MÉCANISMES DE SÉCURITÉ LIÉS À LA TRANSMISSION DES IMAGES

Stéphane Roche & Jean-Luc Dugelay

Département Multimédia
Institut EURECOM,
1 2229 route des Crêtes, B.P. 193,
F-06904 Sophia Antipolis Cedex, FRANCE
{roche, dugelay}@eurecom.fr
http://www.eurecom.fr/~image

1 INTRODUCTION

L'avénement de nombreuses applications multimédia et la mise en service de nouveaux supports de communication (Internet, Réseaux mobiles,...) qui par nature sont peu sécurisés nécessitent une nouvelle approche des problèmes liés à la sécurité des données audio et vidéo. On peut distinguer les services suivant [3] :

- la protection du copyright (section 2) visant à protéger l'auteur d'un document (image) contre une appropriation illicite de la paternité du document vidéo,
- l'intégrité (section 2.5) garantissant la non falsification d'une image,
- le contrôle d'accès (section 3) permettant de restreindre la divulgation d'un document en fonction de l'appartenance d'un utilisateur à une classe donnée,
- ainsi que la non répudiation, qui n'a pas encore fait l'objet d'études significatives et ne sera pas abordées dans la suite de cet article.

Ces services sont bien évidemment non exclusifs et se retrouvent bien souvent complémentaires dans un schéma complet. Cet article s'attachera à montrer dans quelle mesure ces services peuvent être intégrés à des techniques largement utilisées en compression d'image et en théorie des communications [2].

2 LA PROTECTION DU COPYRIGHT

Tout éditeur d'image (propriétaire), doit être en mesure de prouver qu'une de ses images circulant sur un réseau est effectivement sa propriété. Ceci afin de se déjouer des opérations frauduleuses faisant usage de ses images sans autorisation. Parmi les différentes voies susceptibles d'assurer la protection du copyright des images, le tatouage que l'on retrouve également dans la littérature sous les termes de "watermarking" ou "fingerprinting" constitue actuellement le domaine de recherche le plus actif en sécurisation des images.

2.1 PROBLÉMATIQUE

Dans ce problème, on distingue trois intervenants (fig.1) : le **propriétaire** de l'image, l'**utilisateur** qui peut être bienveillant ou malveillant et le **certificateur** qui joue le rôle d'arbitre entre ces deux entités.

L'utilisateur dispose d'une version de l'image signée par le propriétaire (opération $\oplus$). En cas de conflict sur la propriété du document, le propriétaire doit être en mesure de prouver que l'image incriminée contient effectivement sa marque (opération $\ominus$), et ceci même si l'utilisateur a perturbé cette image (opération $\otimes$).

Contrairement aux problèmes de confidentialité où l'objectif est de protéger le contenu de l'image de toute divulgation, le système de copyright doit s'attacher à minimiser l'impact visuel de la signature sur le document vidéo.
L'information (signature) ajoutée à l'image originale doit identifier sans ambiguïté le propriétaire [5], [11] et doit rester indélébile quelques soient les perturbations non destructrices que subit l'image. Les perturbations que l'on doit considérer peuvent résulter à la fois de manipulations malveillantes ou d'opérations usuelles telles les changements d'échelle, d'espace de représentation ou de format de stockage. Cette problématique peut se résumer dans le schéma ci-dessous (fig.1).

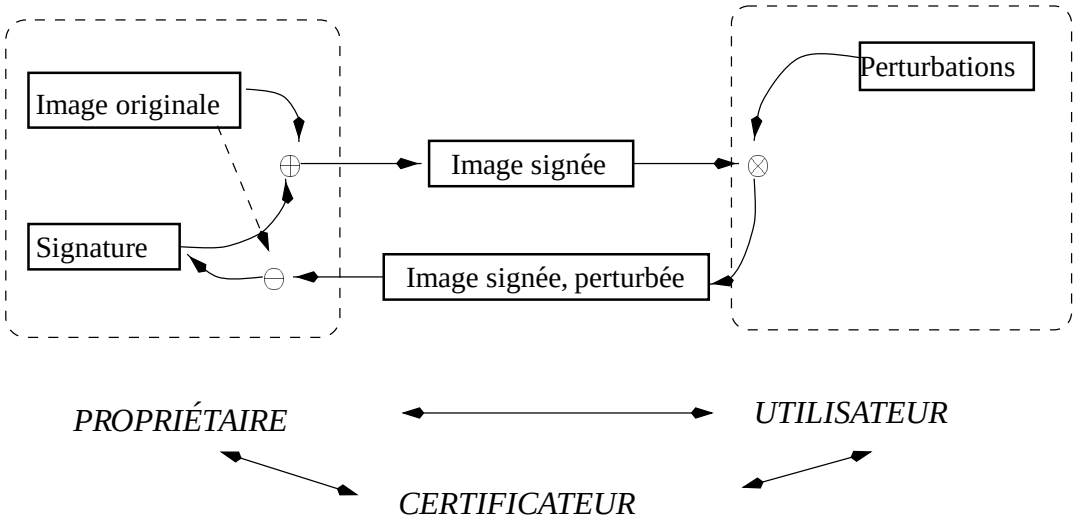

FIG. 1 – *Problématique du copyright*

2.2 PREMIÈRES SIMULATIONS

Les premières recherches répondant au problème de la protection du copyright par tatouage d'image se sont orientées vers l'utilisation de transformations (DCT) largement employées en codage de source. L'idée est de tirer partie de l'analyse fréquentielle que réalise implicitement ces transformées [4]. La signature est dissimulée dans les composantes de hautes fréquences pour lesquelles l'oeil est faiblement sensible. Ces techniques présentent un coût de mise en oeuvre réduit, et garantissent l'invisibilité du tatouage, cependant elles ne permettent pas l'extraction du tatouage avec un bon niveau de fiabilité.

Ceci est dû :

- à la localisation spatiale de l'information associée à un bit de la signature. En effet, les techniques de codage source dont découlent ces premières simulations sont basées sur des opérations par blocs. Les auteurs sélectionnent pseudo-aléatoirement un bloc de l'image pour insérer un bit de la signature. Si ce bloc est malencontreusement suprimé par une opération d'extraction de région d'intérêt, la signature est perdue.

- à la localisation fréquentielle de la signature, inhérente au fait que l'on se limite à la bande des hautes fréquences pour garantir un faible impact psychovisuel. Ces composantes fréquentielles sont potentiellement suprimées par des systèmes à taux de compression élevé qui, certes peuvent entrainer une légère dégradation de l'image mais lui conserve un intéret économique.

2.3 REFORMULATION DU PROBLÈME EN TERMES DE RAPPORT SIGNAL/BRUIT

Afin de résoudre les lacunes précédentes, des schémas issus de la théorie des communications ont été introduits.

2.3.1 Type Signature-Bruit-Bruit : SBB

Dans ce premier modèle, la signature est vue comme un signal S noyé dans du bruit. On distingue deux types de bruits : Le premier B_1 est constitué par l'image originale et représente l'information dans laquelle on va chercher à dissimuler la signature (opération $\oplus$ fig.1). Le second B_2 modélise les modifications de l'image après l'insertion de la signature et comprend notamment des opérations d'extraction, de filtrage, de requantification, ...(opération $\otimes$ fig.1)
Les problèmes d'invisibilités et de robustesse peuvent ainsi être décrits en termes de rapport signal à bruit,

- S/B_1 : invisibilité.

- S/B_2 : robustesse dans le cas où l'on admet la connaissance de l'image originale lors du processus d'identification.

- $S/(B_1 + B_2)$: robustesse dans le cas où l'on ne dispose pas de l'image originale.

Si l'on admet l'hypothèse simplificatrice : *tous les bruits sont Gaussiens*, ce modèle permet d'estimer la capacité C du canal de transmission (image) en fonction du degré de visibilité de la signature grâce à la formule due à Shannon, $C = W \log_2(1 + S/B)$ où W est la largeur de bande du signal signature.

2.3.2 Type Signature-Porteuse-Bruit : SPB

L'image originale constitue une onde porteuse vis-à-vis de notre signal à transmettre qui est le tatouage. Les différentes manipulations intentionnelles ou non que l'on peut réaliser sur l'image signée sont comme précédemment modélisées par un bruit (Gaussien).
Ces modèles bien que présentant un caractère objectif ne rendent pas compte de la répartition de l'énergie du bruit propre à chaque type d'attaque, on se trouve face à des problèmes liés à la modélisation du bruit (attaque). Cependant, ils présentent un caratère *a priori* qui permet de les intégrer dans l'élaboration de la signature (système adaptatif).

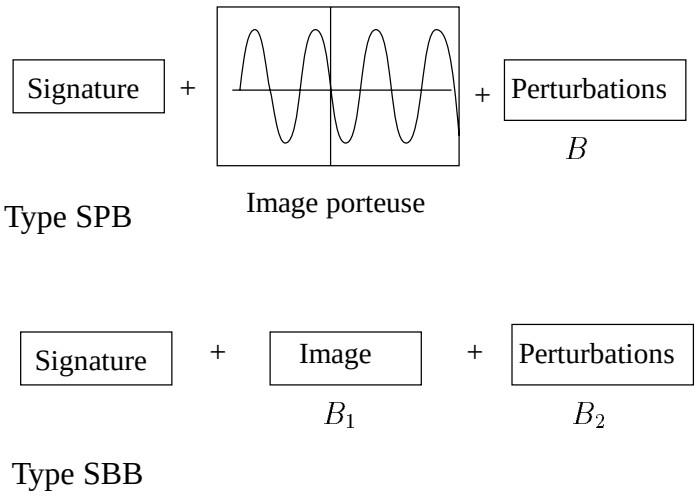

FIG. 2 – *modélisation des données du problème de copyright*

2.4 CONSIDÉRATIONS ISSUES DE LA REFORMULATION

2.4.1 Étalement du spectre de la signature

La modélisation du problème *via* la théorie des communications a inspiré une famille de méthodes reposant sur l'étalement de spectre.

Le concept motivant ces techniques est de rendre la signature peut visible, en répartissant son énergie sur l'ensemble du contenu fréquentiel de l'image lors de l'insertion ($\oplus$ fig.1). L'énergie de la signature associée à chaque composante fréquentielle présente ainsi un niveau faible. Cette répartition entraine également une immunité de la signature à un grand nombre de traitements ($\otimes$ fig.1) qui bien souvent ne déteriorent que quelques composantes fréquentielles. Lors de la procédure d'extraction de la signature ($\ominus$ fig.1), la recombinaison des bandes de faible énergie permet d'obtenir un signal de niveau suffisant pour rendre la signature perceptible.
D'un point de vue mathématique, on extrait de l'image originale un ensemble de n fonctions orthogonales $\{\phi_i\}$ qui dans le cas idéal constitue une base de l'image. Ces fonctions jouent le rôle de porteuses pour les n bits de la signature à insérer. L'orthogonalité de ces fonctions garantie qu'il n'y ait pas d'interférences entre les différents bits de la signature. On cherchera des fonctions ϕ_i le plus proche possible d'un bruit blanc afin que chacune d'elle recouvre une grande partie du spectre. Dans cette configuration, on peut raisonnablement assurer que toute perturbation visuellement acceptable ne supprimera pas la signature. Le choix des fonctions ϕ_i donnent lieu à une grande variété de systèmes qu'il convient d'explorer [1],[10].

2.4.2 Ajout d'un niveau de redondance dans la signature

La robustesse du tatouage ne peut pas être obtenue par une insertion directe de celui-ci dans l'image. En effet, pour rester indélébile, il devrait présenter une invariance par rapport à l'ensemble des transformations ne dégradant pas significativement l'image. Ceci apparait peu raisonnable et nous conduit à accepter de perdre une partie du signal représentant la signature si la redondance dans ce signal est telle que l'on puisse néanmoins retrouver l'information originale.

Une possibilité pour introduire de la redondance dans la signature est proposée implicitement dans les techniques à étalement de spectre. En effet, à chaque bit i de la signature est associé une fonction ϕ_i qui va recouvrir plusieurs pixels de l'image assurant ainsi une duplication. On peut parler de redondance analogique.
Une autre voie que l'on qualifiera de redondance logique pourrait s'inspirer des codes correcteurs à haut pouvoir de correction [9].
Les limitations dans l'ajout de redondance sont principalement dues au fait que le support dont nous disposons pour dissimuler l'information est borné. On devra donc ajuster la redondance en fonction du rapport S/B_1 fournit par le modèle (type SBB, fig.2).

2.5 DÉRIVATION DES TECHNIQUES DE SIGNATURE AU CONTRÔLE DE L'INTÉGRITÉ D'UNE IMAGE

Le développement de logiciels de retouche d'image tel que PhotoShop a rendu aisé la manipulation des images. Aussi il peut s'avérer très intéressant de garantir l'intégrité d'une image. Tout destinataire d'une image doit pouvoir vérifier que celle-ci n'a pas été modifiée au cours de son acheminement. Ceci peut être appréhendé par une méthodologie très similaire à celle employée lors de la protection du copyright. On s'assure qu'une marque répartie sur toute l'image n'a pas été modifié significativement. Les techniques d'étalement de spectre sont ici particulièrement bien adaptées pour l'introduction du motif. La différence majeure entre les systèmes de protection du copyright et d'intégrité réside dans l'interprétation que l'on fait du motif extrait. Dans le premier cas, on exploite la redondance du motif pour s'affranchir d'éventuelles corruptions de l'image et reconstruire l'identificateur du propriétaire, alors que dans le second cas on utilise cette redondance pour définir un intervalle de confiance représentant la probabilité que l'image ait été manipulée.

Elle implique néanmoins la mise en oeuvre de techniques de tatouage ne nécessitant pas la connaissance de l'image originale [6].

3 LE CONTRÔLE D'ACCÈS

3.1 PROBLÉMATIQUE

L'émergence de services à la carte telle la télévision à péage, les bases de données multimédia fait naître le besoin de systèmes capables d'offrir des accès multiniveaux. Les mécanismes de contrôle d'accès doivent présenter un impact minimum sur le taux de compression des données ainsi que sur le temps nécessaire pour disposer des images. De plus, les flux de données à traiter sont très important et très fortement corrélés.

3.2 UNE APPROCHE CONJOINTE : COMPRESSION, CONTRÔLE D'ACCÈS

Dans ce contexte, nous avons développé un algorithme de compression basé sur les systèmes de fonctions itérées [8] qui intègre la fonction de contrôle d'accès hiérarchique.

3.2.1 Rappels sur les techniques de compression fractale

L'idée sous-jacente au codage fractal est de représenter l'image x_c par un ensemble de transformations W auquel on associe un processus itératif. Ce processus consiste, à

partir de n'importe quelle image, à appliquer récursivement les transformations associées. L'image initiale permet simplement de spécifier la résolution de l'image finale.
L'objectif du codage est d'assurer la convergence du processus itératif vers un point fixe (attacteur x_a) constituant une approximation aussi fidèle que possible de l'image originale x_c. Le problème du codage peut être formulé en termes d'optimisation sous contraintes :

1. La première est constituée par le modèle de transformations W adoptées. Généralement il s'agit d'un modèle affine comprenant les 8 isométries du plan, un moyennage couplé à une décimation, et une transformation photométrique ($s \cdot z + o$) où s et o sont des paramètres à estimer et z le niveau de gris.

2. La seconde stipule que les fonctions recherchées doivent être contractantes afin d'assurer la convergence du processus itératif de décodage.

L'attracteur vérifiant la propriété d'invariance : $W(x_a) = x_a$ et étant donnée que l'on désire : $x_c \approx x_a$, on va chercher W tel que $W(x_c) \approx x_c$ sous les contraintes (1) et (2).

Ce problème d'optimisation est trop complexe et est réduit en considérant des transformations locales W_k blocs à blocs. On doit donc déterminer les paramètres s_k, o_k et l'isométrie associée à chaque bloc B_k constituant une partion de l'image (fig.3).
Nous invitons le lecteur désirant des précisions sur la compression fractale à consulter la référence [7]

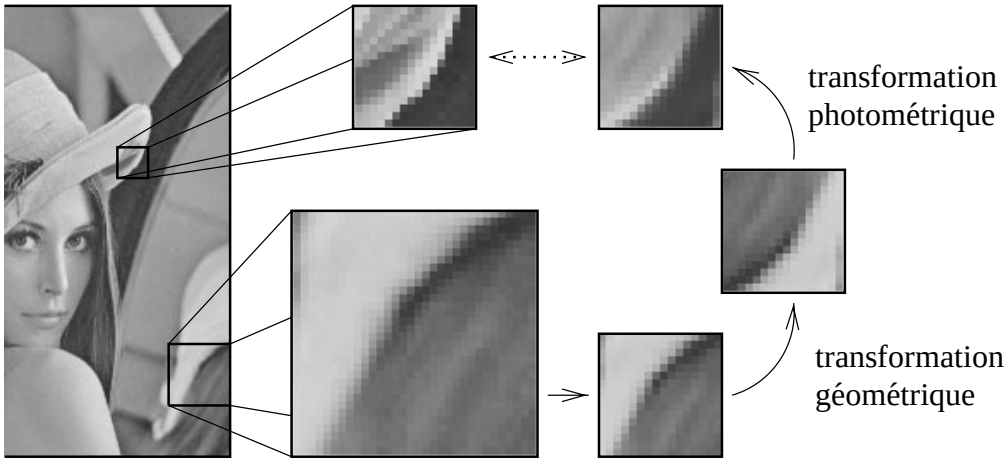

FIG. 3 – *Codage fractal*

3.2.2 Contrôle d'accès basé sur les I.F.S.

Le contrôle d'accès est obtenu en perturbant le niveau de reconstruction du processus itératif de décodage. Nous perturbons la convergence en modifiant les paramètres d'échelle s_k de la transformation photométrique. De manière pratique, nous masquons partiellement le niveau de visibilité des valeurs binaires de ces paramètres (fig.4). Un masquage total entraîne une dégradation presque totale de l'image (fig.5a) alors que la divulgation progressive des bits permet de tendre vers l'image originale (fig.5d).

Notre approche conjointe (compression, sécurité) nous permet à la fois de minimiser l'impact de la sécurisation sur le taux de compression et de tenir compte de la spécificité

des données traitées (image fixe). De plus, l'ensemble des utilisateurs peuvent disposer d'une même implémentation (logiciel ou matérielle) quelque soit leur niveau d'accès. Seule la clé composée à partir des paramètres s_k différencie le type d'utilisateur.

	MSB			s_k bits				LSB
a	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**
b	**1**	**0**	**0**	**1**	**1**	×	×	×
c	**1**	**0**	**0**	**1**	×	×	×	×
d	**1**	**0**	**0**	×	×	×	×	×
e	**1**	**0**	×	×	×	×	×	×
f	**1**	×	×	×	×	×	×	×
g	×	×	×	×	×	×	×	×

FIG. 4 – *Masques des paramètres s_k (a) sans cryptage jusqu'à (g) cryptage total*

Une extension de cet algorithme permettant de protéger graduellement les régions d'intérêt d'une séquence vidéo est actuellement en cours d'étude. On applique graduellement les masques définis précédemment aux paramètres s_k associés à des blocs présentant une forte activité temporelle.

4 REMARQUES & CONCLUSIONS

Cet article introduit la sécurisation des images en termes de protection du copyright et de contrôle d'accès. En ce qui concerne le tatouage, les premiers systèmes existent mais doivent maintenant évoluer vers des systèmes intégrant plus largement des techniques connues en codage canal et en théorie de l'information. Ces systèmes devrons également répondrent à des questions plus générales à propos des tolérances sur la dégradation d' une image, du protocole liant le propriétaire et le certificateur,...
Le système proposé en contrôle d'accès résout conjointement les problèmes de compression (codage de source) et de limitation d'accès.

5 REMERCIEMENTS

Ce travail est soutenu par le groupe télécommunications & détection —DGA/DRET—. Les auteurs tiennent également à remercier Messieurs R. Molva et E. Polidori pour leur participation à ce projet.

Références

[1] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report, NEC Research Institute, 95.

[2] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report, NEC, 95.

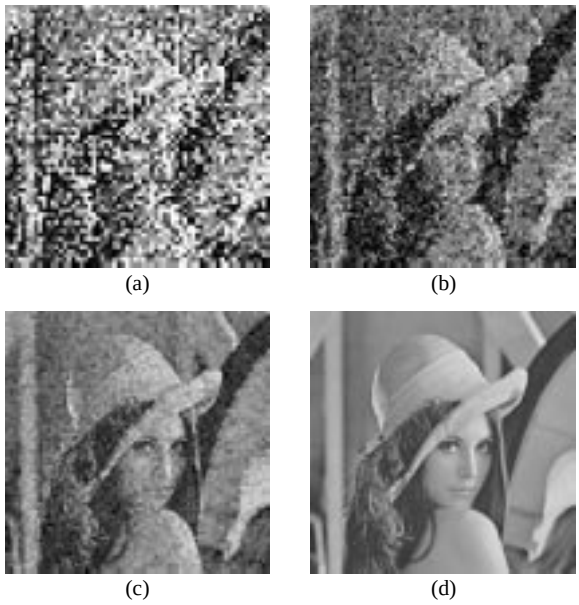

FIG. 5 – *compression fractale de lena avec contrôle du niveau de reconstruction* (a) *8/8 bits protégés,* (b) *6/8 bits protégés,* (c) *5/8 bits protégés, et* (d) *sans restriction d'accès (0/8 bit protégé).*

[3] F. Kaderali, W. Poguntke, A. Rieke, and M. Schneider. Security in special: the quality of security service. In *ECMAST-96*.

[4] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *1995 IEEE Workshop on Nonlinear Signal and Image Processing*.

[5] K. Matsui and K. Tanaka. Video-steganography: How to secretly embed a signature in a picture. In *IMA Intellectual Property Project Proceedings.*

[6] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In *Proceedings of the SPIE,* 96.

[7] S. Roche and J.-L. Dugelay. Improvements in ifs formulation for its use in still image coding. In *1995 IEEE Workshop on Nonlinear Signal and Image Processing.*

[8] S. Roche, J.-L. Dugelay, and R. Molva. Multi resolution access control algorithm based on fractal coding. In *Proceedings ICIP-96*.

[9] N. Sendrier. *Codes correcteurs d'erreurs à haut pouvoir de correction.* PhD thesis, Université Paris VI, 91.

[10] J.R. Smith and B.O. Comiskey. Modulation and information hiding in images. In *Workshop on Information Hiding*, 96.

[11] R.G. Van Schyndel, A.Z. Tirkel, and C.F. Osborne. A digital watermark. In *Proceedings ICIP-94*.