Compte-rendu hebdomadaire

Compte-rendu 14

Valentin Noyé

12 janvier 2026 - 16 janvier 2026

GitHub : https://github.com/owilo/SecretSharing

1 Résumé des tâches réalisées cette semaine

1. Finalisation de la rédaction, correction et mise en page de l'article TIFS.
2. Poursuite de la rédaction de l'article ICIP 2026 et de la génération des résultats.
3. Section 2.1 – Formulation du PSNR entre une image secrète et une image reconstruite après bruitage des parts par JPEG.

2 Travail réalisé

2.1 Formulation du PSNR en fonction du QF

Pour rappel, un pixel p est reconstruit en un pixel p' par interpolation de Lagrange selon une valeur de part potentiellement bruitée y'_j :

$$p' = f(0) = \sum_{j=1}^{k} y'_j \, \ell_j(0), \qquad \ell_j(0) = \prod_{\substack{m=1 \\ m \neq j}}^{k} \frac{x_m}{x_m - x_j}, \tag{1}$$

Notons que pour la suite, nous travaillons dans le corps fini $\mathbb{F}_{2^8}$. Supposons que nous sélectionnons les points d'évaluation x_i selon une loi uniforme, ce qui est souvent le cas en pratique lors que les participants souhaitent combiner leurs parts. On en déduit :

$$\begin{aligned} (x_1, \ldots, x_k) \sim U(\mathbb{F}_{2^8})^k &\implies (\ell_1(0), \ldots, \ell_k(0)) \sim U(\mathbb{F}_{2^8})^k \\ &\implies p' \sim U(\mathbb{F}_{2^8}) \end{aligned} \tag{2}$$

La somme de l'erreur et du pixel d'origine p reste en majorité indépendante de p car elle dépend notamment des points d'évaluation x_i. Ainsi, le pixel p' suit une loi uniforme indépendante de p. Cette propriété sur p' est donc nécessaire pour déterminer le PSNR moyen en fonction du QF de JPEG.

On rappelle la formule du MSE entre une image originale dont les pixels sont représentés par p_i et une image reconstruite bruitée dont les pixels sont représentés par p'_i :

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^{N^*} (p_i - p'_i)^2 \tag{3}$$

avec N le nombre de pixels de l'image d'origine et N^* le nombre de pixels bruités par combinaison de parts bruitées (car les pixels inchangés ne contribuent pas au calcul de l'erreur).

Considérons $p_i \sim X$ où X représente la distribution de l'histogramme du dataset d'images, et $p'_i \sim U(\mathbb{F}_{2^8})$ comme déduit dans l'équation (2). Soit μ le MSE moyen pour N^* pixels bruités dans l'image :

$$\begin{aligned}\mu = \frac{1}{N^*}\sum_{i=1}^{N^*}(p_i - p'_i)^2 &= \mathbb{E}\left((X-U)^2\right) \\ &= \mathrm{Var}(X) + \mathrm{Var}(U) + \left(\mathbb{E}\left[X\right] - \mathbb{E}\left[U\right]\right)^2\end{aligned} \tag{4}$$

On en déduit le MSE sur l'image reconstruite :

$$\mathrm{MSE} = \frac{N^*}{N}\mu = \rho\mu \tag{5}$$

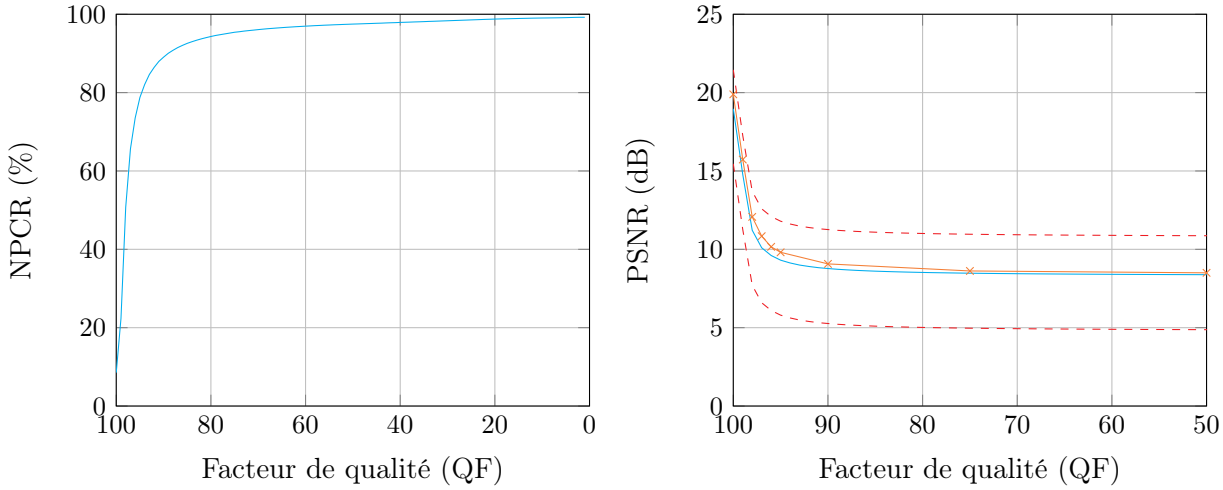
où ρ correspond au nombre de pixels affectés (soit le NPCR), N le nombre de pixels et N^* le nombre de pixels bruités. La formule de l'équation (4) permet d'en déduire une limite inférieure et supérieure de la valeur de μ.

$$\begin{aligned}\mathrm{Var}(U) \leq \mu &\leq \mathrm{Var}(U) + \max(\mathrm{Var}(X)) \\ \frac{256^2-1}{12} \leq \mu &\leq \frac{256^2-1}{12} + 127.5^2 \\ 5461.25 \leq \mu &\leq 21717.50\end{aligned} \tag{6}$$

Ainsi, on détermine μ empiriquement en déduisant X selon les images du dataset BOWS2, en calculant alors $\mu = \mathbb{E}\left((X-U)^2\right) = 9\ 681,27$. Le PSNR résultant pour un NPCR donné (selon un certain QF de JPEG et une seule part bruitée) est alors le suivant :

$$\mathrm{PSNR} = 10\log\left(\frac{255^2}{\rho\mu}\right) \tag{7}$$

En faisant alors varier le QF de JPEG sur notre dataset (avec $\mu = 9\ 681,27$) sur une seule part bruitée selon un partage de secret avec seuil $(3, 255)$, on en déduit tout d'abord le NPCR dans la figure 1a ce qui nous permet d'obtenir la valeur ρ nécessaire au calcul du PSNR de la figure 1b. Dans cette figure 1b, les lignes pointillées en rouge représentent les limites minimales et maximales du PSNR calculées dans l'équation (6). La courbe bleue représente la courbe du PSNR théorique calculée à partir de l'équation (7). La courbe orange représente le PSNR moyen calculé empiriquement sur 100 images avec 100 ensembles de valeurs de x_i différentes selon un partage de secret avec seuil $(3, 255)$. Nous observons une bonne approximation du PSNR selon nos précédents calculs.



(a) NPCR en fonction du QF de JPEG

(b) PSNR en fonction du QF de JPEG

FIGURE 1 – Courbes du NPCR et du PSNR en fonction du QF de JPEG sur des images reconstruites avec 1 part bruitée.

3 Travail à effectuer

1. Continuer la rédaction et la génération des résultats pour l'article ICIP 2026.
2. Concrétiser l'application des codes correcteurs d'erreur de Reed-Solomon sur le partage d'images secrètes [1].

4 Activités

4.1 Réunions

Point avec William et Pauline (Lundi 12/01/2026)
Détails sur la poursuite de l'écriture de l'article ICIP. Finalisation et envoi de l'article TIFS.

4.2 Présentations

Journée des doctorants (Mercredi 14/01/2026)

Références

[1] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Commun. ACM*, 24(9) :583–584, September 1981.