IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

TRAITEMENT SÉCURISÉ DE L'INFORMATION

Protection des données

Projet: Tatouage d'images chiffrées homomorphiquement

Reda Bellafqira
LaTIM INSERM UMR 1101
Département Data Science

2024

Introduction

Ce projet vise à implémenter la méthode de tatouage sécurisée proposée dans [1]. Cette méthode permet l'insertion d'une marque à la fois dans le domaine en clair et chiffrée homomorphiquement. L'algorithme de tatouage utilisé est la QIM (Quantization Index Modulation) [2], décrit par l'équation suivante :

$$QIM_{\Delta,b}(m) = \begin{cases} \left\lfloor \frac{m}{\Delta} \right\rfloor \Delta & \text{si } \left\lfloor \frac{m}{\Delta} \right\rfloor \mod 2 = b \\ \left\lfloor \frac{m}{\Delta} \right\rfloor \Delta + \Delta & \text{sinon.} \end{cases} \tag{1}$$

où $\lfloor \cdot \rfloor$ désigne la partie entière, Δ est le pas de quantification, b est le bit de la marque, et m est le message à tatouer. Pour récupérer le bit $b^{\{ext\}}$ inséré dans un message tatoué $m^{\{wat\}}$ par une QIM paramétrée par Δ, on procède comme suit :

$$b^{\{ext\}} = \left\lfloor \frac{m^{\{wat\}}}{\Delta} \right\rfloor \mod 2 \tag{2}$$

Comme illustré dans la figure 1, pour tatouer une image I de taille $h \times w$ avec une marque $b^{\{message\}}$ de taille s, nous suivons les étapes suivantes :

Insertion de la marque : Pré-traitement

— L'image est aplatie (ou *reshaped*) sous forme de vecteur I_v de taille $h \times w$.

— Le vecteur est découpé en blocs de taille s, $I_v = \{I_v[i] \mid i \in \frac{h \times w}{s}\}$.

— Une pré-marque $b^{\{premarque\}}$ de taille s est insérée dans chaque bloc de I_v en utilisant la modulation QIM (voir l'équation (1)) avec un $\Delta = 1$. Le rôle de $b^{\{premarque\}}$ est de faciliter l'insertion et l'extraction de la marque $b^{\{message\}}$.

— Le vecteur pré-marqué $I_v^{\{pr\}}$, après l'insertion de la pré-marque dans tous les blocs, est chiffré en utilisant le cryptosystème de Paillier [3], composante par composante avec un aléa différent, pour obtenir $I_v^{\{pr,enc\}}$.

Insertion dans le domaine en clair $(ins1)$

— La marque $b^{\{message\}}$ est insérée dans chaque bloc de $I_v^{\{pr,enc\}}$, à la fois dans le domaine en clair et chiffré, en commençant par le domaine en clair. Cette insertion consiste

à ajouter $b^{\{message\}}$ à $I_v^{\{pr\}}$ à partir de sa version chiffrée homomorphiquement $I_v^{\{pr,enc\}}$. Plus précisément, pour le $j^{\text{ème}}$ composant du $i^{\text{ème}}$ bloc pré-marqué chiffré $I_v^{\{pr,enc\}}[i][j]$, l'insertion du $j^{\text{ème}}$ bit de $b^{\{message\}}$ dans $I_v^{\{pr\}}[i][j]$ est donnée par :

$$I_v^{\{pr,enc,ins1\}}[i][j] = I_v^{\{pr,enc\}}[i][j] \times E[b^{\{message\}}[j], r] \tag{3}$$

$$= E[I_v^{\{pr\}}[i][j] + b^{\{message\}}[j], r' \times r] \tag{4}$$

où $E[\cdot]$ désigne la fonction de chiffrement de Paillier, et r', r sont les aléas correspondants à $I_v^{\{pr,enc\}}[i][j]$, $E[b^{\{message\}}[j], r]$, respectivement.

Insertion dans le domaine chiffré $(ins2)$

L'insertion dans le domaine chiffré tire parti des propriétés sémantiquement sûres du cryptosystème de Paillier, permettant à un message d'avoir plusieurs chiffrés différents en modifiant simplement son aléa. L'algorithme d'insertion est probabiliste et fonctionne comme suit :

Algorithm 1 Insertion dans le domaine chiffré

1: **while** $E[I_v^{\{pr,ins1\}}[i][j], r'] \mod 2 \neq b^{\{message\}}[j]$ **do**
2: $\quad r \leftarrow \text{rand}()$
3: $\quad E[I_v^{\{pr,ins1\}}[i][j], r'] \leftarrow E[I_v^{\{pr,ins1\}}[i][j], r'] \times E[0, r]$
4: **end while**

Notez bien que l'algorithme 1 ne modifie pas les valeurs en clair.

Extraction de la marque

L'extraction de la marque peut se faire également dans le domaine en clair et chiffré.

Extraction dans le domaine chiffré

— L'extraction du $j^{\text{ème}}$ bit dans le domaine chiffré est donnée par l'équation suivante :

$$b^{\{ext\}}[j] = I_v^{\{pr,enc,ins1,ins2\}}[i][j] \mod 2 \text{ for } j \in \{1...s\} \tag{5}$$

— Cette procédure est répétée sur tous les blocs de $I_v^{\{pr,enc,ins1,ins2\}}$ pour extraire le $b^{\{ext\}}$.

— Vérifiez bien que la marque extraite $b^{\{ext\}}$ correspond bien à la marque insérée $b^{\{message\}}$.

Extraction dans le domaine en clair

— En supposant la disponibilité d'un vecteur en clair $I_v^{\{pr,ins1\}}$, l'extraction dans ce domaine nécessite la connaissance de la pré-marque $b^{\{premarque\}}$.

— La première étape consiste à appliquer l'extraction via la QIM pour récupérer un message $b^{\{ext1\}}$ comme suit :

$$b^{\{ext1\}} = \lfloor \frac{I_v^{\{pr,ins1\}}}{\Delta} \rfloor \mod 2 \tag{6}$$

— Finalement, la marque $b^{\{ext\}}$ est calculée en utilisant l'opérateur XOR ($\oplus$) entre $b^{\{ext1\}}$ et $b^{\{premarque\}}$ pour obtenir $b^{\{ext\}}$.

$$b^{\{ext\}} = b^{\{ext1\}} \oplus b^{\{premarque\}} \tag{7}$$

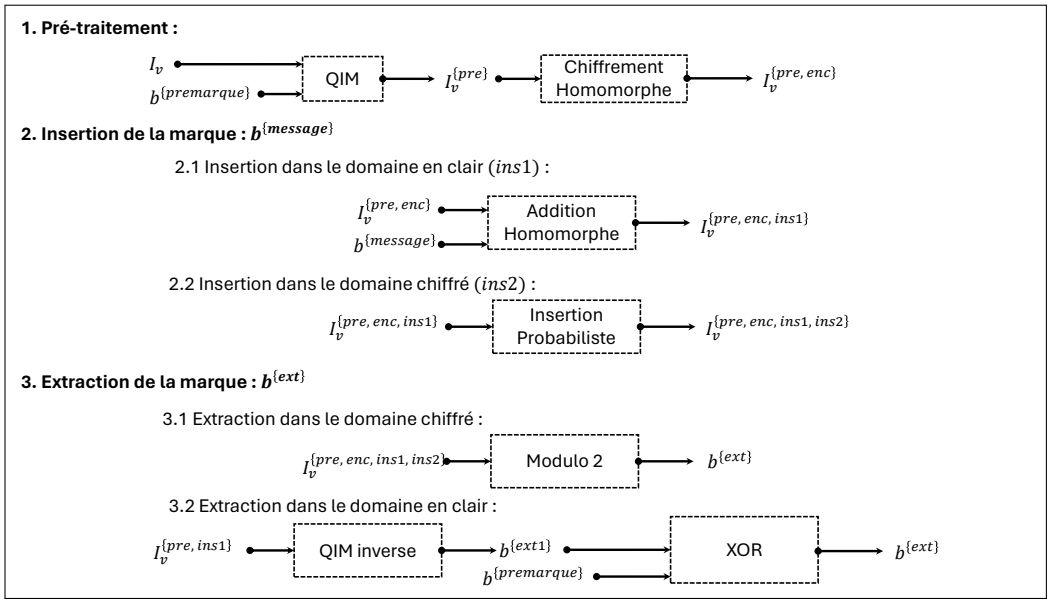

FIGURE 1 – Architecture générale de la modulation du tatouage dans le domaine chiffré homomorphiquement

— Comme pour l'extraction dans le domaine chiffré, cette procédure est répétée pour tous les blocs de $I_v^{\{pr,ins1\}}$ afin d'extraire $b^{\{ext\}}$. Ensuite, vérifiez qu'elle correspond effectivement à la marque insérée, notée $b^{\{message\}}$.

Les livrables de ce projet sont :

— Le(s) code(s) en python/notebook en explicitant une démo de la solution implémentée. Le notebook doit nous permettre de faire fonctionner votre démo sans votre aide.

Références

[1] Dalel Bouslimi, Reda Bellafqira, and Gouenou Coatrieux. Data hiding in homomorphically encrypted medical images for verifying their reliability in both encrypted and spatial domains. In *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 2496–2499. IEEE, 2016.

[2] Brian Chen and Gregory W Wornell. Quantization index modulation : A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information theory*, 47(4) :1423–1443, 2001.

[3] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques*, pages 223–238. Springer, 1999.