HAL
open science

Contributions au tatouage des maillages surfaciques 3D

François Cayre

To cite this version:

François Cayre. Contributions au tatouage des maillages surfaciques 3D. Modélisation et simulation. Télécom ParisTech, 2003. Français. NNT : . tel-00005731

HAL Id: tel-00005731

https://pastel.hal.science/tel-00005731v1

Submitted on 5 Apr 2004

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

TÉLÉCOM Paris
Université catholique de Louvain

Contributions au tatouage des maillages surfaciques 3D

THÈSE

présentée et soutenue publiquement le 9 décembre 2003

pour l'obtention des

Doctorat de l'École Nationale Supérieure des Télécommunications
spécialité Signal et Image

Doctorat de l'Université catholique de Louvain
faculté des Sciences Appliquées

par

François Cayre

Composition du jury

Président :	Jean-Jacques Quisquater	UCL
Rapporteurs :	Jean-Marc Chassery	INPG
	Olivier Devillers	INRIA Sophia-Antipolis
Examinateur :	Francis Schmitt	ENST Paris
Directeurs de thèse :	Benoît Macq	UCL
	Henri Maître	ENST Paris

Département Traitement du Signal et des Images (CNRS-LTCI) **ENST/TSI**
Laboratoire de Télécommunications et Télédétection **UCL/TELE**

Remerciements

Je tiens tout d'abord à exprimer ma reconnaissance à Henri Maître et Benoît Macq, qui ont accepté de me faire confiance pendant cette aventure d'un peu plus de trois ans. Qu'ils soient ici remerciés de la liberté totale dont j'ai pu bénéficier au sein de leurs équipes, de leur soutien indéfectible, de leur confiance surtout et enfin de leur regard critique sur ces travaux. Puissent-ils considérer ce travail comme l'expression la plus sincère de ma gratitude.

J'adresse de chaleureux remerciements à Olivier Devillers, qui s'est vite piqué au jeu du tatouage et m'a été d'une aide décisive en géométrie algorithmique. Qu'il soit ici remercié de s'être penché sur quelques-uns de mes problèmes, avec efficacité et rapidité, et d'avoir accepté de bien vouloir être rapporteur de ce travail. Ma gratitude va bien évidemment aussi à Jean-Marc Chassery, qui me fait l'honneur de s'intéresser à ces travaux, et d'en être le rapporteur. Je remercie aussi Francis Schmitt pour avoir suivi mes développements avec un œil acéré, même si les réflexes d'un tatoueur devant un maillage lui ont parfois paru un peu étranges. Merci également à Jean-Jacques Quisquater d'avoir accepté de juger ce travail : un intérêt tout particulier a été porté aux aspects de sécurité.

Je remercie encore Pierre Alliez, qui m'a permis de passer quelques jours décisifs au sein de PRISME, ainsi que Teddy Furon, Patrick Bas, Damien Delannay, Jean-François Delaigle, Frédéric Lefèbvre, Patrice Rondao-Alface et autres BMW... Mes remerciements vont également à Franck Davoine, de qui tout est parti, à Vincent Blondel, pour ses lumières en optimisation combinatoire, à Ton Kalker pour sa clarté et sa gentillesse, et à Isabelle Bloch, pour la musique et la littérature, et aussi un peu la science.

Merci aussi et surtout aux thésards de TELE et de TSI, qui ont réussi à me supporter pendant ces trois ans, merci à Marcella et Eduardo (et à Diego !), à Julien et Pauline, à Stéphane, Najib et Elen, merci à Oscar et Gaspar, les Heckle et Jeckle ibériques, à Yiolanda, Christophe (le Gosse), Yannis, Mariam, et Sabine. Et puis aussi à Christophe (celui qui milite pour l'abolition des structures musicales), Sveta, Ferdaous, Ryad Abdelfattah, Carlos, Alex (dans les caméras moultispectrals), Ève, Teh, Céline, Julie, Cléo, Slim, Ilaria, Tony, Yu, Grégoire et les autres...

Il n'aurait pas été possible d'arriver à bon port en si bon état tant moral que physique, politique, artistique, ou psychique sans les contributions très appréciées de : Ben et Élise (GNUno rulez !), Roland (revoir Liège...), Nico, Lolo, Amaël, Rocco, Stévos et les fadas du Square, MM. Saclier, Duce et Dumont (qui bien que roux reste un fort honnête homme), Nico et Sophie (je prends 10% des parts de la bergerie), Marie et Mathilde (pour les jeudis à la Flèche et plus encore), Tiphaine (des livres), Sophie (des bois) et Élise (des montagnes), Gégé (de la Butte), Lapin, Gibourse et Sophie, Taffitt, Deniche (depuis la sup...), Louloute, Mérou, Crapule, et les gentils habitants de l'Ami Zondubô, Émeline et Caro (tous ensemble !), Patrice (not only hit music), Gégé (l'autre), Laure (pour un peu tout), Cécile (qui joue la vingt-neuvième de Mozart au cor à une heure du matin), Cécile (qui dort à une heure du matin), Cyrille et Carlotta (ma cabane au Canada...), Denis, Paul, Emma, mes voisins (pour leur patience à toute épreuve), la Tatarogne, Choucou et Bichou, Duchmoll, tout le monde à Miers, Nantes, Nice et ailleurs, et mes parents.

The man who trades freedom
for security does not deserve
nor will he ever receive either.
Benjamin Franklin

Table des matières

Introduction générale **1**

1 Préambule : l'homme, le secret et le pouvoir 1
1.1 Lire un secret 2
1.2 Ecrire un secret 4
2 Positionnement de la thèse 8
3 Plan du manuscript 9

Tatouage et objets 3D

Chapitre 1
Les techniques d'écriture secrète et leurs applications **15**

1.1 Bref historique de l'écriture discrète 15
1.2 Tatouage et distribution des œuvres : une situation 21
1.3 Techniques numériques et cadres applicatifs 24
1.3.1 Stéganographie et contenus augmentés 25
1.3.2 Tatouage fragile, authentification et intégrité 27
1.3.3 Tatouage robuste et protection des documents 27
1.4 Le tatouage et son environnement 28
1.4.1 Vocabulaire 28
1.4.2 Le tatouage comme problème de télécommunication 29
1.4.3 Typologie des attaques 29

1.4.4 Sociologie économique de la piraterie 30
1.5 Conclusion 32

Chapitre 2
Surfaces et maillages **33**

2.1 Introduction 33
2.2 Principaux types de données surfaciques 33
2.2.1 Nuage de points 33
2.2.2 Non-Uniform Rational B-Splines (NURBS) 35
2.2.3 Maillages surfaciques 36
2.3 Surfaces triangulées 36
2.3.1 Propriétés topologiques 37
2.3.2 Triangulation de Delaunay 38
2.3.3 L'algorithme *Marching Cubes* 39
2.4 Paramétrisation des surfaces triangulées 40
2.4.1 Définition 41
2.4.2 Paramétrisation harmonique 43
2.4.3 Paramétrisation barycentrique de Tutte 44
2.4.4 Paramétrisation conforme 44
2.4.5 Paramétrisation de Floater 46
2.4.6 Découpe en disque topologique 47
2.5 Structures de données associées 47
2.5.1 Représentation brute 48
2.5.2 Représentation en demi-arête 48
2.5.3 Représentation *winged-edge* 49
2.6 Attributs supplémentaires 49
2.6.1 Grandeurs différentielles locales 50
2.6.2 Textures 51
2.6.3 Transparence 51
2.6.4 Réflectance 52
2.7 Modèles de distance entre maillages 53
2.7.1 Distance de Hausdorff et distance moyenne 53
2.7.2 Laplacien géométrique 54
2.8 Conclusion 54

Chapitre 3
Traitements usuels sur les maillages **55**

3.1 Codage de source 55
3.1.1 Schémas de prédiction/correction géométrique 55
3.1.2 Méthodes fondées sur la valence 56
3.1.3 Méthode de Taubin (MPEG-4) 62
3.2 Traitements affectant la géométrie uniquement 64
3.2.1 Ajout de bruit 64
3.2.2 Lissage 64
3.2.3 Rotation, translation et mise à l'échelle uniforme 65
3.2.4 Transformations perspectives 65
3.3 Traitements affectant la connexité 66
3.3.1 Renumérotation des points 66
3.3.2 Coupe 67
3.3.3 Décimation 67
3.3.4 Subdivision 69
3.3.5 Remaillage 70
3.4 Conclusion 71

Chapitre 4
État de l'art **73**

4.1 Schémas avec configuration géométrique locale 73
4.1.1 Arrangement global 75
4.1.2 Arrangement local 75
4.1.3 Arrangement indexé 78
4.2 Schémas sans configuration géométrique locale 79
4.2.1 Schéma de Wagner 79
4.2.2 Schéma *Vertex Flood* 81
4.2.3 Schéma pour l'intégrité 81
4.3 Autres espaces de représentation 83
4.3.1 Schéma dans l'espace spectral de la géométrie 83
4.3.2 Espace d'analyse multirésolution des maillages 84
4.3.3 Espace des NURBS 84
4.4 Conclusion 85

Contributions

Chapitre 5
Tatouage fragile par invariants géométriques **89**

5.1 Motivations 89
5.2 Une primitive géométrique d'insertion 90
5.2.1 Description 90
5.2.2 Remarques sur la sécurité 92
5.2.3 Parcours en ruban pour un arrangement global 94
5.2.4 Un arrangement local 99
5.3 Arrangement indexé pour le tatouage fragile 103
5.3.1 Surcoût de codage 103
5.3.2 Stratégie pour le choix d'un autre invariant 103
5.3.3 Codage des numéros des bits par invariant 105
5.3.4 Validation de l'approche par arrangement indexé 106
5.4 Optimisation du nombre de sites 109
5.4.1 Algorithme 109
5.4.2 Preuve de terminaison 110
5.4.3 Discussion 112
5.5 Application au tatouage fragile 114
5.5.1 Contrôle de la distorsion 114
5.5.2 Détection 114
5.5.3 Sécurité des clefs 118
5.5.4 Résultats 119
5.6 Perspectives 121
5.6.1 Application du parcours optimal à la stéganographie 121
5.6.2 Application de l'arrangement indexé à l'intégrité 121
5.6.3 Tatouage de tous les triangles 123
5.6.4 Allocation adaptative des bits 123
5.7 Conclusion 123

Chapitre 6
Autour de la décomposition spectrale de la géométrie **125**

6.1 Cadre théorique 125
6.1.1 Opérateur laplacien pour le codage de source 126
6.1.2 Décomposition spectrale 127
6.1.3 Spectre de la géométrie 129
6.2 Partition du maillage 130
6.2.1 Remarques pratiques pour l'implantation 130
6.2.2 Un outil générant des partitions 131
6.2.3 Artefacts visuels dus à la partition 132
6.3 Bases de décomposition fixes 133
6.3.1 Augmentation des partitions et recouvrement 134
6.3.2 Transfert sur la connexité régulière 135
6.3.3 Cylindres topologiques 137
6.4 Un codeur/décodeur géométrique spectral 138
6.4.1 Schémas d'implantation 138
6.4.2 Transmission progressive de la géométrie 139
6.4.3 Compression et bases naturelles 140
6.4.4 Transmission et bases fixes 141
6.4.5 Remarques sur la décomposition spectrale 145
6.5 Tatouage spectral de la géométrie 146
6.5.1 Schéma de tatouage 147
6.5.2 Force et distorsion 151
6.5.3 Résultats 152
6.6 Conclusion 155

Conclusion **157**

Bibliographie

Introduction générale

1 Préambule : l'homme, le secret et le pouvoir

S'il n'est pas encore tout à fait déplacé d'appliquer quelques principes, il faut mettre sans doute en exergue celui qui, avec Rabelais, nous exhorte à ne pas pratiquer de science sans conscience, sous peine de ruine de l'âme. Historiquement, le rapport de la société des hommes avec le secret est un sujet sensible. Il nous a paru primordial de retracer une brève histoire du secret dans l'humanité, afin de dégager clairement les enjeux à l'œuvre dans la démocratisation des techniques d'écriture secrète. En effet, il apparaît que les implications d'un développement de ces techniques dépassent de loin les seules perspectives marchandes.

L'adjectif "secret" provient du verbe latin "secernere", qui signifie "écarter", il entre dans la langue française vers 1180 ; le substantif "secret", qui dérive lui du neutre de l'adjectif latin "secretus", se répand vers 1380 hors du Poitou, où il est attesté depuis 1110 (la victoire de notre prononciation du mot "secret" sur sa variante de l'époque "segret" a dû attendre le XVIIIème siècle.) On doit donc en déduire que pendant les deux premiers siècles, les gens disaient plus volontiers "C'est secret", que "C'est un secret", chargeant ainsi dès l'origine le mot avec une certaine gravité. L'invention de la langue autour du secret s'arrête, puis reprend un peu avant la fin du XVIème siècle (époque à laquelle se structure le français moderne). C'est seulement à partir de 1560 qu'est attesté le sens de "mystère", il a donc fallu encore presque deux siècles pour que le mot commence à s'émanciper de sa gravité première. "Etre dans le secret", qui date de 1690, commence alors seulement à connoter le mot politiquement, pour l'associer à la pratique du complot, fort répandue à l'époque. Il serait plaisant de pouvoir comparer cette évolution du mot secret dans les différentes langues. Le mot se charge de multiples sens tous très voisins (le secret était aussi un débarras isolé dans les habitations, d'où découle l'expression *mettre au secret*). Parmi les onze que recense Littré, on trouve "Qui ne peut être point pénétré", relatif à la cryptographie[1], et "Qui n'est pas apparent, visible", relatif à la stéganographie[2]. Au passage, l'article *stéganographie* est plus laconique, évoquant une simple "écriture en signes secrets et convenus", et est illustré avec une citation prenant "secret" dans son acception cryptographique[3] !

A l'heure où les menaces sur la liberté d'expression sont chaque jour moins camouflées, il importe de mesurer le fantastique rôle des techniques numériques d'écriture secrète dans la

[1]"Vous n'aurez point pour moi de langages secrets" - Racine, *Britannicus*, II, 3.

[2]"Oui, vos moindres discours ont des grâces secrètes" - Racine, *Esthétique*, III, 4.

[3]"La stéganographie, l'art facile de combiner des lettres ne présentant un sens que pour les initiés qui possèdent la clef, existe de toute antiquité." Cahun, *Liberté*, 27 mai 1867.

dynamique qui oppose depuis toujours les individus à leurs formes d'organisation politique[4]. Pour cela, nous interrogeons la transition historique subtile entre vouloir lire et pouvoir écrire un secret. Les étapes de ce passage sont marquées par les différentes stratégies que les dirigeants ont successivement employées pour maintenir la cohésion de la communauté autour d'eux. Cette mise au point liminaire se propose essentiellement de replacer les techniques d'écriture secrète dans leur contexte global, et non plus seulement suivant la seule perspective actuelle, marchande en l'occurence, comme il arrive trop souvent.

1.1 Lire un secret

Il semble bien que la relation de l'homme au secret n'est pas aussi claire qu'il peut y paraître a priori. Historiquement, il s'avère que l'on a d'abord cherché à lire un secret, et que l'écriture (e.g. la maîtrise) des secrets a été l'objet d'une attention plus tardive, fondée sur l'organisation de l'homme en communautés, aux jeux de pouvoirs complexes, et conditionnée par la création d'outils adéquats. Lire le cours, présumé secret, des événements a été la grande affaire des hommes depuis leur accession au stade de créature intellectuelle, capable de prendre consciemment en compte la succession d'observations d'événements environnementaux importants, souvent bouleversants pour la communauté. Dans la plupart des tribus agraires, un dépositaire important du pouvoir dans la communauté était celui censé établir le contact avec le monde des représentations ésotériques influant sur la prospérité du groupe. Il faut y lire l'embryon des premières croyances, et partant celui des premières religions[5]. Le chamane, le prêtre, le mage, tous sont les représentants de cette interface avec l'illusion première nécessaire à l'homme, celle du secret encore à découvrir, de l'accès rare à la connaissance totale. On notera le caractère éminemment anthropologique de la plupart des textes religieux fondateurs, la morale étant l'outil par lequel on codifie de manière irrévocable, apparemment ex nihilo (donc secrètement, car on trace alors la ligne de partage fondamentale entre ce qui relève du sacré et du profane), des règles censées maximiser la prospérité du groupe. Les règles d'association entre individus mâles et femelles ont généralement pour but de minimiser les risques de dégénérescence génétique[6], et les règles de respect de l'intégrité physique des autres individus ont généralement un effet économique bénéfique car stabilisateur, sur le développement de la communauté.

[4]Sur le secret en tant que ferment communautaire, voir par exemple *La communauté inavouable* (notamment la partie consacrée au groupe *Acéphale*), de Maurice Blanchot, Minuit, 1996.

[5]La paléo-anthropologie a récemment établi que les premières sépultures à caractère religieux datent de -100000 ans, et qu'elles ont été le fait tant de l'homme de Néanderthal (habitant l'Europe, aujourd'hui disparu), que de l'*homo sapiens* dont nous descendons (et qui lui seul semble avoir découvert l'art). Les deux hominidés étaient en outre si génétiquement différents qu'il faut parler de deux espèces distinctes (aucune descendance commune possible bien qu'ils se soient côtoyés pendant des millénaires), mais ont toutes les deux connu l'angoisse métaphysique. Voilà qui, un siècle plus tard, crédite Renan de manière posthume, lequel se plaignait de ce que "Hegel est insoutenable dans le rôle exclusif qu'il attribue à l'humanité, laquelle n'est sans doute pas la seule forme consciente du divin, bien que ce soit la plus avancée que nous connaissions." (cité par G. Campioni in *Les lectures françaises de Nietzsche*, PUF, 2001, p. 94)

[6]Voir entre autres *L'Érotisme*, de Georges Bataille (pour une présentation, certes encore hégélienne, des aspects communautaristes), Minuit, 1957, et *Histoire naturelle de l'amour*, de Helen Fisher (pour une mise en perspective avec le règne animal en général), Robert Laffont, 1998. Par exemple, la ruine des Habsbourg en Europe est due aux tares mentales des héritiers, conçus après trop de mariages consanguins.

La genèse de ces règles (la religion est littéralement ce qui relie les hommes entre eux) peut être vue comme le terreau expérimental de la pratique politique. Les deux sentiments les plus souvent inspirés aux individus par les dirigeants pour les tenir ensemble en pratique semblent être la peur et l'espoir, alternant au rythme des phases de crise et de prospérité. Si en temps de crise un groupe est davantage soudé par la peur, la paix et le développement économique nécessitent un liant social tout aussi efficace mais moins coûteux. L'espoir de déchiffrer l'apparition de phénomènes bouleversants comme les catastrophes naturelles, les épidémies et les guerres, pour s'en protéger, constitue le plus clair de l'effort humain en temps de paix, afin d'arriver à l'illusion d' "un monde qui ne se contredise pas, ni ne trompe, ni ne change, un monde *vrai* - un monde où l'on ne souffre pas..." [7] Ces événements restant en général rares à l'échelle de l'individu, même dans les époques les plus troublées, il a bien fallu, puisque l'expérience de personne n'était assez longue, se résoudre à introduire l'inconnu dans le raisonnement - ou plus précisément à raisonner juste sur des concepts ésotériques. Ainsi, pour reprendre l'exemple de Mircea Eliade[8], lorsqu'il s'agit de se sédentariser, une communauté choisira bien sûr la proximité d'un cours d'eau, et si aucun autre avantage naturel ne peut être exploité, décidera au hasard de la situation du campement sur ce cours d'eau. On préférera l'endroit où tel chasseur a abattu son premier oiseau, ou l'endroit où il vient de pleuvoir.

Plus les choix stratégiques faits pour la communauté devaient paraître indiscutables, plus ils devaient donner l'impression de résulter d'un processus ésotérique, dont les règles de production étaient d'autant moins accessibles au plus grand nombre (par définition). Au besoin, on pourra s'aider de la figure d'un dieu terrifiant poussant parfois l'absurde jusqu'à exiger des sacrifices humains dans la communauté (cf. les cultes de Baal et Moloch[9] en Europe ou celui des dieux Incas). Les choix et règles établies à l'occasion de la formation de la communauté sont appelées le mythe. Ce qui est important ici n'est pas tant le résultat de l'oracle que le secret avec lequel il est produit. Plus un mode de production d'oracles passe pour incompréhensible, plus l'oracle est réputé sage. Le mouvement premier de l'esprit humain est de repérer des similitudes entre les événements et les choses, de valider telle prophétie et d'infirmer telle autre, et par là de légitimer telles croyances, de les hiérarchiser, de les sélectionner minutieusement, afin de rendre le monde habitable poétiquement comme dirait Hölderlin (la validation par l'esprit des illusions destinées à l'âme constitue une condition nécessaire de l'humanité). Il est d'ailleurs notoire que l'homme a dépensé énormément plus de ressources et gaspillé beaucoup plus de forces pour des motifs irrationnels que rationnels. Dans le but de préserver la cohésion du groupe à travers les âges, il a fallu devenir capable de transmettre le mythe, au début de manière orale puis de manière écrite. Dans le cas des croyances comportant un héritage écrit, il est apparu nécessaire de sacraliser l'ouvrage relatant le mythe. Notre époque mesure autant qu'une autre les aberrations et la bêtise irrationnelle qui en découlent. La sacralisation de l'ouvrage mythique ouvre la voie à une nouvelle forme de prophétie, basée sur l'étude du texte sacré.

Pour naître, cette forme de prophétie nouvelle a nécessité d'élargir l'espace des oracles possibles, de le rendre virtuellement infini - sa crédibilité en dépendait. Ce sont les chercheurs

[7] Nietzsche, *Fragments Posthumes*, 9 [60], automne 1887.

[8] *Le sacré et le profane*, Gallimard, 1965.

[9] Termes qui tous deux désignent le maître, le seigneur. Cf. Voltaire, *Dictionnaire philosophique*, Religion, Seconde Question.

hébraïques les premiers qui ont opéré la connexion entre le secret et le nombre[10]. En effet, l'interprétation ésotérique de la bible hébraïque, la Cabale, repose à la fois sur les occurrences des suites de lettres et sur l'association d'un nombre à une lettre. Sans doute pour la première fois, la Cabale investit le nombre comme objet de divination, comme voie d'accès à la connaissance totale, comme vecteur du secret. Et de fait, même un moderne bon teint manifeste davantage de curiosité envers la numérologie qu'envers la lecture des entrailles du chat du voisin[11], la lecture de n'importe quel hebdomadaire imprimé sur papier bon marché suffit à s'en convaincre. Toutefois, le nombre cabalistique diffère beaucoup du nôtre : il méprise l'algèbre[12]. Seule est prise en compte sa signification symbolique ésotérique, ainsi par exemple du nombre sept qui représente la puissance. Dans l'optique consistant à percer le grand secret de la création, il semble qu'il faille se doter du nombre et d'une logique[13], fut-elle fantasque[14]. Tous les moyens sont donc bons pour générer l'illusion nécessaire à la communauté, mais les premiers et encore les plus profonds sont ésotériques, apparemment seuls habilités à rendre à l'homme l'intelligibilité perdue des événements extérieurs qu'il subit.

1.2 Ecrire un secret

La complexité des communautés et la richesse de leurs interactions ainsi que le développement économique acquis en temps de paix ont été à l'origine de régimes politiques

[10]Plus tard, et toujours dans le but de justifier le mythe par le secret, Voltaire rappelle qu'au début de notre ère "on reprocha aussi aux premiers chrétiens la supposition de quelques vers acrostiches d'une ancienne sybille, lesquels commençaient tous par les lettres initiales du nom de Jésus-Christ, chacune dans leur ordre." (Voltaire, *Dictionnaire philosophique*, article *Christianisme*, Recherches historiques sur le Christianisme, Gallimard, 1994, p. 175)

[11]"La curiosité n'est pas un goût pour ce qui est bon ou ce qui est beau, mais pour ce qui est rare, unique, pour ce qu'on a et que les autres n'ont point.", La Bruyère, *Les Caractères*, XIII, 2, De la mode.

[12]"L'apparente "objectivité" du calcul est toujours une illusion. Ses opérations ne s'appliquent à la réalité qu'au prix d'une réduction telle que ses résultats ne s'y rapportent que de ce point de vue particulier." - M. Bounan, *Sans valeur marchande*, Le sujet de la science, Allia, 2001.

[13]"[...] A la base de la construction logique du nombre figure donc un axiome non analytique, qui est en réalité une assertion relative à l'univers [son infinité]", R. Blanché et J. Dubucs, *La logique et son histoire*, Armand Collin, 1970, p. 339.

[14]Dans son étude consacrées aux fous littéraires (*Aux confins des ténèbres*, Gallimard, 2002), Raymond Queneau évoque ces psychotiques persuadés d'avoir résolu la quadrature du cercle. Par exemple, un de ces Quadrateurs, Lucas, en cherchant le volume d'une pyramide accepte sans trop s'émouvoir que $\sqrt{6-\sqrt{3}} = 6$ et $2-\sqrt{3} = 3$! Il déclare que le calcul différentiel et intégral, *puisqu'il* ne reconnaît qu'une seule valeur à π, conduit à des résultats "non seulement inexacts, mais même contradictoires". Entre autres, il nie encore l'existence du dodécaèdre, de l'hyperbole, il expose une méthode unique de résolution des équations de n'importe quel degré, l'aire de ses cercles est indépendante de leur périmètre, etc. Lucas et une cinquantaine d'autres ont servi de matière à Queneau pour son Chambernac rédigeant son Encyclopédie des sciences inexactes dans *Les Enfants du limon*. Ils ont tous été *publiés*, parfois même décorés comme Joseph Lacomme, analphabète, qui apprit à compter avec les numéros des maisons dans les rues, et calcula que $\pi = 25/8$ en creusant inlassablement son puit nuit et jour (approximation tout de même moins bonne que celle d'Archimède, mais que ses admirateurs, car il en eut, trouvaient meilleure au motif que le résultat tombe juste après la 3ème décimale). Joseph Lacomme obtint plusieurs distinctions et diplômes à la fin du XIXème siècle, dont une médaille de la Société des sciences et des arts de Paris, pour ses travaux sur la quadrature du cercle, qui connurent une quinzaine de réimpressions (Queneau, *op. cit.*, p. 80). La plupart de ces brillants exposés se terminent par un auto-portrait pathétique du nouveau démiurge ou par un délire de persécution, pouvant aller dans son intensité jusqu'à dissoudre la grammaire elle-même.

variés, tendant à la démocratie en cas de période de prospérité longue. On peut arguer du fait que les régimes politiques et leurs moyens d'existence s'intellectualisent avec la prospérité du groupe et son importance. Ainsi, il est sans doute plus sûr de recourir aux médias pour influencer des millions de personnes plutôt que d'envoyer l'armée. Le même raisonnement n'est pas nécessairement valable pour des groupes plus petits. Historiquement, la conquête puis la conservation du pouvoir est l'affaire d'une minorité, dans l'écrasante majorité des civilisations. La taille des groupes à diriger augmentant, il a fallu à la minorité des maîtres développer des moyens moins coûteux que les guerres et les sacrifices pour garantir la cohésion des individus autour d'elle. L'expérience a voulu que la connaissance a priori d'information sur l'adversaire aidait à prendre souvent une longueur d'avance sur lui. Le besoin d'un échange sûr d'information sensible, qu'on ne pouvait intercepter, se faisait jour. Deux grandes voies ont été retenues : brouiller le contenu de l'information à transmettre, et rendre la transmission indétectable. Les deux techniques semblent avoir été développées en parallèle, de manière ad hoc. La première évoluerait vers la cryptographie moderne dès lors que les outils algébriques seraient disponibles, la seconde poursuivrait son chemin autour d'évolutions souvent proches de recettes de cuisine, fédérant le tout sous le terme de stéganographie[15].

Si vouloir lire un secret est à l'origine de la divination, pouvoir en écrire relève de la politique et de ses moyens. C'est la nature supposée de l'émetteur de l'information secrète, humaine ou non, qui fait qu'on parle de divination ou de science. La séparation tardive entre l'alchimie et la chimie comme entre la sorcellerie et la médecine[16] relève de la même évolution menant d'une approche irrationnelle, parce que fondée sur trop peu d'observations, à une science se caractérisant par la mise en relation abstraite d'observations plus nombreuses réputées ainsi plus fiables. Cependant, si le développement de la chimie et de la médecine correspond à une volonté d'aménager des conditions d'existence physique, il faut reconnaître que celui de la cryptographie et de la stéganographie a pour unique objet les conditions d'existence politique de l'homme. Longtemps l'apanage des militaires[17] et de la classe dirigeante, ces techniques semblent bénéficier aujourd'hui d'une relative libéralisation avec l'émergence de notions comme le respect de la vie privée et du secret des correspondances dans les civilisations les plus prospères. Il est possible d'y distinguer un des signes du déplacement du pouvoir de la sphère politique vers la sphère purement économique. En effet, la généralisation du secret dans l'usage des communications entre individus ne laisse pas d'affaiblir l'Etat dans sa relation avec l'individu, ce qui est au passage une des caractéristiques de l'illusion marchande aujourd'hui en vogue.

A l'heure où l'écrasante majorité des communications entre communautés prospères s'effectue sous forme numérique, il faut accepter que le nombre termine sa révolution secrète

[15]Nous renvoyons au beau livre de Simon Singh, *Histoire des Codes Secrets*, J.C. Lattès, 1999, pour plus de détails sur les techniques utilisées en cryptographie au cours des âges.

[16]"Le grand et puissant docteur de la Renaissance, Paracelse, en brûlant les livres savants de toute l'ancienne médecine, les grecs, les juifs et les arabes, déclare n'avoir rien appris que de la médecine populaire, des bonnes femmes, des bergers et des bourreaux ; ceux-ci étaient souvent d'habiles chirurgiens (rebouteurs d'os cassés, démis), et de bons vétérinaires." - Jules Michelet, *La Sorcière*, IX, Satan médecin. Les positions sociales ambiguës du rebouteux et de la sorcière sont magistralement illustrées, respectivement, dans les deux nouvelles *Le rebouteux* et *L'enfant* d'Octave Mirbeau (*Contes cruels*, Les Belles Lettres, 2000).

[17]"La cryptographie est un auxiliaire puissant de la tactique militaire." - Général Lewal, *Etudes de guerre*.

débutée avec la Cabale et devienne une sorte de matière première sur laquelle toute puissance politique ou économique cherche à développer son pouvoir. Le nombre est devenu aujourd'hui notre principal vecteur du secret. En pratique, le mouvement de la libéralisation des techniques de secret numérique est double. Premièrement, en protégeant mieux le secret des correspondances, c'est l'Etat qui a le plus à craindre pour sa cohésion, en permettant à des minorités de mieux s'organiser (l'internationalisation et la sécurisation des communications entre syndicats, entre opposants politiques et entre journalistes ne sont que des symptômes de la même évolution). Aucun Etat n'ayant jamais fait confiance à ses citoyens, il faut en déduire que le pouvoir, au sens des moyens de la cohésion du groupe, s'est déplacé de la sphère politique[18]. Si les techniques numériques du secret prennent un tel essor, il faut interroger le principal bénéficiaire de cette libéralisation. Il est tout de même troublant que des techniques d'ordinaire si pointues et cruciales tombent tout à coup dans l'escarcelle du public[19], même si pour déchiffrer les messages, les Etats préfèrent en général se servir de moyens détournés[20]. Deuxièmement, de nos jours, non seulement les communications sont numériques, mais beaucoup de marchandises s'échangent encore sous cette forme (les communications elles-mêmes sont d'abord et avant tout des marchandises suivant le dogme actuel). Il importe donc de protéger le nombre-marchandise, et les efforts en ce sens tendent à montrer que c'est là que s'est déplacé l'objet du pouvoir. Il réside à présent non seulement dans la maîtrise du nombre support de communication, mais aussi dorénavant dans celle du nombre support de marchandise. En quelque sorte, et à puissance de calcul constante, la longueur de clef autorisée par un Etat mesure le déplacement du pouvoir vers la sphère économique (i.e : la quantité globale d'information que l'Etat accepte de ne plus pouvoir connaître rapidement).

Les dernières années laissent présager d'une mise sous tutelle de l'internet par les Etats afin d'assurer le libre échange des marchandises, y compris et surtout numériques. Aux États-Unis, l'extension du Digital Millenium Copyright Act (DMCA) s'appelle le Super-DMCA : dans six États (Caroline du Sud, Floride, Géorgie, Alaska, Tennesse et Colorado), il est désormais illégal d'utiliser le chiffrage du courrier électronique, un pare-feu, de partager sa connexion xDSL avec un tiers, etc. car dans ce cas l'origine et le destinataire de la communication sont inconnus du fournisseur d'accès. Extrait du texte de loi du Colorado[21], partagé textuellement par les six États car issu de la MPAA[22] (Motion Picture Association of America) :

```
A person commits a violation under this section if he or she knowingly
(...) possesses, uses, manufactures, develops, assembles, distributes,
transfers, imports into this state, licenses, leases, sells, offers to
```

[18]Plus incisif, Emmanuel Todd diagnostique un néant de volonté politique dont l'incompétence économique des élites serait le fondement, voir *L'illusion économique*, Gallimard, 1998.

[19]Le fait le plus troublant ici n'est pas que des Etats permettent l'utilisation de ces techniques (ils n'autorisent que ce qu'ils savent être en mesure de déchiffrer), mais le fait que des livres et des publications sur le sujet soient si facilement accessibles.

[20]Comme par exemple le programme Carnivore du FBI qui agit comme un vers sur le réseau et envoie directement les clefs privées des utilisateurs à la NSA, voir : http ://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.

[21]http ://www.leg.state.co.us/2003a/inetcbill.nsf/fsbillcont/A2F0DA113DF2BFC087256CC2006BFB94 ?Open&file=1303_ren.pdf

[22]Texte de la MPAA : http ://www.eff.org/IP/DMCA/states/sdmca_model_final.pdf

```
sell, promotes, or advertises for sale, use, or distribution any
communication device to :
- [...]
- conceal or to assist another to conceal from any communication
service provider, or from any lawful authority, the existence or place
of origin or destination of any communication that utilizes a
communication device.
```

Voilà qui n'a clairement plus rien à voir avec la protection des artistes, et investit le fournisseur d'accès de tous les droits, sans aucune contrepartie pour le consommateur qui se voit au passage dépouillé de son droit à la vie privée. Ce texte illustre comment un Etat parvient à organiser sa survie (à travers sa mission de surveillance) avec l'aide d'un acteur du monde économique : le fournisseur d'accès. Toutefois, priver les individus du secret de leurs communications se révèle en pratique aussi inefficace[23] que délétère. En France par exemple, la récente Loi sur la confiance dans l'Economie Numérique vise, entre autres, à restreindre la liberté d'expression des utilisateurs du réseau afin d'empêcher que puisse être porté atteinte à l'image des personnes morales, censées ne pas pouvoir se défendre face à des avis que pourraient exprimer des personnes physiques sur des forums ou des pages personnelles. En particulier, tout contenu jugé diffamatoire par une personne morale ou physique devra être retiré, sans jugement de justice quant au fond[24], qui devra faire l'objet d'une procédure connexe. Une autre forme d'atteinte à l'expression libre est celle plus classique des régimes autoritaires qui filtrent le contenu passant au travers de leur pare-feu national. En concurrence des agressions marchandes et autoritaires contre le premier espace d'expression libre et mondial, il est naturel de développer des outils nouveaux de communication. C'est le sens des initiatives portées par exemple par le groupe d'hacktivistes Cult of the Dead Cow[25], tant par le développement d'un réseau peer-to-peer crypté que par la mise à disposition du public d'un navigateur web avec fonctions de stéganographie intégrées[26]. Ces initiatives, loin d'être isolées, témoignent de la subtilité avec laquelle se remodèlent sous nos yeux les rapports des Etats, et des personnes morales en général, avec les individus.

Si un message crypté peut facilement être détecté et stoppé, il n'en va pas de même pour un contenu invisible. Outre les implications politiques insoupçonnées portées par les techniques abordées ici, il faut encore souligner les extraordinaires perspectives ouvertes par le tatouage, tant pour l'authentification des données multimédia dont les média sont friands que pour la libre diffusion de contenus par les particuliers. En effet, il devient pour la première fois possible de se passer des majors dans la diffusion et la rémunération des artistes[27].

[23] La CIA, qui faisait écouter les conversations privées de Ben Laden à ses visiteurs avant 2001, fait aujourd'hui pénitence : dans tout le flot de communications interceptées elle a vu passer l'annonce des attentats de septembre, mais n'a pas su faire remonter correctement l'information, lui attribuer de la valeur. Voir encore les campagnes de blocage d'Echelon par email, en ajoutant une liste de mots-clefs destinés à provoquer systématiquement un traitement par le système (terrorist, bomb, T4, white house, nuclear, etc.) en vue de saturer ses capacités dans un grand bruit de fond sémantique.

[24] Voir l'article 43-8 de la LEN, disponible sur http ://www.telecom.gouv.fr/internet/projet_len.html

[25] Extrait de la déclaration cDc : "We are hackers and free speech advocates, and we are developing technologies to challenge state-sponsored censorship of the Internet.", accessible sur http ://www.cultdeadcow.com/cDc_files/declaration.html

[26] http ://sourceforge.net/projects/camerashy

[27] Des groupes aussi talentueux (mais déjà connus !) que Public Enemy ou Smashing Pumpkins ont court-

Le tatouage pourrait être utilisé par un lecteur approprié pour établir des statistiques de popularité fonction du nombre de fois qu'un morceau est réellement joué. A l'opposé de la vision faisant de ces techniques un outil de plus dans le conditionnement des individus en purs consommateurs, se dessine la possibilité de pouvoir communiquer sûrement, de vérifier l'intégrité du contenu éditorial d'un médium, de favoriser la diversité culturelle... Sans risque de trop se méprendre, il est possible d'affirmer que la problématique de la mise à disposition du public des outils stéganographiques réside à long terme dans la mise en place de formes d'organisation sociale nouvelles[28]. Cet objectif impose de développer un système efficace de recherche, d'éducation et de culture, toutes exigences qui s'accordent mal de la censure, et qui nécessitent réciproquement de généraliser l'usage de techniques fiables d'écriture secrète chez les individus. Franklin voyait juste historiquement : on n'échange pas impunément sa liberté contre sa sécurité.

2 Positionnement de la thèse

Les techniques numériques d'écriture secrète font depuis une dizaine d'année l'objet d'une attention accrue de la part des chercheurs en traitement du signal, théorie de l'information, sécurité ou encore même en droit. En effet, profitant de l'imperfection des sens humains, il devient possible de dégager un degré de liberté dans la représentation numérique d'un contenu afin d'y cacher de l'information. La plupart des média numériques ont déjà été mis à profit pour ce style particulier d'applications : le texte, le son, l'image. Il est même possible de tatouer un programme exécutable en machine (ici, c'est la perception temporelle de l'exécution du programme que l'on exploite). Si la grande majorité des travaux dans ce domaine a porté jusqu'à présent sur l'image, le son et la video, en raison des volumes importants de ce type de média échangés sur le réseau, c'est à présent vers les prochains types de média appelés à davantage s'échanger qu'il faut se tourner : essentiellement la géométrie.

Le tatouage est aujourd'hui déjà assez vieux de ses quinze ans pour souffrir de quelques malentendus. Le plus grossier consistant à dire qu'il sera l'outil ultime pour lutter contre le piratage des contenus multimédia. Il faut tout d'abord attirer l'attention sur le fait, symptomatique, que seul a été mesuré le manque à gagner dû au piratage. Personne ne semble croire que le piratage, parce qu'il offre un accès plus large aux contenus, n'aiguise l'acuité du consommateur, et le détourne des réalisations préformatées à grands frais : cette façon d'envisager le phénomène réduit l'individu exclusivement à sa seule abstraction économique. Les majors comptent en fait surtout sur l'aspect psychologique de dissuasion offert par le tatouage. Paradoxalement, les majors ont été parmi les premières à ne pas croire à la chimère de la sécurisation totale des échanges par le tatouage. Par contre, autant les applications

circuité les chaînes de distribution classique en proposant le téléchargement d'albums depuis leur site. En outre, l'offre d'Apple avec son iStore permet de faire payer la musique sans le coût de distribution, et connaît un beau succès.

[28]"Peut-être le temps est-il très proche où l'on s'avisera que la pierre angulaire des édifices sublimes et inconditionnés que les philosophes dogmatiques se sont plus à élever n'étaient au fond que superstition populaire venue d'un temps immémorial, quelconque jeu de mot peut-être, suggestion aberrante de la grammaire, ou encore généralisation téméraire de quelques faits limités, très personnels, d'un caractère très humain, trop humain." - Nietzsche, *Par delà Bien et Mal*, Préface.

fiables de type orwellien semblent compromises, autant des applications relevant de la vérification de l'intégrité des contenus échangés restent un but parfaitement atteignable. Plus généralement, les techniques dites de *Trusted Computing* offrent aux majors une excellente garantie de confiance dans la machine cliente... mais les pirates ne tarderont pas à en profiter eux aussi pour garantir à leurs propres systèmes le même niveau de sécurité [65].

Les précédents travaux en tatouage font apparaître des verrous technologiques encore à lever avant une utilisation à grande échelle, nous aurons l'occasion de les présenter. En fait, y compris pour la géométrie, les leçons sont nombreuses à tirer des travaux en tatouage d'image. En particulier, les principaux cadres applicatifs restent les mêmes, avec leurs jeux de contraintes. D'une manière générale, nous essaierons dans ce travail de multiplier les analogies entre le tatouage de la géométrie et celui des média plus conventionnels.

Ce travail vise à explorer les différentes pistes en vue de l'implantation de techniques numériques d'écriture secrète sur un type bien particulier de médium : les surfaces maillées triangulées. En effet, il apparaît que ce type de médium sera de plus en plus utilisé à mesure que le débit du réseau permettra son acheminement et que les machines disposeront de la puissance de calcul nécessaire à son traitement. Pour l'heure, les données géométriques restent volumineuses, même si ce verrou technologique tend à s'effacer, notamment par le développement récent de méthodes efficaces de compression. En réalité, le principal écueil au traitement automatisé de ces données d'un genre particulier réside dans l'absence d'outils mathématiques adaptés aussi performants que l'analyse de Fourier ou l'analyse par ondelettes peuvent l'être sur des média classiques. Toutefois, nous montrerons que cet écueil se fait plus ou moins sentir en fonction du cadre applicatif considéré. Malgré tout, il reste évident que l'absence d'outils de traitement du signal sur des surfaces maillées reste très pénalisant pour le développement crédible de méthodes de tatouage robuste.

La plupart des travaux prenant pour objet les surfaces maillées sont à l'heure actuelle en plein essor. Qu'il s'agisse de compression, de paramétrisation, de remaillage ou d'échantillonnage, aucun de ces points pourtant cruciaux ne semble encore avoir trouvé une forme stable. Il faut donc percevoir ce travail comme un panorama de ce qui est possible dans l'état actuel des connaissances.

3 Plan du manuscript

Dans le premier chapitre, nous détaillerons les différents cadres applicatifs dans lesquels les techniques numériques d'écriture secrète sont les plus adaptées. Nous en profiterons pour clarifier notre lexique, mentionner quelques principes de base en sécurité, et présenter les principales techniques utilisées tant à l'incrustation qu'à l'extraction de l'information cachée. Il s'agit d'une introduction sous l'angle systémique du tatouage. Nous présenterons aussi les différents types d'attaque possible sur un tatouage, et nous donnerons enfin une typologie des stéganalystes et de leurs moyens.

Le deuxième chapitre sera l'occasion de présenter les principales représentations de l'information tridimensionnelle : nuages de points, NURBS, maillages surfacique et volumique. Nous expliquerons pourquoi nous avons voulu consacrer ce travail aux maillages surfaciques triangulés. Puis, nous préciserons les spécificités de l'information surfacique maillée, et ses répercussions sur les stratégies de tatouage à mettre en œuvre dans l'état actuel des connais-

sances. Nous définirons quelques termes de topologie et nous présenterons la relation d'Euler, essentiellement afin de préciser le type d'objets maillés que nous pourrons traiter. En particulier, nous nous attacherons à montrer comment représenter en mémoire un maillage suivant ses propriétés topologiques, comment on peut comparer deux tels maillages, et nous préciserons les premières observations dont il faudra tenir compte pour élaborer une méthode de tatouage sur ces objets.

Les traitements pouvant être appliqués à une structure maillée surfacique diffèrent sensiblement de ceux concernant les types plus classiques de données. Nous présenterons notamment en détails trois grands schémas de compression de l'information géométrique surfacique, puis nous procéderons à l'inventaire des manipulations possibles, suivant qu'elles modifient ou non la structure sur laquelle est représentée l'information géométrique. Cette liste, non exhaustive car en constante évolution, sera l'objet du troisième chapitre. Nous avons souhaité réserver une place à part pour le codage de source car nous trouverons là l'occasion de présenter divers parcours du maillage, et il sera utile de les avoir à l'esprit pour comprendre comment en tirer parti afin d'optimiser le nombre de sites pouvant être tatoués. Au fil des manipulations présentées, nous tenterons de les classer de manière économique : suivant qu'un pirate y a un accès plus ou moins facile.

C'est alors seulement que nous serons en mesure de présenter dans le quatrième chapitre les méthodes de tatouage existantes pour les surfaces maillées. Nous distinguerons tout d'abord les méthodes spatiales des méthodes mettant en jeu un espace de tatouage plus complexe. Les méthodes utilisant un espace de tatouage complexe sont souvent fondées sur une représentation bien particulière du maillage (décomposition spectrale, *progressive mesh*, etc.) Nous passerons brièvement sur le détail de la représentation (sauf pour la décomposition spectrale), pour saisir les grandes options retenues par les concepteurs des méthodes de tatouage. En nous intéressant aux méthodes spatiales, nous isolerons plus particulièrement les méthodes dites à configuration géométrique. Pour ces méthodes, nous nous attarderons sur la notion importante d'arrangement de l'information cachée, et nous en préciserons les trois types possibles. Nous donnerons une analogie avec le tatouage d'image pour les deux premiers types, mais le troisième demeure propre aux maillages (nous aurons toutefois l'occasion de présenter deux méthodes l'utilisant).

Dans le cinquième chapitre, nous présenterons nos travaux en tatouage par invariants géométriques, avec des applications possibles en stéganographie et en authentification. A cette occasion, les trois types d'arrangement de l'information cachée seront séparément mis à profit. Nous serons alors en mesure de les associer à des cadres applicatifs particuliers. En particulier, nous commencerons par présenter chaque méthode de tatouage (pour la stéganographie et l'authentification) avec son parcours naïf du maillage correspondant. Puis, nous donnerons un algorithme de parcours du maillage qui optimise le nombre de sites tatouables auxquels on peut accéder. Nous expliciterons alors les modifications minimes induites par l'utilisation du parcours optimal, et les options que nous avons retenues pour prouver l'efficacité de notre méthode. Dans le cas de la stéganographie, nous pourrons garantir une borne sur la capacité (proportionnelle au nombre de sites tatouables pouvant être accédés) et sur la distortion introduite dans le maillage. Dans le cas de l'authentification, nous saurons optimiser la répétition du message sur le maillage en cachant un bit par triangle dans la totalité des triangles.

Enfin, nous explorons au sixième chapitre une méthode de tatouage mettant en jeu un

espace particulier de représentation de l'information géométrique : celui de la décomposition spectrale de la géométrie. Cet espace nous a semblé propice à l'élaboration de méthodes de tatouage plus robustes. Nous présenterons en détails comment parvenir à une telle décomposition. Pour cela, nous introduirons en préliminaire la notion de paramétrisation, et nous illustrerons avec la paramétrisation harmonique de Tutte, que nous avons retenue. Nous aurons également besoin de définir un opérateur laplacien (topologique) sur le graphe de connexité du maillage, nous en donnerons différentes variantes suivant le calcul de leurs poids. Nous serons alors en mesure de définir la décomposition spectrale. Nous pourrons alors établir la distinction entre bases de décompositon fixe et optimale. Pour des raisons de temps de calcul et de relative indépendance vis à vis de la topologie du maillage, nous verrons en quoi l'implantation de telles méthodes fondées sur la décomposition spectrale nécessite de partitionner le maillage en disque topologiques "augmentés" jusqu'à contenir tous le même nombre de points. Nous avons développé une alternative à la méthode d'augmentation classique, qui autorise un recouvrement entre les disques (nous montrerons au passage l'amélioration apportée par notre méthode d'augmentation dans l'optique d'une transmission progressive de la géométrie). Enfin, nous exposerons notre méthode de tatouage dont nous présenterons les performances face à l'attaque de compression spectrale et diverses autres attaques.

Tatouage et objets 3D

Chapitre 1

Les techniques d'écriture secrète et leurs applications

1.1 Bref historique de l'écriture discrète

Il faut ici distinguer deux types de méthodes stéganographiques : celles reposant sur une avancée technique, et celles rendues possibles par une avancée purement scientifique. Dans la première catégorie, on peut ranger des stratagèmes aussi variés que l'encre sympathique[29], le crâne d'un émissaire, des tablettes de cire apparemment vierges, les micro-impressions des imprimantes laser, etc. On se souvient moins que Giacomo Casanova, afin de planifier son évasion de la prison des Plombs à Venise, échangeait force missives avec son complice en les cachant dans la doublure d'un livre, que leur gardien commun se faisait une joie de faire circuler naïvement entre eux, se réjouissant de contribuer à l'élévation morale des deux détenus. Casanova fut, dans la longue histoire de cette prison autrement plus redoutable qu'Alcatraz, le seul à s'en être échappé[30]. L'histoire regorge d'exemples d'astuces de cet acabit, et il est à parier que la plupart des prisonniers du monde ont un jour songé au problème de la communication secrète... Nous n'aborderons pas davantage ces techniques, pour nous concentrer sur les méthodes plus scientifiques, dans lesquelles une méthode est seule à l'œuvre.

Le premier traité abordant la stéganographie semble être celui de l'abbé Trithemius, *Steganographia* (écrit en 1499, publié en 1606). Le livre IV propose une étude des acrostiches stéganographiques et donne une liste de mots dont la deuxième lettre peut servir à trans-

[29]Dans *Le Scarabée d'or*, Poe ne met pas seulement en scène un cryptologue averti : William Legrand est aussi versé dans l'art de rendre l'écriture invisible. "Vous savez bien qu'il y a, il y en a eu de tout temps, des préparations chimiques, au moyen desquelles on peut écrire sur du papier ou sur du velin des caractères qui ne deviennent visibles que lorsqu'ils sont soumis à l'action du feu. On emploie généralement le safre, digéré dans l'eau régale et délayé dans quatre fois son poids d'eau ; il en résulte une teinte verte. Le régule de cobalt, dissout dans l'esprit de nitre, donne une couleur rouge. Ces couleurs disparaissent plus ou moins longtemps après que la substance sur laquelle on a écrit s'est refroidie, mais reparaissant à volonté par une application nouvelle de la chaleur." (Edgar Poe, *Le Scarabée d'or*, in *Histoires extraordinaires*, trad. Ch. Baudelaire.)

[30]Cette histoire, tirée des Mémoires de Casanova, est publiée sous le titre *Histoire de ma fuite des Plombs* (10/18, 1999). Mais Casanova fut encore, entre autres, le banni d'Italie qui fut chargé, par privilège royal, de fonder l'ancêtre de la Loterie Nationale en France, tant il avait rapidement su se mettre en cour de ce côté-ci des Alpes afin de fuir la justice de son pays...

mettre un message secret. La plupart des idées proposées dans cet ouvrage seront compilées par Gaspar Schott en 1665 dans son *Schola Steganographica*, il y rajoute une méthode permettant de cacher des messages dans une partition de musique en associant une lettre à une note. Il a fait école puisque nombre de musiciens, Bach le premier[31], se sont servi du thème musical en si bémol, la, do, si pour leurs œuvres : ce thème s'écrit B.A.C.H. dans la notation allemande. Schumann encore a rendu hommage à sa fiancée Ernestine von Fricken (Estrella dans le Carnaval), originaire du village de Asch en Bohême[32]. Pour cela, le Carnaval adopte les tonalités la, mi bémol, do, si (A-Es-C-H) et la bémol, do, si (As-C-H dans la notation allemande). La gravure était elle aussi un moyen de coder de l'information : les feuilles des arbustes généreux qui ornent le frontispice des *Opera Mundi* du cryptographe attitré d'Henri IV, François Viète[33] (1540-1603), ne sont pas disposées innocemment... Il faut attendre 1594 et la publication par Sir Hugh Platt de *The Jewel House of Art and Nature, conteining divers rare and profitable Inventions*, pour que le sujet trouve un nouveau souffle. L'auteur y expose une méthode de stéganographie permettant d'écrire secrètement un message, qui ne puisse être découvert ni même suspecté. Mais, sans se cantonner aux techniques subtiles, il faut reconnaître à Boccace (1313-1375) d'avoir écrit un des plus fameux acrostiches stéganographiques avec son *Amorosa Visione*.

Il est en général un "média" sur lequel on peut cacher de l'information et qui n'est pas souvent mentionné : le langage parlé. On opère une modulation secrète (pseudo-déterministe ou pas) des syllabes entendues (réellement dans le cas de l'argot ou marmonnées en lisant un grimoire hermétique). En effet, l'histoire montre que deux procédés ont été utilisés pour cacher (ou tout au moins bien dissimuler) un message dans le langage parlé. Le premier procédé est la dérivation synonymique, qui est au cœur de l'argot, du jargon, de la langue verte, du blason. Le second est la dérivation phonétique, qui concerne l'alchimie, ou Langue des Oiseaux, la transmission ésotérique de l'information. Nous esquissons rapidement la description de ces deux procédés, mais le lecteur *curieux* est invité à se reporter aux références pour plus de détails, souvent étonnants. Naturellement, des connexions existent : on trouve des ouvrages consacrés au blason hermétique...

Nous souhaitons évoquer un instant des procédés parfois oubliés qui montrent à quel point l'homme s'est intéressé au problème, dans la vie de tous les jours, en utilisant son "média" le plus immédiatement accessible : le langage parlé. La dérivation synonymique se

[31]Citons parmi les plus connus "L'Art de la fugue", de J.-S. Bach, "Sechs Fugen über den Namen Bach", Op. 60, de Schumman, les "Fantaisie et fugue sur B.A.C.H." et "Prélude et fugue sur B.A.C.H." de Liszt, et la "Fantaisie et fugue sur B.A.C.H." de Reger (*Dictionnaire encyclopédique de la musique*, p. 172, Oxford, D. Arnold Ed., Robert Laffont, 1988).

[32]U. Michels, *Guide illustré de la musique*, p. 141, Fayard, 1988.

[33]Viète, qui se vantait d'habiter au Parc Soubise un château construit par la fée Mélusine, est aujourd'hui redécouvert comme inventeur de la cryptanalyse moderne. Son exploit le plus retentissant fut le déchiffrement d'une lettre du commandeur Moreo au roi d'Espagne qui détaillait par le menu les complots ourdis dans l'ombre depuis Madrid en vue de déstabiliser le roi amateur de poule au pot avec l'aide à Paris de leurs affidés de la Ligue catholique, emmenés par le duc de Mayenne. Il est tout à fait curieux de constater que les Espagnols, même après avoir amèrement constaté qu'il était percé à jour, ont continué d'utiliser ce chiffre faible... Ce qui nous paraît aujourd'hui une erreur de débutant s'explique peut-être par le fait que le chiffre devait être cassé par un humain, et non par une armada de processeurs en parallèle. Même à l'époque, donc, ce calcul s'est avéré faux : les chiffres espagnols ont été paisiblement cassés des années durant grâce à la "Règle infaillible" (fondée sur sa "logique spécieuse") de Viète, qui se disait "Poitevin de Fontenay" - où les liens insoupçonnés qui unissent la culture du secret et le Poitou réapparaissent.

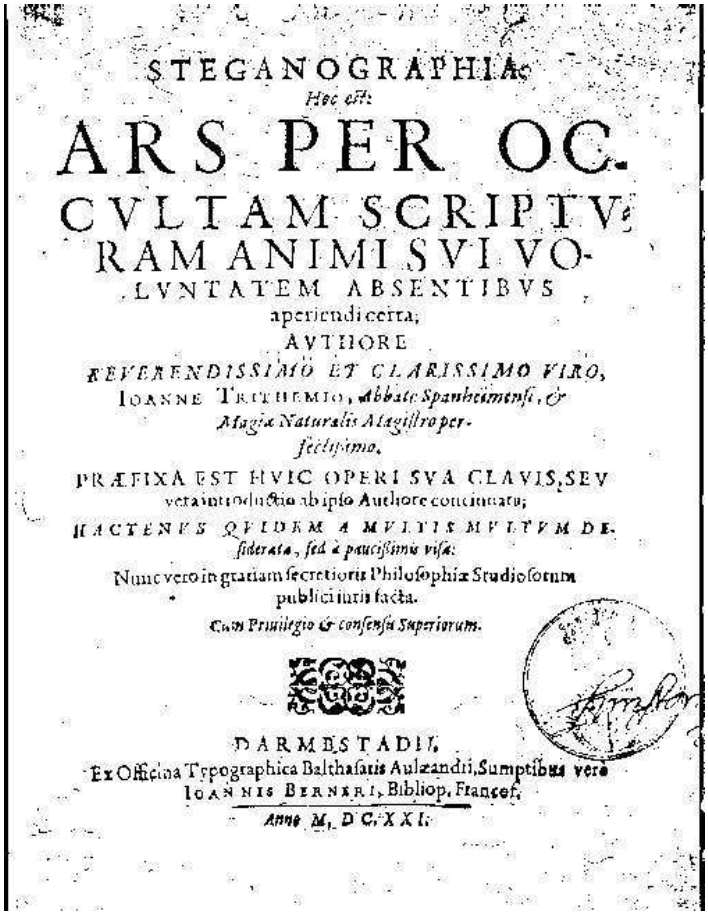
STEGANOGRAPHIA:
Hoc est:
ARS PER OC-
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimensi, &
Magiæ Naturalis Magistro per-
fectissimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
veraintroductio ab ipso Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
siderata, sed à paucissimis visa:
Nunc vero in gratiam secretioris Philosophiæ Studiosorum
publici iuris facta.
Cum Priuilegio & consensu Superiorum.
DARMESTADII,
Ex Officina Typographica Balthasaris Aulæandri, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DCXXI.

FIG. 1.1 – Première page du *Steganographia* de l'abbé Trithemius (©Fabien Petitcolas).

comprend intuitivement, en réalité implicitement (elle est déterminée par des règles comme nous verrons) : elle est adaptée à une communication rapide, sans écrit. Par contre, le procédé de dérivation phonétique mène souvent à des constructions non intuitives, qui sont une *optimisation* de contraintes, comme dans la célèbre lettre de George Sand à Alfred de Musset : ce procédé n'est donc utilisable qu'à l'écrit (il suffira de marmonner le texte lu pour commencer à faire apparaître son autre dimension[34]).

La dérivation synonymique consiste à *maquiller* le langage naturel. C'est *en référence* au français que l'argot et le blason doivent être interprétés. La science du blason, ou héraldique (en quelque sorte l'ancêtre du rébus), vise à glisser une identité dans une composition graphique aux règles précises. Les illettrés, nombreux à l'époque, pouvaient ainsi deviner l'identité de la personne qui passait dans la rue en si grand équipage. Le blason, comme tout langage, a lui aussi été détourné pour y faire circuler des messages cachés, le plus souvent grivois ou licencieux, ou destinés à moquer le prince. Plus particulièrement, les modes de

[34]Ce qui est précisément tout le contraire de la stratégie phonétique de Flaubert, qui hurlait les phrases de ses romans depuis son "gueuloir", dans sa propriété isolée, afin de s'assurer de leur fluidité (d'une certaine manière pour "gommer les ambiguïtés phonétiques") - le recours quasi-systématique à l'imparfait aidant passablement il est vrai.

dissimulation du blason semblent à rapprocher du jargon Lanternois cher à Rabelais[35] (*Pantagruel*, IX), dont la phonétique donne l'impression de se rapprocher de celle d'une langue indo-européenne sans qu'il soit possible pour un non-initié d'y rien comprendre, seul Panurge le parle couramment[36] ! Le jargon est situé à la limite de la stéganographie et de la cryptographie. Marcel Schwob a assez bien montré dans ses *Etudes sur l'argot français* (Allia, 1999) que le jargon de la Coquille (célèbre bande de malfrats, tricheurs et voleurs assemblés en confrérie au XVIème siècle), ancêtre de l'argot[37], prend sa source dans la dérivation synonymique et le loucherbème, ou langage des bouchers, ancêtre de notre verlan (désormais supplanté par le "veul", une sorte de jusqu'auboutisme du verlan, dans les foyers de création argotique les plus en pointe). L'idée de la dérivation synonymique est qu'en jargon on exprime finalement peu de concepts, mais chacun avec de multiples mots. Le loucherbème est le nom du procédé générique de l'écriture inaccessible pour un non initié : le mot sera d'abord inversé, puis on lui ajoutera le préfixe "l" le plus souvent, et un suffixe, variable et peu important (le suffixe "-bème" a quasiment disparu mais il était très utilisé à l'époque). Le mot loucherbème veut donc dire boucher, car la profession des bouchers a été la première à systématiser ce procédé. C'est ce jargon des Coquillars qui a été utilisé par Villon dans ses *Ballades en Jargon*, car le poète, outre l'admiration qu'il vouait à Rabelais, était lié, au moins d'amitié disent les mauvaises langues, avec les gens de la Coquille. D'un point de vue cryptographique, la sécurité de l'argot (son incompréhension pour un non initié) repose sur le secret du procédé employé : sitôt éventé, les dictionnaires d'argot devenaient possibles, condamnant la langue verte à évoluer sans cesse. Toutefois, les catégories de Schwob permettent encore d'appréhender correctement l'argot moderne, dont un des dictionnaires les

[35] Afin de prémunir son identité réelle contre les multiples censures de ses œuvres par la Sorbonne, François Rabelais signait d'un anagramme : Alcofribas Nasier. Plus légèrement, il est encore l'auteur de la fameuse contrepèterie concernant les femmes folles de la messe. Toutefois, la banalité du procédé contrepétrique, et surtout la bienséance, dissuadent de s'y intéresser plus longtemps - bien qu'il s'agisse d'un procédé concernant pleinement notre propos, tout comme le palindrome, dont le plus ancien fut écrit par un moine dans un vieux français encore teinté de latin : on lit une prière de dévotion à l'endroit et un tissu de blasphèmes outrageants à l'envers...

[36] Voici un passage en Lanternois : "[...] Lors respondit Panurge. "Prug frest strinst sorgdmand strochdt drhds pag brleland. [..] Bouille kalmuch monach drupp delmeupplist rincq dlrnd dodelb vp drent loch minc stz rinquald de vins ders cordelis bur iocst stzampenards." À quoy dist Epistemon. "Parlez vous christian : mon amy, ou langaige patelinoys ? Non c'est langaige lanternoys." [...]" Rabelais, *Pantagruel*, Ch. IX, *Comment Pantagruel trouva Panurge lequel il ayma toute sa vie*, in *Œuvres Complètes*, Gallimard, Bibliothèque de la Pléïade, 1994, pp. 247 *sq.* Il n'est pas impossible que Rabelais ait jeté là les bases d'une nouvelle langue : il suffit de rappeler qu'il nous a légué environ 500 mots que nous utilisons encore (comme "encyclopédie"), parmi les milliers d'autres de son invention que nous n'avons pas conservés (à l'instar du trop obscène "circumbilivagination", auquel on a préféré tergiversation, qui illustre pourtant bien mieux par quel assemblage finalement surréaliste de latin mêlé de grec sont nés ces mots, leur conférant un sens quasi-implicite pour les *happy few* de l'époque). En réalité, il était plus difficile d'*entendre* Rabelais en 1535 qu'aujourd'hui, fut-ce dans le texte, littéralement "inouï" - ce qui augmentait l'effet comique. François Ier, qui protégea un temps Rabelais des foudres de la Sorbonne, se faisait lire *Pantagruel* et *Gargantua* à voix haute (Rabelais, *Op. cit.*, Introduction, p. IX).

[37] Schwob note que si le mot argot a d'abord désigné une bande de malfaiteurs avant de s'appliquer à leur langage, il faut alors sans doute chercher l'étymologie d'argot dans les quatre sections de la cour des Miracles : Egypte, Boëme, Argot, Galilée. Argot serait le mot d'argot pour désigner Arabie, ainsi qu'en témoignent St-Lago pour St-Lazare, ou Italgo pour Italien ; les zouaves en expédition ont ramené Arbico pour Arabe (Schwob, *op. cit.*, p. 37).

plus fameux fut rédigé par deux inspecteurs du Quai des Orfèvres en vue de l'édification des jeunes recrues.

Si la dérivation synonymique est un des deux principaux procédés de l'argot (avec le loucherbème), le pendant de la Langue des Oiseaux est manifestement la dérivation phonétique[38]. Afin d'avoir l'idée la plus récente et claire du procédé[39], sans exhumer les ouvrages ésotériques de Fulcanelli, célèbre initié encore en activité à Paris au début du XXème siècle (et qui serait selon d'aucuns le pseudonyme de Camille Flammarion[40] (1842-1925) - célèbre astronome et érudit, fondateur en 1887 de la Société astronomique de France, et auteur en 1862 d'une curieuse *Pluralité des Mondes Habités*), il faut se reporter aux œuvres de quatre écrivains de sa connaissance qu'il fréquentait au Chat Noir : Gaston Leroux[41], Maurice Leblanc[42], Alfred Jarry[43] et Raymond Roussel. Une hypothèse souvent tue à leur sujet veut que leurs ouvrages aient tous pour canevas l'oeuvre de Fulcanelli, du point de vue des procédés introduisant le mystère (c'est dire la complexité supposée des ouvrages de l'alchimiste). Selon cet initié, l'étymologie du mot cabale doit être trouvée dans l'ancien grec $\kappa\alpha\rho\beta\alpha\nu$ ("qui parle un langage incompréhensible"). Le langage hermétique, à travers la cabale[44] du même nom, distincte et sans doute plus récente que la Cabale hébraïque, aurait donc "visé l'ésotérisme le plus absolu, en greffant sur les méthodologies classiques, dans les traités alchimiques, un système linguistique hybride fait des assonances qui détournaient les mots d'usage courant. Il fallait ainsi lire non seulement le sens commun mais aussi suivant les sens que les mots, par affinité phonétique, pouvaient prendre dans l'antique idiome hellénique." [45]. Ce procédé, dans les détails duquel nous n'entrerons pas davantage, interdit quasiment toute analyse fondée sur la logique classique[46]. Roussel nous a légué une idée d'un des procédés dans sa compilation d'oeuvres de grande jeunesse intitulée *Comment j'ai écrit certains de mes livres.*

[38]La tradition hermétique veut voir par exemple, dans l'image d'un St-François d'Assise familier des animaux et des oiseaux en particulier, une preuve à peine dissimulée de l'initiation du *Poverello* d'Ombrie aux connaissances occultes.

[39]En jazz vocal, André Minvielle utilise un procédé similaire : à travers un flot ininterrompu de mots, quelques-uns se détachent et forment ensemble un curieux assemblage du plus bel effet.

[40]Exemple de dérivation phonétique hermétique : Flammarion = Flamme d'Orion = ... = Fulcanelli. Le passage d'un terme à l'autre se fait en maniant des symboles (sel, soufre, soleil, pluton, etc.) dont les interactions sont codifiées, dans une langue ressemblant fort au grec ancien.

[41]Faut-il rappeler les tenants et les aboutissants du *Mystère de la chambre jaune* ?

[42]Il multiplie les anagrammes pour son héros Arsène Lupin : Luis Perenna, Paul Sernine, etc.

[43]Dont le penchant avéré pour le déguisement des mots est connu : Ubu ne manie que trop la "pompe à phynances".

[44]Voici, naturellement enveloppée d'un mystère qui en est la marque de fabrique, la définition que donne Fulcanelli de la cabale hermétique : "Le latin caballus et le grec $\kappa\alpha\beta\alpha\lambda\lambda\eta\sigma$, signifient tous deux cheval de somme ; or, notre cabale soutient réellement le poids considérable, la somme des connaissances antiques et de la chevalerie ou "cabalerie" médiévale, lourd bagage de vérités ésotériques transmis par elle à travers les âges. C'était la langue secrète des cabaliers, cavaliers ou chevaliers. Initiés et intellectuels en avaient tous la connaissance. Les uns et les autres, afin d'accéder à la plénitude du savoir, enfourchaient métaphoriquement la cavale, véhicule spirituel dont l'image type est le Pégase ailé des poètes helléniques. Lui seul facilitait aux élus l'accès des régions inconnues ; il leur offrait la possibilité de tout voir et de tout comprendre, à travers l'espace et le temps..." (cité par A. Aromatico, *L'alchimie*, Gallimard, 1996, p. 45).

[45]A. Aromatico, *op. cit.*, p. 54.

[46]Au sujet de son *Ulysse*, James Joyce n'écrivait-il pas : "J'y ai mis tant d'énigmes que cela aura de quoi occuper les universitaires pendant encore quelques siècles... C'est ça l'immortalité."

Il y pousse le procédé à fond et obtient un effet poétique inédit et très efficace en pratique[47]. Ces textes courts présentent tous la même particularité : les premiers et derniers mots étant fixés par leur proximité phonétique (à un phonème près en général), l'auteur en déduisait une histoire permettant de faire le lien. Par exemple, le texte *Parmi les Noirs* débute par les mots "Les lettres du blanc sur les bandes du vieux billard", et se termine par "LES... LETTRES... DU... BLANC... SUR... LES... BANDES... DU... VIEUX... PILLARD." Nous citons Roussel[48] : "Dans la première [phrase], "lettres" était pris dans le sens de "signes typographiques", "blanc" dans le sens de "cube de craie" et "bandes" dans le sens de "bordure". Dans la seconde, "lettres" était pris dans le sens de "missives", "blanc" dans le sens d'"homme blanc" et "bandes" dans le sens de "hordes guerrières". Les deux phrases trouvées, il s'agissait d'écrire un conte pouvant commencer par la première et finir par la seconde." Du propre aveu de Roussel, il s'agit d'un procédé purement poétique, qui a été appelé translittération[49]. En liant ainsi deux phrases si proches phonétiquement par un récit-tampon, Roussel découvre au lecteur un nouvel espace de l'imaginaire qui interroge la nature même du texte. En ne donnant ainsi que *l'illusion* d'un sens caché, Roussel invente une sorte de "tatouage littéraire" de l'imaginaire, à considérer le tatouage en général comme l'écriture d'un message dans une langue imaginée pour l'occasion, donc factice. La marque que Raymond Roussel introduit dans ses textes est une sorte de bruit de fond poétique reconnaissable qui favorise également toutes les conjectures de l'imaginaire, et dont la "couleur poétique" dépend du problème littéraire combinatoire que l'on s'est proposé d'optimiser (l'effet poétique obtenu n'est probablement pas prévisible d'ailleurs, car dépendant trop des viscissitudes et des contraintes du langage). Ce procédé est à rapprocher de la Langue des Oiseaux, fonctionnant elle aussi par dérivation phonétique, et dont nous pouvons à présent proposer un exemple : Hubert Champagne, lui aussi initié, ne signait jamais que de sa devise latine "Uber Campa Agna", autre exemple de translittération, laissant ainsi deviner les liens, au moins littéraires, unissant les quatre écrivains habitués du Chat Noir à la tradition occulte. L'époque était aussi celle d'un Paris du début du XXème siècle encore baigné par l'orientalisme et son goût du mystère. Peut-être le coup de génie de ces écrivains fut-il d'avoir mis au point une mécanique littéraire qui introduit l'illusion du sens caché. Bien évidemment, d'autres procédés trop ardus pour être décrits ici, furent développés par les quatre écrivains[50].

Parallèlement, les techniques purement cryptographiques poursuivent leur développe-

[47]Le procédé de Roussel, à la différence du procédé hermétique, ne "suggère" pas un message en grec ancien, mais en français. Les musiciens potaches l'emploient dans une histoire sur la petite vertu supposée des filles de Lille car, paraît-il, le concerto en sol mineur (on notera que Simmons a proposé un cryptosystème avec des caractéristiques similaires de "double-décodage" [70]).

[48]Voir *Comment j'ai écrit certains de mes livres*, Gallimard, 1935.

[49]La théorie du sens caché dans les livres de Roussel ne trouve aucun écho chez Foucault dans son *Raymond Roussel* (Gallimard, 1963), même s'il prend soin de ne pas réfuter totalement cette éventualité. Il pensait certainement à *Locus Solus* (Pauvert, 1965), objet paraît-il d'intenses conjectures hermétiques.

[50]Toujours chez Roussel, l'écriture de ses *Impressions d'Afrique* lui a réclamé pas moins de sept ans (long poème en alexandrins sur 7 sept niveaux d'imbrication de parenthèses...) Mais il faut encore souligner que Roussel, méprisé de son vivant en tant qu'écrivain, fut également un joueur d'échecs émérite, qui laissa son nom dans l'histoire du jeu pour en avoir proposé une vision révolutionnaire : faire jouer les pièces "en coopération". Il a ainsi pu résoudre le premier, en trois mois et demi, le mat difficile dit "avec Fou et Cavalier", en 1932. En regard du degré de sophistication des procédés d'écriture qui ont pu être utilisés, l'anecdote est de taille.

ment. Mais c'est en 1605 que Sir Francis Bacon[51], dans *Proficience and Advancement of Learning Divine and Humane*, donne sa préférence aux méthodes n'attirant pas la suspicion, c'est à dire à la stéganographie : "in regarde of the rawnesse and unskilfulnesse of the handes, through which they passe, the greatest Matters, are many times carried in the weakest cyphars". En disséquant les œuvres de Shakespeare, avec les outils cryptographiques de l'époque et un alphabet élisabéthain, certains pensent y avoir trouvé en filigrane le nom de Francis Bacon, qui n'était pas seulement un des cryptologues les plus renommés de son temps, mais aussi poète. Il est vrai que la vie obscure et mal connue de Shakespeare, couplée à la réputation de Bacon de conseiller de l'ombre, a pu alimenter toutes les controverses. Suivant l'avis de Bacon, la stéganographie tend à devenir un art supérieur en finesse et en efficacité à la cryptographie. Ce point de vue reste à notre sens encore valable aujourd'hui : un pare-feu sur le réseau peut très bien interdire la transmission de messages à forte entropie (supposés cryptés), sans jamais pouvoir déceler aucun contenu caché dans une image ou un son[52].

Plus près de nous, Gustavus Simmons a mis en évidence l'existence d'un canal subliminal [69, 70] dans l'algorithme DSA (Digital Signature Algorithm) utilisé par le gouvernement américain. L'algorithme ElGamal est lui aussi susceptible de transmettre quelques dizaines de bits de manière subliminale. Toujours dans le domaine des outils cryptographiques, il est pour le moins surprenant que le protocole SSH (Secure SHell) n'impose pas de "Self-Describing Padding" mais un bourrage aléatoire, invérifiable, offrant par là un boulevard à l'évaporation des clefs chiffrant la connexion en cours, entre autres. Voilà qui plaide éloquemment pour l'utilisation de logiciels dont le code source est accessible. La découverte de canaux subliminaux par Simmons date de la guerre froide, lorsque les deux super-puissances devaient chacune pouvoir vérifier le nombre de têtes nucléaires de l'adversaire sans divulguer leur emplacement, variable dans le temps. Les USA et l'URSS se mirent d'accord sur un protocole cryptographique, dont Simmons a prouvé qu'il autorisait la transmission d'un bit d'information cachée au moins, augmentant potentiellement d'autant la connaissance de l'adversaire sur la localisation des missiles.

1.2 Tatouage et distribution des œuvres : une situation

Nous venons de dresser un bref panorama de la stéganographie et de son utilisation au cours des siècles, mais le tatouage son descendant trouve son origine dans le filigrane. C'est au XIVème siècle à Fabriano en Italie que les ouvriers produisant le papier renommé de cette région, eurent l'idée d'y inclure les premiers filigranes, essentiellement à des fins d'authentification de la provenance du papier. On visite aujourd'hui le musée dédié à ces premiers filigranes. Le filigrane trouva naturellement son cadre d'application privilégié dans les billets de banque. Voisin de la technique du filigrane, la flétrissure royale imposée sur l'épaule du criminel permettait de marquer à vie la félonie du sujet. Dans *Les trois mousquetaires*,

[51] Dont l'appartenance hypothétique à l'ordre secret de la Rose-Croix, souvent évoquée, semble à rejeter.

[52] La légende des messages subliminaux prétendûment contenus dans les chansons de rock jouées à l'envers doit rester pour ce qu'elle est : une fiction inquisitrice égarée en plein XXème siècle. Le procès intenté à Judas Priest a permis de mettre en évidence que quantité de chansons jouées à l'envers peuvent suggérer des messages cachés, mais qui n'ont pas souvent de sens...

Alexandre Dumas[53] met en scène la flétrissure de Milady, qui permettra à D'Artagnan de la reconnaître à Béthune, même et surtout *Vingt ans après*. De nos jours, on utilise le marquage à l'encre pour tracer la provenance des viandes. Chez les Maori, entre autres, le tatouage marque le passage du garçon dans l'âge adulte à la suite d'une cérémonie initiatique[54]. Si le marquage autre que symbolique est récent chez l'homme, les canidés utilisent le marquage olfactif à l'urine pour délimiter leur territoire sans doute depuis qu'ils existent.

On peut argumenter que les besoins en tatouage étaient relativement limités dans un monde alors uniquement analogique, et la révolution numérique n'a fait que remettre au goût du jour cette technique. En effet, copier un document analogique implique nécessairement une perte de qualité de la copie par rapport à l'original, alors que la duplication de symboles numériques ne nécessite aucune transcription matérielle, autorisant la duplication parfaite à l'infini de l'original. Le tatouage numérique doit son développement pratique à celui d'internet essentiellement, et surtout au fait que les limites du système sensoriel humain ne lui permettent pas de distinguer deux objets très proches en apparence. Mais nous ne percevons que trop bien quelle est la finalité plus profonde du tatouage. Cette finalité consiste à pouvoir dégager artificiellement, par des moyens purement techniques, l'authenticité d'une œuvre d'art (et par là, de nos jours, sa valeur[55]). Benjamin[56] notait en 1972 qu' "à la plus parfaite reproduction il manquera toujours *une* chose : le *hic* et *nunc* de l'œuvre d'art - l'unicité de son existence au lieu où elle se trouve."[57] Il définit ainsi l'authenticité de l'œuvre d'art, et poursuit : "Tous ces caractères [d'authenticité] se résument dans la notion d'aura, et on pourrait dire : à l'époque de la reproductibilité technique, ce qui dépérit dans l'œuvre d'art, c'est son aura."[58] La perception de l'œuvre change alors : à sa transcendance passée, réelle ou supposée, se substitue de nos jours une pure immanence. Le rapport à l'art, ce succédané de religion pour d'aucuns, est bouleversé, glissant à peu de choses près de l'extase du croyant s'étant déplacé tout exprès pour admirer la Vierge de la chapelle Sixtine, à la névrose compulsive du collectionneur de gigaoctets de MP3.

Se pose alors le problème de l'économie artistique : "[...] le fait qui est ici décisif : pour la première fois dans l'histoire universelle, l'œuvre d'art s'émancipe de l'existence parasitaire qui lui était impartie dans le cadre du rituel. De plus en plus, l'œuvre d'art reproduite devient reproduction d'une œuvre d'art conçue pour être reproductible. De la plaque photographique, par exemple, on peut tirer un grand nombre d'épreuves ; il serait absurde de demander laquelle est authentique. [...] La reproductibilité technique des films est inhérente

[53]Il est facile de se tromper dans la généalogie de Dumas. Nous parlons évidemment d'Alexandre Dumas père (1802-1870), lui-même fils du général de division Alexandre Dumas-Davy de la Pailleterie (1762-1806, fils d'Antoine-Alexandre Davy et de Marie-Zézette Dumas), et non d'Alexandre Dumas fils (1824-1895), lequel est donc le petit-fils du premier Alexandre, en date et non en littérature, chez les Dumas.

[54]"[...] De même dans les traditions occidentales le tatouage a longtemps passé pour mettre à l'abri des démons, des mauvais esprits, des maladies et des accidents. Les marins, qui ont un engouement particulier pour les tatouages, croient, dit-on, que ceux-ci protègent des maladies vénériennes. [...] Dans la marine américaine, un cochon et un coq, tatoués sur le cou-de-pied gauche, préservent de la noyade." E. Mozzani, *Le livre des superstitions*, Robert Laffont, 1995, p. 1693.

[55]Une copie faite au XVIème d'une œuvre originale datant de l'Antiquité, est *aujourd'hui* considérée comme authentique.

[56]W. Benjamin, *L'œuvre d'art à l'époque de sa reproductibilité technique*, Allia, 2003, trad. M. de Gandillac.

[57]W. Benjamin, *op. cit.*, II, p. 13.

[58]W. Benjamin, *op. cit.*, II, p. 16.

à la technique même de leur production. Celle-ci ne permet pas seulement, de la manière la plus immédiate, la diffusion massive des films, elle l'exige."[59] On appréhende alors plus finement la dynamique qui cette fois lie le producteur d'une œuvre à ceux qui en jouissent : "Des calculs ont montré qu'en 1927 l'amortissement d'un grand film exigeait qu'il fût vu par neuf millions de spectateurs. Au début, il est vrai, l'invention du parlant a constitué une régression ; son public a été limité par les frontières linguistiques, à l'époque même où le fascisme insistait sur les intérêts nationaux. Cette régression, vite atténuée par l'usage de la post-synchronisation, doit moins nous retenir que le rapport avec le fascisme. Les deux phénomènes sont simultanés car ils sont liés à la crise économique. Les mêmes perturbations qui, à l'échelle générale, ont conduit à chercher les moyens de sauvegarder les rapports de propriété par la force, ont amené le capital investi dans le cinéma, menacé par la crise, à hâter la mise au point du parlant."[60] Le tatouage numérique, dans sa composante orwellienne fantasmée, s'inscrit précisément dans la collection des "moyens de sauvegarder les rapports de propriété par la force." Naïvement, le tatouage aurait donc eu pour objet, au début, d'insuffler de l'aura à une œuvre numérique, de garantir son authenticité (au sens de Benjamin) et par là sa valeur, marchande aujourd'hui.

Pourtant, Benjamin nous avait mis en garde : "dès lors que le critère d'authenticité n'est plus applicable à la production artistique, toute la fonction de l'art se trouve bouleversée. Au lieu de reposer sur le rituel, elle se fonde désormais sur une autre pratique : la politique."[61] Le tatouage, en tant qu'il est censé participer du processus de reproductibilité et de distribution des œuvres numériques, doit donc avant tout être compris dans sa dimension politique pratique, *en rapport* avec l'idée fondamentale de reproduction en série qui est un bouleversement récent. En suivant Benjamin, il faut éviter le contrens selon lequel c'est le caractère *numérique* des œuvres à protéger qui aurait impulsé l'effort autour du tatouage numérique. C'est bien plutôt que les machines devaient enfin pouvoir rendre son utilisation *automatique*, voire *systématique* (le climat politique des années 1930 influencerait donc d'une certaine manière encore notre conception de la protection des droits[62], mais en démocratie sociale ce sont les pratiques qui tempèrent les lois et non l'inverse, et le législateur manque encore de recul sur l'étendue et la nature des pratiques réelles en la matière).

En effet, les cahiers des charges en tatouage pour la protection des droits stipulent tous une robustesse face à la conversion numérique/analogique/numérique - on n'a jamais vraiment souligné les implications d'une telle extension *de facto* au monde analogique, trahissant

[59] W. Benjamin, *op. cit.*, IV, p. 24.

[60] W. Benjamin, *op. cit.*, IV, p. 25.

[61] W. Benjamin, *op. cit.*, IV, p. 26. Et comme le rappelle Benjamin en terminant son étude, on ne sait que trop par quels autres funestes moyens la politique peut se continuer...

[62] Par le même jeu d'analogie, Sade le premier, qui a passé la moitié de sa vie *au secret*, rapprochait *logique* de *cruel*... Pour Sade, la logique *est* cruelle - et c'est bien là l'aspect le plus angoissant et précurseur de son œuvre, pour qui prend la peine de passer outre son prime abord logorrhéïque. Il faut encore ajouter que la littérature contemporaine de Sade comportait un courant dit réglementariste (par exemple, Rétif de la Bretonne, l'adversaire farouche de Sade, prenait dans son *Pornographe* le prétexte d'une correspondance entre deux amis pour discuter un règlement des maisons closes). Sur ce sujet, voir G. Bataille, *La littérature et le mal*, Sade, Gallimard, 1957. Voir encore le film de Pier Paolo Pasolini, *Salò ou les 120 journées de Sodome*, qui met en scène le calvaire de 18 jeunes gens sous la contrainte d'un règlement sadique, brimés par des notables de la république fantoche que Mussolini avait proclamée à Salò, en Lombardie, de septembre 1943 à avril 1945.

la chronologie réelle : ce sont les progrès en traitement du signal et des images qui ont permis l'actualisation d'une idée rendue nécessaire, en son temps, par la seule reproductibilité technique de l'œuvre d'art. Les problèmes de *distribution* liés à Internet sont en cela un épiphénomène, certes aggravant. Le défi politique porté par le tatouage robuste est donc en réalité l'ultime tentative d'affirmation *systématique* des rapports de propriété dans le domaine des œuvres, problématique datant très exactement selon Benjamin de la photographie et de la reproduction en série en général. Contrairement à la cryptographie, les techniques de tatouage sont utilisées en vue d'annexer même les œuvres de l'ancien monde purement analogique, *parce que* leur mode de reproduction technique (et de transmission) est aujourd'hui essentiellement numérique. En dernier lieu, le tatouage numérique pour la protection des droits doit se comprendre *en réponse* au développement technique de la reproduction en série des œuvres, et donc aussi comme son complément historique dans un monde devenu numérique entre-temps. Ce qui est en jeu est donc la proximité économique entre un artiste et son public : s'il devient de moins en moins possible de distribuer de manière rentable un artiste dans le monde entier, il se produira mécaniquement une restriction du public jusqu'à des échelles jamais connues. Une caméra DV et un PC standards permettent même de rêver d'un cinéma entre *happy few...* pour des projections forcément moins fréquentes et plus variées, recréant les conditions d'un nouveau rapport à l'art. Simplement parce que la renommée deviendrait plus locale, on rendrait à nouveau possible les légendes : ce que seulement quelques-uns ont vu. Stratégiquement, il eut sans doute été plus judicieux de la part des majors de tenter de maintenir inabordable pour un particulier le niveau d'équipement technologique nécessaire à la *création* des contenus. Mais, comme Sony et Philips le démontrent (toutes deux produisent des artistes et vendent des graveurs de CD), personne n'a encore vraiment choisi.

Prenant le contrepied de ces considérations, il faut aussi s'intéresser aux autres applications du tatouage, non moins chargées politiquement, que son aptitude, réelle ou pas, à assurer la conservation des rapports de propriété. Par exemple, garantir l'intégrité d'un média numérique peut s'avérer de la plus haute utilité[63]. De même, le tatouage peut encore servir à augmenter l'accès à l'information par les déficients, trop facilement assimilés à des poids morts depuis le XVIème siècle[64]. Nous allons à présent nous attarder sur le tatouage numérique, et détailler ses variantes mises chacune en regard de leur cadre applicatif respectif.

1.3 Techniques numériques et cadres applicatifs

Nous détaillons à présent les principaux cadres applicatifs dans lesquels les techniques d'écriture secrète jouent un rôle prépondérant. Partant de la stéganographie pure et de ses relations avec la cryptographie, nous abordons les deux types de tatouage : fragile et ro-

[63]On ne connait que trop la tendance des autocrates, Staline en tête, à effacer des photos officielles les personnalités gênantes. Lorsque Benjamin souligne le déplacement du rapport à l'art vers la politique, il pensait au cinéma de propagande soviétique, au culte de la personnalité démultiplié par les reproductions en série, etc.

[64]Dans son *Histoire de la Folie à l'âge classique*, Gallimard, 1972, Foucault montre que les sourds et muets avaient été un peu trop rapidement considérés comme fous, et enfermés (selon le fameux axiome qui veut qu'un néant de langage implique un néant de pensée). Depuis, leur alphabétisation a été rendue possible par d'autres techniques - mais leur accès égal à l'information n'est toujours pas garanti.

buste. Pour commencer, nous donnons une classification de ces techniques sur la Fig. 1.2. Nous n'aborderons pas davantage les spécificités des techniques cryptographiques outre me-

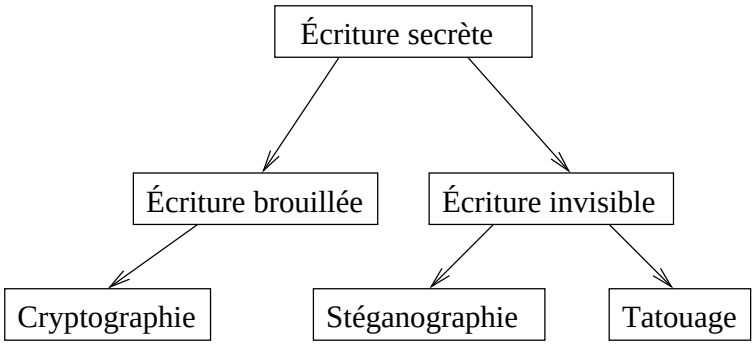

Fig. 1.2 – Classification des différentes techniques d'écriture secrète.

sure. Il faut cependant distinguer les deux formes possibles de chiffrage : privé et public. Le chiffrage privé, ou symétrique, nécessite la même clef pour brouiller les données que pour les déchiffrer. A l'inverse, la cryptographie publique, ou asymétrique, nécessite seulement que les clefs de chiffrage et de déchiffrage vérifient une certaine relation. L'exemple le plus utilisé de cryptographie asymétrique est l'algorithme RSA, du nom de ses trois co-inventeurs (Rivest, Shamir et Adelman). En pratique, les opérations de cryptographie publique nécessitent beaucoup plus de calculs que leurs équivalents symétriques, d'où leur limitation au chiffrage de la clef de déchiffrage d'un algorithme symétrique uniquement (par exemple dans Pretty Good Privacy, de Philip Zimmermann).

Nous nous devions de rappeler cette différence car le tatouage nécessite lui aussi l'utilisation de clefs, et le plus souvent ces algorithmes sont symétriques, même si Teddy Furon [30] a proposé une méthode de tatouage asymétrique (le mot asymétrique ne peut pas être entendu strictement de la même manière ici que dans le cas de la cryptographie, pour des raisons que nous ne détaillerons pas).

1.3.1 Stéganographie et contenus augmentés

La stéganographie peut avoir d'autres applications que la communication secrète, nous renvoyons à l'introduction pour cet aspect. Parmi ces autres applications, nous souhaitons mentionner l'augmentation de contenus. Par augmentation de contenu, on entend l'ajout d'information cachée dans un média afin qu'un utilisateur équipé du décodeur approprié puisse exploiter des fonctionnalités supplémentaires. Les deux exemples que nous citons concernent la mise à disposition des sourds et malentendants d'un terminal spécial, et la transition douce entre le monde des récepteurs analogiques et numériques. Bien entendu, les applications de communication secrète restent le principal motif de développement de telles techniques.

Les contraintes pesant sur les systèmes de cryptographie sont au nombre de deux :
- la modification du média doit être imperceptible ;
- la capacité du canal stéganographique doit être élevée.

Aide aux sourds et malentendants

Aujourd'hui, l'accès des sourds et malentendants à la télévision est limité par le faible nombre de programmes sous-titrés, ou utilisant le télétexte. Une solution proposée consiste à enfouir dans le signal vidéo l'information nécessaire à l'animation d'un clône tridimensionnel synthétique qu'un décodeur ad hoc viendrait superposer à l'image reçue dans un coin de l'écran. L'avantage de ce système est de ne requérir aucun changement de matériel chez les utilisateurs (ils gardent leur télévision), et ceux qui en ont besoin s'équipent du décodeur capable de séparer l'information cachée du signal vidéo, et d'animer le clône 3D. C'est l'objet du projet Artus[65].

Transition tout-analogique vers tout-numérique

En télévision, le passage du tout-analogique vers le tout-numérique est prévu à l'horizon 2010 pour la France. Cependant, la technologie des récepteurs est fondamentalement différente. Or, on ne peut décemment envisager une transition brutale pour les utilisateurs, qui devraient pouvoir pour certains continuer à recevoir leurs programmes analogiques, alors que les premiers équipés demanderont à profiter immédiatement des avantages du numérique. Pour cela, on utilise le fait que la compression du flux numérique autorise de faire passer davantage de données qu'avec une transmission analogique, sur la même bande passante. L'idée consiste à récupérer une partie du spectre des transmissions analogiques pour y placer l'information numérique souhaitée. De cette manière, on peut opérer en douceur la transition entre les deux modes de communication. Plusieurs canaux numériques peuvent ainsi être véhiculés dans le spectre d'un seul canal analogique [63]. Cela peut se faire en utilisant l'idée de Costa [18].

Communication secrète

On dénombre environ une vingtaine de logiciels spécialement dédiés aux communications secrètes[66] qui utilisent la stéganographie. La plupart des médias ont été mis à contribution : le texte[67], le son (WAV[68], MP3[69]), l'image (essentiellement les formats non compressés[70], mais aussi JPEG[71]). Toutefois, il existe quelques logiciels qui cachent l'information dans les parties du fichiers de média réservées d'ordinaire aux commentaires[72]. Dans ce cas, la taille du fichier média augmente en fonction de ce que l'on y cache, et cela peut attirer la suspicion. Le principal avantage devant rester de ne pas attirer l'attention sur le fichier échangé, ces méthodes doivent être proscrites ou réservées à de petits fichiers à cacher. Pour donner une idée de la capacité du canal stéganographique dans une image non compressée, il faut savoir qu'il est possible d'utiliser, avec la modification des LSB (Least Significant

[65] http ://www.telecom.gouv.fr/rnrt/projets/res_01_37.htm
[66] http ://www.cl.cam.ac.uk/ fapp2/steganography/stego_soft.html
[67] http ://www.ctgi.net/nicetext
[68] ftp ://idea.sec.dsi.unimi.it/pub/security/crypt/codes/s-tools4.zip
[69] http ://www.cl.cam.ac.uk/ fapp2/steganography/mp3stego/index.html
[70] http ://www.outguess.org
[71] ftp ://ftp.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz
[72] http ://camouflage.unfiction.com/

Bits), les quatre derniers plans de bits (en utilisant de la diffusion d'erreur pour atténuer les désagréments visuels). Ainsi, une image bitmap en niveaux de gris peut être divisée en deux parties : les quatre plans de bits les plus importants véhiculent l'information visuelle de l'image, tandis que les quatre derniers peuvent être entièrement dévolus au codage d'un fichier caché, moyennant l'emploi de techniques de diffusion d'erreur afin d'adoucir l'aspect visuel obtenu.

La principale contrainte pesant sur ces systèmes est celle de l'imperceptibilité, tant perceptuelle que statistique - tout en cherchant à maximiser la capacité du canal caché.

1.3.2 Tatouage fragile, authentification et intégrité

L'authentification a pour but de procurer une information sur une modification éventuelle d'un média. Une manière d'y parvenir est d'insérer dans le média un tatouage fragile. Un tatouage fragile a pour objet de disparaître à la moindre modification. Ainsi, s'attendant à retrouver une marque fragile, on pourra décider de l'authenticité du média considéré. Si la marque fragile a disparu, on n'accordera plus aucune confiance au média, et on évitera de l'utiliser.

Si l'on désire obtenir davantage d'information sur les modifications éventuelles subies par le média, on aborde le problème de l'intégrité. Dans ce cas, la marque à cacher de manière fragile sera constituée d'information grossière sur le média lui-même. Il devient ainsi possible de détecter l'endroit et la nature des changements opérés sur le média.

Les contraintes pesant sur ce genre de système sont :
- la modification du média doit être imperceptible ;
- la capacité du canal caché est faible (authenticité) ou moyenne (intégrité) ;
- la robustesse de la marque doit être faible.

1.3.3 Tatouage robuste et protection des documents

Il s'agit ici de ce qui représentait l'espoir le plus important au milieu des années 1990 lorsque naissait le tatouage. Par protection des documents, nous entendons d'une part protection de la copie, et d'autre part protection du droit d'auteur. Ces deux applications ont en commun de devoir mettre en œuvre une marque très résistante à différentes manipulations.

La protection de la copie se propose d'inscrire dans le média les modes d'accès autorisés au média : lecture (une fois), lecture (nombre indéfini de fois), copie (une seule fois, à des fins de sauvegarde), ou copies multiples. Ce genre de système est utilisé dans le système de protection du DVD Millenium. Le contenu d'un DVD est d'abord tatoué, puis crypté. Lorsqu'un contrevenant cherche à décrypter le contenu du DVD, il reste le tatouage. Ainsi, un lecteur commercial standard est prévu pour ne pouvoir jouer que deux types de contenus : les DVD cryptés et tatoués, ou alors les DVD ni cryptés ni tatoués. Si on cherche à jouer un DVD décrypté dans un lecteur standard, la lecture sera refusée car pour le lecteur, le contenu est probablement piraté. En outre, lorsqu'un utilisateur réalise son propre DVD, il ne cherchera vraisemblablement pas à protéger son contenu (ou tout au moins, pas avec la même technologie de tatouage). Ce système permet de jouer les DVD du monde commercial, et ceux réalisés par l'utilisateur lui-même. Du point de vue du tatouage, un tel système requiert une capacité très faible du canal de tatouage, deux ou trois bits suffisent.

Dans le cadre de la protection du droit d'auteur, on cherche à inscrire dans le média un identifiant relatif à l'ayant-droit de l'œuvre. Généralement, cet identifiant mesure 64 bits. Naturellement, l'inscription de la marque doit être très robuste. Plus précisément, on souhaite que la marque disparaisse seulement dans le cas d'attaques tellement sévères sur le média qu'elles en empêchent toute utilisation commerciale du fait de la perte de qualité due à ces attaques. L'identifiant est ensuite stocké chez une tierce partie de confiance qui fait le lien entre l'identifiant et le nom de l'ayant-droit. A ce jour, aucune jurisprudence sur le sujet n'est disponible.

Ces deux applications requièrent quant à elles de satisfaire aux contraintes suivantes :
- la modification du média doit être imperceptible ;
- la capacité du canal de tatouage varie de faible (protection de la copie) à moyenne (protection du droit d'auteur) ;
- la marque doit être très robuste.

En général, on cherchera à pouvoir insérer deux tatouages dans un média : l'un robuste et l'autre fragile. Ainsi, on arrive à protéger à la fois le contenu et les droits.

1.4 Le tatouage et son environnement

1.4.1 Vocabulaire

Après avoir donné une liste des applications dans lesquelles les techniques de tatouage ou de stéganographie sont centrales, il convient de préciser le lexique que nous utiliserons par la suite, relativement aux notions de tatouage. Nous détaillons à présent les principaux termes utilisés :
- Média : le contenu pouvant subir une modification de nature à enfouir de l'information cachée à l'intérieur ;
- Signature, marque : ce que l'on cache dans le cadre du tatouage, fragile comme robuste ;
- Marquage, tatouage, filigranage, incrustation, insertion, enfouissement : les opérations agissant sur l'information en vue de la cacher ;
- Attaque : du point de vue de la marque, n'importe quelle manipulation sur le média. On distingue les attaques autorisées des attaques malveillantes (destinées à attaquer spécifiquement la marque) ;
- Extraction, relecture : l'opération visant à récupérer la marque ;
- Capacité : le nombre de bits d'information cachée que l'on peut inscrire à l'aide d'un schéma particulier de tatouage ;
- Robustesse : ensemble des attaques auxquelles résiste tel schéma particulier de tatouage ;
- Resynchronisation : procédé visant à s'affranchir des attaques modifiant le positionnement absolu du tatouage.
- Clef : le paramètre secret sur lequel repose la possibilité de relecture ;
- Tatouage additif (linéaire) : le message à cacher est transformé en un signal que l'on ajoute de manière additive au média ;
- Tatouage substitutif (non linéaire) : consiste à isoler une caractéristique du média et à la forcer à l'état désiré pour chaque bit à cacher ;

- Tatouage aveugle : le média original n'est pas nécessaire à l'étape d'extraction ;
- Tatouage supervisé : le média original est nécessaire à l'étape d'extraction, principalement à des fins de resynchronisation ;
- Espace de tatouage : espace dans lequel a lieu l'incrustation.

1.4.2 Le tatouage comme problème de télécommunication

Parmi d'autres points de vue possibles, le tatouage a pu être formulé comme un problème de communication classique : le canal de communication est le média, et le message à transmettre est la marque. Les pertes sur le canal modélisent les attaques. Nous récapitulons cette modélisation sur la figure suivante :

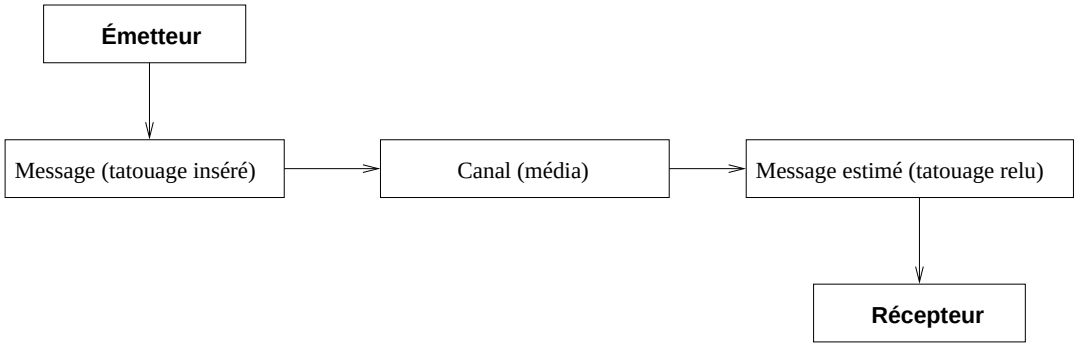

FIG. 1.3 – Modélisation du tatouage comme un problème de communication : le canal de communication est le média dans lequel on cherche à retrouver le message inséré à l'aide de la clef secrète.

Notre travail s'inscrit clairement dans cette approche. Ainsi, nous nous fixerons comme objectif d'optimiser la capacité du canal caché sous contraintes de quelques attaques autorisées, considérées comme non intentionnelles.

1.4.3 Typologie des attaques

Il convient également de présenter une typologie des différentes manières d'attaquer la marque. Le but ici n'est pas de donner une liste d'attaques pour tel média, mais plutôt de classer les attaques en fonction de l'aspect du processus de tatouage qui est mis en déroute.

- Attaques géométriques : on classe dans cette catégorie les modifications du support sur lequel vit le signal de tatouage. Par exemple, dans le cas de l'image, une rotation, une déformation de tapis[73], etc. Le principal écueil à craindre ici est une désynchronisation du signal de tatouage entre l'incrustation et l'extraction : la marque est toujours présente mais le décodeur ne sait plus où la chercher,
- Attaques sur le signal de tatouage : ce sont les manipulations s'apparentant à un filtrage. On range dans cette catégorie les différents filtrages connus : lissage, réhaussement de contraste, ainsi que la compression avec perte, etc. Ici c'est la puissance

[73]La déformation de tapis consiste en de petites déformations locales de la grille d'échantillonnage.

du signal de tatouage qui risque de devenir trop faible pour que l'extraction s'opère correctement (l'attaque consistant à effacer un signal de resynchronisation est donc à ranger dans cette catégorie) : c'est typiquement le mode d'action d'une *averaging attack*[74],

– Attaques de protocole : ces attaques opèrent à un niveau d'abstraction supérieur. On cherche ici à induire en erreur le processus d'extraction par différentes manières, dont les plus courantes consistent à insérer plusieurs signaux de tatouage au lieu d'un seul comme s'y attendrait le module d'extraction (par exemple, la *copy attack*[75] ou le surmarquage[76]). On peut également faire en sorte de créer un nouveau média en moyennant plusieurs versions tatouées du même média (*averaging attack*)

Précisons d'emblée qu'aucune méthode de tatouage pour aucun média ne propose une robustesse suffisamment élevée face à ces trois types d'attaques. C'est la raison pour laquelle il convient en premier lieu d'identifer clairement les attaques qu'aura à subir la marque. Le tatouage reste un art auquel la science prête ses moyens.

1.4.4 Sociologie économique de la piraterie

Au jeu du chat et de la souris, il n'est jamais inutile de bien cerner l'adversaire et ses motivations. Nous présentons ici une brève typologie des pirates et de leurs moyens, présentée sous un angle économique. Nous tirons ce formalisme de [65]. On se propose de donner un modèle simple de l'économie de la piraterie face à l'industrie de loisirs. Pour cela, il faut considérer que le coût des biens piratés est une fonction du coût de la création de la première copie pirate, noté e, et du coût de la distribution de chaque copie pirate, noté d. Ainsi, il en coûtera $d + \frac{e}{n}$ de créer et distribuer chacune des n copies pirates d'un contenu. Aujourd'hui seul vraiment subsiste le problème du coût e de création de la première copie pirate (il ne coûte rien, en regard de e, de distribuer une version pirate sur un réseau *peer-to-peer* ou d'utiliser un réseau de redistribution maintes fois amorti ; d peut donc être quasi-nul). Ici, la qualité de la copie est fonction des moyens financiers : on trouve sur eMule des copies de films acquis dans la salle de projection elle-même (le bon sens réclame donc de rémunérer correctement le projectioniste pour plus de sécurité), mais le même jour circule déjà en Asie un DVD du même film, de qualité optimale, car le pirate aura eu accès à la matrice de duplication. Il faut donc classer les pirates selon leurs moyens, évaluer les risques qu'ils représentent, et établir une politique de sécurité en conséquence. Nous appelons artisan, industriel et État les trois types de pirates potentiels, suggérant ainsi une gradation dans la quantité et la qualité de leurs moyens, et aussi des besoins différents. Par pirate, nous entendons quelqu'un qui recherche un accès frauduleux à une information, supposée protégée par un système de sécurité (cryptographie et/ou stéganographie). Le motif du piratage tient successivement du défi (pour l'artisan), de l'enjeu économique (pour l'industriel), voire de la surveillance des individus (pour l'État). Les mafias sont un cas à part qui relève à la fois de l'industriel et de l'État (elles peuvent se servir de la piraterie pour subvenir à la fois à des besoins économiques et de surveillance). Bien entendu, chacun de nos trois personnages conceptuels (artisan, industriel, État) peut éventuellement découvrir (voire organiser) une

[74]Estimer le signal de tatouage, puis le "soustraire" le mieux possible du médium.
[75]Recopier un signal de tatouage associé à un médium sur un autre médium.
[76]Introduire plusieurs tatouages sur un médium déjà tatoué, suivant la même technique.

faille dans le système de sécurité, se réservant pour lui seul la possibilité d'un coût e faible. Mais seul un artisan pourra avoir la naïveté d'en faire part au reste du monde. C'est en ce sens que l'artisan est le principal garant des systèmes de sécurité actuels.

L'artisan

L'artisan, même s'il peut utiliser un réseau *peer-to-peer* pour transmettre efficacement les contenus pirates qu'il a créés, ne peut jamais consacrer que de faibles moyens à la création de sa première copie pirate. Ainsi, son investissement sur e est-il très faible, de l'ordre de quelques dizaines de milliers d'euros au maximum (quelques gros PC et du matériel électronique). L'histoire économique de l'industrie de loisirs se borne à imposer un coût e moyen dépassant les possibilités d'un artisan. Cela peut être un simple particulier comme une personne connaissant les détails du problème. Il arrive qu'une personne seule casse un système dont on croyait que cela était au-dessus de ses moyens : c'est le cas de Serge Humpich qui, profitant d'une faille d'implantation mathématique de l'algorithme de cryptage de la carte à puce, a menacé la sécurité, et donc l'existence, du système bancaire pour particuliers. Une tentative réussie de piraterie s'appelle, pour l'artisan, un *exploit* - et il est de bon ton de se prévaloir de ses exploits sur un forum. L'artisan cherche à relever un défi pour des raisons esthétiques, voire politiques : il représente le piratage romantique. Toutefois, il peut arriver qu'il travaille ensuite, par désillusion ou vénalité, pour un industriel ou un État.

L'industriel

L'industriel est appelé ainsi en raison de sa capacité déjà conséquente de création et de distribution propre des copies pirates. Il peut s'agir d'une branche d'une organisation criminelle, comme d'une multinationale recherchant des informations sur un concurrent. Un coût e de plusieurs dizaines de millions d'euros leur est parfaitement envisageable. D'autant que pour eux, n n'est jamais très grand non plus (au besoin). L'industrie de loisirs cherche à ce qu'un industriel du piratage mette plusieurs mois à forcer le système de sécurité, environ le temps qu'un contenu ait été rentabilisé par les producteurs du contenu. Toutefois, les industriels de la piraterie multimédia trouvent souvent plus efficace en première approche d'infiltrer un agent ayant accès au contenu original. C'est généralement un industriel qui corrompt les projectionistes des salles de cinéma.

L'État

L'État, en tant que personnage conceptuel, désigne ici une entité ayant un besoin spécifique de *surveillance* des individus qui le composent. Un État considère que la connaissance d'informations sur ses individus est un gage de sa survie. Les moyens qu'il peut consacrer à cet objectif sont sans équivalent : il dispose de moyens tant matériels que financiers ou humains. Un État n'a pas nécessairement besoin de distribuer des copies pirates (à moins de considérer une mafia, qui dispose en général déjà de son propre réseau de distribution), forcer le système de sécurité lui suffit : il peut concentrer tous ses efforts dessus.

1.5 Conclusion

L'écriture secrète sur les médias numériques est un défi qui mobilise les compétences de milliers de personnes dans le monde, vers des objectifs très divers. On peut, comme nous l'avons fait, choisir de modéliser ce problème par une approche télécommunications : le canal de transmission est le contenu sur lequel on écrit le message à transmettre. Le bruit sur le canal de transmission correspond aux attaques, intentionnelles ou non, subies par la marque qui est la représentation physique du message à transmettre. Par attaque, on entend n'importe quelle manipulation appliquée au média. Les développeurs de méthodes de tatouage cherchent à proposer des solutions dont le niveau de sécurité dissuade un artisan ou un industriel du piratage.

Chapitre 2

Surfaces et maillages

2.1 Introduction

Dans ce chapitre, nous présentons divers types de données surfaciques 3D, leur mode d'acquisition privilégié, et leur modélisation. Nous traitons ensuite spécifiquement des surfaces triangulées dont nous rappelons quelques propriétés topologiques, et nous présentons les principaux outils pour la génération d'une telle connexité à partir d'échantillons bruts. Ensuite, nous expliquons comment coder efficacement en mémoire des relations complexes d'adjacence de facettes. Nous donnons aussi une liste d'attributs souvent attachés à la géométrie (sommets ou facettes), généralement résultats d'une mesure physique. Nous terminons en précisant comment on peut comparer deux structures géométriques surfaciques maillées.

2.2 Principaux types de données surfaciques

Fondamentalement, il existe deux types de données surfaciques 3D : celles qui sont acquises par numérisation, et celles qui sont créées par assemblage de surfaces paramétrées (comme en CAO). Le premier type est souvent issu de mesures laser, de calculs de stéréovision, de mesures radiologiques médicales, suivis de traitement d'image. Le second peut résulter d'assemblage logique ou géométrique de volumes élémentaires dont on prend les enveloppes, ou de portions de surfaces analytiques juxtaposées. Cette seconde représentation provient soit de traitements élaborés accomplis sur le premier type de données, soit de données purement synthétiques. Pour l'un comme pour l'autre de ces types de représentation, un besoin commun d'affichage rapide s'est vite fait sentir. Ce besoin a trouvé une solution aujourd'hui universellement adoptée par les cartes graphiques à base de remplissage de triangles. Pour cette raison, la représentation des surfaces par des triangulations a progessivement acquis une grande popularité que ce soit pour représenter des nuages de points ou des surfaces structurées.

2.2.1 Nuage de points

L'acquisition de données surfaciques est pratiquée dans des domaines aussi variés que la cartographie, la muséologie, le cinéma ou la médecine. On utilise des outils d'acquisition

comme un scanner laser, plusieurs vues stéréoscopiques ou un tomographe à rayons X. Le résultat est une collection de mesures de grandeurs physiques en une multitude de points dont la machine fournit aussi les coordonnées cartésiennes. Lorsque le processus d'acquisition est terminé, l'appareil renvoit donc les coordonnées de N points et le résultat de la mesure physique en ce point (couleur, réflectance, chaleur, etc.) Ces points ne sont pas connectés entre eux. Ils sont l'image d'une certaine géométrie, mais la connexité est encore indéterminée ou implicite si l'acquisition se fait sur un échantillonnage régulier. Il appartiendra à un mailleur de s'acquitter de ce travail.

Nous présentons un exemple de nuage de points (voir Fig. 2.1). Il s'agit de mesures aériennes en vue de cartographier le milieu péri-urbain. Le dispositif d'acquisition est constitué d'un avion balayant aussi régulièrement que possible le sol à l'aide d'un laser. En mesurant le temps que met le rayon pour revenir après réflection sur le sol, on assigne une altitude à la mesure. Ici, l'application vise à cartographier en 3D la ville de Bruxelles afin d'en construire un modèle numérique.

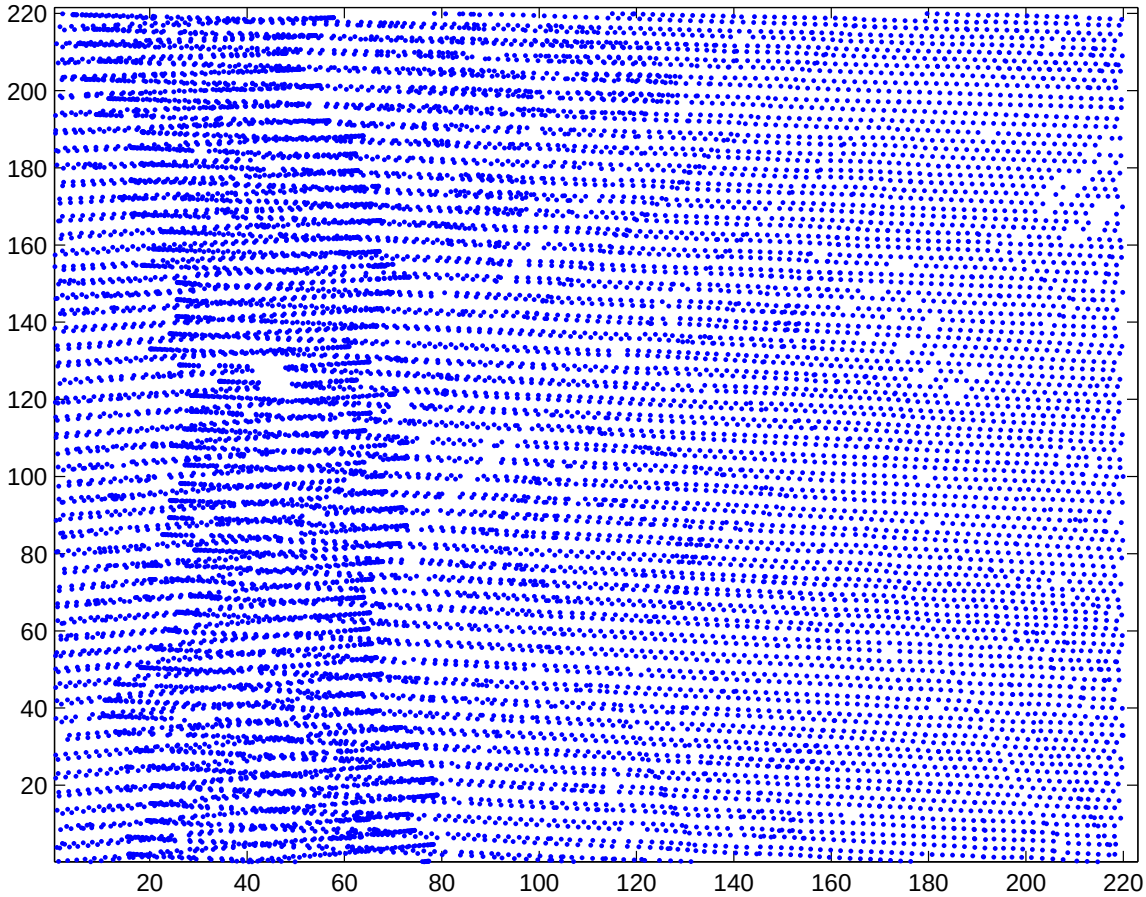

Fig. 2.1 – Surface d'une ville vue du ciel. En chaque point on connaît l'altitude du sol ou du bâtiment. La bande verticale sur la gauche contenant beaucoup plus de points qu'ailleurs correspond à un recouvrement du balayage aérien. Données : Copyright ©EuroSense.

Dans les représentations par nuages de points, la géométrie est fixée par le mode de

balayage. Pour un certain nombre d'objets tout d'abord, cette géométrie est très irrégulière. C'est le cas de surfaces résultant de la détection de points par traitement d'un volume de données (détection de discontinuités par exemple) ou d'appariement stéréographique. Dans de nombreux cas, les données sont plus structurées car elles résultent de mesures prises selon un échantillonnage régulier, ce qui leur confère des propriétés d'ordre dans l'espace. Malheureusement, l'échantillonnage est régulier dans un repère lié au capteur et non à l'objet, et lorsqu'on se place dans un référentiel lié à l'objet l'ordonnancement des points est remis en cause et par suite la notion de surface s'appuyant sur ces points. Un grand nombre de travaux de ces récentes années a été consacré à retrouver une continuité de la surface de l'objet à partir de ces mesures éparses.

2.2.2 Non-Uniform Rational B-Splines (NURBS)

Dans l'industrie mécanique, on produit deux sortes de surfaces : les surfaces fonctionnelles, qui permettent au produit de remplir sa fonction, et les surfaces libres, souvent pour des raisons esthétiques. C'est la raison pour laquelle on utilise en CAO des surfaces paramétrées dont on peut garantir qu'elles respectent les contraintes fortes liées aux surfaces fonctionnelles, et qu'elles disposent néanmoins de toute la souplesse nécessaire à la création de surfaces libres. Ces surfaces sont généralement paramétrées par un système de points de contrôle et de pondération.

La construction de surfaces par NURBS utilise des B-Splines monodimensionnelles. Nous rappelons comment les calculer récursivement. Soit $U = \{t_0, t_1, ..., t_m\}$ un ensemble ordonné de valeurs non décroissantes (i.e : $t_i \leq t_{i+1}$), et $N_{i,k}$ une famille de B-Splines normalisées. L'initialisation de la récurrence se formule par :

$$N_{i,0}(u) = \begin{cases} 1 & si \quad t_i \leq u < t_{i+1} \\ 0 & sinon. \end{cases} \tag{2.1}$$

La récurrence suivante permet de calculer des B-Splines de degré quelconque :

$$N_{i,k}(u) = \frac{u - t_i}{t_{i+k} - t_i} \times N_{i,k-1}(u) + \frac{t_{i+k+1} - u}{t_{i+k+1} - t_{i+1}} \times N_{i+1,k-1}(u). \tag{2.2}$$

Enfin, on demande à un vecteur w de poids et un ensemble P de points de contrôle de paramétrer la combinaison de B-Splines monodimensionnelles d'ordres k et l pour obtenir une surface. La surface NURBS obtenue est donnée par :

$$S_{NURBS}(u, v) = \sum_{i=0}^{n} \sum_{j=0}^{m} P_{i,j} \times R_{i,k,j,l}(u, v), \tag{2.3}$$

où :

$$R_{i,k,j,l}(u, v) = \frac{w_{i,j} \times N_{i,k}(u) \times N_{j,l}(v)}{\sum_{r=0}^{n} \sum_{s=0}^{m} w_{r,s} \times N_{r,k}(u) \times N_{s,l}(u)}. \tag{2.4}$$

Ainsi, créer une surface respectant des surfaces fonctionnelles devient un problème de positionnement de points de contrôles et la mise au point d'un système de poids. En outre, les surfaces produites ont de bonnes propriétés de dérivabilité. De plus, l'expression paramétrique de la surface permet un échantillonnage rapide en vue de l'affichage.

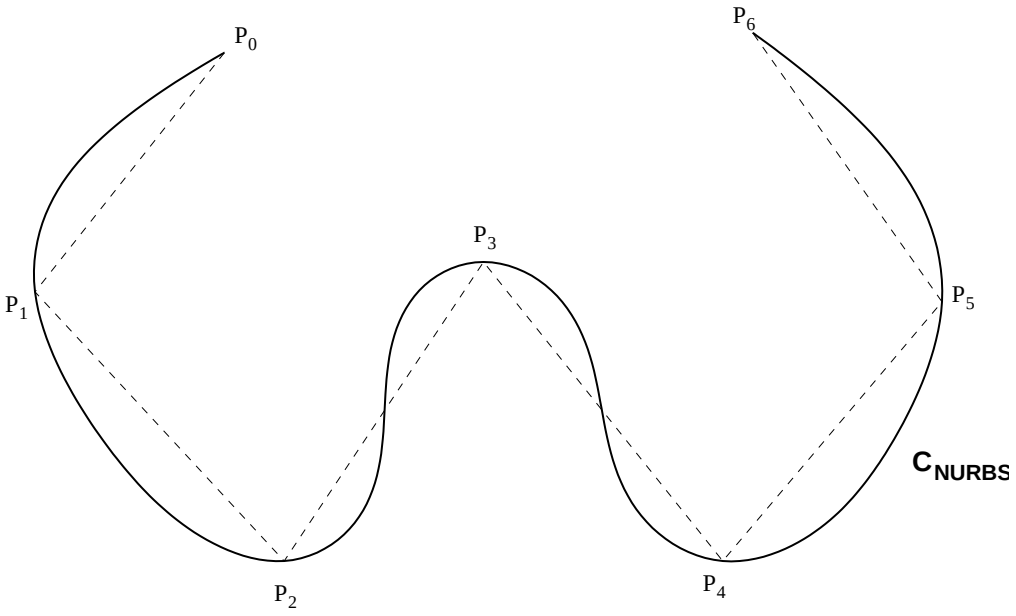

FIG. 2.2 – Exemple de courbe obtenue par combinaison de splines monodimensionnelles (les points de contrôle appartiennent à la courbe dans cet exemple de splines d'interpolation, mais nous aurions pu choisir des splines d'approximation qui ne passent pas par les points de contrôle).

2.2.3 Maillages surfaciques

Les cartes graphiques 3D ont été conçues pour accélérer l'affichage des triangles. On sait déjà échantillonner (au moins dans l'espace paramétrique) les surfaces issues de NURBS pour en faire un nuage de points, et nous montrerons dans la partie suivante comment relier entre eux les points d'un nuage. Pour ces raisons, décrire en machine une surface par un maillage s'est rapidement imposé comme une étape intermédiaire. Cela est encore plus vrai dès lors que les cartes graphiques modernes proposent un pipe-line câblé et programmable par l'utilisateur pour créer des effets personnalisés en un point ou sur une facette. En outre, à l'heure de la grande mise en réseau, les maillages présentent l'intéressant avantage de pouvoir se transmettre de manière hiérarchique. Un maillage surfacique est donc constitué d'un nuage de points et d'un ensemble d'arêtes les reliant entre eux. On ne se donne pas d'hypothèse sur la nature des facettes. Toutefois, tout polygone pouvant être triangulé, on choisit au début de câbler uniquement l'accélération de l'affichage des triangles. Dans la suite, nous commettrons l'abus de confondre maillage surfacique et surface triangulée.

2.3 Surfaces triangulées

Une surface triangulée constituée de N sommets peut être vue comme un signal $\mathcal{S} = \{\mathcal{V}, \mathcal{E}\}$ avec $\mathcal{V} = \{p_i\}$ (avec $p_i \in \mathbb{R}^3$ $\forall i \in \{1, ..., N\}$), $\mathcal{E} \subset \mathcal{V}^2$ et $|\mathcal{V}| = N$ ($|\mathcal{V}|$ représente le cardinal de $\mathcal{V}$). L'ensemble $\mathcal{V}$ code les coordonnées des points du maillage, et représente sa *géométrie*. L'ensemble $\mathcal{E}$ est constitué de toutes les paires de points codant les arêtes de

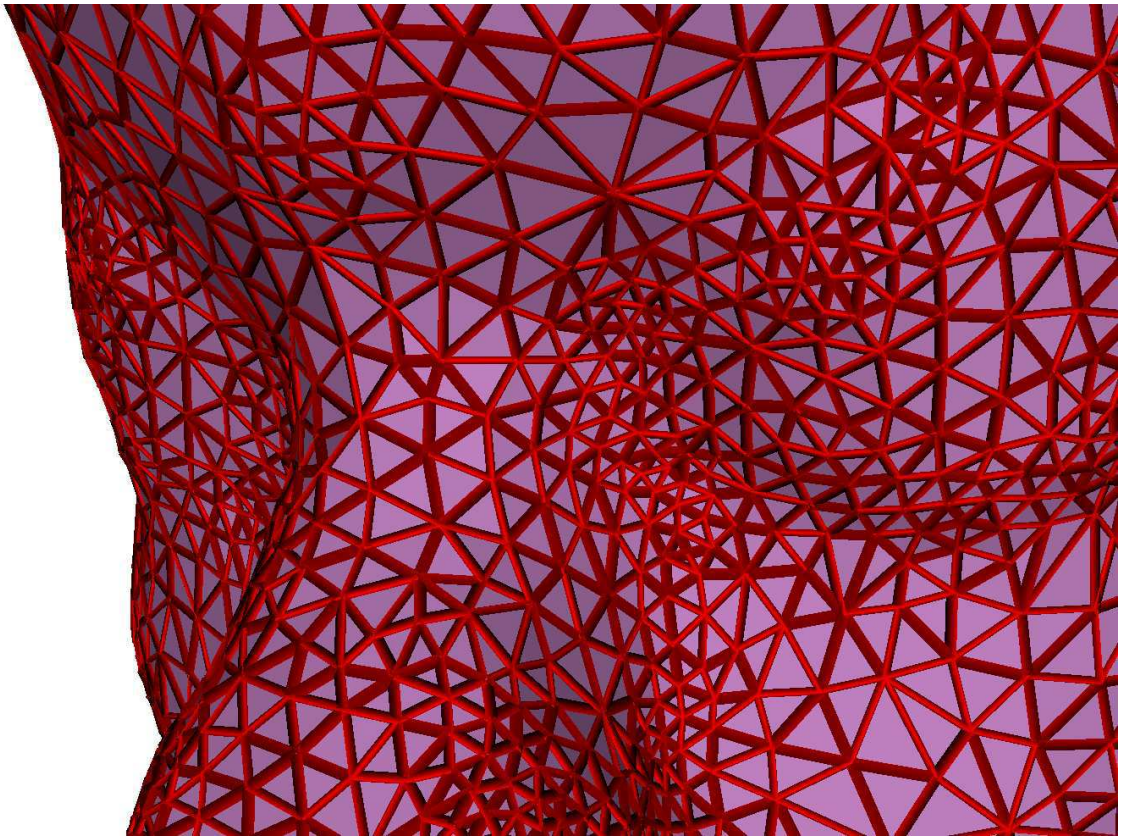

FIG. 2.3 – Zoom sur un maillage muséologique. Données : Télécom Paris.

l'objet et représente la *connexité* de l'objet, et on appelle a le nombre d'arêtes du maillage. On dit que la géométrie $\mathcal{V}$ est définie sur la connexité $\mathcal{E}$ de l'objet 3D. La connexité établit des relations entre les points : on pourra aussi considérer le *graphe* de la connexité se déduisant de $\mathcal{E}$ par recherche de cycles. De ce graphe découlent les facettes du maillage, dont le nombre est noté f. Pour nous, toutes les facettes seront des triangles. Nous illustrons notre propos sur la Fig. 2.4, où nous mettons en perspective une grille d'échantillonnage régulière avec une grille irrégulière. Pour la suite, il est utile de définir le voisinage $p^\star$ d'un point $p \in \mathcal{V}$:

$$\forall p' \in \mathcal{V} \ , \ p' \in p^\star \iff \{p, p'\} \in \mathcal{E}. \tag{2.5}$$

Par convention, on choisit de ne pas inclure un point dans son voisinage : $p \notin p^\star$. On appelle *degré* d_p, ou encore *valence*, d'un point p le cardinal de son voisinage : $d_p = |p^\star|$. C'est le nombre d'arêtes incidentes en p.

2.3.1 Propriétés topologiques

De cette information de connexité découle la topologie du maillage considéré. À une surface triangulée, on associe généralement sa caractéristique d'Euler-Poincaré, notée $\chi(\mathcal{S})$:

$$\chi(\mathcal{S}) = N - a + f. \tag{2.6}$$

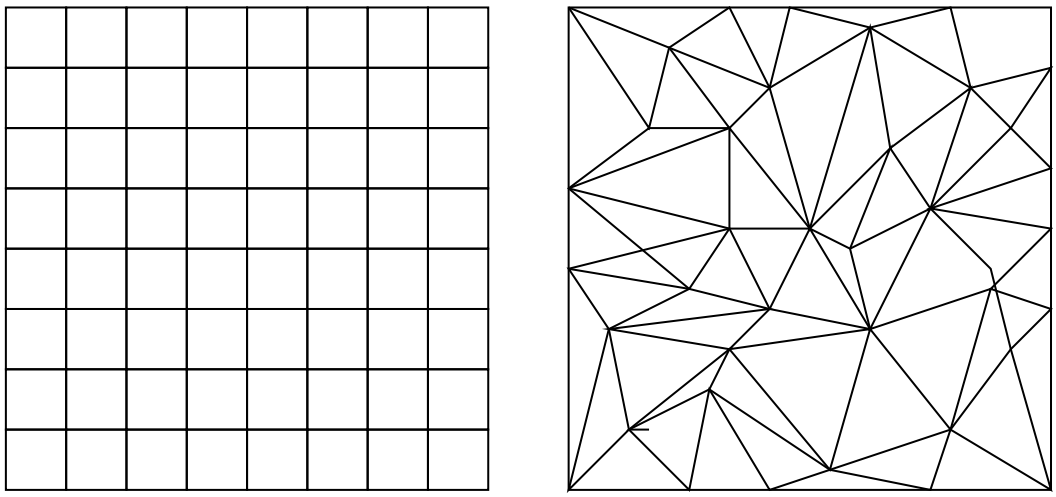

FIG. 2.4 – Deux grilles d'échantillonnage. Gauche : régulière. Droite : irrégulière. Dans le premier cas, chaque point d'échantillonnage a le même nombre de voisins, situés à égale distance les uns des autres. Dans le second cas, il faut à chaque fois déterminer dynamiquement le voisinage d'un sommet.

La relation d'Euler relie la caractéristique d'Euler-Poincaré aux caractéristiques topologiques de la surface :

$$\chi(\mathcal{S}) = N - a + f = 2(c - g) - b. \tag{2.7}$$

où g est le genre de la surface, c le nombre de composantes connexes, et b le nombre de bords.

Une surface triangulée est dite une *variété* si toutes ses arêtes sont incidentes à deux facettes exactement, et si tout sommet possède un voisinage homéomorphe à un disque. Une surface triangulée est dite variété avec bords s'il s'agit d'une variété partout sauf pour un ou plusieurs cycles disjoints d'arêtes incidentes à une seule face chacune. Ces arêtes sont appelées arêtes de bord, et leurs points extrémaux ont un voisinage homéomorphe à un demi-disque.

2.3.2 Triangulation de Delaunay

Soit $\mathcal{V}$ un ensemble de sites du plan. On appelle simplexe de Delaunay tout simplexe de dimension n $p_0, ..., p_n$ ($p_i \in \mathcal{V}$) tel qu'il existe une boule passant par $p_0, ..., p_n$ ne contenant pas de point de $\mathcal{V}$ en son intérieur. On appelle triangulation de Delaunay le complexe composé des simplexes de Delaunay de $\mathcal{V}$. Si nous appelons T une telle triangulation, nous pouvons calculer sa granularité : à chaque triangle t de T on associe le rayon r_t du plus petit cercle contenant t, et on appelle grain de T la grandeur :

$$G(T) = \max_{t \in T} r_t. \tag{2.8}$$

On sait en outre (voir [11] pour les détails) que parmi toutes les triangulations T d'un ensemble de points P du plan, les triangulations de Delaunay de P sont celles qui ont le grain le plus fin.

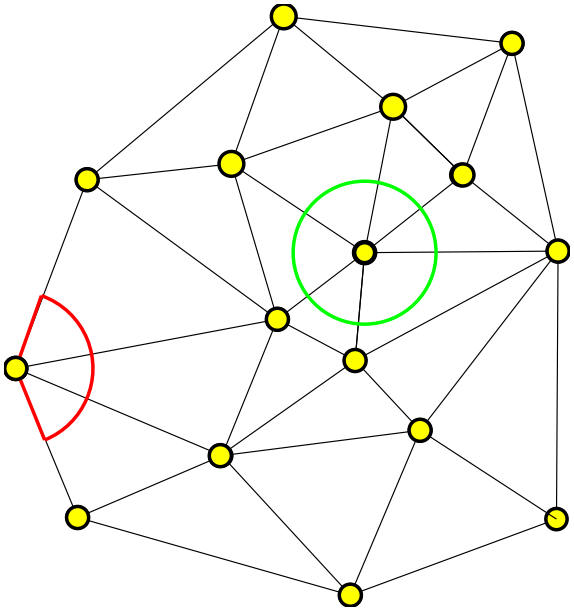

FIG. 2.5 – Variété avec bords : un sommet à l'intérieur du maillage à un voisinage homéomorphe à un disque (vert), au conraire d'un point appartenant à un bord (rouge).

On peut également souhaiter définir la finesse d'une triangulation. Soit T une triangulation d'un ensemble $\mathcal{V}$ de n points du plan. On définit la finesse de T comme étant le vecteur $Q(T) = (\alpha_1, ..., \alpha_{f'})$, où les α_i sont les angles des f triangles de T classés par ordre lexicographique. Ces angles sont bien sûr en nombre $f' = 3 \times f$. La finesse sert également à caractériser les triangulations de Delaunay, car la triangulation qui maximise la finesse selon l'ordre croissant est une triangulation de Delaunay.

Il existe également une version tridimensionnelle volumique de la triangulation de Delaunay, appelée tétraédrisation de Delaunay. Toutefois, pour les maillages surfaciques tridimensionnels, on essaiera souvent de rester dans une représentation bidimensionnelle. Pour cela, on procèdera si possible à une paramétrisation du maillage si celui-ci contient au moins un bord. La triangulation de Delaunay peut ainsi avoir lieu dans l'espace paramétrique, pour ensuite calquer la triangulation obtenue dans le plongement 3D.

2.3.3 L'algorithme *Marching Cubes*

Une méthode pour générer une première triangulation à partir d'un nuage de points totalement non structurée est l'algorithme *Marching Cubes* [51]. La boîte englobante du nuage est divisée en voxels (des cubes), de plus en plus petits au fur et à mesure de la précision demandée.

Si l'on dispose d'une fonction capable de dire si tel point est à l'intérieur ou à l'extérieur de la surface fermée, l'algorithme regarde chaque sommet des voxels et détermine s'il est à l'intérieur ou à l'extérieur de la surface fermée. En pratique, cela se fait par un inventaire des configurations possibles. Pour un voxel, cela fait $2^8 = 256$ combinaisons possibles. Toutefois, en tenant compte de configurations équivalentes qui se déduisent l'une de l'autre, on descend

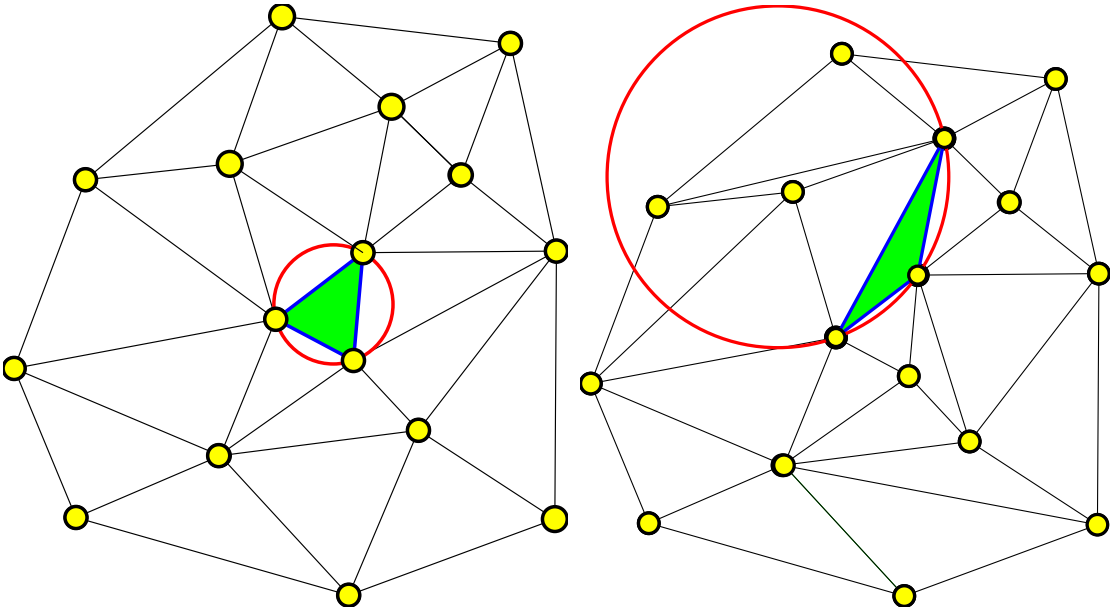

FIG. 2.6 – Le même ensemble de points maillés avec une triangulation de Delaunay (à gauche), et avec une triangulation quelconque (à droite). Le simplexe vert de gauche est un simplexe de Delaunay, pas celui de droite (la boule passant par les sites est représentée en rouge), elle contient d'autres sommets que ceux du simplexe inscrit.

à 15 configurations canoniques. Ces doublons se déduisent en :

- opérant une rotation autour d'un des trois axes principaux du voxel ;
- opérant une symétrie de la surface par rapport à l'un des trois axes principaux ;
- inversant l'état des sommets du voxel et le sens des normales aux triangles.

Ainsi, en fonction de la configuration canonique à laquelle se ramène le voxel considéré, on déduit la triangulation correspondante. En réduisant de plus en plus la taille des voxels, on obtient un maillage qui s'approche de plus en plus de la surface. L'algorithme fournit en outre une manière de se déplacer de voxels en voxel qui permet de suivre la surface.

Un inconvénient de cet algorithme est qu'il a tendance à produire rapidement une masse très volumineuse de données. Toutefois, il est utilisé pour extraire une première connexité d'un nuage de points denses. On peut ensuite s'adonner à la gamme des pré-traitements : lissage, filtrage topologique, remaillage, simplification, etc. L'acquisition de données 3D n'est pas un processus simple, et la création d'un maillage correct l'est sans doute encore moins.

2.4 Paramétrisation des surfaces triangulées

Une surface peut être vue comme une variété riemannienne (i.e : munie d'une métrique) bidimensionnelle plongée dans l'espace euclidien tridimensionnel. On souhaite généralement travailler dans un espace de même dimension que la variété. C'est pourquoi on a développé des techniques dites de paramétrisation, destinées à décrire la surface par un jeu de deux paramètres. La paramétrisation est au centre de beaucoup de problèmes en informatique

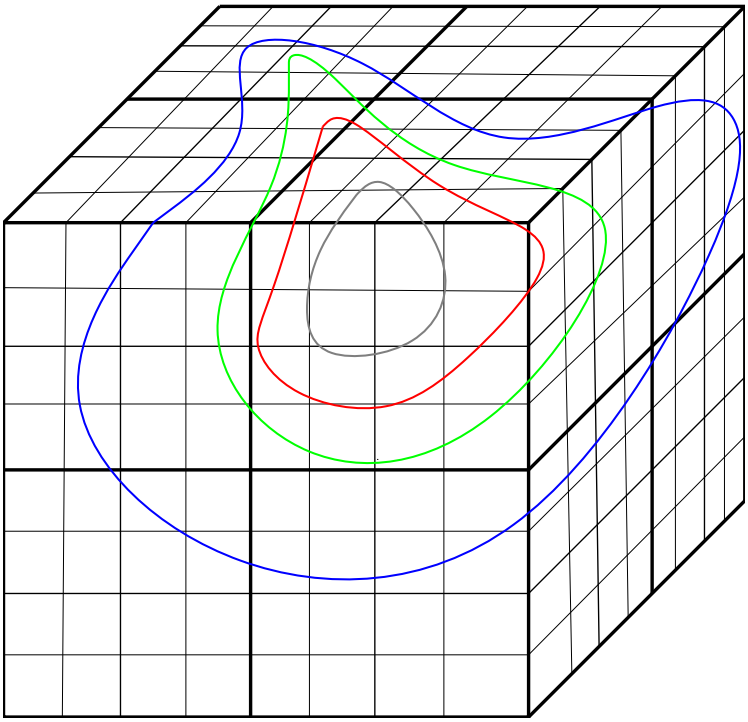

FIG. 2.7 – Découpage de la boîte englobante en voxels de plus en plus fins dans l'algorithme *Marching Cubes*.

graphique : plaquage de texture, remaillage, simulation, etc. Effectuer une paramétrisation dépend de la topologie de la surface. Nous décrivons ci-dessous diverses paramétrisations avec leurs propriétés. Nous nous concentrons sur les paramétrisations des surfaces 3D triangulées.

2.4.1 Définition

Une paramétrisation P d'une variété triangulée avec bords S est une triangulation dans le plan paramétrique (u, v) isomorphe au graphe de connexité de S. Chaque sommet 3D $p_i \in \mathcal{V}$ se voit associer son image 2D P_i par paramétrisation :

$$P(u, v) = \begin{pmatrix} x_S(u, v) \\ y_S(u, v) \\ z_S(u, v) \end{pmatrix}. \tag{2.9}$$

On peut donc regarder un maillage de différentes manières : suivant son graphe de connexité, sa représentation 3D, ou encore sa paramétrisation. La première information permet les calculs topologiques, la seconde associe la géométrie, et la troisième permet d'effectuer dans le plan 2D des calculs de distance en rapport avec la métrique du maillage 3D. Les paramétrisations que nous discutons ici sont moins générales que celles de [67] (qui ne sont pas limitées par la topologie), mais ce sont celles qui demeurent les plus employées du fait de

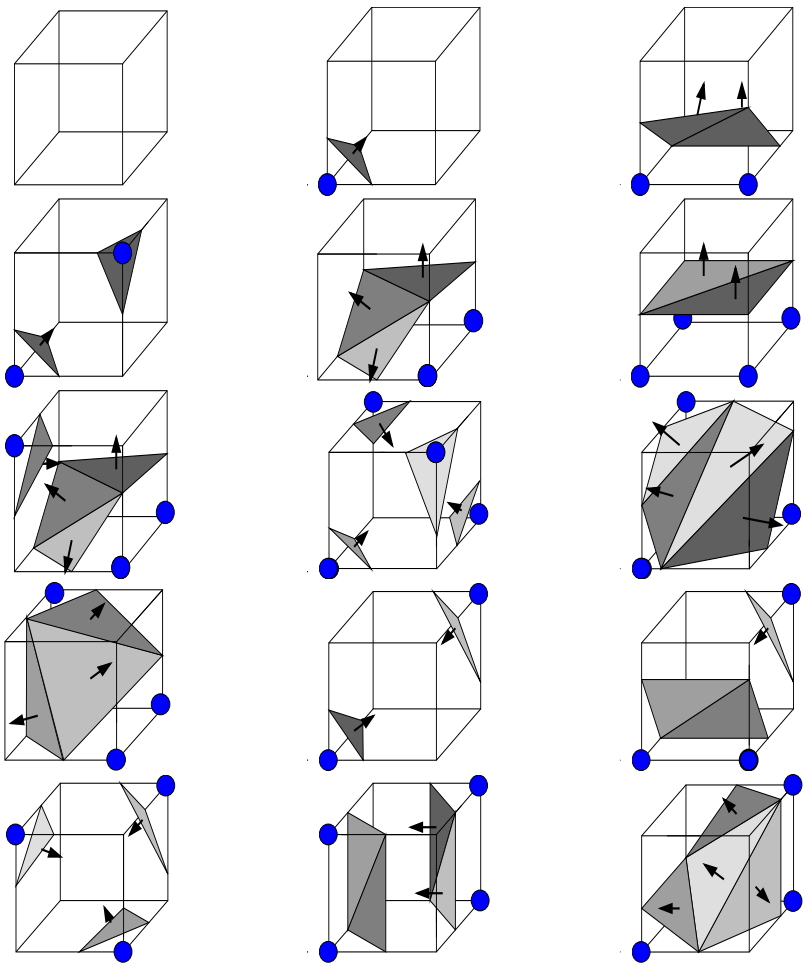

FIG. 2.8 – Les 15 configurations canoniques de l'algorithme *Marching Cubes*. Les sommets des voxels à l'intérieur de la surface sont figurés par des sphères bleues (lorsqu'elles sont visibles). Les normales aux triangles sont figurées lorsqu'elles sont visibles.

leur relative facilité d'implantation. Pour nous, une paramétrisation P est donc une triangulation planaire isomorphe au graphe de connexité $\mathcal{E}$ du maillage $\mathcal{S}$. Comme nous nous intéressons aux variétés avec bord, il faut encore savoir comment sont fixés les bords dans la paramétrisation. Deux cas sont possibles : soit on fixe arbitrairement les sommets du bord sur le périmètre d'un convexe du plan, soit au contraire on laisse les bords libres (deux points seulement du bord sont fixés). Nous donnons ici une description des deux principaux types de paramétrisation, ainsi que deux exemples.

Nous précisons ici que nous aurons besoin au chapitre 6 d'utiliser une paramétrisation définie sur une variété avec bord. Toutes celles que nous présentons ici ne pourront pas nous être utiles. En effet, le chapitre 6 envisage la transmission progressive de la géométrie tatouée. Nous verrons que l'encodeur et le décodeur ont besoin de se synchroniser sur la même paramétrisation, dépendante du maillage, avant toute opération d'encodage ou de décodage de la géométrie. Du seul point de vue du décodeur, on ne peut donc pas se servir

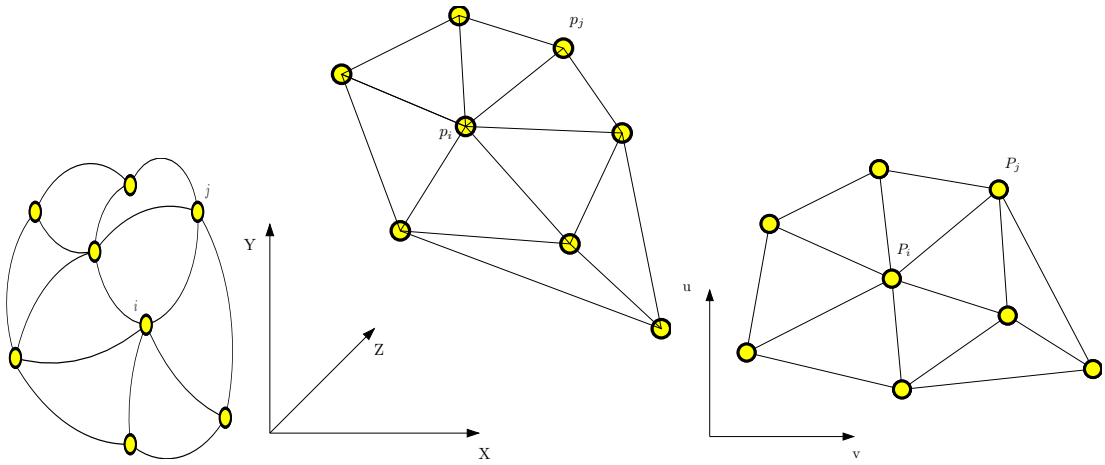

FIG. 2.9 – Trois manières de regarder un maillage d'une variété avec bords : son graphe de connexité, sa représentation spatiale, sa paramétrisation.

de l'information géométrique pour établir la paramétrisation. Cette remarque prendra tout son sens par la suite. Nous précisons à chacune des paramétrisations que nous présentons si elle pourra nous être utile (i.e : fait-elle appel ou non à l'information géométrique du maillage).

2.4.2 Paramétrisation harmonique

Lorsque l'on effectue une paramétrisation, il se produit immanquablement une distorsion des longueurs relatives des arêtes (ce problème est discuté dans [13]). La paramétrisation qui minimise cette distorsion est qualifiée d'harmonique [22, 23]. Une fois le bord fixé, la paramétrisation harmonique existe et est unique et continue. Malheureusement, trouver exactement la paramétrisation harmonique nécessite de résoudre un système d'équations différentielles partielles [23]. Pour des raisons de calcul, on cherche plutôt à en calculer une approximation [21]. Soit P_h une telle approximation de paramétrisation harmonique. Nous obtiendrons P_h en assimilant chaque arête à un ressort dont nous donnons la constante de raideur, et en minimisant itérativement l'énergie de ce système de ressorts (au début du processus, les points sont jetés au hasard sur l'espace paramétrique, sauf les points du bord qui sont fixés une fois pour toute). Soit E_{harm} l'énergie d'un tel système de ressorts associé à la paramétrisation P. Cette énergie est à minimiser dans l'espace paramétrique en fonction de mesures prises sur le maillage [21] :

$$E_{harm}(P) = \frac{1}{2} \sum_{\{i,j\} \in \mathcal{E}} \kappa_{i,j} \|P_i - P_j\|^2, \tag{2.10}$$

où $\kappa_{i,j}$ sont les constantes de raideur des ressorts. En appelant $L_{i,j}$ la longueur de l'arête $\{i, j\}$ sur le maillage et $A(i, j, k)$ l'aire de la facette $\{i, j, k\}$ sur le maillage, les constantes de raideur sont calculées comme suit pour une arête $\{i, j\}$ commune aux facettes $\{i, j, k_1\}$ et $\{i, j, k_2\}$ (si l'expression suivante concerne une arête appartenant au bord, elle ne contient

qu'un seul terme) :

$$\kappa_{i,j} = \frac{L_{i,k_1}^2 + L_{j,k_1}^2 + L_{i,j}^2}{A(i,j,k_1)} + \frac{L_{i,k_2}^2 + L_{j,k_2}^2 + L_{i,j}^2}{A(i,j,k_2)}. \tag{2.11}$$

Par définition :

$$P_h = \arg\min_P E_{harm}(P). \tag{2.12}$$

Cette paramétrisation ne pourra manifestement pas nous être utile par la suite car les poids $\kappa_{i,j}$ sont fonction de mesures géométriques prises sur le maillage.

2.4.3 Paramétrisation barycentrique de Tutte

La première tentative pour proposer une paramétrisation vient de Tutte [75], qui place chaque point de la paramétrisation au barycentre (paramétrique) de ses voisins. Soit P_i le point de l'espace paramétrique correspondant au point p_i du maillage 3D. Nous cherchons une paramétrisation telle que :

$$P_i = \sum_{P_j \in P_i^\star} w_{ij} P_j, \tag{2.13}$$

avec w_{ij} constant pour $p_j \in p_i^\star$ et :

$$\sum_j w_{ij} = 1. \tag{2.14}$$

La paramétrisation de Tutte propose donc de placer P_i comme suit :

$$w_{ij} = \frac{1}{d_{P_i}} \quad \forall j \in P_i^\star, \tag{2.15}$$

où d_{P_i} représente la valence de P_i. On remarque au passage que l'on se sert bien des propriétés de voisinage du graphe de connexité, sans les modifier (nous ne faisons que lire des valences), garantissant ainsi l'isomorphie. Nous illustrons cette paramétrisation dans la Fig. 2.10. Cette paramétrisation présente la propriété de minimiser la somme des longueurs des arêtes au carré dans l'espace paramétrique [75]. La paramétrisation barycentrique de Tutte est donc une paramétrisation harmonique avec $\kappa_{i,j} = 1$. On l'obtient de manière itérative en appliquant la transformation Eq. 2.13 jusqu'à convergence.

En outre, comme nous l'avons vu, strictement aucune grandeur géométrique n'entre en compte dans le calcul de cette paramétrisation. Nous pourrons donc l'utiliser par la suite en vue de synchroniser l'encodeur et le décodeur uniquement à l'aide d'information de connexité, sans information géométrique.

2.4.4 Paramétrisation conforme

Une paramétrisation conforme tend quant à elle à préserver localement les angles. Elle s'obtient par minimisation de l'énergie de Dirichlet. On note P_c une telle paramétrisation conforme. Dans [61], on définit l'énergie de Dirichlet d'une triangulation *orientée* par :

$$E_D(P) = \sum_{i=1}^{N} \sum_{j \in i^\star} \cot \alpha_{i,j} \|P_i - P_j\|^2. \tag{2.16}$$

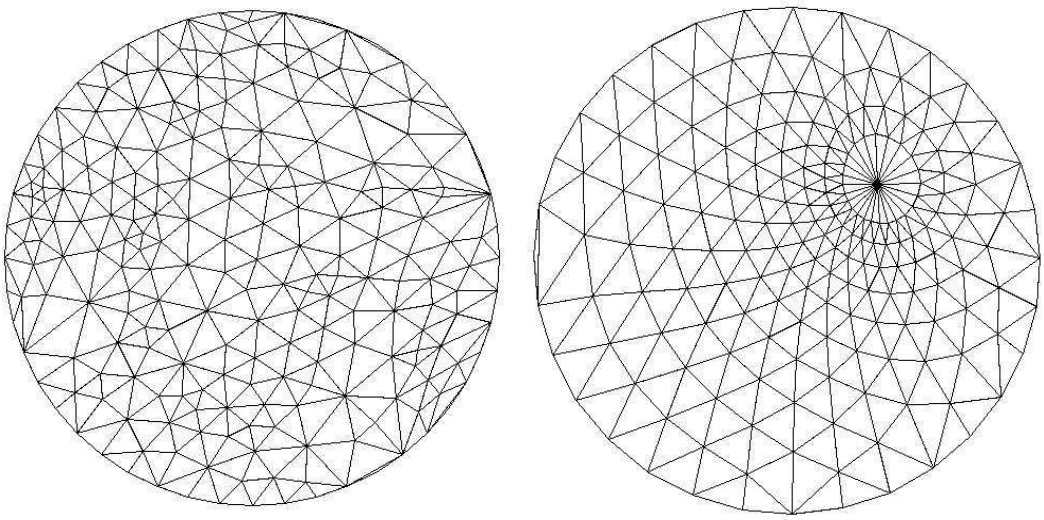

FIG. 2.10 – Exemples de paramétrisation barycentrique de Tutte : tous les points de l'espace paramétrique sont au barycentre de leurs voisins. Le bord est fixé : tous ses points ont été équirépartis sur le cercle unité. A droite, on a paramétrisé une calotte d'une sphère régulièrement échantillonnée (on reconnaît le pôle de forte valence en haut à droite.)

La paramétrisation P_c est donnée par :

$$P_c = \arg\min_P E_D(P). \tag{2.17}$$

Dans l'expression de l'énergie de Dirichlet, l'angle $\alpha_{i,j}$ est pris à gauche sur le maillage (voir Fig. 2.11).

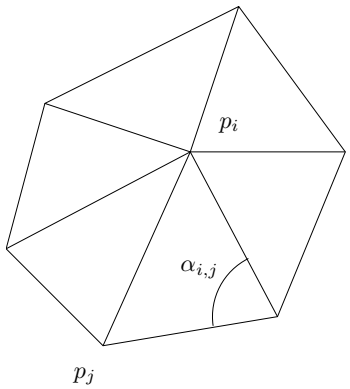

FIG. 2.11 – Définition de l'angle $\alpha_{i,j}$ pour une paramétrisation conforme.

Là encore, nous ne pourrons pas utiliser cette paramétrisation dans la suite. Le problème porte ici sur l'angle $\alpha_{i,j}$ qui ne serait pas encore connu au décodeur.

2.4.5 Paramétrisation de Floater

Floater [28] a proposé une autre manière de trouver les poids w de la paramétrisation de Tutte, qui place également un point P à l'intérieur d'un polygone convexe composé de ses voisins. Pour chaque point P de la paramétrisation, on trace la ligne qui le relie à un de ses voisins P_l. Cette ligne rencontre le polygone formant le voisinage de P en intersectant l'arête $P_{r(l)}P_{r(l)+1}$ (voir Fig. 2.12).

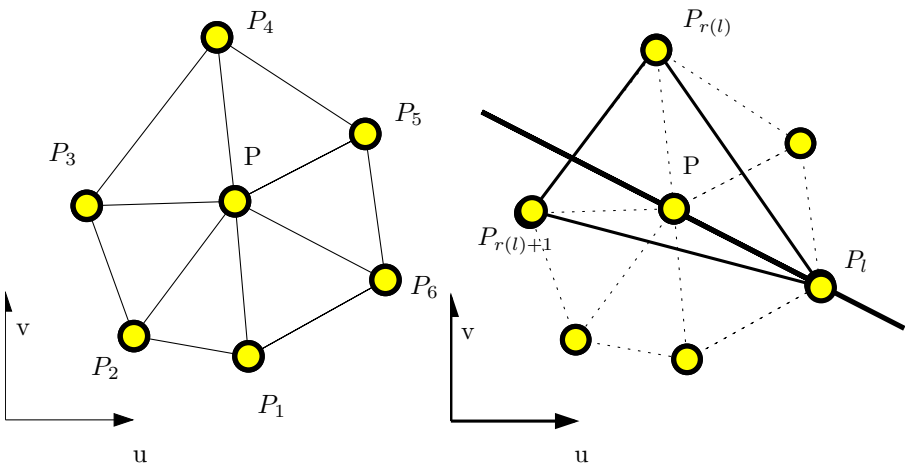

FIG. 2.12 – Paramétrisation de Floater : recherche du polygone convexe $P_l P_{r(l)} P_{r(l)+1}$.

On peut alors trouver un triplet $\{\delta_1, \delta_2, \delta_3\}$ tel que :

$$\begin{cases} P = \delta_1 P_l + \delta_2 P_{r(l)} + \delta_3 P_{r(l)+1}, \\ \delta_1 + \delta_2 + \delta_3 = 1. \end{cases} \tag{2.18}$$

On définit alors les grandeurs $\mu_{k,l}$ par :

$$\mu_{k,l} = \begin{cases} \mu_{l,l} = \delta_1, \\ \mu_{r(l),l} = \delta_2, \\ \mu_{r(l)+1,l} = \delta_3, \\ \mu_{k,l} = 0 \;\; sinon. \end{cases} \tag{2.19}$$

Finalement, les poids de la paramétrisation sont définis par :

$$w_{ij} = \frac{1}{d_{P_i}} \sum_{P_l \in P_i^\star} \mu_{j,l}. \tag{2.20}$$

On vérifie bien que $\sum_j w_{i,j} = 1$. Cette paramétrisation a été appelée *shape-preserving* car elle tend à conserver localement les angles.

Nous aurions pu utiliser cette paramétrisation, mais nous avons souhaité garder le maximum de points communs avec les méthodes auxquelles nous souhaitons nous comparer. Nous utiliserons en réalité une paramétrisation barycentrique de Tutte, que nous n'avons pas cherché à améliorer.

2.4.6 Découpe en disque topologique

Les paramétrisations que nous venons de présenter requièrent une variété avec bord pour être valides (homéomorphes à un disque). Ce n'est en pratique pas souvent le cas des surfaces rencontrées, qui peuvent être de genre quelconque. Toutefois, il est toujours possible de découper une surface triangulée pour en faire un disque. Sur le bord, on trouvera bien sûr plusieurs fois chaque point. On appelle le bord issu d'une telle découpe le schéma polygonal de la surface.

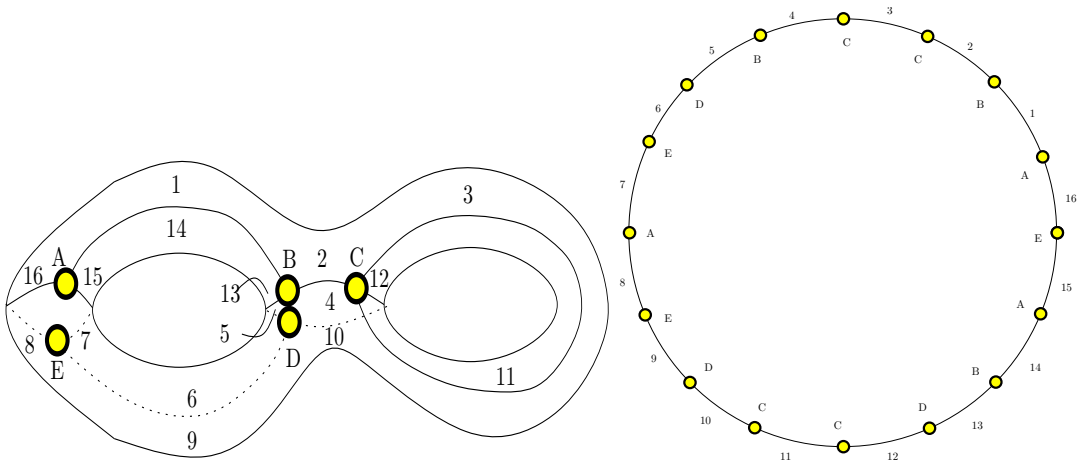

Fig. 2.13 – Découpe d'une surface en disque topologique. A droite : une surface de genre 2 (double tore). A gauche : son schéma polygonal.

Trouver le schéma polygonal d'une surface triangulée n'est pas trivial. Une surface de genre g nécessite de trouver $2g$ cycles d'arêtes dans le graphe de connexité partageant deux à deux un même point (AEA, BCDC, ABDEA, CC dans notre exemple). Ainsi, en coupant suivant les arêtes formant les cycles, on obtient un disque topologique. Fondés sur une simplification des idées présentées dans [77], F. Lazarus [48] a présenté deux algorithmes produisant un tel schéma polygonal. Une méthode permettant de minimiser la somme des longueurs des arêtes des cycles est présentée dans [24]. Lors de calculs opérés sur un tel découpage de la surface, il faut veiller à ce que les effets de bords ne viennent pas trop perturber la reconstruction de la surface lorsque l'on repasse dans le plongement 3D.

2.5 Structures de données associées

Nous expliquons à présent de quelle manière peuvent être décrits les maillages en machine. Il s'agit essentiellement de disposer d'un codage de la connexité de manière à accéder rapidement aux points formant telle facette ou au voisinage d'un point par exemple. Nous présentons le codage naïf de la connexité, qui n'est autre que la transcription en machine du codage brut dans un format VRML par exemple. Enfin nous présentons la structure half-edge qui, en dépit du surcoût de codage qu'elle introduit, permet un accès beaucoup plus rapide aux informations pertinentes de connexité.

2.5.1 Représentation brute

Le codage brut de la connexité repose sur le stockage en mémoire d'un tableau de description des facettes. Chaque cellule du tableau comporte un nombre d'éléments dépendant du nombre de points formant la facette dans le cas général, mais constant et égal à trois dans le cas de surfaces triangulées. Une telle cellule débute avec le nombre de points dans la facette, et énumère ensuite la liste des points concernés. Ce codage brut est très compact mais ne

T_1	$p^1_{T_1}$	$p^2_{T_1}$	$p^3_{T_1}$
T_2	$p^1_{T_2}$	...	...
...	...	...	$p^3_{T_{f-1}}$
T_f	$p^1_{T_f}$	$p^2_{T_f}$	$p^3_{T_f}$

Fig. 2.14 – Codage brut de la connexité d'un maillage triangulé de f facettes en machine. Chaque cellule correspond à une facette et est constituée du nombre de points qui la constituent, et de la liste de ses points.

permet pas d'effectuer rapidement des opérations de recherche complexe sur la connexité. Par exemple, retrouver le voisinage d'un point avec cette structure nous condamne à parcourir le tableau dans son ensemble. La complexité est donc en $O(f)$ si le maillage contient f facettes. Le principal défaut de cette structure de données est donc de ne pas disposer d'information d'adjacence sur les facettes.

Cette représentation est celle utilisée dans le codage des maillages polygonaux dans le format VRML. Nous donnons ci-dessous un exemple d'un tel codage pour un tétraèdre. On constate au passage, et cette remarque sera capitale en codage de source, que l'information de connexité est très redondante : chaque index de sommet est écrit trois fois.

2.5.2 Représentation en demi-arête

Dans cette représentation, chaque arête est constituée de deux structures de demi-arête : une par orientation possible de l'arête. Une demi-arête est une structure comprenant le point de départ sur l'arête, le point terminal, et la facette à laquelle appartient cette demi-arête (voir Fig. 2.16). Toutes les demi-arêtes d'une même facette sont chaînées entre elles dans le sens horaire (ou anti-horaire). On peut ainsi circuler sur les facettes. La complexité de l'obtention du voisinage d'un point p est donc en $O(d_p)$ pour une 2-variété. Cette structure ne gère malheureusement pas les surfaces non-orientables.

```
VRML V2.0 utf8
Shape {
  geometry IndexedFaceSet {
    coord Coordinate {
      point [
        0.94 0.00 -0.33 ,
       -0.47 0.81 -0.33 ,
       -0.47 -0.81 -0.33 ,
        0.00 0.00 1.00 ,
        ]
     }
    coordIndex [
        2, 1, 0, -1,
        3, 2, 0, -1,
        1, 3, 0, -1,
        2, 3, 1, -1,
        ]
  }
}
```

FIG. 2.15 – Codage d'un tétraèdre dans la norme VRML2.0 : l'information coordIndex codant la connexité est très redondante car chaque index de point est répété trois fois (exemple tiré de [71]).

2.5.3 Représentation *winged-edge*

La structure en demi-arête est limitée aux surfaces orientables, ce qui peut parfois constituer une limitation. Afin de les pallier, la structure *winged-edge* propose que chaque arête pointe non seulement vers ses deux points extrémaux et ses deux facettes incidentes, mais aussi vers les quatre autres arêtes appartenant aux deux facettes incidentes (voir Fig. 2.17). Cette structure de données permet de s'affranchir de la contrainte d'orientabilité de la surface mais au prix de certaines opérations élémentaires plus complexes.

Il existe encore une dernière structure de données, appelée *radial-edge*, qui peut représenter des surfaces de topologie arbitraire. Mais sa complexité impose de seulement la mentionner sans l'aborder plus avant. Le lecteur se reportera à [80] pour une description détaillée.

2.6 Attributs supplémentaires

Jusqu'à présent, nous n'avons modélisé que la géométrie des maillages et leur connexité. Pourtant, un maillage peut faire appel à d'autres données, annexes. Ces attributs peuvent être classés suivant qu'ils se rapportent à des point ou à des facettes.

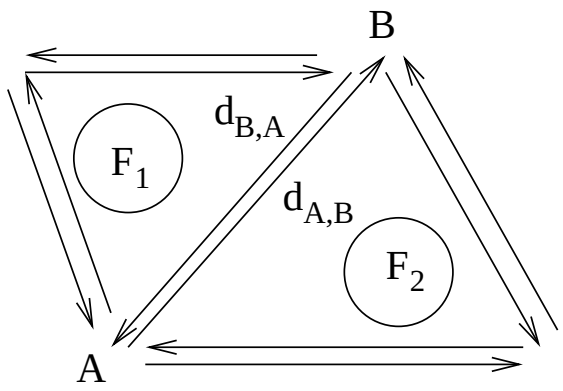

FIG. 2.16 – Structure de données en demi-arête : l'arête AB est constituée des deux demi-arêtes $d_{A,B}$ et $d_{B,A}$ pointant chacune à la fois sur la facette à laquelle elle appartient (F_2 pour $d_{A,B}$ et F_1 pour $d_{B,A}$) , et sur la demi-arête suivante de sa facette (dans le sens horaire sur la figure).

2.6.1 Grandeurs différentielles locales

Afin de modéliser convenablement l'interaction lumière-matière pour l'affichage et le rendu, on a généralement besoin de calculer les normales locales en chaque point, ou en chaque facette. On peut encore avoir besoin d'estimer le flot de courbure de la surface. Il s'agit ici de grandeurs différentielles du premier et du second ordre.

En chaque point, la surface peut être approchée par son plan tangent, de normale $\overrightarrow{n}$. La manière dont se plie la surface en ce point est décrite par la courbure en chaque direction. Pour chaque vecteur $\overrightarrow{e_\theta}$ de direction θ, la courbure normale $\kappa^N(\theta)$ au point considéré est la courbure de la courbe appartenant à la fois à la surface et au plan contenant $\overrightarrow{n}$ et $\overrightarrow{e_\theta}$. Les deux courbures principales κ_1 et κ_2 (de directions principales respectives $\overrightarrow{e_1}$ et $\overrightarrow{e_2}$) sont les valeurs extrémales de $\kappa^N(\theta)$ (voir Fig. 2.18). La courbure moyenne κ_H est définie comme la moyenne des courbures normales :

$$\kappa_H = \int_0^{2\pi} \kappa^N(\theta) d\theta. \tag{2.21}$$

On peut exprimer la coubure normale en n'importe quelle direction en fonction des deux courbures principales :

$$\kappa^N(\theta) = \kappa_2 \sin^2(\theta) + \kappa_1 \cos^2(\theta). \tag{2.22}$$

On en déduit que :

$$\kappa_H = \frac{\kappa_1 + \kappa_2}{2}. \tag{2.23}$$

Pour terminer, on définit la courbure gaussienne comme le produit des deux courbures principales :

$$\kappa_G = \kappa_1 \kappa_2. \tag{2.24}$$

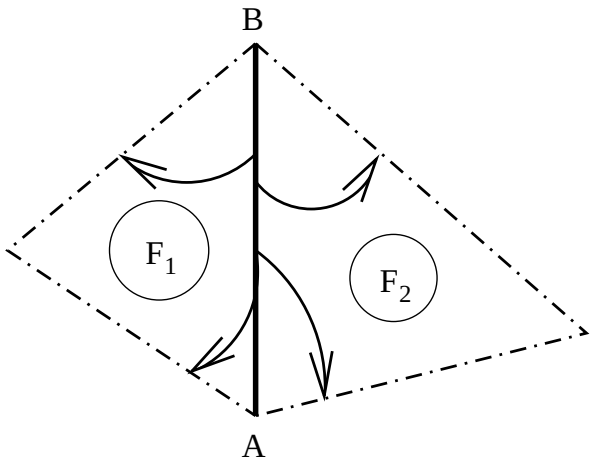

FIG. 2.17 – Structure de données *winged-edge* : l'arête AB pointe sur les points A et B, sur les facettes F_1 et F_2, ainsi que sur les quatre arêtes en pointillés.

2.6.2 Textures

Il arrive généralement qu'un maillage soit la représentation d'un objet réel, disposant d'un aspect propre à la matière qui le compose. Il s'agit ici de données photogrammétriques, que l'on appelle textures. Une texture est codée sous forme d'une image attachée à chacune des facettes de l'objet. Afin de plaquer la texture sur l'objet, on a besoin de paramétriser l'objet afin de calculer ses coordonnées de texture. Une fois l'objet paramétrisé, on vient superposer la texture sur la paramétrisation pour ensuite revenir dans le plongement.

On stocke donc le résultat d'une paramétrisation (qui forme les coordonnées de texture), et la texture elle-même constituée de pixel est souvent stockée sous forme d'un fichier séparé. En effet, ce sont les coordonnées de texture les plus importantes : elles permettent de plaquer n'importe quelle image sur la surface sans nécessiter de coûteux calculs (la paramétrisation ayant été effectuée une fois pour toutes).

2.6.3 Transparence

Dans le domaine biomédical ou de la CAO, où la superposition 3D de plusieurs maillages est nécessaire à la bonne compréhension de leur interaction spatiale, il est souvent utile de pouvoir rendre certaines parties des maillages transparentes. On attache alors aux facettes un facteur de transparence qui sera pris en compte matériellement par le dispositif d'affichage. Il est à noter que l'évolution des matériels d'affichage courants ne tend pas vers la prise en charge de maillages de plus en plus volumineux, mais au contraire vers l'accélération des opérations visant à effectuer les plaquages de texture et le rendu de la transparence, de manière à proposer un rendu plus réaliste à un moindre coût.

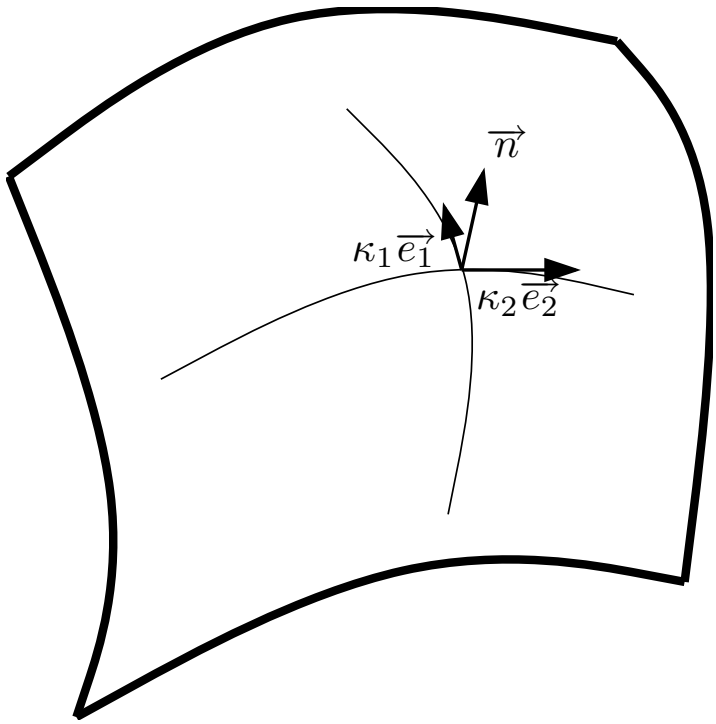

FIG. 2.18 – Propriétés différentielles locales du premier ordre (normale locale) et du second ordre (courbures et directions principales).

2.6.4 Réflectance

Lorsqu'on scanne un objet, on le fait sous certaines conditions particulières de luminosité. Néanmoins, on souhaite pouvoir être capable de modéliser fidèlement le comportement de l'objet dans n'importe quelles conditions d'éclairage. Pour cela, on souhaite accéder aux propriétés locales de réflectance du matériau de l'objet. On cherche alors un modèle de réflectance, qui doit permettre d'associer à chaque élément de surface de l'objet une fonction de transfert entre énergie incidente et réfléchie, pour chaque longueur d'onde du spectre à étudier. On trouve dans [54] un modèle appelé BDRF (pour Bidirectional Reflectance Distribution Function).

Ce modèle est défini en chaque élément de surface comme le rapport de la radiance réfléchie sur l'irradiance incidente. Son unité est l'angle solide inverse :

$$f_r(\theta_i, \rho_i, \theta_r, \rho_r) = \frac{dLr(\theta_r, \rho_r)}{dEi(\theta_i, \rho_i)}, \tag{2.25}$$

où les directions incidente (θ_i, ρ_i) et réfléchie (θ_r, ρ_r) sont exprimées par rapport à la normale à l'élément de surface considéré.

2.7 Modèles de distance entre maillages

Il faut noter par avance qu'il n'existe aucune paramétrisation universelle des surfaces 2D de l'espace 3D (comme par exemple les coordonnées cylindriques pour les objets à description radiale ou les coordonnées sphériques pour les objets à description centrale). Par suite, aucune théorie de traitement linéaire de la géométrie n'a encore vu le jour, comme l'analyse spectrale des fonctions d'une variable. Une des conséquences de cet état de fait est qu'il n'existe pas de rapport signal à bruit entre deux signaux surfaciques 3D. Qu'il s'agisse de compresser la géométrie d'un maillage (codage de source) ou bien de la tatouer, on souhaite disposer d'une mesure permettant d'évaluer la distorsion introduite par le traitement considéré. Du fait de l'absence de SNR, il faut adopter une autre mesure. Nous examinons tout d'abord les principales solutions proposées pour comparer des maillages.
Nous désignons par $\mathcal{S}$ et $\mathcal{S}'$ les deux maillages dont on veut mesurer la distance.

2.7.1 Distance de Hausdorff et distance moyenne

Nous présentons ici deux distances, l'une fondée sur une norme L_∞, et l'autre sur une norme L_2. Chacune de ces distances permet de quantifier la différence entre deux maillages quelconques même s'ils n'ont pas le même nombre de points.

Distance de Hausdorff

La distance de Hausdorff est définie entre chaque point de $\mathcal{S}$ et tous les points de $\mathcal{S}'$. Dans un premier temps, il faut définir la distance d'un point à un maillage. Soit p un point, on définit la distance $e(p, \mathcal{S})$ à un maillage $\mathcal{S}$ par :

$$e(p, \mathcal{S}) = \min_{p' \in \mathcal{V}} d(p, p'), \tag{2.26}$$

où $d(p, p')$ représente la distance euclidienne entre les points p et p'. On peut alors définir la distance de Hausdorff unilatère $E(\mathcal{S}, \mathcal{S}')$ comme :

$$E(\mathcal{S}, \mathcal{S}') = \max_{p \in \mathcal{V}} e(p, \mathcal{S}'). \tag{2.27}$$

Cette distance est qualifiée d'unilatère car on a en général : $E(\mathcal{S}, \mathcal{S}') \neq E(\mathcal{S}', \mathcal{S})$. Afin d'obtenir une distance (donc symétrique), on définit la distance de Hausdorff :

$$E_H(\mathcal{S}, \mathcal{S}') = \max\{E(\mathcal{S}, \mathcal{S}'), E(\mathcal{S}', \mathcal{S})\}. \tag{2.28}$$

Toutefois, pour des raisons de temps de calcul, on emploie plus souvent la distance de Hausdorff unilatère.

Distance moyenne

Si l'on veut une distance exprimant la distance quadratique moyenne entre les deux surfaces (l'équivalent de l'écart quadratique moyen des fonctions d'une variable), on peut adopter le choix suivant, appelé distance moyenne. Le calcul de cette distance repose sur un

rééchantillonnage des objets, pour autant que les maillages soient uniformément échantillonnés :

$$E_m(\mathcal{S}, \mathcal{S}') = \frac{1}{Aire(\mathcal{S})} \sum_{\mathcal{S}} e(p, \mathcal{S}') d\mathcal{S}. \tag{2.29}$$

2.7.2 Laplacien géométrique

Le laplacien géométrique a été utilisé pour la première fois dans des travaux sur la compression spectrale de la géométrie d'objets 3D [42], afin d'introduire une mesure de la régularité locale de la surface. En effet, les normes vues précédemment ne permettent pas de faire la différence entre un simple ajout de bruit sur les coordonnées des points (donnant un effet visuel extrêmement déplaisant) et une version compressée de la géométrie (où l'aspect visuel est nettement plus acceptable).
Le laplacien géométrique $GL(p)$ en un point p est défini par :

$$GL(p) = p - \frac{\sum_{p' \in p^\star} d(p, p')^{-1} p'}{\sum_{p' \in p^\star} d(p, p')^{-1}}. \tag{2.30}$$

Le laplacien géométrique exprime la distance entre le point et le barycentre des points qui lui sont connexes dans le maillage. Par exemple, si la surface est localement plane avec des voisins équirépartis autour de p, alors $GL(p)$ sera proche de 0.

Pour des maillages ayant même nombre de points et pour lesquels la correspondance entre points est connue, on calcule une mesure globale :

$$E_{GL}(\mathcal{S}, \mathcal{S}') = \frac{1}{2N} \sum_{i=1}^{N} d(p_i, p'_i) + \frac{1}{2N} \sum_{i=1}^{N} \|GL(p_i) - GL(p'_i)\|, \tag{2.31}$$

dans laquelle on voit comment le laplacien géométrique intervient pour ajouter à la distance entre sommets une information de régularité.

2.8 Conclusion

Les maillages 3D peuvent être vus comme une grille d'échantillonnage irrégulière à la topologie quelconque sur laquelle on vient définir des coordonnées cartésiennes représentant la géométrie de l'objet. En sus, pour faciliter l'affichage et le rendu, on associe souvent aux points et/ou aux facettes les normales locales qui rendent compte de la courbure locale de l'objet. L'aspect de la matière composant l'objet est codé sous forme de texture : des images qui doivent être plaquées le plus fidèlement possible sur l'objet. Cette étape dépend de la qualité de la paramétrisation. Enfin, un maillage, suivant ses propriétés topologiques, ne nécessitera pas la même structure de données qu'un autre maillage plus simple. Pour notre part, nous avons employé la structure de données en demi-arête pour nos expérimentations.

Chapitre 3

Traitements usuels sur les maillages

On souhaite introduire des tatouages robustes aux manipulations de l'objet. Dans cette partie, nous donnons donc une liste de traitements pouvant être appliqués à un objet 3D. Nous distinguons les traitements portant uniquement sur les coordonnées des points, de ceux modifiant également l'information de connexité. Parmi les manipulations n'agissant que sur la géométrie, nous commençons par détailler plus précisément différentes techniques de codage de source.

3.1 Codage de source

Le codage de source [16, 19, 33, 32, 64] est une opération qui peut éventuellement faire varier les coordonnées des points des objets tridimensionnels (compression avec perte). Les différentes familles de codage de source se distinguent par la manière de représenter la connexité. On les regroupe généralement en trois familles :

- celles pour laquelle aucun codage de la connexité n'a lieu (méthodes spectrales),
- celles codant le graphe de la connexité (par exemple la technique préconisée par MPEG-4 [72, 34]),
- celles reposant sur un codage implicite de la connexité (aussi appelées méthodes fondées sur la valence [73, 4, 45, 76]).

Sauf pour les méthodes spectrales, les méthodes de codage de source n'utilisent pas de décorrélation de l'information géométrique : on utilise des schémas de prédiction/correction géométrique. Les méthodes spectrales seront détaillées au chapitre 6.

3.1.1 Schémas de prédiction/correction géométrique

Les points 3D à transmettre sont préalablement ordonnés. On utilise généralement l'une ou l'autre des deux méthodes suivantes pour prédire la position d'un nouveau point à partir de ses antécédents. La première méthode se base sur les deux derniers antécédents (prédiction suivant la règle du triangle) et la seconde sur les trois derniers (prédiction suivant la règle du parallélogramme). La régle de prédiction fondée sur les triangles mesure le vecteur 3D entre le nouveau point à insérer et le milieu du segment formé par ses deux antécédents. La règle de prédiction fondée sur les parallélogrammes mesure le vecteur 3D d'erreur entre la

position du nouveau point à insérer et le point formant un parallélogramme avec les trois derniers antécédents.

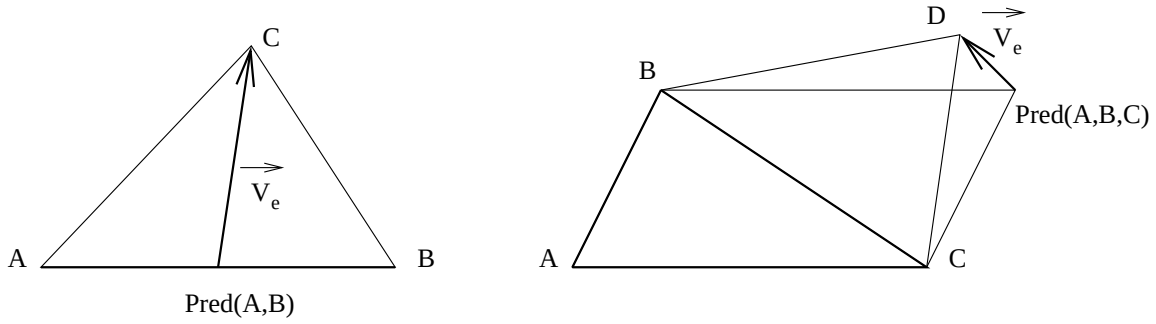

FIG. 3.1 – Schémas de prédiction à partir d'un triangle (à gauche) ou d'un parallélogramme (à droite) : le vecteur d'erreur est mesuré par rapport à la position prédite. En pratique, la prédiction fondée sur la règle du parallélogramme se montre plus efficace : la norme V_e des vecteurs d'erreur est en moyenne plus petite.

Intuitivement, la règle du parallélogramme fonctionne mieux que celle du triangle car la position géométrique de points voisins est généralement corrélée. En pratique la règle du parallélogramme est en effet meilleure que celle du triangle : les vecteurs d'erreur produits sont plus petits en moyenne.

3.1.2 Méthodes fondées sur la valence

Nous présentons deux exemples de méthodes fondées sur la valence : la première propose un codage statique du maillage, la seconde met en œuvre un codage multirésolution. Dans les deux approches, l'idée est que seul l'envoi des valences dans un certain ordre (éventuellement avec quelques codes signalant une exception dans le traitement) suffit à reconstituer la connexité. L'important est de traverser le maillage de manière causale et déterministe, en ne se servant que de l'information de valence.

Méthode de Touma et Gotsman

La première méthode fondée sur la valence [73] propose un encodage statique de la connexité. Elle est valable pour les variétés orientables uniquement. En effet, cette propriété permet d'établir un *ordre local* sur le voisinage d'un sommet, en tournant par exemple dans le sens horaire. Une conséquence de cette propriété est que si un cycle de sommets est retiré du maillage, on crée deux autre maillages, l'un étant à l'intérieur du cycle, et l'autre à l'extérieur. Dans la suite, un tel cycle de sommets sera appelé une liste active. L'idée revient à faire croître cette liste jusqu'à ce que tous les sommets soient parcourus (i.e : soient à l'intérieur du cycle formé par la liste active). Un point à l'intérieur de la liste active est dit conquis. Un point à l'extérieur est dit non conquis. Lorsqu'un point est conquis, la totalité des arêtes adjacentes sont également conquises. Ainsi, un point de la liste active contient des arêtes conquises et non conquises, et est relié par une arête à chacun de ses voisins dans la liste active.

L'encodage de la connexité débute par la sélection d'un triangle dont les trois arêtes forment la liste active initiale. Chaque point de la liste active est passé en revue dans le sens horaire. L'algorithme étend alors la liste active en sélectionnant, dans le sens anti-horaire, les arêtes encore libres autour du point en cours de traitement. Chacune de ces arêtes se voit associé un code *add*, suivi de la valence du sommet non conquis de l'arête en cours de conquête. Une fois toutes les arêtes libres du point conquises, on le place à l'intérieur de la liste active (il est alors conquis). Si la liste active vient à s'intersecter au cours de son expansion, on la découpe alors en deux listes actives, qui seront parcourues successivement. Une telle intersection de la liste active avec elle-même génère un code *split*. L'encodage se termine lorsque toutes les arêtes du maillage sont conquises.

La procédure de décodage est alors triviale : chaque code *add* rencontré provoque l'insertion d'un nouveau point. Ce nouveau point forme alors un nouveau triangle en le connectant avec le point en cours de traitement dans la liste active et à son successeur dans cette liste. Le code de valence permet de déduire le nombre d'arêtes libres pour chaque nouveau sommet dans la liste active.

Il est à noter dès à présent que nous utiliserons une idée semblable dans nos algorithmes de tatouage (au chapitre 5), en rajoutant une contrainte supplémentaire.

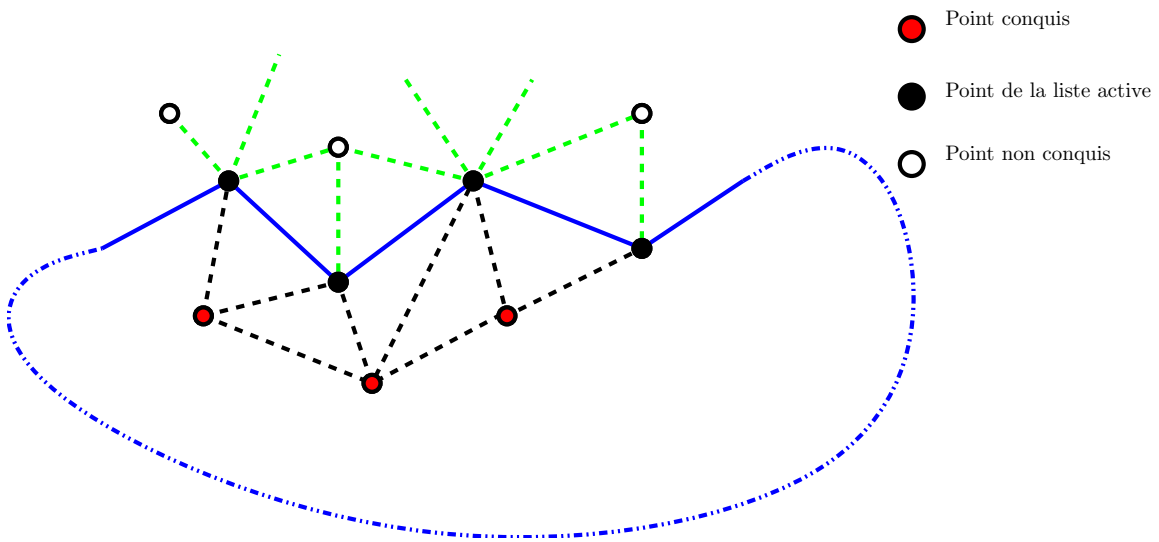

Fig. 3.2 – Propagation sur le maillage grâce à l'information de valence dans la méthode de Touma et Gotsman : il suffit de coder les valences des points que l'on conquiert pour propager la liste active.

Le codage de l'information de géométrie aurait pu être effectué à partir d'une prédiction par la règle du triangle, mais les auteurs ont opté pour une prédiction à base de parallélogramme. Le triangle considéré pour la prédiction est celui formé par le point de la liste active en cours de traitement, son prédécesseur, et le point conquis dont ils sont les voisins.

Méthode d'Alliez et Desbruns

Cette méthode [4] est une extension multirésolution[77] de l'idée précédente, elle autorise la transmission progressive de l'information géométrique maillée. La différence essentielle est qu'ici, lors du décodage, la rencontre d'un code *add* ne génère pas un triangle mais reconstitue tout le voisinage du nouveau point en cours de décodage. Afin de générer cette liste de points, on commence par paver le maillage avec deux types de cellules : les cellules régulières (constituées d'un point, le centre de la cellule, et de son voisinage) et les cellules dégénérées (constituées d'un seul triangle, n'ayant pas de centre). Chaque cellule dispose également de ports d'entrée/sorties. Un port est constitué d'une arête de la frontière de la cellule, et d'un sommet. Il y a autant de ports que d'arêtes sur la frontière de la cellule. Arbitrairement on impose un seul port d'entrée dans la cellule. Le port d'entrée a son sommet appartenant à la cellule. Tous les autres ports, de sortie de la cellule, ont un sommet hors de la cellule. Des cellules régulières et dégénérées suffisent à paver le maillage.

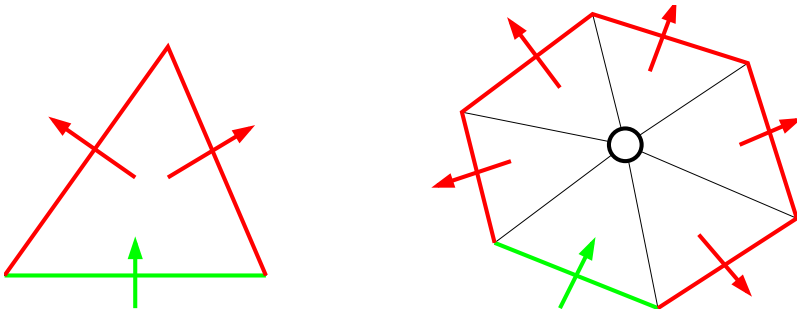

FIG. 3.3 – Les deux types de cellules dans la méthode d'Alliez et Desbrun : à gauche une cellule dégénérée, à droite une cellule régulière. Son centre a ici une valence de 6. Nous avons représenté les ports d'entrée en vert, et les ports de sorties en rouge.

On commence à parcourir le maillage en sélectionnant un port arbitrairement (i.e : on choisit une arête et un des points avec lesquels elle forme un triangle). Ce port est considéré comme un port d'entrée dans une cellule. On sélectionne ainsi implicitement la première cellule, dont on déduit alors tous les ports de sortie. Les sommets du premier port d'entrée sont marqués comme conquis, et le port est placé dans une file. On commence à itérer en extrayant le port de la file, et on examine l'état de son sommet :

- *Si le sommet du port est marqué conquis ou à supprimer* : il n'y a rien à faire, car la cellule dont ce port est celui d'entrée a déjà été visitée. On écarte ce port, et on sélectionne le suivant dans la file.
- *Si le sommet du port est encore libre et si sa valence est inférieure ou égale à* d_{max} (valence maximale choisie à 6) : la cellule implicitement désignée par le port d'entrée est régulière. Son centre sera marqué *à supprimer*, supprimé, puis le polygone de son ancien voisinage sera retriangulé de manière implicite. Les sommets de l'ancien voisinage sont marqués *conquis*. On génère alors un symbole *add* suivi de la valence du point dont on

[77] Pour un maillage, le passage d'une résolution à une autre, plus grossière, est caractérisé par la suppression d'un (resp. d'une) ou plusieurs sommets (resp. arêtes). La méthode que nous présentons ici supprime, pour passer à une résolution plus grossière, un ensemble de sommets dont les voisinages ne se recouvrent pas.

vient d'effectuer la suppression. On collecte alors tous les ports de sortie (dans le sens horaire ou anti-horaire), et on les place dans la file. On sélectionne ensuite le prochain port dans la file, et on traitera ainsi la prochaine cellule dont il est le port d'entrée.

– *Sinon (le sommet du port a une valence supérieure à d_{max} ou bien son sommet est marqué conquis)* : nous sommes en présence d'une cellule dégénérée. On déclare *conquis* le sommet du port d'entrée de la cellule dégénérée, et on place ses deux ports de sortie dans la file. Lors de la rencontre d'une cellule dégénérée, on envoit un code spécial signalant la dégénérescence.

Dans l'algorithme précédent, d_{max} est fixé à 6. Nous discuterons cette valeur au fil de la description de l'algorithme. Nous sommes en mesure de paver de manière déterministe le maillage avec des cellules régulières (en majorité), et des cellules dégénérées (plus rares). Pour passer à une résolution plus grossière, on viendra supprimer les centres des cellules régulières et retrianguler leur intérieur de manière implicite.

Chaque point conquis se voit attribuer une étiquette positive ou négative s'il faut localement maximiser ou minimiser sa valence, respectivement. On cherche à tendre vers une valence moyenne de 6 sur le maillage décimé (dans un maillage chaque sommet a en moyenne 6 voisins). La Fig. 3.4 expose la manière dont on propage les étiquettes positives et négatives sur la périphérie de l'ancienne cellule régulière. En particulier, chaque sommet marqué positivement (resp. négativement) tendra vers une valence élevée (faible) après la retriangulation. On détermine ainsi la retriangulation de la cellule régulière en fonction de la valence du centre de la cellule et des étiquettes positives et négatives du port d'entrée, puis on propage ces étiquettes.

Lors de la conquête d'une cellule régulière, il se peut qu'un certain nombre des sommets de sa frontière soient déjà marqués avec des étiquettes positives et/ou négatives n'étant compatibles avec aucune configuration canonique. Dans ce cas, on ignore l'anomalie, et on retriangule tout de même suivant la Fig. 3.4. Les étiquettes des sommets conquis ne sont pas modifiées.

Sur la Fig. 3.4 on donne les 16 configurations canoniques pour le remaillage des cellules régulières. En effet, ayant fixé $d_{max} = 6$, il ne reste que 4 possibilités pour la valeur de la valence du centre de la cellule : 3, 4, 5, et 6. Ensuite, le jeu des étiquettes positives et négatives sur le port d'entrée impose lui aussi 4 configurations par type de valence. Ce jeu d'étiquettes devant être implicite, cela implique de faire figurer la convention avec laquelle on le propage en passant d'une résolution à l'autre : après suppression du centre, les étiquettes de la cellule sont entièrement déterminées par la Fig. 3.4.

On voit au passage qu'en faisant ce choix pour la distribution des étiquettes positives et négatives lors de la retriangulation, on tend à faire en sorte qu'un sommet sur deux de la frontière de la cellule régulière ait une valence plus faible. On tend donc à maximiser le nombre de sommets de valence 3, ce qui perturbe la distribution naturelle des valences, centrée autour de 6.

Pour pallier ce problème, on effectue dans la foulée une autre étape de décimation guidée par la valence. Cette fois, on fixera d_{max} à 3 afin de corriger l'effet de décalage des codes de valence vers 3 lors de l'étape précédente. Une niveau de résolution comporte en réalité l'effet de deux conquêtes : la première portant sur les cellules régulières dont le centre a une valence d'au plus 6, et la seconde, de nettoyage, porte uniquement sur les cellules régulières dont le centre a une valence de 3. La décimation de nettoyage impose également de modifier

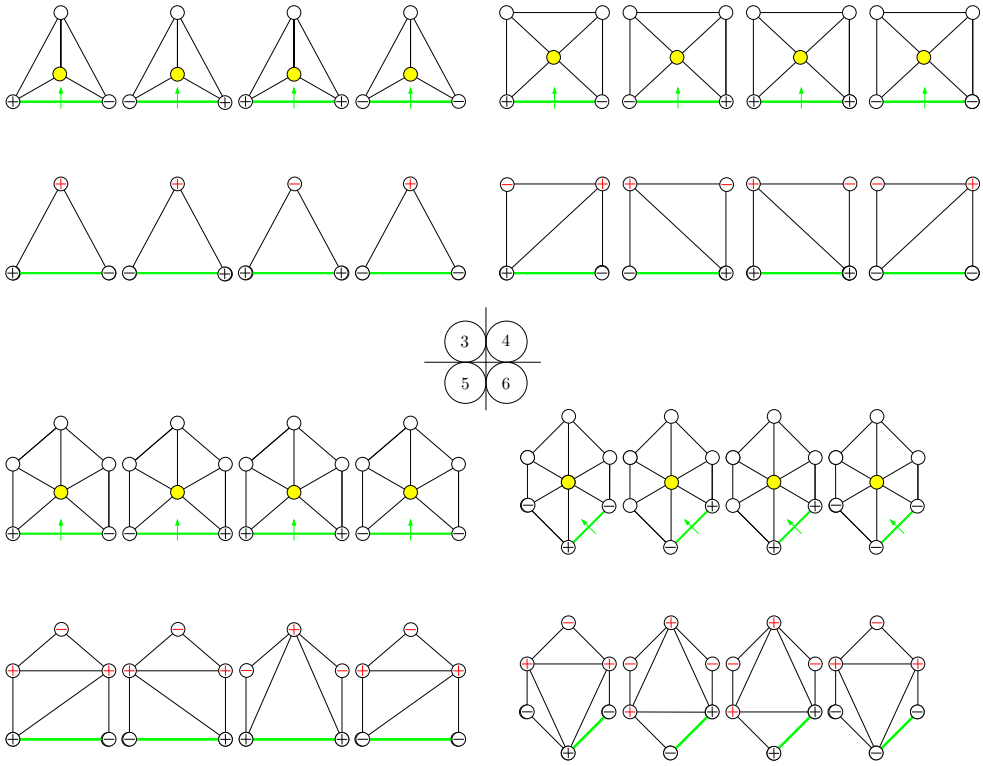

FIG. 3.4 – Triangulations canoniques dans la méthode d'Alliez et Desbrun. Chaque valence possible (3, 4, 5, 6) pour le centre de la cellule régulière engendre quatre jeu d'étiquettes possibles sur le port d'entrée. A chaque fois, il faut définir la retriangulation (du haut vers le bas pour chaque valence) et la propagation des étiquettes.

légèrement les ports de sortie des cellules régulières (dont le centre est à valence 3) : on prendra les quatre ports de sortie dont les arêtes appartiennent aux deux faces adjacentes à la frontière de la cellule régulière.

Pour le décodeur, qui reconstruit les cellules une par une au rythme de l'arrivée des symboles de valence ou de dégénéresence, les étiquettes positives/négatives fournissent le moyen d'une découverte déterministe de la cellule. Les huit cas sont listés sur la Fig. 3.5. Lorsqu'un code de valence $v \geq 3$ arrive, on sait que l'on doit créer $v-2$ nouvelles facettes. Les huit cas synthétisent comment les déterminer. On reconstitue ainsi de manière déterministe le jeu d'étiquettes pour tous les points de la cellule, afin de pouvoir progresser dans le décodage. On arrive alors à décoder la frontière externe de la cellule uniquement avec l'information de valence et le jeu d'étiquettes du port d'entrée. C'est ainsi que le codeur et le décodeur sont correctement synchronisés : grâce à la propagation implicite des étiquettes tant au codage qu'au décodage. Cette approche fondée sur un parcours implicite a pu encore être généralisée aux maillages non nécessairement triangulés, et aux données volumétriques hexaédriques.

On arrive ainsi à représenter hiérarchiquement et de manière déterministe un maillage, en utilisant uniquement l'information de valence. L'optimalité de ce codage a été discutée dans [45], il tend à se rapprocher d'un optimum énoncé par Tutte [75] dans le cas des maillages planaires.

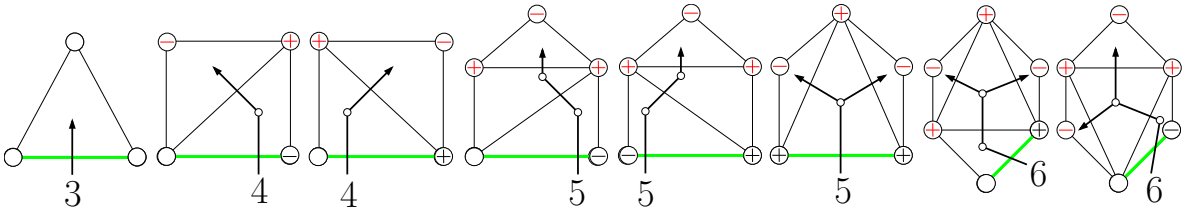

FIG. 3.5 – Découverte déterministe de la cellule régulière par l'information de valence dans la méthode d'Alliez et Desbrun. Etant donné le port d'entrée (avec ses étiquettes) dans la cellule régulière à créer, le code de la valence $v \geq 3$ suffit à déterminer comment créer les $v - 2$ nouveaux triangles. Les codes laissés en blanc signifient que le signe de l'étiquette est indifférent.

Prédire correctement la position du centre des cellules régulières est l'objet de la compression de l'information géométrique. Pour cela, les auteurs se placent dans une base de Frenet locale à la cellule et prédisent les erreurs radiale et tangentielle sur la position du centre de la cellule.

Méthode de Valette (ondelettes surfaciques)

La méthode de Valette [76] est une généralisation de la méthode de Lounsbery [52] pour les maillages de subdivision. Un maillage est dit de subdivision lorsqu'il est le résultat d'un processus itéré de subdivisions régulières partout ou par morceaux. Nous donnons sur la Fig. 3.6 un exemple de prédiction par subdivision régulière pour deux triangles. Cette méthode est limitée car elle impose une contrainte forte sur la connexité du maillage. La subdivision

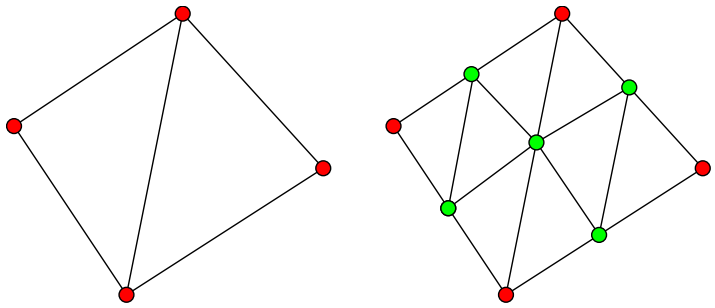

FIG. 3.6 – Exemple de subdivision régulière d'un triangle en quatre autres triangles (subdivision de Loop [50]).

consiste à prédire la position de points, pour ensuite ne stocker que l'erreur commise. On place alors du mieux qu'on peut les prédictions des nouveaux points. Dans la Fig. 3.6, ils sont placés au milieu des arêtes des triangles à subdiviser. On peut alors écrire naturellement le passage d'un niveau d'analyse j de maillage $\mathcal{S}^j(\mathcal{V}^j, \mathcal{E}^j)$ au suivant $(j+1)$ par un système de deux filtres d'analyse $\mathcal{A}^j$ et $\mathcal{B}^j$, et la reconstruction s'effectue à l'aide des filtres $\mathcal{Q}^j$ et $\mathcal{R}^j$. Dans ce cas précis d'un maillage de subdivision, il n'y a pas d'innovation de l'information de

connexité : la subdivision est unique. On passe implicitement de la connexité de $\mathcal{E}^j$ à celle de $\mathcal{E}^{j+1}$. L'analyse s'écrit donc :

$$\mathcal{V}^{j+1} = \mathcal{A}^j \times \mathcal{V}^j, \tag{3.1}$$

$$\mathcal{D}^{j+1} = \mathcal{B}^j \times \mathcal{V}^j, \tag{3.2}$$

où les $\mathcal{D}^j$ sont les coefficients d'ondelettes permettant de reconstruire $\mathcal{V}^{j+1}$ avec $\mathcal{V}^j$ par :

$$\mathcal{V}^{j+1} = \mathcal{Q}^j \times \mathcal{V}^j + \mathcal{R}^j \times \mathcal{D}^j. \tag{3.3}$$

Nous représentons les vecteurs d'erreur à coder sur la Fig. 3.7.

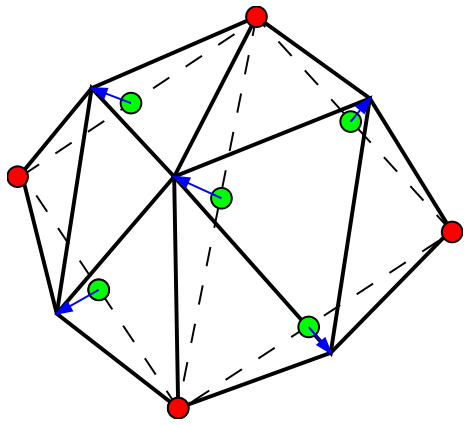

Fig. 3.7 – Vecteurs d'erreur à coder dans l'hypothèse d'une analyse multirésolution par subdivision régulière de Loop.

On peut généraliser cette technique restreinte aux maillages de subdivision grâce à une subdivision plus riche, irrégulière, permettant d'appréhender n'importe quelle connexité. Cette subdivision irrégulière recense 15 configurations canoniques (et dont nous donnons quelques exemples sur la Fig. 3.8), et elle autorise la subdivision d'un triangle en 4, 3, 2 triangles, ou le laisser inchangé.

A l'encodage, il faut donc trouver un moyen d'apparier les facettes entre elles du mieux possible afin de ne jamais bloquer l'algorithme. Les auteurs proposent une manière d'y parvenir pouvant éventuellement faire appel à une convention faisant d'une arête une facette spéciale, dégénérée. On donne ci-dessous (voir Fig. 3.9) un exemple de fusion des facettes opérée par l'algorithme.

Une fois les facettes groupées, on envoie un code décrivant la configuration de la subdivision irrégulière. Afin de procéder à une réelle analyse par ondelettes, les auteurs complètent cette technique par un lifting, qui permet d'obtenir à la résolution j la meilleure approximation $\mathcal{V}^j$ de $\mathcal{V}^{j+1}$ au sens des moindres carrés [60].

3.1.3 Méthode de Taubin (MPEG-4)

Ce codage est celui employé dans la compression du format binaire VRML et dans MPEG-4 3D Mesh Coding [72]. Il ne s'applique qu'aux maillages de connexité uniquement triangulaire. Le principe en est le suivant : le maillage est, si nécessaire, découpé de telle manière

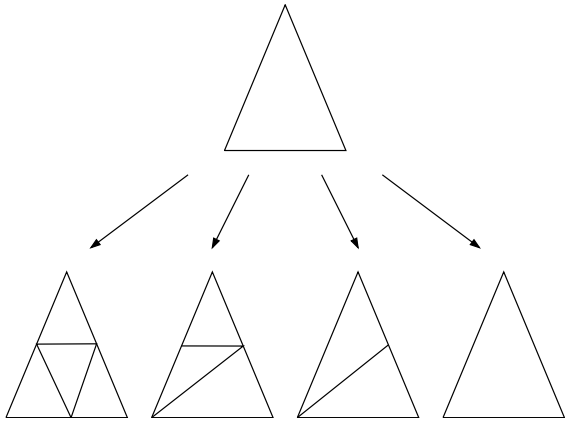

FIG. 3.8 – Quelques cas possibles parmi ceux d'une subdivision irrégulière d'un triangle en un nombre variable d'autres triangles.

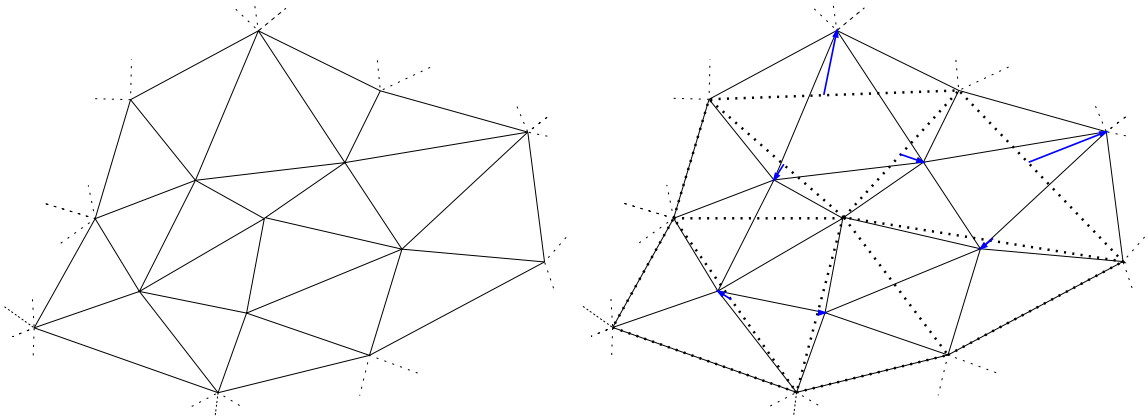

FIG. 3.9 – Fusion des facettes dans la méthode de Valette : une heuristique se charge de regrouper les facettes avant décimation.

que chaque arête appartienne au plus à deux facettes [34]. Ensuite, chaque composante est littéralement pelée en longs rubans de triangles de manière à obtenir un arbre couvrant des faces. A ce premier arbre est adjoint un arbre de recouvrement des sommets. Ainsi, le graphe de connexité "pelé" peut-il se projeter sur un plan 2D. Le graphe alors projeté sur le plan se réduit à un polygone simple qu'il est possible de coder de manière extrêmement compacte avec un alphabet de quatre symboles. Les deux arbres de recouvrement contiennent toute l'information nécessaire à la reconstruction de la connexité originale.

La compression de la géométrie a alors lieu sur les longues bandes de triangles par prédiction et correction. Un codage correct de la géométrie nécessite un minimum de 10 bits par échantillon pour obtenir un effet visuel satisfaisant avec une prédiction fondée sur les parallélogrammes. Cette méthode de compression est la seule faisant l'objet d'une normalisation (VRML 2.0 Binaire et MPEG-4 3D Mesh Coding).

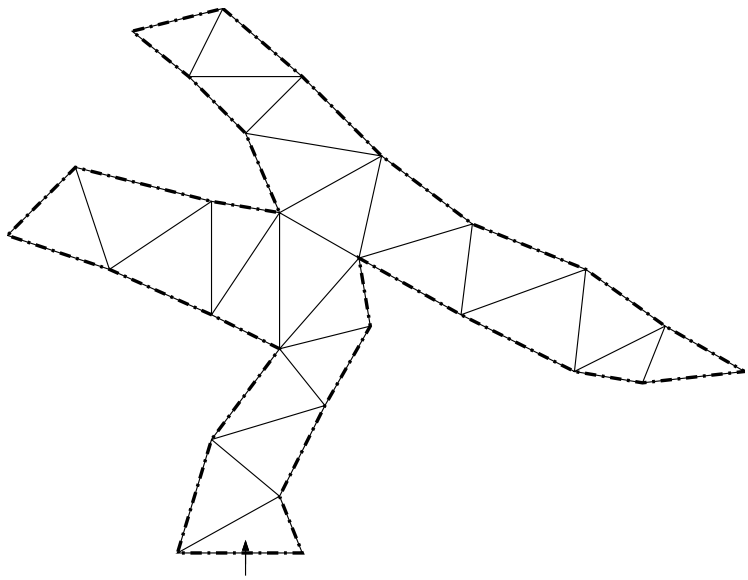

FIG. 3.10 – Encodage de la connexité dans MPEG-4 : le maillage est pelé, puis projeté sur le plan afin d'obtenir un polygone simple. On part alors d'un triangle et d'une direction d'entrée pour commencer à décrire l'arbre de connexité des triangles avec l'alphabet de quatre symboles nécessaires pour fixer les quatre situations possibles relativement au(x) triangle(s) suivant(s) : *G* (resp. *D*) si son unique fils est à gauche (resp. droite), *2* s'il a deux fils et *F* s'il est une feuille. Muni d'une orientation ou d'un sens de parcours, l'arbre en parcouru en profondeur d'abord. Ici le code de connexité est : GDGDGG22DGDGDGFDGDGFDGDGF.

3.2 Traitements affectant la géométrie uniquement

Si le codage de source demeure le principal traitement subi par les signaux, il n'en reste pas moins que le tatouage peut éventuellement souffrir d'autres opérations. Ce sont typiquement celles proposées dans la plupart des logiciels de modélisation 3D. Nous en donnons à présent une liste non exhaustive. Dans chaque cas, nous discutons l'impact de la manipulation considérée sur le schéma de tatouage.

3.2.1 Ajout de bruit

L'ajout de bruit sur les coordonnées des points est souvent le résultat de la transmission sur des canaux médiocres. C'est aussi l'une des attaques classiques de ceux qui cassent les tatouages ; c'est enfin une façon de modéliser la compression géométrique.

3.2.2 Lissage

Lors de l'acquisition des données 3D par un scanner, il arrive couramment que la surface présente un aspect rugueux. Afin d'éliminer cet artefact des techniques de lissage ont été proposées comme celle exposée dans [71]. Taubin reprend la définition du filtrage gaussien [49, 81] et propose un opérateur laplacien défini sur les surfaces maillées. A chaque point p_i

on ajoute son laplacien pondéré par λ :

$$p'_i = p_i + \lambda\, \Delta p_i, \tag{3.4}$$

avec $0 \leq \lambda \leq 1$. Le laplacien de Taubin est défini en posant :

$$\Delta p_i = \sum_{j \in i^\star} w_{ij}(p_j - p_i). \tag{3.5}$$

On impose encore :

$$\sum_{j \in i^\star} w_{ij} = 1. \tag{3.6}$$

On a donc :

$$p'_i = (1-\lambda)p_i + \lambda \sum_{j \in i^\star} w_{ij} p_j, \tag{3.7}$$

On choisit alors des poids $w_{i,j}$ fonctions des arêtes liant p_i à ses voisins :

$$w_{ij} = \frac{\phi(p_i, p_j)}{\sum_{k \in i^\star} \phi(p_i, p_k)}. \tag{3.8}$$

où d_i est la valence du sommet $p - i$. Les fonctions ϕ ne dépendant que des arêtes, on peut proposer plusieurs choix :

$$\phi(i,j) = \frac{1}{d_i}, \tag{3.9}$$

$$\phi(i,j) = \|p_i - p_j\|^\alpha. \tag{3.10}$$

Un autre choix consiste à prendre pour $\phi(i,j)$ le rapport de la somme des aires des deux faces adjacentes à l'arête $\{i,j\}$ sur deux fois l'aire du voisinage de p_i. Nous illustrons un tel filtrage gaussien, avec $\phi(i,j) = \frac{1}{d_i}$ et $\lambda = 0.2$, sur la Fig. 3.11. Nous avons effectué 4000 itérations. Nous reviendrons sur cet opérateur dans le chapitre consacré à la décomposition spectrale.

3.2.3 Rotation, translation et mise à l'échelle uniforme

Il s'agit ici des manipulations le plus souvent appliquées aux objets 3D. Sous cette appellation on regroupe les transformations affines : la rotation, la mise à l'échelle et la translation, ou encore une combinaison des trois. Afin d'être robuste face à ces transformations, les schémas de tatouage doivent en fait les prendre en compte dès leur conception. Dans la grande majorité des cas, on utilise des primitives d'insertion de la marque naturellement invariantes par transformation affine.

3.2.4 Transformations perspectives

A la différence des précédentes, les transformations perspectives ne sont pas linéaires. Elles sont utilisées pour déterminer l'image d'un objet 3D par un système optique et sont disponibles dans les modeleurs commerciaux. Là encore, on privilégierait un espace de tatouage naturellement invariant. Toutefois comme les transformations perspectives transforment des données 3D en données 2D, on perd généralement le tatouage.

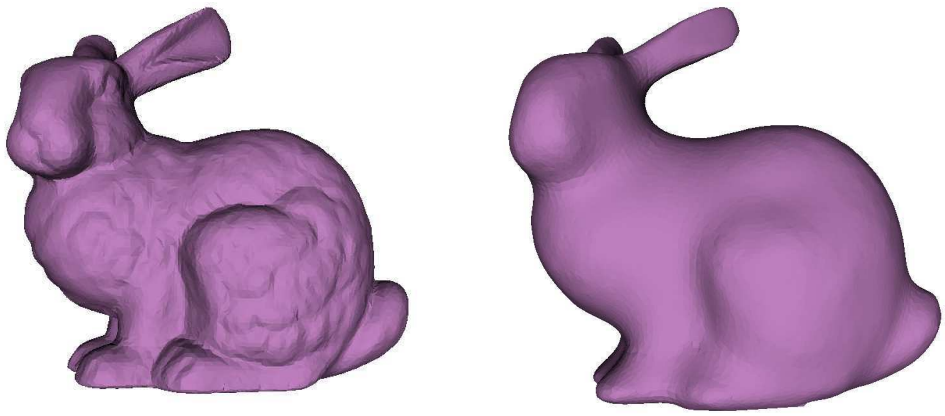

FIG. 3.11 – Exemple de maillage exagérément lissé. A gauche : original (données : Stanford 3D Scanning Repository). A droite : maillage lissé.

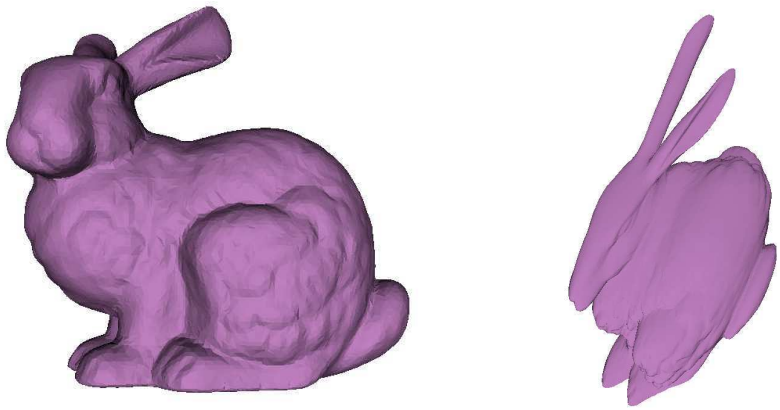

FIG. 3.12 – Exemple de transformation perspective. Données : Stanford 3D Scanning Repository.

3.3 Traitements affectant la connexité

Nous présentons à présent une liste non exhaustive de quelques traitements modifiant l'information de connexité. L'information géométrique peut même varier également. Du point de vue du tatouage, cette classe de transformations complique passablement la conception d'un procédé d'insertion robuste de la marque.

3.3.1 Renumérotation des points

Après certains traitements supposant une modification de la connexité (décimation, remaillage), les points sont renumérotés, certains ayant disparu ou leur nombre ayant changé. Certains schémas primitifs de tatouage pouvaient utiliser l'index du point considéré pour inscrire un bit à cacher, ils étaient donc très sensibles à la renumérotation. Toutefois, la

plupart des schémas actuels n'utilisent plus cette information.

3.3.2 Coupe

La coupe, ou section, est une modification de la connexité consistant à extraire telle ou telle partie du maillage. C'est l'équivalent du fenêtrage (*crop*) pour le cas de l'image fixe. La géométrie et la connexité des sommets restants sont inchangées. Les schémas de tatouage se servant de la connexité pour situer l'information cachée peuvent être mis en défaut par ce type de manipulation.

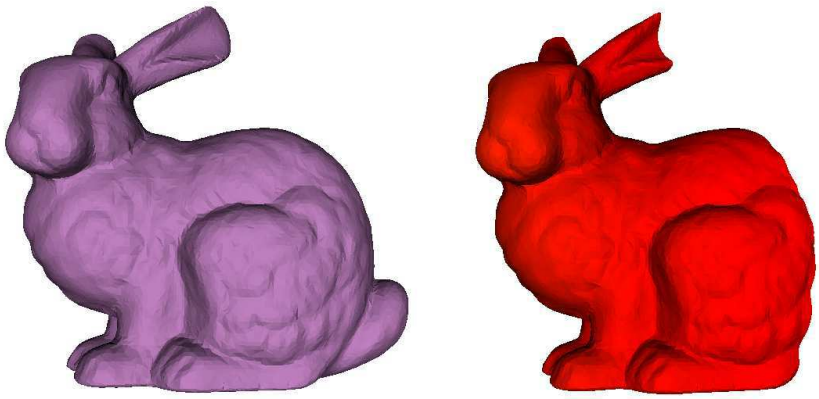

FIG. 3.13 – A gauche : original. A droite : exemple de coupe (par un plan).

3.3.3 Décimation

Les objets 3D correspondent à un type de données complexe. Ils sont donc extrêmement lourds à manipuler. Au début de l'imagerie 3D, se posait le problème d'un affichage rapide de tels objets sur des dispositifs aux capacités limitées. En observant que la suppression de quelques points ou arêtes judicieusement choisis ne dénaturait pas l'aspect visuel de l'objet, la communauté s'est mise à la recherche de moyens de simplifier les maillages, de les décimer. Cet axe de recherche a été particulièrement fécond et de nombreux travaux portent sur ce domaine. On distingue deux sortes d'algorithmes de décimation : ceux procédant par l'effondrement de points, et ceux supprimant des arêtes (voir Fig. 3.14). Tous ces algorithmes ont en commun de proposer une méthode déterministe de remaillage local. La plupart du temps, le choix du point ou de l'arête à effondrer s'opère en fonction de l'évaluation d'une fonction d'énergie locale. On choisit généralement de minimiser une forme quadratique comme dans l'exemple que nous développons ci-dessous.

Dans [31], une technique de décimation appelée QEM (pour Quadric Error Metric) permet de simplifier un maillage à l'aide de l'opérateur d'effondrement d'arête. Chaque itération de l'algorithme classe les arêtes par priorité. La priorité est donnée aux effondrements d'arête minimisant une certaine erreur. L'erreur $E(p'_i)$ commise en remplaçant p_i, appartenant à un plan de normale $\overrightarrow{n}$ et de constante d, par le point p'_i, est calculée comme étant la distance

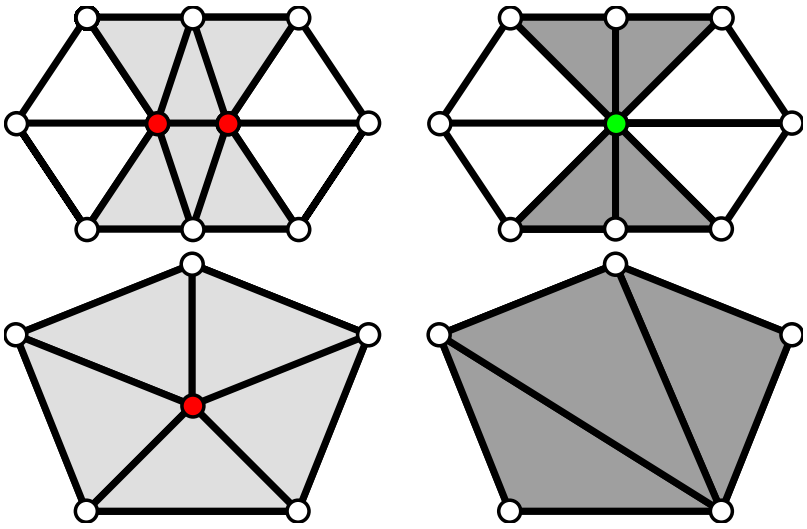

FIG. 3.14 – Principaux opérateurs de décimation (également appelés opérateurs d'Euler) entraînant une modification locale de la connexité. En haut : effondrement d'arête. En bas : effondrement de point.

au carré du point au plan :

$$E(p'_i) = (\overrightarrow{n}^T p'_i + d)^2 = p'^T_i (\overrightarrow{n}\,\overrightarrow{n}^T) p'_i + 2d\overrightarrow{n}^T p'_i + d^2. \tag{3.11}$$

Il s'agit d'une forme quadratique avec un terme linéaire et une constante. On met le tout sous la forme :

$$E(p'_i) = p'^T_i A p'_i + 2b^T p'_i + c. \tag{3.12}$$

Finalement, l'erreur totale commise en un point en remplaçant p_i par p'_i est calculée comme la somme des erreurs commises par rapport aux plans des facettes du voisinage de p_i. L'erreur en un point p_i est minimisée pour p_i qui est le seul à appartenir à tous les plans des facettes de son voisinage, voir Fig. 3.15.

La décimation consiste à trouver un point $\bar{p}$ remplaçant au mieux l'arête $\{p_i, p_j\}$ à effondrer. L'erreur commise est donc fonction en réalité des deux points extrémaux de l'arête. Pour une approximation du calcul de l'erreur commise en remplaçant une arête par un point, les auteurs proposent de faire la somme des erreurs en chaque point de l'arête à effondrer. C'est en ce sens que l'on arrive à classer les arêtes par priorité. Bien entendu, la file de priorité est remise à jour après chaque effondrement.

Minimiser l'erreur commise en remplaçant p_i par p'_i revient à résoudre un système linéaire. La solution est donnée par :

$$p'^{min}_i = -A^{-1}b. \tag{3.13}$$

Et l'erreur minimale ainsi commise vaut :

$$E_{min} = E(p^{min}_i) = -b^T A^{-1} b + c. \tag{3.14}$$

Du point de vue du tatouage, la modification de l'objet porte à la fois sur les informations de connexité et de géométrie. C'est donc toute la *représentation* de l'objet qui change.

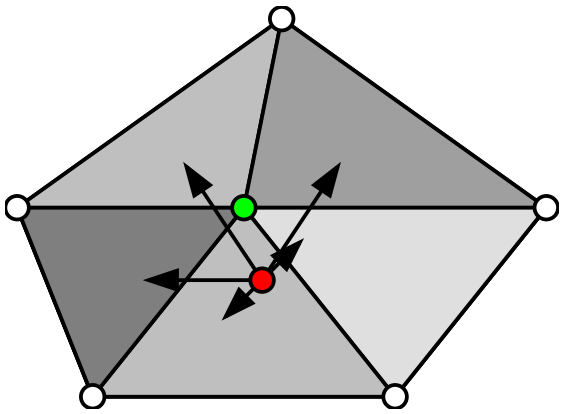

Fig. 3.15 – Calcul de l'erreur quadratique en un point dans QEM : c'est la somme des distances au carré d'un point aux plans des facettes.

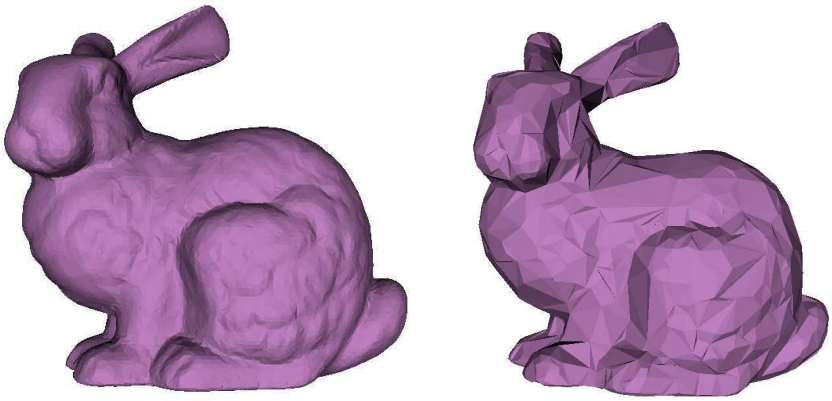

Fig. 3.16 – Exemple de simplification uniforme. A gauche : original. A droite : version simplifiée (90% des points effondrés).

Pourtant, la géométrie au sens large ne s'en trouve pas nécessairement bouleversée. Nous illustrons cette méthode de simplification à la Fig. 3.16 où 90% des points ont été supprimés.

3.3.4 Subdivision

Le problème de la subdivision prend encore sa source en visualisation. Une fois le maillage simplifié, on cherche un moyen d'augmenter son nombre de points de manière automatique, sans recourir aux sommets originaux. Une procédure permettant de rajouter des points se révèle en machine plus efficace que le stockage et l'affichage des points réels.

On distingue les procédures de subdivision d'approximation (Loop [50]) et d'interpolation (Butterfly modifié [20, 83]). Nous ne présentons que les subdivisions régulières définies sur des triangles, même s'il en existe pour des quadrilatères (Catmull-Clark pour l'approximation [14] et Kobbelt pour l'interpolation [46]). Les subdivisions d'interpolation sont beaucoup

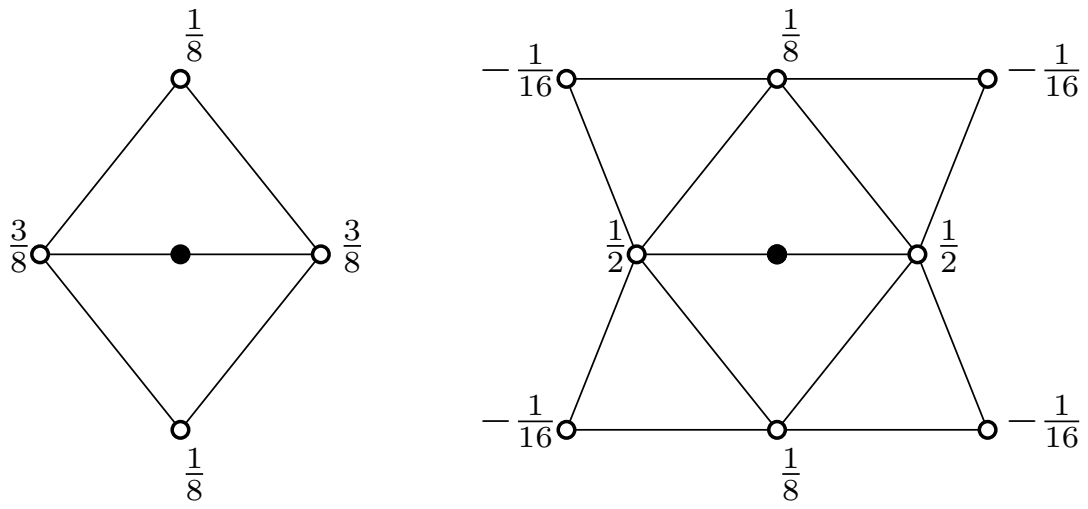

Fig. 3.17 – Voisinages et poids pour le calcul des coordonnées d'un nouveau sommet dans les schémas de subdivision de Loop (à gauche) et Butterfly modifié (à droite) pour l'interpolation. Les sommets à rajouter sont en noir.

plus souples à manier (puisque les sommets originaux appartiendront au maillage final), mais donnent généralement des surfaces de moins bonne qualité que les subdivisions par approximation.

Une fois la procédure de subdivision choisie, on s'intéresse généralement à la surface limite obtenue par un tel procédé. En particulier, on chercher à caractériser la dérivabilité de la surface limite. Elle est par construction de classe C^2 partout sauf sur les lignes de crête et les bords, où elle peut être de classe C^1 [66].

Généralement, une procédure de subdivision rajoute un sommet au milieu d'une arête (voir Fig. 3.6) et indique comment placer correctement ce sommet en fonction de son voisinage. Les coordonnées du nouveau sommet sont calculées en modulant les coordonnées de son voisinage par des poids idoines. Ensuite, le nouveau sommet est connecté à ses nouveaux voisins, et le processus est itéré jusqu'à obtenir le nombre de sommets souhaité. Nous donnons sur la Fig. 3.17 les voisinages et les poids des subdivisions de Loop et du schéma Butterfly modifié.

3.3.5 Remaillage

Il arrive que certains traitements complexes que l'on ait à effectuer sur des maillages requièrent une connexité particulière (typiquement une connexité régulière avec des valences égales à 6, ou une connexité de subdivision [78]).

Un pré-traitement est alors nécessaire : on vient remailler l'objet avec la connexité souhaitée. Un remaillage peut également être utile dans le cas où l'on souhaite répartir judicieusement les points en fonction de la courbure de l'objet [5]. Là non plus, la géométrie au sens large n'est que peu affectée par ces opérations. En revanche, la représentation entière de l'objet est modifiée. On distingue généralement deux approches en remaillage : celle qui modifie le maillage original [74, 38, 47, 12], et celle qui s'en sert pour guider la création d'un

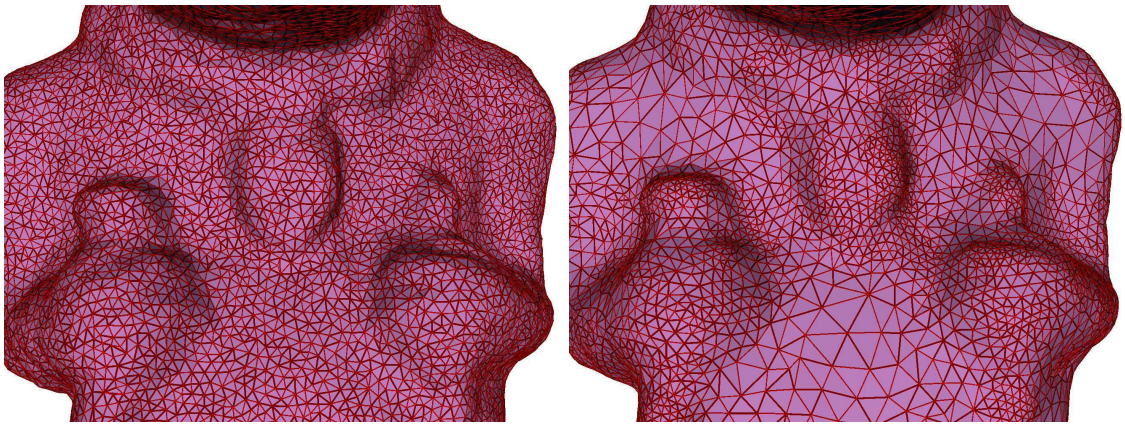

FIG. 3.18 – Exemple de remaillage. A gauche : original, maillage uniforme. A droite : version remaillée, avec une densité adaptée à la courbure. Données : Télécom Paris [36].

maillage neuf [5, 2, 3]. Il s'agit d'une des manipulations les plus sévères qu'un schéma de tatouage ait à affronter.

3.4 Conclusion

Il existe tant de manipulations sur les surfaces maillées que nous avons préféré mentionner les principales, et les séparer en deux catégories suivant qu'elles mofidient ou non la connexité de la surface originale. En effet, du point de vue du tatouage, il arrive que l'on se serve de l'information de connexité pour insérer et relire l'information. Nos travaux en tatouage par invariants se placent par exemple dans cette optique. Mais la même surface pouvant être représentée de multiples façons, il se pose le problème de la représentation canonique de cette surface. Une telle représentation n'existe pas en général, et on adopte la représentation la plus adaptée au but à atteindre : en visualisation on cherchera à simplifier le maillage, en simulation on cherchera à uniformiser les éléments de surface, en traitement de la géométrie on cherchera à atteindre une connexité de subdivision.

Chapitre 4

État de l'art

Examinons maintenant les diverses techniques de tatouage des objets 3D. Elles empruntent des éléments déjà validés en 2D. Par exemple, on cherchera à répéter la marque et à enfouir un même bit de nombreuses fois de façon à compenser la fragilité du tatouage par une forte redondance. On utilisera également souvent des clefs secrètes afin de brouiller soit l'ordre de parcours des diverses facettes, soit l'ordre d'apparition des bits de la marque. Néanmoins, comme nous allons le voir, la géométrie des objets maillés offre de nombreuses solutions originales aux tatoueurs.

Nous classons les différents schémas suivant qu'ils font ou non appel à une configuration géométrique pour insérer la marque. En effet, les techniques fondées sur une configuration géométrique reposent toutes sur le même paradigme d'*arrangement* de la marque. A l'inverse, les autres méthodes ont pour point commun de disperser l'information utile de manière plus fine sur le maillage.

Avant d'aller plus loin, il convient d'avertir le lecteur que les références en tatouage 3D ne détaillent que trop rarement de façon précise la manière dont l'information est exactement encodée. Cet état de l'art est donc aussi précis que les références nous l'ont permis. En particulier, la description des schémas par invariants géométriques reste particulièrement lapidaire sur le sujet (quand on ne se contente pas de mentionner uniquement la nature de l'invariant que l'on modifie). Pour nous, nous tenterons au contraire au chapitre 5 de détailler le mieux possible notre méthode d'insertion géométrique.

4.1 Schémas avec configuration géométrique locale

L'information de connexité peut être mise à profit dans le cadre du tatouage. Les schémas utilisant cette information font appel à une configuration géométrique : un ou plusieurs triangles voisins. L'information cachée est alors codée en modifiant des invariants géométriques. Du type d'invariant retenu dépend la robustesse *a priori* du schéma, on choisit donc les invariants en fonction des transformations que subiront les objets [27]. Nous en donnons une liste non exhaustive :

- Sont invariants par rotation et translation : la longueur d'un segment, l'aire d'un polygone et le volume d'un polyèdre.
- Sont invariants par transformée affine : le rapport des longueurs de deux segments

colinéaires, le rapport de l'aire de deux polygones coplanaires et le rapport des volumes de deux polyèdres.
- Seul le birapport de quatre points alignés est invariant par transformation projective [25].

Les méthodes retenues vont alors introduire de légères modifications dans les invariants choisis. Comme il n'y a pas d'invariant, à part la valence, aux perturbations des positions des sommets, elles sont sensibles à l'ajout de bruit. Elles pourront résister à des modifications locales de la connexité pourvu que la localisation soit bonne. On distingue trois manières de localiser l'information utile, appelées arrangements.
- Soit on utilise un parcours canonique du graphe de connexité (comme dans les méthodes de compression), l'arrangement est dit global,
- Soit on utilise un parcours canonique de chacune des sous-parties du maillage, et l'arrangement est dit local,
- Soit enfin on marque explicitement la *localisation* de l'information. On est alors confronté à deux exigences : marquer une configuration géométrique pour éviter de l'utiliser une seconde fois, et aussi inscrire un index permettant de replacer l'information cachée au sein de la marque. Il faut, lors de la détection, savoir distinguer les configurations géométriques codant l'information utile des autres, et il faut savoir quel bit du message telle configuration code effectivement. L'arrangement est alors dit indexé.

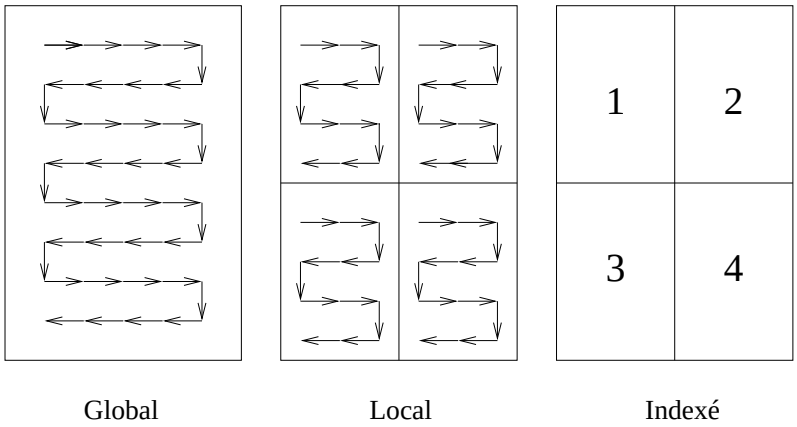

Fig. 4.1 – Les trois types d'arrangements disponibles. Les arrangements globaux et locaux nécessitent un parcours du maillage : il faut alors choisir un germe relativement stable. Seul l'arrangement indexé permet une relecture en aveugle sans nécessiter de parcours particulier du graphe de connexité.

Les deux premiers types d'arrangements doivent trouver un germe[78] pour initialiser le parcours canonique du graphe de connexité. On peut utiliser deux techniques pour cela :
- des séquences de synchronisation, qui sont des marques connues qui débutent le message utile et que l'on retrouve par des séquences d'essai-erreur,

[78]Le germe d'un parcours est soit un triangle, une arête ou un sommet. Le type du germe dépend des spécificités du parcours. Le choix du germe détermine le parcours, un peu comme la graine d'un générateur pseudo-aléatoire détermine la suite de nombre fournis par le générateur.

– des initialisations sur des configurations remarquables du volume ou de la partition. On peut par exemple utiliser comme germe, s'il s'agit d'un côté, celui dont le volume du tétraèdre sous-tendu par ses deux triangles incidents est maximal. Comme les rapports des volumes de polyèdres restent inchangés dans le cas de transformations affines, cette initialisation sera robuste à ces transformations. De même, s'il fallait un germe qui soit un triangle, le triangle d'aire la plus grande ferait l'affaire dans le cas de transformations rigides (rotation, translation, etc.) mais il n'est pas robuste à une transformation affine.

4.1.1 Arrangement global

Dans [8], une méthode de tatouage (appelée *triangle flood*) fondée sur un parcours global du graphe de connexité est présentée. Ce parcours peut être vu sous forme d'arbre. Partant d'un triangle, on vient collecter les sommets qui forment un triangle avec un côté adjacent du triangle initial. On s'intéresse aux hauteurs issues de ces sommets dans les triangles adjacents. On ordonne ensuite ces hauteurs, à la fois pour fixer l'ordre de parcours des triangles, et aussi pour insérer l'information à cacher. On itère ensuite sur les triangles adjacents, en parcourant l'arbre *en largeur d'abord*.

C'est l'ordre des hauteurs qui fixe l'ordre des bits de la marque. On impose que les hauteurs, ordonnées, aient une distance d_{min} entre chacune d'elles successivement. La première modification des hauteurs a pour but d'imposer la contrainte sur d_{min}. Le décodeur peut alors reconstituer le parcours en réordonnant les hauteurs, et en ne s'occupant que de celles dont les écarts successifs sont supérieurs à d_{min}. La deuxième opération vise à inscrire les valeurs de bits de la marque, en modifiant encore les hauteurs. A l'inscription de la marque, on respecte la contrainte sur d_{min} afin de ne pas effacer le parcours que l'on vient de créer (nous retrouverons ce problème de causalité au chapitre 5).

L'intervalle admissible de modification des hauteurs est calculé de manière à :

– Conserver le parcours (contrainte à respecter sur d_{min})

– Insérer m bits par modification de hauteur (l'auteur prend $m = 2$)

On a représenté un maillage et l'arbre correspondant sur la Fig. 4.2. On notera que l'on peut gérer des maillages qui ne sont pas nécessairement des variétés (voir les sommets 4 et 5), et que le cas spécial où un même sommet appartient à deux triangles adjacents au triangle père dans l'arbre génère une exception (considérer le sommet 2).

Un tel parcours n'admet aucune modification de la connexité et instaure un ordre global d'arrangement des bits de la marque sur le maillage. Le décodage prend fin lorsque tous les bits sont retrouvés (la longueur du message caché est supposée connue au détecteur), ou que l'on détecte une séquence spéciale de bits indiquant la fin du message (solution non retenue par l'auteur).

4.1.2 Arrangement local

Nous donnons ici deux exemples d'arrangement local de l'information cachée. Le premier se sert de sites admissibles proches pour déterminer le numéro du bit que l'on va cacher. Le second découle quant à lui d'un arrangement global : là encore la marque est enfouie selon un arbre de recouvrement des sommets, mais les auteurs partitionnent le maillage au

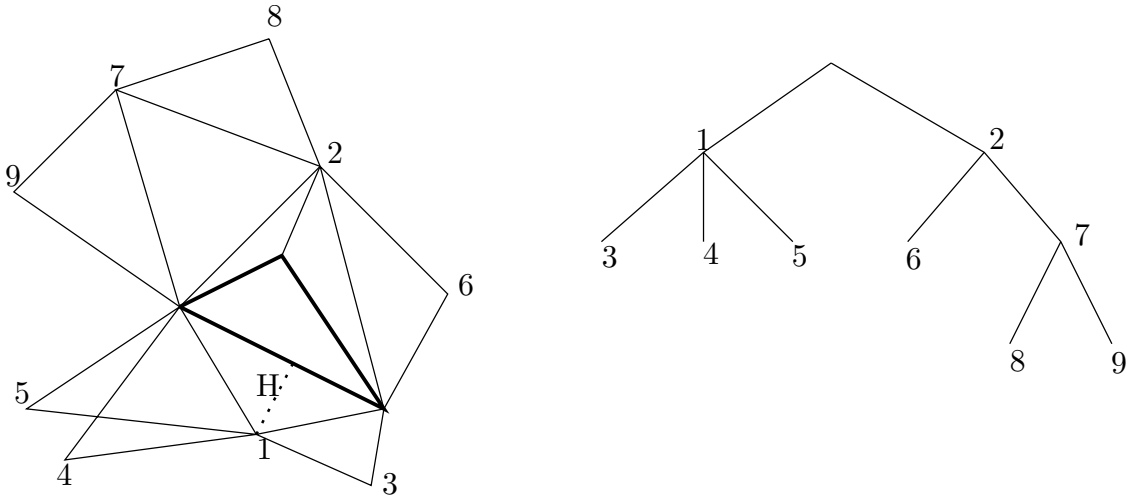

FIG. 4.2 – Parcours global du maillage dans l'algorithme *triangle flood* [8] en largeur d'abord. Le triangle initial est représenté en gras à droite, l'arbre obtenu est à droite. Le sommet 2 génère une exception (il est commun à deux triangles adjacents aux triangle en gras) de manière à ce que l'arbre ne le contienne qu'une seule fois. Ce parcours permet de gérer des maillages qui ne sont pas nécessairement des variétés (les sommets 4 et 5 partagent une arête commune à trois triangles).

préalable et appliquent un arrangement global sur chacune des partitions. En partitionnant le maillage, on peut rendre local un arrangement global.

Schéma de Harte

Dans [35], la marque est répétée sur des parties du maillage qui ne se recouvrent pas. Pour cela, une sélection des sommets pouvant être modifiés est dressée. On considère qu'un sommet peut être marqué s'il n'appartient pas à un segment trop long. On calcule alors la somme D_i des longueurs de chaque sommet p_i à ses voisins :

$$D_i = \sum_{p_j \in p_i^\star} \|p_i p_j\|. \tag{4.1}$$

Un sommet p_i est déclaré valide si pour un certain seuil T :

$$D_i < T. \tag{4.2}$$

Tous les sommets voisins sont déclarés invalides. L'idée de [35] consiste à se servir du voisinage d'un sommet valide p_i pour établir un espace de tatouage dans lequel on modifie p_i. On remarque que les voisins de p_i valides peuvent définir un ellipsoïde (voir Fig. 4.3) centré autour de μ_i :

$$\mu_i = \frac{1}{d_{p_i}} \sum_{p_j \in p_i^\star} p_j. \tag{4.3}$$

La forme de l'ellipsoïde est donnée par la matrice de covariance S_i :

$$S_i = \frac{1}{d_{p_i}} \sum_{p_j \in p_i^\star} (p_j - \mu_i)(p_j - \mu_i)^T. \tag{4.4}$$

La surface de l'ellipsoïde est constituée des points p tels que :

$$(p - \mu_i)^T S_i^{-1} (p - \mu_i) = K, \tag{4.5}$$

où K est un facteur de normalisation. Soit M_t le nombre de sommets valides pour l'insertion de B bits. Les M_t sommets sélectionnés sont partagés aléatoirement en plusieurs ensembles de B sommets. A l'intérieur de chacun de ces ensembles, on vient ordonner les B sommets qui le composent en se fondant sur les distances entre les centres de leur ellipsoïde. Associés aux numéros de 1 à B, les sommets sont donnés par :

$$i = \arg\min_j \sum_{k=1, k \neq j}^{B-1} \|\mu_k - \mu_j\|^2, \tag{4.6}$$

où l'on ne considère que les $B-1$ plus proches ellipsoïdes pour le calcul. Une fois qu'un sommet a obtenu son numéro, son ellipsoïde ne rentre plus en ligne de compte pour l'attribution des autres numéros.

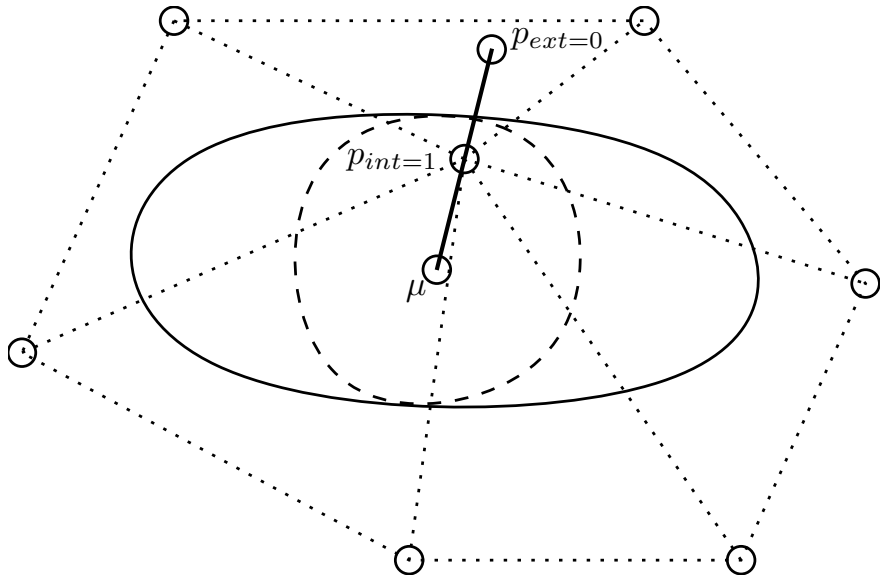

FIG. 4.3 – L'espace de tatouage associé à l'ellipsoïde dans [35]. Ici p_i est situé à l'intérieur de l'ellipsoïde et code un 1 par convention. Si l'on voulait cacher un 0, il fait amener p_i en p_{ext}

Une fois les numéros attribués aux sommets, il ne reste plus qu'à insérer l'information. Ici, l'ellipsoïde matérialise un intérieur et un extérieur. L'intérieur sert à coder les 1, l'extérieur les 0. Si le sommet code déjà dans la bonne valeur de bit, il n'est pas modifié, sinon il est poussé de l'intérieur vers l'extérieur de l'ellipsoïde (pour passer de 1 à 0), ou l'inverse (pour passer de 0 à 1). Le déplacement se fait selon la droite $\mu_i p_i$.

Lorsque les B premiers bits sont insérés, on renouvelle le même algorithme pour les B sommets de l'ensemble suivant de sommets valides. Chaque bit est donc répété $\lfloor M_t/B \rfloor$ fois. L'ordre des bits est uniquement fonction des $B-1$ plus proches ellipsoïdes, l'arrangement est donc local.

Schéma TVR

L'invariant utilisé dans le schéma TVR [56] est le rapport des volumes de deux tétraèdres. Pour cette raison, ce schéma nécessite un arrangement global ou local (version TVR Cluster). Il faut en effet un tétraèdre de référence auquel rapporter le volume des autres. Les tétraèdres sont formés par une arête (p_3p_4 sur la figure 4.4) et les deux triangles incidents ($p_1p_3p_4$ et $p_2p_3p_4$). Le parcours du graphe de connexité repose sur un arbre de recouvrement des points.

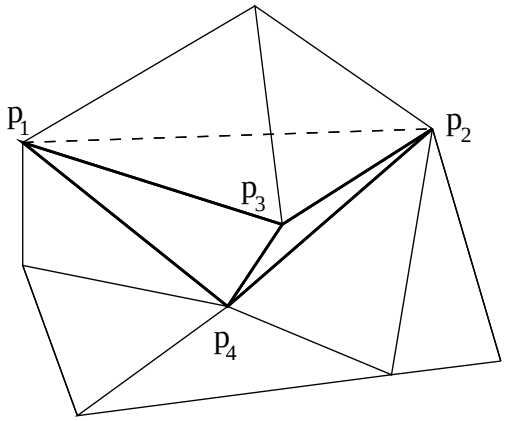

FIG. 4.4 – Schéma *Tetrahedral Volume Ratio* : encodage du parcours unique du maillage. Tous les volumes des tétraèdres sont rapportés à celui du tétraèdre initial (le premier dans le parcours du graphe). On insère l'information en modifiant les coordonnées des points des tétraèdres au numérateur (dans les rapports de volumes).

Une fois cet arbre construit, on se sert des arêtes qu'il définit pour référencer les tétraèdres et leur ordre de parcours. Pour retrouver le début du parcours canonique (global ou local), on procède par essais successifs jusqu'à trouver une séquence de synchronisation réputée connue. Dans le cas d'un arrangement local, les sous-parties du maillages sont définies par les branches de l'arbre de recouvrement des points que l'on utilise.

4.1.3 Arrangement indexé

Le schéma TSQ [56] est un des deux seuls exemples connus d'implantation d'un arrangement indexé avec [82] (nous réaliserons notre propre arrangement indexé au chapitre 5). Ce schéma s'appuie sur une configuration géométrique composée de quatre triangles, chaque configuration contenant deux bits d'information cachée. La capacité d'insertion est donc la moitié de celle du schéma précédent. L'insertion repose sur la modification de paires de rapports entre les bases des triangles et les hauteurs associées. La configuration est constituée d'un triangle, central, et de ses trois triangles adjacents. Le triangle central valide la présence

d'information cachée dans la configuration, un des trois triangles adjacents sert à coder le numéro du bit caché, et les deux derniers triangles codent l'information utile. Les auteurs ne précisent pas davantage comment ils codent géométriquement l'information, même si l'on peut supposer qu'ils cherchent à quantifier des rapports de grandeurs géométriques.

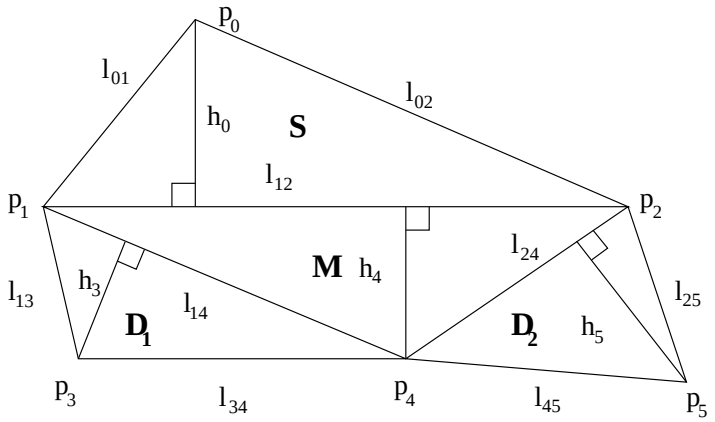

Fig. 4.5 – Schéma *Triangle Similarity Quadruple* : la configuration géométrique est composée de quatre triangles adjacents. Le triangle central valide la configuration comme porteuse d'information cachée. Le numéro du bit caché et deux valeurs indexées sur le numéro sont cachées dans les trois triangles restants.

4.2 Schémas sans configuration géométrique locale

Afin de s'affranchir de la contrainte de connexité à base de triangles, certains schémas de tatouage se basent sur des points uniquement. Les calculs de tatouage peuvent faire intervenir le voisinage local du sommet, mais la relecture ne nécessitera pas de retrouver des configurations géométriques locales dans lesquelles calculer des invariants. Ces schémas utilisent en général une référence à l'objet entier et se révèlent alors sensibles à l'attaque de coupe, bien que leur robustesse face à d'autres attaques plus complexes comme le remaillage ou la simplification soit élevée. Les deux premières approches présentées ici cherchent soit à modifier la courbure locale de l'objet, soit à modifier la distance des points au centre de masse de l'objet.

La troisième approche vise au contraire à renseigner l'utilisateur sur l'intégrité du maillage. Le marquage devra permettre de vérifier un certain calcul pour tous les sommets. On utilisera alors un autre espace non pour davantage de robustesse mais pour davantage de sécurité.

4.2.1 Schéma de Wagner

Ce schéma [79] insère l'information dans les valeurs relatives des normales locales en chaque sommet : il modifie donc la courbure locale de l'objet. Les normales locales sont

calculées ainsi :

$$n_i = \frac{1}{d_{p_i}} \sum_{v \in p_i^\star} (v - p_i). \tag{4.7}$$

On calcule la longueur moyenne de ces normales n_i sur l'ensemble du maillage :

$$d = \frac{1}{L} \sum_{i=0}^{L} \|n_i\|. \tag{4.8}$$

Et l'on quantifie les normales sur c/d niveaux, c étant une clef secrète. On définit alors le laplacien quantifié k_i par :

$$k_i = \left\lfloor \frac{c}{d} \|n_i\| \right\rfloor. \tag{4.9}$$

La marque est calculée à partir d'une fonction $f(p)$ continue définie sur la sphère unité. La marque f peut alors être un logo projeté sur la sphère unité, ou une séquence pseudo-aléatoire. De la même manière que ci-dessus, on quantifie la valeur que prend f dans chaque direction n_i en valeurs w_i :

$$w_i = \left\lfloor 2^b f(\frac{n_i}{\|n_i\|}) \right\rfloor, \tag{4.10}$$

où b est le nombre de bits servant à coder chaque w_i. L'insertion remplace b bits de k_i par ceux de w_i, on obtient alors les entiers k'_i. On calcule les vecteurs laplaciens modifiés :

$$n'_i = \frac{k'_i d}{c} \frac{n_i}{\|n_i\|}, \tag{4.11}$$

et on détermine les nouvelles coordonnées p'_i et v' des points qui satisfont les équations suivantes :

$$n'_i = \frac{1}{d_{p'_i}} \sum_{v' \in p_i^\star} (v' - p'_i). \tag{4.12}$$

Ce système de $L + 1$ équations est singulier : on ne peut reconstruire un objet uniquement à partir de ses normales locales. On laisse alors environ 20% des points inchangés. Puisque la majorité des points ont été modifiés, on doit calculer le nouveau paramètre global c' pour la relecture en fonction de la nouvelle moyenne d_n des normales locales modifiées :

$$c' = c \frac{d}{d_n} \tag{4.13}$$

Au lieu de la norme euclidienne classique, on peut choisir d'utiliser une autre norme, invariante par transformation affine, telle que décrite dans [55].
Pour la relecture, on cherche à retrouver la fonction f qui fait office de marque. Toutefois, l'auteur n'explique pas comment, même s'il l'affirme, il peut rendre son tatouage indécelable, ni avec quelle sécurité.

4.2.2 Schéma *Vertex Flood*

L'algorithme *Vertex Flood* [7, 8] repose sur une modification de la distance des points au centre de gravité de l'objet. On choisit une distance maximale D_{max} au centre de gravité de l'objet. L'intervalle $[0; D_{max}]$ est alors subdivisé en $m = 2^N$ intervalles : c'est l'espace de tatouage. Les sommets sont déplacés sur la droite passant par le centre de gravité et le sommet à tatouer, pour amener le sommet à la distance voulue du centre de gravité. On peut cacher plusieurs marques en sélectionnant différents sous-ensembles de points pour chacune d'entre elles. Toutefois, une coupe modifiant l'ensemble des points sur lesquels on calcule le centre de gravité, la marque est perdue par une coupe. En revanche, ce schéma s'adapte naturellement aux maillages quelconques (soupe de polygones, maillages non nécessairement conformes, dégénérescences, entre autres).

4.2.3 Schéma pour l'intégrité

Dans [82], Yeo et Yeung proposent une méthode permettant d'attester de l'intégrité de la position de chaque sommet. Comme souvent avec les schémas pour l'intégrité, il vaut mieux expliquer d'abord comment fonctionne le décodeur. Soit p_i un sommet dont on souhaite tester l'intégrité. On va chercher à générer deux valeurs à partir de p_i : l'index de *localisation* $L(p_i)$ et l'index de *valeur* $v(p_i)$. On utilise $L(p_i)$ pour fixer l'index du bit de la marque W que l'on est en train de relire. Un bit du tatouage est repéré par sa position dans un tableau grace à l'index de localisation, et l'index de valeur code effectivement sa valeur. Un sommet du maillage va coder un bit du tatouage. Parallèlement, une clef de vérification K, indexée par $v(p_i)$, permet d'attester que le sommet est intègre si :

$$K(v(p_i)) = W(L(p_i)) \tag{4.14}$$

Si les valeurs diffèrent, le sommet est déclaré non intègre. Le but du tatouage est ici de faire en sorte que tous les sommets soient intègres au regard de l'Eq. 4.14. Une mauvaise clef K conduira à déclarer seulement un sommet sur deux intègre en moyenne.

Nous commençons par expliquer comment calculer l'index de localisation. La marque W est ici une image binaire de taille 64×64. L'index de localisation $L(p_i)$ sera en réalité composé de deux index : $L_x(p_i)$ en abscisse et $L_y(p_i)$ en ordonnée. Pour les calculer, on commence par définir l'ensemble $\mathcal{N}(p_i)$ constitué de p_i et de ses voisins $p_j \in p_i^\star$ tels que $j < i$. On peut ainsi modifier les sommets dans l'ordre dans lequel ils sont énumérés sans risquer d'effacer ce qu'on vient d'écrire (problème de causalité). Il faut ensuite s'intéresser au barycentre s de p et de ses voisins :

$$s = \frac{1}{1 + d_p} \sum_{p_i \in p \cup p^\star} p_i. \tag{4.15}$$

Ensuite, muni d'une fonction q de normalisation et de quantification, on établit les index de localisation à l'aide de deux fonctions f_x et f_y :

$$L_x(p) = f_x(q(s_x), q(s_y), q(s_z)), \tag{4.16}$$

$$L_y(p) = f_y(q(s_x), q(s_y), q(s_z)), \tag{4.17}$$

où f_x et f_y servent à assigner un couple d'index à p (les auteurs semblent suggérer une combinaison des $q(s)$ modulo la taille de la marque). On effectue ainsi l'équivalent d'une paramétrisation du barycentre s.

Pour calculer l'index de valeur, on part de p et, conservant la fonction q, on a besoin de trois tables secrètes K_1, K_2 et K_3 combinées entre elles par un ou exclusif :

$$K(v(p)) = K_1(q(p_x)) \oplus K_2(q(p_y)) \oplus K_3(q(p_z)). \tag{4.18}$$

Ces tables mesurent 256 bits chacunes. Elles peuvent découler de séquences de bits issues d'un générateur pseudo-aléatoire pour plus de souplesse. Du point de vue de la sécurité, la taille de l'espace d'attaque exhaustive sera donc de $256 \times 256 \times 256 = 2^{24}$ clefs.

Enfin, le décodeur saura fournir la proportion c de sommets non intègres :

$$c = \frac{\#\{p|K(v(p)) \neq W(L(p))\}}{N}. \tag{4.19}$$

Si le maillage n'a subi aucune modification, on a naturellement $c = 1$.

Le but du tatouage est donc de perturber localement chaque sommet de manière à ce que l'Eq. 4.14 soit vérifiée en chacun d'eux. Pour insérer l'information, on choisit de perturber p en p' jusqu'à ce que $K(v(p'))$ prenne la valeur désirée. Mais il faut prêter spécialement attention au fait qu'en choisissant une telle stratégie on se doit de respecter un ordre sur le parcours des sommets qui soit le même au codeur et au décodeur. Dans [82], on utilise l'ordre de description des sommets dans le fichier représentant le maillage. C'est là le principal écueil de cette méthode, qui ne tolère donc aucune modification de la connexité, consisterait-elle seulement en une renumérotation des sommets.

Afin de perturber p en p', on met en œuvre un algorithme itératif. On choisit des pas de perturbation Δ_x, Δ_y et Δ_z que l'on incrémente doucement d'une itération à l'autre. Le début de l'exécution de l'algorithme est donné par :

$$\begin{aligned}
&p' \leftarrow (p_x + \Delta_x, p_y, p_z),\\
&p' \leftarrow (p_x - \Delta_x, p_y, p_z),\\
&p' \leftarrow (p_x, p_y + \Delta_y, p_z),\\
&p' \leftarrow (p_x, p_y - \Delta_y, p_z),\\
&p' \leftarrow (p_x, p_y, p_z + \Delta_z),\\
&p' \leftarrow (p_x, p_y, p_z - \Delta_z),\\
&p' \leftarrow (p_x + \Delta_x, p_y + \Delta_y, p_z),\\
&etc...
\end{aligned}$$

Après relecture de la marque, l'utilisateur dispose de la valeur c pour estimer l'ampleur des dégradations subies par le maillage. Eventuellement, on pourra faire aussi apparaître dans un visualiseur les sommets non intègres. Enfin, une solution à mi-chemin consiste à prendre un logo bien défini pour marque W. Si le maillage n'a subi aucune modification, l'image extraite sera parfaitement nette. A l'inverse, plus les modifications auront porté sur un nombre important de sommets, plus l'image W apparaîtra bruitée. Cette solution peut être envisagée si l'inspection visuelle en détails des sommets non intègres est trop coûteuse.

4.3 Autres espaces de représentation

Nous présentons ici deux schémas de tatouage qui utilisent un espace différent de représentation des données maillées 3D. Le premier tire parti de la décomposition spectrale, qui sera abordé au chapitre 6. Le deuxième se place dans la représentation multirésolution *Progressive meshes* due à Hoppe [37]. Nous présenterons encore un troisième schéma, spécifiquement destiné à la CAO, qui permet de tatouer des NURBS.

4.3.1 Schéma dans l'espace spectral de la géométrie

Comme nous le présenterons en détails au chapitre 6, on peut décomposer la géométrie du maillage sur une base de fonctions propres. On effectue la projection des trois vecteurs de coordonnées X, Y et Z pour obtenir leurs transformés P, Q et R. L'espace de projection est dit spectral, et les transformés P, Q et R sont composés de coefficients spectraux. Cet espace a pu être utilisé pour le tatouage [58]. Ce schéma propose une méthode additive d'insertion de la marque dans le domaine spectral de décomposition de la géométrie. Il nécessite une resynchronisation géométrique sur le modèle original préalable à la relecture (imposé par les propriétés de non-invariance en rotation de la décomposition spectrale). Par répétition du message c fois, on obtient la séquence b :

$$b_i = m_j \ \ , \ \ jc \leq i < (j+1)c. \tag{4.20}$$

Ensuite on vient moduler classiquement la séquence des b_i :

$$b'_i = \begin{cases} -1 & \text{si } b_i = 0 \\ 1 & \text{sinon.} \end{cases} \tag{4.21}$$

L'insertion se fait alors additivement dans l'espace transformé de la géométrie à l'aide d'une séquence pseudo-aléatoire s binaire à valeur dans $-1, 1$:

$$\begin{cases} P'_i = P_i + \alpha.b'_i.s_i \\ Q'_i = Q_i + \alpha.b'_i.s_i \\ R'_i = R_i + \alpha.b'_i.s_i, \end{cases} \tag{4.22}$$

où α représente la force d'insertion. L'extraction de la marque repose sur un alignement préalable entre le maillage tatoué et l'original. Cet alignement opéré, la décomposition spectrale du maillage dont on souhaite extraire la marque donne les coefficients $\hat{P}, \hat{Q}, \hat{R}$, et celle du maillage original les coefficients P, Q, R. On calcule ensuite la corrélation globale q_j :

$$q_j = \frac{1}{3} \sum_{X \in \{P,Q,R\}} \sum_{i=j.c}^{(j+1).c-1} (\hat{X}_i - X_i).s_i. \tag{4.23}$$

Pour obtenir la séquence estimée $\hat{b}'$, il suffit de tester le signe de chaque élément q_i :

$$\hat{b}'_i = signe(q_i). \tag{4.24}$$

La démodulation pour obtenir la séquence originale b est immédiate par inversion de 4.21.

Ce schéma a été utilisé pour insérer des messages de 32 bits avec une très bonne robustesse. Pour des raisons qui seront éclaircies au chapitre 6, la décomposition spectrale limite à 7000 sommets la taille des maillages que cette méthode peut traiter (en utilisant [68] pour le calcul des fonctions de base).

4.3.2 Espace d'analyse multirésolution des maillages

Il est possible de définir une analyse multirésolution des maillages [37]. Des schémas de tatouage ont été développés pour utiliser ces bases d'ondelettes [62].
Le message à cacher passe dans une fonction de hachage dont le résultat initialise un générateur pseudo-aléatoire. C'est cette séquence qui sera utilisée comme information utile. Elle est ensuite classiquement ajoutée de manière additive comme un bruit sur le signal décomposé sur les fonctions de base. On commence par construire un vecteur de tatouage w de taille L, utilisé pour perturber les fonctions de base B. Sous forme matricielle, l'insertion s'écrit :

$$\mathcal{V}' = \mathcal{V} + B \times w$$

où B est la matrice des fonctions de base de la transformée en ondelettes. Cette méthode nécessite un alignement préalable du maillage à contrôler sur le maillage original avant de pouvoir relire la marque, de manière non aveugle. Lorsque l'objet a été coupé, il est encore possible de récupérer une synchronisation par corrélation géométrique locale entre les deux objets. Plus généralement, il faut que les deux maillages à contrôler disposent de la même connexité. Si besoin est, on aura recours à un remaillage de l'objet. La marque $\hat{w}$ est estimée en résolvant le système de moindres carrés :

$$B \times \hat{w} = \mathcal{V}_{\mathcal{R}} - \mathcal{V},$$

où $\mathcal{V}_{\mathcal{R}}$ est la géométrie du maillage recalé sur l'original. Afin de tester la présence de la marque, on effectue une corrélation ρ de la marque estimée avec la marque originale :

$$\rho = \frac{\sum_{i\in[1,L]}(\hat{w}_i - \overline{\hat{w}})(w_i - \overline{w})}{\sqrt{\sum_{i\in[1,L]}(\hat{w}_i - \overline{\hat{w}})^2 \times \sum_{i\in[1,L]}(w_i - \overline{w})^2}},$$

où $\overline{x}$ représente la moyenne des éléments du vecteur x. La corrélation ρ est ensuite soumise à un test statistique pour garantir la présence de la marque. Les auteurs rapportent de très bons résultats en robustesse, principalement dus à un réalignement géométrique de bonne qualité sur l'original.

4.3.3 Espace des NURBS

Dans les domaines de la conception assistée par ordinateur, on préfère souvent manipuler des surfaces (ou leurs paramètres) que des maillages. On utilise généralement des NURBS (Non-Uniform Rational B-Splines) pour cela. Dans [57], on trouve plusieurs méthodes de tatouage dédiées à cet espace particulier de représentation des surfaces. Les méthodes varient en fonction des contraintes sur la forme et de celles pesant sur la discrétion de l'insertion. En effet, les surfaces fonctionnelles de l'objet ne tolèrent aucune altération, par contre on pourra jouer sur la forme dans le cas de surfaces libres. En outre, le tatouage peut induire une paramétrisation plus fine de l'objet, nécessitant l'insertion de points de contrôle qui peuvent paraître suspects à un éventuel attaquant. Nous montrons sur la Fig. 4.6 un exemple de spline reparamétrée en rajoutant des points de contrôle et en changeant la forme.

On procède par reparamétrisation des splines à l'aide d'une fonction rationnelle dont les termes du rapport sont linéaires. Le choix d'une telle fonction permet de garder le même

nombre de points de contrôle et n'alourdit pas l'objet par de l'information due au seul tatouage. Une telle reparamétrisation laisse un seul degré de liberté pour encoder l'information utile (sous contrainte de respecter les limites originales de l'espace paramétrique). On insère quelques bits dans la variation de ce seul paramètre. Cette méthode nécessite donc elle aussi le modèle original pour retrouver la marque. Afin de maximiser la capacité, on répète cette procédure sur toutes les surfaces élémentaires qui sont agencées dans un arbre.

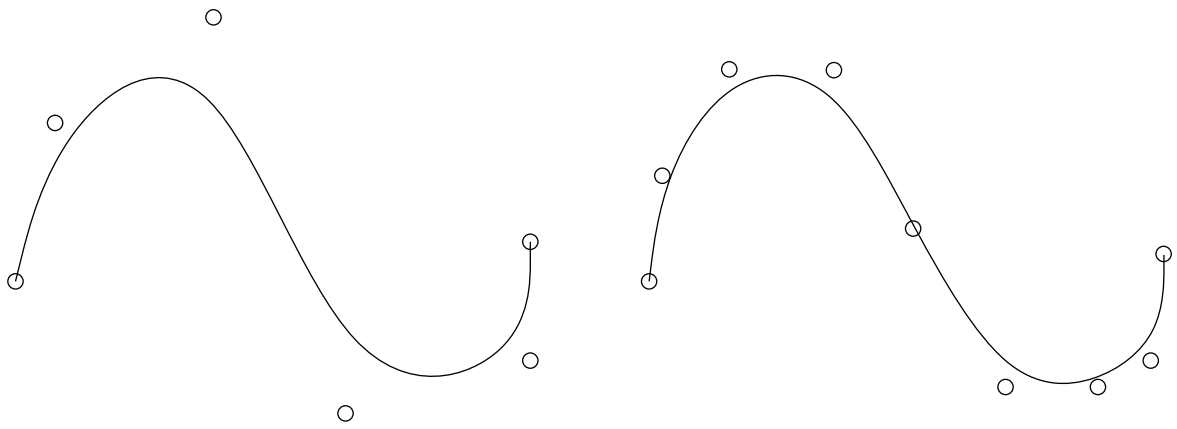

Fig. 4.6 – Tatouage d'une spline en rajoutant des points de contrôle. La forme est supposée libre et a été modifiée.

Une approche étendue permet de doubler la capacité. En effet, on peut étendre la reparamétrisation aux deux splines dont le produit tensoriel forme la surface de l'objet. L'insertion par reparamétrisation concerne alors les deux splines élémentaires, doublant ainsi la capacité.

4.4 Conclusion

La classification que nous avons établie introduit de fait une démarcation par la robustesse entre les différentes méthodes. En particulier, les schémas reposant sur la modification d'un invariant sont plutôt fragiles, et ne tolèrent pas de modification de la connexité, excepté dans le cas d'un arrangement indexé. Ils sont également assez sensibles au bruit. De ce fait, ils paraissent indiqués dans des applications de type authentification. Le chapitre 5 sera pour nous l'occasion de détailler notre approche du tatouage par invariant géométrique. Nous verrons que nous garantirons un certain nombre de spécifications usuelles en tatouage, qui ne sont pas souvent mentionnées ensemble dans la littérature. Nous serons en mesure de donner une probabilité de fausse alarme (ce que seul [62] propose), parce que nous montrerons comment accéder à tous les sites pouvant porter la marque (comme dans [82, 7, 57]), en mettant en place un arrangement indexé (ce qu'utilisent [56] et [82]). Enfin, nous estimerons nous aussi la taille de l'espace des clefs effectivement utilisables (ce que seul [82] garantit). Nous estimerons encore la taille de la plus petite surface protégée, ce qu'à notre connaissance aucune méthode ne mentionne. Enfin, nous expliquerons comment appliquer notre méthode à la stéganographie.

Concernant les autres représentations de l'information 3D des maillages (nous laissons de côté les NURBS), il faut noter qu'il s'agit de représentations autorisant la transmission progressive de la géométrie. Nous détaillerons au chapitre 6 le contexte dans lequel nous avons abordé le tatouage dans l'espace spectral de la géométrie. Nous avons choisi cette représentation car elle permet des analogies fortes avec la transformée de Fourier sur des surfaces régulièrement échantillonnées. Nous montrerons comment modifier l'algorithme de décomposition spectrale pour améliorer la qualité de la transmission progressive de la géométrie. Ce sera l'occasion de développer un codeur de source spectral pour la géométrie. Ce codeur nous permettra de tester notre méthode de tatouage spectral face au codage de source.

Contributions

Chapitre 5

Tatouage fragile par invariants géométriques

5.1 Motivations

On peut parfois lire dans la littérature que des algorithmes de tatouage qui modifient un invariant géométrique sont robustes. Cela n'est vrai que pour la classe de transformations autorisées. Une manipulation modifiant la connexité peut également effacer la marque : un remaillage par exemple suffit à lessiver tout à fait le maillage tatoué. Cette famille d'algorithmes ne peut donc pas être employée pour des applications de type protection des droits.

Par contre, le tatouage par invariant semble être un bon choix dans des applications de type authentification. En effet, on connaît exactement la classe de manipulations qui n'entraîneront pas le lessivage de la marque : les transformations affines, projectives, etc. Ainsi en cas de perte du tatouage, on pourra affirmer que s'est produite une manipulation non autorisée dessus. Eventuellement on redemandera la transmission de l'objet. On utilise alors un tatouage fragile, *conçu* pour s'effacer à la moindre manipulation non autorisée. Une telle technique trouverait son application naturelle dans l'authentification des maillages muséologiques ou biomédicaux.

C'est sous cet angle que nous avons abordé la conception d'une méthode de tatouage pour l'authentification. Nous utilisons pour ce faire une primitive géométrique d'insertion afin de cacher les valeurs des bits. Cette primitive possède plusieurs particularités qui la rendent particulièrement flexible. Nous commençons par définir notre primitive géométrique d'insertion de l'information cachée. Ensuite, nous validons notre primitive à l'aide d'un arrangement global/local de l'information (notre primitive sert à cacher les valeurs des bits, il faut donc que l'arrangement utilisé propose une numérotation implicite des bits). Nous aborderons alors la conception de l'algorithme de tatouage fragile pour l'authentification, fondé sur un arrangement indexé. Après avoir énoncé les contraintes (sur le parcours du graphe de connexité) liées à notre primitive munie d'un arrangement indexé, nous procèderons à une évaluation des performances brutes de l'arrangement indexé. Enfin, nous proposerons un parcours du graphe de connexité qui maximise le nombre de sites pour le tatouage effectivement atteints. Nous montrerons que notre parcours s'effectue en temps linéaire pour les surfaces de genre nul, sans y être limité. Nous serons alors en mesure de proposer une

modélisation statistique de la confiance dans le résultat issu du détecteur. Nous fixerons notamment une probabilité de fausse alarme de 10^{-7}, et nous discuterons le nombre de bits effectivement utilisés pour garantir l'invisibilité statistique de la marque. Les résultats préciserons les performances globales de l'algorithme, et permettront d'évaluer empiriquement la taille de la plus petite surface protégée (MWS dans la littérature, pour Minimum Watermark Segment). En effet, nous souhaitons pouvoir retrouver la marque même si le maillage a été coupé, et nous utilisons un arrangement indexé à dessein. Seul ce type d'arrangement permet de s'affranchir, du mieux possible, de l'attaque de coupe. Nous présenterons dans la section 5.2 une primitive géométrique permettant d'insérer un bit dans une configuration géométrique locale composée d'un seul triangle. Puis nous montrerons dans la section 5.3 comment lui adjoindre un arrangement indexé. Cette primitive géométrique impose une contrainte de causalité sur l'ordre de parcours des sommets, nous verrons dans la section 5.4 comment optimiser le nombre de sites en fonction de cette contrainte de causalité (nous retrouvons ici le même problème que dans [82] - mais nous utiliserons quant à nous l'arrangement indexé précisément dans le but de s'affranchir du problème causal *à la relecture*, et par là résister à la coupe). Dans la section 5.5, nous implanterons enfin une méthode de tatouage fragile que nous pourrons caractériser finement.

5.2 Une primitive géométrique d'insertion

Nous détaillons ici la manière dont nous codons l'information de la valeur des bits à cacher. Cette insertion prend la forme d'une procédure géométrique substitutive. Cette procédure géométrique d'insertion présente les deux avantages d'être flexible et de nécessiter un support compact. Afin d'*illustrer* les performances brutes de notre primitive géométrique d'insertion de la valeur des bits, nous utilisons un arrangement global puis local. Nous avons donc cherché à cacher quelques kilobits d'information dans une dizaine de maillages afin de vérifier la pertinence de notre stratégie d'insertion de la valeur des bits.

La procédure géométrique en question est fondée sur la manipulation d'un invariant géométrique autorisant la translation, la rotation et la mise à l'échelle uniforme. Nous choisissons de modifier le rapport des longueurs de deux segments situés sur la même droite. Cette modification a lieu dans le plan du triangle considéré. Nous schématisons cette procédure sur la Fig. 5.1.

5.2.1 Description

Le principe utilisé est le suivant : le côté de référence étant noté AB, on vient perturber la projection de C sur AB de manière à ce que la projection de C sur AB tombe dans le sous-espace binaire souhaité. Pour cela, il nous faut tout d'abord préciser la manière dont sont construits les sous-espaces binaires.

On commence tout d'abord par diviser le segment $[AB]$ en un nombre pair arbitraire de parties : ce nombre est appelé la *finesse* du tatouage. Ensuite, on associe à chaque partie un symbole binaire de tatouage “0” ou “1”, en alternant la succession des symboles de manière à minimiser le nombre de transitions entre les parties étiquetées “0” et “1” (voir Fig. 5.1) : on utilisera donc par exemple la séquence “01100110” plutôt que “01010101” qui comporte 3

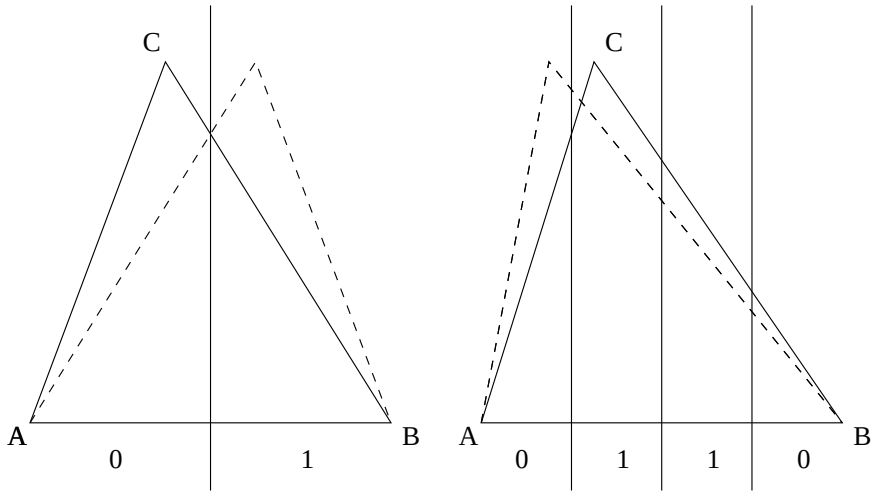

FIG. 5.1 – Procédure d'inscription de l'information cachée. La projection du point C sur la base AB du triangle sélectionne une zone "0" ou "1". Pour forcer la valeur du bit contenu dans un triangle, on effectue une simple symétrie par rapport au plan de symétrie le plus proche. A gauche : distorsion maximale, la configuration dégénère en une simple symétrie par rapport à la médiatrice de [AB]. A droite : distorsion deux fois moindre, le plan de symétrie est situé au quart de AB.

frontières de plus entre parties "0" et "1". La taille des parties est donc directement proportionnelle à la longueur du segment $[AB]$, et varie alors avec chaque triangle considéré. Cette partition du segment $[AB]$ est ensuite étendue à la droite (AB) par répétition, voir Fig. 5.2.

A présent, nous décrivons la manière dont nous tirons parti de cette partition pour insérer l'information à cacher. Nous considérons les plans 3D perpendiculaires à (AB) et passant par les points de la partition marquant une transition entre une zone étiquetée "0" et une zone étiquetée "1". Ces plans seront en réalité des plans de symétrie en fonction desquels nous déplacerons le point C. Ainsi, si la projection de C sur la droite (AB) tombe sur une partie étiquetée avec le symbole binaire à coder souhaité, nous ne faisons rien. Par contre, dans le cas où une modification du point C est nécessaire pour coder le symbole souhaité, nous procéderons à une symétrie par rapport au plan le plus proche. Nous donnons sur la Fig. 5.3 une simulation d'une telle procédure sur un maillage contenu dans le plan 2D.

Cette procédure géométrique permet donc de fixer la distorsion introduite, et de l'exprimer en fonction du nombre de parties souhaitées sur le segment $[AB]$: c'est la finesse. En outre, elle ne requiert qu'un seul triangle pour cacher un bit, elle utilise donc aussi peu de sommets que possible. Nous reproduisons sur la Fig. 5.4 l'évolution du plus grand déplacement requis pour cacher un bit en fonction du nombre de parties sur le segment $[AB]$. Comme l'on pouvait s'y attendre, l'évolution du plus grand déplacement est inversement proportionnelle à la finesse de la procédure.

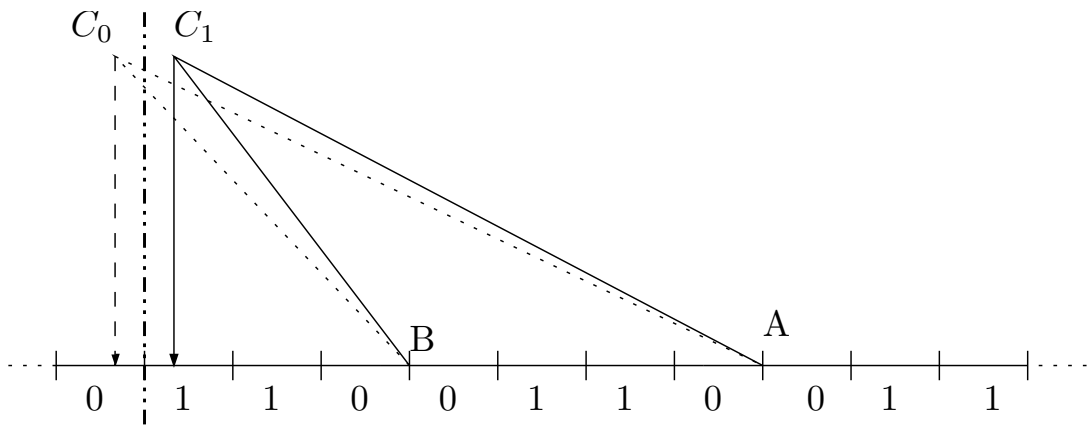

FIG. 5.2 – Répétition des sous-espaces binaires dédiés au codage de la valeur des bits.

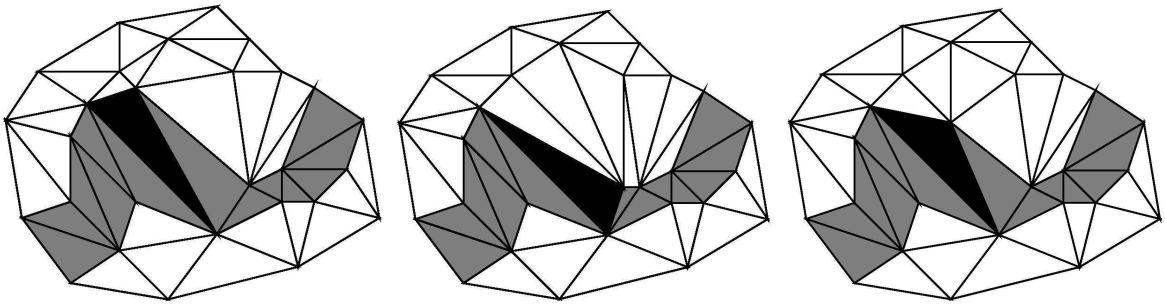

FIG. 5.3 – Simulations sur un maillage du plan 2D de la procédure géométrique d'insertion. Nous appliquons la procédure sur le triangle noir au centre du ruban gris. A gauche : le maillage original, le point C du triangle noir est celui situé le plus haut. Au centre : la partition de la procédure contient 2 parties, c'est la primitive la moins fine qui puisse être. A droite : la partition contient quatre parties, la distorsion introduite est un peu plus fine.

5.2.2 Remarques sur la sécurité

Nous discutons à présent la sécurité offerte par cette procédure géométrique d'insertion de la valeur. Un message bien caché est un message qui ne puisse pas même être seulement détecté. En tatouage substitutif, on vient en général caler une variable sur une valeur particulière, et l'espace dans lequel est calculé cette variable de tatouage est modulé par un secret. En ce qui concerne notre procédure géométrique, il faut remarquer qu'on ne vient pas caler une variable de tatouage (ici le point C) sur une valeur particulière, à considérer le tatouage comme une bijection entre un ensemble de valeurs particulières de la variable de tatouage, et celui des valeurs binaires qu'elles codent. Or, nous nous autorisons une plage de variation (continue par morceaux) déterminée par la finesse de la procédure : le sommet C peut être positionné n'importe où *pourvu* que sa projection sur AB tombe là où il faut. La marque enfouie par cette méthode est donc très probablement indétectable.

Tirant parti de ce degré de liberté supplémentaire, qui rend l'imperceptibilité computationnelle possible (en ne nécessitant pas de valeurs particulières de la variable de tatouage

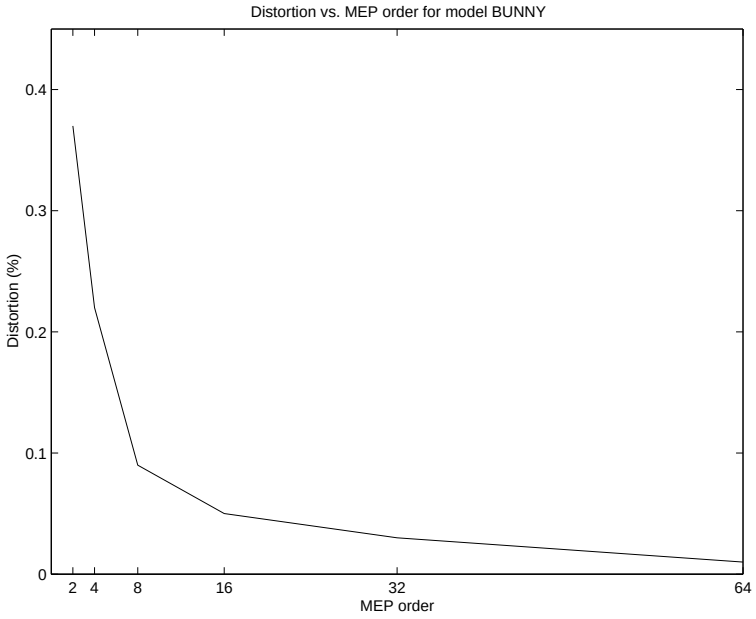

FIG. 5.4 – Evolution (par rapport à la longueur moyenne des arêtes du maillage) du plus grand déplacement de point causé par l'insertion d'information cachée en fonction de la finesse de subdivision de l'arête de référence AB (dénoté MEP order).

pour coder la valeur des bits), nous avons opté pour une simple symétrie. En effet, supposons un pirate qui souhaite retrouver la valeur des bits cachés : la première chose qu'il doit faire en examinant les triangles est de déterminer lequel des trois sommets est le point C. L'utilisation d'une symétrie ne fournit pas d'information au pirate pour détecter sur quel sommet a été appliquée la procédure géométrique. En conséquence, la sécurité de cette procédure d'inscription de la valeur des bits dépendra de la sécurité avec laquelle seront codés les *numéros* des bits, seule information permettant de reconstituer quels furent les sommets modifiés dans chaque triangle, et aussi dans quel *ordre*. C'est la raison pour laquelle nous avons souhaité donner un aperçu aussi précis que possible des différents types d'arrangement de l'information cachée que cette procédure autorise.

Ces remarques sont à la base de l'approche de la sécurité que nous avons eue dans ce travail : nous souhaitons conserver le plus longtemps possible cette imperceptilibité-là à notre avantage. Dans un premier temps, nous chercherons à mieux caractériser les performances de notre procédure d'insertion de la valeur des bits de tatouage. Nous utiliserons pour cela un arrangement global que nous rendrons facilement local, et qui nous permettra de simuler les conditions d'une application de type stéganographique. Et dans un deuxième temps, nous reviendrons à des idées plus communes en tatouage pour réaliser un arrangement indexé de notre procédure. Ce sera l'occasion de développer une méthode de tatouage fragile pour l'authentification. Dans ce dernier cas, nous serons amenés à proposer une évaluation, en nombre de bits, de la sécurité offerte par notre méthode de tatouage fragile, en ce qui concerne la *détection* d'un éventuel message caché (dont la présence ne pourra donc être trahie que par le codage des *numéros* des bits).

5.2.3 Parcours en ruban pour un arrangement global

Si, dans le cas de la stéganographie LSB[79] pour l'image, on cache l'information pixel à pixel, en balayant l'image ligne par ligne (ou colonne par colonne), on peut considérer ce balayage comme définissant un ruban de pixels pris les uns après les autres. C'est sur ce ruban que l'on vient déposer l'information à cacher, définissant implicitement l'ordre dans lequel les bits à cacher sont inscrits les uns après les autres.

Nous souhaitons donc reproduire cette idée dans le cas des maillages triangulés. Nous verrons comment contourner l'absence de parcours canonique sur un maillage arbitraire, et comment en tirer parti pour une plus grande sécurité. Mais avant, il faut définir un moyen de fixer ce qui sera le premier triangle du ruban.

Début et fin du ruban

Dans [7], plusieurs solutions sont proposées, consistant à réduire drastiquement l'espace des triangles possibles pour le choix du premier dans le ruban, quitte à procéder ensuite par essai/erreur, par exemple :

- choisir le triangle de plus petite (ou plus grande) aire
- choisir le triangle de plus petit (ou plus grand) périmètre
- choisir un triangle parmi ceux ayant le plus (ou le moins) de voisins (et procéder ensuite par essai/sélection)

Dans le cas où plusieurs triangles sont éligibles, on procèdera par essai/erreur. La sélection a alors lieu en cherchant à retrouver une séquence connue d'initialisation. Pour notre part, nous faisons en sorte de ne pouvoir conserver qu'un seul triangle pour le premier dans le ruban.

Rappelons que l'inscription de l'information cachée ne modifie pas la connexité des triangles du maillage, mais se greffe uniquement sur l'information de géométrie (les coordonnées cartésiennes). En outre, nous faisons l'hypothèse vraisemblable en stéganographie qu'aucune contrainte de robustesse ne pèse sur notre méthode : nous souhaitons uniquement illustrer, et deux interlocuteurs utilisant un tel canal stéganographique peuvent facilement s'arranger pour que l'objet ne subisse pas de distorsion (en attachement d'un mail par exemple) : le tout est qu'il continue d'avoir l'air d'un objet innocent, ce qui est aussi censé le protéger d'une certaine manière. Nous pouvons donc sélectionner pour premier triangle du ruban celui qui nous agrée le plus (par exemple le plus petit). Arbitrairement, nous choisissons de prendre le tout premier triangle décrit dans l'information de connexité.

Une fois le premier triangle dans le ruban trouvé, il faut fixer le terme du ruban. Pour cela, deux solutions sont généralement proposées : soit on identifie une séquence connue de sortie, et on s'arrête dans le parcours lorsqu'on retrouve cette séquence, soit on connait la quantité d'information cachée à retrouver, et on s'arrête lorsqu'on l'a atteinte. Dans le cas présent, nous supposerons connue une telle taille, et nous arrêterons de relire l'information cachée lorsque suffisamment de bits auront été décodés. Le but étant ici l'illustration des performances de la primitive géométrique ainsi que le détail de la mise en œuvre qu'elle implique, on pourra se contenter d'un nombre faible de bits cachés (quelques kilobits). Plus loin,

[79] La stéganographie LSB consiste à remplacer les trois ou quatre plans de bits de poids faible de l'image pour y cacher l'information.

nous ajouterons d'autres briques non moins essentielles comme un arrangement indexé, et un parcours optimal du graphe de connexité au regard d'une certaine contrainte de causalité sur le parcours (comme dans [82]).

Ruban et sécurité

A présent que les deux extrémités du ruban de triangles sont déterminées, il importe de savoir comment construire ce ruban. Nous fixons les deux exigences suivantes concernant ce ruban :

- il doit définir l'ordre implicite des bits d'information cachée,
- c'est sur lui que repose le secret de l'information cachée.

La première exigence découle de la transposition des techniques de stéganographie LSB dans le cas qui nous préoccupe, tandis que la seconde compose avec l'information arbitraire de connexité. Dans le cas de la stéganographie LSB, le pixel suivant dans le ruban de pixels est implicite, alors que dans le cas des maillages triangulés, deux choix sont possibles. Nous expliquons à présent pourquoi.

La nature d'un ruban consiste à établir une suite d'éléments ordonnés entre eux : pour chaque élément du ruban, on doit pouvoir déduire quel sera l'élément suivant. Dans le cas de la stéganographie LSB, cette déduction s'appuie uniquement sur la grille d'échantillonnage des pixels, la déduction est implicite. Dans le cas des triangles, il nous faut préciser ses attributs vis-à-vis de leur appartenance au ruban. Nous considérons un triangle comme ayant un *côté d'entrée*, et également un *côté de sortie*. Ainsi, si le côté d'entrée est connu, il reste deux possibilités pour le côté de sortie. Afin de fixer le côté de sortie pour chaque triangle dans le ruban, nous faisons appel à un générateur de nombres binaires pseudo-aléatoires.

Un triangle étant donné avec son côté d'entrée, un appel au générateur binaire pseudo-aléatoire déterminera lequel des deux autres côtés utiliser pour fixer le côté de sortie. Naturellement, nous avons besoin pour cela de fixer un sens d'orientation. Pour cela, nous nous appuyons sur l'orientation horaire autour de la normale au triangle. Ainsi, par rapport au côté d'entrée, nous savons parmi les deux côtés de sortie possibles lequel sera le premier, et lequel sera le second. Nous récapitulons cette manière de voir dans la Fig 5.5. Naturellement, le côté de sortie d'un triangle devient le côté d'entrée du prochain triangle dans le ruban, et on construit ainsi un ruban aussi long que l'objet le permet. Si un bord se présente, on détecte un triangle n'ayant alors qu'un seul côté possible de sortie, que nous empruntons sans incrémenter notre compteur de numéros de bits.

De cette manière, le ruban est parfaitement déterminé, et donc l'ordre dans lequel les bits sont cachés. En outre, puisque le choix du triangle suivant le ruban dépend d'un générateur pseudo-aléatoire, on est en mesure de garantir une sécurité accrue, puisque reposant sur les numéros de bits cachés. De plus, il suffit qu'un attaquant commette une seule erreur dans le choix du triangle suivant pour que tout le reste du ruban qu'il tente de constituer soit erronné. Bien entendu, afin de rendre la stéganalyse encore plus difficile, il est nécessaire de crypter l'information à cacher de manière à ce qu'un stéganalyste ne puisse s'aider de la sémantique de l'information cachée. Nous représentons sur la Fig 5.6 un ruban d'une capacité de 4Kbits sur le modèle *bunny*.

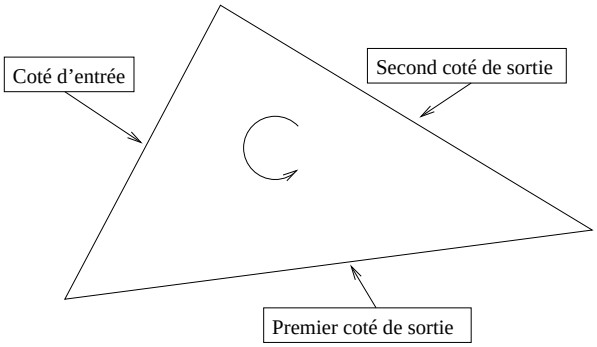

FIG. 5.5 – Comment déterminer le triangle suivant dans le ruban, étant donné le côté d'entrée ? L'ordre des deux côtés de sortie est déterminé par rapport à l'orientation de la normale au triangle. Sur la figure, la normale est dirigée vers le lecteur.

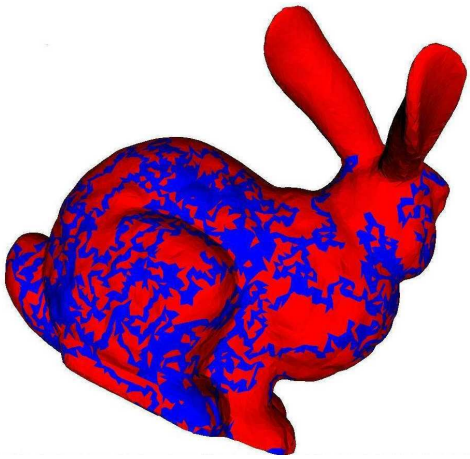

FIG. 5.6 – Exemple de ruban d'information cachée. Le ruban contient 4096 triangles, soit 4Kbits d'information cachée.

Implantation

La seule précaution à prendre désormais est de garantir que la sélection pseudo-aléatoire des triangles du ruban ne fasse pas en sorte qu'on vienne effacer ce que l'on a déjà écrit. Pour cela, il faut s'arranger pour qu'aucun point déjà dans le ruban ne puisse être modifié lors d'une itération ultérieure. Cela est possible de deux façons, voir Fig. 5.7 :

- Cas 1 : Tout d'abord, un sommet déjà tatoué lors de l'inscription d'un bit i pourrait à nouveau être candidat à un déplacement pour un bit $i + k$ si le parcours le ramenait en position d'être choisi. Le bit i serait alors potentiellement erroné après l'écriture du bit $i + k$,
- Cas 2 : Mais aussi un sommet ayant servi de base AB au tatouage du bit i pourrait être déplacé lors du tatouage du bit $i + k$. A la relecture le bit serait potentiellement erroné puisque la base servant au calcul de la projection de C sur AB serait modifiée.

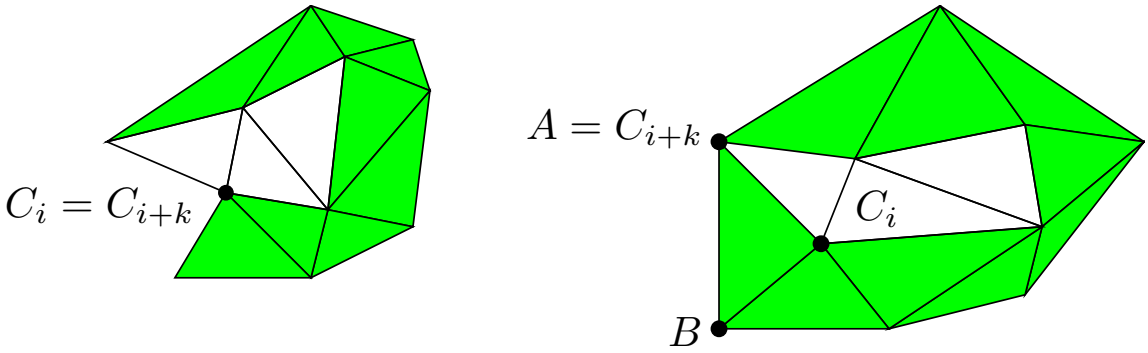

FIG. 5.7 – Les deux cas pouvant entrainer l'effacement du tatouage. A gauche : cas 1. A droite : cas 2.

Au fur et à mesure que l'on crée le ruban, on crée une liste des points interdits pour une future modification. Si un futur site nécessite de modifier les coordonnées d'un sommet déjà interdit, on le déclare invalide, et on poursuit la construction du ruban jusqu'à ce que l'on trouve un triangle valide. Chaque triangle valide pour l'insertion de données cachées voit son point C ajouté à la liste des points interdits : comme A et B appartenaient au triangle précédent, ils étaient invalidés auparavant et les trois sommets A, B et C sont dorénavant invalidés. De cette manière, tous les points du rubans sont interdits. Bien évidemment, on constitue la même liste à la relecture afin de garantir la synchronisation entre l'insertion et l'extraction. En procédant ainsi, la taille du ruban produit peut excéder la taille du message à cacher. Nous donnons ci-dessous le pseudo-code de l'algorithme :

```
Initialisation de l'arête initiale (marquer A et B interdits)

TantQue il existe encore un bit à écrire ou à relire
  Si C est un voisin non interdit de A et B
    Écrire ou relire la valeur du bit dans ABC
    Marquer C comme interdit
  Fin
Décider pseudo-aléatoirement si B ← C ou A ← C
FinTantQue
```

La remarque la plus importante est que si un sommet dans lequel on tente de cacher de l'information est déjà interdit, on passe au triangle suivant sans rien faire. Ainsi, la longueur du ruban peut très bien excèder, de beaucoup, la longueur en bits de la marque que l'on souhaite insérer. La différence est le nombre de triangle qu'il a fallu parcourir afin de trouver à nouveau un sommet non encore interdit.

Remarque sur la sécurité

Même munie d'un module de diffusion d'erreur, la stéganographie LSB de l'image 2D produit encore des distributions suspectes de niveaux de gris jusque dans les 3ème et 4ème plans de bits, rendant l'image suspecte de contenir de l'information cachée. La méthode de

stéganographie que nous évoquons, fondé sur un parcours *pseudo-aléatoire*, ne *peut* pas présenter ce genre de faille. En effet, comme discuté précédemment, la détectabilité du message caché repose uniquement sur l'information qu'un pirate pourrait trouver sur l'ordre des bits : l'insertion géométrique de la valeur des bits par symétrie n'aide en rien le pirate. Or, si l'on rend le parcours pseudo-aléatoire, guidé par une clef secrète, et que l'on choisit une finesse qui rende l'insertion imperceptible, il devient improbable de détecter la simple présence d'un message caché.

Avec une telle approche, nous ne voyons pas comment un stéganalyste pourrait seulement déterminer si un maillage contient de l'information cachée ou pas. En effet, ne pouvant déterminer quels sommets furent modifiés, et dans quel ordre, par la procédure géométrique, il n'aurait d'autre alternative que de tenter de reconstituer un éventuel parcours (nous raisonnons ici au pire des cas : avec un message caché non crypté. Le stéganalyste pourrait ainsi s'aider d'une éventuelle sémantique en clair pour faire progresser son étude. Il va de soit que le chiffrage du contenu à cacher prive le stéganalyste d'une telle ressource, et intervient comme toujours en *complément* des techniques de tatouage). Deux composantes rentrent dans la détermination du parcours :

- la clef secrète qui initialise le générateur pseudo-aléatoire guidant le parcours en ruban,
- l'arête initiale du ruban et le premier point à tatouer,

En général, la clef secrète mesure 64 bits. Enfin, le choix de l'arête initiale est fonction de la taille du maillage : en notant e le nombre d'arêtes du maillage, cette partie du parcours secret repose sur $1 + \lfloor \log_2(e) \rfloor$ bits. La longueur de clef utilisée pour déterminer le parcours secret du ruban est donc de $65 + \lfloor \log_2(e) \rfloor$ bits. Encore cette valeur repose-t-elle sur un raisonnement supposant que le cryptanalyste dispose d'une sémantique pour s'aider.

Remarque pratique

En reconsidérant notre procédure géométrique d'insertion de la valeur, il apparaît en pratique que si le point C est déjà très proche d'un plan de symétrie, on risque l'instabilité numérique dans les calculs. Ce cas se produit toutefois rarement. En l'état, nous détectons une exception de virgule flottante et annulons la procédure : le bit n'est pas inséré. Le parcours précédent, s'il devait servir à une application de stéganographie réelle et non à une évaluation de performances, devrait proposer une répétition de chaque bit afin de tenir compte de ces exceptions.

Toutefois, nous ne devons pas perdre de vue que l'objectif de notre propos est la création d'un algorithme de tatouage fragile, pour lequel ces quelques exceptions seront tolérables statistiquement. En conséquence, il n'est pas nécessaire de s'appesantir sur cet aspect, mais il se révèlera plus profitable (voir section 5.4) de bien dégager les caractéristiques du parcours en ruban.

Densité locale d'information

Dans le meilleur des cas, un triangle peut voir ses trois sommets contribuer à l'insertion de l'information cachée. Dans le pire des cas, aucun de ses sommets ne participe au tatouage. Entre les deux extrêmes, un triangle peut voir un ou deux de ses sommets coder de l'information. En effet, nous montrons sur la Fig. 5.8 comment il est possible que les trois sommets

d'un triangle codent tous des bits du tatouage. On a donc quatre degrés possibles de densité locale d'information, suivant le nombre de sommets d'un triangle qui codent effectivement de l'information cachée.

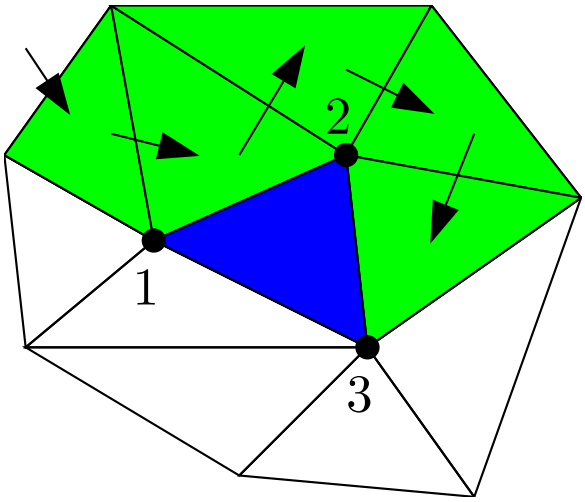

Fig. 5.8 – Exemple de parcours permettant au triangle central de voir ses trois sommets participer au codage de l'information cachée.

Nous donnons sur la Fig. 5.9 deux exemples de maillages sur lesquels un ruban d'information cachée a été inscrit : la densité locale d'information a également été peinte en différentes couleurs (quatre).

Le principal écueil de cette méthode est de ne pas pouvoir garantir le temps d'insertion du fait de la sélection pseudo-aléatoire des triangles dans le ruban, et de leur éventuelle admissibilité suivant que leur point C est déjà ou pas dans la liste de points interdits (le ruban en train de se construire). De fait, lorsque l'on cherche à cacher un nombre de bits proche du nombre de points dans le maillage, le temps de calcul explose car trouver aléatoirement un sommet non interdit devient de moins en moins fréquent au fur et à mesure que l'on a déjà caché de l'information. Nous proposons ci-dessous un moyen de corriger légèrement ce problème. En pratique, on ne peut pas atteindre la capacité maximale, mais on peut tout de même se servir d'environ 75% des points pour cacher de l'information, ce qui reste parfaitement suffisant pour les buts d'illustration que nous nous sommes fixés.

5.2.4 Un arrangement local

Une première manière de casser l'explosion du temps de recherche d'un sommet non encore interdit consiste à utiliser plusieurs rubans, avec bien entendu la même liste de points interdits pour tous. Cela revient en pratique à partitionner le maillage en sous-parties qui ne se recouvrent pas, au sens de l'insertion. Il s'agit donc d'un arrangement local. Nous choisissons de le mettre ici en œuvre essentiellement à des fins d'illustration. Nous verrons en section 5.4 une deuxième manière de parcourir le maillage en temps acceptable car linéaire. La chronologie de ces travaux a voulu que nous nous intéressions au parcours du graphe

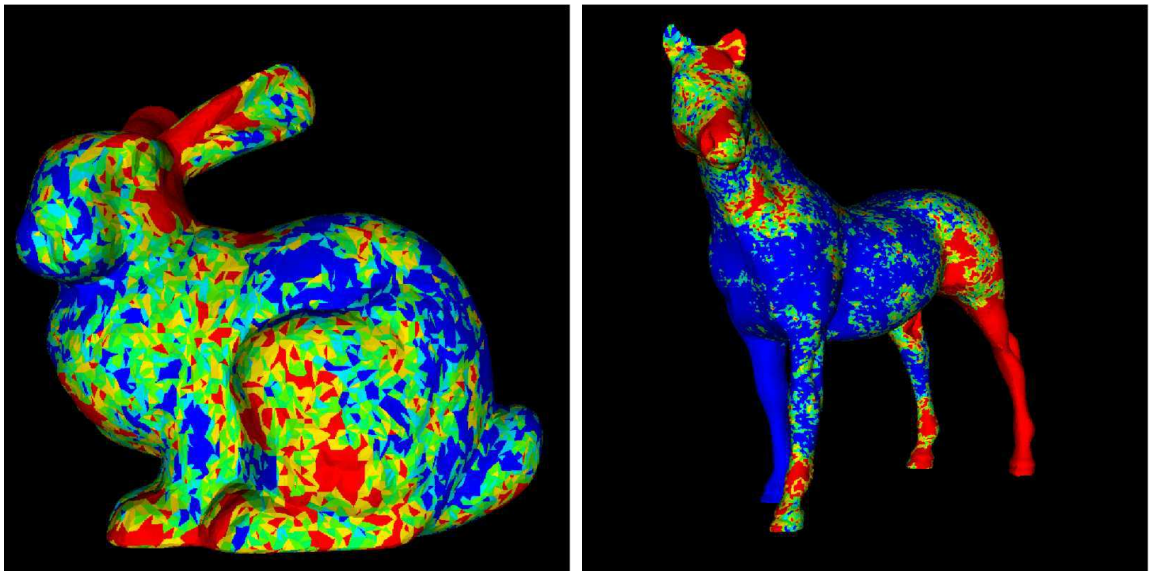

FIG. 5.9 – Maillage *bunny* contenant 12Kbits d'information cachée et maillage *horse* contenant 40Kbits d'information cachée. Chacune des quatre couleurs du ruban correspond au nombre de sommets du triangle utilisés pour coder des bits bleu=3 (saturées), vert= 2, jaune= 1, rouge= 0 (vides).

après avoir bien défini notre procédure géométrique, d'où l'utilisation de parcours naïfs pour l'illustration.

Stratégie

Nous procédons comme suit : lorsque nous détectons un trop grand nombre de triangles non admissibles à la suite, nous lançons un autre ruban sur le maillage, avec la même liste de points interdits. Cette liste matérialisera donc cette fois l'*ensemble* des rubans lancés sur le maillage. Expérimentalement, ce nombre limite de triangles a été fixé à 50. Cet ajustement ne permet pas de gagner en capacité, mais en temps de calcul. Nous représentons sur la Fig. 5.10 l'allure du temps de calcul nécessaire pour cacher 12Kbits d'information dans le modèle *bunny*.

Nous donnons sur la Fig. 5.11 le résultat de tests de capacité effectués sur onze maillages, et sur la Fig. 5.9, nous montrons deux des modèles après insertion de plusieurs Kbits d'information cachée.

Résultats et mesures

En pratique, nous avons donc utilisé un arrangement local pour cacher l'information. Nous définissons encore quelques mesures permettant de mieux appréhender le comportement de l'algorithme. On souhaite caractériser les performances de l'algorithme en termes de capacité et de distorsion, et pouvoir donner une idée de l'efficacité du codage dans le temps.

Pour caractériser les performances de capacité, nous proposons une borne supérieure.

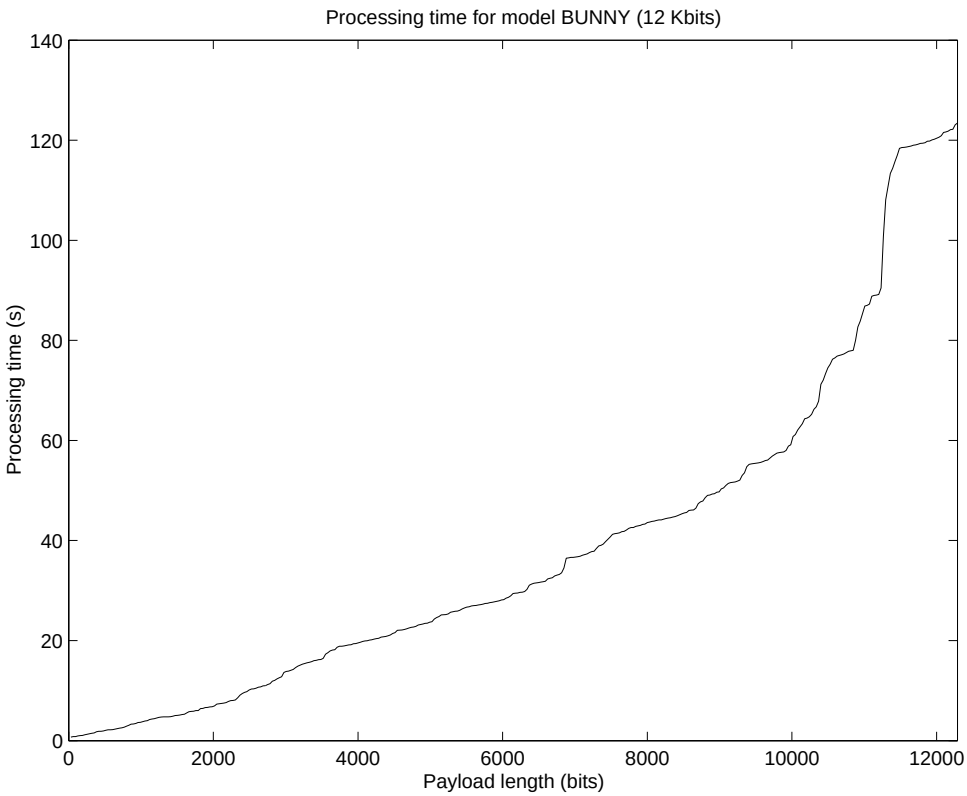

FIG. 5.10 – Temps de calcul (Pentium/800MHz) pour cacher 12Kbits dans le modèle *bunny*. Les discontinuités de la courbe correspondent au lancement d'un nouveau ruban sur le maillage. Un nouveau ruban est lancé chaque fois que 50 triangles non admissibles de suite sont visités.

Notre algorithme nécessitant de fixer les deux premiers points du ruban, ces deux points seulement ne pourront jamais être perturbés pour cacher de l'information. Si tous les sommets étaient atteignables, la capacité maximale théorique pour ce schéma serait donc de $N-2$ bits, car on vient cacher un bit dans chaque sommet libre. Toutefois, il s'agit d'une borne supérieure, jamais atteinte en pratique par un tel parcours simpliste (nous nous consacrerons par la suite à l'élaboration d'un parcours davantage adapté à notre primitive géométrique d'insertion). On quantifie le taux de remplissage du maillage par :

$$R_{capa} = \frac{N_{bits}}{N-2}, \tag{5.1}$$

où N_{bits} est le nombre de bits cachés. En pratique, nous avons procédé par sondage de la capacité pour savoir quelle quantité d'information nous pourrions cacher : nous avons cherché à cacher beaucoup car ainsi davantage de sommets contribuent à modifer le maillage, et l'évaluation de la procédure géométrique est d'autant plus valable. Nous présentons les résultats pour deux maillages à la topologie complexe (*skull* et *pelvis*, voir Fig. 5.11) : ce sont les objets les moins favorables car le ruban s'engouffre souvent dans une anse et peine à en ressortir. Nous avons arrêté le sondage de la capacité du canal lorsque le temps de calcul dépassait 3 minutes.

Dans le but de quantifier la distorsion introduite par le tatouage, nous avons choisi le rapport entre la plus grande perturbation due au tatouage (une distance d_{max}) et la moyenne des longueurs des arêtes du maillage l_{moy} :

$$R_{dist} = \frac{d_{max}}{l_{moy}}. \tag{5.2}$$

Enfin, nous voulons avoir une idée du chemin parcouru en trop. En effet, dans le meilleur des cas, il ne faudra parcourir que N_{bits} triangles pour trouver tous les sites nécessaire au codage. Or, l'aléa introduit dans le parcours fait que l'algorithme retombe sur des points invalidés car déjà porteurs d'information. Il faut donc faire un peu de chemin pour retomber sur des sites encore libres. Pour quantifier cela, nous mettons en rapport le nombre de triangles $N_{parcours}$ qu'il aura finalement fallu parcourir pour cacher toute l'information avec le nombre de bits cachés :

$$R_{cod} = \frac{N_{parcours}}{N_{bits}}. \tag{5.3}$$

Précisons que nous donnerons en section 5.4 un algorithme permettant un parcours optimal du maillage en $O(N)$. Nous donnons sur la tableau 5.11 les résultats des sondages de capacité de 11 maillages, avec les mesures introduites plus haut. On notera qu'il n'est pas rare d'obtenir des taux de remplissage voisinant les 80%. Cela se produit surtout sur les maillages avec une topologie simple, éventuellement avec bords.

Objet	N	R_{capa}	R_{cod}	R_{dist}	N_{bits} (Kbits)	Remarque
horse	48485	84.5%	6.5	0.15%	40	genre 0
bouddha	32328	79.2%	7.1	0.19%	25	trous
face	26460	77.4%	7.3	0.19%	20	1 bord
bunny	14007	87.7%	8.4	0.22%	12	1 bord
inopl	9831	83.3%	7.5	0.23%	8	1 bord
venus	8016	89.4%	8.1	0.22%	7	genre 0
hand	6650	61.6%	6.3	0.21%	4	genre 0
woman	7723	53.0%	6.2	0.23%	4	genre 0
anttoon	7082	57.8%	5.9	0.18%	4	genre 2
skull	11051	37.1%	7.8	0.24%	4	genre élevé, trous
pelvis	4189	48.9%	7.6	0.25%	2	genre élevé, trous

FIG. 5.11 – Résultats obtenus sur onze maillages en stéganographie avec arrangement local avec une finesse de 32.

Nous avons encore vérifié que les bits sont correctement relus après une rotation, une translation ou une mise à l'échelle uniforme. En effet, c'étaient les classes de transformation auxquelles notre primitive était censée résister en raison de l'invariant géométrique manipulé.

Conclusion

Nous avons donc validé notre primitive géométrique d'insertion de la valeur des bits à cacher, au moyen d'une méthode simple de stéganographie pour les maillages surfaciques

3D triangulés orientables. Cette méthode présente les avantages d'être robuste face à la rotation, la translation et la mise à l'échelle uniforme, et d'introduire le secret dans le numéro des bits cachés. Par contre, elle a l'inconvénient de nécessiter un sondage préalable de la capacité du canal stéganographique. Ce problème sera résolu dans la section 5.4. Au moins cet inconvénient met-il l'accent sur une problématique que nous aborderons plus loin lors de la conception d'un parcours adapté.

5.3 Arrangement indexé pour le tatouage fragile

A des fins d'authentification des maillages, nous avons souhaité développer une méthode de tatouage fragile basée sur la procédure géométrique décrite plus haut. La procédure géométrique fournit un certain nombre d'invariances, mais nous souhaitons pouvoir récupérer la marque y compris sur des extraits de maillage. Ainsi, nous souhaitons une robustesse face aux opérations suivantes :

- translation
- rotation
- mise à l'échelle uniforme
- coupe

Si l'invariant géométrique retenu pour notre procédure d'insertion offre naturellement la robustesse face aux trois premières opérations, il reste à mettre en oeuvre une stratégie particulière afin de s'affranchir autant que possible de la coupe. Pour cela, nous avons mis en œuvre un arrangement indexé.

5.3.1 Surcoût de codage

Nous rappelons que nous voulons cacher 64 bits (leur numéro et leur valeur). L'utilisation d'un arrangement indexé entraine donc un surcoût de codage, dû aux numéros. Si l'on veut cacher C_{utile} bits, il faudra en réalité en inscrire :

$$C_{total} = C_{utile} \times (1 + \log_2(C_{utile})), \tag{5.4}$$

sur le maillage. Dans toute la suite de ce travail, et pour conserver le point de vue généralement admis, nous continuerons de parler de capacité *utile* : lorsque nous cacherons 64 bits utiles, il faudra garder à l'esprit qu'en réalité il aura fallu en inscrire 448.

Enfin, il est une autre information à inscrire, qui ne représente pas la marque mais qui valide une configuration géométrique comme tatouée. En effet, il faut savoir reconnaître un site tatoué en tant que tel avant de chercher à y décoder quoi que ce soit. Nous verrons comment ce problème trouve naturellement sa solution.

5.3.2 Stratégie pour le choix d'un autre invariant

Nous nous proposons donc de coder à présent aussi les numéros des bits par la manipulation d'un invariant géométrique. La manipulation de cet invariant devra être plus fine que celle proposée pour le codage de la valeur des bits : on cherche ici à cacher les $\log_2(C_{utile})$ bits

qui coderont leur numéro. Ainsi, nous pouvons représenter sur la Fig. 5.12 l'allure des surfaces isovaleurs (pour les numéros) de quelques invariants. Nous n'avons souhaité considérer que des invariants pouvant être calculés dans un seul triangle.

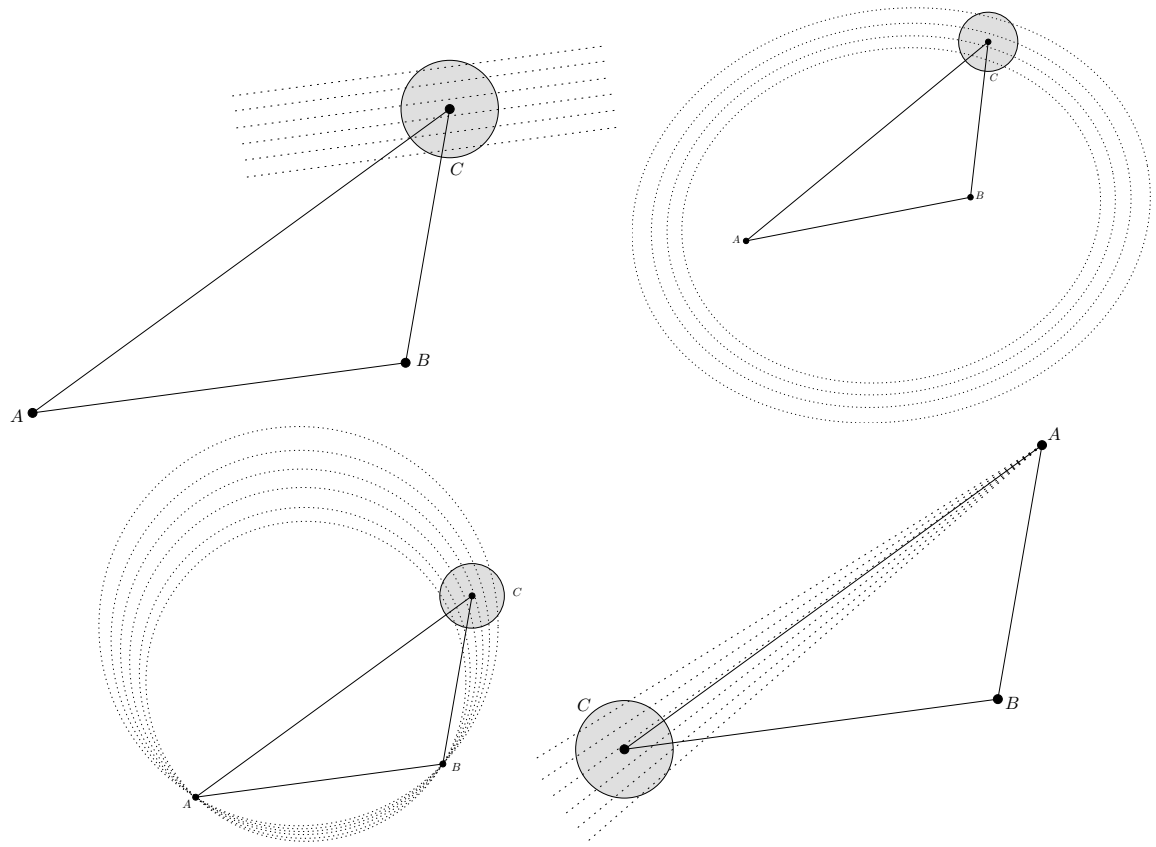

FIG. 5.12 – Allure des isovaleurs en tatouage suivant la modification de trois invariants. En haut à gauche : en modifiant l'aire en jouant sur la hauteur. En haut à droite : en modifiant le périmètre. En bas : en modifiant l'angle de valeur médiane (à gauche s'il est en C, à droite s'il est en A). Nous avons choisi de modifier des rapports d'aires (en haut à gauche).

Enfin, il faut remarquer que la procédure géométrique d'insertion de la valeur du bit modifie le point à perturber *parallèlement* aux deux points de référence de la base du triangle. Ainsi, si nous trouvons une autre procédure qui perturbe le point dans le plan *perpendiculaire* à la base du triangle et contenant le sommet à modifier, nous disposons d'un autre degré de liberté dans le codage. Manifestement, le premier invariant de la Fig. 5.12, fondé sur la manipulation de l'aire, convient parfaitement : il autorise une manipulation géométrique pour l'insertion du numéro *indépendante* de celle dédiée à l'insertion de la valeur du bit. Il s'agit en quelque sorte d'un codage CDMA (Code Division Multiple Access) géométrique de l'information.

5.3.3 Codage des numéros des bits par invariant

L'invariant que nous avons retenu est le rapport des aires de deux polygones. Les deux polygones qui nous intéressent sont le triangle (ABC) (d'aire S), et le carré imaginaire ayant $[AB]$ pour côté. Notre second invariant est donc : $\frac{AB^2}{S}$. En modifiant la hauteur du triangle (ABC) dans un plan perpendiculaire à (AB), on ne change pas l'aire du carré imaginaire, et seule l'aire du triangle s'en trouve modifiée (voir Fig. 5.13). Soit H la hauteur s'appuyant sur (AB), on utilise la relation triviale :

$$H \times AB = 2 \times S. \tag{5.5}$$

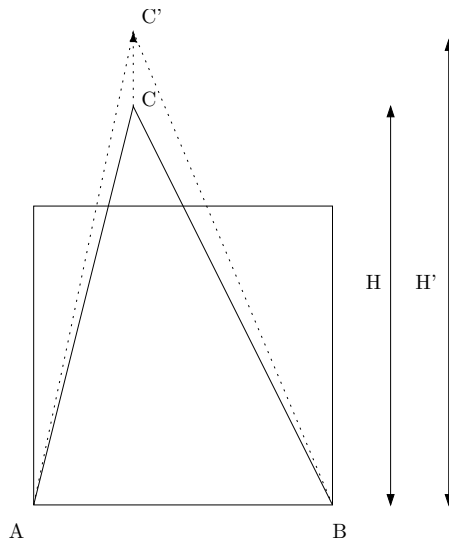

FIG. 5.13 – L'invariant utilisé pour coder le numéro des bits du message : le rapport de l'aire du carré imaginaire de côté $[AB]$ sur l'aire du triangle ABC. En modifiant la hauteur du triangle issue de $[AB]$, on ajuste l'aire du triangle sans toucher à celle du carré.

C'est donc en réalité en modifiant la hauteur du triangle s'appuyant sur AB que l'on vient perturber l'invariant $\frac{AB^2}{S}$.

Modulation secrète de l'invariant

La primitive géométrique d'insertion de la valeur ne cale pas le point C à modifier sur une valeur précise : une large plage de variation correspondant à la finesse utilisée est admise. Or, en procédant par symétrie, on ne vient pas introduire de perturbation statistique. Par contre, lorsque nous utilisons un arrangement indexé, il faut comme nous l'avons mentionné plus haut, pouvoir identifier un site tatoué comme tel.

S'il est facile à un pirate de trouver les sites tatoués, il tentera probablement ensuite d'obtenir une bonne approximation de la clef. Afin de cacher l'information de validité d'un site comme tatoué à un éventuel attaquant, nous modulons secrètement l'espace dans lequel la décision a lieu. Nous évaluerons plus loin la sécurité qu'offre ce procédé.

Soit K une clef codée sur N_K bits servant à paramétrer le processus d'insertion. Cette clef est composée par concaténation de deux clefs K_1 et K_2 codées respectivement sur N_{K_1} et N_{K_2} bits. On a également besoin de deux paramètres internes T_1 et T_2 dont nous verrons plus loin comment leur valeur a été fixée (dans la section 5.5.3). La modulation secrète en question associe une grandeur g_{ABC} au triangle (ABC) :

$$g_{ABC} = \left(T_1 + \frac{K_1}{2^{N_{K_1}}}\right)^{\left(T_2 + \frac{K_2}{2^{N_{K_2}}}\right)} \times \frac{AB^2}{S}. \tag{5.6}$$

La clef K sert à paramétrer secrètement l'étape d'écriture du numéro du bit dans le triangle. Ainsi, si le message caché contient C_{utile} bits, le numéro n du bit contenu dans le triangle est donné par :

$$n = \lfloor g_{ABC} \rfloor \% C_{utile}, \tag{5.7}$$

où % représente l'opérateur modulo.

Marquage d'un triangle comme tatoué

Pour autant, la nouvelle valeur de $g_{ABC'}$ lors de l'insertion n'est toujours pas fixée exactement. Pour lever l'indétermination, nous choisissons de faire coder à g_{ABC} l'information de validité d'un site tatoué. Un triangle sera déclaré porteur d'information cachée si g_{ABC} est placée sur l'échelle des entiers en modifiant la hauteur H telle que :

$$|g_{ABC} - \frac{1}{2} - \lfloor g_{ABC} \rfloor| < \epsilon. \tag{5.8}$$

Nous retrouvons ici un procédé classique en tatouage substitutif : caler une valeur sur la médiane d'un intervalle. En général, on procède ainsi pour augmenter la robustesse du schéma de tatouage face à la quantification. Mais même si nous pouvons éventuellement tirer parti d'une telle stratégie en terme de robustesse, il faut reconnaître que nous cherchons uniquement à marquer un triangle comme tatoué.

5.3.4 Validation de l'approche par arrangement indexé

Nous souhaitons vérifier ici la pertinence de l'arrangement indexé. Nous rappelons qu'un tel arrangement doit permettre de retrouver la marque en décodant les triangles dans n'importe quel ordre. Pour cela, chaque triangle est positionné de telle manière que AB soit son plus petit côté, ceci afin de faciliter la relecture en ne réclamant pas d'examiner les trois permutations circulaires possibles pour le choix de A, B et C. Lors de l'insertion, chaque triangle tatoué voit ses points interdits, afin de pallier les risques d'effacement de la Fig. 5.7.

A la relecture, nous énumérons encore les triangles un par un, les positionnons sur leur base de référence (AB est le côté le plus court), et si le triangle est reconnu porteur d'information on décode le contenu du bit caché (numéro et valeur). Comme on ne peut garantir le nombre de sites tatoués dès l'insertion (pour modéliser le comportement statistique du détecteur), il faut se résigner à adopter un processus de décision à la majorité pour le décodeur.

Robustesse face à l'attaque de coupe

Nous avons mis en œuvre un arrangement indexé précisément dans le but de nous affranchir de l'attaque de coupe. C'est donc face à une telle attaque de coupe que nous avons évalué les performances de l'arrangement indexé : nous avons fait varier le nombre de triangles disponibles pour la relecture et avons noté en fonction la proportion de bits correctement relus. Les résultats portent sur une moyenne de trois maillages. Il faut donc près de 40% des triangles pour espérer relire la marque. C'est encore très insuffisant - nous ferons mieux par la suite (section 5.4) - mais cela démontre la validité de l'approche par arrangement indexé. Pour la détection, nous avons requis un rapport minimum de trois des deux occurences avec lesquelles les valeurs binaires ont été détectées (rapport entre la plus grande et la plus petite occurence) pour chaque numéro.

La prochaine section concerne l'élaboration d'un parcours maximisant le nombre de sites atteints, et permettant de bien meilleures performances face à l'attaque de coupe. Mais avant, il nous faut examiner en quoi notre façon de passer en revue les triangles un par un à l'insertion est contre-productive en terme de répétition de l'information cachée.

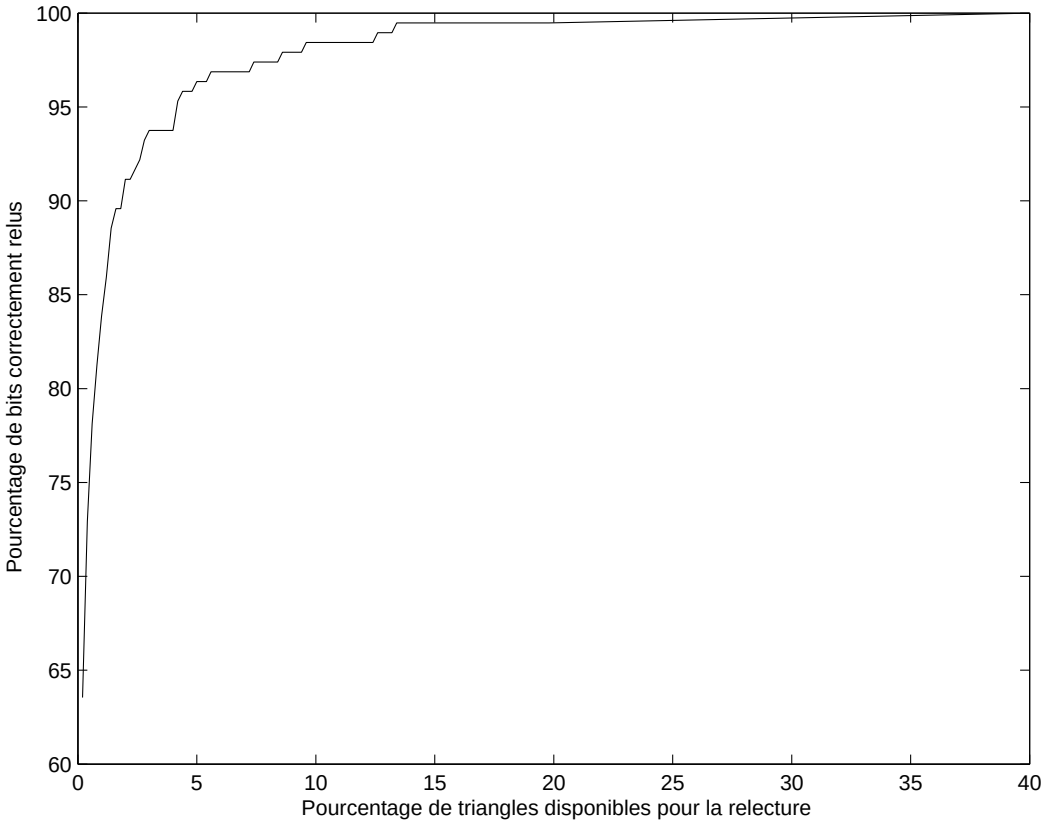

Fig. 5.14 – Attaque de coupe avec un parcours naïf du maillage : 40% du maillage original est requis afin de détecter correctement la marque.

Localisation de l'information cachée

Nous montrons sur la Fig. 5.15 la répartition des sites tatoués lorsque les triangles sont naïvement passés en revue les uns après les autres. En particulier, on constate que la surface contient encore de nombreuses zones non tatouées.

Cette mauvaise utilisation de la surface a deux origines :

- *Le passage en revue des triangles un par un à l'insertion* : en n'utilisant pas l'information de connexité pour se déplacer, nous n'optimisons pas le nombre de sites atteints. Dans la section suivante, nous développerons un parcours adapté fondé sur la croissance d'une liste active,
- *La convention qui fait de AB le plus petit côté d'un triangle* : pour faciliter la relecture, nous avons introduit une convention qui se révèle contre-productive car elle fait peser une contrainte de plus sur l'admissibilité des sites. Dans la section suivante, nous abandonnerons cette convention : le temps de relecture sera multiplié par trois (pour tester les trois permutations circulaires sur A, B et C), mais de par la nature de l'arrangement indexé, restera linéaire en nombre de triangles.

Fig. 5.15 – Répartition de l'information cachée lorsque l'on cherche les sites en énumérant les triangles un par un. Les triangles en vert sont porteurs d'information cachée, les triangles rouges ne codent pas d'information cachée. Le maillage contient encore une importante surface ne contenant pas d'information cachée. En outre, le nombre de sites utilisés est imprévisible.

5.4 Optimisation du nombre de sites

Nous nous consacrons à présent à l'élaboration d'un parcours optimal du maillage, au sens du nombre de sites atteints pour le tatouage. C'est ce parcours qui nous permettra de construire les autres éléments d'un schéma de tatouage fragile, comme une modélisation statistique de la confiance dans la sortie du détecteur. Comme nous venons de l'évoquer, nous abandonnons la contrainte qui demande que AB soit le plus petit côté du triangle (le temps de calcul restant linéaire) pour bénéficier d'un degré de liberté supplémentaire dans la diffusion de la marque.

A cette fin, nous rappelons que la seule contrainte pesant sur notre méthode d'insertion concerne la causalité : il faut s'assurer de ne jamais venir réécrire là où l'on a déjà écrit, et éviter les causes d'effacement qui sont exposées en Fig. 5.7. Le schéma de Yeo et Yeung [82] partage cette contrainte d'un parcours spécial respectant la causalité (les auteurs n'utilisent pas l'arrangement indexé pour s'affranchir de la coupe, et doivent donc, contrairement à nous, reproduire le même parcours à l'insertion et à la relecture). C'est pour cette raison que nous utilisons un jeu d'étiquettes pour marquer les sommets interdits. L'idée dont nous nous inspirons est tirée de la méthode de compression statique de Touma et Gotsman [73] (section 3.1.2). Le parcours de leur graphe de connexité est implicite, comme nous l'avons vu précédemment, et repose sur la croissance d'une région modélisée par une liste d'arêtes formant un cycle (plusieurs cycles dans le cas de surface avec genre non nul).

Nous allons présenter un parcours fondé sur la croissance d'une liste active de sommets (dont les arêtes qui les relient forment également un cycle). Nous montrerons qu'à chaque itération, on dispose d'un sommet admissible pour l'insertion. Enfin, nous donnerons le nombre de sites atteints par l'algorithme, dont nous prouverons qu'il tourne en temps linéaire sur des surfaces de genre nul, sans y être limité.

5.4.1 Algorithme

Nous exposons ici un algorithme permettant d'atteindre tous les sites possibles du maillage au regard de notre procédure géométrique d'insertion. Un point traversé (ou conquis) devient toujours *interdit*, mais nous devons encore initialiser l'algorithme en interdisant les deux sommets de la première arête choisie arbitrairement. Un triangle dont tous les sommets sont interdits est dit *tatoué*. Nous verrons qu'à proprement parler, l'implantation que nous discutons dans les résultats ne permet pas de cacher de l'information dans chacun des triangles (notre réflexion se fonde sur les sommets). Cela est dû à notre procédure géométrique, mais il n'en reste pas moins que le parcours que nous présentons ouvre tout de même la voie au tatouage de *tous* les triangles - et c'est pourquoi nous conservons cette appellation de triangle tatoué. Soient A et B les deux sommets de l'arête initiale dont on fait l'embryon de notre "liste active".

```
Initialisation de l'arête initiale (marquer A et B interdits)

TantQue il existe un point non interdit
  Si ABC est un triangle orienté de S tel que
       A et B soient interdits, mais pas C
    Insérer l'information dans ABC
    Marquer C comme interdit
  Fin
FinTantQue
```

On ne peut exprimer plus simplement la contrainte de causalité de la procédure géométrique d'insertion : dans tout triangle ABC candidat à l'insertion, il faut un point non interdit (C) et il faut, afin de maximiser le nombre de sites, que les deux autres (A et B) soient déja interdits.

5.4.2 Preuve de terminaison

Notre algorithme contient une boucle `TantQue`. Nous devons donc nous assurer qu'il termine bien. S'il termine, c'est que tous les points auront pu servir à cacher de l'information, sauf les deux premiers sommets de l'arête initiale. Nous apportons ici la preuve que notre algorithme atteint exactement $N - 2$ sites valides pour l'insertion.

Lemme

Tant qu'il existe des sommets libres, à chaque itération de l'algorithme on trouve un triangle valide pour l'insertion, c'est-à-dire avec deux points interdits et un point libre (non interdit).

Preuve

Soit q un point libre n'appartenant pas à un triangle avec deux points interdits (voir Fig. 5.16). On peut alors trouver un chemin menant de q à un point déjà interdit (avant la première itération, les deux points de l'arête initiale sont déjà interdits).

Ce chemin possède nécessairement (au moins) une arête avec un sommet interdit, q'', et l'autre encore libre, q'. En tournant autour de q'', on crée un autre chemin qui contient nécessairement un autre point interdit r, car un point n'est interdit que *par rapport à deux voisins déjà interdits*, et un point encore libre s (éventuellement $s = q'$).

Le triangle dans lequel cacher l'information est donc $sq''r$, avec s dans le rôle du sommet non interdit.

Implantation

Afin d'accélérer la recherche du triangle dans lequel insérer l'information, on maintient à jour la liste des sommets appartenant à (au moins) un triangle avec ses deux autres points interdits. On procède comme suit : lorsqu'un point est sur le point d'être interdit, on parcourt la liste de tous les triangles incidents et on détecte ceux pour lesquels un seul sommet est

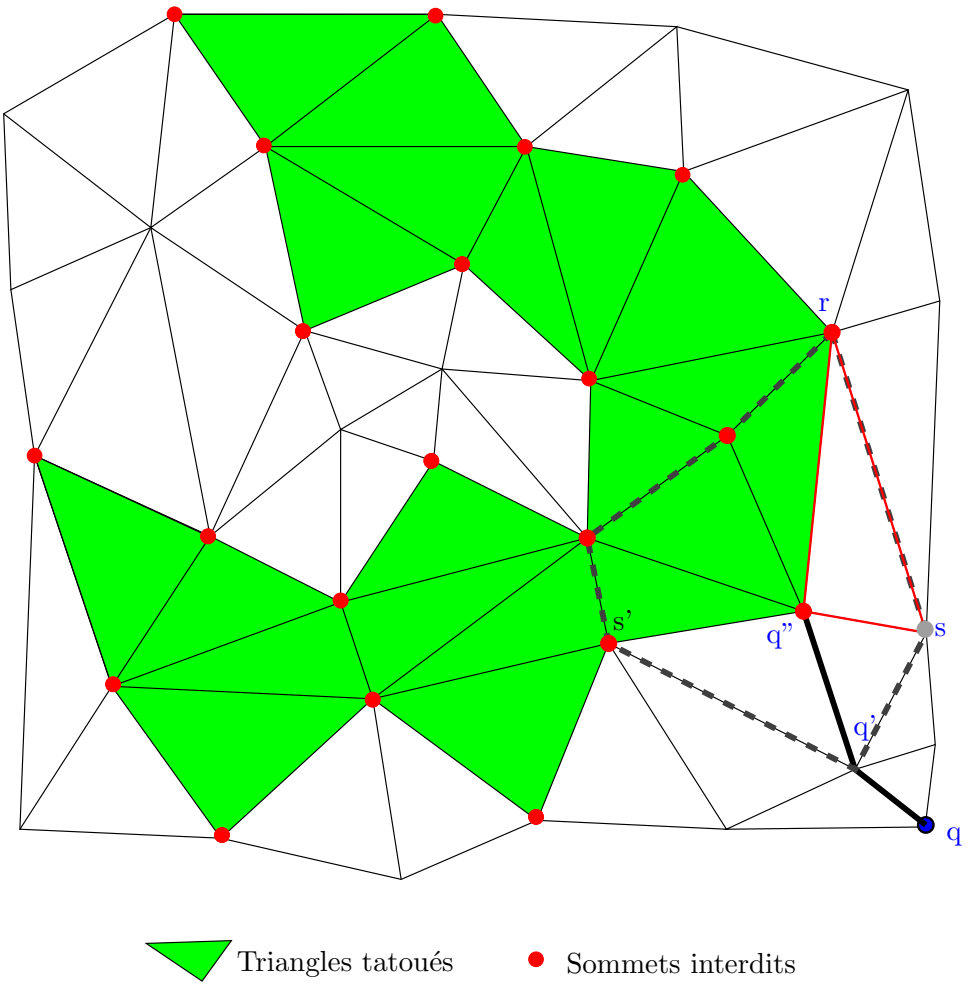

FIG. 5.16 – A chaque itération, on peut trouver un triangle valide pour l'insertion. Le chemin menant de q à q'' est représenté en gras. Le chemin (ici un cycle) autour de q'' est en pointillés. Au moins une arête (rs) sur ce chemin contient un sommet interdit (r) et l'autre libre (s). On marque alors l'information dans le site $sq''r$.

encore libre. Ce sommet est alors placé dans la liste. Nous retrouvons ici l'idée ancienne de la "liste active" que Touma et Gotsman ont utilisée [73].

Complexité

L'algorithme, du point de vue de la complexité, est en réalité constitué d'une boucle `Pour` (puisque chaque itération de la boucle `TantQue` interdit un sommet et que tous les sommets deviennent interdits), et d'une boucle imbriquée itérant sur toutes les arêtes adjacentes au sommet en cours de traitement. La complexité est donc la somme des valences de tous les points, ce qui est moins que $6N$ (par relation d'Euler). Notre algorithme permettant de maximiser le nombre de sites a donc une complexité linéaire en nombre de sommets.

5.4.3 Discussion

Regardons à présent un peu plus attentivement notre algorithme. Lorsque nous interdisons un point p, c'est relativement aux deux seuls points précédemment interdits q et r avec lesquels il forme un triangle.

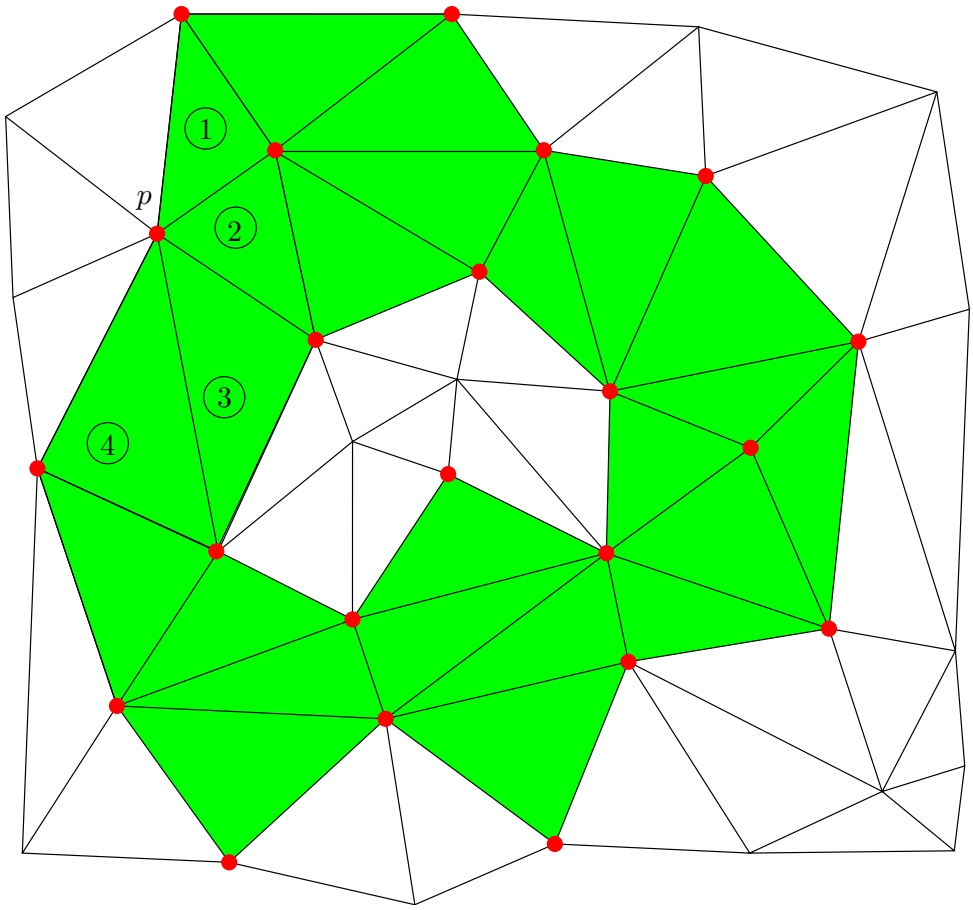

FIG. 5.17 – Nombre de sites : par rapport à l'itération de la Fig. 5.16, le sommet p ci-dessus permet de marquer en réalité plusieurs triangles (ici quatre).

Si l'on regarde la Fig. 5.16, en imaginant que l'algorithme soit au début de l'itération suivant celle ayant vu l'interdiction de s, et que le point q' soit tiré de la "liste active", il est effectivement valide au regard du triangle $q'q''s$, mais également au regard du triangle $q'q''s'$.

Ce qui revient à dire qu'à chaque fois que nous interdisons un point par rapport à *un seul* triangle, nous perdons en réalité substantiellement au regard de tous les triangles qui pourraient alors être utilisés pour coder un bit. Ainsi, le nombre de sites atteignables passerait-il tout simplement de $N-2$ à f (le nombre de triangles dans le maillage), et on sait par relation d'Euler que l'on a $f \simeq 2N$.

Mais pour cela, il nous faut sans doute une procédure d'insertion différente de celle que nous avons développée. En effet, il s'agit maintenant d'affiner la position d'un point par rapport à plusieurs triangles parmi ceux qui lui sont adjacents. La méthode d'insertion que

nous avons présentée a l'avantage certain d'être déterministe, mais si on voulait coder un bit dans chaque triangle, il faudrait procéder par perturbation des sommets (en partant par exemple d'un schéma à la Yeo et Yeung [82]). Le temps de calcul ne serait plus garanti.

Par contre, en marquant tous les triangles, on ne serait plus obligé de marquer aussi le fait qu'un site est tatoué : cette distinction n'aurait plus lieu d'être puisque tous le seraient. On se souvient que le marquage de cette information permettait également (implicitement) de retrouver la bonne orientation du triangle lors de l'insertion : quel sommet avait été potentiellement modifié. C'est pour cette raison qu'en l'état, notre procédure géométrique ne nous permet pas de marquer de l'information dans tous les triangles (seulement dans $N-2$ sommets), alors que notre parcours du graphe de connexité nous l'autorise pourtant.

Toutefois, nous risquons une piste pour tourner cette nouvelle difficulté. Puisqu'on ne pourrait plus se servir de l'information d'orientation du triangle à l'insertion, il faudrait privilégier une sorte plus spécifique d'invariants : les invariants "invariants par permutation circulaire" des sommets lors du calcul. Par exemple, le rapport de l'aire sur le périmètre élevé au carré est un tel invariant. Notre stratégie de CDMA géométrique aurait vécu, car il faudrait concaténer le numéro du bit et sa valeur associée, et cacher ce message dans un site. Notons qu'il reste en théorie possible d'organiser une imperceptibilité computationnelle (ou calculatoire) en marquant tous les triangles : il suffit que chaque sommet se trouve dans un volume, et non sur une position particulière. Notre nouvel algorithme s'écrit alors :

```
Initialisation de l'arête initiale (marquer A et B comme interdits)

TantQue il existe un point non interdit
  Si ABC est un triangle orienté de S tel que
       A et B soient interdits, mais pas C
    Trouver T l'ensemble des triangles tels que
       C est leur dernier point à interdire
    Insérer l'information dans chaque triangle de T
      en perturbant C
    Marquer C comme interdit
  Fin
FinTantQue
```

Nous n'avons pas souhaité nous consacrer à ce problème pour deux raisons :

- L'équirépartition des bits du message caché n'est plus garantie ;
- L'insertion devient un problème d'optimisation géométrique.

En effet, il n'est déjà pas acquis que l'intersection de volumes valides pour l'insertion existe, mais la trouver revient à proposer des ensembles {numéro de bit, valeur de bit} valides, et à choisir le moins mauvais au regard de l'équirépartition des bits du tatouage. Nous risquerions bien de défaire ce que nous avions voulu faire si nous persistions dans cette voie. Aussi nous faut-il nous restreindre à notre borne de $N-2$ sites atteints.

Du point de vue de la sécurité d'une application de type stéganographie, il faut souligner qu'il pourrait être utile de se servir de toute la capacité (mettre les f triangles de $\mathcal{S}$ à profit, ou un maximum d'entre eux, plutôt que les seuls $N-2$ sommets), afin que personne ne puisse développer de version "améliorée", libérant ainsi environ N bits supplémentaires (par

relation d'Euler) pour l'évasion discrète d'une clef secrète par exemple. La même remarque, en stéganographie LSB pour l'image revient à fixer une valeur sur *toute* la dynamique admissible en un pixel (sinon il resterait quelques bits non employés qu'un développeur malintentionné ou un tant soit peu malin pourrait mettre à profit).

5.5 Application au tatouage fragile

A présent, nous avons toutes les briques nécessaires au développement d'un algorithme de tatouage fragile. Nous allons utiliser une procédure géométrique de finesse 64, supportée par un arrangement indexé et un parcours optimal : nous pouvons déjà garantir que nous résisterons à la translation, la rotation et la mise à l'échelle, ainsi qu'à la coupe. Nous pouvons encore garantir le nombre de sites utilisés ($N - 2$). Jointe à notre équirépartition des bits de la marque, il devient possible de procéder à une modélisation statistique de la confiance dans la détection. Puis, sous cette contrainte, nous serons en mesure d'évaluer la taille de la plus petite surface protégée, ainsi que celle de la clef K utilisée pour brouiller les numéros des bits.

5.5.1 Contrôle de la distorsion

Au minimum, une méthode de tatouage doit permettre de régler l'ampleur de la distorsion introduite dans le média hôte. Au mieux, elle se doit de s'y adapter. Dans le domaine des surfaces, aucun modèle psycho-visuel de perception n'a encore vu le jour. Il faudra donc nous contenter de limiter la distorsion introduite : nous la contraindrons à rester dans un disque de rayon δ_{adm}, voir Fig. 5.18. On rappelle que tous les manipulations ont lieu dans le *plan* du triangle. Nous avons fixé δ_{adm} en fonction de la diagonale de la boîte englobante de l'objet d_{bbox} :

$$\delta_{adm} = 10^{-3} \times d_{bbox}. \tag{5.9}$$

On pourrait encore imaginer de contraindre la distorsion introduite à l'intérieur d'une ellipse dont les axes principaux seraient les vecteurs du champ local de courbure (rendant ainsi possible l'adaptation *de facto* aux objets de CAO, sans doute au prix d'une baisse drastique du nombre de sites car les contraintes fonctionnelles de l'objet enlèveront des degrés de liberté). Toutefois, notre stratégie simpliste permet de bien illustrer les idées que nous développons dans ce travail, et nous les appliquerons dans nos exemples à des maillages muséologiques.

5.5.2 Détection

Nous souhaitons pouvoir donner, comme seulement Praun [62] et Benedens [9] l'ont fait, une indication de la confiance dans la détection. Pour cela, nous modélisons notre méthode du point de vue statistique de la manière suivante : on va s'intéresser, pour chaque numéro de bit, à la différence signée e_{01} entre le nombre de uns relus, et celui des zéros, dans l'ordre : le signe de e_{01} est important. En effet, comme nous pouvons garantir le nombre de sites utilisés pour le tatouage, nous pouvons procéder à une modélisation statistique plus fine pour le détecteur que celle à la majorité, simpliste, que nous avons employée plus haut.

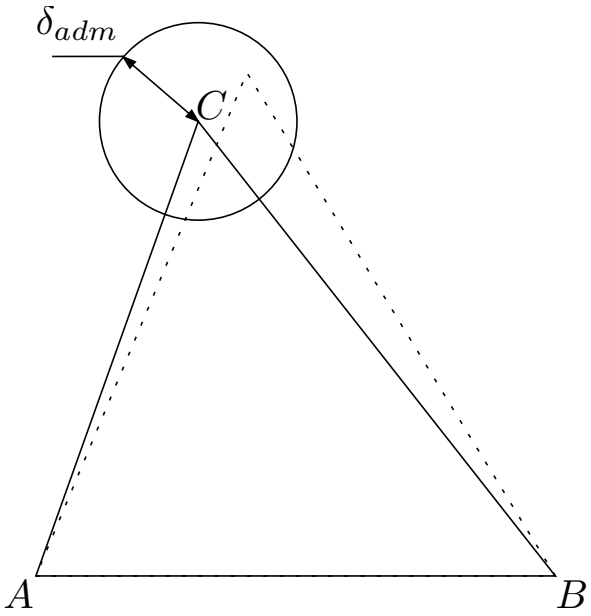

FIG. 5.18 – Contrôle a minima de la distorsion introduite : elle est contrainte de rester dans une boule de rayon δ_{adm}.

Si un maillage n'est pas tatoué avec la clef K présentée lors de la relecture, alors la distribution des e_{01} sera centrée autour de zéro. A l'inverse, si la clef K présentée est celle ayant servi à l'insertion, alors on aura, pour chaque e_{01}, soit $e_{01} << -1$ (si l'on a tatoué un 0), soit $e_{01} >> 1$ (si l'on a tatoué un 1). Nous avons donc besoin d'une distribution de référence indiquant ce qu'est statistiquement un maillage non tatoué avec K.

Distribution de référence

Nous adoptons le cadre classique en tatouage qui consiste à modéliser le canal caché par une loi gaussienne. Avant d'en estimer les paramètres, il faut disposer d'échantillons représentatifs d'une loi gaussienne non perturbée par le tatouage associé à la clef K. Deux solutions permettent de générer facilement ces échantillons :

- Soit on utilise d'autres clefs secrètes,
- Soit on va tester les valeurs des bits avec K dans un espace de numéro non tatoué

La première solution présente l'inconvénient de devoir réserver des clefs à cet usage, et de les maintenir secrètes (sinon on pourrait tenter une optimisation face à *ces* clefs-là seulement). La seconde solution, que nous avons employée, n'utilise que la clef K. On se souvient qu'un site est déclaré tatoué si :

$$|g_{ABC} - \frac{1}{2} - \lfloor g_{ABC} \rfloor| < \epsilon. \tag{5.10}$$

Ainsi, l'insertion du numéro du bit n'a fait que centrer la distribution des valeurs de tatouage autour de $\frac{1}{2}$. Si nous examinons les distributions détectées autour d'autres valeurs, on obtiendra autant d'échantillons que l'on voudra représentatifs du maillage non tatoué avec K. Nous avons pris nos échantillons autour des 8 valeurs suivantes : 0.1, 0.2, 0.3, 0.4,

0.6, 0.7, 0.8 et 0.9, avec le même ϵ. Nous reproduisons sur la Fig. 5.19 une telle distribution, pour laquelle on a tracé, après estimation des paramètres, la loi normale associée. On vient ainsi relire, à chaque valeur testée, des bits dans un espace dont on sait qu'il n'est pas tatoué.

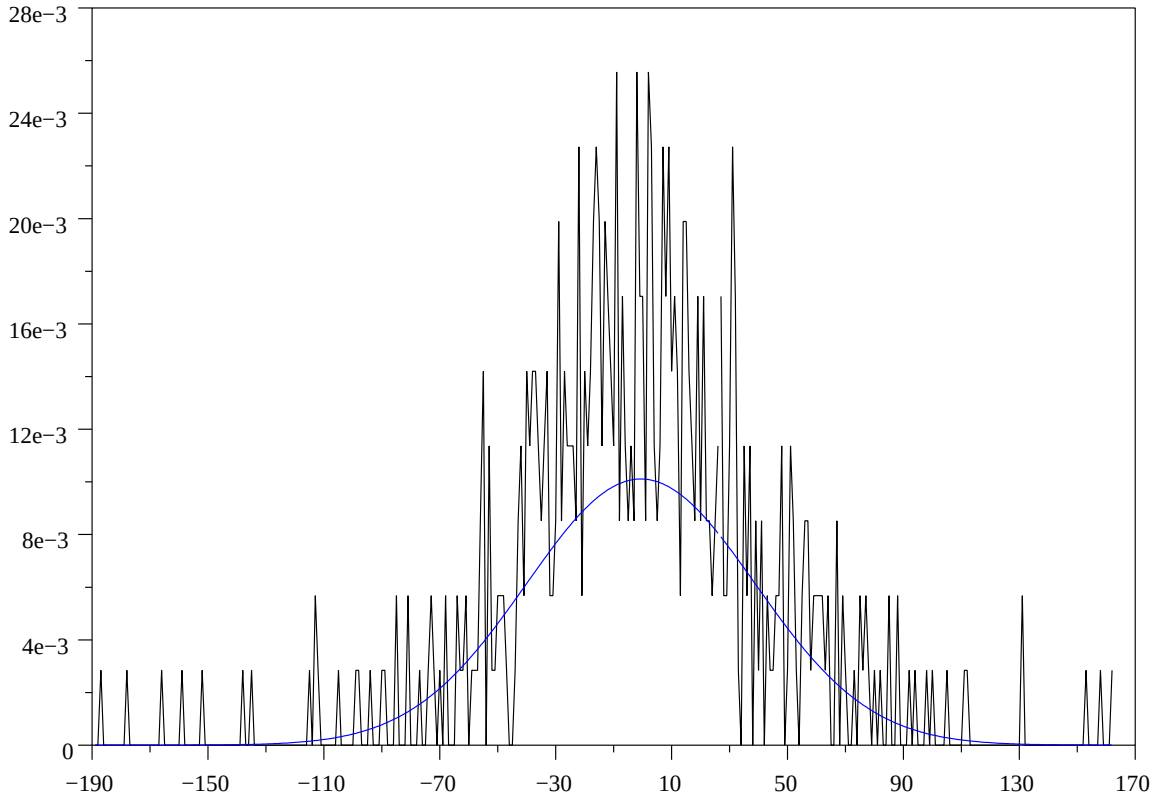

FIG. 5.19 – Distribution de référence des différences signées e_{01} des valeurs des bits. On a mesuré $8 \times 64 = 512$ différences e_{01} (8 valeurs de tests 0.1, 0.2, 0.3, etc. pour chacun des 64 numéros de bits). On modélise ainsi l'écart normal entre le nombre de 1 et de 0 relus sur un maillage non tatoué avec K. Le maillage d'exemple comporte 45906 sommets (BigHead_2). La distribution est centrée près de zéro : on trouve environ autant de un que de zéros sur un maillage non tatoué avec K.

Seuil de fausse alarme

Nous donnons sur la Fig. 5.20 l'allure de la distribution des différences des valeurs des bits pour un tatouage ne contenant que des "1" (les valeurs des différences signées sont toutes positives). Une telle distribution indique que pour un maillage tatoué avec K, la distribution des e_{01} pour chaque numéro est très fortement perturbée par le tatouage. En particulier,

on peut tester la déviation de chacun des e_{01} (pour chaque numéro de bit) par rapport à la distribution de référence, et fixer en conséquence un seuil paramétré par une probabilité de fausse alarme P_{fa}. Nous avons fixé $P_{fa} = 10^{-7}$ pour notre implantation. Nous en avons déduit un seuil de 3.7665 pour la loi $\mathcal{N}(0,1)$, en pratique le seuil est fixé à $3.7665 \times (\mu + \sigma)$ où μ et σ sont les paramètres estimés de la loi normale de référence.

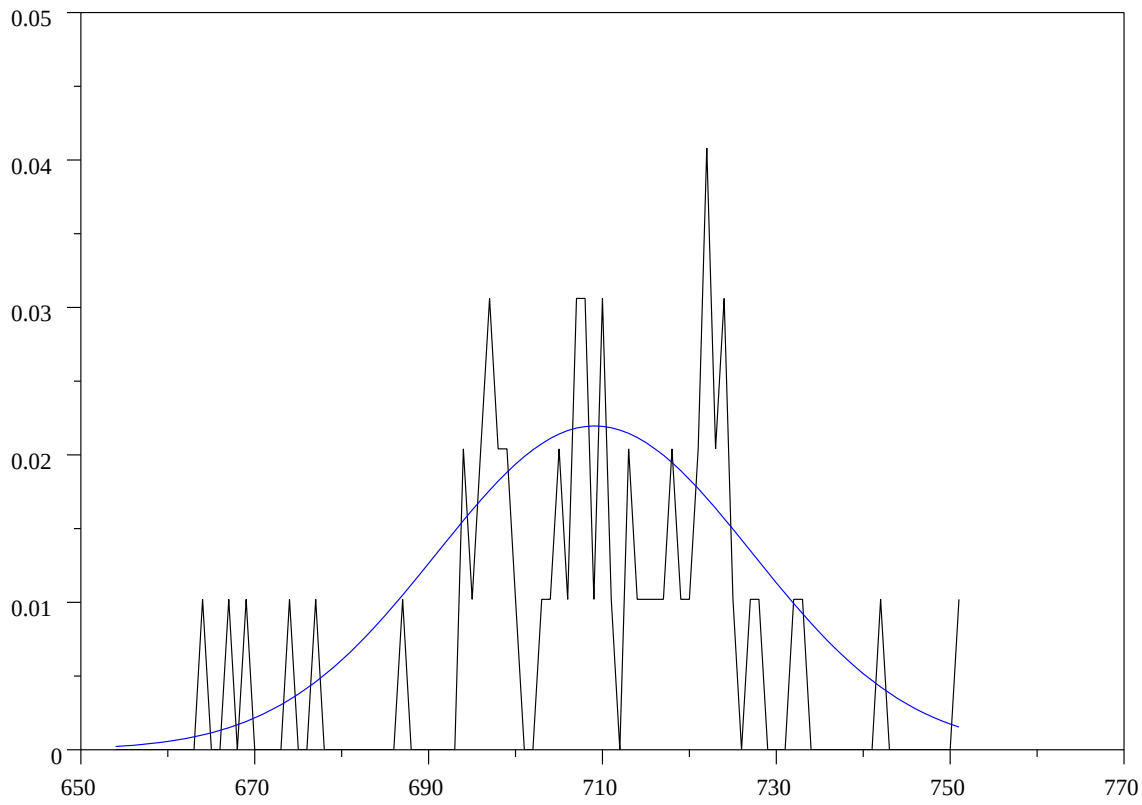

Fig. 5.20 – Distribution (pour les 64 numéros) des différences des valeurs des bits relus pour un tatouage ne contenant que des "1" (tous les e_{01} sont positifs). Par simplicité lors de la détection, nous faisons comme si nous ne cherchions à relire que des "1" : nous testons en réalité les $|e_{01}|$ (une distribution tatouée n'en reste pas moins suspecte). Le maillage d'exemple comporte 45906 sommets (BigHead_2). La distribution est centré près de $45906/64 = 717.3$: les sommets sont utilisés au maximum pour cacher de l'information.

Nous procédons en pratique à un décodage dur de l'information tatouée : le plus petit des $|e_{01}|$ valide ou non la détection entière. On pourrait encore mettre en œuvre un décodage doux en assignant à chaque symbole une probabilité propre. Nous représentons sur la Fig. 5.21 le seuil de détection, et les sorties du détecteur pour 500 clefs dont celle (numéro 250) qui a été effectivement utilisée pour cacher un message. Nous décrivons dans la section suivante

comment nous fixons la taille de l'espace des clefs, que nous évaluons à 2^{24}.

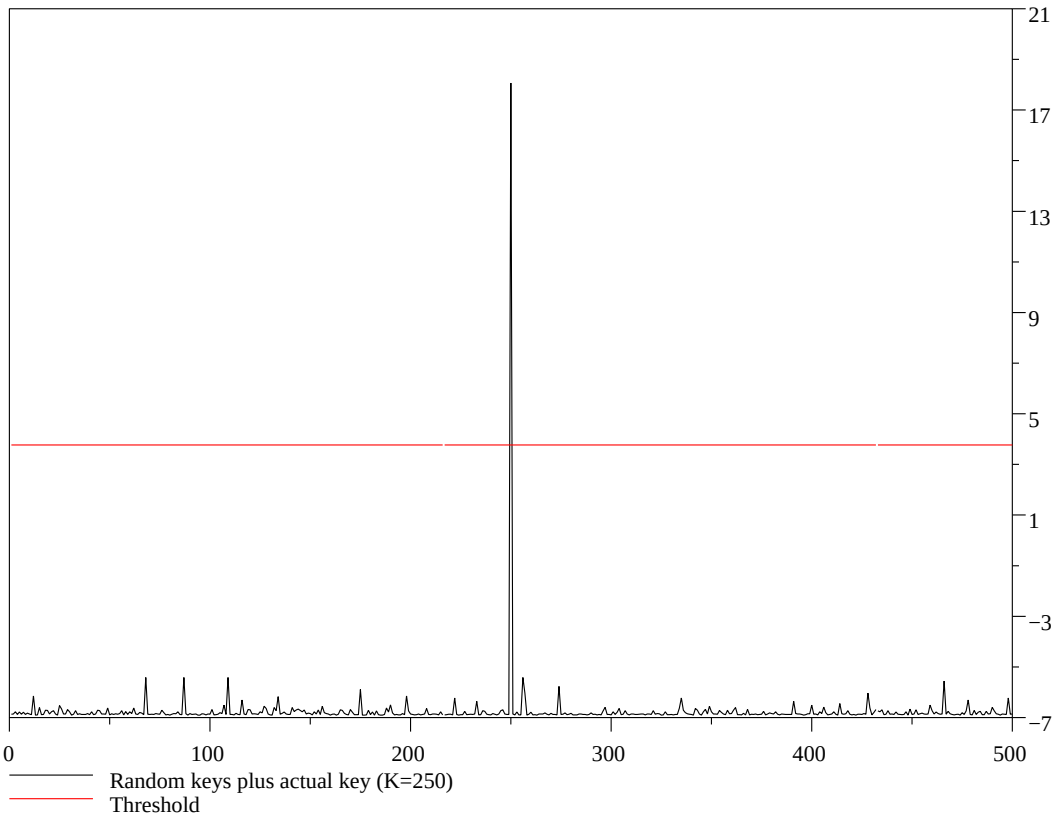

Fig. 5.21 – Sortie du détecteur pour 500 clefs. Seule la clef 250 a été effectivement utilisée pour insérer un message de 64 bits. Le seuil vaut 3.7665, et la sortie de la clef 250 vaut 18.0722.

5.5.3 Sécurité des clefs

On lit souvent dans la littérature du tatouage que la clef secrète mesure 64 bits, comme le message, sous-entendu : *tous* les 64 bits de la clef contribuent à la sécurité du tatouage. En cryptographie, les 64 bits participent effectivement à la sécurité (sous réserve d'absence de canal subliminal) car on vient tester le résultat (binaire) d'un calcul.

En tatouage, on vient tester une corrélation. On peut donc imaginer deux clefs (l'une des deux étant "la bonne") donnant un motif pseudo-aléatoire de 64 bits identique à quelques valeurs près. La corrélation sera élevée même dans le cas de la mauvaise clef, et un tatouage (faux) sera détecté, mais le pirate aura trouvé une bonne approximation. Nous cherchons à quantifier la taille de l'espace des clefs effectivement utilisables dans notre schéma.

Il faut à présent remarquer que le calcul de g_{ABC} fait intervenir deux formes linéaires en K_1 et en K_2. Ainsi, le résultat du calcul de g_{ABC} sera-t-il potentiellement proche pour deux clefs proches en valeurs : c'est précisément ce que nous voulons éviter. Nous avons choisi les valeurs T_1, T_2, et les longueurs de clefs de manière à ce que la clef la plus proche en valeur de la bonne clef donne une probabilité de fausse alarme de 10^{-1}. Autrement dit, nous organisons l'imperceptibilité statistique du tatouage et nous en déduisons expérimentalement les longueurs de clefs et les paramètres internes de l'algorithme. Nous avons fixé dans un premier temps T_1 et T_2 de manière à obtenir dès l'origine une bonne équirépartition des numéros des bits avant tatouage. Ensuite, nous avons augmenté la longueur des clefs jusqu'à ce qu'elles permettent encore de bien discerner deux clefs proches en valeur numérique.

Nous avons fixé les paramètres internes à $T_1 = 10$ et $T_2 = 4$. Les longueurs de clefs utilisables ont été déterminées expérimentalement et fixées à $N_{K_1} = 14$ et $N_{K_2} = 10$ bits. Ainsi, la sécurité de notre schéma, au sens de l'imperceptibilité statistique est-elle seulement de 24 bits.

Cela veut dire que si le message caché est effectivement crypté avec 64 bits, son imperceptibilité ne repose en réalité que sur 24 bits. D'un point de vue de pirate, il faudra une recherche brute parmi 2^{24} attaques pour tomber sur une clef donnant une réponse suffisante à la détection. Sur un PC basique, un test de clef prend environ 6 secondes (sur 100K triangles). Détecter si un tatouage est présent, sans connaître la clef secrète, prendra donc un peu plus de 3 ans, sur une seule de ces machines.

5.5.4 Résultats

Nous avons testé notre méthode sur plusieurs maillages et avons déterminé le nombre de triangles nécessaires à la détection correcte du tatouage, voir Tab. 5.22. Ce nombre est aussi appelé *Minimum Watermark Segment* dans la littérature. Il s'agit de la plus petite quantité de média protégée. Pour notre schéma, il faut 600 triangles au maximum pour retrouver la marque de 64 bits. Ce résultat plutôt satisfaisant tient au fait que peu de sites sont rejetés à cause des contraintes de distorsion ou d'exception en virgule flottante. L'apport du parcours optimal est assez saisissant lorsque l'on compare ces 600 triangles aux 40% du maillage nécessaires pour retrouver la marque avec un parcours naïf (voir le maillage Twins sur la Fig. 5.14).

Notre méthode de tatouage a été conçue pour résister à la translation, la rotation, et à la mise à l'échelle : nous l'avons vérifié en relisant la marque sur un maillage tatoué ayant subi une combinaison aléatoire des trois (ligne RST dans le Tab.5.22). La ligne MWS donne le nombre minimal de triangles nécessaires pour relire la marque (chaque triangle est permuté trois fois pour retrouver son orientation à l'insertion). Nous avons encore vérifié que d'autres manipulations effacent bien la marque : un lissage barycentrique de Taubin (seulement une itération suffit), une compression MPEG-4 3D Mesh Coding (standard : 12 bits de quantification des erreurs de prédiction géométrique), et un bruit faible sur les coordonnées (d'amplitude égale à $d_{bbox} \times 10^{-7}$). Il y a tout lieu de penser qu'à chaque fois que la marque est effacée, c'est parce que beaucoup de sites tatoués ne sont plus reconnus comme tels, et qu'ensuite éventuellement le numéro de bit qu'ils codent est faussé. En effet, les modifications géométriques codant les numéros des bits sont plus fines que celles codant les valeurs.

Objet	Horse	BigHead_1	BigHead_2	African	Twins
Sommets	48485	21777	45906	57639	83241
Triangles	96966	43550	91808	115282	166482
Genre	0	0	0	2	1
Sites tatoués	47131	21683	45726	57611	83212
Utilisation des sommets	97.21%	99.57%	99.61%	99.95%	99.97%
Répétition moyenne	736.4	338.8	714.1	900.2	1300.2
RST	Oui	Oui	Oui	Oui	Oui
MWS (triangles)	>600	>580	>590	>560	>550
Bruit faible	Non	Non	Non	Non	Non
Compression MPEG-4	Non	Non	Non	Non	Non
Lissage (2 itérations)	Non	Non	Non	Non	Non

FIG. 5.22 – Résultats obtenus en tatouage fragile.

Nous sommes maintenant en mesure de chiffrer la densité locale d'information utile que nous insérons, exprimée comme le rapport de la capacité utile sur le MWS : nous cachons 0.11 bit utile par triangle (soit 0.75 bit réel par triangle à cause de l'arrangement indexé). En effet, nous considérons qu'au pire il nous faut 600 triangles pour cacher 64 bits sous les contraintes que nous avons fixées. Par la relation d'Euler, on peut multiplier ces quantités par deux pour obtenir la densité par sommet. Notre schéma de tatouage fragile propose finalement les caractéristiques suivantes :

- Tatouage *expressément* robuste à la translation, la rotation et la mise à l'échelle uniforme,
- Parcours des $N-2$ sites utilisables en temps $O(N)$,
- Arrangement indexé permettant de pallier la coupe,
- Capacité de 64 bits utiles (448 bits réels),
- Sécurité sur la relecture du tatouage : 64 bits,
- Sécurité sur la détection du tatouage : 24 bits,
- Plus petite surface protégée : 600 triangles (déterminé expérimentalement),
- Densité minimum d'information : 0.2 bit/sommet,
- Probabilité de fausse alarme $P_{fa} = 10^{-7}$.

Nous voulons voir ici un avantage de notre méthodologie : la caractérisation des performances est plus complète que pour la plupart des méthodes à base d'invariants géométriques. A notre connaissance, nous sommes les seuls à proposer à la fois une estimation de la longueur de clef utile et de la densité d'information utile. Toutefois, tout au long de la conception de notre méthode, nous avons fait apparaître des remarques qui méritent d'être détaillées au titre des perspectives ouvertes par cette étude[80].

[80]"On commence en tout genre par le simple, ensuite vient le composé, et souvent enfin on revient au simple par des lumières supérieures. Telle est la marche de l'esprit humain.", Voltaire, *op. cit.*, p. 447. Puisse cette forte pensée nous consoler de n'avoir pas été davantage éclairé plus tôt !

5.6 Perspectives

Nous avons conçu, séparément, trois briques permettant de réaliser diverses variations autour du tatouage par invariant géométrique : une primitive géométrique d'insertion de la valeur des bits, un arrangement indexé pour leur numéro, et un parcours performant du graphe de connexité. Nous avons voulu détailler soigneusement les caractéristiques de chacune d'entre elles, car il nous sera plus facile de spéculer sur les limites de l'approche par invariants géométriques. L'application que nous visions d'emblée était le tatouage fragile, mais nous pouvons à présent discuter, par exemple, de l'application du parcours optimal à la stéganographie. Comme nous l'avons présenté dans les résultats, la marque que nous insérons est extrêmement fragile - l'étude de la robustesse face à la quantification pourrait nécessiter de trop baisser la capacité utile ou la longueur des clefs utilisées contre la détection, et c'est la raison pour laquelle nous ne voyons pas d'autre application que le tatouage fragile et la stéganographie pour l'approche par invariant. Toutefois, il reste possible d'esquisser les nouvelles caractéristiques d'un schéma optimisé pour la stéganographie, d'un autre pour l'intégrité, mais aussi d'améliorer notre méthode de tatouage fragile, et de soulever les nouvelles difficultés techniques qui y sont liées.

5.6.1 Application du parcours optimal à la stéganographie

Nous avons vu dans le cadre du tatouage par arrangement indexé que nous cachons en réalité $1 + \log_2(C_{utile}) = 7$ bits par site. Puisque dans le cadre de la stéganographie nous considérons un arrangement global (i.e : les numéros des bits cachés sont implicites), nous pouvons libérer les $\log_2(C_{utile})$ bits de codage du numéro des bits pour augmenter la capacité utile. Soit N_{bps} le nombre de bits cachés par site, nous répétons R fois chaque bit afin de pallier les inévitables erreurs de transmission dans le canal stéganographique (dues par exemple aux exceptions en virgule flottante). La capacité C_{stego} en bits de notre schéma de stéganographie s'écrit donc :

$$C_{stego} = \lfloor (N-2) \times N_{bps} \times \frac{1}{R} \rfloor. \tag{5.11}$$

Une autre modification à apporter concerne le parcours, et nécessiterait de choisir le sommet suivant de manière pseudo-aléatoire dans la liste active : cela rendrait la seule reconstitution de la *séquence* des bits cachés improbable. Enfin, puisque l'on se servirait du parcours pour orienter implicitement les triangles à la relecture, on pourrait se dispenser de marquer un triangle comme tatoué, et laisser flotter indifféremment g_{ABC} dans $[\lfloor g_{ABC} \rfloor; \lfloor g_{ABC} \rfloor + 1[$, cela afin de reconquérir l'imperceptibilité computationnelle perdue. Avec cette technique, nous ne voyons pas même comment on pourrait suspecter seulement l'existence d'un message caché.

5.6.2 Application de l'arrangement indexé à l'intégrité

Si un pirate modifie une partie seulement du maillage, on aimerait pouvoir en être informé. Pour cela, sans disposer encore d'outil fiable pour quantifier une telle modification, on pourrait toutefois dans un premier temps mettre en œuvre une stratégie d'inspection visuelle. En effet, les $N-2$ sites étant atteints (et très peu rejetés), on peut considérer que

la dispersion de l'information couvre tout le maillage. L'arrangement indexé autorise la mise en évidence des zones ayant éventuellement été malicieusement modifiées. En effet, dans la zone incriminée, plus aucun sommet ne sera reconnu comme tatoué. Notons cependant qu'il conviendrait sans doute de développer ici des techniques de morphologie mathématiques pour mieux agréger entre elles les parties dégradées.

Il faut reconnaître que cette application est cruciale : si une partie du maillage seulement avait été modifiée, supposée petite, la détection du tatouage eût tout de même été probablement suffisante pour relire la marque. La modification malicieuse serait passée inaperçue. On pourrait imaginer de donner l'alarme lorsque la plus petite surface connexe non tatouée excède un seuil significatif, ou de noter l'ampleur des modifications par rapport à $N - 2$, pour indiquer à l'utilisateur s'il doit procéder à une inspection visuelle. Pour cela, on peut commencer par mettre en valeur les triangles porteurs d'information cachée détectés comme tels, et les autres, comme illustré sur la Fig. 5.23 (où le maillage tatoué n'a subi aucune manipulation).

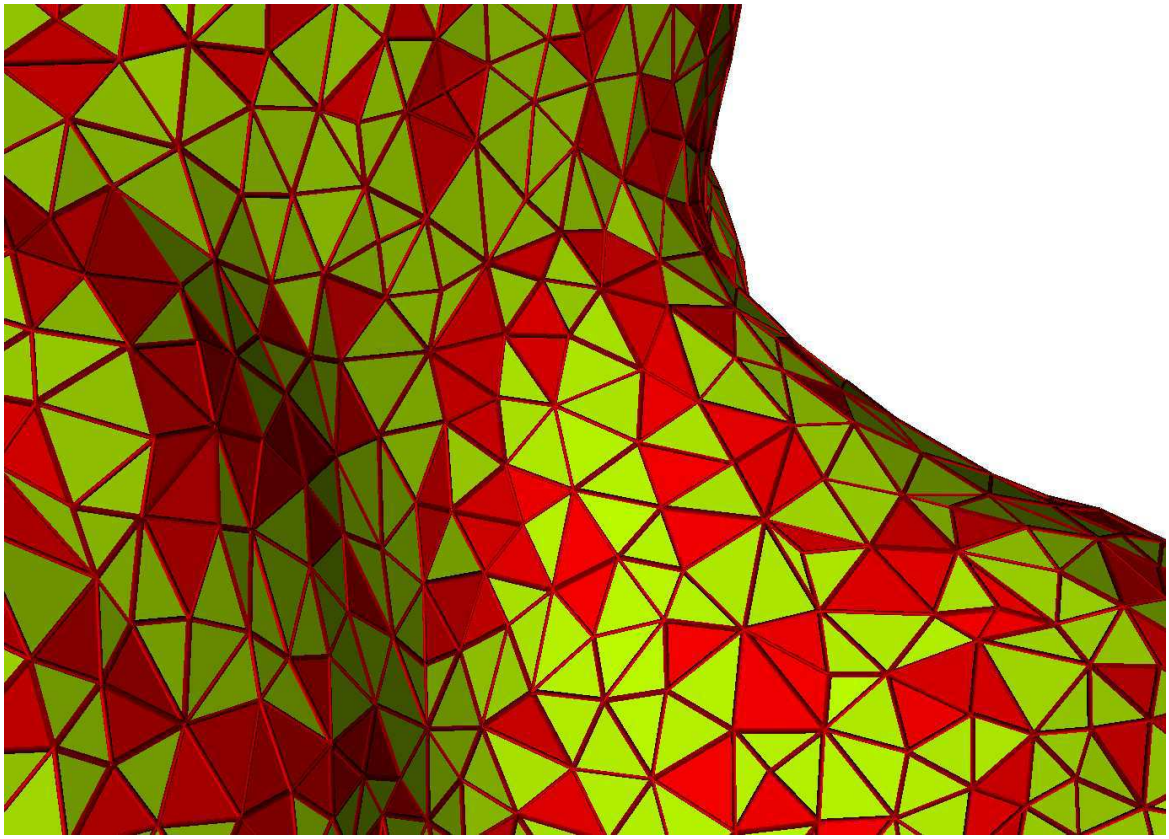

Fig. 5.23 – Localisation de l'information tatouée : les triangles porteurs d'information sont en vert, les autres en rouges. Comme attendu, environ un triangle sur deux code de l'information (soit le nombre de sommets à peu près). Des techniques de morphologie mathématique permettraient d'agréger ensemble les zones dont la densité de triangle porteurs d'information serait inférieure à un certain seuil, afin de visualiser les zones modifiées.

5.6.3 Tatouage de tous les triangles

Nous l'avons détaillé plus haut, notre parcours permettrait de tatouer tous les triangles (et non plus seulement $N - 2$ sommets), au prix d'une modification substantielle de la procédure entière d'inscription géométrique de l'information. Nous avons suggéré l'utilisation d'invariants dont le calcul est invariant par permutation circulaire des sommets, comme le rapport de l'aire sur le périmère au carré.

Toutefois, il n'est pas évident de concevoir une procédure d'inscription qui autorise ce mode de relecture. En effet, on devra fixer la valeur de cet invariant dans un nombre variable (parfois élevé) de triangles connexes. Nous laissons ce problème à la sagacité du lecteur intéressé. La résolution de ce problème serait bienvenue car n'ayant plus besoin d'orienter les triangles, le tatouage fragile réellement imperceptible deviendrait possible car la présence du tatouage pour un pirate ne serait plus trahie par l'Eq. 5.8. Enfin, il serait encore envisageable de bénéficier d'un module d'inspection visuelle de l'intégrité (même si elle serait sans doute de moins bonne qualité qu'avec l'information d'orientation des triangles disponible). Comme un maillage contient environ deux fois plus de triangles que de sommets, la taille du MWS diminuerait en rapport (la densité des sites serait multipliée par deux pour un même nombre de bits).

5.6.4 Allocation adaptative des bits

Dans la présente implantation, nous forçons les bits à être inscrits les uns après les autres, dans l'ordre des numéros de la marque. Une telle stratégie peut sans doute être améliorée en plaçant les numéros des bits dans une file de priorité et en déterminant dynamiquement le bit à inscrire (et donc son numéro) en fonction de la géométrie, sous contrainte d'équirépartition des numéros.

Les avantages attendus sont de deux ordres :

- *Minimisation de la distorsion* On favoriserait les numéros entraînant la plus petite distorsion,
- *Optimisation du nombre de sites tatoués* Il devient possible de se servir de quasiment tous les $N-2$ sites atteints, car on pourra sans doute trouver à chaque itération un bit à inscrire qui ne génère pas d'erreur de traitement (distorsion géométrique ou exception en virgule flottante).

5.7 Conclusion

Nous avons proposé, autour du tatouage fragile, un tour d'horizon des possibles, tant en stéganographie qu'en protection de l'intégrité, de notre approche par invariants géométriques. Nous avons souhaité insister sur l'aspect modulaire de notre raisonnement, afin de bien séparer ce qui peut encore porter à amélioration. Au final, nous avons développé une méthode de tatouage fragile permettant de déterminer nombre de caractéristiques utiles au tatoueur, comme la probabilité de fausse alarme, la taille de la plus petite surface protégée (MWS), la classe de robustesse admissible, la sécurité face à la détection pirate, le tout avec un parcours optimal du graphe en $O(N)$.

Chapitre 6

Autour de la décomposition spectrale de la géométrie

Dans cette dernière partie de notre travail[81], nous avons voulu étudier la robustesse du tatouage face à la compression de la géométrie. Pour cela, nous avons dû sélectionner une méthode de codage de source ne nécessitant pas ou peu de travail sur la connexité (nécessitant généralement le traitement de beaucoup d'exceptions - pour les bords, les trous, etc.) Aussi notre choix s'est-il porté sur les méthodes de compression dites spectrales. En outre, cette représentation permet la transmission de la géométrie de manière progressive, et est à peu près aux maillages ce que la DCT par bloc est aux images. Ce choix se justifie encore par le fait que de nombreuses méthodes robustes de tatouage en image et en audio ont été développées dans un espace transformé, souvent aussi pour profiter de modèles psycho-visuels ou psycho-auditifs.

Après avoir présenté l'espace de la décomposition spectrale, nous développerons ensuite un codeur spectral de la géométrie dont nous détaillerons les variantes suivant qu'elles visent la compression ou la transmission progressive. En effet, nous verrons que deux implantations sont possibles, suivant que l'on requiert ou non des bases fixes de décomposition d'une connexité qui reste arbitraire. Ce codeur nous permettra de tester ensuite une méthode de tatouage simple dans l'espace spectral de la géométrie, dont nous montrerons qu'il résiste à la quantification du codage de source spectral. Dans l'immédiat, nous reproduisons sur la Fig. 6.1 les modèles originaux que nous avons utilisés afin qu'ils servent de référence. L'intérêt de fandisk est de n'être pas un objet naturel, et donc de présenter des surfaces planes (les surfaces fonctionnelles de l'objet de CAO) sur lesquelles les artefacts dus à la décomposition spectrale se verront bien mieux que sur des objets naturels comme les trois autres objets.

6.1 Cadre théorique

Nous présenterons tout d'abord l'espace de décomposition spectrale de la géométrie d'un point de vue théorique. Nous reprendrons pour cela le cadre énoncé par Taubin [71] et adapté à la compression par Karni et Gotsman ([56] puis [57]). Ensuite, nous détaillerons les difficultés pratiques d'implantation de tels schémas de représentation, qui bien que parfois

[81] Nous sommes redevables de son aide à Patrice Rondao-Alface pour ce chapitre.

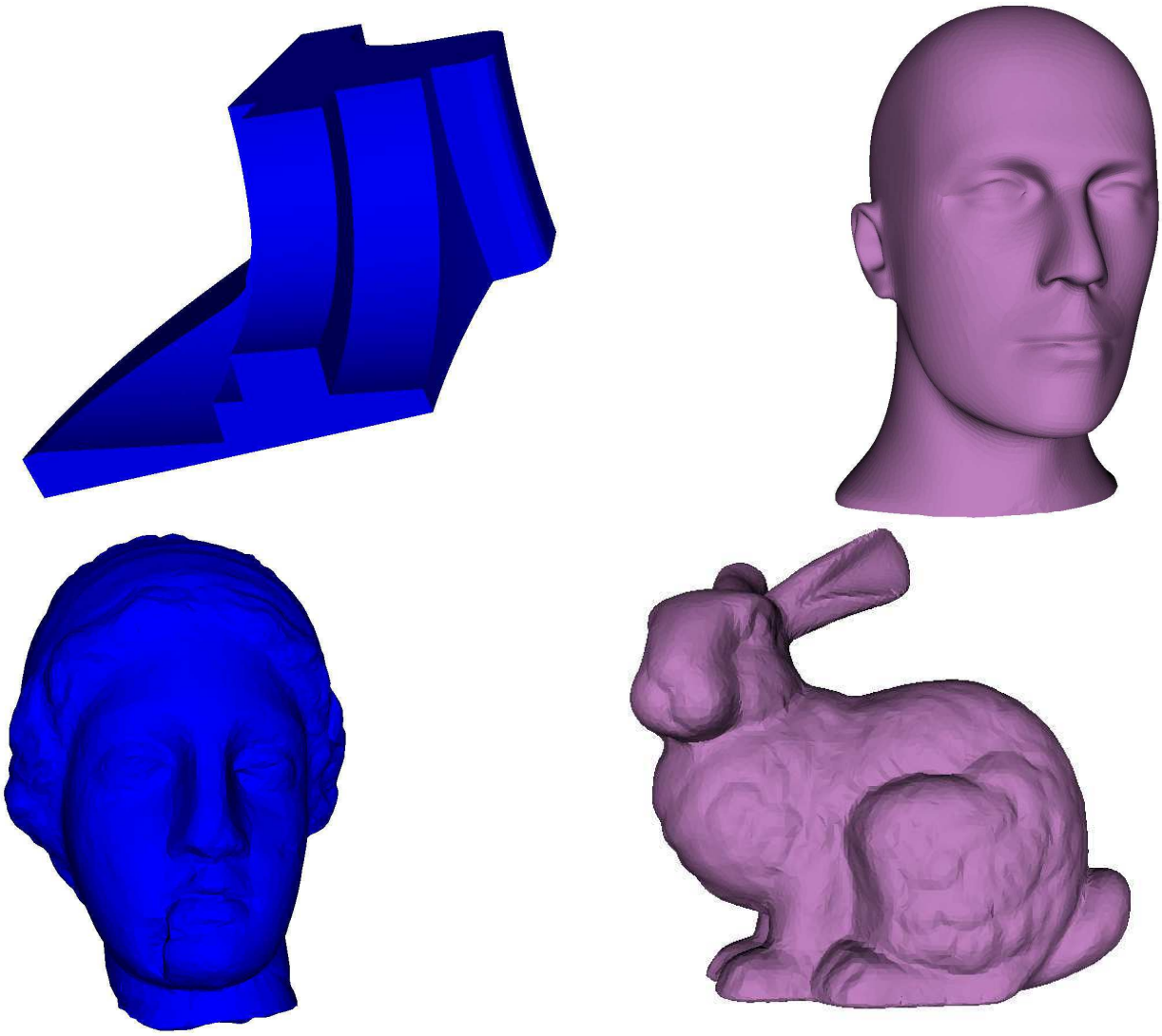

FIG. 6.1 – Modèles originaux utilisés dans cette partie : fandisk, head, venus et bunny.

importantes, ont été généralement minimisées, voire passées sous silence. Nous développerons en conséquence notre propre implantation d'un quantificateur spectral de la géométrie, et nous justifierons nos choix au regard des problèmes que nous avons rencontrés, et que les références ne nous avaient pas laissé imaginer. Du fait de ces difficultés qui nous ont contraints à des adaptations *ad hoc*, nous avons dû nous résigner à développer les bases davantage techniques que théoriques de l'étude que nous nous proposions au départ.

6.1.1 Opérateur laplacien pour le codage de source

Le codage prédictif peut être considéré comme une détection d'innovation filtrée et sa transmission par une compression adaptée à ses statistiques. On commence par transmettre la composante continue du signal, puis les innovations détectées. Dans ce cadre, l'opérateur

laplacien est un détecteur d'innovation efficace et reconnu. Pour l'image 2D, le noyau Δ du laplacien s'écrit :

$$\Delta = \begin{pmatrix} 0 & -\frac{1}{4} & 0 \\ -\frac{1}{4} & 1 & -\frac{1}{4} \\ 0 & -\frac{1}{4} & 0 \end{pmatrix}. \tag{6.1}$$

La somme des poids du noyau est nulle, ce qui rend la transformation unitaire. Taubin [71] a proposé d'étendre cette approche aux maillages surfaciques tridimensionnels en s'adaptant à la valence locale du sommet en cours de traitement. Le laplacien Δp_i en un sommet p_i s'écrit :

$$\Delta p_i = \sum_{p_j \in p_i^\star} w_{i,j}(p_i - p_j) = p_i - \sum_{p_j \in p_i^\star} w_{i,j} p_j, \tag{6.2}$$

sous la contrainte d'une transformation unitaire :

$$\sum_j w_j = 1 \ \ \forall p_i. \tag{6.3}$$

Le calcul des poids peut faire ou non appel à la géométrie. Le rapport de la longueur de l'arête $p_i p_j$ sur la somme des longueurs des arêtes est un exemple de calcul des poids faisant appel à la géométrie. Pourtant, nous cherchons précisément à transmettre cette géométrie : nous ne pouvons donc utiliser que des poids dont le calcul ne fait pas intervenir la géométrie. Le choix se porte naturellement sur :

$$w_{i,j} = \frac{1}{d_{p_i}} \ \ \forall j, \tag{6.4}$$

où d_{p_i} est la valence du sommet p_i. Cet opérateur, ramené à la grille régulière 2D, est la définition du laplacien classique car $d_{p_i} = 4$ pour un pixel. Il est possible de formuler le problème non plus localement comme nous venons de la faire, mais globalement. On forme la matrice laplacienne C, à partir de son terme courant :

$$C_{ij} = \begin{cases} 1 & \text{si } i = j, \\ -d_{p_i}^{-1} & \text{si } p_j \in \{p_i^*\} \text{ et } d_{p_i} \neq 0, \\ 0 & \text{sinon.} \end{cases} \tag{6.5}$$

La matrice C n'est pas circulante dans le cas général : elle l'est uniquement si la connexité est régulière. C'est pourquoi nous retrouvons le cadre de la transformation de Fourier si la connexité est régulière (l'opérateur laplacien est alors stationnaire), et nous nous contenterons, suivant la littérature, de parler de décomposition spectrale dans le cas général d'une connexité arbitraire. Dans ce dernier cas, le mot spectral n'est pas tout à fait usurpé : nous verrons qu'il se réfère au spectre de la matrice C.

6.1.2 Décomposition spectrale

C'est pour la première fois dans [42] que la géométrie est décomposée sur une base spectrale (au sens du spectre d'une matrice) dans une optique de transmission de la géométrie.

Naturellement, les poids choisis sont ceux délaissés par Taubin : les inverses des valences. En effet, on diagonalise C pour obtenir la matrice de projection B :

$$\begin{pmatrix} e_0 & 0 & ... & ... & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & e_i & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & ... & ... & 0 & e_{N-1} \end{pmatrix} = B^{-1}CB. \tag{6.6}$$

Les valeurs propres e sont des modes propres de déformation définis sur la connexité $\mathcal{E}$. En mécanique, on parlerait de modes de vibration propres car ils sont utilisés pour simuler le comportement d'une surface lorsqu'elle subit un choc. On peut les assimiler à des fréquences, l'analyse de Fourier est ainsi étendue aux données discrètes irrégulièrement échantillonnées. Zéro est une valeur propre, et le vecteur propre associé ne contient que des 1 : la composante continue est donc un plan puisque l'on attribue le même poids à tous les sommets, chaque sommet intérieur est donc placé au barycentre de ses voisins - sur un plan (voir Fig. 6.2). On projette ensuite l'information géométrique constituée des trois vecteurs X, Y, Z sur les vecteurs de base pour obtenir sa décomposition spectrale sous forme de trois vecteurs de coefficients spectraux :

$$\begin{cases} P = BX \\ Q = BY \\ R = BZ \end{cases} \tag{6.7}$$

La reconstitution de l'information géométrique à partir de l'information spectrale se fait naturellement en revenant dans la base spatiale par l'inverse de la matrice de projection :

$$\begin{cases} X = B^{-1}P \\ Y = B^{-1}Q \\ Z = B^{-1}R \end{cases} \tag{6.8}$$

Les fonctions de base sont ici des maillages que l'on vient combiner linéairement entre eux pour obtenir le maillage original. Nous reproduisons sur la Fig. 6.2 les 9 maillages de la base de reconstruction B^{-1} pour le petit maillage au centre de la Fig. 3.6 (possédant 9 sommets) ayant une connexité de subdivision. La composante continue est en haut à gauche, et les 8 autres maillages sont ordonnés par valeurs propres associées décroissantes. Les deux derniers maillages de la première ligne ne sont pas tout à fait plans. Dans une optique de transmission, on enverra tout d'abord les coefficients spectraux relatifs à la composante continue, puis les autres coefficients amèneront progressivement l'innovation géométrique manquante. De récents travaux relient la matrice C à l'inverse de celle de Karhunen-Loeve et discutent l'optimalité d'une telle approche en 1 et 2 dimensions [6]. Toutefois, dans une optique de transmission, on sait qu'il ne faut pas utiliser la base de Karhunen-Loeve : les fonctions de base à transmettre dépendent de l'objet et induisent un surcoût prohibitif de transmission. Nous verrons dans la section 6.3 comment pallier ce problème.

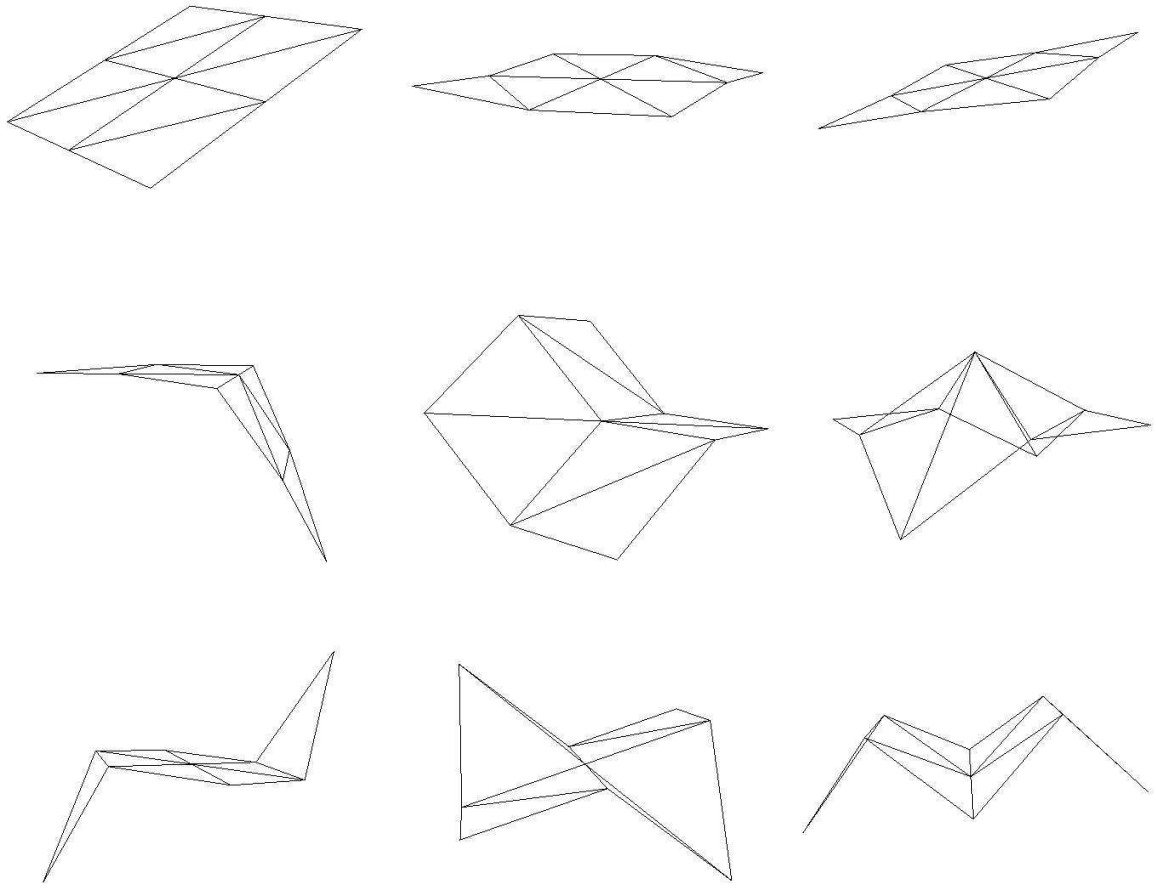

FIG. 6.2 – Les 9 maillages de la base de décomposition spectrale (ordonnés par valeurs propres croissantes). En haut à gauche : le maillage (plan) de la composante continue.

6.1.3 Spectre de la géométrie

En classant les valeurs propres par ordre croissant, on associe dans [42] à chaque triplet de coefficients spectraux sa valeur spectrale S_i :

$$S_i = \|P_i\|^2 + \|Q_i\|^2 + \|R_i\|^2. \tag{6.9}$$

On obtient alors le spectre de la géométrie que nous illustrons sur la Fig. 6.3. On constate que les valeurs spectrales décroissent globalement, et que l'on parvient ainsi à décorréler l'information géométrique en utilisant uniquement l'information de connexité. Toutefois, le spectre de la géométrie ne nous sera plus d'aucune utilité par la suite qu'en tatouage. En effet, dans la section 6.5 nous nous intéresserons aux spectres sur X, Y, et Z pris séparément pour modifier les relations entre les scalaires d'un même triplet spectral.

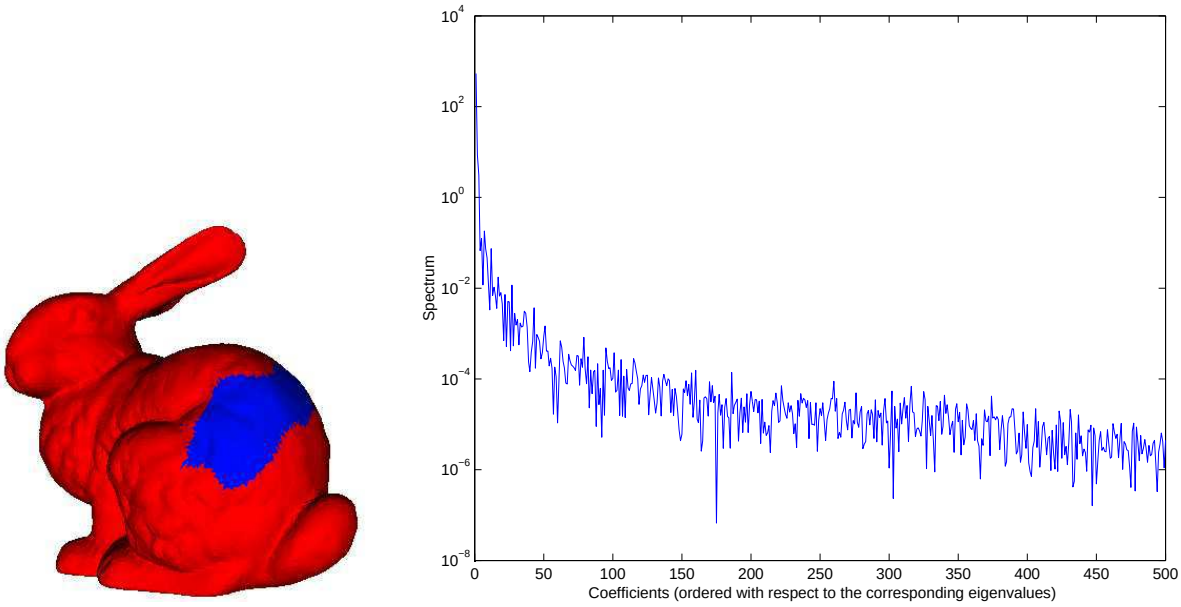

FIG. 6.3 – Le spectre de la géométrie (échelle logarithmique) de la partition foncée (500 sommets).

6.2 Partition du maillage

La décomposition spectrale demande de diagonaliser une matrice carrée dont la taille est N. Pour des maillages complexes de plusieurs dizaines de milliers de points, diagonaliser la matrice C associée est difficile. Il existe des méthodes permettant d'estimer quelques valeurs propres de grandes matrices [68], mais le calcul exhaustif de toutes les valeurs propres peut s'avérer difficile, notamment à cause de problèmes de stabilité numérique. Nous verrons que ce sera l'une des sources des difficultés rencontrées.

6.2.1 Remarques pratiques pour l'implantation

Dans une optique de transmission, le décodeur doit connaître les fonctions de base *avant* que n'arrive le premier coefficient spectral. En pratique, pour respecter cette contrainte de causalité, il faut procéder comme suit :

- Envoi préalable de la connexité,
- Calcul des bases de décomposition,
- Analyse (codeur) ou synthèse (décodeur).

La connexité peut être envoyée arbitrairement, par l'une des méthodes exposées en 3.1. Nous rappelons que nous n'avons pas souhaité traiter ce problème, qui est déjà résolu, en vue de l'étude qui nous intéressait.

En pratique, comme nous l'avons vu, c'est la diagonalisation de C qui pénalise l'algorithme appliqué aux grands maillages, pour deux raisons :

- le temps de calcul devient rédhibitoire,
- des problèmes de stabilité numériques interviennent.

Pour pallier ce problème, la solution proposée dans [42] consiste à diviser le maillage en sous-maillages au moyen d'une partition du graphe de connexité. Chaque partition peut au besoin être traitée séparément sur un processeur. Ainsi, on divise le problème en sous-problèmes dont la taille autorise une exécution raisonnable en machine. Toutefois, même en procédant ainsi le temps de calcul peut s'avérer encore long. C'est la raison pour laquelle nous suivrons une autre stratégie issue de [43], fondée sur des bases fixes de décomposition.

6.2.2 Un outil générant des partitions

Afin de créer des partitions, les auteurs de [42] utilisent un outil de partionnement de graphe appelé MeTiS [44]. Le partionnement permet de se ramener à des matrices de taille plus modeste (typiquement 500) dont le temps de diagonalisation devient acceptable. Toutefois, MeTiS ne garantit qu'un nombre moyen de sommets par partition. La découpe est guidée par la minimisation de la longueur des bords des partitions. Nous donnons sur la Fig. 6.4 la représentation graphique de telles partitions obtenues avec MeTiS en ayant fixé 480 sommets par partition en moyenne comme but.

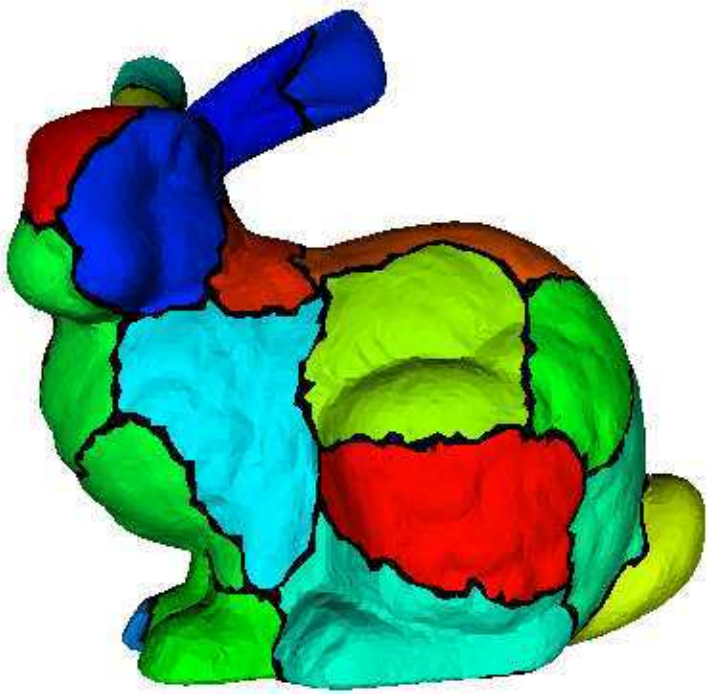

Fig. 6.4 – Découpe du maillage en partition de 480 sommets en moyenne (minimum 446, maximum 531). Les triangles ayant une arête séparant deux partitions sont peints en noir. Les partitions situées à la base de chaque oreille contiennent deux bords (cylindre topologique).

6.2.3 Artefacts visuels dus à la partition

L'utilisation du laplacien place les points en fonction du barycentre de leur voisinage. Lorsque peu de coefficients spectraux sont utilisés pour reconstruire l'objet, les sommets ont tendance à s'organiser d'abord au centre géométrique de la partition, loin de la frontière. Nous illustrons sur la Fig. 6.5 le type d'artefacts se produisant aux frontières des partitions. Pour cela, nous avons reconstruit progressivement une sphère régulièrement échantillonnée. Sur la ligne du haut, la sphère n'a pas été partitionnée : la reconstruction porte sur la totalité de l'objet. Sur la ligne du bas, la sphère a été partitionnée en deux : on observe des effets de bords sur la frontière dus à la partition de l'objet en deux.

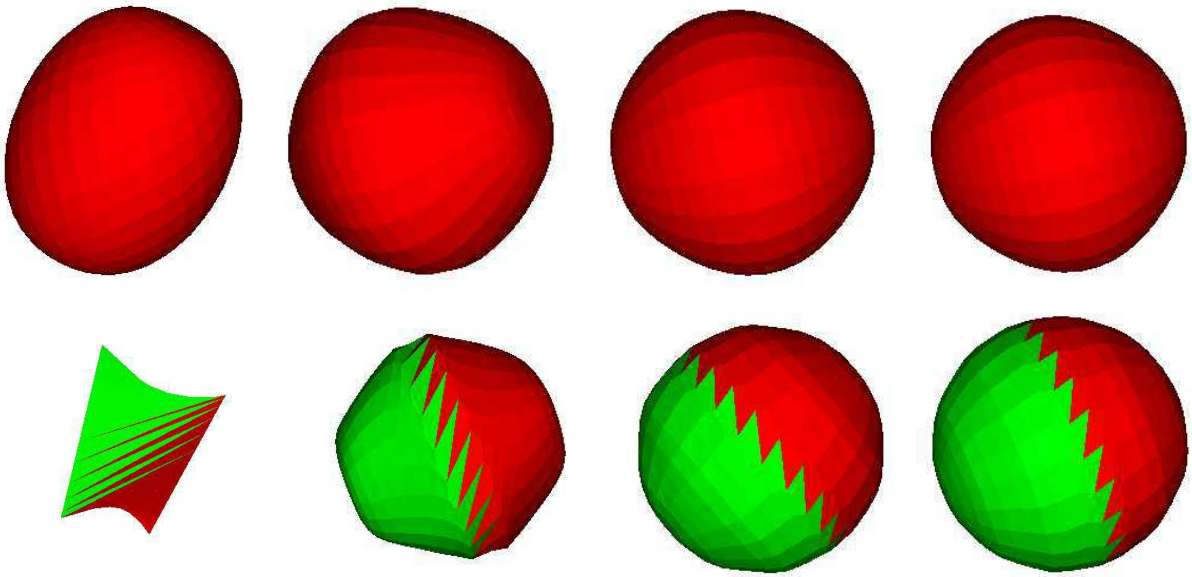

FIG. 6.5 – Artefact visuel dû à la partition du maillage (à diverses étapes de la reconstruction). En haut : la sphère n'est pas partitionnée (1%, 2%, 5%, 10% des coefficients). En bas : La sphère a été partitionnée en deux (1%, 5%, 20%, 30% des coefficients). Les artefacts dus à la partition apparaissent nettement sur la frontière : ces effets de bord mettent un certain temps à disparaître lors de la reconstruction (dans l'image en bas à droite, 30% des coefficients ont été utilisés pour reconstruire l'objet, les artefacts sont encore perceptibles).

C'est la raison pour laquelle sur la Fig.6.6 on constate un tassement des sommets à l'intérieur des partitions : nous avons illustré la reconstruction d'un objet avec peu de coefficients afin de mettre en évidence les artefacts aux frontières des partitions. On notera que ces artefacts se produisent essentiellement au tout début de la transmission progressive de la géométrie : en effet sur la Fig. 6.6 à droite, 2% des coefficients spectraux ont été utilisés pour recontruire la géométrie, alors qu'à gauche les artefacts sont notablement réduits (objet reconstruit avec 5% des coefficients spectraux), même si le coloriage des partition permet encore de les distinguer facilement.

Nous verrons plus loin (dans la section 6.3.1) comment nous pourrons pallier sensiblement ces artefacts, par l'introduction d'un recouvrement entre les partitions. Nous détaillons à

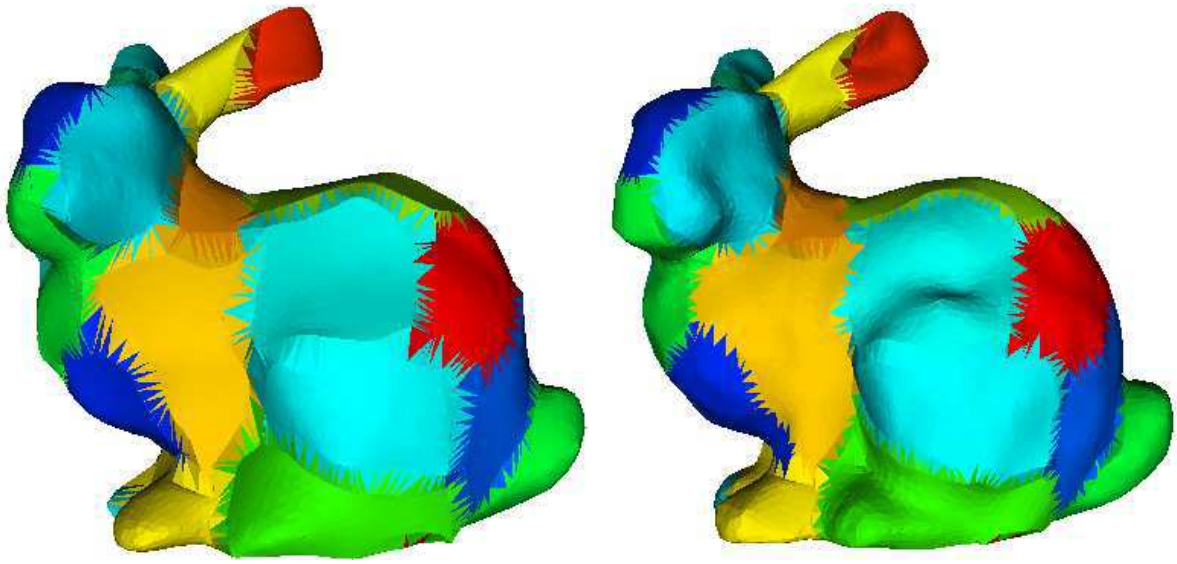

FIG. 6.6 – Artefacts dus à la partition du maillage : au début de la reconstruction, les sommets ont tendance à se placer d'abord au centre de chaque partition (à gauche : 2% des coefficients spectraux, à droite : 5%).

présent la technique consistant à utiliser des bases fixes de décomposition.

6.3 Bases de décomposition fixes

La partition du maillage permet de réduire le temps de calcul en diminuant la taille de la matrice C. Une deuxième solution pour cela est de choisir une base de décomposition fixe permettant de précalculer les transformations. Cela permet de réduire le temps de calcul à la fois au codeur et au décodeur. Pour cela, on remplace la connexité originale par une connexité régulière de valence 6 partout sauf sur les bords [43]. Les vecteurs de base sont alors les mêmes pour toutes les partitions. L'économie en temps s'accompagne d'un gain en mémoire du même ordre. Nous avons choisi (d'après [43]) d'utiliser des grilles régulières contenant un nombre au carré de sommets. La paramétrisation de Tutte (cf. section 2.4.4, [75]) d'une telle connexité, avec un nombre variable de sommets, est représentée sur la Fig. 6.7.

Les bases de décomposition spectrale sont alors symétriques, de taille fixée, et peuvent même être codées en dur dans le codeur et le décodeur afin de réduire encore le temps de calcul. Sur une telle structure, on peut procéder à une transformée de Fourier rapide, car alors l'opérateur laplacien est stationnaire presque partout. Afin de décomposer la géométrie partitionnée sur une telle base, il faut résoudre deux problèmes :

- *Augmenter la taille de chaque partition jusqu'au nombre carré immédiatement supérieur au nombre de sommets dans la partition.* En effet, notre boîte noire MeTiS ne fait que viser un nombre moyen de sommets dans les partitions, et nous avons besoin

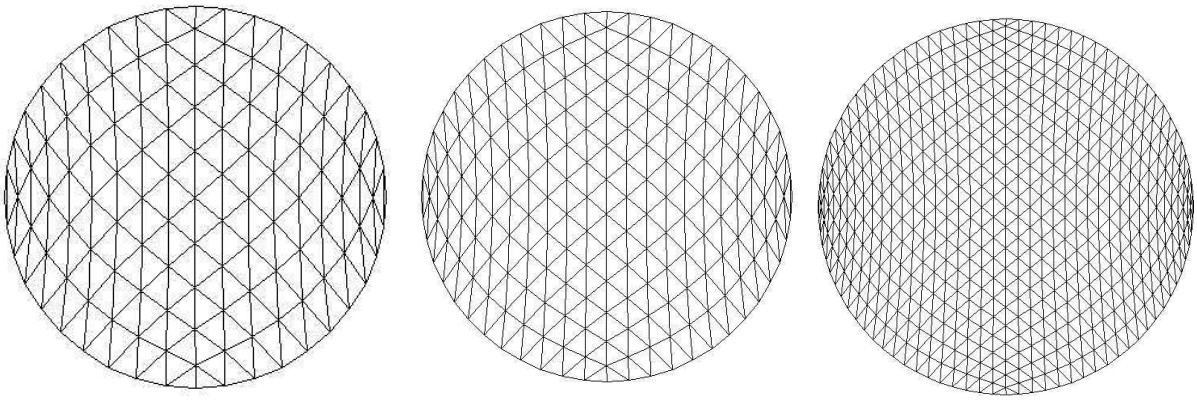

FIG. 6.7 – Paramétrisations barycentriques d'une connexité régulière de valence 6 partout sauf sur les bords (pour un nombre au carré variable de sommets : $11^2 = 121$, $14^2 = 196$, et $23^2 = 529$). Une grille de n^2 sommets en contient $4(n-1)$ sur les bords. Une telle connexité a des bases de décomposition dont la taille est fixe, et qui peuvent être codées en dur au codeur comme au décodeur. Nous avons utilisé la dernière grille, contenant 529 sommets.

de partitions dont le nombre de sommets peut être fixé arbitrairement),

– *Etablir une bijection entre les sommets du maillage original et ceux du maillage de connexité régulière.* La suite de la stratégie de [43] consiste à apparier les sommets de la connexité originale avec ceux de la connexité régulière (on vient en quelque sorte assigner de nouveaux voisins, 6 presque partout, à chaque sommet : notre bijection est en réalité un appariement entre les sommets de la base naturelle et ceux de la base fixe).

6.3.1 Augmentation des partitions et recouvrement

Deux approches sont possibles pour augmenter la taille des partitions jusqu'au nombre carré immédiatement supérieur. Nous présentons l'approche originale, due à Karni et Gotsman[43], qui consiste à rajouter des sommets n'apportant pas d'innovation géométrique. Ensuite, nous présentons notre propre approche, qui étend les partitions en les faisant se recouvrir. Nous comparerons plus loin notre approche par recouvrement avec celle de [43] dans le cadre de la transmission progressive de la géométrie.

Augmentation de Karni et Gotsman

Pour augmenter les tailles de leurs partitions, les auteurs de [43] insèrent des sommets fictifs qui n'apportent pas d'innovation géométrique. Ils procèdent en rajoutant autant de sommets qu'il faut en les plaçant au barycentre des points d'un triangle (voir Fig. 6.8). Ces sommets fictifs sont connus implicitement au décodeur. Il suffit d'avoir les mêmes règles implicites d'augmentation au codeur et au décodeur : on sait des deux côtés combien de sommets rajouter et où, pour arriver à augmenter les partitions jusqu'au carré supérieur. Par exemple, on insérera des sommets fictifs dans les premiers triangles de la connexité

originale.

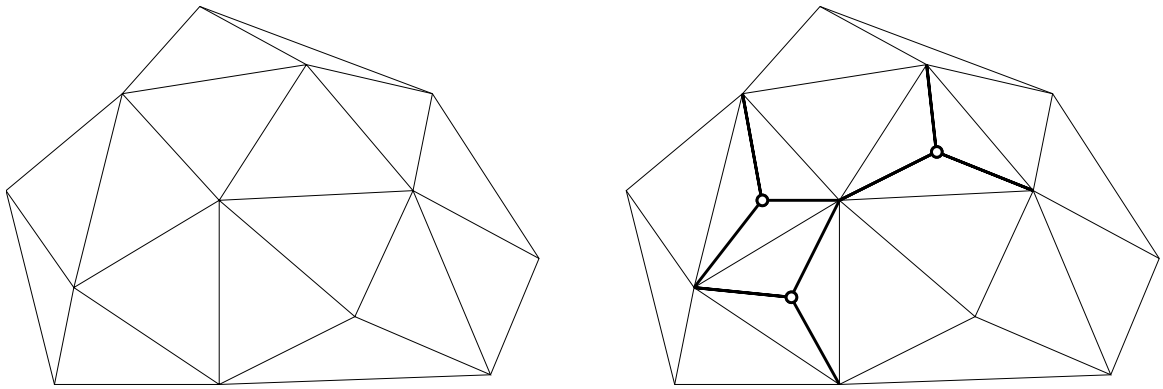

FIG. 6.8 – Augmentation des partitions d'après [43]. On insère implicitement des sommets fictifs qui n'apportent pas d'innovation géométrique, à partir de la connexité originale. Cela vaut tant pour le codeur que pour le décodeur. A gauche, un maillage de 13 sommets, auxquels trois sommets fictifs ont dû être ajoutés (à droite) pour arriver à $4^2 = 16$.

Augmentation par recouvrement

Nous inspirant des transformées avec recouvrement, nous choisissons d'augmenter nos partitions en allant chercher des sommets dans les partitions voisines. Nous procédons par un mouvement en spirale dirigé vers l'extérieur, en conquérant les sommets un-par-un jusqu'à ce que le carré supérieur soit atteint. Nous schématisons notre méthode en Fig. 6.9. Chaque partition augmentée comporte exactement un nombre au carré de sommets (n^2) même si le nombre de sommets sur les bords peut être différent de $4(n-1)$.

Nos résultats en transmission progressive de la géométrie montreront l'apport de notre approche par recouvrement face aux artefacts visuels dus à la partition du maillage. Nous illustrons visuellement sur la Fig. 6.10 l'apport du recouvrement dans les débuts d'une transmission progresssive de la géométrie. Toutefois, ce recouvrement a un coût, que nous avons caractérisé à l'aide de courbes débit/distorsion (cf. Section 6.4.3).

Enfin, lors de la reconstruction, les coordonnées d'un sommet appartenant à plusieurs partitions seront calculées comme le barycentre des contributions de chaque partition pour ce sommet. Nous opérons ainsi un moyennage qui rend plus douce la transition entre les partitions au début de la transmission.

6.3.2 Transfert sur la connexité régulière

Nous souhaitons à présent établir une bijection entre la connexité originale augmentée et la 6-connexité régulière. Cette bijection sera établie dans l'espace paramétrique barycentrique de Tutte. On cherche donc à assigner de nouveaux voisins à chaque sommet de la connexité originale, de manière à ce qu'ils aient tous 6 voisins sauf sur les bords (voir Fig. 6.11).

Soient P_o et P_r les coordonnées paramétriques des sommets de la connexité originale et de la connexité régulière, respectivement. On cherche une bijection b^{opt} parmi toutes les

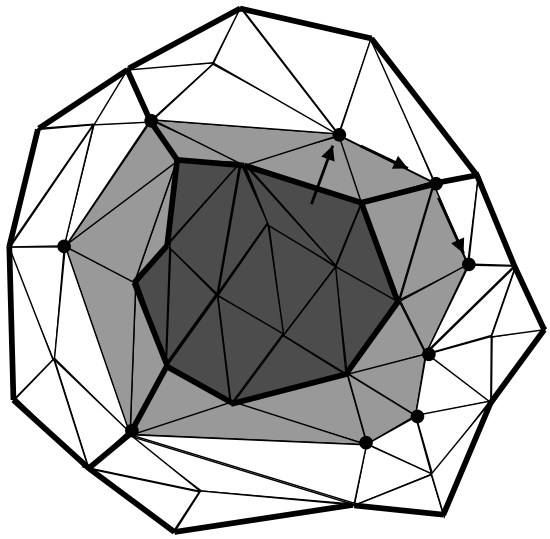

FIG. 6.9 – Augmentation des partitions par recouvrement : on vient conquérir en spirale des sommets situés dans les partitions voisines.

bijections possibles $b : P_o \leftrightarrow P_r$ telle que :

$$b^{opt} = \min_b \sum_i \|P_o(i) - P_r(i)\|^2 \tag{6.10}$$

Deux solutions ont été envisagées. Dans la première, adoptée dans [43], on résout localement l'optimisation en divisant l'espace paramétrique en parties de plus en plus grosses. Considérons maintenant le problème tel qu'il se pose en réalité. Nous devons associer un sommet de P_o avec exactement un autre de P_r, sous contrainte de minimiser la distance paramétrique entre les sommets ainsi appariés.

On peut voir ce problème comme un problème de couplage maximal dans un graphe biparti, ou comme un problème d'affectation. On doit trouver une matrice de permutation des sommets qui minimise l'erreur totale commise dans l'espace paramétrique. Pour cela, on construit la matrice des coûts entraînés par l'assignation d'un sommet $P_o(i)$ de la paramétrisation naturelle à un sommet $P_r(j)$ de la paramétrisation fixe (le coût est la distance paramétrique entre $P_o(i)$ et $P_r(j)$). Les problèmes de couplage maximal dans un graphe biparti sont résolus en général par la méthode de Ford-Fulkerson [29] (pour la maximisation de flot dans un graphe avec puits et source), moyennant une petite extension du graphe biparti pour lui adjoindre une source et un puits (voir [17]). Si l'on le voit comme un problème d'affectation, on pourra utiliser une heuristique du genre de la méthode des Hongrois, que nous ne détaillons pas (voir [1] pour les détails). Pour notre part, nous avons choisi cette dernière voie, en utilisant une heuristique développée dans [41] dont le code source est accessible depuis le réseau.

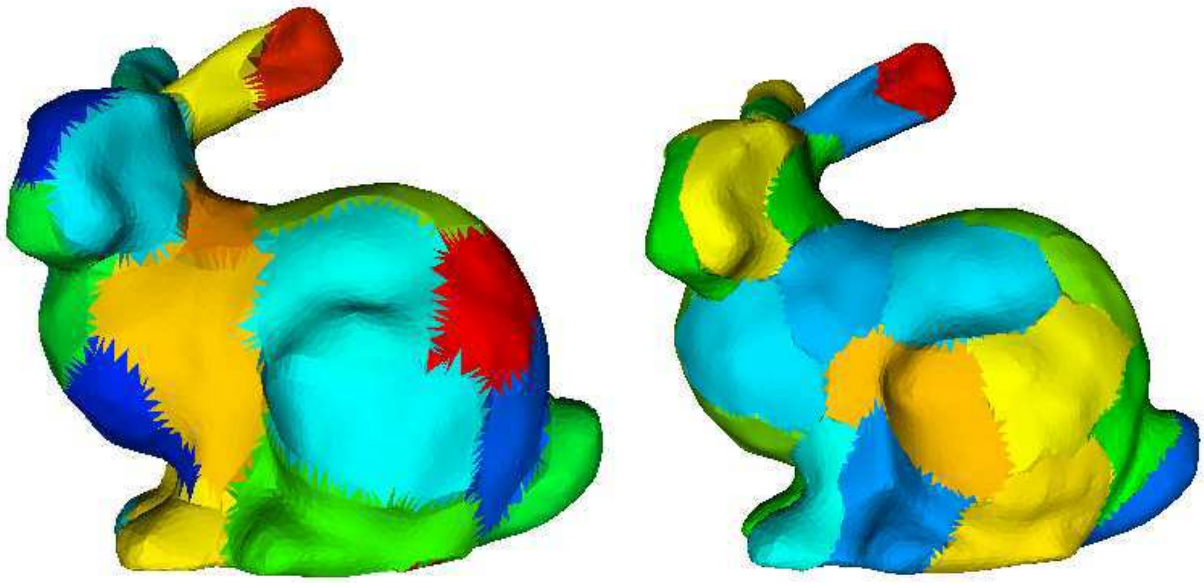

Fig. 6.10 – Effet du recouvrement sur les artefacts visuels dus à la partition du maillage : à droite, l'objet est partitionné en partitions de 500 sommets, puis reconstruit avec 5% des coefficients spectraux sur les bases naturelles. A gauche, la taille moyenne des partitions est de 400 sommets, auxquels sont rajoutés 20% de sommets en plus par augmentation ; le maillage est toujours reconstruit avec 5% des coefficients spectraux sur les bases naturelles. Le recouvrement permet d'atténuer les artefacts aux frontières des partitions. Les coefficients spectraux n'ont pas été quantifiés.

6.3.3 Cylindres topologiques

MeTiS ne donne malheureusement aucune garantie quant à la topologie des partitions obtenues, spécialement dans le cas de longues formes élancées (oreille de lapin, patte de cheval, etc.) qui peuvent générer des partitions homéomorphes à des cylindres, même si la grande majorité des partitions obtenues sont homotopes à des disques. Lors de l'assignation, il faut donc composer avec ce bord supplémentaire. Pour cela, nous plaçons le bord supplémentaire au centre de la partition paramétrisée, pour obtenir l'équivalent d'un disque audio physique, avec le trou au centre. Aucun traitement particulier n'est effectué pour les sommets du bord intérieur de la paramétrisation naturelle cylindrique. Les partitions n'ayant pas une topologie de disque posent problème pour la reconstruction progressive de la géométrie avec des bases fixes de décomposition (le problème ne se produit pas avec des bases naturelles). En effet, il faudra en pratique transmettre la quasi-totalité des coefficients spectraux avant que la reconstruction soit visuellement acceptable. Nous illustrons ce problème, que ne semblent pas avoir rencontré les auteurs de [42, 43], sur la Fig. 6.12. En pratique, nous fixons une certaine distance visuelle minimale (calculée par l'Eq. 2.31) qui détermine le nombre de coefficients spectraux à envoyer avant affichage pour chaque partition.

Nous n'avons malheureusement trouvé aucune explication de ce phénomène, et nous sommes contentés de pallier ses désagréments du mieux que nous avons pu. En particulier,

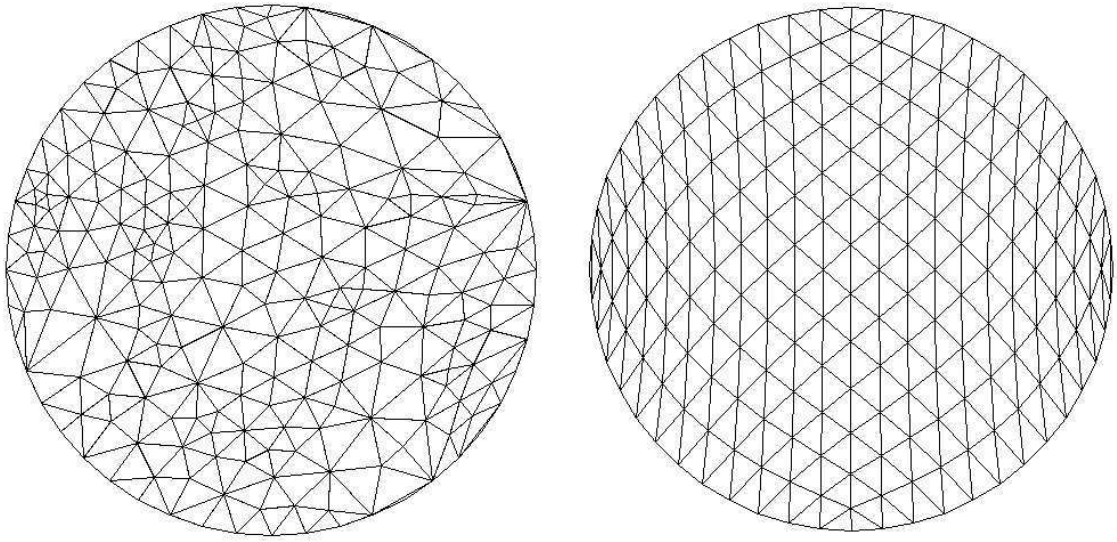

FIG. 6.11 – L'établissement de la bijection entre la connexité originale augmentée (à gauche) et la connexité régulière (à droite) se fait dans l'espace paramétrique barycentrique de Tutte.

ces partitions seront détectées lors de l'insertion du tatouage et ne pourront pas être tatouées. Dans une optique de transmission progressive de la géométrie, il faudrait veiller à placer au début de la transmission l'intégralité des coefficients de ces partitions problématiques. Une convention implicite à ce sujet serait nécessaire entre l'encodeur et le décodeur. Une telle solution devrait être envisagée tant qu'un moyen de partitionner un maillage quelconque en disques topologiques n'aura pas été trouvé.

6.4 Un codeur/décodeur géométrique spectral

Nous avons à présent tous les outils pour construire un codeur et un décodeur fonctionnant fondé sur la décomposition spectrale. De façon à réduire la longueur du message transmis, les coefficients spectraux doivent être quantifiés (idéalement en s'adaptant au signal) et codés de manière entropique. Nous avons fabriqué un codeur de Huffman pour l'occasion [39]. Chaque vecteur de coefficients spectraux est traité de la même manière : ses éléments sont quantifiés uniformément sur 14 bits (comme proposé dans [42]), puis mis en forme dans un train binaire compressé.

6.4.1 Schémas d'implantation

Nous donnons ici les deux schémas fonctionnels reflétant notre implantation tant pour le codeur que le décodeur. En particulier, nous traitons les partitions l'une après l'autre. La mise en forme du train binaire spectral est constituée de tronçons comme suit : les coefficients spectraux étant classés par valeur propre associée croissante dans chaque partition, on vient les ordonner d'abord suivant les partitions, puis par valeur décroissante. Le premier

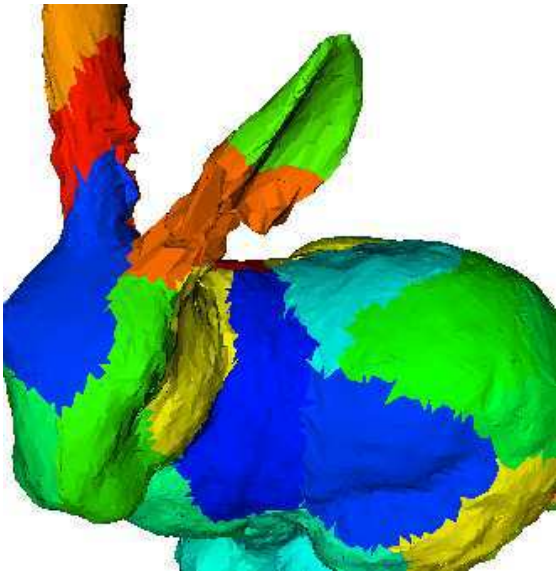

FIG. 6.12 – Mauvaise impression visuelle lors de la reconstruction d'une partition homotope à un cylindre en utilisant des bases fixes (voir chaque oreille), alors que les sous-maillages homotopes à des disques sont mieux reconstruits (à nombre égal de coefficients spectraux pour chaque partition).

tronçon donnera toutes les premières composantes continues des partitions, le second tronçon apportera le second coefficient spectral de toutes les partitions, etc. Nous illustrons la mise en forme du train binaire permettant d'obtenir une transmission progressive de la géométrie sur la Fig. 6.13. Le schéma du codeur est illustré sur la Fig. 6.14, et le schéma du décodeur sur la Fig. 6.15.

6.4.2 Transmission progressive de la géométrie

Nous présentons dans ce paragraphe les résultats que nous avons obtenus en compression spectrale de la géométrie, et donc aussi en transmission progressive comme la décomposition spectrale le permet. Afin de tracer les courbes débit/distorsion, nous avons choisi de mesurer la distorsion à l'aide d'une distance fondée sur le laplacien géométrique (comme dans [42]), voir Eq. 2.30. Nous donnons nos résultats tant avec des bases naturelles de décomposition, que des bases fixes (ce que n'ont pas fait les auteurs de [43]). Il semble donc que nous soyons les premiers à nous y aventurer. Comme nous l'avons précisé plus haut, la décomposition spectrale permet la transmission progressive de la géométrie. Nous l'illustrons en Fig. 6.16 pour un maillage de CAO permettant de mieux appréhender les artefacts visuels dus à ce type de transmission. On constate, pour ce type d'objets, qu'il faut attendre la fin de la transmission pour disposer d'un objet utilisable qui soit non seulement visuellement satisfaisant, mais aussi numériquement. Sans doute avons-nous ici affaire à un phénomène de Gibbs provoquant des oscillations résiduelles lorsque l'on coupe les hautes fréquences dans une transformée à fenêtre (notre fenêtre est ici une partition).

$(PQR)_1^1$	$(PQR)_1^2$	...	$(PQR)_1^{N_P}$
$(PQR)_2^1$	...		$(PQR)_2^{N_P}$

...

$(PQR)_z^1$	...	$(PQR)_z^{N_P}$

FIG. 6.13 – Mise en forme des triplets de coefficients spectraux dans le train binaire. On appelle N_P le nombre de partitions contenant chacune z sommets.

6.4.3 Compression et bases naturelles

Nous avons voulu aussi montrer l'apport de notre procédure de recouvrement dans la transmission progressive avec des bases de décomposition naturelles (c'est à dire hors de leur but premier qui était d'augmenter les partitions jusqu'au même nombre de sommets). Nous avons fixé à notre procédure de recouvrement d'atteindre 20% de sommets en plus par partition. Les résultats montrent que si l'apport est indéniable au début de la transmission (voir Fig. 6.10), on paie en revanche un surcoût de transmission (de l'ordre de 2 bits par sommet) dû à un nombre plus important de partitions à transmettre (voir Fig. 6.17 et Fig. 6.18). Toutefois, sur des objets naturels, nous avons pu vérifier que l'œil s'accomode d'un maillage reconstruit avec un surcoût de seulement 1 bit/sommet. Les bases naturelles sont celles offrant le meilleur taux de compression, et sont donc dédiées à des applications d'archivage par exemple, car la lenteur du décodeur interdit leur utilisation pour la transmission avec un rendu progressif.

Les résultats obtenus sont conformes à ceux présentés dans [42], même si notre quantificateur (uniforme) est loin d'être adapté à la distribution des coefficients spectraux. On notera enfin que la métrique visuelle utilisée pour quantifier la distorsion varie avec le maillage et la manipulation considérés (comparer les ordonnées des Fig. 6.17 et 6.18) : on ne peut donc pas établir pour l'heure de valeur de la métrique visuelle universelle pour laquelle déclarer que le maillage est convenablement reconstruit. Une telle valeur dépend encore de chaque maillage. C'est sans doute la raison pour laquelle les résultats sont un peu moins bons. Toutefois, nous disposons à présent d'un codeur de source géométrique spectral, contre lequel nous nous proposons de développer un schéma de tatouage robuste face à ce type de compression de la géométrie. Nous n'avons présenté que les résultats concernant le codage de source de la géométrie, cela afin de pouvoir comparer avec [42].

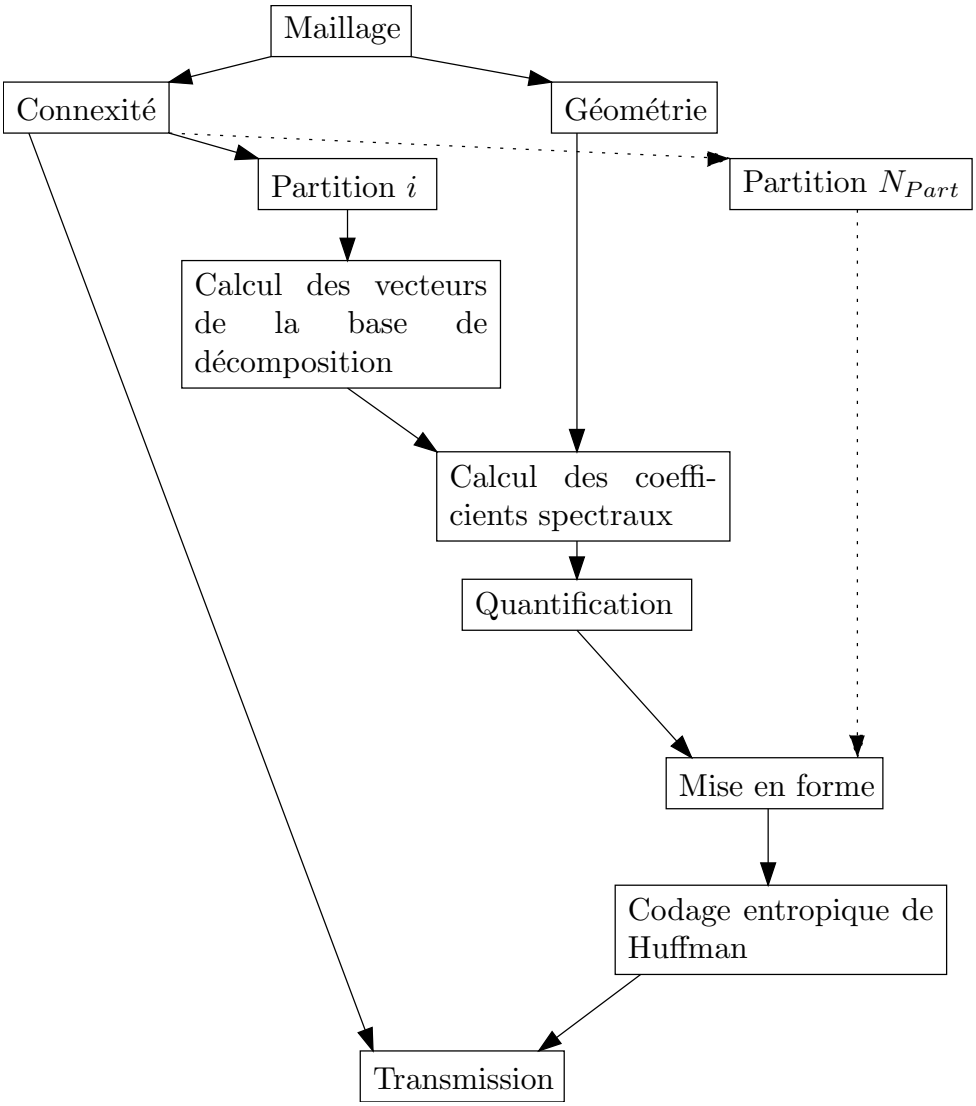

FIG. 6.14 – Schéma du codeur spectral de la géométrie.

6.4.4 Transmission et bases fixes

Nous donnons sur la Fig. 6.19 une courbe débit/distorsion correspondant à l'utilisation de bases fixes de décomposition. Nous rappelons que [43] ne propose pas les résultats associés à cette technique, et on comprendra sans doute pourquoi au vu de la courbe. En pratique, nous n'avons pas implanté l'augmentation de Karni et Gotsman : nous avons donc demandé à MeTiS des partitions un peu en deçà d'une valeur carrée, afin de recourir le moins possible à l'augmentation par recouvrement (la courbe notée "NO LOT" sur la Fig. 6.19). Ensuite, nous avons fait jouer à plein le recouvrement (courbe notée "LOT") en demandant 20% d'augmentation des partitions en moyenne, et c'est cette différence que les résultats permettent d'apprécier. Les bases fixes, même si elles induisent un important surcoût comme nous verrons, restent les seules à permettrent un affichage suffisamment rapide à mesure que

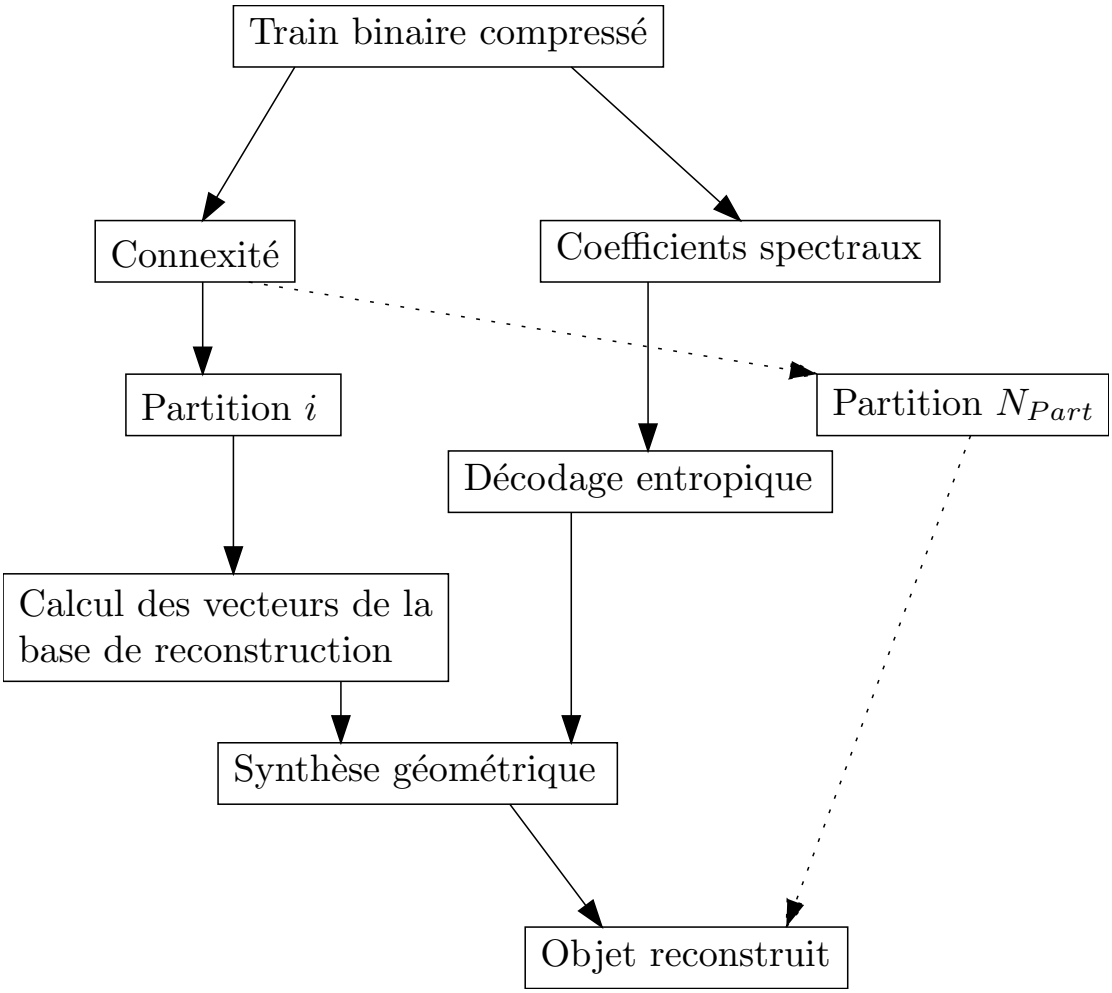

FIG. 6.15 – Schéma du décodeur spectral de la géométrie.

les coefficients spectraux arrivent au décodeur.

Une remarque s'impose encore : pour utiliser le recouvrement, nous devons nécessairement demander à MeTiS des partitions plus petites que si nous ne l'utilisions pas. Ainsi, les risques de créer des partitions homéomorphes à des cylindres s'amenuisent-elles. De fait, sur la Fig. 6.19, le recouvrement a permis de générer seulement deux partitions homotopes à des cylindres, contre quatre sans l'utiliser. Même si le recouvrement améliore la transmission par bases fixes, celle-ci reste de nettement moins bonnes qualité que la transmission utilisant les bases naturelles du maillage.

En effet, il apparaît clairement que l'utilisation de bases fixes nécessite un très grand surcoût de transmission. Mais on notera cependant combien le recouvrement améliore les performances de la compression par bases fixes (de l'ordre de 12 bits par sommet). En fait, la compression par bases fixes sans recouvrement ne compresse en réalité que très peu l'information : un maillage non compressé voit chacune des coordonnées de ses sommets codées sur un entier de 32 bits (96 bits/sommets), or on atteint seulement 68 bits/sommets sans recouvrement, et on atteint environ 52 bits/sommets avec (sur la Fig. 6.19). Cela est

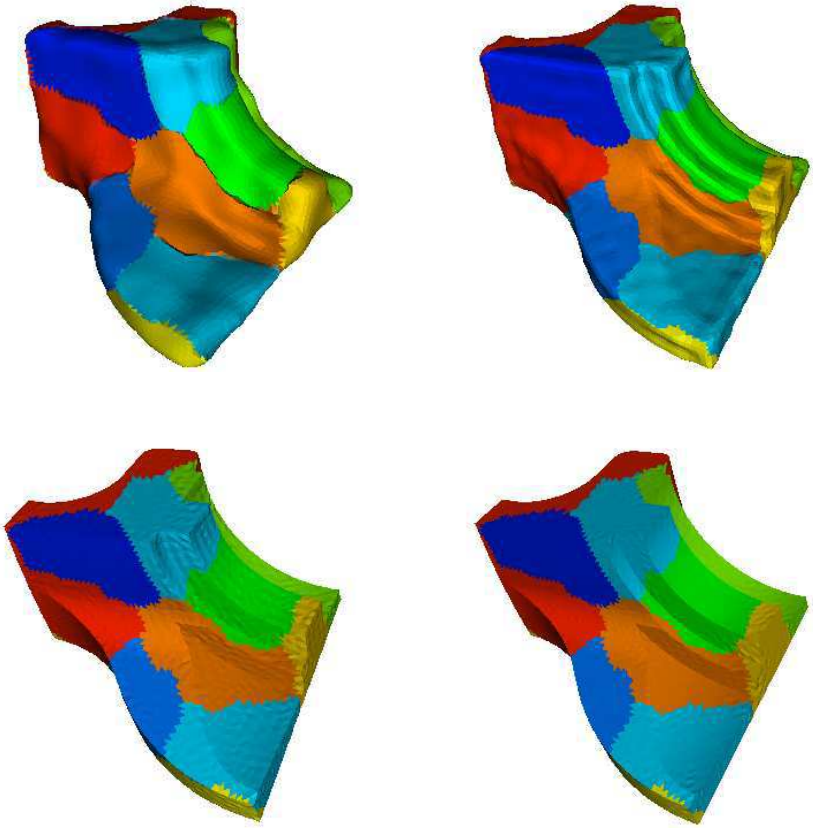

FIG. 6.16 – Visualisation d'un objet de CAO reconstruit à diverses étapes de la transmission. Sur ces objets, on doit attendre la toute fin de la transmission pour retrouver un objet utilisable. La décomposition spectrale n'est pas adaptée à la compression d'une telle géométrie non naturelle. On a représenté une reconstruction avec 5%, 15%, 25%, et 95% des coefficients spectraux. Données : Pratt & Whitney.

dû au fait que l'on cherche à décorréler la géométrie sur une connexité régulière sans rapport avec elle. Or, comme nous l'avons vu, la connexité semble transporter d'elle-même une partie de l'information géométrique - et c'est cette information que nous perdons par l'utilisation de bases fixes de décomposition. La première étude sur la forme contenue dans la connexité est présentée dans [40], et soulève davantage de questions, passionnantes au demeurant, qu'elle n'en résout.

Nous représentons sur la Fig. 6.20 la courbe débit-distorsion en bases fixes pour le modèle *head* (pour comparer avec la Fig. 6.17). Toutes les partitions sont des disques topologiques, contrairement à la Fig. 6.19. Il faut attendre plus longtemps le premier affichage, mais il est de meilleure qualité qu'avec des bases naturelles, et la qualité augmente quasi-linéairement avec la quantité d'information spectrale transmise.

Nous justifions à présent perceptuellement, autant qu'il est possible, notre choix de 14

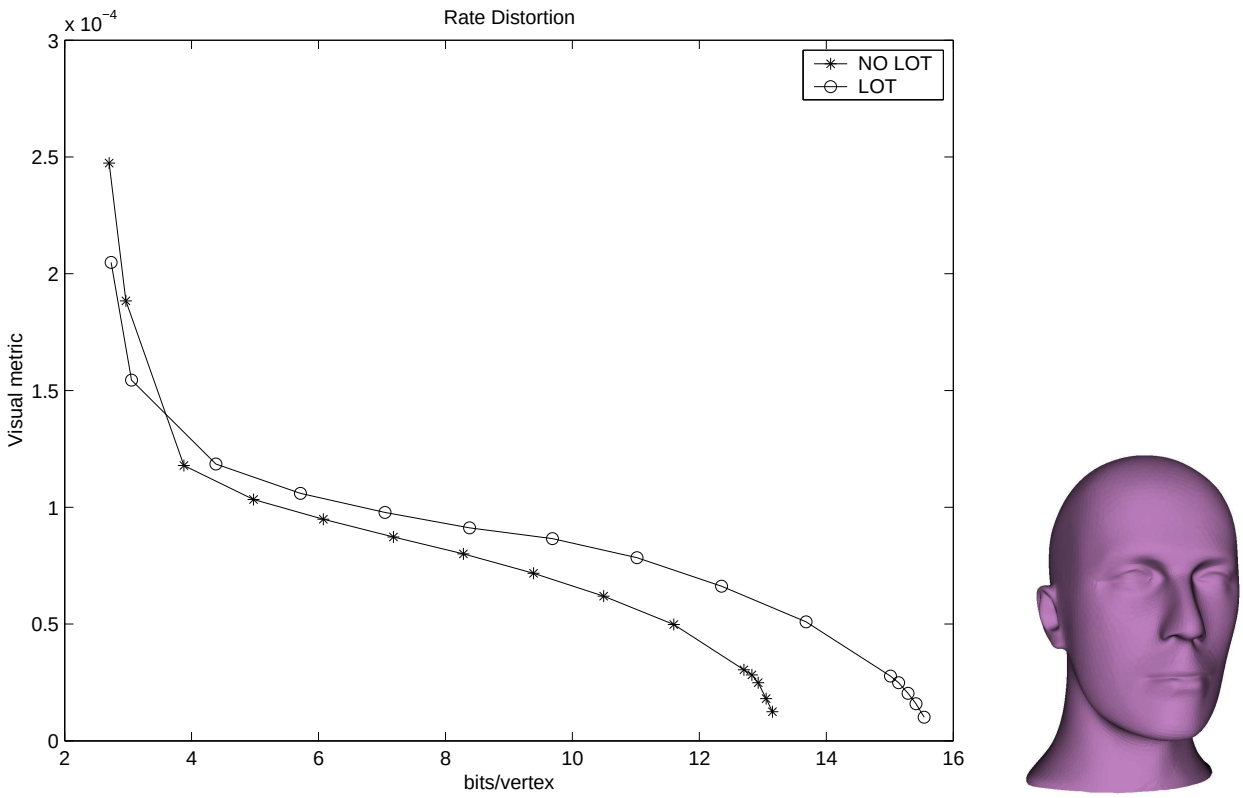

FIG. 6.17 – Résultats en compression spectrale de la géométrie (bases naturelles) : courbes débit/distorsion pour la mesure de l'Eq. 2.30. Le recouvrement (noté LOT) fait intervenir un surcoût en fin de transmission qui compense la meilleure qualité visuelle obtenue au début de la transmission progressive de la géométrie. Les courbes ne s'annulent pas à la fin de la transmission à cause de la quantification des coefficients spectraux. Données : Technical Arts, Co.

bits de quantification. On note sur la Fig. 6.19 que l'on n'atteint pas, en pratique, une reconstruction parfaite à la fin de la transmission. Cela est dû à la quantification. Nous illustrons sur la Fig. 6.21 les artefacts visuels liés à la quantification des coefficients spectraux (bases fixes). En outre, comme le montre le bruit persistant sur le cylindre topologique vert à la base de l'oreille gauche sur la Fig. 6.21, les partitions homotopes à des cylindres sont celles qui souffrent le plus de la quantification des coefficients spectraux. Toutefois, nous croyons que le problème consistant à partitionner un maillage en disques topologiques, s'il est ardu, dépasse de loin notre seul cadre de travail : on pourrait par exemple imaginer de distribuer plus efficacement les calculs de remaillage, de paramétrisation, etc. On peut voir le problème de trouver le schéma polygonal d'un maillage comme un point de départ pour la résolution de celui qui nous occupe. Les disques topologiques sont cependant convenablement reconstruits avec 14 bits de quantification, même sur des bases fixes de décomposition qui décorrèlent pourtant moins bien l'information géométrique.

Si l'utilisation des bases fixes de décomposition est possible pour des objets naturels, il n'en va pas de même pour les modèles de CAO, qui sont particulièrement affectés par la

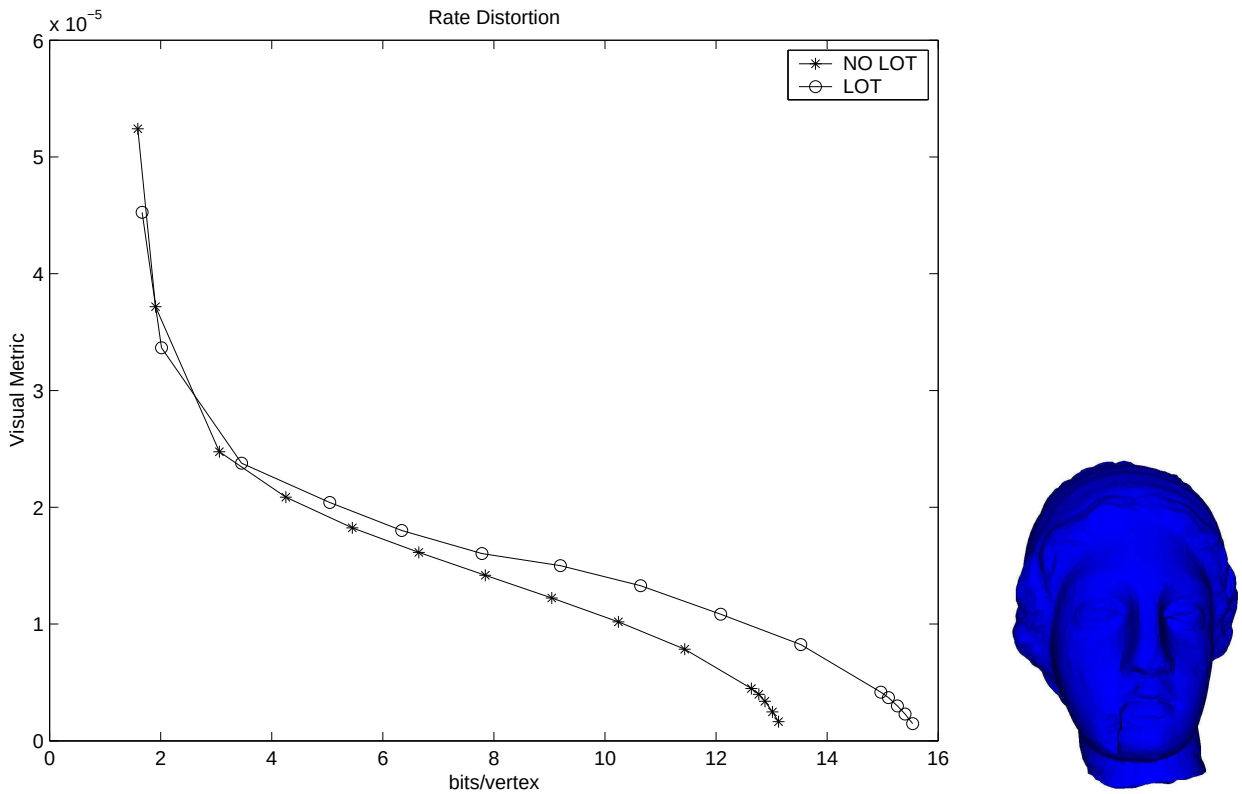

FIG. 6.18 – Résultats en compression spectrale de la géométrie (bases naturelles) : courbes débit/distorsion pour la mesure de l'Eq. 2.30. Le recouvrement (noté LOT) fait intervenir un surcoût en fin de transmission qui compense la meilleure qualité visuelle obtenue au début de la transmission progressive de la géométrie.

quantification des coefficients spectraux, comme illustré sur la Fig. 6.21 pour laquelle on a pourtant utilisé 16 bits de quantification. En particulier, la décomposition spectrale ne permet pas de garantir la parfaite reconstruction des surfaces fonctionnelles de l'objet, et se révèle pour cette raison, croyons-nous, intrinsèquement inadaptée à ce genre d'objets.

6.4.5 Remarques sur la décomposition spectrale

C'était pour des raisons d'implantation et de complexité que Taubin n'avait pas utilisé son opérateur laplacien pour la compression, et nous avons voulu explorer ce qu'il en est avec les moyens d'aujourd'hui. Comme nous l'avons vu, afin de ne pas être limités par la taille du maillage à traiter, il faut le partitionner. Cette première étape introduit des artefacts visuels à la reconstruction sur les bords des partitions.

La qualité de la décorrélation de la géométrie est optimale si l'on utilise les bases naturelles de décomposition, mais au prix d'un temps de calcul plus important, et d'un usage de la mémoire plus dispendieux (il faut stocker toutes les fonctions de base de chaque partition). Seule l'utilisation de bases fixes permet aujourd'hui un temps de calcul acceptable (quelques minutes) et propice à la transmission progressive (en terme de rendu progressif

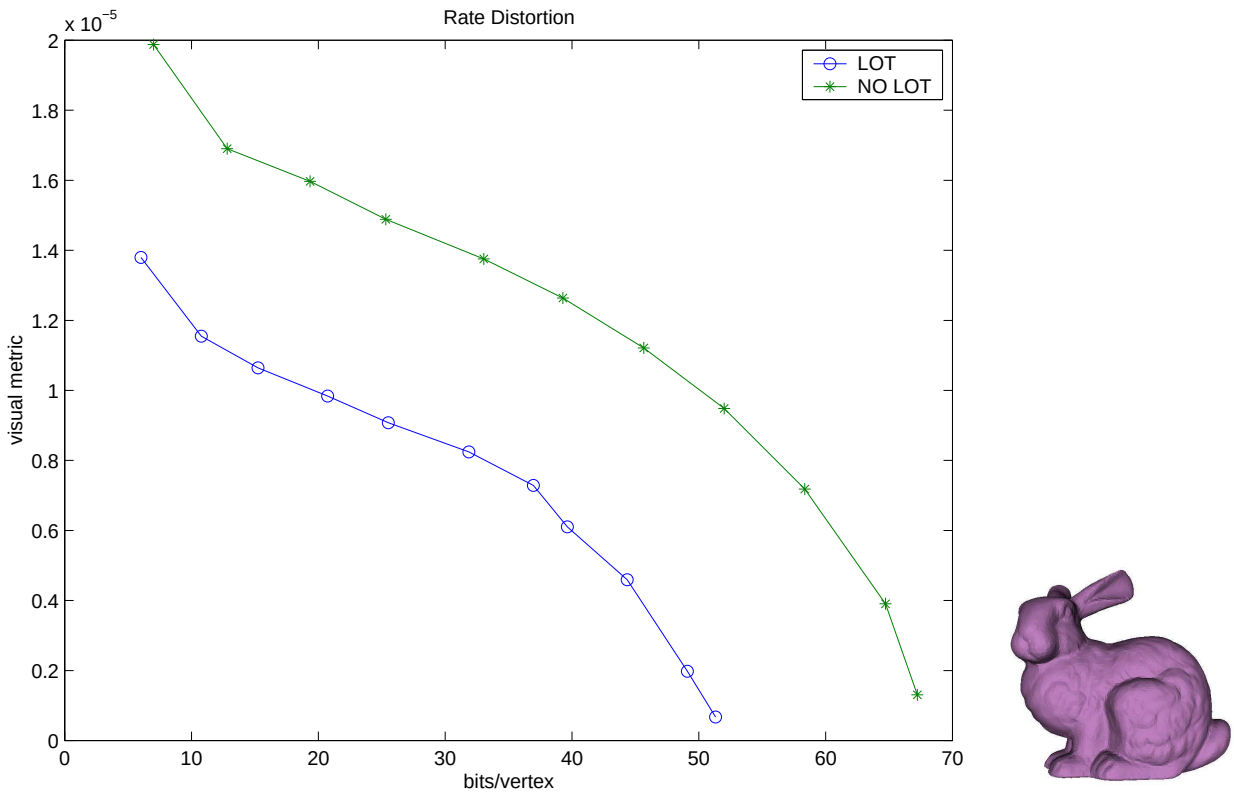

FIG. 6.19 – Résultats en compression spectrale de la géométrie (bases fixes) : courbes débit/distorsion pour la mesure de l'Eq. 2.30. Le recouvrement (noté LOT) améliore la qualité de la transmission, même si la qualité de la décorrélation est bien moindre. Données : Stanford 3D Scanning Repository.

rapide au décodeur). Toutefois, c'est au prix d'un surcoût de transmission important dû à l'inadaptation de la grille régulière aux données géométriques que l'on se propose pourtant de compresser.

C'est en tenant compte des limitations de l'environnement de calcul que l'on optera pour l'une ou l'autre technique. Pour nous, nous avons utilisé des bases fixes de décomposition pour deux raisons supplémentaires :

- Nous souhaitions uniquement tester l'effet de la quantification des coefficients spectraux (nous ne cherchons pas à transmettre efficacement la géométrie),
- L'attaque sur la marque est plus pernicieuse encore que si l'on utilisait des bases naturelles.

6.5 Tatouage spectral de la géométrie

Après avoir présenté précisément notre codeur spectral de la géométrie, nous pouvons aborder la conception d'un schéma de tatouage pour l'espace de la décomposition spectrale de la géométrie. Nous utiliserons pour le tatouage une décomposition spectrale avec les pro-

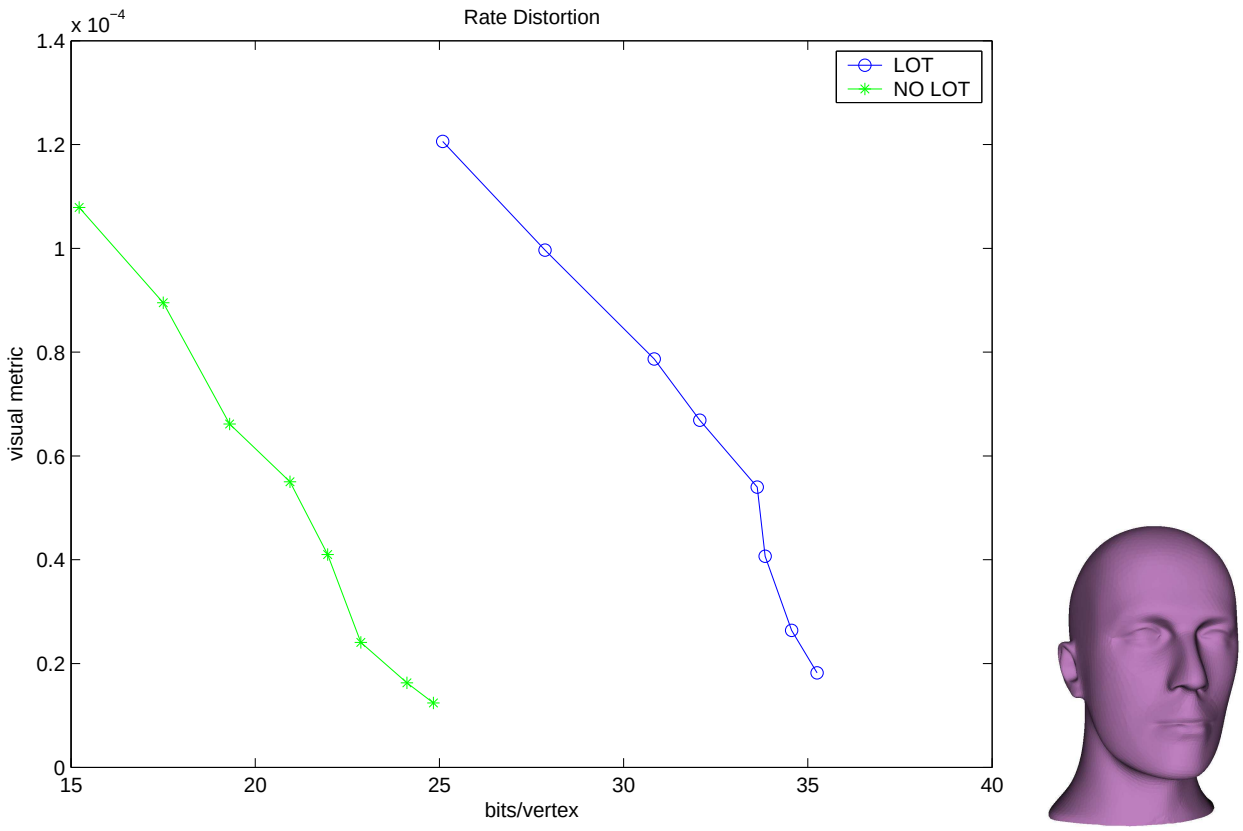

FIG. 6.20 – Résultats en compression spectrale de la géométrie (bases fixes) : courbes débit/distorsion pour la mesure de l'Eq. 2.30. Le recouvrement (noté LOT) améliore la qualité de la transmission, même si la qualité de la décorrélation est bien moindre. Données : Technical Art, Co.

priétés suivantes : utilisation de bases fixes avec recouvrement de 20%. L'utilisation d'un domaine de représentation redondant pour le tatouage n'est pas neuve, voir par exemple [59] pour l'image 2D. Pour nous, nous nous proposons de modifier les relations des coefficients spectraux entre eux. Nous représentons sur la Fig. 6.22 les trois spectres de chaque coordonnée X, Y et Z d'une partition. Comme pour nos travaux en tatouage fragile, nous essaierons de masquer la présence du tatouage à un éventuel pirate, en ne fixant pas de valeur prédéfinie de notre variable de tatouage. Nous détaillons à présent plus précisément notre schéma de tatouage spectral de la géométrie. Ce schéma sera de type substitutif, à l'inverse de celui proposé dans [58] qui, toujours dans l'espace spectral de la décomposition, est de type additif.

6.5.1 Schéma de tatouage

Notre méthode de tatouage agit de la même manière sur toutes les partitions, décomposées chacune sur des bases fixes. Les 3 vecteurs X, Y, Z de N coordonnées sont transformés en vecteurs spectraux P, Q, R, ordonnés suivant les valeurs propres croissantes. Chaque triplet

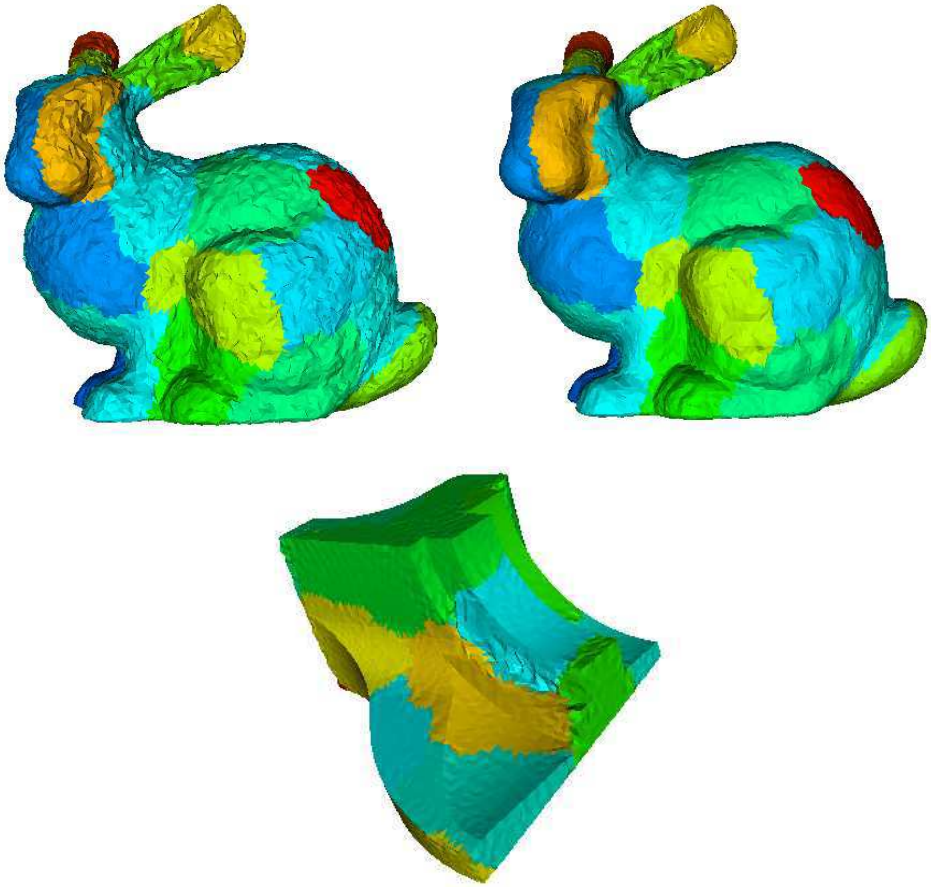

FIG. 6.21 – Artefacts liés à la quantification des coefficients spectraux en utilisant des bases fixes : en haut à droite, 12 bits de quantification ; en haut à gauche, 14 bits. L'effet de la quantification est particulièrement sensible sur les partitions homéomorphes à des cylindres. En bas : modèle de CAO reconstruit à l'aide de bases fixes, avec 16 bits de quantification des coefficients spectraux. La décomposition spectrale, à cause de la perte due à la quantification, est inadaptée à ce genre d'objets.

spectral P_i, Q_i, R_i est considéré séparément pour y cacher un bit. On procède simplement en déplaçant la valeur médiane du triplet de part ou d'autre de la moyenne du minimum et du maximum. Pour des raisons d'imperceptibilité, on ne peut pas effectuer de déplacement trop important : ce déplacement sera donc rapporté à un facteur r. Nous avons fixé expérimentalement $r = 10$. Le tatouage se fait sur les coefficients non quantifiés.

On s'étonnera à bon droit du caractère sommaire, voire grossier, de notre procédure d'insertion de la marque. Cependant, nous souhaitons tester notre méthode de tatouage face à la compression géométrique spectrale de la géométrie. Une telle compression, comme nous l'avons vu, ne peut être efficace qu'en utilisant des bases naturelles de décomposition. Par contre, afin de gagner en temps de calcul, nous avons construit un espace de tatouage fondé sur des bases fixes de décomposition. Ne connaissant pas les interactions entre le passage d'une base naturelle de décomposition à une bases fixe, nous avons préféré débuter

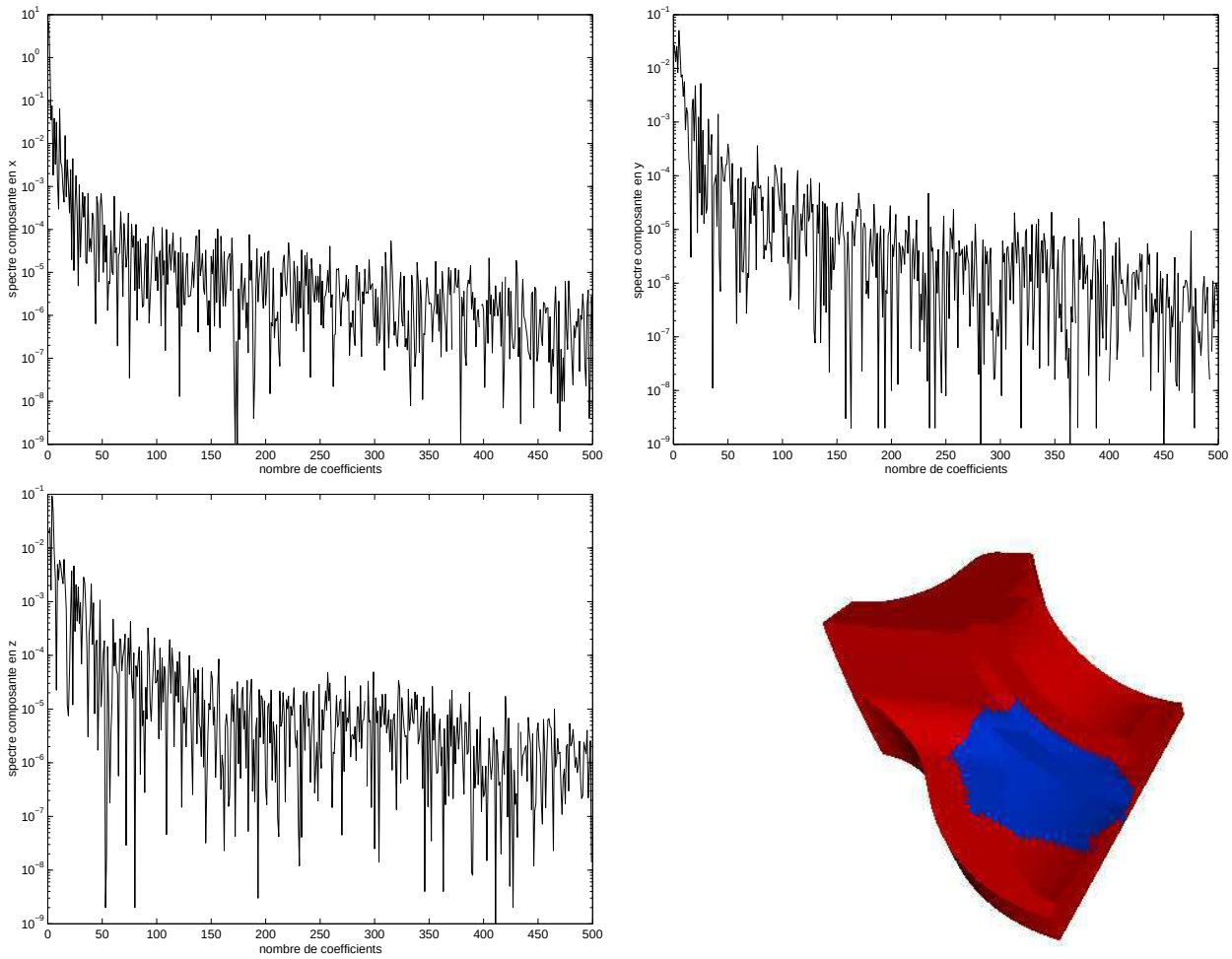

FIG. 6.22 – Spectres de chaque coordonnée X, Y et Z d'une partition d'un modèle de CAO. Notre schéma de tatouage modifiera les relations des coefficients spectraux entre eux.

notre étude avec une manipulation sensible des coefficients spectraux. Nous reconnaissons là l'aspect le moins achevé de notre étude.

Afin d'assurer l'imperceptibilité du tatouage, on ne peut pas tatouer tous les triplets (à commencer par la composante continue). Si chaque partition contient N_P sommets (autant de triplets spectraux), on commencera à tatouer à partir du triplet numéro t_0. On peut ainsi définir la force d'insertion f en fonction du rapport entre le numéro du premier triplet porteur d'information, et le nombre de sommets dans la partition :

$$f = \frac{t_0}{N_P} \tag{6.11}$$

La stratégie de codage de canal que nous avons mise en œuvre est fondée sur une simple répétition. Chaque bit est donc répété n_r fois par partition, avec :

$$n_r = \lfloor \frac{N_P - t_0}{64} \rfloor \tag{6.12}$$

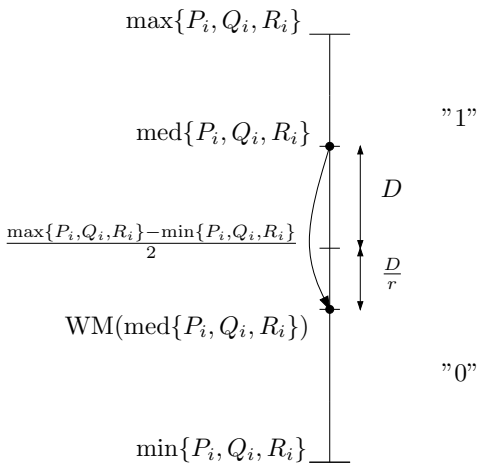

FIG. 6.23 – Schéma de tatouage spectral : un triplet spectral permet de cacher un bit.

Toutefois, entre chaque répétition, une clef secrète modifie l'ordre dans lequel les bits sont inscrits. Cela permet à la fois de garantir le secret (en le faisant porter sur les numéros des bits cachés), et surtout de donner à chaque bit caché la même chance d'être relu. A la détection, la clef permet de relire immédiatement la marque. Nous utilisons alors une simple stratégie de détection à la majorité : la valeur du bit relue est celle ayant été détectée le plus souvent.

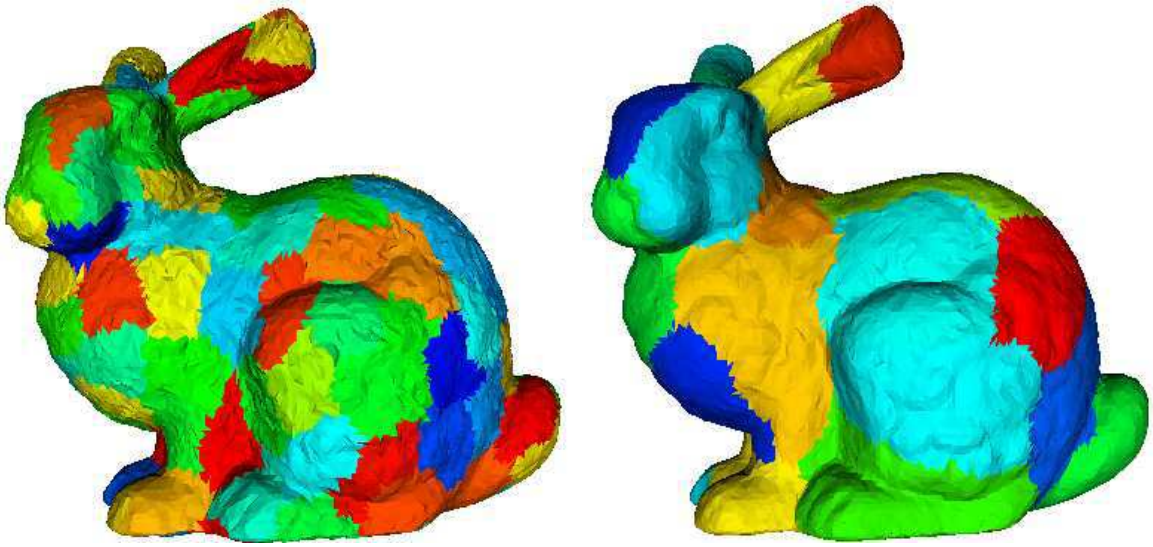

FIG. 6.24 – Tatouage, à force égale, du même objet avec une taille de partition $N_P = 100$ (gauche) et $N_P = 500$ (droite).

Enfin, nous avons vérifié la cohérence entre les tailles de partition en compression et en tatouage. Sur la Fig. 6.24, nous montrons le même objet naturel tatoué avec une taille de partition de $N_P = 100$ sommets et $N_P = 500$. Nous vérifions que la taille de partition que

nous avons employée en compression peut encore servir au tatouage. On observe un effet du tatouage bien plus visible s'il y a moins de sommets par partition. Nous conserverons donc notre taille de partition autour de 500 sommets ($23^2 = 529$ avec des bases fixes). On peut ainsi imaginer un codeur/tatoueur géométrique spectral effectuant le travail de tatouage directement après la projection de la géométrie sur les bases de décomposition, et avant la quantification.

6.5.2 Force et distorsion

Nous cherchons à présent à évaluer la distorsion introduite par notre schéma de tatouage. Pour cela, nous traçons la courbe de la distorsion en fonction de la force d'insertion. Nous mettons aussi en évidence l'apport du recouvrement dans un tel contexte. Les Fig. 6.25 et Fig. 6.26 montrent l'effet du tatouage sur la distorsion, avec et sans recouvrement. En particulier, on constate que le recouvrement permet de tatouer des fréquences plus basses à distorsion égale. Nous pensons que ce résultat est dû au fait que nous tatouons les moyennes/hautes fréquences, dont le recouvrement se fixe précisément pour objectif de limiter les perturbations erratiques aux frontières des partitions. Nous rappelons que dans le cadre des bases fixes de décomposition, nous opérons un moyennage des coordonnées des sommets appartenant à plusieurs partitions.

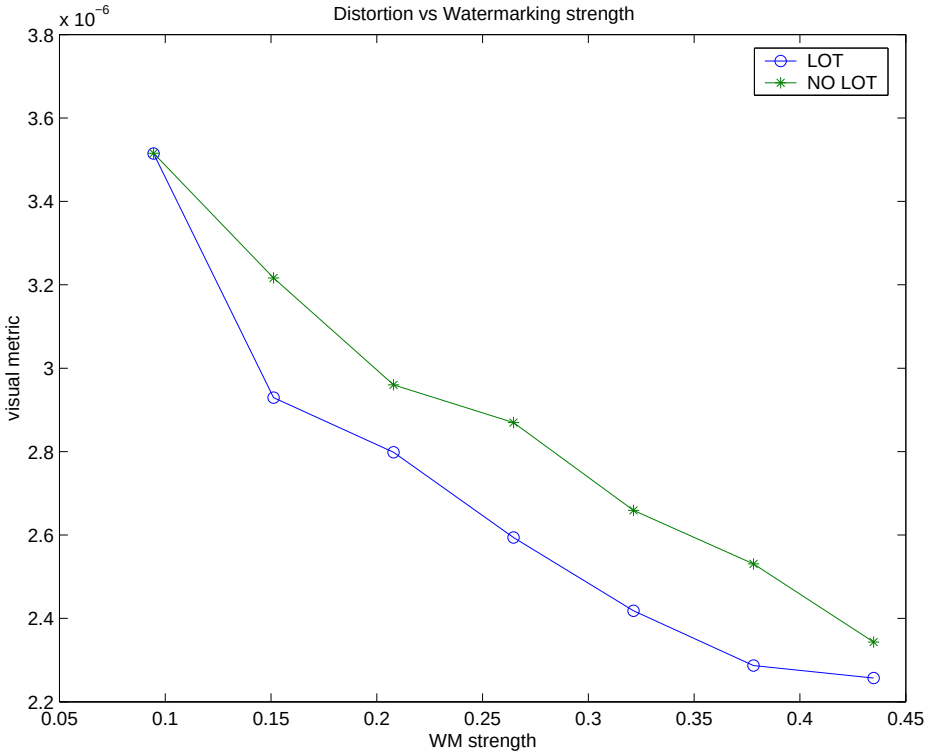

FIG. 6.25 – Courbe force/distorsion pour un modèle naturel, avec et sans recouvrement.

La métrique de distorsion que nous avons employée ne permet pas de fixer une même valeur limite d'imperceptibilité, ni pour les différentes manipulations (compression géomé-

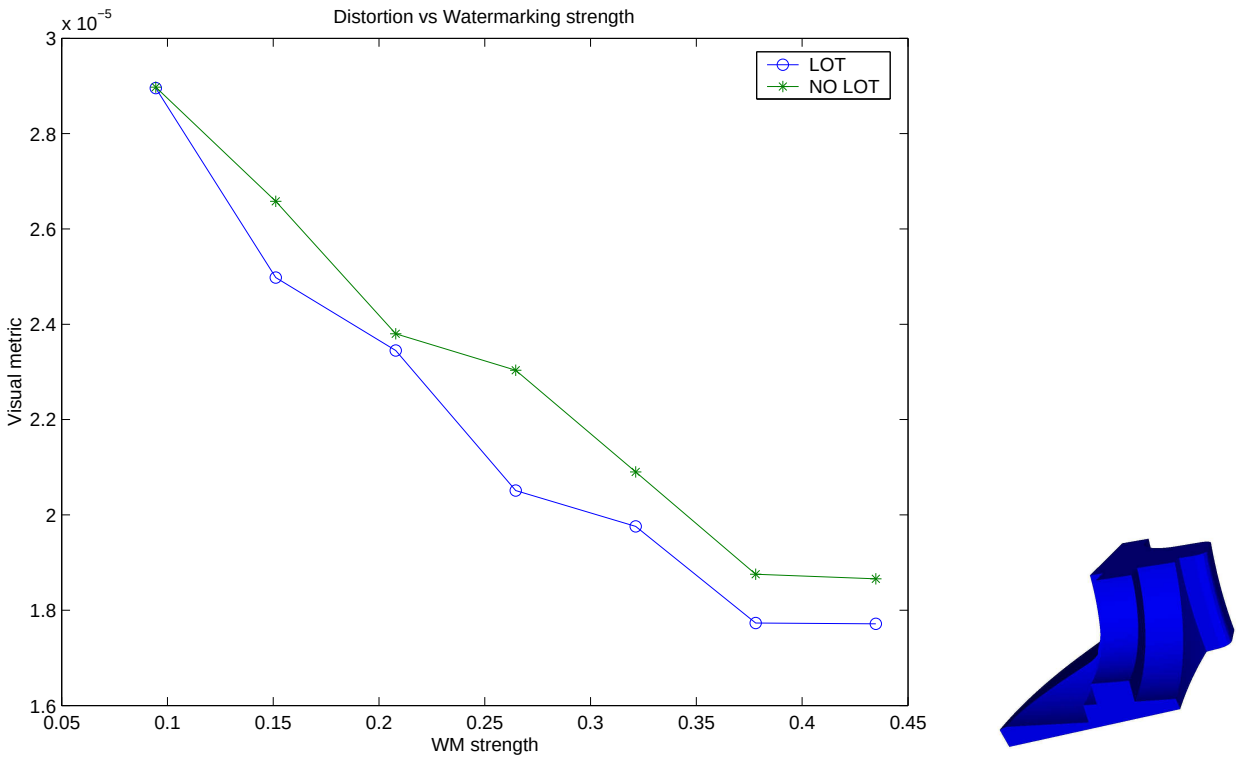

FIG. 6.26 – Courbe force/distorsion pour un modèle de CAO, avec et sans recouvrement.

trique ou tatouage), ni pour les différents modèles. En cela, le traitement de la géométrie se distingue encore du traitement du signal sur des données régulièrement échantillonnées : nous ne disposons toujours pas d'outil permettant une comparaison fiable entre deux objets, comme le PSNR entre deux images. En conséquence, la mesure que nous utilisons ne peut servir qu'à l'évaluation ponctuelle de la distorsion : pour une manipulation donnée sur un objet particulier, on ne pourra que mesurer l'influence de tel ou tel paramètre. Nous ne nous autoriserons donc pas à comparer ce qui ne peut l'être.

Nous avons donc fixé empiriquement, pour chaque objet, la force maximale de tatouage à la limite de l'imperceptibilité. Par exemple, nous avons fixé la force de tatouage à 0.33 pour le modèle de la Fig. 6.25, et à 0.4 celle du modèle de CAO de la Fig. 6.26 (le tatouage se voit toutefois toujours sur ces modèles, quelle que soit la force de tatouage employée, car les surfaces fonctionnelles planes trahissent la moindre modification). Ce type de modèle se prête mal aux manipulations par décomposition spectrale, mais permet de mieux mettre en évidence les artefacts dus au tatouage, comme illustré sur la Fig. 6.27 (à comparer avec l'objet naturel de la Fig. 6.24).

6.5.3 Résultats

Nous présentons à présent les résultats que nous avons obtenus pour diverses attaques : translation, mise à l'échelle uniforme, rotation, lissage par laplacien, ajout de bruit et compression spectrale par quantification et codage entropique. Notons tout d'abord que les calculs

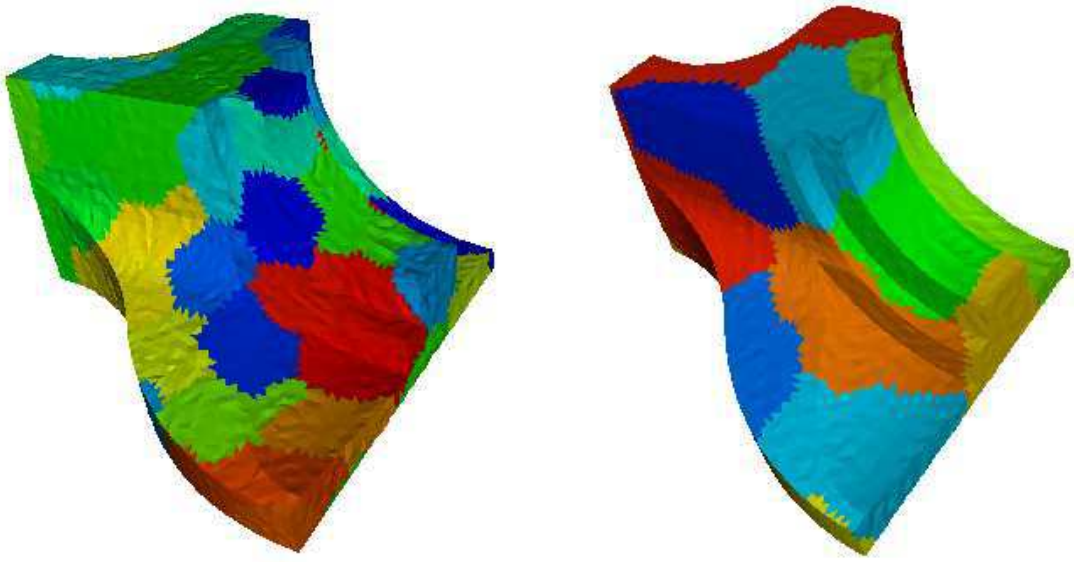

FIG. 6.27 – Artefacts dus au tatouage pour un modèle de CAO : $N_P = 100$ (gauche) et $N_P = 500$ (droite). La force de tatouage est la même pour les deux images que pour la Fig. 6.24

de décomposition se font dans le repère de référence de l'objet, et qu'une rotation efface donc potentiellement la marque. Un préalable à la relecture de la marque serait le recalage de l'objet à tester sur l'objet original. Pour cela, on peut utiliser différentes méthodes [15, 10, 26], et les auteurs de [58] proposent de recaler l'objet en se servant des 5 premières valeurs propres de la décomposition spectrale. Nous n'avons malheureusement pas eu l'opportunité d'implanter un tel recalage, et les résultats doivent donc s'entendre indépendamment de perturbations de la connexité. Nous exposons en Fig. 6.28 les résultats obtenus pour diverses attaques uniquement géométriques. On voit en particulier que la robustesse à la rotation n'est effective que pour de petits angles de rotation.

Objet	Bunny	Horse	Venus	Head
Bruit	0.44%	0.37%	0.25%	0.25%
Lissage (itérations)	20	20	20	20
Translation	OK	OK	OK	OK
Mise à l'échelle	0.2	0.2	0.2	0.2
Rotation	<15°	<15°	<15°	<15°
Quantification spectrale (bits)	14	14	14	14

FIG. 6.28 – Résultats obtenus en tatouage spectral face à diverses manipulations géométriques. Nous avons relevé les valeurs limites pour lesquelles les 64 bits ont été correctement relus.

Enfin, nous montrons sur la Fig. 6.29 la proportion de bits correctement relus en fonction

du nombre de bits de quantification des coefficients spectraux du codeur géométrique spectral (bases naturelles). Nous représentons les courbes correspondant à un tatouage avec et sans recouvrement entre partitions. On constate que la marque est correctement relue à partir de 14 bits de quantification, ce qui est la limite inférieure d'utilisation du codeur. Nous pouvons donc déclarer notre schéma de tatouage robuste face à une telle compression géométrique. En outre, le recouvrement n'influence quasiment pas la relecture.

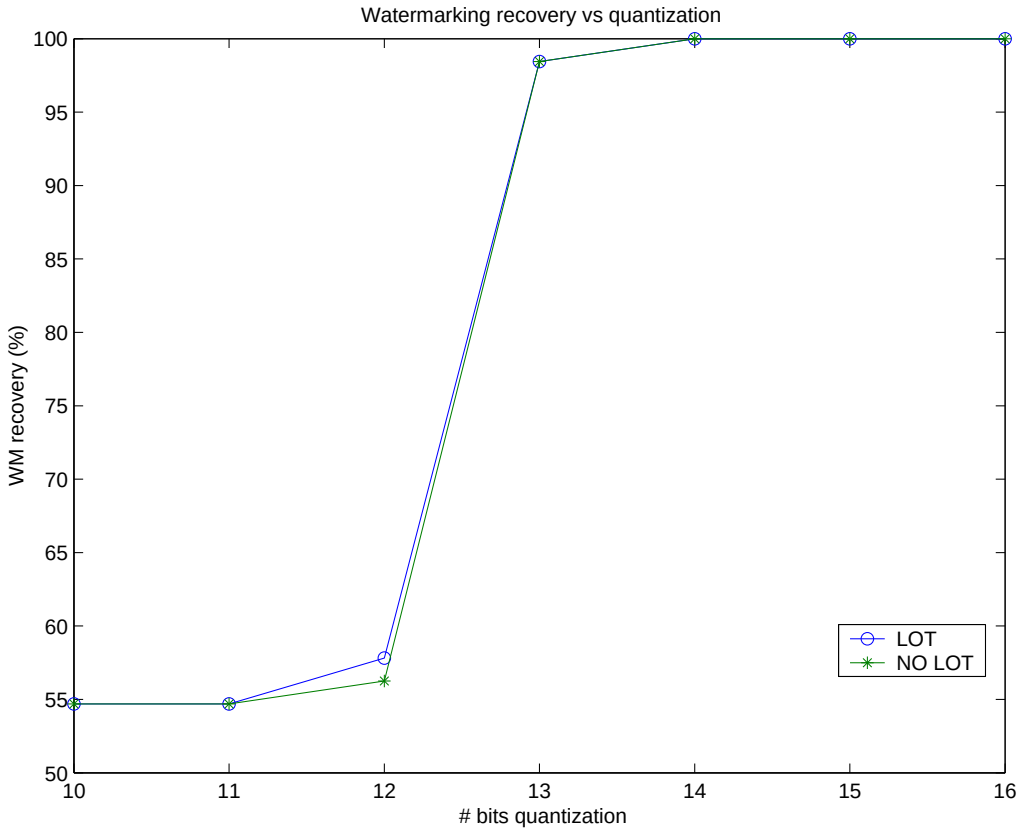

FIG. 6.29 – Robustesse de notre schéma spectral (bases fixes) face à une compression géométrique spectrale (bases naturelles). La marque est correctement relue à partir de 14 bits de quantification des coefficients spectraux, ce qui est la limite inférieure d'utilisation de notre codeur géométrique spectral.

Il va de soi que si l'on souhaite en sus une robustesse face à des attaques modifiant la connexité, on devra, en l'état, procéder à un recalage sur l'objet original. Le schéma de tatouage n'est alors plus aveugle, et nécessite de revoir les détails du cadre applicatif. Notons que Patrice Rondao-Alface tente dans ses travaux de thèse à l'UCL de se passer d'un tel recalage, et de retrouver directement sur le modèle à tester une zone tatouée à partir des seules caractéristiques différentielles de l'objet (ombilics, etc.) Il s'agit en quelque sorte de tatouage de seconde génération (fondé sur le contenu) pour les objets 3D.

6.6 Conclusion

Nous confessons bien humblement le caractère encore exploratoire de ces travaux sur la décomposition spectrale des objets surfaciques 3D. Comme nous l'avons vu, il nous a fallu trouver des solutions ad hoc aux problèmes soulevés par l'implantation de références restées parfois évasives sur ces difficultés. Nous pensons particulièrement aux problèmes de partition homotopes à des cylindres, et à l'assignement d'une connexité fixe à une géométrie définie sur une connexité arbitraire.

Malgré tout, il nous a été possible de développer un codeur/décodeur géométrique spectral, adapté à la compression (avec des bases naturelles de décomposition) et à la transmission progressive de la géométrie (avec des bases fixes). La réalisation de ce codeur nous a permis de développer une nouvelle approche, fondée sur le recouvrement entre partitions. Nous avons montré l'apport du recouvrement dans le cadre de la transmission progressive de la géométrie, et le (léger) surcoût induit en compression.

Des contraintes temporelles nous ont interdit de procéder au développement d'une méthode de tatouage plus élaborée. En particulier, nous aurions souhaité rendre l'insertion adaptative (autant que possible), et implanter une méthode de recalage qui aurait permis de tester la robustesse de notre schéma de tatouage face à des attaques modifiant la connexité (simplification, coupe, etc.) Toutefois, cette approche par recalage présente l'inconvénient majeur de rendre la méthode de tatouage non aveugle. Nous avons évoqué une approche visant à s'affranchir de ce problème.

Pourtant, nos résultats en tatouage sont plutôt encourageants : la robustesse naturelle de notre schéma permet de s'affranchir de plusieurs attaques géométriques. En outre, si l'on devait malgré tout considérer une approche par recalage (des axes d'inertie dans le cadre d'une analyse en composantes principales, ou en utilisant les 5 premières valeurs propres comme dans [58]), les résultats face à la rotation montrent que l'on peut sans doute se contenter d'un recalage même médiocre pour aligner l'objet à tester sur l'objet original.

Conclusion

Le tatouage des objets surfaciques 3D, s'il a été rendu nécessaire par le développement de leurs applications et la baisse de leur coût de transmission, n'en souffre pas moins encore de l'absence d'une théorie du traitement numérique de la géométrie analogue à celle du traitement du signal. Comme pour les autres types de données multimédia, les besoins existent pourtant, et varient de la protection des droits et de la copie (tatouage robuste), à l'authentification et l'intégrité (tatouage fragile).

Notre travail s'est donc organisé autour de deux axes : le tatouage fragile par invariants géométriques à des fins d'authentification, voire d'intégrité, et le tatouage dans l'espace de décomposition spectrale de la géométrie pour des applications de type protection des droits. Tout au long de nos développements, nous avons surtout cherché à proposer un cadre de travail qui, partant des contraintes liées à la structure même des objets 3D, permette aux tatoueurs de "retrouver leurs sensations" dans ce nouveau contexte parfois si déroutant. Nous espérons nous être acquittés correctement de cette tâche dans la première partie de notre travail, et regrettons que la décomposition spectrale se soit montrée si retorse dans la seconde partie. Nous concluons ce travail autour de chacun des deux thèmes que nous avons abordés.

Tatouage fragile par invariants

En tatouage fragile par invariants, nous avons clairement séparé ce qui relève des prérogatives des tatoueurs (la technique d'écriture de l'information cachée), de celles des algorithmiciens (le parcours du maillage). Ainsi, nous avons pu proposer une méthode de tatouage fragile qui, à notre connaissance, est la seule à permettre d'appréhender correctement nombre de concepts communs en tatouage : plus petite quantité de média protégée, seuil de fausse alarme, sécurité des clefs employées pour dissimuler le message, et classe de robustesse.

Sans doute la suite logique de cette partie serait-elle la mise au point d'une méthode de vérification de l'intégrité, comprise en complément de notre méthode pour l'authentification, ou encore l'étude de la robustesse face au codage de source (afin d'étendre la classe de robustesse à des méthodes de compression avec pertes). En outre, notre méthode a l'avantage d'être purement analytique là où les autres doivent recourir à une heuristique locale [82]. C'est, croyons-nous, une bonne propriété de notre méthode, qu'il faudrait chercher à préserver : la caractérisation fine de grandeurs comme la longueur de clé utilisée ou la robustesse face à la quantification des coordonnées en dépend.

Tatouage dans l'espace de la décomposition spectrale

L'implantation d'une méthode de décomposition spectrale s'est révélée en pratique beaucoup plus ardue que prévu. Au moins les difficultés que nous avons souhaité mettre en lumière illustrent-elles les points d'achoppement d'une telle approche : ne pouvant diagonaliser rapidement la matrice laplacienne d'un grand maillage, nous avons été confrontés au problème de la partition de tels maillages. Une grande partie de ce travail a visé à pallier les inconvénients de la partition, tout en satisfaisant l'exigence d'un temps de calcul acceptable. En introduisant un recouvrement entre les partitions, nous avons dégagé un degré de liberté supplémentaire qui permet de réduire les artefacts aux frontières des partitions. Nous avons montré quels avantages la transmission progressive pouvait en tirer.

Nous avons pu ainsi caractériser un espace de tatouage, fondé sur des bases fixes de décomposition de la géométrie, qui autorise une robustesse naturelle plus importante que l'approche par invariants face aux attaques géométriques. Toutefois, toutes les méthodes actuelles de tatouage se voulant robustes ne sont pas aveugles, et nécessitent un recalage sur l'objet original. Cette contrainte est, à notre sens, trop forte pour le cadre applicatif visé. C'est la raison pour laquelle nous avons cherché à caractériser les performances de notre méthode de tatouage face à des attaques uniquement géométriques, et en aveugle. Nous pensons que le développement d'une méthode de tatouage dans l'espace de décomposition spectrale de la géométrie, à la condition qu'elle repose sur des partitions fondées sur le contenu de l'objet, est prometteur. Puisse ce travail éclairer la lanterne de ceux qui suivront cette voie, davantage que nous ne l'avons été.

Perspectives

En tatouage fragile, les perspectives ouvertes par notre travail portent essentiellement sur l'intégrité et la robustesse face à la quantification. Il s'agit d'extensions de notre schéma qui ne remettent pas en cause ce que nous avons fait. En effet, on peut conserver tout à fait le cadre de travail que nous avons proposé pour mener à bien ces développements : l'intégrité gagnerait à être mise en évidence par des techniques de morphologie mathématique, et notre procédé analytique d'inscription de l'information cachée autorise le calcul de bornes sur la tolérance de notre schéma face à la quantification des coordonnées.

Cependant, il n'en va pas de même en tatouage dans l'espace de la décomposition spectrale de la géométrie. En effet, le développement d'une méthode de tatouage robuste (aux modifications de la connexité) *et aveugle* reste le grand défi à relever. A notre sens, il faudra pour cela privilégier une approche fondée sur l'analyse du contenu de l'objet. Un tel travail pourra par exemple prendre [53] comme point de départ afin de dégager les caractéristiques sémantiques de l'objet (lignes de crête, etc.) La manipulation des coefficients de la décomposition spectrale de la géométrie interviendrait après ce premier travail de synchronisation sur les caractéristiques sémantiques de l'objet.

Publications

Tatouage par invariants

- F. Cayre & B. Macq, “Spatial watermarking with 3D triangle meshes”, SPIE 46th annual meeting, San Diego, CA, Août 2001.
- F. Cayre & B. Macq, “Data hiding in 3D triangle meshes”, IEEE Transactions on Signal Processing, Vol. 51, Issue 4, pp. 939–949, Avril 2003.
- F. Cayre, F. Schmitt & H. Maître, “Tatouage fragile d’objets 3D triangulés”, Colloque GRETSI, Paris, Septembre 2003.

Tatouage spectral

- F. Cayre, P. Rondao-Alface, F. Schmitt & H. Maître, “Compression and watermarking of 3D triangle meshes”, SPIE 47th annual meeting, Seattle, WA, Juillet 2002.
- F. Cayre, P. Rondao-Alface, F. Schmitt, B. Macq & H. Maître, “Application of spectral decomposition towards compression and watermarking of 3D triangle mesh geometry”, Allerton Conference, Urbana-Champaign, IL, Octobre 2002.
- F. Cayre, P. Rondao-Alface, F. Schmitt & H. Maître, “Application of spectral decomposition to compression and watermarking of 3D triangle mesh gemetry”, Signal Processing : Image Communications, 18(4), pp. 309–319, Avril 2003.

Autres

- F. Cayre & F. Davoine, “Vers un tatouage d’images mou”, Traitement du Signal, 18(4), 2001.
- J. Vorbrüggen & F. Cayre, “The CERTIMARK benchmark : architecture and future perspectives”, Proc. IEEE Conference on Multimedia and Expo ICME’02, Lausanne, Vol. 2, pp. 485–488, Août 2002.
- P. Rondao-Alface, B. Macq, F. Cayre, F. Schmitt & H. Maître, “Lapped spectral decomposition for 3D triangle meshes compression”, IEEE Intl. Conf. on Image Processing ICIP’03, Barcelone, Octobre 2003.

En cours

- Chapitre de livre en français sur le tatouage, sous la direction de Franck Davoine et Stéphane Pâteux.
- F. Cayre, O. Devillers, F. Schmitt & H. Maître, “A new framework for fragile watermarking of 3D triangle meshes with geometrical invariants”.

Bibliographie

[1] R.K. Ahuja, T.L. Magnanti, et J.B. Orlin. *Network flows : theory, algortihms and applications*. Prentice Hall, 1993.

[2] P. Alliez, D. Cohen-Steiner, O. Devillers, B. Levy, et M. Desbrun. Anisotropic polygonal remeshing. Dans *ACM Trans. Graphics, Special issue for SIGGRAPH conference*, 2003. to appear.

[3] P. Alliez, É. Colin de Verdière, O. Devillers, et M. Isenburg. Isotropic surface remeshing. Dans *Proc. Shape Modelling International*, pages 49–58, 2003.

[4] P. Alliez et M. Desbrun. Progressive compression for lossless transmission of triangle meshes. Dans *Proceedings of SIGGRAPH 2001*, pages 198–205, 2001.

[5] P. Alliez, M. Meyer, et M. Desbrun. Interactive geometry remeshing. *ACM Transactions on Graphics*, pages 347–354, 2002. SIGGRAPH '02 Conference Proceedings.

[6] M. Ben-Chen et C. Gotsman. On the optimality of spectral compression of mesh geometry. Preprint 2003, http ://www.cs.technion.ac.il/ gotsman/publications.html.

[7] O. Benedens. Geometry-based watermarking of 3d models. *IEEE Computer Graphics and Applications*, 19(1) :46–55, Jan 1999.

[8] O. Benedens. Two high capacity methods for embedding public watermarks into 3d polygonal models. Dans *Proceedings of ACM Multimedia*, pages 95–99, 1999.

[9] O. Benedens et C. Busch. Towards blind detection of robust watermarks in polygonal models. Dans *Proceedings of EUROGRAPHICS*, volume 19, pages 199–208, 2000.

[10] P.J. Besl et N.D. McKay. A method for registration of 3d shapes. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 14(2) :239–256, 1992.

[11] J.-D. Boissonnat et M. Yvinec. *Géométrie Algorithmique*. Édiscience international, 1995.

[12] M. Botsch et L. Kobbelt. Resampling feature and blend regions in polygonal meshes for surface anti-aliasing. Dans *Proc. Eurographics*, pages 402–410, 2001.

[13] M.P. Do Carmo. *Riemannian Geometry*. Prentice Hall, Inc., 1992.

[14] E. Catmull et J. Clark. Recursively generated b-splines surfaces on arbitrary topological meshes. *Computer Aided Design*, 10(6) :350–355, 1978.

[15] Y. Chen et G. Medioni. Object modeling by registration of multiple range images. *Image Vision Comput.*, 10(3) :145–155, 1992.

[16] M. Chow. Optimized geometry compression for real-time rendering. *IEEE Visualization*, pages 347–354, 1997.

[17] T. Cormen, C. Leiserson, et R. Rivest. *Introduction à l'algorithmique.* Dunod, 1994.

[18] M. Costa. Writing on dirty papers. *IEEE Trans. on Information Theory*, 29(3), 1983.

[19] M. Deering. Geometry compression. Dans *Proc. SIGGRAPH 95*, pages 13–22, 1995.

[20] N. Dyn, D. Levin, et J.A. Gregory. A butterfly subdivision scheme for surface interpolation with tension control. Dans *Proc. ACM Trans. Graphics*, volume 9 :2, pages 160–169, 1990.

[21] M. Eck, T. DeRose, T. Duchamp, H. Hoppe, M. Lounsbery, et W. Stuetzle. Multiresolution analysis of arbitrary meshes. *Computer Graphics*, 29 :173–182, 1995.

[22] J. Eells et L. Lemaire. Another report on harmonic maps. *Bull. London Math. Soc.*, 20 :385–524, 1988.

[23] J. Eells et J.H. Sampson. Harmonic mappings of riemannian manifolds. *Amer. J. Math.*, 86 :109–160, 1964.

[24] J. Erickson et S. Har-Peled. Optimally cutting a surface into a disk. Dans *Proc. 18th Annual Symposium on Comput. Geom.*, pages 244–253, 2002.

[25] G. Farin. *Curves and surfaces for CAGD : a practical guide.* Academic Press, fourth edition édition, 1996.

[26] O. Faugeras. The representation, recognition, and locating of 3d objects. *Int. J. Robotic Res.*, 5(3) :27–52, 1986.

[27] O. Faugeras. *Three-Dimensional Computer Vision.* MIT Press, 1993.

[28] M. Floater. Parameterization and smooth approximation of surface triangulations. Dans *Computer Aided Geometric Design*, volume 14, pages 231–250, 1997.

[29] L.R. Ford et D.R. Fulkerson. *Flows in networks.* Princeton university press, 1963.

[30] T. Furon, I. Venturini, et P. Duhamel. Unified approach of asymmetric watermarking schemes. Dans *Proc. SPIE Security and Watermarking of Multimedia Contents III*, volume 4314, pages 269–279, 2001. San Jose, CA.

[31] M. Garland et P. Heckbert. Surface simplification using quadric error metrics. Dans *Proccedings of SIGGRAPH*, pages 209–216, 1997.

[32] S. Gumhold et W. Strasser. Real-time compression of triangle mesh connectivity. Dans *Proc. SIGGRAPH*, pages 133–140, 1998.

[33] A. Guéziec, F. Bossen, G. Taubin, et C. Silva. Efficient compression of non-manifold polygonal meshes. Dans *Proc. IEEE Visualization*, pages 73–80, 1999.

[34] A. Guéziec, G. Taubin, F. Lazarus, et W. Horn. Cutting and stitching : Converting sets of polygons to manifold. *IEEE Trans. on Visualization and Computer Graphics*, 7(2) :136–151, Apr-Jun 2001.

[35] T. Harte et A.G. Bors. Watermarking 3d models. Dans *Proc. of Int. Conf. on Image Processing (ICIP)*, volume 3, pages 661–664, Rochester, NY, USA, Sept 2002.

[36] C. Hernandez et F. Schmitt. Multi-stereo 3d object reconstruction. Dans *Proc. 1st Intl. Symposium on 3D Data Processing Visualization and Transmission (3DPVT)*, 2002.

[37] H. Hoppe. Progressive meshes. Dans *Proceedings of SIGGRAPH*, pages 99–108, 1996.

[38] H. Hoppe, T. DeRose, T. Duchamp, J. McDonald, et W. Stuetzle. Mesh optimization. Dans *Proc. SIGGRAPH*, pages 19–26, 1993.

[39] D.A. Huffman. A method for the construction of minimum-redundancy codes. *Inst. Radio Engineering*, pages 1098–1101, 1952.

[40] M. Isenburg, S. Gumhold, et C. Gotsman. Connectivity shapes. Dans *Proc. Visualization'01 Conference*, pages 135–142, 2001.

[41] R. Jonker et A. Vogenant. A shortest augmenting path algorithm for dense and sparse linear assignment problems. *Computing*, 38 :325–340, 1987.

[42] Z. Karni et C. Gotsman. Spectral compression of mesh geometry. Dans *Proceedings of SIGGRAPH*, pages 279–286, 2000.

[43] Z. Karni et C. Gotsman. 3d mesh compression using fixed spectral bases. Dans *Proceedings of Graphics Interface*, pages 1–8, Jun 2001.

[44] G. Karypis et V. Kumar. Metis : A software package for partitioning unstructured graphs, partitioning meshes and computing fill-reducing orderings of sparse matrices. Rapport technique, Univ. of Minnesota, Dpt. of Computer Science, 1998.

[45] A. Khodakovsky, P. Alliez, M. Desbrun, et P. Schröder. Near-optimal connectivity encoding of 2-manifold polygon meshes. *Journal of Graphical Models/special issue*, 64(3-4) :147–168, 2002.

[46] L. Kobbelt. Interpolatory subdivision on open quadrilateral nets with arbitrary topology. Dans *Proc. Eurographics*, pages 409–420, 1996.

[47] L. Kobbelt, J. Vorsatz, U. Labsik, et H.-P. Seidel. A shrink wrapping approach to remeshing polygonal surfaces. Dans *Proc. Eurographics*, pages 119–130, 1999.

[48] F. Lazarus, M. Pocchiola, G. Veger, et A. Verroust. Computing a canonical polygonal schema of an orientable triangulated surface. Dans *Proc. 7th Annual ACM Symposium on Computational Geometry*, pages 80–89, 2001.

[49] T. Lindebergh. Scale-space for discrete signals. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 12(3) :234–254, March 1990.

[50] C. Loop. Smooth subdivision surfaces based on triangles. Mémoire de D.E.A., Dept. of Mathematics, Univ. Utah, 1987.

[51] W. Lorenson et H. Cline. Marching cubes : a high resolution 3d surface construction algorithm. Dans *Proc. SIGGRAPH*, pages 163–169, 1987.

[52] M. Lounsbery. *Multiresolution analysis for surfaces of arbitrary topological type*. Thèse de doctorat, Dpt. Computer Science and Engineering, Univ. of Washington, 1994.

[53] B. Lévy, S. Petitjean, N. Ray, et J. Maillot. Least squares conformal maps for automatic texture atlas generation. Dans *Proc. SIGGRAPH*, volume 21, pages 362–371, 2002.

[54] F.E. Nicodemus, J.C. Richmond, et J.J. Hsia. Geometrical considerations and nomenclature for reflectance. Rapport technique, National Bureau of Standards, monograph 160, 1977.

[55] G.M. Nielson et T.A. Foley. *Mathematical methods in computer aided geometric design*, chapitre A survey of applications of an affine invariant norm, pages 445–467. Academic Press, Boston, 1989.

[56] R. Ohbuchi, H. Masuda, et M. Aono. Watermarking three-dimensional polygonal models. Dans *Proceedings of ACM International Conference on Multimedia*, pages 261–272, Nov 1997.

[57] R. Ohbuchi, H. Masuda, et M. Aono. A shape-preserving data embedding algorithm for nurbs curves and surfaces. Dans *Proceedings of Computer Graphics International*, pages 170–177, Jun 1999.

[58] R. Ohbuchi, S. Takahashi, T. Miyazawa, et A. Mukayiama. Watermarking 3d polygonal meshes in the mesh spectral domain. Dans *Proceedings of Graphics Interface*, pages 9–17, Jun 2001.

[59] S. Pereira, J. Ò Runaidh, et T. Pun. Secure robust digital watermarking using the lapped orthogonal transform. Dans *Proc. SPIE Electronic Imaging*, pages 11–30, San Diego, 1999.

[60] B. Pesquet-Popescu et J.-C. Pesquet. *Le traitement des images*, chapitre Ondelettes et traitement d'images. Hermès/IC2, 2003.

[61] U. Pinkall et K. Polthier. Computing discrete minimal surfaces. *Experimental mathematics*, 2(2) :15–36, 1993.

[62] E. Praun, H. Hoppe, et A. Finkelstein. Robust mesh watermarking. Dans *Proceedings of SIGGRAPH*, pages 49–56, 1999.

[63] R. Puri, K. Ramchandran, et S.S. Pradhan. On seamless digital upgrade of analog transmission systems using coding with side information. Dans *Proc. Allerton Conf. on Communication, Control and Computing*, Allerton, IL, Oct. 2002.

[64] J. Rossignac. Edgebreaker : connectivity compression for triangle meshes. *IEEE Trans. on Visualization and Computer Graphics*, 1(5) :47–61, 1998.

[65] S. Schechter, R. Greenstadt, et M. Smith. Trusted computing, peer-to-peer distribution, and the economics of pirated entertainment. *2nd Workshop on economics and information security, College Park, MD, 2003*, 2003.

[66] P. Schröder et D. Zorin. *Subdivision for modeling and animation.* SIGGRAPH 1996 Course Notes.

[67] L. Schumaker. Triangulations in cagd. *IEEE Computer Graphics and Applications*, pages 47–52, 1993.

[68] J.A. Scott. An arnoldi code for computing selected eigenvalues of sparse, real, unsymmetric matrices. *ACM Trans. on Mathematical Software*, 21(4) :432–475, 1995.

[69] G. Simmons. The history of subliminal channels. *IEEE Journal on Selected Area in Communications*, 16(4) :452–462, 1998.

[70] G. Simmons. Results concerning the bandwith of subliminal channels. *IEEE Journal on Selected Area in Communications*, 16(4) :463–473, 1998.

[71] G. Taubin. A signal processing approach to fair surface design. Dans *Proceedings of SIGGRAPH*, pages 351–358, 1995.

[72] G. Taubin et J. Rossignac. Geometric compression through topological surgery. Dans *ACM Transactions on Graphics*, volume 17(2), pages 84–115, Apr 1998.

[73] C. Touma et C. Gotsman. Triangle mesh compression. Dans *Proceedings of Graphics Interface*, pages 26–34, 1998.

[74] G. Turk. Re-tiling polygonal surfaces. Dans *Proc. ACM SIGGRAPH*, pages 55–64, 1992.

[75] W.T. Tutte. How to draw a graph. Dans *Proceedings of the London Mathematical Society*, volume 10, pages 304–332, 1960.

[76] S. Valette, H.-Y. Kim, H.-Y. Yung, I. Magnin, et R. Prost. A multiresolution wavelet scheme for irregularly subdivided 3d triangular mesh. Dans *Proc. of IEEE Intl. Conf. on Image Processing ICIP'99, Oct. 25-28, Kobe, Japan*, volume 1, pages 171–174, 1999.

[77] G. Vegter et C.K. Yap. Computational complexity of combinatorial surfaces. Dans *Proc. 6th Annual ACM Symposium on Computational Geometry*, pages 102–111, 2000.

[78] J. Vorsatz, C. Rössl, L. Kobbelt, et H.-P. Seidel. Feature sensitive remeshing. Dans Blackwell, éditeur, *Computer Graphics Forum, Proc. Eurographics*, pages 393–401, 2001.

[79] M.G. Wagner. Robust watermarking of polygonal meshes. Dans *Proceedings of Geometric modeling & processing*, pages 201–208, Hong-Kong, 2000.

[80] K. Weiler. *Geometric Modelling for CAD applications.* North Holland, 1988. The Radial-Edge Structure : A Topological Representation for Non-Manifold Geometric Boundary Representations.

[81] A.P. Witkin. Scale-space filtering. Dans *Proc. 8th Intl. Joint Conference on Artificial Intelligence (IJCAI), Karlsruhe, Germany*, pages 1019–1022, 1983.

[82] B.-L. Yeo et M.M. Yeung. Watermarking 3d objects for verification. *IEEE Computer Graphics and Applications*, 19(1) :46–55, 1999.

[83] D. Zorin, P. Schröder, et W. Sweldens. Interpolating subdivision for meshes with arbitrary topology. Dans *Proc. SIGGRAPH*, pages 189–192, 1996.

Résumé

Les méthodes de tatouage actuelles pour les maillages surfaciques 3D sont essentiellement le fait de la communauté CAO, et sont assez peu adaptées à une étude en termes de tatouage. Dans un premier temps, nous avons abordé dans ce travail le tatouage par invariants géométriques, dédié aux applications de tatouage fragile. Dans un deuxième temps, nous avons utilisé l'espace de la décomposition spectrale de la géométrie afin d'y enfouir une marque que nous voulons robuste face à la quantification des coefficients spectraux.

En tatouage fragile, nous proposons notamment une approche flexible et modulaire permettant l'analyse fine, d'un point de vue du tatouage, des performances de notre méthode (classe de robustesse, probabilité de fausse alarme, etc.) Les applications visées par cette approche concernent tant la stéganographie que l'intégrité ou l'authentification des maillages. Nous décrivons une méthode de tatouage fragile pour l'authentification construite avec les modules que nous présentons.

Le tatouage dans l'espace de la décomposition spectrale de la géométrie, à travers son étude face à la compression géométrique spectrale, implique le développement d'un codeur de source géométrique spectral. Nous étudions les difficultés liées à l'implantation d'une telle décomposition, tant pour le codage de source que pour le tatouage. Nous terminons en montrant que notre schéma de tatouage se révèle robuste face à la compression géométrique spectrale.

Mots-clés: Tatouage, surface maillée 3D, invariant géométrique, décomposition spectrale

Abstract

Nowadays' watermarking methods for 3D meshes generally arise from the CAD community. A thorough study of their watermarking performances are generally not easily tractable. In the first part of this work, we investigate watermarking with geometric invariant towards fragile watermarking purposes. In the sencond part, we deal with spectral decomposition of the geometry towards robust watermarking against spectral compression.

Within the fragile watermarking framework, we propose a flexible and modular approach that enables precise analysis of watermarking performances (robustness, false alarm, etc.) Applications concerned by our technique range from steganography and integrity to authentication of meshes. We describe a watermarking algorithm for authentication based on our building blocks.

Spectral decomposition is an interesting new research line for geometry compression. We aimed at developping both a spectral geometry coder and a watermarking scheme in the mesh spectral domain. We study the difficulties that arise when implementing such a spectral decomposition, for compression and watermarking. Our works ends with the evidence of our watermarking scheme's robustness against spectral compression.

Keywords: Watermarking, 3D mesh, geometric invariant, geometry spectral decomposition