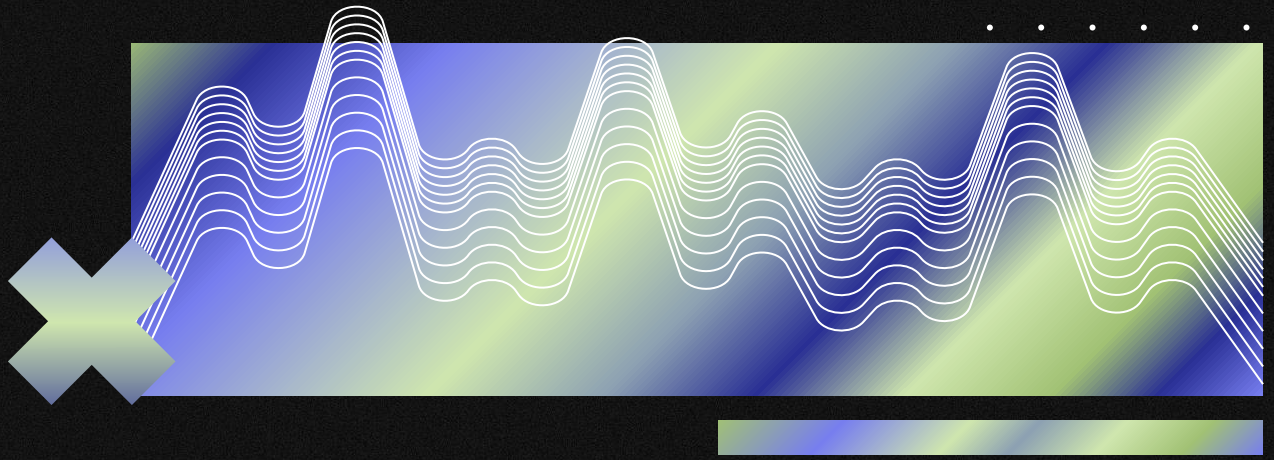


Débruitage par CNN d'images chiffrées ou secrètes bruitées

REINDERS Erwan - CLÉMENT Ange

Sous la direction de :

William PUECH - Bianca JANSEN van RENSBURG - Nicolas DIBOT - Pauline PUTEAUX

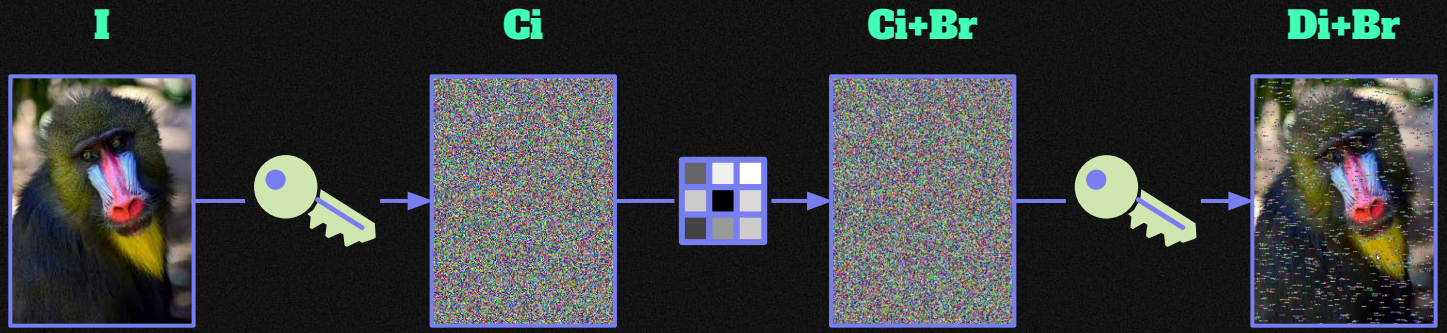
Sommaire

01

La problématique

Débruitage par CNN d'images chiffrées ou secrètes bruitées

La problématique



Bruit + Chiffrement de données

En 1999 par **Joan Daemen** et **Vincent Rijmen**

Blocs de 16 octets

Clefs de 16,24 ou 32 octets

Chiffrement

Advanced Encryption Standard

NIST

```
procedure Round(State,ExpandedKey[i])
    SubBytes(State);
    ShiftRows(State);
    MixColumns(State);
    AddRoundKey(State,ExpandedKey[i]);
end procedure
```

```
procedure Rijndael(State,Cipherkey)
    KeyExpansion(CipherKey,ExpandedKey)
    AddRoundKey(State,ExpandedKey[0])
    for i = 1 to Nr – 1 do
        Round(State,ExpandedKey[i])
    end for
    FinalRound(State,ExpandedKey[Nr])
end procedure
```

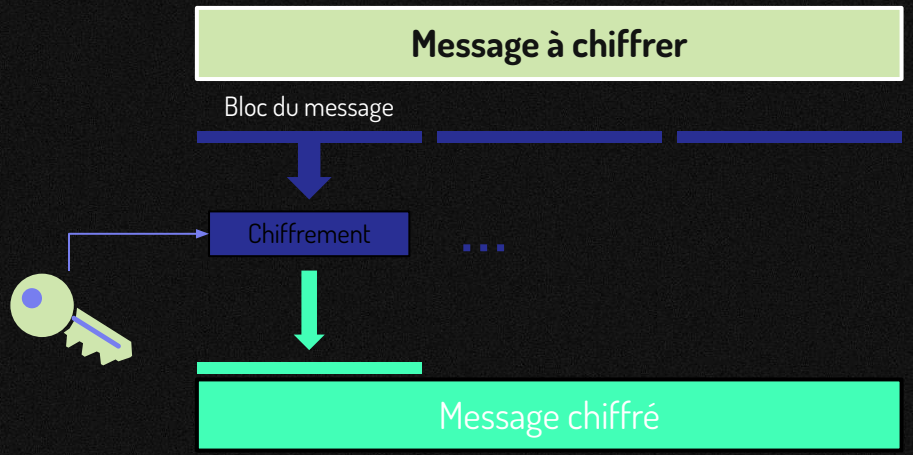
```
procedure FinalRound(State,ExpandedKey[Nr])
    SubBytes(State);
    ShiftRows(State);
    AddRoundKey(State,ExpandedKey[Nr]);
end procedure
```

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Chiffrement

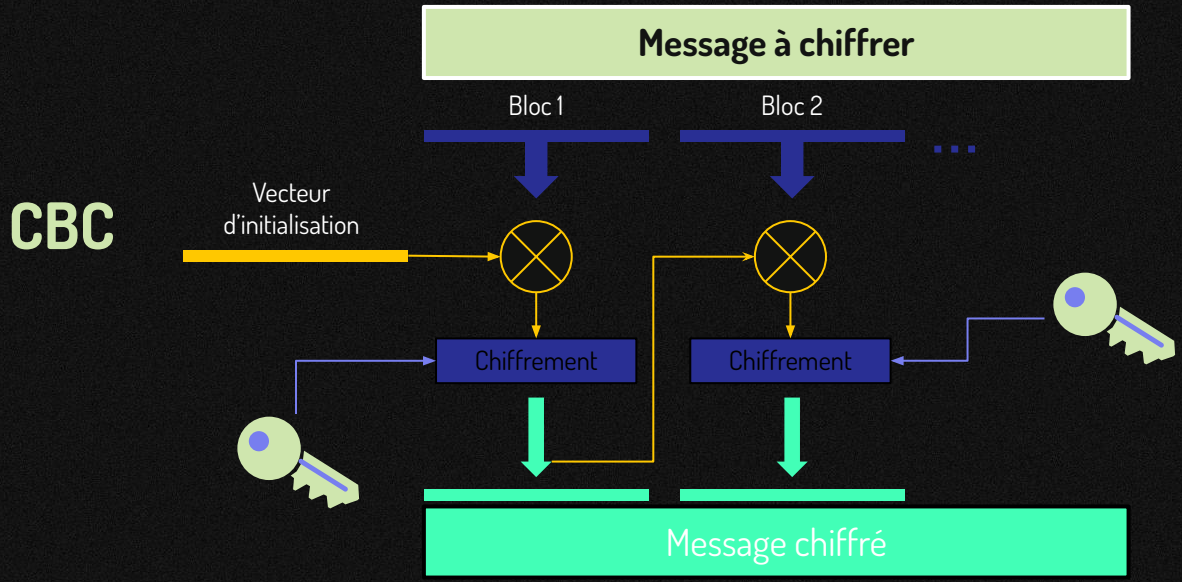
Advanced **E**ncryption **S**tandard

ECB



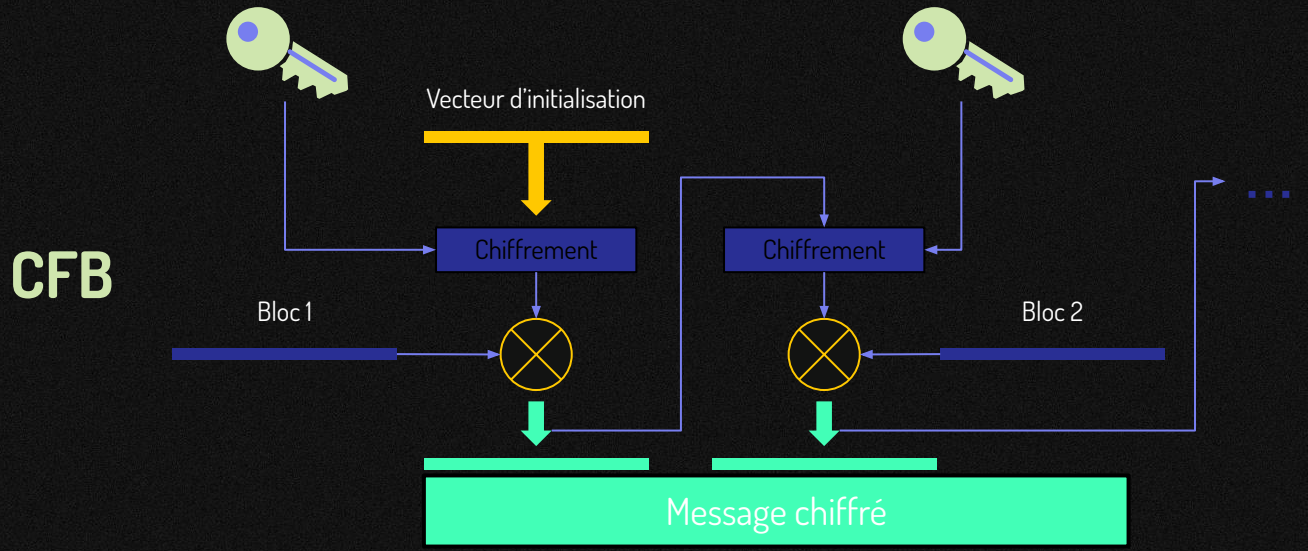
Chiffrement

Advanced Encryption Standard



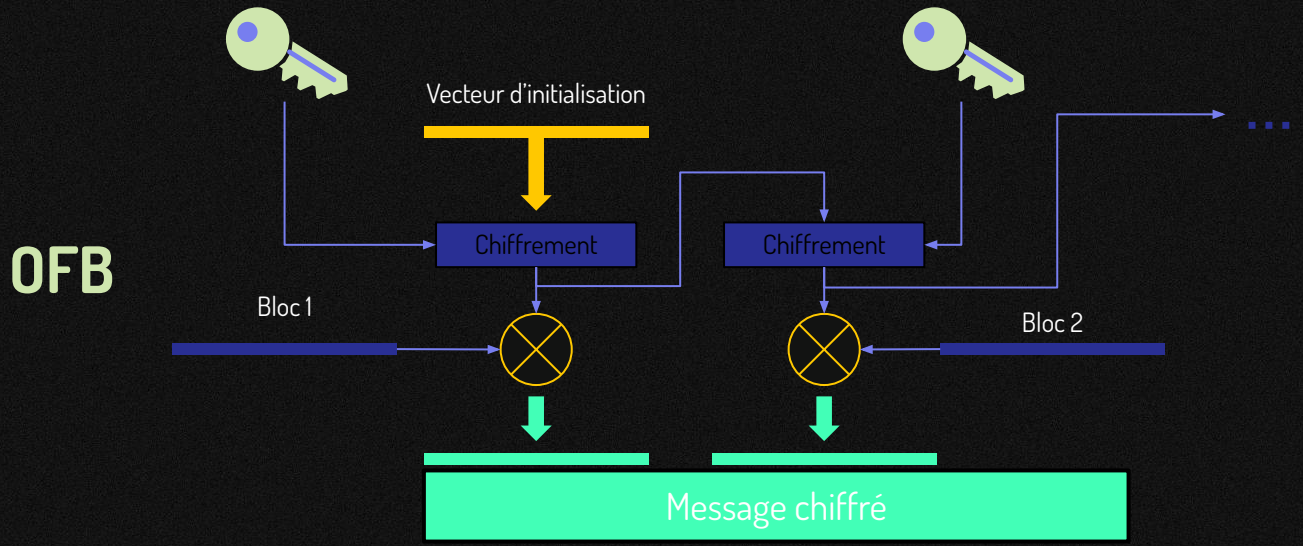
Chiffrement

Advanced **E**ncryption **S**tandard



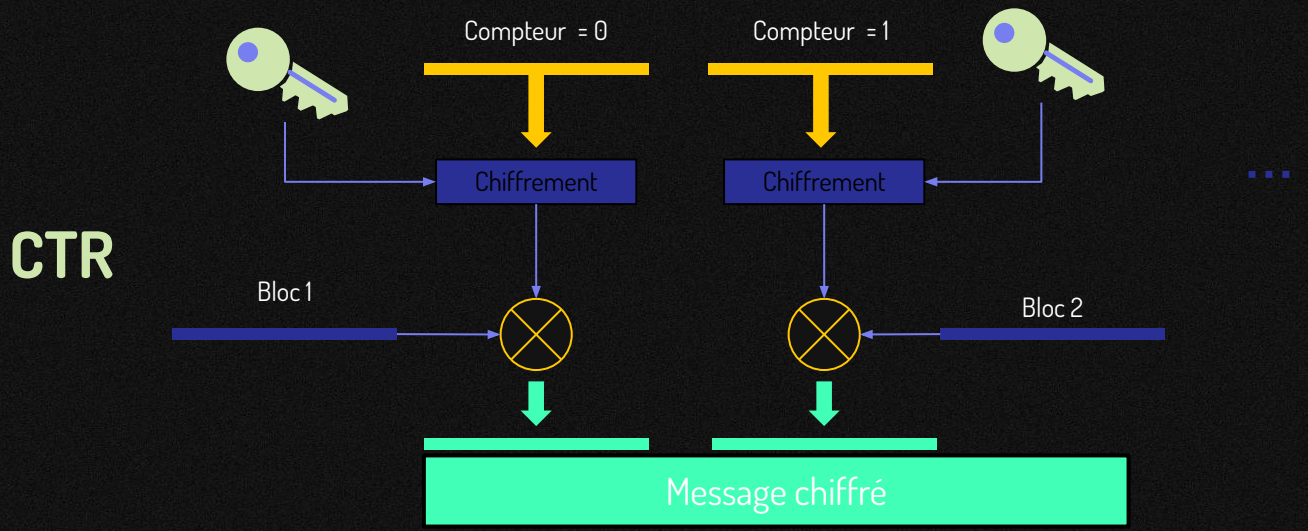
Chiffrement

Advanced **E**ncryption **S**tandard



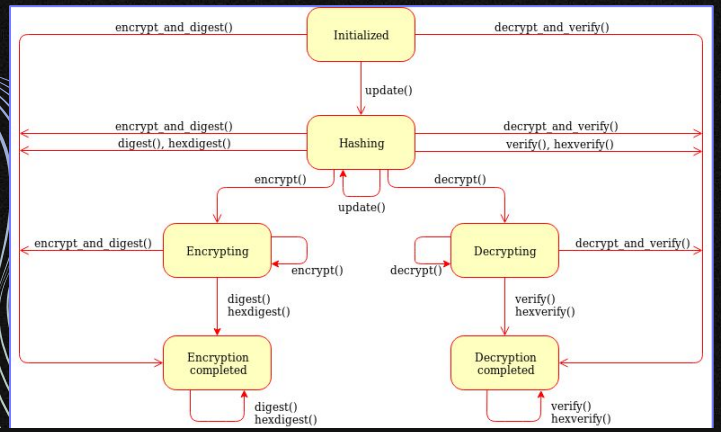
Chiffrement

Advanced Encryption Standard



Chiffrement

Advanced **E**ncryption **S**tandard



Machine à état d'un objet de chiffrement

CCM CTR + CBC-MAC

EAX

GCM Galois Counter Mode

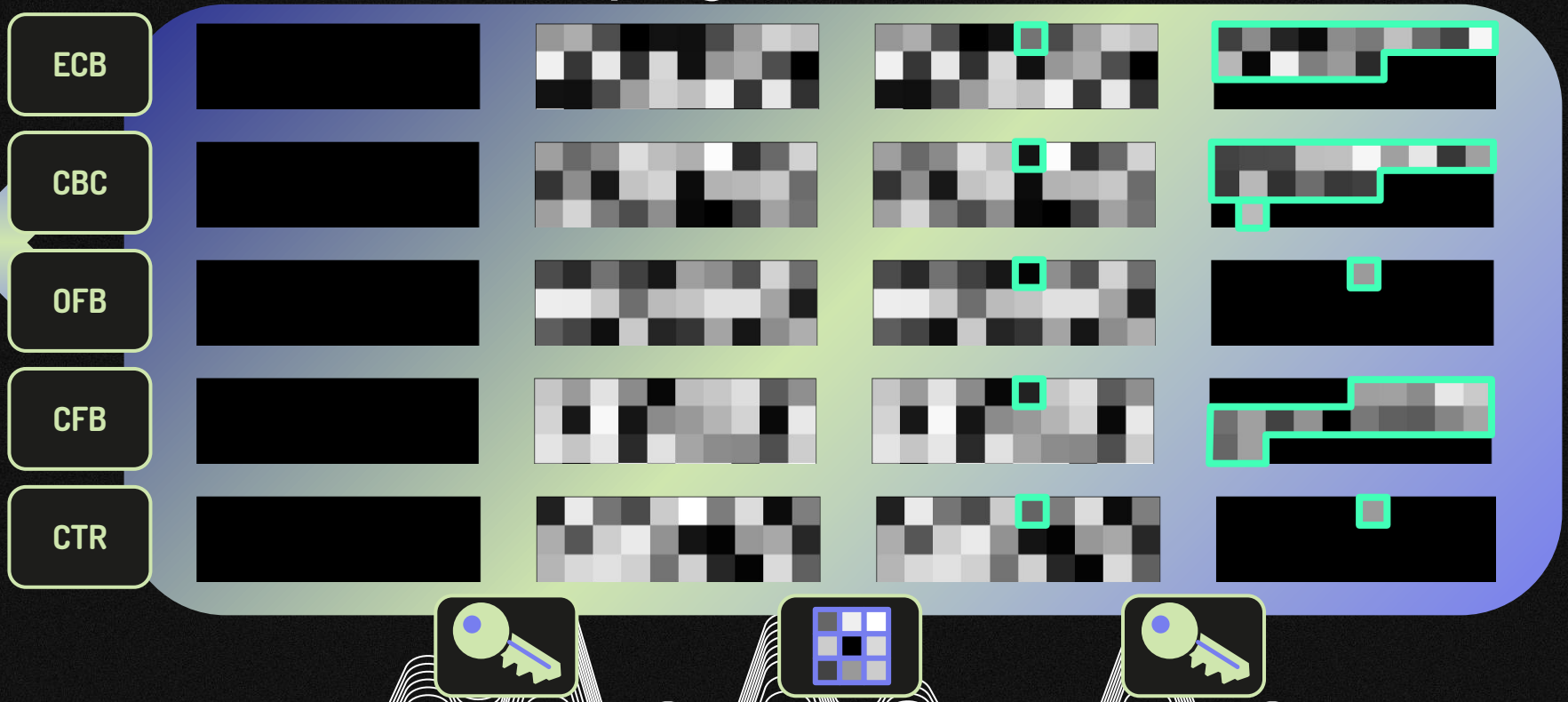
SIV Synthetic Initialization Vector

OCB Offset CodeBook

https://pycryptodome.readthedocs.io/en/latest/src/cipher/aes.html

https://pycryptodome.readthedocs.io/en/latest/

Propagation du bruit



Chiffrement

Pas de blocs de chiffrement

Pas de clefs

Basé sur des parts de secrets

Shamir

k

Partage du secret (3,5)

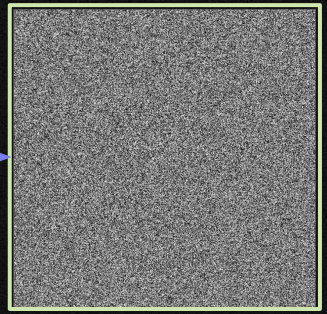
n

1 2 3 4 5

3 <= k < n

Reconstruction

k < 3



Shamir

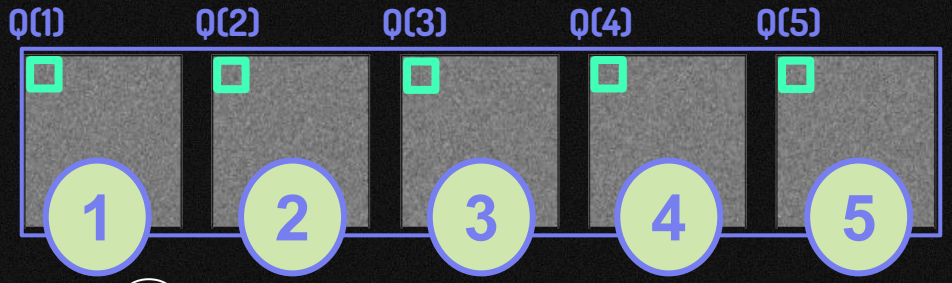
$S \in K$

K un champ de valeurs où nos valeurs à partager sont comprises.

On se donne un polynôme $Q \in K^{k-1}[X]$ pour chacune des valeurs du message à partager :

$$Q(X) = q_0 + q_1 X + q_2 X^2 + ... q_{k-1} X^{k-1}$$

Tous les coefficients q_n sont aléatoires, à l'exception de q_0, qui vaut **S**.

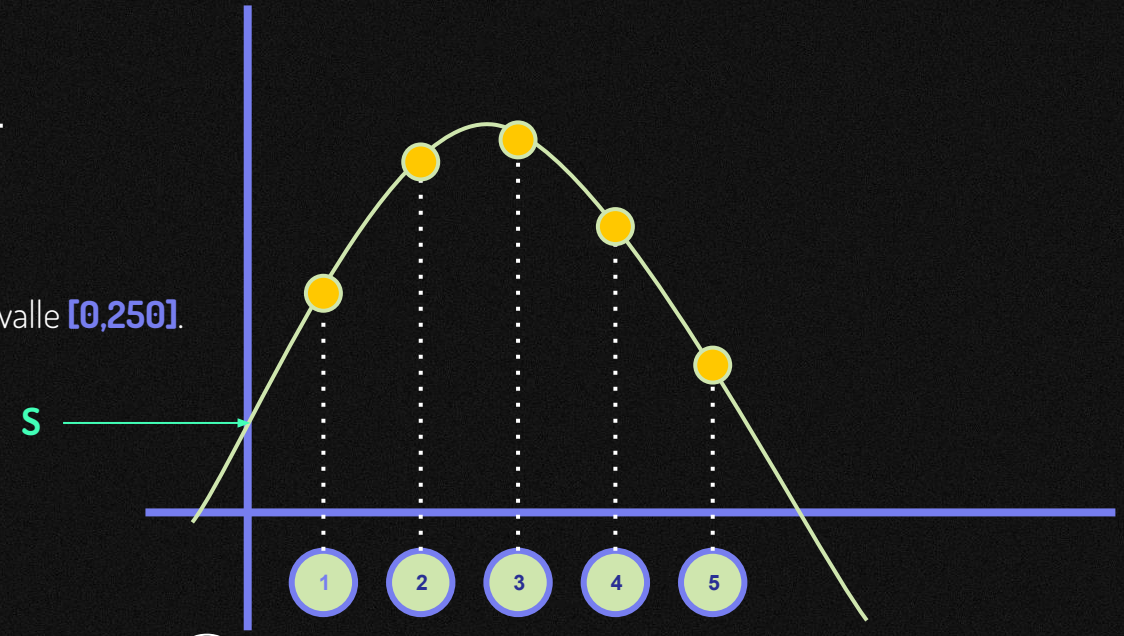


Shamir

Interpolation de Lagrange

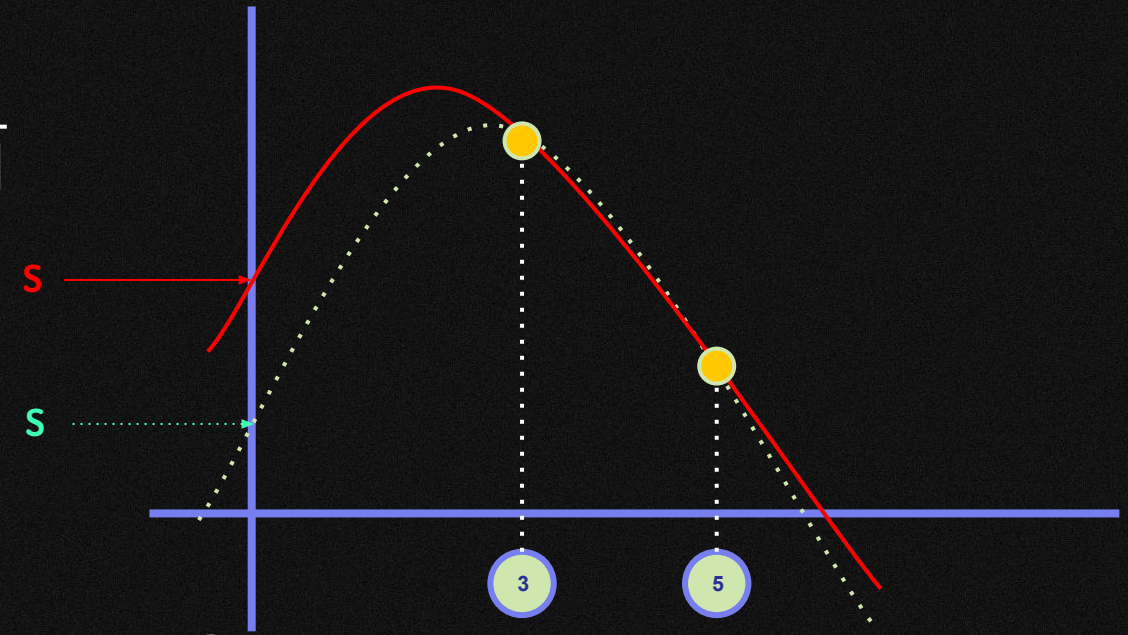
$$Q(X) = \sum_{q=1}^{k} Siq \prod_{l=1, l\neq q}^{k} \frac{X - il}{iq - il}$$

Les valeurs des pixels sont renvoyées sur l'intervalle **[0,250]**.



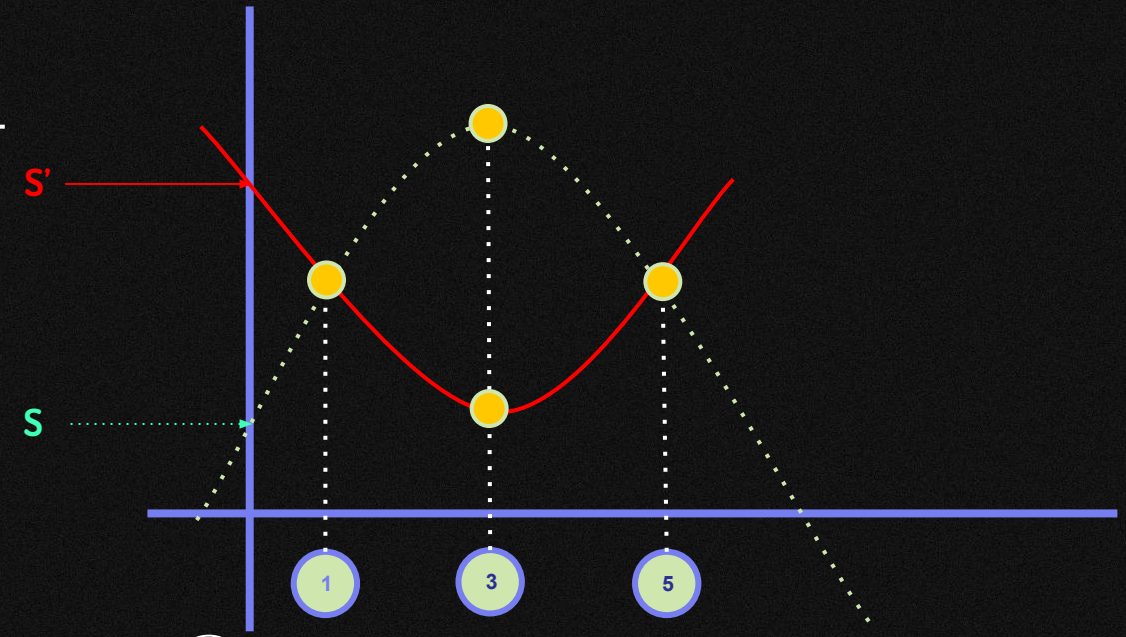
Shamir

$$Q(X) = \sum_{q=1}^{k} Siq \prod_{l=1, l \neq q}^{k} \frac{X - il}{iq - il}$$



Shamir

$$Q(X) = \sum_{q=1}^{k} Siq \prod_{l=1, l \neq q}^{k} \frac{X - il}{iq - il}$$



02

Techniques existantes

Débruiteurs, CNN classifieurs

CFB puis ECB

Propager le bruit au sein de l'image afin de faciliter sa localisation.

- Chiffrement et déchiffrement par **CFB-ECB**.
- **Segmentation de l'image** en blocs clairs et blocs bruités par utilisation de l'entropie locale de Shannon.
- Deux phases principales :
  - **Initialisation** des états possibles des blocs de pixels (score entre zéro et un, avec un pour bloc en clair).
  - **Correction** par tests combinatoires sur les 129 configurations de bits possibles.

Il devient plus facile de détecter un voisinage proche de deux blocs bruité qu'un seul pixel bruité.

$$b_{enc}(i) = \mathcal{E}_K(\mathcal{E}_K(b_{enc}(i-1)) \oplus b_{clear}(i)).$$

$$b_{clear}(i) = \mathcal{D}_K(\mathcal{E}_K(b_{enc}(i-1)) \oplus b_{enc}(i))$$

Value	Description	Correction
0	"pixel block considered as clear"	complete
1	"pixel block considered as probably incorrectly decrypted pixel block due to noise spreading from the previous pixel block during decryption"	in progress
2	"pixel block considered as probably incorrectly decrypted pixel block due to noise corruption during transmission/storage or noise spreading from the previous pixel block during decryption"	to correct later

P. Puteaux and W. Puech, "**CFB-Then-ECB Mode-Based Image Encryption for an Efficient Correction of Noisy Encrypted Images**," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 9, pp. 3338-3351, Sept. 2021, doi: 10.1109/TCSVT.2020.3039112.

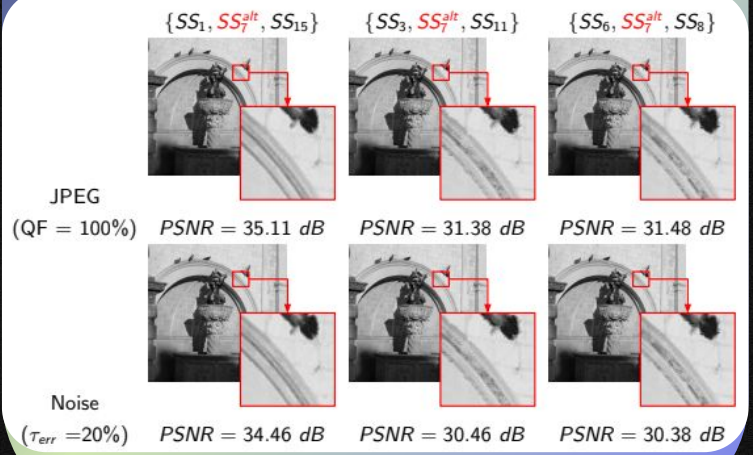
Correction de parts de secret bruitées

Débruitage de données chiffrées à l'aide de techniques dites de **partage de secrets par la méthode de Shamir**.

- **Application concrète** liée à de possibles compressions avec perte.
- Étant donné un **bruit spécifique** de type poivre et sel, on applique un écart avec une valeur médiane pour déterminer la vraie valeur.

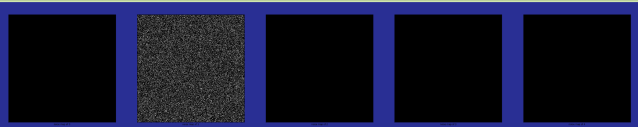
Mise en application concrète d'un scénario de débruitage sur des données chiffrées par partage de secret.

$$p_{SS_m^{alt}}(i,j) = p_{SS_m}(i,j) + \mathcal{N}(i,j) \text{ with } \mathcal{N}(i,j) \in \{-1, 0, +1\}$$



L. Bertojo and W. Puech, "**Correction of Secret Images Reconstructed from Noised Shared Images**," 2022 Eleventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2022, pp. 1-6, doi: 10.1109/IPTA54936.2022.9784125.

Correction de parts de secret bruitées



PSNR avec l'originale : 15 dB
UACI avec l'originale : 6.67 %
NPCR avec l'originale : 32.47 %

PSNR avec l'originale : 25.7 dB
UACI avec l'originale : 1.74 %
NPCR avec l'originale : 23.7 %

L. Bertojo and W. Puech, "**Correction of Secret Images Reconstructed from Noised Shared Images**," 2022 Eleventh International Conference on Image Processing Theory, Tools and Applications (IPTA), 2022, pp. 1-6, doi: 10.1109/IPTA54936.2022.9784125.

OpenCV Denoising

Méthode de débruitage utilisée dans un cas plus général de débruitage d'images.

- Se base sur de la **reconnaissance de patterns** sur une image.
- Utilisée principalement pour du débruitage de **vidéos**.

Donne des résultats imparfaits pour de la génération d'images débruitées.

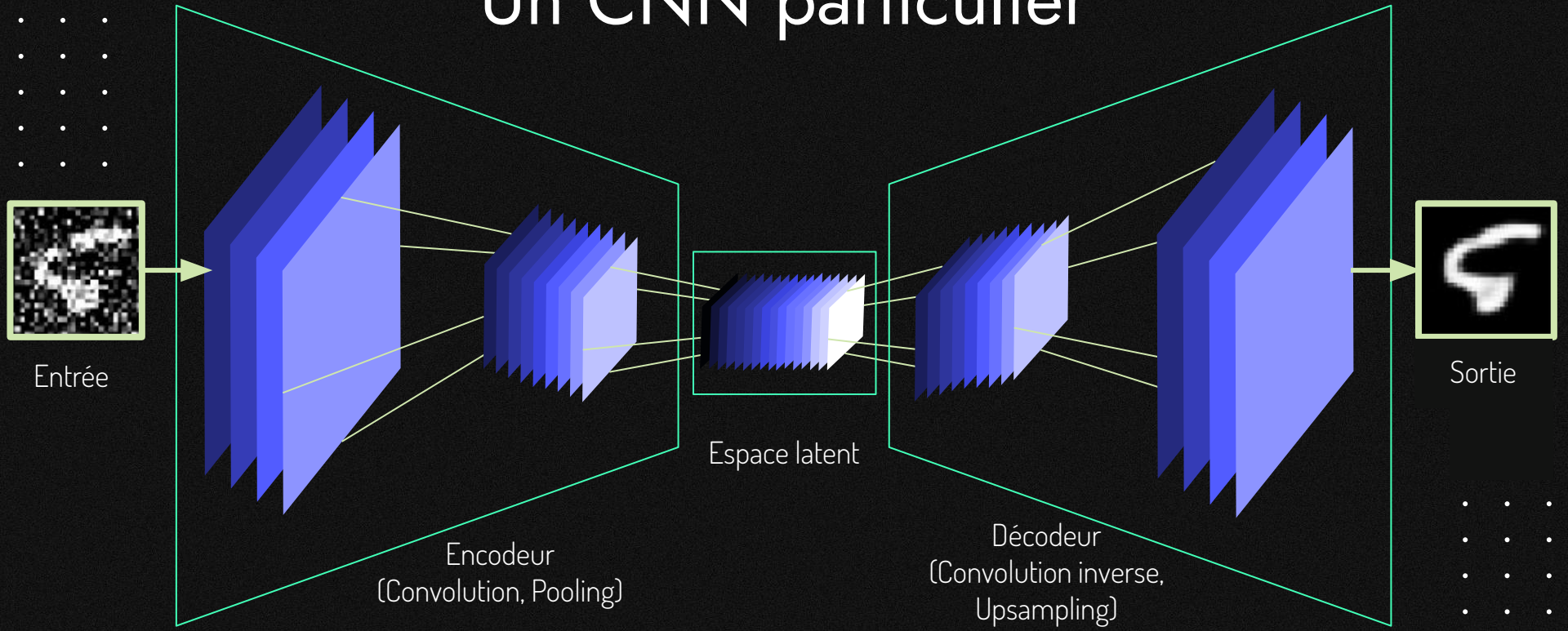
https://docs.opencv.org/3.4/d1/d79/group__photo__denoise.html

03

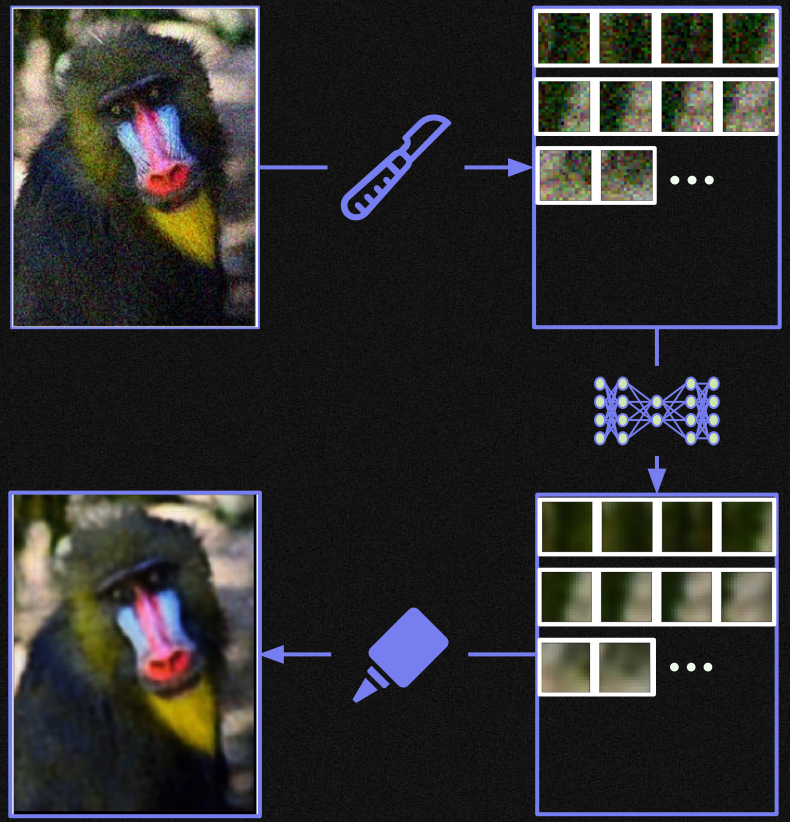
CNN auto-encodeurs

Première approche, ignore le chiffrement

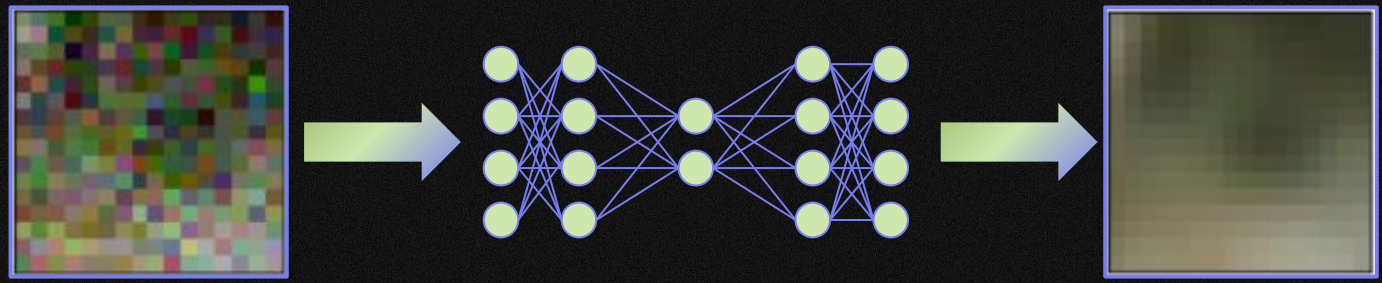
Un CNN particulier



Idée de débruitage par CNN



CNN Autoencodeurs



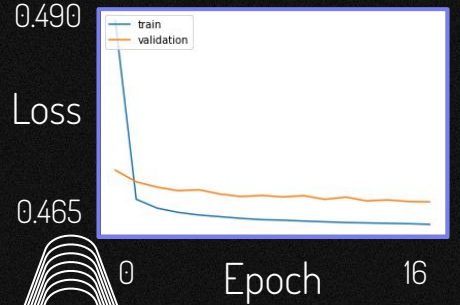
Total : 43432 blocs (16x16)

Train : 34890 (~80%)

Test : 8542 (~20%)

Epoch : 16

Batch_size : 128

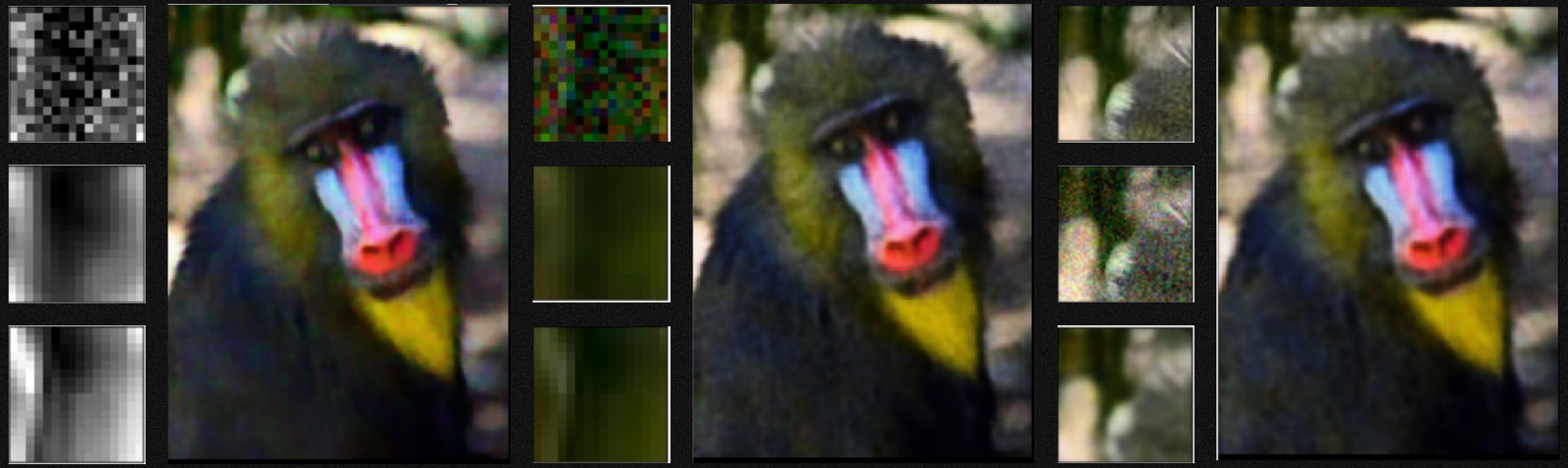


Types d'autoencodeurs testés

Bruité

Débruité

Vérité de terrain



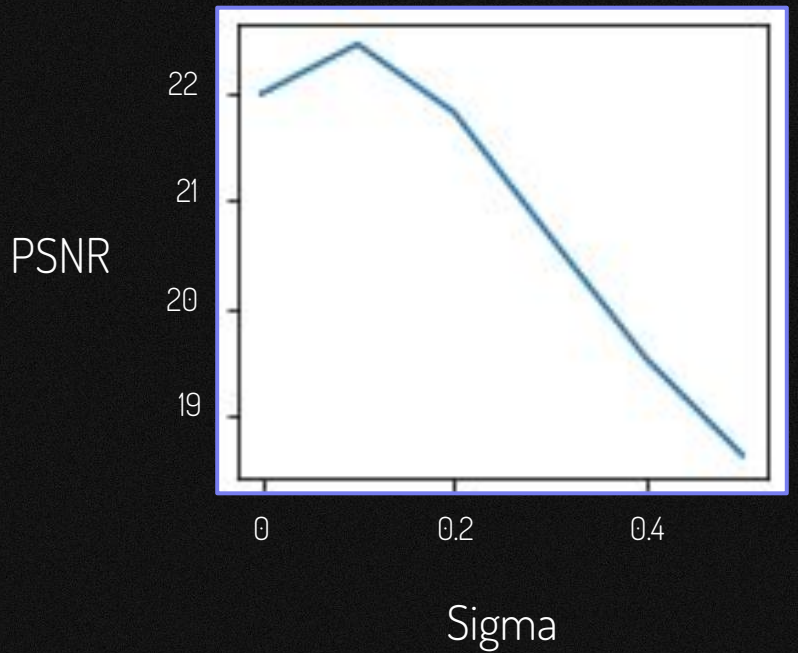
En niveau de gris

En couleurs

De grands blocs

Evaluation

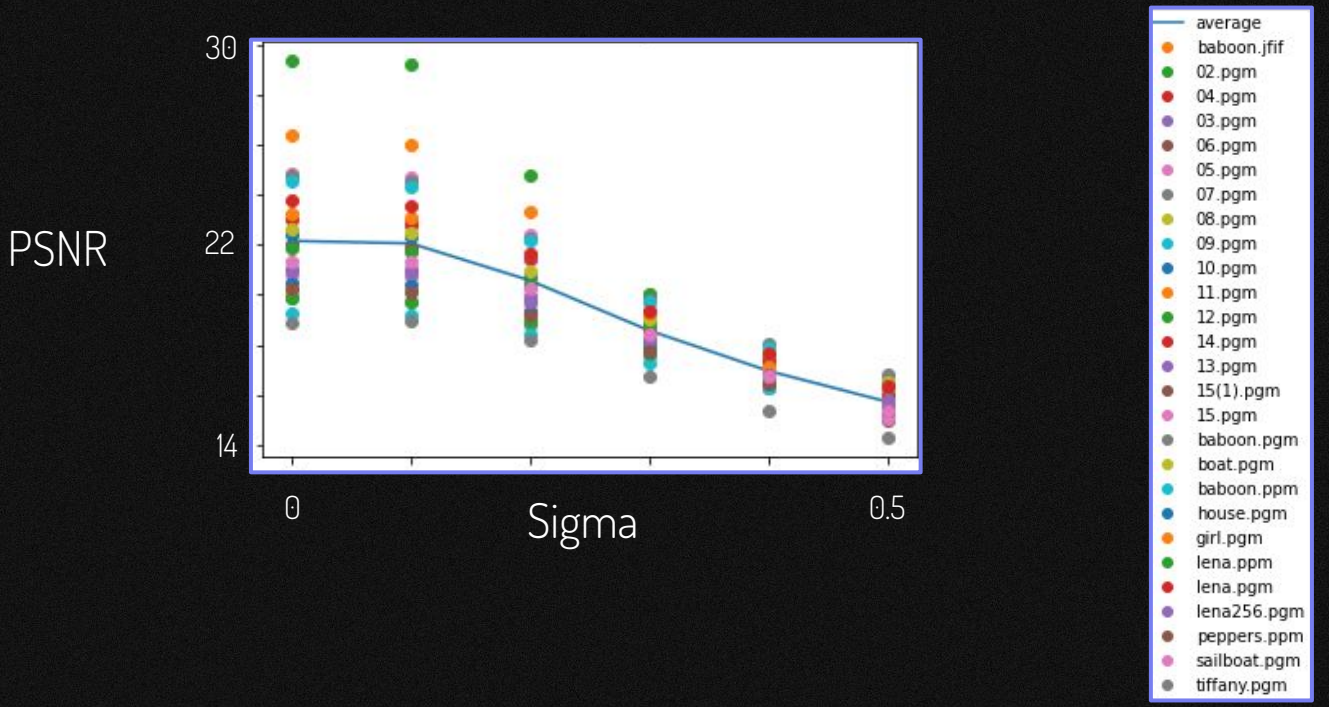
Courbe du PSNR en fonction du bruit de l'image "14.pgm" avec la méthode de blocs en niveau de gris



14.pgm

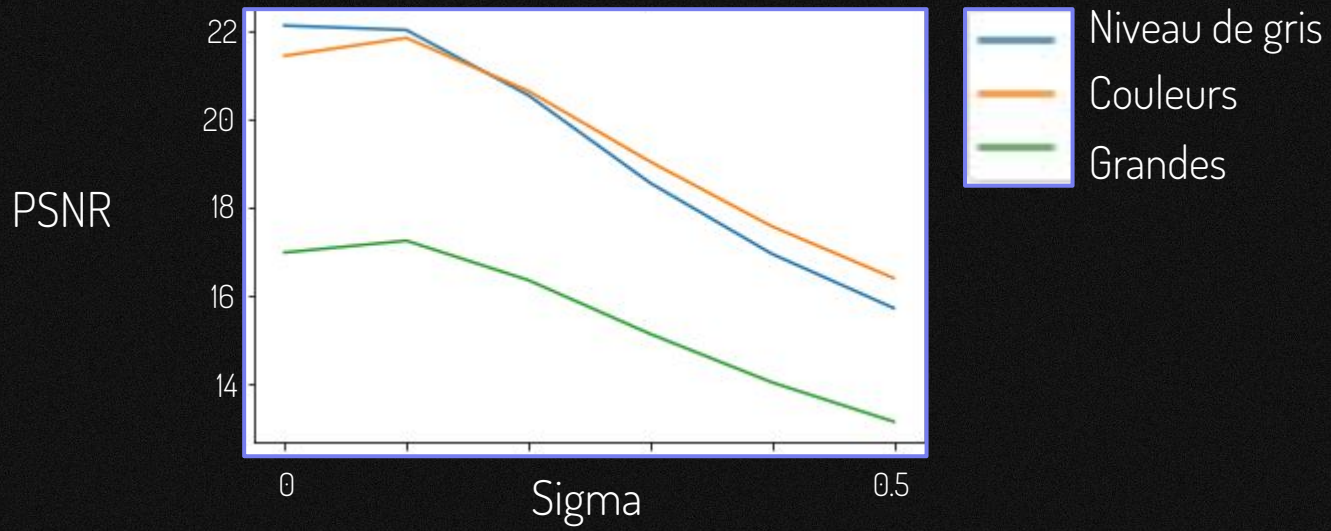
Evaluation

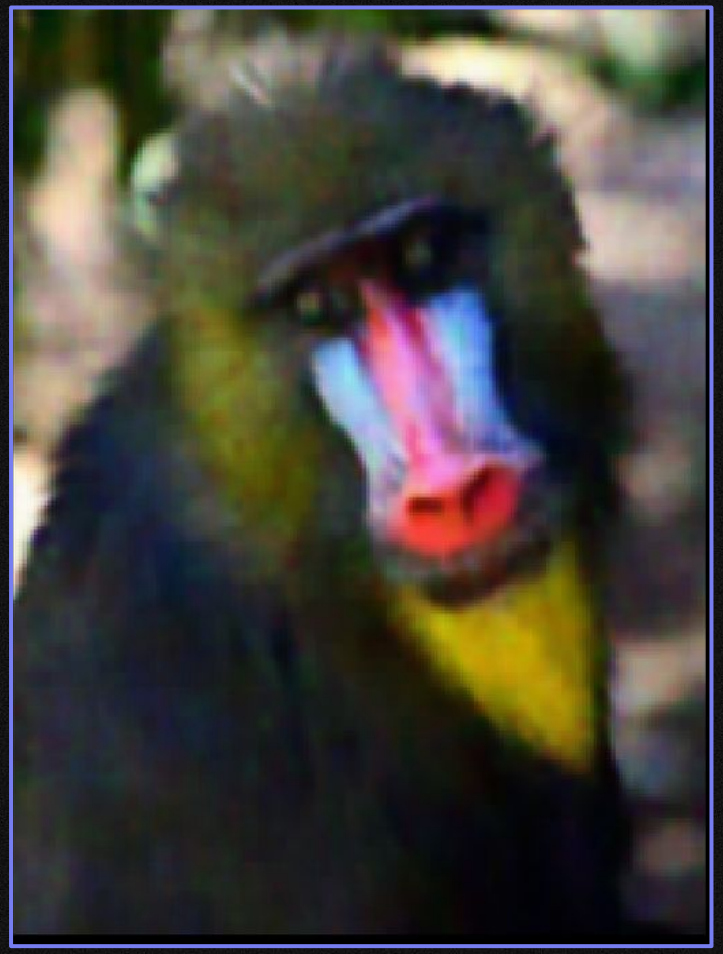
Courbe du PSNR en fonction du bruit de toutes les images avec la méthode de blocs en niveau de gris



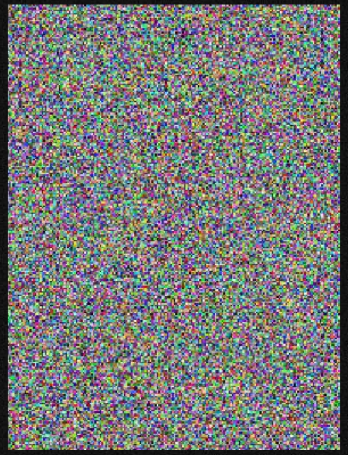
Evaluation

Courbe du PSNR en fonction du bruit de la moyenne de toutes les images avec les trois méthodes





CBC



PSNR avec l'originale: 37.80 dB
UACI avec l'originale : 5.39 %
NPCR avec l'originale : 10.71 %

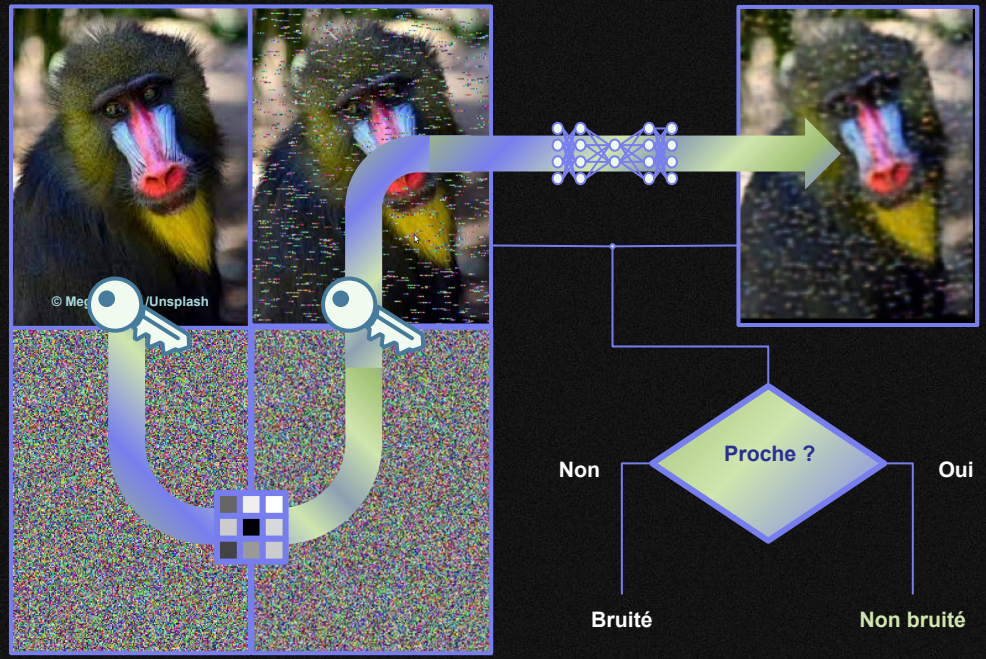
PSNR avec l'originale: 22.43 dB
UACI avec l'originale : 5.04 %
NPCR avec l'originale : 96.48 %

04

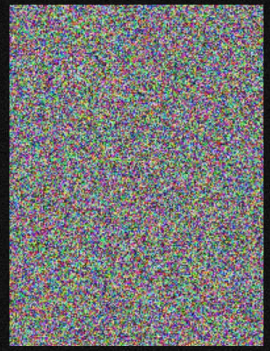
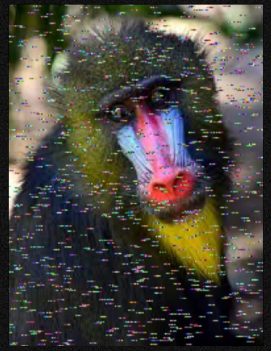
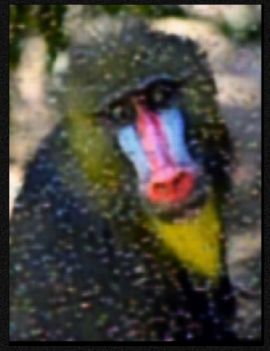
Notre technique

Débruitage sans flou, utilisation de l'image chiffrée

Détection des erreurs



Résultats

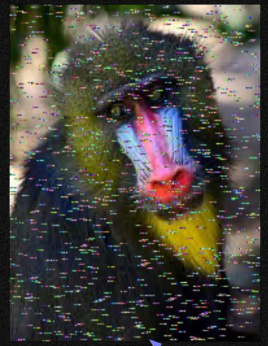
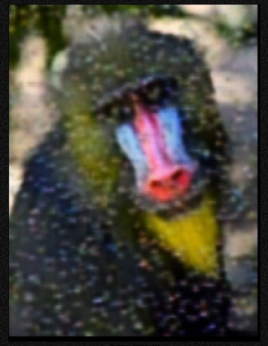
PSNR avec l'originale : 49.331 dB
UACI avec l'originale : 0.397%
NPCR avec l'originale : 0.722 %

PSNR : 38.23 dB
UACI : 4.66 %
NPCR : 9.32%

Bruit : 1 bloc sur 10 de +-1

ECB

Résultats

PSNR avec l'originale : 49.39 dB
UACI avec l'originale : 0.426 %
NPCR avec l'originale : 0.71 %

PSNR : 37.9 dB
UACI : 0.42 %
NPCR : 0.71 %

Bruit : 1 bloc sur 10 de +-1

CBC

Résultats

PSNR avec l'originale : 50.19 dB
UACI avec l'originale : 0.24 %
NPCR avec l'originale : 0.48 %

PSNR : 47.33 dB
UACI : 0.63 %
NPCR : 0.93%

PSNR : 31.33 dB
UACI : 50.85 %
NPCR : 93.59%

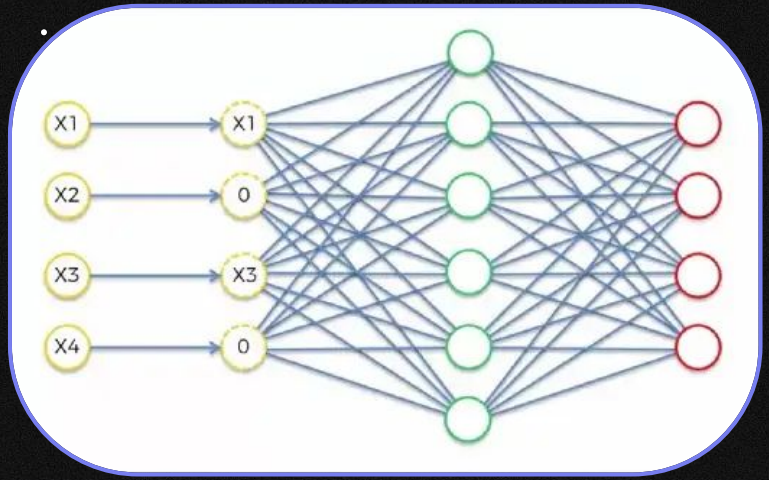
OFB

05

Améliorations

Pour la suite ...

Amélioration de l'auto-encodeur

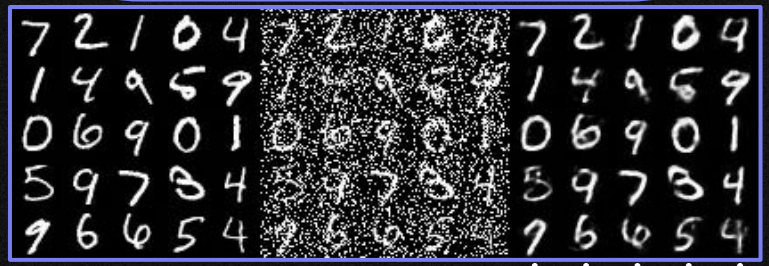


Améliorations possibles

- Plus d'entraînement, avec plus d'images
- Essayer d'autres méthodes de coût

Denoising Auto Encoder : DAE

- Plus adapté au débruitage
- Plus long et complexe à entraîner



https://towardsdatascience.com/denoising-autoencoders-explained-dbb82467fc2.

Autres pistes pour le chiffrement

Chiffrement **Homomorphique**

Corps Gallois pour le partage de secrets

Chiffrement par **génération chaotique**

- Arnold's Cat Map
- Baker's Map
- Two-Dimensional Logistic Chaotic Map

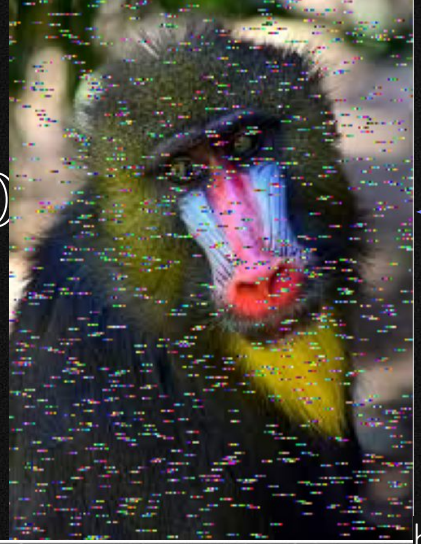
M. Preishuber, T. Hütter, S. Katzenbeisser and A. Uhl, "**Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption**," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 9, pp. 2137-2150, Sept. 2018, doi: 10.1109/TIFS.2018.2812080.

Naveed Islam, Zafar Shahid, William Puech. "**Denoising and error correction in noisy AES-encrypted images using statistical measures**", Signal Processing: Image Communication, Volume 41, 2016, Pages 15-27, ISSN 0923-5965,

06

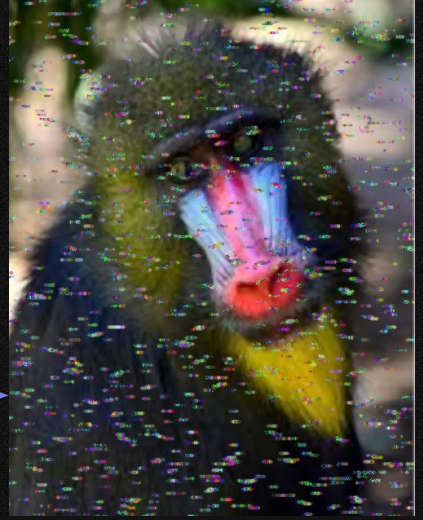
Conclusion

La conclusion

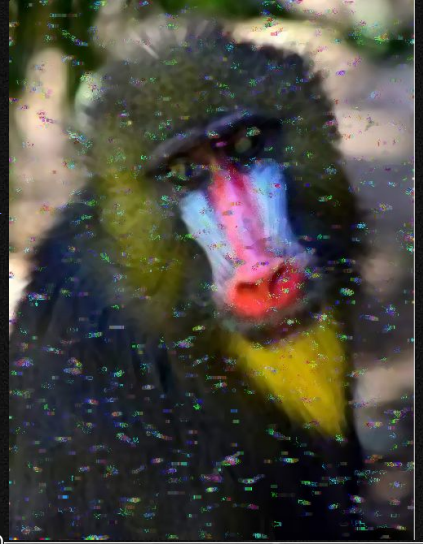


Original

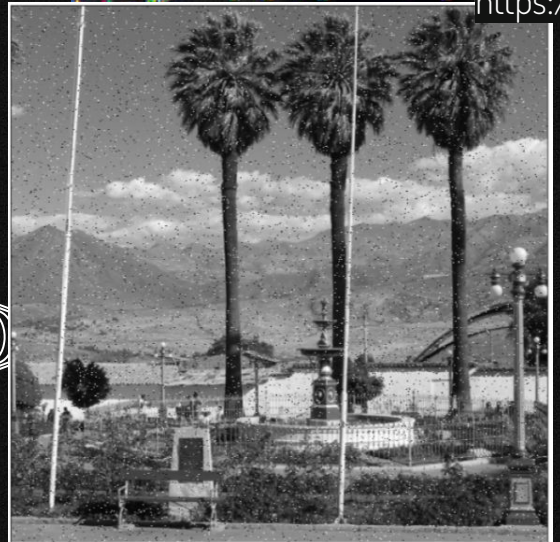
Débruité (3)



Débruité (6)



https://online-photo-converter.com/image-noise-reduction



Fin

Des questions ?