Analyse et traitement des images dans le domaine chiffré

Pauline Puteaux

Réunion d'équipe

Le 12 janvier 2018

Thèse dirigée par William Puech – LIRMM, ICAR Image et Interaction

Mon parcours

Généralités

Pauline PUTEAUX, 23 ans
Étudiante en Informatique, spécialisée en sécurité
Doctorante (sous contrat doctoral UM), monitrice à la FdS (mission d'enseignement)
pauline.puteaux@lirmm.fr

Projets de recherche

- Contrat CNRS d'un mois, au LIRMM – équipe ICAR (2017)
  - "Recompression d'images JPEG crypto-compressées"
  - Encadré par William Puech
- Stage de recherche de 6 mois, au LIRMM – équipe ICAR (M2, 2017)
  - "Analyse de la signification d'un critère statistique en fonction de la taille d'un bloc de pixels dans une image pour la sécurité et l'authentification des images"
  - Encadré par William Puech
- Stage de recherche de 15 semaines, au LIRMM – équipe ICAR (M1, 2016)
  - "Insertion de données cachées réversible dans le domaine chiffré"
  - Encadré par William Puech

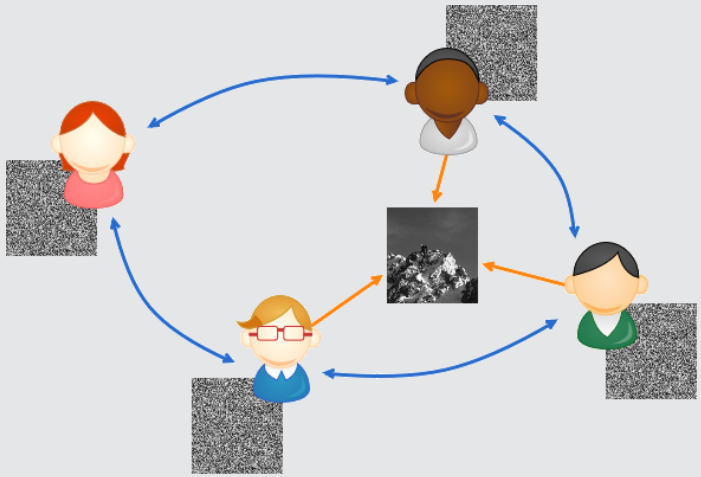
Sujet et problématique de la thèse

Traitement des images dans le domaine chiffré

- Problème de la sécurité des données multimédia
- Transfert ou archivage de ces données sous forme chiffrée
- Nécessité de les analyser et de les traiter sans la clef

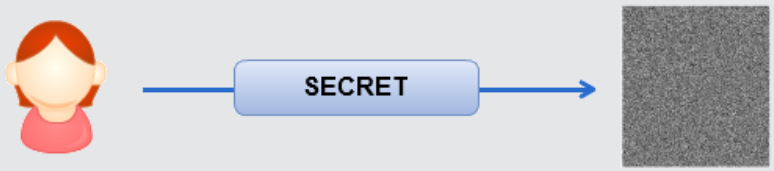
Applications visées

Partage d'images secrètes entre plusieurs personnes (VSS)

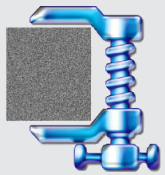


Indexation et recherche d'images dans des BDD chiffrées

Insertion de données cachées dans des images chiffrées



Recompression d'images crypto-compressées



Etat de l'art (1)

Visual Secret Sharing (VSS)

M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, pp. 1–12, 1994.

Indexation et recherche d'images dans des BDD chiffrées

C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," *IEEE Transactions on Image Processing*, vol. 21, no. 11, pp. 4593–4607, 2012.

W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, pp. 725 418–725 418, 2009.

Etat de l'art (2)

Insertion de données cachées dans des images chiffrées (RDHEI)

X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," in *Electronic Imaging 2008*. International Society for Optics and Photonics, pp. 68 191E–68 191E, 2008.

J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

Recompression d'images crypto-compressées

V. Itier and W. Puech, "How to recompress a JPEG crypto-compressed image ?," in *Electronic Imaging 2017*. Society for Imaging Science and Technology, 2017.

P. Korshunov and T. Ebrahimi, "Scrambling-based tool for secure protection of JPEG images," in *Image Processing (ICIP), 2014 IEEE International Conference on*. IEEE, pp. 3423–3425, 2014.

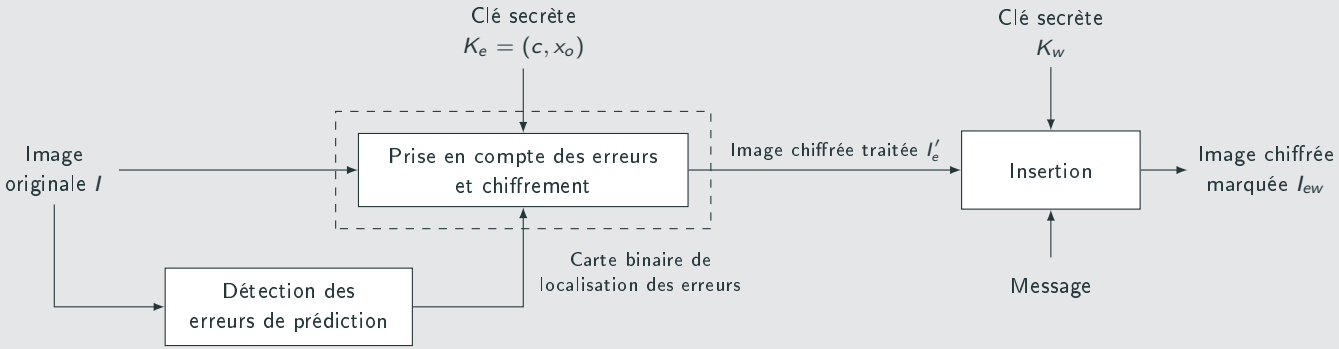
W. Puech and J. M. Rodrigues, "Crypto-compression of medical images by selective encryption of DCT," in *Signal Processing Conference, 2005 13th European*. IEEE, pp. 1–4, 2005.

Insertion haute capacité dans le domaine chiffré (1)

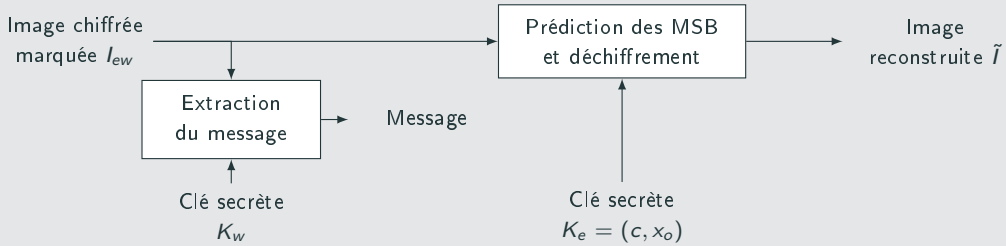
Prédiction des MSB

- Insertion effectuée en substituant les MSB des pixels
- Valeurs initiales prédites lors de la phase de reconstruction

Méthode générale de chiffrement / insertion du message



Méthode générale de déchiffrement / extraction du message



Insertion haute capacité dans le domaine chiffré (2)

Approche CPE-HCRDH

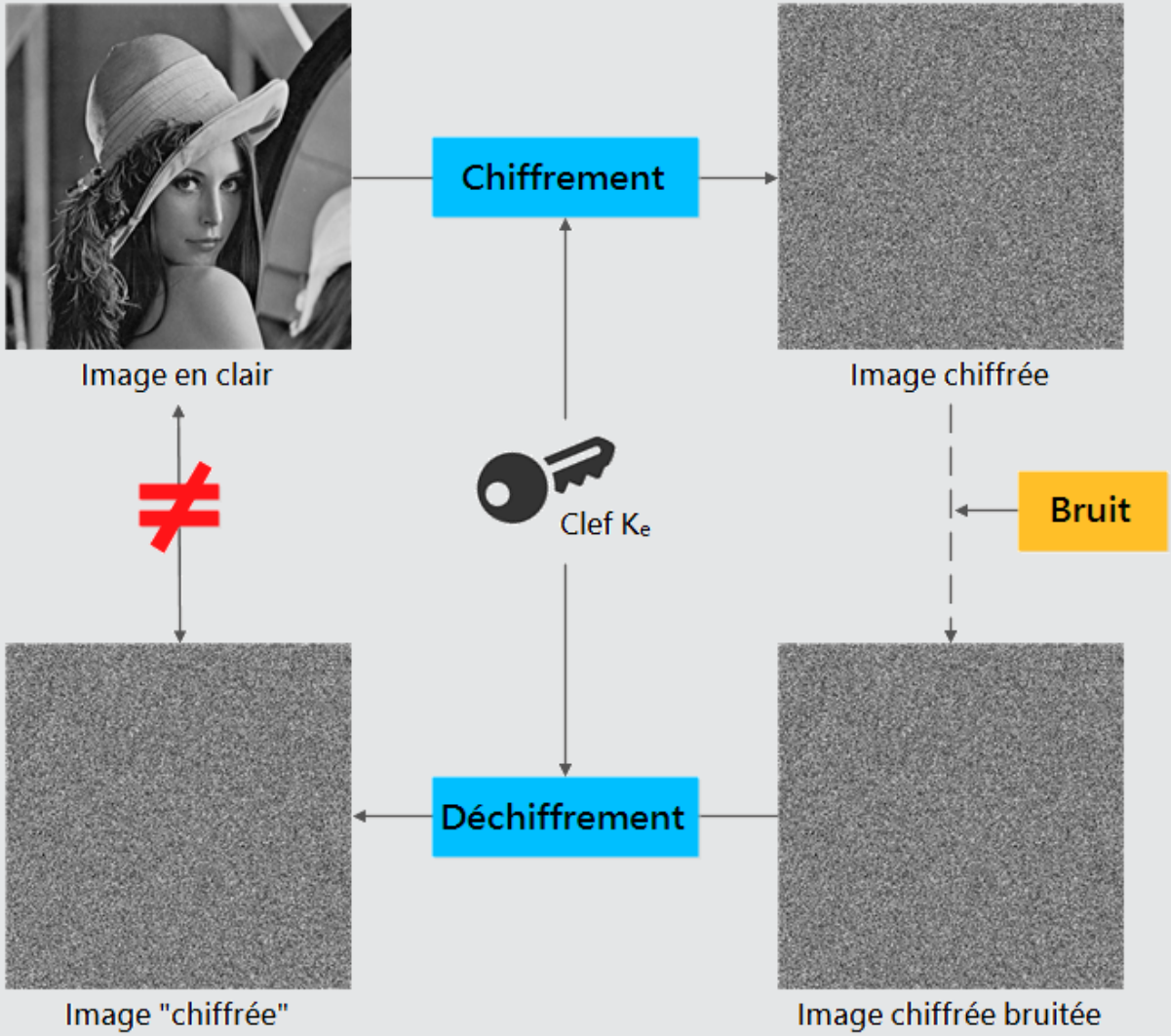
- Correction des erreurs de prédiction
- Insertion très haute capacité (payload $= 1$ *bpp*)
- Bonne qualité de l'image reconstruite (PSNR $\sim 57,4$ *dB*)

Approche EPE-HCRDH

- Signalement des erreurs de prédiction
- Image parfaitement reconstruite (PSNR $\to +\infty$)
- Haute capacité de dissimulation (payload $\sim 0,9681$ *bpp*)

Correction d'images chiffrées par mesure entropique (1)

Pourquoi corriger une image chiffrée ?



Correction d'images chiffrées par mesure entropique (2)

Entropie d'une image en clair vs entropie d'une image chiffrée

$$\begin{aligned} \log_2\left(\sqrt{2\pi e(l-1)q(1-q)}\right) + O\left(\frac{1}{l-1}\right) &< \log_2(l), \\ H_c &< H_e. \end{aligned}$$

L'entropie comme critère de décision

- Entropie au sein d'un bloc :

$$H_{(k,l)}(B) \leq \log_2(\min(k,l))\ bpp.$$

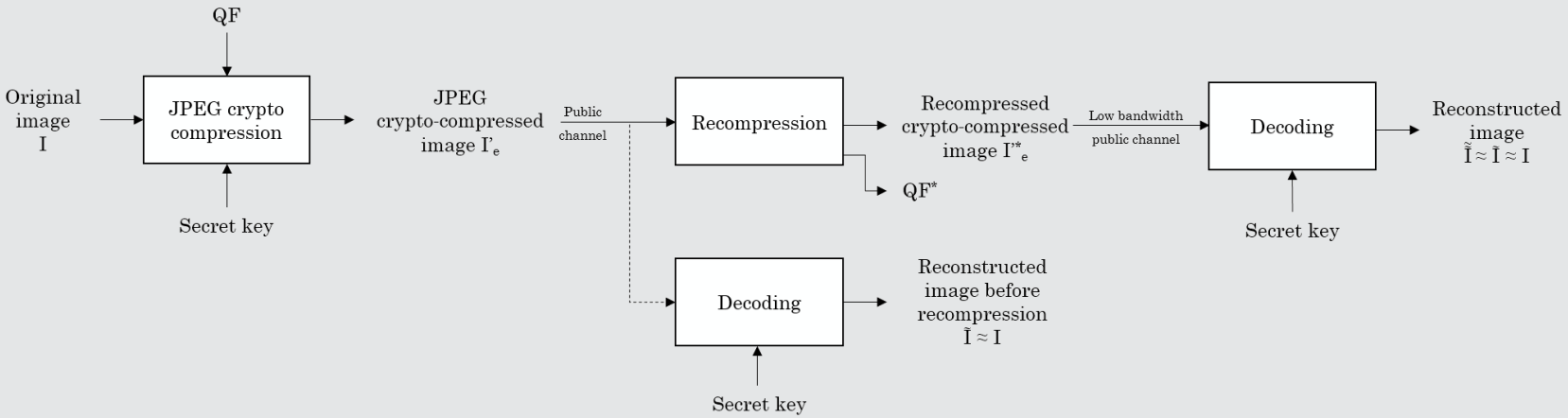
- Déterminer si un bloc de pixels est en clair ou est chiffré.
  - Entropie d'ordre 0
  - Entropie de la carte des distances (corrélation entre les pixels)
  - Entropie jointe
- Analyse de la signification de l'entropie comme critère de décision en fonction de la taille d'un bloc de pixels dans une image.
  - Blocs les plus petits possible
  - Nécessité de quantifier l'histogramme de l'image pour le calcul

Recompression d'images crypto-compressées (1)

Contexte

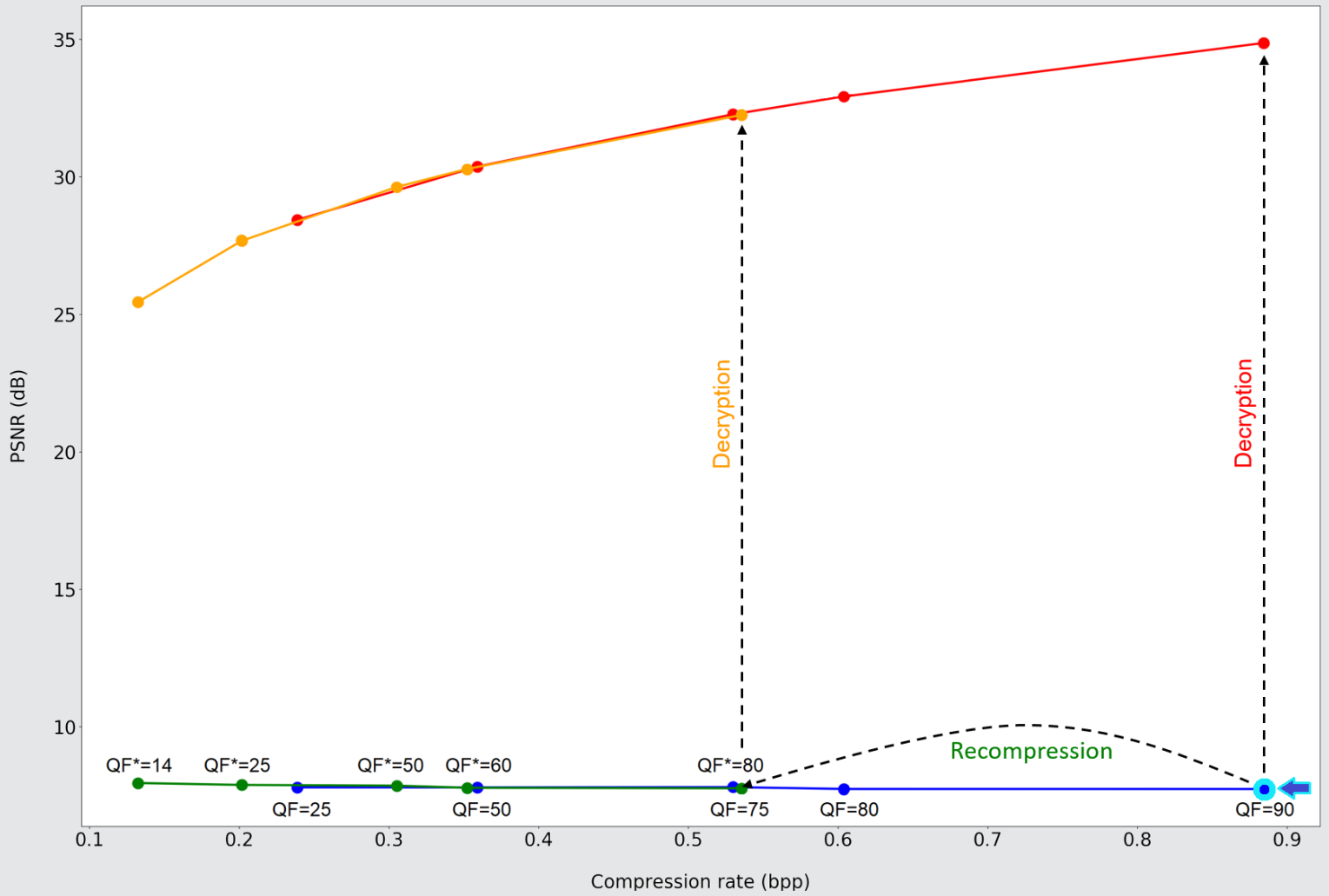
- Transfert/stockage d'images
- Protection des données visuelles
- Taille voulue la plus petite possible (coût transfert/stockage)
- Traitement dans le domaine chiffré

Méthode générale



Recompression d'images crypto-compressées (2)

Taux de recompression vs qualité de l'image reconstruite



Publications et communication (1)

Conférence nationale

P. Puteaux et W. Puech, "Analyse de la taille minimale d'un bloc de pixels afin d'obtenir une valeur significative de l'entropie : application à la correction d'images chiffrées," *CORESA 2017*, 2017.

Conférences internationales

P. Puteaux and W. Puech, "Local Shannon entropy-based image features for statistical and security analysis," in *Acoustics, Speech and Signal Processing (ICASSP), 2018 IEEE International Conference on*, 2018 (submitted).

P. Puteaux and W. Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," in *IEEE Image Processing Theory Tools and Applications (IPTA), 2017 7th International Conference on*. p : 1-6, 2017.

P. Puteaux and W. Puech, "High-capacity reversible data hiding in encrypted images using MSB prediction," in *Electronic Imaging 2017*. Society for Imaging Science and Technology, 2017.

P. Puteaux, D. Trinel and W. Puech, "High-capacity data hiding in encrypted images using MSB prediction," in *IEEE Image Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on*. p : 1-6, 2016.

Publications et communication (2)

Revues internationales

P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," in *IEEE Transactions on Information Forensics and Security*, 2018.

Présentation au GDR ISIS

Journée *Entropies, divergences et mesures informationnelles classiques et généralisées*

P. Puteaux and W. Puech, "Correction d'images chiffrées par mesure entropique," 24 mai 2017, Paris.

En cours...

V. Itier, P. Puteaux and W. Puech, "Recompression without key of JPEG crypto-compressed images," in *IEEE Transactions on Circuits and Systems for Video Technology*.

P. Puteaux and W. Puech, "Embedding more than 1 *bpp* in a context of MSB-based reversible data hiding in encrypted images," in *IEEE Image Processing (ICIP). 2018 25th International Conference on*, 2018.

Nouvelles pistes de recherche (1)

Poursuivre les travaux effectués lors des précédents projets

- Insertion haute capacité dans le domaine chiffré
  - Augmenter la capacité d'insertion
  - Améliorer la qualité de l'image reconstruite
- Correction des images chiffrées bruitées
  - Réduire la taille des blocs pour diminuer la complexité de calcul
  - Exploiter la similarité entre les blocs d'une même image (calcul de divergences K-L)
- Recompression d'images crypto-compressées
  - Effectuer une étude de la robustesse de notre méthode de recompression à d'autres approches de crypto-compression
  - Améliorer l'estimation du facteur de qualité

Nouvelles pistes de recherche (2)

Chiffrement homomorphe

- Un algorithme de chiffrement $\mathcal{E}()$ est dit homomorphe si en connaissant $\mathcal{E}(m_x)$ et $\mathcal{E}(m_y)$, il est possible d'obtenir $\mathcal{E}(m_x \oplus m_y)$ sans déchiffrer $\mathcal{E}(m_x)$ et $\mathcal{E}(m_y)$. On a :

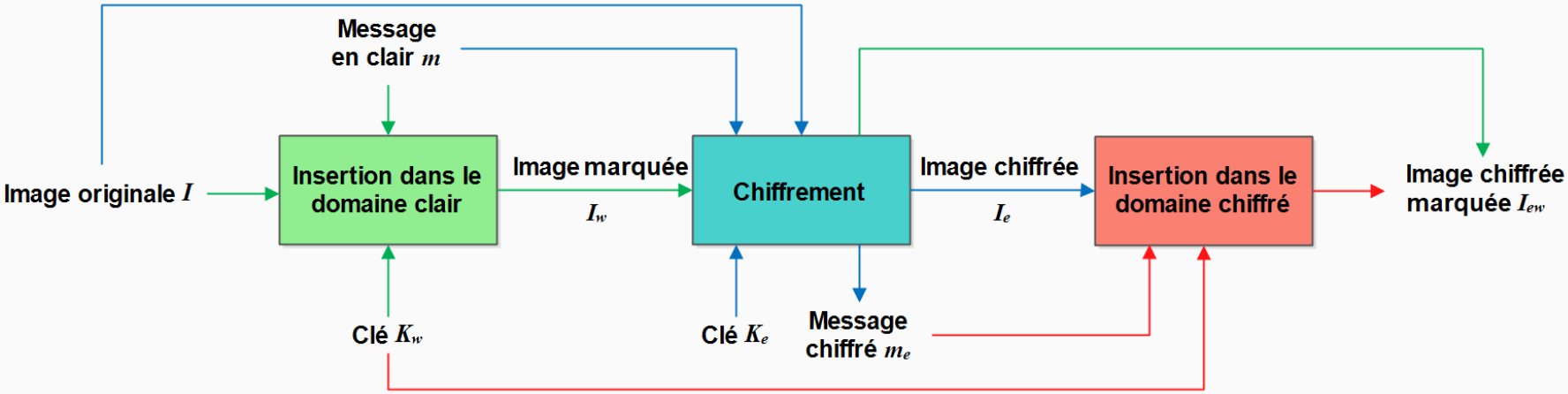
$$\mathcal{E}(m_x \oplus m_y) = \mathcal{E}(m_x) \otimes \mathcal{E}(m_y)$$

- Idées à développer
  - Chiffrement homomorphe à l'insertion de données cachées ou à l'extraction de features
  - Protocole avec des algorithmes existants (Paillier)
  - Définir de nouveaux algorithmes de chiffrement

Nouvelles pistes de recherche (3)

Chiffrement homomorphe à l'insertion de données cachées

$$\mathcal{E}(I \oplus m) = \mathcal{E}(I) \otimes \mathcal{E}(m)$$



Merci pour votre attention !