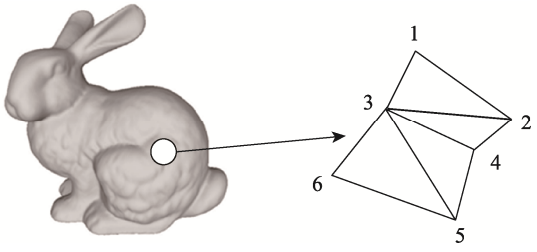
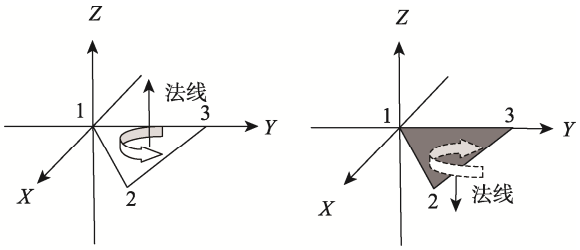


图 1　Bunny 及其局部网格
Fig.1 Bunny and its local mesh



面元素排列：1,2,3　2,3,1　3,1,2　　面元素排列：1,3,2　2,1,3　3,2,1

图 2　右手法则
Fig.2 Right hand rule

2　无失真数据隐藏算法

2.1　混沌逻辑映射生成模式序列

为了提高数据隐藏的安全性，使用如式（1）所示的混沌逻辑映射，在嵌入和提取数据之前先生成混沌序列[16]。

$$x_i = \mu x_i(1-x_i); i = 0,1,2,... \tag{1}$$

式中：x_i 为序列 x 的元素；μ 为控制参数，当 $3.569\ 945 < \mu \leqslant 4$ 时，x 为混沌序列[9]。

然后通过式（2）将混沌序列 x 中的值乘以 3，向下取整得到模式序列 x'。模式序列中元素 x_i' 的取值有 3 种可能，0、1 和 2，对应 3 种嵌入和提取模式。

$$x_i' = \lfloor x_i \times 3 \rfloor; i = 0,1,2,... \tag{2}$$

使用混沌映射具有 2 个优势。一方面，秘密数据嵌入和提取之前通过混沌序列生成模式序列，随机选择嵌入和提取模式，增加了秘密数据的安全性；另一方面，通过给定相同的控制参数 μ 和初始值 x_0，得到相同的混沌序列，以此保证嵌入和提取不会出错。

2.2　嵌入过程

设有三维载体模型 C，秘密数据序列 $I=I_i$，i=0,1,2,3,…,L_I，三角面 $F=F_i$，i=0,1,2,3,…,L_F。L_I 和 L_F 分别为 I 和 F 的长度，L_I 要小于 L_F。由于三角面的组成元素为顶点的索引，所以 3 个元素不相等且有大小顺序。嵌入过程如下。

1）加载载体模型 C。

2）读取 F_i，找出 F_i 3 个组成元素的最小值 s、中间值 m 和最大值 l。

3）根据模式序列 x' 的元素值 x_i' 确定嵌入模式。如果 x_i' 为 0，选择 S 模式——F_i 的第 1 个元素不能为 s；如果 x_i' 为 1，选择 M 模式——F_i 的第 1 个元素不能为 m；如果 x_i' 为 2，选择 L 模式——F_i 的第 1 个元素不能为 l。

4）嵌入秘密数据序列 I 中的元素 I_i。S 模式中，I_i 为 0 则 F_i 的第 1 个元素为较小值 m，为 1 则 F_i 的第 1 个元素为较大值 l；M 模式中，I_i 为 0 则 F_i 的第 1 个元素为较小值 s，为 1 则 F_i 的第 1 个元素为较大值 l；L 模式中，I_i 为 0 则 F_i 的第 1 个元素为较小值 s，为 1 则 F_i 的第 1 个元素为较大值 m。

5）$i=i+1$，如果 $i=L_\mathrm{I}$ 则嵌入结束，得到三维隐写模型 C'，否则回到步骤 2。

下面举例详细说明，假设 μ 为 4，x_0 为 0.4，那么模式序列 x'={1, 2, 0, 1,…}。设秘密数据序列 I={0, 1, 1, 0,……}，现有 4 个三角面（表 1）。如图 3 所示，第 1 个三角面元素排列为 1, 2, 3，模式序列第 1 个值为 1，选择 M 模式，面的第 1 个元素 $m\neq2$，所以剩下 2 种排列方式为 123 和 312。秘密数据序列第 1 个值为 0，所以面的第 1 个元素选择较小值 m=1，嵌入数据后的面元素排列为 123。同理可重新排列另外 3 个三角面的面元素。

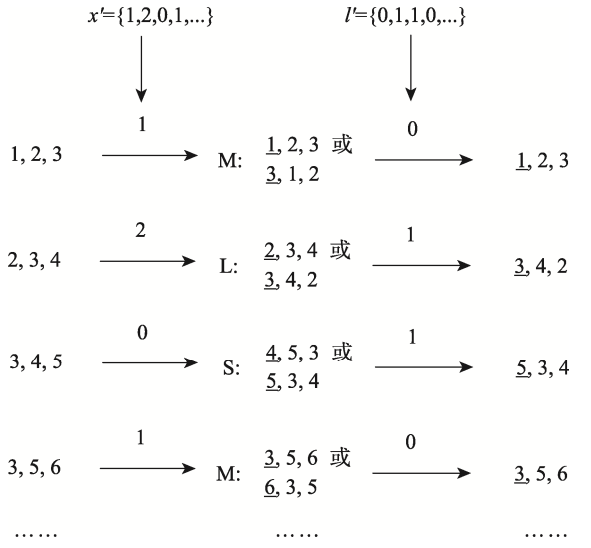


图 3　秘密数据嵌入过程
Fig.3 Process of embedding secret data

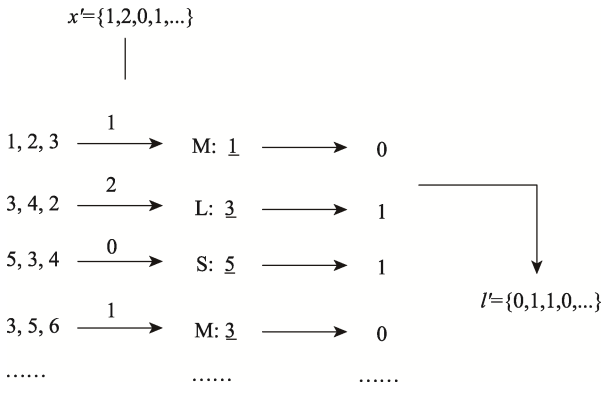


图 4　秘密数据提取过程
Fig.4 Process of extracting secret data

2.3　提取过程

提取之前，需要通过参数 μ 和初始值 x_0 得到模式序列 x'，然后选择提取模式。提取过程如以下。

1）加载隐写模型 C'。

2）读取隐写模型三角面 F_i'，找出 F_i' 3 个组成元素的最小值 s、中间值 m 和最大值 l。

3）根据模式序列 x' 的元素值 x_i' 确定提取模式。如果 x_i' 取 0，选择 S 模式；如果 x_i' 取 1，选择 M 模式，如果 x_i' 取 2，选择 L 模式。

4）提取秘密数据 I_i'。S 模式中，F_i' 的第 1 个元素为 m 则 I_i' 为 0，为 l 则 I_i' 为 1；M 模式中，F_i' 的第 1 个元素为 s 则 I_i' 为 0，为 l 则 I_i' 为 1；L 模式中，F_i' 的第 1 个元素为 s 则 I_i' 为 0，为 m 则 I_i' 为 1。

5）$i=i+1$，如果 $i=L_{\mathrm{I}}$ 则提取结束，得到秘密数据序列，否则返回步骤 2。

如图 4 所示，第 1 个面元素排列为 1, 2, 3，模式序列第 1 个值为 1，选择 M 模式，面的第 1 个元素为 1，是 s，所以第 1 个秘密数据为 0。同理可提取剩下的秘密数据。

3　实验结果与分析

实验在 Pycharm2020、Meshlab、MeshMixer 环境中进行，采用斯坦福大学 3D 模型库[17]中的 Bunny、Dragon 和 Armadillo 作为载体，见图 5。

a　Bunny　　b　Dragon　　c Armadillo

图 5　3D 模型
Fig.5 3D model

3.1　不可感知性

不可感知性的衡量标准有信噪比（signal-to-noise ratio，SNR）和归一化豪斯多夫距离（Normalised Hausdorff Distance，NHD）。SNR 是衡量隐写模型与载体模型失真程度的 1 个参数，计算公式为[18]：

$$S_{\mathrm{NR}}=10\lg\frac{\sum_{i=1}^{N_V}[(v_{i,x}-\overline{v}_x)^2+(v_{i,y}-\overline{v}_y)^2+(v_{i,z}-\overline{v}_z)^2]}{\sum_{i=1}^{N_v}[(g_{i,x}-v_{i,x})^2+(g_{i,y}-v_{i,y})^2+(g_{i,z}-v_{i,z})^2]} \tag{3}$$

式中：N_{v} 为三维模型顶点的数量；$\overline{v}_x$、$\overline{v}_y$、$\overline{v}_z$ 为载体模型的平均坐标值；$v_{i,x}$、$v_{i,y}$、$v_{i,z}$ 为载体模型的坐标值；$g_{i,x}$、$g_{i,y}$、$g_{i,z}$ 为隐写模型的坐标值。

NHD 从 2 个点集最大不匹配度反向衡量算法的不可见性，由网格模型包围盒的对角线长度除以豪斯多夫距离得到，豪斯多夫距离计算见式（4）。NHD 接近 10^{-4} 的值表示在视觉上可以接受的失真[9]。

$$H(P,Q)=\max\{h(P,Q),h(Q,P)\} \tag{4}$$

$$h(P,Q)=\max_{p\in P}\{\min_{q\in Q}\{d(p,q)\}\} \tag{5}$$

式中：P 为载体模型顶点集合，Q 为隐写模型顶点集合。$h(P,Q)$ 计算见式（5），是集合 P 中点 p 到距离此点最近的 Q 集合中点 q 之间的最大距离，$h(Q,P)$ 同理。

表 2　不可见性对比
Tab.2 Contrast of invisibility

算法	类别	模型	SNR	NHD/10^{-5}
文献[9]	可逆数据隐藏	Bunny	—	0.98
		Dragon	—	0.73
		Armadillo	—	0.71
文献[10]	可逆数据隐藏	Bunny	—	—
		Dragon	143.23	0.73
		Armadillo	161.14	0.08
文献[13]	零水印	Bunny	∞	0
		Dragon	∞	0
文献[14]	零水印	Bunny	∞	0
		Dragon	∞	0
文中算法	无失真数据隐藏	Bunny	∞	0
		Dragon	∞	0
		Armadillo	∞	0

表 2 对比了文中算法与其他算法在不同载体模型上的不可见性。可以看出，文中算法与零水印的效果一样，在 3 个载体模型上的 SNR 都为 ∞，NHD 都为 0。说明嵌入秘密数据后的隐写模型与原始载体模型完全一致，没有任何失真。

3.2　嵌入容量

文中算法通过重新排列面元素的顺序来嵌入数据，一个面可以嵌入 1bit 秘密数据。由欧拉公式（6）可知简单非空心多面体的面、边以及顶点的数量关系[19]。其中，V、E、F 分别是简单非空心多面体的顶点数、边数和面数。

$$V-E+F=2 \tag{6}$$

假设一个三角形流形网格包含足够多的边和三角形。此外，假设边界边的数量与非边界边的数量之比可以忽略，边数可以由式（7）近似得到[20]。

$$E\approx\frac{3\times F}{2} \tag{7}$$

因此，三维模型的顶点与面的关系可近似式（8）。

$$F\approx 2\times V-4 \tag{8}$$

当顶点数量足够多时，文中算法的嵌入容量近似为 2 比特每顶点（Bit Per Vertex，BPV）。

3.3 鲁棒性

文中算法通过重排面元素隐藏秘密数据，没有修改顶点，因此可以抵抗针对顶点的攻击，如噪声攻击、平滑攻击和平移、旋转、缩放等仿射变换攻击。

为了验证文中算法，采用错误比特率（Bit Error Ratio, BER）和相关系数 ρ[14]进行客观判断。BER 和 ρ 的计算分别见式（9）和式（10）。

$$B_{\mathrm{ER}}=\frac{R}{N} \tag{9}$$

$$\rho(W',W)=\frac{\sum_{i=0}^{N-1}(w_i'-\overline{w}')(w_i-\overline{w})}{\sqrt{\sum_{i=0}^{N-1}(w_i'-\overline{w}')^2\sum_{i=0}^{N-1}(w_i-\overline{w})^2}} \tag{10}$$

式中：R 为提取错误的秘密数据比特数；N 为秘密数据总比特数；W' 为提取的秘密数据；W 为原始秘密数据；$\overline{w}'$ 为 W' 的均值；$\overline{w}$ 为 W 的均值。相关值越大，2 串秘密数据之间的相似性越大。一般在相关性检验中设置一个阈值，如果 ρ 大于 0.5，说明嵌入的秘密数据已经成功提取[21]。

通过 MeshLab 软件和 python 编程对 Dragon 模型进行了多种攻击，见表 3。可以看出，文中算法对于随机噪声、拉普拉斯平滑和旋转、平移、缩放等仿射变换攻击，BER 都为 0，ρ 都为 1，说明文中算法可以完全抵抗这几种攻击。

表 3 不同攻击下的鲁棒性测试
Tab.3 Robustness tests under different attacks

攻击类别	攻击条件与参数	BER	ρ
旋转（MeshLab）	0~360°	0	1
平移（MeshLab）	−10~10	0	1
放大缩小（MeshLab）	0.1~10	0	1
随机噪声（python）	强度 0.5%~5%；生成 100 次，取平均值	0	1
拉普拉斯平滑（MeshLab）	迭代 1 ~ 10 次	0	1

表 4 满容量嵌入下不同比例剪切测试
Tab.4 Cropping tests of different proportions under full capacity embedding

剪切比例/%	BER 值/%	ρ
1	2.11	0.96
2	4.81	0.90
3	9.38	0.81
4	15.26	0.76
5	23.89	0.68

剪切攻击会减少模型的顶点和面的数目，是网格模型类算法中对嵌入的秘密数据破坏最严重的攻击[22]。剪切攻击对鲁棒性的影响和剪切比例、剪切位置和嵌入容量均有关，如果剪切部分不含秘密数据，那么提取数据的正确性不受影响。嵌入容量越大，不含密的三角面占比越小，所能完全抵抗的剪切比例越小。

为了测试对剪切含密三角面的鲁棒性，将 871 414 bit 秘密数据满容量嵌入 Dragon 模型（含有 871 414 个三角面），表 4 展示了不同剪切比例下的 BER 和 ρ。当秘密数据嵌满 Dragon 模型，剪切比例小于 5%时，文中算法的 ρ 仍大于 0.6，BER 仍小于 25%，表明文中算法对剪切攻击有一定的抵抗能力。

3.4 安全性

文中算法有 2 个安全性保障：载体无失真和混沌逻辑映射选择模式。相较于传统算法，由于载体模型与隐写模型的完全一致性而不易被人发现，增加了安全性，即使被发现，若不知道参数 μ 和初始值 x_0，也无法正确提取出秘密数据。

参数的范围 $\mu\in(3.569\,945,4]$，$x_0\in(0,1)$，此次嵌入过程取 μ=4、x_0=0.065。图 6 展示了不同 μ 时，提取过程中 BER 随 x_0 取值变化的波动范围。可以看出，当 μ 和 x_0 取值不正确时，提取后数据的 BER 值都小于 40%。实际中 μ 和 x_0 的取值有无数个，说明文中算法具有较高的安全性。

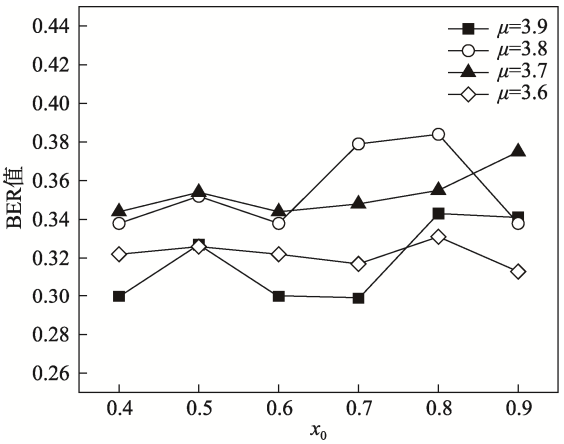


图 6 嵌入模式参数对 BER 的影响
Fig.6 Effects of embedded pattern parameters on BER

3.5　相关工作综合比较

零水印不对载体做任何修改，可逆数据隐藏提取秘密数据后可以恢复载体。文中算法属于无失真数据隐藏，只改变面元素的排列，对载体不造成任何失真。表 5 将文中算法与最新的零水印和可逆数据隐藏方法进行了比较。可以看出，文中方法兼顾了零水印的无失真和可逆数据隐藏的盲提取，嵌入容量较大，鲁棒抗性方面优于可逆数据隐藏，与零水印方法相当。

表 5　三维数据隐藏算法比较
Tab.5 Comparison of 3D data hiding

方法	失真程度	不修改或可恢复载体	容量	盲提取	鲁棒性	文献
可逆数据隐藏	轻微失真	是	1-3	是	RST	[9]
可逆数据隐藏	轻微失真	是	1.07	是	无	[10]
零水印	无失真	是	小于 1	否	RST，噪声，剪切，平滑	[13]
零水印	无失真	是	小于 1	否	RST，噪声，剪切，平滑	[14]
无失真数据隐藏	无失真	是	2	是	RST，噪声，剪切，平滑	文中

注：RST 属于仿射变换攻击。

4　结语

文中提出了一种基于面元素重排的三维网格模型无失真数据隐藏算法，具有以下优势：这种方法做到了更加便捷的盲提取；这种方法通过重排面元素顺序隐藏秘密数据，不会对载体模型造成任何失真，可以用于载体不容修改的军事和医学领域；未修改载体模型顶点数据，所以生成的隐写模型在网上进行传输时，即使遭到仿射变换攻击和顶点平滑等攻击等，也能保证提取的秘密数据完全正确；使用参数 μ 和 x_0 选择嵌入与提取模式，更具安全性，因而适用于秘密通信和版权保护等领域。

由于文中算法是空间域的，在抵抗剪切攻击方面有一定的不足，但对于较短的秘密数据可以重复嵌入到模型中，以提高对剪切攻击的抵抗性。

参考文献：

[1] JIANG Rui-qi, ZHANG Wei-ming, HOU Dong-dong, et al. Reversible Data Hiding for 3D Mesh Models with Three-Dimensional Prediction-Error Histogram Modification[J]. Multimedia Tools and Applications, 2018, 77(5): 5263-5280.

[2] ZHANG Qi-long, SONG Xiao-ying, WEN Tao, et al. Reversibility Improved Data Hiding in 3D Mesh Models Using Prediction-Error Expansion and Sorting[J]. Measurement, 2019, 135: 738-746.

[3] ZHANG Qi-long, SONG Xiao-ying, WEN Tao, et al. Reversible Data Hiding for 3D Mesh Models with Hybrid Prediction and Multilayer Strategy[J]. Multimedia Tools and Applications, 2019, 78(21): 29713-29729.

[4] HONSINGER C W, JONES P W, RABBANI M, et al. Lossless Recovery of an Original Image Containing Embedded Data: US, 6278791[P]. 2001-08-21.

[5] TIAN Jun. Reversible Data Embedding Using A Difference Expansion[J]. IEEE Transactions on Circuits & Systems for Video Technology, 2003, 13(8): 890-896.

[6] NI Zhi-cheng, SHI Yun Q, ANSARI N, et al. Reversible Data Hiding[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2006, 16(3): 354-362.

[7] JHOU C Y, PAN J S, CHOU D. Reversible Data Hiding Base on Histogram Shift for 3D Vertex[C]// International Conference on Intelligent Information Hiding & Multimedia Signal Processing, IEEE, 2007.

[8] WU Hao-tian, DUGELAY J L. Reversible Watermarking of 3D Mesh Models by Prediction-error Expansion[C]// IEEE Workshop on Multimedia Signal Processing, IEEE, 2008:797-802.

[9] GIRDHAR A, KUMAR V. A Reversible and Affine Invariant 3D Data Hiding Technique Based on Difference Shifting and Logistic Map[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(12): 4947-4961.

[10] 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.

[11] 温泉, 孙锬锋, 王树勋. 零水印的概念与应用[J]. 电子学报, 2003(2): 214-216.
WEN Quan, SUN Tan-feng, WANG Shu-xun. Concept and Application of Zero-watermark[J]. Acta Electronica Sinica, 2003,31(2): 214-216.

[12] 杜顺, 詹永照, 王新宇. 基于形状直径函数的三维网格模型零水印算法[J]. 计算机辅助设计与图形学学报, 2013, 25(5): 653-658.
DU Shun, ZHAN Yong-zhao, WANG Xin-yu. A Zero Watermarking Algorithm for 3D Mesh Models Based on Shape Diameter Function[J]. Journal of Computer-Aided Design & Computer Graphics, 2013, 25(5): 653-658.

[13] WANG Xin-yu, ZHAN Yong-zhao. A Zero-Watermarking Scheme for Three-Dimensional Mesh Models Based on Multi-Features[J]. Multimedia Tools and Applications, 2019, 78(19): 27001-27028.

[14] LEE Jung-san, LIU Chieh, CHEN Ying-chin, et al. Robust 3D Mesh Zero-watermarking Based on Spherical Coordinate and Skewness Measurement[J]. Multimedia Tools and Applications, 2021, 80(17): 25757–25772.

[15] JIANG Rui-qi, ZHOU Hang, ZHANG Wei-ming, et al. Reversible Data Hiding in Encrypted Three- Dimensional Mesh Models[J]. IEEE Transactions on Multimedia, 2018, 20(1): 55-67.

[16] ANDRECUT M. Logistic Map as a Random Number Generator[J]. International Journal of Modern Physics B, 1998, 12(9): 921-930.

[17] The Stanford 3D Scanning Repository[DB/OL]. http://graphics.stanford.edu/data/3Dscanrep/, 2021.

[18] DEERING M. Geometry Compression[C]// ACM. //Proceedings of the 22nd Annual Conference on Computer Graphics and Interactive Technology. 1995: 13-20.

[19] 刘雄伟, 彭维, 郑海波. 边界表示的拓扑与几何一致性[J]. 华侨大学学报(自然科学版), 2000(1): 51-56.
LIU Xiong-wei, PENG Wei, ZHENG Hai-bo. The Consistency in Topology and Geometry of Boundary Representation[J]. Journal of Huaqiao University (Natural Science), 2000(1): 51-56.

[20] CHENG Yu-ming, WANG C M. A High-capacity Steganographic Approach for 3D Polygonal Meshes[J]. The Visual Computer, 2006, 22(9): 845-855.

[21] NARENDRA M, VALARMATHI M L, ANBARASI L J. Watermarking Techniques for Three-dimensional (3D) Mesh Models: a Survey[J]. Multimedia Systems, 2022, 28: 623-641.

[22] ANBARASI L J, MODIGARI N. Optimization of 3D Triangular Mesh Watermarking Using ACO-Weber's Law[J]. KSII Transactions on Internet and Information Systems, 2020, 10(14): 4042-405.

责任编辑：曾钰婵