

Projet : Ultimate 3D Crypto-Compressor

Sujet #1 Crypto-compression d'objets 3D

Lien Git : <https://github.com/BarriolRemy/Ultimate-3D-Crypto-Compressor>

I. Etat de l'art des méthodes de compression d'objets 3D et des méthodes de chiffrement d'objets 3D

A. Compression d'objet 3D

Il existe un grand nombre de manières de compresser un objet 3D. Comme nous pouvons le voir dans l'image ci dessous, tirés de “*3D mesh compression: survey, comparisons and emerging trends*”¹, il existe plusieurs ensembles d'algorithmes qui ont ce but.

Chaque ensemble d'algorithmes sera adapté à certains contextes plus que d'autres.

Les algorithmes *Single-rate* auront pour but de compresser l'ensemble de l'objet, et l'objet suite à sa décompression sera similaire ou presque. Ces algorithmes vont beaucoup dépendre de la manière dont l'objet est structuré. En effet, certains objets seront seulement constitués de triangles quand d'autres ne seront pas uniquement composés de triangles comme faces. Certains algorithmes seront donc élaborés pour certains types d'objet précisément.

Les algorithmes “*Progressive*”, permettent quant à eux de pouvoir visualiser l'objet sans que l'on ait nécessairement la totalité des données. Il est possible de reconstruire l'objet suivant plusieurs niveaux de détails.

Les algorithmes “*Random accessible*”, quant à eux, permettent de décompresser seulement certaines parties de l'objet que l'on veut visualiser, dans le cas où d'autres parties ne nous intéressent pas. Tout l'avantage sera donc de pouvoir décompresser seulement les parties intéressantes pour l'utilisateur et contrairement aux algorithmes précédents qui nécessitent de décompresser l'ensemble du modèle.

Les algorithmes “*Progressive random accessible*” permettent tout simplement d’avoir plusieurs niveaux de détails comme pour les algorithmes Progressive mais seulement sur certaines parties comme pour les algorithmes “*Random accessible*”.

Les algorithmes “*Mesh Sequence Compression*” concernent quant à eux les objets comportant beaucoup de données en plusieurs frames, comme par exemple des animations 3D. Les séquences de mesh auront des cas plus particuliers puisque qu’il y aura une cohérence (ou non dans certains cas) entre chaque frame, il y aura donc des moyens d’exploiter cela.

La figure ci-dessous montre non seulement ces différents ensembles, mais plus précisément une liste d’algorithmes précis produites ainsi qu’une spécialisation méthodique de ces dits algorithmes.

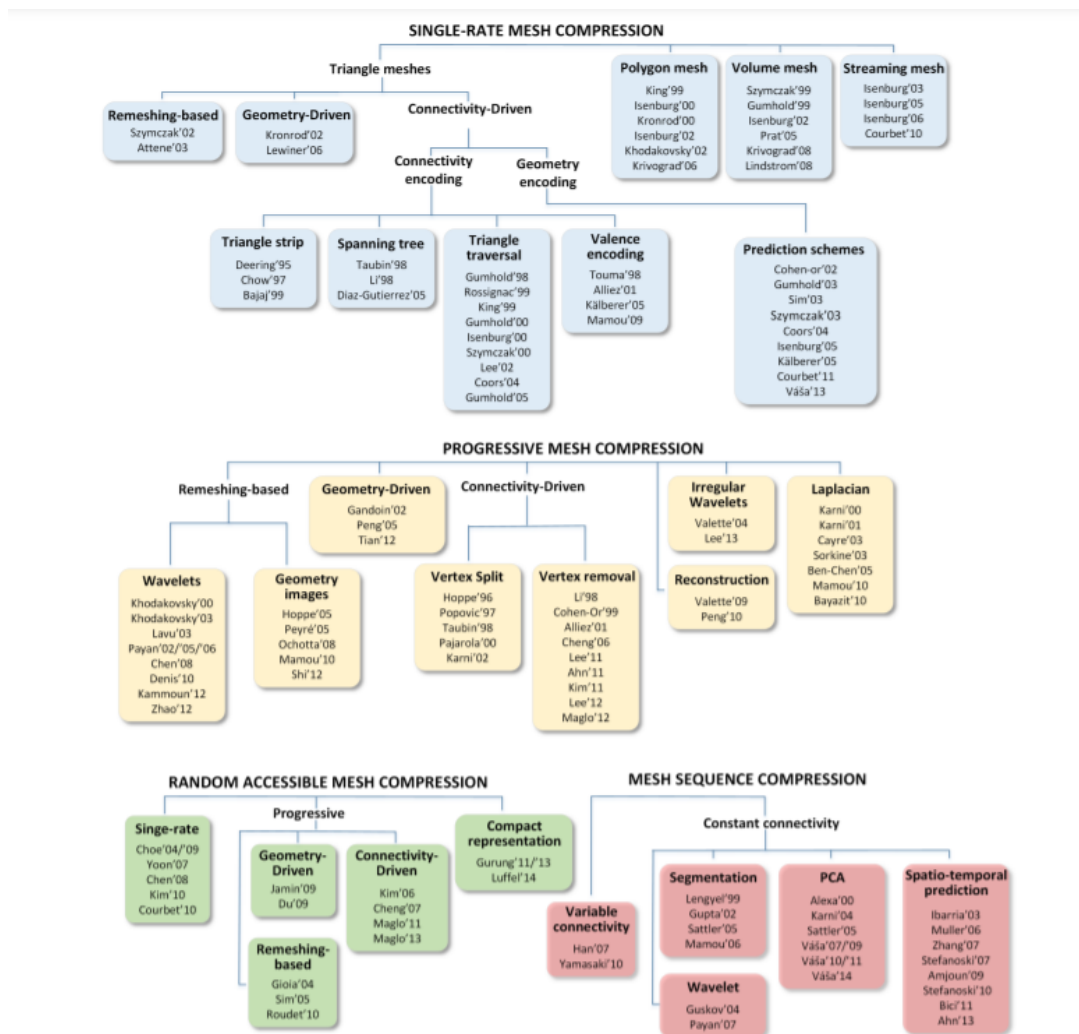


Fig. 1. Taxonomy of 3D mesh compression techniques.

Fig. 1. Taxonomy of 3D mesh compression techniques from “3D mesh compression: survey, comparisons and emerging trends”¹

Le document dont nous tirons cette image nous permet d'accéder facilement à un grand ensemble d'articles décrivant les algorithmes, qui possède plus de huit pages de bibliographies.

B. Mesure de qualité

Puisque nous implémenterons peut être un algorithme de compression pouvant provoquer des pertes par rapport à notre objet de base, alors ils nous faudra des moyens de mesurer la qualité d'un modèle décompressé par rapport aux modèles de base.

Grâce à l'article *Assessing Visual Quality of 3D Polygonal Models*², nous allons pouvoir tester, suivant nos cas (certaines mesures ne s'appliquent que dans certains cas), la qualité de nos compressions et ainsi mesurer les pertes provoquées par notre/nos algorithmes.

C. Chiffrement d'objet 3D

Concernant le chiffrement, nous pouvons nous porter vers plusieurs solutions.

Nous pouvons, par exemple, nous porter sur les algorithmes de chiffrement asymétrique comme le RSA. Comme le suggère l'article *An asymmetric and optimized encryption method to protect the confidentiality of 3D mesh model*³, il n'est pas possible d'utiliser directement le RSA sur un modèle 3D comme sur une image ou un texte, puisque nous manipulons des coordonnées 3D, donc des floats. La méthode se reposera donc sur le fait d'effectuer une transformation en cosinus discret pour ainsi normaliser ces valeurs pour avoir des entiers, sur lequel nous pourrons appliquer le RSA, pour obtenir le modèle crypter, nous appliquerons une normalisation inverse et appliquerons une transformé inverse pour obtenir les coordonnées du modèles chiffré. Cette méthode va plus globalement chiffrer les faces de l'objet, en chiffrant les vertices de groupé par la face qu'ils dessinent.

L'article *Homomorphic Encryption-Based Robust Reversible Watermarking for 3D*⁴ explore quant à lui une autre solution, il va premièrement utiliser le cryptosystem proposé par Pascal Paillier en 1999. Dans cette méthode, nous allons diviser le modèle par patches et ensuite chiffrer ces patches (contrairement à la méthode précédente qui chiffré les faces). L'article a aussi pour rôle d'intégrer un tatouage numérique au modèle 3D, notre sujet ne se portant pas sur cela, nous ne nous intéresserons pas à cette partie.

L'article *A Novel Reversible Data Hiding Method for 3D Model in Homomorphic Encryption Domain*⁵ utilise la même méthode que celle précédente,

à la différence où les vertices ne seront pas regroupés par patches à la manière précédente, ils seront classifiés suivant un certain algorithme détaillé dans l'article.

L'article *Polygon Mesh Encryption Based on 3D Lorenz Chaotic Map* ⁶ quant à lui, décrit une méthode de chiffrement utilisant la 3D Lorenz Chaotique Map pour chiffrer les vertices de l'objet 3D.

Nous pourrions aussi explorer l'idée d'utiliser les méthodes de chiffrement applicables sur des images si nous choisissons la méthode de compression Geometry Image.

II. Bibliographie

¹ A. MAGLO, G. LAVOUÉ, F. DUPONT, C. HUDELOT (2013) 3D mesh compression: survey, comparisons and emerging trends. *ACM Computing Surveys*, Vol. 9, No. 4, Article 39.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.687.74&rep=rep1&type=pdf>

N. A. DODGSON, M. S. FLOATER, M. A. SABIN (2005) Advances in Multiresolution for Geometric Modelling. <https://link.springer.com/content/pdf/10.1007%2Fb138117.pdf>

² A. BULBUL, T. CAPIN, G. LAVOUÉ, M. Preda (2011) Assessing Visual Quality of 3D Polygonal Models. *IEEE Signal Processing Magazine*, Vol. 28, Issue 6.
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.420.3997&rep=rep1&type=pdf>

³ YAQIAN LIANG, FAZHI HE, HAORAN LI (2019) An asymmetric and optimized encryption method to protect the confidentiality of 3D mesh model. *Advanced Engineering Informatics*, Vol 42.
https://www.sciencedirect.com/science/article/pii/S1474034619300679?casa_token=adE52OhUdaoAAAAA:igtDQWZlthwImSCjrGXRdcqv6-6Uj5DunQD6D5haT9LfEQfJwXgsNiSptm8WlTb0L3XtNqaLQ

⁴ LI LI, SHENGXIAN WANG, SHANQING ZHANG, TING LUO, CHING-CHUN CHANG (2020) Homomorphic Encryption-Based Robust Reversible Watermarking for 3D Model. *Symmetry*. <https://www.mdpi.com/2073-8994/12/3/347>

⁵ TING LUO, LI LI, SHANQUIN ZHANG, SHENXIAN WANG, WEI GU (2021) A Novel Reversible Data Hiding Method for 3D Model in Homomorphic Encryption Domain. *Symmetry*. <https://www.mdpi.com/2073-8994/13/6/1090>

⁶ NASHWAN ALSALAM ALI, ADBUL MONEM S. RAHMA, SHAIMAA H. SHAKER (2021) 3D Polygon Mesh Encryption Based on 3D Lorenz Chaotic Map. *International Journal of Interactive Mobile Technologies*, Vol 15, No 15
https://www.researchgate.net/profile/Shaimaa-Hameed/publication/353829271_3D_Polygon_Mesh_Encryption_Based_on_3D_Lorenz_Chaotic_Map/links/611a75b61ca20f6f86275721/3D-Polygon-Mesh-Encryption-Based-on-3D-Lorenz-Chaotic-Map.pdf