3D Point Cloud Encryption through Chaotic Mapping

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

Abstract. 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. (1) 3 random sequences are generated by the logistic chaotic mapping. Each random vector is sorted to randomly shuffler each coordinate of the 3D point clouds. (2) A random 3×3 invertible rotation matrix and a 3×1 translate vector are generated by the logistic mapping. Then each 3D point is projected to another random place using the above random rotation matrix and translate vector in the homogeneous coordinate. We test the above 2 encryption schemes of 3D point cloud encryption using various 3D point clouds. The 3D point clouds can be encrypted and decrypted correctly. In addition, we evaluated the encryption results by VFH (Viewpoint Feature Histogram). The experimental results show that our proposed methods can produce nearly un-recognized encrypted results of 3D point clouds.

Keywords: 3D Point Clouds, Encryption, Chaotic Mapping, Point Feature Histogram, View Feature Histogram

1 Introduction

Nowadays, tremendous visual contents such as images, videos and 3D models are transmitted to thousands of people by social network software and cloud storages. Besides images and videos, the 3D models are increasingly growing with the image based 3D modeling and 3D print technologies. Some Apps on the smartphone such as Autodesk 123D Catch[1] allow users to shot photos of one subject from various views and upload all the photos to Autodesk cloud server. Then the 123D service on the cloud server will return a 3D model of subject to the users. Desktop software such as Google Sketchup[2] also makes one editing 3D models easily. The 3D models are going into our daily life step by step. In the industry, the virtual reality technology is now a hot topic, which needs plenty of 3D models to build the virtual world. The governments are scanning

[1] http://www.123dapp.com/

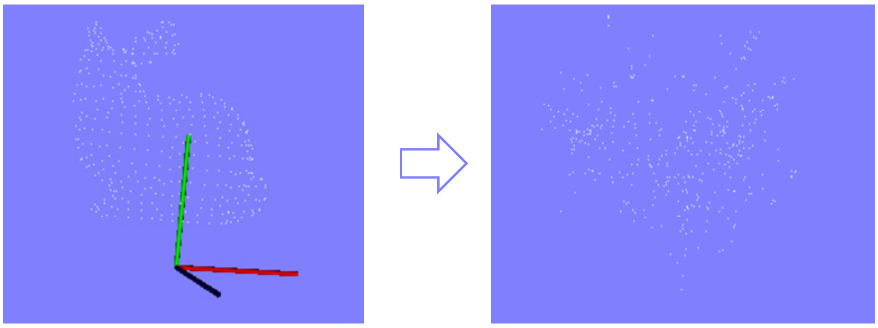
[2] http://www.sketchup.com/

the whole city into 3D virtual city models by laser scanners and multi-view cameras.

Previous Work. The image encryption and video encryption technologies have been studied for a long time. The particular properties of chaos [1] [2], such as sensitivity to initial conditions and system parameters, pseudo-randomness, ergodicity and so on, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. The inherent properties connect it directly with cryptographic characteristics of confusion and diffusion, which is presented in Shannon`s works. Chaotic system is reliable to design secure image and video encryption scheme because of its high complexity [3] [4] [5] [6] [7] [8] [9].

However, less people consider the problem of the encryption of 3D contents. The 3D digitalized objects are defined by means of two types of 3D contents: 3D solid models and 3D shell (boundary) models. A solid model defines the volume of the physical object that represents, whereas a shell model represents the surface, not the volume. In [10], Rey has addressed the encryption of 3D solid models, however, the encryption of 3D shell model has not appeared in the literature.

Thus 3D shell model encryption technologies are required in order to accomplish a high level of security, integrity, confidentiality and to prevent unauthorized access of sensitive 3D models during the storage or transmission over an insecure channels. The 3D contents contains of various types such as 3D point clouds, 3D meshes and 3D models with textures. Different 3D types should correspond to different encryption methods. To the best of our knowledge, there is little work that considering encryption of 3D shell models [12].



Input 3D Point Cloud

The Encrypted 3D Point Cloud

Fig. 1. The encryption of 3D point cloud

Different from text encryption techniques, visual data has some special characteristics, such as bulk data capacity and high correlation among pixels or points. Traditional encryption algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not suitable for visual data encryption. Different from images or videos, the 3D contents contains points, meshes and textures in 3D space. The traditional image or video encryption method are not suitable for 3D contents. Thus, new method of 3D content encryption should be proposed.

Our Approach. As an attempt towards 3D security, in this papers, it is the first time for the 3D point clouds to be encrypted by chaotic mapping, as shown in Fig.1. 2 schemes of encryption using chaotic mapping have been proposed to encrypt 3D point clouds. According to the first scheme, three random sequences are generated by the logistic chaotic mapping. Each random vector is sorted to randomly shuffler each coordinate of the 3D point clouds. According to the second scheme, a random 3×3 invertible rotation matrix and a 3×1 translate vector are generated by the logistic mapping. Then each 3D point is projected to another random place using the above random rotation matrix and translate vector in the homogeneous coordinate. We test the above 2 encryption schemes of 3D point cloud encryption using various 3D point clouds. The 3D point clouds can be encrypted and decrypted correctly. In addition, we evaluated the encryption results by VFH (Viewpoint Feature Histogram). The experimental results show that our proposed methods can produce nearly un-recognized encrypted results of 3D point clouds. The **contributions** of this work includes:

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.

2 Cryptography Primitive

In this section we briefly introduce the cryptography primitive we used in this paper. The simple but efficient chaotic mapping (logistic) is defined as follows:

$$\begin{aligned} & x_{n+1} = \mu x_n (1 - x_n) \\ & 3.569945672... < \mu \leq 4 \\ & 0 \leq x_n \leq 1 \\ & n = 0,1,2,... \end{aligned} \tag{1}$$

When the parameter μ and the initial value x_0 follow the Eq. 1, the outputs of this chaotic mapping x_n become chaotic state and have good potential to form a random sequence.

3 Point Cloud Encryption via the Logistic Mapping

We propose 2 schemes for point cloud encryption via the logistic mapping. In the first scheme, we use the logistic mapping to generate 3 random vectors to shuffle the 3 coordinates of the point clouds. In the second, we generate a random transformation matrix for each 3D point using the logistic mapping. We will describe the details of these to encryption scheme in this section and compare them in the next 2 sections.

3.1 Scheme 1: Random Vector (RV)

In the 3D Euclidean space, each point has 3 coordinates. Thus, we generate 3 random vectors using the logistic mapping for the 3 coordinates. As shown in Fig. 2, each coordinate of each point is corresponded to a random number in the random vector. Then, the random vectors are sorted to new orders. The corresponding coordinates are reordered by the new orders of the random vectors. Then the coordinates of each point are confused to form the final encrypted 3D points. The decryption is the inverse procedure of encryption. The encrypted coordinates are resorted to the original position according the logistics mapping with the same key used in the encryption.

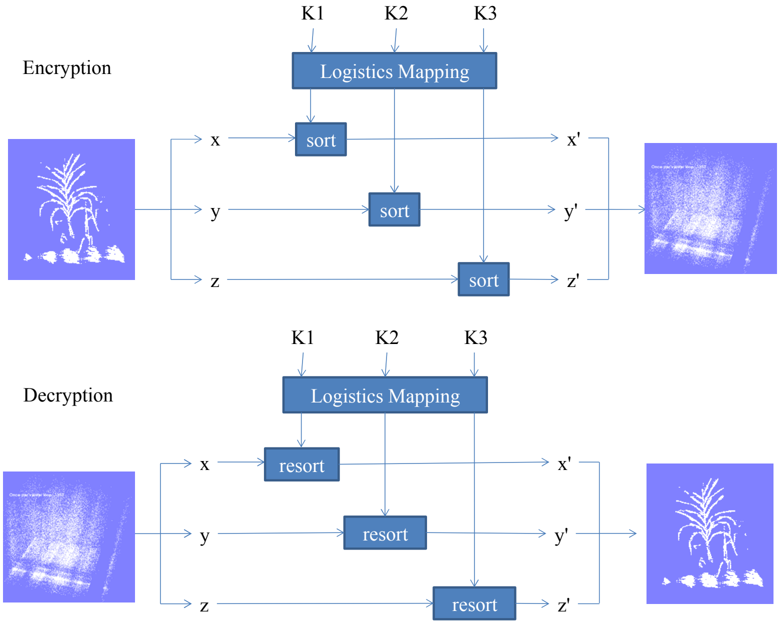


Fig. 2. Random vector based encryption and decryption

A 3D point can be represented as $p = (x, y, z)$. A point cloud consists of a set of 3D points: $P = \{p_1, p_2, \ldots, p_n\}$. The 3 coordinates of the 3D point cloud can be represented as $X = \{x_1, x_2, \ldots, x_n\}, Y = \{y_1, y_2, \ldots, y_n\}, Z = \{z_1, z_2, \ldots, z_n\}$. We use the logistic mapping to randomly shuffle the three vector X, Y, Z for encryption and obtain 3 new vectors: $X' = \{x_1', x_2', \ldots, x_n'\}, Y = \{y_1', y_2', \ldots, y_n'\}, Z = \{z_1', z_2', \ldots, z_n'\}$. The decryption procedure is to remap X', Y', Z' to X, Y, Z so as to obtain the original point cloud.

3.2 Scheme 2: Random Transformation Matrix (RTM)

A point in the 3D Euclidean space can be transformed to another location using the translate and rotation operations A 4×4 transformation matrix T consists of a 3×3 rotation matrix R and a 3×1 translate matrix $t = (t_x, t_y, t_z)$. A 3D point can be represented as a homogeneous coordinate: $p = (x, y, z, 1)$. Then the transformation of a 3D point is shown in Eq. (2).

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

where $p' = (x', y', z', 1)$ is the transformed point of the original 3D point. As shown in Fig. 3, we use the logistic mapping to generate random and invertible matrix T. All the 3D points are transformed to another position randomly. In the decryption phase, we use the invert matrix T^{-1} to re-transform each point to the original position to obtain the original 3D point cloud.

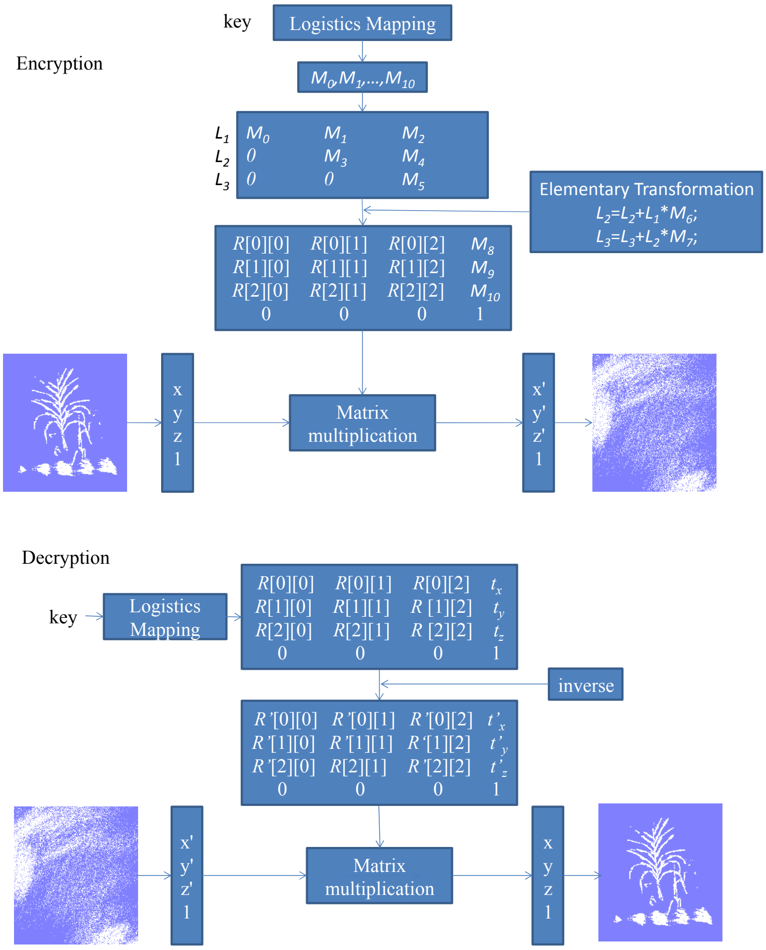

Encryption
key
Logistics Mapping
$M_0, M_1, \ldots, M_{10}$
L_1 M_0 M_1 M_2
L_2 0 M_3 M_4
L_3 0 0 M_5
Elementary Transformation
$L_2 = L_2 + L_1 * M_6$;
$L_3 = L_3 + L_2 * M_7$;
$R[0][0]$ $R[0][1]$ $R[0][2]$ M_8
$R[1][0]$ $R[1][1]$ $R[1][2]$ M_9
$R[2][0]$ $R[2][1]$ $R[2][2]$ M_{10}
0 0 0 1
x y z 1
Matrix multiplication
x' y' z' 1
Decryption
key
Logistics Mapping
$R[0][0]$ $R[0][1]$ $R[0][2]$ 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
inverse
$R'[0][0]$ $R'[0][1]$ $R'[0][2]$ 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
x' y' z' 1
Matrix multiplication
x y z 1

Fig. 3. Random transformation matrix based encryption and decryption

4 Simulation Results

We use plenty of plain 3D point clouds to test our method, as shown in Fig.4, with secret keys. The 3D point clouds with various contents are tested. All the encryption results can be correctly decrypted to the original plain 3D point clouds with the correct keys. The simulation results are quite satisfactory.

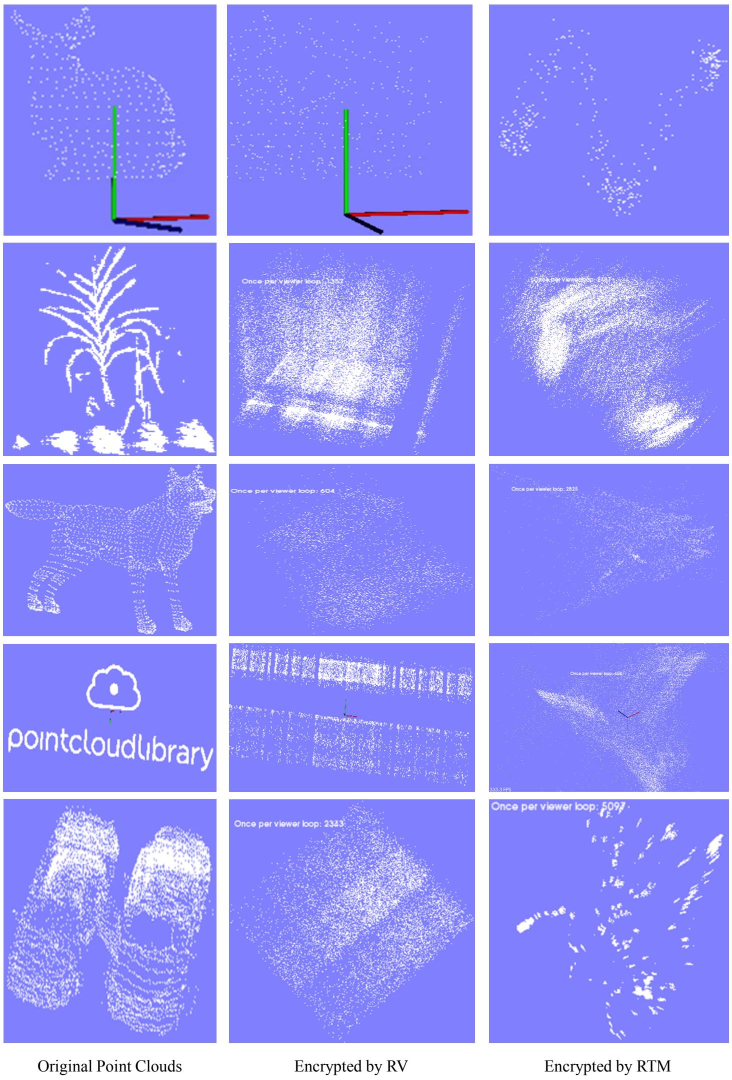

pointcloudlibrary
Once per viewer loop: 604
Once per viewer loop: 2343
Once per viewer loop: 5097
Original Point Clouds
Encrypted by RV
Encrypted by RTM

Fig. 4. The simulation results. We test our method on 3D point clouds with various contents including animal, plant, text, car etc. The left is the original point clouds. The middle is the encrypted results by the Random Vector scheme (RV) as described in Section 3.1. The Right is the encrypted results by the Random Transformation Matrix (RTM) as described in Section 3.2.

5 Security and Performance Analysis

A well designed image encryption scheme should be robust against different attacks, such as brute-force attack and statistical attack. In this section, we analyze the security of the proposed encryption methods using various 3D point clouds.

5.1 Resistance to the brute-force Attack

Key Space. The key space of the image encryption scheme should be large enough to resist the brute-force attack, otherwise it will be broken by exhaustive search to get the secret key in a limited amount of time. The key space of our method is described as follow:

The Random Vector (RV) scheme. We give each coordinate vector of point clouds a pair of key for the logistic mapping:

$$3.569945672\ldots < \mu_x, \mu_y, \mu_z \leq 4$$

$$0 \leq x_0^x, x_0^y, x_0^z \leq 1$$

The Random Transformation Matrix (RTM) scheme. We give each point a pair of key for the logistic mapping:

$$3.569945672\ldots < \mu_0, \mu_1, \ldots, \mu_N \leq 4$$

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

where, N is the number of the point in a point cloud. The precision of 64-bit double data is 10^{-15}. Thus, the key space of the RV scheme is about $(10^{15})^6 = 10^{90} \approx 2^{224}$, which is nearly equal to the max key space (2^{256}) of practical symmetric encryption of the AES. The key space of the RTM scheme is about $(10^{15})^{2N} = 10^{30N} \approx 2^{75N}$. If $N > 3$, the key space will be much larger than the max key space of AES. Our key space is large enough to resist brute force attack.

Sensitivity of Secret Key. The chaotic system are extremely sensitive to the system parameter and initial value. A light difference can lead to the decryption failure. To test the secret key sensitivity of our 3D point cloud encryption scheme, we change the secret key as follow:

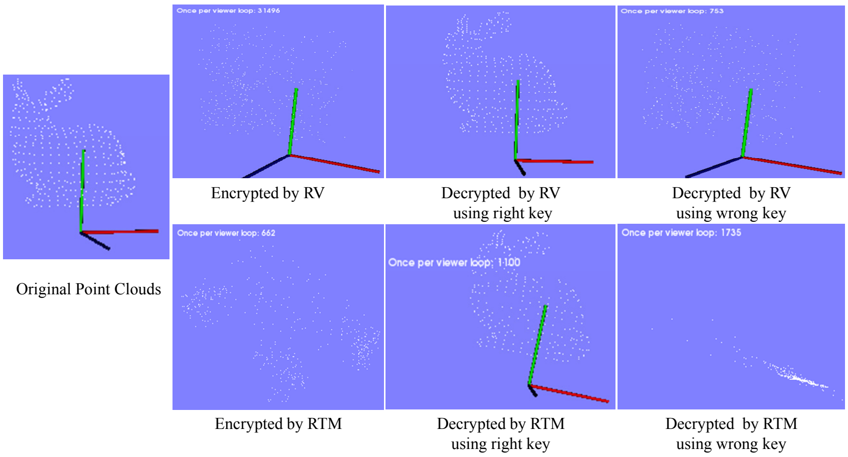
The RV scheme:

μ_x from 3.86 to 3.8600001
μ_y from 3.77 to 3.7700001
μ_z from 3.91 to 3.9100001

The RTM scheme:

$$\mu_i = \mu_i + 0.0000001, i = 1,2, \ldots, N$$

We use the change key to decrypt the encrypted 3D point cloud in Fig. 5 by the RV and the RTM scheme, respectively, while the other secret keys remain the same. The decryption results are shown in Fig.5. The decrypted 3D point clouds are completely different from the original 3D point cloud. The test results of the other secret key are similar. The experiments show that both the 2 schemes are quite sensitive to the secret key, which also indicates the strong ability to resist exhaustive attack.


Once per viewer loop: 31496
Once per viewer loop: 753
Once per viewer loop: 662
Once per viewer loop: 1100
Once per viewer loop: 1735

Encrypted by RV

Decrypted by RV using right key

Decrypted by RV using wrong key

Original Point Clouds

Encrypted by RTM

Decrypted by RTM using right key

Decrypted by RTM using wrong key

Fig. 5. We slightly change the key and get the completely wrong decrypted results.

5.2 Resistance to the Statistic Attack

The Point Feature Histograms (PFH) are informative pose-invariant local features which represent the underlying surface model properties at a point.

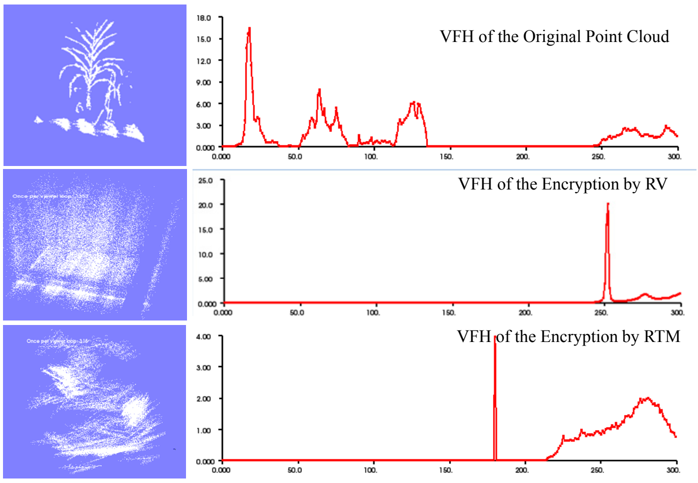


Fig. 6. The VFH of the original point cloud, the encrypted result by RV and RTM

The Viewpoint Feature Histogram (VFH) descriptor is a novel representation for point clusters for the problem of Cluster (e.g., Object) Recognition and 6 DOF Pose Estimation. The major difference between the PFH descriptors and VFH, is that for a given point cloud dataset, only a single VFH descriptor will be estimated, while the resultant PFH data will have the same number of entries as the number of points in the cloud [11]. We use the VFH for the evaluation of our 3D point cloud encryption. As shown in Fig. 6, the VFHs of the encrypted results by both the RV scheme and the RTM scheme are completely different from the VFH of the original point cloud, which makes statistical attacks impossible.

5.3 The Speed of the Encryption and Decryption

The image encryption scheme is implemented by C++ and the PCL library[3] on personal computer with AMD A10 PRO-7800B R7,12 cores, 4c+8G 3.5GHz and 4.00G RAM. The consumption time encryption and decryption is recorded for different number of points in the cloud. The larger the number is, the more time it needs for encryption and decryption.

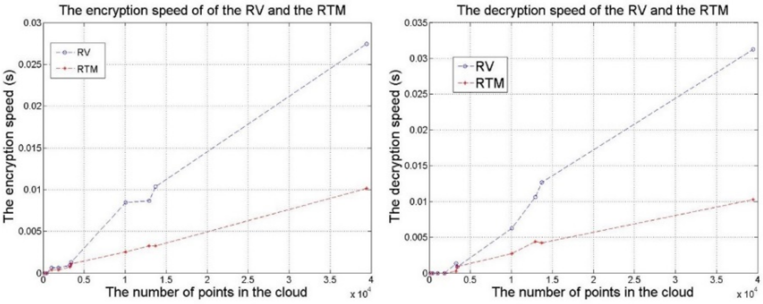


Fig. 7. The speed of the encryption and decryption of the RV and the RTM scheme.

As shown in Fig. 8, we test the speed of the encryption and decryption progress using the two proposed schemes for point cloud encryption. The RTM scheme is less time consuming than the RV scheme.

6 Conclusion and Discussion

In this paper, we propose two schemes for the encryption of 3D point clouds using chaotic mapping. This is the first work that addresses the 3D point cloud encryption. Two schemes of 3D point cloud encryption using the logistic chaotic mapping are proposed. The VFH are used to evaluate the encryption result of 3D point cloud. In the future work, we will extend our work in 2 directions: (1) building a 3D point cloud encryption evaluation bench mark dataset with corresponding evaluation methods, (2) extending the point cloud encryption methods to 3D meshes and 3D surface models.

[3] http://www.pointclouds.org/

Acknowledgement

The work is supported by the National Natural Science Foundation of China (No.61402021), the Science and Technology Program of the State Archives Administration (2015-B-10), and the open funding project of State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (Grant No.BUAA-VR-16KF-09).

Reference

1. Huang C, Nien H (2009) Multi chaotic systems based pixel shuffle for image encryption. Opt. Commun. 282:2123–2127
2. Lian S, Sun J,Wang Z (2005) A block cipher based on a suitable use of the chaotic standard map. Chaos Soliton Fract 26(1):117–129
3. Zhen, P., Zhao, G., Min, LQ., Jin, X. Chaos-Based Image Encryption Scheme Combining DNA Coding and Entropy. Multimedia Tools and Applications (MTA), Published Online: 10 April (2015)
4. Wang YZ., Ren GY., Jiang JL., Zhang J., Sun LJ. Image Encryption Method Based on Chaotic Map. 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA), pp.2558-2560 (2007)
5. Xin Jin, Kui Guo, Chenggen Song, Xiaodong Li, Geng Zhao, Jing Luo, Yuzhen Li, Yingya Chen, Yan Liu, and Huaichao Wang, Private Video Foreground Extraction through Chaotic Mapping based Encryption in the Cloud, International Conference On Multimedia Modelling (MMM) 2016, Miami, USA, 2016.1.4-1.6
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, Chinese Automation Congress (CAC) 2015, Wuhan, China, 2015.11.27- 11.29
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
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
9. Yuzhen Li, Xiaodong Li, Xin Jin*, Geng Zhao, Shiming Ge, Yulu Tian, Xiaokun Zhang, Kejun Zhang, and Ziyi Wang, An Image Encryption Algorithm based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map, International Conference on Applications and Techniques for Information Security (ATIS) 2015, Beijing, China, 2015.11.4-11.6
10. A. Mart´ın del Rey. A Method to Encrypt 3D Solid Objects Based on Three-Dimensional Cellular Automata. In Proceedings of the 10th International Conference on Hybrid Artificial Intelligent Systems (HAIS) 2015, Bilbao, Spain, June 22-24, pp. 427-438, 2015.
11. Radu Bogdan Rusu, Nico Blodow, Michael Beetz. Fast Point Feature Histograms (FPFH) for 3D Registration. IEEE International Conference on Robotics and Automation. 2009
12. Éluard M, Maetz Y, Doërr G. Geometry-preserving Encryption for 3D Meshes[C] Compression Et Représentation Des Signaux Audiovisuels. 2013.