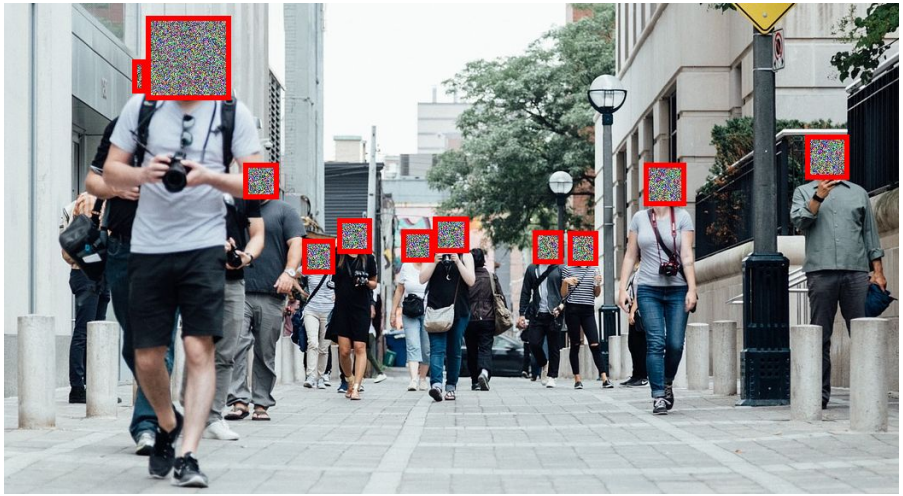
Chiffrement multimédia

Pauline PUTEAUX

Chargée de recherche CNRS, CRIStAL (Lille)

Besoin important en sécurité

- Besoin grandissant en cybersécurité
- Vidéo-surveillance, visioconférence, réseaux sociaux, cloud…
- Sécuriser la donnée elle-même, ~~ou son support physique ?~~
  - Préservation de la vie privée
  - Respect des droits d'auteur
  - Véracité des données

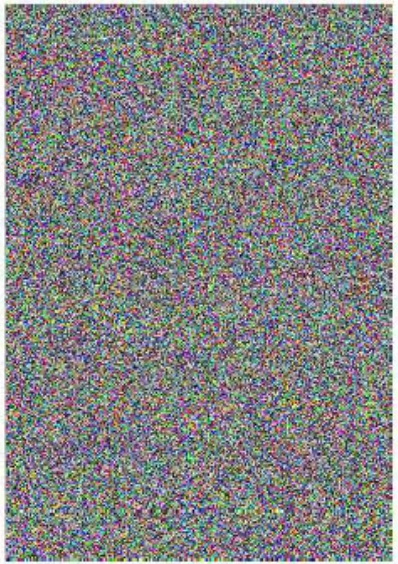


Protection des données multimédia

- D’après CISCO, les données multimédia > 80% du trafic global sur internet
  - Intérêt de mettre au point des méthodes efficaces pour sécuriser les données multimédia !

- Différentes pistes de recherche
  - Chiffrement
  - Stéganographie
  - Tatouage
  - Analyse forensique
  - Biométrie

Chiffrement

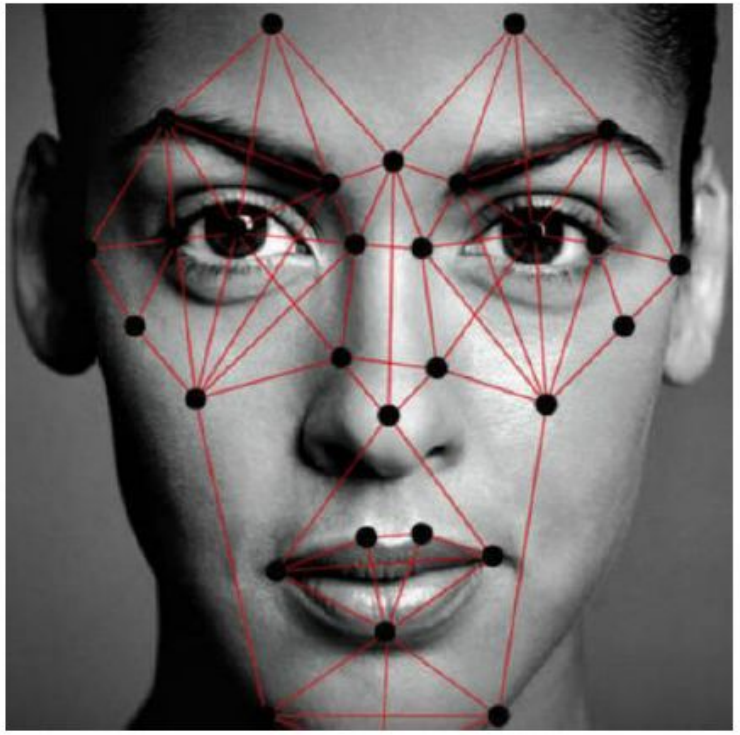



Stéganographie

Tatouage

Analyse forensique

Biométrie



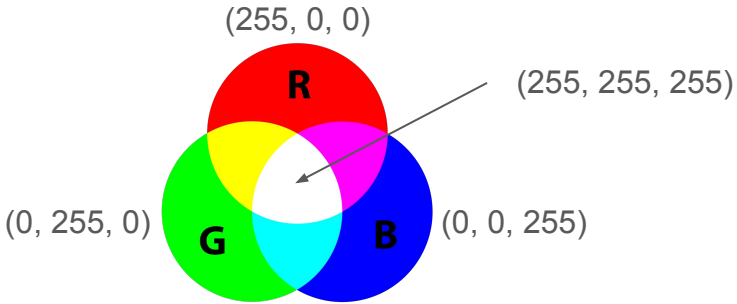
Principe de Kerckhoffs

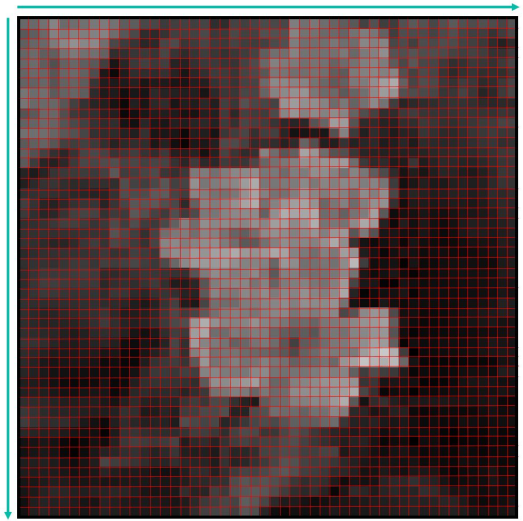
- Le secret ne devrait pas se trouver dans la méthode de protection : mais dans la clé utilisée !
  - "La sécurité ne devrait pas dépendre de paramètre qu'il n'est pas aisé de modifier."
- Sans la clé, il ne doit pas être possible de déduire l'information secrète à partir de la donnée sécurisée.
- Avec la clé, il doit être possible de déduire l'intégralité de l'information secrète.

A. Kerckhoffs, *La cryptographie militaire*, Journal des sciences militaires, 1883.

Qu’est-ce qu’une image ?

- Représentation classique
  - Tableau à deux dimensions
  - Un élément = un pixel
  - Chaque pixel est encodé avec :
    - 8 bits pour une image en niveaux de gris : valeurs comprises entre 0 et 2^8
    - 24 bits pour une image couleur : valeurs entre 0 et 2^{24}



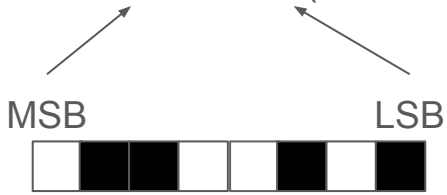


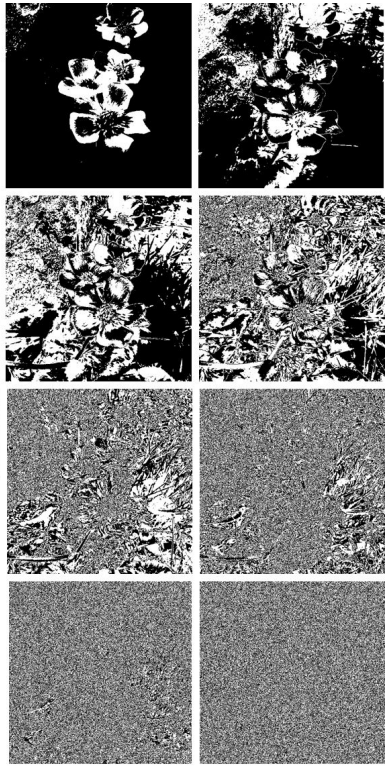
Qu’est-ce qu’une image ?

- Plans binaires
  - Ensemble de bits à une position donnée pour tous les pixels
  - Plan binaire le plus significatif : plan MSB
  - Plan binaire le moins significatif : plan LSB

$154 = 1x2^7 + 0x2^6 + 0x2^5 + 1x2^4 + 1x2^3 + 0x2^2 + 1x2^1 + 0x2^0$

= **1**001 101**0** (notation binaire)





Mesures de la qualité d'une image

- Mesure en prenant une image comme référence
- PSNR (Peak Signal to Noise Ratio)
  - Basée sur l'erreur quadratique moyenne
  - Différence pixel à pixel
  - Ne prend pas en compte le système visuel humain
  - ~10 dB : images complètement différentes → +∞: images identiques
- SSIM (Structural SIMilarity)
  - Mesure subjective
  - Basée sur le système visuel humain
  - 0 : images complètement différentes → 1: images identiques
- Reconnaissabilité
  - Peut-on prédire le contenu de l'image ?

Mesures de la qualité d’une image

“Ceci est un chat”

“Ceci est un chien” (“Ceci n’est pas un chat”)

PSNR = 10.66 dB
SSIM = 0.126

Chiffrement d’images

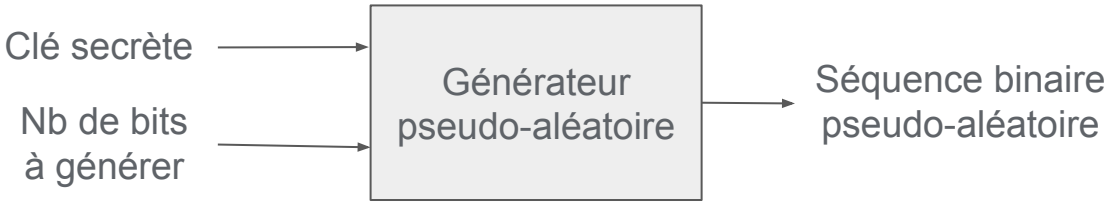
- But : Préserver la sécurité visuelle / vie privée
- Impossible de deviner le contenu original
  - Le contenu chiffré doit être très différent de sa version originale
- Rendre aléatoire l’information à protéger
  - Équiprobabilité des valeurs
  - Distribution uniforme
  - Maximisation de l’Entropie de Shannon

- Comment peut-on faire cela ?

C. E. Shannon, *A mathematical theory of communication*, The Bell system technical journal 27(3), 1948.

Chiffrement d'images

- Comment peut-on faire cela ?



- Même clé secrète utilisée comme paramètre = même séquence binaire pseudo-aléatoire générée
- Utilisation de cette séquence binaire pour modifier un plan binaire
  - Addition (ou-exclusif)
  - Permutation (mélange)
- Pour le déchiffrement = application de l'opération inverse avec la même clé secrète

Chiffrement d’images

- En fonction de l’application, différents niveaux de sécurité :
  - Transparent
    - Haute définition protégée, mais une version dégradée pour toujours être visualisée
  - Suffisant
    - Le contenu est sécurisé, mais certains contours ou formes sont toujours visibles
  - Confidentiel
    - Aucune information visuelle ne peut être extraite

- Comment peut-on utiliser la structure intrinsèque de l’image pour retrouver ces différents niveaux de sécurité visuelle ?