Journal of System Simulation

Volume 30 | Issue 7 Article 40

1-8-2019

3D Wireframe Model Encryption Based on Chaos

Zhao Geng
1.Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

Shuyun Zhu
1.Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;2.Xidian University, University, Xi'an 710071, China;

Jin Xin
1.Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

Xiaodong Li
1.Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

See next page for additional authors

3D Wireframe Model Encryption Based on Chaos

Abstract

Abstract: With the rapid growth of graphics data in the network environment, the security of graphics data has become a new challenge of network security that needs to be solved urgently. Encryption of 3D models is also urgent. *In this paper, an encryption scheme for 3D wireframe model is proposed by using chaos mapping. The method is divided into two parts: confusion and diffuse. A random invertible matrix is generated by using logical mapping to spread the points. The side is scrambled by Arnold's cat map, then the encrypted vertices and polygons are combined to form the final encrypted 3D wireframe model. The* extensive tests results show that each 3D wireframe model can be properly both encrypted and decrypted. The encryption method can also well resist violent attacks, statistical attacks and so on.

Keywords

3D wireframe, chaotic logistic map, Arnold's cat map, encryption, VFH

Authors

Zhao Geng, Shuyun Zhu, Jin Xin, Xiaodong Li, Hongbo Sun, Zhili Xu, Yin Sui, Zhaohui Tian, and Sun Nan

Recommended Citation

Zhao Geng, Zhu Shuyun, Jin Xin, Li Xiaodong, Sun Hongbo, Xu Zhili, Yin Sui, Tian Zhaohui, Sun Nan. 3D Wireframe Model Encryption Based on Chaos[J]. Journal of System Simulation, 2018, 30(7): 2753-2760.

第 30 卷第 7 期 系统仿真学报© Vol. 30 No. 7
2018 年 7 月 Journal of System Simulation Jul., 2018

基于混沌的 3D 线框模型加密方法

赵耿[1]，祝淑云[1,2]，金鑫[1*]，李晓东[1]，孙红波[1]，徐治理[1,2]，殷岁[1]，田朝辉[1,2]，孙楠[1]
（1.北京电子科技学院 北京 100070；2.西安电子科技大学 西安 710071）

摘要：随着网络环境中图形数据的急速增长，图形数据安全处理成为了亟待解决的网络安全新挑战。对 3D 模型的加密也是刻不容缓。*利用混沌映射提出了一种针对 3D 线框模型的加密方案。该方法分为两部分：混淆和扩散。利用逻辑映射生成一个随机可逆矩阵对点进行扩散，利用 Arnold's cat map 对边进行置乱，加密的顶点，多边形合成在一起，形成最终的加密 3D 线框模型。*结果表明：对每个 3D 线框模型都能正确的加解密。该加密方法也能很好的抵抗暴力攻击、统计攻击等。

关键词：3D 线框；混沌逻辑映射；Arnold's cat map；加密；Viewpoint Feature Histogram (VFH)
中图分类号：TP391 文献标识码：A 文章编号：1004-731X (2018) 07-2753-08
DOI: 10.16182/j.issn1004731x.joss.201807040

3D Wireframe Model Encryption Based on Chaos

Zhao Geng[1], *Zhu Shuyun*[1,2], *Jin Xin*[1*], *Li Xiaodong*[1], *Sun Hongbo*[1], *Xu Zhili*[1,2], *Yin Sui*[1], *Tian Zhaohui*[1,2], *Sun Nan*[1]

(1.Beijing Electronic Science and Technology Institute, University, Beijing 100070, China; 2.Xidian University, University, Xi'an 710071, China)

Abstract: With the rapid growth of graphics data in the network environment, the security of graphics data has become a new challenge of network security that needs to be solved urgently. Encryption of 3D models is also urgent. *In this paper, an encryption scheme for 3D wireframe model is proposed by using chaos mapping. The method is divided into two parts: confusion and diffuse. A random invertible matrix is generated by using logical mapping to spread the points. The side is scrambled by Arnold's cat map, then the encrypted vertices and polygons are combined to form the final encrypted 3D wireframe model. The* extensive tests results show that each 3D wireframe model can be properly both encrypted and decrypted. The encryption method can also well resist violent attacks, statistical attacks and so on.

Keywords: 3D wireframe; chaotic logistic map; Arnold's cat map; encryption; VFH

引言

如今，随着 3D 打印和 3D 建模技术的日益成熟，3D 模型逐步走进了大众的视野，对数字化的 3D 模型的分析和管理也引起了广泛的关注。计算机生成的图形的技术已经在过去十年中稳步增长。今天，虚拟对象用于许多应用中，包括游戏，模拟工具，用户界面。动画大片电影本质上依赖于合成丰富和复杂的 3D 世界并结合视觉效果，这被认为是娱乐行业的规范。我们的城市的虚拟版本是使用带激光传感器的多元相机系统构成的。因此，在不久的将来 3D 模型将普遍的应用到现实生活中。但是在 3D 模型加密方面还鲜有人涉及。

三维图像的直观和强烈的视觉冲击使它必然在未来的海量信息时代里成为主流图像形式。正是因为三维图像能够更加全面地展示物体，一旦三维

收稿日期：2016-08-15 修回日期：2017-12-19；
基金项目：国家自然科学基金(61772047)，国家档案局科技计划项目(2015-B-10)，虚拟现实技术与系统国家重点实验室开放课题(BUAA-VR-16KF-09)；
作者简介：赵耿(1964-)，男，四川广元，博士后，教授，研究方向为混沌密码，语音处理与语音识别。

图像信息泄露，其所造成的危害远超二维图像，所以研究三维图像的加密刻不容缓。

1 国内外研究现状分析

3D 模型[1]分为两种：实体模型和边界模型。实体模型表示的是物体的体积，而边界模型表示的是物体的表面。实体模型更加真实，更全面的展示信息，主要用于医疗和工程方面。然而边界模型主要应用于游戏和电影中。随着 3D 模型的应用越来越广泛，也逐步出现了安全隐患，如在不安全的通道传输以及未经授权的访问。研究 3D 模型安全的人也逐步增多。

3D 图形[2]数据有很多种，例如点云模型，线框模型以及纹理模型，不同的模型有不同的加密方法。相比点云模型，线框模型和纹理模型结构相对比较复杂。因此传统的加密方法，如数据加密标准(DES)，国际数据加密算法(IDEA)和高级加密标准(AES)等，并不适合 3D 图像加密。文献[3]提出了纹理模型加密。文献[4]中提到点云模型加密，它是利用逻辑映射对点云模型进行加密。文献[5]也是针对点云模型加密的，它提出了基于一系列随机排列和旋转，使 3D 点云模型几何变形进行加密。文献[6]是针对 3D 实体模型的进行加密的，它利用 3D 细胞自动机将 3D 实体模型进行混淆和扩散达到加密的目的。文献[7]提出了在保留 3D 对象的几何属性(例如边界框和凸包)时的基于置换的加密算法。文献[8]提出通过位屏蔽和使用 Salsa20/12 流密码的置换过程对纹理图像进行加密。混沌系统具有一些特殊的性质，如对初值和系统参数的敏感性，伪随机性等混沌特性。基于此，本文提出基于混沌的针对线框模型的加密方法。主要提出了基于混沌的 4 种加密方案。即 1.顶点由 1D 逻辑映射加密，多边形由 Arnold 混沌映射加密；2.顶点由 1D 逻辑映射加密，多边形由 1D 逻辑映射加密；3.顶点和多边形都由 2D Arnold 加密；4.顶点由 2D Arnold 加密，多边形由 1D 逻辑映射加密。

2 基本理论

随着混沌理论的不断发展，利用混沌原理实现对信息数据加密的算法如雨后春笋，越来越多。混沌理论是一种兼具了质性思考与量化分析的方法，一般用于对动态系统中，需要以连续整体的数据关系才能进行解释和预测的行为，属于一种相对复杂的系统演化理论，可以将有序状态下的系统数据转化为无序状态，从而实现对于确定性系统中随机变化问题的讨论。在实际应用中，混沌理论具有几个非常显著的特点：一是混沌系统行为本身包含了多个有序分量，经相互组合而成，但是并不能针对其中每一个有序分量进行主导；二是混沌系统的调节采用的是随机的方式，不过这些部分全部都是确定的；三是初始条件在很大程度上影响着混沌系统的发展，如果两个相同的混沌系统处于不同的初始条件，则伴随着发展的持续，混沌系统将会朝着不同的方向发展。这些算法都有一些共同的特性。混沌的特殊性质如对初始条件敏感的系统参数，长期不可预测性、伪随机性，遍历性等混沌动力学是常规密码学的有前途的替代算法。与密码学中的加密方法“混淆”和“扩散”有着本质的联系,因此混沌理论作为传统密码学的一个新分支,得到了广泛的研究和应用。混沌来自于非线性动力系统，而动力系统又描述的是任意随时间变化的过程，这个过程是确定性的、类似随机的、非周期的、具有收敛性的。固有属性直接与混淆和扩散的加密特征相联系。由于其高度的复杂性，混沌系统更可靠地设计安全图像加密方案。随着对图像加密算法各方面性能的要求持续提高，混沌系统正在朝高维、超混沌不断演进。本文介绍了混沌理论、密码学等基础知识及混沌系统在图形加密中的应用，研究了混沌图像、3D 模型加密与 DNA 计算、压缩感知理论的结合，在相关研究成果的基础上，提出对 3D 线框模型并进行了理论分析和 Matlab 仿真实验。

2.1 混沌逻辑映射

本节主要介绍这篇论文所使用方法的密码学基

https://dc-china-simulation.researchcommons.org/journal/vol30/iss7/40
DOI: 10.16182/j.issn1004731x.joss.201807040

础，本文使用的是简单高效的混沌逻辑映射[9]，此系统[10]具有极其复杂的动力学行为，在保密通信领域的应用十分广泛，Logistic 映射是一种较为典型的混沌现象，该映射结构简单，运算效率高，特别适用于系统加密。为了解决 3D 模型在保密传输过程中高效地加密和解密，本文采用混沌加密的思想，利用 Logistic 映射产生混沌序列，顺序改变 3D 模型的顶点坐标，实现 3D 模型的加密。其定义为：

$$x_{n+1} = ax_n(1-x_n)$$
$$3.569\,945\,672\cdots < a \leqslant 4, 0 \leqslant x_n \leqslant 1 \quad (1)$$

式中：$a \in [0,4]$ 被称为 Logistic 参数。研究表明，当 $x_n \in [0,4]$ 时，Logistic 映射工作处于混沌状态，也就是说，有初始条件 x_0 在 Logistic 映射作用下产生的序列是非周期的、不收敛的，而在此范围之外，生成的序列必将收敛于某一个特定的值。x_n 为初值，在 a 的取值符合 $3.569\,945\,672\cdots < a \leqslant 4$ 的条件，特别是比较靠近 4 时，迭代生成的值是出于一种伪随机分布的状态，而在其他取值时，在经过一定次数的迭代之后，生成的值将收敛到一个特定的数值，这对于我们来说是不可接受的。

2.2 2D Arnold's cat

猫映射是一种混沌系统，它将明文当做混沌系统的初始值进行迭代或演化来达到将明文进行置乱的效果。Cat 映射可以把图像中各像素点的位置进行置换[11]，使其达到加密的目的。同理，它也能对 3D 线框模型的顶点坐标索引进行置乱，即对 3D 线框模型的多边形进行加密。需要注意的是，Arnold 变换具有周期性，即多次应用 Cat 映射迭代以后，又会回到原始的状态。不同的迭代次数得到的结果也是不同的，3D 线框模型的大小不同，重复出现原始模型的迭代次数就不一样。因此可以把 3D 模型大小即顶点个数作为密钥。定义如下：

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^N * \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\mathrm{mod}\, n) \quad (2)$$

式中：$N \geq 1$，N 为迭代次数，$x_n, y_n \in \{0,1,\cdots,n-1\}$。这里 n 为密钥，x_n, y_n 为初始值。

2.3 方法简介

本文提出在 3D 安全领域基于混沌映射的线框模型加密的方法。在本文的加密方案中，首先 logistic 映射迭代生成一个随机可逆矩阵，利用这个矩阵对 3D 线框模型的顶点进行扩散[12]，生成新的坐标。然后利用 Arnold's cat map 对顶点的索引进行置乱[13]，达到边加密的效果。经大量仿真测试后，结果表明，该方案对所有 3D 线框模型都能够正确的加解密，加密后的结果类似于一个球体，完全辨别不出来原始模型，而且能够抵抗多种攻击。

3 加解密算法

描述了 3D 线框模型的加密方法。首先，本文将 3D 线框模型分解为顶点，多边形。然后这两个部分分别使用两种加密方法，即对于顶点，本文分别使用 logistic 映射和 2D Arnold cat 进行加密，对于多边形，也分别利用 logistic 映射和 2D Arnold cat 进行加密。所以本文提出 4 种加密方案进行比较，如表 1 所示。

表 1 加密算法
Tab. 1 Encryption Algorithm

方法	顶点	多边形
第 1 种	1D logistic	2D Arnold
第 2 种	1D logistic	1D logistic
第 3 种	2D Arnold	2D Arnold
第 4 种	2D Arnold	1D logistic

在 3.1 节中有详细描述。最后，加密的顶点，多边形被合成到加密的 3D 线框模型中，结果与安全性分析显示第一种加密效果最好，加密结果如图 1 所示。

3.1 3D 线框模型加密

加密过程分为两部分：顶点加密和多边形加密。利用三维随机矩阵进行顶点加密或多边形加密，利用 Arnold's cat map 进行顶点加密或多边形边加密。下面将详细介绍这 4 种算法。

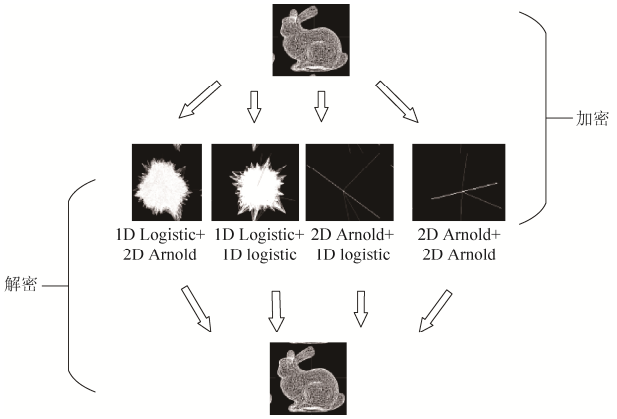

图 1 加密和解密结果示意图

Fig. 1 Encryption and decryption results

3.1.1 逻辑映射顶点加密

本节将分别介绍基于混沌逻辑映射[14]和 2D Arnold cat 的顶点加密过程。

本文利用逻辑映射迭代生成 3 *3 的可逆矩阵，利用可逆矩阵将线框模型的顶点置乱，生成一系列新的顶点，达到将 3D 模型置乱的效果。使用 1D logistic 映射的具体算法如下：

1、采用 1D 逻辑映射加密方法生成密钥；

2、将所述密钥转换成 Logistic 混沌系统的初始值和参数，生成一系列伪随机数，将所述串伪随机数变换成为一个 3×3 随机可逆矩阵；

3、将原 3D 线框模型中的顶点与所述随机可逆变换矩阵进行矩阵乘运算，得到新的位置坐标；

4、将步骤 3 中最后得到的新的点位置坐标重新写入 3D 线框模型文件，得到最终顶点加密后 3D 线框模型。

变换矩阵如式(3)：

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} m[0][0] & m[0][1] & m[0][2] \\ m[1][0] & m[1][1] & m[1][2] \\ m[2][0] & m[2][1] & m[2][2] \end{pmatrix} \times \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad (3)$$

如图 2 所示加密流程图，通过逻辑映射迭代生成一系列的伪随机序列流，组成三维随机可逆矩阵，通过矩阵乘生成新的顶点坐标，将原始模型置乱。

3.1.2 2D Arnold 顶点加密

线框模型的顶点坐标是三维向量表示(*x*,*y*,*z*)，本文使用方程式(2)定义的 2D Arnold 产生大小为 2M 的随机向量，利用排序算法对随机向量进行排序，并保留索引，按照索引对应关系，对顶点坐标进行排序，得到排序后的向量，也就是新坐标(*x*, *y*, *z*)。

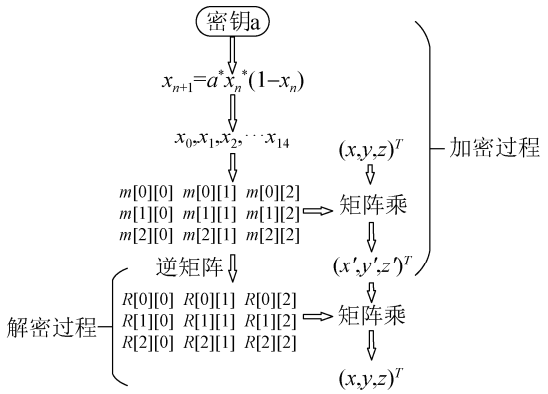

图 2 顶点加密和解密流程图

Fig. 2 Flow chart of vertex encryption and decryption

3.1.3 2D Arnold 多边形加密

3D 纹理模型中的多边形(以三角形为例)采用三元组列表的形式：$P=\{(A_1,B_1,C_1),\cdots,(A_i,B_i,C_i)\}$ 其中 (A_i,B_i,C_i) 以顶点索引的形式表示三角形的 3 个顶点。利用 2D Arnold cat 产生的密钥进行排序，然后按照对应顺序对顶点进行排序，得到新多边形。映射将顶点索引进行置乱，以达到对边加密的目的。首先我们 3M 大小的矩阵变成 2N 大小，利用方程(2)进行矩阵乘，得到新的顶点坐标索引 P^j，$P^j=\{(A_1^j,B_1^j,C_1^j),\cdots,(A_i^j,B_i^j,C_i^j)\}$，其中 (A_i^j,B_i^j,C_i^j) 是加密 3D 模型的新三角形。

3.1.4 逻辑映射多边形加密

与 2D Arnold 加密多边形类似，本文使用方程式(1)定义的 1D 逻辑映射产生大小为 3M 的随机向量，利用排序算法对随机向量进行排序，并保留索引，按照索引对应关系，对顶点索引进行排序，得到排序后的向量，新顺序的向量表示为 $\boldsymbol{P^j}$，

$\boldsymbol{P^j}=\{(A_1^j,B_1^j,C_1^j),\cdots,(A_i^j,B_i^j,C_i^j)\}$，

式中：(A_i^j,B_i^j,C_i^j) 是加密 3D 模型的新三角形。

如图 1 所示。从图 1 中我们可以看出，4 种加密算法都能加密原始 3D 线框模型，相对来说，第 1 种和第 2 种加密方法的加密模型更加的不规则，

DOI: 10.16182/j.issn1004731x.joss.201807040

而第 3 种和第 4 种加密方法效果差强人意，没有第 1 种和第 2 种方法加密效果显著。

3.2 解密过程

3.2.1 顶点解密

在图 2 的解密流程图中，利用混沌逻辑映射生成随机可逆矩阵，把原始点随机变换到其他地方。解密过程就是加密过程的逆过程，利用和加密时相同的初始值和参数以及逆矩阵可以还原出原始的顶点。具体算法如下：

1、根据密钥，迭代 Logistic 混沌映射得到伪随机数序列；

2、根据 logistic 混沌映射出的序列重新构造随机可逆变换矩阵；

3、求出随机可逆变换矩阵的逆矩阵，与加密后点坐标的矩阵相乘，得到的即为原始 3D 顶点。如图 2 所示解密过程。

利用 2D Arnold 加密的解密算法就是排序算法的逆过程,利用 2D Arnold 的逆运算生成 3M 的随机向量，利用排序算法对随机向量进行排序，并保留索引，按照索引对应关系，对顶点索引进行排序，得到排序后的向量，新顺序的向量就是原始 3D 模型的顶点。

3.2.2 边解密

该过程就是边加密的逆过程，对于 2D Arnold 解密算法就是利用 C 的逆矩阵与顶点坐标索引进行矩阵乘还原出原始多边形。对一个置乱 N 次的线框模型，只要恢复后的模型的置乱次数 k 满足 $0\leqslant k\leqslant N$，线框模型的恢复都可以通过对加密模型作 N-k 次 Arnold 反变换得到，显然当 k=0 时，反变换后的模型的多边形就是原始线框模型的多边形。即：

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} == C^{-N} * \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} (\mathrm{mod}\, n) \tag{4}$$

利用 1D logistic 进行多边形加密的解密算法就是排序算法的逆过程，利用 logistic 映射生成 3M 随机向量，然后对加密后的坐标进行坐标还原。如图 1 解密结果所示。

4 仿真结果

本文使用各种 3D 线框模型来验证我们提出的方法。本文分别测试了表 1 中的 4 种方法。使用正确的密钥将所有加密的结果解密为原始的纯 3D 模型。经过大量线框模型来测试 4 种加密算法，都能正确的加解密，如图 3 所示，我们可以看出，加密效果有显著差异。相对来说，使用 1D logistic 对 3D 模型的顶点加密效果比 2D Arnold 效果好。

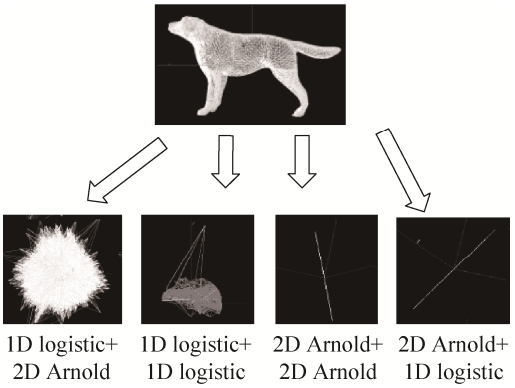

图 3 仿真结果
Fig. 3 Simulation results

5 安全性分析

在本节中，我们验证了加密方法的密钥敏感性、鲁棒性、以及抗统计攻击等。此外，我们还对各种方法的加密效果以及安全性进行了对比。

5.1 抗暴力攻击

5.1.1 密钥空间

加密方案的密钥空间应该足够大来抵抗暴力攻击，否则就会在有限的时间内枚举出正确密钥，这样的加密方案很容易就会被破解，无疑是不安全的。如果对模型的每一个点用不同的密钥来加密，则：

$3.569\,945\,672\cdots < a_0, a_1, \cdots, a_N \leqslant 4$，

$0 \leqslant x_0^0, x_0^1, \cdots, x_0^N \leqslant 1$

这里，N 为线框模型顶点数量，64 位的 double 型数据的精确度为 10~15。所以该加密方案的密钥

空间大约为 $(1\,015)2N=1\,030N\approx 275N$ 。如果 $N\geqslant 3$ 会比 AES 的最大密钥空间大很多。而且，对于 2D Arnold cat 映射， $N\geqslant 1$， p， q 为整数，显然，密钥空间也是相当大的。所以，该加密方法的密钥空间足够大，足够抵御暴力攻击。

5.1.2 密钥敏感性

混沌系统对系统参数和初值很敏感，稍微有点不同加密结果就解密不出来，该文使用 1D logistic 和 2D Arnold 对初始值和系统参数变化都很敏感，该文用初始值和系统参数作为密钥，稍微改变密钥就能使解密后的结果和原始的 3D 模型有很大的不同。为了测试密钥敏感性，对于每个例子，本文稍微改变一下密钥，看一下解密结果。令：

$$a_i=a_i+0.000\,000\,1,\ i=0,1,\cdots,n$$

结果显示，使用稍微改变过的密钥的解密结果是不可识别的并且完全不同于原始的 3D 模型。这表明本文提出的 4 种加密方法都有很好的密钥敏感性，足以抵抗暴力攻击。如图 4 所示。

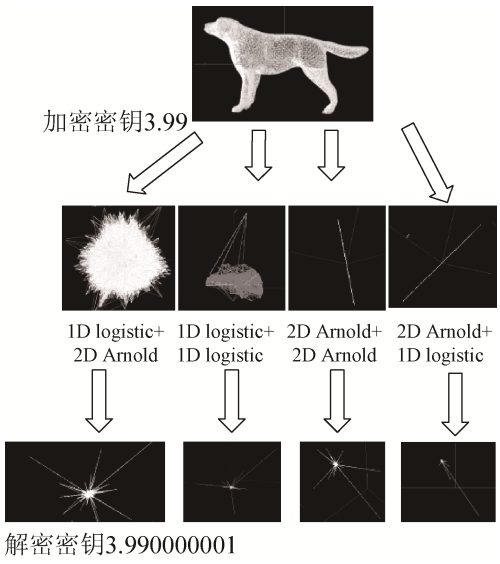

图 4 密钥敏感性
Fig. 4 Key sensitivity

5.2 抗统计攻击

该加密方案的根本就是对顶点进行的处理，包括点坐标的变换以及索引的置乱。所以，本文可直接利用视点特征直方图(View Feature Histogram，VFH)描述子来描述顶点的基本特征[15]，它是一种新的特征表示形式，应用在点云聚类识别和六自由度位姿估计问题。VFH 源于 FPFH，本文利用 FPFH 强大的识别力，但是为了使构造的特征保持缩放不变性的性质同时，还要区分不同的位姿，计算时需要考虑加入视点变量，通过统计视点方向与每个法线之间角度的直方图来计算视点相关的特征分量。默认的 VFH 的实现使用 45 个子区间进行统计，而对于视点分量要使用 128 个子区间进行统计，这样 VFH 就由一共 308 个浮点数组成阵列。利用 VFH 来评估 3D 线框模型加密即可。

如图 5 所示，从图中可以看出，3D 线框模型在加密前后的 VFH 是完全不同的。原始 3D 模型的 VFH 波动较大，不平滑，而加密后的 3D 模型的 VFH 相对比较平滑，加密效果显著，而且使用 logistic 顶点加密方法比 2D Arnold 顶点加密方法效果好。所以第一种加密方法和第二种加密方法都能够很好的抵抗统计攻击。而且,实验证明顶点数目越多，加密效果越好。

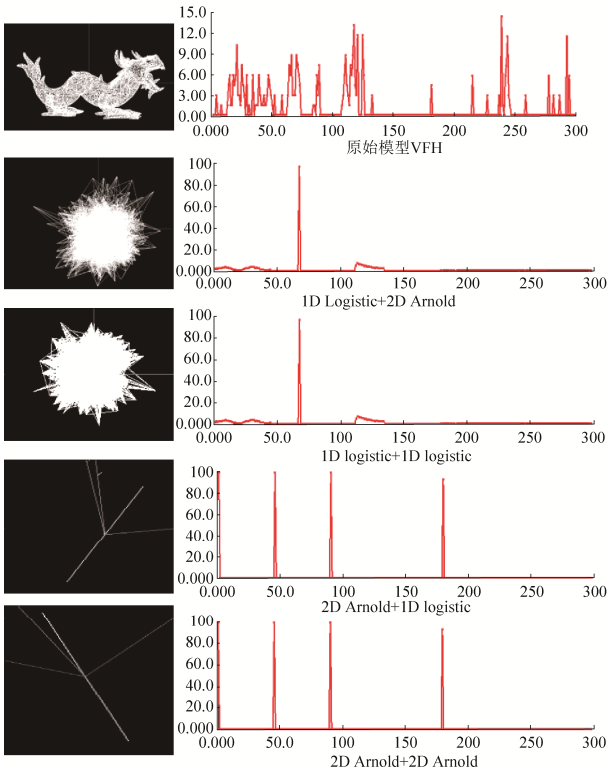

图 5 3D 模型 VFH 评估
Fig. 5 3D model VFH assessments

6 时间复杂度

基于第五节对抗统计攻击性能的分析，我们可以看出使用 1D logistic 加密顶点比使用 2D Arnold 加密顶点效果好，所以本文排除第三种和第四种加密方案，本节对第一种和第二种加密方案的加解密速度进行比较，如图 6 所示，显示的是两种方案的加解密时间[16]，从图中可以看出，利用第一种方案加密 3D 模型的加解密时间远远优于第二种方案，所以本文选取第一种方案进行 3D 模型加密。

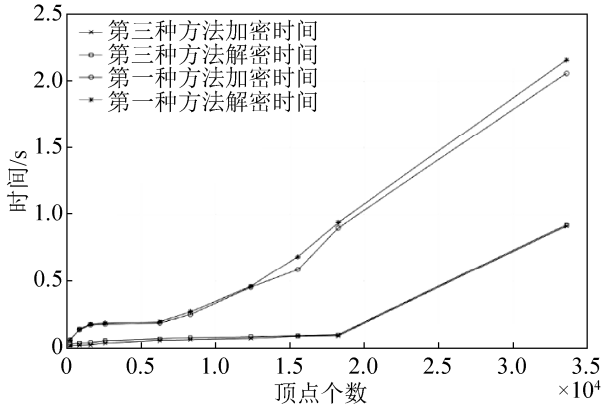

图 6 加解密时间

Fig. 6 Encryption and Decryption time

本文加解密结果是基于 AMD A10 PRO-7800B R7，12 Compute Cores @ 3.5GHz 4GB 内存硬件环境以及 matlab2015a 软件环境计算出来的。加解密时间是随着模型的复杂度改变的，模型越复杂，时间越长。

7 结论

混沌系统的极端敏感性可以有效提高加密方案的复杂度，有效增强纹理的混淆和扩散能力。由于线框模型数据量大，密钥敏感性相应的增大，能够有效抵抗选择明文攻击。原始 3D 线框模型的微小改变可以导致加密效果全面改变。以前的 3D 模型加密主要集中在点云模型和实体模型上，在这篇论文中，本文提出了四种加密方案，这四种线框模型加密方案都可以抵抗暴力攻击，统计攻击，分析证明第一种加密方案相对较好。并且该加密方法很容易通过软件实现，该加密方法可广泛应用推广到线框模型安全存储和传输加密中。所以本文提出了基于 1D logistic 映射和 2D Arnold 的线框模型加密方案。这四种方案都是在 matlab2015a 以及 QT5.4 环境下实现的。第一种方案是利用混沌逻辑映射生成一个三维随机矩阵，把原始坐标变成一个新的坐标，然后，利用 Arnold's cat map 将顶点置乱从而达到边加密。然后将加密后的顶点与多边形合成加密后的 3D 模型。本文利用 VFH 描述子对加密结果进行评估，结果表明，该方案不仅能正确的加解密 3D 线框模型，而且具有足够大的密钥空间和足够高的安全性，不仅能抵抗暴力攻击，也足以抵抗统计攻击。

未来将继续探索线框加密的算法和 3D 纹理模型的加密算法以及实现。

参考文献:

[1] Lee S H, Kwon K R, Hwang W J, et al. Key-dependent 3D model hashing for authentication using heat kernel signature[J]. Digital Signal Processing(S1051-2004), 2013, 23(5):1505-1522.

[2] 赵维，茅坪，沈凡宇. 下一代三维图形引擎发展趋势研究[J]. 系统仿真学报, 2017, 29(12): 2935-2944.
Zhao Wei, Mao Ping, Shen Fanyu. Research on the Development Trend of Next Generation 3D Graphics Engine [J]. Journal of System Simulation, 2017, 29(12): 2935-2944.

[3] Jin X, Zhu S, Xiao C, et al. 3D textured model encryption via 3D Lu chaotic mapping[J]. Science China Information Sciences, December.CCF-B, SCIE. 2017, 60(12): 122107.

[4] 吴肇星，金鑫，宋承根，等. 基于随机可逆矩阵的 3D 点云模型加密[J]. 系统仿真学报，2016, 28(10): 2455-2459.
Wu Zhaoxing, Jin Xin, Song Chenggen, et al. Random Reversible Matrix based Point Cloud Encryption [J]. Journal of System Simulation, 2016, 28(10): 2455-2459.

[5] Jolfaei A, Wu X W, Muthukkumarasamy V. A 3D Object Encryption Scheme Which Maintains Dimensional and Spatial Stability[J]. IEEE Transactions on Information Forensics & Security(S1556-6013), 2015, 10(2): 409-422.

[6] Rey A M D. A Method to Encrypt, \(3\), D Solid Objects

Based on Three-Dimensional Cellular Automata[M]// Hybrid Artificial Intelligent Systems. Springer International Publishing, 2015:427-438.

[7] Éluard M, Maetz Y, Doërr G. Geometry-preserving Encryption for 3D Meshes[C]//Compression Et Représentation Des Signaux Audiovisuels. 2013.

[8] Jolfaei A, Wu X W, Muthukkumarasamy V. A Secure Lightweight Texture Encryption Scheme[M]// Image and Video Technology-PSIVT 2015 Workshops. Springer International Publishing, 2015.

[9] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map[J]. Chaos Soliton Fract, 2005, 26(1): 117-129.

[10] 江东, 孔德善, 刘绪坤, 等. 磁悬浮系统仿真及混沌特性研究[J]. 系统仿真学报, 2017, 29(3): 572-580.
Jiang Dong, Kong Deshan, Liu Xukun, et al. Study on maglev system simulation and chaos characteristics [J]. Journal of System Simulation, 2017, 29(3): 572-580.

[11] Jin X, Guo K, Song C, et al. Private Video Foreground Extraction Through Chaotic Mapping Based Encryption in the Cloud[C]// International Conference on Multimedia Modeling. Springer, Cham, 2016:562-573.

[12] Wang Y, Ren G, Jiang J, et al. Image Encryption Method Based on Chaotic Map[C]// IEEE Conference on Industrial Electronics and Applications. IEEE, 2007:2558-2560.

[13] Jiang R, Zhou H, Zhang W, et al. Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models[J]. IEEE Transactions on Multimedia, 2017, (99): 1.

[14] Jin X, Tian Y, Song C, et al. An invertible and anti-chosen plaintext attack image encryption method based on DNA encoding and chaotic mapping[C]// Chinese Automation Congress. IEEE, 2016:1159-1164.

[15] Li Y, Li X, Jin X, et al. An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map[J]. Applications and Techniques in Information Security, Springer, Berlin, Heidelberg, 2015: 3-13

[16] Jin X, Chen Y, Ge S, et al. Color Image Encryption in CIE L*a*b* Space[C]// International Conference on Applications and Techniques in Information Security. Springer, Berlin, Heidelberg, 2015: 74-85.

[17] Rusu R B, Blodow N, Beetz M. Fast point feature histograms (FPFH) for 3D registration[C]// IEEE International Conference on Robotics and Automation. IEEE, 2009:3212-3217.

[18] Jin X, Yin S, Li X, et al. Color image encryption in YCbCr space[C]// International Conference on Wireless Communications & Signal Processing. IEEE, 2016: 1-5.

《系统仿真学报》荣获“2017 中国国际影响力优秀学术期刊”证书

由中国学术期刊（光盘版）电子杂志社与清华大学图书馆联合成立的中国学术文献国际评价研究中心，发布了 2017 版《中国学术期刊国际引证年报》，《系统仿真学报》荣获“2017 中国国际影响力优秀学术期刊”。

《年报》（2017 版）采用的统计源期刊为 20192 种，涵盖 WoS 收录的 SCI 期刊 8874 种、SSCI 和 A&HCI 期刊 4645 种，ESCI 期刊 5578 种；增补期刊 1762 种。参照中外文学术期刊总被引频次、影响因子、半衰期等各项国际引证指标，计算期刊影响力指数(CI)，对国内 6210 种学术期刊排序，遴选了人文社科、自然科学与工程技术两个类别的 TOP10%为国际影响力品牌学术期刊。TOP5%以内的期刊为“最具国际影响力学术期刊”、TOP5-10%之间的为“国际影响力优秀学术期刊”。

DOI: 10.16182/j.issn1004731x.joss.201807040