Stratégies d'insertion informée pour un algorithme de tatouage utilisant l'interpolation bilinéaire

Vincent Martin Marie Chabert Bernard Lacaze

IRIT/ENSEEIHT

2, rue Camichel, 31000 TOULOUSE

{martin, chabert, lacaze}@enseeiht.fr

Résumé

Les techniques d'interpolation d'images ont pour propriété de préserver la qualité visuelle, qui est l'une des principales contraintes du tatouage d'image numérique. Cet article présente un algorithme de tatouage utilisant l'interpolation bilinéaire. Il s'agit d'une technique substitutive et de codage informé. Ses propriétés d'imperceptibilité, de robustesse et de sécurité ont été démontrées et comparées avec des méthodes classiques. Il est possible d'établir ses performances théoriques en présence de bruit. On s'intéresse plus particulièrement à l'utilisation de cette expression théorique dans des stratégies d'insertion informée.

Mots clefs

tatouage numérique, interpolation, insertion informée

1 Introduction

Le tatouage numérique consiste à insérer une information dans le contenu d'un document, sous les contraintes d'imperceptibilité, de sécurité et de robustesse aux attaques. Ses applications vont de la gestion des droits d'auteurs numériques à la protection d'intégrité. Dans le tatouage à étalement de spectre à Séquence Directe (DS), on module le message par une séquence pseudo-aléatoire avant de l'ajouter au document. Un corrélateur est utilisé au décodage, parfois associé à un préfiltrage de Wiener (DS+W) [1]. Le tatouage informé consiste à profiter de la connaissance du document lors de l'insertion [2]. On parle de codage informé lorsque le tatouage est construit en fonction de l'image, notamment pour respecter l'imperceptibilité. Si de plus on connaît le décodeur lors de l'insertion, on peut utiliser une stratégie d'insertion informée pour atteindre un objectif fixé en réception. Le principe du tatouage informé a notamment été utilisé dans les techniques d'étalement de spectre amélioré linéaire (LISS) [3] et dans les techniques de *binning* aléatoire [4], dont la plus populaire est le Schéma de Costa Scalaire à Transformation d'étalement (ST-SCS) [5]. Dans ces techniques, le document original n'est plus une source d'interférence.

L'interpolation [6] est souvent considérée comme une source d'erreur dans les schémas de tatouage d'image. En effet, elle est associée à un ré-échantillonnage lors d'attaques géométriques ou lors d'une insertion dans un domaine transformé. Au sein d'un algorithme de tatouage, l'interpolation n'a été utilisée que dans le cas d'objets 3D [7] ou dans un but cryptographique [8].

Les notations suivantes seront utilisées : soit $M = [m(l)]_{l\in\{1,\dots,L\}}$ le message binaire de taille L. Soit I l'image originale, W le tatouage et $I_W = I + W$ l'image tatouée. On utilise la notation matricielle suivante : $I = [i(n_1, n_2)]_{n_1\in\{1,\dots,N_1\},n_2\in\{1,\dots,N_2\}}$. I_W est transmise et peut être attaquée, devenant I'_W. Certaines attaques sont modélisées par un bruit additif blanc gaussien (AWGN) : $I'_W = I_W + B$ où $b(n_1, n_2) \sim \mathcal{N}(0, \sigma_B^2)$. Soit σ_W^2 la variance de $w(n_1, n_2)$. On définit le Rapport Document à Tatouage (DWR), le Rapport Document à Bruit (DNR) et le Rapport Tatouage à Bruit (WNR) :

$$\text{DWR} = \frac{\sigma_I^2}{\sigma_W^2},\ \text{WNR} = \frac{\sigma_W^2}{\sigma_B^2},\ \text{DNR} = \frac{\sigma_I^2}{\sigma_B^2}$$

Dans la partie 2, on introduit un algorithme de tatouage utilisant l'interpolation bilinéaire. On étudie ses performance théoriques dans la partie 3. La partie 4 s'intéresse plus particulièrement à l'utilisation de stratégies d'insertion informée. Les propriétés d'imperceptibilité, de robustesse et de sécurité sont étudiées dans la partie 5.

2 Algorithmes de tatouage informé utilisant l'interpolation

2.1 Principe général

Afin de mettre à profit les propriétés perceptuelles de l'interpolation dans un schéma de tatouage, on se propose de générer un tatouage à partir du résultat d'une interpolation. Certains pixels sont inchangés et sont utilisés pour interpoler la valeur d'autres pixels. Le schéma général de cette classe d'algorithmes, appelée W-interp, est présenté Fig. 1. Ce schéma a été proposé initialement dans [9]. Deux variantes ont été étudiées en détail : W-bilin, utilisant l'interpolation bilinéaire [10] et W-spline, utilisant l'interpolation par splines bicubiques [9].

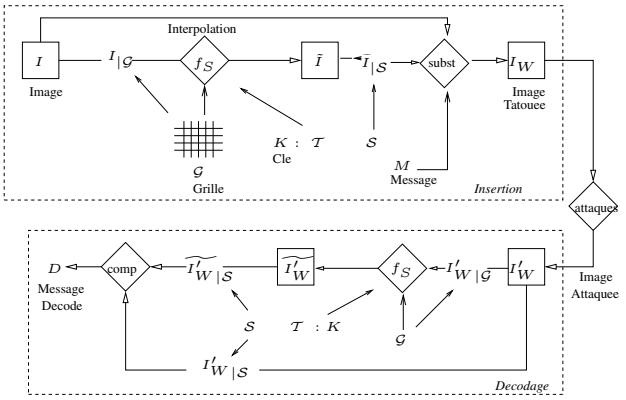

Figure 1 – *Classe de méthodes de tatouages W-interp*

Le principe de W-interp est le suivant. On sélectionne dans I deux ensembles disjoints de coordonnées respectives $\mathcal{G}$ et $\mathcal{S}$. $\mathcal{G}$ représente la grille. Le tatouage est inséré dans $\mathcal{S} \subset \{1,\dots,N_1\} \times \{1,\dots,N_2\} \setminus \mathcal{G}$. Soit $N_\mathcal{S}$ le cardinal de $\mathcal{S}$ et $P_\mathcal{S} = N_\mathcal{S}/L$ la redondance. $\mathcal{S}$ est divisé en L ensembles disjoints et choisis aléatoirement, de taille $P_\mathcal{S}$: $\mathcal{S} = \mathcal{S}_1 \cup \cdots \cup \mathcal{S}_L$, $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset \quad \forall i \neq j$. $\mathcal{S}_k$ est associé au bit $m(k)$ du message. De plus, tout algorithme de tatouage est associé à une clé secrète K, connue à l'insertion et au décodage, qui empêche les pirates de décoder le tatouage. Ici, soit $\mathcal{T}$ un ensemble de paramètres aléatoires spécifiquement introduits pour garantir la sécurité de l'algorithme. K est composée des coordonnées du tatouage $\mathcal{S}$ et des paramètres de sécurité associés ($K = \{\mathcal{S}, \mathcal{T}\}$). Soit $I_{|\mathcal{G}}$ la restriction de I à $\mathcal{G}$. Enfin, soit g une fonction

$$g(I_{|\mathcal{G}}; \mathcal{G}, \mathcal{T}) = \widetilde{I}$$

qui produit $\widetilde{I}$ telle que $\widetilde{I}_{|\mathcal{G}} = I_{|\mathcal{G}}$ et que I et $\widetilde{I}$ soient proches perceptuellement. Remarquons que $I_{|\mathcal{S}}$ n'est pas fournie à g. g estime des échantillons manquants à partir d'un sous-ensemble de I. g peut donc être considérée comme une fonction d'interpolation.

A l'insertion, si $m(l) = 1$ les valeurs $I_{|\mathcal{S}_l}$ des pixels de $\mathcal{S}_l$ sont substituées par leur équivalent $\widetilde{I}_{|\mathcal{S}_l}$ fourni par g, donc $I_{W|\mathcal{S}_l} = \widetilde{I}_{|\mathcal{S}_l}$. Si $m(l) = -1$, $I_{W|\mathcal{S}_l} = I_{|\mathcal{S}_l}$.
Après d'éventuelles attaques, on compare au décodage $I'_{W|\mathcal{S}}$ et $\widetilde{I'_{W|\mathcal{S}}}$. Soit $R = \widetilde{I'_{W|\mathcal{S}}} - I'_{W|\mathcal{S}}$. Pour un bit donné $m(l)$, l'erreur quadratique moyenne $\rho^2(l) = \frac{1}{|\mathcal{S}_l|} \sum_{(n_1,n_2)\in\mathcal{S}_l} r(n_1,n_2)^2$ est comparée à un seuil ν dépendant de l'image. Si $\rho^2(l) < \nu$, la décision est $d(l) = +1$, sinon $d(l) = -1$. ν est choisi empiriquement à partir du résultat du décodage : $\nu = \frac{1}{L}\sum_{l=1}^{L} \rho^2(l)$.

g sera souvent une fonction linéaire des éléments de $\mathcal{G}$. Elle agira donc comme un filtre local. L'imperceptibilité impose que W modifie les hautes et moyennes fréquences de I. g agit donc comme un filtre passe-bas, et le tatouage consiste à modifier les coefficients passe-haut de I.

Ce cadre général fournit des algorithmes de tatouage substitutifs aveugles, car I n'est pas utilisée au décodage. W-interp est une méthode à rejet des interférences de l'hôte car en l'absence d'attaque, on obtient un décodage parfait. On peut alors insérer jusqu'à $N_\mathcal{S}$ bits (débit accessible de $N_\mathcal{S}/N$). W-interp est un algorithme de tatouage informé. En effet, il utilise I pour générer W afin de respecter un modèle perceptuel, donc il s'agit de codage informé. Par contre, la seule stratégie d'insertion informée est ici le rejet des interférence de l'hôte, i.e. maximiser la détection à distortion constante et en l'absence d'attaque.

Une variante de W-interp est caractérisée par le choix d'une fonction g, d'une grille $\mathcal{G}$, des positions $\mathcal{S}$ des points à tatouer, ainsi que des paramètres de sécurité $\mathcal{T}$.

2.2 Variante W-bilin

On se limite dans cet article à la variante W-bilin, où g réalise une interpolation bilinéaire. L'interpolation bilinéaire au point (x, y) est la moyenne de ses 4 plus proches voisins sur la grille, pondérée par leur distance à (x, y) :

$$\begin{aligned} i_{int}(x,y) = \frac{y-y_1}{y_2-y_1}\left(\frac{x-x_1}{x_2-x_1}i(x_2,y_2) + \frac{x_2-x}{x_2-x_1}i(x_1,y_2)\right) \\ + \frac{y_2-y}{y_2-y_1}\left(\frac{x-x_1}{x_2-x_1}i(x_2,y_1) + \frac{x_2-x}{x_2-x_1}i(x_1,y_1)\right) \end{aligned}$$

Dans W-bilin, on substitue $i(n_1, n_2)$ par

$$\widetilde{i}(n_1,n_2) = i_{int}(n_1 + \tau_x(n_1,n_2), n_2 + \tau_y(n_1,n_2))$$

où $\tau_x(n_1, n_2)$ et $\tau_y(n_1, n_2)$ sont des variables aléatoires i.i.d. uniformément distribuées sur $]-a, +a[$. Une augmentation de a bénéficie à la robustesse et à la sécurité, mais la distortion augmente elle aussi. On choisira comme grille $\mathcal{G} = ((2\mathbb{Z}+1) \times 2\mathbb{Z}) \cup (2\mathbb{Z} \times (2\mathbb{Z}+1))$, qui a la forme d'un damier.

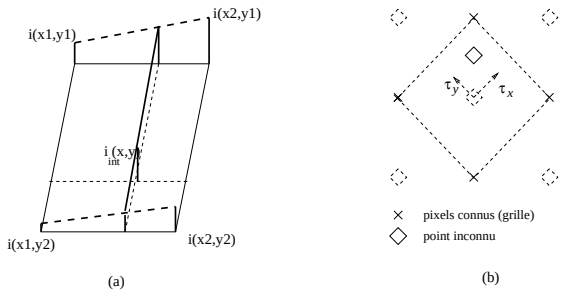

Figure 2 – *(a) Interpolation bilinéaire (b) Décalages aléatoires*

3 Performances théoriques face au bruit additif blanc gaussien

3.1 Influence de $\mathcal{T}$ sur la détection

Soit $g_{k,l}$ le poids du pixel $i(n_1-k, n_2-l)$ dans $\widetilde{i}(n_1, n_2)$. Le décodage compare $R = \{r(n_1, n_2)\}$ à un seuil, avec

$$r(n_1, n_2) = \epsilon_{I_W}(n_1, n_2) + \epsilon_B(n_1, n_2), \text{ où}$$
$$\epsilon_X(n_1, n_2) = \tilde{x}(n_1, n_2) - x(n_1, n_2)$$
$$= \sum_{k=-1}^{1} \sum_{l=-1}^{1} g_{k,l}(x(n_1-k, n_2-l) - x(n_1, n_2))$$

$$\text{Alors } \mathrm{E}[\epsilon_B] = 0 \text{ et } \sigma^2_{\epsilon_B} = (1+\Delta_{\mathcal{T}})\sigma_B^2$$

où la constante $\Delta_{\mathcal{T}}$ dépend de $\mathcal{T}$: $\Delta_{\mathcal{T}} = \sum_{k=-1}^{1}\sum_{l=-1}^{1} \mathrm{E}[g_{k,l}^2]$. Pour W-bilin, comme les élément des $\mathcal{T}$ sont uniformément répartis sur $[-a, a]$,

$$\Delta_{\mathcal{T}} = 4(\frac{1}{4} + a^2/3)^2$$

Sans décalage, $\Delta_{\mathcal{T}} = 0.25$. De plus, on peut déterminer a si $\Delta_{\mathcal{T}}$ est donné.

3.2 Détection

ϵ_I suit une loi gaussienne généralisée, ce qui permet de construire un décodeur optimal [9]. Pour simplifier, on modélise ici l'erreur d'interpolation par une distribution gaussienne : $\epsilon_I(n_1, n_2) \sim \mathcal{N}(0, \sigma^2_{\epsilon_I})$. La détection consiste en un test d'hypothèse binaire :

• hypothèse H_0 : absence de tatouage,

• hypothèse H_1 : présence d'un tatouage.

Soit P_d la probabilité de détection et P_{fa} celle de fausse alarme. Le détecteur de Neyman-Pearson maximise P_d à P_{fa} donnée. La statistique de test correspondante est ici

$$T = \sum_{\mathcal{S}} r(n_1, n_2)^2$$

Sous H_0, $R \sim \mathcal{N}(0, (1+\Delta_{\mathcal{T}})\sigma_B^2 + \sigma^2_{\epsilon_I})$.
Sous H_1, la substitution à l'insertion conduit à $\epsilon_{I_W}(n_1, n_2) = 0$, donc $R \sim \mathcal{N}(0, (1+\Delta_{\mathcal{T}})\sigma_B^2)$.
R étant gaussienne centrée, T suit une distribution du χ^2_P sous les deux hypothèses. Soit $\mathrm{F}_{\chi^2_P}$ la fonction de répartition de χ^2_P. On décide H_1 quand $T < \eta$ avec

$$\eta = (1+\Delta_{\mathcal{T}})\sigma_B^2 \mathrm{F}^{-1}_{\chi^2_P}(1 - \mathrm{P_{fa}})$$

Dans ce cas, $P_d = 1 - \mathrm{F}_{\chi^2_P}(\eta/((1+\Delta_{\mathcal{T}})\sigma_B^2 + \sigma^2_{\epsilon_I}))$.
La distance de Kullback-Leibler D_{KL} entre les distributions de T sous H_0 et H_1 est utilisée comme borne supérieure des performances de détection, similaire à la capacité dans le problème du décodage [13]. Soit f_T la densité de probabilité de T. Ici,

$$D_{\text{KL}} = \int_{-\infty}^{+\infty} f_{T|H_0}(t) \log \frac{f_{T|H_0}(t)}{f_{T|H_1}(t)} \mathrm{d}t$$

Pour W-interp, approximons T par une loi normale, si $P_{\mathcal{S}}$ est grand (théorème central limite). On compare $\mathcal{N}(\mu_{T|H_0}, \sigma^2_{T|H_0})$ et $\mathcal{N}(\mu_{T|H_1}, \sigma^2_{T|H_1})$, donc

$$D_{\text{KL}} = \frac{1}{2}\left(\log \frac{\sigma^2_{T|H_1}}{\sigma^2_{T|H_0}} + \frac{(\mu_{T|H_0} - \mu_{T|H_1})^2 + \sigma^2_{T|H_0} - \sigma^2_{T|H_1}}{\sigma^2_{T|H_1}}\right)$$

On compare sur la Fig. 3 les performances de W-bilin et des algorithmes classiques DS, DS+W et LISS. DS et DS+W ont une performance bornée par les interférences de l'image hôte. Pour les techniques de tatouage informé W-interp et LISS, $D_{\text{KL}} \to +\infty$ lorsque le bruit diminue. W-interp est la meilleure technique en cas de bruit faible. Par contre, W-interp n'est pas robuste à un fort bruit, auquel les techniques de type DS sont plus robustes.

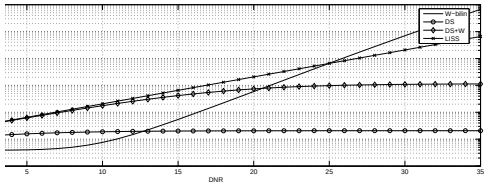

Figure 3 – *Comparaison des D_{KL}, Lena, DWR=38 dB, $N = 2^{18}$*

3.3 Décodage

Pour le décodage, on estime M à partir de I'_W grâce au Taux d'Erreur Bit (TEB) : $\text{TEB} = (1 - \sum_{l=1}^{L} \delta(d(l), m(l)))/L$. Le seuil de décision optimal η_{th} minimise le TEB. Si les bits $\{-1, +1\}$ sont équiprobables, η_{th} est solution de :

$$\frac{1}{\sigma^2_{R|H0}} f_{\chi^2_P}(\frac{\eta_{\text{th}}}{\sigma^2_{R|H0}}) = \frac{1}{\sigma^2_{R|H1}} f_{\chi^2_P}(\frac{\eta_{\text{th}}}{\sigma^2_{R|H1}})$$

La Fig. 4 montre l'amélioration apportée par η_{th} par rapport à un décodage sous-optimal avec le seuil empirique. La Fig. 5 montre qu'à WNR raisonnable, W-interp offre de très bonnes performances face au bruit AWGN.

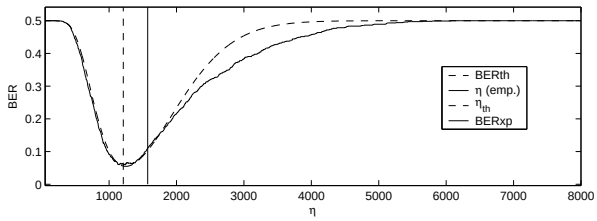

Figure 4 – *Choix de η : DWR=38 dB, $L = 1024$, WNR=-10 dB*

4 Liens avec l'insertion informée

Une contribution originale de cet article consiste à utiliser la relation entre W-interp et le tatouage informé pour améliorer ses performance. Deux principes sont abordés : la compensation des distortions et l'insertion informée.

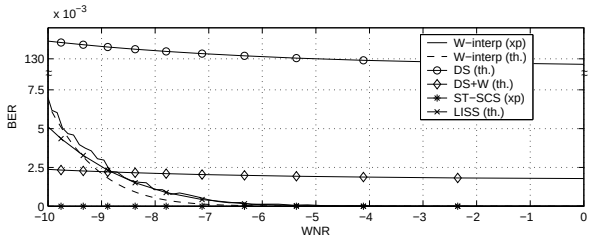

Figure 5 – *Robustesse au bruit AWGN, $L = 300$, DWR=38 dB*

4.1 W-interp et Compensation des Distortions

Dans la technique de *binning* QIM [14], l'insertion consiste à quantifier I selon un pas de quantification Δ :

$$i_W(n_1, n_2) = Q_\Delta(i(n_1, n_2) + d) - d$$

où d contient l'information sur le message et Q_Δ est l'opérateur de quantification. La technique de compensation des distortions (DC-QIM) permet d'améliorer ses performances en présence de bruit AWGN. Son principe est le suivant : changer Δ en Δ/α, avec $\alpha < 1$, permet d'augmenter la robustesse d'un facteur $1/\alpha^2$, mais la distortion augmente également en $1/\alpha^2$. Pour conserver une distortion constante, on réintroduit donc une fraction $(1 - \alpha)$ de l'erreur de tatouage :

$$\begin{aligned} i_W(n_1, n_2) &= Q_{\Delta/\alpha}(i(n_1, n_2) + d) - d \\ &\quad + (1 - \alpha)(i(n_1, n_2) - Q_{\Delta/\alpha}(i(n_1, n_2) + d) - d). \end{aligned}$$

On calcule la valeur optimale de α en fonction de σ_B^2.
Cette idée peut être appliquée à W-interp : lorsque $\Delta_\mathcal{T}$ augmente à $N_\mathcal{S}$ constant, la distance entre les distribution de T sous H_0 et H_1 augmente, mais DWR diminue. Soient $\mathcal{T}'$ des paramètres tels que $\Delta_{\mathcal{T}'} > \Delta_\mathcal{T}$. On propose la stratégie d'insertion suivante sous H_1 :

$$\begin{aligned} i_W(n_1, n_2) &= \tilde{i}(n_1, n_2) + (1 - \alpha)(i(n_1, n_2) - \tilde{i}(n_1, n_2)) \\ &= i(n_1, n_2) + \alpha(\tilde{i}(n_1, n_2) - i(n_1, n_2)) \end{aligned}$$

Sous H_1, $R \sim \mathcal{N}(0, (1 + \Delta_{\mathcal{T}'})\sigma_B^2 + (1 - \alpha)^2\sigma_{\epsilon_I}^2)$: la distortion des compensations ajoute des interférences au décodage. Supposons l'influence $\sigma^2_{\epsilon_I(\mathcal{T}')}$ de $\mathcal{T}'$ sur ϵ_I connue. A distortion constante,

$$\alpha = \sqrt{\sigma^2_{\epsilon_I(\mathcal{T})}/\sigma^2_{\epsilon_I(\mathcal{T}')}}$$

η_{th} et le TEB dépendent des variances $(1 + \Delta_{\mathcal{T}'})\sigma_B^2$ et $(1 + \Delta_{\mathcal{T}'})\sigma_B^2 + (1 - \alpha)^2\sigma^2_{\epsilon_I(\mathcal{T}')}$. On peut donc calculer numériquement $\Delta_{\mathcal{T}^*}$ qui minimise ce TEB. En pratique, on peut fournir au décodeur une clé $\mathcal{T}$ ayant une distribution uniforme sur $[-1, 1]$. A l'insertion comme au décodage, il suffira ensuite de pondérer $\mathcal{T}$ par un paramètre a pour utiliser $\Delta_{\mathcal{T}^*}$.
En l'absence de modèle simple, on calcule numériquement $\sigma^2_{\epsilon_I(\mathcal{T}')}$ pour chaque image. Pour modéliser l'influence de $\mathcal{T}$ sur ϵ_I, on propose cependant d'utiliser le modèle de Markov-Gauss suivant : la différence U entre deux pixels de I voisins est supposée gaussienne centrée ($U \sim \mathcal{N}(0, \sigma_U^2)$) [15]. Sous l'hypothèse (abusive) d'indépendance des éléments de U, on peut montrer comme précedemment pour ϵ_B que

$$\sigma^2_{\epsilon_I(\mathcal{T})} = \Delta_\mathcal{T}\sigma_U^2$$

La validité de ce modèle dépend de I. Notamment, il est bien vérifié par l'image Lena lorsque $\Delta_\mathcal{T}$ est faible (cf Fig. 6). Les courbes théoriques des Figs 7 et 8 montrent que selon ce modèle, DC-W-bilin apporte une nette amélioration des performances. Les résultats expérimentaux utilisant $\Delta_{\mathcal{T}^*}$ calculé théoriquement grâce au modèle précédent confirment l'intérêt de DC-W-bilin (cf Fig. 9).

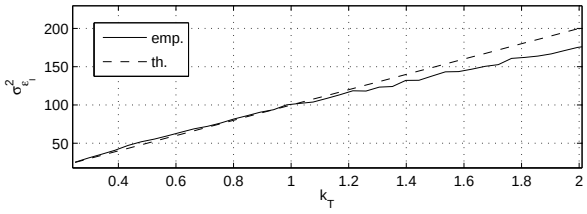

Figure 6 – $\sigma^2_{\epsilon_I}$ *en fonction de* $\Delta_\mathcal{T}$*, Lena*

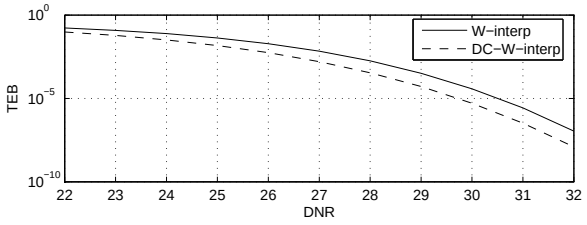

Figure 7 – *Amélioration des performances théoriques par DC-W-bilin, Lena, DWR=38 dB, $L = 256$, $P_\mathcal{S} = 178$*

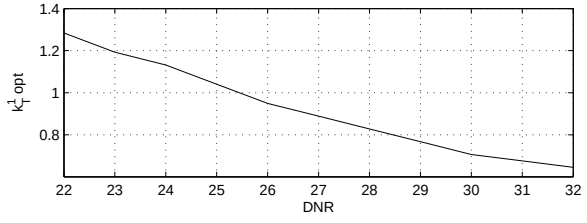

Figure 8 – *Choix optimal de $\Delta_\mathcal{T}$ pour DC-W-bilin, Lena, DWR=38 dB, $L = 256$, $P_\mathcal{S} = 178$*

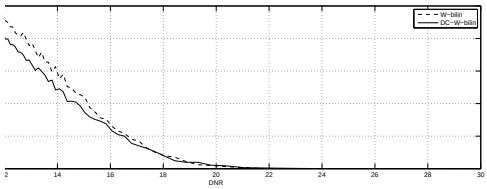

Figure 9 – *Amélioration des performances pratiques par DC-W-bilin, Lena, DWR=38 dB, $L = 256$, $P_\mathcal{S} = 178$*

4.2 Stratégies d'insertion informée

La stratégie d'insertion classique, utilisée également dans la version de base de W-bilin, consiste à maximiser la détection à distortion fixée. La connaissance du détecteur (et de ses performances théoriques) lors de l'insertion permet d'appliquer d'autres stratégies d'insertion, autour des critères de détection, distortion et robustesse [2][13]. La distortion sera mesurée ici par DWR. On choisit de mesurer la détection par la distance de Kullback-Leibler D_{KL}, dans le cas où σ_B^2 est nul. La robustesse est un critère à définir pour chaque technique. Pour DS, il s'agit de la puissance σ_B^2 de bruit qu'un pirate doit ajouter pour fausser le détecteur [2]. Pour W-bilin, le seuil η_{th} dépend déjà de σ_B^2. On préfère donc choisir comme critère de robustesse le TEB, calculé numériquement en fonction des distributions de T sous H_0 et H_1, à σ_B^2 connu.

Maximiser la robustesse à distortion constante. On veut minimiser le TEB à σ_B^2 donné et à distortion fixe. Alors DC-W-bilin constitue déjà une stratégie d'insertion pratique pour ce problème. Par contre, DC-W-bilin nuit à la détection (cf Fig 10 : sans DC, D_{KL} serait infini).

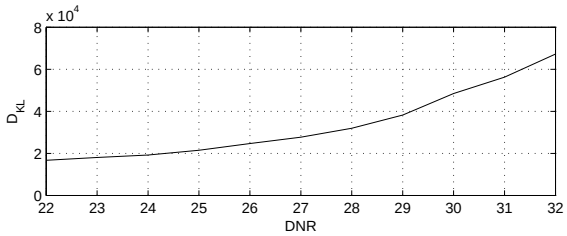

Figure 10 – *D_{KL} pour DC-W-bilin si l'attaque n'a pas lieu*

Minimiser la distortion à détection constante. Cette stratégie est inutile pour W-bilin car une détection parfaite ($D_{\text{KL}} = +\infty$) est possible pour tout DWR en changeant $N_{\mathcal{S}}$ (comme pour DC-W-interp, cette limitation de $\mathcal{S}$ peut se recalculer en réception).

Minimiser la distortion à robustesse constante. A DNR et TEB fixés, une diminution de $N_{\mathcal{S}}$, $\Delta_{\mathcal{T}}$ ou α permet de diminuer la distortion. Plusieurs stratégies sont possibles : diminuer $N_{\mathcal{S}}$, chercher le couple $(\alpha, \Delta_{\mathcal{T}})$ optimal à $N_{\mathcal{S}}$ fixé, ou bien ou effectuer une compensation des distortions sans contrepartie sur $\Delta_{\mathcal{T}}$: si $m(l) = 1$ on insère $i(n_1, n_2) + \alpha(\tilde{i}(n_1, n_2) - i(n_1, n_2))$, avec $\Delta_{\mathcal{T}} = 4/9$ et α variable. Cette technique permet d'améliorer DWR de façon significative, au prix d'une grande perte de performance de décodage (cf Fig. 11). On pourrait également combiner les trois techniques.

5 Etude de W-bilin

5.1 Imperceptibilité

La Fig. 12 montre un exemple de tatouage généré par W-bilin. Grâce à l'utilisation de l'interpolation, les plus grandes déformations sont situées dans les zones de plus

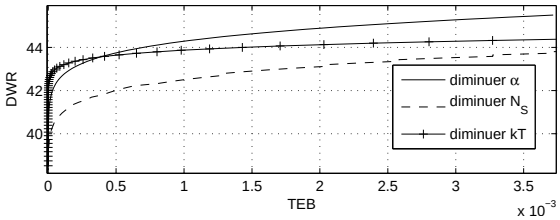

Figure 11 – *Maximisation de DWR en fonction du TEB, Lena, $L = 256$, WNR=-6 dB, $P_{\mathcal{S}} = 178$*

grande activité locale (contours, textures), là où elles sont le moins perceptible.
La qualité perceptuelle est confirmée par des mesures objectives. La Mesure de Similarité Structurelle (SSIM) [11] mesure la dégradation de l'information structurelle dans l'image, de 0 (pas de similarité) à 1 (pas de distortion). Les résultats expérimentaux (cf Tab.1) montrent que selon ce critère, W-bilin offre de meilleurs résultats que la technique DS classique combinée avec le masque de Fonction de Visibilité du Bruit (NVF) [12] ou à une insertion dans le domaine de la DCT avec un masque approprié [1].

DS	0.9827	DS+NVF	0.9897
DS+DCT	0.9897	W-bilin	0.9929

Tableau 1 – *Qualité perceptuelle selon le critère SSIM, DWR=38 dB*

La puissance d'insertion est contrôlée par le DWR. Le tatouage est imperceptible pour DWR>38 dB. Pour W-bilin,

$$\text{DWR} = \frac{2\sigma_I^2 N}{\sigma_{\epsilon_I}^2 N_{\mathcal{S}}}$$

Figure 12 – *Lena (détail) : originale, tatouée et tatouage, DWR=38 dB*

5.2 Robustesse

W-bilin est particulièrement robuste au débruitage car W est très corrélé à I, donc difficile à estimer (cf Fig. 13). Sa robustesse à la compression JPEG et à l'égalisation d'histogramme est également montrée sur les Figs. 14 et 15. Par contre, W-bilin est sensible aux attaques désynchronisantes telles qu'une rotation. Même en cas de resynchronisation, l'attaque géométrique génère un bruit d'interpolation qui gêne le décodage. Des techniques de resynchronisation exploitant les spécificités de W-bilin sont à l'étude.

5.3 Sécurité

La sécurité de W-bilin repose sur les paramètres $K = \{\mathcal{S}, \mathcal{T}\}$. S'il ne connaît pas les décalages $\mathcal{T}$, un pirate ne peut pas décoder M à partir de I_W. En effet, on peut montrer que pour la distribution de $\mathcal{T}$ utilisée ici, l'emploi de

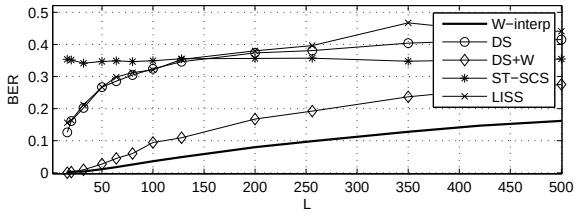

Figure 13 – *Robustesse au débruitage, DWR=38 dB*

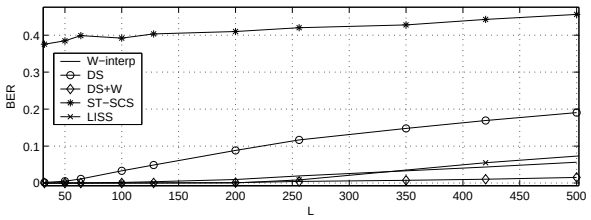

Figure 14 – *Robustesse à l'égalisation d'histogramme, DWR=38 dB*

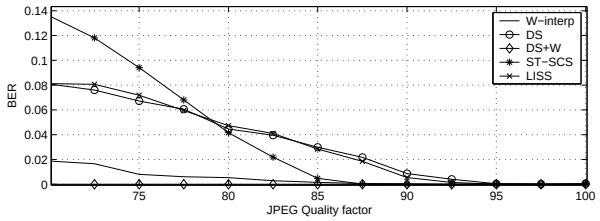

Figure 15 – *Robustesse à la compression JPEG,* $L = 64$*, DWR=38dB*

mauvais paramètres introduit un bruit d'estimation de l'interpolation de variance $\sigma_S^2 = \frac{7}{8}\sigma_{\epsilon_I}^2$. Par contre, s'il a accès à $N_o > 1$ images tatouées avec la même clé, le pirate peut essayer d'estimer K car l'insertion du tatouage a modifié la distribution d'une erreur d'interpolation. Notamment, un algorithme d'Estimation-Maximisation (EM) a été proposé pour estimer simultanément $\mathcal{S}$ et $\mathcal{T}$ [9].

6 Conclusion

W-interp est un algorithme de tatouage utilisant l'interpolation bilinéaire, qui offre des propriétés intéressantes d'imperceptibilité, de sécurité et un rejet des interférences de l'image hôte. W-interp est robuste à des attaques de faible puissance. Il s'agit d'une technique de codage informé, car le tatouage est construit à partir de l'hôte. Afin de tirer profit de la connaissance des performances théoriques du détecteur lors de l'insertion, on a proposé dans cet article d'utiliser des stratégies d'insertion informée. Notamment, la compensation des distortions, similaire à celle des algorithmes quantificatifs, permet d'améliorer significativement les performances de décodage. Elle rejoint la stratégie de maximisation de la robustesse à distortion constante.

Références

[1] J.R. Hernández et F. Pérez-González. Statistical analysis of watermarking schemes for copyright protection of images. *IEEE Proc., Special Issue on Identification and Protection of Multimedia Information*, 87(7) :1142–1166, 1999.

[2] M.L. Miller, I.J. Cox, et J.A. Bloom. Informed embedding : Exploiting image and detector information during watermark insertion. *IEEE Int. Conf. on Image Processing - ICIP*, 3 :1–4, 2000.

[3] H.S. Malvar et D.A.F. Florêncio. Improved spread spectrum : a new modulation technique for robust watermarking. *IEEE Trans. on Signal Processing*, 51(4) :898–905, 2003.

[4] P. Moulin et R. Koetter. Data-hiding codes. *Proc. of the IEEE*, 93(12) :2083–2127, 2005.

[5] J.J. Eggers, R. Bauml, R. Tzschoppe, et B. Girod. Scalar Costa Scheme for Information Embedding. *IEEE Trans. on Signal Processing*, 51(4) :1003–1019, 2003.

[6] P. Thévenaz, T. Blu, et M. Unser. Image interpolation and resampling. Dans I. Bankman, éditeur, *Handbook of Medical Imaging, Processing and Analysis*, chapitre 25, pages 393–420. Acad. Press, San Diego, USA, 2000.

[7] R. Ohbuchi, H. Masuda, et M. Aono. A Shape-Preserving Data Embedding Algorithm for NURBS Curves and Surfaces. *Proc. of the Comp. Graphics Int. (CGI)*, pages 170–177, 1999.

[8] G. Boato, C. Fontanari, et F. Melgani. Hierarchical deterministic image watermarking via polynomial interpolation. *Proc. of ICIP*, 2005.

[9] V. Martin, M. Chabert, et B. Lacaze. Substitutive watermarking algorithms based on interpolation. *Proc. of EUSIPCO*, 2006.

[10] V. Martin, M. Chabert, et B. Lacaze. A novel watermarking scheme based on interpolation for digital images. *Proc. of ICASSP*, 2006.

[11] Zhou Wang, A.C. Bovik, H.R. Sheikh, et E.P. Simoncelli. Image quality assessment : From error visibility to structural similarity. *IEEE Trans. on Image Proc.*, 13 :600–612, 2004.

[12] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, et T. Pun. A stochastic approach to content adaptive digital image watermarking. *International Workshop on Information Hiding*, pages 212–236, 1999.

[13] J. Delhumeau, T. Furon, N. Hurley, et G. Silvestre. Improved polynomial detectors for side-informed watermarking. *Proc. SPIE*, 2003.

[14] B. Chen et G.W. Wornell. Quantization index modulation : A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. on Information Theory*, pages 1423–1443, 2001.

[15] K. Sullivan, U. Madhow, S. Chandrasekaran, et B. S. Manjunath. Steganalysis of spread spectrum data hiding exploiting cover memory. *Proc. SPIE*, pages 38–46, 2005.