WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# 2D DCT-Based Encryption Method for 3D Printing Model

***Giao N. Pham[1], and Binh A. Nguyen[2]***

[1]Dept. of Computing Fundamentals, FPT University, Hanoi, Vietnam
[2]ICT Department, FPT University, Hanoi, Vietnam
E-mail: giaopn@fe.edu.vn, binhnase04865@fpt.edu.vn

ABSTRACT

This paper presents an encryption algorithm for 3D printing models in the frequency domain of discrete cosine transform. Facet data of 3D triangle mesh 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 generate the encrypted 3D triangle mesh. 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 decrypting error is approximate to zero. The proposed algorithm is provided a better method and more security than previous methods.

## 1. Introduction

Three dimension (3D) printing is a process of making 3D solid objects from a digital file and widely used in many areas of life [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, users can buy a 3D printer and download 3D printing models from Internet to print out objects without any permission from the original providers. Moreover, some special models and anti-weapon models must be secured from un-authorized users. Therefore, 3D printing models should be encrypted before being stored and transmitted in order to ensure the access and to prevent illegal copying.

For meeting to above issues, we would like to propose a random encryption algorithm for 3D printing models in this paper. The data format of 3D printing models is the 3D triangle mesh [2, 3]. Each facet of 3D triangle mesh is distorted by the geometric transformation process and three vertices of that facet are used to construct a three by three (3x3) dimensional matrix. The coefficients of the constructed matrix are randomly encrypted by the random numbers of another 3x3 matrix to generate the encrypted 3D triangle mesh. To clarify the proposed algorithm, we organize our paper as follow. In Sec. 2, we show the proposed algorithm, and experimental results. Sec. 3 will show conclusion.

## 2. The Proposed Method& Experimental Results

The proposed method is described in Fig. 1. In DCT domain, the DC coefficient is encrypted by the key value **K**. The key value **K** is generated by the SHA-512 hashing algorithm [4] that use a user's key input. The length of each key value is 512 bits. Experimental results are shown in Fig. 2.The content of 3D printing models is completely altered after the encryption process. Pirates or un-authorized users cannot extract or view the content of 3D triangle meshes.

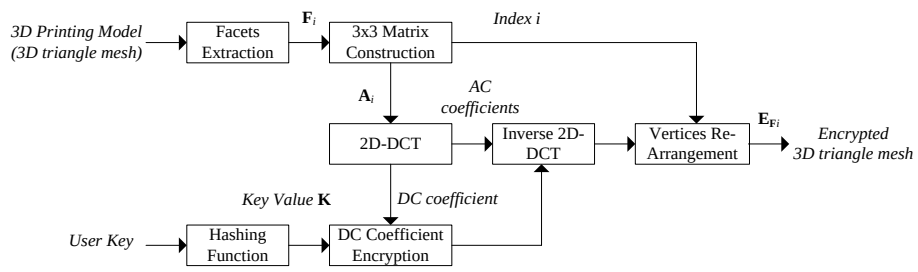
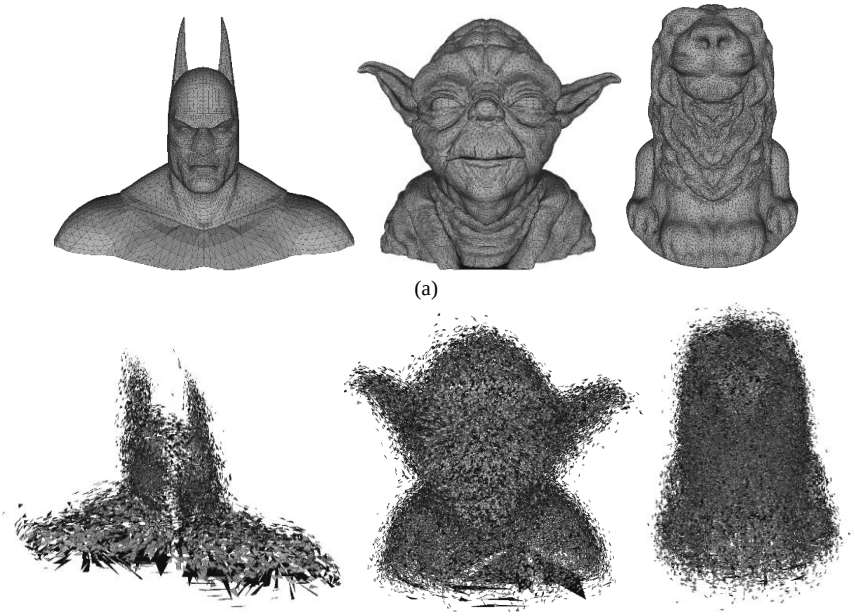



Figure 1. The Proposed Method.

**An Encryption Method For 3D Printing Model**



(a)

(b)

Figure 2. (a) Original 3D printing models and (b) Encrypted 3D printing models.

## 3. Conclusion

In this paper, we proposed an effective 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 work is supported by FPT University, Hanoi, Vietnam

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

[3] The VRML Consortium Incorporated, VRML format document, 1997.

[4] RSA Lab., *Password-Based Cryptography Standard*, Oct. 2006.