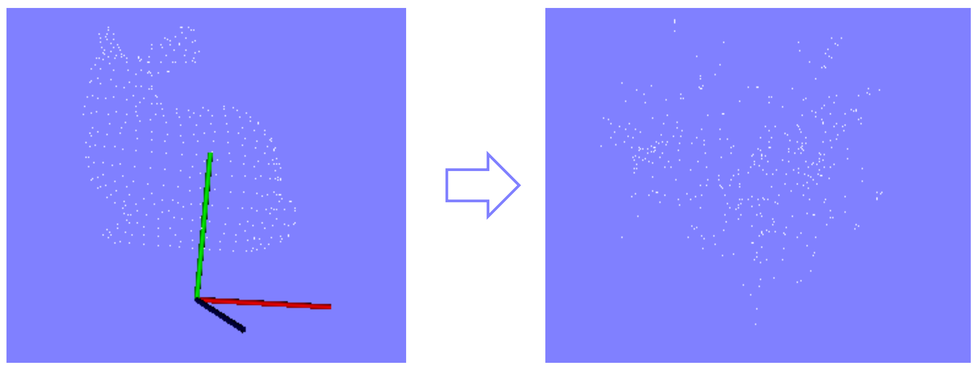
3D Point Cloud Encryption through Chaotic Mapping

BestiVictory

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

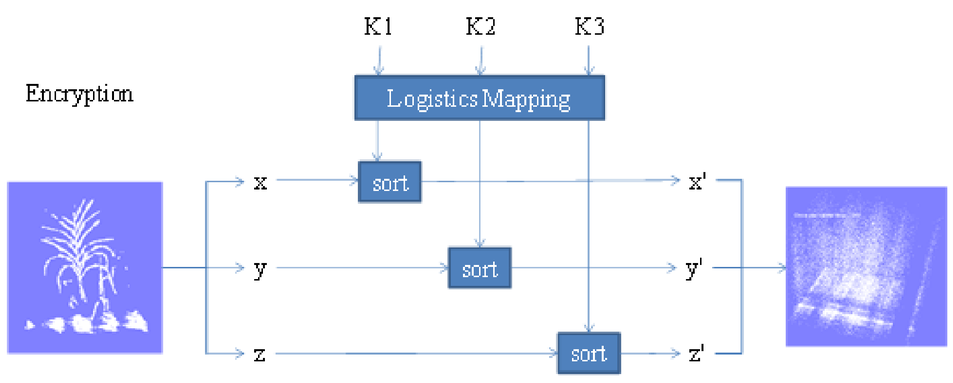
Beijing Electronic Science and Technology Institute, 100070,Beijing, China
GOCPCCC Key Laboratory of Information Security, 100070,Beijing, China
***Corresponding Authors: {jinxin,lxd}@besti.edu.cn**

Background. Three dimensional (3D) contents such as 3D point clouds, 3D meshes and 3D surface models are increasingly growing and being widely spread into the industry and our daily life. However, less people consider the problem of the privacy preserving of 3D contents. As an attempt towards 3D security, in this papers, we propose methods of encrypting the 3D point clouds through chaotic mapping. 2 schemes of encryption using chaotic mapping have been proposed to encrypt 3D point clouds.

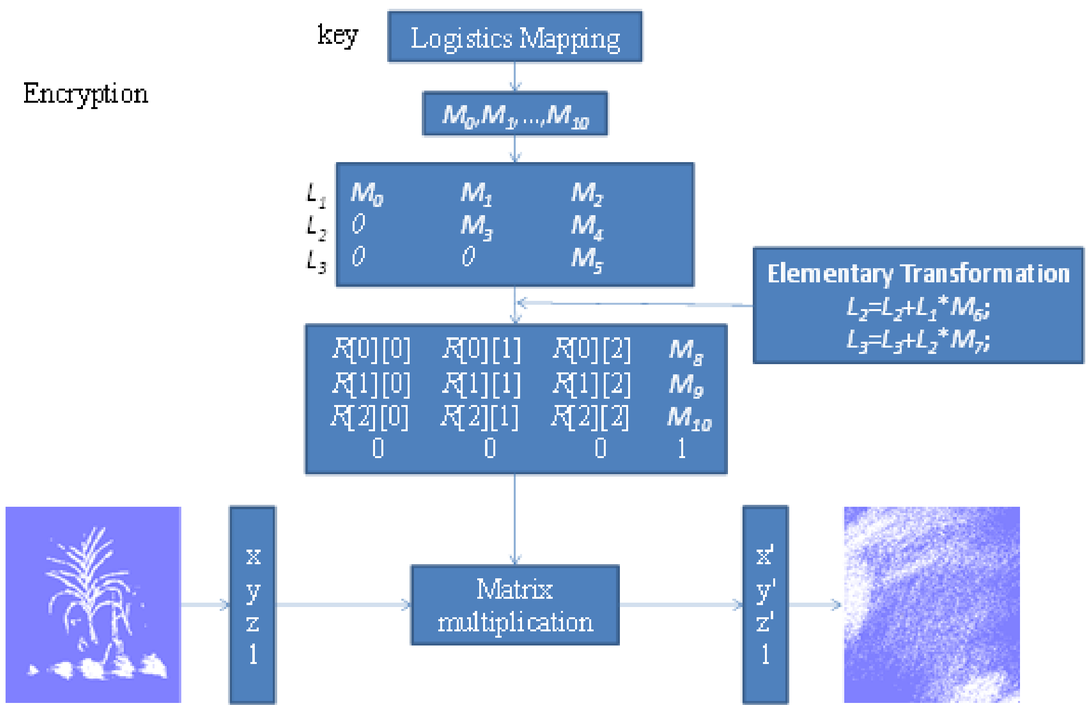


Input 3D Point Cloud — The Encrypted 3D Point Cloud

Scheme 1: Random Vector (RV).

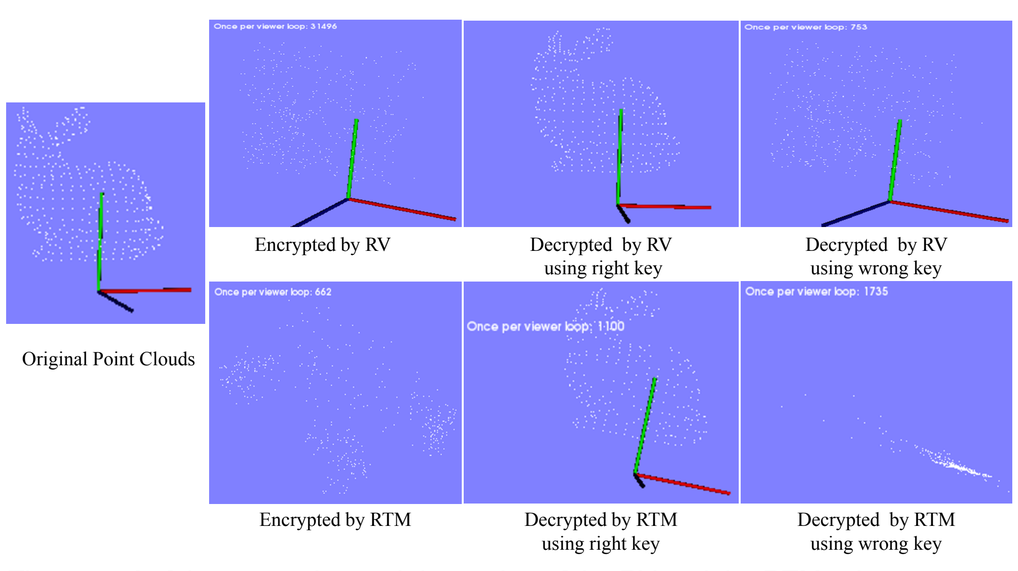


Scheme 2: Random Transformation Matrix (RTM).



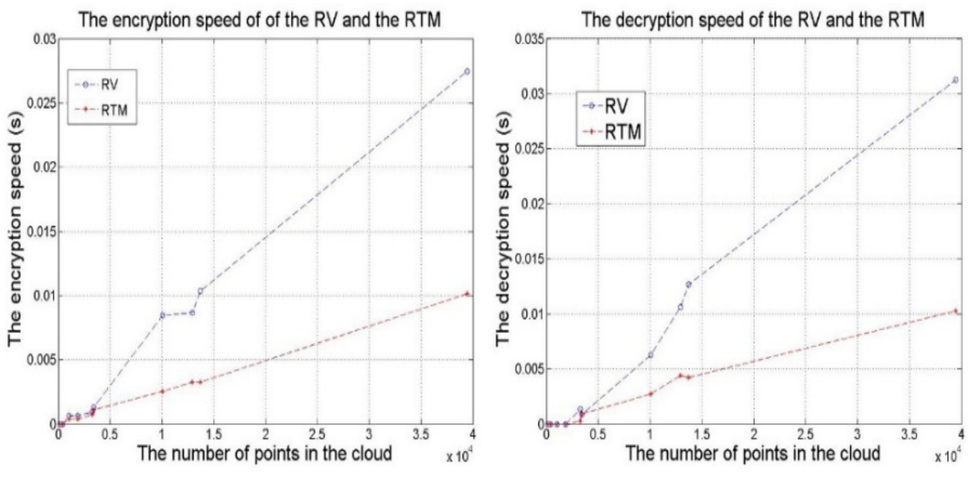
To test the secret key sensitivity of our 3D point cloud encryption scheme, we add 0.0000001 to the secret key. The result shows as follow:

Sensitivity of Secret Key.

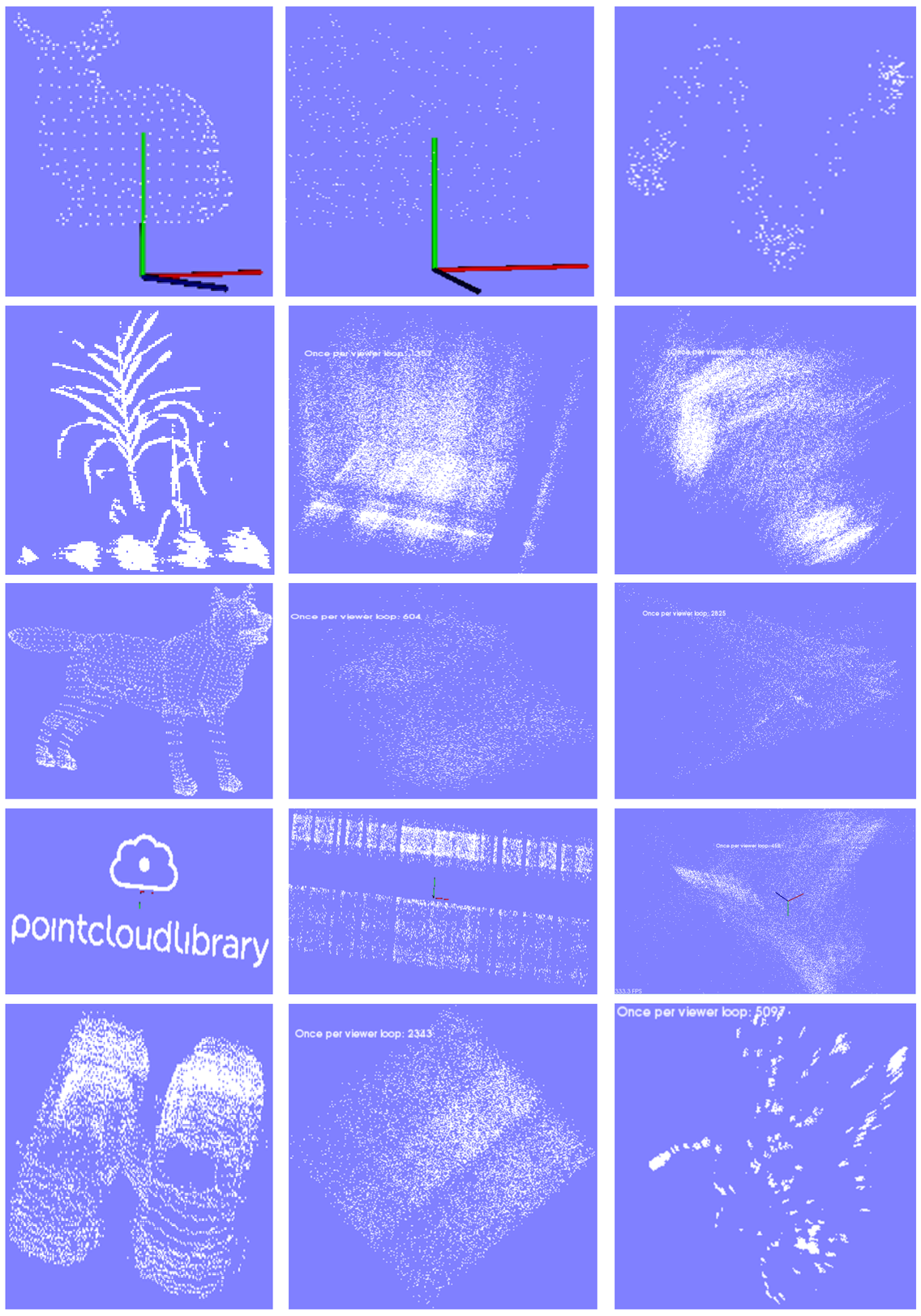


Original Point Clouds — Encrypted by RV — Decrypted by RV using right key — Decrypted by RV using wrong key — Encrypted by RTM — Decrypted by RTM using right key — Decrypted by RTM using wrong key

The **speed** of the encryption and decryption of the RV and the RTM scheme.

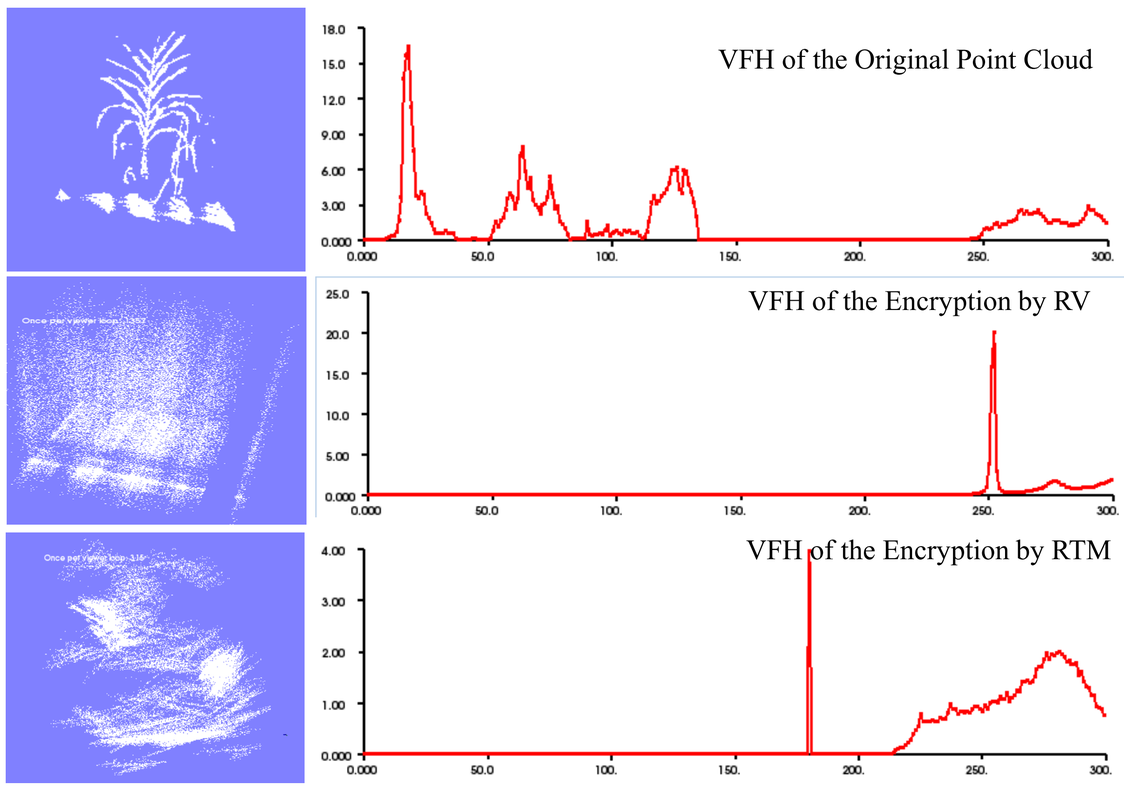


Encryption Results.



Original Point Clouds — Encrypted by RV — Encrypted by RTM

We use the **Viewpoint Feature Histogram (VFH)** for the evaluation of our 3D point cloud encryption.



The **contributions** of this work.

1.The first work that addresses the 3D point cloud encryption.
2.Two schemes of 3D point cloud encryption using the logistic chaotic mapping.
3.Using VFH to evaluate the encryption result of 3D point cloud.