

Rapport N°5

Semaine : 21/11/2022

Ce compte rendu est le cinquième dans le cadre du projet image du premier semestre de Master 2 IMAGINE. Il comprend nos avancées dans la recherche et l'implémentation de l'environnement de recherche.

Tâches effectuées

Entretien avec monsieur Puech :

Lors de notre entretien avec monsieur Puech le lundi 21/11, nous avons échangé autour de différents algorithmes de chiffrement. Dans un premier temps, nous avons évoqué Shamir, avec les deux modes que nous avons pu mettre en place. Il nous a indiqué qu'il serait intéressant d'avoir un algorithme de Shamir sur des corps Gallois $GF(2^8)$.

On a également abordé les techniques de chiffrement liées à la génération chaotique de nombres. Cette génération se base sur le principe de la génération de séquences aléatoires, avec comme spécificité qu'à un moment donné de la génération, on va obtenir une grande variation d'une génération à l'autre (notion de chaos car forte tendance aléatoire entre deux générations successives).

Monsieur Puech nous a alors indiqué que ce type de chiffrement pourrait être intéressant à mettre en place pour le projet.

Entretien avec Pauline Puteaux :

Lors de notre oral du 23/11, nous avons échangé avec Pauline Puteaux sur notre travail, et sur la manière d'aborder certaines autres techniques de chiffrement.

Premièrement, concernant notre travail, nous avons échangé sur les techniques déjà implémentées de chiffrement. Nous avons ainsi parlé de AES, avec du chiffrement par bloc. Notre méthodologie se base sur des blocs en ligne, ce qui peut poser problème pour certains cas de détection, alors qu'un bloc carré fonctionnerait mieux.

Nous avons également parlé de Shamir, et du fait qu'il n'était potentiellement pas utile de s'attarder trop sur la mise en place en profondeur des corps Galois $GF(2^8)$.

Nous avons aussi parlé des autoencoders, et du fait que les autoencoders variationnels ne sont pas si intéressants pour notre traitement.

Enfin, nous avons discuté des méthodes de chiffrement par homomorphisme. L'homomorphisme se base sur l'application d'opérateurs sur deux structures algébriques similaires. Dans notre cas, les deux structures similaires sont les images claires et chiffrées. Ainsi, l'homomorphisme peut se voir comme une traduction entre des opérations que l'on ferait dans l'espace image claire, avec des opérations que l'on ferait dans l'espace image chiffrée. Cependant, pour notre cas d'utilisation, cela ne nous sera pas utile. En effet, même si on peut faire de la supposition sur les différents types de bruits appliqués, elles ne sont pas très précises. Arriver à débruiter dans l'espace des images chiffrées reste de même complexité que d'arriver à débruiter dans l'espace de images déchiffrées.

Au niveau du code :

Sur les CNN, nous avons essayé d'appliquer les techniques de débruitage à des images complètes (pas les chiffres MNIST). Pour cela, on découpe des photographies en blocs, puis

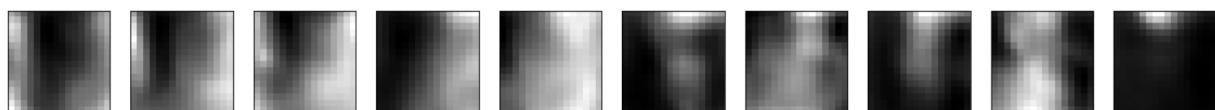
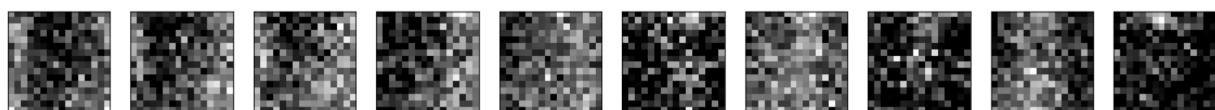
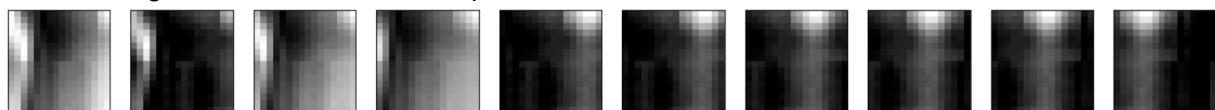
on entraîne un auto encodeur afin de débruiter ces blocs. Enfin, on peut reconstituer une image à partir de ses blocs.

- Premièrement, nous avons essayé d'utiliser des petits blocs de 16x16 en niveaux de gris. Ainsi, une photographie est découpée en blocs rouges, verts et bleus.

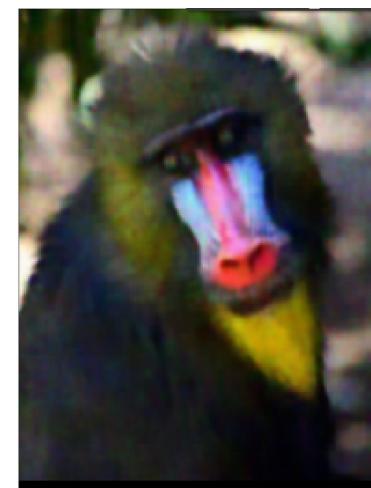
Première ligne : les blocs en niveau de gris

Deuxième ligne : les blocs bruités

Troisième ligne : les blocs débruités par CNN

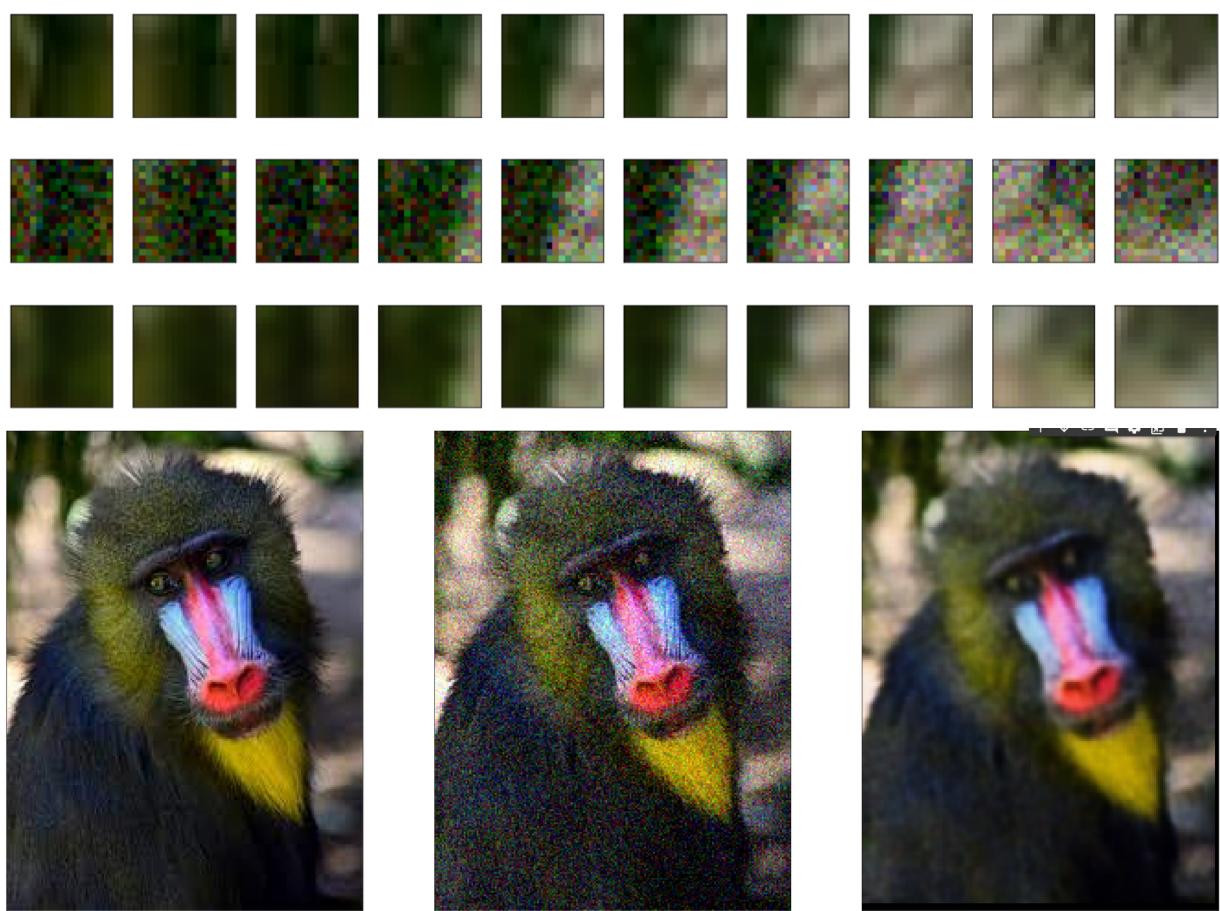


On reconstruit donc l'image à partir de blocs 16x16, mais on peut spécifier un padding afin de simuler un glissement du bloc le long de l'image. Ces résultats ont été réalisés avec un padding de 4 ($\frac{1}{4}$ de la taille du bloc) : (à gauche : l'image originale, au milieu : image bruitée, à droite : image débruitée par CNN)

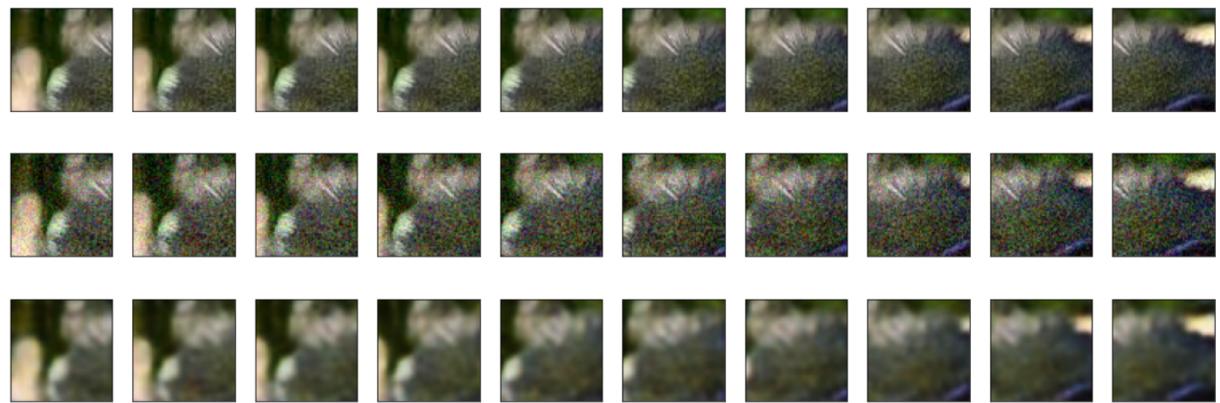


On constate que l'image reconstituée est généralement floue. De plus, comme les couleurs sont traitées de manière séparée, des tâches de couleur peuvent apparaître.

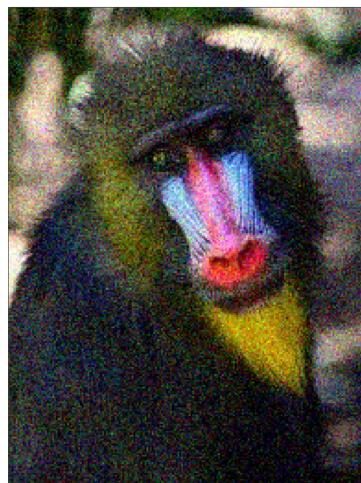
- Ensuite, nous avons choisi d'utiliser des blocs RGB. Pour cela, il a fallu adapter le CNN afin qu'il accepte ces blocs (on a donc une entrée de taille (16, 16, 3))



- Enfin, nous avons essayé d'agrandir la taille des blocs, ils ont maintenant une taille de 64x64.



La reconstruction à été faite avec un padding de 16 ($\frac{1}{4}$ de la taille des blocs)



On constate qu'une augmentation de la taille des blocs ne résulte pas à une augmentation de la qualité visuelle.

Au niveau de la recherche d'informations :

- Nous nous sommes ainsi renseignés sur les algorithmes de chiffrement par génération chaotique. Nous avons donc regardé le papier suivant :

Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption, de Mario Preishuber, Thomas Hütter, Stefan Katzenbeisser, and Andreas Uhl.

Qui dresse un portrait global de ces méthodes de chiffrement chaotique, avec un regard plus critique sur l'analyse sécuritaire de ces méthodes de chiffrement. En effet, les métriques qui sont souvent utilisées pour garantir la sécurité de telles méthodes de chiffrement, ne sont pas suffisantes, car ces techniques de chiffrement souffrent d'une dépendance trop forte à leur algorithme. Le cas de la sécurité n'est pas un aspect essentiel de notre projet, mais reste à prendre en compte dans le cas de scénarios concrets de chiffrement de données.

- Nous avons ainsi regardé le principe de chiffrement homomorphique, afin de voir si cela pouvait nous servir pour la suite du projet, mais c'est une piste que nous avons abandonnée pour les raisons décrites plus haut.

Reste à faire

Au niveau de ce qu'il nous reste à effectuer :

- Mise en place d'une interface de présentations de résultats de débruitement.
- Mise en place d'un poster retraçant ce que nous avons fait durant ce projet.