

HAI918I tp 2

Houle Adrien

Septembre 2023



1 Chiffrement d'image par AES

Ici on va faire du chiffrement d'iamge par AES, par bloc ECB tout d'abord avec mon image de babouin puis une image médicale.

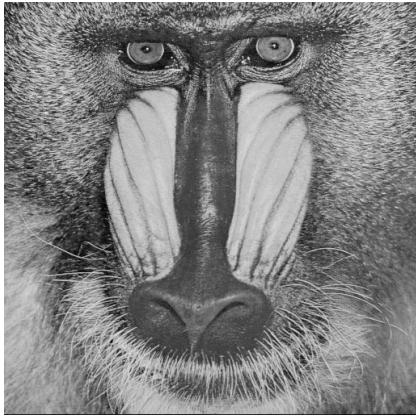


Figure 1: Image avant chiffrement

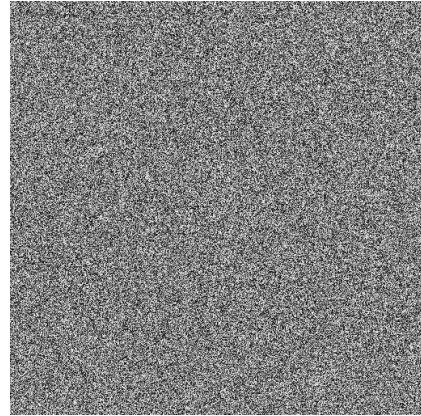


Figure 2: Image après chiffrement ECB

Pour l'image de babouin et sa version chiffré on a :

entropie non chiffré : 7.47443

entropie chiffré : 7.99934

PSNR 9.11788

Histogramme :

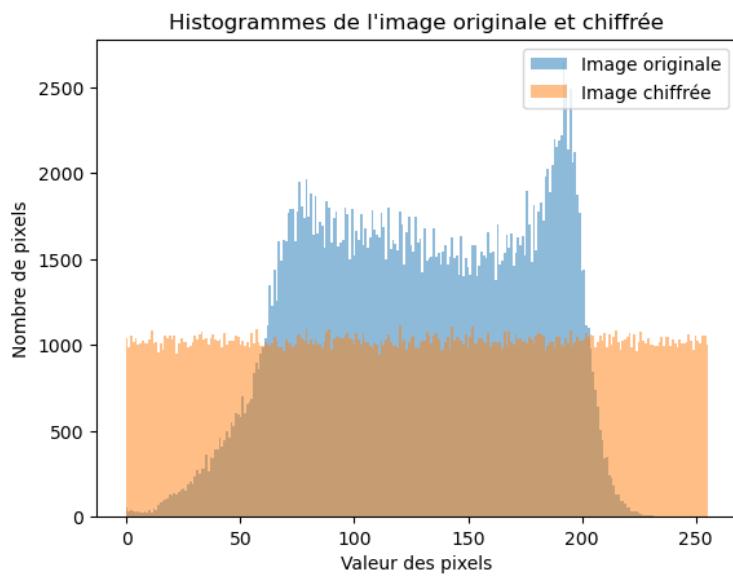


Figure 3: Histogramme image avant et après chiffrement ECB



Figure 4: Image médicale avant chiffrage

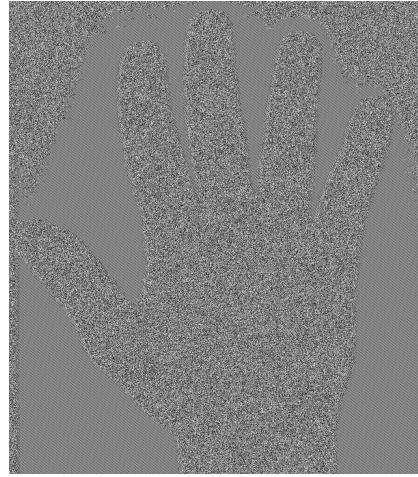


Figure 5: Image médicale après chiffrage ECB

Pour l'image de médicale et sa version chiffré on a :
entropie non chiffré : 6.02857
entropie chiffré : 7.1997
PSNR 6.48918
Histogramme :

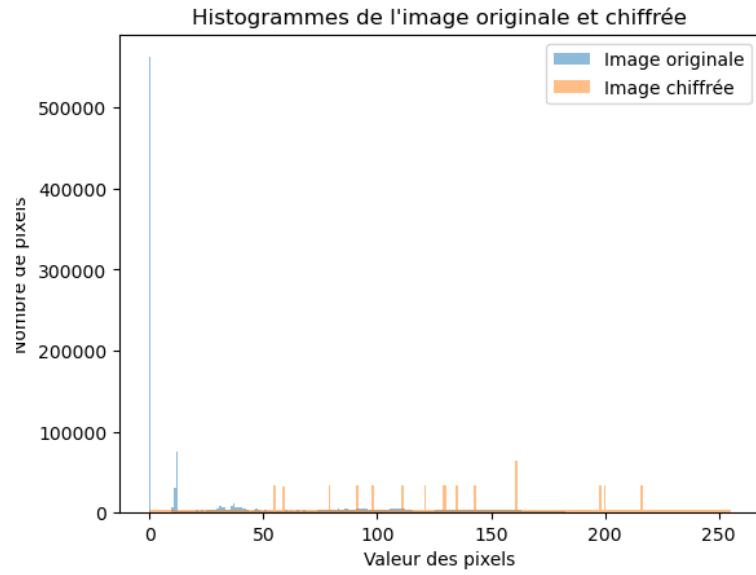


Figure 6: Histogramme image avant et après chiffrement ECB

On voit sur ce chiffrement des patrons permettant de reconnaître l'image ce qui est mauvais.

2 Chiffrement d'image par AES autres méthodes

a) OFC

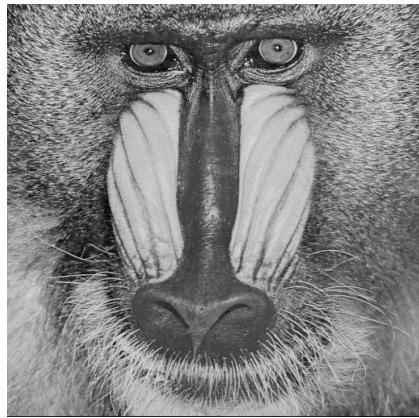


Figure 7: Image avant chiffrement

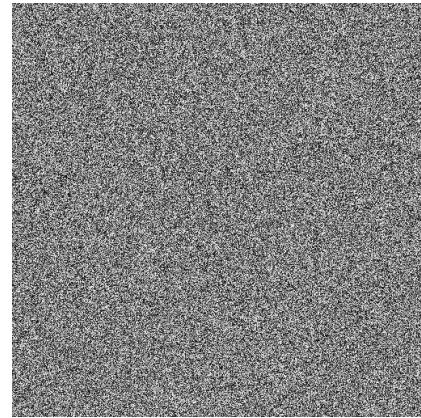


Figure 8: Image après chiffrement OFC

Pour l'image de babouin et sa version chiffré on a :
entropie non chiffré : 7.47443
entropie chiffré : 7.99932
PSNR : 9.2268
Histogramme :

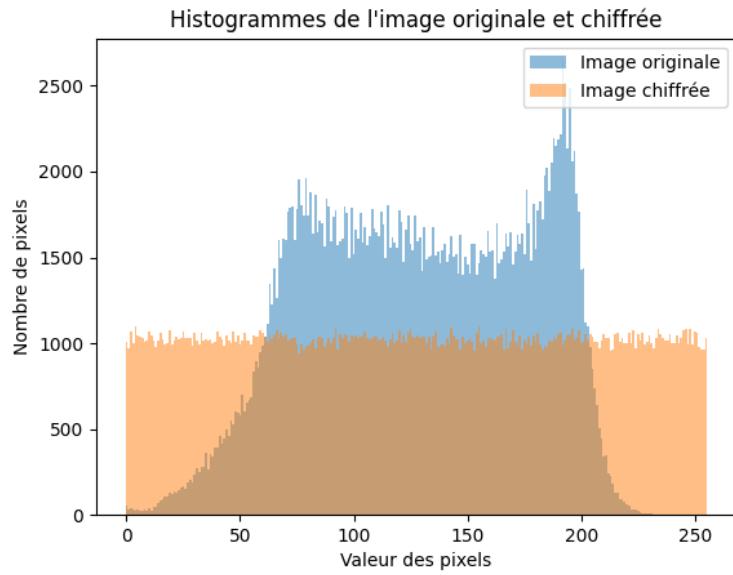


Figure 9: Histogramme image avant et après chiffrement OFC



Figure 10: Image médicale avant chiffrage



Figure 11: Image médicale après chiffrage OFC

Pour l'image de médicale et sa version chiffré on a :

entropie non chiffré : 6.02857

entropie chiffré : 7.99985

PSNR 6.22101

Histogramme :

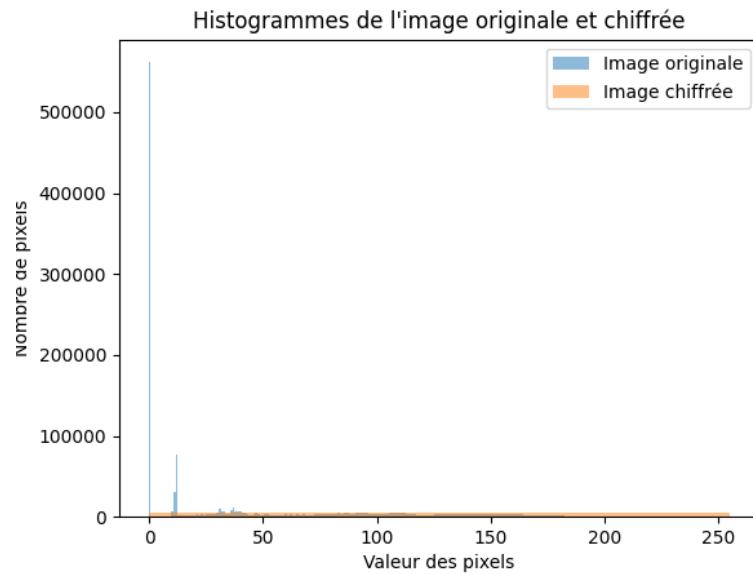


Figure 12: Histogramme image avant et après chiffrement OFC

b) CFB

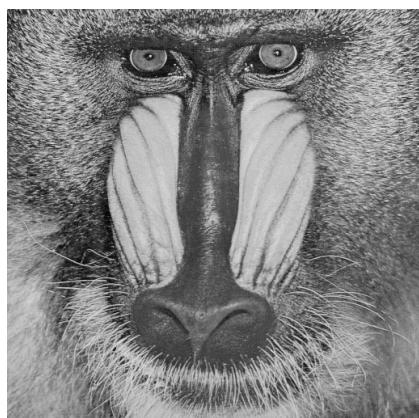


Figure 13: Image avant chiffrement

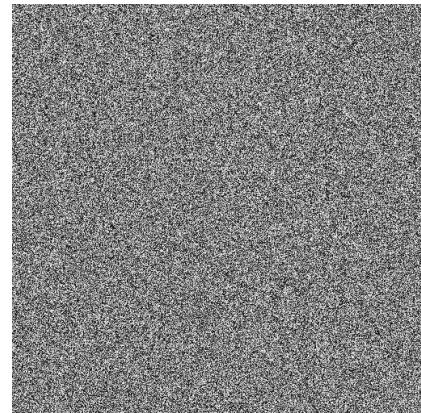


Figure 14: Image après chiffrement CFB

Pour l'image de babouin et sa version chiffré on a :
 entropie non chiffré : 7.47443
 entropie chiffré : 7.99925
 PSNR 9.24261

Histogramme :

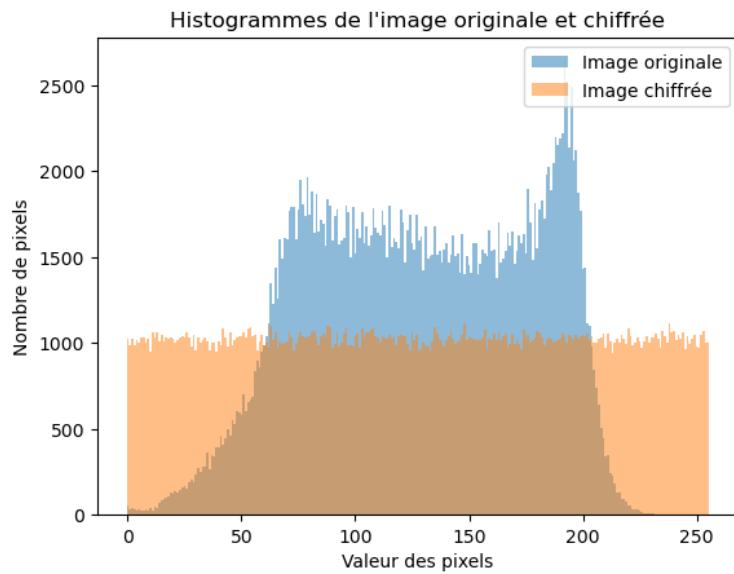


Figure 15: Histogramme image avant et après chiffrement CFB



Figure 16: Image médicale avant chiffrement

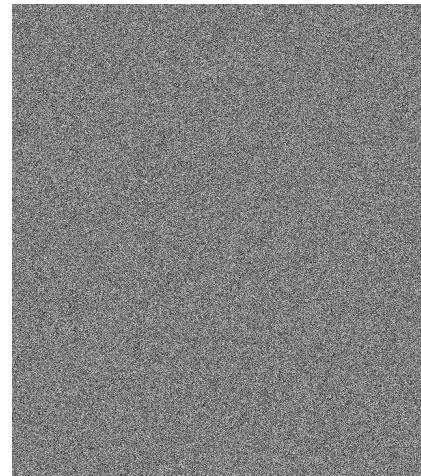


Figure 17: Image médicale après chiffrement CFB

Pour l'image de médicale et sa version chiffré on a :

entropie non chiffré : 6.02857

entropie chiffré : 7.99984

PSNR 6.22101

Histogramme :

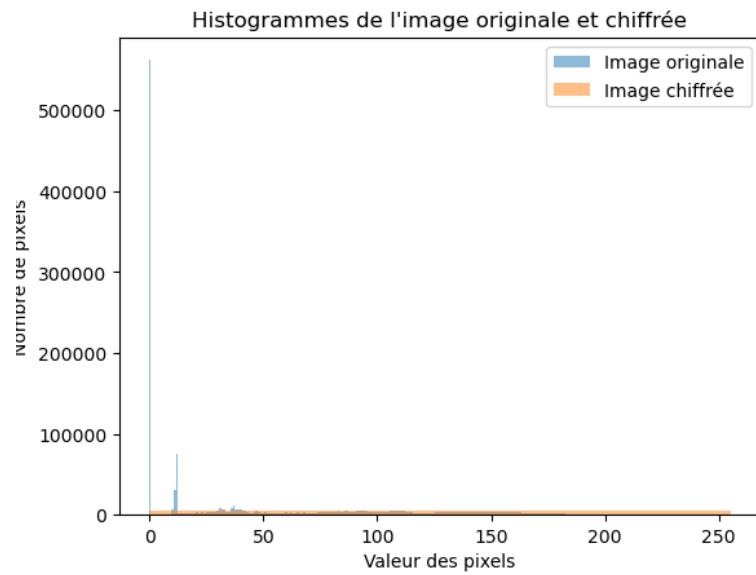


Figure 18: Histogramme image avant et après chiffrement CFB

c) CBC

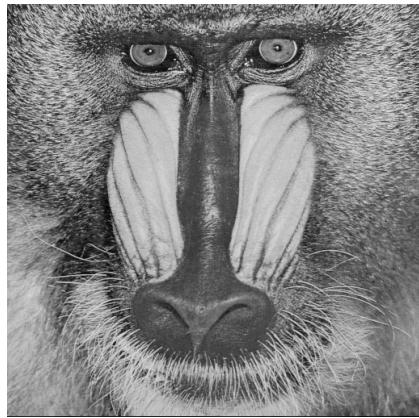


Figure 19: Image avant chiffrement

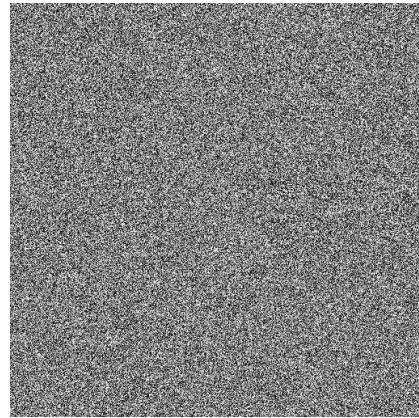


Figure 20: Image après chiffrement
CBC

Pour l'image de babouin et sa version chiffré on a :
entropie non chiffré : 7.47443
entropie chiffré : 7.99938
PSNR 9.2366
Histogramme :

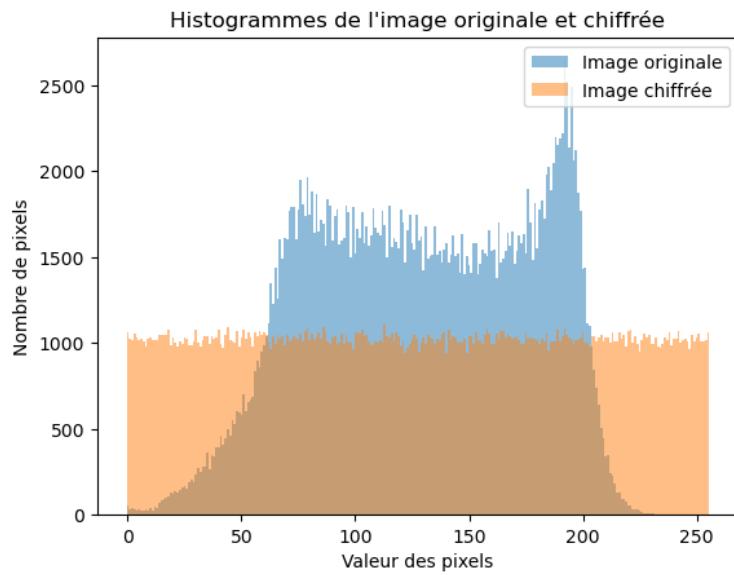


Figure 21: Histogramme image avant et après chiffrement CBC



Figure 22: Image médicale avant chiffrage

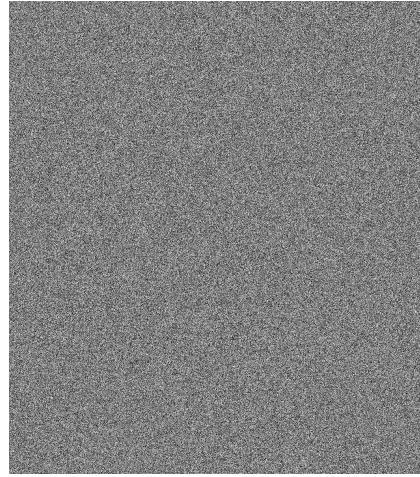


Figure 23: Image médicale après chiffrage CBC

Pour l'image de médicale et sa version chiffré on a :
entropie non chiffré : 6.02857
entropie chiffré : 7.99985
PSNR 6.21054
Histogramme :

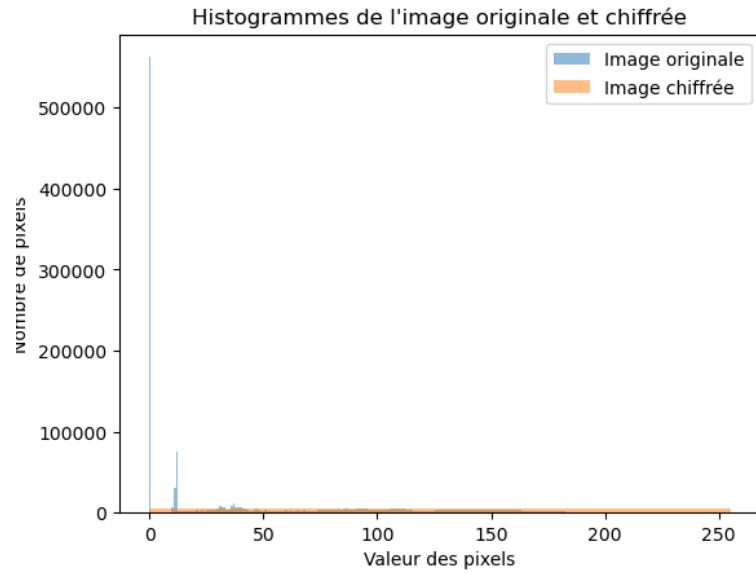


Figure 24: Histogramme image avant et après chiffrement CBC

d) CTR

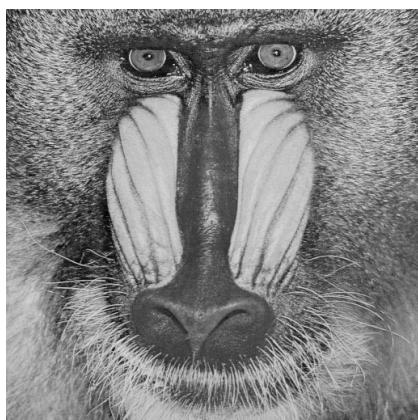


Figure 25: Image avant chiffrement

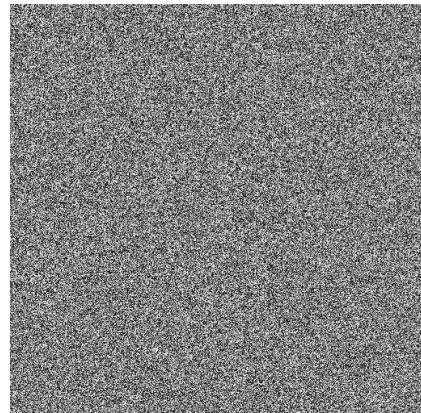


Figure 26: Image après chiffrement
CTR

Pour l'image de babouin et sa version chiffré on a :
 entropie non chiffré : 7.47443
 entropie chiffré : 7.99928
 PSNR : 9.23911

Histogramme :

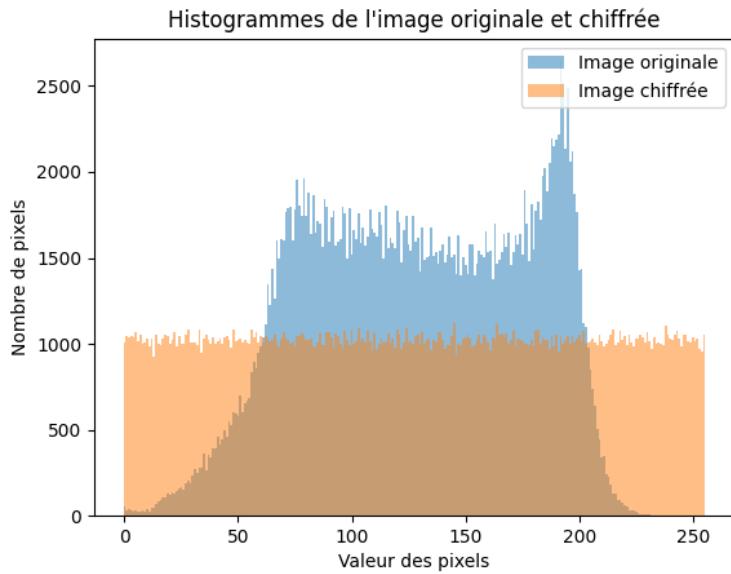


Figure 27: Histogramme image avant et après chiffrement CTR



Figure 28: Image médicale avant chiffrement

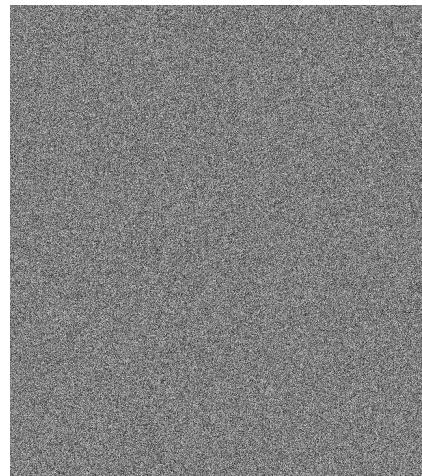


Figure 29: Image médicale après chiffrement CTR

Pour l'image de médicale et sa version chiffré on a :

entropie non chiffré : 6.02857

entropie chiffré : 7.99988

PSNR 6.21392

Histogramme :

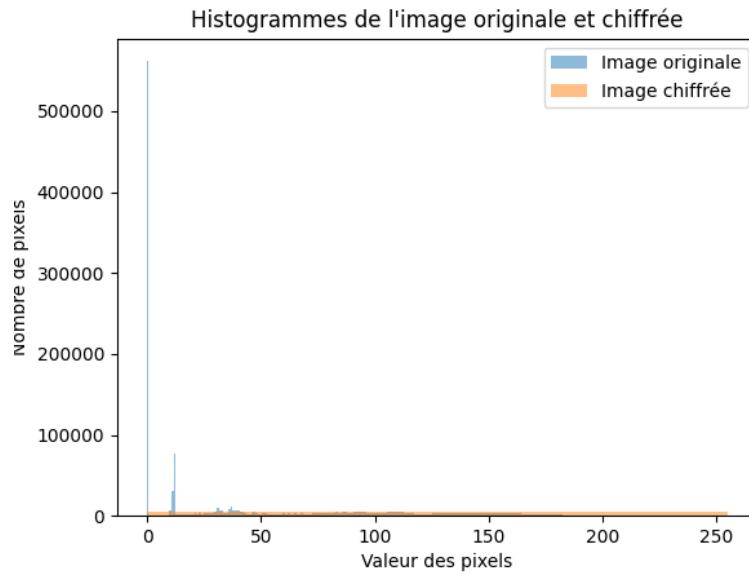


Figure 30: Histogramme image avant et après chiffrement CTR

3 3)Image bruitée

Tout d'abord j'ai rajouter du bruit sur le bits a poids le plus faible de chaque bloc :

```
void AES::AddNoiseToEncryptedImage(unsigned char *encryptedImage, unsigned int imageLen) {
    for (unsigned int i = 0; i < imageLen; i += blockBytesLen) {
        // on modifie la valeur du premier byte de chaque bloc
        if(encryptedImage[i] & 0x01) {
            encryptedImage[i] -= 1;
        }
    }
}
```

Figure 31: Code de mise en place bruit

Puis comme pour la question précédente j'ai fait tout les algo avec mes deux images en ajoutant cette fois du bruit a mon image chiffré puis je l'ai décrypté :

a) OFC

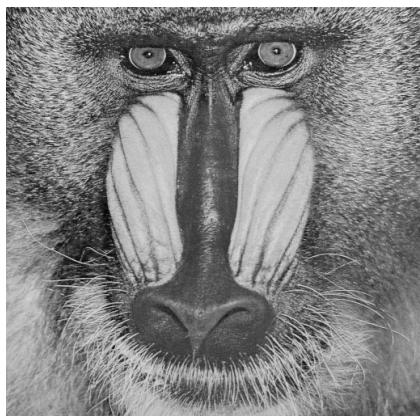


Figure 32: Image avant chiffrement

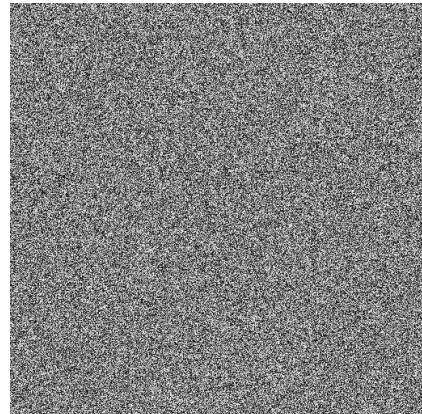


Figure 33: Image après chiffrement et bruitage OFC

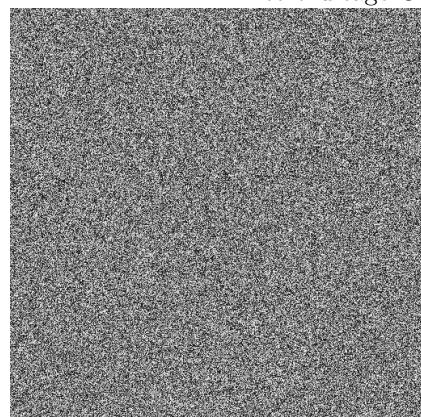


Figure 34: Image après déchiffrement OFC

Histogramme :

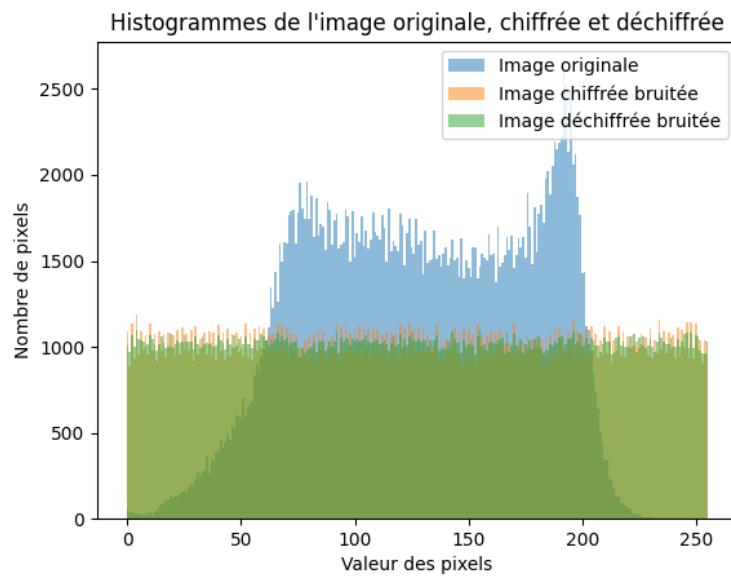


Figure 35: Histogramme image avant , après chiffrement avec bruit et après déchiffrement OFC



Figure 36: Image avant chiffrement

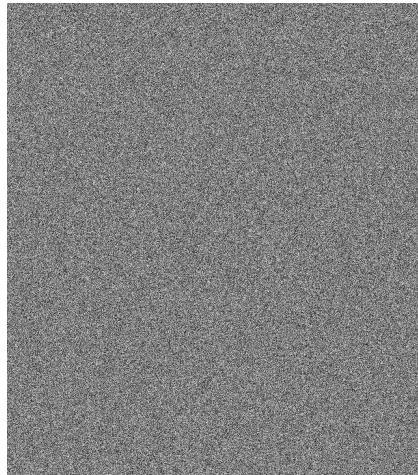


Figure 37: Image après chiffrement et bruitage OFC

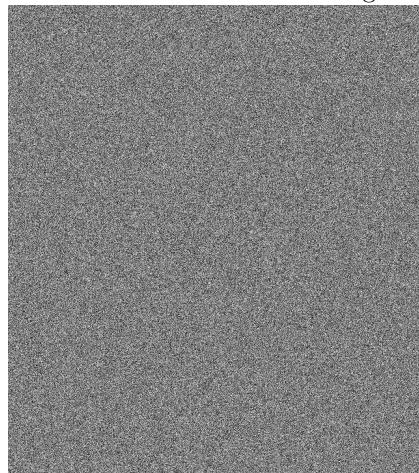


Figure 38: Image après déchiffrement OFC

Histogramme :

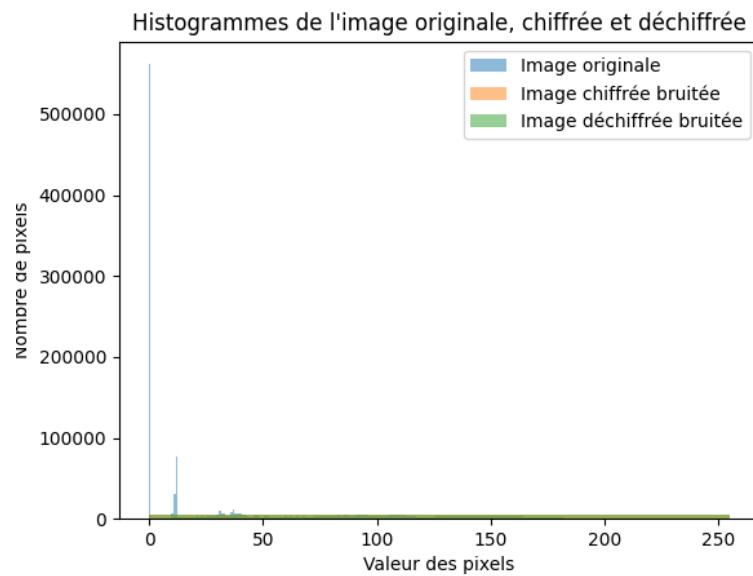


Figure 39: Histogramme image avant , après chiffrement avec bruit et après déchiffrement OFV

b) CFB

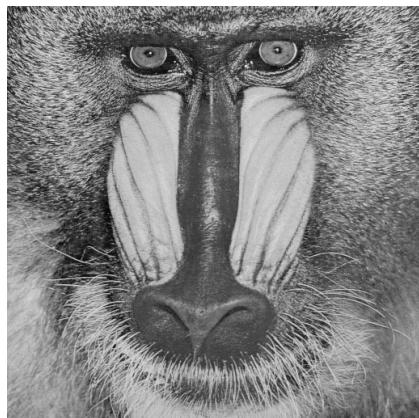


Figure 40: Image avant chiffrement

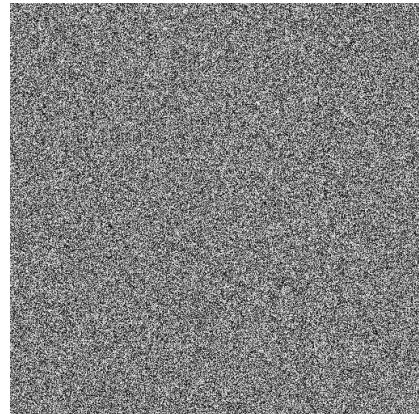


Figure 41: Image après chiffrement et bruitage CFB

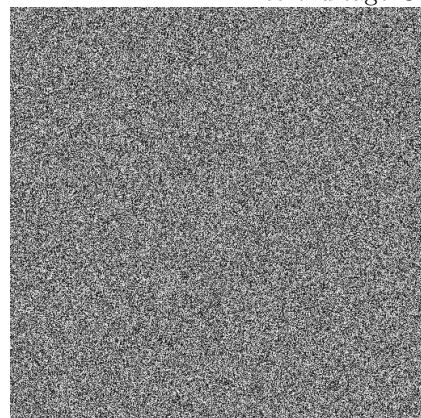


Figure 42: Image après déchiffrement CFB

Histogramme :

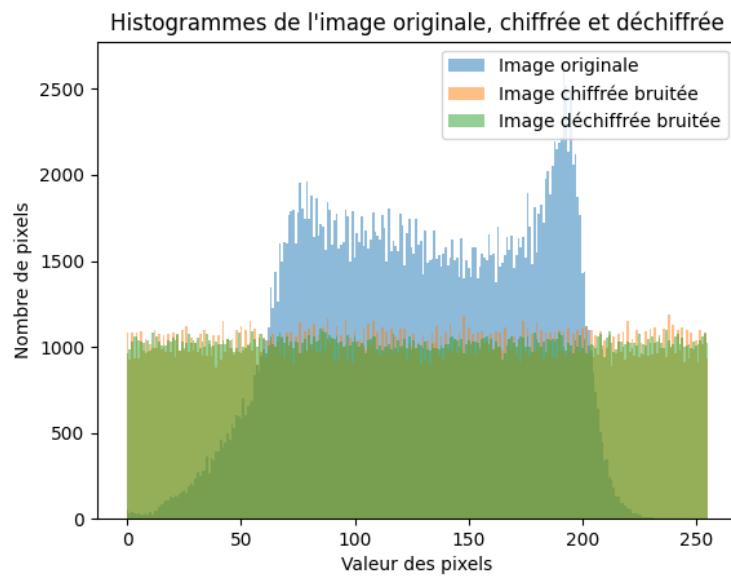


Figure 43: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CFB



Figure 44: Image avant chiffrement

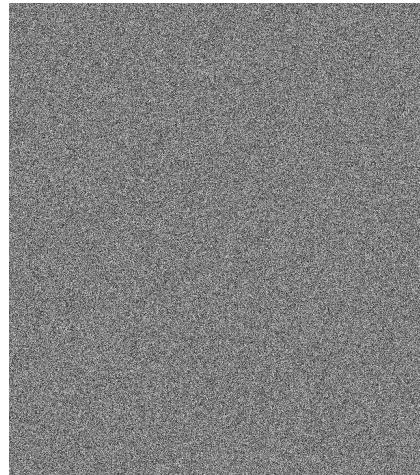


Figure 45: Image après chiffrement et bruitage CFB

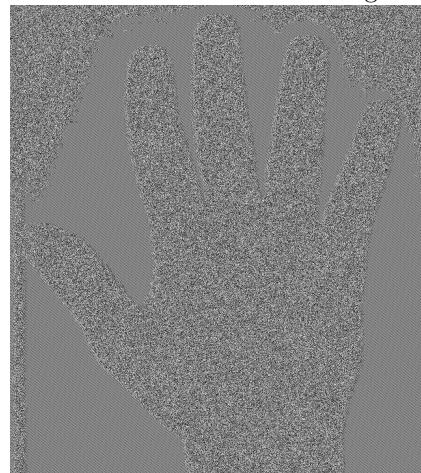


Figure 46: Image après déchiffrement CFB

Histogramme :

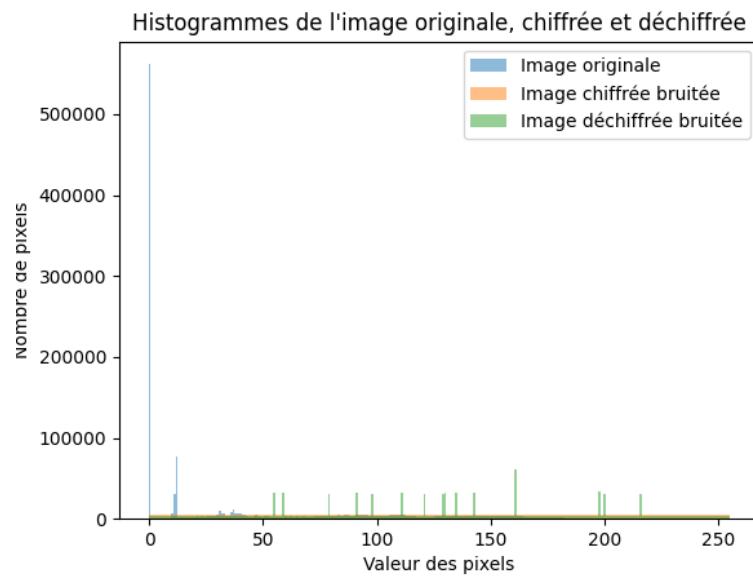


Figure 47: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CFB

c) CBC

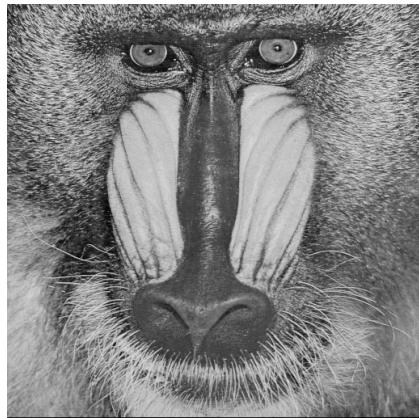


Figure 48: Image avant chiffrement

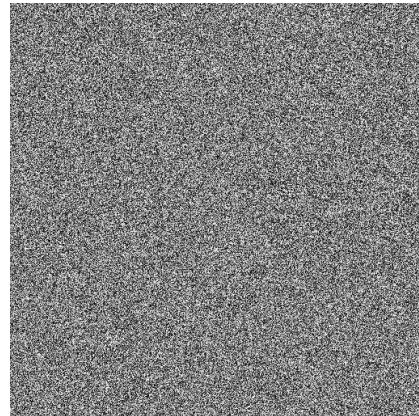


Figure 49: Image après chiffrement et bruitage CBC



Figure 50: Image après déchiffrement CBC

Histogramme :

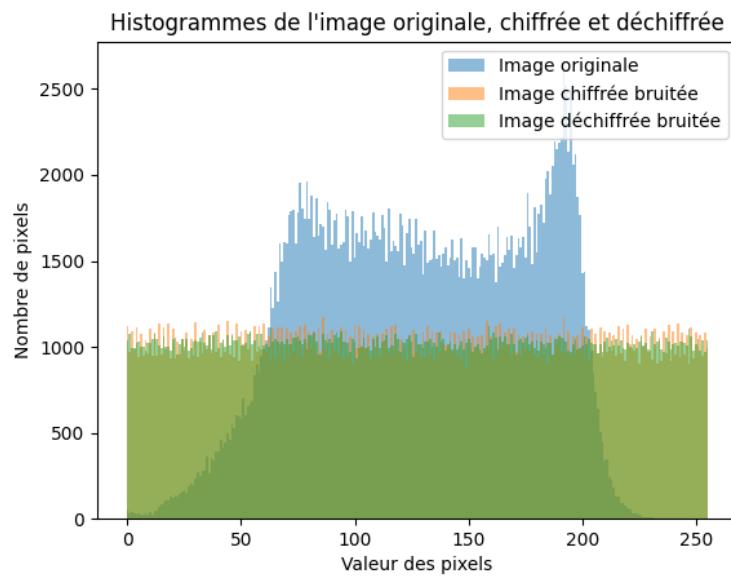


Figure 51: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CBC



Figure 52: Image avant chiffrement

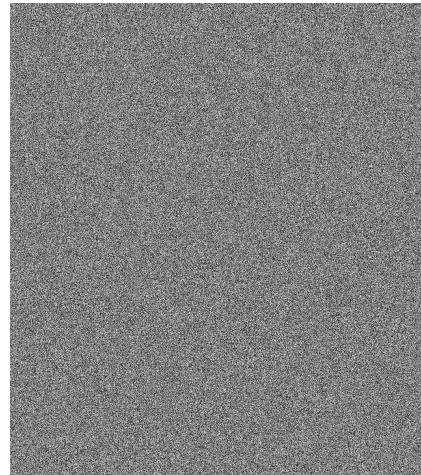


Figure 53: Image après chiffrement et bruitage CFB

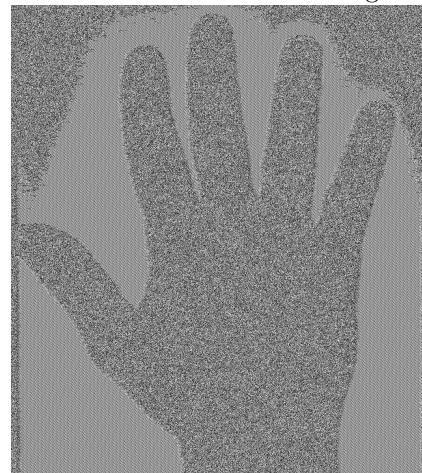


Figure 54: Image après déchiffrement CFB

Histogramme :

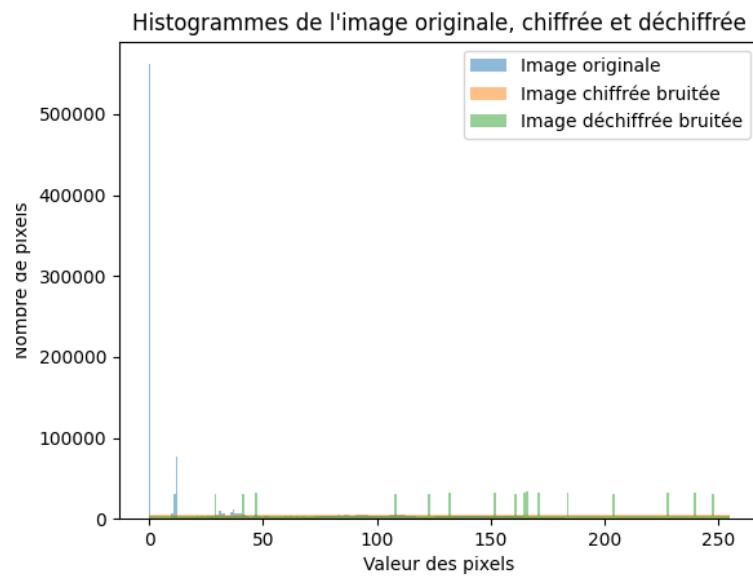


Figure 55: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CBC

d) CTR

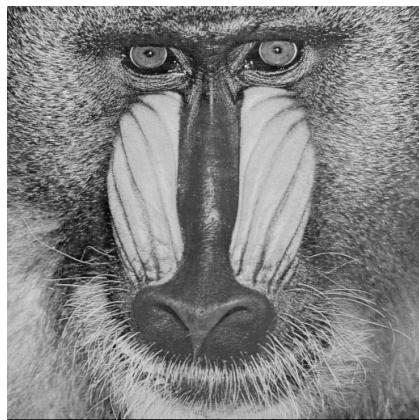


Figure 56: Image avant chiffrement

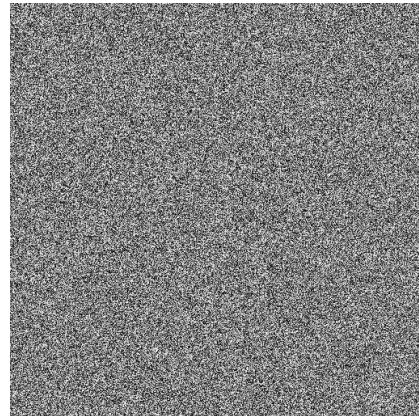


Figure 57: Image après chiffrement et bruitage CTR

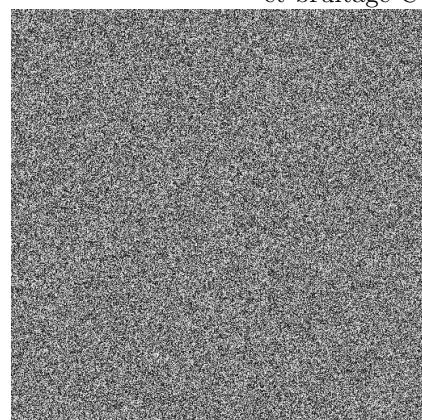


Figure 58: Image après déchiffrement CTR

Histogramme :

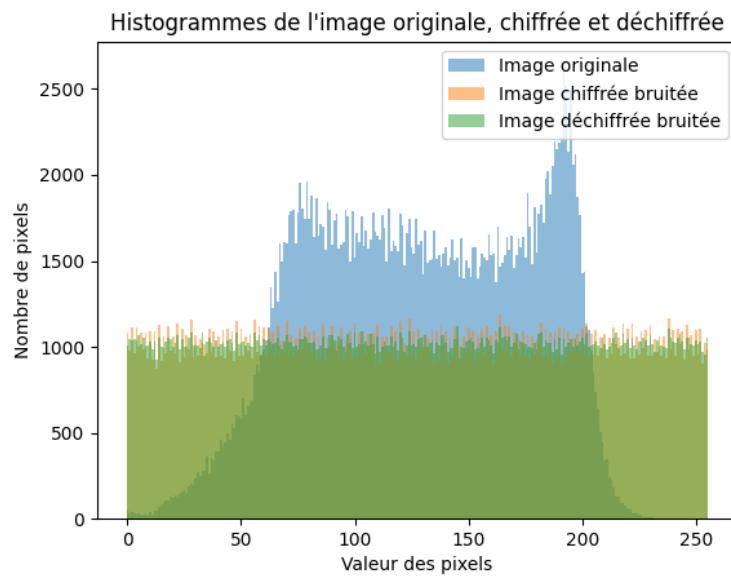


Figure 59: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CTR



Figure 60: Image avant chiffrement

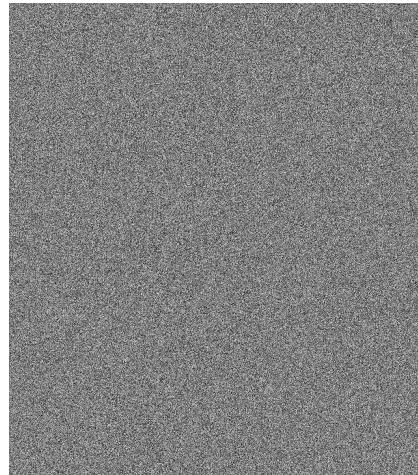


Figure 61: Image après chiffrement et bruitage CTR

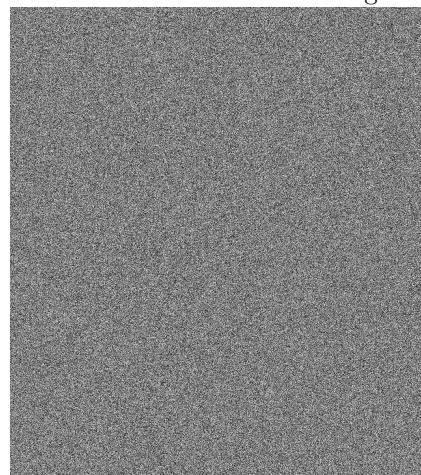


Figure 62: Image après déchiffrement CTR

Histogramme :

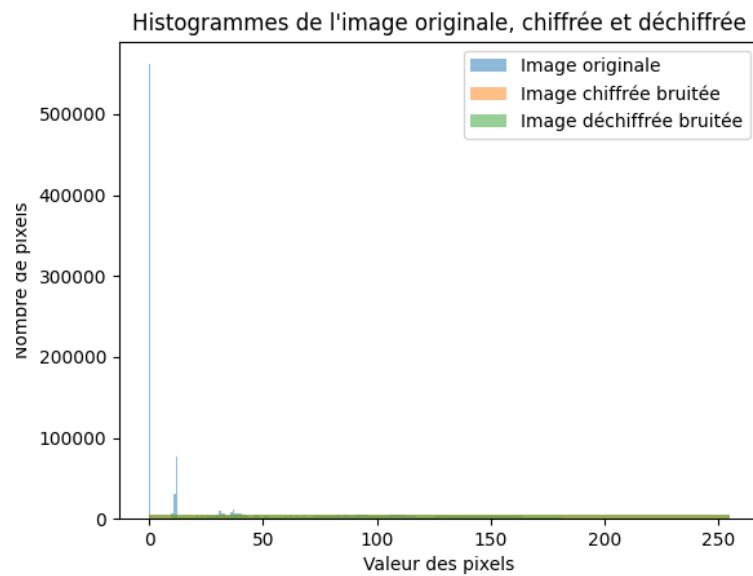


Figure 63: Histogramme image avant , après chiffrement avec bruit et après déchiffrement CTR

e) ECB

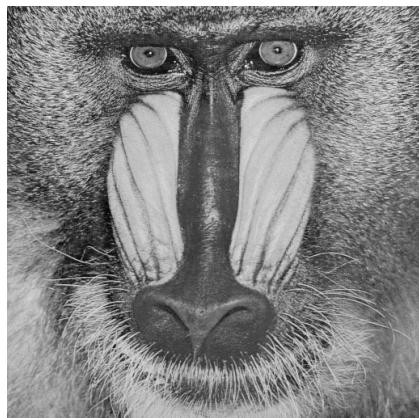


Figure 64: Image avant chiffrement

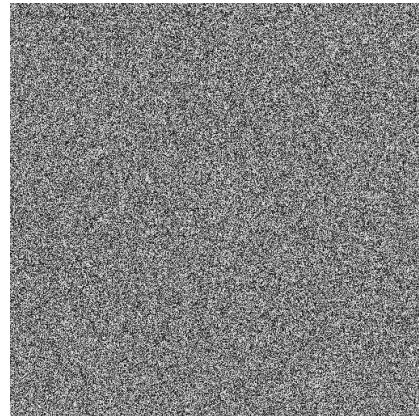


Figure 65: Image après chiffrement et bruitage ECB

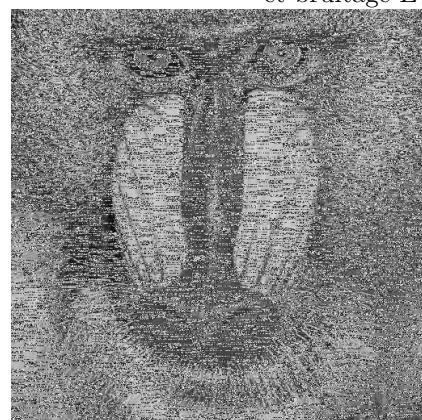
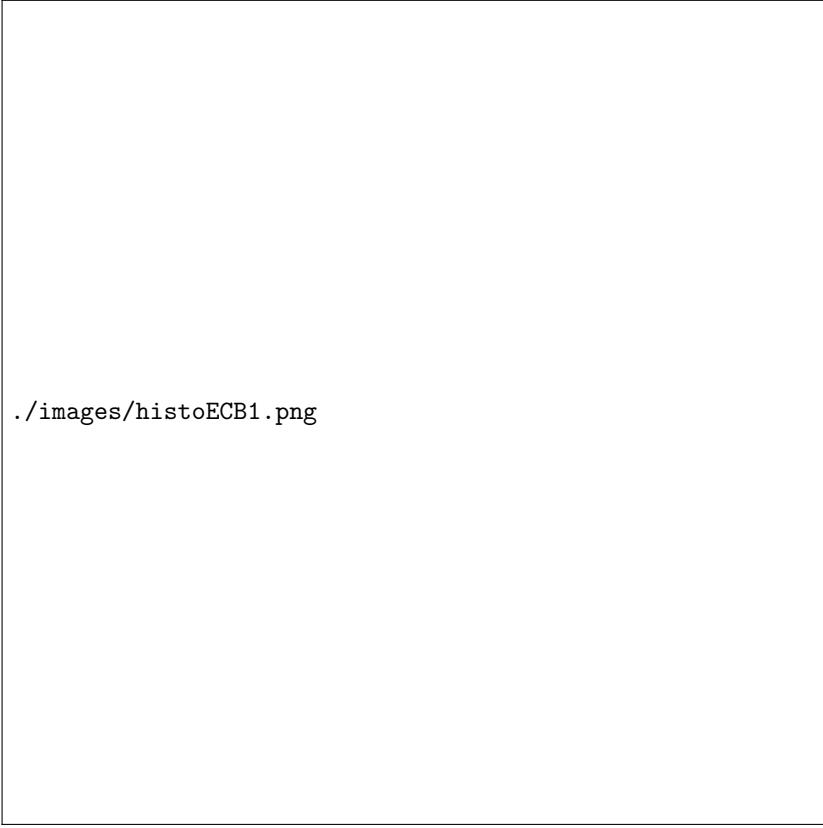


Figure 66: Image après déchiffrement ECB

Histogramme :



./images/histoECB1.png

Figure 67: Histogramme image avant , après chiffrement avec bruit et après déchiffrement ECB



Figure 68: Image avant chiffrement

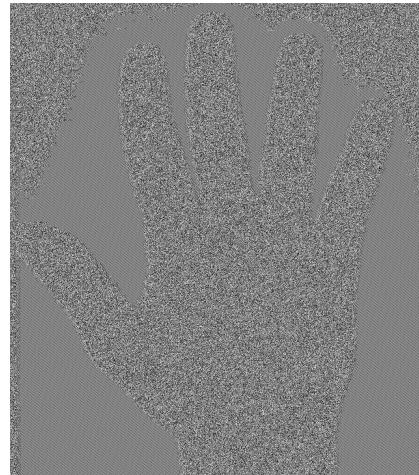
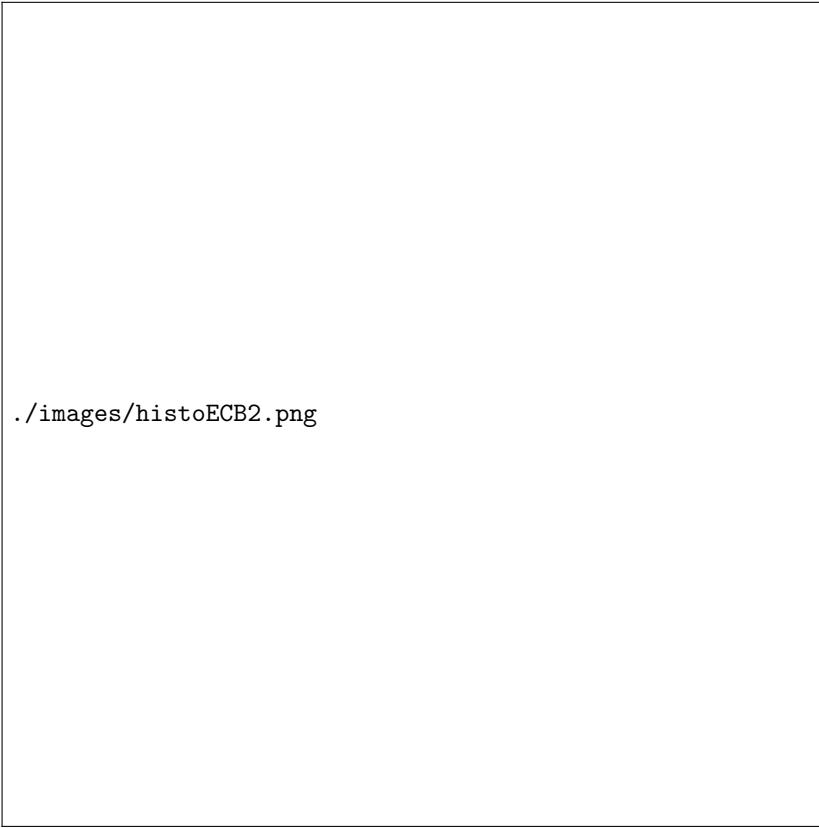


Figure 69: Image après chiffrement et bruitage ECB



Figure 70: Image après déchiffrement ECB

Histogramme :



./images/histoECB2.png

Figure 71: Histogramme image avant , après chiffrement avec bruit et après déchiffrement ECB