Compte-rendu hebdomadaire

Compte-rendu 4

Valentin Noyé

20 octobre 2025 - 24 octobre 2025

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

1 Résumé des tâches réalisées cette semaine

1. Revue d'un article TCSVT sur le partage d'images secrètes, sur l'authentification des participants, sur l'identification de participants malhonnêtes puis sur la reconstruction du secret.
2. Section 2.1 – Étude concise de quelques observations et expériences menées sur les corps finis.
3. Section 2.2 – Analyse de l'impact du facteur de qualité JPEG sur le NPCR ainsi que sur la répartition des différences entre les pixels de l'image d'origine et de l'image compressée.
4. Section 2.3 – Implémentation de deux nouvelles méthodes de réduction des nuances de pixels vers $GF(251)$ (écriture en clair dans les parts et division des pixels en deux corps finis $GF(107)$ et $GF(149)$), comparaison des métriques et résultats visuels avec les précédentes approches.

2 Travail réalisé

2.1 Observations supplémentaires sur les corps finis

L'arithmétique des corps finis n'est pas toujours intuitive, notamment car celle-ci ne contient pas de relation d'ordre et la plupart des opérations ne sont pas linéaires ou ne peuvent pas être exprimées de la même manière que dans le domaine des réels. Par exemple, l'inverse de $x \bmod p$ dans $GF(p)$ ou de $x \bmod f(x)$ dans $G(p^m)$ où $f(x)$ est un polynôme irréductible, ne possède pas une structure particulière selon la valeur de x, et cette propriété rend difficile l'analyse de l'interpolation de Lagrange, par exemple, dans un corps fini.

En revanche, nous observons dans un premier lieu qu'une mesure de distance est possible. Il s'agit de la distance de Hamming telle qu'utilisée dans les codes correcteurs de Hamming, généralisables dans tout $GF(p)$. D'autres méthodes pour corriger l'erreur, comme les codes de Gabidulin, emploient la distance du rang.

Par ailleurs, nous voulions confirmer l'existence d'un ensemble de x_i optimal, minimisant l'erreur lors de la reconstruction d'un secret. Pour $k = 3$ shares, un triplet de points d'évaluation (indices) $\{x_a, x_b, x_c\}$ paraît générer des résultats optimaux lorsque $x_a \oplus x_b = x_c$. Or, cette observation ne semble pas triviale à démontrer, et encore moins du fait que cela ne se généralise pas pour toute valeur de k.

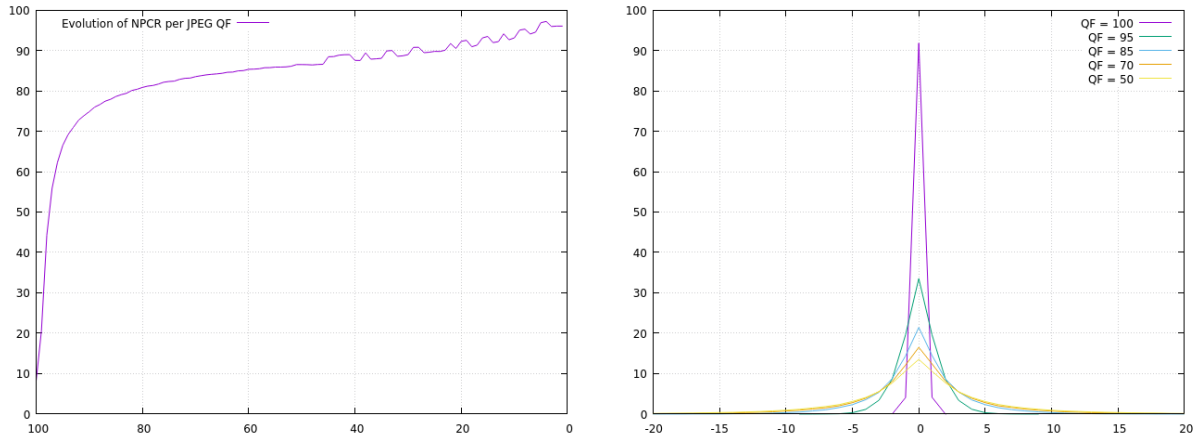
2.2 Analyse du NPCR sur des images compressées avec JPEG

Dans cette section, nous faisons varier le facteur de qualité FQ de la compression JPEG sur les images de la figure 1, puis nous analysons l'évolution du NPCR ainsi que la répartition des différences entre les pixels de l'image d'origine et de l'image compressée.

(a) Baboon (b) Frog (c) Louvre (d) Peppers (e) Stop

FIGURE 1 – Images employées pour l'évaluation du NPCR après compression JPEG.

Dans la figure 2a, le facteur de qualité QF varie entre 100 (qualité maximale) et 1 (qualité minimale). Nous constatons que l'évolution du NPCR ne suit pas une tendance linéaire mais exponentielle notamment pour des QF élevées. Par exemple, un QF de 97 est suffisant pour que 50% des valeurs de pixel aient été modifiées. Pour des QF moyens ou faibles, le NPCR évolue plus lentement. Entre autres, la figure 2b met en évidence la répartition des différences entre l'image originale et l'image compressée avec JPEG pour différentes valeurs de QF. Cette observation correspond à celle relevée dans la figure 2a et démontre une plus grande variance pour des QF plus faibles.



(a) Évolution du NPCR en fonction du QF (b) Répartition des différences en fonction du QF

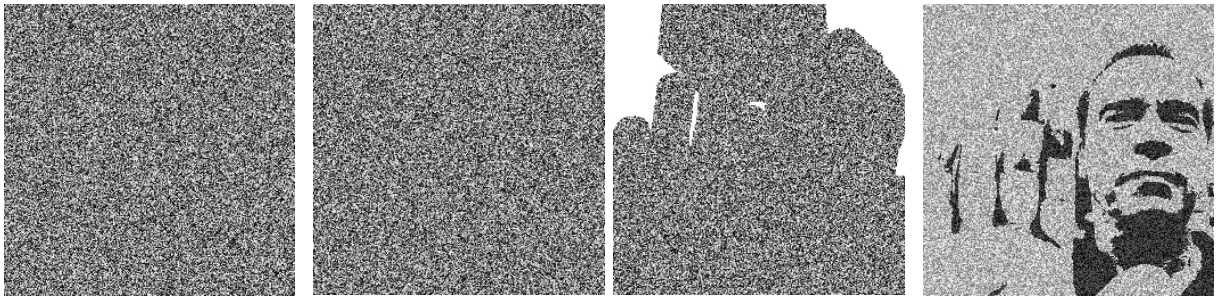
FIGURE 2 – Images employées pour l'évaluation du NPCR après compression JPEG.

2.3 Analyse des méthodes de réduction des valeurs de pixel dans GF(251)

Deux méthodes ont été implementées afin de réduire les valeurs de pixels contenues dans l'intervalle $[0, 255]$ vers $[0, 250]$ enfin d'être exploitables par une approche employant $GF(251)$. Dans ce compte-rendu, deux autres méthodes ont été utilisées afin de voir leur impact et de pouvoir les comparer avec les méthodes existantes. Dans la première, nous encodons les pixels $>$ 250 dans chacune des parts de l'image. Dans la seconde, les pixels sont seuillés et séparés dans deux corps finis $GF(107)$ et $GF(149)$ dans lesquels nous effectuons les opérations classiques de partage de secret. L'image employée est l'image Stop de la figure 1e.

La figure 3 montre la première part obtenue par l'emploi de chacune des méthodes précédemment mentionnées. Nous sommes en mesure de reconnaître certaines formes et structures dans

les parts générées avec ces deux méthodes.



(a) Limite à 250 (b) Étirement d'hist. (c) Écriture en clair (d) Deux corps

FIGURE 3 – Première part obtenue avec chacune des méthodes

Le tableau 1 met en évidence le fait que ces deux dernières méthodes influent sur la sécurité des parts.

Méthode	**PSNR (dB)** $\downarrow$	**NPCR (%)** $\uparrow$	**UACI (%)** $\uparrow$	**Entropie (bits/px)** $\uparrow$
Limite à 250	8.4658	99.6475%	30.8701%	7.96885
Étirement d'hist.	8.47922	99.6765%	30.8646%	7.96868
Écriture en clair	9.79412	88.6307%	25.2342%	7.6845
Deux corps	12.2749	99.2889%	19.7519%	7.84195

TABLE 1 – Métriques de comparaison entre l'image originale et la première part

En revanche, ces deux nouvelles méthodes reconstruisent les images sans perte, comme le montre la figure 4. Or, nous ne voyons pas grandement la différence avec les pré-traitements précédemment employés.

(a) Limite à 250 (b) Étirement d'hist. (c) Écriture en clair (d) Deux corps

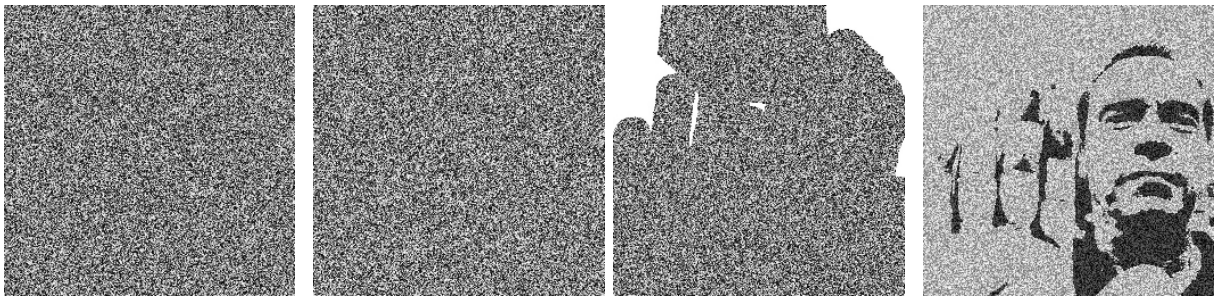
FIGURE 4 – Reconstruction avec chacune des méthodes

Le tableau 2 met cela en valeur de manière quantitative.

Méthode	**PSNR (dB)** $\uparrow$	**NPCR (%)** $\downarrow$	**UACI (%)** $\downarrow$	**Entropie (bits/px)**
Limite à 250	44.0964	11.0428%	0.204803%	7.11753
Étirement d'hist.	66.0466	1.61591%	0.00633689%	7.1859
Écriture en clair	∞	0%	0%	7.21997
Deux corps	∞	0%	0%	7.21997

TABLE 2 – Métriques de comparaison entre l'image originale et sa reconstruction

Enfin, nous essayons de reconstruire le secret avec $k-1$ parts. Nous constatons une vulnérabilité de ces méthodes dans la figure 5.



(a) Limite à 250 (b) Étirement d'hist. (c) Écriture en clair (d) Deux corps

FIGURE 5 – Reconstruction erronée avec chacune des méthodes

En effet, cette reconstruction fait paraître les mêmes propriétés quantitatives que ses parts dans le tableau 3.

Méthode	**PSNR (dB)** ↓	**NPCR (%)** ↑	**UACI (%)** ↑	**Entropie (bits/px)** ↑
Limite à 250	8.49079	99.6414%	30.7627%	7.96885
Étirement d'hist.	8.38498	99.6338%	31.1768%	7.96869
Écriture en clair	9.81532	88.6063%	25.1581%	7.68417
Deux corps	12.253	99.3118%	19.7866%	7.84191

TABLE 3 – Métriques de comparaison entre l'image originale et une reconstruction erronée

3 Travail à effectuer

1. Analyser la capacité à reconstruire les coefficients du polynôme de Shamir selon différentes configurations d'erreur.
2. Explorer les méthodes étudiées dans le survey de Saha *et al.*, et notamment en ce qui concerne le Verifiable SIS (VSIS) [1].
3. Concrétiser l'application des codes correcteurs d'erreur de Reed-Solomon sur le partage d'images secrètes [2].
4. Continuer l'article inachevé de Laura Bertojo sur l'analyse de l'erreur sur la reconstruction de l'image secrète avec des parts bruitées.

4 Activités

4.1 Réunions

Point avec William (Lundi 20/10/2025)

1. Pour gérer les valeurs dans $GF(251)$, encoder en clair les valeurs > 250 ou travailler dans deux groupes de nuances $GF(p)$ et $GF(q)$ où $p + q = 256$.
   ◇ **Fait** (2.3)
2. Maintenir l'usage de $GF(251)$ dans les tests et évaluations des résultats etc.
3. Étudier $GF(257)$ et son application en SIS.
   ◇ **Fait** (son utilisation n'est pas complètement intéressante)
4. Calculer la distribution du NPCR parmi des images reconstruites avec parts bruitées.
   ◇ **Fait** (2.2)
5. Appliquer la méthode du débruitage par filtre médian en prenant en compte la carte de contours (filtre médian orienté) pour réduire l'erreur sur les contours.

6. Comprendre comment l'erreur est calculée dans un groupe fini, notamment en $GF(251)$ ou $GF(2^8)$.
   ◇ **En cours** (2.1, nécessite une étude approfondie)
7. Voir s'il est possible de déterminer les coefficients du polynôme a seulement un delta d'erreur ± 1 sur le secret récupéré (Pour $k = 3$, 27 configurations possibles dont 2 donnant le polynôme $s + ax + bx^2 \pm 1$).
8. Soit k parts pour reconstruire le secret, voir comment utiliser utiliser $k' > k$ parts pour renforcer la correction de l'erreur sachant que certaines parts peuvent être bruitées.

Réunion de suivi (Mercredi 22/10/2025)

Références

[1] Sanchita Saha, Arup Kumar Chattopadhyay, Anup Kumar Barman, Amitava Nag, and Sukumar Nandi. Secret image sharing schemes : A comprehensive survey. *IEEE Access*, 11 :98333–98361, 2023.

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