Sujet Puech

A) Questions sur l'article

B) Insertion de données cachées

1. Applications :
    - Watermarking : Protection de propriété intellectuel (copyright)
    - Steganographie : Insertion de messages cachés pour communiquer sans soupçons
    - Detection de copy : (Cinema retrouver la place d'ou à été pris un vidéo)
2. IDC vs Chiffrement : Le chiffrement vise à rendre un message inintelligible sauf pour une personne possédant un méthode de déchiffrement adapté alors que l'IDC vise à dissimuler un message dans un autre message.
3. Méthode d'IDC générale :
    - Synchronisation : parcours de sommets, faces, ordonnancement unique
    - Phase d'insertion : media marqué avec un message secret à l'aide d'une clé secrète.
        - Injection : message insérée dans le média
        - Substitution : message remplace l'information redondante qui altère le moins le media
        - Distorsion : différences entre objets supports et marqués
    - Phase d'extraction : information cachée retrouvée avec l'ordre de la synchronisation + clé secrète
4. Compromis :
    - Robustesse : tatouage
    - Capacité : IDC haute capacité
    - Imperceptibilité : stéganographie (évaluation avec PSNR ou RMSE)
    - Complexité :
    - Sécurité : secret de la clé, difficile estimer paramètre de la méthode

Sujet Puteaux

A) Questions de cours

1. Les générateurs aléatoire sont initialisé avec une graine qui sera la clé de déchiffrement. Ces générateurs permettent de générer des séquences de nombres pseudo aléatoire permettent de rendre des données inintelligible facilement.
2. Dans un chiffrement symétrique on peut rendre les données d'une image illisible en faisant un XOR entre une image normale et une image randomisé et cela avec la même clef.
3. Une clef publique et une clef secrète, les information son facile à calculer dans un sens mais très difficile dans l'autre (exponentiation) sauf si on connaît une information secrete
4. à faire

B) Entropie de Shannon

1. si la méthode de chiffrement est efficace alors chaque valeur de pixels est equiprobable l'antropie est donc log2(2^4) = 4 bit / pixels