Compromis sécurité / robustesse en resynchronisation pour le tatouage

François Cayre, Cléo Baras, Vincent del Medico

Compromis sécurité / robustesse en resynchronisation pour le tatouage

F. Cayre[1] C. Baras[1] V. Del Medico[1]

[1] GIPSA-Lab, DIS, équipe C2S

Domaine Universitaire, 961 rue de la Houille Blanche – BP46

F-38402 St-Martin d'Hères CEDEX

{francois.cayre,cleo.baras}@gipsa-lab.inpg.fr, vincent.del.medico@gmail.com

Résumé

Nous présentons la problématique qui se pose en tatouage numérique lors de la resynchronisation, et la faille de sécurité récurrente dans les méthodes de l'état de l'art. Nous proposons une méthode de resynchronisation simple pour circonvenir cette faille, et présentons les résultats préliminaires que nous avons obtenus.

Mots clefs

Tatouage numérique, resynchronisation, sécurité.

1 Introduction

Le tatouage permet d'insérer une marque imperceptible dans un document numérique, et a pour vocation différentes applications de protection des droits (identification du propriétaire) ou de protection de la copie (droits d'utilisation), etc. La conception d'un système de tatouage doit alors prendre en compte l'intervention d'un adversaire (un individu malintentionné) qui chercherait :

– par différentes attaques (de robustesse), à outrepasser la protection du document offerte par le tatouage,
– voire à retourner à son profit la technique de tatouage (attaques de sécurité) en estimant le secret utilisé pour paramétrer l'algorithme de tatouage.

Schématiquement, du point de vue des attaques de robustesse, le système de tatouage doit faire face à deux grandes familles d'attaques :

1. les attaques de type "filtrage", dans lesquelles on peut classer des manipulations comme la compression ou le débruitage ;
2. les attaques de type "désynchronisation", qui concernent toutes les manipulations qui viennent modifier la grille d'échantillonnage. Par exemple, dans le cas de signaux audio : l'étirement temporel ou le fenêtrage et dans le cas des images, la mise à l'échelle, la rotation, etc.

Le problème de la désynchronisation reste actuellement un vaste sujet de recherche en tatouage, d'autant qu'elle permet un effacement à moindre coût du signal de tatouage. En effet, dans les schémas de tatouage à quantification de type QIM/SCS [1], on perd la synchronisation avec les coefficients auxquels appliquer le jeu de quantificateurs. Dans les schémas par étalement de spectre [2], c'est l'étape de corrélation qui souffre de la désynchronisation, et la réponse du détecteur devient quasi-nulle. Ce problème n'a pour l'instant été abordé que sous l'angle de la robustesse : plusieurs mécanismes de resynchronisation ont été proposés pour permettre la détection correcte du tatouage même en présence d'attaques désynchronisantes. L'angle de la sécurité n'a été que peu considéré [3].

Dans cet article, nous nous intéressons plus particulièrement au mécanisme de resynchronisation d'un schéma de tatouage par étalement de spectre, conçu dans un but de *détection*, c'est-à-dire où l'on ne cherchera qu'à décider si oui ou non un signal contient un autre signal, de tatouage, supposé secret. Les mécanismes de synchronisation proposés dans la littérature présentent une faille de sécurité majeure, qui laisse penser qu'un adversaire disposant de plusieurs contenus tatoués (cadre Watermark-Only-Attack [4]) pourrait estimer le secret sur lequel repose le tatouage.

Nous limiterons le cadre des attaques à deux types de désynchronisation (qui font sens en pratique, par exemple pour les signaux audio) : l'étirement uniforme d'un facteur α du signal tatoué, et le fenêtrage (i.e. l'extraction d'une partie du signal tatoué).

Dans une première partie, nous mettrons en évidence la faille de sécurité des systèmes de synchronisation pour les schémas additifs par étalement de spectre. Nous en déduirons une nouvelle technique de resynchronisation, décrite dans une deuxième partie. Puis nous présenterons les résultats expérimentaux, mettant en évidence les performances de notre méthode pour la détection et la resynchronisation du tatouage.

2 Position du problème

2.1 Notations

Formellement, on dénote par $\mathbf{x}$ un signal hôte, de durée N échantillons, dans lequel cacher un signal de tatouage $\mathbf{w}$ (de durée N) pour obtenir le signal tatoué $\mathbf{y}$ (de durée N) :

$$\mathbf{y} = \mathbf{x} + \mathbf{w}.$$

La distorsion d'insertion est caractérisée par WCR, le rapport de puissance suivant :

$$WCR_{dB} = 10\log_{10}\left(\frac{\sigma^2_{\mathbf{w}}}{\sigma^2_{\mathbf{x}}}\right).$$

La statistique utilisée pour tester la présence du signal de tatouage est basée sur la corrélation.

2.2 Stratégies pour la resynchronisation

Nous discutons ici les différentes stratégies proposées dans la littérature pour la resynchronisation, en nous plaçant du point de vue d'un signal monodimensionnel, même si certaines des stratégies proposées ont été développées spécifiquement pour l'image.

Domaine invariant. Les stratégies basées sur un domaine invariant (par ex. [5]) consistent à effectuer le tatouage dans un espace invariant à certaines manipulations. Elles limitent donc *de facto* les manipulations autorisées auxquelles le système de tatouage peut être robuste.
D'un point de vue sécurité, le domaine d'insertion étant supposé connu de l'adversaire, on retrouve la situation classique pour laquelle les attaques de sécurité proposées dans [4] sont possibles, étant admis qu'elles se fondent sur le fait qu'aucune resynchronisation n'est nécessaire (ou, ce qui est équivalent, qu'elle a déjà été effectuée).

Recherche exhaustive. Les stratégies par recherche exhaustive [6] proposent de tester toutes les manipulations possibles parmi celles autorisées (et tous leurs paramètres). Elle offre actuellement le niveau de sécurité le plus elevé. On peut en effet considérer que la sécurité est essentiellement fonction du WCR, de l'ensemble des attaques de désynchronisation admises, et de la discrétisation de l'espace des paramètres des attaques : par exemple, pour une opération d'étirement du signal $\mathbf{y}$, la stratégie de resynchronisation teste dans ce cas les N décalages possibles, et ce sur tous les facteurs d'étirement autorisés. Une stratégie simple pour contrer les attaques proposées par [4] consiste alors à distribuer des contenus $\mathbf{y}$ tatoués avec des $\mathbf{w}$ ayant déjà subi de petites désynchronisations.
Néanmoins, le coût de cette stratégie au moment de la détection est généralement considéré comme prohibitif, l'excluant généralement des implémentations pratiques.

Structure périodique dans le spectre d'autocorrélation. Cette stratégie [7], sur laquelle notre étude se focalise, est actuellement la plus usitée et la plus prometteuse : en effet, elle est aujourd'hui la plus robuste et permet d'inverser la plupart des désynchronisations usuelles. Néanmoins elle présente un trou de sécurité évident.
Initialement développée pour l'image, elle consiste à répéter périodiquement (tous les N_p échantillons) un signal élémentaire de tatouage (ou *pattern*) $\mathbf{p}$, de durée N_p, pour créer le signal de tatouage $\mathbf{w}$:

$$\mathbf{w}(n) = \sum_{i=0}^{P-1} \mathbf{p}(n - iN_p)\Pi_{N_p}(n - iN_p) = \mathbf{p}(n\%N_p),$$

où Π_{N_p} désigne la fonction porte de durée N_p[1], P est le nombre de fois où le pattern $\mathbf{p}$ est inséré, et $\%$ désigne l'opérateur modulo.
Cette structure particulière de $\mathbf{w}$ laisse apparaître une structure périodique dans le spectre d'autocorrélation de $\mathbf{y}$, que le détecteur met à profit pour inverser les désynchronisations subies par le tatouage : la période initiale étant connue, un simple rapport avec la période observée après désynchronisation permet d'estimer le facteur d'étirement α qui a été appliqué à $\mathbf{y}$. Ensuite, le détecteur teste toutes les corrélations avec $\mathbf{p}$ pour retrouver le fenêtrage éventuellement subi par $\mathbf{y}$, puis procède à la décision.
Cette structure périodique du spectre d'autocorrélation peut également être utilisée par l'adversaire : il peut bien évidemment, une fois l'étirement temporel inversé et le fenêtrage annulé, construire l'estimateur suivant :

$$\hat{\mathbf{p}}(n) = \frac{1}{P}\sum_{i=0}^{P-1} \mathbf{y}(n + iN_p),$$

et donc estimer l'unique secret (le pattern) de l'algorithme de tatouage. Cette stratégie présente donc une faille de sécurité majeure.

2.3 Synchronisation et sécurité

Augmenter le niveau de sécurité des techniques de resynchronisation en tatouage peut alors être vu, soit comme devoir augmenter le niveau de sécurité de la méthode par répétition périodique, soit comme devoir augmenter la robustesse et la vitesse de resynchronisation de la méthode par recherche exhaustive.

3 Méthode proposée

Nous proposons ici une variation très simple de la méthode de resynchronisation par répétition. Cette variation consiste à répéter le signal élémentaire $\mathbf{p}$ non plus de manière périodique, mais de manière aléatoire[2], autorisant même que ces signaux élémentaires se superposent dans le signal de tatouage.
Bien évidemment, la structure périodique dans le spectre d'autocorrélation de $\mathbf{y}$ disparaît *de facto*, supprimant ainsi la faille de sécurité de la technique par répétition *périodique*. D'autres approches, assez peu robustes, ont été développées par le passé pour masquer le dispositif de synchronisation [3]. Ce travail s'inscrit dans cette veine, à la différence que nous souhaitons nous appuyer sur des développements menant à des performances quantifiables.

3.1 Construction du signal de tatouage

Notons $(\delta_i)_{i=0..P-1}$ une suite de P entiers relatifs choisis de manière uniformément aléatoire dans $[-RN_p; RN_p]$

[1] avec $\Pi_{N_p}(n) = 0$ si $n < 0$ ou $n \geq N_p$ et $\Pi_{N_p}(n) = 1$ sinon

[2] ou pseudo-aléatoire, faisant l'objet d'une clé secrète dite de synchronisation connue du seul propriétaire du document et à ne pas divulguer ; mais on montrera par la suite que la connaissance de cette clé n'est pas nécessaire au détecteur.

(avec $R \in]0,1]$). Chaque point de cette suite indique la position des P patterns insérées dans le signal de tatouage $\mathbf{w}$. Ce dernier est alors construit à partir de $\mathbf{p}$ de la façon suivante :

$$\mathbf{w}(n) = \sum_{i=0}^{P-1} \mathbf{p}(n - \delta_i - iN_p)\Pi_{N_p}(n - \delta_i - iN_p).$$

Plusieurs patterns (par exemple, la i-ème et la $i+1$-ème) peuvent donc :
- tantôt être distants de plusieurs échantillons (cas où $\delta_{i+1} - \delta_i > 0$), rendant certaines parties du signal de tatouage nulles,
- tantôt se chevaucher sur plusieurs échantillons du signal tatoué $\mathbf{y}$ (cas où $\delta_{i+1} - \delta_i < 0$). Pour des raisons de simplicité, on supposera que ces chevauchements ne peuvent pas impliquer plus de deux patterns.

Finalement, à un instant n proche de l'instant $\delta_i + iN_p$ où débute la i-ème pattern, en considérant le chevauchement éventuel induit par la présence des autres patterns (notamment la $i+1$-ème), le signal tatoué $\mathbf{y}$ s'écrira :

$$\mathbf{y}(n) = \mathbf{p}(n\%N_p) + \mathbf{x}(n) + \underbrace{\mathbf{p}(n - (\delta_{i+1} - \delta_i) - N_p\%N_p)}_{\mathbf{b}(n)}.$$

Nous noterons $\mathbf{b}$ le bruit engendré par une pattern pouvant se superposer à la pattern considérée et on appellera par la suite *bruit de recouvrement*.

3.2 Modélisation des attaques de désynchronisation

Les attaques envisagées ici sont :
- un étirement de l'échelle des indices des échantillons, pouvant être réalisé aussi bien par des techniques d'interpolation classique que par un rééchantillonnage du signal (après conversion du signal numérique en signal analogique),
- le fenêtrage. Signalons le peu d'importance du fenêtrage, pour des raisons qui deviendront plus claires par la suite, nous autorisant à nous concentrer sur l'étirement temporel.

On suppose donc que l'attaque par étirement de l'échelle des indices est uniquement paramétrée par un facteur d'étirement α, inconnu du détecteur. Le signal tatoué y obtenu après étirement et noté $\hat{\mathbf{y}}^{(\alpha)}$ voit sa durée passer de N à $N^{(\alpha)} = (1+\alpha)N$ échantillons.

3.3 Détecteur

Le problème de la détection *combiné à celui de la resynchronisation* se ramène alors à estimer au mieux le facteur d'étalement α et à déterminer la présence ou non du tatouage (sous la forme des P signaux élémentaires $\mathbf{p}$).

Analyse de la corrélation en présence d'un tatouage. La détection reste fondée sur un calcul de corrélation entre la pattern $\mathbf{p}$ supposée connue du détecteur et le signal tatoué étiré $y^{(\alpha)}$. Diverses études [8] ont déjà montré que la corrélation est d'autant plus fiable que la pattern $\mathbf{p}$ est préalablement étirée du même facteur d'étalement que celui appliqué au signal tatoué $y^{(\alpha)}$[3]. Ce dernier étant pour l'instant inconnu, nous introduisons la corrélation entre la pattern $\mathbf{p}$ étirée d'un facteur β, notée $\mathbf{p}^{(\beta)}$, de durée $N_p^{(\beta)} = (1-\beta)N_p$, et le signal tatoué étiré $\mathbf{y}^{(\alpha)}$ analysé à partir de l'échantillon n :

$$C_n^{(\beta)} = \langle \mathbf{p}^{(\beta)} | \mathbf{y}^{(\alpha)}[n] \rangle = \frac{1}{N_p^{(\beta)}} \sum_{i=0}^{N_p^{(\beta)}-1} \mathbf{p}^{(\beta)}(i)\mathbf{y}^{(\alpha)}(n+i) \tag{1}$$

Décider au regard de cette corrélation $C_n^{(\beta)}$ si le signal tatoué contient une pattern à la position n relève d'un test d'hypothèse conditionné par le facteur d'étalement β :
- H_0 : Aucune pattern n'est insérée à partir de l'échantillon n dans le signal tatoué étiré ;
- H_1 : Une pattern est insérée à partir de l'échantillon n dans le signal tatoué étiré.

Sous l'hypothèse H_0, le signal tatoué étiré ne contenant pas de pattern à partir de l'échantillon n, la corrélation se réduit donc à :

$$\begin{aligned} C_n^{(\beta)} &= \langle \mathbf{p}^{(\beta)} | \mathbf{x}^{(\alpha)}[n] \rangle + \langle \mathbf{p}^{(\beta)} | \mathbf{b}^{(\alpha)}[n] \rangle \\ &= \frac{1}{N_p^{(\beta)}} \sum_{i=0}^{N_p^{(\beta)}-1} \mathbf{p}^{(\beta)}(i)\mathbf{x}^{(\alpha)}(n+i) + \\ &\quad \frac{1}{N_p^{(\beta)}} \sum_{i=0}^{N_p^{(\beta)}-1} \mathbf{p}^{(\beta)}(i)\mathbf{b}^{(\alpha)}(n+i) \end{aligned}$$

où $\mathbf{x}^{(\alpha)}[n]$ (resp. $\mathbf{b}^{(\alpha)}[n]$) est le signal hôte (resp. le bruit de recouvrement) étiré du facteur α et analysé à partir de l'échantillon n.

À supposer que $\mathbf{x}$ suive une loi normale centrée et de variance $\sigma_{\mathbf{x}}^2$, on peut montrer que la statistique de $\langle \mathbf{p}^{(\beta)} | \mathbf{x}^{(\alpha)}[n] \rangle$ suit une loi normale de moyenne nulle et de variance $\sigma_{\mathbf{x}}^2 \sigma_{\mathbf{p}}^2 / N_p^{(\beta)}$. De la même façon, au regard du recouvrement uniformément aléatoire entre les patterns, on montre qu'en première approximation $\langle \mathbf{p}^{(\beta)} | \mathbf{b}^{(\alpha)}[n] \rangle$ suit une loi normale centrée et de variance $R\sigma_{\mathbf{p}}^4 / N_p^{(\beta)}$.

Finalement, puisque les patterns sont réputées être insérées de manière indépendante à la fois entre elles et par rapport à $\mathbf{x}$, la statistique de la corrélation $C_n^{(\beta)}$ est :

$$C_n^{(\beta)} \sim \mathcal{N}\left(0, {\sigma_c^{(\beta)}}^2\right), \text{ avec } {\sigma_c^{(\beta)}}^2 = \frac{(\sigma_{\mathbf{x}}^2 + R\sigma_{\mathbf{p}}^2)\sigma_{\mathbf{p}}^2}{N_p^{(\beta)}} \tag{2}$$

Sous l'hypothèse H_1, la corrélation s'incrémente d'un terme, lié à la présence de la pattern $\mathbf{p}$ à l'échantillon n :

$$\begin{aligned} C_n^{(\beta)} = \; & \langle \mathbf{p}^{(\beta)} | \mathbf{p}^{(\alpha)} \rangle \\ & + \langle \mathbf{p}^{(\beta)} | \mathbf{x}^{(\alpha)}[n] \rangle + \langle \mathbf{p}^{(\beta)} | \mathbf{b}^{(\alpha)}[n] \rangle. \end{aligned}$$

[3] De même en image [7], on suréchantillonne couramment la pattern. On considérera donc cette étude comme étant réalisée "au pire des cas".

Sa moyenne en est modifiée, puisqu'elle prend désormais en compte la valeur de la corrélation de la pattern avec elle-même (i.e. $\sigma^2_{\mathbf{p}}$ en négligeant ici les effets de l'étirement) Finalement, la statistique de la corrélation devient en première approximation :

$$C_n^{(\beta)} \sim \mathcal{N}\left(0, {\sigma_c^{(\beta)}}^2\right). \quad (3)$$

On peut alors fixer un seuil de décision τ au dessus duquel la corrélation obtenue indique la présence d'une pattern insérée à partir d'une position n dans le signal. Ce seuil est lié à une probabilité de fausse alarme p_{fa}, fixant la probabilité de commettre une erreur dans la décision[4]. En utilisant la relation classique liant la probabilité de fausse alarme et le seuil de décision en présence de variables aléatoires gaussiennes, on déduit :

$$\tau = \sqrt{2\,{\sigma_c^{(\beta)}}^2}\,\mathrm{erf}^{-1}\left(1-2p_{fa}\right),$$

où erf est la fonction d'erreur classique.

Estimateur du facteur d'étirement. Étant donnée la méthode d'insertion des P patterns dans le signal tatoué, pour chaque valeur du facteur d'étalement β testé, si l'on calcule la corrélation $C_n^{(\beta)}$ pour chaque échantillon n du signal tatoué étiré, on s'attend à dénombrer P valeurs de corrélations supérieures à τ lorsque le signal est tatoué et aucune lorsque le signal ne l'est (aux erreurs de décision près liées à la p_{fa} et à la probabilité d'erreur sur la détection des patterns).
L'estimateur du facteur d'étalement est donc construit de la façon suivante. Pour chaque valeur du facteur d'étirement β testée, les corrélations $C_n^{(\beta)}$ sont ajoutées dès qu'elles sont supérieures au seuil τ :

$$S(\beta) = \sum_{n\in\mathcal{C}^{(\beta)}} C_n^{(\beta)}$$
$$\text{avec } \mathcal{C}^{(\beta)} = \{n \in [0..N^{(\alpha)}-1]/C_n^{(\beta)} \geq \tau\}$$

On notera $\hat{P}(\beta) = \mathrm{Card}(\mathcal{C}^{(\beta)})$ le nombre de corrélations $C_n^{(\beta)}$ supérieures à τ pour la valeur β testée, autrement dit, le nombre de patterns détectées dans le signal $\mathbf{y}^{(\alpha)}$.
Le facteur d'étalement estimé $\hat{\alpha}$ est finalement la valeur de β maximisant la somme des corrélations supérieures à τ :

$$\hat{\alpha} = \mathrm{argmax}_\beta S(\beta) \quad (4)$$

Détection du tatouage. Une fois le facteur d'étirement $\hat{\alpha}$ estimé, la décision sur la présence d'un tatouage dans le signal peut être prise directement à partir de la somme des corrélations $S(\hat{\alpha})$ et du nombre de patterns détectées $\hat{P}(\hat{\alpha})$. Nous avons choisi de considérer la valeur moyenne des corrélations détectées :

$$C_{moy} = \frac{S(\hat{\alpha})}{\hat{P}(\hat{\alpha})},$$

et de fixer un seuil de décision à $1/2$:

- Si $C_{moy} \geq 1/2$, le détecteur décide que le signal est tatoué ;
- Si $C_{moy} < 1/2$, le détecteur décide que le signal n'est pas tatoué.

Cette manière de combiner les micro-décisions pour former la décision globale est intuitive, mais fondée sur le sentiment que plus on a de corrélations qui dépassent τ, moins on commettra d'erreurs en décidant la présence de $\mathbf{p}$ dans $\mathbf{x}$. Ce critère présente deux particularités :

- contrairement aux stratégies de l'état de l'art, il ne nécessite pas de localiser précisement la position des patterns dans le signal avant de prendre une décision sur la présence du tatouage ;
- il est indépendant du nombre de patterns insérées dans le signal et donc du fenêtrage effectué par l'adversaire.

4 Résultats expérimentaux

4.1 Estimateur du facteur d'étirement α

On s'intéresse aux performances de l'estimateur du facteur d'étirement établi Eq. (4).
Le signal hôte $x \sim \mathcal{N}(0, \sigma^2_{\mathbf{x}})$ de durée $N = 1000$ est ici tatoué par $P = 3$ patterns de durée $N_p = 256$ de sorte que le WCR soit égal à -10 dB. Une interpolation cubique du signal tatoué est ensuite effectuée avec différents facteurs d'étirement α compris entre -0.2 et 0.2[5]. Le détecteur détermine finalement le facteur d'étirement estimé $\hat{\alpha}$ en effectuant une recherche exhaustive de sa valeur dans $[-0.2; 0.2]$ avec un pas de 0.01. Le lecteur aura noté que l'on conserve la complexité de la recherche exhaustive, mais que l'on diminue la taille du problème, puisqu'elle est appliquée à $\mathbf{p}$ et non plus à $\mathbf{y}$.
La Fig. 1 présente la fonction de répartition de l'erreur absolue e d'estimation, c'est-à-dire $e = |\alpha - \hat{\alpha}|$, lorsque α varie dans $[-0.2; 0.2]$, et lorsque la probabilité de fausse alarme p_{fa} sur la micro-détection des patterns dans le signal est fixée à 5.10^{-4}. On constate donc que dans 80% des cas, l'erreur d'estimation sur le facteur d'étirement est inférieure au pas de recherche, i.e. à 10^{-2}.

4.2 Détection du tatouage

Cette section est consacrée à la performance de détection du tatouage, en présence d'une attaque désynchronisante. Lorsque le signal est tatoué, $P = 6$ patterns $\mathbf{p} \sim \mathcal{N}(0, \sigma^2_{\mathbf{p}})$ de durée $N_p = 256$ sont insérées dans un signal hôte $x \sim \mathcal{N}(0, \sigma^2_{\mathbf{x}})$ de durée $N = 2000$ échantillons avec un facteur de recouvrement $R = 0.05$. La probabilité de fausse alarme p_{fa} prise en compte pour la détection des patterns est fixée à 10^{-6}. La désynchronisation est provoquée par une interpolation cubique du signal tatoué avec un facteur d'étirement α. Les résultats présentés sont obtenus après moyennage sur 10000 simulations. Chaque simulation dure moins de 0.1 seconde sur une machine classique.
La Fig. 2 présente la probabilité d'erreur concernant la dé-

[4] Autrement dit, de décider la présence d'une pattern là où aucune n'a été insérée effectivement.

[5] Ces limites étant courantes lorsqu'on traite des signaux audio.

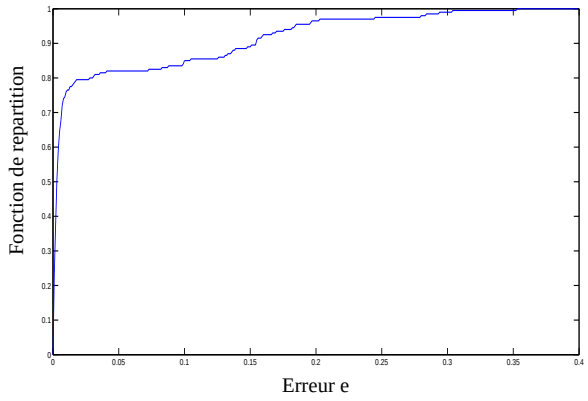

Figure 1 – *Fonction de répartition de l'erreur absolue sur l'estimation du facteur d'étirement.*

cision sur la présence d'un tatouage[6] en fonction du WCR et pour différentes valeurs de α. Notons, que dans le pire cas (ici pour un WCR de -20 dB), la probabilité de fausse alarme de détection du tatouage[7] est de $3.4\,10^{-2}$; pour des WCR supérieurs à -14 dB, elle devient nulle (à l'erreur de précision près, due au choix des paramètres de simulation). On remarque que les facteurs d'étirement négatifs (induisant une compression du signal) ont une influence plus importante que les facteurs positifs (provoquant une expansion du signal) sur les performances du détection. Un système pratique utiliserait vraisemblablement un suréchantillonnage de $\mathbf{p}$ pour pallier ce défaut.

5 Conclusions et perspectives

Nous avons présenté une manière de circonvenir le trou de sécurité inhérent aux méthodes de resynchronisation basées sur l'ajout périodique de patterns lorsqu'elles doivent faire face à un étirement uniforme et un fenêtrage du signal tatoué. Cette méthode utilise ces même patterns mais les introduit de manière aléatoire dans le signal hôte ; elle se base sur une estimation du facteur d'étirement et sur une décision simultanée de la présence du tatouage (indépendamment du fenêtrage). Ce détecteur requiert une recherche exhaustive du facteur d'étirement mais, contrairement aux stratégies de la littérature, effectue cette recherche sur des signaux de taille bien plus petite. Toutefois, en dépit des résultats préliminaires plus que prometteurs exposés ici, il reste encore :

– à relier plus précisément la probabilité de fausse alarme prise sur les micro-décisions (de présence des patterns) à la probabilité de fausse alarme globale de présence du tatouage ;
– à préciser davantage le niveau de sécurité offert par cette méthode ;
– à l'appliquer sur des signaux réels 1D (de type audio) puis à le généraliser à des signaux 2D.

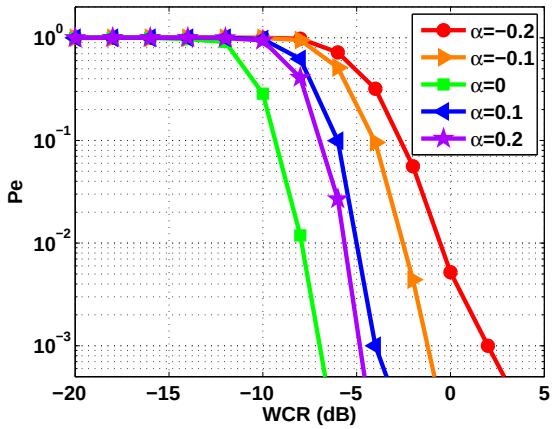

Figure 2 – *Probabilité d'erreur concernant la décision sur la présence du tatouage.*

[6] Autrement dit, lorsque le détecteur décide que le signal analysé n'est pas tatoué alors qu'il l'est en réalité.

[7] Autrement dit, lorsque le détecteur décide que le signal analysé est tatoué alors qu'il ne l'est pas en réalité.

Références

[1] J. Eggers, R. Bäuml, et B. Girod. Scalar costa scheme for information embedding. *IEEE Trans. on Signal Processing*, 51 :1003–1019, 2003.

[2] T. Furon. A constructive and unifying framework for zero-bit watermarking. *IEEE Trans. on Information Forensics and Security*, 2(2) :149–163, 2007.

[3] D. Delannay et B. Macq. Method for hiding synchronization marks in scale and rotation resilient watermarking schemes. Dans *Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, San Jose, CA, USA, 2002.

[4] F. Cayre, C. Fontaine, et T. Furon. Watermarking security : Theory and practice. *IEEE Trans. Signal Processing*, 53(10) :3976–3987, 2005.

[5] H.-S. Kim et H.-K. Lee. Invariant image watermark using Zernike moments. *IEEE Trans. on Circuits and Systems for Video Technology*, 13(8) :766–775, 2003.

[6] M. Barni. Effectiveness of exhaustive search and template matching against watermark desynchronization. *IEEE Sig. Proc. Letters*, 12(2) :158–161, 2005.

[7] F Deguillaume, S Voloshynovskiy, et T Pun. Method for the estimation and recovering from general affine transforms in digital watermarking applications. Dans *Electronic Imaging 2002, Security and Watermarking of Multimedia Contents IV*, San Jose, CA, USA, 2002.

[8] C. Baras, N. Moreau, et B. Zayen. Mécanisme de synchronisation dans des systèmes de tatouage audio pour des perturbations désynchronisantes à forte dérive. Dans *GRETSI*, Louvain-la-Neuve, Belgique, 2005.