



Nouvelles méthodes de synchronisation de nuages de points 3D pour l'insertion de données cachées

Vincent Itier

1^{er} décembre 2015

Rapporteurs :

M. Vincent CHARVILLAT

M. Guillaume LAVOUÉ

Examineurs :

M. Stéphane BESSY

M. Jean-Marc CHASSERY

M. Gilles GESQUIÈRE

Invité :

M. Jean-Pierre PEDEBOY



Directeur de thèse :

M. William PUECH

Co-encadrant :

M. Gérard SUBSOL

- 1 Contexte
 - Problématique
 - Solution
- 2 État de l'art
 - Notions générales
 - Synchronisation 3D
 - Insertion de données cachées 3D
- 3 Contributions
 - Insertion de données cachées haute capacité
 - Chemin hamiltonien
 - Insertion
 - Codage Arithmétique Statique
 - Améliorations : robustesse, sécurité, qualité
 - Synchronisation robuste
 - Synchronisation sécurisée
- 4 Conclusion
- 5 Perspectives

STRATÉGIES

Applications CAO/SGDT pour les industries :

- de la chaussure
- de la maroquinerie
- de l'ameublement

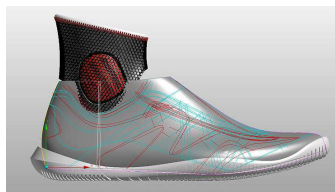
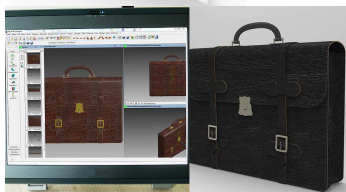


STRATEGIES



Plus de 1000 clients internationaux :

- New Balance
- Clarks
- Adidas ...

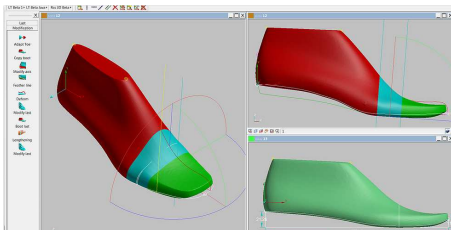


Besoin industriel : Romans CAD software

- Protection d'objets 3D
 - ▶ Autorisation d'impression 3D
 - ▶ Vérification d'intégrité
- Enrichissement de contenu
 - ▶ Méta-données : logo, texture ou lignes de style
- Création collaborative
 - ▶ Traçage, historique



STRATEGIES



Solution : Insertion de données cachées



Maillage original



Message

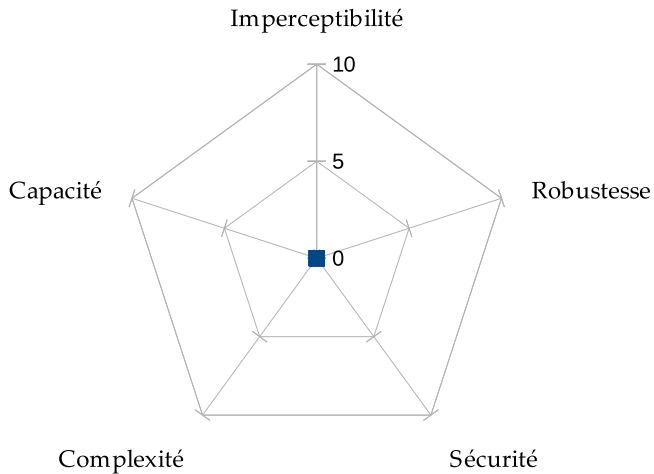


Maillage marqué

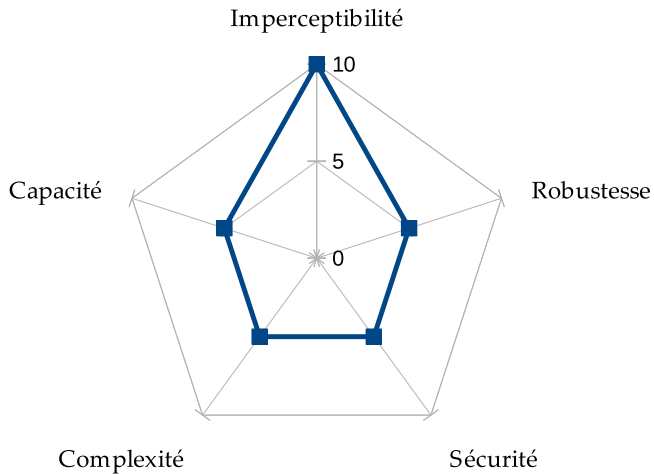
Propriétés requises

- Compatible avec le format
- Conservation de la taille en octets
- Extraction sans le maillage original

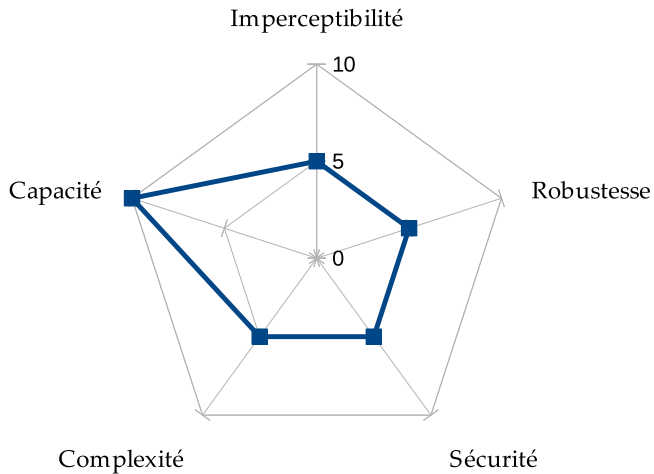
Solution : Insertion de données cachées



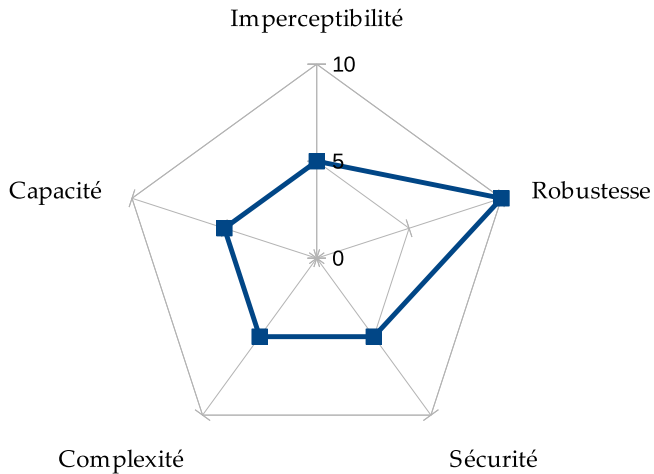
Solution : Insertion de données cachées



Solution : Insertion de données cachées



Solution : Insertion de données cachées



1 Contexte

2 État de l'art

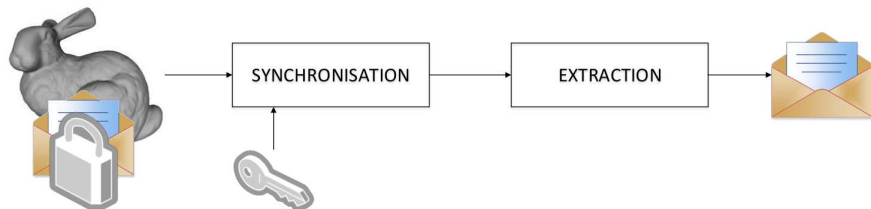
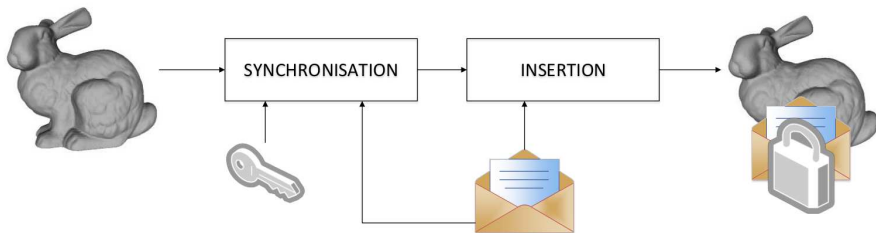
- Notions générales
- Synchronisation 3D
- Insertion de données cachées 3D

3 Contributions

4 Conclusion

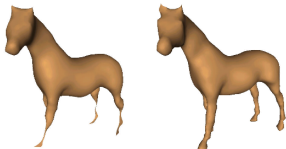
5 Perspectives

Insertions de données cachées : deux étapes

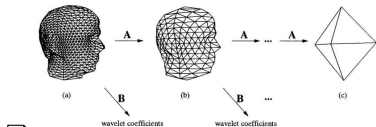
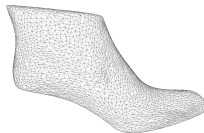
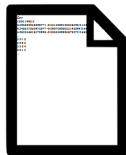


Représentation

- **Format de stockage**
 - ▶ Ordre des points et des facettes dans le fichier
- **Domaine spatial**
 - ▶ Géométrie \mathbb{R}^3
 - ▶ Connectivité
- **Domaines transformés**
 - ▶ basé analyse fréquentielle
 - ▶ basé multi-résolution



Z. Karni et C. Gotsman
Spectral Compression of Mesh Geometry.
SIGGRAPH, 2000

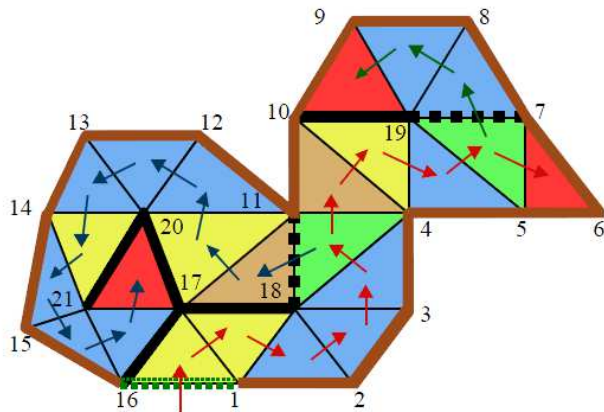


M. Lounsbery, T. D. DeRose et J. Warren
Multiresolution Analysis for Surfaces of Arbitrary Topological Type.
Transactions on Graphics, 1997

Domaine spatial, domaines transformés ?

Facteurs	Domaine spatial	Domaines transformés
Imperceptibilité	Contrôlable	Contrôle indirect
Robustesse	-	++
Capacité	++	-
Complexité	=	=
Sécurité	=	=

Par déroulement des facettes :



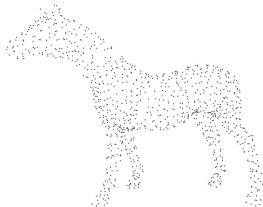
J. Rossignac

Edgebreaker: Connectivity Compression for Triangle Meshes.

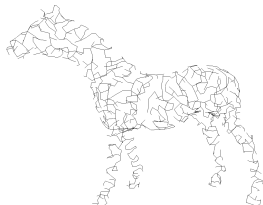
IEEE Transactions on Visualization and Computer Graphics, 1999

Basée graphe :

- Parcours en largeur, en profondeur
- Arbre Couvrant de Poids Minimum Amat *et al.* 2010 :



Nuage de 3006 points 3D



ACPM construit sur le nuage de points



P. Amat, W. Puech, S. Druon et J.-P. Pedeboy

Lossless 3D steganography based on MST and connectivity modification.
Signal Processing: Image Communication, 2010

Techniques d'insertion

- **Additif** : addition du message au support
- **Substitutif** : remplacement d'une partie du support par le message

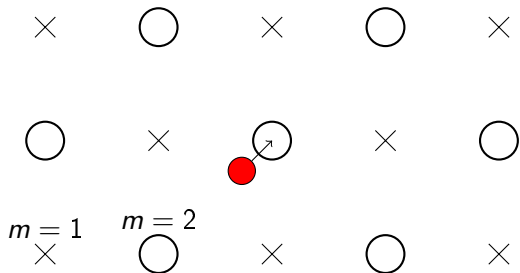


Illustration de la méthode QIM, Chen et Wornell



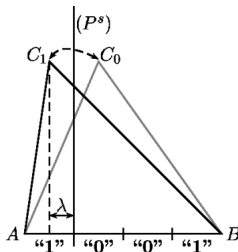
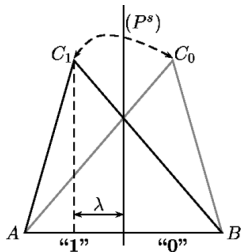
B. Chen et G. W. Wornell

Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia.

Journal of VLSI signal processing systems for signal, image and video technology, 2001

Méthode de Cayre et Macq 2003 :

- Ordonnancement des facettes
- Insertion : Déplacement d'un sommet par rapport à l'arête opposée



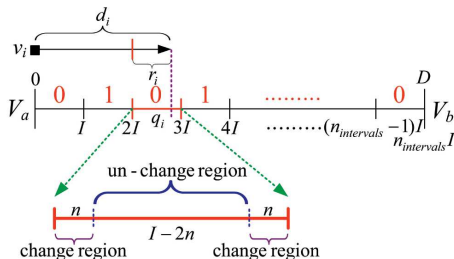
F. Cayre et B. Macq

Data hiding on 3-D triangle meshes.

IEEE Transactions on Signal Processing, 2003

Méthode de Chao *et al.* 2009 :

- Ordonnancement des facettes
- Analyse en composantes principales : V_a , V_b
- Multi-niveaux: projection dans un sous-intervalle



M.-W. Chao, C.-H. Lin, C.-W. Yu et T.-Y. Lee

A High Capacity 3D Steganography Algorithm.

IEEE Transactions on Visualization and Computer Graphics, 2009

Méthode	capacité	
	théorique (bits)	expérimentale (bps)
Cayre et Macq 2003	$ V $	< 1
Wang et Cheng 2005	$3 V $	3
Cheng et Wang 2007	$\alpha V $	3-6
Chao <i>et al.</i> 2009	$69 V $	40
Li <i>et al.</i> 2011	$ P \lfloor \log_2(M \times N) \rfloor$	50
Gao <i>et al.</i> 2012	$3\Omega(H - L + 1)$	1-2
Yang <i>et al.</i> 2013	$\alpha V $	45-60
Tsai 2015	$ P \lfloor \log_2(M \times M) \rfloor$	50
Amat <i>et al.</i> 2010	$ V /4$	0.25

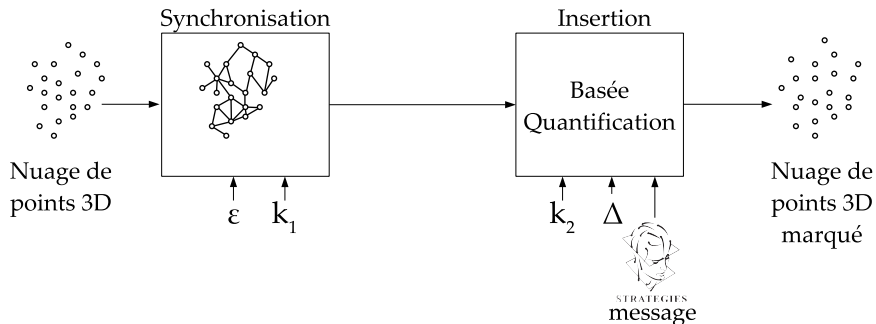


Méthode d'IDC haute capacité sur un nuage de points 3D

- Haute capacité : **domaine spatial**
 - ▶ Sommets supports du message
- Synchronisation des sommets dans un nuage de points 3D :
 - ▶ Ordre fichier
 - ▶ Déroulement des facettes
 - ▶ **Basée graphe**
 - + Sur le nuage de points (ne nécessite pas de maillage particulier)
 - + Robuste au réordonnancement du fichier
 - + Plusieurs parcours uniques en fonction du sommet de départ
 - Calcul du graphe
 - Stabilité des graphes
- Substitution par:
 - ▶ **Quantification**

- 1 Contexte
 - Problématique
 - Solution
- 2 État de l'art
 - Notions générales
 - Synchronisation 3D
 - Insertion de données cachées 3D
- 3 Contributions
 - Insertion de données cachées haute capacité
 - Chemin hamiltonien
 - Insertion
 - Codage Arithmétique Statique
 - Améliorations : robustesse, sécurité, qualité
 - Synchronisation robuste
 - Synchronisation sécurisée
- 4 Conclusion
- 5 Perspectives

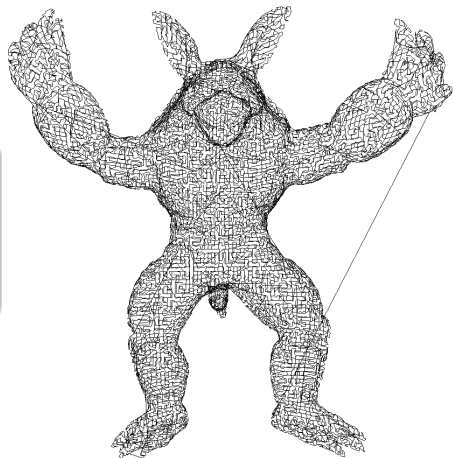
IDC haute capacité dans un nuage de points 3D



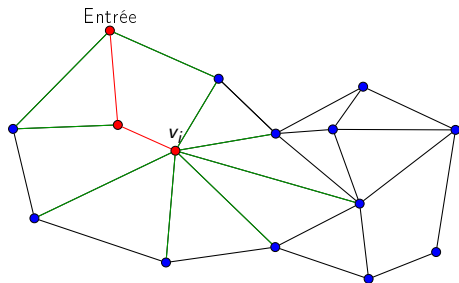
- k_1 , k_2 : clés secrètes
- Δ : pas de quantification
- ϵ : paramètre de synchronisation

Construction

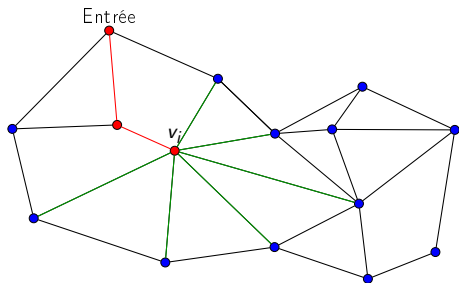
- v_0 : Sommet d'entrée
- Sur le graphe complet
- Recherche du plus proche voisin



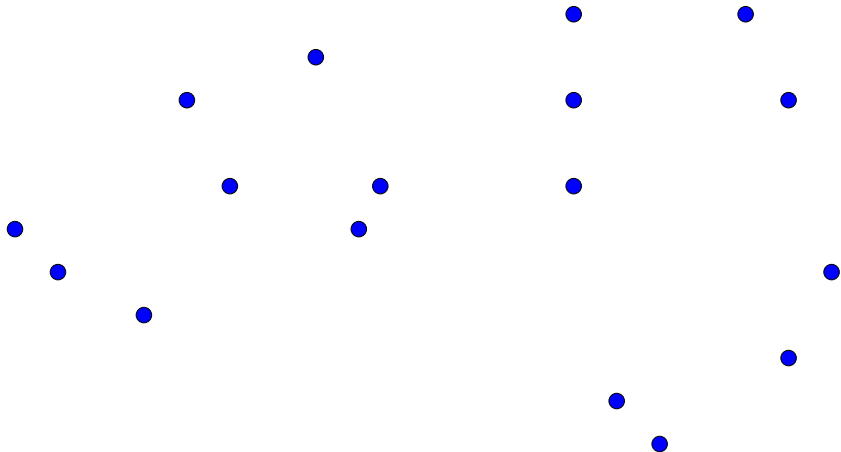
Chemin hamiltonien vs ACPM



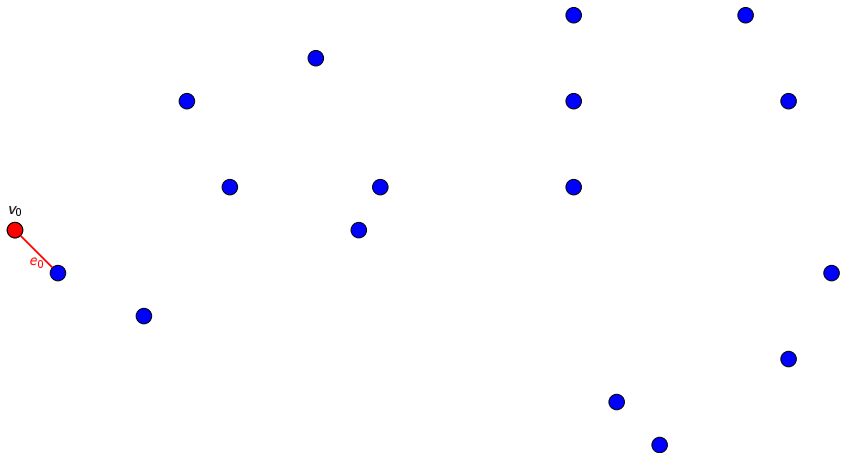
ACPM Prim : $\mathcal{O}(|E||V|)$



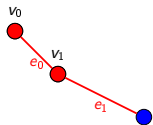
Chemin hamiltonien: $\mathcal{O}(|V|^2)$



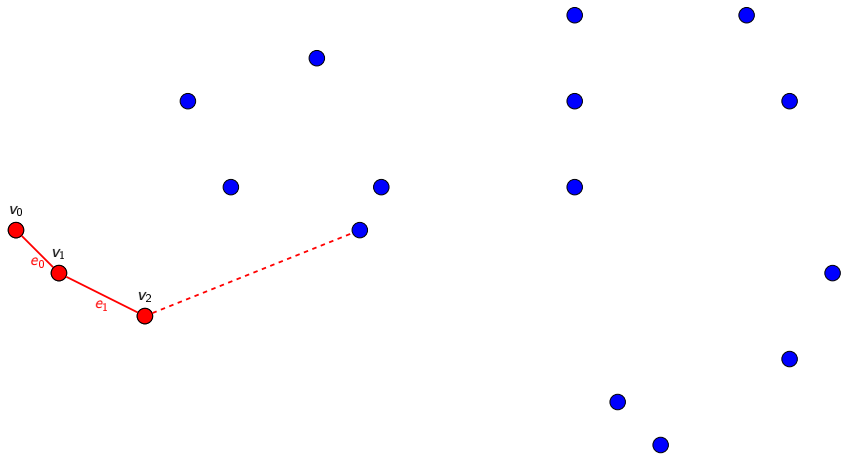
Chemin hamiltonien



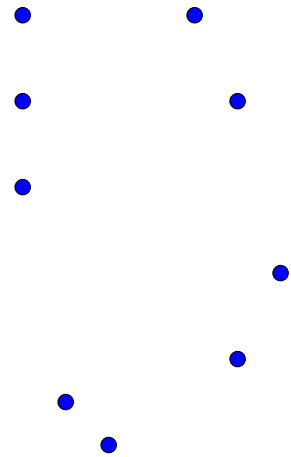
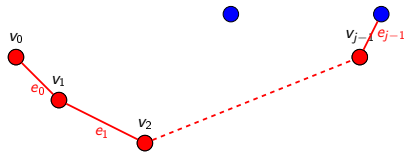
Chemin hamiltonien



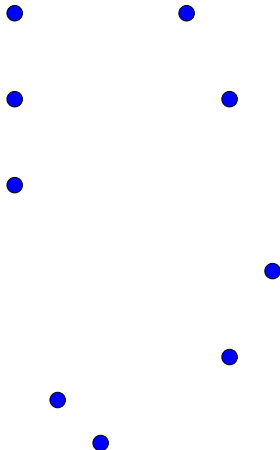
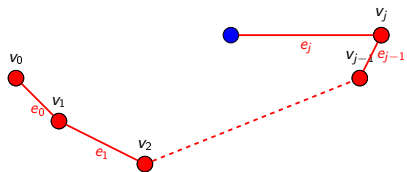
Chemin hamiltonien



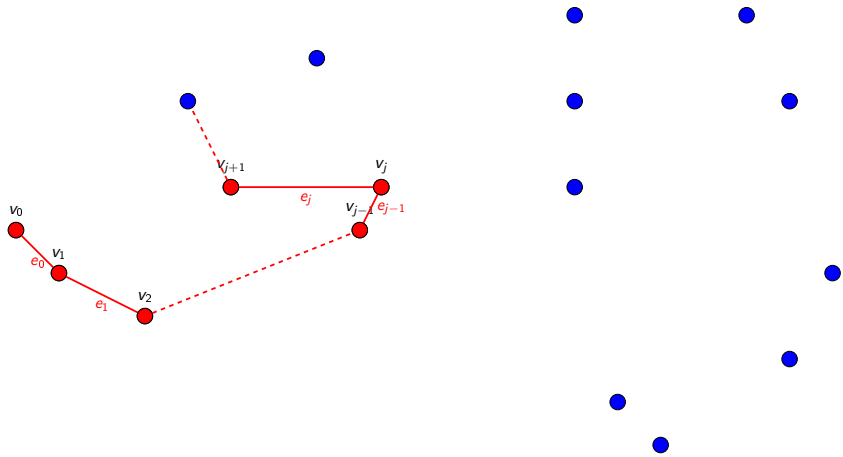
Chemin hamiltonien



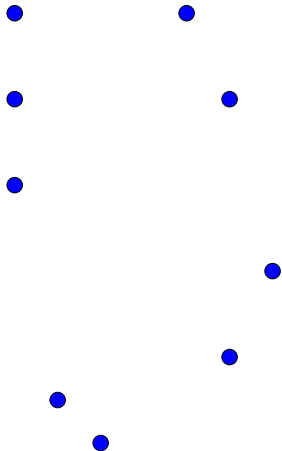
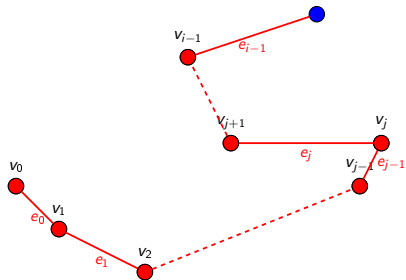
Chemin hamiltonien

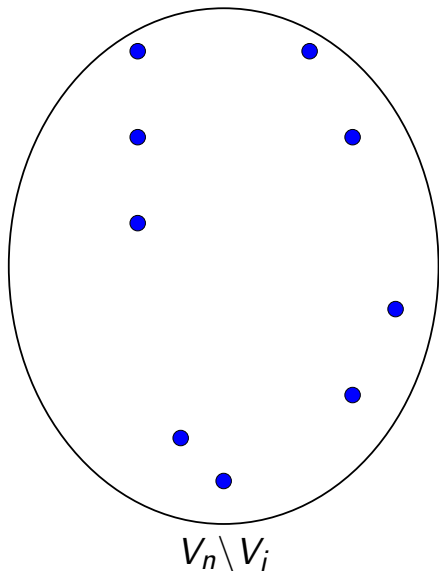
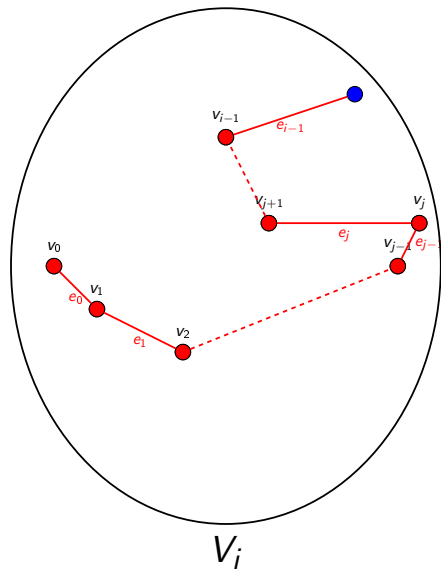


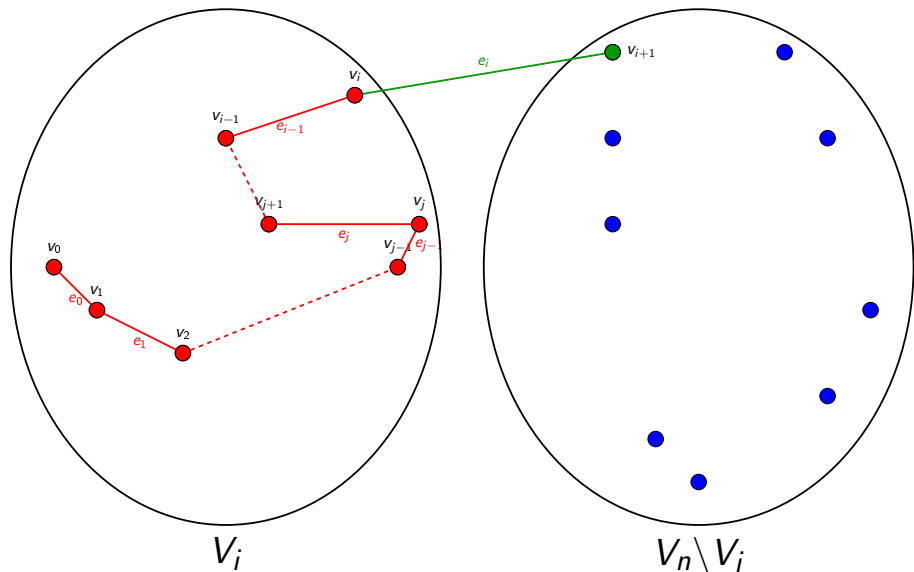
Chemin hamiltonien

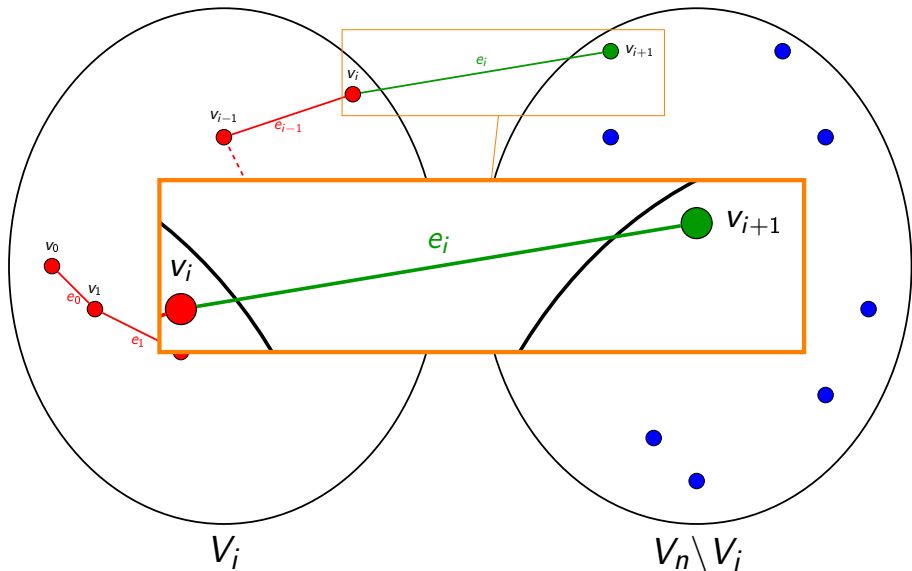


Chemin hamiltonien



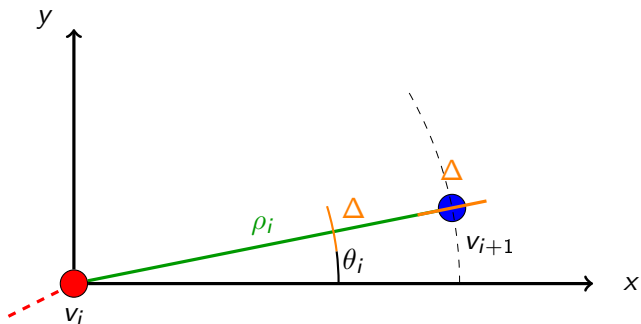






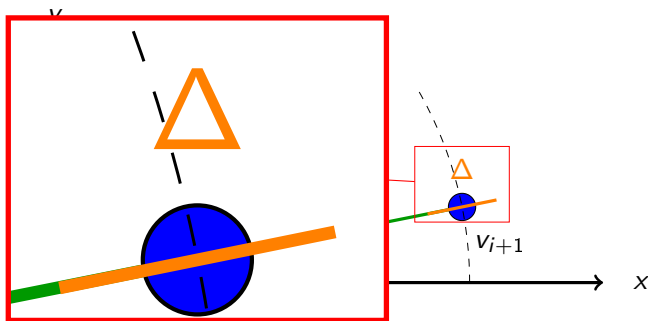
Insertion dans $p_i = (\rho_i, \theta_i, \phi_i)$

- Pas de quantification : Δ
- Lettre s_j du message \mathbf{M} sur un alphabet \mathcal{S} de taille n
- Insérer une lettre par coordonnée : diviser Δ en n sous-intervalles



Insertion dans $p_i = (\rho_i, \theta_i, \phi_i)$

- Pas de quantification : Δ
- Lettre s_j du message \mathbf{M} sur un alphabet \mathcal{S} de taille n
- Insérer une lettre par coordonnée : diviser Δ en n sous-intervalles



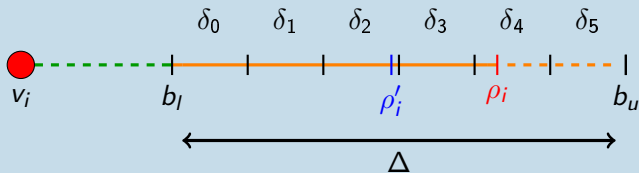
Exemple sur la coordonnée ρ_i

- 1 Trouver la borne inférieure de l'intervalle Δ

$$b_l = \lfloor \frac{\rho_i}{\Delta} \rfloor \times \Delta \quad (1)$$

- 2 Diviser Δ en n sous-intervalles δ_j , $i \in [0, n[$
- 3 Trouver δ_j correspondant à s_j

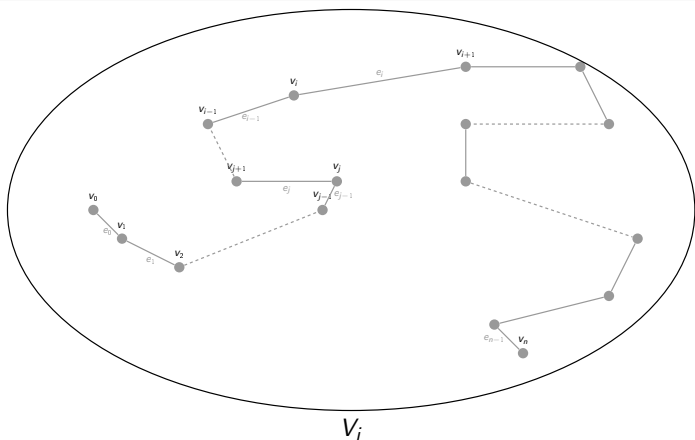
Exemple : $n = 6$, $m = s_2$



Stabilité de la synchronisation

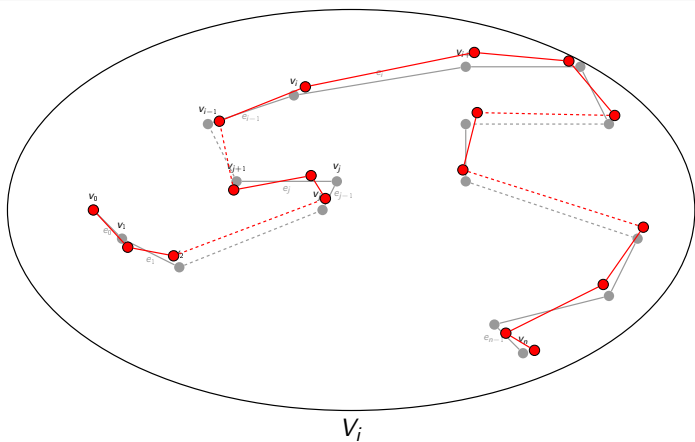
Le parcours des sommets doit être le même au décodage :

- 1 Conservation du chemin après $j > i$
- 2 Conservation du chemin avant $j < i$: problème de causalité



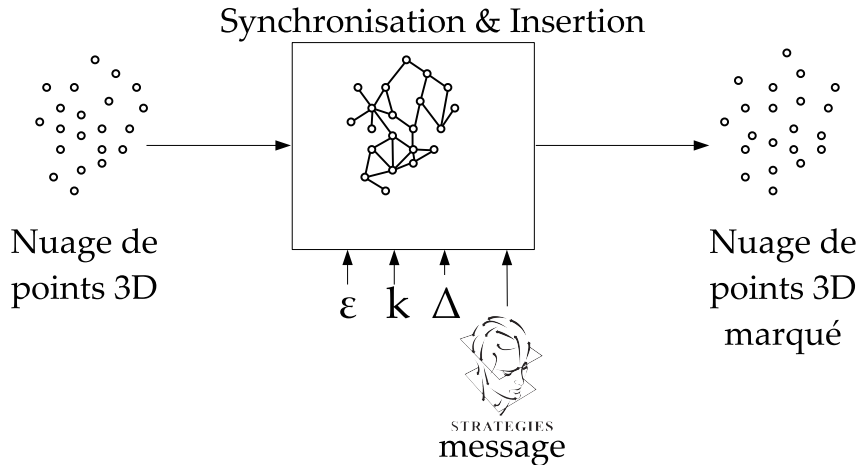
Le parcours des sommets doit être le même au décodage :

- 1 Conservation du chemin après $j > i$
- 2 Conservation du chemin avant $j < i$: problème de causalité

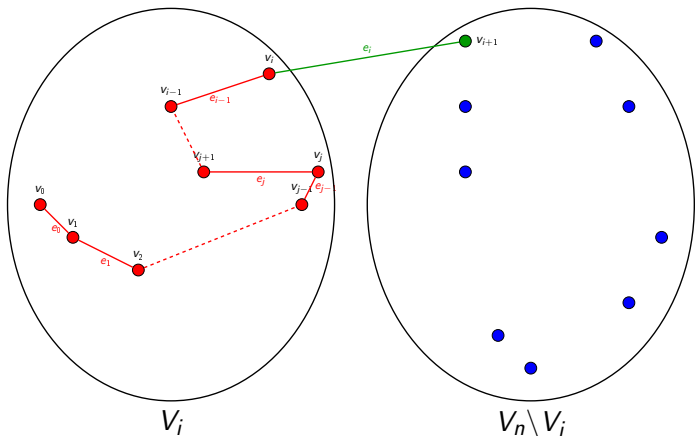


Déplacement itératif

- 1: Résolution par construction



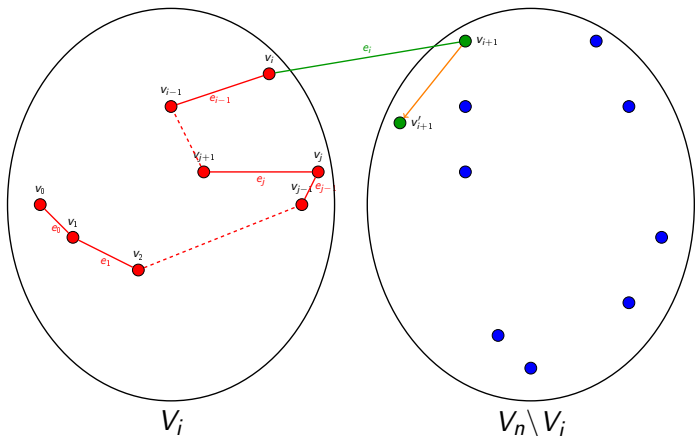
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

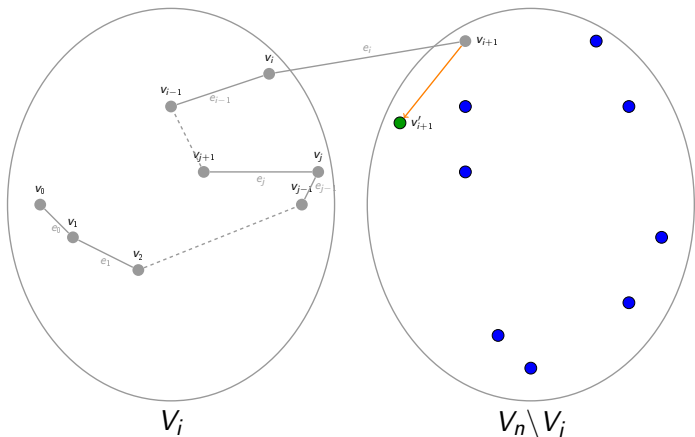
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

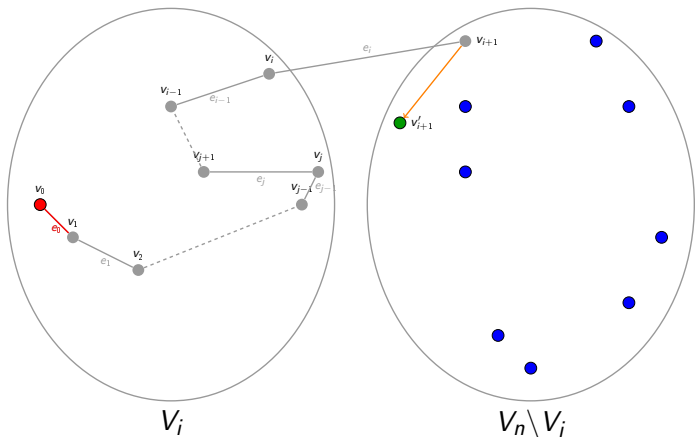
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

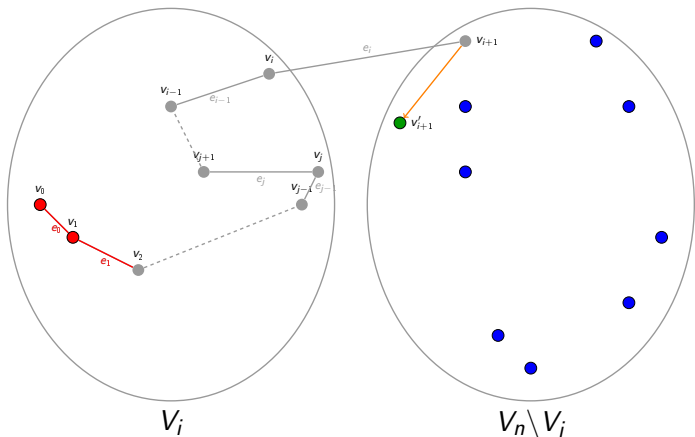
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

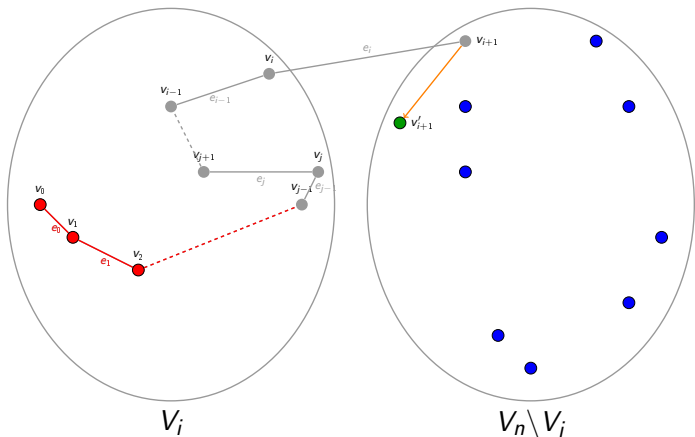
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

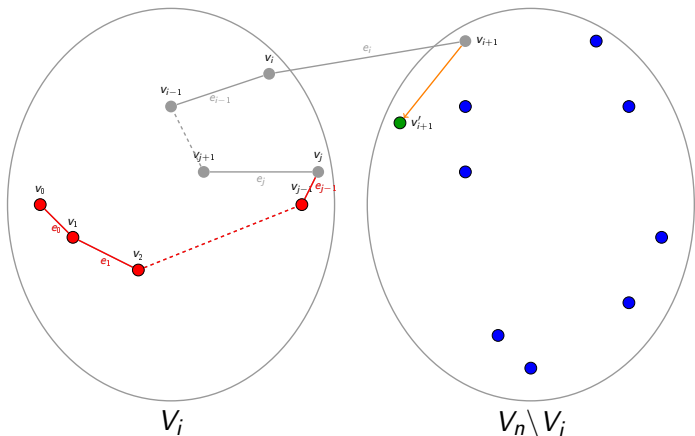
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

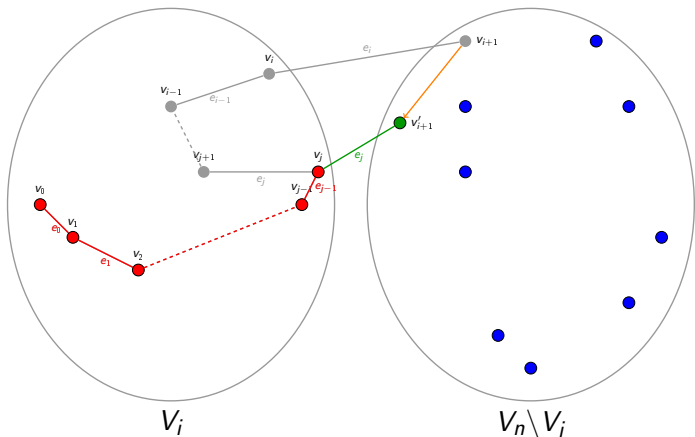
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

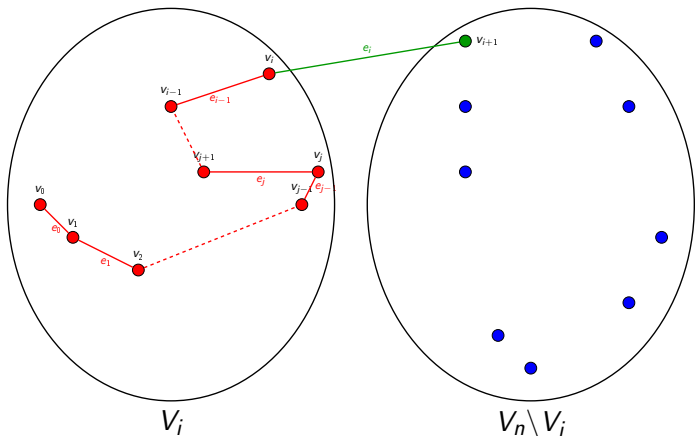
Problème de rapprochement à l'étape i



Condition :

$$\|v_j, v_{j+1}\|_2 < \|v_j, v'_{i+1}\|_2, \quad \forall v_j \in V_i, j \neq i,$$

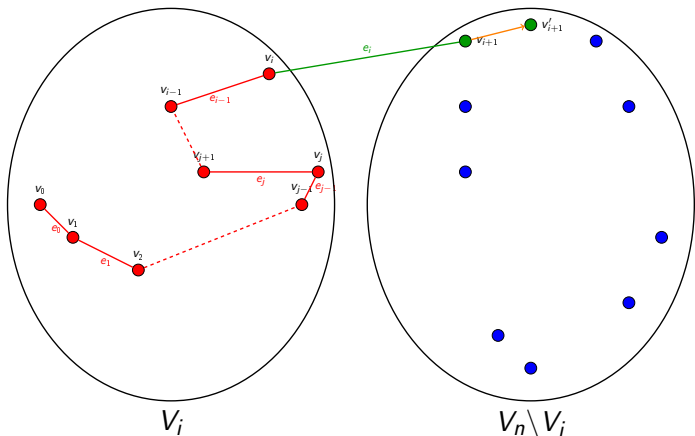
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

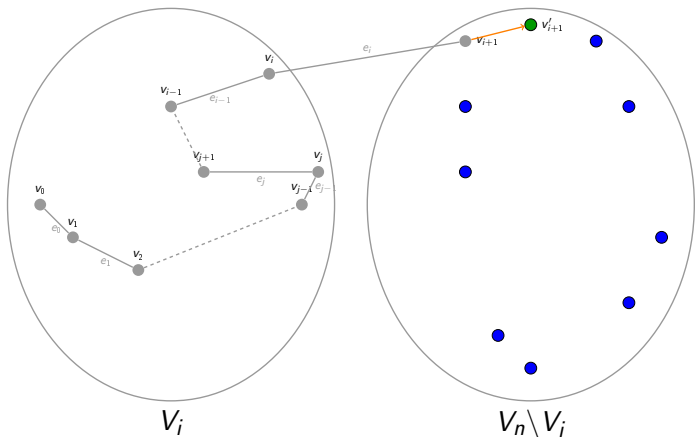
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \quad \forall v_j \in V_n \setminus V_i, \quad j \neq i+1.$$

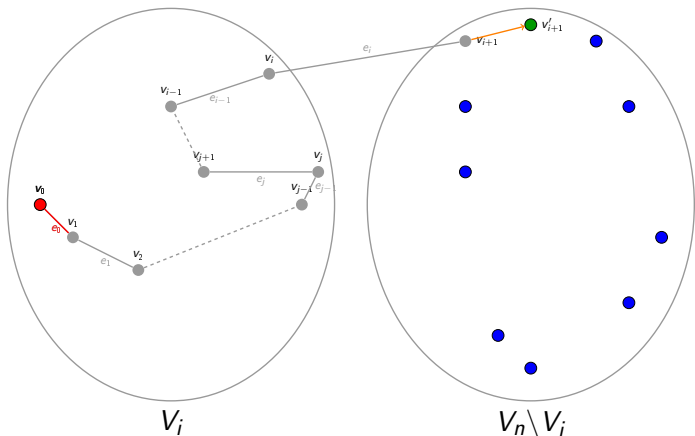
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

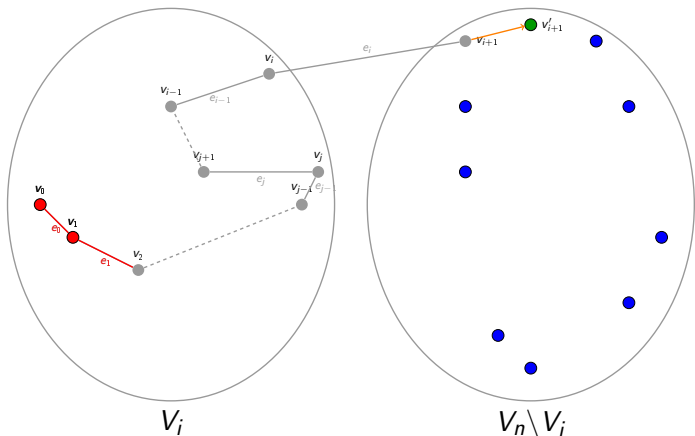
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

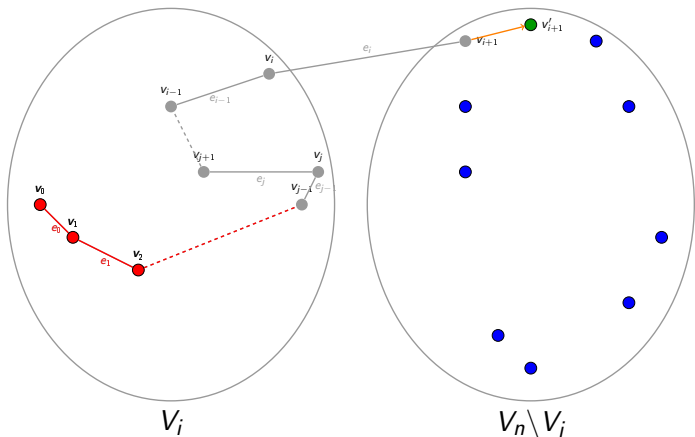
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

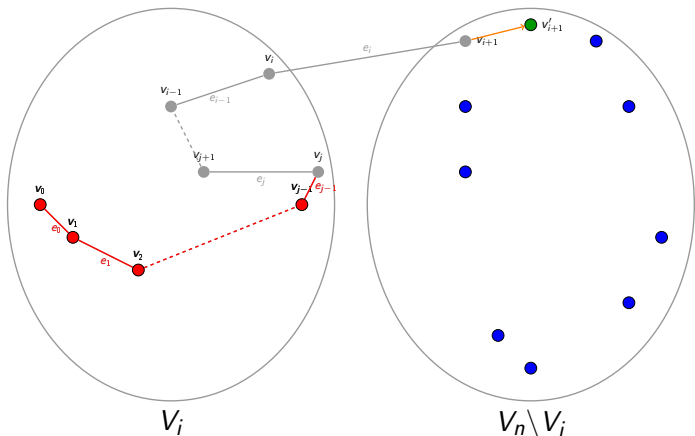
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

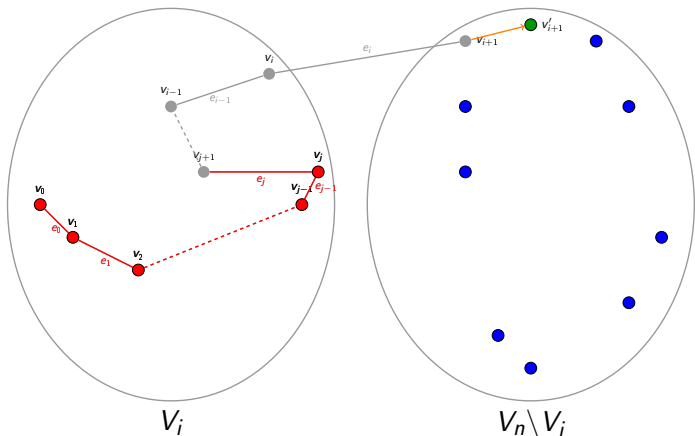
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

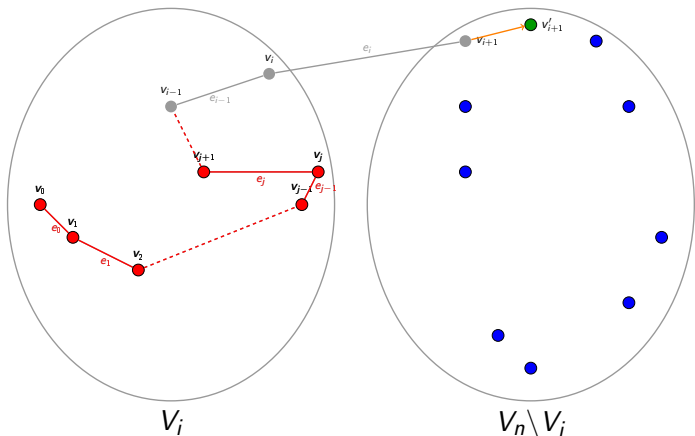
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

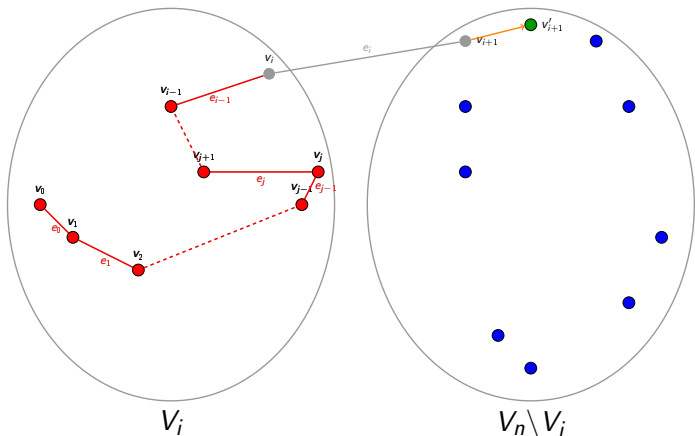
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

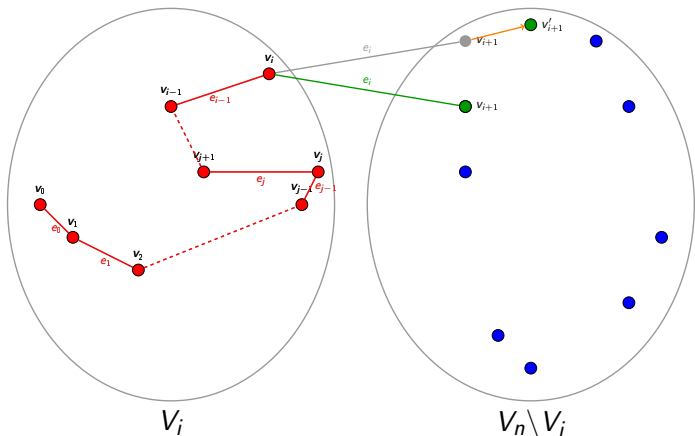
Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

Problème d'éloignement à l'étape i



Condition :

$$\|v_i, v'_{i+1}\|_2 < \|v_i, v_j\|_2, \forall v_j \in V_n \setminus V_i, j \neq i+1.$$

Vérification des configurations

- 2: Résolution par évitement
 - ▶ Ne pas déplacer le sommet

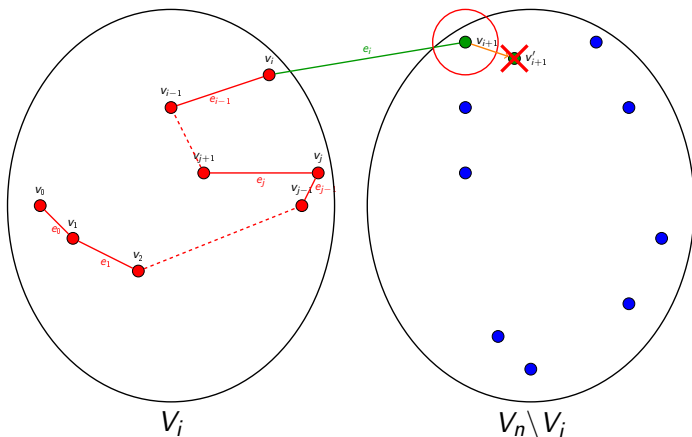
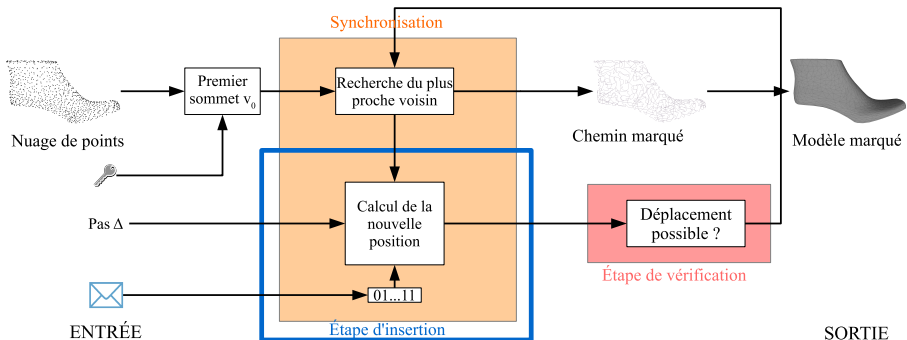
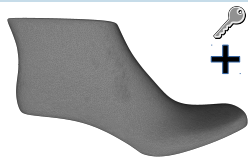


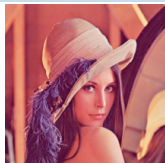
Schéma de la méthode



Capacité et qualité :



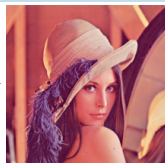
Maillage original
45 002 sommets



Message
(212x212)≈ 1Mb

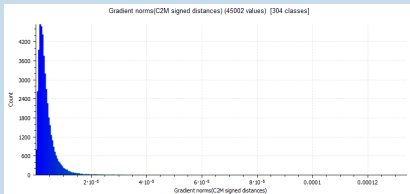
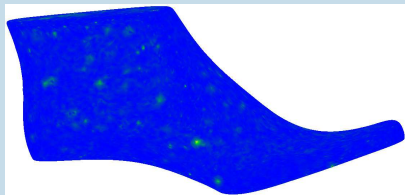


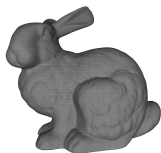
Maillage marqué
19.9 bps



Message extrait
BER : 2.5×10^{-4}
PSNR : 45.42 dB

Distorsions du maillage :





Bunny 34 834 sommets

Résultats

- Maillages normalisés : arête moyenne = 1
- $PSNR_1(M, M') = 20 \log_{10} \frac{D_{max}}{RMSE_v(M, M')}$

Comparaison avec l'état de l'art sur le maillage Bunny

Méthodes	Capacité (bits)	Hausdorff $\times 10^{-3}$	$PSNR_1$ (dB)
Chao <i>et al.</i>	940 464	N.A.	100.57
Gao <i>et al.</i>	51 408	0.55	70.02
$n=2, \Delta = 1.10^{-4}$	108 578	1.00	127.30
$n=256, \Delta = 1.10^{-4}$	830 304	0.27	127.24

Insertion basée Codage Arithmétique Statique

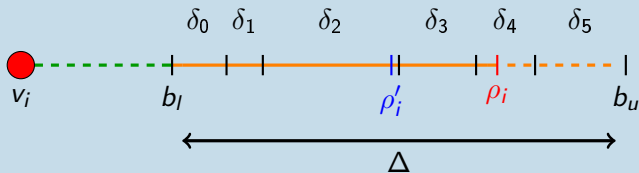
Exemple sur la coordonnées ρ_i

- 1 Probabilité d'appartenance au message

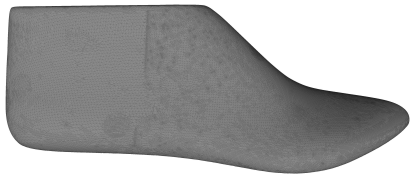
$$p(s_j) = \frac{|M|_{s_j}}{|M|} \quad (2)$$

- 2 Trouver δ_j correspondant à s_j

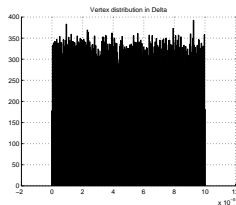
Exemple : $n = 6$, $m = s_2$, $p(s_0) = 0.12$, $p(s_1) = 0.08$, $p(s_2) = 0.3$,
 $p(s_3) = 0.17$, $p(s_4) = 0.13$, $p(s_5) = 0.2$



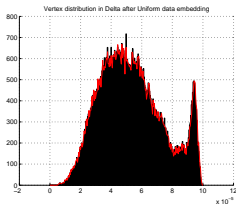
Imperceptibilité statistique : distribution des ρ_i dans Δ



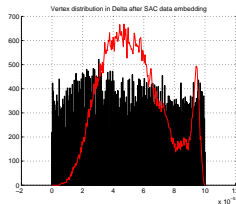
Forme de chaussure
83 698 sommets



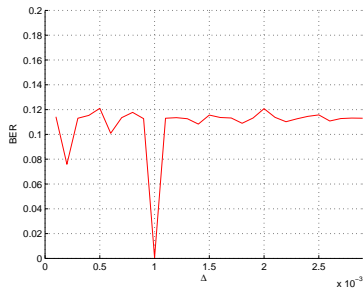
Distribution originale



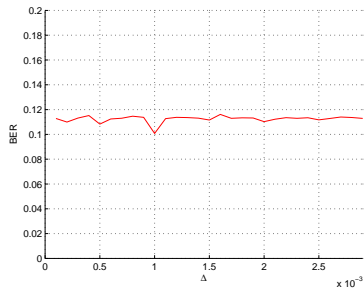
Distribution insertion uniforme



Distribution insertion CAS



Méthode uniforme

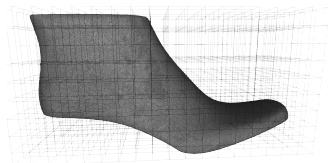


Méthode CAS

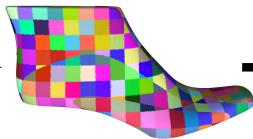
- 1 Contexte
 - Problématique
 - Solution
- 2 État de l'art
 - Notions générales
 - Synchronisation 3D
 - Insertion de données cachées 3D
- 3 Contributions
 - Insertion de données cachées haute capacité
 - Chemin hamiltonien
 - Insertion
 - Codage Arithmétique Statique
 - Améliorations : robustesse, sécurité, qualité
 - Synchronisation robuste
 - Synchronisation sécurisée
- 4 Conclusion
- 5 Perspectives

Amélioration de la robustesse du chemin hamiltonien

- Regroupement de sommets
- Prise en compte des cas d'ambiguïtés



Maillage original
188 609 sommets



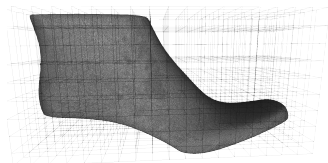
333 groupes



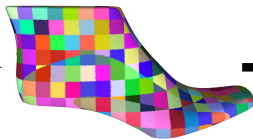
333 sommets

Amélioration de la robustesse du chemin hamiltonien

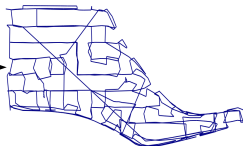
- Regroupement de sommets
- Prise en compte des cas d'ambiguïtés



Maillage original
188 609 sommets



333 groupes



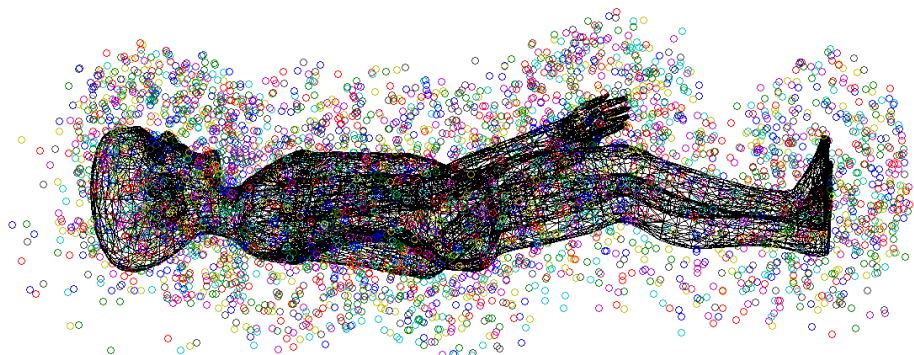
Chemin hamiltonien
sur les 333 sommets

Augmenter la sécurité

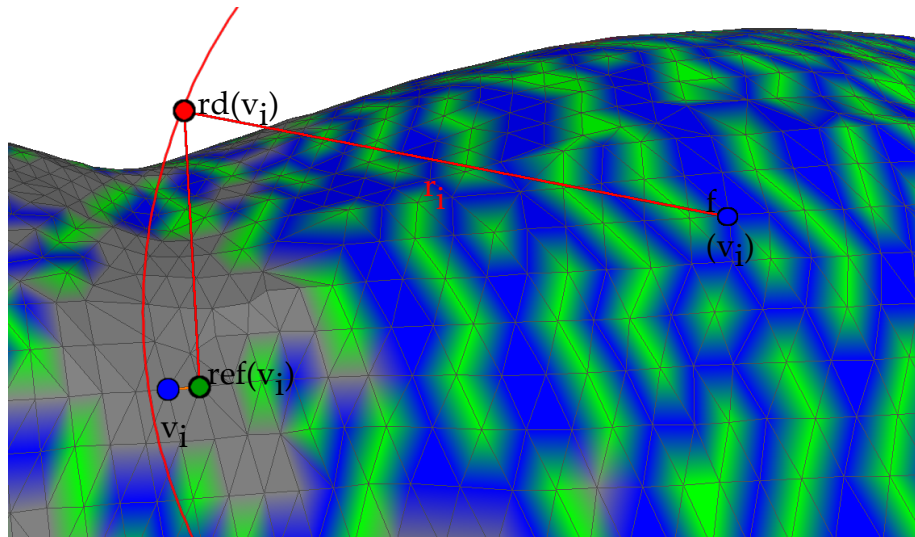
- Chemin hamiltonien déterministe
 - ▶ Sélection pseudo aléatoire des sommets
- Si $|M| \ll \text{capacité}$: message localisé autour du point d'entrée
 - ▶ Diffusion du message

Stratégie de résolution de l'étape de vérification

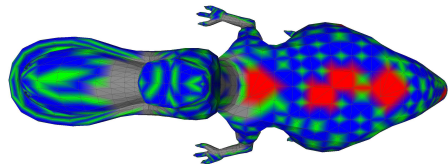
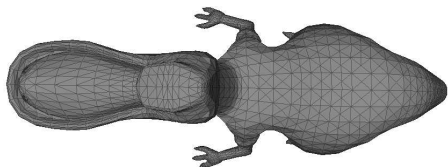
- Sommets non déplaçables
 - ▶ Supprimer totalement les erreurs



Points générés pseudo-aléatoirement pour Alien 7 401 sommets.



Vue d'ensemble de la construction du chemin.

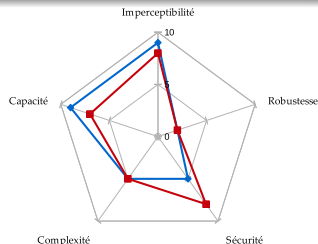


Supprimer toutes les erreurs

- Ambiguïtés : zones planes, régulières
- Suppression \implies peu de distorsions
- Remaillage

Comparaison avec la méthode initiale sur le maillage Bunny

Méthode	Capacité (bits)	Hausdorff $\times 10^{-3}$	$PSNR_1$ (dB)	BER $\times 10^{-3}$
$n = 2$, $\Delta = 1.10^{-4}$ pas de déplacements	108 578	1.00	127.30	N.A.
$n = 256$, $\Delta = 1.10^{-4}$ pas de déplacements	830 304	0.27	127.24	0.042
$n = 256$, $\Delta = 1.10^{-4}$ avec améliorations	411 864	1.918	82.55	0





- 1 Contexte
- 2 État de l'art
- 3 Contributions
- 4 Conclusion**
- 5 Perspectives

Résultats obtenus

- Méthodes de synchronisation sur les graphes
 - ▶ Analyse de la stabilité des Arbres Couvrants de Poids Minimum [3]
 - ▶ Chemin hamiltonien [2]
 - ▶ Chemin hamiltonien robuste [1]
 - ▶ Chemin de sauts pseudo-aléatoires [4]

- [1] V. Itier, W. Puech, J.-P. Pedeboy, et G. Gesquière
Construction of a unique robust hamiltonian path for a vertex cloud.
IEEE International Workshop on Multimedia Signal Processing, p : 105-110, 2013
- [2] V. Itier, W. Puech, G. Gesquière, et J.-P. Pedeboy
Joint synchronization and high capacity data hiding for 3D meshes.
SPIE Electronic Imaging, vol. 9393, p : 5-15, 2015
- [3] V. Itier, N. Tournier, W. Puech, G. Subsol, et J.-P. Pedeboy
Analysis of an EMST-based path for 3D meshes.
Computer-Aided Design, Elsevier, vol. 64, p : 22-32, 2015
- [4] V. Itier, W. Puech et A.G. Bors, et J.-P. Pedeboy
Secure high capacity data hiding for 3D meshes.
IS&T Electronic Imaging, 2016

Résultats obtenus

- Analyse de la sécurité [4, 5]
- Insertion haute capacité
 - ▶ binaire [2]
 - ▶ basée sur le Codage Arithmétique Statique [6, 7]

Transfert

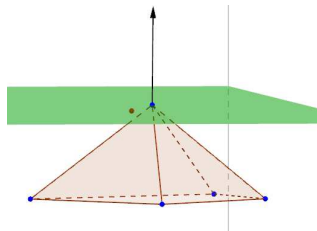
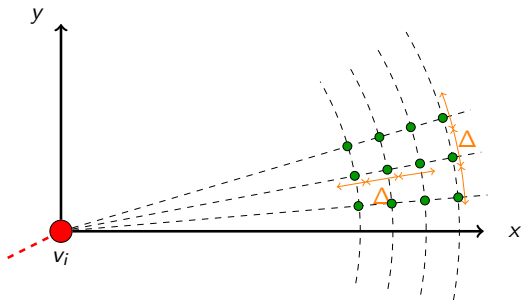
- Intégration dans les logiciels de Strategies
 - ▶ Premiers tests par des clients

- [5] V. Itier, W. Puech et A.G. Bors
Cryptanalysis aspects in 3-D watermarking.
IEEE International Conference on Image Processing, p : 4772-4776, 2014
- [6] V. Itier, W. Puech, et J.-P. Pedeboy
High capacity data-hiding for 3D meshes based on static arithmetic coding.
IEEE International Conference on Image Processing, 2015
- [7] V. Itier, W. Puech, et J.-P. Pedeboy
High capacity data hiding for 3D point clouds based on Static Arithmetic Coding.
Multimedia Tools and Applications, soumis



- 1 Contexte
- 2 État de l'art
- 3 Contributions
- 4 Conclusion
- 5 Perspectives**

Analyse compromis insertion vs distorsions



Stéganalyse

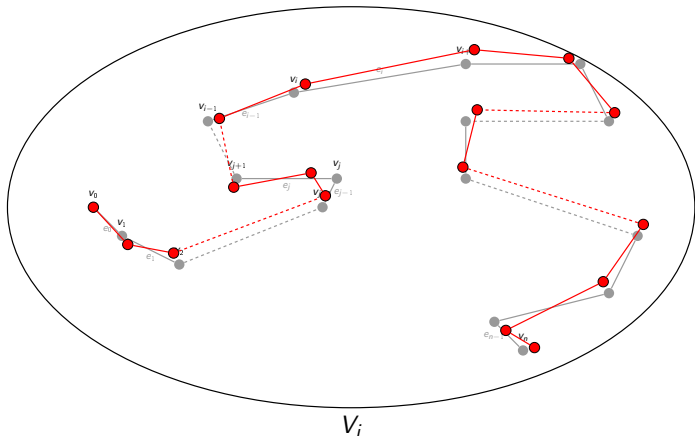
- Analyse des distributions après CAS
- Outil d'analyse général

Méthode d'insertion de données cachées robuste

- Basée sur la synchronisation robuste
- Insertion en utilisant les statistiques des groupes de sommets

Stabilité générale des graphes : par optimisation

- Calculer les positions codant l'information
- Ne provoquant pas de désynchronisation
- En réduisant les distorsions







Merci de votre attention


 P. Amat, W. Puech, S. Druon, and J.P. Pedeboy.
Lossless 3D steganography based on MST and connectivity modification.
Signal Processing: Image Communication, 25(6):400–412, 2010.

 F. Cayre and B. Macq.
Data hiding on 3-D triangle meshes.
IEEE Transactions on Signal Processing, 51(4):939–949, 2003.

 M.-W. Chao, C.-H. Lin, C.-W. Yu, and T.-Y. Lee.
A high capacity 3D steganography algorithm.
IEEE Transactions on Visualization and Computer Graphics, 15(2):274–284, 2009.

 Y.-M. Cheng and C.-M. Wang.
An adaptive steganographic algorithm for 3D polygonal meshes.
The Visual Computer, 23(9-11):721–732, 2007.

 X. Gao, C. Zhang, Y. Huang, and Z. Deng.
A robust high-capacity affine-transformation-invariant scheme for watermarking 3D geometric models.
ACM Transaction on Multimedia Computing, Communications and Applications, 8(2S):34:1–34:21, 2012.

 M. T. Li, N. C. Huang, and C. M. Wang.
A novel high capacity 3D steganographic algorithm.
International Journal of Innovative Computing, Information and Control, 7(3):1055–1074, 2011.

 Y.-Y. Tsai.
An efficient 3D information hiding algorithm based on sampling concepts.
Multimedia Tools and Applications, pages 1–17, 2015.



C.-M. Wang and Y.-M. Cheng.

An efficient information hiding algorithm for polygon models.

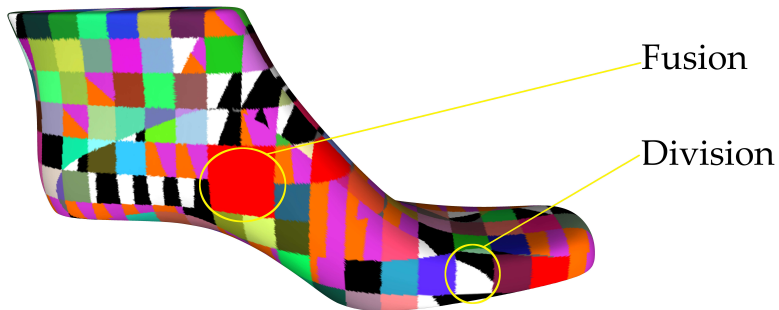
Computer Graphics Forum, 2005.



Y. Yang, N. Peyerimhoff, and I. Ivrissimtzis.

Linear correlations between spatial and normal noise in triangle meshes.

IEEE Transactions on Visualization and Computer Graphics, 19(1):45–55, 2013.



Code binaire de Golay

- Taille bloc 23
- Taille message 12

Exemple : $n = 2$



Sans correction



Avec CCE

pas : $\Delta = 10^{-4}$

Quantification :

- En fonction de n
- Livre-code des intervalles $\delta_j = [b_j, b_{j+1}[$, $j \in [0, n - 1]$
- Borne : $b_j = \Delta \sum_{i=0}^j p(s_i)$

