

HAI918I - Image, Sécurité et Deep Learning

TP1

Ingo Diab

2023

Table des matières

1	Chiffrement d'images par permutation	3
1.1	Permutation	3
1.2	PSNR & Entropie	5
1.3	Histogrammes	5
1.4	Inverse	5
2	Chiffrement d'images par substitution	6
2.1	Substitution	6
2.2	PSNR & Entropie	8
2.3	Histogrammes	9
2.4	Inverse	9
3	Trouver la clé	10

1 Chiffrement d'images par permutation

1.1 Permutation

Pour chiffrer une image par permutation, nous utilisons un `rand()` avec une certaine seed (clé). Ce `rand()` modulo le nombre de pixels nous permet de trouver la position du pixel sur l'image chiffrée. Si cette position est déjà occupée (nous avons une carte d'occupation), alors nous regardons le pixel suivant jusqu'à trouver un pixel "libre".



FIGURE 1 – Image de base

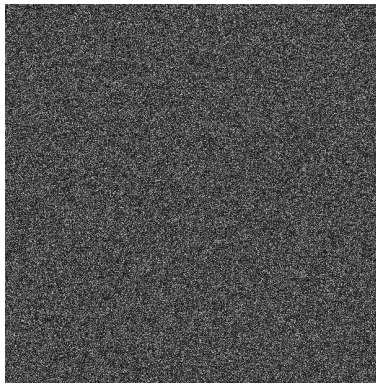


FIGURE 2 – Image chiffrée par permutation (clé 120)

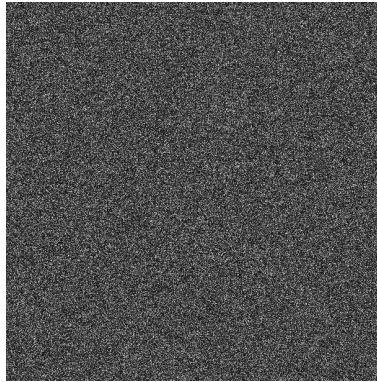


FIGURE 3 – Image chiffrée par permutation (clé 50)



FIGURE 4 – Image alternative

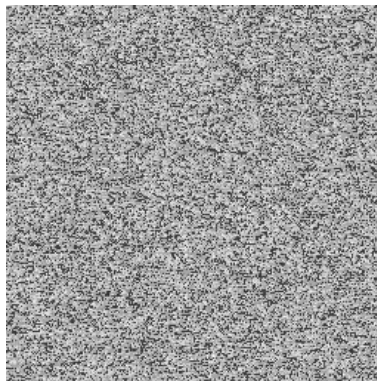


FIGURE 5 – Image alternative chiffrée par permutation (clé 120)

1.2 PSNR & Entropie

On s'aperçoit que le PSNR est de 10dB et que l'entropie de l'image originale est la même que celle de l'image chiffrée (7.5).

```
PSNR : 10.0755  
Entropie originale : 7.51312  
Entropie chiffrée : 7.51312
```

FIGURE 6 – Entropies et PSNR entre l'image de base et celle chiffrée avec la clé 120

1.3 Histogrammes

On s'aperçoit que l'histogramme de l'image originale est le même que celui de l'image chiffrée.

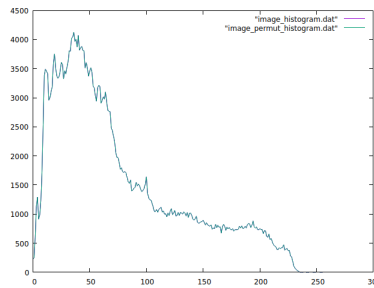


FIGURE 7 – Histogrammes de l'image originale et de l'image chiffrée

1.4 Inverse

Pour inverser la permutation avec la clé, il suffit d'échanger de nouveaux les places des pixels.

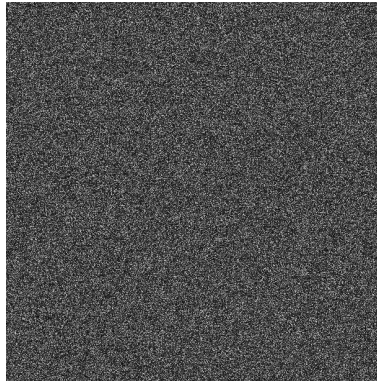


FIGURE 8 – Image chiffrée par permutation (clé 120)



FIGURE 9 – Image déchiffrée par permutation inverse

2 Chiffrement d'images par substitution

2.1 Substitution

Pour chiffrer une image par substitution, nous utilisons une image aléatoire générée avec `rand()` et une certaine clé. Chaque pixel de l'image de sortie correspond au pixel de l'image d'entrée + le pixel de l'image aléatoire + le pixel précédent sur l'image de sortie (à part pour le premier pixel car il n'a pas de précédent).



FIGURE 10 – Image de base

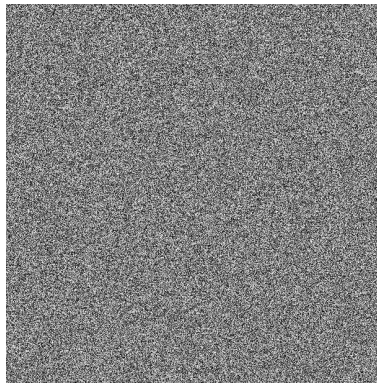


FIGURE 11 – Image chiffrée par substitution (clé 120)

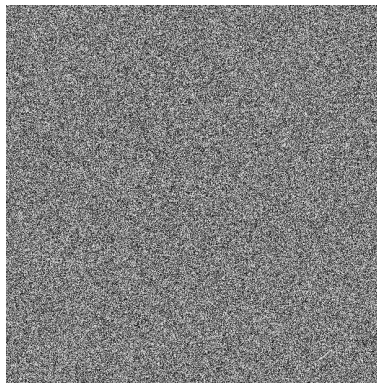


FIGURE 12 – Image chiffrée par substitution (clé 50)



FIGURE 13 – Image alternative

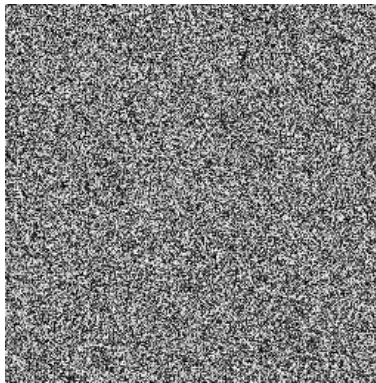


FIGURE 14 – Image alternative chiffrée par substitution (clé 120)

2.2 PSNR & Entropie

On s'aperçoit que le PSNR est de 7.6dB (plus bas qu'avec permutation) et que l'entropie de l'image originale (7.5) est plus basse que celle de l'image chiffrée (8).

```
PSNR : 7.61979
Entropie originale : 7.51312
Entropie chiffrée : 7.9995
```

FIGURE 15 – Entropies et PSNR entre l'image de base et celle chiffrée avec la clé 120

2.3 Histogrammes

On s'aperçoit que l'histogramme de l'image originale est différent de celui de l'image chiffrée avec substitution.

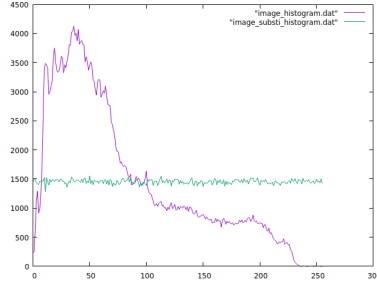


FIGURE 16 – Histogrammes de l'image originale et de l'image chiffrée

2.4 Inverse

Pour inverser la substitution avec la clé, il suffit de faire chaque pixel de l'image d'entrée - le pixel de l'image aléatoire - le pixel précédent sur l'image d'entrée (à part pour le premier pixel car il n'a pas de précédent).

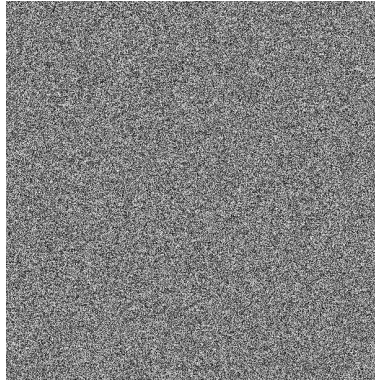


FIGURE 17 – Image chiffrée par substitution (clé 120)



FIGURE 18 – Image déchiffrée par substitution inverse

3 Trouver la clé

Pour trouver la clé de chiffrement, on a testé toutes les clés possible (dans ce tp entre 1 et 256). Pour chaque image on calcule l'entropie et on garde l'image dont l'entropie est la plus faible. Arthur m'a envoyé une image chiffrée par substitution avec une clé entre 1 et 256. J'ai pu la trouver en testant toutes les clés possibles et en gardant l'image avec la plus faible entropie.

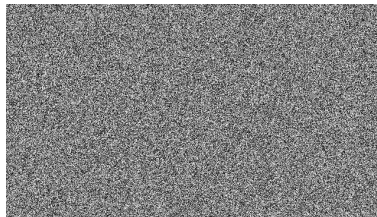


FIGURE 19 – Image chiffrée par Arthur



FIGURE 20 – Image déchiffrée par substitution (clé 17)