# 引入梅森旋转算法的三角网格模型部分隐写算法*

焦 然 王宜敏
(上海大学计算机工程与科学学院 上海 200444)

**摘 要**：提出一种随机选取三角网格模型的部分顶点进行隐写以提高安全性的算法。算法中利用主成分分析(PCA)算法对三角网格模型进行分析，建立模型的顶点顺序。接着，对每个模型算出一个独特值。利用伪随机发生器算法梅森旋转法输入相同的种子数会得到一样的随机数序列的特点，用模型计算得到的独特值作为种子建立随机顶点索引序列。依照这个随机索引序列对顶点进行部分。隐写算法能有效降低现有的基于机器学习的隐写分析算法的识别含秘模型的正确率。

**关键词**：信息隐藏；三维模型隐写；三维模型隐写分析；梅森旋转法
**中图分类号**：TP2 **文献标识码**：A **国家标准学科分类代码**：510.1050

## 3D trangle mesh part steganography algorithm with Mersenne twister

Jiao Ran Wang Yimin
(School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China)

**Abstract**: his paper propose a new algorithm to hide information in part vertices of a 3D triangle mesh to improve the security. The algorithm first use the PCA method to analysis the 3D model and establish a unique vertex sequence. After that, to compute a seed from the mesh for the pseudorandom number generator called Mersenne twister. With the same seed, pseudorandom number generator will produce the same pseudorandom list. Than, to pick part vertices for hiding by using the pseudorandom list to index the vertex sequence. This steganography method effective reduce the accuracy of the steganalysis algorithm.

**Keywords**: information hiding; 3D steganography; 3D steganalysis; Mersenne twister

## 0 引 言

随着移动互联网的兴起，社会的信息化程度进一步加深。近年来，不断有突发信息安全事件的新闻被报道。现在的信息安全问题已经从国家，机关单位和公司的层面变得与普通人息息相关[1]。一直以来，人们都将密码技术和信息安全划上等号，不过随着计算机技术和网络技术的出现，通信的方式已经发生了巨大的改变，信息安全的内涵也不断增加。对密码学来说，随着高性能计算技术的应用，原先认为安全的密码加密方法被超级计算机等陆续攻破；并且，加密后的信息本身就呈现出乱码的状态，很容易被攻击者识别并展开攻击进而破解。就算无法破解，信息的有效传递也难以继续[2]。如此，不同于加密方法的信息安全技术得到各界越来越多的关注。信息隐藏是其中之一。

信息隐藏技术旨在将秘密信息隐蔽在载体对象中，让非接收者无法察觉到秘密信息从而达到信息安全目的。信息隐藏有两个重要分支，一个是数字水印，一个是信息隐写。数字水印技术主要用于媒体对象的版权保护等工作，强调算法的鲁棒性，而其嵌入信息的量毕竟少，不适合用于通信。信息隐写关注信息的嵌入量，可以在一个载体中嵌入大量信息，其适合秘密信息的传递，被许多信息安全研究者所研究。一般的载体对象是在互联网中广泛应用的通信媒介，如数字图像、数字音频和数字视频等[3]。其中，以数字图像位载体的信息安全研究吸引了众多的研究者。进过信息隐藏算法处理过的对象被称为含密对象。随着计算机硬件水平的不断发展，原本只有专门的计算机设备才可以快速处理的数字三维模型也被可以用在日常的通信过程中。随着三维模型在通信中的广泛应用，以三维模型位载体对象的信息隐藏工作也进入研究者的视野。

信息隐藏具有不可感知性，鲁棒性和容量 3 个属性。不可感知性指的是含密模型不易被攻击者察觉，鲁棒性指的是在受到一定攻击的情况下信息的完整度，其和不可感

收稿日期：2017-05
* 基金项目：国家自然科学基金(61402279，U1536108)、上海自然科学基金(14ZR1415900)、上海高校青年教师培养计划项目资助

知性是信息隐藏算法安全性的主要考量。容量是算法在载体中嵌入的信息量的大小[4-5]。

## 1　三维模型上的隐写研究

### 1.1　三维模型上的隐写算法研究现状

隐写算法的研究侧重点和注重鲁棒性的数字水印算法不同,其关注容量和不可感知性多于关注算法的鲁棒性[6]。

Ohbuchi 等人[7]首先提出了将信息隐藏于三维模型中的研究方向。他们的工作提出了多个方法,探索了隐藏信息于三维模型中的各种可能的方式,如 TSQ 算法和 TSPS 算法。Cayre 等人[8]提出了一种基于量化调制的三维模型隐写算法。算法将三角形的一条边作为状态边分隔成等分小段表示 0 或者 1 两种状态,然后通过调整三角形中不属于该边的顶点的位置来隐藏信息的比特数据。Chao 等人[9]在基于量化调整的隐写算法思想基础上,通过寻找 mesh 中两点连线作为状态边,将所有顶点投影在其上来隐藏信息。并且,算法可以进行多层隐写,大大提高了算法的容量。杨飚等人[10]提出一种以三维模型中各区域的结构复杂度为标准选取复杂度高的区域的顶点用于承载秘密数据。该方法很好地保持了二面角及面法向量的统计特性。

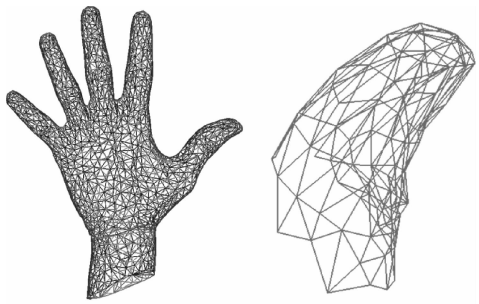
随着三维模型上的隐写算法不断发展,针对其的隐写分析算法研究也受到了重视。Yang 等人[11]提出了一种提取三维模型几何特征进行分析从而甄别含密模型的算法。该算法首先抽取模型的顶点,边和面的几何特征,然后在其上进行统计。特征的统计量组成一个 208 维的特征向量,然后用有监督机器学习算法对其训练得到分类器。Li 等人[12]在 Yang 的工作的基础上加入了曲率特征进行分析,并且讨论了不同分类方法对预测结果的优势所在,提高了检测的成功率。

### 1.2　三角网格模型和 OFF 格式

数字三维模型是一个三维对象的三维曲面的数字表达,其可以通过专门的三维建模过程得到。而对一个三维对象,其数字表达的形式多种多样,有构造型立体几何法、边界法、参数法和单元法 4 种。利用三角形来离散表达三维曲面是广泛应用的表达形式,用这种方法表达的三维模型又被称为三角网格模型,如图 1 所示。大部分的信息隐藏工作采用三角网格模型进行研究。

OFF 是用来承载网格模型的文件格式之一,它可以简洁的对三角网格模型的顶点和三角形顶点索引信息进行记录。其文件格式示例如表 1 所示,第 1 行为格式标识;第 2 行为 3 个整数,依次为顶点个数,三角面个数和边的个数;从第 3 行开始,每行用 3 个单精度浮点左边是手的三角网格模型,右边是模型手的拇指部分。

数表示一个顶点的在 $x$、$y$、$z$ 轴上的坐标,这个被称为顶点坐标表;表示完所有顶点后,开始进入三角面的顶点索引表,每一行的第一个为面所含顶点个数的数量,用整数表



(a) 手的三角网格模型　　(b) 模型手的拇指部分

图 1　三角网格模型示意图

示,然后是与顶点数量相同的 3 个顶点在顶点表位置的索引。通过这个方式,可以很容易的将数字表达的三角网格模型保存下来。OFF 模型的优点是简单明了的保存了网格的几何拓扑信息,满足了信息隐藏研究的要求。但是其缺点是扩展性较弱,对于其他的模型性质如颜色等无法保存。这里还有一些更复杂的三维模型文件存储格式,如 PLY、OBJ 等。

**表 1　OFF 文件格式示例**

| | |
|---|---|
| 1 | OFF |
| 2 | 4706 9408 14112 |
| 3 | 0.144529　−0.014328　0.381773 |
| 4 | −0.15378　−0.045707　0.361045 |
| … | … |
| 5100 | 3 2449 2463 2465 |
| 5101 | 3 471 2451 2450 |
| … | … |

基于前人工作的基础上,提出一种保证三维网格模型上的隐写算法可在具有一定容量的前提下,提高含密模型的不可感知性的隐写算法。该算法降低了含密模型在现有的隐写分析方法下被检测出来的概率,提高秘密信息的安全性。主要包括:

1)引入伪随机数发生器算法对隐写进行加密,提高安全性。引入后,算法不依赖提前预设的密钥序列,对每个模型都将

2)采用部分隐写,提高含密模型的不可感知性。根据选择的嵌入比例,对现有的隐写分析方法最多提高 8.97% 的安全性能。

## 2　算法介绍

在 1.1 节中提到的基于三维模型的隐写算法,都将密码学的方法引入到隐写算法中。其方法是依赖一个发送方和接收方都知道的密钥对三角网格模型的顶点隐写顺序加以控制。该方法中,利用伪随机数发生器梅森旋转演算法将密钥通过算法对每个模型计算出来,而不需要预先设置密钥,提高了秘密信息的安全性。

### 2.1　梅森旋转演算法简介

随机数是众多仿真模拟中非常重要的组成，但是因为各种因素，不借助专业的硬件设备，计算机不能仅仅依赖程序得到真正的随机数，只能通过程序得到尽可能“随机”的伪随机数。梅森旋转演算法是一种周期长，占用内存少，稳定性高的伪随机发生器，在计算机应用中被广泛采用[13]。

梅森旋转算法因为周期取自一个梅森素数而得名[8]。最常用的是其的衍生版本 MT19937，其周期长度为 $2^{19937}-1$[14]。伪随机发生器依赖一个伪随机种子建立随机数序列。梅森旋转算法得到种子后，利用线性反馈移位寄存器产生随机数。MT19937 采用了一个 19937 位的寄存器因此可以获得 $2^{19937}-1$ 的周期。周期决定了随机数序列可以产生的最多不重复的数的数量，越长说明算法越优秀。梅森旋转法是现状公认的最好的随机数发生器。

对一个伪随机数发生器来说，输入相同的随机种子可以得到相同的随机数列。基于此，对每个模型计算得到一个特殊值，作为伪随机发生器的种子，产生随机序列。

### 2.2　隐写算法过程

隐写算法一般分为两个过程，一个是发送端的嵌入过程，将秘密信息嵌入到载体对象中；另一个是接收端的提取过程，将含密对象的秘密信息进行提取。这两个过程在图 2 中进行了展示，其过程类似。本节将详细讲解嵌入过程。

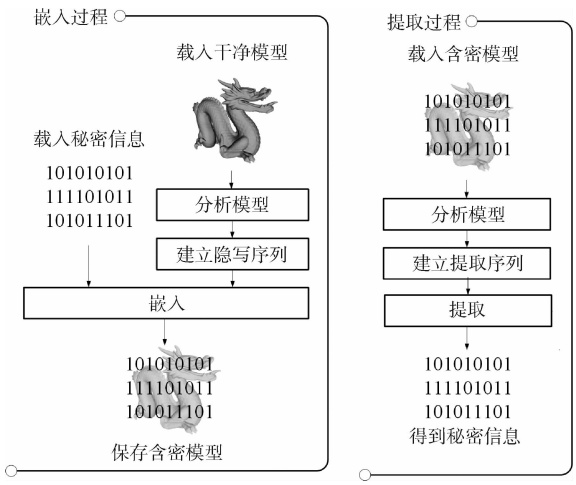



图 2　隐写算法的过程

首先，将平移模型使得模型质心 $V_g$ 与坐标原点重合。质心计算方法如式(1)所示。

$$V_g = \sum_{i=1}^{N_V} V_i \tag{1}$$

其中 $N_V$ 是三角网格模型中顶点的数量。接着，对顶点进行[−1,1]的归一化。然后用主成分分析(PCA)算法对三角网格模型进行分析，得到其的主成分轴，以及各个顶点在两个主成分轴 $P_1$ 和 $P_2$ 上的坐标。选择 $P_1$ 上坐标值最小的点为 $V_a$，坐标值最大的点为 $V_b$，$P_2$ 上坐标最大点为 $V_c$。接着，以 $\overrightarrow{V_aV_b}$ 为 $x$ 轴，$\overrightarrow{V_aV_b}\times\overrightarrow{V_aV_c}$ 为 $y$ 轴，$V_a$ 为坐标原点构建坐标系。

然后，构建顶点隐写序列。将 $V_a$ 作为第一个顶点对整个模型按照其几何拓扑结构进行广度遍历，遍历顺序按照顶点之间边的长度，距离短的先被遍历到。广度遍历后得到每个模型唯一的顶点序列 $S_v$。然后将 $V_a$、$V_b$ 和 $V_c$ 从 $S_v$ 中删去。接着，计算随机种子：

$$Seed = \lceil (V_{ax} + V_{ay} + V_{az}) \times 10^4 \rceil \tag{2}$$

其中 $V_{ax}$ 表示 $V_a$ 的 $x$ 轴坐标，其他同理。根据随机数种子对 $S_v$ 进行打乱，得到最终的顶点隐写序列 $S_R$。算法通过一个迁入率参数 $C_{ap}$ 来选择嵌入的顶点数目。

根据顶点隐写序列，逐个对顶点进行隐写。隐写时，将状态边 $V_aV_b$ 平均分为 $n_{\text{interval}}$ 份。每一小段都表示为 $R_0$ 和 $R_1$ 中的一个，并且两个状态间隔出现。顶点 $V_i$ 在 $V_aV_b$ 投影的位置所在的段的状态即可以作为其所表达的信息。具体计算方法如式(3)所示。

$$\begin{aligned} &D_i/I = b_i \cdots k_i \\ &b_i = \lceil D_i/I \rceil \end{aligned} \tag{3}$$

式中：$D_i = |V_{ix} - V_{ax}|$，$I = D_i/n_{\text{interval}}$。$b_i$ 表示点落的段序号，$k_i$ 表示点在段内的长度。隐写的时候，$b_i$ 会遇到两种状况，一种是 $b_i$ 所在的段与隐写比特一致，还有一种是不一致。针对后者，需要对点 $V_i$ 进行平移操作让 $b_i$ 改变到可以正确表达其信息的位置。这里，将每个状态段再细分为改变和不改变区域，落在改变区域的点状态与段的状态相反。段的前后 1/4 为改变区域，中间 1/2 为不改变区域。这样，只需要将 $V_i$ 平移到最近的改变区域，较移到其他段的平移量要小得多，提高了算法的不可感知性。如果只是单层的隐写，算法的隐写容量有限，因此，采用多层隐写的方法。多层隐写是在偶数层时对状态轴平移 1/2 再进行一次嵌入。在多层隐写中，针对奇数和偶数层，有不同的状态计算方法和平移方法，对 $k_i$ 如式(4)所示。

$$k_i = \begin{cases} D_i \% I, & \text{奇数层} \\ (D_i + I/2) \% I, & \text{偶数层} \end{cases} \tag{4}$$

接着对点进行平移，改变后的 $D_i$ 如式(5)所示。

$$D_i' = \begin{cases} D_i + (1/4 - k_i/2), & b_i \text{ 状态与信息相同} \\ D_i - \text{sgn}(1/4 - k_i/2\partial_i, & b_i \text{ 状态与信息不同} \end{cases} \tag{5}$$

其中 $\text{sgn}x = \begin{cases} -1, x < 0 \\ 1, x \geqslant 0 \end{cases}$，$\partial_i = \min(k_i, I - k_i)/2$。

在提取过程中，信息比特通过计算顶点的位置来获取：

$$bit_i = \begin{cases} k_i \% 2, I/4 \leqslant k_i \leqslant 3I/4 \\ 1 - k_i \% 2, k_i < I/4 \text{ 或 } k_i > 3I/4 \end{cases} \tag{6}$$

在多层隐写中，提取完一层的信息之后，为了继续对下一层信息进行提取，可以用式(7)进行一个恢复操作，将顶点位置恢复到隐写该层信息之前的状态。

$$D_i' = \begin{cases} D_i - (I/2 - k_i), I/4 \leqslant k_i \leqslant 3I/4 \\ D_i + \text{sgn}(I/2 - k_i), k_i < I/4 \text{ 或 } k_i > 3I/4 \end{cases} \tag{7}$$

## 3　实验和结果

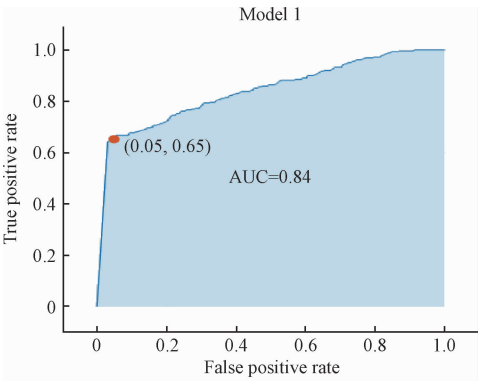
实验采用的三角网格模型数据集来自于普林斯顿大学网格模型数据库,由 380 个不同的三维模型组成。这些模型都采用 OFF 文件格式进行保存。

隐写分析方法采用 Li 的方法,提取了模型的顶点,边的二面角,面法向,顶点法向,顶点处高斯曲率和曲率半径等特征。特征维度为 52 维。

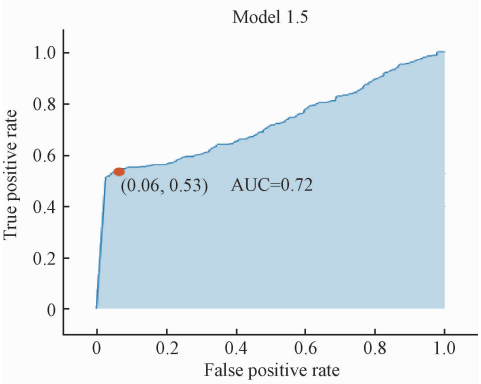
试验中,设定 $n_{\text{interval}}=10\ 000$,隐写层数 $L=10$。针对不同的迁入率 $C_{\text{ap}}$ 进行实验分析,看 $C_{\text{ap}}$ 多少对隐写分析正确率的影响。分类训练器采用的是二次判别分析方法(quadratic discriminant analysis,QDA),其对样本较小的几何有较好效果[15]。实验时,抽取了干净的载体模型的特征向量,不同 $C_{\text{ap}}$ 的含密模型的特征向量,分别组成集合进行交叉判定。交叉判定的交叉集数量 $k=5$。不同 $C_{\text{ap}}$ 下交叉判定的正确率如表 2 所示。不同迁入率下的 ROC 曲线如图 3 所示。

**表 2　不同 $C_{\text{ap}}$ 下交叉判定正确率**　　(%)

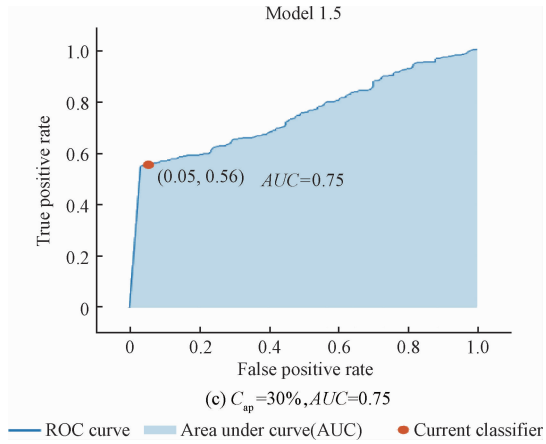
| $C_{\text{ap}}$ | 正确率 | 减少比例 |
|---|---|---|
| 100 | 80.3 | —— |
| 30 | 75.1 | 6.48 |
| 20 | 73.1 | 8.97 |




(a) $C_{\text{ap}}$=100%,$AUC$=0.84




(b) $C_{\text{ap}}$=20%,$AUC$=0.72




(c) $C_{\text{ap}}$=30%,$AUC$=0.75

图 3　不同 $C_{\text{ap}}$ 下 ROC 曲线

从表 2 中发现,当只对三角网格的部分顶点进行隐写的时候,其不可感知性得到显著提高。相比于全部隐写,$C_{\text{ap}}$ 选取 20%和 30%,其安全性提高了 8.97%和 6.48%。而根据多层隐写,其嵌入的信息量如下:

$$M=C_{\text{ap}}\times L\times N_V\times 3$$

而其每个顶点平均嵌入的信息量就有 $3C_{\text{ap}}\times L$ bit,其容量依然很高,满足信息安全的通信要求。在 $C_{\text{ap}}=20\%$,$L=10$ 的情况下,容量顶点数比可以达到 600%,嵌入信息密度达到 6 bit/v,平均每个顶点嵌入 6 bit 信息。并且,在此基础上层数可以选择更高,信息容量可以进一步提升。

## 4　结　　论

本文提出一种三维模型的隐写算法思路。算法通过 PCA 分析模型计算得到其特殊值,利用特殊值作为伪随机种子生成随机序列进行加密。利用多层隐写,在保证一定的信息容量的基础上,提出了选取三维模型上部分顶点进行嵌入的思路。算法较好的提高了含密模型在现有隐写分析方法下的安全性能。在实际应用过程中,更好的安全性会给信息的通信带来更多的保障,因此本文的思路值得探索。

## 参考文献

[1]　彭珺,高珺. 计算机网络信息安全及防护策略研究[J]. 计算机与数字工程,2011,39(1):121-124.

[2]　李文峰,杜彦辉. 密码学在网络安全中的应用[J]. 信息网络安全,2009(4):40-42.

[3]　李蛟,于莲芝,陈菊萍,等. 音频信息隐藏与伪装技术的研究与实现[J]. 仪器仪表学报,2006,27(s3):2470-2472.

[4]　陈萌. 数字水印技术及应用[J]. 国外电子测量技术,2006,25(3):60-62.

[5]　PETITCOLAS F A P, ANDERSON R J, KUHN M G. Information hiding-a survey[J]. Proceedings of

the IEEE, 1999, 87(7): 1062-1078.

[6] RANA M S, SANGWAN B S, JANGIR J S. Art of hiding: An introduction to steganography [J]. International Journal of Engineering & Computer Science, 2012, 1(1):11-12.

[7] OHBUCHI R, MASUDA H, AONO M. Watermaking three-dimensional polygonal models [C]. ACM International Conference on Multimedia, ACM, 1997:261-272.

[8] CAYRE F, MACQ B. Data hiding on 3-D triangle meshes[J]. Signal Processing IEEE Transactions on, 2003, 51(4):939-949.

[9] CHAO M W, LIN C H, YU C W, et al. A high capacity 3D steganography algorithm [J]. IEEE Transactions on Visualization & Computer Graphics, 2009, 15(2):274-284.

[10] 杨飚，吕梦琪，王宜敏，等. 基于复杂区域多层嵌入的三维模型隐写[J]. 电子测量技术，2016,39(12):164-167.

[11] YANG Y, IVRISSIMTZIS I. Mesh discriminative features for 3D steganalysis[J]. Acm Transactions on Multimedia Computing Communications & Applications, 2014, 10(3):1-13.

[12] LI Z, BORS A G. 3D mesh steganalysis using local shape features[C]. IEEE International Conference on Acoustics, Speech and Signal Processing, 2016.

[13] TIAN X, BENKRID K. Mersenne twister random number generation on FPGA, CPU and GPU[C]. Nasa/esa Conference on Adaptive Hardware and Systems,IEEE Computer Society, 2009:460-464.

[14] HARASE S. On the F 2-linear relations of Mersenne twister pseudorandom number generators [J]. Mathematics & Computers in Simulation, 2014, 100(C): 103-113.

[15] WANG J, PLATANIOTIS K N, LU J, et al. Kernel quadratic discriminant analysis for small sample size problem[J]. Pattern Recognition, 2008, 41(5):1528-1538.

## 作者简介

**焦然**，硕士研究生，主要研究方向为计算机图形学、信息隐藏等。

E-mail:jiaoran1990@t. shu. edu. cn