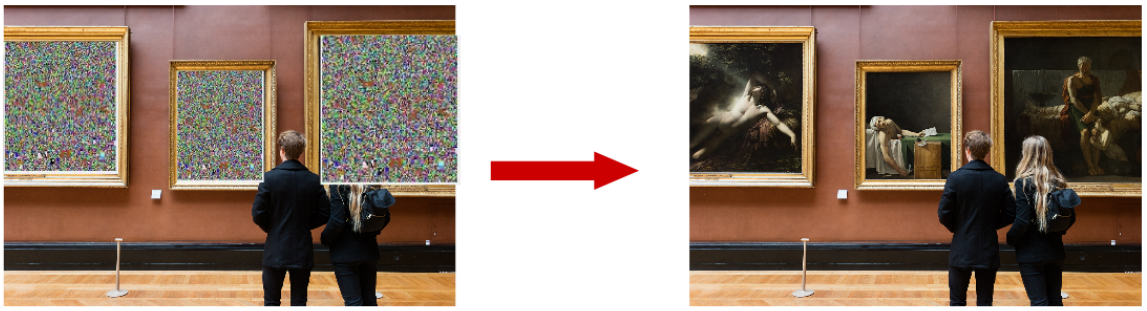
Compte Rendu Semaine 1

Sujet: Musée Sécurisé Virtuel
Binôme: Zoltan Barbusse & Maëva Dalila

Contexte

L'objectif est de développer un système permettant, à partir d'une peinture chiffrée par permutation de pouvoir visualiser la peinture en clair si l'on possède la clé secrète.



Étapes identifiées

01	**Chiffrement / Déchiffrement**	• Définition de la clé • Chiffrement par permutation (lignes/col / bloc /pixels ou permutation de plan • Déchiffrement avec comparaison
02	**Traitement de la photo : Recalage**	• Acquisition de l'image • Définition de la projection • Recalage
03	**Analyse des résultats sur images réelles**	• Analyse de la performance recalage • Analyse de la performance chiffrement/déchiffrement
04	**Réalité augmentée**	• OpenCV : Module AR • Test et Performances

On identifie les étapes principales nécessaires à la réalisation du projet. L'étape 1 nécessitera d'effectuer une recherche sur l'état de l'art sur le chiffrement par permutation. L'étape 2 sera une application des cours de vision par ordinateur et enfin l'étape 3 sera une étape d'analyse des performances qui sera effectuée pour chaque implémentation d'algorithmes.

L'étape 4 est une étape optionnelle qui sera réalisée sous réserve d'avoir assez de temps.

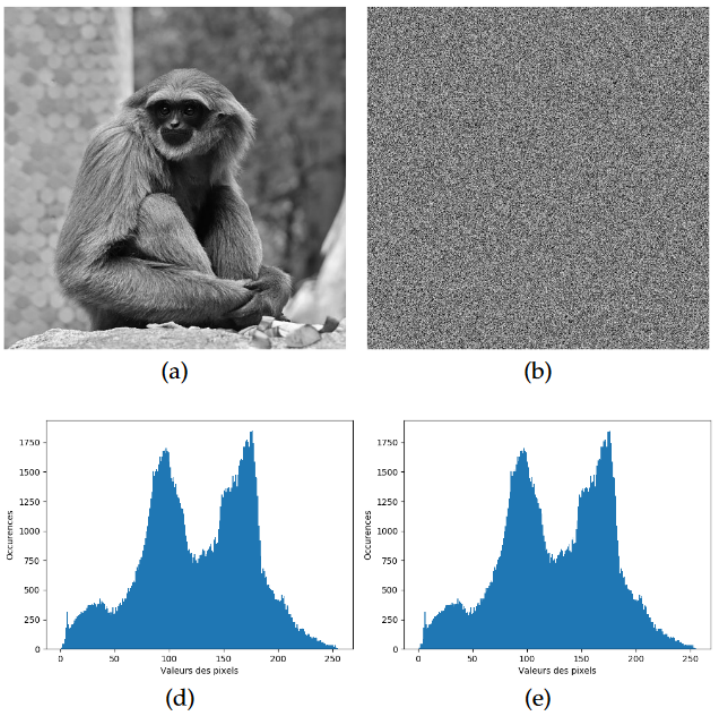
Choix Techniques

On fait le choix de travailler en C++ avec la librairie OpenCV qui bénéficie d'une large documentation en ligne et d'un module AR si l'on souhaite porter le projet sur smartphone.

Etat de l'art

Principe du chiffrement par permutation :
À l'aide d'une clé secrète on initialise un générateur de nombres pseudo-aléatoires qui définit les permutations des pixels dans l'image. On définit cette permutation comme sans répétition: aucune position de pixel ne reste inchangée. Ce chiffrement conserve certaines propriétés de l'image comme la distribution, mais est visuellement efficace (on ne reconnaît pas l'objet chiffré par permutation). Il est également possible d'appliquer une permutation sur les lignes ou sur les colonnes.

Exemple de chiffrement par permutation sur une image en niveaux de gris (extrait de [1])



Il existe aussi des méthodes basées sur la théorie du chaos, les permutations sont alors déterminées en appliquant la carte du chat d'Arnold ou encore la carte du boulanger.

Les permutations peuvent être appliquées aux pixels, mais aussi directement aux bits les composant, changeant ainsi les valeurs des pixels.

Lien vers le dossier contenant les articles de recherche : Lien Drive

Chiffrement (par permutation)

Point d'entrée : les travaux de recherche de Pauline Puteaux (Enseignante M2-IMAGINE Codage et Compression)

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
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.
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.
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.