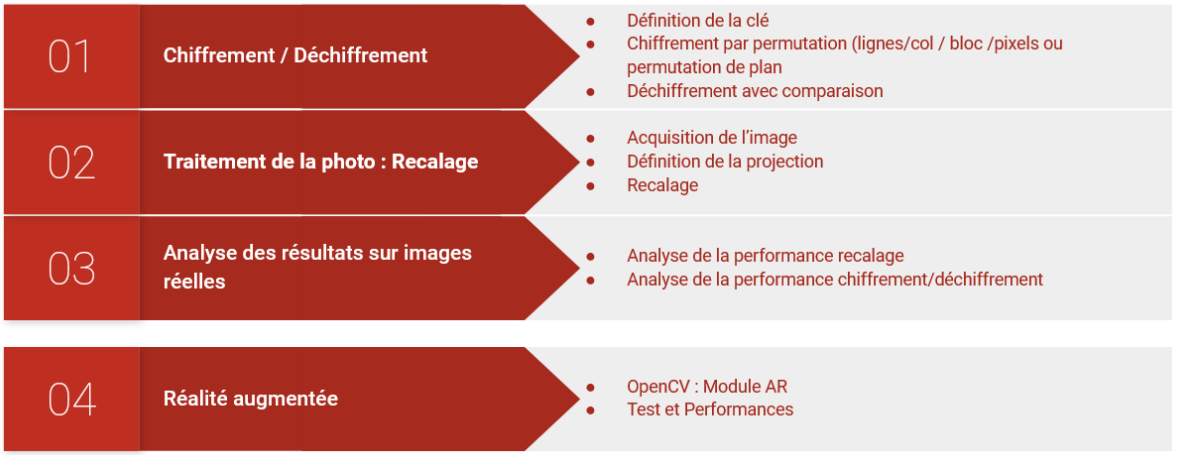
# CR 3 : Musée Sécurisé Virtuel

**Semaine 8 au 14 novembre 2021**

Contexte

On cherche à chiffrer puis acquérir et déchiffrer des images, correspondant à des œuvres dans un musée.




## Etude sur le chiffrement par permutation

Les méthodes principales sont :

- méthode naïve : permutation sans répétition sur
  - la position des pixels
  - les lignes / colonnes de l'image
  - blocs de pixels
- méthodes basées sur la théorie du chaos:
  - la carte du chat d'Arnold
  - la carte du boulanger
- permutation sur les bits composant les pixels => non
  Utilisation dans le contexte de l'impression impossible

On obtient ainsi 2 niveaux d'études : les méthodes s'appliquant aux pixels, et les méthodes s'appliquant aux plans binaires (changement de la valeur des pixels). On pourra ainsi effectuer une troisième étude sur les méthodes combinant ces 2 premières méthodes.

**On choisit d'implémenter une méthode naïve (permutation de blocs de pixels) et une méthode basée chaos (TBD).**

On effectuera un chiffrement total de l'œuvre (contrairement à un chiffrement sélectif ou partiel).

## Chaîne de chiffrement

Chiffrement symétrique

GNPA : générateur de nombre pseudo aléatoire pour générer un flot de chiffrement de la même taille que le message à chiffrer. Dans le cas de la permutation, on cherche à permuter ici les positions, notre génération S doit donc fournir les futurs indices des pixels sans répétition.


On s'intéresse ici aux papiers [9], [2] et [3] qui proposent respectivement une approche de chiffrement par permutation par blocs de pixels, basée chaos - Cat Map et basée chaos - Baker Map. Ces différentes méthodes définissent nos objectifs d'implémentation pour l'étape 4.

**Timeline**


**Première étapes à réaliser (méthode naïve):**

Pour nous permettre de définir les bases de notre projet, nous réalisons les étapes suivantes avant d'affiner les tâches et la répartition globale (cf. paragraphe suivant).

1. En C++ sans openCV
    a. Implémenter une permutation basique de pixels sur la base de l'Algorithme de Fisher-Yates sur des vectors (lineaire) ✅
2. Avec OpenCV
    a. Installation OpenCV ✅
    b. Implémentation de la permutation par blocs de pixels
    c. Implémentation des outils d'analyse
        i. Histogramme ✅
        ii. PSNR

**Répartition globale des tâches**

Maëva :

- Mise en place de l'environnement de développement
    - Git
    - Installation OpenCV sur session (+ PC)
    - Outils d'analyse : Histogramme, PSNR
- Implémentation basée Chaos
- à deux : AR Reconnaissance Image depuis un PC perso
- Analyse des performances méthode basée chaos
- à deux : Poster + Soutenance (à décomposer par la suite)
- Rédaction rapports impairs

Zoltan :

- Installation OpenCV sur session (+ PC)
- Implémentation méthode naïve : permutation par bloc
- à deux : AR Reconnaissance Image depuis un PC perso
- Analyse des performances méthode naïve
- à deux : Poster + Soutenance (à décomposer par la suite)
- Rédaction rapports pairs

## Bibliographie


1. Pauline Puteaux. Analyse et traitement des images dans le domaine chiffré. Autre [cs.OH]. Université Montpellier, 2020. Français. ⟨NNT : 2020MONTS119⟩. ⟨tel-03117770⟩

2. Chen, Guanrong, Yaobin Mao, and Charles K Chui. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps." Chaos, Solitons and Fractals 21.3 (2004): 749-61. Web.

3. A novel fast image encryption scheme based on 3D chaotic baker maps.

4. K. Usman, H. Juzoji, I. Nakajima, S. Soegidjoko, M. Ramdhani, T. Hori, and S. Igi. Medical image encryption based on pixel arrangement and random permutation for transmission security.2007 => pixel permutation Row Col

5. Patro, K Abhimanyu Kumar, and Bibhudendra Acharya. "Secure Multi–level Permutation Operation Based Multiple Colour Image Encryption." Journal of Information Security and Applications 40 (2018): 111-33. Web. => permutation Only

6. Jolfaei, Alireza, Xin-Wen Wu, and Vallipuram Muthukkumarasamy. "On the Security of Permutation-Only Image Encryption Schemes." IEEE Transactions on Information Forensics and Security 11.2 (2016): 235-46. Web. => permutation Only

7. Anwar, Shamama, and Solleti Meghana. "A Pixel Permutation Based Image Encryption Technique Using Chaotic Map." Multimedia Tools and Applications 78.19 (2019): 27569-7590. Web.

8. Dufaux, F., and T. Ebrahimi. "Scrambling for Privacy Protection in Video Surveillance Systems." IEEE Transactions on Circuits and Systems for Video Technology 18.8 (2008): 1168-174. Web.

9. C. V. Wright, W.-C. Feng, and F. Liu. Thumbnail-preserving encryption for JPEG. In ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec), pages 141–146. ACM, 2015. (Permutation par bloc de pixel)

10. Li, Zhen, Changgen Peng, Weijie Tan, and Liangrong Li. "A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation." Symmetry (Basel) 12.9 (2020): 1497. Web.

11. Diaconu, Adrian-Viorel. "Circular Inter–intra Pixels Bit-level Permutation and Chaos-based Image Encryption." Information Sciences 355-356 (2016): 314-27. Web.

12. Kaur, Manjit, and Vijay Kumar. "A Comprehensive Review on Image Encryption Techniques." Archives of Computational Methods in Engineering 27.1 (2020): 15-43. Web.