SCIENCE CHINA
Information Sciences

3D Textured Model Encryption via 3D Lu Chaotic Mapping

Jin Xin, Zhu Shuyun, Xiao Chaoen, Sun Hongbo, Li Xiaodong, Zhao Geng and Ge Shiming

Citation: SCIENCE CHINA Information Sciences ; doi: 10.1007/s11432-017-9266-1

View online: http://engine.scichina.com/doi/10.1007/s11432-017-9266-1

Published by the Science China Press

SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

3D textured model encryption via 3D Lu chaotic mapping

Xin JIN[1], Shuyun ZHU[1,3], Chaoen XIAO[2], Hongbo SUN[1], Xiaodong LI[1*], Geng ZHAO[1] & Shiming GE[4*]

[1]*Department of Computer Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China;*
[2]*Department of Electronic Information Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China;*
[3]*Xidian University, Xi'an 710071, China;*
[4]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*

Abstract In the emerging Virtual/Augmented Reality (VR/AR) era, three dimensional (3D) content will be popularized just as images and videos today. The security and privacy of these 3D contents should be taken into consideration. 3D contents contain surface models and solid models. Surface models include point clouds, meshes and textured models. Previous works mainly focused on the encryption of solid models, point clouds and meshes. This work focuses on the most complicated 3D textured model. We propose a 3D Lu chaotic mapping based encryption method for 3D textured models. We encrypt the vertices, polygons, and textures of 3D models separately using the 3D Lu chaotic mapping. Then the encrypted vertices, polygons and textures are composited together to form the final encrypted 3D textured model. The experimental results reveal that our method can encrypt and decrypt 3D textured models correctly. Furthermore, typical statistic and brute-force attacks can be resisted by the proposed method.

Keywords 3D model, Surface model, Textured model, 3D model encryption, 3D Lu chaotic mapping

Citation Xin Jin, Shuyun ZHU, Chaoen XIAO, et al. 3D textured model encryption via 3D Lu chaotic mapping. Sci China Inf Sci, for review

1 Introduction

Today, images and videos are ubiquitous in our daily life. In the near future, 3D models will be obtained increasingly easily with depth sensors, 3D cameras, computational photography technologies, etc. In the industry, virtual reality and augmented reality technologies are now hot topics, which need numerous 3D models to build the virtual world. The virtual versions of our cities are built using multi-camera systems with laser sensors. The security of the 3D models should be taken into consideration now. The privacy and confidentiality in the 3D models should be protected by encryption algorithms during the transmission over the internet.

Typically speaking, there exist two types of 3D models: solid and surface. The 3D solid model contains voxels inside the models. Rey [1] proposes an encryption method for 3D solid models. The surface models only describe the surface of a 3D model. Surface models include point clouds, meshes, and textured models.

* Corresponding author (email: lxd@besti.edu.cn, geshiming@iie.ac.cn)

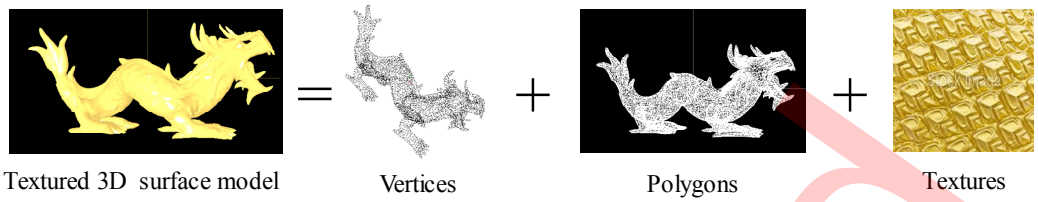

Figure 1 A full 3D surface model containing vertices, polygons and textures.

Current methods in this direction only consider the solid models [1], the point clouds models [2,3], the meshes [4] and the textures [5]. This paper focus on encryption of 3D surface models. A full 3D textured surface model often contains vertices, polygons and textures, as shown in Figure 1. We propose a chaotic mapping based encryption method of 3D textured model. The core idea is that the vertices, the polygons and the textures are encrypted by the Lu chaotic mapping.

Organization. We organize the rest of our paper as follows: In section 2, we give a brief review of related work in this field. The core method and the preliminaries are presented in Section 3. The simulation results are shown in Section 4. We perform security and performance analysis in Section 5. At last we give conclusions and discuss future work in Section 6.

2 Previous Work

As mentioned earlier, current methods in this direction only consider the solid models [1], the point clouds models [2,3], the meshes [4] and the textures [5].

Rey [1] proposes an encryption method for 3D solid models. Rey uses 2D Arnold cat map and 3D celluar automata for 3D solid models encryption. Jolfaei et al. [2] propose a encryption method for 3D point clouds. They use a series of random permutations and rotations. The point clouds are deformed by the random permutations and rotations. Jin et al. [3] propose a encryption method for 3D point clouds. They use a random invertible matrix generated by logistic mapping to shuffle 3D points. Eluard et al. [4] propose a encryption method of 3D meshes. They use a couple of permutation-based algorithms for 3D meshes encryption. Jolfaei et al. [5] propose an encryption method for textures based on bit masking using a stream cipher.

In summary, current 3D model encryption methods have not considered the full 3D texture model, which contain vertices, polygons and textures. This paper focuses on the encryption of 3D textured models. For an alternative way of conventional cryptographic algorithms for encryption [6–10], chaotic maps [11] [12–16] are the dominant technologies used in 2D image encryption [17–24] as well as 3D model encryption [1–5].

3 3D Textured Model Encryption

In this section, we describe the proposed encryption method of 3D textured model. As shown in Figure 2, firstly, we decompose the 3D textured model into vertices, polygons and texture. Then these three parts are encrypted using 3D Lu chaotic mapping. At last, the encrypted vertices, polygons and texture are composited into the encrypted 3D textured model.

3.1 Preliminaries

We adopt a high-order chaotic mapping. 3D Lu mapping is a 3D chaotic map, which is described by Eq. 1.

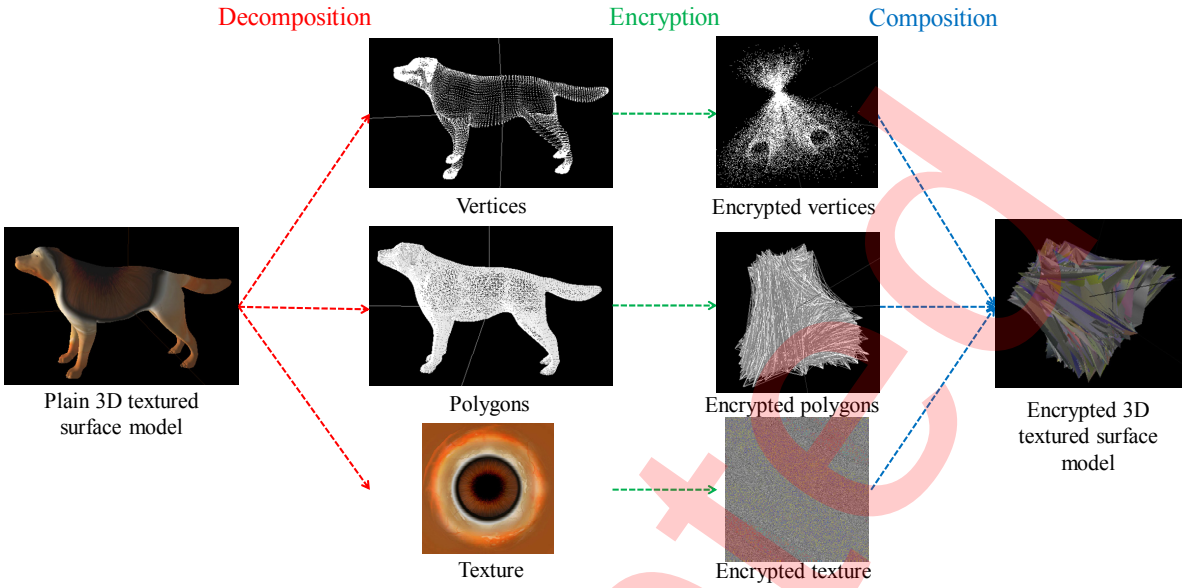

Figure 2 Proposed method for 3D textured model encryption.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + cy, \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

where (x, y, z) is the system trace. When the system parameters are $a = 36, b = 3, c = 20$, the system is in the chaotic state and contains a strange attractor.

3.2 Vertex Encryption

The vertices in a 3D textured model are in the form of a list of triplets:

$$V = \{(X_1, Y_1, Z_1), ..., (X_N, Y_N, Z_N)\}, \tag{2}$$

where (X_i, Y_i, Z_i) is the 3D coordinate of a vertex. N is the number of the vertices. We use the 3D Lu mapping defined in Eq. 1 to produce a random vector with dimensions of $3N$:

$$LV = \{(LV_1, LV_2, L_3), ..., (LV_{3N-2}, LV_{3N-1}, LV_{3N})\}. \tag{3}$$

Then we take the element-wise product of V and LV:

$$VLV = \{(X_1LV_1, Y_1LV_2, Z_1LV_3), ..., (X_NLV_{3N-2}, Y_NLV_{3N-1}, Z_NLV_{3N})\}. \tag{4}$$

The new vector VLV contains novel coordinates of the original 3D vertices:

$$(X_i, Y_i, Z_i) \rightarrow (X_iLV_{3(i-1)}, Y_iLV_{3(i-1)+1}, Z_iLV_{3(i-1)+2}), 1 \leqslant i \leqslant N. \tag{5}$$

Table 1 The secret keys of the 3D Lu maps in Eq. 1. In all the 3 encryption phases, $a = 36, b = 3, and c = 20$.

Encryption Phases	Keys
vertices encryption	$x_0^v = -6.045, y_0^v = 2.668, z_0^v = 16.363$
polygons encryption	$x_0^p = -5.045, y_0^p = 2.668, z_0^p = 16.363$
texture encryption	$x_0^{t1} = -6.045, y_0^{t1} = 2.668, z_0^{t1} = 20.363, x_0^{t2} = -5.045, y_0^{t2} = 3.668, z_0^{t2} = 16.363$

3.3 Polygon Encryption

The polygons (taking the triangle as an example) in a 3D textured model are in the form of a list of triplets:

$$P = \{(A_1, B_1, C_1), ..., (A_i, B_i, C_i), ..., (A_M, B_M, C_M)\}, \tag{6}$$

where (A_i, B_i, C_i) represents the three vertices of a triangle in the form of the indices of the vertices. $1 \leqslant i \leqslant M, 1 \leqslant A_i, B_i, C_i \leqslant N$. N is the number of vertices. We use the 3D Lu mapping defined in Eq. 1 to produce a random vector with dimensions of $3M$:

$$LP = \{(LP_1, LP_2, L_3), ..., (LP_{3M-2}, LP_{3M-1}, LP_{3M})\}. \tag{7}$$

We make the element-to-element correspondences between P and LP:

$$\begin{cases} A_i \longleftrightarrow LP_{3(i-1)+1} \\ B_i \longleftrightarrow LP_{3(i-1)+2}. \\ C_i \longleftrightarrow LP_{3(i-1)+3} \end{cases} \tag{8}$$

Then we subject LP to an ascending sort. The sorted LP is denoted as LP^{sort}. According to the new order in LP^{sort}, we reorder the element in P using the correspondences described in Eq. 8. The vector with new order of P is denoted as P'.

$$P' = \{(A'_1, B'_1, C'_1), ..., (A'_i, B'_i, C'_i), ..., (A'_M, B'_M, C'_M)\}, \tag{9}$$

where (A'_i, B'_i, C'_i) is the new triangle of the encrypted 3D model.

3.4 Texture Encryption

The textures in 3D textured model is represented as 2D images with corresponding texture coordinates. We use the image encryption method of [21] to encrypt the texture images. We substitute the one dimensional (1D) logistic mapping used in [21] with 3D Lu mapping. We first separate each of a texture image into RGB channels. Then each channel of the texture image is encrypted by using the method of [21] (the 3D Lu mapping version). At last, the encrypted RGB channels are composited together to obtain the final encrypted textures.

4 Simulation Results

We use various 3D textured models to verify our proposed method, as shown in Figure 3. The secret keys of the vertices, polygons and textures are listed in Table 1.

We use four Lu maps in our method. The texture encryption contains 2 Lu maps. We can correctly decrypt all the encrypted results to the original plain 3D models using the correct secret keys. The simulation results are satisfactory.

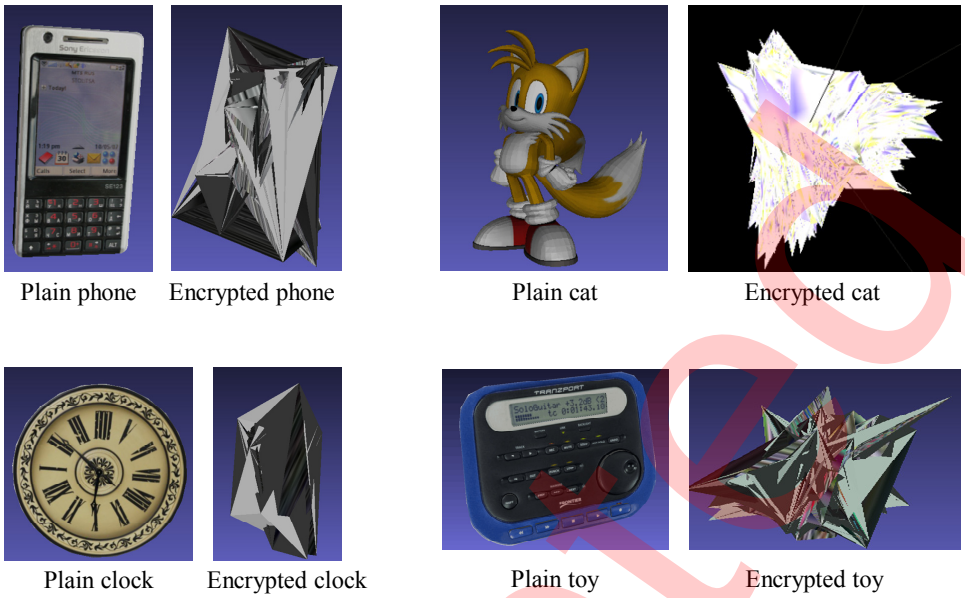

Figure 3 Simulation results. We test our method on 3D models with various contents.

5 Security and Performance Analysis

In this section, we illustrate the robustness of our method against various attacks such as statistical attack and brute-force attack. Besides, we analyse the security and performance of our method.

5.1 The brute-force Attack

5.1.1 *Key Space*

To resist the brute-force attack, the key space of the 3D textured model encryption should be large enough, without which, the encryption results will be broken by brute-force search to obtain the secret key within a linear computational time. In our experiments, we use the keys of 12 key values which are shown in Table 1.

Our key space is approximately $(10^{15})^{12} = 10^{180} \approx 2^{599}$ (based on the precision of 64-bit double data). Our key space is larger than the standard implementation of the AES [25] algorithm. In summary, the key space of our method is large enough to resist the brute-force attack.

5.1.2 *Sensitivity of Secret Key*

The Lu map we use is quite sensitive to the change in the initial values and system parameters. We use the initial values and system parameters as our secret keys, which are described in Section 5.1.1. A very slightly change can make the decrypted results very different from the original plain 3D textured model. We show examples in Figure 4 with slightly changes of the original keys. Then we show more examples in Figure 5, in which for each example, we slightly change the original keys twice to show the sensitivity of our method.

The changed keys are used to decrypt the encrypted 3D models. Note that, we do not change other secret keys. The decrypted results using the slightly changed keys are not recognizable and are completely different from the plain 3D models. This reveals that our method can resist an exhaustive attack.

5.2 Resistance to the Statistic Attack

5.2.1 *The Histogram Analysis*

For vertices, the Viewpoint Feature Histogram (VFH) is to describe the statistic feature of point clouds. We leverage the VFH to check the statistical characteristics of the 3D textured models before and after

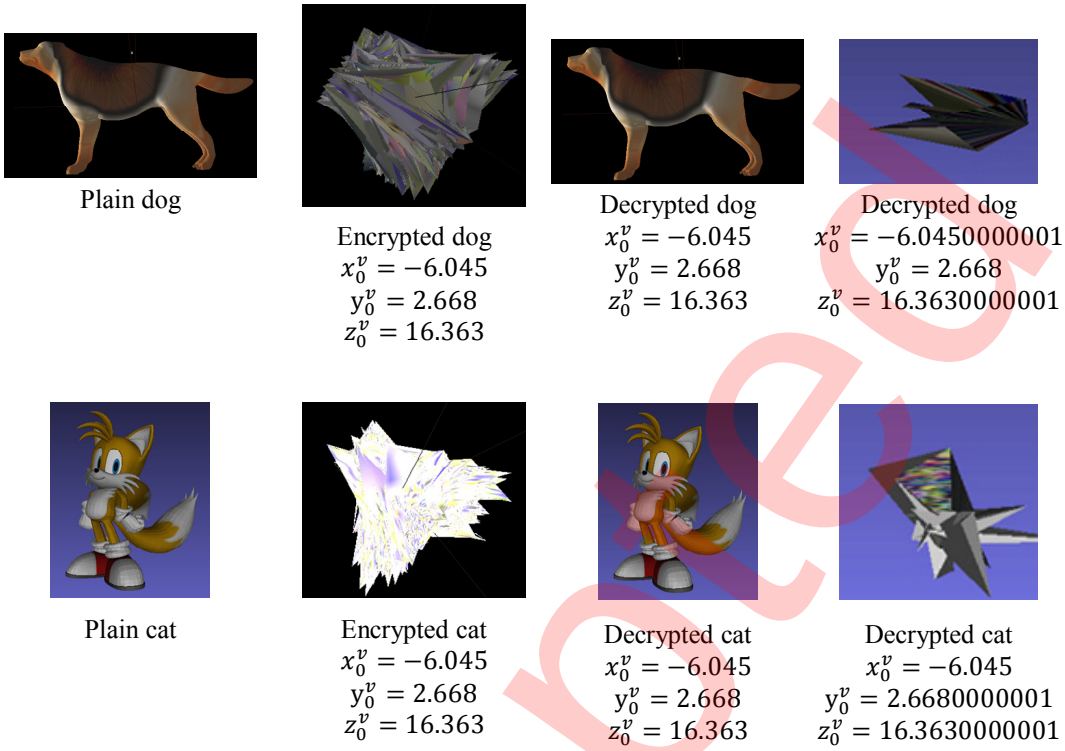

Figure 4 Decryption with slightly changed keys. The *dog* and *cat* examples are shown. We only show the changed keys. The full original keys are shown in Table 1.

encryption. As shown in Figure 6, the VFH of the 3D textured models before and after encryption are completely different, which leads to impossible statistical attacks.

5.2.2 *Distribution of Occupied Positions*

We further analyse the occupied positions of the 3D vertices. As defined in [1], we compute the occupied position per x-coordinate, y-coordinate and z-coordinate of a 3D lattice $Z = (z_{ijk})$.

The matrices obtained for the plain 3D vertices and the encrypted 3D vertices are very different. Furthermore, in Figure 7, we show the DOP per z-coordinate in the original plain vertices and the encrypted ones. The DOPs of the 3D vertices before and after encryption are completely different. The distribution of the encrypted vertices is more random than that of the original plain vertices.

5.3 The Speed of the Encryption and Decryption

The 3D textured model encryption scheme is implemented on PC with AMD A10 PRO-7800B, 12 Processor Cores 4C+8G 3.4GHz and 4.00G RAM. We show the computation times of the encryption and decryption against the number of vertices of 3D textured models in Figure 8. We implement our method in MATLAB 2015a. The computation times of the encryption and decryption can be reduced by converting the MATLAB codes to other languages such as C/C++ or Python.

6 Conclusion

Previous works mainly focused on encryption of solid models, point clouds, and meshes. This work deal with the encryption of 3D textured models. We propose a chaotic mapping based encryption method for a 3D textured model. We encrypt the vertices, the polygons and the textures of 3D models separately using the 3D Lu chaotic mapping. Then the encrypted vertices, polygons and texture maps are composited together to form the final encrypted 3D textured model. The experimental results reveal that our method

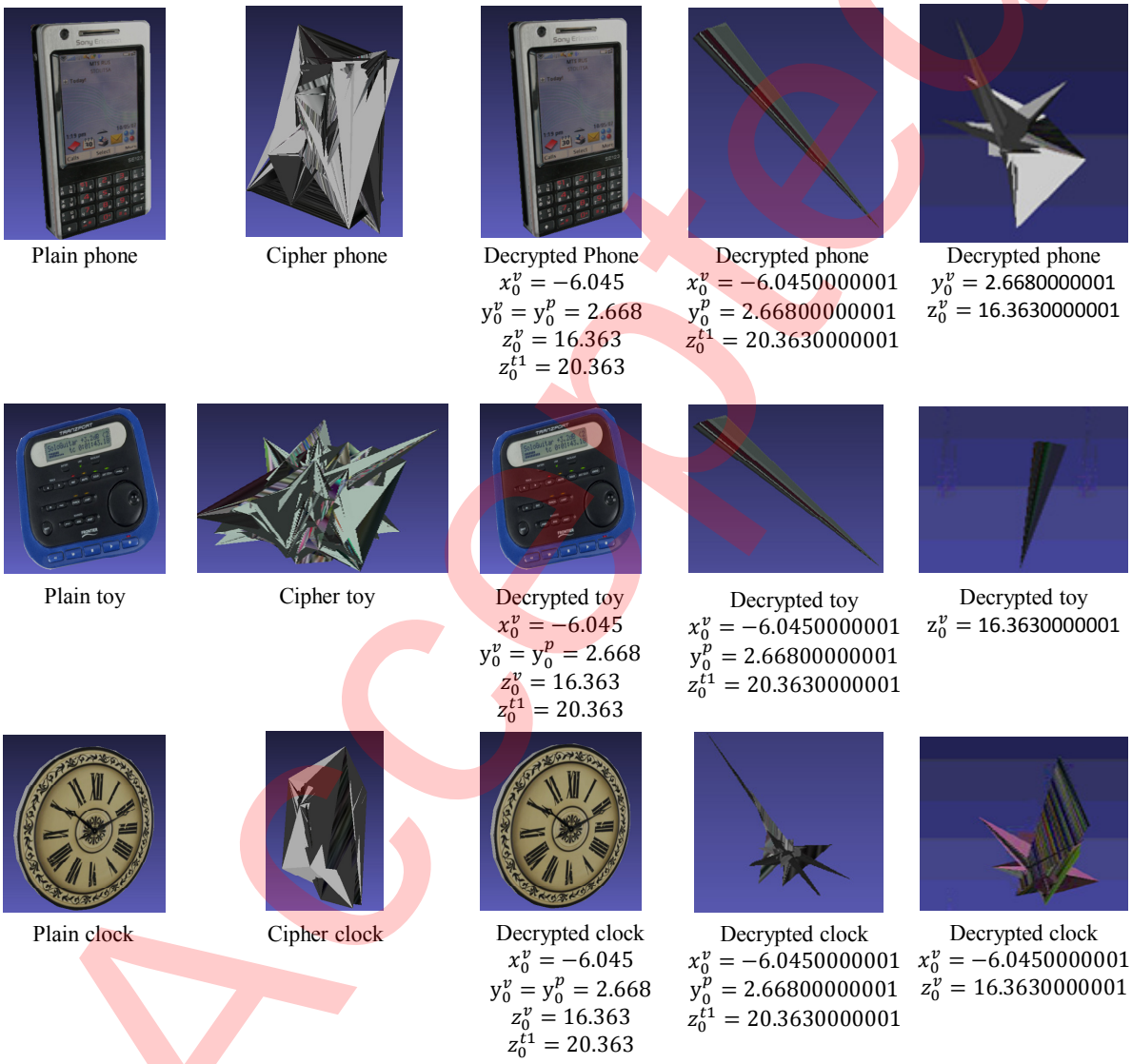

Figure 5 Decryption with slightly changed keys. The *phone*, *toy* and *clock* examples are shown. We only show changed keys. The full original keys are shown in Table 1. Note that, in this figure, for each example, we slightly change the original keys twice to show the key-sensitivity of our method. For each example, the decrypted results of both times are completely different from the correctly decrypted results.

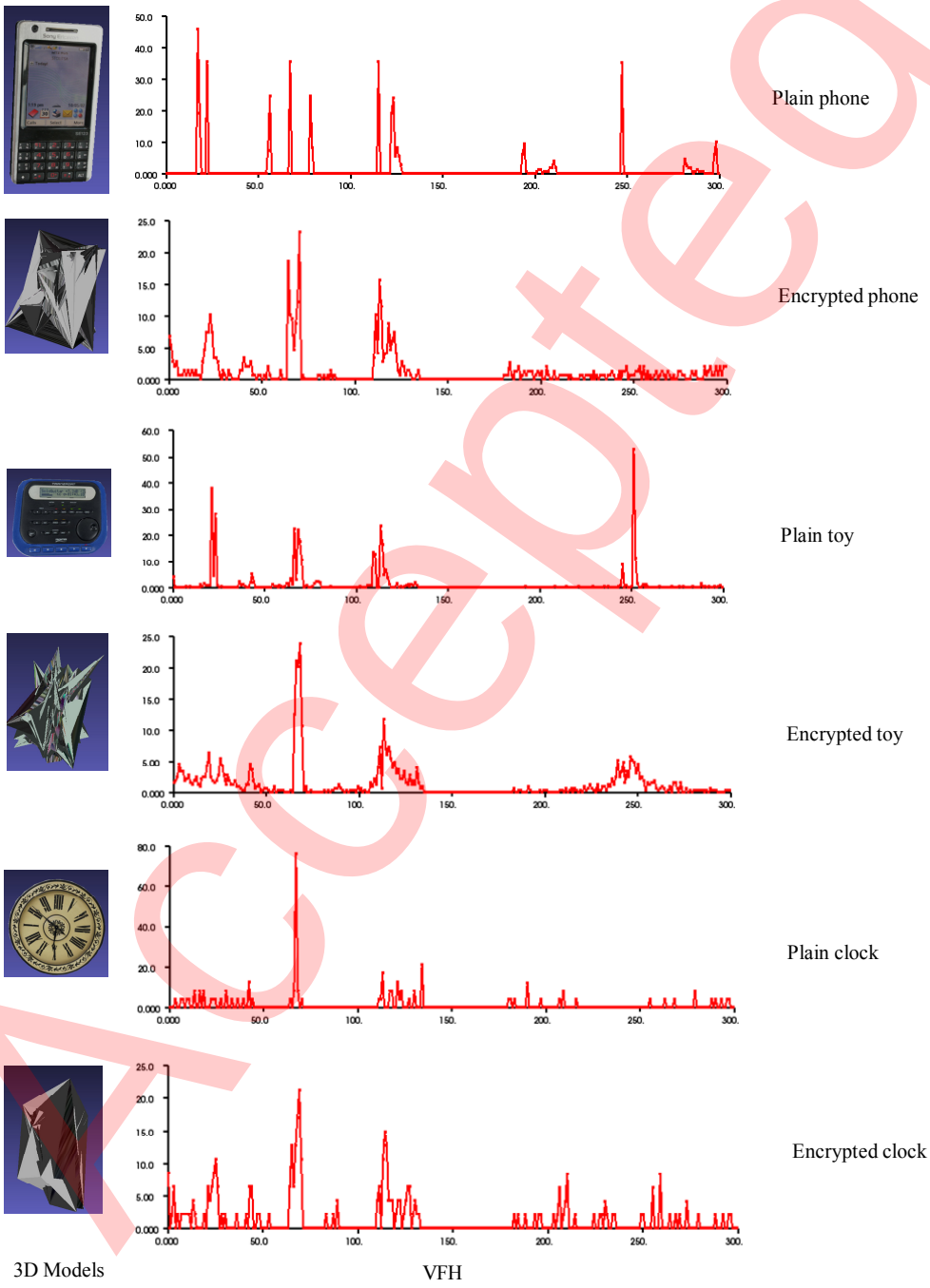

Figure 6 Viewpoint Feature Histogram (VFH) of 3D textured models before and after encryption.

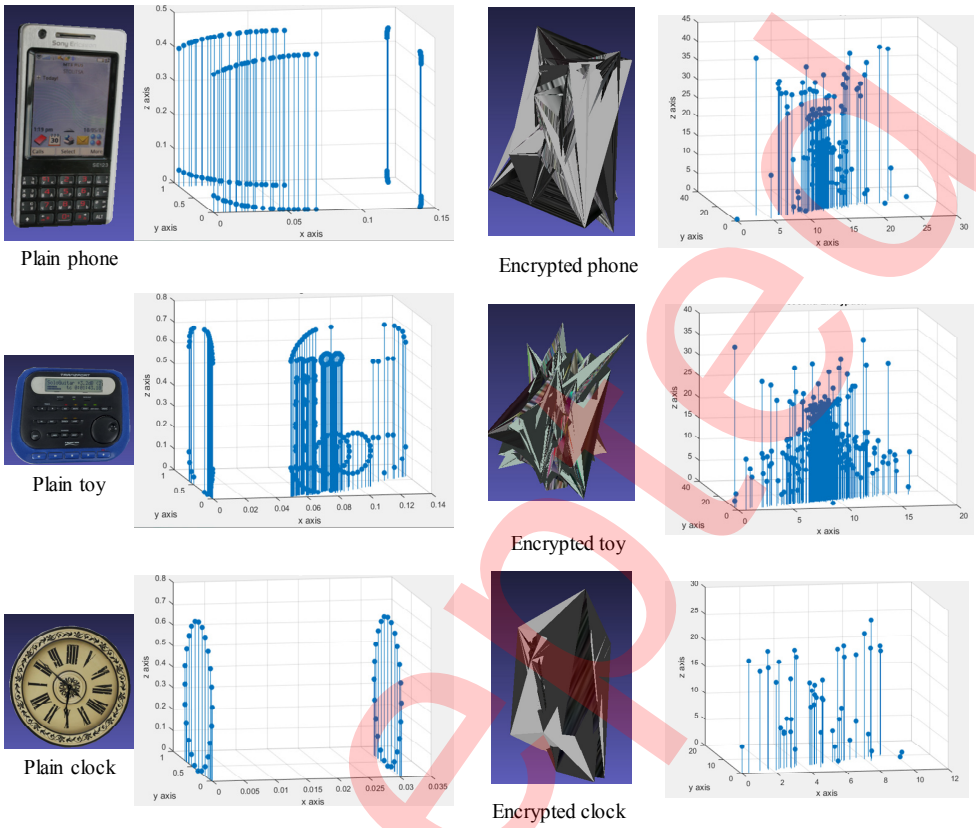

Figure 7 Distribution of occupied positions per z-coordinate of the 3D textured models before and after encryption.

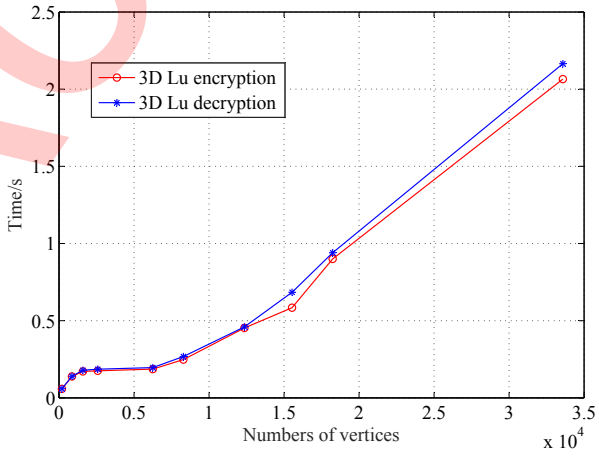

Figure 8 Encryption and decryption time costs of the proposed method for 3D model encryption against the number of vertices.

can encrypt and decrypt 3D textured models correctly. Furthermore, typical statistic and brute-force attacks can be resisted by the proposed method.

Acknowledgements

This work is partially supported by the National Natural Science Foundation of China (Grant NO.61402021, 61401228, 61640216, 61772047), the Science and Technology Project of the State Archives Administrator (Grant NO. 2015-B-10), the open funding project of State Key Laboratory of Virtual Reality Technology and Systems, Beihang University (Grant NO. BUAA-VR-16KF-09), the Fundamental Research Funds for the Central Universities (Grant NO.2016LG03, 2016LG04), the China Postdoctoral Science Foundation (Grant NO.2015M581841), and the Postdoctoral Science Foundation of Jiangsu Province (Grant NO.1501019A).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Ángel Martín del Rey. A method to encrypt 3d solid objects based on three-dimensional cellular automata. In *Hybrid Artificial Intelligent Systems - 10th International Conference, HAIS 2015, Bilbao, Spain, June 22-24, 2015, Proceedings*, pages 427–438, 2015.
2 Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. A 3d object encryption scheme which maintains dimensional and spatial stability. *IEEE Trans. Information Forensics and Security*, 10(2):409–422, 2015.
3 Xin Jin, Zhaoxing Wu, Chenggen Song, Chunwei Zhang, and Xiaodong Li. 3d point cloud encryption through chaotic mapping. In *Advances in Multimedia Information Processing - PCM 2016 - 17th Pacific-Rim Conference on Multimedia, Xi'an, China, September 15-16, 2016, Proceedings, Part I*, pages 119–129, 2016.
4 Marc Eluard, Yves Maetz, and Gwenael Doerr. Geometry-preserving encryption for 3d meshes. In *COmpression et REprsentation des Signaux Audiovisuels (CORESA)*, pages 7–12, 2013.
5 Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. A secure lightweight texture encryption scheme. In *Image and Video Technology - PSIVT 2015 Workshops - RV 2015, GPID 2013, VG 2015, EO4AS 2015, MCBMIIA 2015, and VSWS 2015, Auckland, New Zealand, November 23-27, 2015. Revised Selected Papers*, pages 344–356, 2015.
6 Zuobin Ying, Hui Li, Jianfeng Ma, Junwei Zhang, and Jiangtao Cui. Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating. *SCIENCE CHINA Information Sciences*, 59(4):042701:1–042701:16, 2016.
7 Kai Zhang, Jianfeng Ma, Jiajia Liu, and Hui Li. Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption. *SCIENCE CHINA Information Sciences*, 59(9):99105, 2016.
8 Zhao Chen, Liuguo Yin, Yukui Pei, and Jianhua Lu. Codehop: physical layer error correction and encryption with ldpc-based code hopping. *SCIENCE CHINA Information Sciences*, 59(10):102309, 2016.
9 Zhenfu Cao. New trends of information security - how to change people's life style? *SCIENCE CHINA Information Sciences*, 59(5):050106:1–050106:3, 2016.
10 Hongbo Yu, Yonglin Hao, and Dongxia Bai. Evaluate the security margins of sha-512, SHA-256 and DHA-256 against the boomerang attack. *SCIENCE CHINA Information Sciences*, 59(5):052110:1–052110:14, 2016.
11 Om Prakash Verma, Munazza Nizam, and Musheer Ahmad. Modified multi-chaotic systems that are based on pixel shuffle for image encryption. *JIPS*, 9(2):271–286, 2013.
12 Hai Jin, Weiqi Dai, and Deqing Zou. Theory and methodology of research on cloud security. *SCIENCE CHINA Information Sciences*, 59(5):050105:1–050105:3, 2016.
13 Angsheng Li, Xuechen Li, Yicheng Pan, and Wei Zhang. Strategies for network security. *SCIENCE CHINA Information Sciences*, 58(1):1–14, 2015.
14 Hongtao Li, Jianfeng Ma, and Shuai Fu. A privacy-preserving data collection model for digital community. *SCIENCE CHINA Information Sciences*, 58(3):1–16, 2015.
15 Xuezhen Huang, Jiqiang Liu, Zhen Han, and Jun Yang. Privacy beyond sensitive values. *SCIENCE CHINA Information Sciences*, 58(7):1–15, 2015.
16 Bin Liu, Fei Gao, Wei Huang, Dan Li, and Qiaoyan Wen. Controlling the key by choosing the detection bits in quantum cryptographic protocols. *SCIENCE CHINA Information Sciences*, 58(11):1–11, 2015.
17 Ping Zhen, Geng Zhao, Lequan Min, and Xin Jin. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimedia Tools Appl.*, 75(11):6303–6319, 2016.
18 Hongjun Liu, Xingyuan Wang, and Abdurahman Kadir. Image encryption using DNA complementary rule and chaotic maps. *Appl. Soft Comput.*, 12(5):1457–1466, 2012.
19 Xiaopeng Wei, Ling Guo, Qiang Zhang, Jianxin Zhang, and Shiguo Lian. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, 85(2):290–299, 2012.

20 Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, 52(11-12):2028–2035, 2010.

21 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. In *2015 Chinese Automation Congress (CAC)*, pages 1159–1164, Nov 2015.

22 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. In *The 6th International Conference on Applications and Techniques for Information Security (ATIS), Beijing, China, 4-6 November, 2015*, pages 74–85, 2015.

23 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. In *The 6th International Conference on Applications and Techniques for Information Security (ATIS), Beijing, China, 4-6 November, 2015*, pages 3–12, 2015.

24 Xin Jin, Sui Yin, Xiaodong Li, Geng Zhao, Zhaohui Tian, Nan Sun, and Shuyun Zhu. Color image encryption in ycbcr space. In *8th International Conference on Wireless Communications & Signal Processing, WCSP 2016, Yangzhou, China, October 13-15, 2016*, pages 1–5, 2016.

25 Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 344–371, 2011.