Journal of System Simulation

Volume 28 | Issue 10 Article 23

8-13-2020

Random Reversible Matrix based Point Cloud Encryption

Zhaoxing Wu
Beijing Electronic Science and Technology Institute, Beijing 100070, China;

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

Chenggen Song
Beijing Electronic Science and Technology Institute, Beijing 100070, China;

Chunwei Zhang
Beijing Electronic Science and Technology Institute, Beijing 100070, China;

See next page for additional authors

Random Reversible Matrix based Point Cloud Encryption

Abstract

Abstract: Paying less attention to the privacy protection in the 3D model, an encryption scheme based on chaotic map of 3D point cloud model was proposed, which realized the encryption of 3D point cloud, that used *chaotic maps* to generate a 3×3 *random reversible matrix* and a 3×1 *translation vector*, used the above random reversible matrix and the translation vector can transform each point of the point cloud to a homogeneous coordinate. After a lot of tests on different 3D point cloud models were carried out, the test results show that each point cloud model can be correctly encrypted and encrypted. In addition, the results of encryption was evaluated by the *view feature histogram* (VFH). Evaluation results show talmost no recognition of the encrypted 3D point cloud.

Keywords

3D point clouds, encryption, chaotic mapping, point feature histogram, view feature histogram

Authors

Zhaoxing Wu, Jin Xin, Chenggen Song, Chunwei Zhang, and Xiaodong Li

Recommended Citation

Wu Zhaoxing, Jin Xin, Song Chenggen, Zhang Chunwei, Li Xiaodong. Random Reversible Matrix based Point Cloud Encryption[J]. Journal of System Simulation, 2016, 28(10): 2455-2459.

第 28 卷第 10 期 系统仿真学报© Vol. 28 No. 10
2016 年 10 月 Journal of System Simulation Oct., 2016

基于随机可逆矩阵的 3D 点云模型加密

吴肇星，金鑫，宋承根，张春伟，李晓东
（北京电子科技学院，北京 100070）

摘要：针对 3D 模型中存在的隐私保护问题，提出一种基于混沌映射的 3D 点云模型加密方案。利用*混沌映射*生成一个 3×3 *随机可逆矩阵*和一个 3×1 *平移向量*，利用以上的随机可逆矩阵和平移向量可以将点云中的每一个点变换到一个齐次坐标。用以上加密方案对不同的 3D 点云模型进行大量测试的结果显示，每个点云模型都能正确地加解密。通过运用*视点特征直方图*对加密的结果进行评估，结果表明：该方案能够生成难以辨认的密文 3D 点云。

关键词：3D 点云；加密；混沌映射；点特征直方图；视点特征直方图
中图分类号：TP391 文献标识码：A 文章编号：1004-731X (2016) 10-2455-05

Random Reversible Matrix based Point Cloud Encryption

Wu Zhaoxing, *Jin Xin*, *Song Chenggen*, *Zhang Chunwei*, *Li Xiaodong*

(Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: Paying less attention to the privacy protection in the 3D model, an encryption scheme based on chaotic map of 3D point cloud model was proposed, which realized the encryption of 3D point cloud, that used *chaotic maps* to generate a 3×3 *random reversible matrix* and a 3×1 *translation vector*, used the above random reversible matrix and the translation vector can transform each point of the point cloud to a homogeneous coordinate. After a lot of tests on different 3D point cloud models were carried out, the test results show that each point cloud model can be correctly encrypted and encrypted. In addition, the results of encryption was evaluated by the *view feature histogram* (VFH). Evaluation results show talmost no recognition of the encrypted 3D point cloud.

Keywords: 3D point clouds; encryption; chaotic mapping; point feature histogram; view feature histogram

引言

如今，许多人通过社交软件和云存储传递着大量的视觉信息，包括图片、视频和 3D 模型等。随着三维建模和三维打印技术的发展，3D 模型的数量也在日益增长。智能手机上的一些应用（如 Autodesk 123D Catch）让用户从不同的角度拍摄同一个物体并把这些照片上传到 Autodesk 云服务器上。然后 123D 云服务器返回给用户一个构建好的 3D 模型。人们也会用谷歌 Sketchup 这样的桌面软件很容易地对 3D 模型进行编辑。3D 模型正逐步走进我们的日常生活中。在工业领域，虚拟现实技术是现在一个很热门的话题。这虚拟世界需要大量的三维模型来构建。政府正在用激光扫描仪和多视点相机将整个城市扫描成虚拟城市。

收稿日期：2016-05-30 修回日期：2016-07-11；
基金项目：国家自然科学基金(61170037, 61402021)；中央高校基本科研业务费(2015XSYJ25)；国家档案局科技计划(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：吴肇星(1995-)，男，山东淄博，本科生，研究方向为可视媒体加密。

1 简介

1.1 前期工作

混沌的一些的特殊性质[1-2]，比如对初始条件和系统参数的敏感性、伪随机性和各态历经性等使混沌力学有可能替代传统的加密算法。由于混沌系统的高复杂性，混沌系统可以用来设计安全可靠的图像和视频加密方案[3-9]。

然而，很少有人会考虑到 3D 图像的加密的问题。3D 模型有两种类型：三维实体模型和三维壳(边界)模型。实体模型用体积表示的物体，而壳模型是用面来表示物体。在文献[10]中，雷伊已经给出了三维实体模型的加密，但 3D 壳模型的加密却没有在文献中出现。

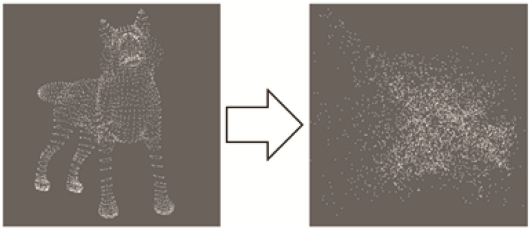
因此为了实现高水平的安全性、完整性和机密性，防止有敏感信息的 3D 模型在不安全通道中存储或传输时有未经授权的访问，需要研究 3D 模型加密技术。3D 图像数据有很多种，比如 3D 点云模型、3D 线框模型和 3D 纹理模型。不同的 3D 数据类型应该对应不同的加密算法。几乎没有人在做三维点云模型的加密工作。

与文本加密技术不同,可视化数据具有一些特殊的特征，如大数据容量和像素或点之间的高相关性。传统的加密算法，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)等等，不适合视觉数据加密。不同的图像或视频，3D 内容包含点，在 3D 空间网格和纹理。传统的图像或视频加密方法不适合 3D 内容[11]。因此，本文提出了新的 3D 内容加密方法。

1.2 方法简介

本文首次提出了在 3D 安全领域的基于混沌映射的3D 点云加密，图 1 显示了 3D 点云模型的加密。

在本文的方案中，利用混沌映射生成一个 3×3 随机可逆矩阵和一个 3×1 平移向量，利用以上的随机可逆矩阵和平移向量可以将点云中的每一个点变换到一个齐次坐标。本文用以上加密方案对不同的 3D 点云模型进行了大量测试后，测试结果显示每个点云模型都能正确地加解密。另外，本文用视点特征直方图（VFH）对加密的结果进行评估。评估结果显示，几乎辨认不出加密后的 3D 点云。



原始 3D 模型　　加密后 3D 模型

图 1　3D 点云模型加密

2 密码学基础

在这一节中简介本文中用到的密码学基础，本文使用了简单高效的逻辑混沌映射，定义如下：

$$x_{n+1}=\mu x_n\left(1-x_n\right)$$
$$3.569945672\cdots<\mu\leqslant 4 \quad (1)$$
$$0\leqslant x_n\leqslant 1$$
$$n=0,1,2\cdots$$

当参数 μ 和初始值 x_0 服从公式(1)，混沌映射 x_n 的输出会呈现混沌状态，并适合产生随机序列。

3 基于逻辑映射的点云加密

本文设计了一种基于逻辑映射的点云加密。在这种方案中，利用混沌映射生成一个 3×3 随机可逆矩阵和一个 3×1 平移向量，利用以上的随机可逆矩阵和平移向量可以将点云中的每一个点变换到一个齐次坐标。在这一节解释这种加密方案的细节。

在 3D 点云空间内一个点通过旋转和平移操作可以变换到另外一个地方。我们设计了一个 4×4 随机可逆变换矩阵，此矩阵由一个 3×3 旋转矩阵 R 和一个 3×1 平移矩阵 $T=(t_x, t_y, t_z)$。一个点可以用齐次坐标表示为：$p=(x, y, z, 1)$T。

变换矩阵如公式(2)

$$\begin{pmatrix} x' \\ y' \\ z' \\ 1 \end{pmatrix} = \begin{bmatrix} R[0,0] & R[0,1] & R[0,2] & t_x \\ R[1,0] & R[1,1] & R[1,2] & t_y \\ R[2,0] & R[2,1] & R[2,2] & t_z \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

本文使用逻辑映射产生随机可逆矩阵 $\boldsymbol{T}$，如图 2 所示。所有 3D 点随机变换到其他位置。在解密阶段，我们用逆矩阵 $\boldsymbol{T}$-1 把每个点还原到原始位置，获得原始点云，如图 3 所示。

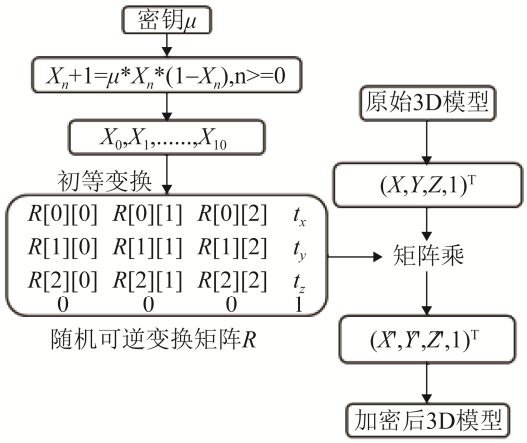


图 2 加密过程

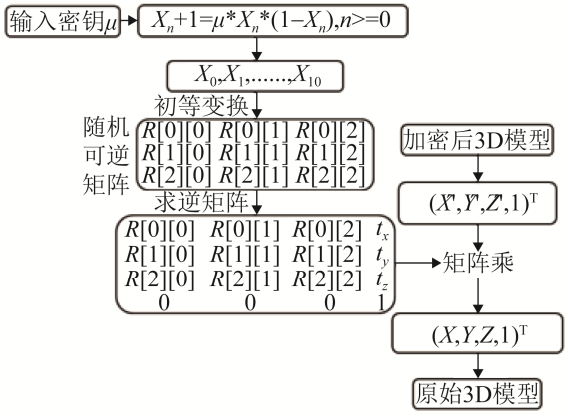
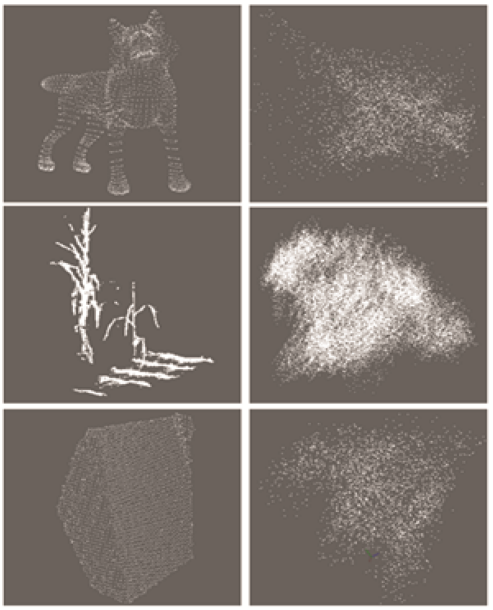


图 3 解密过程

4 仿真结果

我们使用大量点云模型来测试我们的方案，如图 4 所示，不同内容的 3D 点云能正确的加密，并且使用正确的密钥能将加密结果还原成原始 3D 点云模型，可以看出加密效果很显著。



原始 3D 模型 加密后 3D 模型

图 4 加密结果

5 安全性分析

5.1 抵抗暴力攻击

密钥空间 加密方案的密钥空间应该足够大以抵抗暴力攻击，否则可能在有限的时间内枚举到正确密钥，这样的加密方案无疑是脆弱的。

假设给每个点一个密钥用来逻辑映射：

$$3.569945672\cdots < \mu_0, \mu_1, \cdots, \mu_N \leqslant 4$$

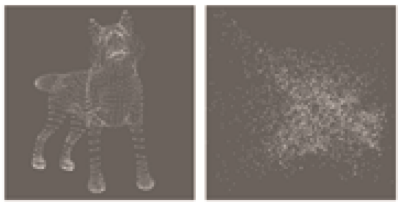
$$0 \leqslant x_0^0, x_0^1, \ldots x_0^N \leqslant 1$$

这里，N 是点云中点的数量，64 位 double 型数据的精准度为 10~15。因此本方案的密钥空间大约为(1 015)2 N=1 030 N≈275 N。如果 N>3，其密钥空间会比 AES 的最大密钥空间大很多。因此本方案的密钥空间足够抵御暴力攻击。

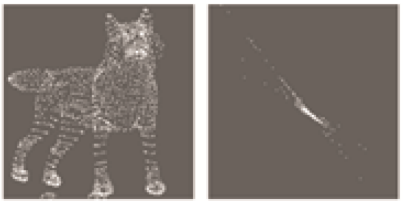
密钥敏感性 混沌系统对系统参数和初始值尤其敏感。一点点的不同可能会导致解密失败。为了测设我们解密方案的密钥敏感度，我们这样变换密钥：

$$\mu_i = \mu_i + 0.000\,000\,1, i = 1, 2, \cdots, N$$

本文利用改变过的密钥去解密加密后的模型，结果如图 5 所示。结果显示，本方案对密钥极其敏感，能够抵御穷举攻击。



原始 3D 模型　　加密后模型
密钥 3.89



解密后模型　　解密后模型
正确密钥 3.89　　错误密钥 3.890 001

图 5　密钥敏感度

5.2 抗统计攻击

点特征直方图(Point Feature Histogram, PFH)是饱含信息的姿态无关局部特征，它能代表点的基本表面特征。而视点特征直方图（View Feature Histogram, VFH）描述子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。

PFH 描述子与 VFH 描述子的主要区别在于，对于一个点云数据集，只需一个 VFH 描述子即可，而 PFH 数据的入口数量会和点云中点的数量相同，因此我们采用 VFH 来评估 3D 点云模型加密。图 6 为测评结果，可以看出足以抵抗统计攻击。

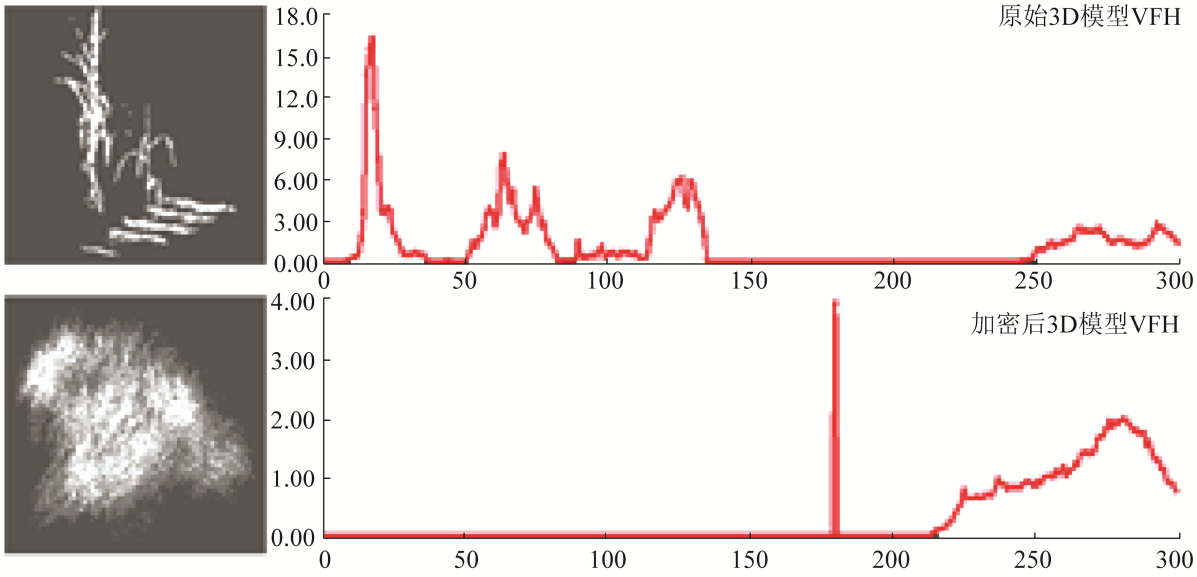


图 6　3D 模型 VFH

5.3 加解密速度

本加密方案是在装有 AMD A10 PRO-7800B R7,12 cores, 4c+8G 3.5GHz and 4.00G RAM 的 PC 机上运行并测试的，搭建了 C++，PCL library 的环境。加解密速度根据点云中点的数量的不同而不同。点的数量越多，加解密需要的时间相应的多，如图 7 所示。

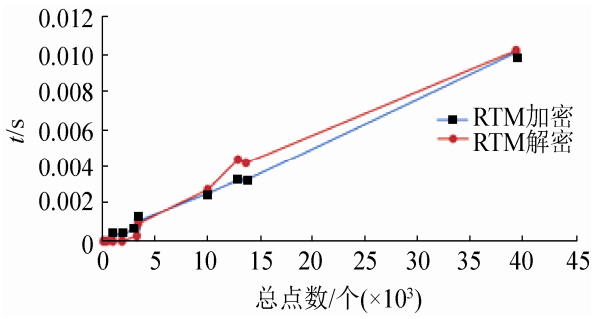


图 7　加解密速度

6 结论

在这篇论文中，本文提出了基于随机可逆矩阵的 3D 点云加密方案，这是第一个针对 3D 点云的加密方案。本文采用通过混沌映射产生随机可逆变换矩阵进行加密，使用了 VFH 描述子评估 3D 点云的加密结果。将来会在这两方面拓展我们的成果：(1) 建立相应评估方法的 3D 点云加密评估打分系统，(2) 对 3D 线框模型和 3D 表面模型设计加密方法。

参考文献:

[1] Huang C, Nien H. Multi chaotic systems based pixel shuffle for image encryption [J]. Opt. Commun. (S0030-4018), 2009, 282: 2123-2127.

[2] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map [J]. Chaos Soliton Fract (S0960-0779), 2005, 26(1): 117-129.

[3] Zhen P, Zhao G, Min LQ, et al. Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy [J]. Multimedia Tools and Applications (MTA) (S1380-7501),2015, 75(11)1-17.

[4] Wang YZ, Ren GY, Jiang JL, et al. Image Encryption Method Based on Chaotic Map [C]// 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA). USA: IEEE, 2007: 2558-2560.

[5] Xin Jin, Kui Guo, Chenggen Song, et al. Private Video Foreground Extraction through Chaotic Mapping based Encryption in the Cloud [C]// International Conference On Multimedia Modelling (MMM) 2016, Miami, USA. Springer International Publishing, (S0018-1560), 2016,9516:562-573.

[6] Xin Jin, Yulu Tian, Chenggen Song, Guangzheng Wei, Xiaodong Li, Geng Zhao, and Huaichao Wang, An Invertible and Anti-Chosen Plaintext Attack Image Encryption Method based on DNA Encoding and Chaotic Mapping [C] Chinese Automation Congress (CAC) 2015, Wuhan, China, 2015.11.27- 11.29, DOI:10.1109/CAC.2015.7382673, IEEE (S1045-9227) 1159-1164.

[7] Xin Jin, Yan Liu, Xiaodong Li, Geng Zhao, Yingya Chen, and Kui Guo, Privacy Preserving Face Identification through Sparse Representation, Chinese Conference on Biometric Recognition (CCBR) 2015, Tianjin, China, 2015.11.13-11.15. Springer International Publishing (S0302-9743) 2015, 9248:160-167

[8] Xin Jin, Yingya Chen, Shiming Ge, Kejun Zhang, Xiaodong Li, Yuzhen Li, Yan Liu, Kui Guo, Yulu Tian, Geng Zhao, Xiaokun Zhang, and Ziyi Wang, Color Image Encryption in CIE L*a*b* Space, International Conference on Applications and Techniques for Information Security (ATIS) 2015, Beijing, China, 2015.11.4-11.6. Springer Berlin Heidelberg (S1865-0929), 2015, 557:74-85

[9] Yuzhen Li, Xiaodong Li, Xin Jin, et al. An Image Encryption Algorithm based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map [C]// International Conference on Applications and Techniques for Information Security (ATIS) 2015, Beijing, China. 2015: 11.4-11.6. Springer Berlin Heidelberg (S1865-0929), 2015, 557:3-13

[10] A Mart´ın del Rey. A Method to Encrypt 3D Solid Objects Based on Three-Dimensional Cellular Automata [C]// Proceedings of the 10th International Conference on Hybrid Artificial Intelligent Systems (HAIS), Bilbao, Spain, Springer International Publishing (S0302-9743) 2015, 9121: 427-438.

[11] Radu Bogdan Rusu, Nico Blodow, Michael Beetz. Fast Point Feature Histograms (FPFH) for 3D Registration [C]// IEEE International Conference on Robotics and Automation, 2009. USA: IEEE (S1050-4729), 2009, 3212-3217.

[12] Jianbing Shen, Xiaogang Jin, Chuan Zhou. A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation PCM, Springer Berlin Heidelberg (S0302-9743), 2005, 3768: 270-280.