Crypto-compression d'objets 3D
CR 1

Master 2 Informatique, IMAGINE
Université de Montpellier
2021 - 2022
GITHUB:https://github.com/EmeryBV/Crypto-compression_of_3D_objects

Équipe :
- Charles Sayamath
- Emery Bourget-Vecchio

UNIVERSITÉ DE MONTPELLIER

FACULTÉ DES SCIENCES MONTPELLIER

Etat de l’art

Etat de l’art **2**
Représentation de maillage 3D 3
Méthode de compression de maillage 3D 4
Compression mono-résolution. 4
Codage de la connectivité 4
Triangle strip 4
Spanning tree 5
Parcours des triangles 5
Encodage par valence 6
Progressive compression 9
Contraction d’arêtes et expansion de sommets 9
Décimation de sommets 10
Compression de maillage irrégulier 11
Remaillage 12
Compression par ondelette 12
Méthodes de chiffrement de maillage 3D 13
Chiffrement chaotique 13
Chiffrement sélectif 14
Références 15
Compression 15
Chiffrement 16

- **Représentation de maillage 3D**

Un maillage est composé des éléments géométriques suivants :

- les sommets qui sont les éléments de bases d'un maillage
- les arêtes qui sont des segments reliant deux sommets différents
- les faces qui sont des polygones composés par les sommets et arêtes

Un maillage va être découpé en différentes catégories d'informations :

- La géométrie du maillage qui correspond à la position dans le monde de chaque sommet du maillage
- La connectivité du maillage qui correspond aux relations entre les éléments du maillage qui permettent de le former
- Une catégorie optionnelle contenant les informations de couleurs, normales, etc.

- # Méthode de compression de maillage 3D

Les maillages 3D peuvent être considérés comme la représentation la plus populaire de volume et de surface et sont utilisés sur une variété d'appareils possédant des contraintes de performances bien différentes.

Dans un besoin de réalisme et de fidélité, ces derniers deviennent au cours du temps de plus en plus détaillés et complexes. Cela s'accompagne ainsi d'une augmentation de leur volume de données et peut alors poser des problèmes dus aux contraintes des différents supports sur lesquels ils sont affichés (mémoire, vitesse, etc.).

Pour résoudre ces problèmes, des méthodes de compression de maillage 3D ont été développées afin de réduire le volume de données requis pour les représenter, facilitant ainsi le stockage et la transmission de ceux-ci.

Ces méthodes peuvent être regroupées sous trois catégories.

I. Compression mono-résolution.

La compression mono-résolution est une famille d'algorithmes permettant de supprimer les redondances d'un maillage. Dans la grande majorité d'entre eux, la connectivité et la géométrie sont encodées séparément mais pas indépendamment.

1. Codage de la connectivité

Il existe actuellement 4 grandes familles d'algorithmes de compression de la connectivité.

1. Triangle strip

La connectivité d'un maillage est représentée sous forme de liste cyclique des indices de sommet; cette représentation est extrêmement redondante. La première personne à avoir proposé une méthode pour pallier cela est **Deering** en 1995. Sa méthode consiste à découper le maillage sous forme de bande triangulaire (triangular strips). Pour cela, il ordonne les sommets dans une liste telle que chaque sommet de cette liste forme un triangle avec ses deux prédécesseurs.

En ne conservant que la façon dont on passe d'un triangle à un autre, on réduit ainsi fortement l'entropie de la connectivité initiale.

Deering remarque également que dans les triangles strip, une grande partie des sommets intérieurs étaient encodés deux fois. Il a donc créé une liste qui contient les 16 derniers éléments utilisés, cela a permis de réduire le coût des sommets réutilisés.
Les résultats expérimentaux ont montré que les résultats s'étendaient de 3.3 à 9.8 bpv

2. *Spanning tree*

Tutte a montré en 1962 qu'un graphe planaire, représentant la connectivité d'un maillage triangulaire, peut être codé avec un minimum de 3.24 bits par sommets. Cette borne théorique est la référence en ce qui concerne la compression de la connectivité.

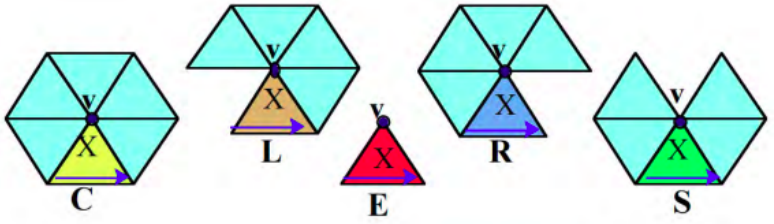
La connectivité d'un maillage peut être modélisée comme celle d'un graphe. En effet, les sommets peuvent correspondre aux nœuds qui sont liés par des arêtes pour former des faces. Cette analogie a permis d'appliquer des méthodes venant de la théorie des graphes afin de les appliquer dans la compression de la connectivité de maillage.
C'est ainsi qu'en 1998, **Taubin et Rossignac** sont parvenus à trouver un algorithme grâce à deux arbres couvrants.
Ici nos deux arbres couvrants sont composés d'une part des sommets et d'une autre part des triangles. Dans ce cas, il y a 2 fois plus de triangles que de sommets.
Cette méthode garantit un coût compris entre 2.5 et 6.

3. *Parcours des triangles*

Le but ici est de compresser un maillage à l'aide de l'approche de région croissante (region growing) en générant un arbre couvrant de triangle composé de bande. Pour générer de tels arbres, l'algorithme traite itérativement les triangles du maillage avec un premier parcours en largeur. À chaque étape de la compression, certaines faces ont déjà été parcourues ou non.
L'avantage ici est la simplicité de ce type d'algorithme, l'arbre couvrant est facile à générer et contient directement tous les éléments du maillage.

The Cut-Border machine a été le premier algorithme développé en 1998 par **Gumhold et Straßer**. Leur méthode consiste à développer les bords formés par le triangle initial en parcourant itérativement les triangles adjacents.

Puis en 1999, **Rossignac** développe l'algorithme Edgebreaker qui garantit un coût de 4 bpv.
Cette méthode se base sur l'utilisation d'une porte. Cette dernière est le point d'entrée à une face par une de ses arêtes. En partant d'une porte donnée, la configuration du sommet opposé offre cinq possibilités.



- Le patch est complet, on code donc un C.
- La porte de gauche ne mène à aucune face (inexistante ou déjà traitée), on code donc un L.
- Si les deux portes adjacentes ne mènent à aucune face, on code un E.
- La porte de droite ne mène à aucune face, on code un R.
- Si le patch n'est pas complet mais que les deux portes adjacentes sont présentes, on code un S

4. Encodage par valence

Un maillage contient approximativement 2 fois moins de sommets que de triangles. Il est donc plus avantageux de parcourir un graphe en décrivant la valence de chacun des sommets que de parcourir l'entièreté des triangles. Les premières personnes à avoir utilisé cette approche sont en 1998. Le principe de leurs méthodes est de considérer chaque arrêté en frontière formé par le triangle initial puis d'étendre itérativement cette frontière afin d'ajouter les sommets adjacents. La connectivité est encodée par la valence des sommets insérés.
De plus, la liste générée des valences des sommets peut être facilement encodée par un codeur entropique (2.3bpv).

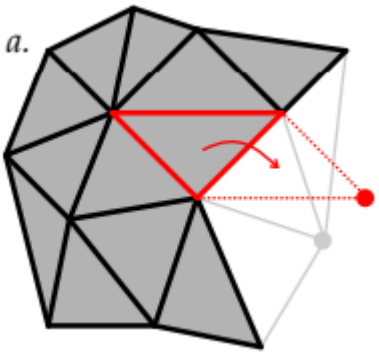
C'est aujourd'hui encore l'un des meilleurs algorithmes pour coder la connectivité.

2. <u>Codage de la géométrie</u>

La compression de la géométrie d'un maillage, c'est-à-dire les coordonnées des sommets, suivent à peu près tous le même type d'enchaînement:

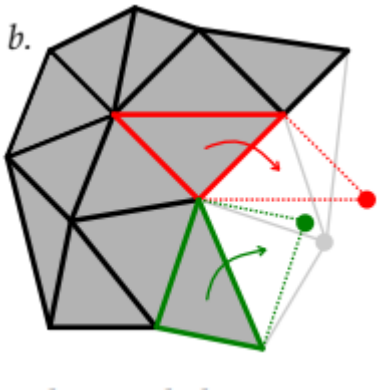
Quantification: Les coordonnées des sommets sont généralement des nombres flottants. Si l'on prend deux sommets proches, les premières décimales de leurs coordonnées seront normalement les mêmes, mais à un certain moment, les derniers décimales seront sûrement totalement chaotiques. Ainsi l'entropie pour coder ce style d'information sera très élevé car il sera presque impossible de réaliser de la prédiction. Pour pallier ce problème, la solution est de rendre nulles toutes les décimales trop superflues, c'est la quantification. En appliquant cette quantification, on a donc une compression avec perte, cependant cela n'a pas de grand impact puisque les données retirées ont des valeurs tellement faibles que cela reste négligeable.

Prédiction: La prédiction géométrique permet à partir de sommets voisins de pouvoir prédire la position d'un sommet. La méthode la plus populaire est la prédiction par parallélogramme. Le but étant de d'ajouter un sommet à un triangle afin de former un parallélogramme comme dans le schéma suivant.



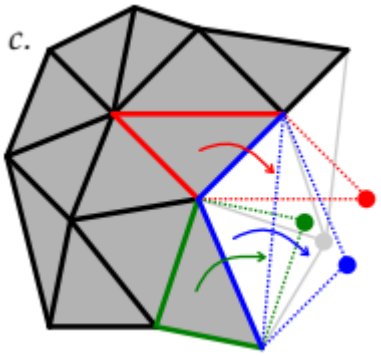
Prédiction par parallelogram

Sim et al ont développé en 2005 cette prédiction en faisant la moyenne de prédiction par parallélogramme si cela est possible. Cette méthode peut être utilisée 75% du temps.



Prédiction avec double parallélogrammes

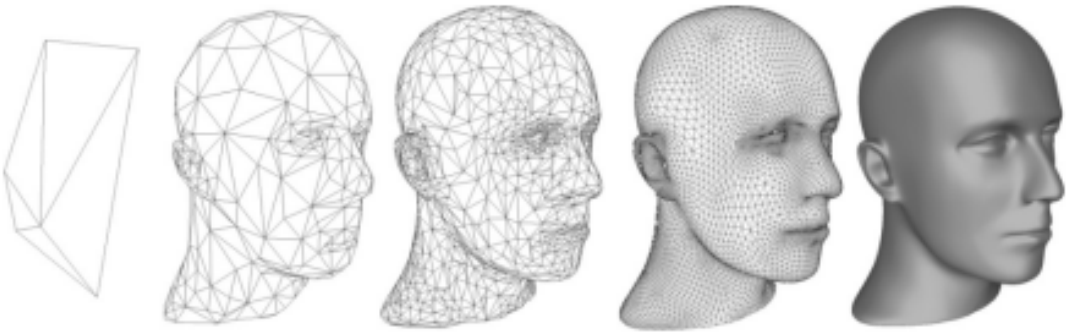
Enfin “Freelence coder” utilise quant à lui la prédiction de 3 parallélogrammes dont 2 standards et un nouveau qui représente les arêtes extérieures deux parallélogrammes standards.



Freelence prediction

Ainsi beaucoup d'algorithmes se base sur cette méthode comme **Cohen-Or** en 2002 qui présente le “multiaway prediction” qui consiste à prédire la position du nouveau sommet à partir de la prédiction d’un maximum de parallélogramme basé sur les sommets déjà encodé.

II. Progressive compression

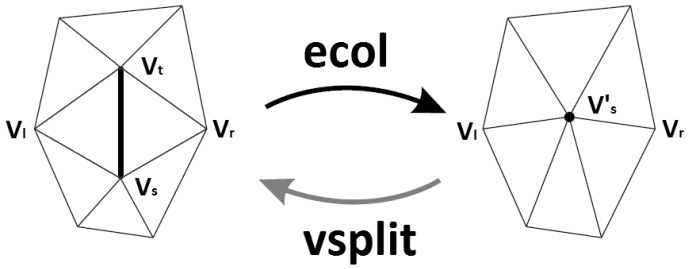


Compression progressive d'un maillage

L'idée des méthodes de compression progressives consiste à simplifier incrémentalement un maillage (selon différentes techniques de simplification de maillage) tout en stockant les informations nécessaires à la reconstruction de ceux-ci lors de la phase de décompression. La simplification est effectuée jusqu'à l'obtention d'un maillage M_0 sur lequel va se baser la phase de décompression.

On obtient alors un maillage très simplifié contenant en plus des bits permettant l'ajout successif de détail. Ainsi, il va être possible de reconstruire successivement le maillage originel en raffinant continuellement M0 à un niveau de détail de plus en plus grand au fur et à mesure de la décompression.

1. Contraction d'arêtes et expansion de sommets



Opérations edge-collapse/vertex split

- La première méthode de compression progressive a été introduite par **Hoppes** [1996] et se base sur les opérations de contraction d'arêtes (edge collapse) et son inverse, l'expansion de sommets (vertex split).

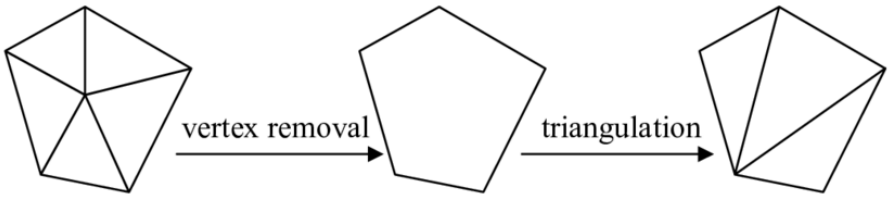
  Ainsi, la compression du maillage va consister à contracter des arêtes en fonction d'une métrique minimisant l'erreur dûe à la décimation de l'arête. Les arêtes sont ainsi pondérées à l'aide de cette valeur et celles possédant le poids le plus faible vont être contractées.

L'algorithme encode les index des deux sommets de l'arête contractée ainsi que l'index du sommet résultant à chaque itération.

A l'étape finale, on obtient un fichier composé du maillage simplifié M_0 et des informations nécessaires pour effectuer l'opération inverse de reconstruction de maillage. La méthode permet d'obtenir une compression de l'ordre de 37 bits par sommets avec une quantification de 10 bits.

- D'autres méthodes se basant sur cette première ont pu être développées. **Pajarola et Rossignac** [2000] proposent une méthode dans laquelle est utilisée un arbre de recouvrement (spanning tree) qui stocke les opérations d'expansions de sommets afin d'améliorer la compression de la connectivité. On obtient des résultats de compression de l'ordre de 22 bits par sommets toujours avec une quantification de 10 bits.

2. <u>Décimation de sommets</u>



Décimation de sommet suivi d'une triangulation

Certaines méthodes se basent plutôt sur la décimation de sommet. Cette fois-ci, on supprime des sommets en effectuant par la suite une triangulation de la zone lors de la compression du maillage. Le maillage est reconstruit en y insérant des sommets en s'aidant du barycentre de la zone.

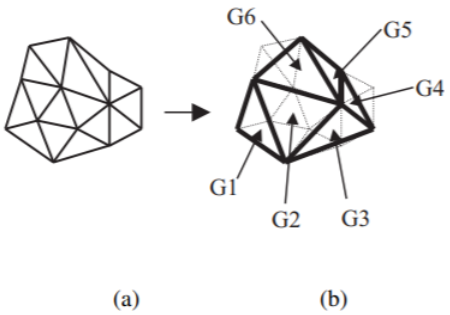
- **Alliez et Desbrun** [2001] se basent sur la notion de valence des sommets, étudiée dans les méthodes de compression mono-résolution, pour simplifier le maillage. A chaque itération, l'algorithme va supprimer les sommets avec une valence inférieure à 6 (supprimer les sommets avec une valence supérieure à ce nombre entraîne une augmentation de la valence des sommets restants) puis effectuer une triangulation de la zone. Une phase de de nettoyage est alors entreprise sur les sommets résultants pour supprimer les sommets avec une valence de 3 afin d'homogénéiser le nombre de valence des sommets.

  La connectivité du maillage est ainsi compressée et encodée sous forme de liste de valence des sommets décimés. La géométrie du maillage est compressée en quantifiant les sommets puis encodée en s'aidant du barycentre de la zone du sommet décimé. La méthode permet d'obtenir une compression de l'ordre de 19 bit par sommets avec une quantification de 12 bits.

- D’autres méthodes plus récentes se basent également sur la notion de valence et offrent une meilleure performance que la précédente en améliorant l’encodage de la connectivité et de la géométrie.
  Lee et al. [2012] part de la méthode précédente et utilise une quantification des sommets adaptative afin d’améliorer la compression de la géométrie.

3. Compression de maillage irrégulier

- **Valette et Prost** [2004] propose une méthode se basant sur l’opération de subdivision inverse sur des maillages irréguliers. Elle consiste à décimer le maillage originel à l’aide de subdivision des faces. A l’aide d’opération de edge-flip sur les faces subdivisées, ces dernières vont être fusionnées entre elles, ce qui va permettre d’obtenir des maillages simplifiés.



Simplification de maillage par subdivision inverse

La connectivité va être encodée à l’aide de certains ensembles de données :

- le type de subdivision effectué sur les faces (4, 3, 2, 1 faces)
- l’information sur les opérations de edge flip effectuées (notamment l’information de si un basculement d’arête a été effectué et la position de l’arête en question)

En s’aidant de ces informations, il va être possible de restituer le maillage initial à partir d’un maillage très simplifié M_0 et des informations de subdivision . La géométrie est encodée à l’aide d’un lifting en ondelette

La méthode permet d’obtenir une compression de l’ordre de 19 bit par sommets avec une quantification de 12 bits.

4. Remaillage

Les méthodes précédentes sont des méthodes ‘fine to coarse’ et se basent sur la simplification d’un maillage originel pour obtenir à la fin un maillage décimé que l’on pourra reconstruire à l’aide d’informations stockées.

Certaines méthodes font néanmoins la réflexion inverse et partent donc d'un maillage décimé pour obtenir à la fin un maillage fidèle à l'originel. Ces méthodes ont alors une approche 'coarse to fine'. Elles sont notamment utilisées dans le cas où la connectivité du maillage n'a pas à être reconstruite parfaitement.

- **Valette et al.** [2009] propose une méthode nommée 'Incremental parametric refinement' se basant sur une génération de maillage avec une approche de Delaunay.

  L'algorithme part d'un maillage préalablement simplifié. A chaque itération de reconstruction, la méthode subdivise si nécessaire les arêtes triées en fonction de leur longueur. Ainsi, l'arête sélectionnée va être subdivisée en y insérant un sommet et une triangularisation va être effectuée à l'aide de ce dernier. Des opérations de basculement d'arêtes vont être effectuées pour correspondre à des propriétés locales de Delaunay.

  Ainsi, pour encoder la connectivité, il suffit de stocker pour chaque arête l'information pour savoir si celle-ci a été subdivisée ou non.

  La géométrie est compressée en utilisant une quantification adaptative des sommets en fonction de la résolution du maillage. La méthode permet d'obtenir une compression de l'ordre de 15 bit par sommets avec une quantification de 12 bits.

5. Compression par ondelette

   Les méthodes de cette catégorie se basent également sur des opérations de remaillage et ont donc des approches 'coarse to fine'. Ainsi, on part d'un maillage très décimé que l'on va par la suite raffiner à l'aide de subdivision.

- **Khodakovsky et al.** [2000] ont ainsi proposé l'utilisation d'ondelette afin de compresser notre maillage. Pour chaque sommet créé par subdivision, on applique un déplacement afin de faire correspondre le maillage actuel avec le maillage original. Ces déplacements sont ainsi stockés en tant que coefficient d'ondelette.

  Ainsi, pour ces méthodes, les données du maillage original vont être remplacées par un maillage décimé ainsi qu'une séquence de coefficient d'ondelette qui vont servir au raffinement de notre maillage.

  Pour encoder ces données, la méthode fait appel à un codage Zerotree. La méthode permet d'obtenir une compression de l'ordre de 8 bit par sommets avec une quantification de 12 bits.

- Diverses méthodes plus récentes utilisent également les ondelettes afin de compresser un maillage 3D. **Kammoun et al.** [2012] d'optimiser la transformée en ondelette afin d'améliorer les performances de codage du maillage.

- ## Méthodes de chiffrement de maillage 3D

Le développement de l'utilisation de modèles 3D s'accompagne également du souci de sécurité et de protection des données. Les domaines du médical, de l'armement et de l'industrie sont en effet très sensibles à ces problèmes-ci. Il est alors nécessaire de pouvoir développer des technologies ayant comme objectif de chiffrer ces données 3D et de les protéger d'éventuelles utilisations malicieuses.

I. Chiffrement chaotique

La plupart des méthodes récentes sont développées à partir de chiffrement basé sur des systèmes de chaos.

La théorie du chaos étudie le comportement des systèmes qui sont très sensibles aux conditions initiales. Un moindre changement dans l'initialisation de l'expérience amènera à des résultats très différents. Utiliser cette propriété dans le domaine du chiffrement est alors intéressant.

Les algorithmes de chiffrement chaotiques fonctionnent à l'aide de deux phases : une phase de confusion et une phase de diffusion qui sont des notions définies par **Shannon** en 1945.

Lors de la phase de confusion, le message d'entrée est modifié de sorte à ce qu'on ait un message non reconnaissable en sortie. Dans le cas de maillage 3D une méthode serait de permuter la position des éléments afin d'obtenir un maillage complètement différent.

Pour ajouter une sécurité supplémentaire, la phase de diffusion fait en sorte de dé-corréler le message en clair et le message chiffré. Modifier un élément du premier va alors avoir un grand impact sur le message résultant. La phase diffusion rend difficile la détection de pattern en dispersant ceux présents dans le message original dans le message chiffré.

Ces phases sont ainsi effectuées un grand nombre de fois afin de pouvoir obtenir un message chiffré de manière robuste.

- **Xingyuan Wang et al.** [2019] proposent par exemple une méthode se basant sur le chiffrement des sommets de maillage triangulaire en utilisant un système de carte chaotique.

Ces cartes chaotiques permettent d'effectuer des substitutions et des mélanges de données pour les chiffrer de manière sécurisée car ces cartes génèrent des données très difficiles à prédire.

L'objet 3D est tout d'abord séparé en une collection d'objets 2D similaire au format d'une image. On chiffre alors ces images grâce à des phases de confusion et de diffusion.

La phase de confusion va insérer des points aléatoires dans le maillage afin de le rendre différent de l'original tout en alternant des opérations de mélanges des éléments à l'aide d'une carte chaotique 1D.

La phase de diffusion va alors s'occuper d'encoder la partie réelle de chacun des sommets à l'aide d'un XOR et d'effectuer un mélange de la partie réelle à l'aide d'une séquence générée par le système chaotique.

- D'autre méthodes se basent sur l'utilisation de carte 3D de chat Arnold (3D Arnold cat map) pour chiffrer les objets 3D. Ces cartes permettent d'effectuer des transformations chaotiques sur les sommets d'un maillage à l'aide d'une matrice afin de modifier leurs coordonnées. La particularité de cette méthode est qu'en appliquant un certain nombre de fois la carte Arnold sur notre maillage, il est possible de retrouver le maillage en clair. Ce nombre est appelé la période d'une transformation Arnold.
Bendon Raj et al. [2019] s'aide par exemple de ces cartes pour pouvoir chiffrer différents modèles. La méthode utilise notamment des combinaisons de cartes 2D et 3D appliquées sur les sommets et les faces afin de former le modèle 3D chiffré.

II. Chiffrement sélectif

Le chiffrement sélectif est un type de chiffrement permettant de plus ou moins garder le format du fichier. Il existe 3 types niveaux de chiffrement sélectif:

- **Le chiffrement transparent** qui permet de conserver la forme et le contenu de l'objet, cependant la haute qualité de cet objet est bloquée.
- **Le chiffrement suffisant** qui permet de laisser la forme reconnaissable mais pas son contenu
- **La confidentialité visuelle** qui bloque la forme et le contenu de l'objet.

Éluard et al ont présenté en 2013 des algorithmes de chiffrement sélectifs en conservant la géométrie.
Les trois méthodes sont:

"CoordinateShuffling" qui consiste à mélanger indépendamment les coordonnées des sommets.

"Dithering applique" qui ajoute un bruit additif

"FragmentScaling" qui partitionne l'espace 3D et modifie l'échelle de ces subdivisions pour déformer l'objet 3D.

Gschwandtner et Uhl ont proposé une méthode de chiffrement en se basant sur un maillage 3D progressif. Comme chaque couche contient des informations qui permettent de raffiner et d'améliorer la qualité du maillage jusqu'à arriver au maillage initial, il est intéressant de chiffrer certaine couche pour ainsi empêcher l'accès au maillage initial.

Références

I. Compression

- Adrien Maglo, Guillaume Lavoue, Florent Dupont, Céline Hudelot, 2013. 3D mesh compression: survey, comparisons and emerging trends. ACM Comput. Surv. 9, 4, Article 39 (September 2013), 40 pages.

- Florian Caillaud. Compression progressive de maillages surfaciques texturés. Autre [cs.OH]. Université de Lyon, 2017. Français. ffNNT : 2017LYSEI004ff. fftel-01783933

- Recent Advances in Compression of 3D Meshes, Pierre Alliez, Craig Gotsman

- Geometry Compression, Deering, 1995

- Geometric Compression Through Topological Surgery, Gabriel Taubin and Jarek Rossignac

- Edgebreaker: Connectivity compression for triangle meshes Jarek Rossignac

- Triangle Mesh Compression, Costa Touma, Craig Gotsman

- Real time compression of triangle mesh connectivity, Gumhold et Straßer

- Progressive meshes, Hugues Hoppe, 1996

- Progressive compression for lossless transmission of triangle meshes. In Proceedings of SIGGRAPH, 195–202, Pierre Alliez and Mathieu Desbrun, 2001a

- Compressed Progressive Meshes, IEEE Transactions on Visualization and Computer Graphics 6 (2000), 79–93, Issue 1, Renato Pajarola and Jarek Rossignac, 2000

- Sébastien Valette, Rémy Prost. A Wavelet-Based Progressive Compression Scheme For Triangle Meshes : Wavemesh. IEEE Transactions on Visualization and Computer Graphics, Institute of Electrical and Electronics Engineers, 2004, 10 (2), pp.123-129. ff10.1109/TVCG.2004.1260764ff. ffhal00537014f

- Sébastien Valette, Raphaëlle Chaine, Rémy Prost. Progressive Lossless Mesh Compression Via Incremental Parametric Refinement. Computer Graphics Forum, Wiley, 2009, 8 (5), pp.1301-1310. ff10.1111/j.1467-8659.2009.01507.xff. ffhal-00533562f

- Progressive Geometry Compression, Andrei Khodakovsky, Peter Schröder, Wim Sweldens

II. Chiffrement

- Survey on 3D Content Encryption, Nashwan Alsalam Ali, Abdul Monem S. Rahma, Shaimaa H. Shaker
- ,Xingyuan Wang, MingXiao Xu & Yong Li
- A New Transformation of 3D Models Using Chaotic Encryption Based on Arnold Cat Map, Benson Raj and al.
- Sécurisation des maillages 3D pour l'industrie de la chaussure et la maroquinerie, Sébastien Beugnon
- Impact of geometry-preserving encryption on rendering time. In 2014 IEEE International Conference on Image Processing, ICIP 2014, Paris, France, October 27-30, 2014, pages 4787–4791. IEEE, 2014, M. Éluard, Y. Maetz, et G. J. Doërr.
- Geometry-preserving Encryption for 3D Meshes, Marc Éluard, Yves Maetz, and Gwenaël Doërr
- Gschwandtner, Michael & Uhl, Andreas. (2009). Protected Progressive Meshes. 35-48. 10.1007/978-3-642-10520-3_4.