Analyse d'images secrètes bruitées

E. Reinders[1] B. Jansen van Rensburg[1,2] P. Puteaux[3] W. Puech[1]

[1] LIRMM, Univ. Montpellier, CNRS, Montpellier, France
[2] Stratégies, Rungis, France
[3] Univ. Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL, F-59000 Lille, France

Résumé

La protection de données multimédia est un sujet d'actualité crucial. L'un des moyens d'y parvenir est d'appliquer sur ces données des méthodes de partage de secret. Les parts ainsi générées et distribuées peuvent cependant être compressées par des algorithmes de compression avec pertes, tels que JPEG. Dans cet article, nous analysons l'impact d'une compression JPEG sur une part dans la reconstruction d'une image secrète. Pour cela, nous nous appuyons sur une méthode développée en 2022 par Bertojo et Puech [1] pour la correction d'images secrètes bruitées, reconstruites à partir de parts compressées avec JPEG.

Mots clefs

Sécurité multimédia, Partage d'image secrète, Compression JPEG, Reconstruction en présence de bruit.

1 Introduction

Dans un monde en constante évolution numérique, il est devenu courant de sauvegarder et de partager des contenus multimédia (images, vidéos et données 3D) sur différents appareils ou réseaux informatiques. La démocratisation de ces pratiques entraîne inévitablement des questionnements quant à la sécurisation de ces données multimédia. Des techniques comme le chiffrement, basé sur une ou plusieurs clés utilisées pour permuter et substituer les données à sécuriser, ou encore le tatouage, basé sur l'insertion de données cachées pour vérifier l'intégrité par exemple, ont vu le jour. Ces données multimédia représentent souvent de gros volumes d'informations à traiter pour les réseaux informatiques, et doivent par conséquent être compressées. Pour les images, le standard de compression est JPEG (*Joint Photographic Experts Group*) [2]. Une alternative au chiffrement ou au tatouage, est le partage de secret, qui permet de partager un secret entre n personnes, et de le reconstruire avec k parmi ces n personnes. Ainsi, en 1979, Shamir [3] et Blakley [4] ont proposé chacun leur propre schéma de partage de secret. La particularité de ces schémas est que, contrairement à la cryptographie, il n'y a plus de clés à échanger, mais des parts du secret.

Naor et Shamir [5] ont proposé en 1994 le premier schéma de partage d'image binaire, basé sur un schéma de cryptographie visuelle. Appliqué au partage d'image secrète, les parts s'apparentent à des images. En 2002, Thien et Lin [6] ont amélioré ce partage, afin de pouvoir l'appliquer à des images en niveaux de gris. Chaque valeur de pixels de l'image constitue un secret et doit appartenir à un corps fini $\mathbf{GF}(251)$, induisant un traitement spécifique sur les pixels de valeur supérieure à 250. La méthode de Yang *et al.* [7] a permis ensuite de s'affranchir de ce problème, en travaillant sur un corps fini $\mathbf{GF}(2^8)$.Même s'ils représentent une grande évolution dans le partage d'image secrète, les travaux effectués dans ce domaine ont pour inconvénient principal de ne pas prendre en compte des parts bruitées lors de la reconstruction. Il est en effet possible que certaines d'entre elles subissent des transformations, comme une compression JPEG. Bertojo et Puech [1] ont proposé une première analyse et une correction d'images secrètes bruitées à cause de l'utilisation de parts compressées avec JPEG lors de la reconstruction.

Dans cet article, nous analysons en détail la dégradation sur une image secrète reconstruite, induite par l'utilisation d'une part compressée avec JPEG. En section 2, nous analysons l'impact d'une part compressée avec JPEG sur la reconstruction d'une image secrète. En section 3, nous présentons des résultats expérimentaux issus d'une telle reconstruction. Enfin, en section 4, nous concluons sur le travail présenté, et discutons des perspectives d'amélioration.

2 Analyse

Dans cette section, nous analysons le modèle du bruit impactant une image secrète quand celle-ci est reconstruite à partir de k parts dont certaines sont bruitées. Le bruit subi par certaines parts peut être généré pendant une transmission sur des réseaux bas débit par exemple, ou à cause d'une compression avec pertes telle que JPEG.

2.1 Partage d'image avec Shamir

Pour pallier les problèmes induits par le chiffrement, Shamir a décrit en 1979 une méthode de partage de secret [3]. Sur la base de n utilisateurs, il a proposé de générer n parts d'un secret $\mathcal{S}$, afin qu'il soit possible de reconstruire le secret à partir de k parts, avec $1 < k \leq n$. Pour cela, Shamir suggère de partager des couples de valeurs $S_i = (x_i, y_i = f(x_i))$, avec $i \in \{1, ..., n\}$, les coordonnées d'un point d'un polynôme $f(.)$ de degré $k-1$. Ce polynôme est construit de telle sorte que le secret soit reconstruit pour $x = 0$, avec $f(0) = \mathcal{S}$. Shamir se base sur le partage d'une donnée entière non signée, définie sur un

corps fini $\mathbb{F}_p$ de cardinalité p. L'utilisation d'un tel anneau $\mathbb{Z}/p\mathbb{Z}$ permet une approximation sûre lors de la reconstruction du secret par la suite. Par conséquent, le polynôme de degré $k-1$ est généré à partir de $k-1$ coefficients aléatoires a_j, avec $j \in \{1, ..., k-1\}$, tels que $a_j < p$ et $a_0 = \mathcal{S}$:

$$f(x) = \mathcal{S} + \sum_{j=1}^{k-1} a_j \times x^j \mod p. \quad (1)$$

Afin de pouvoir reconstruire le secret $\mathcal{S} = a_0$ avec l'interpolation de Lagrange, au minimum k parts $S_i = (x_i, y_i)$ sont nécessaires :

$$f(x) = \sum_{i=1}^{k} y_i \times \prod_{u=1, u\neq i}^{k} \frac{x - x_u}{x_i - x_u} \mod p, \quad (2)$$

avec :

$$f(0) = a_0 = \sum_{i=1}^{k} y_i \times \prod_{u=1, u\neq i}^{k} \frac{x_u}{x_i - x_u} \mod p. \quad (3)$$

Le partage de secret peut s'étendre à du partage d'image secrète, en considérant une image secrète comme une matrice de pixels secrets. Les secrets deviennent alors les niveaux de gris (NDG), codés sur 8 bits, des pixels de l'image à partager. Pour ce faire, nous considérons un polynôme par pixel de l'image secrète. Soit une image secrète I, composée de $W \times H$ pixels $p_{w,h}$, avec $(w, h) \in [\![0, W[\![\times [\![0, H[\![$ leur position, nous générons alors n parts, sous la forme de couples de valeurs $S_i = (x_i = i, y_i = I_i)$, avec $i \in \{1, ..., n\}$ et I_i l'image part de même taille que l'image secrète. Ces parts peuvent se voir plus simplement comme des images I_i indexées de 1 à n. Pour I_i, à partir d'un pixel $p_{w,h}$ de I et de l'équation 1, nous générons n pixels $p_{w,h}(x_i)$ suivant :

$$p_{w,h}(x) = p_{w,h} + \sum_{j=1}^{k-1} a_{j,w,h} \times x^j \mod 251. \quad (4)$$

Nous prenons $p = 251$, car il s'agit du plus grand nombre premier inférieur à 2^8. Par conséquent, soit les NDG entre 251 et 255 ne sont pas traités et restent en clair dans les images parts, soit un pré-traitement de l'image secrète est nécessaire afin de ramener les valeurs des NDG entre 0 et 250.

2.2 Analyse du bruit induit dans une part par une compression JPEG

Une part I_i peut être bruitée, soit pendant une transmission bas débit ou sans fil, soit lors d'une compression avec pertes. Dans cette section nous analysons en particulier l'impact du bruit sur une telle part compressée avec JPEG [2], standard en matière de compression d'images. Lors d'une compression JPEG d'une image, après un changement d'espace couleur et d'éventuels sous-échantillonnages, les pixels, par bloc de 64, subissent une transformation DCT (*Discrete Cosine Transform*). Cette étape génère des coefficients DCT $F(u, v)$ pour chaque bloc, quantifiés selon des coefficients de quantification $q(u, v)$, dépendant d'un facteur de quantification QF compris entre 1 et 100 :

$$F'(u, v) = \left[\frac{F(u, v)}{q(u, v)}\right], \quad (5)$$

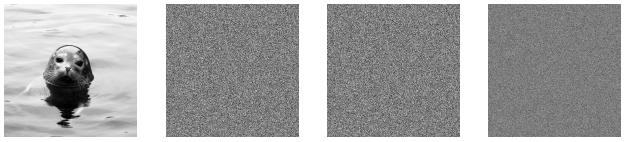
avec $u, v \in \{0, \ldots, 7\}$ et $[.]$ correspondant à l'entier le plus proche. C'est durant la phase de quantification que la perte par compression JPEG a principalement lieu. Un codage entropique est alors appliqué sur les coefficients quantifiés $F'(u, v)$, suivant un ordre zig-zag. Dans le cas $QF = 100$, l'image à compresser est faiblement impactée car tous les coefficients de quantification $q(u, v)$ valent 1, soit :

$$F'(u, v) = [F(u, v)]. \quad (6)$$

Afin d'analyser les effets d'une compression JPEG avec $QF = 100$, nous avons compressé 1000 parts générées à partir d'images de la base BOWS-2 [8]. Nous remarquons alors au décodage, que sur les 1000 images compressées, en moyenne $90,79\%$ des pixels restent inchangés ($0,04\%$ d'écart type), $4,59\%$ sont modifiés de +1 niveau de gris et $4,62\%$ de -1 niveau de gris (pour un écart type de $0,03\%$ dans les deux cas), soit un taux d'erreur $\tau = 9,21\%$. À partir d'un pixel $p_{w,h}(x_i)$ de la part I_i, nous obtenons alors un pixel bruité $p^*_{w,h}(x_i)$:

$$p^*_{w,h}(x_i) = p_{w,h}(x_i) + N_{w,h}, \text{ avec } N_{w,h} = \begin{cases} +1 \\ 0 \\ -1 \end{cases}, \quad (7)$$

tel que $Prob(N_{w,h} = 0) = 100 - \tau$, $Prob(N_{w,h} = +1) = Prob(N_{w,h} = -1) = \frac{\tau}{2}$.



(a) (b) (c) (d)

FIGURE 1 – *Compression JPEG avec QF = 100 sur une image de BOWS-2 [8] : a) Image secrète I, b) Part I_i, c) I_i compressée avec JPEG : I^*_i, d) Différence entre I_i et I^*_i.*

La figure 1 illustre le bruit induit dans une part par une compression JPEG. À partir de l'image secrète illustrée en figure 1.a, n parts sont générées, dont une est illustrée en figure 1.b. Ces parts sont semblables visuellement à des images de bruit aléatoire (PSNR avec l'image originale secrète de 6,74 dB, pour un SSIM de 0,01). Si la part illustrée figure 1.b est compressée avec JPEG (QF=100), nous obtenons une part bruitée très similaire (PSNR avec la figure 1.b de 58,35 dB, pour un SSIM de 0,99), comme illustrée en figure 1.c. En observant les différences entre la part originale et la part bruitée, illustrées figure 1.d, nous remarquons que la majorité des pixels n'est pas impactée par cette compression (NDG = 128), et que $9,18\%$ sont impactés de $+1$ (NDG = 255) ou de -1 (NDG = 0).

2.3 Impact d'une part bruitée sur la reconstruction d'une image secrète

En section 2.2, nous avons constaté que la compression JPEG avec $QF = 100$ d'une part introduisait un bruit. Utiliser des parts bruitées pour la reconstruction d'une image secrète risque donc d'induire des erreurs au moment de la reconstruction. Supposons que k' parts bruitées selon l'équation 7, avec $k' \leq k$, soient utilisées pour reconstruire

une image secrète. À la place de l'image secrète originale I, nous obtenons alors une image secrète bruitée I^*, composée de pixels $p^*_{w,h}$ reconstruits à partir de polynômes approximés $p^*_{w,h}(x)$:

$$\begin{aligned} p^*_{w,h} &= p^*_{w,h}(0) \\ &= \sum_{m=1}^{k'} p^*_{w,h}(x_m) \prod_{u=1,u\neq m}^{k} \frac{x_u}{x_u - x_m} \\ &+ \sum_{m=k'+1}^{k} p_{w,h}(x_m) \prod_{u=1,u\neq m}^{k} \frac{x_u}{x_u - x_m} \mod 251. \end{aligned} \tag{8}$$

Le bruit de reconstruction $\Delta^{err}_{w,h}$ est donc la différence entre $p_{w,h}(0)$ et $p^*_{w,h}(0)$:

$$\begin{aligned} \Delta^{err}_{w,h} &= p_{w,h}(0) - p^*_{w,h}(0) \\ &= \sum_{m=1}^{k'} N_{w,h}(x_m) \prod_{u=1,u\neq m}^{k} \frac{x_u}{x_u - x_m} \mod 251, \end{aligned} \tag{9}$$

avec $N_{w,h}(x_m)$ le bruit appliqué à la part I_m.
Dans cet article, nous limitons cette analyse à une seule image part bruitée ($k' = 1$) et une reconstruction avec 3 parts ($k = 3$). Nous définissons la part bruitée I_m, en position m, et les deux parts positionnées de part et d'autre de I_m à la distance $\pm\delta$: $I_{m-\delta}$ et $I_{m+\delta}$. Le bruit de reconstruction Δ^{err} appliqué sur l'image reconstruite I^*, représenté par l'équation 9, se ramène alors à :

$$\Delta^{err} = N_{w,h} \times \left(\frac{1 - m^2}{\delta^2}\right) \mod 251, \tag{10}$$

avec $N_{w,h}$ le bruit subi par l'image part I_m, comme défini dans l'équation 7.

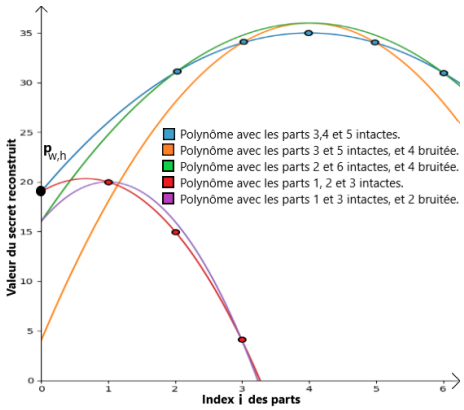


FIGURE 2 – *Impact de la valeur de m et de δ dans la reconstruction du secret.*

Prenons $p_{w,h} = 19$. Dans la figure 2, nous construisons un polynôme $f(.)$ de degré deux (courbe bleue), à partir des parts $p_{w,h}(3) = 34$, $p_{w,h}(4) = 35$ et $p_{w,h}(5) = 34$. Supposons désormais la part $p^*_{w,h}(4) = 36$ bruitée de $+1$, le polynôme orange est alors obtenu. D'après l'équation 10, nous nous retrouvons avec un scénario de reconstruction $m = 4$, $\delta = 1$ et $N_{w,h}(4) = 1$. La valeur $p^*_{w,h}$ reconstruite est de 4, soit $\Delta^{err}_{w,h} = 15$. La courbe verte correspond à une reconstruction avec $p^*_{w,h}(4) = 36$ et $p_{w,h}(2) = p_{w,h}(6) = 31$, soit $m = 4$, $\delta = 2$ et $N_{w,h}(4) = 1$. Dans ce cas, $\Delta^{err}_{w,h} = 3$.

Nous remarquons que quand δ croit, alors le bruit de reconstruction s'atténue. Nous construisons un autre polynôme pour le même secret $p_{w,h} = 19$, mais en utilisant les parts $p_{w,h}(1) = 20$, $p_{w,h}(2) = 15$ et $p_{w,h}(3) = 4$ (courbe rouge). Supposons que nous nous retrouvons à nouveau dans une reconstruction incluant une part bruitée, avec $m = 2$, $\delta = 1$ et avec le même bruit tel que $p^*_{w,h}(2) = p_{w,h}(2) + 1$. Nous obtenons alors la courbe violette, et nous remarquons que reconstruire à partir d'une part bruitée en position plus faible (m), atténue la valeur du bruit à la reconstruction du secret. Pour un m et un δ donnés, nous obtenons alors cinq scénarios possibles de bruit pour $p^*_{w,h}$:

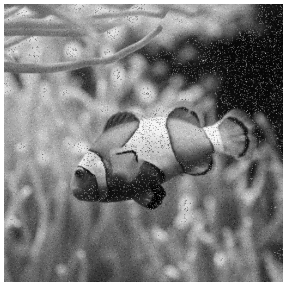
$$\begin{cases} p_{w,h} & \text{si } N_{w,h} = 0, \\ p_{w,h} + \Delta^{err}_{w,h} & \text{si } p_{w,h} < 251 - \Delta^{err}_{w,h} \text{ et } N_{w,h} = 1, \\ p_{w,h} + (\Delta^{err}_{w,h} - 251) & \text{si } p_{w,h} \geq 251 - \Delta^{err}_{w,h} \text{ et } N_{w,h} = 1, \\ p_{w,h} - (\Delta^{err}_{w,h} - 251) & \text{si } p_{w,h} < \Delta^{err}_{w,h} \text{ et } N_{w,h} = -1, \\ p_{w,h} - \Delta^{err}_{w,h} & \text{si } p_{w,h} \geq \Delta^{err}_{w,h} \text{ et } N_{w,h} = -1. \end{cases} \tag{11}$$

Nous nous retrouvons avec un bruit à la reconstruction de type **poivre et sel mod 251**.

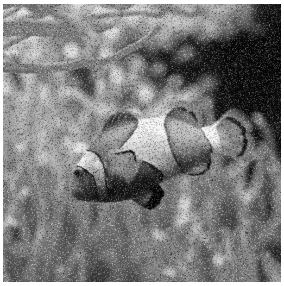
3 Résultats

(a) Image secrète
PSNR = +∞, SSIM = 1,0

(b) Δ^{err}=3 (m=8,δ=4)
PSNR = 43,89 dB, SSIM = 0,98



(c) Δ^{err}=48 (m=7,δ=1)
PSNR = 20,22 dB, SSIM = 0,38



(d) Δ^{err}=120 (m = 11,δ=1)
PSNR = 16,03 dB, SSIM = 0,14

FIGURE 3 – *Reconstructions d'une image secrète, issue de BOWS-2 [8], pour différentes valeurs de* Δ^{err} *(*$\tau = 9,21\%$*) : a) Image secrète originale, b) c) d) Images secrètes reconstruites pour différentes valeurs de* Δ^{err}.

La figure 3 illustre la reconstruction d'une image secrète selon différentes configurations possibles de m et δ, avec en figure 3.a la reconstruction sans part bruitée (image secrète originale). Nous remarquons figure 3.b que pour des valeurs faibles de bruit Δ^{err} à la reconstruction ($\Delta^{err} = 3$), l'image reconstruite est visuellement très similaire à l'image secrète originale. Seules quelques variations vi-

sibles s'opèrent au moment d'ajouter (ou retrancher) 3 à un pixel bruité de valeur d'intensité supérieure à 248, ou inférieure à 3. D'après les scénarios possibles de bruit, présentés dans l'équation 11, nous nous retrouvons dans le cas d'un scénario de bruit décrit ligne 3 ou 4, entraînant de fortes variations entre pixels originaux et bruités. Pour une configuration induisant un bruit Δ^{err} plus important à la reconstruction de l'image secrète (illustré figure 3.c et 3.d), un pixel reconstruit bruité $p^*_{w,h}$ est plus fortement impacté pour un scénario de bruit décrit ligne 2 ou 5. Un scénario de bruit décrit ligne 3 ou 4 a, pour cette configuration, une plus grande probabilité d'apparition, mais ne va pas faire autant varier la valeur du pixel bruité $p^*_{w,h}$, que pour une configuration de bruit Δ^{err} plus faible. Cela a pour conséquence directe de limiter l'apparition du phénomène de forte variation entre pixels originaux et bruités dans l'image reconstruite.

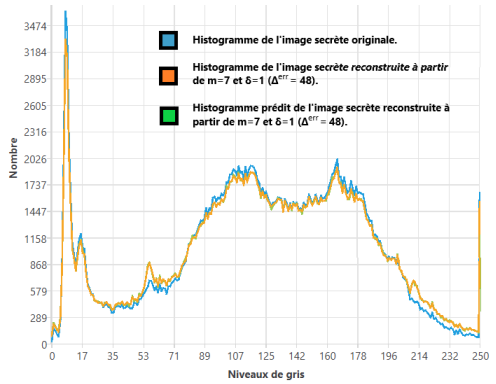


FIGURE 4 – *Exemple de prédiction d'histogramme d'une image secrète reconstruite pour la configuration m = 7, δ = 1 ($\Delta^{err} = 48$) et τ = 9,21%.*

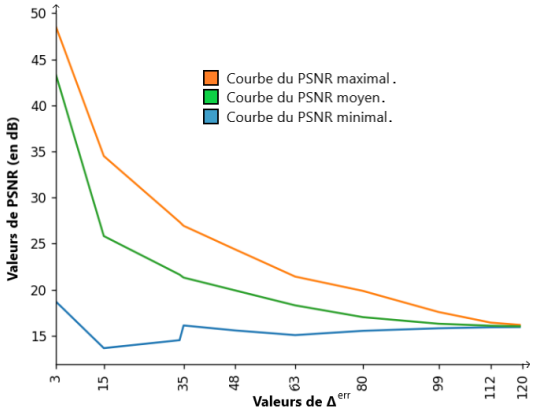


FIGURE 5 – *Variation du PSNR en fonction de la valeur Δ^{err} sur 200 images de BOWS-2 [8] pour un τ = 9,21%.*

À partir de m et δ, nous connaissons donc le bruit appliqué à la reconstruction d'une image secrète. Nous pouvons par conséquent prédire l'histogramme de l'image reconstruite. En effet, comme illustré figure 4, partant de l'histogramme de l'image secrète (courbe bleue), supposons que $\frac{\tau}{2}\%$ des pixels de I^* sont bruités de $+\Delta^{err}_{w,h}$, $\frac{\tau}{2}\%$ de $+(251 - \Delta^{err}_{w,h})$ et $(100 - \tau)\%$ restent inchangés : nous obtenons la courbe verte. Celle-ci correspond assez fidèlement à l'histogramme réellement obtenu après reconstruction sur une telle configuration (courbe orange).
Sur la figure 5, les courbes bleue,verte et orange, représentent respectivement les valeurs de PSNR minimales, moyennes et maximales obtenues avec les valeurs de $\Delta^{err} = \{3, 15, 34, 35, 48, 63, 80, 99, 112, 120\}$, sur 200 images de BOWS-2 [8]. Nous remarquons que plus la valeur de Δ^{err} augmente, et plus la qualité de l'image reconstruite, par rapport à l'image secrète originale, diminue.

4 Conclusion

Dans cet article, nous avons proposé une analyse de la reconstruction d'une image secrète à partir d'une part compressée avec JPEG ($QF = 100$), et de deux autres parts intactes ($k = 3$). Une compression JPEG ($QF = 100$) impacte la part compressée, induisant des erreurs de reconstruction dans l'image secrète. Dépendant des index m et δ des parts utilisées au moment de reconstruire ce secret, le bruit induit à la reconstruction (bruit **poivre et sel mod 251**) varie et impacte plus ou moins fortement l'image secrète reconstruite. Nous avons également démontré qu'il est possible de prédire l'histogramme d'une image reconstruite bruitée, dès lors que nous connaissons la configuration de bruit appliquée, en fonction des parts utilisées pour la reconstruction. Cette prédiction d'histogramme peut être utile pour nous guider dans la reconstruction de l'image secrète.
En perspectives, il serait intéressant de chercher à débruiter ces images reconstruites, par emploi de réseaux de neurones entraînés sur ce type de bruit par exemple.

Références

[1] L. Bertojo et W. Puech. Correction of Secret Images Reconstructed from Noised Shared Images. Dans *IEEE IPTA*, pages 1–6, 2022.

[2] G. K. Wallace. The JPEG still picture compression standard. *IEEE Transactions on Consumer Electronics*, 38(1) :XVIII–XXXIV, 1992.

[3] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11) :612–613, 1979.

[4] G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of the National Computer Conference*, 48 :313–317, 1979.

[5] M. Naor et A. Shamir. Visual cryptography. Dans *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 1–12. Springer, 1994.

[6] C. C. Thien et J. C. Lin. Secret image sharing. *Computers & Graphics*, 26(5) :765–770, 2002.

[7] C. N. Yang. New visual secret sharing schemes using probabilistic method. *Pattern Recognition Letters*, 25(4) :481–494, 2004.

[8] P. Bas et T. Furon. Image database of BOWS-2. http ://bows2.eclille.fr/.