Protection des maillages 3D

Vincent Itier

9 Novembre 2015

Plan

1 Maillage 3D

2 Protection des médias visuels

3 Insertion de données cachées 3D

4 Conclusion et perspectives

Section 1

Maillage 3D

1 Maillage 3D
- Représentation surface 3D
- Manipulations
- Évaluation de la qualité

2 Protection des médias visuels

3 Insertion de données cachées 3D

4 Conclusion et perspectives

Maillage 3D

(a) (b)

Figure – a) Nuage de 5002 points 3D, b) maillage triangulé associé.

Maillage 3D

Représentation

- $M = (V, K)$
- $V = \{v_1, \ldots, v_n\},\ v_i \in \mathbb{R}^3,\ 1 \leq i \leq n$
- K connectivité topologique

Maillage 3D

Représentation

- K :
- Facettes F : $f = \{v_0, \ldots, v_n\}$
- Arrêtes E : $e = \{v_i, v_j\}$

Maillage 3D

Définitions :

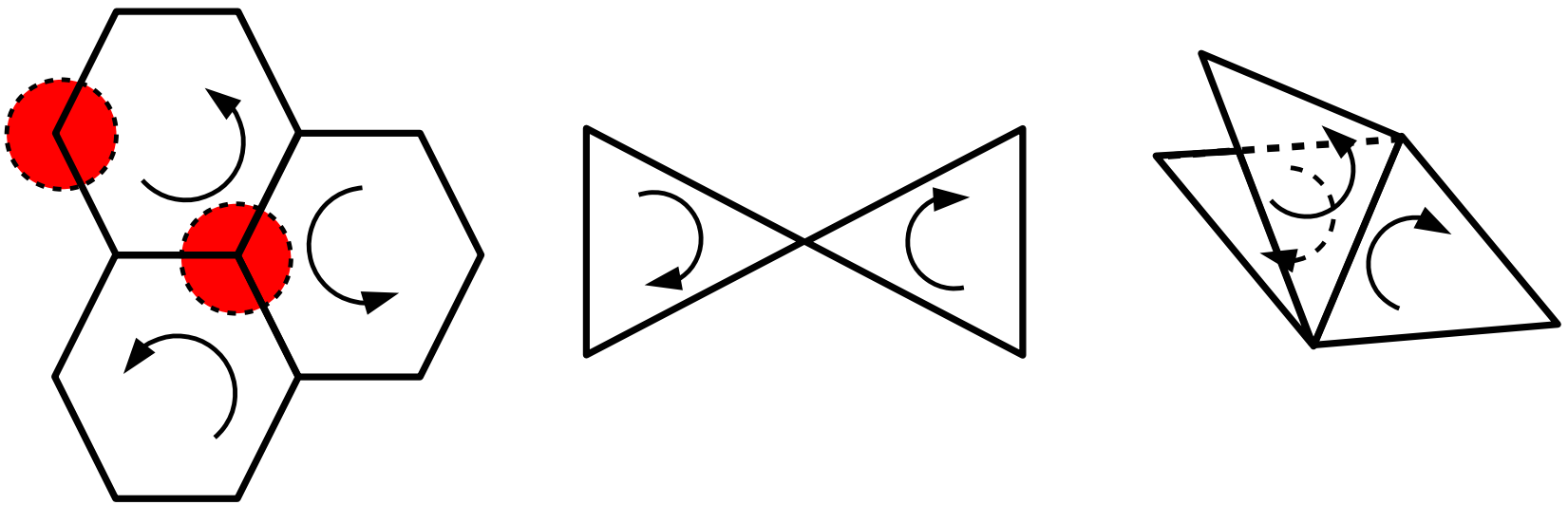
- Degré d'un polygone est le nombre d'arêtes qui le composent.
- Valence d'un sommet est définie comme le nombre d'arêtes incidentes.

Exemple :

- 1-ring neighborhood : Distances géodésiques ou de courbures locales.

Maillage 3D

Propriétés : 2-variétés



(a) (b) (c)

Figure – Exemple de configuration a) 2-variété, b) non-variété orientable, c) non-variété non orientable.

Maillage 3D

Caractéristique d'Euler

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

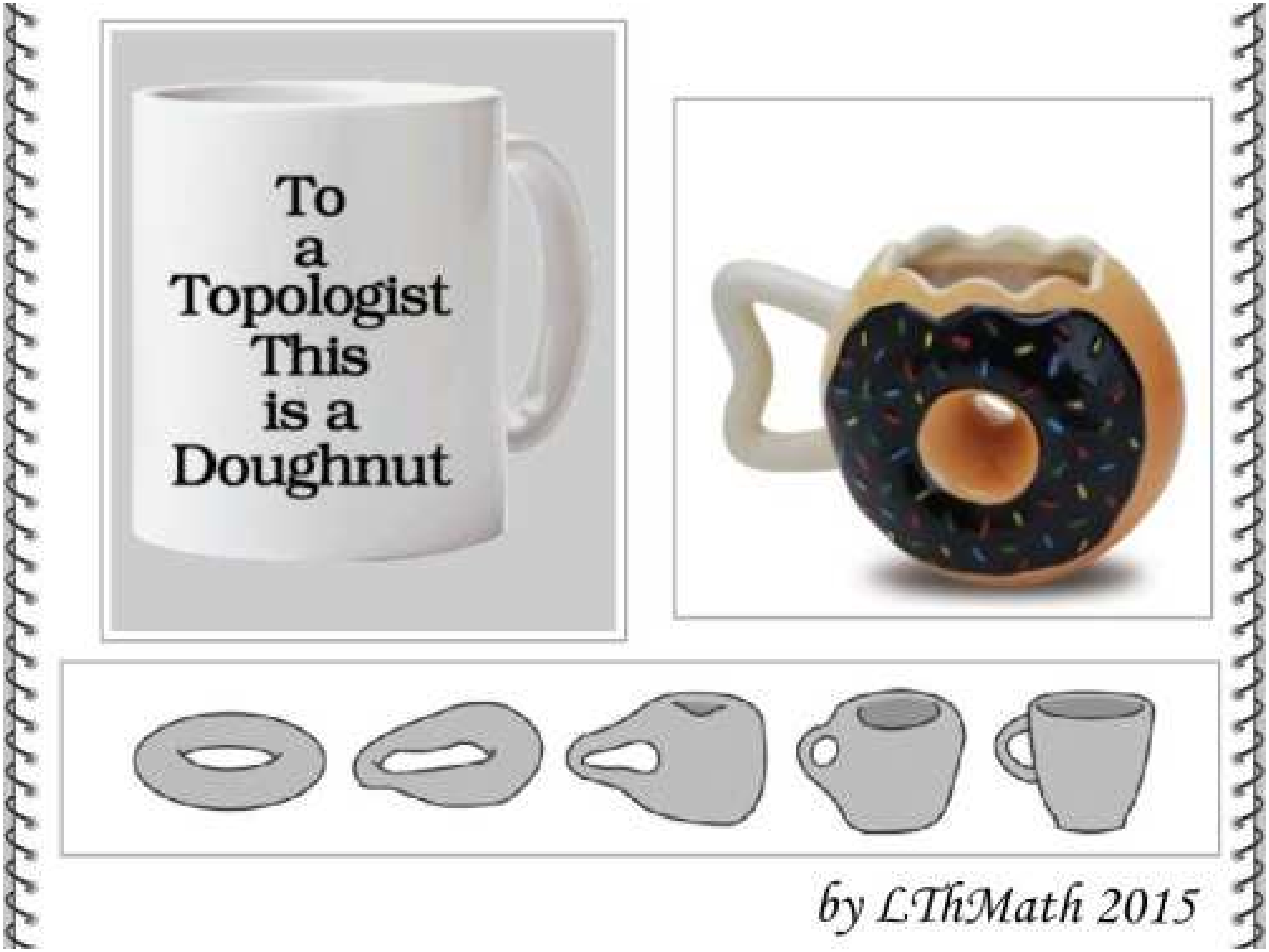
Pour un maillage 3D $M = (V, F, E)$:

$$\chi(M) = |V| - |E| + |F| \tag{2}$$

Exemple :

- sphere : $\chi(M) = 2$
- donut : $\chi(M) = 0$
- double donut : $\chi(M) = -2$

Maillage 3D



Maillage 3D

Stockage

Nombreux formats : STL, PLY, OFF...

Exemple OFF

```
OFF
1000 1996 0
4.394422054290771 -0.3315080106258392 0.1344770044088364
4.548637866973877 -0.09076900035142899 0.4463599920272827
4.085364818572998 -0.06663899868726730 0.4451819956302643
...
3 0 1 2
3 0 2 3
3 3 2 4
3 2 1 5
...
```

Modifications

Catégories

- Transformations affines
- Ajout de bruit et lissage
- Attaque sur la connectivité
- Ré-échantillonnage
- Attaques topologiques
- Compression

Modifications

Transformations affines

- Translation
- Rotation
- Changement d'échelle uniforme/non uniforme
- Combinaisons

Modifications

Ajout de bruit et lissage

- Amélioration la qualité visuelle d'un maillage
- Sur la géométrie du maillage

Modifications

Attaque sur la connectivité

- Changement des relations d'adjacences entre les primitives du maillage
- Remaillage complet
- Retournement d'arêtes
- Sans distorsion : réorganisation de l'ordre des primitives dans le format de représentation

Modifications

Ré-échantillonnage

- Nouveau maillage respectant la forme topologique $\neq$ connectivité
- Subdivision du maillage
- Simplification du maillage

Modifications

Attaques topologiques

- Découpage
- Remplissage de trous
- Changement de la caractéristique d'Euler

Modifications

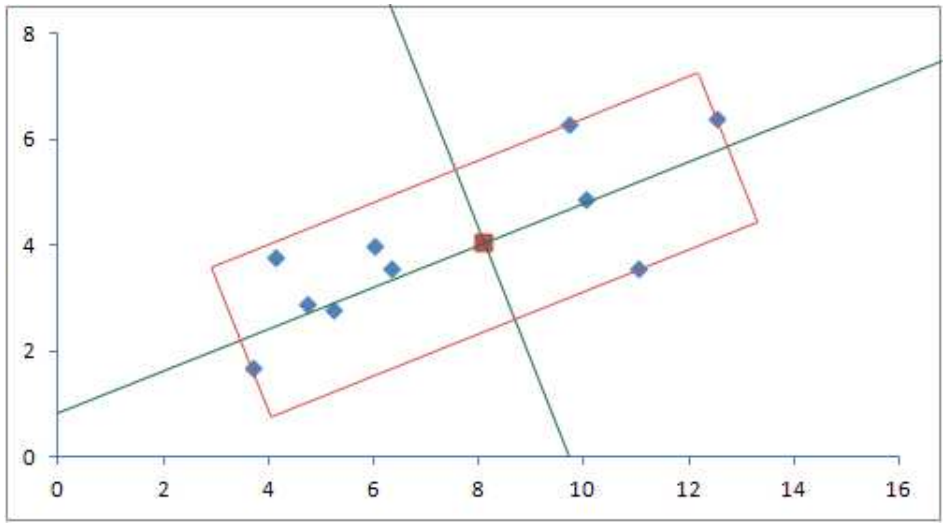
Compression

- Avec pertes (Quantification des coordonnées des sommets)

Recalage de maillages

ACP (Analyse en Composante Principale)

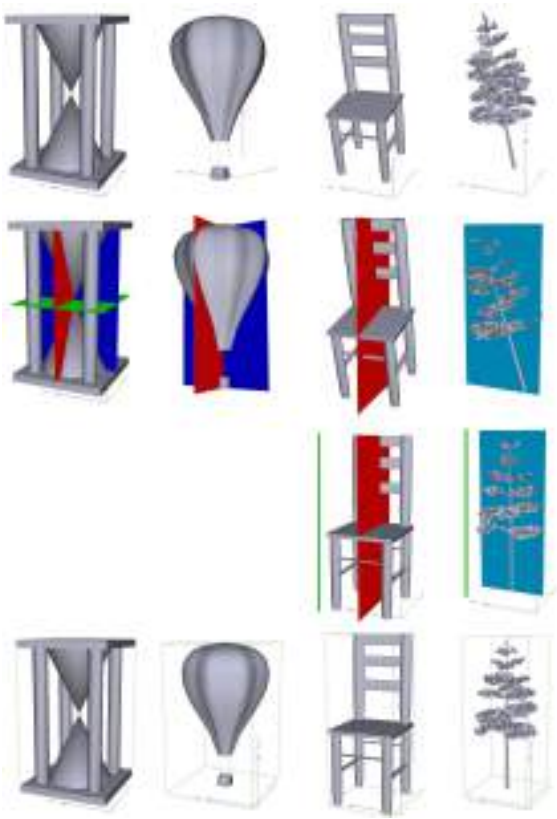
- Réduire le nombre de directions
- Trouver les directions principales



ACP

Recalage de maillages

ACP pour les maillages 3D



ACP [Chaouch *et al.* 2008]

Évaluation de similarité

Métriques

- Distance de Hausdorff.
- RMS (root square error).
- MRMS (maximum of the two asymetric RMS).
- GL_1,GL_2, [Karni and Gotsman 00],[Sorkine *et al.* 03].
- Mesure basée sur la rugosité $3DWPM_1$, $3DWPM_2$, [Drelie Gelasca *et al.* 05], [Corsini *et al.* 07].
- $MSDM_1$, $MSDM_2$ (Mesh Structural Distortion Measure), [Lavoué *et al.* 06] [Lavoué 11].
- ...

Distance de Hausdorff

Distance entre un point $p \in S$, et un point $p' \in S'$

$$d(p, \mathcal{S}') = \min_{p' \in \mathcal{S}'} \left\| p - p' \right\|_2 , \tag{3}$$

Distance de Hausdorff

$$d(\mathcal{S}, \mathcal{S}') = \max_{p \in \mathcal{S}} d(p, \mathcal{S}'). \tag{4}$$

En général, $d(S, S') \neq d(S', S)$:

Distance de Hausdorff symétrique

$$d_s(\mathcal{S}, \mathcal{S}') = \max(d(\mathcal{S}, \mathcal{S}'), d(\mathcal{S}', \mathcal{S})), \tag{5}$$

Distance de Hausdorff

Distance entre un point $p \in S$, et un point $p' \in S'$

$$d(p, \mathcal{S}') = \min_{p' \in \mathcal{S}'} \left\| p - p' \right\|_2 , \tag{6}$$

Distance de Hausdorff

$$d(\mathcal{S}, \mathcal{S}') = \max_{p \in \mathcal{S}} d(p, \mathcal{S}'). \tag{7}$$

En général, $d(S, S') \neq d(S', S)$:

Distance de Hausdorff symétrique

$$d_s(\mathcal{S}, \mathcal{S}') = \max(d(\mathcal{S}, \mathcal{S}'), d(\mathcal{S}', \mathcal{S})), \tag{8}$$

RMSE (root mean square error)

RMSE point/surface

$$RMSE(\mathcal{S}, \mathcal{S}') = \sqrt{\frac{1}{|\mathcal{S}|} \int \int_{p \in \mathcal{S}} d(p, \mathcal{S}')^2 \mathrm{d}\mathcal{S}}. \quad (9)$$

RMSE symétrique

$$MRMSE(\mathcal{S}, \mathcal{S}') = \max(RMSE(\mathcal{S}, \mathcal{S}'), RMSE(\mathcal{S}', \mathcal{S})). \quad (10)$$

Approximation RMSE entre M et M'

RMSE : appariement sommets

$$RMSE_v(M, M') = \sqrt{\frac{1}{|V|}\sum_{1}^{|V|} \left\| v_i - v'_i \right\|_2^2}, \tag{11}$$

RMSE : appariement des normales

$$RMSE_n(M, M') = \sqrt{\frac{1}{|V|}\sum_{1}^{|V|} \left\langle n_i, n'_i \right\rangle^2}, \tag{12}$$

PSNR

PSNR : en fonction du RMSE

$$PSNR_v(M, M') = 20 \log_{10} \frac{D_{max}}{RMSE_v(M, M')}, \quad (13)$$

D_{max} longueur de la diagonale de la boîte englobant de M

MSDM

Métrique perceptuelle

$$MSDM(M, M') = \left(\frac{1}{n_w} \sum_{j=1}^{n_w} LMSDM(a_j, b_j)^3 \right)^{\frac{1}{3}} . \quad (14)$$

$$LMSDM(a, b) = \left(0.4 \times L(a, b)^3 + 0.4 \times C(a, b)^3 + 0.2 \times S(a, b)^3\right)^{\frac{1}{3}} , \quad (15)$$

où L, C, S fonctions de comparaison de courbures, de contrastes et de structures

Évaluation de la qualité

Outils

- Metro
- MeshLab
- MEPP
- CloudCompare

Section 2

Protection des médias visuels

1 Maillage 3D

2 Protection des médias visuels
- Objectifs
- Méthodes
- Stéganographie

3 Insertion de données cachées 3D

4 Conclusion et perspectives

Pour quoi faire ?

- Application militaire.
- Imagerie Médicale (vie privée).
- Jeux-vidéos (contenu additionnel).
- Photographie, streaming... (droit d'auteur).

Pour quoi faire ?

Ce qu'il est possible de faire :

- Cacher le contenu.
- Traçage de traitre.
- Confidentialité.
- Intégrité.
- Disponibilité.
- Authentification.
- Non-répudiation.

Méthodes de protections

Méthodes :

- Chiffrement.
  - Transforme les données originales de façon inintelligible.
- Tatouage.
  - Cache des données de façon imperceptible dans un média.

Méthodes

Cryptographie

- Confidentialité visuelle (données sensibles, jeux vidéo,...).
- Déchiffrement : moins de sécurité.

Tatouage

- Copyright.
- Authentification.
- Intégrité.
- Méta-données.

Cryptographie

Chiffrement

- Chiffrement complet : confidentialité visuelle.
- Chiffrement sélectif : aperçu etc...

Cryptographie

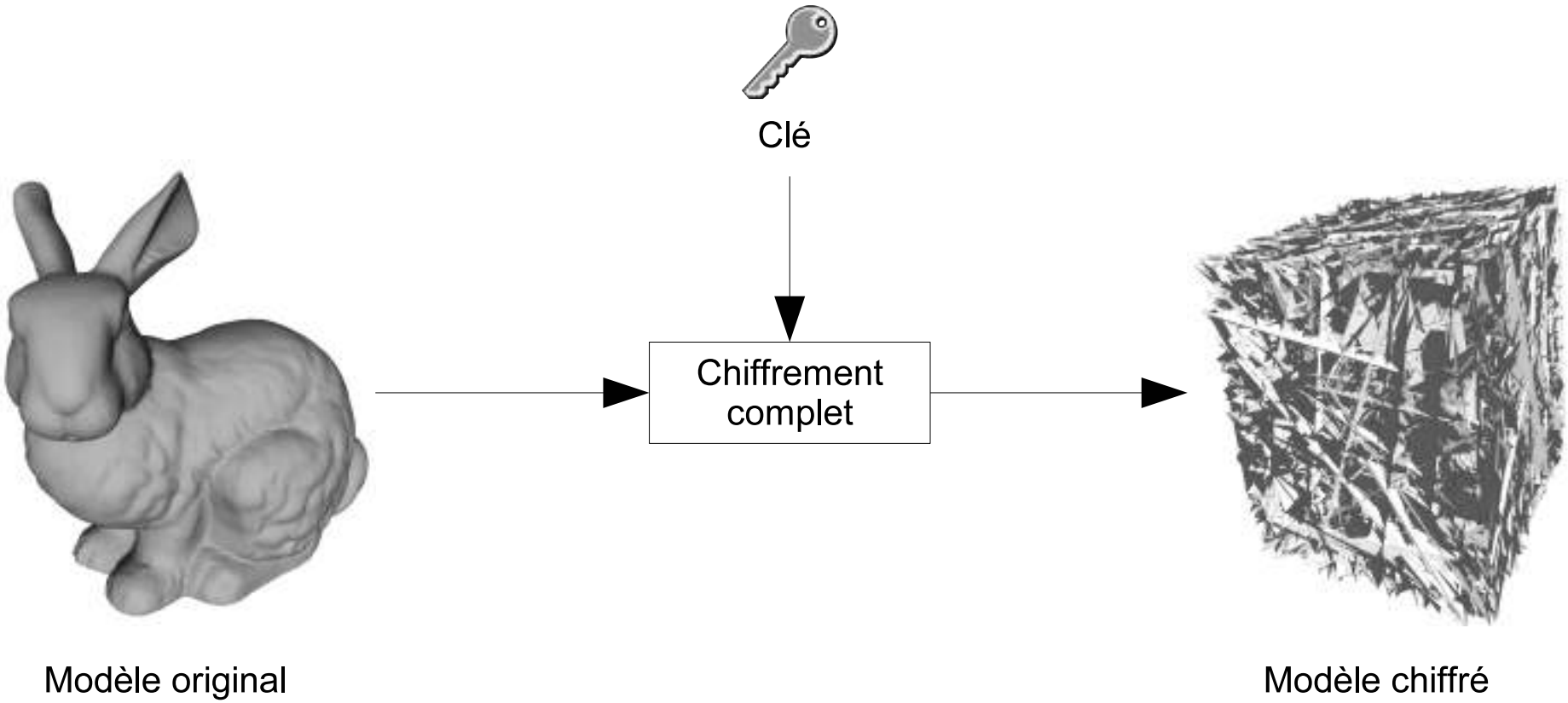


Schéma de chiffrement complet.

Cryptographie

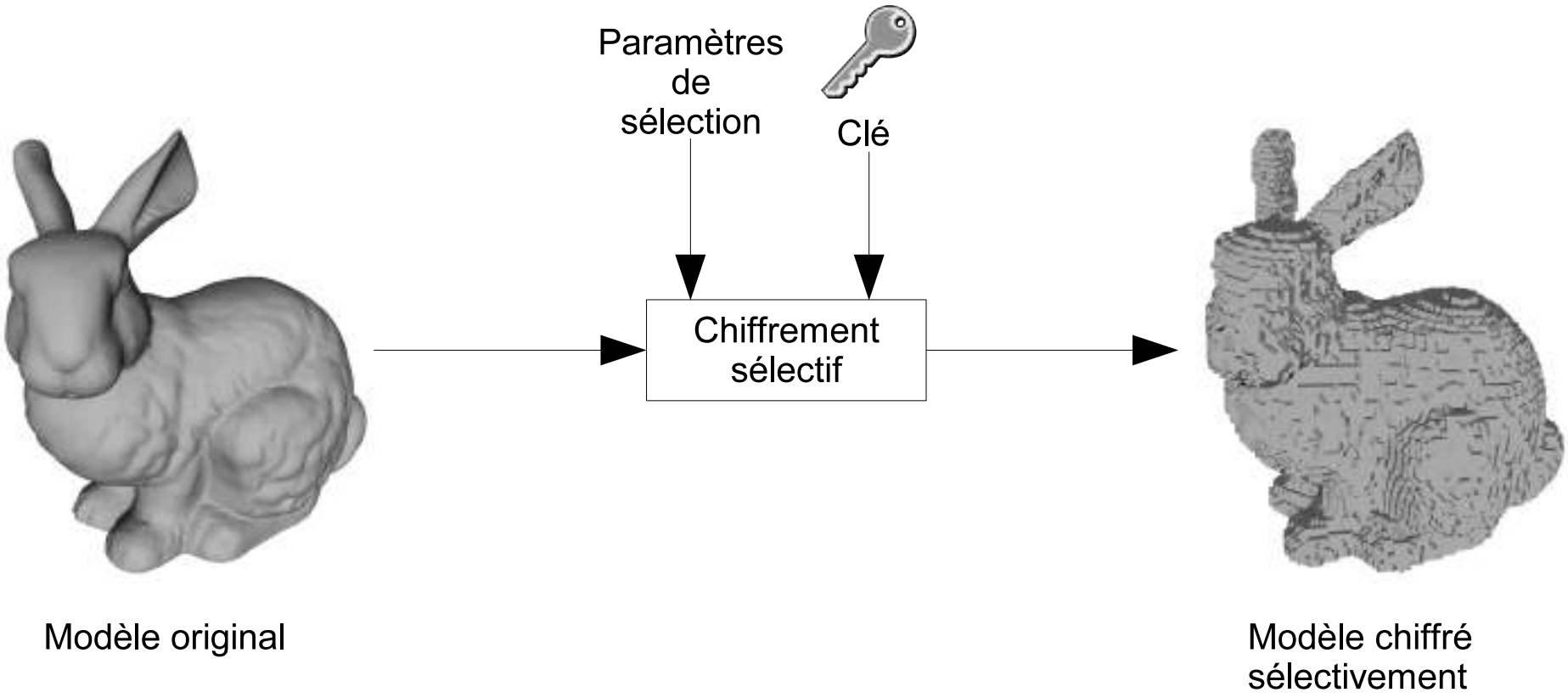


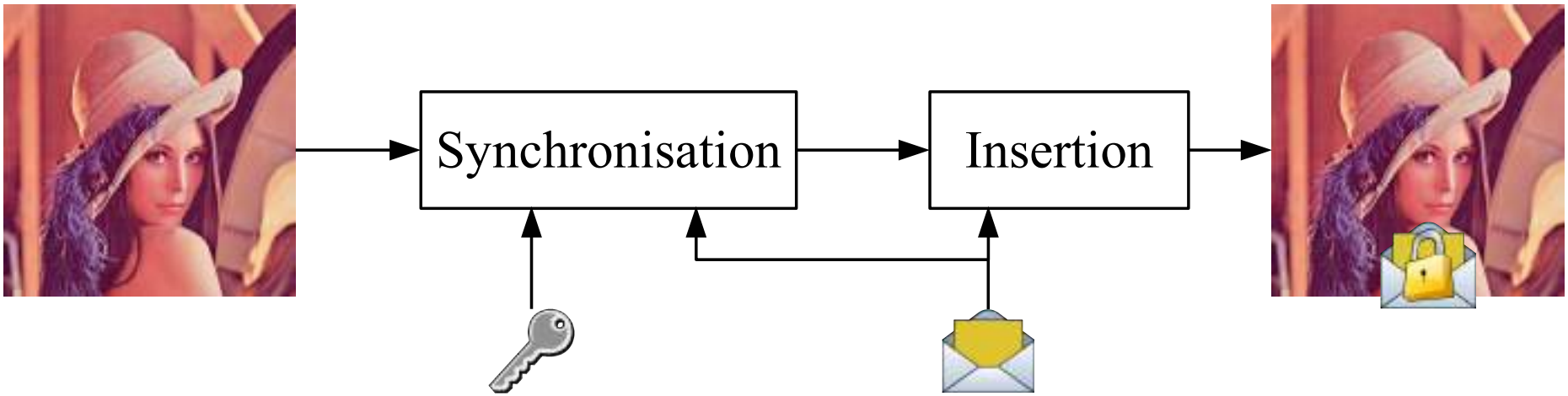
Schéma de chiffrement sélectif.

Méthodes d'insertion de données cachées

Propriétés

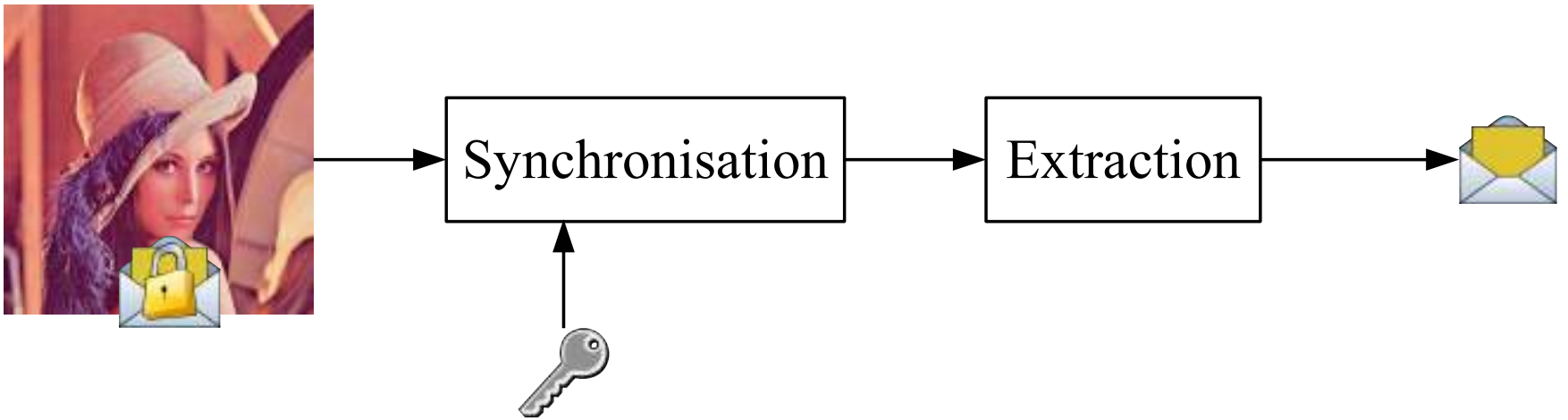
- Compatible avec le format : lisible avec les logiciels standards.
- Aveugle, semi-aveugle, non-aveugle : a priori sur le média.
- Confidentialité.
- Intégrité.
- Disponibilité.
- Authentification.
- Non-répudiation.

Schéma d'une méthode d'insertion de données cachées



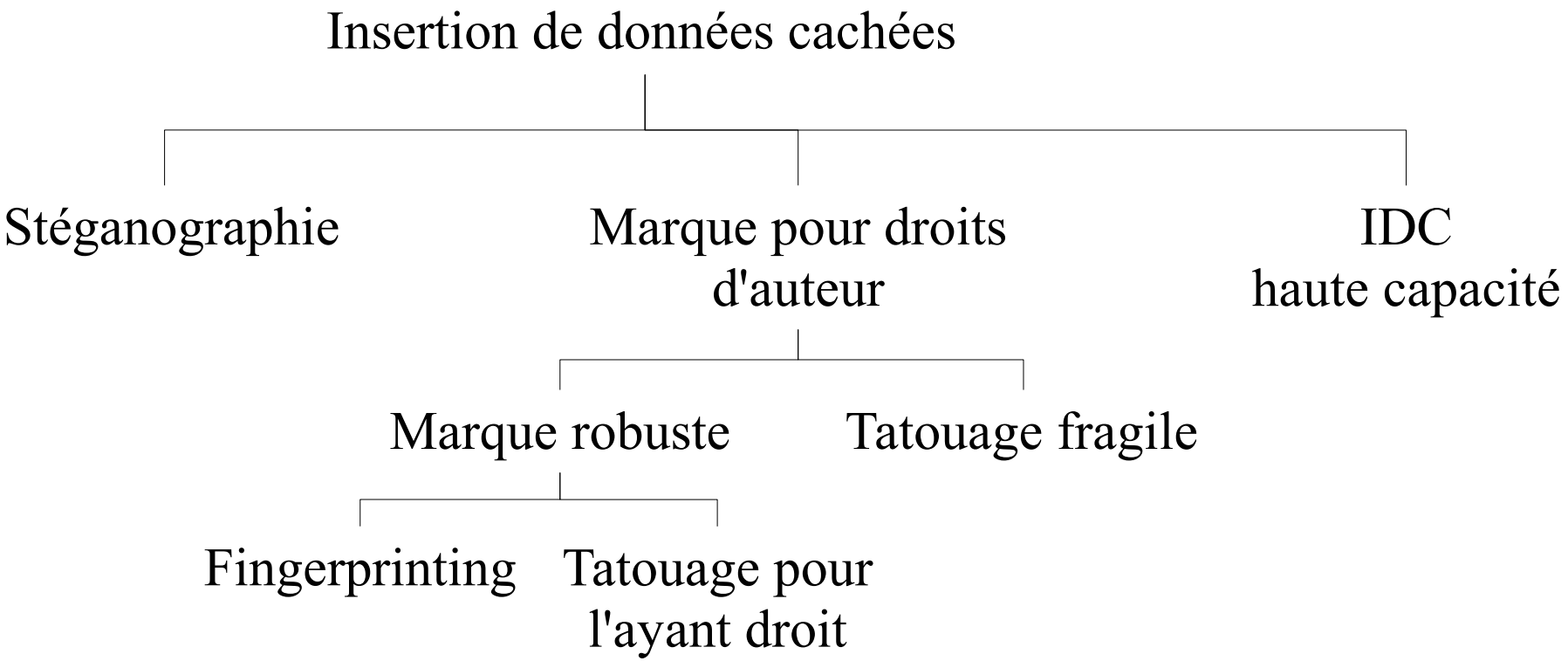
L'image est marquée avec un message secret à l'aide d'une clé secrète.

Schéma d'une méthode d'extraction de données cachées



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

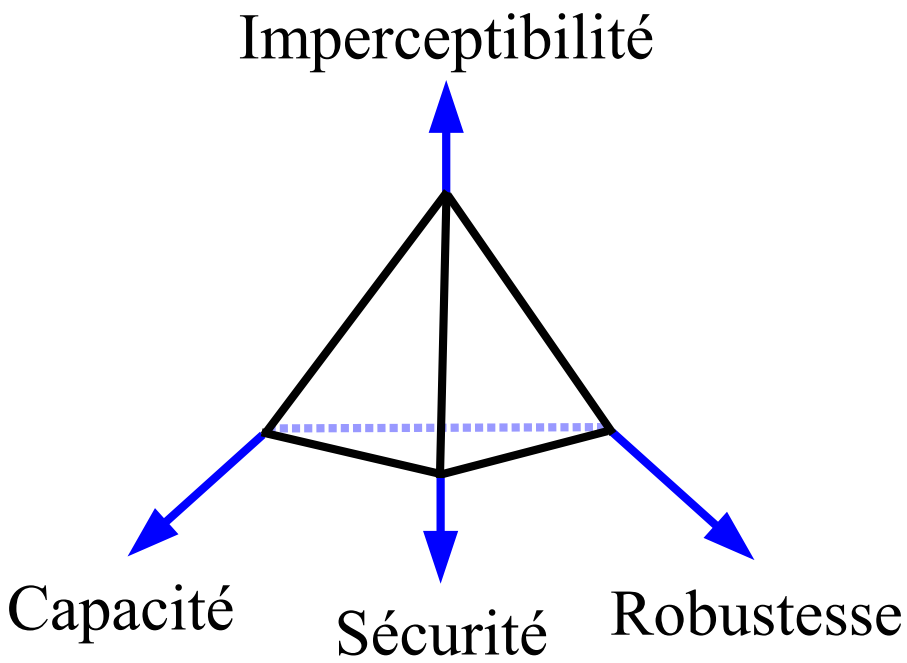
Classification des méthodes d'insertion de données cachées



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 cette différence entre les objets supports et les objets marqués.

Schéma des compromis



Comparaison entre une 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 important
Capacité	Haute	Moindre

Évaluation de la robustesse

Nombre d'erreurs binaires entre m et m'

$$NE = |m| - |m'| + \sum_{i=0}^{|m|-1} \begin{cases} 1 \ si & m_i \neq m'_i \\ 0 \ sinon \end{cases} \tag{16}$$

BER

$$BER = \frac{NE}{|m|} \tag{17}$$

Capacité des méthodes

Méthode	Capacité	Robustesse
0-bits	1 bit	+++
Tatouage	identifiant : 64, 128 bits	++
Fingerprinting	borne min nombre d'utilisateurs	+
Tatouage fragile	max	-
Stéganographie	borne max pour rester indétectable	- -
Haute capacité	max	- -

Imperceptibilité

Évaluation à l'aide de métriques

- Métriques subjectives
  - Distance
  - Percepetuelle
- Métriques objectives
  - MOS (score d'opinion moyen)

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]

Propriétés

Réversibilité

- Imagerie médicale
- Applications militaires
- CAO

Aveugle

- Ne nécessite pas de connaissance *a priori*
- Semi-aveugle (partie de l'information disponible)
- Non-aveugle plus robuste (extraction par différence)

Attaques sur l'insertion de données cachées

Attaques[1]

- Les attaques de suppression qui ont pour but de supprimer la marque.
- Les attaques géométriques qui n'ont pas pour but de supprimer la marque elle même, mais de faire perdre la synchronisation des données cachées.
- Les attaques cryptographiques qui ont pour but d'extraire le message ou les paramètres secrets utilisés pour l'insertion.
- Les attaques de protocole qui ont pour but d'attaquer le concept de tatouage en lui même.

[1] Voloshynovskiy.

Stéganographie & stéganalyse

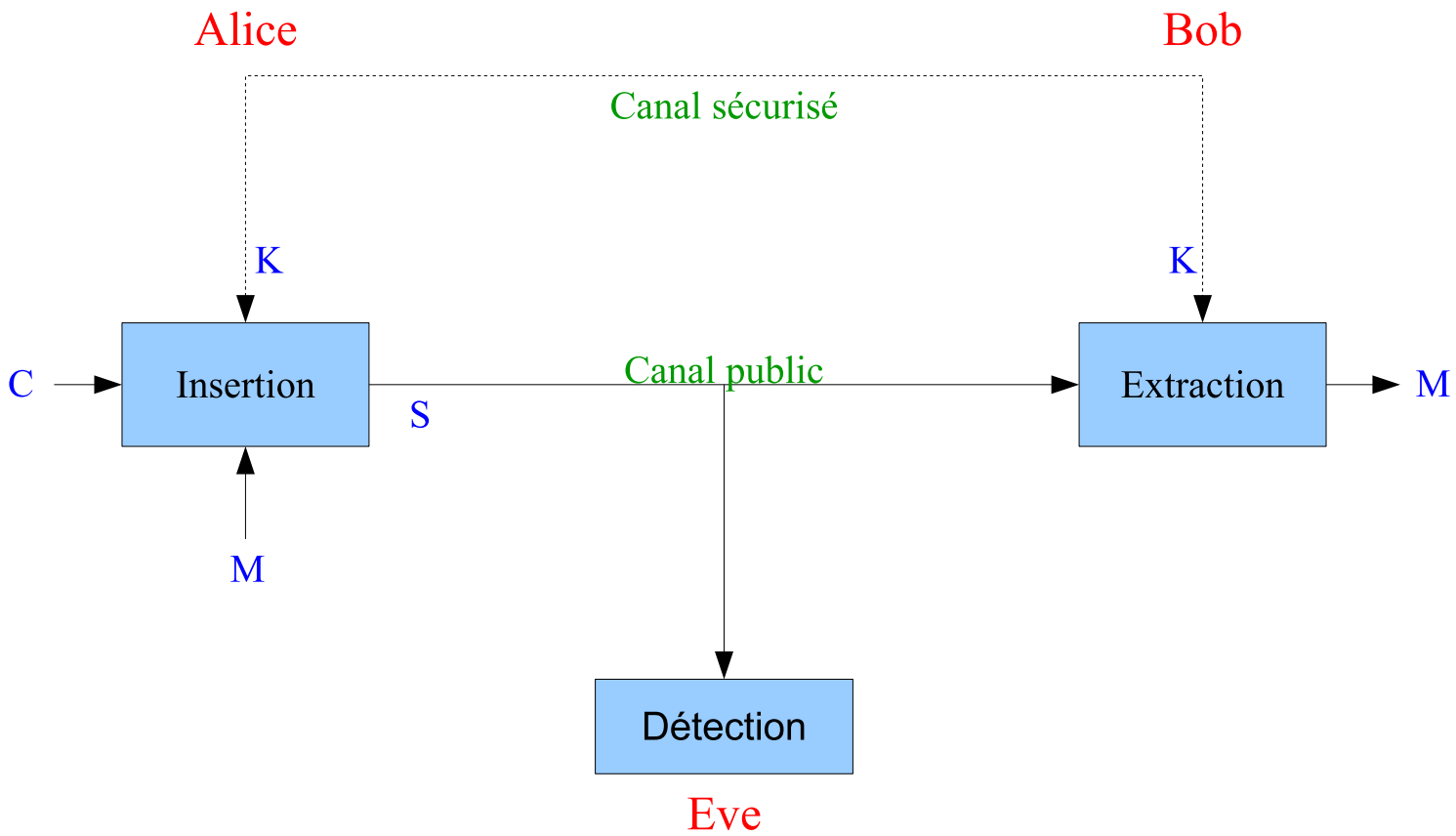


Schéma d'une méthode de stéganographie, le média support C (cover), le stego-média S, le message secret M, et la clé secrète K (key)

Section 3

Insertion de données cachées 3D

1 Maillage 3D

2 Protection des médias visuels

3 Insertion de données cachées 3D
- Généralités
- Domaine d'insertion
- Synchronisation
- Problème de causalité
- Méthodes robustes
- Méthodes haute-capacité
- Exemple méthode haute capacité

4 Conclusion et perspectives

Principes

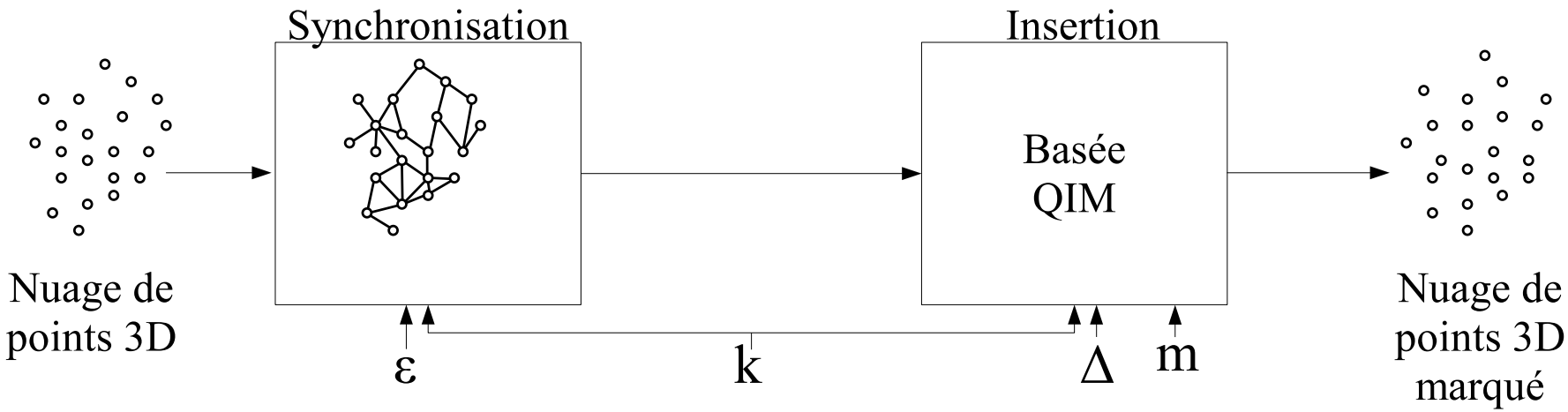
Étapes :

- Synchronisation 3D
- Insertion sur une primitive (Sommets, arrêtes, facettes...)

Difficultés par rapport aux médias visuels 2D :

- Choix de la primitive ? (2D pixels)
- Comment définir un ordre sur cette primitive ? (2D évident)
- Problème de causalité

Exemple

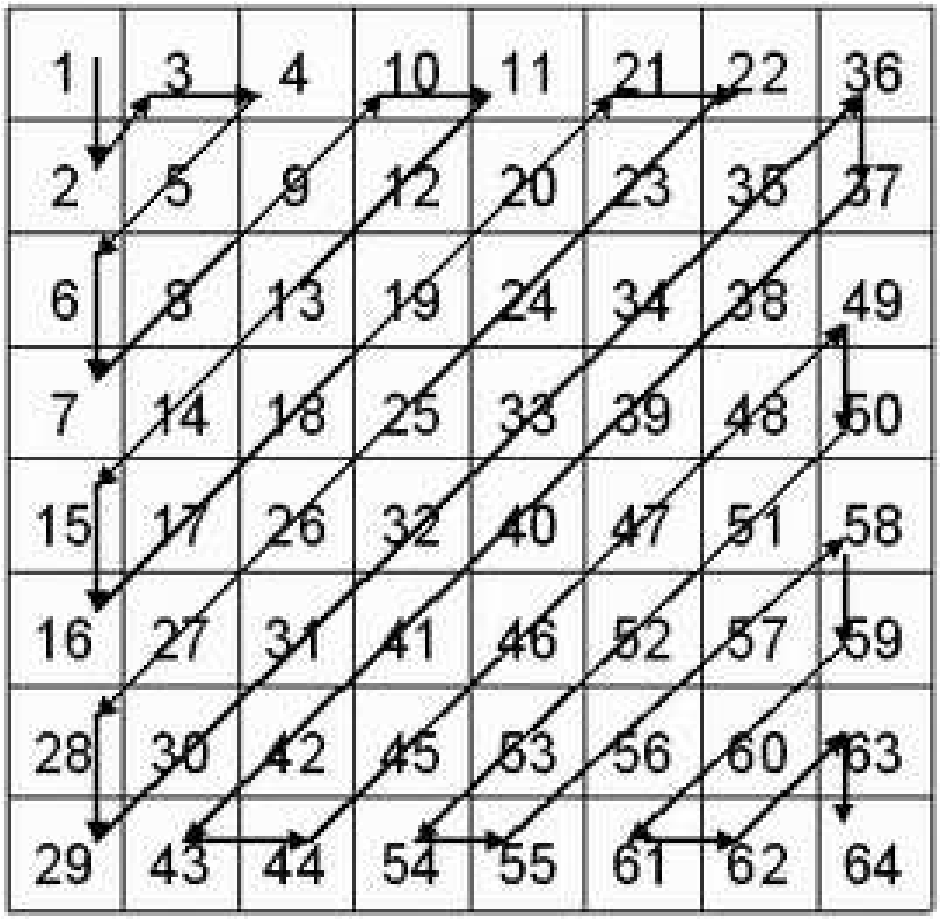


Étapes de l'insertion de données cachées 3D.

Domaine spatial vs 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 important
Capacité	Haute	Moindre

Synchronisation 2D



Chemin en ZigZag d'une image 2D.

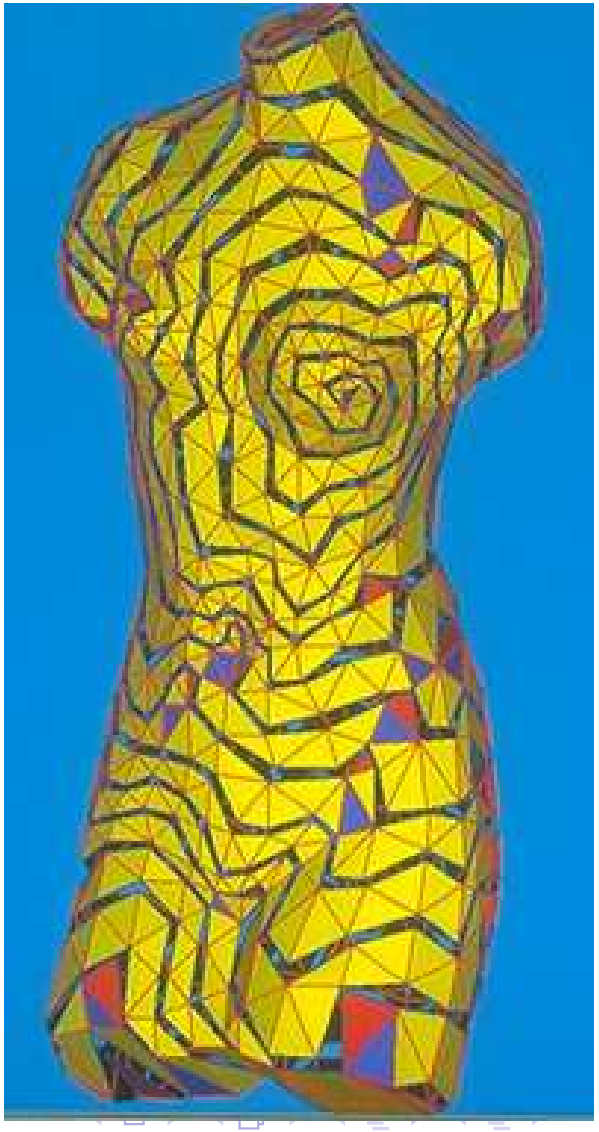
Exemple de chemin unique :

- Lignes et colonnes.
- ZigZag.
- Blocs.

Synchronisation 3D

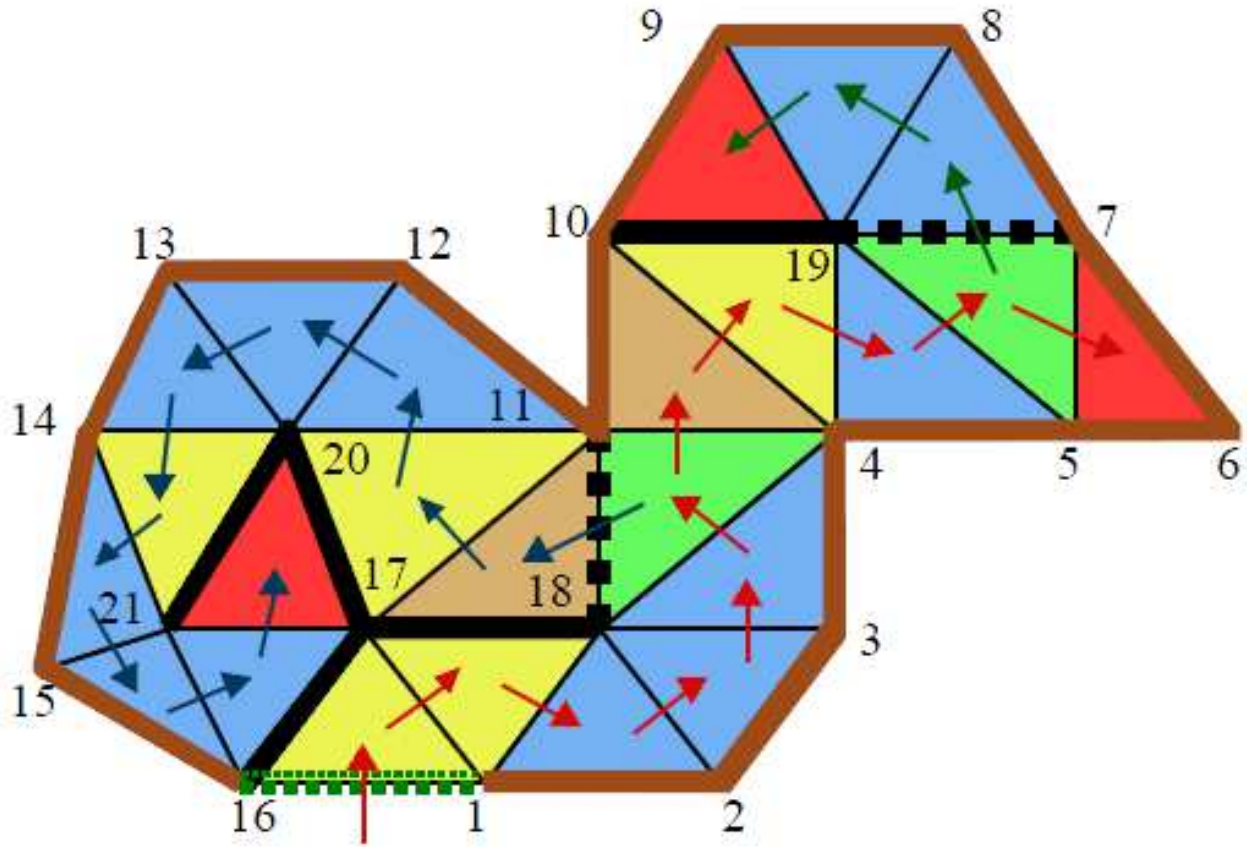
Ordonnancement facettes :

- “Edgebreaker" [Rossignac :1999] pour la compression
- TSPS (Triangle Strip Peeling Sequence) [Ohbuchi :1997]
- parcours en largeur/ profondeur



Synchronisation 3D

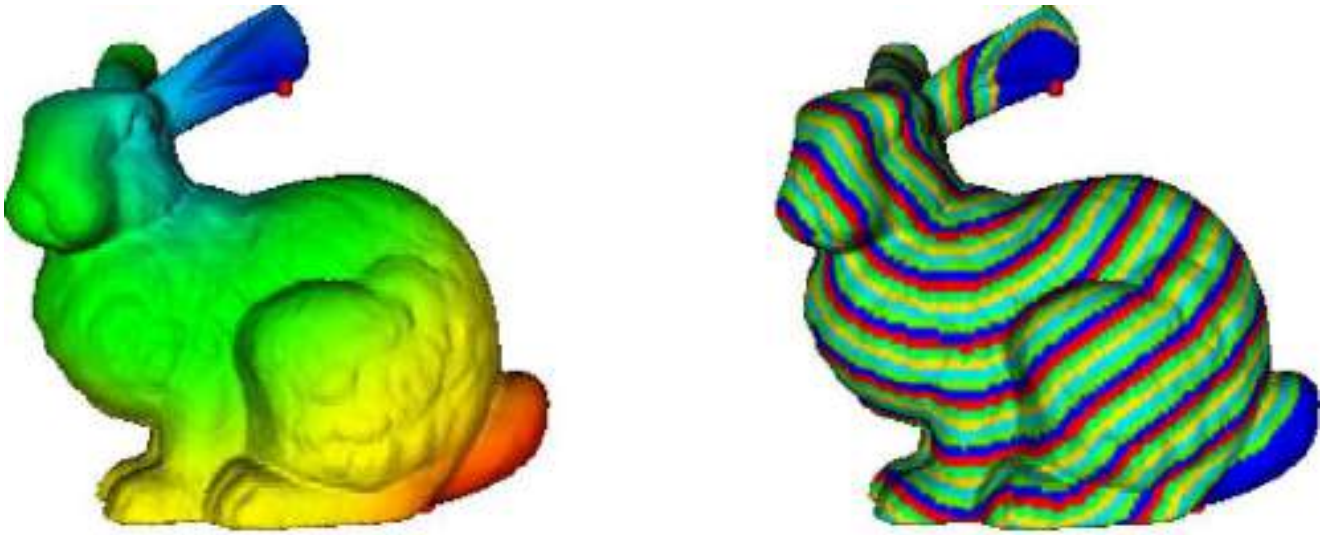
Ordonnancement facettes :



Déroulement des facettes

Synchronisation 3D

Ordonnancement par patchs :



(a) (b)

Iso-geodesic mesh strip generation [Luo :2011]

Synchronisation 3D

Ordonnancement par patchs :

Patchs [Wang :2009]

Synchronisation 3D

Ordonnancement par graphes :

- Parcours en largeur, en profondeur
- Arbre couvrant de poids minimum
- Chemin hamiltonien

Synchronisation 3D

(a) (b)

a) Nuage de 3006 points 3D, b) ACPME construit sur le nuage de points

Synchronisation 3D

(a) (b)

a) Nuage de 3006 points 3D, b) Chemin hamiltonien construit sur le nuage de points

Influence de l'insertion sur la synchronisation

Définition :

Un problème de causalité survient lorsque l'insertion modifie les caractéristiques utilisées pour la synchronisation. Ce qui implique une erreur partielle ou totale à l'extraction.

Exemples :

- Déplacement du centre de gravité
- Déplacement des points du graphes

Domaines d'insertion

Support message

- Géométrie (statistique)
- Domaine transformé

Références

Domaine spatial

- Histogramme des normales [Benedens 1999]
- Histogramme des distances radiales [Zafeiriou *et al.* 2005]
- Histogramme des distances au centre [Cho *et al.* 2007] [Bors et Luo 2013]

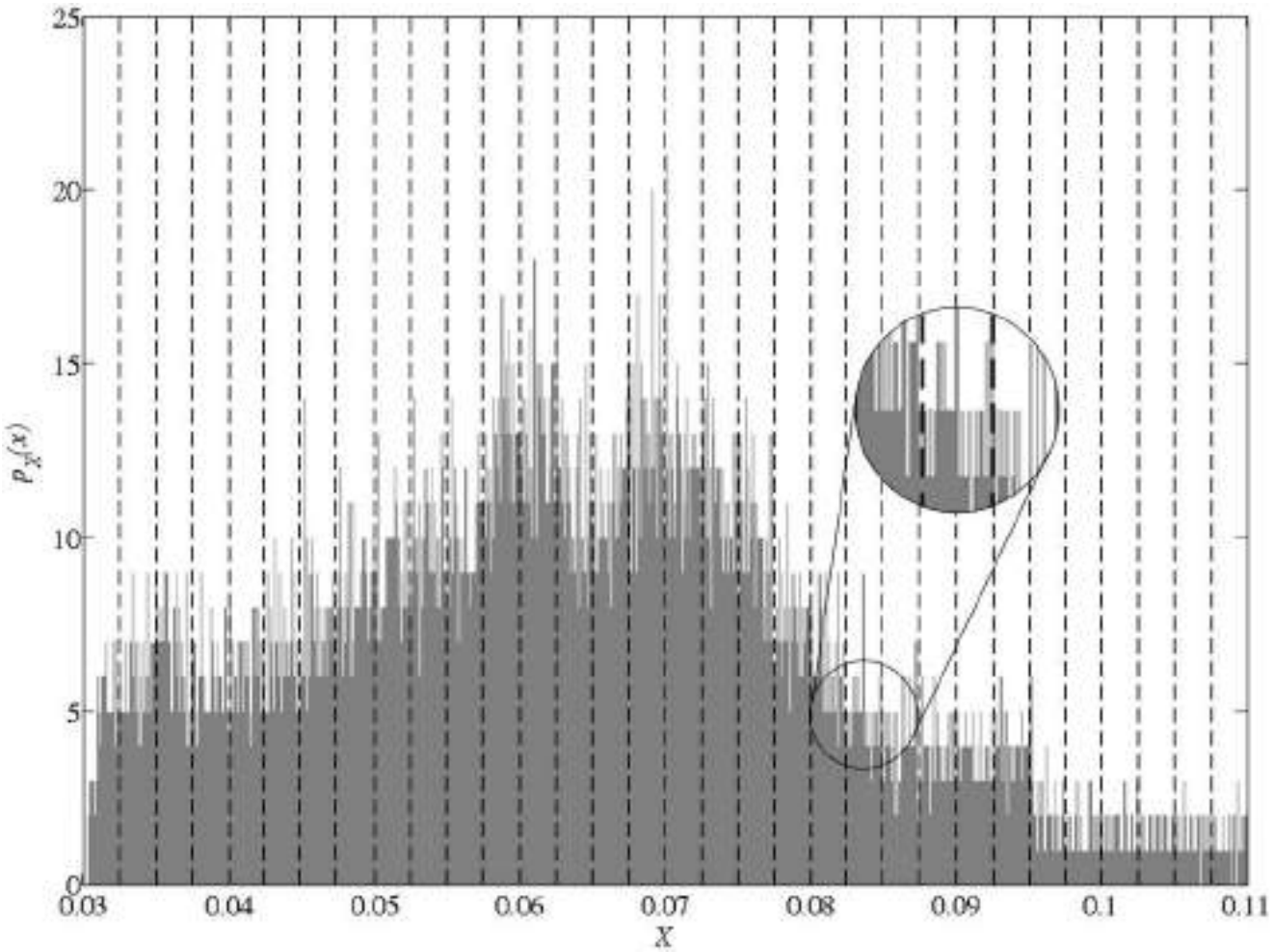
Références

Domaine transformé

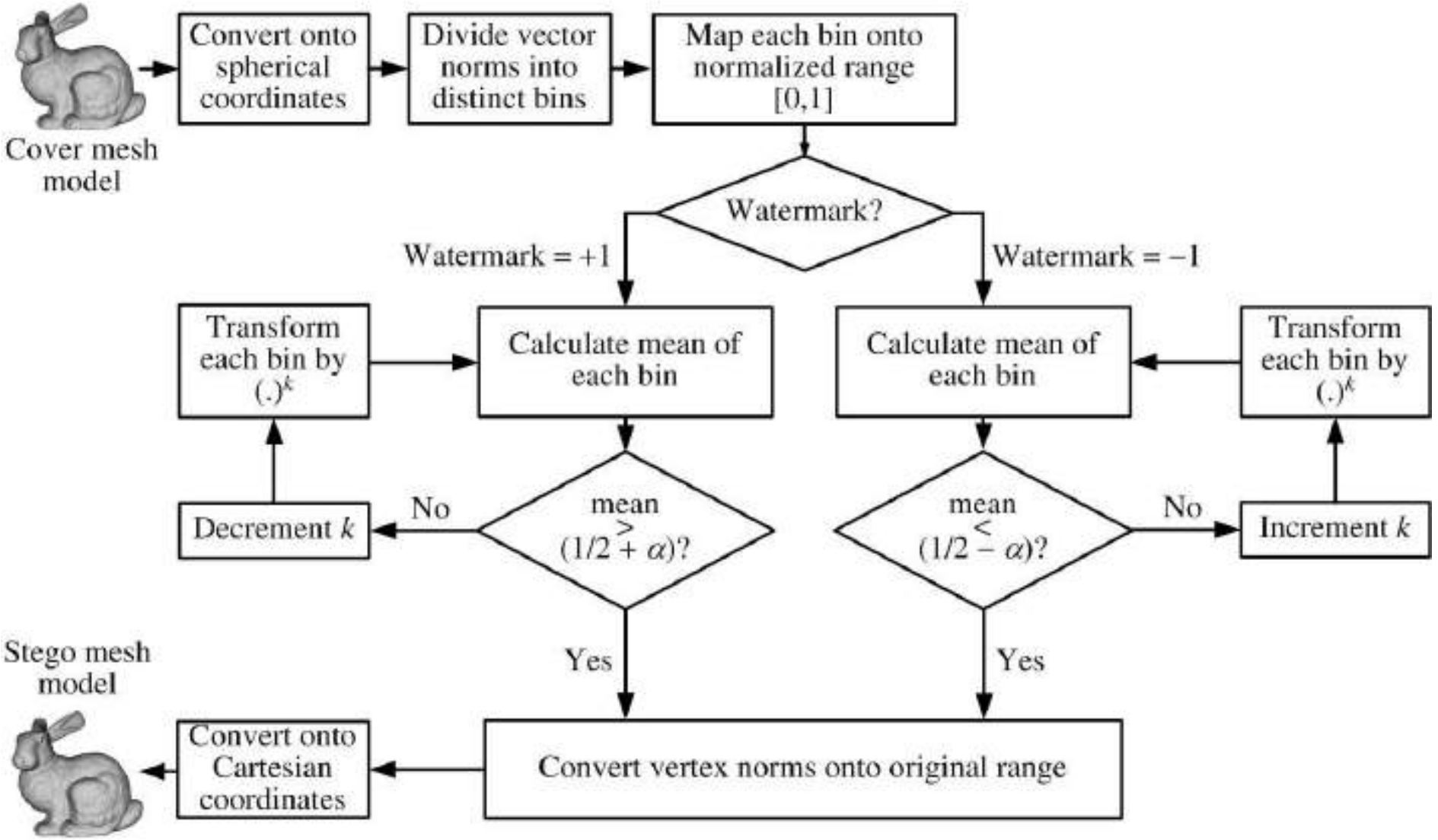
- Différence des coefficients de Laplacienne[Ohbuchi *et al.* 2001] [Lavoué *et al.* 2007]
- MHT (Manifold Harmonics Transform) [Liu *et al.* 2008] [Wang *et al.* 2009]
- Harmoniques sphériques [Konstantinides *et al.* 2009]
- Décomposition multi-résolution [Praun *et al.* 1999] [Ucchedu *et al.* 2004] [Wang *et al.* 2008]

Méthode statistique

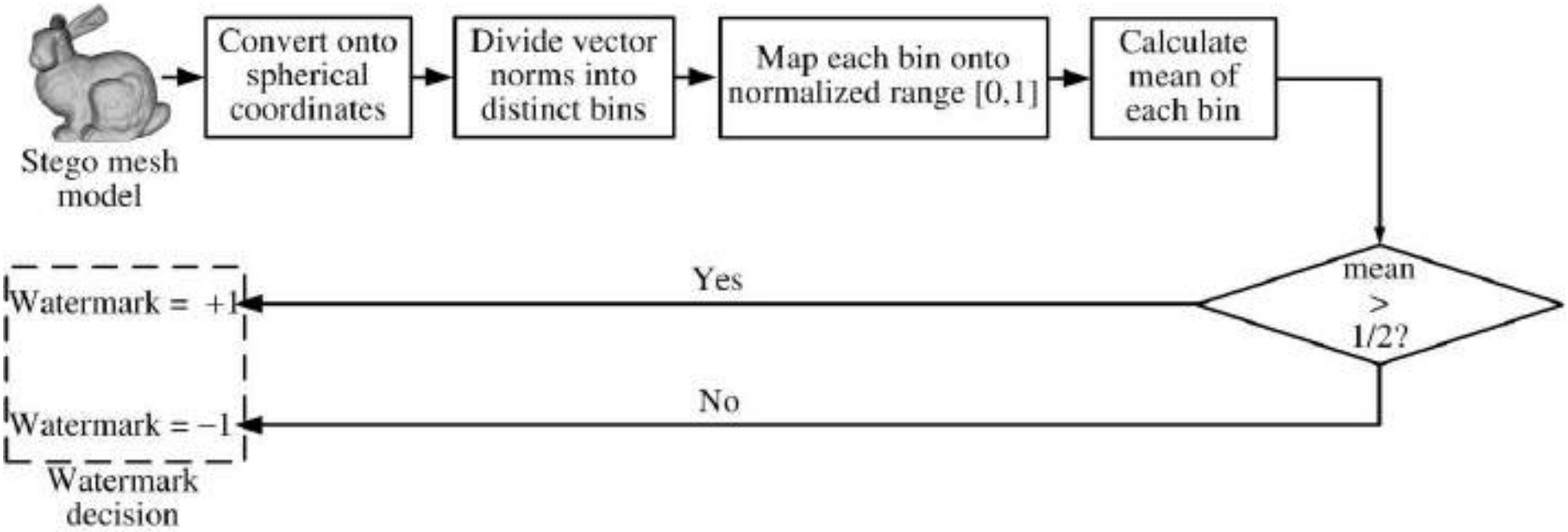
Méthode de Cho



Méthode de Cho : Insertion



Méthode de Cho : Extraction



Méthode de Cho : Étapes

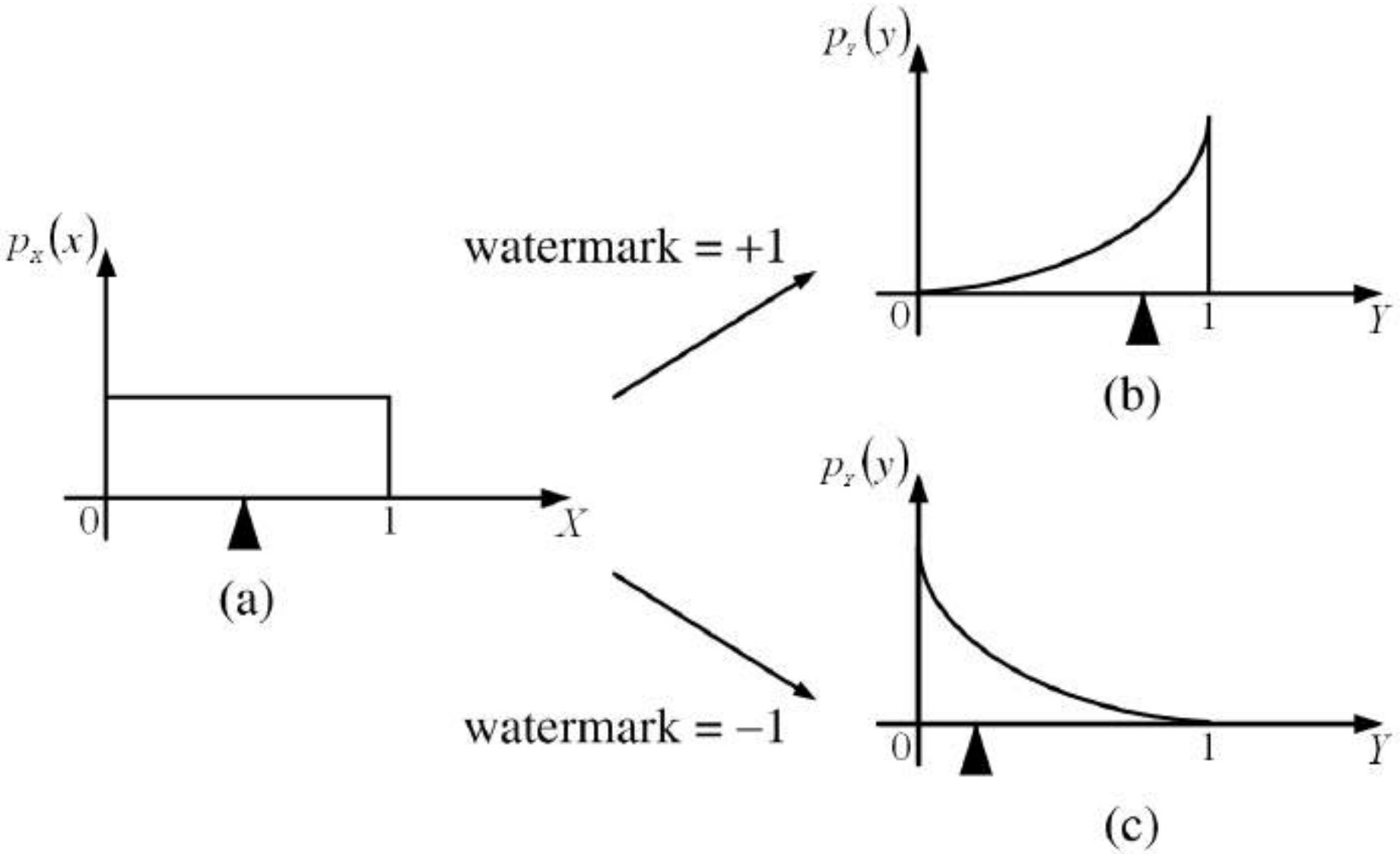
1. Calculer le centre de gravité g
2. Transformation coordonnées sphériques par rapport à g
3. Divisions en n classes (Bins)
4. Normalisation des bins entre $[0, 1]$
5. Insertion itérative dans chaque bins en fonction du message

Méthode de Cho : Modifier les statistiques

Statistiques :

- Moyenne
- Variance

Méthode de Cho : Modifier la moyenne



Méthode de Cho : Modifier la moyenne

Modifier la moyenne :

α force insertion / sensibilité aux erreurs

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

Méthode de Cho : Modifier la moyenne

Modifier la moyenne :

$$\rho'_{n,j} = (\rho_{n,j})^{k_n}$$

où k_n est calculé comme :

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

Méthode de Cho : Modifier la moyenne

Problème :

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

Solution :

Insertion itérative

Méthode de Cho : Modifier la moyenne

Problème :

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

Solution :

Insertion itérative

Méthode de Cho : Modifier la moyenne

Insertion itérative 1 :

1. $k_n = 1$
2. $\rho'_{n,j} = (\rho_{n,j})^{k_n}$
3. $m'_n = \frac{1}{M_n} \sum_{j=0}^{M_n-1} \rho'_{n,j}$
4. si $m'_n < \frac{1}{2} + \alpha$, $k_n = k_n - \Delta k$ aller à 2
5. $\rho_{n,j} = \rho'_{n,j}$

Méthode de Cho : Fin

Transformation inverse

- Normalisation inverse des bins
- Transformation coordonnées cartésiens

Méthode de Cho : Bilan

Bilan

- Insertion longue (fonction de Δk) /extraction rapide
- Robuste / faible capacité / aveugle
- Force d'insertion laissée à l'utilisateur (méthode [Bors et Luo 2013])

Méthodes haute capacité domaine spatial

Méthode	capacité théorique pour un maillage de $\|V\|$ sommets	capacité bps
Cayre et Macq 2003	$\|V\|$	< 1
Wang et Cheng 2005	$3 \times \|V\|$	3
Cheng et Wang 2007	$\|V\| \times \alpha$ un entier donné	3-6
Chao *et. al* 2009	$69 \times \|V\|$	40
Li *et. al* 2011	$\|P\| \times \lfloor \log_2(M \times N) \rfloor$	50
Tsai 2015	$\|P\| \times \lfloor \log_2(M \times M) \rfloor$	> 8
Gao *et. al* 2012	$3 \times (H - L + 1)\Omega$	1-2
Yang *et. al* 2013	$\|V\|\times$ fonction du facteur de tolérance aux distorsions ε	45-60
Wang and Wang 2006	$1.5 \times \|V\|$	< 1.5

Schéma d'insertion haute capacité

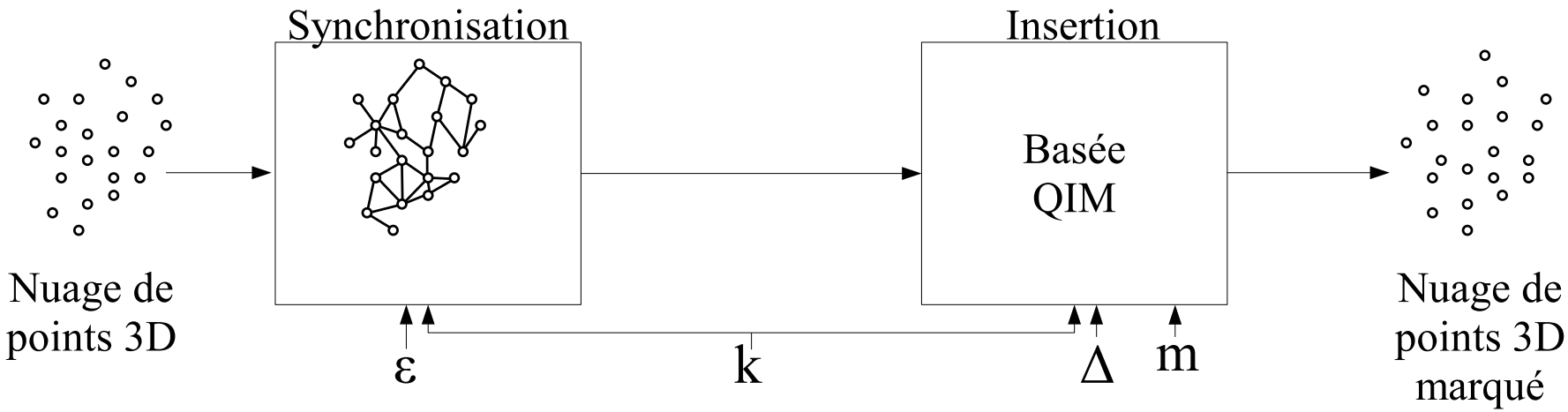
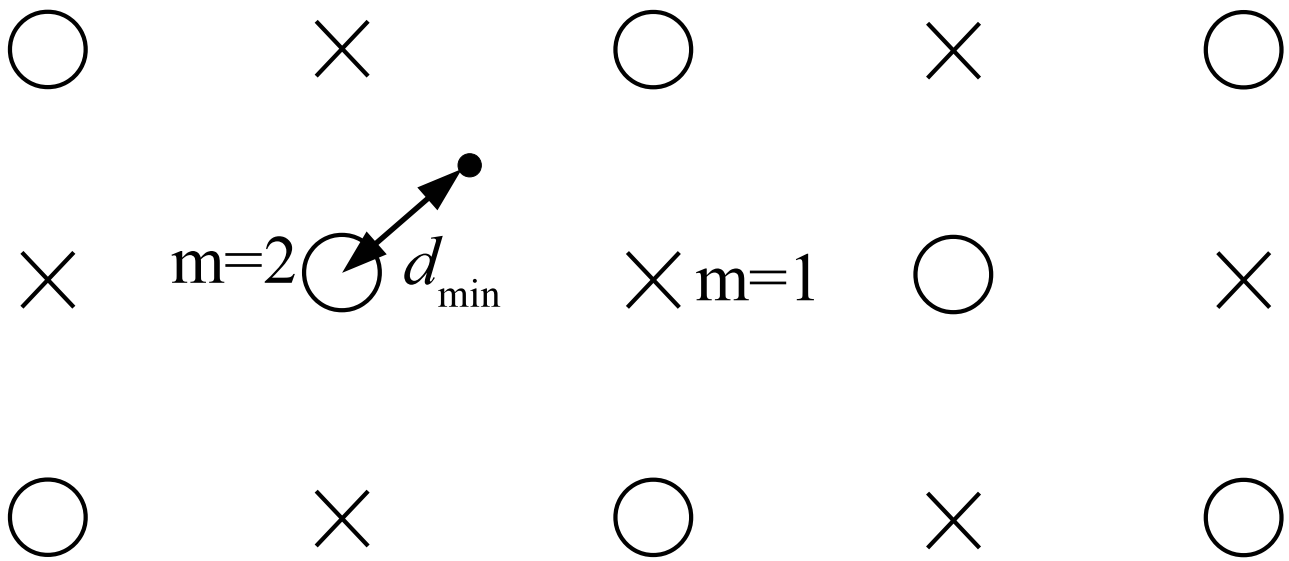


Schéma d'insertion haute capacité



Idées

Insertion haute capacité dans la géométrie

- Utiliser le plongement 3D
- Synchronisation des sommets
- Méthode d'insertion sur les sommets

Synchronisation

Ordonnancement des sommets

- PCA : recalage

Insertion

Insertion par sommets

- LSB (bits de poids faibles) [Yang :2014]
- Subdivisions PCA [Chao :2009]
- Insertion sur les arrêtes du chemin [Itier :2015]

Construction d'un chemin Hamiltonien

Pour un maillage de n sommets :

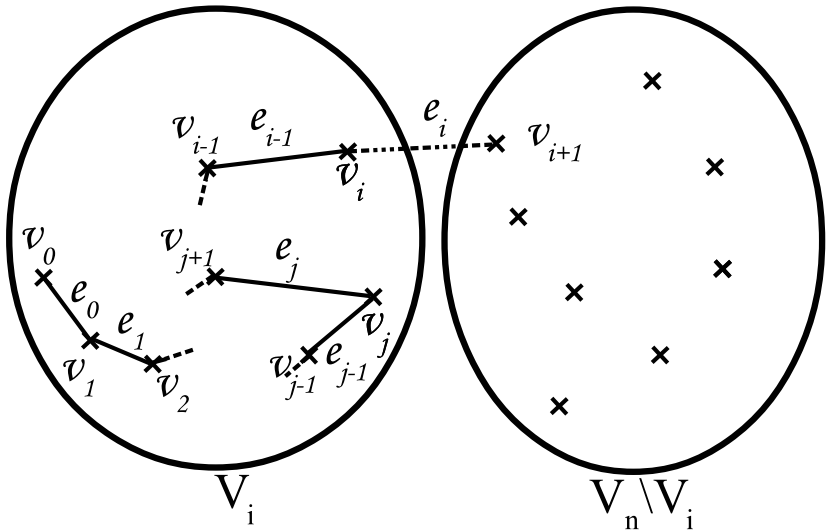
On définit : G_n un graphe, $G_n = (V_n, E_m, \omega)$

- V_n l'ensemble des sommets.
- E_m l'ensemble des arêtes $\neq$ de la topologie, $m = n(n-1)/2$.
- $\omega : E_m \rightarrow \mathbb{R}^+$ la fonction de coût sur chaque arêtes, $\omega(e) = \|e\|_2, e \in E_m$.

Construction d'un chemin Hamiltonien

A l'étape i :

- P_i sous chemin Hamiltonien, $P_i = (V_i, E_i)$.
- V_i ensemble des sommets.
- E_i ensemble des arrêtes.

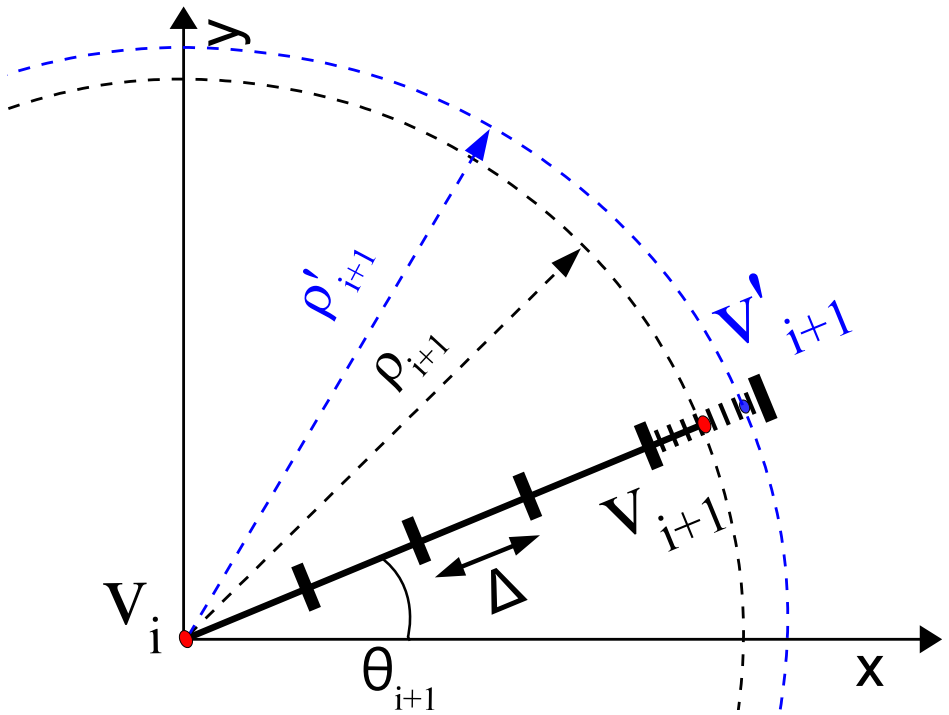


État du système à $t = i$.

Insertion

Déplacement

- Δ borne de déplacement
- Coordonnés sphériques : $v_i(x_i, y_i, z_i) = v_i(\rho_i, \theta_i, \phi_i)$

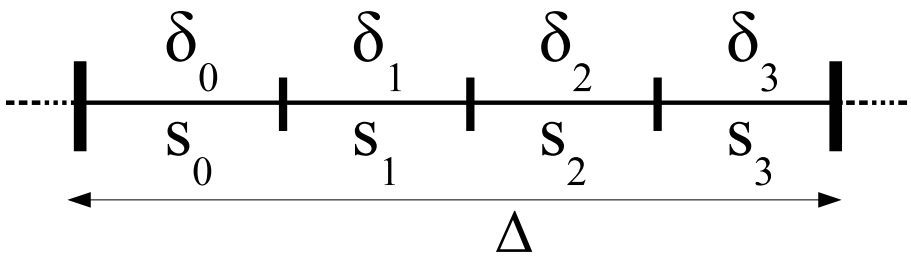


Déplacement ρ_{i+1}, projection sur un plan.

Insertion

Insertion uniforme

- q base.
- Message $\mathbf{M}$ de taille $|\mathbf{M}| < n/2$ sur un alphabet $\mathcal{S} = \{s_0, ..., s_{q-1}\}$
- $s_j \in \mathbf{M}$.
- Probabilité d'apparition d'une lettre : $p(s_j) = \frac{|\mathbf{M}|_{s_j}}{|\mathbf{M}|} = \frac{1}{|\mathcal{S}|}$
- $|\delta_{s_j}| = \frac{\Delta}{q}$ taille d'un sous intervalle δ_{s_j}



Codage uniforme d'une valeur, $q = 4$

Insertion

Borne inférieure de l'intervalle :

$$b_l = \lfloor \frac{c_{i+1}}{\Delta} \rfloor \times \Delta. \tag{18}$$

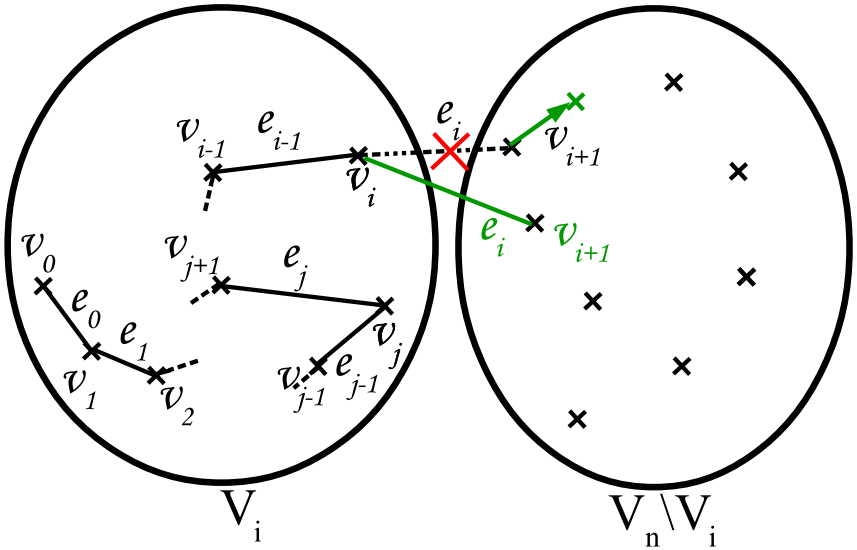
Valeur d'une coordonnée c_{i+1}

$$val(c_{i+1}) = \lfloor q(c_{i+1} - b_l) \rfloor. \tag{19}$$

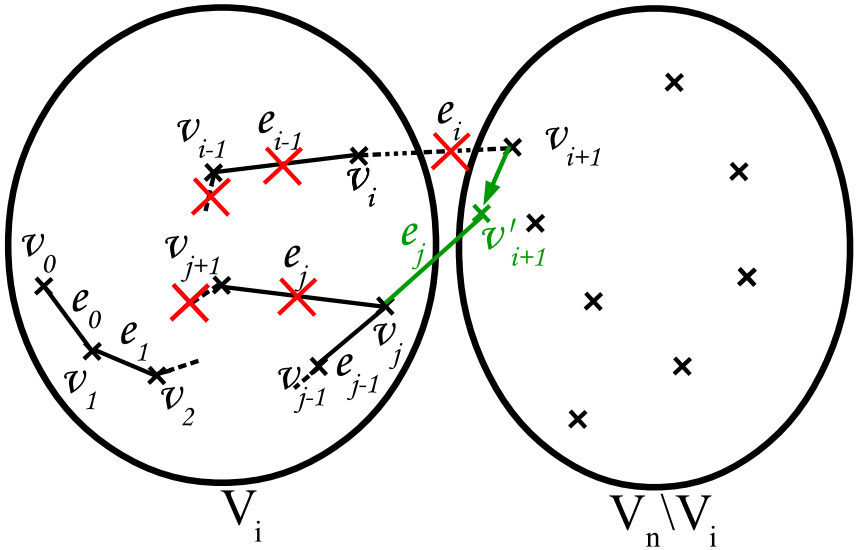
Insertion de s_j sur une coordonnée c_{i+1}

$$c'_{i+1} = \begin{cases} b_l + \frac{j\Delta}{q} & \text{if } val(c_{i+1}) < j \\ b_l + \frac{(j+1)\Delta}{q} - \gamma & \text{else,} \end{cases} \tag{20}$$

Problème de causalité

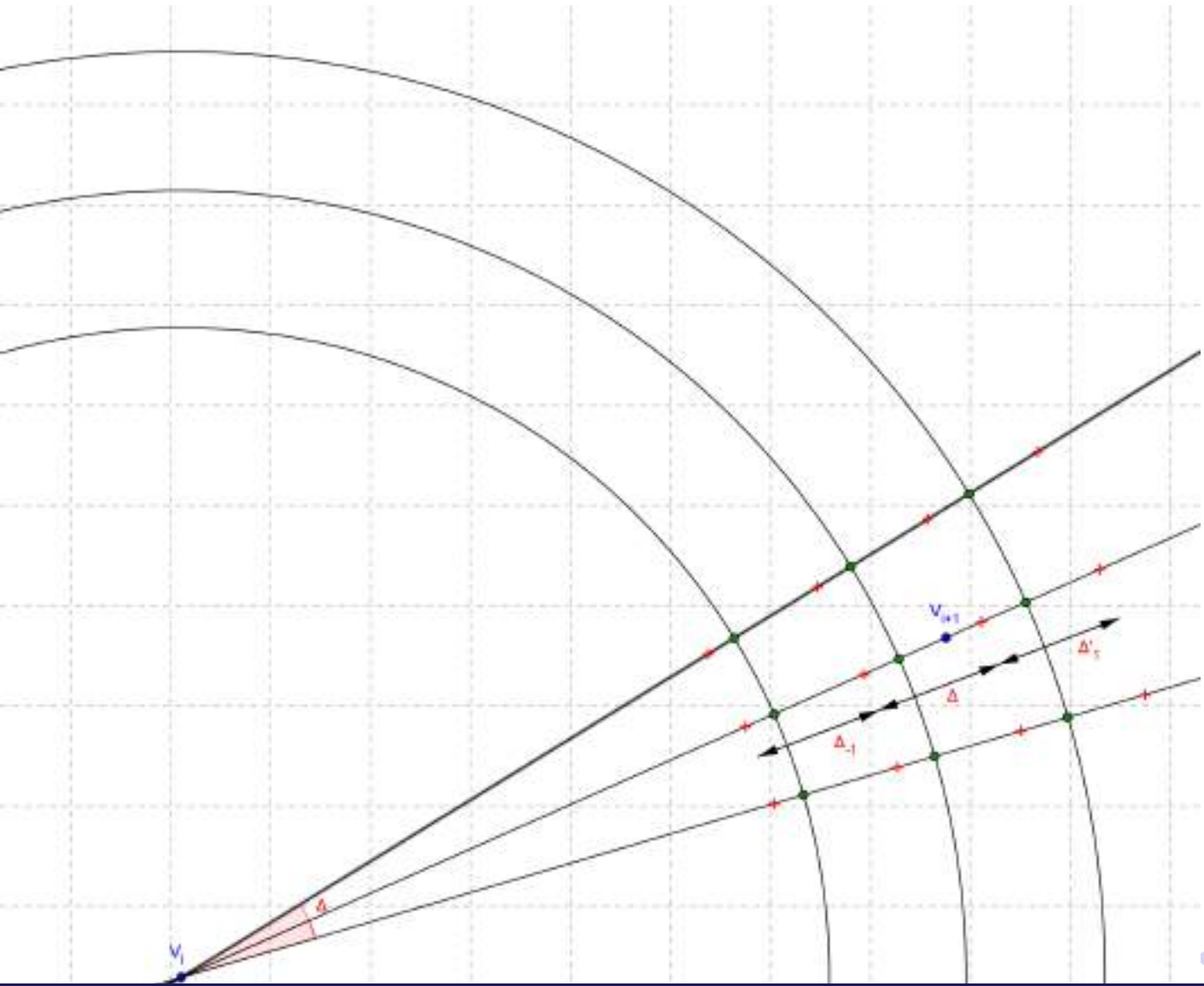


v_{i+1} est déplacé trop près du sous-chemin.



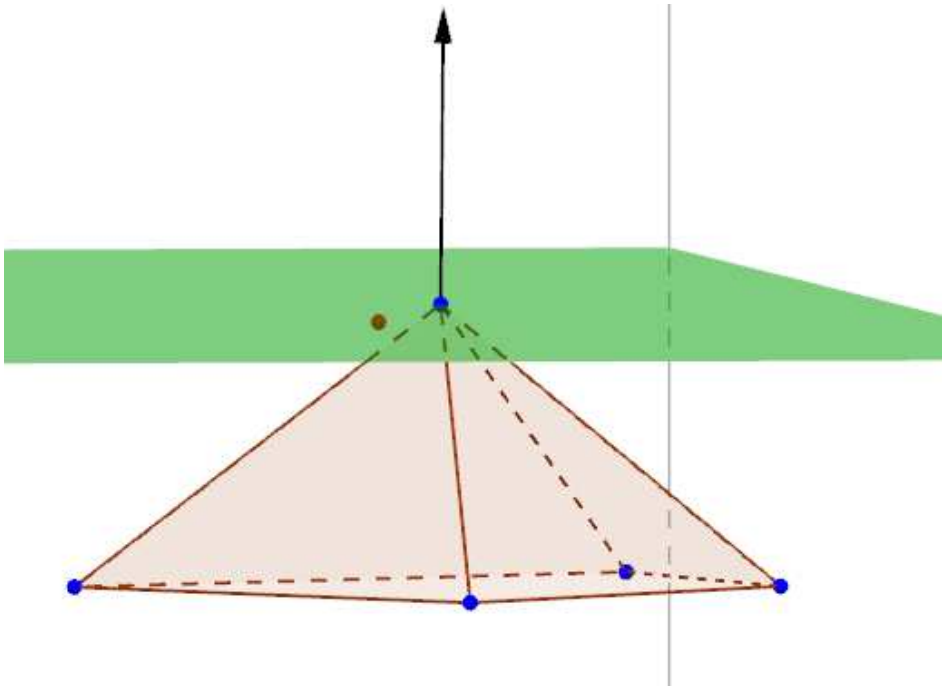
v_{i+1} est déplacé trop loin de son père.

Meilleure position



- Intervalles : Δ_{-1}, Δ_0, Δ_{+1}
- $3^3 = 27$ positions

Réduction des distorsions



Sommet $v(x_v, y_v, z_v)$
Plan P : $ax + by + cz + d$

$$d_{v,P} = \frac{|ax_v + by_v + cz_v|}{\sqrt{a^2 + b^2 + c^2}} \quad (21)$$

Exemple

(a)

(b)

a) Maillage original 100759 sommets, b) Image 224×224 pixels : 1204224 bits.

Comparaison

Table – Comparaison de l'état de l'art sur l'objet "Bunny".

Method	Capacity	Hausdorff Distance $\times 10^{-6}$	$PSNR_1$
[Chao :2009]	940464		100.57
[Gao :2012]	51408	5.48	
[Itier :2015]	54289	1.10	127.3

Section 4

Conclusion et perspectives

1 Maillage 3D

2 Protection des médias visuels

3 Insertion de données cachées 3D

4 Conclusion et perspectives

Conclusion

Conclusion

- Méthode différentes ! compromis : capacité, robustesse, distorsions
- Définir ses besoins et cas d'utilisation !

Perspectives

Perspectives

- Stéganographie/stéganalyse 3D
- Sécurité des méthodes

Robustesse $\neq$ Sécurité

- La sécurité à un scope plus large. (Ne traite pas seulement du retrait du tatouage).
- Sécurité $\neq$ Robustesse. [Perez-Freire *et al.*, 09] :
  La difficulté d'estimer les paramètres secrets de la fonction d'insertion en se basant sur l'observation d'un média tatoué.
- Existe en 2D, peu en 3D :
  Pas de méthodes robustes en 3D.

Scénarios à étudier

Diffie-Hellman[1]

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

[1] "New directions in cryptography",IEEE Transactions on Information Theory, 1976.