Selective Encryption for 3D Printing Model in DCT Domain

Giao N. Pham[1], Jin-Hyeok Park[1], Oh-Heum Kwon[1], Ha-Joo Song[1]
[1]Dept. of IT Convergence & Application Engineering
Pukyong National University, Pusan, South Korea
ngocgiaofet@gmail.com, detdetplus@naver.com,
ohkwn@pknu.ac.kr, hjsong@pknu.ac.kr

Suk-Hwan Lee[2], Kwang-Seok Moon[3], Seok-Tae Kim[4], Yeong-Rak Choi[5], Ki-Ryong Kwon[1]
[2]Dept. of Information Security, Tongmyong University
[3]Dept. of Electronics Engineering, [4]Dept. of Information and Communications, Pukyong National University
[5]Social Network Communication
skylee@tu.ac.kr, ksmoon@pknu.ac.kr, krkwon@pknu.ac.kr

***Abstract* - In this paper, we present a selective encryption algorithm for 3D printing models in the frequency domain of discrete cosine transform to prevent illegal copying, access in the secured storage. The facet data of 3D printing model is extracted to construct a three by three matrix that is then transformed to the frequency domain of discrete cosine transform. The proposed algorithm is based on encrypting the DC coefficients of matrixes of facets in the frequency domain of discrete cosine transform in order to obtain the encrypted 3D printing model. Experimental results verified that the proposed algorithm is very effective for 3D printing models. The entire 3D printing model is altered after the encryption process. The proposed algorithm also provide a better method and more security than previous methods.**

Keywords* - *3D printing data, 3D printing security, Selective Encryption, DCT.

I. INTRODUCTION

Recent years, three dimension (3D) printing is widely used in many areas of life as healthcare, industry, automotive and many sectors [1]. Due to the fact that the benefits of 3D printing is enormous in all domain and the price of a 3D printer is not expensive, the individual user can buy a 3D printer and download 3D models on Internet to print out physical 3D objects without any permission from the original providers. Moreover, some special models and anti-weapon models must be secured from un-authorized users. Thus 3D printing data should be encrypted before being stored and transmitted in order to ensure the access and to prevent illegal copying.

For meeting to issues above, we would like to propose a selective encryption algorithm in DCT domain for 3D printing models in this paper. The data format of 3D printing is the 3D triangle mesh. The main content of the proposed algorithm is to extract facets from 3D triangle mesh, and three vertices of each facet is then used to construct a three by three (3x3) dimensional matrix. The proposed algorithm is based on encrypting the DC coefficients of the constructed matrixes in DCT domain [2] to generate the encrypted 3D triangle mesh. To clarify the proposed algorithm, we organize our paper as follow: In Sec. 2, we look into previous encryption techniques for 3D models and explain the relation of 3D triangle mesh to the proposed algorithm. In Sec. 3, we show the proposed algorithm in detail. Experimental results and the evaluation of the proposed algorithm will be shown in Sec. 4. Sec. 5 shows the conclusion.

Corresponding author: Prof. Ki-Ryong Kwon, Pukyong National University, Busan, South Korea.

II. RELATED WORKS

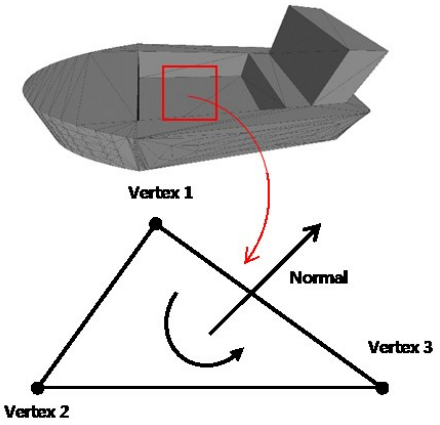

Figure 1. Structure of 3D Triangle Mesh.

Marc et al. [3] proposed a method to encrypt 3D objects based on geometry preserving. The key idea of this method only permute some facets of a 3D object. It is not effective to the various formats of 3D printing data. Moreover, reconstruction cannot fully restore the encrypted 3D objects and the security of this method is very low. Cai et al. [4] proposed an encryption approach for CAD models, which is based on geometric transformation encryption mechanisms of features of CAD models. The key content of this approach is centered on an Enhanced Encryption Transformation Matrix, which is characterized parametric, randomized and self-adaptive for feature encryption. This method only changes a little the shape of 3D CAD models.

Currently, 3D printing technology often uses 3D triangle meshes [5, 6] to print physical 3D objects. A 3D triangle mesh is a set of facets. Each facet contains three vertices (a triangle) and a normal vector (see Fig. 1). Each vertex is presented by three coordinates x, y and z. Due to the fact that the normal vector of a facet does not determine the shape of a 3D triangle mesh. So, in order to encrypt a 3D triangle mesh we only extract facets and encryption all 3D triangles of a 3D triangle mesh by the secret key.

III. THE PROPOSED ALGORITHM

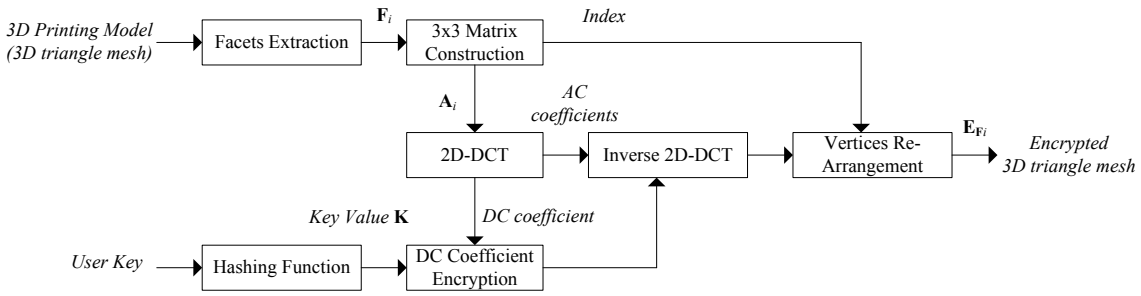

Figure 2. The proposed algorithm.

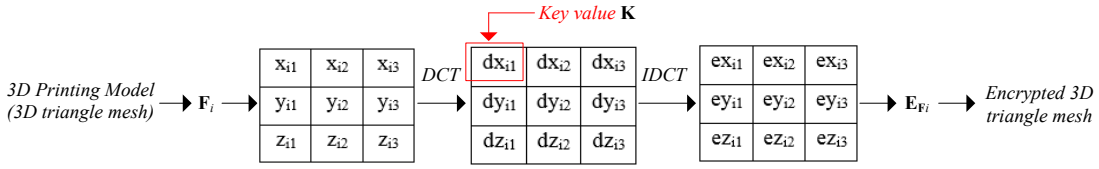

Figure 3. Selective encryption process in DCT domain of a 3D triangle mesh.

The proposed algorithm is described in Fig. 2. Facets are firstly extracted from 3D triangle mesh and three vertices of each facet is used to construct a 3x3 matrix as shown in Fig. 3. These matrixes are then transformed to DCT domain. In DCT domain, DC coefficients are selected and encrypted by a secret key value. The secret value is generated by a hashing function with a user's key input. After the DC coefficients encryption process in DCT domain, DCT coefficients which include the encrypted DC coefficient and AC coefficients, are performed inverse DCT in order to change all coefficients one more time. Finally, the coefficients of the inverse DCT process will be re-arranged to generate the encrypted facet. The vertices re-arrangement process uses the index of 3x3 matrix that is previously constructed. The encrypted 3D triangle mesh is a set of the encrypted facets.

As the mention above, a 3D triangle mesh contains a set of facets. Each facet includes three vertices. Each vertex is presented by x, y and z coordinates. We consider a 3D triangle mesh $\mathbf{M} = \{\mathbf{F}_i | i \in [1, |\mathbf{M}|\}$ with $|\mathbf{M}|$ is the cardinalities of a 3D triangle mesh; $\mathbf{F}_i = \{v_{i1}, v_{i2}, v_{i3}$ and $\mathbf{n}_i\}$ is indicated the i^{th} facet with three vertices $\{v_{i1}, v_{i2}, v_{i3}\}$ and the normal vector $\mathbf{n}_i$. Due to the fact that the normal vector of a facet does not determine the shape of 3D triangle mesh, we briefly consider the facet $\mathbf{F}_i$ includes three vertices as $\mathbf{F}_i = \{v_{i1}, v_{i2}, v_{i3} | i \in [1, |\mathbf{M}|]\}$. The encrypted facet $\mathbf{E}_{\mathbf{F}i}$ includes three encrypted vertices e_{i1}, e_{i2} and e_{i3}. The encrypted 3D triangle mesh $\mathbf{E}_M$ is a set of the encrypted facets. Fig. 3 show the encryption process in the DCT domain of a 3D triangle mesh.

IV. Experimental Results

We experimented the proposed method with 3D triangle meshes. The format of 3D triangle meshes is STL file, VRML file [5, 6]. In order to evaluate the proposed method, we perform visualization experiments, evaluate the security and computation time of the proposed method. The experimental results of visualization are shown in Fig. 4. The number of facets in each 3D triangle mesh is different. After the selective

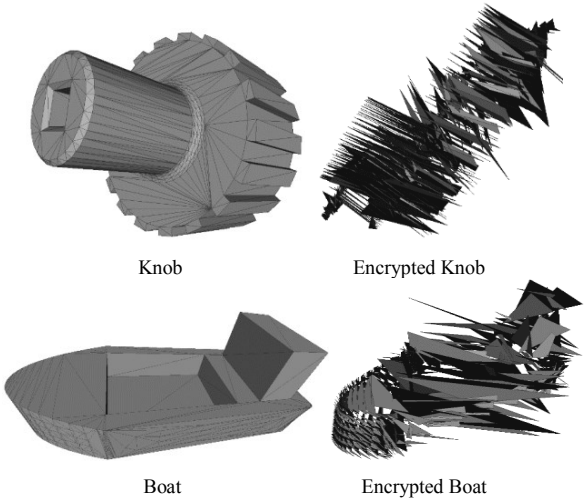

Figure 4. Experimental results of visualization.

-encryption process, facets are distorted into small facets or big facets and positioned disorderly. This leads to the shape of 3D triangle meshes is changed. Consequently, the content of 3D triangle meshes is completely altered after the selective encryption process. Pirates or un-authorized users cannot extract or view the content of 3D triangle meshes.

To evaluate the security of the proposed method, we will analyze the entropy of the encrypted 3D triangle mesh. If the entropy is high, the security will be high. Fig. 5 show the entropy of the proposed method compared to the entropy of previous methods according to the number of facets. The entropy of the proposed method is always higher than the entropy of previous methods. Consequently, the proposed method is better and more security than previous methods.

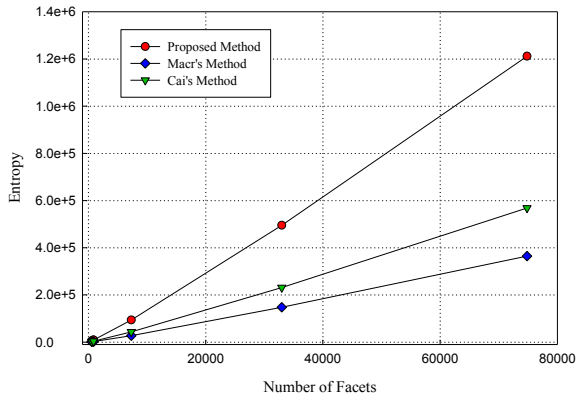

Figure 5. Entropy of the proposed method according to the number of facets.

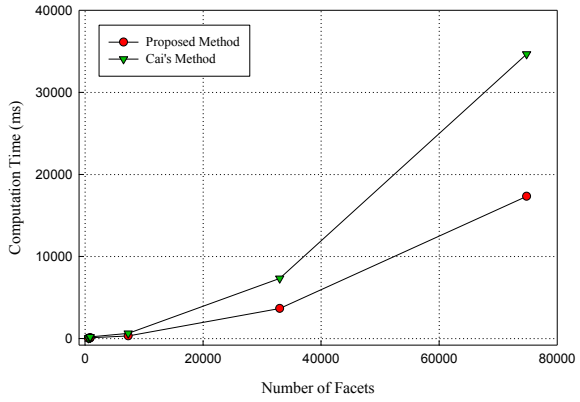

Figure 6. Computation time according to the number of facets.

The computation time of the proposed method is also dependent on the number of facets. If the number of facets is small, the computation time is small and otherwise. In Marc's method [3], he did not show the computation time, so we could not compare Marc's methods with our method. In Cai's method [4], he only analyzes the complexity time. The computation time of Cai's method is dependent on the time of valid check CAD model, time of feature encryption and time of CAD model encryption. He concluded that his method is enough to meet user's requirements. With the dependent on three processes in Cai's method, we consider and evaluate that the computation time of Cai's method is greater at least two the computation time of our method. Compared to Cai' method, our method is faster than Cai's method. Fig. 6 show the computation time of the proposed method and Cai's method according to the number of facets.

V. CONLUSION

In this paper, we proposed a selective encryption algorithm for 3D printing models in DCT domain. The proposed algorithm is very more effective than previous methods. It is also responsive to the various formats of 3D printing model. It provides a better solution and is more security than the previous proposed methods. In future, we improve the proposed algorithm and apply it to the secured storage and transmission systems.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (No. 2016R1D1A3B03931003, No. 2017R1A2B2012456) and he Korea Technology and Information Promotion Agency for SMEs (TIPA) grant funded by the Korea government (Ministry of SMEs and Startups) (No. C0407372), and the MSIP (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2017-2016-0-00318) supervised by the IITP (Institute for Information & communications Technology Promotion).

REFERENCES

[1] 3D Systems Circle Rock Hill, "White paper: How 3D Printing works, The Vision, Innovation and Technologies behind Inkjet 3D Printing," Jan., 2012.

[2] G. Strang, "The Discrete Cosine Transform," Society for Industrial and Applied Mathematics, Vol. 41, No. 1, pp. 135–147, 1999.

[3] E. Marc, Y. Maetz, and D. Gwenael, "Geometry-preserving Encryption for 3D Meshes," in Proc. of Conference: Compression at Representation Signal Audio, pp.7-12, Nov. 2013.

[4] X.T. Cai, F.Z. He, W.D. Li, X.X. Li, and Y.Q. Wu, "Parametric and Adaptive Encryption of Feature-Based Computer-Aided Design Models for Cloud-based Collaboration," Integrated Computer-Aided Engineering, vol. 24, pp. 129–142, 2017.

[5] STL format in 3D printing, https://all3dp.com/what-is-stl-file-format-extension-3d-printing/, accessed 2017.

[6] The Virtual Reality Modeling Language, http://www.cacr.caltech.edu/~slombey/asci/vrml/, accessed 2017