Compte-rendu hebdomadaire

Compte-rendu 3

Valentin Noyé

13 octobre 2025 - 17 octobre 2025

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

1 Résumé des tâches réalisées cette semaine

1. Section 2.1 – Recherches mathématiques complémentaires.
2. Section 2.2 – Étude de la propagation de l'erreur des parts sur le secret, et analyse de l'impact des choix de certains paramètres (choix des x_i, choix des parts sur un polynôme symétrique ou non symétrique autour d'une part bruitée).
3. Section 2.3 – Implémentation d'une méthode de correction d'erreur sur l'image secrète par l'emploi d'un filtre médian sur la part bruitée selon Bertojo *et al.* [1].

2 Travail réalisé

2.1 Étude sur les matrices de Vandermonde

Soit un polynôme $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ que nous souhaitons évaluer en tout point $x_i \in \{x_0, \ldots, x_k\}$ pour produire $y_i \in \{y_0, \ldots, y_k\} = \{p(x_0), \ldots, p(x_k)\}$. Considérons le vecteur des coefficients $\mathbf{a}$ et le vecteur $\mathbf{y}$ tels que :

$$\mathbf{a} = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix}$$

La matrice de Vandermonde est définie pout tout x_i :

$$V = \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \cdots & x_k^n \end{pmatrix}$$

Ainsi, on évalue le polynôme en tout x_i simplement par la multiplication suivante :

$$V\mathbf{a} = \mathbf{y}$$

Comme par interpolation de Lagrange, nous pouvons retrouver les coefficients $\mathbf{a}$ du polynôme à partir des x_i et y_i :

$$\mathbf{a} = V^{-1}\mathbf{y}$$

2.2 Étude de la répartition et du choix des parts sur l'erreur

2.2.1 Formulation

Soit un polynôme de Shamir d'ordre $k-1$ tels que les points (x_i, y_i) permettent de le reconstruire. À la réception, on obtient un message erroné/bruité avec une erreur (nulle ou non) e_i sur chaque point : $(x_i, y_i + e_i)$ où i représente l'indice de la i-ème part.

Il est possible d'en déduire l'erreur par interpolation de Lagrange, ce qui nous ramène à une erreur totale sur le secret récupéré :

$$e_s = \sum_{i=1}^{k} e_i \ell_i(0)$$

où $\ell_i(0)$ représente le polynôme de base de Lagrange évalué en 0. Celui-ci est défini comme ceci :

$$\ell_i(0) = \prod_{i \neq j} \frac{-x_i}{x_j - x_i}$$

On porte ici à notre attention le choix des points d'évaluation du polynôme. Selon ceux qui sont sélectionnés, il est possible d'atténuer l'erreur en réduisant la valeur de $\ell_i(0)$. Ici, cela se fait en choisissant à la fois des x_i proches de 0 ou éloignés entre eux. Or, ces observations ont été menées dans $\mathbb{R}$, il serait donc nécessaire d'observer leur impact dans un groupe fini.

Pour visualiser cela, des graphes simples ont été construits :

— Trois points fixes ($x_1 = 1$, $x_2 = 2$, $x_3 = 3$) : Lien vers Desmos

— Trois points paramétrables : Lien vers Desmos

2.2.2 Variation des positions d'évaluation

En partant de notre observation dans la section précédente, on fixe $n = k = 3$. À chacune des trois parts est attribué un point d'évaluation $x_i \neq 0$ afin d'en déduire un triplet $\{x_a, x_b, x_c\}$ permettant de minimiser l'erreur de reconstruction après bruitage par JPEG d'une des parts avec un facteur de qualité de 100. Le tableau 1 compare les différentes valeurs de PSNR obtenues entre l'image originale et reconstruite selon le choix du triplet et de la part bruitée. Certaines configurations génèrent de meilleurs résultats, (écart, distance à 0), mais il est compliqué d'en déduire un motif exact notamment car nous travaillons dans $GF(2^8)$.

Position $\{x_a, x_b, x_c\}$ des parts	**PSNR (dB)**			**Résultat**
	x_a bruitée	**x_b bruitée**	**x_c bruitée**	
$\{1, 2, 3\}$	37,8404	37,7696	**38,1076**	Bon
$\{1, 3, 5\}$	17,3956	**18,1893**	17,6045	Mauvais
$\{1, 255, 254\}$	37,4888	**37,9200**	37,0166	Bon
$\{1, 128, 129\}$	35,6655	**37,2565**	37,2217	Bon
$\{1, 2, 128\}$	17,4473	**19,4793**	17,8018	Mauvais
$\{85, 170, 255\}$	36,8729	37,7711	**38,2042**	Bon

TABLE 1 – Comparaison du PSNR selon le choix de la position d'évaluation des parts.

2.2.3 Variation des parts sélectionnées sur un polynôme autour d'une part bruitée

Dans cette section, on observe l'impact d'une image bruitée sur le PSNR de l'image résultante selon la configuration sélectionnée en partant du principe que la part bruitée par JPEG (qualité 100) se situe en position $\lceil \frac{n}{2} \rceil$ et que les indices sélectionnés pour différentes valeurs de k se réflètent autour de cette part. Nous choisissons $n = 11$ et faisons varier k. Ici, $\lceil \frac{n}{2} \rceil = 6$ représente

l'indice de la part bruitée. Un exemple de choix pour $k = 7$ est $\{1, 2, 5, \mathbf{6}, 7, 10, 11\}$, les indices sont à part égale des deux côtés de 6. Dans cette étude, nous évaluons également l'impact d'un polynôme symétrique autour de l'indice de la part bruitée (6).

En premier lieu, le tableau 2 montre l'impact des parts sélectionnées sur le PSNR entre l'image d'origine et l'image reconstruite lorsque le polynôme est quelconque. Même s'il est difficile d'en tirer une conclusion, utiliser des parts plus ou moins consécutives avec la part centrale semble générer de meilleurs résultats avec $k = 3$ et $k = 5$. Or, ce n'est pas le cas avec $k = 7$.

$k = 3$		$k = 5$		$k = 7$	
Parts	PSNR (dB)	Parts	PSNR (dB)	Parts	PSNR (dB)
$\{5, 6, 7\}$	**26,8976**	$\{4, 5, 6, 7, 8\}$	**25,5713**	$\{3, 4, 5, 6, 7, 8, 9\}$	18,7725
$\{4, 6, 8\}$	18,0107	$\{3, 5, 6, 7, 9\}$	19,3392	$\{2, 4, 5, 6, 7, 8, 10\}$	**26,8436**
$\{3, 6, 9\}$	20,4105	$\{2, 5, 6, 7, 10\}$	18,2958	$\{1, 4, 5, 6, 7, 8, 11\}$	18,0132
$\{2, 6, 10\}$	18,3406	$\{1, 5, 6, 7, 11\}$	16,9767	$\{2, 3, 5, 6, 7, 9, 10\}$	17,1793
$\{1, 6, 11\}$	17,9646	$\{3, 4, 6, 8, 9\}$	20,5127	$\{1, 3, 5, 6, 7, 9, 11\}$	17,1946
		$\{2, 4, 6, 8, 10\}$	18,0875	$\{1, 2, 5, 6, 7, 10, 11\}$	17,3086
		$\{1, 4, 6, 8, 11\}$	18,2684	$\{2, 3, 4, 6, 8, 9, 10\}$	17,3535
		$\{2, 3, 6, 9, 10\}$	17,7004	$\{1, 3, 4, 6, 8, 9, 11\}$	19,8637
		$\{1, 3, 6, 9, 11\}$	17,4815	$\{1, 2, 4, 6, 8, 10, 11\}$	19,3408
		$\{1, 2, 6, 10, 11\}$	24,1160	$\{1, 2, 3, 6, 9, 10, 11\}$	21,7802

TABLE 2 – PSNR des reconstructions sur un polynôme non symétrique.

Le tableau 3 montre l'impact des parts sélectionnées sur le PSNR lorsque le polynôme est symétrique autour de 6. Nous constatons ici que nous gardons des tendances et magnitudes relativement similaires quelque soit la forme du polynôme.

$k = 3$		$k = 5$		$k = 7$	
Parts	PSNR (dB)	Parts	PSNR (dB)	Parts	PSNR (dB)
$\{5, 6, 7\}$	**26,9714**	$\{4, 5, 6, 7, 8\}$	**25,6984**	$\{3, 4, 5, 6, 7, 8, 9\}$	18,7823
$\{4, 6, 8\}$	17,9843	$\{3, 5, 6, 7, 9\}$	19,5049	$\{2, 4, 5, 6, 7, 8, 10\}$	**27,5153**
$\{3, 6, 9\}$	20,3524	$\{2, 5, 6, 7, 10\}$	18,4134	$\{1, 4, 5, 6, 7, 8, 11\}$	18,1708
$\{2, 6, 10\}$	18,0939	$\{1, 5, 6, 7, 11\}$	16,9396	$\{2, 3, 5, 6, 7, 9, 10\}$	17,1786
$\{1, 6, 11\}$	17,9898	$\{3, 4, 6, 8, 9\}$	20,4681	$\{1, 3, 5, 6, 7, 9, 11\}$	17,2116
		$\{2, 4, 6, 8, 10\}$	17,9373	$\{1, 2, 5, 6, 7, 10, 11\}$	17,3273
		$\{1, 4, 6, 8, 11\}$	18,0692	$\{2, 3, 4, 6, 8, 9, 10\}$	17,3808
		$\{2, 3, 6, 9, 10\}$	17,5666	$\{1, 3, 4, 6, 8, 9, 11\}$	20,0701
		$\{1, 3, 6, 9, 11\}$	17,4783	$\{1, 2, 4, 6, 8, 10, 11\}$	19,2976
		$\{1, 2, 6, 10, 11\}$	24,1600	$\{1, 2, 3, 6, 9, 10, 11\}$	21,8667

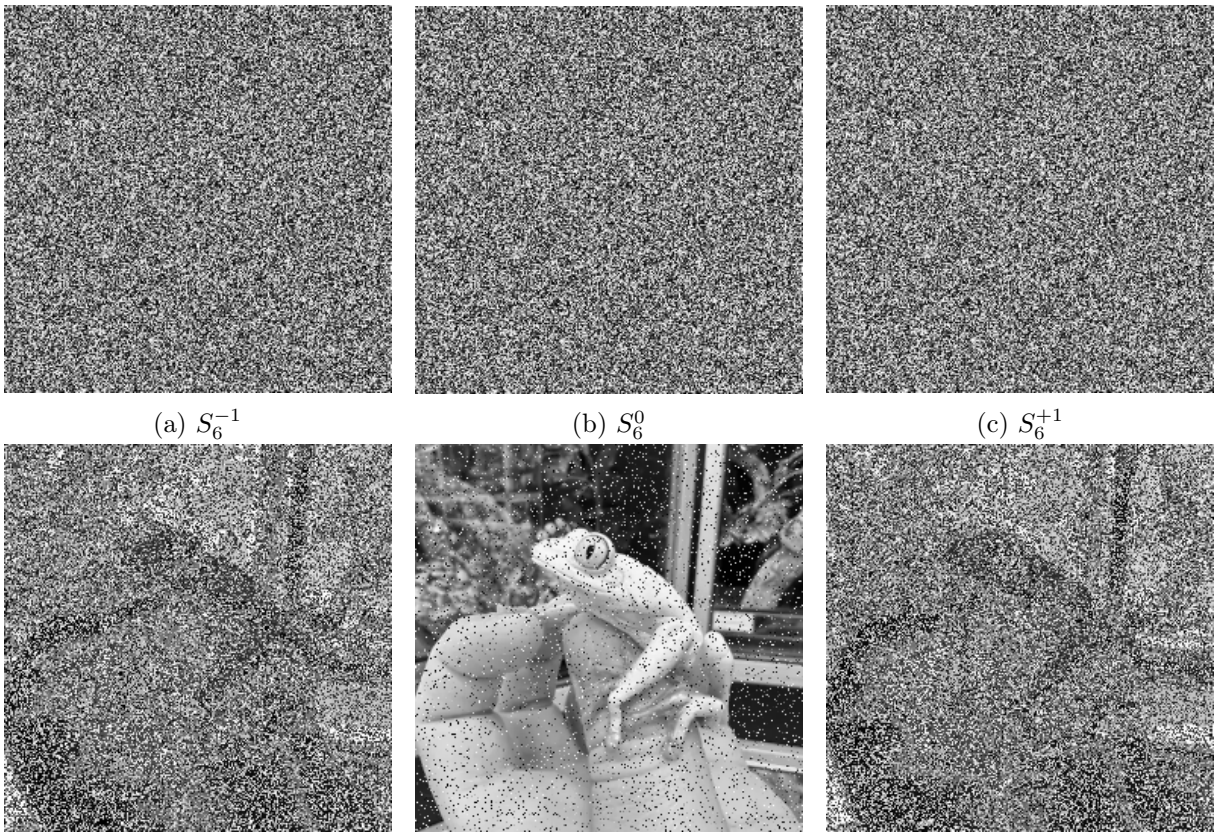
TABLE 3 – PSNR des reconstructions sur un polynôme symétrique.

2.3 Méthode de correction d'erreur par filtrage médian

Dans cette section, une méthode basée sur un filtrage médian tel qu'implémentée par Bertojo *et al.* [1] est appliquée sur notre image afin d'en concevoir son efficacité. Ici, $n = 11$ et $k = 3$. L'image d'entrée est divisée en 11 parts pour lesquelle on sélectionne les parts S_3, S_6 et S_9 où la part S_6 est la part centrale bruitée par JPEG avec un facteur de qualité de 100, donnant ainsi S_6^0. Ainsi, certaines valeurs de S_6^0 ont une erreur de ± 1.

Il existe deux parts S_6^{-1} et S_6^{+1} où à chaque pixel est soutrait 1 et ajouté 1 respectivement, et pour lesquelles les parts bruitées $\{S_6^{-1}, S_6^0, S_6^{+1}\}$ permettent une reconstruction de l'ensemble des

pixels d'origine de l'image d'entrée à partir des deux autres parts S_3 et S_9. La figure 1 permet de constater l'effet de l'ajout de ± 1 sur la reconstruction avec la part bruitée.



(a) S_6^{-1} (b) S_6^0 (c) S_6^{+1}

(d) I^{-1} (e) I^0 (f) I^{+1}

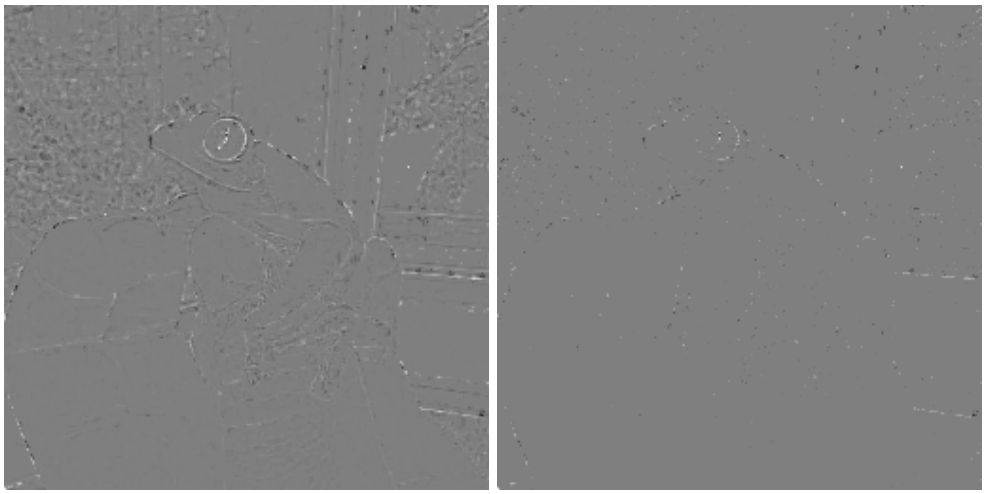
FIGURE 1 – Parts bruitées S_6^v et reconstructions I^v.

Le filtre médian est une méthode classique utilisée afin de débruiter les images. Nous l'appliquons à I^0 pour produire I_F. L'image est alors corrigée en évaluant la différence entre les pixels de I_F ainsi que de S_6^{-1}, S_6^0 et S_6^{+1} puis en prenant la valeur de pixel dont cet écart est le plus faible. Nous produisons alors une nouvelle image corrigée I_C, comme présentée dans la figure 2.

(a) Image originale (b) Filtre médian I_F (c) Image corrigée I_C

FIGURE 2 – Résultats du débruitage de l'image secrète après reconstruction.

La figure 3 met en valeur l'efficacité de cette méthode en démontrant les différences entre l'image d'origine et l'image traitée par cette méthode comparée à celle corrigée par filtre médian.



(a) Différence avec filtre médian I_F (b) Différence avec l'image corrigée I_C

FIGURE 3 – Cartes de différence entre l'imagine d'origine et les images reconstruites débruitées.

Enfin, nous mesurons quantitativement ces résultats dans la figure 4. Non seulement nous améliorons la qualité de l'image lors de sa reconstruction, mais nous obtenons notamment un NPCR beaucoup plus faible.

Image débruitée	**PSNR (dB)** ↑	**NPCR (%)** ↓	**UACI (%)** ↓
Filtre médian	31,3034	52,5436	1,16766
Image corrigée	33,4051	2,22626	0,249329

TABLE 4 – Comparaison des métriques entre l'image originale et l'image médiane et corrigée.

3 Travail à effectuer

1. Continuer la recherche ainsi que l'analyse de la reconstruction d'image secrètes lorsque des parts sont bruitées. Réfléchir à des méthodes de débruitage ou de correction de l'erreur dans des images.
2. Continuer l'article inachevé de Laura Bertojo sur l'analyse de l'erreur pour des parts bruitées.

4 Activités

— **Réunions :**

1. Réunion d'équipe – Mardi 14/10/2025
   a) « Improving YOLOv8 for fast few-shot object detection by DINOv2 distillation » par Guillaume Fourret
   b) « Colorectal cancer tumor grade segmentation in digital histopathology images : from giga to mini challenge » par Guillaume Picaud
2. Point avec Pauline – Discussion sur l'avancée des travaux – Mercredi 15/10/2025

Références

[1] Laura Bertojo and William Puech. Correction of secret images reconstructed from noised shared images. In *2022 Eleventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pages 1–6, 04 2022.