CR_1

Mise en place du projet

Dépôt Git du projet :
https://github.com/NeonVhenan/Projet_Image_IMAGINE

Sujet choisi : Musée sécurisé virtuel

Nom du projet : Crypto Musée

Langage de programmation envisagé : C# (car transition pour une application AR sous Unity potentiellement plus simple)

Idée de projet : Utiliser une méthode pseudo-aléatoire mélangeant permutation et substitution XOR en se basant sur des cartes chaotiques.

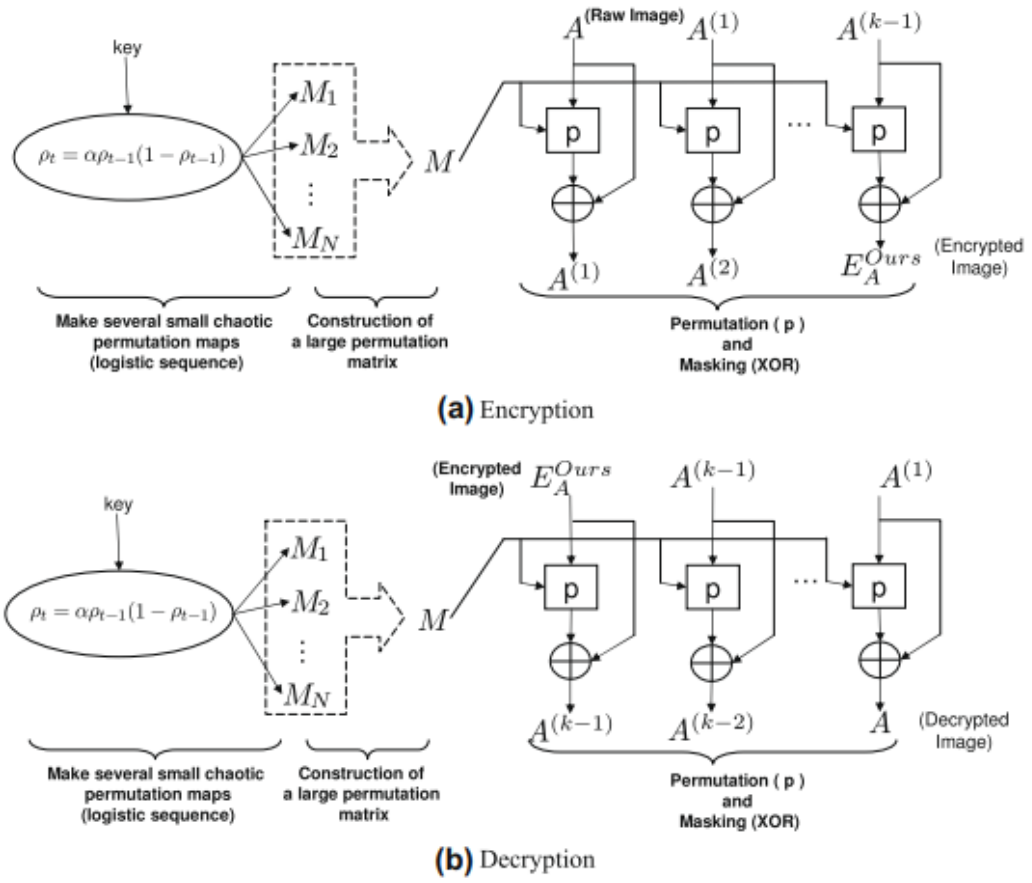
Travail de recherche à effectuer : 2 parties distinctes :

- partie chiffrement : chiffrement et déchiffrement des peintures avec étude documentaire
- partie recadrage : récupération de la peinture chiffrée dans les bonnes proportions à partir d'une photo

Le but est de suivre l'algorithme proposé dans le papier suivant :

An image encryption scheme with a pseudorandom permutation based on chaotic maps par Ji Won Yoon, Hyoungshick Kim (2010)

Les schémas suivants décrivent les méthodes de cryptage et de décryptage des données :



Le cryptage suivra les étapes suivantes :

1. On génère la clef en tant que condition initiale de la carte logistique mais aussi en tant que condition déterminante de la taille des petites matrices de permutation
2. On génère les petites matrices en calculant les valeurs de chaque éléments dans les matrices à l'aide de la carte logistique créée précédemment
3. La construction de la matrice de permutation, qui est une matrice de grande taille, se fait à partir des petites matrices
4. La permutation s'effectue en à l'aide de la matrice de permutation
5. On applique un masque sur l'image permutée à l'aide de la matrice de permutation

La première étape que nous envisageons de réaliser est la phase 1, soit de générer la clef et les petites matrices.

La génération des petites matrices s'effectue à l'aide de la formule suivante :

$$\rho_t = \alpha\rho_{t-1}(1 - \rho_{t-1}),$$
$$M_i(t) \Longleftrightarrow M_i(mod(\rho_t \times 10^3, m_i)),$$

avec Mi $(size\ mi\ x\ mi)$ allant de $\{1,\ldots mi\}$

Les valeurs des matrices sont générées aléatoirement à l'aide de la carte logistique.

La comparaison du résultat final se fera avec la méthode de Baker et la méthode logistique.