Problématique de la Collusion en Tatouage Vidéo

Collusion Issue in Video Watermarking

Gwenaël Doërr et Jean-Luc Dugelay
Institut Eurécom – Département des Communications Multimédia
2229 route des Crêtes – B.P. 193
06904 Sophia-Antipolis Cédex
{doerr, dugelay}@eurecom.fr

Résumé : *L'évaluation de la sécurité des algorithmes de tatouage est récemment devenue une préoccupation majeure et, dans ce contexte, il est pertinent de considérer les attaques par collusion. Ces attaques combinent plusieurs documents tatoués pour produire des documents non tatoués. En vidéo, une telle stratégie est d'autant plus dangereuse que chaque trame vidéo peut être vue comme un document tatoué. Après avoir souligné différentes faiblesses face à ce type d'attaque, une nouvelle stratégie de tatouage cohérente avec le signal porteur est présentée. Le but est de générer un signal de tatouage qui soit en accord avec la redondance du signal vidéo à tatouer, que cette redondance soit temporelle ou spatiale, de sorte que ce signal de tatouage survive aux attaques par collusion.*
Mots clefs : Tatouage, vidéo, sécurité, attaques, collusion.

Abstract : *Security evaluation of released watermarking algorithms has recently become a major concern. In this perspective, it is worth evaluating the importance of the threat of collusion attacks. These attacks combine several watermarked documents to produce unwatermarked content. In video, such a strategy is all the more critical since each individual video frame can be seen as a single watermarked document. Once different weaknesses against collusion attacks have been exhibited, a novel signal coherent watermarking strategy is presented. The goal is to generate a watermark signal coherent with the redundancy of the host video signal, should it be temporal or spatial, so that the embedded watermark is immune against collusion attacks.*
Keywords : Watermarking, video, security, attacks, collusion.

---

1 Introduction

La fin du XXème siècle a vu le monde basculer de l'analogique au numérique et les équipements numériques (lecteurs CD/DVD, ordinateurs, assistants personnels, baladeurs) sont aujourd'hui de plus en plus répandus. Néanmoins, cette formidable révolution technique ne s'est pas faite sans susciter quelques inquiétudes, tout particulièrement en termes de protection des droits numériques. Les copies numériques sont désormais parfaites alors qu'auparavant, chaque génération de copies analogiques introduisait une dégradation supplémentaire. De plus, les réseaux d'échange de fichiers pair à pair permettent d'échanger facilement de très grands volumes de données multimédia. Ainsi, les fournisseurs de contenus ont rapidement vu leurs ventes chuter de façon significative [1]. Ces derniers sont donc très attentifs à toute nouvelle technologie qui améliorerait la gestion des droits numériques et d'empêcher la redistribution illégale de contenus multimédia protégés par le droit d'auteur. Dans cette optique, le tatouage numérique a été introduit au début des années 90 comme un mécanisme de sécurité complémentaire au cryptage. En effet, tôt ou tard, les données cryptées doivent être décryptées pour les rendre accessibles aux utilisateurs. À ce moment précis, les données numériques ne sont plus protégées par le cryptage et peuvent être éventuellement copiées et redistribuées à grande échelle.

Le tatouage numérique a donc été introduit comme une seconde ligne de défense. L'idée de base consiste à protéger un document numérique en enfouissant un signal codant de l'information de façon robuste et imperceptible [2]. Il existe un compromis entre trois paramètres conflictuels : la capacité, l'imperceptibilité et la robustesse. La capacité est la quantité d'information insérée dans un document, c'est à dire le nombre de bits codés par le signal de tatouage. En fonction de l'application, le nombre de bits à cacher peut varier. Si quelques bits suffisent à mettre en place un service de contrôle de copie, il est en revanche nécessaire de cacher beaucoup d'information pour permettre l'authentification de documents multimédia. Par ailleurs, le processus de tatouage va inévitablement modifier le signal hôte et introduire des distorsions. La contrainte d'imperceptibilité impose que ces distorsions restent complètement indécelables par un observateur/auditeur. Dans ce but, les caractéristiques du système audio-visuel humain peuvent être exploitées. Par exemple, le signal de tatouage étant

souvent considéré comme du bruit, il sera moins perceptible dans les zones texturées d'une image que dans les zones unies. Ainsi, amplifier (resp. atténuer) le signal de tatouage dans les zones texturées (resp. uniformes) diminue sa visibilité. Enfin, le tatouage doit être construit de telle sorte qu'il résiste à la plus large palette possible d'opérations qu'un utilisateur puisse effectuer. Cette robustesse face aux traitements usuels du signal (filtrage, compression avec pertes, quantification) est souvent quantifiée en ayant recours à des bancs de test.

Cependant, en dépit des nombreux efforts pour optimiser ce compromis complexe, les quelques tentatives pour introduire un tatouage dans des systèmes de distribution de contenus [3, 4] se sont révélées être des échecs plus ou moins retentissants. L'un des éléments qui explique ces revers est que peu de travaux se sont intéressés à la survie du tatouage face une intelligence malveillante. Ainsi, même si le tatouage numérique a été introduit à l'origine pour des applications vouées à être déployées dans un environnement hostile (contrôle de copie, suivi de copies, etc.), la problématique de la sécurité a été quasiment ignorée. Pour pallier à cette lacune, la section 2 s'efforce dans un premier temps de définir de façon pertinente la notion de sécurité dans le contexte du tatouage numérique et en particulier d'établir une distinction avec le concept de robustesse. Les attaques par collusion sont alors introduites comme un des moyens possibles pour évaluer la sécurité. Ainsi, la section 3 dresse un panorama des attaques par collusion et passe en revue par la même occasion les différentes faiblesses des algorithmes de tatouage vidéo communément utilisés actuellement. Une fois ces menaces clairement identifiées, de nouvelles stratégies de tatouage sont introduites dans la section 4 afin de rendre le signal de tatouage cohérent avec la redondance spatio-temporelle du signal hôte vidéo. Finalement, les différents résultats sont rappelés dans la section 5 et des pistes de recherche sont rapidement proposées.

2 Problématique de la Sécurité

Quand bien même le tatouage numérique a toujours été étiqueté comme une technologie ayant trait à la sécurité, il n'a jamais été vraiment clair ce à quoi ce terme *sécurité* renvoyait. Du fait qu'une clé secrète soit nécessaire pour insérer/extraire le tatouage, une analogie avec les préceptes régissant la sécurité en cryptographie s'est rapidement imposée. Par exemple, en accord avec le second principe de Kerckhoffs [5], un algorithme rendu public ne doit pas pouvoir être "cassé" du moment que la clé demeure secrète. Pendant une très longue période, la communauté a pensé que casser un algorithme de tatouage se résumait à effacer le signal de tatouage. Cependant, des utilisateurs n'ayant pas accès à la clé secrète ne devrait pas être non plus en mesure de détecter, estimer, écrire ou modifier le tatouage enfoui [6]. Par ailleurs, une hypothèse courante en tatouage est que l'attaquant a accès à un unique document tatoué. Mais en pratique, de nombreuses autres situations sont possibles [7]. Ainsi, l'attaquant peut avoir une collection de documents tatoués, des paires de documents originaux/tatoués, etc. Face à cette situation confuse, les sous-sections qui suivent s'efforceront de donner une définition de la sécurité dans le contexte du tatouage.

2.1 Confiance dans un Environnement Hostile

Dans de nombreuses applications, il est nécessaire d'avoir confiance en l'information transportée par le canal de tatouage ; c'est souvent sur la validité de cette information que repose la pérennité du modèle économique. Dans le cadre d'une application de suivi de copies par exemple, le fournisseur de contenu possède un document multimédia de grande valeur qu'il veut distribuer à un large public. Par conséquent, à chaque fois qu'il vend une copie de ce document à un consommateur, il insère un tatouage qui code l'identité du consommateur. Par la suite, si une copie pirate est trouvée, il suffit d'extraire le tatouage pour identifier l'identité de la personne qui n'a pas respecté ses engagements et de prendre les mesures appropriées. L'ensemble du système de protection repose sur la capacité d'identifier, à l'aide du tatouage, les consommateurs qui mettent leur copie légale sur un réseau de distribution non-autorisé. Pour que ce système fonctionne, il est donc nécessaire qu'une personne n'ayant pas accès à la clé secrète ne puisse pas effacer ou modifier le tatouage inséré. De façon similaire, dans une application de contrôle de copie, le tatouage autorise ou non la copie d'un document. Là encore, le tatouage joue un rôle crucial : si un attaquant est capable d'effacer le tatouage, alors il peut copier "librement" les documents qu'il a déprotégés sans reverser le moindre centime aux auteurs.

En revanche, de leur côté, les consommateurs voient le tatouage comme une protection qui les dérange : il les empêche de copier leurs données numériques comme ils le souhaitent, il permet de retrouver l'identité des personnes qui ont permis la distribution illégale de copies... Par conséquent, ces utilisateurs sont susceptibles de déployer des stratégies d'attaque très hostiles. Ils ne vont pas se contenter d'appliquer des traitements usuels tels que filtrage ou compression avec pertes dans l'espoir d'altérer le signal de tatouage. Ils vont plutôt essayer de rassembler le plus d'information possible sur le système de protection pour mettre au point de nouvelles attaques dédiées. C'est ce genre de comportement qui est d'intérêt lorsqu'on parle de sécurité en tatouage numérique. Ainsi, la notion de sécurité est intimement liée avec le besoin de confiance dans un environnement hostile. D'un côté, la pérennité du modèle économique nécessite de faire confiance à l'information codée

par le tatouage. De l'autre coté, les utilisateurs perçoivent la protection apportée par le tatouage comme une gêne et tentent d'altérer la fiabilité du système.

Il faut néanmoins noter que de nombreuses applications n'ont aucune spécification en termes de sécurité. C'est en particulier le cas pour les applications où le tatouage inséré ajoute un service supplémentaire (qualité supérieure, correction d'erreur, information d'indexation). Dans ce cas, les utilisateurs n'ont aucun intérêt à enlever le tatouage et il n'est pas nécessaire de s'inquiéter d'un potentiel comportement malicieux.

2.2 Robustesse et Sécurité

Même au sein de la communauté tatouage, robustesse et sécurité demeurent encore de nos jours des concepts flous qu'il est difficile de distinguer. Il convient donc de donner quelques éléments simples qui différencient ces deux notions. Le premier élément est sans aucun doute l'*environnement*. Comme cela a été mentionné dans la précédente sous-section, parler de sécurité revient à faire l'hypothèse implicite que le système de tatouage évolue dans un environnement hostile. La robustesse s'intéresse plutôt à la survie du tatouage lorsque les documents protégés sont soumis à des traitements courants. Ainsi, un utilisateur qui compresse avec pertes des documents tatoués n'est pas assimilé à une menace contre la sécurité du système, même si cette opération est susceptible d'altérer le signal de tatouage. Le point principal ici est que l'utilisateur n'a pas l'intention d'enlever le tatouage mais cherche juste à réduire la taille de ses données pour faciliter leur stockage/transmission. En d'autres termes, il utilise de façon aveugle des opérations existantes de traitement du signal. Ceci est radicalement différent d'un attaquant hostile dont la stratégie se résume souvent en deux étapes. Dans un premier temps, il va rassembler autant d'éléments d'information que possible sur le système de tatouage ; dans un second temps, il va exploiter cette connaissance pour mettre au point de nouvelles attaques dédiées qui mettront à mal le système. On peut donc dire que le *type de traitement* est un second élément de distinction : générique pour la robustesse et spécialisé pour la sécurité. Enfin, le dernier point a trait à l'*impact des attaques*. Les opérations usuelles de traitement du signal sont seulement susceptibles d'empêcher le détecteur d'extraire le tatouage. En revanche, les attaques contre la sécurité du système peuvent aussi aboutir éventuellement à la détection non autorisée du tatouage, à son estimation, à sa modification ou bien même à l'insertion d'un nouveau tatouage dans un document non protégé.

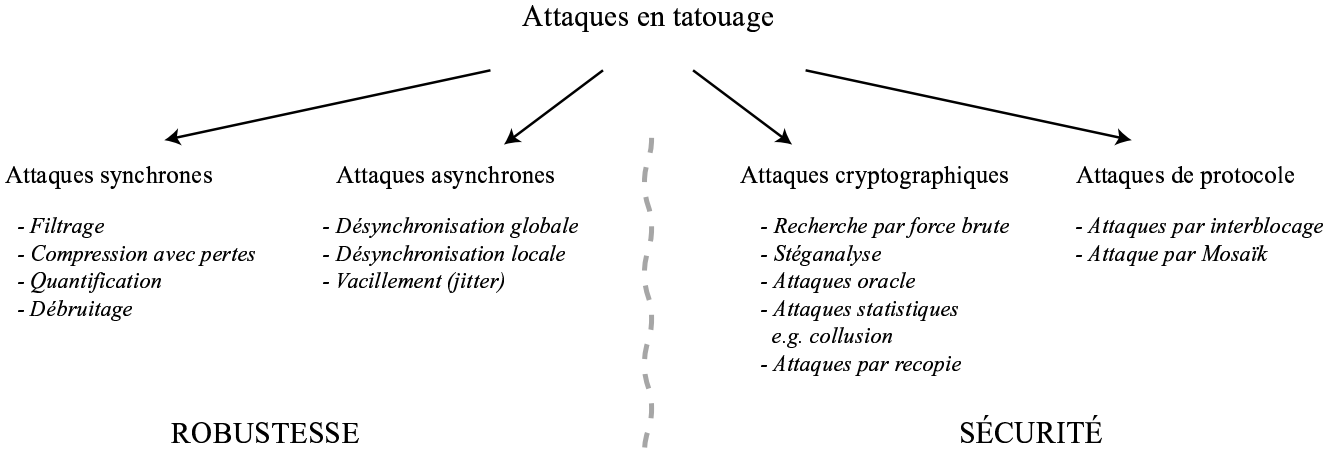

Figure 1 – Classification robustesse/sécurité des attaques couramment utilisées en tatouage numérique.

Une fois ces différences établies, il est utile de regarder dans quelle catégorie tombe telle ou telle attaque. Ainsi, la Figure 1 illustre une telle classification pour une liste non-exhaustive d'attaques couramment utilisées en tatouage numérique. Cette répartition étend les classifications précédemment introduites en tatouage [8, 9]. Dans la partie gauche, les attaques relatives à la robustesse sont séparées en deux catégories. Les attaques synchrones incluent toutes les opérations usuelles telles que filtrage, compression avec pertes, quantification, débruitage qui modifient la valeur des échantillons du signal et qui sont donc susceptibles d'altérer le signal de tatouage. De l'autre côté, les attaques asynchrones regroupent tous les traitements qui modifient la position des échantillons. Par conséquent, la convention de synchronisation entre le tatoueur et le détecteur devient caduque. Ainsi, même si ces traitements ne suppriment pas effectivement le signal de tatouage, le détecteur n'est plus capable d'extraire le tatouage. Un exemple très connu en image fixe est l'attaque StirMark [8, 10] qui introduit localement des déplacements aléatoires de faible amplitude.

Du côté sécurité, les attaques sont aussi divisées en deux catégories. Plutôt que d'attaquer directement le système de

tatouage lui-même, un premier type d'attaque consiste à mettre en défaut le protocole autour. Par exemple, dans le cadre d'une application de protection des droits d'auteur, si un document numérique s'avère contenir deux tatouages distincts, la plupart des algorithmes ne permettent pas de dire à qui revient la paternité de l'oeuvre. Il y a interblocage [11]. De façon différente, les applications de suivi de copies exploitent des robots qui inspectent les sites Internet pour vérifier s'ils hébergent ou non illégalement des documents propriétaires. Une façon simple de faire échouer ces robots est de diviser les documents, par exemple une image, en plusieurs morceaux et de juxtaposer ceux-ci lors de l'affichage. Si ces morceaux sont assez petits, il est alors impossible de détecter le tatouage [12]. À côté de cela , une seconde catégorie d'attaque vise à obtenir des renseignements sur le signal de tatouage lui-même. L'approche la plus simple (et le plus souvent coûteuse) est d'identifier la clé secrète qui a été utilisée par le biais d'une recherche exhaustive. Une autre technique, appelée stéganalyse, a simplement pour objectif de mettre au point des méthodes permettant de dire si un document est tatoué ou non, par quel algorithme, etc [13]. Par ailleurs, dans certaines applications, typiquement le contrôle de copie, le public a accès à un détecteur (oracle). Un attaquant peut alors considérer ce détecteur comme une boite noire et modifier les données numériques de façon itérative jusqu'à ce que la copie soit autorisée [14]. Un exemple d'insertion non autorisée de tatouage est l'attaque par recopie [15,16] : le tatouage est estimé à partir d'un document tatoué et réinséré dans un document non protégé. Enfin, lorsque plusieurs documents tatoués sont considérés, il est souvent possible de mettre le système de tatouage en défaut en les combinant.

2.3 Attaques par Collusion

La collusion est une stratégie d'attaque connue depuis un certain temps déjà en cryptographie : une clique d'utilisateurs malveillants se rassemble et met en commun ses informations/connaissances sur le système de protection, quelles qu'elles soient, pour générer des données non protégées. Ce type de comportement a été mentionné pour la première fois lors de la mise au point de protocoles pour diviser un secret entre plusieurs individus sans qu'aucun d'entre eux n'ait accès à l'ensemble du secret [17]. Un exemple typique est le partage de secret pour contrôler des actions critiques telles que l'ouverture de la porte d'un coffre fort particulier à la banque. Le client et le responsable de la banque ont tous les deux une clé et les deux sont nécessaires pour ouvrir le coffre. Si une partie du secret (clé) manque, la porte du coffre reste fermée. À plus grande échelle, plusieurs clés contenant une partie du secret sont distribuées et il est nécessaire de rassembler au moins k clés différentes pour avoir accès à l'intégralité du secret. Dans ce contexte, les attaquants sont un groupe de u utilisateurs qui cherchent à construire de fausses clés ou à reconstruire l'intégralité du secret quand bien même $u < k$. On retrouve aussi cette problématique de la collusion dans des schémas de distribution dynamique de clés [18] pour les sessions d'audio/vidéo conférences, vidéo à la demande, etc.

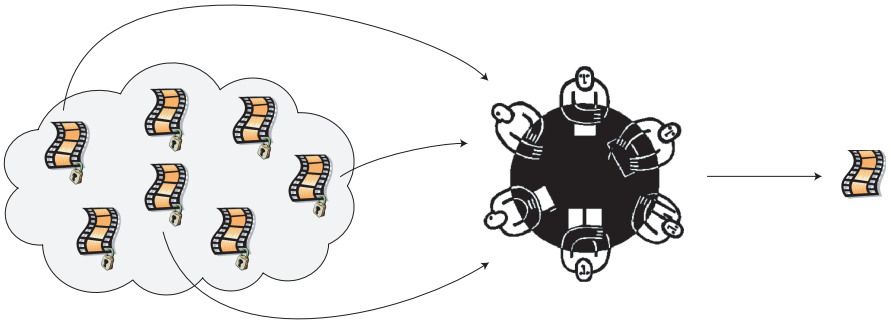

Figure 2 – Collusion en tatouage numérique : Plusieurs utilisateurs rassemblent plusieurs documents tatoués et les combinent pour produire des documents ne contenant plus aucun tatouage.

En tatouage numérique, les attaques par collusion ont été évoquées pour la première fois dans le contexte du suivi de copies [19]. Dans ce type d'applications, les fournisseurs de contenus veulent distribuer un faible nombre de contenus à une très large audience. Ils désirent par conséquent avoir les moyens de pister une copie pirate jusqu'à la personne à l'origine de cette fuite. Dans ce but, au lieu de distribuer exactement le même film à tous les consommateurs, des copies sensiblement différentes sont assignées à chacun d'entre eux. Ainsi, chaque consommateur obtient une copie unique portant un tatouage qui lui est propre. Si un utilisateur isolé rend sa copie disponible sur Internet, il est alors possible de l'identifier en utilisant le tatouage. Face à cette menace, les attaquants sont tentés de se regrouper pour combiner leur différentes copies et générer ainsi un nouveau document qui ne contiendrait plus de tatouage comme illustré dans la Figure 2. Il existe principalement deux stratégies de collusion en tatouage :

1. soit les documents sont analysés pour estimer certaines propriétés du signal de tatouage qui pourraient être utilisées dans un second temps pour retirer le signal de tatouage,
2. soit les documents sont combinés pour estimer directement le document original non tatoué.

Des parades ont déjà été proposées dans la littérature. Par exemple, des codes ayant certaines propriétés assurent que lorsque des documents tatoués sont combinés, certaines parties du tatouage demeurent intactes [20]. Ces parties résiduelles sont alors examinées pour isoler et identifier de façon certaine au moins un des individus dans la clique des attaquants.

3 Collusion en Vidéo

Auhourd'hui, l'évaluation de la sécurité des algorithmes de tatouage est devenue une problématique majeure. Dans ce but, il est nécessaire d'anticiper les comportements hostiles des utilisateurs afin d'introduire à temps des parades appropriées. Dans ce contexte, les attaques par collusion doivent être considérées sérieusement. Le tatouage de vidéo numérique se résume souvent à des approches image par image [21] comme écrit ci-dessous :

$$\check{\mathbf{f}}_t = \mathbf{f}_t + \alpha \mathbf{w}_t, \quad \mathbf{w}_t \sim \mathcal{N}(0,1) \tag{1}$$

où $\mathbf{f}_t$ est la trame vidéo originale à l'instant t, $\check{\mathbf{f}}_t$ sa version tatouée, α la force de tatouage et $\mathbf{w}_t$ le signal de tatouage qui est distribué suivant une loi gaussienne à moyenne nulle et à variance unité. Par conséquent, chaque trame peut être considérée comme un document tatoué individuellement [22,23]. En d'autres termes, un attaquant *isolé* peut mettre au point une attaque par collusion en considérant les différentes trames d'une vidéo tatouée comme autant de documents tatoués ; il n'est plus nécessaire que plusieurs attaquants collaborent. Les sous-sections qui suivent donnent un aperçu des différentes attaques par collusion possibles en vidéo lorsqu'on suit ce raisonnement.

3.1 Estimer une Structure Redondante

Lorsque les tatouages enfouis dans différentes trames ne sont pas complètement décorrélés, une stratégie de collusion est d'examiner les différentes trames tatouées et d'identifier des structures suspectes statistiquement redondantes. Ces fuites d'information peuvent être vues comme une empreinte statistique déposée par l'algorithme de tatouage. Du point de vue d'un attaquant, la situation idéale serait d'avoir accès directement au canal de tatouage $\mathcal{E}_{\mathrm{o}}(\check{\mathbf{f}}_t) = \check{\mathbf{f}}_t - \mathbf{f}_t$. Cependant, en pratique, les trames vidéo originales ne sont pas disponibles et il est impossible d'obtenir cette estimation parfaite du tatouage pour chaque trame. À défaut, du fait de la nature habituellement haute fréquence du tatouage, on peut obtenir une estimation par des méthodes de débruitage ou bien, plus simplement, en calculant la différence entre chaque trame tatouée et sa version filtrée passe-bas :

$$\mathcal{E}(\check{\mathbf{f}}_t) = \check{\mathbf{f}}_t - \mathcal{L}(\check{\mathbf{f}}_t) = \tilde{\mathbf{w}}_t \tag{2}$$

où $\tilde{\mathbf{w}}_t$ est l'estimation du tatouage enfoui à l'instant t et $\mathcal{L}(.)$ un filtre passe-bas, comme par exemple un filtre moyenneur 5×5. Maintenant, ayant à sa disposition une collection de tatouages bruités, l'attaquant doit trouver une structure redondante secrète qui puisse être exploitée par la suite pour retirer le signal de tatouage.

3.1.1 Estimer un Unique Tatouage

Pour s'affranchir de la contrainte de synchronisation temporelle, une solution simple consiste à enfouir toujours le même tatouage de référence $\mathbf{r}$ dans toutes les trames de la vidéo [24]. De plus, si l'algorithme de détection est linéaire, alors accumuler dans le temps des scores de détection calculés à différents instants est équivalent à faire une unique détection en utilisant l'accumulation temporelle des trames vidéo. En d'autres termes, il n'est pas nécessaire de lancer la procédure de détection pour chaque trame, ce qui est utile pour traiter la vidéo en temps réel. En revanche, d'un point de vue sécurité, toujours enfouir le même tatouage rend le signal de référence $\mathbf{r}$ statistiquement visible. En effet, si chaque estimation $\tilde{\mathbf{w}}_t$ est individuellement trop bruitée pour menacer la pérennité de l'algorithme de détection, les combiner raffine de façon significative l'estimation finale $\tilde{\mathbf{r}}$ du tatouage. Une approche consiste par exemple à moyenner des différentes estimations comme suit :

$$\tilde{\mathbf{r}} = \frac{1}{T} \sum_t \tilde{\mathbf{w}}_t \tag{3}$$

où T est le nombre de trames utilisées pour la collusion [22, 25]. Cette estimation est alors remodulée pour effacer de manière efficace le signal de tatouage dans chaque trame [26]. L'ensemble de cette attaque par Estimation du Tatouage et Remodulation (ETR) est illustré dans la Figure 3. Il est important de noter que le processus de raffinement de l'estimation du tatouage est d'autant plus efficace que les trames vidéo utilisées pour la collusion sont différentes. Ainsi cette attaque par

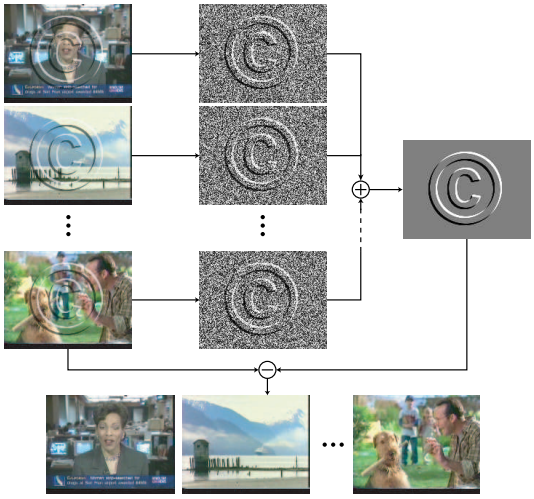

Figure 3 – Attaque par Estimation du Tatouage et Remodulation (ETR) : différentes estimations du tatouage obtenues avec différentes trames vidéo sont combinées pour raffiner l'estimation du tatouage de référence. Ensuite, cette estimation est remodulée pour enlever le signal de tatouage dans chaque trame vidéo.

ETR est plus pertinente dans des scènes dynamiques ou lorsque des trames clefs de la séquence vidéo sont considérées. Par ailleurs, plus on combine un nombre important d'estimations individuelles, meilleure est l'estimation finale $\tilde{\mathbf{r}}$ du tatouage. Ces deux remarques seront aussi valides pour les autres attaques présentées dans cette section.

3.1.2 Estimer une Collection de Tatouages

Une parade immédiate face à la menace d'une attaque par ETR est d'utiliser plus qu'un seul et unique tatouage de référence. Ainsi, pour chaque trame vidéo, le tatouage qui est enfoui est choisi parmi une bibliothèque de N tatouages de référence $\{\mathbf{r}_i\}$ comme noté ci-dessous :

$$\forall t \quad \mathbf{w}_t = \mathbf{r}_{\Phi(t)} \qquad \text{avec} \begin{cases} \mathbf{r}_i \cdot \mathbf{r}_j = \delta_i^j, & 1 \leq i, j \leq N \\ \mathrm{P}(\Phi(t) = i) = 1/N, & 1 \leq i \leq N \end{cases} \tag{4}$$

où $\cdot$ représente l'opérateur de corrélation linéaire et δ le symbole de Kronecker. Cette stratégie de tatouage recouvre un grand nombre d'algorithmes en allant d'une succession périodique des tatouages $\mathbf{r}_i$ à une succession complètement aléatoire [27]. Comme les tatouages de référence sont émis de façon équiprobable, une attaque par ETR est vouée à l'échec. En effet, si un attaquant moyenne plusieurs estimations $\tilde{\mathbf{w}}_t$, il obtient la moyenne des tatouages de référence et ce signal, une fois remodulé, ne tient pas le détecteur en échec.

Le gain en termes de sécurité repose ici sur l'hypothèse qu'un attaquant est incapable de construire des ensembles de trames vidéo portant le même tatouage de référence $\mathbf{r}_i$. Néanmoins, chaque estimation $\tilde{\mathbf{w}}_t$ peut être considérée comme un vecteur dans un espace de grande dimension qui est censé approximer un des tatouages de référence. Par conséquent, une quantification vectorielle permet d'isoler N amas de vecteurs $\mathcal{R}_i$ dont les centroïdes $\tilde{\mathbf{r}}_i$ sont de bonnes estimations des tatouages de référence secrets. Une implantation possible de cette approche est d'utiliser un algorithme des k-moyennes combiné avec une stratégie de division-fusion pour éviter une initialisation aléatoire [28]. Une fois que les tatouages de référence ont été estimés, l'attaquant teste chaque trame vidéo pour identifier quel tatouage est présent et effectue une remodulation pour l'enlever. On remarquera que la précédente attaque par ETR est un cas particulier de cette approche par Quantification des Estimations de Tatouage et Remodulation (QETR) pour $N = 1$.

3.1.3 Estimer un Sous-espace de Tatouage

Les attaques par ETR et QETR exploitent la même faille de sécurité pour vaincre les systèmes de tatouage. Lorsque les tatouages enfouis dans chaque trame sont vus comme des vecteurs dans un espace à grande dimension, les stratégies d'insertion vues précédemment introduisent des points d'accumulation dans l'espace qui peuvent facilement être identifiés

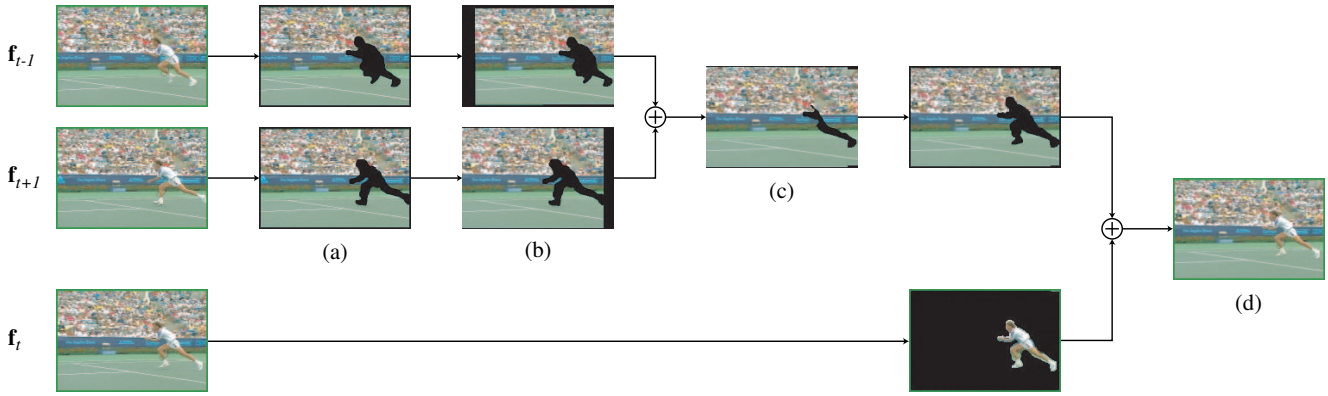

Figure 4 – Moyennage Temporel après Recalage (MTR) : pour chaque trame vidéo : une fois les objets en mouvement isolés (a), les trames voisines sont recalées (b) et combinées pour obtenir une estimation du fond de la trame courante (c). Ensuite, les objets vidéo manquants sont réinsérés.

de façon automatique. Afin d'éviter ce piège, une combinaison de tatouages de référence est enfouie dans chaque trame comme suit :

$$\forall t \quad \mathbf{w}_t = \sum_{i=1}^{N} \frac{\lambda_i(t)}{\sqrt{\sum_{j=1}^{N} \lambda_j(t)^2}} \mathbf{r}_i \tag{5}$$

où les $\lambda_i(t)$ sont N coefficients de mixage variant dans le temps. Comme les tatouages de référence ont une variance unité, les tatouages successifs $\mathbf{w}_t$ décrivent une trajectoire sur la sphère unité. Si cette trajectoire ne présente pas de points d'accumulation, alors une attaque QETR est vouée à l'échec.

Néanmoins, une faiblesse subsiste du fait que le nombre N de tatouages est habituellement largement inférieur à la dimension D de l'espace du média considéré ($N \ll D$). En d'autres termes, le signal de tatouage est borné au sein d'un sous-espace de faible dimension $\mathcal{R} = \mathrm{vect}(\mathbf{r}_i)$. À partir des différentes estimations $\tilde{\mathbf{w}}_t$, des techniques de réduction de dimensions, telles que l'Analyse par Composantes Principales (ACP), permettent donc d'obtenir une estimation $\tilde{\mathcal{R}}$ de ce sous-espace. Par la suite, pour chaque trame vidéo, supprimer l'énergie présente dans ce sous-espace retire le signal de tatouage [29]. Bien entendu, afin d'obtenir une bonne estimation du sous-espace de tatouage $\mathcal{R}$, il est nécessaire de prendre en compte un nombre d'estimations $\tilde{\mathbf{w}}_t$ d'autant plus grand que sa dimension N est grande.

D'autres travaux sont récemment venus renforcer ces résultats [30]. En adoptant une démarche basée sur la théorie de l'information, l'idée est de mesurer l'ignorance à propos du système en utilisant l'entropie conditionnelle comme écrit ci-après :

$$\mathrm{H}(K|\mathbf{d}_1, \ldots, \mathbf{d}_T) = \mathrm{H}(K) - \mathrm{I}(K; \mathbf{d}_1, \ldots, \mathbf{d}_T) \tag{6}$$

où $\{\mathbf{d}_i\}$ est un ensemble de documents tatoués et K le secret à estimer. Ainsi, les fuites d'information sont assimilées à l'information mutuelle entre les documents tatoués et le secret. Lorsque l'entropie conditionnelle $\mathrm{H}(K|\mathbf{d}_1, \ldots, \mathbf{d}_T)$ tombe à zéro, la totalité du secret du système a été dévoilée.

3.2 Combiner Différents Tatouages

Si une structure redondante de tatouage est susceptible d'être facilement estimée par un attaquant, insérer des tatouages complètement indépendants dans des trames successives n'est pas non plus la solution. En effet, en s'appuyant sur le fait que la somme de plusieurs échantillons de tatouage indépendants tend vers zéro, un attaquant peut mettre au point des attaques par collusion très efficaces. Désormais le but n'est plus d'identifier une structure secrète pour enlever ensuite le tatouage, mais plutôt d'estimer directement le document original non tatoué. Bien sûr, pour des raisons de fidélité, ces documents doivent être assez similaires pour être combinés sans dégrader de façon perceptible le document considéré. Les contenus vidéo présentent assez de redondance pour mettre en oeuvre de telles stratégies d'attaque.

3.2.1 Compensation de Mouvement

L'une des toutes premières méthodes de tatouage vidéo considère le contenu vidéo comme un signal monodimensionnel et ajoute simplement un signal de tatouage pseudo aléatoire [31]. D'un point de vue image, cela revient à toujours enfouir

un tatouage différent dans chaque trame vidéo ($\forall(t,t')\,\mathbf{w}_t \neq \mathbf{w}_{t'}$). Dans une séquence vidéo avec peu de mouvement, les trames successives sont fortement corrélées et peuvent être moyennées dans le temps sans endommager de façon notable la qualité de la vidéo. Cependant, comme les tatouages successifs sont indépendants, cette opération de moyennage temporel diminue de façon très significative l'énergie du tatouage $\mathbf{w}_t$ présente dans la trame vidéo $\check{\mathbf{f}}_t$. Afin d'éviter une distortion trop importante, cette stratégie est légèrement modifiée dès lors que la séquence vidéo contient des éléments dynamiques tels que des mouvements de caméra et/ou des objets en mouvements.

En particulier, compenser le mouvement de la caméra permet d'effectuer un Moyennage Temporel après Recalage (MTR) [32]. Comme l'illustre la Figure 4, cette attaque consiste à estimer l'arrière-plan de chaque trame en utilisant les trames voisines. Cela est possible car les trames successives d'une séquence vidéo sont différentes vues du même décor de cinéma, ou encore différentes projections 2D de la même scène 3D. Les objets en mouvement étant plus difficiles à estimer, ils sont conservés tels quels. Cette attaque peut aussi être vue comme un moyennage temporel suivant l'axe du mouvement. Quoi qu'il en soit, du fait que la plupart des algorithmes de tatouage ne prêtent pas attention à l'évolution de la structure de la scène pendant l'enfouissement du tatouage, le MTR parvient à éliminer le signal qui a été introduit. Enfin, il est utile de noter que l'utilisation de mosaïques vidéo pour compresser efficacement l'arrière-plan comme préconisé dans le standard MPEG-4 aurait un impact similaire au MTR sur le tatouage [33].

3.2.2 Autosimilarités

S'il est aisé d'admettre qu'une séquence vidéo est redondante dans le temps, il est moins immédiat de remarquer que chaque trame vidéo présente aussi une certaine redondance spatiale. Ces autosimilarités ont déjà été utilisées auparavant pour concevoir des algorithmes de compression efficaces [34]. Ainsi, à la façon du codage fractal, un attaquant peut mettre au point une Attaque par Remplacement de Bloc (ARB) comme illustré dans la Figure 5 qui consiste à remplacer chaque bloc de l'image par un autre pris ailleurs dans l'image, qui est similaire au bloc d'origine modulo une transformation géométrique et photométrique [35]. De façon différente, l'attaquant peut choisir de combiner plusieurs blocs de sorte que le bloc obtenu soit assez similaire pour être échangé sans menacer d'altérer la qualité visuelle de l'image de façon significative [36]. Évidemment, il existe un compromis entre l'efficacité de l'attaque et son impact perceptuel. Plus le bloc candidat au remplacement est similaire au bloc à remplacer, moins l'attaque est susceptible d'être efficace et inversement. Ce constat a motivé l'introduction d'un schéma adaptatif pour combiner un nombre variable de blocs en fonction de la nature du bloc considéré de sorte d'obtenir une certaine distortion [37]. Il est en effet nécessaire de combiner plus (resp. moins) de blocs pour approximer de façon satisfaisante un bloc texturé (resp. uni). Comme aujourd'hui les algorithmes de tatouage ignorent les autosimilarités du signal, les ARB parviennent la plupart du temps à altérer de façon critique le signal de tatouage.

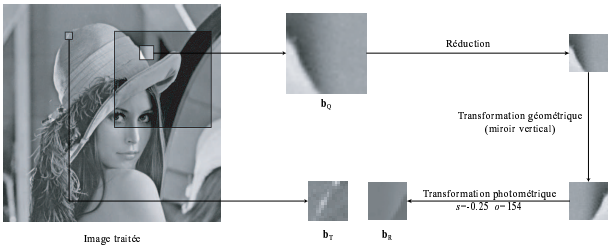

Figure 5 – Attaque par Remplacement de Bloc (ARB) : chaque bloc est remplacé par un bloc pris à une autre position qui lui est similaire à une transformation géométrique et photométrique près.

4 Tatouage Cohérent avec le Signal

D'un côté, une structure de tatouage redondante utilisée pour tatouer des documents différents peut être estimée. D'un autre côté, des tatouages indépendants insérés dans des documents (ou des parties de documents) similaires peuvent être effacés par simple moyennage. Ce constat conduit intuitivement à essayer de respecter une règle d'enfouissement qui assure que *les tatouages insérés dans deux documents sont aussi corrélés que les documents eux-mêmes*. Différentes approches ont déjà été proposées pour remplir ce cahier des charges : rendre le tatouage dépendant des trames vidéos [25], utiliser des signatures numériques binaires des trames vidéos pour générer des tatouages qui sont aussi corrélés que ces signatures [38, 39], enfouir le tatouage à des endroits dépendants du contenu des trames vidéos [22]. Néanmoins, aucune de ces solutions ne s'est révélée vraiment satisfaisante. En considérant plus particulièrement les faiblesse soulignées dans la sous-section 3.2, on

s'aperçoit que le signal de tatouage doit être cohérent avec le contenu de la séquence vidéo, cohérent avec le mouvement de la caméra d'une part (sous-section 4.1) et cohérent avec les autosimilarités du signal d'autre part (sous-section 4.2).

4.1 Gérer le Mouvement de la Caméra

Pour une scène vidéo donnée, l'arrière plan de trames successives correspond à différentes projections 2D d'un même décor 3D. Fondamentalement, le MTR exploite le fait que les algorithmes de tatouage ne prennent pas en compte le mouvement de la caméra. Par conséquent, un point du décor 3D qui est projeté à plusieurs endroits dans des trames vidéo différentes est associé à des échantillons de tatouage non corrélés. Ainsi, moyenner les trames recalées enlève le tatouage. Une riposte possible à cette faiblesse est de renseigner le tatoueur en termes de mouvements de la caméra et de définir une stratégie de tatouage qui force chaque point 3D du décor à toujours être associé avec le même échantillon de tatouage, où qu'il soit visible dans la scène vidéo.

Comme illustré dans la Figure 6, cette tactique a été implantée en ayant recours aux mosaïques vidéo [40]. Pour chaque trame, des paramètres de recalage θ_t sont calculés pour définir la position de la trame dans la mosaïque. Par ailleurs, un tatouage de référence $\mathbf{r}$ de la taille de la mosaïque est construit. La portion $\mathbf{r}_t$ associée à chaque trame vidéo est alors récupérée et recalée pour obtenir le signal $\mathbf{r}_t^{(\theta_t)}$ à enfouir dans chaque trame ; les objets en mouvement ne sont pas tatoués pour suivre la philosophie : *un point 3D porte toujours le même échantillon de tatouage tout au long de la scène*. L'ensemble du processus s'écrit :

$$\mathbf{w}_t = \mathbf{m}_t \otimes \mathbf{r}_t^{(\theta_t)} \tag{7}$$

où $\mathbf{m}_t$ est un masque binaire qui distingue les objets en mouvement de l'arrière-plan et $\otimes$ représente la multiplication pixel à pixel. De son côté, le détecteur vérifie si la portion de tatouage $\mathbf{r}_t^{(\theta_t)}$ est effectivement présente dans chaque trame ou pas. Des précédents travaux en mosaïque vidéo [41, 42] ont été exploités pour implanter cette stratégie de tatouage et démontrer sa supériorité en termes de résistance au MTR [40].

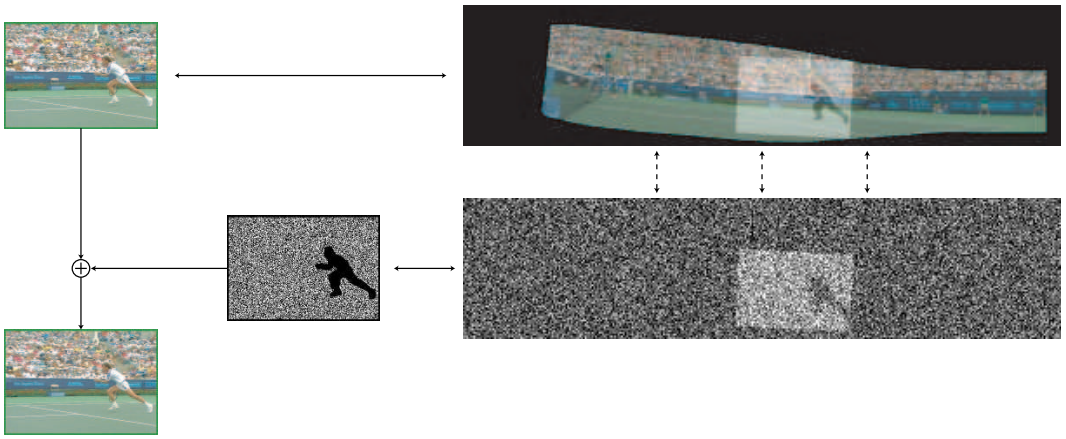

Figure 6 – Tatouage cohérent avec le mouvement de la caméra : la partie du signal de tatouage qui est associée avec la trame vidéo courante est identifiée et recalée. Ensuite, elle est enfouie dans l'arrière-plan de la trame vidéo.

Le fait de gérer le mouvement de la caméra au moment de l'enfouissement a aussi donné des résultats intéressants vis à vis de l'invisibilité du tatouage. Évaluer l'impact de la distorsion induite par le tatouage comme perçue par un utilisateur humain est toujoursun grand défi en vidéo. Le comité VQEG [43], qui est chargé de définir des méthodes pour évaluer la qualité visuelle d'une vidéo, a en effet statué en 1999 (i) qu'aucune des métriques testées n'était meilleure que les autres dans tous les cas, et surtout (ii) qu'aucune d'entre elles pouvait remplacer une inspection visuelle subjective. C'est la raison pour laquelle l'évaluation de la visibilité d'un tatouage en vidéo se résume souvent à une recherche visuelle d'artéfacts. Deux principaux défauts ont précédemment été isolés [44, 45] :

1. *Le scintillement* : Enfouir des tatouages indépendants dans des trames vidéo successives introduit souvent un scintillement désagréable, comme un bruit de capteur ;
2. *La persistance* : Enfouir le même tatouage de référence dans toutes les trames de la vidéo produit un motif fixe, dérangeant visuellement parlant, comme si la scène avait été filmée par une caméra ayant un objectif sale.

Lorsque la stratégie de compensation de mouvement proposée est mise en oeuvre, les tatouages insérés dans chaque trame sont différents. Néanmoins, ils n'introduisent plus de scintillement car le tatouage est cohérent avec le mouvement de la

caméra. En fait, si le tatouage est assez amplifié pour être visible, on a la sensation que la caméra filme une scène qui est déjà bruitée. En d'autres termes, en plus d'assurer une meilleure sécurité, la stratégie proposée simule un monde utopique où le décor de la vidéo serait tatoué avant d'être filmé et cela dérange beaucoup moins le système visuel humain.

4.2 Hériter des Autosimilarités

Si la compensation de mouvement rend le tatouage cohérent avec la redondance temporelle du signal vidéo, il ne résout pas le problème des ARB. Ces attaques profitent du fait que les algorithmes de tatouage ne tiennent pas compte des autosimilarités du signal. Par conséquent, les blocs similaires (modulo une transformation géométrique et photométrique ou une combinaison linéaire) ne sont pas tatoués de façon similaire. Intuitivement, s'il était possible d'assurer le contraire, les ARB devraient être inefficaces. Formulé d'une autre manière, le but est donc d'imposer que *des pixels ayant des voisinages similaires portent des échantillons de tatouage ayant des valeurs proches* i.e. de faire hériter le signal de tatouage des autosimilarités du signal porteur [46]. En admettant qu'il soit possible de définir le voisinage d'un pixel à la position $\mathbf{p}$ dans une trame $\mathbf{f}$ à l'aide d'un vecteur caractéristique $\mathbf{v}(\mathbf{f},\mathbf{p})$, cela revient à écrire :

$$\mathbf{v}(\mathbf{f},\mathbf{p}_{\mathrm{o}}) \approx \sum_k \lambda_k \mathbf{v}(\mathbf{f},\mathbf{p}_k) \Rightarrow \mathrm{w}(\mathbf{f},\mathbf{p}_{\mathrm{o}}) \approx \sum_k \lambda_k \mathrm{w}(\mathbf{f},\mathbf{p}_k) \tag{8}$$

où $\mathrm{w}(\mathbf{f},\mathbf{p})$ est la valeur de tatouage insérée à la position $\mathbf{p}$ dans la trame $\mathbf{f}$. Pour obtenir cette propriété, il suffit de définir la fonction de tatouage $\mathrm{w}(.)$ comme étant une forme linéaire $\varphi(.)$ dans l'espace $\mathcal{V}$ des vecteurs caractéristiques. Cette forme linéaire est complètement définie par les valeurs w_i qu'elle prend sur une base orthonormée. C'est là qu'est injecté du secret dans le système en utilisant la clé secrète pour générer ces valeurs qui déterminent la forme linéaire. Une implantation de cette riposte exploitant des ondelettes de Gabor pour caractériser le voisinage en chaque pixel a montré de bonnes performances vis à vis des ARB [46].

Le fait d'utiliser des filtres de Gabor a par ailleurs permis d'établir un lien intéressant avec des algorithmes de tatouage existants qui enfouissent un signal pseudo-aléatoire de façon multiplicative dans un domaine fréquentiel. En effet, lorsque le signal de tatouage (en utilisant des filtres de Gabor) est exprimé dans le domaine de Fourier, on obtient la relation suivante [47] :

$$\mathbf{W} = \mathbf{H}(K)\mathbf{I}, \quad \text{avec } \mathbf{H}(K) = \sum_{i=1}^{N} w_i \mathbf{H}_i \tag{9}$$

où $\mathbf{W}$ (resp. $\mathbf{I}$) est la transformée de Fourier du tatouage (resp. de l'image) et $\mathbf{H}_i$ est la réponse fréquentiel d'un des filtres de Gabor utilisés pour caractériser le voisinage. Il est à noter que des filtres symétriques par rapport à l'origine dans le domaine fréquentiel ont été utilisés afin d'obtenir un vecteur caractéristique $\mathbf{v}(\mathbf{f},\mathbf{p})$ à valeur réelles. Si on fait tendre la bande passante d'un filtre de Gabor vers 0, on obtient alors deux pics de Dirac symétriques par rapport au centre. Et dans ce cas, le schéma proposé revient à un enfouissement multiplicatif dans le domaine de Fourier [48]. En d'autres termes, un signal de tatouage, obtenu en multipliant le spectre de l'image avec un signal pseudo-aléatoire symétrique par rapport au centre, présente dans le domaine spatial les mêmes autosimilarités que le signal hôte. De même, il est possible de montrer qu'une multiplication dans le domaine DCT [49] produit aussi un tatouage qui a hérité des autosimilarités du signal. Ces deux points ont été vérifiés expérimentalement en vérifiant la résistance de tels tatouages face aux ARB [47].

L'utilisation de schémas de tatouage multiplicatifs était motivé au départ par des raisons de masquage perceptuel dû au contraste : des coefficients de fortes valeurs peuvent transporter des valeurs de tatouage plus grandes sans compromettre l'invisibilité du tatouage [50]. D'un autre côté, en utilisant la linéarité de la fonction de tatouage du système qui a été proposé, on obtient la relation suivante :

$$\mathrm{w}(\mathbf{f},\mathbf{p}) = \|\mathbf{v}(\mathbf{f},\mathbf{p})\| \varphi\left(\frac{\mathbf{v}(\mathbf{f},\mathbf{p})}{\|\mathbf{v}(\mathbf{f},\mathbf{p})\|}\right) \tag{10}$$

Le vecteur $\mathbf{u}(\mathbf{f},\mathbf{p}) = \mathbf{v}(\mathbf{f},\mathbf{p})/\|\mathbf{v}(\mathbf{f},\mathbf{p})\|$, qui est passé en argument de la forme linéaire $\varphi(.)$, est sur la sphère unité. Sous certaines hypothèses, il est possible de montrer que $\varphi(\mathbf{u}(\mathbf{f},\mathbf{p}))$ suit une distribution gaussienne de moyenne nulle et de variance unité [51]. En d'autres termes, l'échantillon de tatouage est amplifié ou atténué en fonction de la valeur de la norme du vecteur caractéristique $\mathbf{v}(\mathbf{f},\mathbf{p})$. C'est là encore une technique couramment utilisée pour mettre en forme le tatouage afin de réduire son impact perceptuel [52].

5 Conclusion

Longtemps négligée, la sécurité est désormais une problématique majeure dans le domaine du tatouage numérique. Cela est lié au fait que la plupart des applications visées, comme la protection des droits d'auteur ou le suivi de copie, sont vouées

à être déployées dans des environnements hostiles, c'est à dire où des attaquants malveillants s'attaquent délibérément au système. Dans cet article, deux principales stratégies de collusion ont été passées en revue : soit des documents différents ont été tatoués avec la même structure de tatouage et le but est d'estimer cette structure de tatouage ; soit le même document a été tatoué de différentes façons et le but est d'approximer directement le document original. Ces attaques qui combinent différents documents tatoués sont d'autant plus critiques en vidéo que chaque trame peut être vue comme un document tatoué distinct. Deux ripostes ont ensuite été introduites afin de rendre le tatouage cohérent avec le signal vidéo. L'une s'appuie sur la compensation de mouvement pour tenir compte de la redondance temporelle, l'autre considère les autosimilarités pour gérer la redondance spatiale.

Les implantations proposées ne sont pas optimales et peuvent être améliorées. De récents travaux ont par exemple proposé d'utiliser un certain type d'ondelettes temporelles pour produire des tatouages compensant le mouvement [53]. Néanmoins, cette démarche *sécurité face aux attaques par collusion* a permis de jeter un éclairage original sur le tatouage vidéo. Tout d'abord, l'importance de tenir compte du signal porteur a été soulignée lorsque le tatouage doit résister à des attaques hostiles type collusion. En particulier, l'utilisation de traitements vidéo tels que les mosaïques, la segmentation d'objets s'est avérée une approche pertinente pour générer des tatouages plus performants. De plus, le cheminement pour obtenir un tatouage cohérent avec le signal a permis de donner un regain d'intérêt pour d'anciens schémas de tatouage multiplicatifs dans le domaine fréquentiel. Enfin, quand bien même la progression de cette étude était guidée par une recherche de sécurité accrue, des résultats très intéressants ont été obtenus en termes d'invisibilité du tatouage inséré. En vue de mettre au point une nouvelle génération de tatoueurs vidéo, il pourrait être utile de réfléchir comment les outils usuels en vidéo peuvent être exploités dans le cadre du tatouage. De même, il pourrait être fructueux de penser comment intégrer une méthode de tatouage dans un système vidéo complet de sorte que le signal inséré n'interfère pas avec les fonctionnalités d'indexation/compression.

Références

[1] Deloitte Development LLC. Facing piracy – Digital theft in the filmed entertainment industry, 2004.

[2] I. Cox, M. Miller, et J. Bloom. *Digital Watermarking*. Morgan Kaufmann Publishers, 2001.

[3] Secure Digital Music Initiative. http ://www.sdmi.org.

[4] DVD Copy Control Association. http ://www.dvdcca.org.

[5] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX :5–83, January 1883.

[6] T. Kalker. Considerations on watermarking security. Dans *Proceedings of the IEEE Fourth Workshop on Multimedia Signal Processing*, pages 201–206, October 2001.

[7] M. Barni, F. Bartolini, et T. Furon. A general framework for robust watermarking security. *Signal Processing, Special Section on Security of Data Hiding Technologies*, 83(10) :2069–2084, October 2003.

[8] F. Petitcolas, R. Anderson, et M. Kuhn. Attacks on copyright marking systems. Dans *Proceedings of the Second International Workshop on Information Hiding*, volume 1525 de *Lecture Notes in Computer Science*, pages 219–239, April 1998.

[9] S. Voloshynovskiy, S. Pereira, V. Iquise, et T. Pun. Attack modeling : Towards a second generation watermarking benchmark. *Signal Processing*, 81(6) :1177–1214, June 2001.

[10] Stirmark. http ://www.petitcolas.net/fabien/watermarking/stirmark.

[11] S. Craver, N. Memon, B.-L. Yeo, et M. Yeung. Resolving rightful ownerships with invisible watermarking techniques : Limitations, attacks, and implications. *Journal on Selected Areas in Communications*, 16(4) :573–586, May 1998.

[12] 2Mosaic. http ://www.petitcolas.net/fabien/watermarking/2mosaic.

[13] R. Chandramouli, M. Kharrazi, et N. Memon. Image steganography and steganalysis : Concepts and practice. Dans *Proceedings of the Second International Workshop on Digital Watermarking*, volume 2939 de *Lecture Notes in Computer Science*, pages 35–49, March 2004.

[14] J.-P. Linnartz. The ticket concept for copy control based on signal embedding. Dans *Proceedings of the Fifth European Symposium on Research in Computer Security*, volume 1485 de *Lecture Notes in Computer Science*, pages 257–274, September 1998.

[15] M. Kutter, S. Voloshynovskiy, et A. Herrigel. Watermark copy attack. Dans *Security and Watermarking of Multimedia Contents II*, volume 3971 de *Proceedings of SPIE*, pages 371–380, January 2000.

[16] M. Holliman et N. Memon. Counterfeiting attack on oblivious block-wise independent invisible watermarking schemes. *IEEE Transactions on Image Processing*, 9(3) :432–441, March 2000.

[17] A. Menezes, P. van Oorschot, et S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[18] A. Eskicioglu. Multimedia security in group communications : Recent progress in key management, authentication and watermarking. *ACM Multimedia Systems, Special Issue on Multimedia Security*, 9(3) :239–248, September 2003.

[19] M. Wu, W. Trappe, J. Wang, et R. Liu. Collusion-resistant fingerprinting for multimedia. *IEEE Signal Processing Magazine*, 21(2) :15–27, March 2004.

[20] D. Boneh et J. Shaw. Collusion secure fingerprinting for digital data. *IEEE Transaction on Information Theory*, 44(5) :1897–1905, September 1998.

[21] G. Doërr et J.-L. Dugelay. A guide tour of video watermarking. *Signal Processing : Image Communication, Special Issue on Technologies for Image Security*, 18(4) :263–282, April 2003.

[22] K. Su, D. Kundur, et D. Hatzinakos. A novel approach to collusion resistant video watermarking. Dans *Security and Watermarking of Multimedia Contents IV*, volume 4675 de *Proceedings of SPIE*, pages 491–502, January 2002.

[23] G. Doërr et J.-L. Dugelay. Collusion issue in video watermarking. Dans *Security, Steganography and Watermarking of Multimedia Contents VII*, volume 5681 de *Proceedings of SPIE*, pages 685–696, January 2005.

[24] T. Kalker, G. Depovere, J. Haitsma, et M. Maes. A video watermarking system for broadcast monitoring. Dans *Security and Watermarking of Multimedia Contents*, volume 3657 de *Proceedings of SPIE*, pages 103–112, January 1999.

[25] M. Holliman, W. Macy, et M. Yeung. Robust frame-dependent video watermarking. Dans *Security and Watermarking of Multimedia Contents II*, volume 3971 de *Proceedings of SPIE*, pages 186–197, January 2000.

[26] S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgärtner, et T. Pun. Generalized watermarking attack based on watermark estimation and perceptual remodulation. Dans *Security and Watermarking of Multimedia Contents II*, volume 3971 de *Proceedings of SPIE*, pages 358–370, January 2000.

[27] E. Lin et E. Delp. Temporal synchronization in video watermarking. *IEEE Transactions on Signal Processing, Supplement on Secure Media*, 52(10) :3007–3022, October 2004.

[28] G. Doërr et J.-L. Dugelay. Security pitfalls of frame-by-frame approaches to video watermarking. *IEEE Transactions on Signal Processing, Supplement on Secure Media*, 52(10) :2955–2964, October 2004.

[29] G. Doërr et J.-L. Dugelay. Danger of low-dimensional watermarking subspaces. Dans *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, volume III, pages 93–96, May 2004.

[30] F. Cayre, C. Fontaine, et T. Furon. Watermarking security, part I : Theory. Dans *Security, Steganography and Watermarking of Multimedia Contents VII*, volume 5681 de *Proceedings of SPIE*, pages 746–757, January 2005.

[31] F. Hartung et B. Girod. Watermarking of uncompressed and compressed video. *Signal Processing*, 66(3) :283–301, May 1998.

[32] G. Doërr et J.-L. Dugelay. New intra-video collusion attack using mosaicing. Dans *Proceedings of the IEEE International Conference on Multimedia and Expo*, volume II, pages 505–508, July 2003.

[33] R. Koenen. MPEG-4 overview. Dans *JTC1/SC29/WG11 N4668*. ISO/IEC, March 2002.

[34] Y. Fisher. *Fractal Image Compression : Theory and Applications*. Springer-Verlag, 1994.

[35] C. Rey, G. Doërr, J.-L. Dugelay, et G. Csurka. Toward generic image dewatermarking ? Dans *Proceedings of the IEEE International Conference on Image Processing*, volume III, pages 633–636, September 2002.

[36] D. Kirovski et F. Petitcolas. Blind pattern matching attack on watermarking systems. *IEEE Transactions on Signal Processing*, 51(4) :1045–1053, April 2003.

[37] G. Doërr, J.-L. Dugelay, et L. Grangé. Exploiting self-similarities to defeat digital watermarking systems – A case study on still images. Dans *Proceedings of the ACM Multimedia and Security Workshop*, pages 133–142, September 2004.

[38] J. Fridrich et M. Goljan. Robust hash functions for digital watermarking. Dans *Proceedings of the International Conference on Information Technology : Coding and Computing*, pages 178–183, March 2000.

[39] D. Delannay et B. Macq. A method for hiding synchronization marks in scale and rotation resilient watermarking schemes. Dans *Security and Watermarking of Multimedia Contents IV*, volume 4675 de *Proceedings of SPIE*, pages 548–554, January 2002.

[40] G. Doërr et J.-L. Dugelay. Secure background watermarking based on video mosaicing. Dans *Security, Steganography and Watermarking of Multimedia Contents VI*, volume 5306 de *Proceedings of SPIE*, pages 304–314, January 2004.

[41] H. Nicolas et C. Labit. Motion and illumination variation estimation using a hierarchy of models : Application to image sequence coding. *Journal of Visual Communication and Image Representation*, 6(4) :303–316, December 1995.

[42] H. Nicolas. New methods for dynamic mosaicing. *IEEE Transactions on Image Processing*, 10(8) :1239–1251, August 2001.

[43] Visual Quality Expert Group (VQEG). http ://www.vqeg.org.

[44] W. Macy et M. Holliman. Quality evaluation of watermarked video. Dans *Security and Watermarking of Multimedia Contents II*, volume 3971 de *Proceedings of SPIE*, pages 486–500, January 2000.

[45] S. Winkler, E. Gelasca, et T. Ebrahimi. Towards perceptual metrics for video watermark evaluation. Dans *Applications of Digital Image Processing*, volume 5203 de *Proceedings of SPIE*, pages 371–378, August 2003.

[46] G. Doërr et J.-L. Dugelay. A countermeasure to resist block replacement attacks. Dans *Proceedings of the IEEE International Conference on Image Processing*, volume I, pages 965–968, September 2005.

[47] G. Doërr et J.-L. Dugelay. How to combat block replacement attacks ? Dans *Proceedings of the 7th Information Hiding Workshop*, volume 3727 de *Lecture Notes in Computer Science*, pages 161–175, June 2005.

[48] M. Barni, F. Bartolini, A. De Rosa, et A. Piva. A new decoder for optimum recovery of nonadditive watermarks. *IEEE Transactions on Image Processing*, 10(5) :755–766, May 2001.

[49] I. Cox, J. Kilian, T. Leighton, et T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12) :1673–1687, December 1997.

[50] J. Foley et G. Legge. Contrast masking in human vision. *Journal of the Optical Society of America*, 70(12) :1458–1470, December 1980.

[51] G. Doërr. *Security Issue and Collusion Attacks in Video Watermarking*. Thèse de doctorat, Université de Nice Sophia-Antipolis, France, June 2005.

[52] S. Voloshynovskiy, A. Herrigel, N. Baumgärtner, et T. Pun. A stochastic approach to content adaptive digital image watermarking. Dans *Proceedings of the Third International Workshop on Information Hiding*, volume 1768 de *Lecture Notes in Computer Science*, pages 211–236, September 1999.

[53] P. Vinod et P. Bora. A new inter-frame collusion attack and a countermeasure. Dans *Proceedings of the 4th International Workshop on Digital Watermarking*, volume 3710 de *Lecture Notes in Computer Science*, pages 147–157, September 2005.

Gwenaël Doërr a obtenu le diplôme d'ingénieur en systèmes de télécommunications de l'Institut National des Télécommunications en 2001. Il a ensuite obtenu une thèse de doctorat en Automatique et Traitement du Signal de l'Université de Nice Sophia-Antipolis en 2005. Ses travaux de thèse portant sur la sécurité des algorithmes de tatouage vidéo face aux attaques par collusion ont été réalisés à l'Institut Eurécom. Depuis Août 2005, il est maître de conférence à University College London Adastral Park Postgraduate Campus. Ses travaux de recherche ont surtout trait à la sécurité multimédia en général, incluant des activités en tatouage numérique (sécurité, treillis modifié) et en biométrie (émissions auto-acoustiques).

Jean-Luc Dugelay a obtenu sa thèse de doctorat en informatique de l'université de Rennes en 1992. Ses travaux de thèse ont été réalisés au CCETT (France Télécom Recherche) de Rennes entre 1989 et 1992. Il a ensuite rejoint l'Institut Eurécom où il occupe maintenant un poste de professeur au sein du département communications multimédia. Ses travaux actuels se situent essentiellement dans le domaine de l'imagerie multimédia, incluant tout particulièrement des activités en sécurité (tatouage et biométrie), compression image et vidéo, analyse d'images de visage, clonage et visages parlants. Il est auteur ou co-auteur de plus 65 publications publiées dans des journaux ou actes de conférences, de 3 chapitres de livre et 3 brevets internationaux. Il a dispensé plusieurs tutoriaux en tatouage numérique, biométrie et compression au cours de conférences majeures comme ACM Multimédia ou IEEE ICASSP. Il a été invité à participer à de nombreux événements scientifiques en tant que membre du comité technique, orateur invité ou président de session. Jean-Luc Dugelay est éditeur associé de plusieurs revues scientifiques internationales (dont IEEE T-IP, IEEE T-MM, EURASIP JASP) et un membre actif de l'IEEE (membre des comités techniques IMDSP et MMSP). Il a co-organisé la 4ème conférence en traitement des signaux multimédia à Cannes en octobre 2001 (IEEE MMSP) et la conférence "Mutimodal User Authentication" en 2003 à Santa Barbara.