

HAI918I - Image, Sécurité et Deep Learning

TP2

Ingo Diab

2023

Table des matières

1	ECB	4
2	CBC	5
3	CFB	6
4	OFB	7
5	Bruit	8

Pour ce tp, j'ai choisi une image classique ainsi qu'une échographie.



FIGURE 1 – Images de base

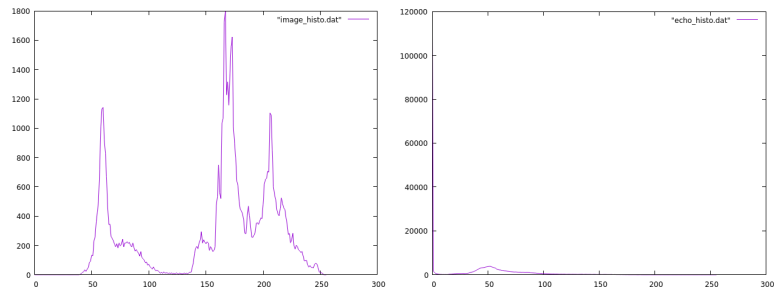


FIGURE 2 – Histogrammes de base

1 ECB

Les images chiffrées par bloc ECB :

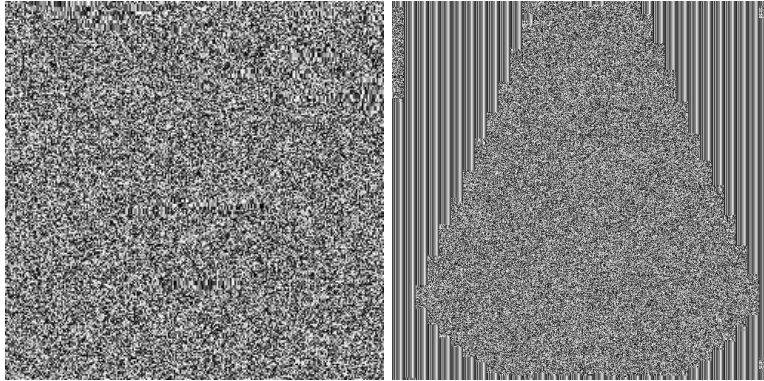


FIGURE 3 – Chiffrées par bloc ECB

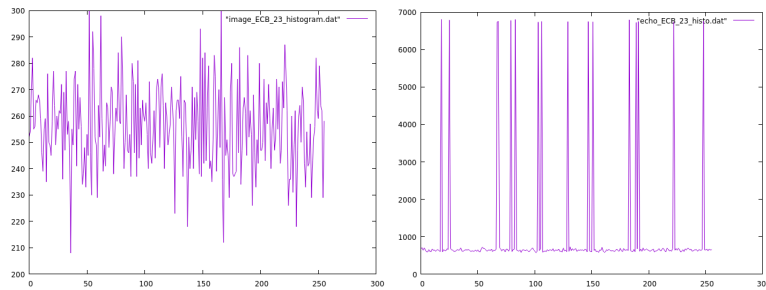


FIGURE 4 – Histogrammes des images chiffrées par bloc ECB

PSNR : 8.41247	PSNR : 6.46019
Entropie originale : 6.96896	Entropie originale : 4.91391
Entropie chiffrée : 7.9972	Entropie chiffrée : 7.2725

FIGURE 5 – PSNR/Entropie

2 CBC

Les images chiffrées par bloc CBC :

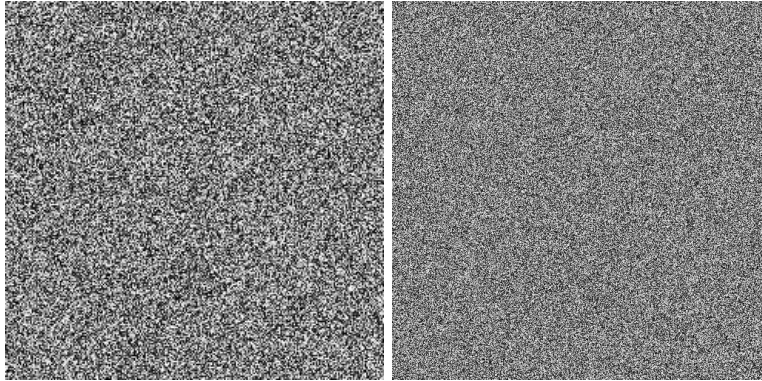


FIGURE 6 – Chiffrées par bloc CBC

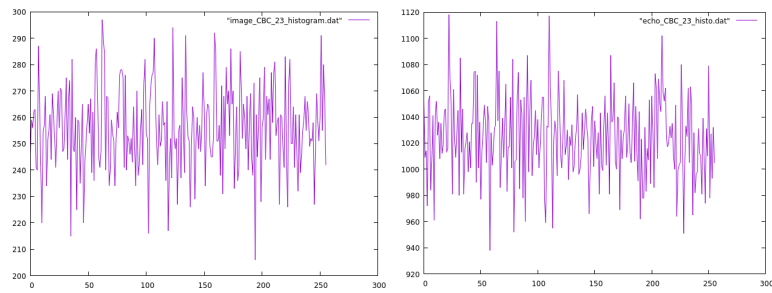


FIGURE 7 – Histogrammes des images chiffrées par bloc CBC

PSNR : 8.41564	PSNR : 6.46019
Entropie originale : 6.96896	Entropie originale : 4.91391
Entropie chiffrée : 7.99717	Entropie chiffrée : 7.2725

FIGURE 8 – PSNR/Entropy

3 CFB

Les images chiffrées par bloc CFB :

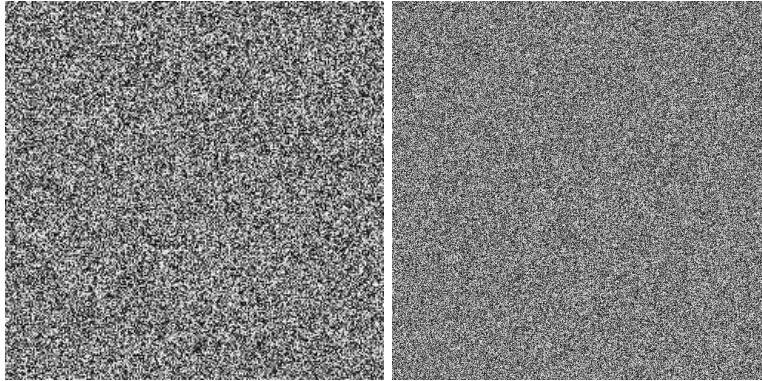


FIGURE 9 – Chiffrées par bloc CFB

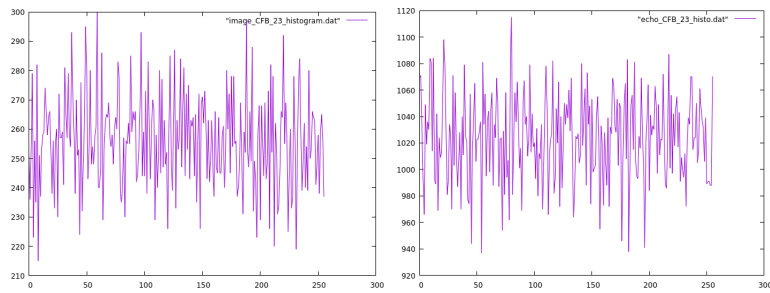


FIGURE 10 – Histogrammes des images chiffrées par bloc CFB

PSNR : 8.41969	PSNR : 6.30268
Entropie originale : 6.96896	Entropie originale : 4.91391
Entropie chiffrée : 7.99714	Entropie chiffrée : 7.99924

FIGURE 11 – PSNR/Entropy

4 OFB

Les images chiffrées par bloc OFB :

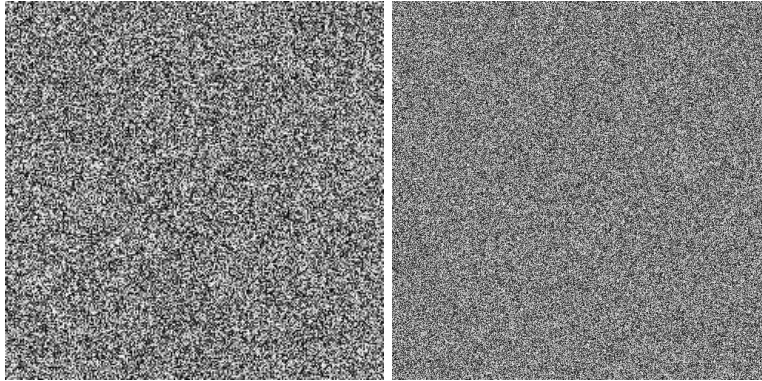


FIGURE 12 – Chiffrées par bloc OFB

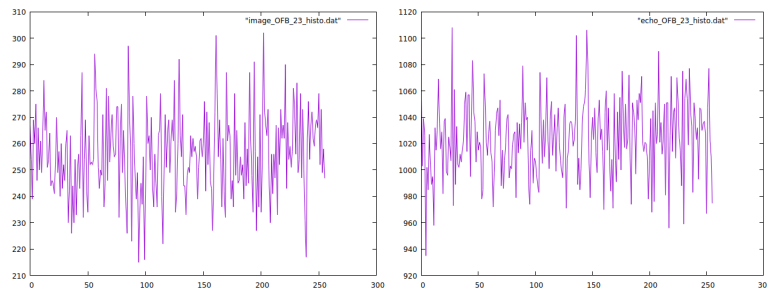


FIGURE 13 – Histogrammes des images chiffrées par bloc OFB

PSNR : 8.40002	PSNR : 6.28911
Entropie originale : 6.96896	Entropie originale : 4.91391
Entropie chiffrée : 7.99725	Entropie chiffrée : 7.99942

FIGURE 14 – PSNR/Entropy

5 Bruit

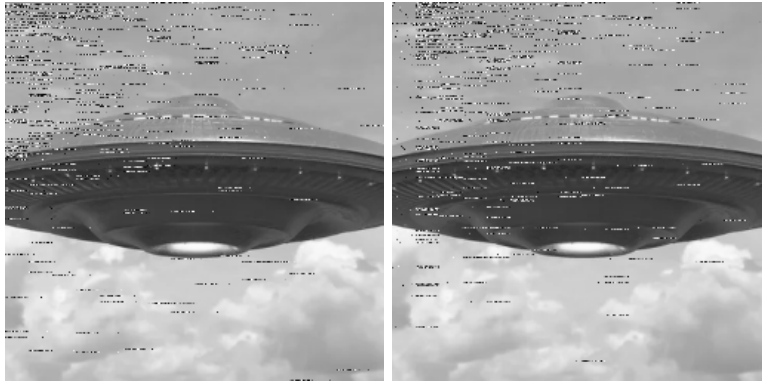


FIGURE 15 – Image chiffrée avec du bruit puis déchiffrée (CBC, CFB)

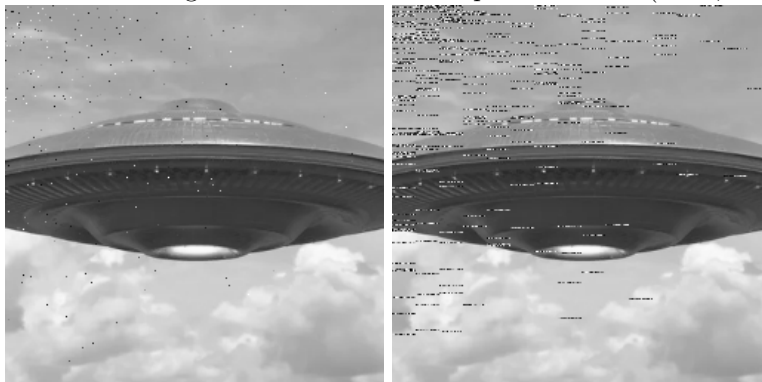


FIGURE 16 – Image chiffrée avec du bruit puis déchiffrée (OFB, ECB)

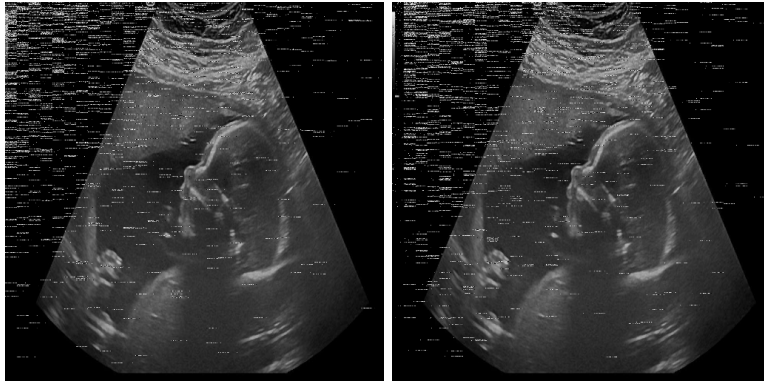


FIGURE 17 – Échographie chiffrée avec du bruit puis déchiffrée (CBC, CFB)

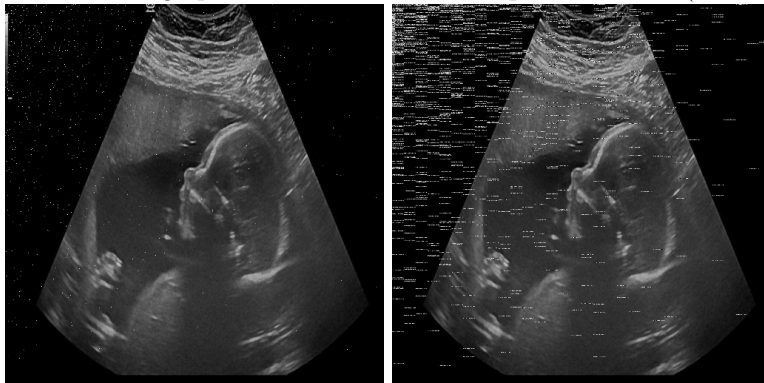


FIGURE 18 – Échographie chiffrée avec du bruit puis déchiffrée (OFB, ECB)

On peut voir que le chiffrement par bloc OFB est bien moins sensible au bruit que l'on a appliqué à l'image chiffrée puis déchiffrée. Cela s'explique par le fait que dans ce chiffrement on utilise les blocs précédents avant le XOR, ce qui permet de ne pas propager les erreurs d'un bloc à l'autre.