

Protection des objets 3D

HMIN 322 : Codage & Compression

Sébastien Beugnon (LIRMM/STRATEGIES)
sebastien.beugnon@lirmm.fr

23 septembre 2019

Outline

Protection des média visuels

Contexte

Applications

Solutions

Objets 3D

Représentation

Manipulations

Évaluation de la qualité

Insertion de données cachées 3D

Synchronisation

Insertion

Méthode de Cho

Conclusion et perspectives

Conclusion

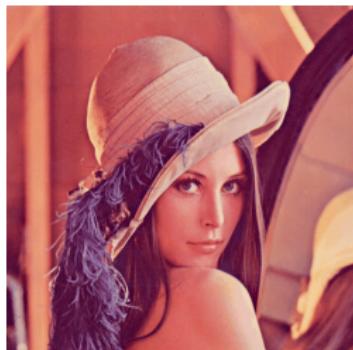
Perspectives

Protection des média visuels

Contexte

Etat actuel

- ▶ Augmentation affolante de la quantité de données multimédia
- ▶ 80% des données transmises sur les réseaux sont des données visuelles



Image



Vidéo



Objet 3D

Contexte

État actuel

- ▶ Augmentation affolante de la quantité de données multimédia
- ▶ 80% des données transmises sur les réseaux sont des données visuelles

Multimédia ? Données visuelles ?

- | | |
|---------|-------------|
| ▶ Image | ▶ Objet 3D |
| ▶ Vidéo | ▶ Biométrie |

Contexte

État actuel

- ▶ Augmentation affolante de la quantité de données multimédia
- ▶ 80% des données transmises sur les réseaux sont des données visuelles

Multimédia ? Données visuelles ?

- ▶ Image
- ▶ Vidéo
- ▶ Objet 3D
- ▶ Biométrie

Contexte

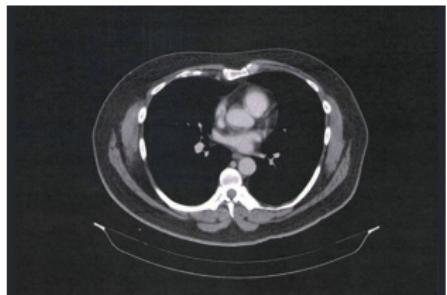
Pourquoi protéger ?

- ▶ Vie privée, propriété, contrefaçon
 - ▶ Éviter les fuites (ou pouvoir les remonter)

Contexte

Pourquoi protéger ?

- ▶ Vie privée, propriété, contrefaçon
 - ▶ Éviter les fuites (ou pouvoir les remonter)
 - ▶ Données médicales de patients
(Etude de Greenbone Networks (GN), septembre 2019)



Etude de GN

Monde/France

- ▶ 399 M/2.94 M images médicales
 - ▶ 24 M/54.000 dossiers patients
 - ▶ 500 serveurs défaillants
 - ▶ DICOM (Protocole)

Applications

Domaines

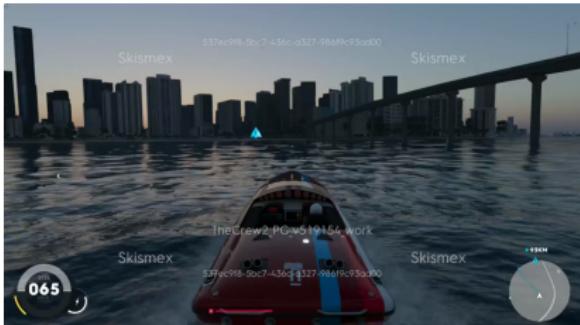
- ▶ Militaire
 - ▶ Médical
 - ▶ Jeu vidéo
 - ▶ *Streaming*
 - ▶ Industrie



Applications

Domaines

- ▶ Militaire
 - ▶ Médical
 - ▶ Jeu vidéo
 - ▶ *Streaming*
 - ▶ Industrie



Applications

Usages

- ▶ Confidentialité
 - ▶ Intégrité
 - ▶ Authentification
 - ▶ Non-répudiation
 - ▶ Disponibilité
 - ▶ Traçage de traître

Solutions

Solutions

- ▶ Cryptographie
 - ▶ Transforme les données originales de façon intelligible
- ▶ Insertion de données cachées
 - ▶ Cache des données de façon imperceptible dans un média

Cryptographie

Définition

Transforme les données originales de façon intelligible

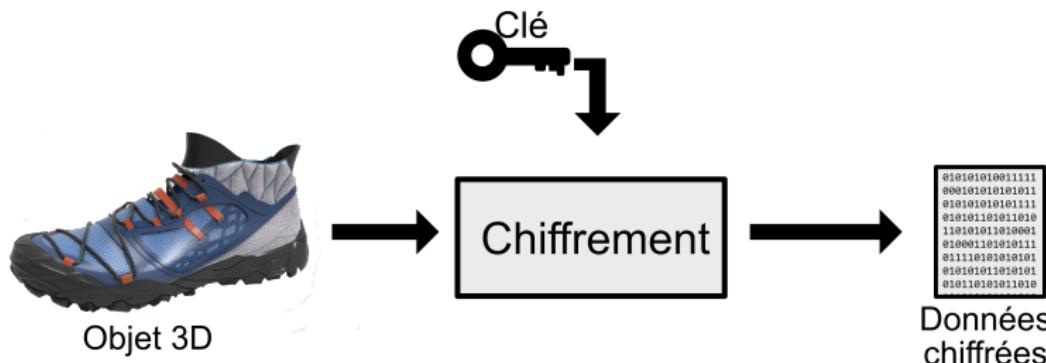
Avantages/Inconvénients

- + Confidentialité visuelle des données sensibles
- Après déchiffrement, il n'y a aucune sécurité

Cryptographie

Chiffrement

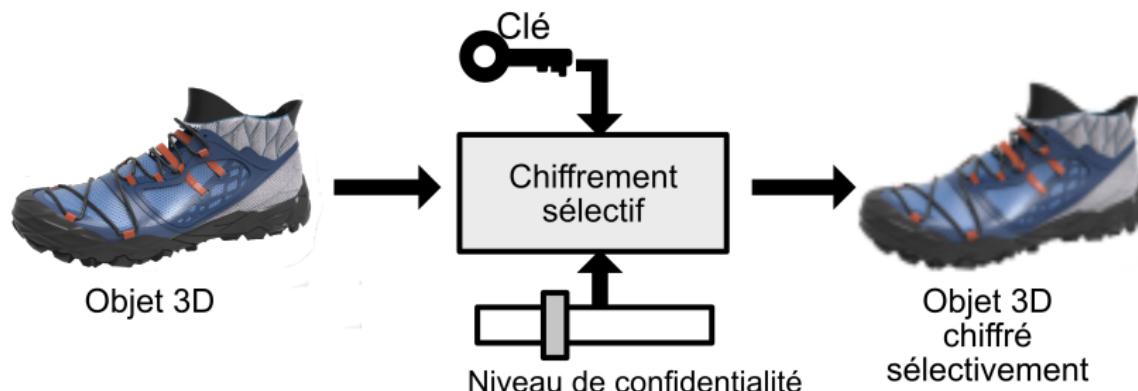
- ▶ Complet
- ▶ Sélectif



Cryptographie

Chiffrement

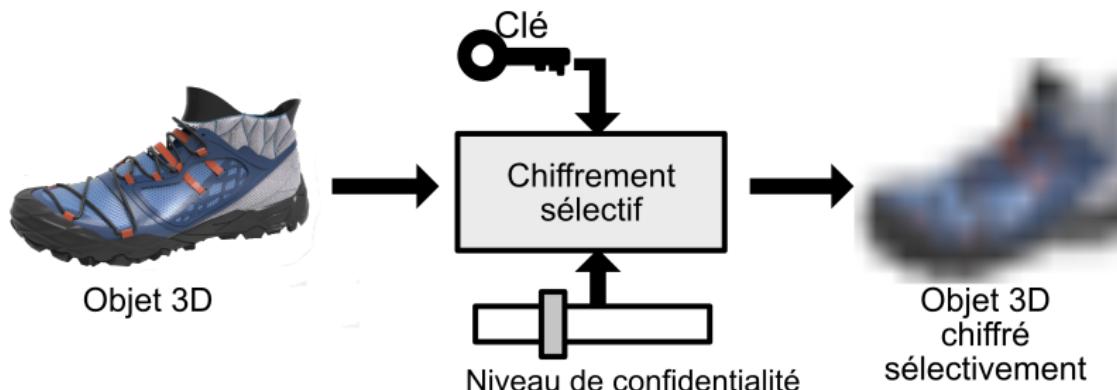
- ▶ Complet
- ▶ Sélectif



Cryptographie

Chiffrement

- ▶ Complet
- ▶ Sélectif



Insertion de données cachées

Définition

L'art de cacher des données de façon imperceptible au sein d'un média

Intérêts

- ▶ Suivi
- ▶ Contenu additionnel
- ▶ Vie privée
- ▶ Droits d'auteur

Protocole en deux étapes

- ▶ Insertion
- ▶ Extraction

Insertion de données cachées

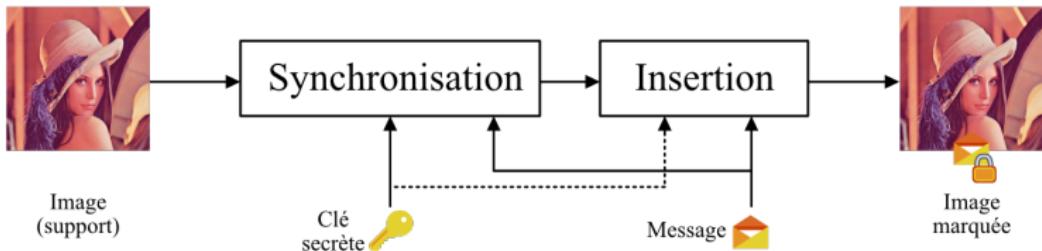
Propriétés

- ▶ Préservation du format (lisible dans des logiciels standards)
- ▶ Confidentialité
- ▶ Intégrité
- ▶ Authentification

A priori sur le média

- ▶ Aveugle (*Blind*, sans référence)
- ▶ Semi-aveugle (*Semi-blind*, avec référence partielle)
- ▶ Non-aveugle (*Non-blind*, avec objet original)

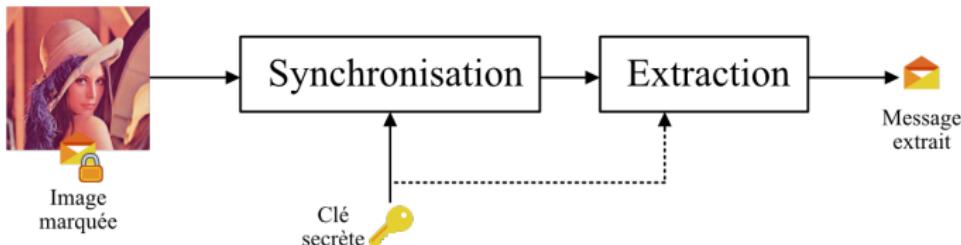
Insertion de données cachées



Phase d'insertion

Le média est marqué avec un message secret à l'aide d'une clé secrète

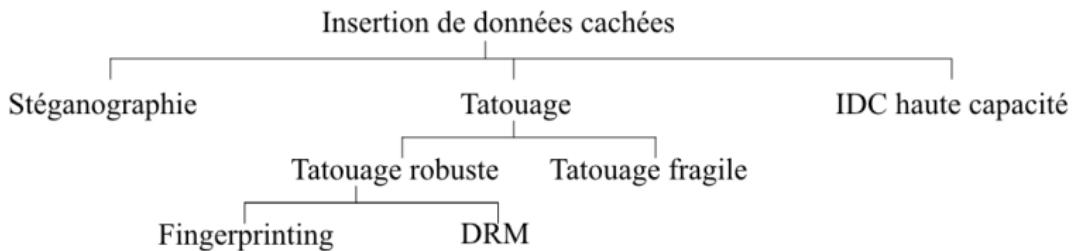
Insertion de données cachées



Phase d'extraction

L'information cachée est retrouvée suivant l'ordre donné par la synchronisation et la clé secrète

Classification des méthodes d'IDC



Mode d'insertion

Injection

Le message est inséré directement dans le média, ce qui provoque une augmentation de la taille du support. Ce comportement est une faille de sécurité par rapport à un potentiel attaquant.

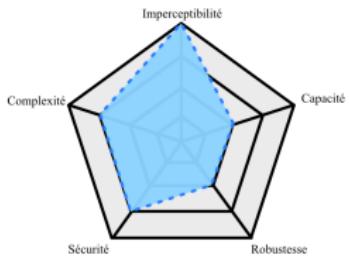
Substitution

Le message est inséré de façon à remplacer l'information redondante du support ou à substituer une partie de l'information qui altère le moins le support. Cette technique est la plus utilisée.

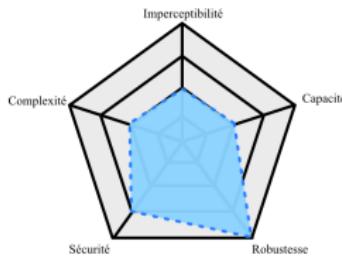
Distorsion

L'extraction se fait en analysant les différentes entre les objets supports et marqués.

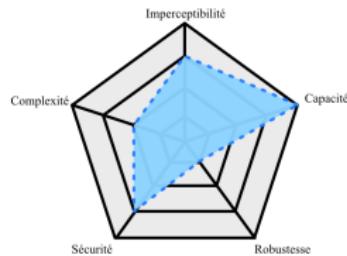
Compromis



Stéganographie



Tatouage



Insertion haute-capacité

Propriétés

- ▶ Robustesse
- ▶ Capacité
- ▶ Imperceptibilité
- ▶ Sécurité
- ▶ Complexité

Évaluation de la robustesse

Nombre d'erreurs binaires entre m et m'

$$NE = |m| - |m'| + \sum_{i=0}^{|m|-1} \begin{cases} 1 & \text{si } m_i \neq m'_i \\ 0 & \text{sinon} \end{cases} \quad (1)$$

BER

$$BER = \frac{NE}{|m|} \quad (2)$$

Capacité des méthodes

Méthodes	Capacité	Robustesse
0-bit	1 bit	+++
Tatouage	identifiant : 64, 128 bits	++
<i>Fingerprinting</i>	borne min = nombre d'utilisateurs	+
Tatouage fragile	max	-
Stéganographie	borne max = pour être indétectable	-
Haute-capacité	max	-

Imperceptible

Évaluation à l'aide de métriques

- ▶ Métriques subjectives
 - ▶ MOS (score d'opinion moyenne)
 - ▶ Distance
 - ▶ Perceptuelle
- ▶ Métriques objectives
 - ▶ PSNR
 - ▶ RMSE

Sécurité

Définitions

- ▶ Secret de la clé et non de la méthode (Kerckhoffs, 1883)
- ▶ Incapacité pour des utilisateurs non autorisés d'accéder au canal de tatouage (Kalker, 2001)
- ▶ Difficulté d'estimer les paramètres secrets de la méthode d'insertion en observant un objet marqué (Perez-Freire, 2009)

Comparaison entre insertion dans le domaine spatial et dans un domaine transformé

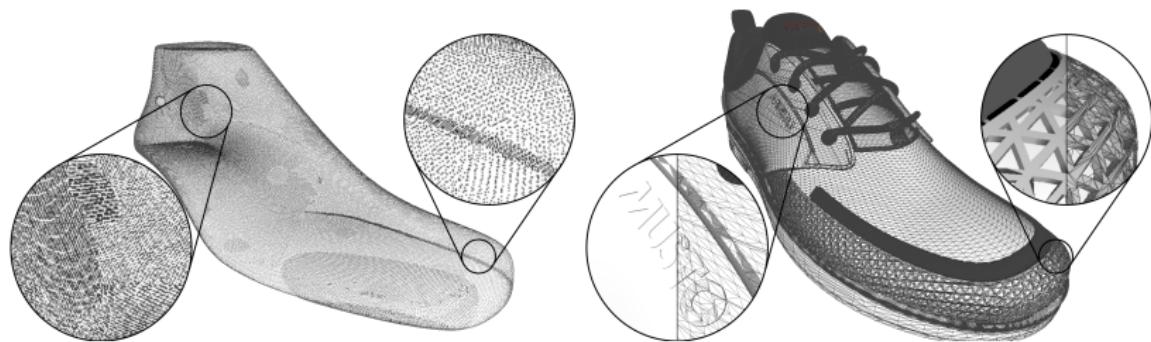
Facteurs	Domaine spatial	Domaines transformés
Coût de calcul	Faible	Important
Robustesse	Faible	Plus robuste
Qualité perceptuelle	Contrôlable	Peu de contrôle
Complexité	Faible	Haute
Temps de calcul	Faible	Plus importante
Capacité	Haute	Moindre

Objets 3D

Représentation

Maillage 3D

- ▶ Principale représentation



Maillage 3D

Représentation

- ▶ $M = (V, K)$
- ▶ Composante géométrique $V = \{v_1, \dots, v_n\} v_i \in \mathcal{R}^3, 1 \leq i \leq n$
 - ▶ $v_i = (x_i, y_i, z_i)$
- ▶ composante de connectivité (ou topologique) K
 - ▶ Facettes $F : f = \{v_0, \dots, v_m\}$
 - ▶ Arêtes $E : e = \{v_i, v_j\}$

Quelques définitions

Degré d'un polygone

Le nombre d'arêtes qui le composent

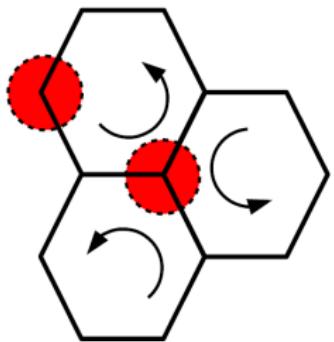
Valence d'un sommet

Le nombre d'arêtes incidentes

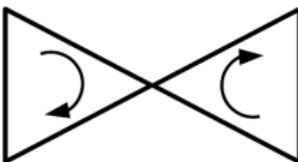
2-variété (two-manifold)

Chaque arête appartient à strictement deux polygones

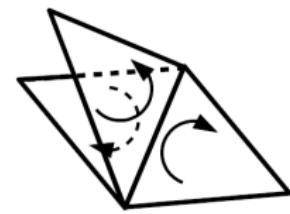
Quelques définitions



(a)



(b)



(c)

- ▶ a) 2-variété
- ▶ b) non-variété orientable
- ▶ c) non-variété non orientable

Quelques définitions

Caractéristiques d'Euler (genre, topologie)

$$\chi(M) = \sum_{i \geq 0} (-1)^i n(i) \quad (3)$$

Pour un maillage 3D 2-variété, $M = (V, F, E)$:

$$\chi(M) = |V| - |E| + |F| \quad (4)$$

Exemples

- ▶ Sphère : $\chi(M) = 2$
- ▶ Donut : $\chi(M) = 0$
- ▶ Double donut (Torus) : $\chi(M) = -2$

Topologie



by LThMath 2015

Manipulations

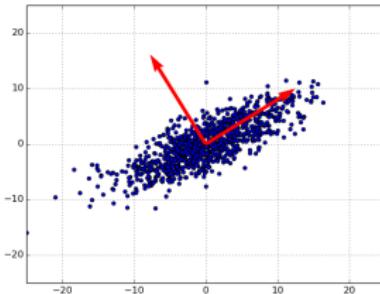
Catégories

- ▶ Transformations affines
- ▶ Ajout de bruit
- ▶ Filtrage
- ▶ Attaque sur la connectivité
- ▶ Ré-échantillonage
- ▶ Attaques topologiques
- ▶ Compression

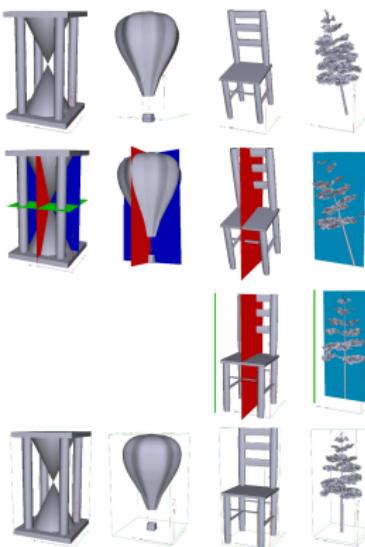
Recalage de maillages

ACP (Analyse en Composante Principale)

- ▶ Réduire le nombre de directions
- ▶ Trouver les directions principales



Recalage de maillages



Mohamed Chaouch et Anne Verroust-Blondet, "A Novel Method for Alignment of 3D Models". IEEE ICSMA, 2008.

Évaluation de la qualité

Métriques (avec référence)

- ▶ Distance de Hausdorff (HD)
- ▶ *Root Mean Square Error* (RMSE)
- ▶ MRMSE (maximum of the two asymmetric RMSE)
- ▶ GL_1 , GL_2 (Karni et Gotsmann, 2000) (Sorkine *et al.*, 2003)
- ▶ PSNR
- ▶ MSDM et MSDM2 (Lavoué *et al.*, 2006) (Lavoué, 2011)
- ▶ FMPD, DAME, TPDM, etc...

Évaluation de la qualité

Outils

- ▶ Metro
- ▶ LibIGL
- ▶ MEPP
- ▶ MeshLab
- ▶ CloudCompare

Insertion de données cachées 3D

Insertion de données cachées 3D

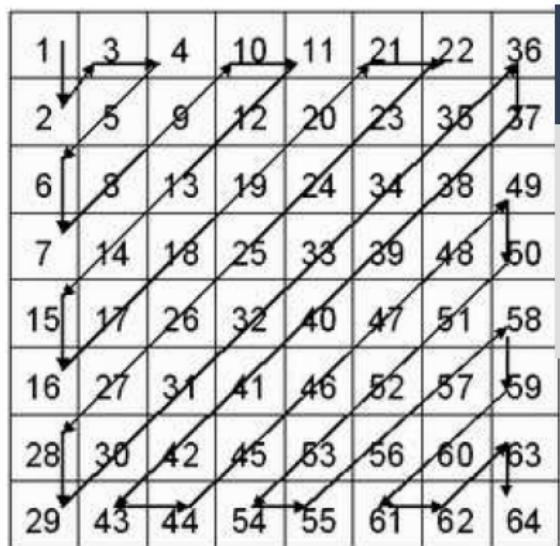
Étapes

- ▶ Synchronisation
- ▶ Insertion sur une primitive (sommet, arrête, facette...)

Différence par rapport à la 2D

- ▶ Choix de la primitive (2D pixel)
- ▶ Ordre non naturel (2D trivial)
- ▶ Problème de causalité

Synchronisation 2D



Exemples d'ordonnancement unique

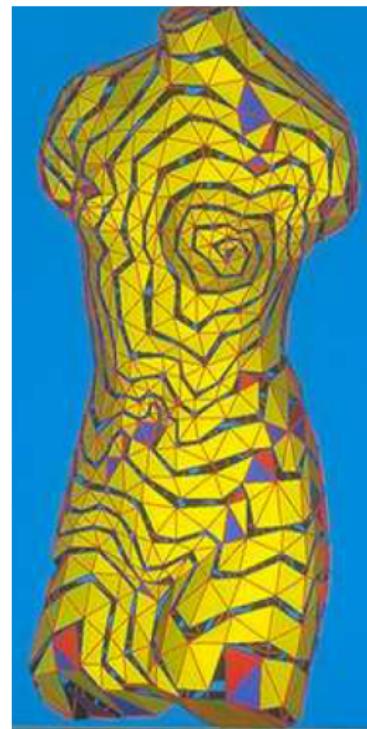
- ▶ Lignes et colonnes
- ▶ Zig-zag
- ▶ Blocs

Chemin en ZigZag d'une image 2D.

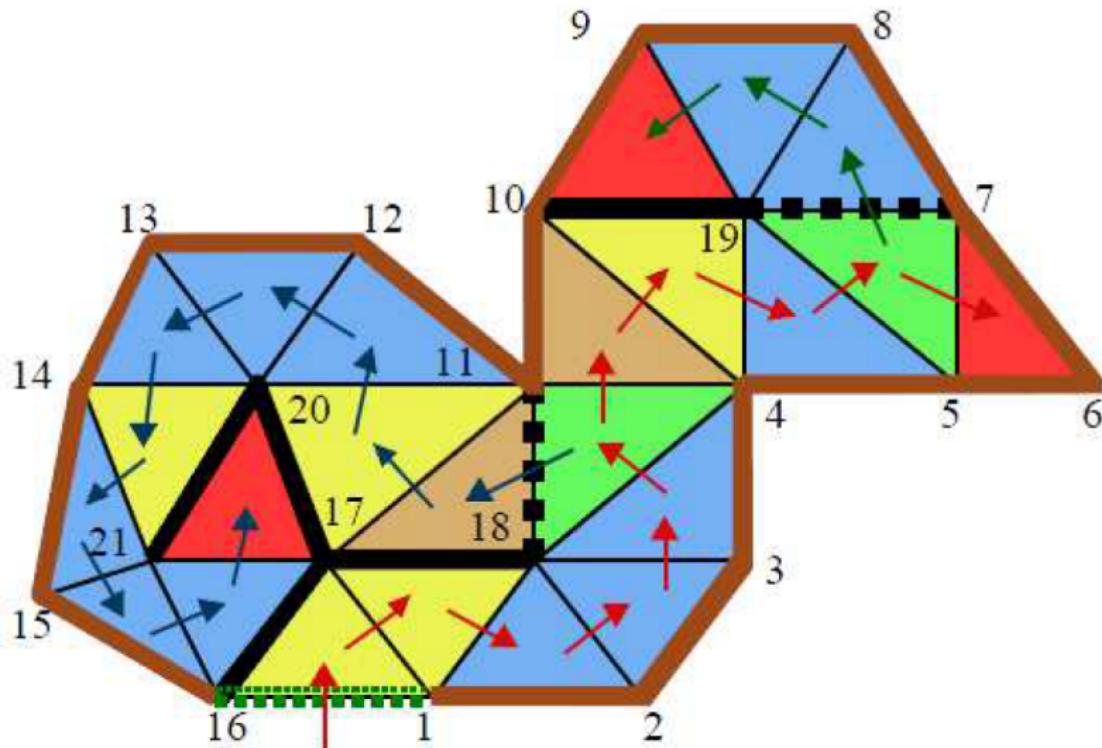
Synchronisation 3D

Ordonnancement par facettes

- ▶ "Edgebreaker" (Rossignac, 1999) pour la compression
- ▶ TSPS (Triangle Strip Peeling Sequence) (Obuchi, 1997)
- ▶ Parcours en largeur/profondeur



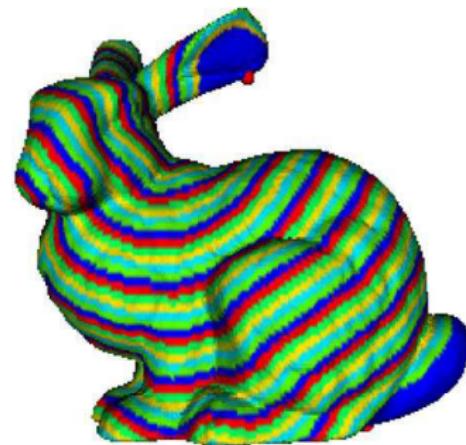
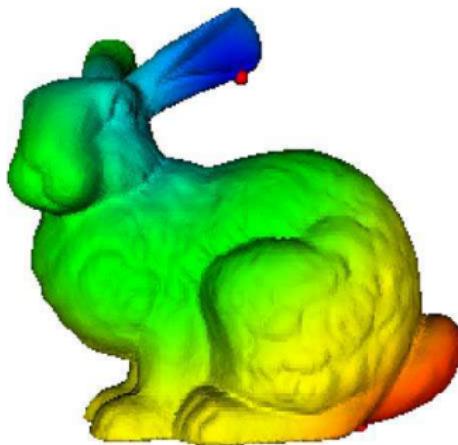
Synchronisation 3D



Synchronisation 3D

Ordonnancement par patchs

- ▶ Génération de séquences de triangles iso-géodésique (Luo, 2011)
- ▶ Iso-geodesic mesh strip generation



Synchronisation 3D

Ordonnancement par patchs

- ▶ Subdivision (Wang, 2009)
- ▶ Kd-Tree, OcTree

Ordonnancement par sommets

- ▶ Ordre des sommets
- ▶ Ordre de tri



Synchronisation 3D

Ordonnancement par graphe

- ▶ Parcours en largeur, en profondeur
- ▶ Arbre couvrant de poids minimum (ACPM)
- ▶ Chemin hamiltonien



(a)



(b)

a)

Synchronisation 3D

Ordonnancement par graphe

- ▶ Parcours en largeur, en profondeur
- ▶ Arbre couvrant de poids minimum (ACPM)
- ▶ Chemin hamiltonien



(a)



(b)

a)

Influence de l'insertion sur la synchronisation

Définition

Un problème de causalité survient lorsque l'insertion modifie les caractéristiques servant à la synchronisation. Cela implique une erreur partielle ou totale à l'extraction

Exemples

- ▶ Déplacement des points du graphe
- ▶ Déplacement du centre de gravité

Insertion

Support du message en 3D

- ▶ Géométrie (statistique)
- ▶ Connectivité
- ▶ Représentation
- ▶ Domaine transformé

Insertion

Domaine spatial

- ▶ Histogramme des normals (Benedens, 1999)
- ▶ Histogramme des distances radiales (Zafeiriou *et al.*, 2005)
- ▶ Histogramme des distances au centre (Cho *et al.*, 2008), (Bors et Luo, 2013)

Insertion

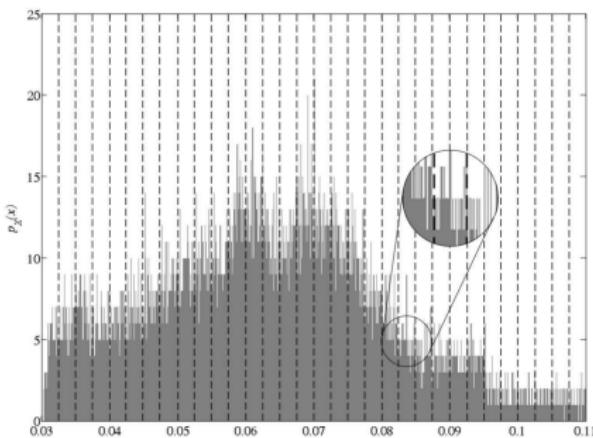
Domaine transformé

- ▶ Différences des coefficients de Laplacienne (Obhuchi *et al.*, 2001) (Lavoué *et al.*, 2007)
- ▶ MHT (Manifold Harmonics Transform) (Liu *et al.*, 2008), (Wang *et al.*, 2009)
- ▶ Harmoniques sphériques (Konstandinides *et al.*, 2009)
- ▶ Décomposition multi-résolution (Praun *et al.*, 1999) (Ucchedu *et al.*, 2004) (Wang *et al.*, 2008)

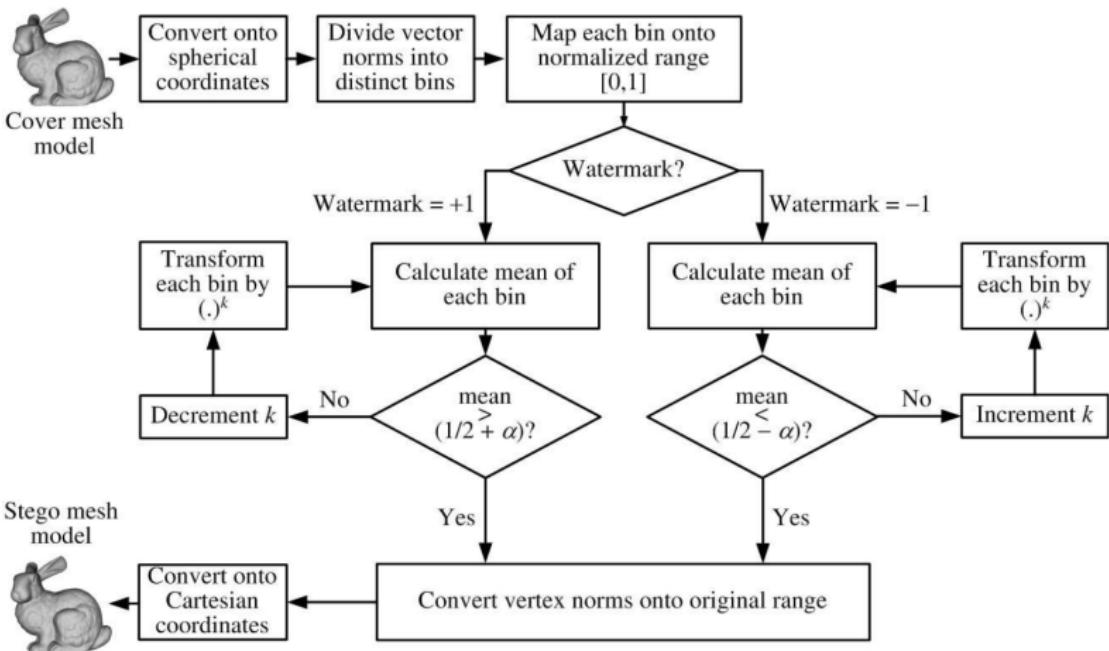
Méthode de Cho (TP)

Méthode sur le domaine spatial

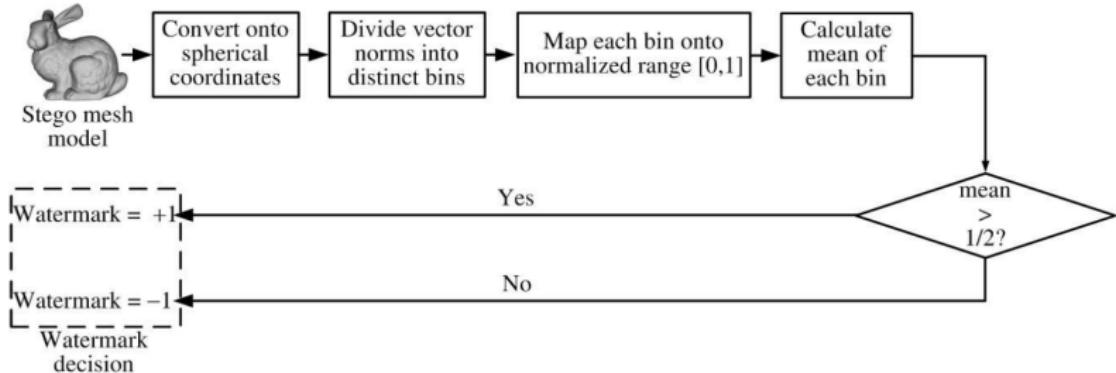
- ▶ Méthode robuste sur statistique (Histogramme des distances au centre)



Méthode de Cho - Insertion



Méthode de Cho - Extraction



Méthode de Cho - Étapes

Étapes

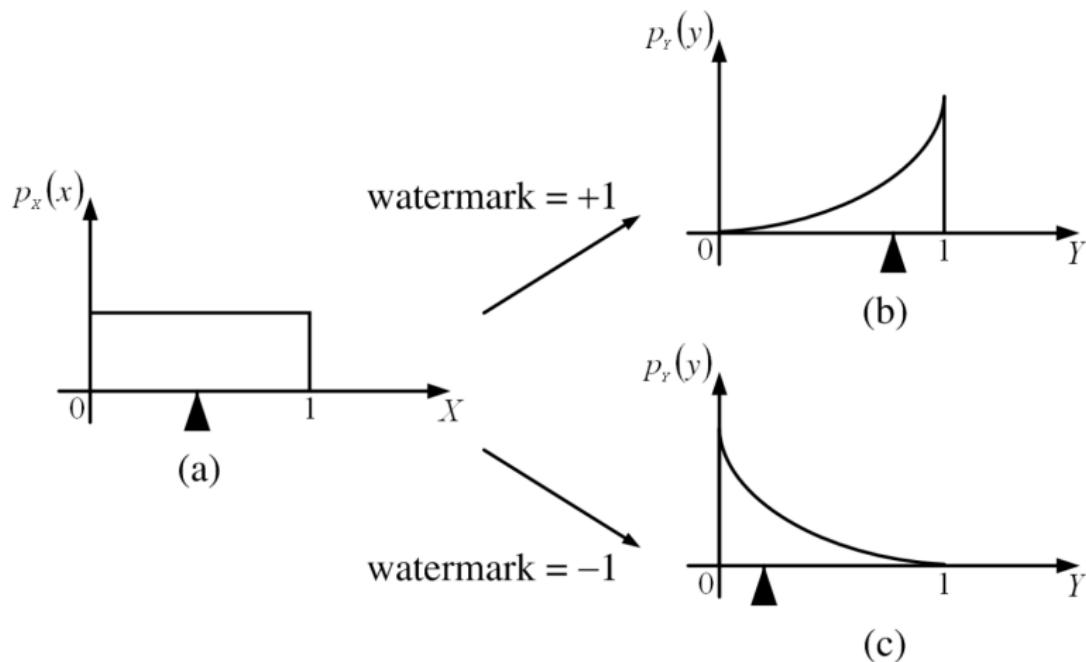
1. Calculer le centre de gravité g
2. Transformer les coordonnées des sommets en coordonnées sphériques en fonction de g
3. Divisions en n classes (*Bins*)
4. Normalisation des *bins* entre $[0, 1]$
5. Insertion itérative dans chaque *bin* en fonction du message

Méthode de Cho - Modification

Statistiques

- ▶ Moyenne
- ▶ Variance

Méthode de Cho - Moyenne



Méthode de Cho - Moyenne

Modifier la moyenne

α force d'insertion / sensibilité aux erreurs

$$m'_n = \begin{cases} \frac{1}{2} + \alpha, & \text{si } w_n = 1 \\ \frac{1}{2} - \alpha, & \text{si } w_n = -1(0) \end{cases} \quad (5)$$

Méthode de Cho - Moyenne

Modifier la moyenne

$$p'_{n,j} = (p_{n,j})^{k_n} \quad (6)$$

où k_n est calculé comme :

$$k_n = \begin{cases} \frac{1-2\alpha}{1+2\alpha}, & \text{si } w_n = 1 \\ \frac{1+2\alpha}{1-2\alpha}, & \text{si } w_n = -1(0) \end{cases} \quad (7)$$

Méthode de Cho - Moyenne

Problème

Distribution non continu, non uniforme $\implies k_n$ ne peut pas être calculé

Solution

Insertion itérative

Méthode de Cho - Moyenne

Insertion itérative

1. $k_n = 1$
2. $p'_{n,j} = (p_{n,j})^{k_n}$
3. $m'_n = \frac{1}{M_n} \sum_{j=0}^{M_n-1} p'_{n,j}$
4. Si $m'_n < \frac{1}{2} + \alpha$, $k_n = k_n - \Delta k$ (Retour à l'étape 2)
5. $p_{n,j} = p'_{n,j}$

Méthode de Cho - Fin

Transformation inverse

- ▶ Normalisation inverse des classes
- ▶ Transformation des coordonnées sphériques en coordonnées cartésiennes

Méthode de Cho - Bilan

Bilan

- ▶ Insertion longue (en fonction de Δk)
- ▶ Extraction rapide
- ▶ Robuste
- ▶ Faible capacité
- ▶ Aveugle
- ▶ Force de l'insertion laissée à l'utilisateur

Conclusion et perspectives

Conclusion

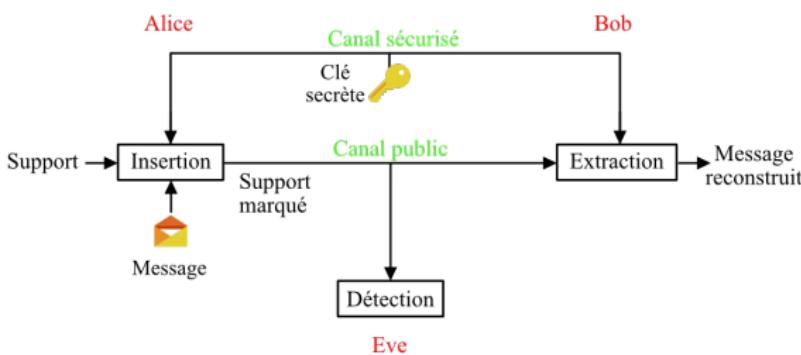
Conclusions

- ▶ Méthodes différentes !
- ▶ Recherche de compromis : capacité, robustesse et distorsions
- ▶ Choisir la méthode répondant le mieux au besoin

Perspectives

Stéganalyse

- ▶ Analyse des supports pour la détection de présence de prisonnier (Li *et al.*, 2017)



Zhenyu Li *et al.*, "Rethinking the high capacity 3D steganography : Increasing its resistance to steganalysis". IEEE ICIP, 2017.

Perspectives

Sécurité

- ▶ La sécurité est un champs plus large
- ▶ Robustesse \neq Sécurité
- ▶ Existe en 2D, peu en 3D
 - ▶ Peu de méthode robuste en 3D

Scénarios à étudier

Diffie-Hellman, 1979

- ▶ WOA (Watermarked Only Attack) observation maillages tatoués
- ▶ KMA (Known Message Attack) observation maillages tatoués et messages associés
- ▶ KOA (Known Original Attack) observation maillages tatouées et originaux



Whitefield Diffie et Martin E. Hellman, "New directions in Cryptography". IEEE Transactions on Information Theory, 1979.