Cryptanalyse de chiffrement sélectif d'images JPEG et de vidéos H.264 et de leurs impacts sur les mesures de qualités

Guillaume Baixas

Responsables de stage :

William Puech et Loïc Dubois

1. Présentation
   - Cursus
   - Mémoire précédent

2. Sujet de stage
   - Objectifs
   - Etat de l’art
   - Axes de recherche

Cursus scolaire

- Bac Scientifique spécialité physique ;
- CPGE Maths Physique ;

  Lycée Arago - Perpignan

- Licence Mathématiques et Informatique ;

  Université de Provence – Marseille

Année en cours :

- Master Mathématiques Statistiques et Applications.

  Université Montpellier 2 - Montpellier

Etude des isométries du Model-Planet

- Nature de l'objet

  Modèle de représentation des notes de musique en 4 dimensions.

- Propriétés

  Invariant par changement de note de référence ;

  Invariant par changement de méthode de construction des notes ;

  Pas d'élément neutre ;

  Inclus dans une sphère 4D.

- Résultat

  L'ensemble des isométries du modèle est le groupe diédral D3XD4.

Représentation du Model-Planet

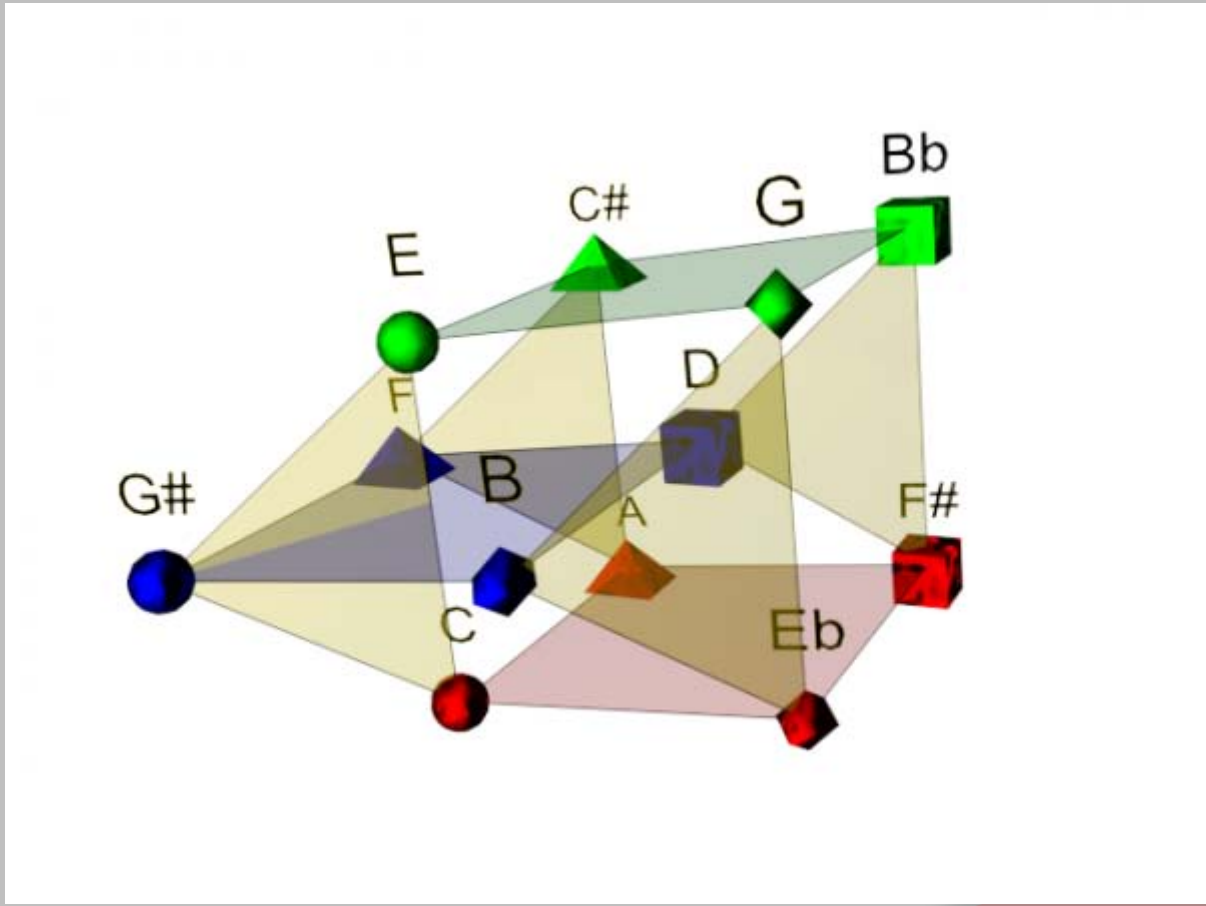
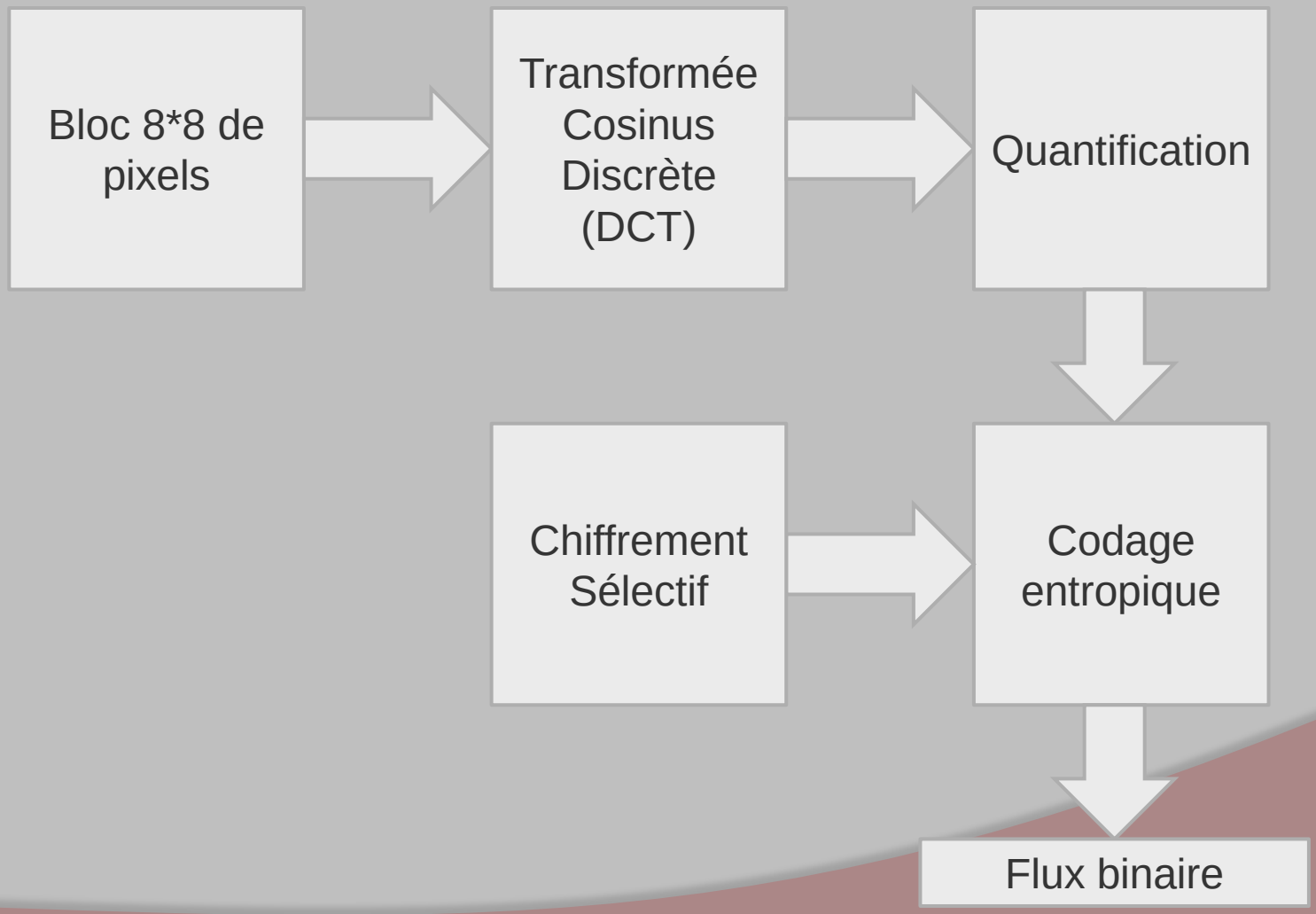


Fig.1. Projection du Model-Planet dans $\mathbb{R}^3$

Objectif du stage

- Connaître le comportement du chiffrement sélectif par AES appliqué aux images JPEG et aux vidéos H.264 ;
- En déduire des propriétés statistiques, des distributions et des intervalles pour les mesures de qualité.

Compression JPEG



Etat de l’art

- Hypothèses sur les distributions de pixels [1] ;
- Hypothèses sur les distributions des coefficients de la DCT [1],[2].

[1] E. Y. Lam and J. W. Goodman, “A mathematical analysis of the DCT coefficient distributions for images,” IEEE Trans. on Image Proc., vol. 9, no. 10, Oct. 2000, pp. 1661-1666

[2]Y. Altunbasak and N. Kamaci, “An analysis of the DCT coefficient distribution with the H.264 video coder”, IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04).

Comparaison des deux distributions

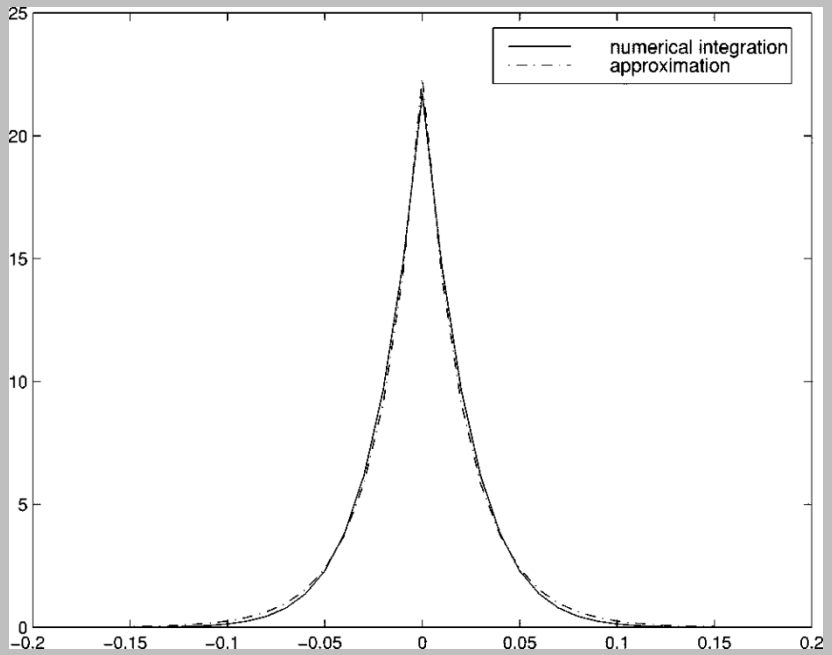


Fig.2. Approximation de la distribution d'un coefficient de la DCT par une distribution Laplacienne.

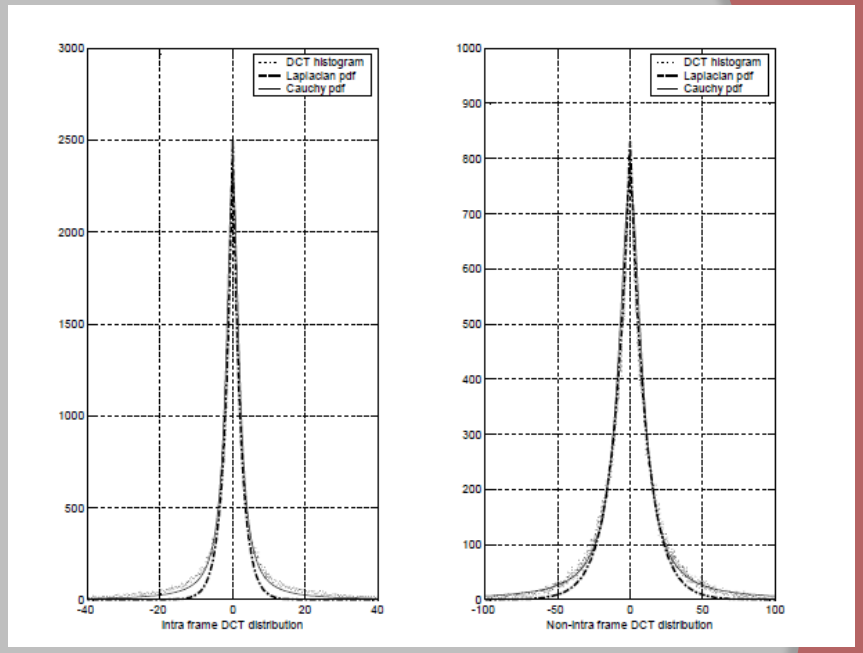


Fig.3. Comparaison de l'approximation de la distribution de la DCT par une distribution Laplacienne et par une distribution de Cauchy

Axes de recherche

- Etudier les distributions de pixels et de coefficients de DCT ;
- En déduire les distributions après quantification et chiffrement sélectif ;
- Obtenir des propriétés sur le comportement du chiffrement sélectif.

Merci de votre attention