

CRYPTO-MUSÉE



MÉRÉDITH CERESOLE - PAULINE CESPEDES
UNIVERSITÉ DE MONTPELLIER - MASTER IMAGINE

clef : N = 32

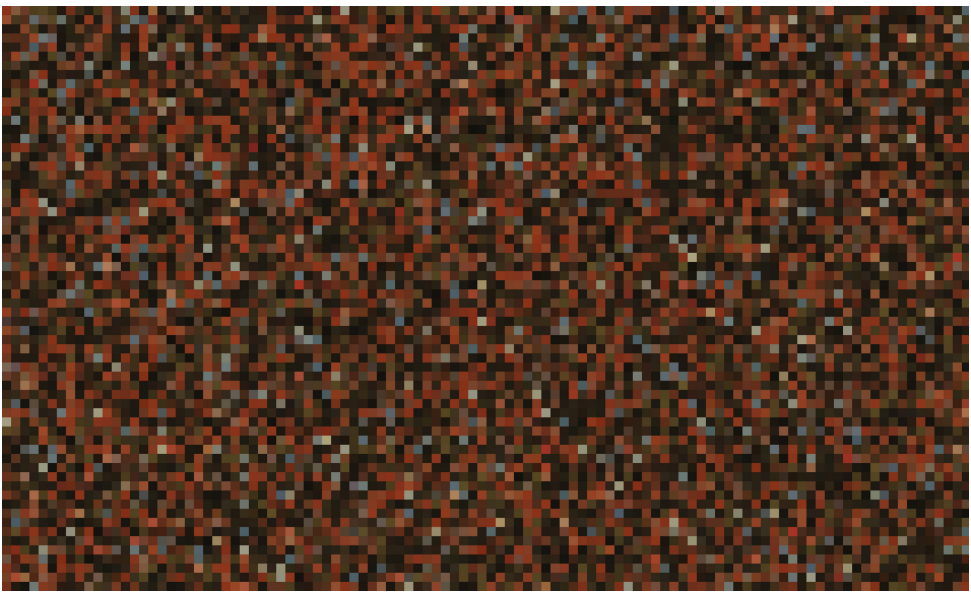


Image chiffrée selon la suite de Chebyshev

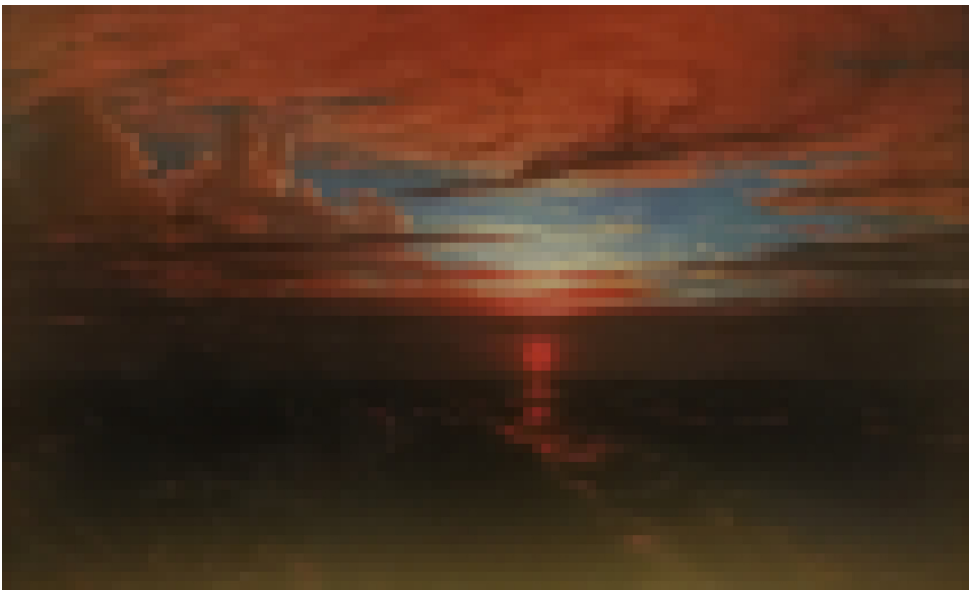


Image déchiffrée légèrement pixelisée

Définition de la taille des blocs

&

Choix de la clé (k et X0)

CHIFFREMENT et DECHIFFREMENT

Photo du tableau à chiffrer ou déchiffrer



création de blocs de pixels

+

utilisation d'un vecteur de permutation



Image chiffrée ou déchiffrée

Tri effectué selon la suite de Chebyshev sur chaque composante puis permutation des blocs de pixels selon l'ordre donné par le tri (vecteur de permutation)

•

Suite de Chebyshev :

$$X_{n+1} = T_k(X_n) = \cos(k * \cos^{-1}(X_n))$$

$$X_n \in [-1, 1]$$

avec k et X0 la clé de chiffrement

•

utilisation du même vecteur de permutation

•

opération inverse pour déchiffrer l'image en prenant compte la taille des blocs (vecteur de permutation obtenu en passant de la liste triée à la liste non triée)

Application interactive

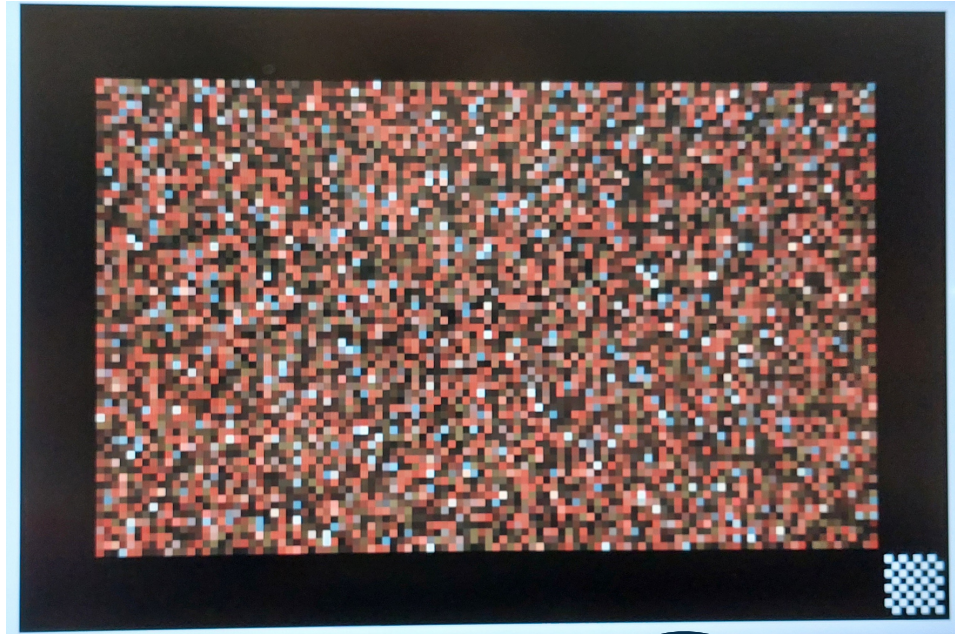
Cadre noir + damier pour la taille des blocs + fond blanc

Détourage de l'image

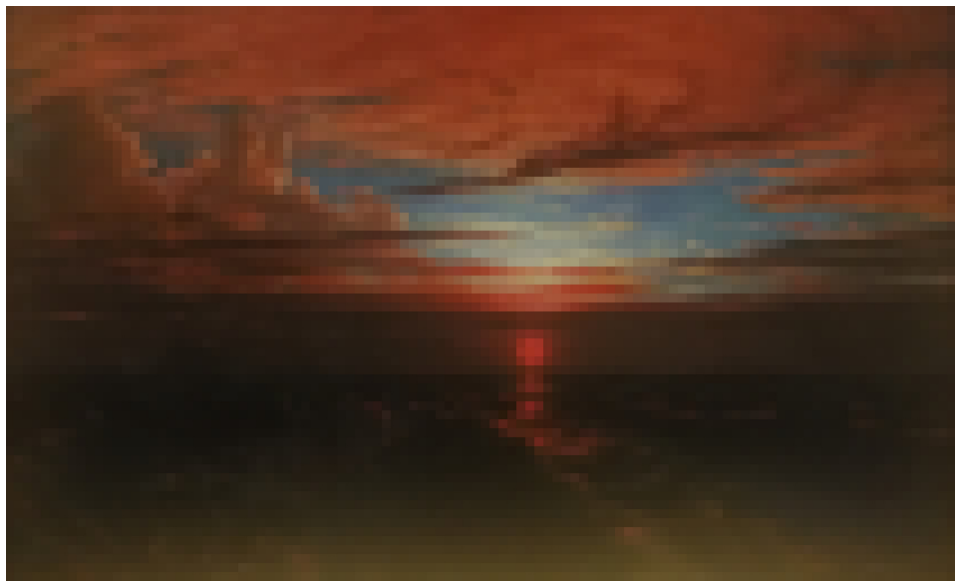
+ Identification de la taille des blocs + Déchiffrement

Pour un résultat optimal, un recadrage est nécessaire. Les couleurs peuvent s'altérer à cause de la photo

Image résultante imparfaite



Recadrage et déchiffrement



Bibliographie :

A novel chaos-based bit-level permutation scheme for digital image encryption par Chong Fu, Bin-bin Lin, Yu-sheng Miao, Xiao Liu, Jun-jie Chen