Mécanismes de Sécurité liés à la Diffusion des Images : Tatouage d'image

THÈSE

présentée et soutenue le 18 mai 1999

pour l'obtention du

Doctorat de l'Ecole Nationale Supérieure des Télécommunications

(spécialité Signal et Images)

par

Stéphane Roche

Composition du jury

Président :	Prof. Claude Gueguen, Get
Rapporteurs :	Prof. Kenneth Rose, University of California Santa Barbara US Prof. Benoit Macq, Université Catholique de Louvain Belgique
Examinateurs :	Dr. Jean-Luc Dugelay, Institut Eurécom (Directeur de la thèse) Prof. Réfik Molva, Institut Eurécom Dr. Michel Granger, HDR Direction Générale de l'Armement Dr. Philippe Nguyen, Thomson-CSF (Expert industriel)

Mis en page avec la classe TheseCRIN.

Remerciements

Mes premiers remerciements s'adressent aux membres de mon jury :

- Monsieur Claude Gueguen (Directeur du GeT) qui en acceptant de présider cette thèse, mais également en qualité de Directeur de l'Institut Eurécom, a montré son plus vif intérêt pour mes travaux.

- Monsieur Kenneth Rose (Professeur au Département d'Electricité et d'Informatique de l'Université de Santa-Barbara) qui a su prendre de son temps à la fois pour relire ce manuscipt et traverser l'Atlantique afin d'assister à ma soutenance.

- Monsieur Benoit Macq (Professeur et Directeur du Laboratoire de Télécommunications et Télédétection de l'Université catholique de Louvain), pour sa relecture constructive en sa qualité d'expert reconnu.

- Monsieur Michel Granger (Chef de Division : Systèmes de Détection, DRET-DGA) pour avoir supporté le projet dans sa phase initiale notamment en me proposant une bourse DRET-CNRS.

- Monsieur Réfik Molva (Professeur Associé au Département Communication d'Entreprise de l'Institut Eurécom) pour avoir pris part au lancement de cette thèse et inculqué les bases de la sécurité.

- Monsieur Philippe Nguyen (Ingénieur de Recherche à Thomson-CSF) qui a apporté son point de vue industriel à cette thèse.

- Monsieur Jean Luc Dugelay (Directeur de Thèse) pour avoir constitué ce jury qui m'honore, mais surtout pour avoir été précurseur en me proposant de travailler sur le tatouage d'image. Il a montré tout au long de cette thèse un enthousiasme sans failles qui fut pour moi d'un grand soutien.

Mes profonds remerciements vont au « team image » : Stéphane, Mathieu, Christian qui ont su détecter les phrases écrites à la hâte, à Sophie, Olivia et Rémy pour l'organisation parfaite de la soutenance, et à Annie qui n'a pas ménagé ses efforts pour la correction orthographique. Si des fautes subsistes elles sont certainement dues à des phrases ajoutées ultérieurement.

Je tiens également à remercier les personnes non-directement impliquées dans cette thèse mais qui ont joué un rôle décisif dans sa réussite, en particuliers : Perrine pour son amitié préservée, Franck pour ses coups de files météo qui ont été indispensables à l'accomplissement de cette thèse. La famille Gélin pour m'avoir communiqué la formule magique : « tout va bien tout va bien... ». Ma famille qui a été inquête tout au long de mes études, et enfin Katia pour ne pas avoir été raisonnable lors de cette fin de thèse.

Je dédie cette thèse à Katia.

Table des matières

Liste des abréviations **xi**

Liste des tableaux **xvii**

Introduction générale **1**

Distribution des rôles **5**

Chapitre 1
Contrôle d'Accès : CA **7**

1 Remarque introductive 8
2 Positionnement et problématique du CA 8
2.1 Eléments de CA admis en sécurité 8
2.2 Spécificités du problème dans le domaine de l'image 10
3 Rappels sur le codage fractal 11
3.1 Photocopieuse à réductions multiples et système de fonctions itérées 11
3.2 Algorithme de codage 14
3.3 Algorithme de décodage 15
4 Le couplage du CA à l'algorithme de compression 16
4.1 Convergence et CA 16
4.2 La stratégie de masquage face aux problèmes de sécurité 18
4.3 Entropie et sécurité : codage de source et sécurité 18
4.4 Algèbre des codes IFS et cryptanalyse différentielle 19
4.5 Structure parallèle et sécurité 19
5 Vers la constitution d'une clé secrète à longueur variable : structure en treillis 20
5.1 Génération de la clé secrète 20
5.2 Discussion sur le processus de génération de clé 21

6 Les extensions possibles à la vidéo et à la sécurisation partielle d'une image 22
6.1 Extension vidéo du codage fractal : approche 3-D 22
6.2 Cryptage localisé (en vue de garantir l'anonymat par exemple) . . . 22
7 Applications 23
7.1 Serveur d'images web sécurisé 23
7.2 Services Multimédia par satellite 24
8 Conclusion 27

Chapitre 2
Problématiques et modèles de tatouage d'image 29

1 Le tatouage d'image : quelle utilité, pour quel service ? 30
1.1 Vérification de l'intégrité du contenu d'une image 30
1.2 Protection des droits d'auteur 35
1.3 Non répudiation de l'accès à une image, traçage de copies illicites . 37
1.4 Gestion du nombre de copies d'une image 37
1.5 Masquage partiel d'une image en vue d'en limiter et contrôler l'accès 38
1.6 Notariat électronique 38
1.7 Autres services 38
1.8 Récapitualtif des différentes formes de tatouage et de leurs propriétés 39
2 Tour d'horizon des manipulations des images 40
2.1 Manipulations par filtrage 41
2.2 Manipulations géométriques 42
2.3 Manipulations par requantification 43
2.4 Manipulations spécifiques 44
2.5 Mosaïque d'images 44
3 Modélisation des systèmes de tatouage : aspects protocoles 46
3.1 Protocoles usuels en sécurité 46
3.2 Informations et individus impliqués dans l'établissement des preuves 47
4 Modélisation des systèmes de tatouage : aspects traitements d'image 52
4.1 Rapport Signal à Bruit et tatouage d'image 53
4.2 Modèle projectif basé sur la séparation de sources 54
5 Les difficultés pour estimer les performances des algorithmes 56
6 Conclusion 57

Chapitre 3
Etat de l'art des techniques de tatouage d'image **59**

1 Organisation du chapitre 60
2 Choix des éléments de l'image recevant l'information de signature : aspects cryptographiques et psychovisuels 60
2.1 Clé secrète et générateur aléatoire 61
2.2 Vérification publique du tatouage 62
2.3 Codage prédictif 62
3 Réaliser l'insertion du tatouage dans un espace transformé 63
3.1 Le domaine DCT 63
3.2 L'espace engendré par la transformée de Fourier-Mellin 64
3.3 Le domaine ondelette 67
3.4 Décomposition de l'image en canaux perceptifs 69
4 Ajout de redondance à la signature initiale 69
4.1 Etalement de spectre 70
4.2 Codes correcteurs 73
5 Fusion des données : signature et image 73
5.1 Modulation de phase 73
5.2 Modulation d'amplitude 74
5.3 Fusion préservant la luminosité moyenne : algorithme **rsppmc** . . 75
5.4 Ajout du tatouage par quantification des coefficients DCT 76
5.5 Ajout du tatouage par substitution de blocs : codage fractal 77
6 Techniques visant à accroître les performances de restitution de la signature lors de la phase d'extraction 79
6.1 Préfiltrage de l'image et blanchiment de l'image 79
6.2 Seuillage adaptatif 79
6.3 Estimation et compensation d'attaques géométriques sans image originale 80
6.4 Test d'hypothèses 81
7 Adaptation des algorithmes proposés en image fixe aux séquences vidéo . . 82
7.1 Les nouvelles contraintes 82
7.2 Système de tatouage utilisant un modèle perceptif dédié à la vidéo . 83
8 Critiques et faiblesses inhérentes aux approches de type tatouage 83
8.1 Les faiblesses face aux attaques de traitements d'image 83

8.2 Evolution conjointe des algorithmes de compression et de tatouage d'image 84
8.3 Le tatouage peut-il résoudre les problèmes de droit d'auteur ? 84
8.4 Nouvelles contraintes à imposer aux algorithmes de tatouage 86
9 Conclusion 87

Chapitre 4
Proposition d'un algorithme de tatouage 89

1 Introduction à la méthode 90
2 Tatouage d'image basé sur un modèle affine d'ifs 90
2.1 Détermination du support du tatouage 91
2.2 Codage du tatouage sur le support 92
2.3 Recombinaison du support : obtention de l'image tatouée 93
2.4 Approximations réalisées lors de l'extraction du tatouage 93
3 Etude des invariances propres au codage fractal 94
3.1 Invariance par réhaussement du niveau de gris moyen 94
3.2 Invariance par réhaussement du contraste 94
3.3 Pseudo-invariance par translation 95
3.4 Pseudo-invariance par changement d'échelle 96
3.5 Extension des invariances 96
4 Schéma global de notre méthode 97
4.1 L'algorithme d'insertion 98
4.2 L'algorithme d'extraction 98
5 Mise en forme de la signature 98
5.1 Types de signature supportés par l'algorithme 98
5.2 Sur-échantillonner (T_{se}) et dupliquer (T_{sed}) 101
5.3 Bruiter 102
5.4 Cryptage et incertitude sur la localisation du tatouage 103
6 Paramétrisation de l'algorithme et problèmes de visibilité 104
6.1 Discrétisation du dictionnaire de codage 105
6.2 Modulation de la signature sur le support 105
7 Resynchronisation des données reçues 106
7.1 Le problème 106
7.2 Méthode directe 106
7.3 Tentative d'optimisation par une approche hiérarchique 108

7.4 Méthode utilisant l'image tatouée standard 108
8 Exploitation de la redondance et reconstruction de la signature 108
8.1 Réjection des bits à faible taux de cohérence 108
8.2 Exploitation de la duplication de la signature par vote 109
8.3 Cas d'une signature de type logo : post filtrage 109
9 Evaluation de la robustesse de l'algorithme face aux traitements de l'image 109
9.1 Protocole du test 110
10 Conclusion 110

Chapitre 5
Proposition d'une alternative au tatouage : l'empreinte externe 113

1 Rappel sur les fonctions de hachage à sens unique 114
2 Du tatouage vers l'empreinte externe 115
2.1 Algorithme de génération de l'empreinte 116
2.2 Algorithme d'extraction de l'ID à partir de l'image et de l'empreinte 116
3 Insertion de notre algorithme dans un protocole complet assurant la protection des droits d'auteurs 119
3.1 Protocole d'enregistrement du copyright d'une image 119
3.2 Protocole de vérification du copyright 119
3.3 Justifications des choix effectués lors de la définition des protocoles 121
4 Evaluation de l'algorithme : un nouveau compromis robustesse / collision d'identification 122
5 Conclusion 123

Chapitre 6
Application aux services de sécurité des algorithmes de tatouage et d'empreinte externe : une étude comparative 127

1 Critiques de la méthode par empreinte externe, comparativement à une approche par tatouage ou autre stratégie 128
1.1 Avantages sur les techniques de tatouage 128
1.2 Avantages sur l'enregistrement du document original lui-même . . . 129
1.3 Limites de l'application de l'empreinte externe 130
2 Comment l'empreinte externe peut répondre à différents scénarii dans le contexte de la protection du copyright 130

2.1 Conflit direct entre deux individus 130
2.2 Vérification du copyright d'une image par un individu quelconque . 130
2.3 Echec à la mise en place de réseaux de ventes parallèles et recèles . 131
3 Notariat électronique par empreinte externe 132
4 Service d'intégrité par tatouage d'image 134
4.1 Service d'intégrité par tatouage fragile 134
4.2 Service d'intégrité par contrôle d'attributs de l'image 134
5 Conclusion 137

Chapitre 7
Conclusions et Perspectives **139**

1 Conclusions 140
2 Perspectives 140
2.1 Algorithmes capables d'intégrer de nouvelles attaques 140
2.2 Tatouage à résistance aléatoire 141
2.3 Intégrité 141
2.4 Extension à la vidéo et à d'autres media 141

Annexe A
Images extraites des simulations sur l'algorithme de tatouage **143**

1 Images originales et images tatouées 143
2 Résistance du tatouage face à une compression Jpeg 147
3 Résistance du tatouage face à des manipulations géométriques 151
4 Résistance du tatouage face à des requantifications 157
5 Résistance du tatouage face à Stirmark et Unzign 159

Bibliographie **161**

Mes publications et brevets **169**

Liste des abréviations

CA contrôle d'accès

DCT transformation en cosinus discrète

DWT transformation en ondelettes discrète

RSA Rivest, Shamir et Adleman (système de cryptage à clé publique)

MSB bits les plus significatifs

LSB bits les moins significatifs

RGB système de coordonnées chromatiques rouge, vert, bleu

HSV système visuel humain

MPEG moving picture experts group (norme de compression vidéo)

JPEG joint photographic expert group (norme de compression d'image)

JBIG joint bi-level image group (norme de compression fax)

GIF graphics interchange format

PN bruit pseudo-aléatoire

ID identificateur

E-ID

PSNR rapport signal à bruit

Xor opérateur logique ou exclusif

Table des figures

Chapitre 1

1 *Schéma de principe du service de CA* 9
2 *Photocopieuse à réduction multiple* 12
3 *Fonctions itérées* 12
4 *Fougère de Barnsley, générée à partir d'un système de quatre fonctions itérées* 13
5 *Codage d'image par fonctions itérées* 15
6 *Décodage d'image par fonctions itérées* 16
7 *Différents niveaux de CA* 17
8 *Dépendance entre les blocs cibles et les blocs sources* 20
9 *Treillis et génération de clés* 21
10 *Codage fractal vidéo : approche 2D plus prédiction* 22
11 *Codage fractal vidéo : approche 3D* 23
12 *Contrôle d'accès localisé pour garantir l'anonymat* 24
13 *Serveur d'images multi-access* 25
14 *Diffusion satellitaire de services Multimédia* 26

Chapitre 2

1 *Dispositif générique d'un système de tatouage* 30
2 *Deux philosophies pour assurer le service d'intégrité.* 32
3 *Garantir l'intégrité d'une image par tatouage d'une mire de référence.* . . . 33
4 *Garantir l'intégrité d'une image par tatouage de caractéristiques de l'image.* 34
5 *Service de protection de la propriété intellectuelle par tatouage d'image* . . 35
6 *Couplage d'un système de tatouage et de confidentialité en vue d'assurer un service de non répudiation de l'accès à une image* 38
7 *Masquage partiel d'une image par tatouage* 39
8 *Répartition de l'énergie au niveau du spectre de fréquence* 41
9 *Schéma de réhaussement du contraste par filtrage* 42
10 *Manipulation d'image par Stirmark* 45
11 *La mosaïque d'image, une parade aux détecteurs automatiques de tatouage* 46
12 *Protocoles de sécurité* 48
13 *Mode d'extraction assisté (non aveugle)* 51
14 *Mode d'extraction semi-aveugle* 52

15 *Mode d'extraction aveugle* 52
16 *Modélisation du problème de tatouage : point de vue perceptif* 53

Chapitre 3

1 *Schéma de principe de la compression JPEG* 65
2 *Construction d'un espace invariant par translation, rotation et changement d'échelle* 66
3 *Décomposition et reconstruction multi-échelle* 68
4 *Décomposition multi-échelle 2-D* 68
5 *Principe d'étalement de spectre par séquence directe* 71
6 *Bloc cible et les deux sous fenêtres de recherche associées* 78
7 *Invariance d'un attracteur et de sa transformée associée* 78
8 *Seuillage adaptatif* 80
9 *Schéma d'attaque par pseudo-tatouage inverse* 86

Chapitre 4

1 *Point de vue classification du codage fractal* 94
2 *Les différents cas relatifs à la translation de l'image tatouée* 95
3 *Primitive hexagonale glissante autorisant des transformations plus fines, favorable à une extension des invariances* 97
4 *Schéma d'insertion du tatouage* 99
5 *Schéma d'extraction du tatouage* 100
6 *Types de signature supportés* 100
7 *Sur-échantillonnage du logo* 101
8 *Duplication du logo* 102
9 *Association entre les bits de signature* 105
10 *Discrétisation du dictionnaire et erreur de reconstruction* 106
11 *Principe du recalage par maximisation de cohérence* 107

Chapitre 5

1 *Fonction de hachage* 114
2 *Principe de l'empreinte externe* 115
3 *Algorithme de création de l'empreinte* 117
4 *Algorithme de vérification de l'empreinte* 118
5 *Protocole d'enregistrement du copyright d'une image* 120
6 *Protocole de vérification du copyright d'une image* 121

Chapitre 6

1 *Cas conflictuel d'un acheteur victime d'un usurpateur* 131
2 *Résolution du conflit si seul P a protégé l'image* 131
3 *Résolution du conflit si AU a également protégé l'image* 132

4 *Signature de contract électronique pour l'achat d'une image* 133
5 *Tatouage itératif d'attribut de l'image* 135
6 *Résultats d'intégrité par tatouage* 136

Liste des tableaux

Chapitre 1

1 *Exemples de masquage d'un paramètre* s_k 18

Chapitre 2

1 *Récapitulatif des différents services et des propriétés des tatouages associés* 40

Chapitre 4

1 *Résistance du tatouage face à des niveaux croissant de compression JPEG* . 111
2 *Exemples de tests de robustesse de l'algorithme de tatouage face à diverses manipulations de l'image.* 112

Chapitre 5

1 *Exemples de tests de robustesse de l'algorithme d'empreinte externe face à diverses manipulations de l'image.* 124
2 *Résistance de l'indentificateur face à des niveaux croissant de compression JPEG* 125

Introduction générale

Initiée en septembre 1995, cette thèse trouve son origine, d'une part dans les connaissances du laboratoire en codage de source et en particulier en codage fractal [77, 23, 21], d'autre part dans les préoccupations sans cesse croissantes d'adjoindre au service de compression de données d'autres types de services, notamment pour assurer des fonctions de sécurité. Cette évolution est attestée entre autres par différents standards en cours comme MPEG qui, outre l'aspect compression, propose des facilités pour indexer, sécuriser, voire composer des scènes. L'émergence des supports numériques, tant pour la transmission que pour le stockage, a précipité cette évolution. Aujourd'hui, la production massive de nouvelles images et vidéo, la copie et la diffusion de celles-ci sont accessibles à un large public. Les copies peuvent être réalisées en grand nombre, sans perte de qualité. De plus, une visibilité mondiale est accessible à quiconque dispose d'un accès internet, facilitant une diffusion massive de l'information comme l'image, la vidéo et l'audio. Cette évolution n'est pas sans poser d'importants problèmes de droits d'auteur. Cette révolution ne comporte pas que des aspects négatifs, elle est potentiellement le vecteur du développement de nouveaux services à forte valeur ajoutée à condition d'en maîtriser les mutations technologiques nécessaires. Parmi ces nouvelles offres, certains opérateurs de télédiffusion proposent un choix de programmes à la carte excessivement varié impliquant une gestion de flots de données très importants ; de nombreux choix dans la visualisation d'un événement sont maintenant laissés à l'initiative de l'utilisateur, il peut par exemple sélectionner l'angle de prise de vue d'une action sportive, visionner la version orignale ou la version sous-titrée d'un film. Autant de nouveaux besoins pour lesquels d'importants mécanismes de sécurité sont requis. Cette thèse a pour champ d'application les données de type image fixe, nous n'excluons pas toutefois la possibilité d'étendre les algorithmes proposés à d'autres types de données multimédia, en particulier à la vidéo ou au son. La nécessité de proposer des algorithmes spécifiques pour assurer des fonctions de sécurité se justifie par la nature même des données traitées ainsi que par l'utilisation finale qui en est faite. Les données multimedia se caractérisent par un très grand volume d'information présentant une redondance élevée. Dans la plupart des applications où interviennent ces trois types de données (image fixe, vidéo, audio), l'homme est l'utilisateur final, à travers des systèmes perceptifs (visuel ou auditif) caractérisés par une grande complexité ainsi qu'une forte subjectivité. Comme en codage de source où les performances en termes de taux de compression sont à ramener à la qualité visuelle ou auditive obtenue, nous retrouverons des compromis similaires, en termes de sécurité comparativement à l'impact psychovisuel. La notion de sécurité pour les images est relativement récente et de nombreux besoins ne sont pas encore clairement identifiés. Néanmoins, on distingue deux grandes familles de

problèmes : La première dont la finalité est de garantir la confidentialité d'un document en masquant son contenu aux personnes non autorisées, la seconde qui répond aux problèmes de protection de droits d'auteur et de vérification d'intégrité d'image. Notons que ces deux principales classes de problèmes sont parfaitement complémentaires. Il serait abusif de considérer la confidentialité comme le degré de sécurité ultime dispensant de toute autre protection. En effet, une fois l'image décryptée, aucun contrôle *a posteriori* ne peut être effectué sur cette image et /ou ses éventuelles copies. Une analyse approfondie des besoins est donc nécessaire pour sélectionner un ensemble de techniques adaptées à chaque problème. Historiquement, les problèmes de confidentialité ont été les premiers à retenir l'attention. Ils ont par exemple été traités dans une utilisation grand public afin de limiter l'accès aux chaînes hertziennes à péage.

Dans le **chapitre 1**, nous proposons une contribution sur le thème du contrôle d'accès par le biais d'une extension de notre codeur/décodeur basé sur une approche fractale. Comme il a été mentionné précédemment, la restriction de l'accès à des images dans le contexte d'un service à péage est une fonctionnalité de plus en plus souvent requise. L'évolution de cette demande va dans le sens d'une personnalisation croissante des services proposés. On peut citer parmi eux, la télévision à la carte, les bibliothèques virtuelles et les serveurs d'agence photo. Pour ces derniers, il peut être intéressant de laisser libre accès à l'ensemble des images mais avec un niveau de qualité très dégradé, constituant ainsi une prévisualisation puis, après achat des droits de certaines photos par les clients, de leur autoriser rapidement un accès « pleine qualité ». Nous montrerons dans le chapitre 1 qu'il peut être avantageusement tiré parti de propriétés inhérentes au codage fractal pour y adjoindre ce type de service. L'auto-similarité constitue l'une de ces propriétés intéressantes. Elle caractérise le fait qu'une même information est présente à différents niveaux dans l'image. Ceux-ci peuvent par exemple constituter différents niveaux de résolutions, ouvrant ainsi une voie pour mettre en place un service de contrôle d'accès multi-résolution.

Après avoir envisagé les potentialités du codage fractal appliqué au contrôle d'accès, nous nous éloignerons de l'aspect codage de source pour aborder les services de protection des droits d'auteur et d'intégrité des documents. L'une des voies les plus prometteuses pour assurer de tels services, réside dans les méthodes dites de tatouage (watermarking). L'idée principale consiste, dans le cas d'une image, à insérer dans celle-ci une information pouvant être utilisée *a posteriori* pour attester par exemple, de la propriété ou d'une falsification (substitution de certaines régions) de l'image. La force de ces approches réside dans leur indépendance vis-à-vis du format de stockage ou de transmission adopté pour le document. Les techniques de tatouage offrent une alternative aux méthodes classiques utilisant un en-tête de fichier pour spécifier des informations relatives à la sécurité de l'image. Dans ce cas l'information contenue dans l'en-tête est pratiquement toujours perdue si l'on opère une conversion de format. Nous dresserons dans le **chapitre 2**, un panorama des problématiques associées aux différents champs d'applications des techniques de tatouage. Nous définirons la notion de tatouage au travers de ses différentes déclinaisons : visible, non-visible, robuste à tout type de manipulations, robuste à des manipulations non malveillantes de l'image du type compression de données. Bien que la modélisation de ces problèmes soit toujours délicate en raison par exemple de paramètres psychovisuels eux- mêmes mal modélisés, nous nous efforcerons de présenter les modélisations adoptées, révélatrices des différents points de vue sous lesquels les problèmes ont

été abordés.

Un état de l'art des méthodes de tatouage d'image sera dressé au **chapitre 3**. Nous positionnerons ces méthodes par rapport aux différentes problématiques décrites dans le chapitre précédent. Nous avons opté pour un découpage du chapitre respectant un schéma générique de tatouage. Pour chaque étape de ce schéma, nous discuterons les différentes solutions et alternatives proposées dans la littérature. Ce découpage permet de couvrir un large éventail des techniques présentées à ce jour. Il inclut les méthodes issues de la communauté codage de source, on y retrouvera en particulier les algorithmes opérant dans les domaines transformés : DCT, Ondelette, Fractal ; les techniques issues de la théorie des communications, à ce titre les techniques d'étalement de spectre et de construction de détecteurs optimaux trouvent également leur place dans cette présentation.

Dans le **chapitre 4**, nous présenterons notre contribution sur le thème du tatouage d'image. Un schéma complet comprenant les phases d'insertion et d'extraction du tatouage y sera décrit. L'information, que l'on souhaite introduire dans l'image peut prendre la forme d'un logo, d'une chaine de caractères ascii, d'un numéro d'identification etc. Cette information doit subir une opération de mise en forme préalablement à son introduction dans l'image. Cette opération vise d'une part à adapter les données à transmettre au canal constitué par l'image, et d'autre part à assurer un cryptage de l'information éventuellement nécessaire pour augmenter la difficulté à extraire l'information de tatouage pour une personne non autorisée ou pour constituer des services de non répudiation basés sur un cryptage à clé publique. Parmi les opérations de mise en forme de l'information, nous détaillerons particulièrement la stratégie d'ajout de redondance pour faire face aux différents types d'attaques exposés au chapitre 2. Les degrés de liberté de notre algorithme permettant la prise en compte de la contrainte d'invisibilité du tatouage seront discutés au regard de leur impact sur la robustesse du tatouage. Nous montrons comment il est possible de paramétrer l'algorithme afin de satisfaire l'invisibilité du tatouage, qui peut être plus ou moins cruciale suivant la qualité de l'image originale et/ou l'exigence du client. Le problème de resynchronisation lors de la procédure d'extraction du tatouage, en particulier lors de manipulations de l'image de type transformation géométrique : translation ou rotation sera étudié en détail.

L'existence du compromis : robustesse du tatouage *vs.* qualité de l'image tatouée ainsi que le problème du datage du tatouage rencontré dans tous les systèmes, nous ont conduits à proposer une alternative. Cette nouvelle approche présentée au **chapitre 5** s'affranchit totalement des problèmes de visibilité puisqu'aucune modification de l'image n'est réalisée. Nous introduirons la notion d'empreinte externe qui constitue une signature du couple (image, propriétaire) ou de toute autre entité numériquement identifiable. Cette signature possède des propriétés de robustesse analogue au tatouage. Le nouveau compromis robustesse *vs.* collision d'identification sera discuté en détail.

Les deux algorithmes développés durant cette thèse ont permis d'envisager différentes applications dans le domaine de la sécurité des images, le **chapitre 6** se propose de les détailler. Nous montrerons en particulier la complémentarité des deux approches (tatouage, empreinte externe) découlant de la spécificité des deux algorithmes. Nous procéderons à une étude comparative des deux algorithmes. Les évaluations récentes des systèmes de tatouage ont révélé que de nombreuses failles existaient dans la mise en place des algorithmes de tatouage. La résistance du tatouage et la non visibilité de celui-ci ne peuvent

constituer les seuls paramètres à prendre en compte. Pour certains types d'applications, en particulier celles dédiées à la résolution des problèmes de droits d'auteur, il est nécessaire de faire une étude approfondie des protocoles à mettre en place pour le dépôt de l'image afin notamment de prendre en compte les possibilités de sur-signature de l'image. Ce point fait l'objet d'une partie importante de ce chapitre au-delà des aspects robustesse et invisibilité traités dans les chapitres 4 et 5. Nous terminerons cette thèse avec le **chapitre 7** relatif aux perspectives offertes par les systèmes de tatouage et d'empreinte externe. Nous analyserons les points constituant encore un obstacle à une introduction massive de systèmes de tatouage dans les applications dédiées aux documents multimedia. Nous donnerons quelques exemples de nouvelles applications qui pourraient naître des nouvelles avancées des méthodes de tatouage. Enfin, nous aborderons la possibilité d'étendre le tatouage d'image à d'autres applications que celles de sécurité. Nous mentionnerons l'intérêt que peut constituer le tatouage d'image pour la recherche dans des bases de données et l'archivage automatique de documents multimedia.

Distribution des rôles

Les processus de sécurité mettent en oeuvre différentes entités interagissant entre elles et donnant lieu à des scénarii parfois complexes. Pour clarifier le discours, il est d'usage en sécurité de représenter chaque entité par des personnages que l'on identifiera par leur prénom.

Nous avons distribué les rôles comme suit :

- Alain : l'auteur, ou le propriétaire d'un bien. Dans notre cas, il s'agira le plus souvent d'une image.
- Claire : la cliente d'Alain
- Julien : le juge amené à trancher d'éventuels conflits. Ce personnage sera systématiquement intègre et non corruptible.
- Isabelle : joue le rôle de l'imposteur, elle est systématiquement malhonnête.

Nous avons décrit dans les grandes lignes, le rôle des différents personnages. Nous donnerons s'il y a lieu des précisions sur leur rôle respectif, au fil de la thèse en fonction du contexte dans lequel ces personnages interviennent.

Chapitre 1

Contrôle d'Accès : CA

L'émergence de services à la carte, telles la télévision interactive, les bibliothèques virtuelles a rendu nécessaire la personnalisation des applications délivrant ces services. Le CA proposé dans ce chapitre offre la possibilité de fournir des accès aux données à différents niveaux de qualité, suivant par exemple le montant des droits payés. Nous montrerons dans ce chapitre qu'il peut être avantageux de coupler un algorithme de compression de données à un mécanisme de CA. Une application de ce système est constituée par la prévisualisation d'image à travers le web. Cette prévisualisation met à disposition des images sur lesquelles est apposé un tatouage visible rendant difficile une utilisation commerciale de l'image.

1 Remarque introductive

Ce chapitre s'inscrit dans cette thèse comme une première tentative de dérivation d'algorithmes de codage de source afin de délivrer un service de sécurité. Nous combinerons dans un même schéma, la fonction initiale de tout codage de source, c'est-à-dire la compression de données avec un service de contrôle d'accès. Ce premier chapitre visera également, au travers du problème de contrôle d'accès, à attirer l'attention du lecteur sur les spécificités des notions de sécurité lorsqu'elles sont appliquées à des données multimédia et en particulier à des images. Certaines approches « classiques », issues principalement du monde informatique doivent être reconsidérées. Le schéma de contrôle d'accès envisagé est basé sur le codage fractal. Après un rappel sur les fondements de ce type de codage, nous montrons comment il est possible de tirer partie de la propriété de convergence, inhérente à ce codeur, pour délivrer de façon progressive des images à différents niveaux de qualité. La dernière partie de ce chapitre est dédiée à la présentation d'applications dans lesquelles un tel schéma peut avantageusement s'insérer. Nous décrirons notamment un service de prévisualisation d'images.

2 Positionnement et problématique du CA

2.1 Eléments de CA admis en sécurité

Le CA est un service largement répandu en sécurité, on le retrouve dans le domaine bancaire, les applications commerciales via Internet, les systèmes informatiques multi-utilisateurs, ainsi que dans les applications de type intranet. Bien qu'il existe de nombreuses variantes de ce service, on peut le définir, d'une façon générale, comme la personnalisation de l'accès à des ressources (information, application, etc.) suivant la catégorie d'appartenance de l'utilisateur (utilisateur privilégié, utilisateur externe à une société, etc.). Le CA comprend généralement plusieurs phases (fig. 1) :

- la première est l'authentification des utilisateurs ;
- la seconde est constituée par la politique d'accès aux ressources (accès partiel, total etc.) ;
- et enfin, on prend éventuellement en compte l'acheminement sécurisé des ressources jusqu'à l'utilisateur.

Afin de mieux appréhender les différents aspects de ce problème et d'éventuellement dégager par la suite des spécificités liées aux images, nous nous proposons d'examiner sommairement quelques applications où un CA intervient.

Dans le système de fichiers Unix, l'utilisateur s'identifie auprès du serveur via une procédure de connexion au cours de laquelle, il communique un mot de passe. La politique d'accès aux ressources du système distingue trois types de droits : le droit en lecture, en écriture et en exécution. Pour ce qui concerne le droit en lecture, l'accès au fichier est autorisé exclusivement par le biais de fonctions systèmes prédéfinies : `read, more, cp,`

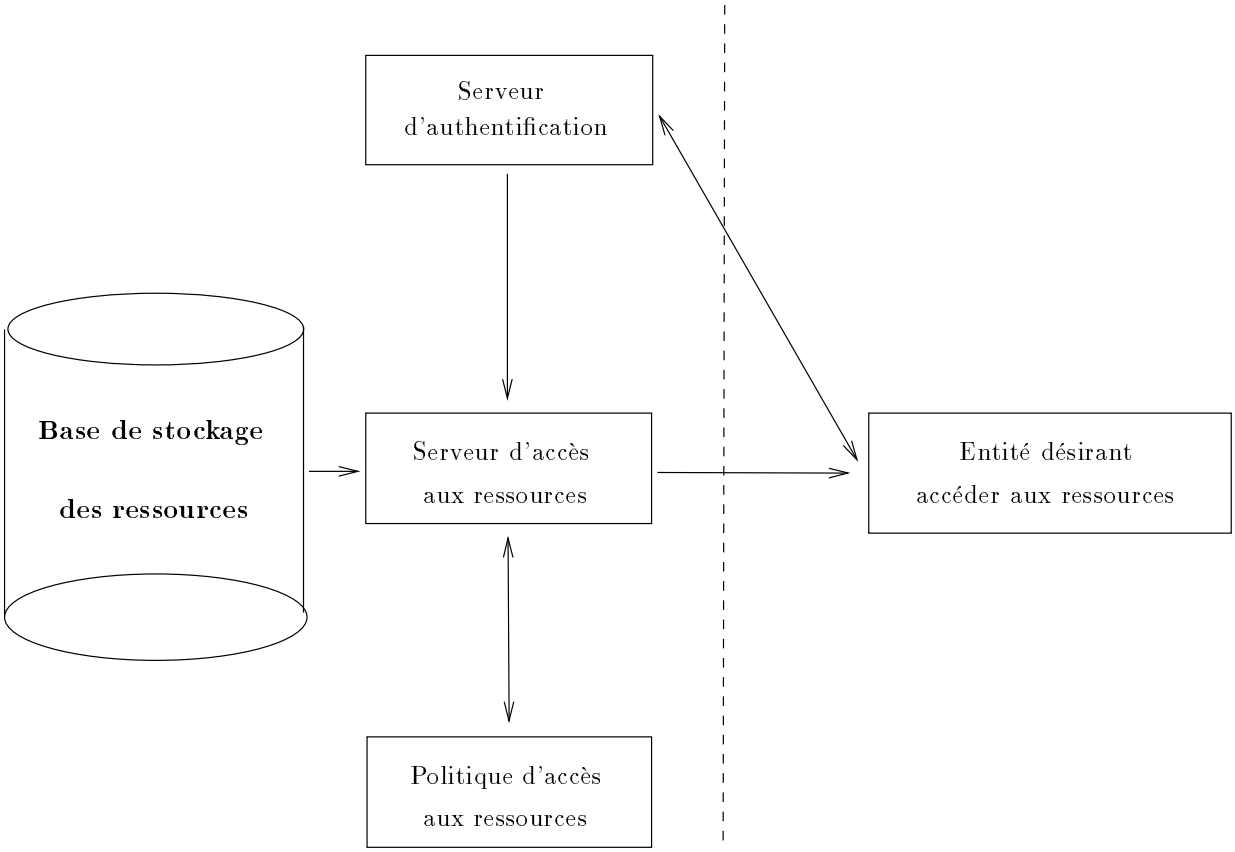


FIG. 1 – *Schéma de principe du service de CA*

etc. Ceci permet ainsi une limitation des opérations pouvant être entreprises par un utilisateur ne disposant que d'un droit de lecture. Le propriétaire de chaque fichier a en charge la spécification des droits pour les fichiers lui appartenant. Il doit positionner les droits vis-à-vis de lui-même, d'un utilisateur membre de son groupe ainsi que d'un utilisateur quelconque. A partir de ces informations, le système construit une matrice d'accès stockant pour chaque ressource les droits d'accès conférés à telle ou telle classe d'utilisateur. C'est sur la base de ces spécifications que le serveur de fichiers autorise éventuellement l'accès d'un fichier à un utilisateur connu du système. Le CA prend place au niveau du serveur de fichier, dans la plupart des systèmes informatiques aucune mesure de sécurité n'est prise lors de la transmission entre ce serveur et les utilisateurs. Un intrus écoutant le réseau peut tout à fait intercepter des données qui ne lui étaient pas initialement destinées. Cette absence de protection se justifie par les pénalités en termes de délais de services qu'entraînerait le chiffrement systématique des données entre le serveur et les utilisateurs. On touche là un des aspects fondamentaux des mécanismes de sécurité qui doivent concilier un degré de protection élevé à une relative transparence pour les utilisateurs. La notion de CA est également présente dans d'autres domaines que l'informatique. Certains systèmes de distributeurs de billets automatiques mettent en oeuvre un CA se limitant à une phase d'authentification. Le possesseur de la carte à puce introduit son code d'accès, le distributeur se contente de vérifier que le code saisi est identique à celui gravé sur la puce et autorise ou interdit alors la distribution de billets. Dans ce système, il est important de noter que la confidentialité dans les échanges (code secret et billets) est obtenue par la simple proximité entre le client et la machine, ce qui limite l'intervention d'un intrus.

2.2 Spécificités du problème dans le domaine de l'image

Les politiques de sécurité envisagées au paragraphe précédent, faisant « l'économie » d'un cryptage des données sur lesquelles s'applique le CA, trouvent place dans le cas où le support de transmission est physiquement protégé. Cette exigence n'est nullement remplie dans de nombreux systèmes manipulant des images. En effet, les images ont pour vocation d'être largement diffusées sur des supports bien souvent pas ou peu protégés. Les transmissions satellites qui constituent un mode de communication émergeant pour la diffusion de programmes télévisuels en sont un exemple. Il faut donc impérativement intégrer au CA un cryptage des données lors de leur acheminement entre le ou les serveurs et l'utilisateur, et ce avec le coût le plus faible possible. Le type de chiffrement à envisager pour des images ou de la vidéo revêt lui-même un caractère particulier. Il existe une certaine tolérance dans l'accès aux données. Par exemple, on ne peut pas considérer que les chaînes à péage pratiquent un chiffrement total de la vidéo, on distingue aisément la présence de personnages, cependant ce type de cryptage suffit pour contraindre les téléspectateurs désireux de voir les programmes de ces chaînes à souscrire un abonnement. Excepté le domaine militaire, le chiffrement total de l'image ne concerne que très peu d'applications, on se contente souvent d'un masquage partiel rendant inutilisable l'image. On note ici une différence fondamentale par rapport au domaine bancaire par exemple où la confidentialité doit être assurée de façon totale. Cette disparité quant aux contraintes d'accès aux données explique en partie la nécessité de développer des algorithmes spécifiques pour les

images et la vidéo. Un autre point important est lié à la nature très redondante des données à traiter. Un individu souhaitant s'approprier illicitement une image peut tenter de tirer profit de la nature très redondante de l'image pour prendre en défaut un algorithme de chiffrement. Nous reviendrons en détail sur ce point au paragraphe 4.3 de ce chapitre. Enfin, des problèmes de mise en oeuvre sont également déterminants. En effet, les images et à plus forte raison la vidéo constituent des volumes d'informations très importants or la plupart des algorithmes de chiffrement ont des coûts calculatoires fonctions du volume d'informations traitées. Dans le choix d'un dispositif de sécurité, la robustesse du système n'est pas la seule caractéristique à prendre en compte. Le dispositif se doit d'être dissuasif vis-à-vis de la majorité des utilisateurs sans être trop contraignant. Le système « idéal » se caractérise donc par un faible impact de la sécurité sur le fonctionnement du service, en termes de :

- sur coût en temps de calcul, et donc délais de service ;
- volume d'information supplémentaire par rapport aux données compressées non sécurisées.

3 Rappels sur le codage fractal

Dans cette section, seules les grandes lignes du codage fractal sont exposées. Le lecteur non familier avec cette technique est invité à consulter une ou plusieurs des références suivantes [34, 47, 48, 77]. Apparu à la fin des années 80 suite aux travaux de M. Barnsley et A. Jacquin [2], le codage fractal trouve son origine dans les systèmes de fonctions itérées developpés par Hutchinson [46]. Cette thèse ne se veut pas un exposé complet sur de tels systèmes, nous nous contenterons d'en donner une notion intuitive au travers de la « photocopieuse à réductions multiples ».

3.1 Photocopieuse à réductions multiples et système de fonctions itérées

Considérons une photocopieuse d'un type un peu particulier. En effet, suivant la procédure définie par la figure 2, cette machine réduit de moitié le document à copier, puis en crée trois reproductions disposées en triangle sur le document « photocopié ». Envisageons maintenant l'utilisation d'une telle photocopieuse en boucle, c'est-à-dire que le document de sortie constitue le document d'entrée de la prochaine photocopie. Il est surprenant de constater qu'après quelques itérations d'un tel processus, le motif obtenu est indépendant de la nature du document initial comme l'atteste la figure 3. Le résultat final dépend uniquement de la « programmation » de la photocopieuse précisant la transformation du document original réalisée lors d'une « reproduction ». De telles photocopieuses, avec un jeu d'instructions (paramètres) réduits, permettent de représenter des objets d'une grande complexité apparente avec un réalisme très proche d'objets naturels. La fougère de Barnsley (fig. 4) en est un exemple. Cette fougère peut être décrite intégralement à l'aide des

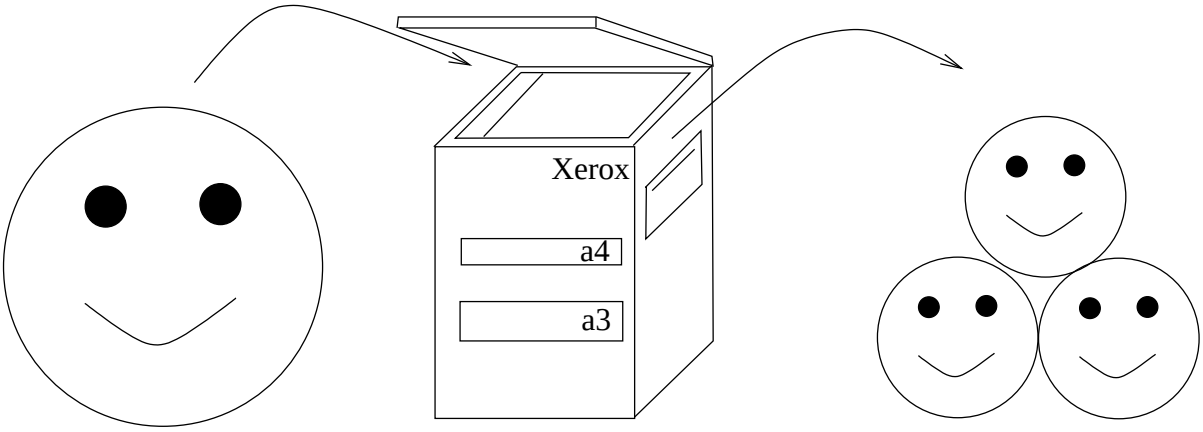


FIG. 2 – *Photocopieuse à réduction multiple*

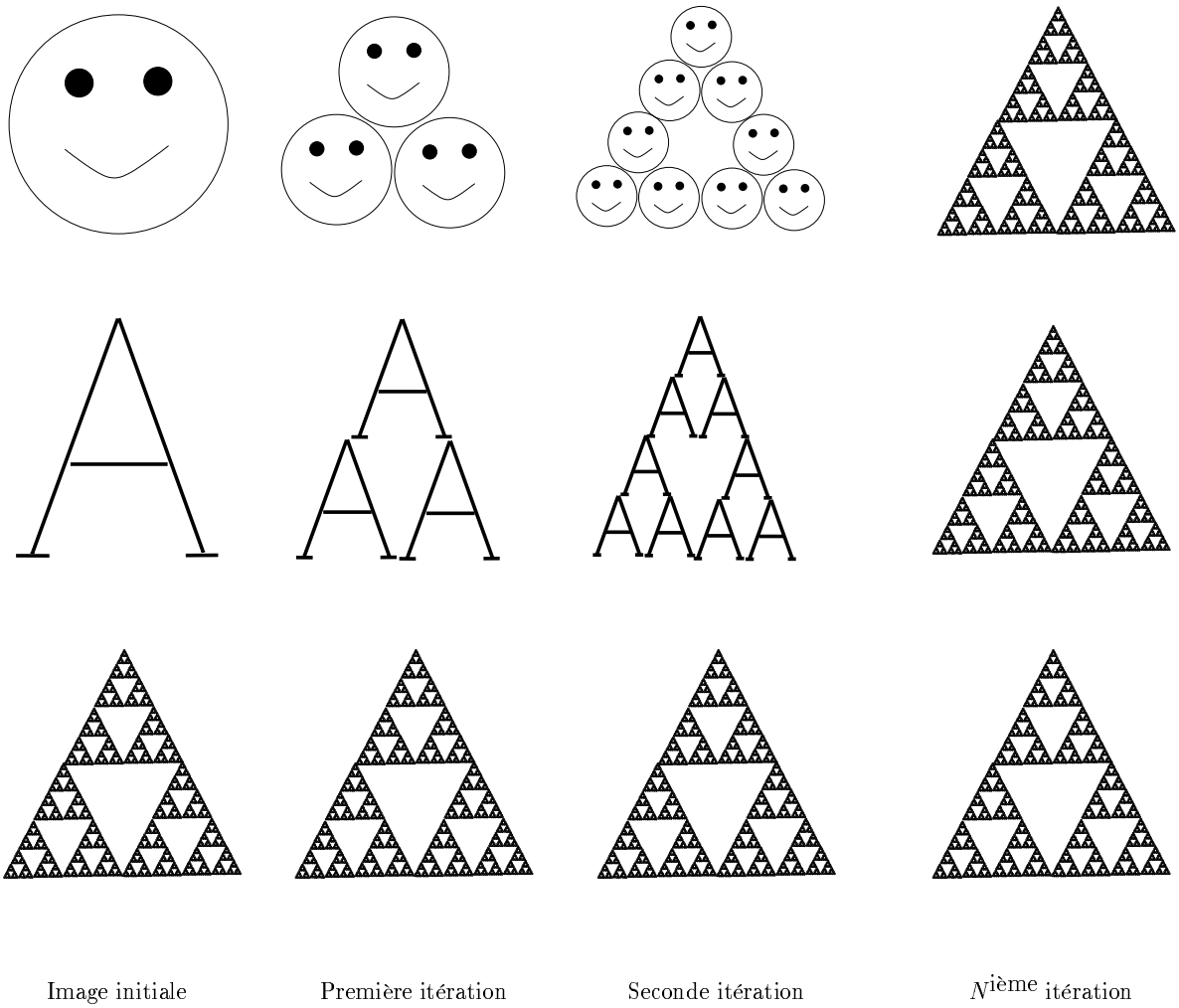


FIG. 3 – *Fonctions itérées*

FIG. 4 – *Fougère de Barnsley, générée à partir d'un système de quatre fonctions itérées*

quatre transformées suivantes.

$$w_1 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0.85 & 0.04 \\ -0.04 & 0.85 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0.02 \\ 0.08 \end{bmatrix}$$

$$w_2 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -0.13 & 0.24 \\ -0.22 & 0.20 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0.12 \\ -0.27 \end{bmatrix}$$

$$w_3 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0.18 & -0.24 \\ 0.21 & 0.20 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} -0.12 \\ -0.30 \end{bmatrix}$$

$$w_4 \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0.16 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 0 \\ -0.42 \end{bmatrix}$$

Il est clair que le codage de cette fougère pixels par pixels (bitmap) ou même sous une forme compressée (*via* Jbig par exemple) représente un volume d'information bien supérieur au codage des coefficients des matrices ci-dessus. On entrevoit ici la possibilité d'utiliser de tel système pour effectuer un codage de source efficace. Il est possible de décrire une image uniquement par un ensemble de transformations.

Il convient à présent de préciser certaines propriétés requises par ces transformations. Afin que le processus itératif converge, c'est-à- dire qu'il admette une limite, les transformations utilisées doivent être contractantes.

Définition 1 (Transformation contractante) *Soit Ω l'espace des images muni d'une*

métrique d. Soient u et v deux images appartenant à cet espace. On dit que la transformation w de Ω dans Ω est contractante si et seulement si :

$$\forall u, v \in \Omega \quad d(w(u), w(v)) < d(u, v)$$

Définition 2 (Attracteur) *Soit w une transformation contractante définie sur l'espace des images (Ω,d). On appelle attracteur associé à w, l'élément x_a de (Ω,d) s'il existe défini par :*

$$x_a = \lim_{n \to \infty} w^n(x_0)$$

où $w^n(x_0)$ désigne la n^e composition de w par elle-même calculée au point x_0.

Théorème 1 (Invariance) *Tout attracteur x_a d'une transformation contractante w est un invariant de cette transformation.*

$$x_a = w(x_a)$$

La notion de transformée contractante induit une invariance de l'attracteur par rapport à l'image initiale.

L'idée sous-jacente au codage fractal est de déterminer une image x_a « proche » de x_c sur le plan perceptif et pouvant être représentée efficacement 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.

3.2 Algorithme de codage

L'objectif du codage est d'assurer la convergence du processus itératif vers un point fixe (attracteur 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 dont :

1. La première est constituée par le modèle de transformation W adopté. 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.

Le principe du codage consiste d'une part à écrire la propriété d'invariance d'un attracteur : $W(x_a) = x_a$ et d'autre part à postuler l'existence d'un attracteur proche de l'image que l'on souhaite coder, autrement dit : $d(x_c, x_a) \to 0$. On est alors amené, sous les contraintes (1) et (2), à chercher parmi l'espace des solutions, la transformée W tel que $d(W(x_c), x_c) \to 0$.

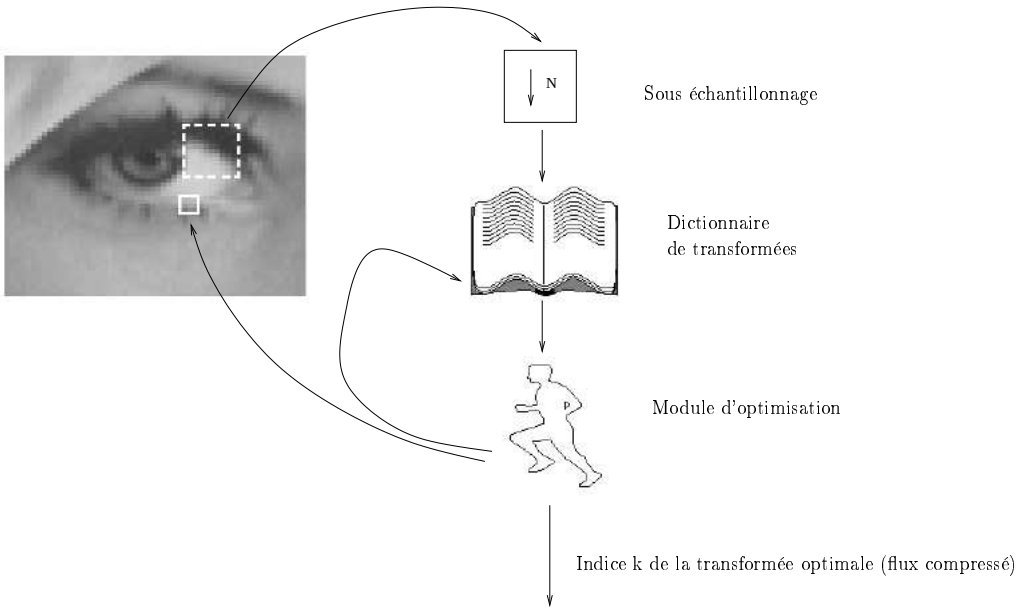


FIG. 5 – *Codage d'image par fonctions itérées*

Ce problème d'optimisation présente une complexité calculatoire trop élevée pour être résolu directement. On procède généralement à la réduction de cette complexité en adoptant des transformations locales W_k blocs à blocs en remplacement de la transformation globale W initialement proposée. Le nouveau problème consiste à déterminer les paramètres s_k, o_k et l'isométrie associés à chaque bloc B_k constituant une partition de l'image (fig. 5). Le flux codé est constitué d'une liste d'indexes faisant référence pour chaque bloc à la transformation associée (l'ensemble des transformées étant compris dans un dictionnaire).

3.3 Algorithme de décodage

Le décodage (fig. 6) consiste à exécuter le processus itératif. Pour ce faire, à partir des indexes contenus dans le flux compressé, on identifie parmi le dictionnaire des transformations, celle qui doit être appliquée à un bloc B_k donné. Une fois cette opération réalisée pour chaque bloc B_k, on applique les transformées W_k et l'on réitère le processus à la manière de la photocopieuse itérative. L'initialisation du processus correspond au choix de l'image d'origine sur laquelle sont appliquées les transformées.

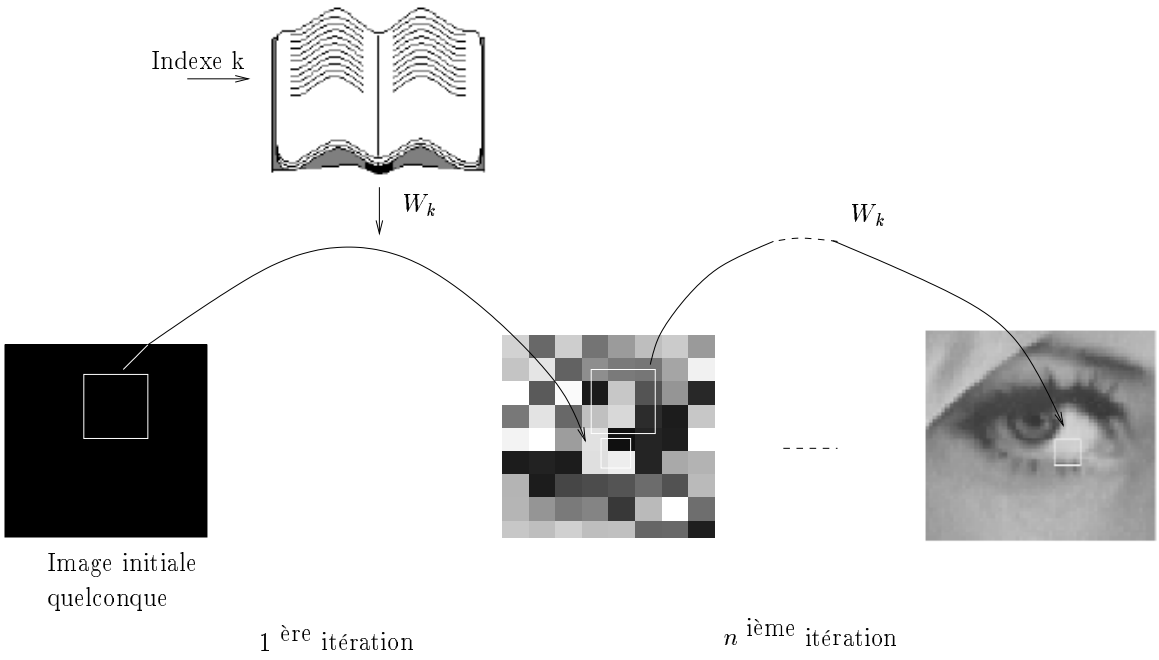


FIG. 6 – *Décodage d'image par fonctions itérées*

4 Le couplage du CA à l'algorithme de compression

4.1 Convergence et CA

Le CA est obtenu en agissant sur le niveau de reconstruction du processus itératif de décodage [82]. Nous proposons de perturber la convergence en modifiant les paramètres d'échelle s_k de la transformation photométrique. De manière pratique, nous masquons partiellement les valeurs binaires de ces paramètres (tab. 1). Nous reviendrons sur la technique de masquage au paragraphe 5, considérons simplement pour l'instant qu'il s'agit d'un processus fixant aléatoirement à 0 ou 1 la valeur des bits à masquer. Un masquage total entraîne une dégradation presque totale de l'image (fig. 7a) alors que la divulgation progressive des bits permet de tendre vers l'image originale (fig. 7d). Il est important de noter que l'opération de masquage conserve à la transformée sa propriété de contractivité. Les valeurs de s_k sont en effet toujours comprises entre -1 et 1. Le masquage des paramètres s_k conduit à une modification du point de convergence et non à une divergence incontrôlée du processus de décodage.

7.a niveau g

7.b niveau e

7.c niveau c

7.d niveau a

FIG. 7 – *Différents niveaux de CA*

	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	×	×	×	×	×	×	×	×

TAB. 1 – *Exemples de masquage d'un paramètre s_k : (a) sans cryptage jusqu'à (g) cryptage total. Le symbole × désigne un bit dont la valeur est aléatoirement 0 ou 1*

4.2 La stratégie de masquage face aux problèmes de sécurité

Les différentes faiblesses (possibles) en termes de sécurité propres à un tel système sont constituées par :

- des attaques par filtrage visant à rendre un aspect acceptable à l'image par des opérations de traitements d'image ;
- une attaque exhaustive sur les valeurs de s_k masquées ;
- une attaque basée sur la corrélation existant entre des régions proches d'une image ;
- une corrélation éventuelle entre différentes données du code, par exemple dans notre cas entre les paramètres s_k et o_k.

Comme décrit dans la section précédente, le critère d'optimisation nécessite l'image originale. Cette condition n'est bien évidemment pas remplie pour une personne lambda, dès lors elle ne peut mettre en place le critère mis en oeuvre pour le codage.

4.3 Entropie et sécurité : codage de source et sécurité

Shannon a introduit la notion « d'incertitude sur la clé » [84] pour mesurer le niveau de sûreté d'un système. L'incertitude sur la clé est définie selon Shannon comme l'entropie conditionnelle d'une clé sachant le cryptogramme qui lui est associé connu. En d'autres termes, quelle information donne la connaissance du message chiffré pour découvrir la clé secrète utilisée ? La transposition mathématique de cette notion est donnée par la distance d'unicité U définie comme le nombre minimal de symboles chiffrés nécessaires tel que, connaissant U symboles l'incertitude sur la clé soit nulle. Shannon a montré que U est inversement proportionnelle à la redondance R de la source exprimée en bits par symbole :

$$U = \frac{H(K)}{R} \tag{1}$$

où le coefficient de proportionnalité $H(K)$ est l'entropie de la clé.
Lorsque la redondance de la source diminue, il est clair que la distance d'unicité U augmente et par conséquence le nombre de symboles nécessaires à la connaissance sans ambiguïté de la clé K.

La transposition de ce résultat à notre contexte n'est pas immédiate, car le codeur utilisé pour supprimer la redondance est un codeur avec pertes. Néanmoins, on peut admettre que la perte d'information induite par le codage ne peut qu'augmenter la distance d'unicité. La formule (1) proposée par Shannon fournit donc une borne inférieure de U.

4.4 Algèbre des codes IFS et cryptanalyse différentielle

L'algèbre des codes IFS est très complexe. Ce point a d'ailleurs constitué le principal obstacle au développement de codeur IFS requérant une structure algébrique facilitant la mise au point d'algorithmes rapides. Les lois élémentaires de l'algèbre telles que l'addition, la soustraction, et la multiplication de deux codes ne sont en effet pas définies. L'absence de structure algébrique simple, découle directement du processus itératif de décodage qui crée des termes quadratiques à la première itération puis cubiques et ainsi de suite. Ceci constitue une contremesure à la mise en place de cryptanalyse différentielle. En quelques mots, la cryptanalyse différentielle consiste à tenter de casser un algorithme de sécurité en étudiant les changements opérés sur le cryptogramme lors d'un changement du texte clair. Dans notre contexte, il s'agit d'étudier les variations de l'image cryptée en fonction du changement de l'image originale. On distingue les attaques à texte clair connu et les attaques à texte clair choisi. Dans le premier cas, on dispose de couples d'images (image originale, image cryptée) mais on ne peut pas influer sur le choix de ces couples contrairement au second cas où des sélections judicieuses peuvent être opérés.

4.5 Structure parallèle et sécurité

Une condition nécessaire pour qu'un algorithme de sécurité soit sûr est qu'il puisse difficilement conduire à la résolution d'un problème de structure parallèle. Dans notre cas, ce type de résolution pourrait consister en une reconstruction locale de l'image.

Pour obtenir une qualité acceptable de l'image, on peut considérer qu'il est nécessaire d'effectuer au moins quatre itérations. Il est intéressant de souligner que lors d'une itération du processus, chaque bloc cible dépend de 4 autres blocs cibles, si l'on considère qu'un bloc source contient 4 blocs cibles (sous-échantillonnage par 2). Pour N itérations un raisonnement par récurrence conduit à la relation suivante :

$$D \approx \gamma^N$$

avec γ : facteur de sous-échantillonnage (généralement $\gamma = 2 \times 2$),
et D : nombre de blocs sources nécessaires à la reconstruction d'un bloc cible.
On en déduit qu'il faut estimer 4^N paramètres s_k pour reconstruire un bloc de l'image correctement. C'est une fonction exponentielle par rapport au nombre d'itérations.

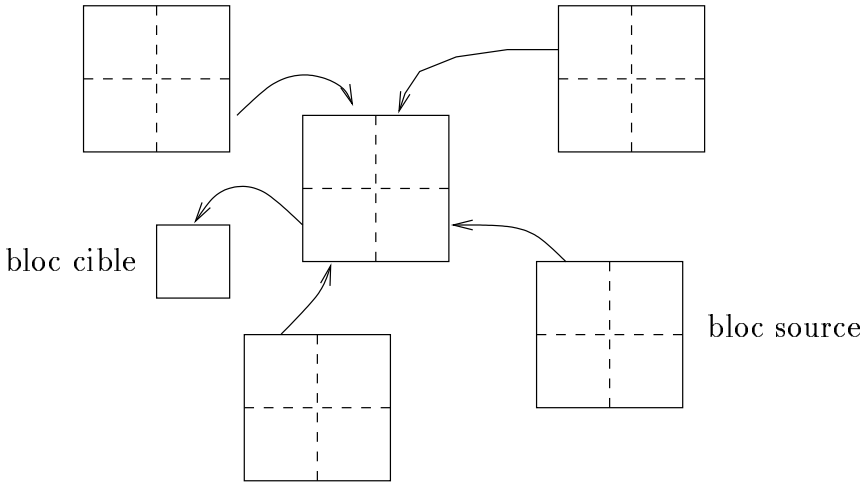


FIG. 8 – *Dépendance entre les blocs cibles et les blocs sources*

5 Vers la constitution d'une clé secrète à longueur variable : structure en treillis

A ce stade, les bits à masquer des paramètres s_k constituent un nombre de bits à gérer beaucoup trop important pour former directement une clé secrète. Il faut donc procéder à une réorganisation de ces bits permettant d'en extraire un nombre réduit constitutif d'une clé, les autres restant dans le flux de données sous une forme masquée. Il est souhaitable que la réorganisation proposée concilie les exigences de sécurité et de choix d'une longueur de clé flexible. Dans la plupart des algorithmes à clé secrète, le générateur de clé constitue un élément fondamental du système. Le soin apporté à sa conception est crucial dans la mesure où une défaillance de celui-ci peut entraîner une inefficacité de la protection sur l'ensemble des images traitées avec cet algorithme. Les clés sont généralement obtenues par des générateurs de séquences pseudo-aléatoires. Il s'agit d'algorithmes déterministes complexes [83] dont les propriétés statistiques sont proches de celles associées à une répartition uniforme. Il en résulte qu'il est difficile de prédire le prochain événement, c'est-à-dire la nouvelle clé générée par l'algorithme. Dans notre schéma de CA, nous proposons de tirer parti des opérations effectuées lors du calcul du code fractal de l'image pour constituer la clé.

5.1 Génération de la clé secrète

Décrivons l'algorithme envisagé à l'aide de la figure 9. Cet algorithme dispose en entrée de l'ensemble des facteurs d'échelle de niveaux de gris s_k issus du calcul du code IFS de l'image. On considère alors pour chaque facteur s_k les n bits devant être masqués, ils sont notés $s_k|_{n\ bits}$; n étant fixé comme indiqué au paragraphe 4 suivant le niveau d'accès souhaité. On combine deux à deux les entités $s_k|_{n\ bits}$ via une opération logique «ou exclusif» notée $\oplus$. Pour chaque combinaison, la seule connaissance du résultat de l'opération $\oplus$ ne permet pas de déduire les valeurs initiales des deux paramètres $s_k|_{n\ bits}$.

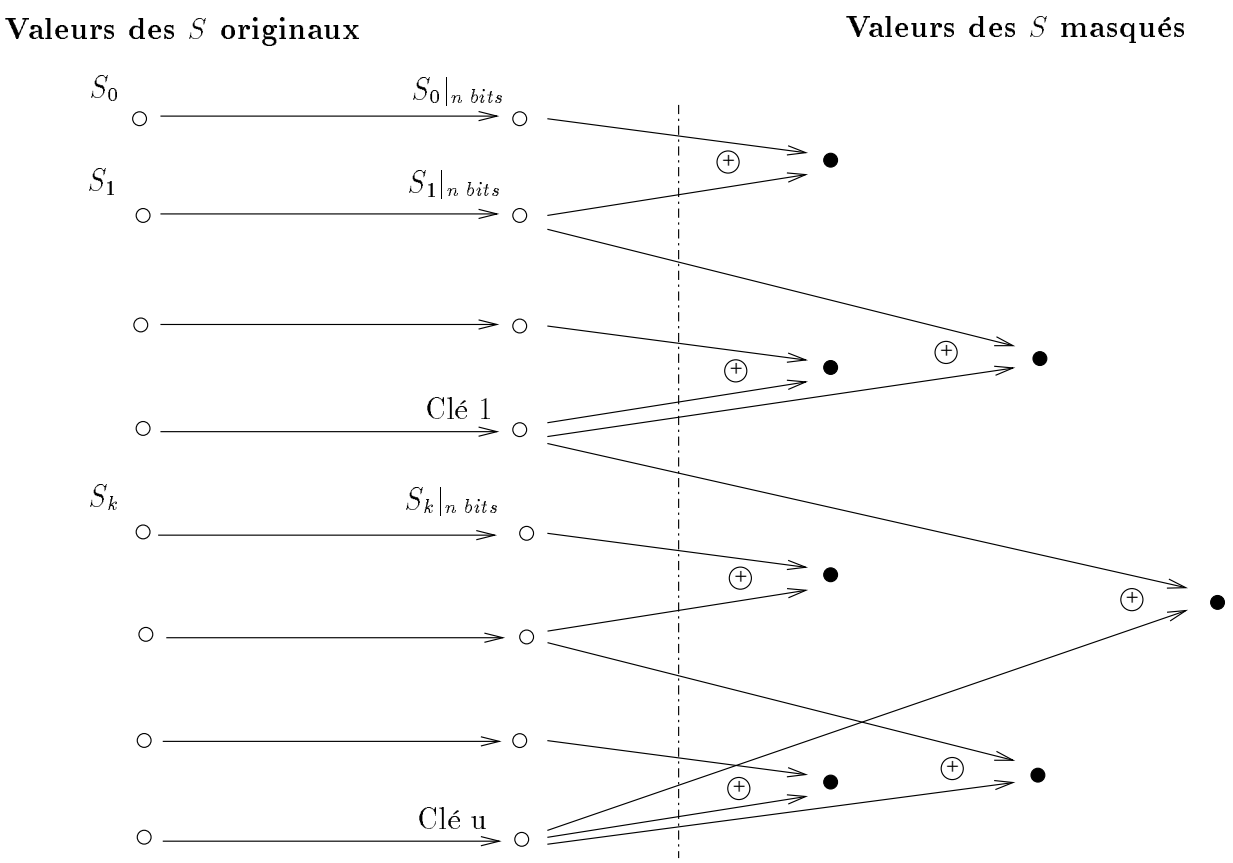


FIG. 9 – *Treillis et génération de clés*

Par contre, connaissant l'un des deux paramètres, on peut facilement retrouver le second en réalisant à nouveau une opération $\oplus$ entre le paramètre $s_k|_{n\ bits}$ connu et le résultat du cryptage, l'opérateur $\oplus$ est en effet son propre inverse. A ce stade, on a réduit donc de moitié le volume d'information secrète nécessaire à déverrouiller le système de CA, puisque la clé secrète est constituée par la concaténation d'un paramètre $s_k|_{n\ bits}$ sur deux. A partir de cette structure élémentaire, nous proposons de construire un treillis (fig. 9) permettant à chaque nouveau niveau de diviser par deux la longueur de la clé.

5.2 Discussion sur le processus de génération de clé

Le système de génération de clé proposé bénéficie des opérations réalisées lors du codage de source. En effet, la compression par IFS conduit à une distribution uniforme des paramètres s_k. En d'autres termes, du point de vue de la sécurité, chacune des clés de l'espace a la même probabilité d'être sélectionnée, ce qui rend difficile une attaque statistique directement basée sur la probabilité d'apparition des clés. L'élimination de la redondance des données compressées engendre également une indépendance des différents bits des paramètres s_k. Autrement dit, la connaissance des n-1 premiers bits d'un s_k ne donne aucune indication pour calculer le n$^{\text{e}}$ bit. Le processus déterministe générant la clé

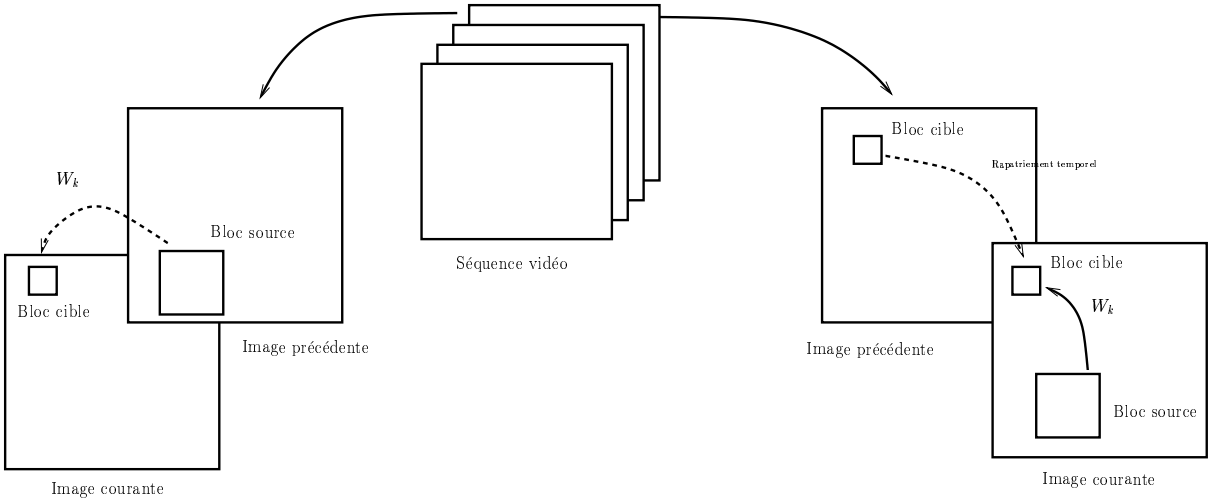


FIG. 10 – *Codage fractal vidéo : approche 2D plus prédiction*

est paramétré par l'image originale qui n'est bien entendu plus accessible après cryptage. Ce dernier point permet d'assurer que le déchiffrement d'une image n'entraîne pas une invalidation totale de l'algorithme. En effet, les autres images sont encore protégées puisque le germe de la clé est différent.

6 Les extensions possibles à la vidéo et à la sécurisation partielle d'une image

6.1 Extension vidéo du codage fractal : approche 3-D

Les extensions vidéo se sont orientées dans deux directions [20, 31] :

- l'une est basée sur le codage fractal de certaines trames plus une prédiction et une compensation de mouvements des trames manquantes (fig. 10).
- l'autre considère des cubes comme primitives de base en remplacement des blocs (fig. 11).

Nous nous intéresserons exclusivement à l'approche 3-D qui présente l'avantage de conserver l'essentiel des propriétés établies pour le codage fractal des images fixes.

6.2 Cryptage localisé (en vue de garantir l'anonymat par exemple)

Pour certaines applications, il peut être intéressant de restreindre le cryptage localement dans le but par exemple de protéger exclusivement les régions d'intérêt, ou bien afin d'assurer l'anonymat d'une personne. Nous avons étudié les possibilités de notre algorithme dans un tel contexte. Les simulations réalisées dans le cadre d'un stage à Eurecom [61, 22] ont également permis d'aborder concrètement les problèmes du codage

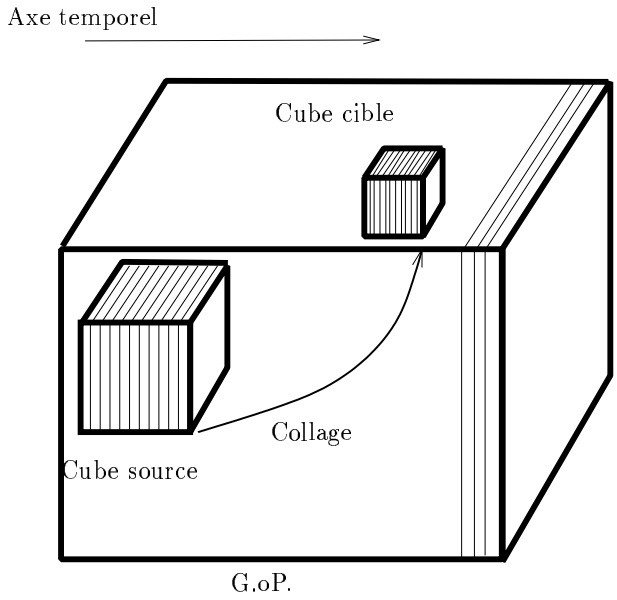


FIG. 11 – *Codage fractal vidéo : approche 3D*

fractal de la vidéo. Nous donnons à titre d'illustration quelques images extraites de la séquence Salesman dans lesquelles on a pratiqué un cryptage du visage (fig. 12). Plus d'informations sont disponibles dans le rapport de stage [61].

7 Applications

7.1 Serveur d'images web sécurisé

L'application envisagée, illustrée par la figure 13 confirme tout l'intérêt que peuvent présenter des approches conjointes (codage de source / contrôle d'accès) dans le contexte d'applications sur Internet. Considérons le serveur d'une agence de photos, il pourrait mettre à disposition de la communauté Internet l'ensemble des images de sa base de données. Ces images seraient accessibles à un utilisateur lambda dans un mode dégradé, afin de servir par exemple de vitrine commerciale ou de pré-sélection. Un client intéressé par l'acquisition d'un niveau de qualité supérieure enverrait une requête au serveur qui après une procédure d'identification lui communiquerait la clé associée au niveau de décodage demandé. Un tel système ne nécessite pas le transport de nouvelles données (exception faite de la clé) lors de la demande d'une image à une qualité supérieure. Notons que le décryptage des images est réalisé chez le client. Le système de contrôle d'accès proposé résout donc simultanément le problème de l'acheminement sécurisé des images chez le client. La seule connaisance des données transitant sur le réseau permet uniquement d'obtenir les images en prévisualisation, c'est-à-dire au niveau de qualité le plus faible. Comme l'indique la figure 13, le système proposé est compatible avec une architecture de distribution des données ayant recours à des serveurs de caches. En effet, les images sont transmises au serveur de cache sous une forme cryptée. Dans ces conditions, la présence

FIG. 12 – *Contrôle d'accès localisé pour garantir l'anonymat*

des images sur le serveur de cache qui par définition est largement accessible à différents utilisateurs, ne constitue pas un problème pour la sécurité du système.

7.2 Services Multimédia par satellite

Les nouveaux sites Internet ont de plus en plus recours à des données volumineuses telles des images ou des séquences vidéo pour rendre les sites plus attractifs. Cette évolution a entraîné des modifications du trafic. Des études montrent une très forte dissymétrie dans les volumes d'information échangées entre les clients et les prestataires (fournisseurs de services évolués). Les requêtes des clients pour télécharger une image ou une vidéo constituent un volume d'information très inférieur au téléchargement lui-même. Le réseau Internet actuel est inadapté à supporter ce type de trafic. Les communications par satellite malgré leur coût élevé peuvent constituer une alternative à cette surcharge du réseau. La société Eutelsat [33] commercialise par exemple un système dans lequel, les masses de données importantes présentes sur de gros serveurs Web sont transmises par des liaisons satellites haut débit pouvant aller jusqu'à 40 Mbps alors que les requêtes des clients sont véhiculées par le réseau terrestre classique.

Le déploiement d'une telle solution n'est pas sans poser de nouveaux problèmes. Il devient par exemple très facile d'écouter un tel réseau. Notre algorithme de CA trouve sa place dans ce contexte où il s'agit simultanément de compresser de larges volumes d'information multimédia (image ou vidéo) et d'assurer un cryptage adapté de ces données avec éventuellement plusieurs niveaux de services en termes de qualité d'image.

La distribution des clés nécessaires à l'obtention des différents niveaux de décryptage peut s'effectuer via un réseau annexe à faible débit, par exemple le réseau terrestre.

Notons que dans notre schéma, l'ensemble des utilisateurs peut disposer d'une même implémentation (logicielle ou matérielle) du décodeur quel que soit leur niveau d'accès. Seule la clé confectionnée à partir des paramètres s_k différencie le type d'utilisateur.

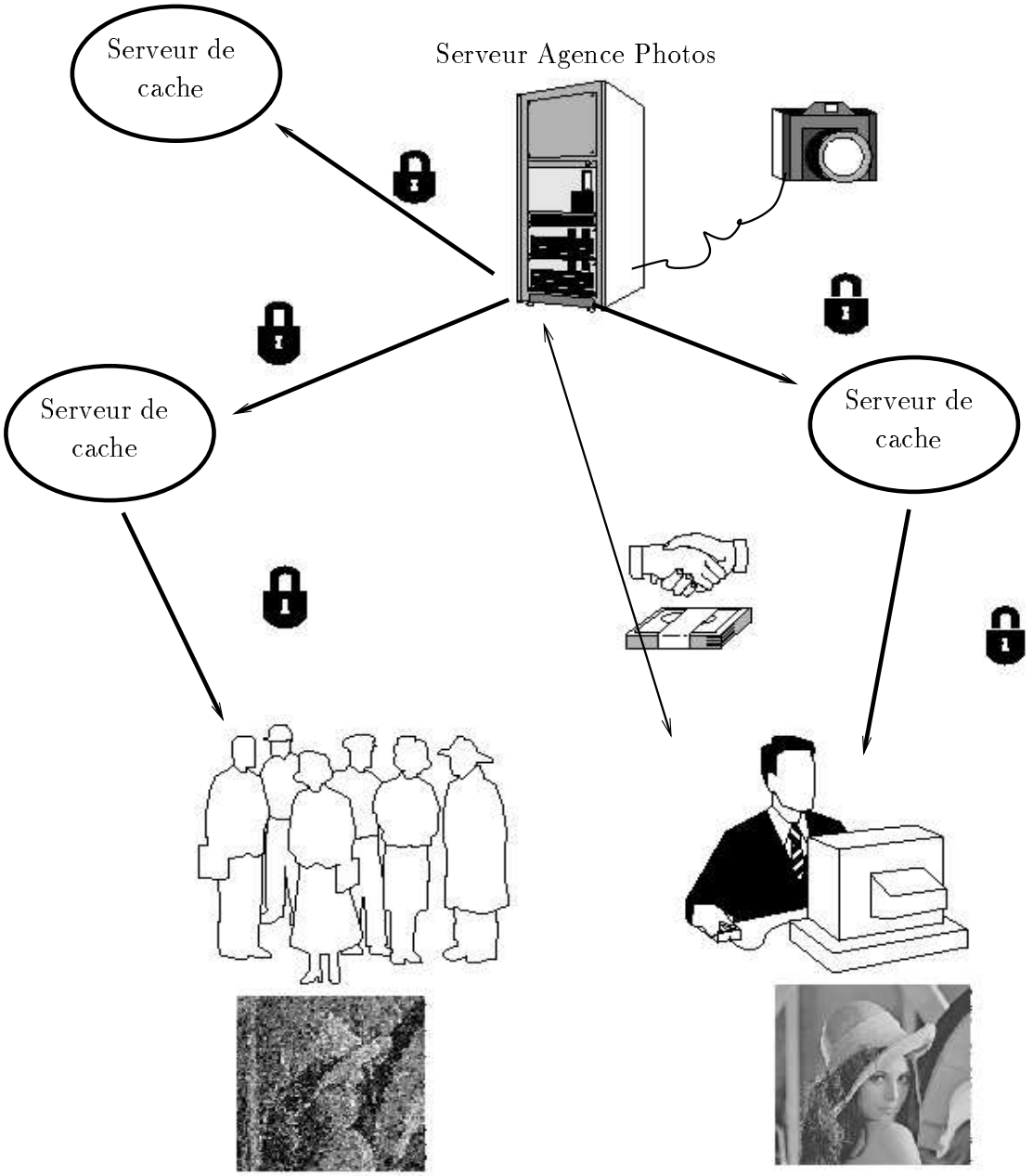


FIG. 13 – *Serveur d'images multi-access*

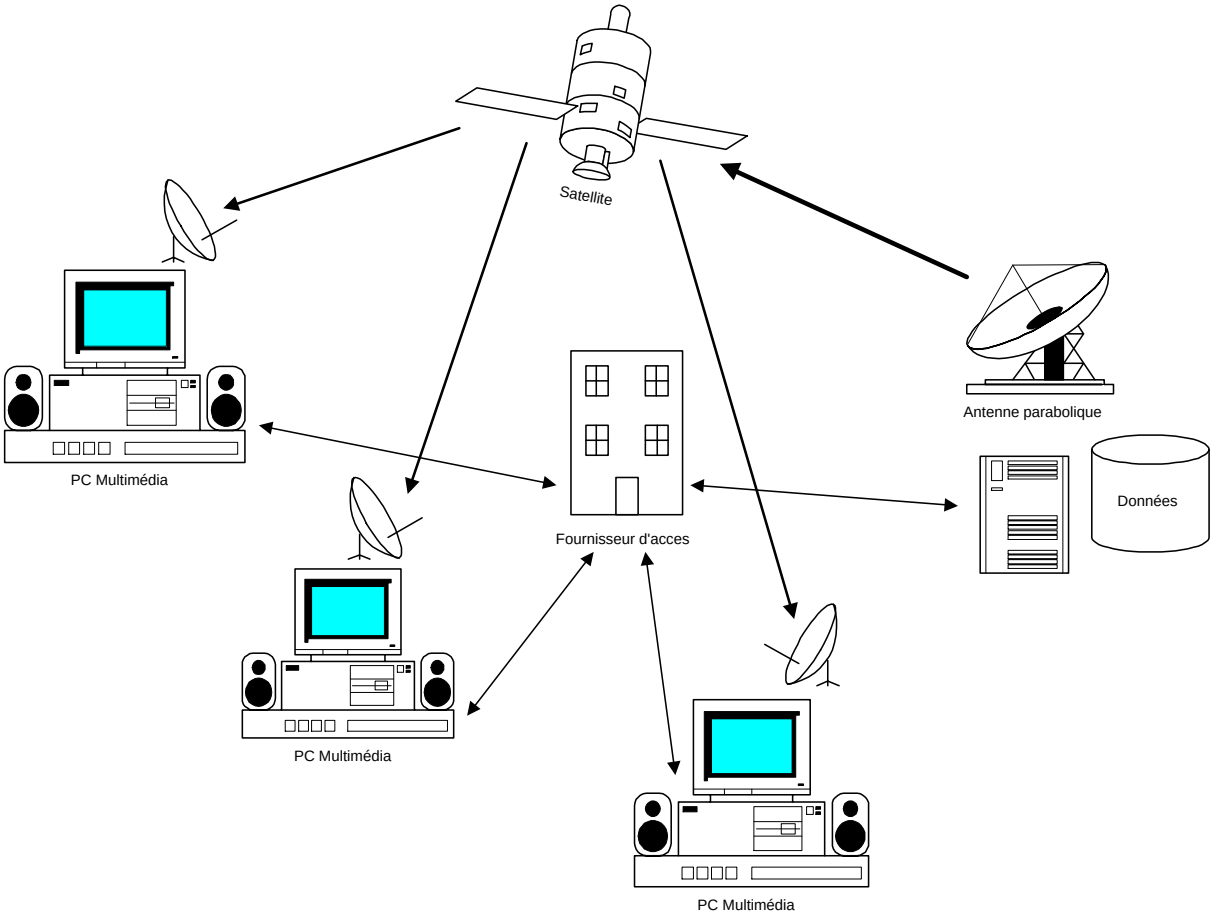


FIG. 14 – *Diffusion satellitaire de services Multimédia*

8 Conclusion

Dans ce chapitre nous avons proposé une approche conjointe (source-cryptographique) afin d'assurer simultanément la compression des images et leur accès contrôlé allouant différents niveaux de qualité. Grâce à l'introduction d'un codage de source simultanément au contrôle d'accès, la stratégie de cryptage tient compte du caractère spécifique des données traitées (les images), et notamment de la très forte redondance et corrélation locales. Notre méthode autorise l'utilisation d'un récepteur unique quel que soit le niveau de service désiré, ceci permet une grande flexibilité du contrôle d'accès qui peut par exemple être modifié et adapté d'un programme à l'autre. Nous avons montré tout l'intérêt de ce type de méthode dans le cadre de transmission sur des supports ouverts (satellite) qui impliquent très souvent un cryptage au moins partiel (pour les images).

Chapitre 2

Problématiques et modèles de tatouage d'image

Le tatouage d'image est apparu au début des années 90 dans le but de résoudre les problèmes liés à la mise en circulation d'oeuvres « copyrightées » via des médias dépourvus de mécanismes de sécurité. Cette absence totale de sécurité est d'autant plus critique que ces supports numériques offrent une très grande facilité à reproduire tout document à l'identique, ainsi qu'à le diffuser très largement au travers de nombreux formats. Les premières applications où est apparue la notion de tatouage étaient vouées à la protection des droits d'auteur, aujourd'hui, la notion de tatouage s'est élargie à d'autres problèmes présentant des spécificités différentes. Dans ce chapitre nous dressons un panorama des différentes formes de tatouage et des problématiques associées tant au niveau protocole que traitement d'image, avant d'aborder au chapitre suivant les solutions proposées dans la littérature.

1 Le tatouage d'image : quelle utilité, pour quel service ?

Le tatouage d'image que l'on peut sommairement décrire à l'aide de la figure 1 consiste à introduire (généralement sous une forme invisible) une information dans une image puis à tenter de la récupérer après que l'image ait éventuellement subi des manipulations de nature variée. Avant d'aller plus en avant dans l'étude de tels systèmes, nous nous proposons d'examiner en détails les différents contextes où le tatouage semble constituer une solution d'avenir. Notre étude est principalement dédiée à des fonctions de sécurité d'image.

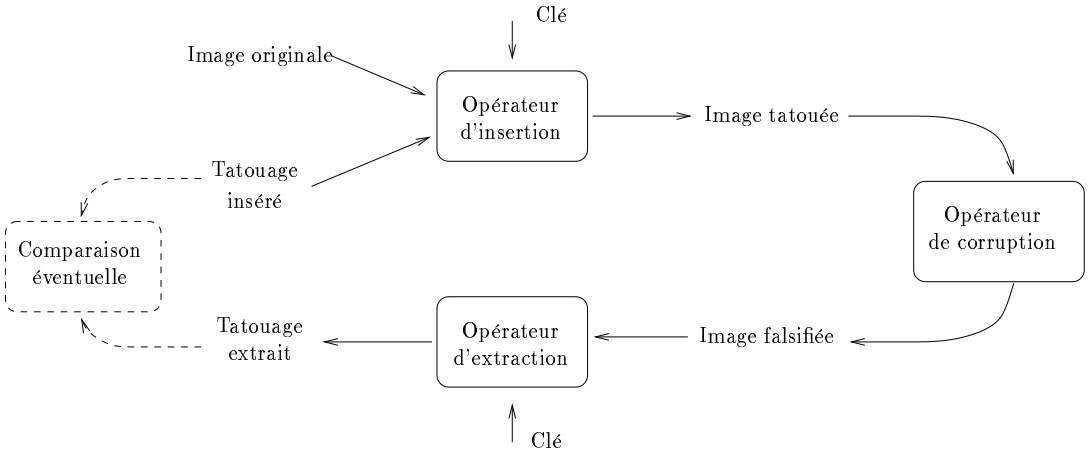


FIG. 1 – *Dispositif générique d'un système de tatouage*

1.1 Vérification de l'intégrité du contenu d'une image

La mise sous format numérique des images offre de nouvelles possibilités pour la manipulation de celles-ci. La retouche d'image qui autrefois nécessitait un matériel professionnel sophistiqué et coûteux peut maintenant être réalisée très rapidement avec un micro ordinateur personnel et un logiciel adapté. Assurer l'intégrité des images devient dans ces conditions un enjeu majeur.

D'une manière générale, en sécurité, il existe deux stratégies pour garantir l'intégrité de données[1], chacune opère à un niveau différent :

Sécurisation au niveau du canal : Cette première stratégie (fig. 2.a) consiste à sécuriser en écriture l'ensemble du canal de transmission par lequel vont transiter les données, de telle sorte qu'elles ne puissent pas être modifiées par une tierce personne. Cette solution, très coûteuse est rapidement inapplicable dès lors que les données circulent sur des réseaux ouverts qui par définition sont peu sûrs et difficilement contrôlables de bout en bout.

1. terme générique pouvant désigner un fichier informatique, une lettre, ou tout autre élément porteur d'information.

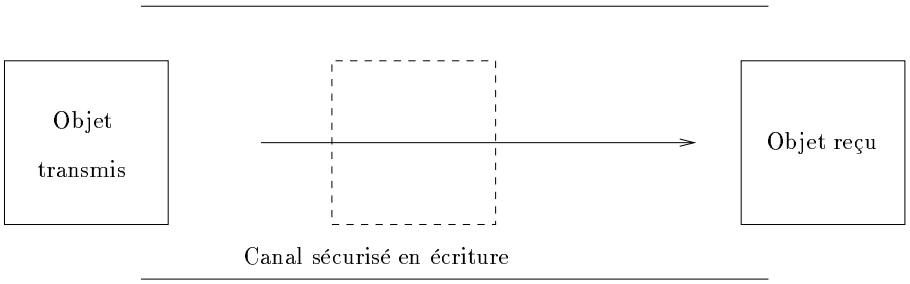
Sécurisation au niveau des données : Cette seconde approche (fig. 2.b), beaucoup plus légère, repose sur le calcul d'une signature associée aux données qui sera systématiquement jointe avec celle-ci. Cette signature est générée par une fonction de hachage permettant de garantir que la modification d'un seul bit des données originales conduirait au calcul d'une signature totalement différente. Avant d'être jointe aux données, cette signature est cryptée par une entité certificatrice (qui peut être le propriétaire des données lui-même). On utilise généralement un algorithme à clé publique tel que RSA pour cette opération. L'entité certificatrice réalise un chiffrement de la signature en utilisant sa clé secrète. Le client souhaitant vérifier l'intégrité des données, commence par déchiffrer la signature au moyen de la clé publique. Cette dernière opération permet d'authentifier la signature et garantit qu'une personne malveillante n'a aucun intérêt à substituer une signature falsifiée à la signature originale, puisqu'elle est dans l'incapacité de fabriquer une signature valide ne possèdant pas la clé secrète. Finalement, le contrôle de l'intégrité des données, réalisé au niveau du terminal de réception, s'effectue en comparant la signature calculée à partir des données reçues avec celle (déchiffrée) jointe aux données. Si celles-ci diffèrent, les données sont détectées comme non intègres et il est demandé de réacheminer les données originales.

Dans le contexte des images, les techniques de tatouage trouvent bien entendu leur place dans la deuxième stratégie, elles peuvent prendre part à la constitution d'un processus « ad hoc » permettant de dissimuler une signature dans l'image afin de jouer le rôle de référence. Précisons à présent la notion d'intégrité pour des images. Dans la communauté sécurité, ce service se définit sans ambiguïté comme celui garantissant que les données reçues sont rigoureusement identiques à celles émises. Cette définition est bien entendu applicable aux images cependant elle présente un intérêt limité. En effet, une image est amenée à subir des transformations telle qu'une compression par exemple sans pour autant que son contenu soit modifié de manière significative. Dans le but d'assurer un service d'intégrité des images, il est primordial de distinguer :

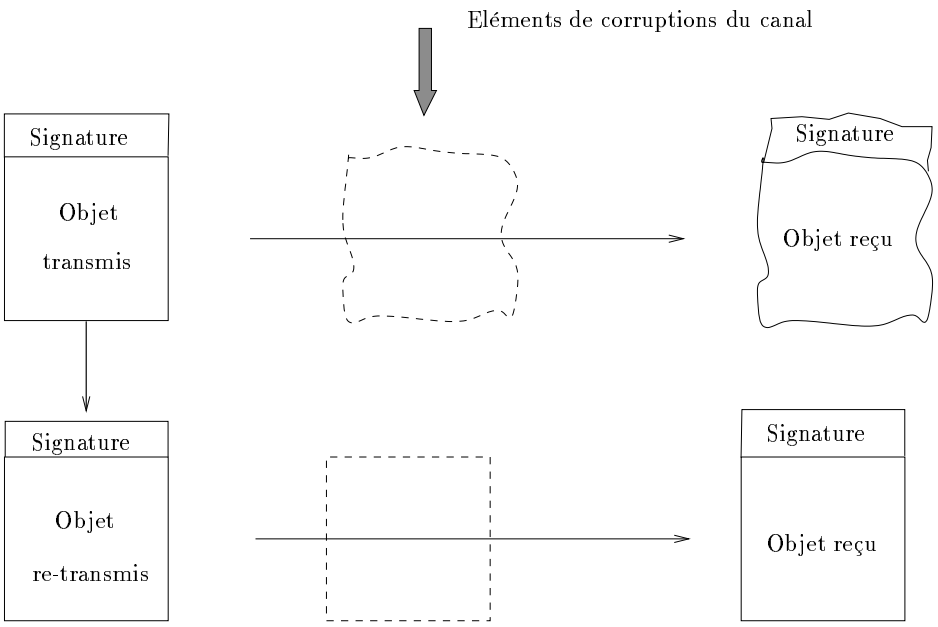
- les manipulations malveillantes consistant à détourner le contenu initial de l'image en supprimant ou en modifiant certaines régions par exemple.

- des manipulations liées à l'utilisation d'une image sous une forme numérique, les changements de formats, le ré-échantillonnage, une translation de l'image de quelques pixels font par exemple partie de cette seconde classe.

Cette distinction n'est malheureusement pas toujours très nette, elle dépend par exemple du type d'image considéré, et surtout de son utilisation. Dans le domaine de l'imagerie satellitaire militaire, chaque détail peut avoir son importance, une compression avec pertes ou un léger sous-échantillonnage de l'image peuvent révéler une intention délibérée de dissimuler une information stratégique telle qu'une route d'accès à un bâtiment par exemple. La définition stricte de l'intégrité reste alors la plus adaptée.

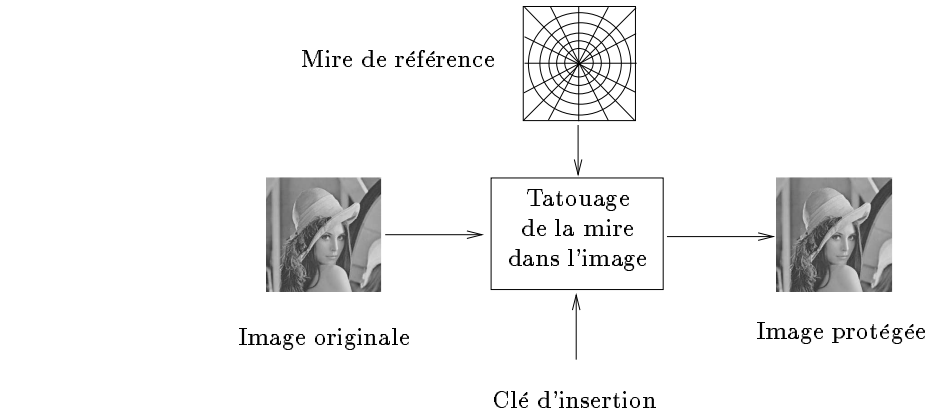


(a)

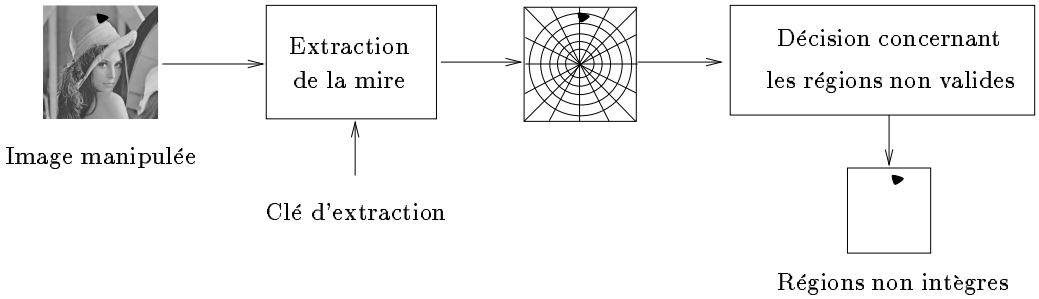


(b)

FIG. 2 – *Deux philosophies pour assurer le service d'intégrité.*
a). sécurisation du média (canal).
b). sécurisation de l'objet



(a)



(b)

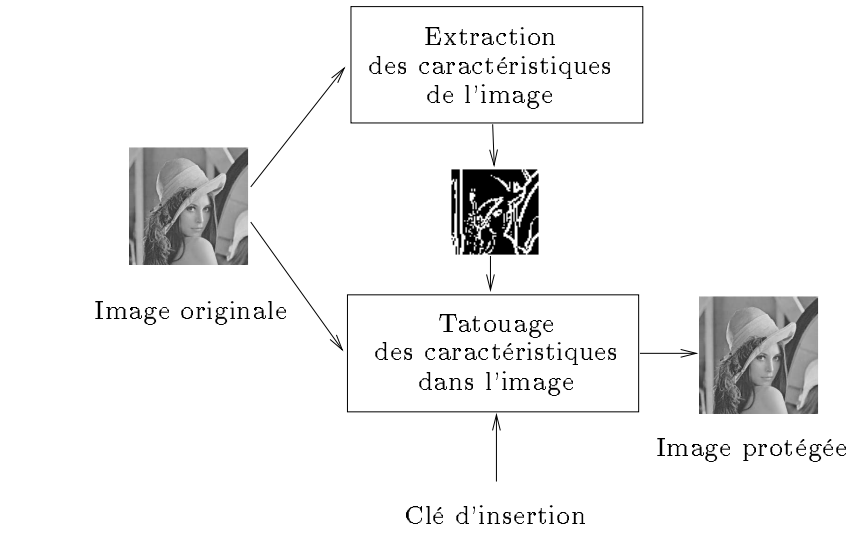
FIG. 3 – *Garantir l'intégrité d'une image par tatouage d'une mire de référence.*
a). protection de l'image.
b). vérification

Les tatouages pouvant assurer l'intégrité d'une image

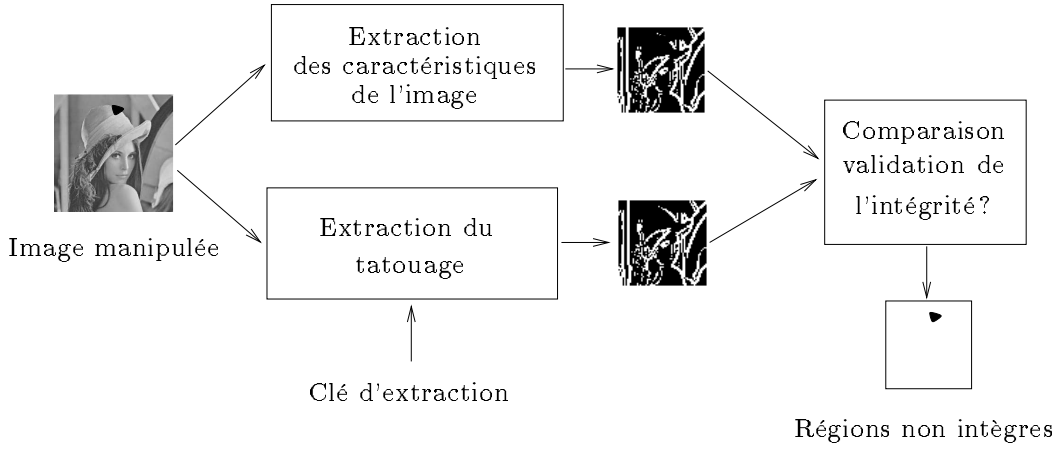
Comme l'indique les figures 3 et 4 nous distinguons deux approches pour assurer l'intégrité d'une image.

- La première a recours à la dissimulation systématique dans l'image d'une mire de référence. Une malversation de l'image est alors détectée par une perte ou déformation partielle de cette mire ;

- la seconde consiste à extraire des caractéristiques de l'image, par exemple les contours puis à les dissimuler dans l'image sous la forme d'un tatouage, constituant ainsi une référence de l'image originale. La procédure de vérification compare les caractéristiques de l'image à tester avec celles de référence contenues dans le tatouage.



(a)



(b)

FIG. 4 – *Garantir l'intégrité d'une image par tatouage de caractéristiques de l'image.*
a). protection de l'image.
b). vérification

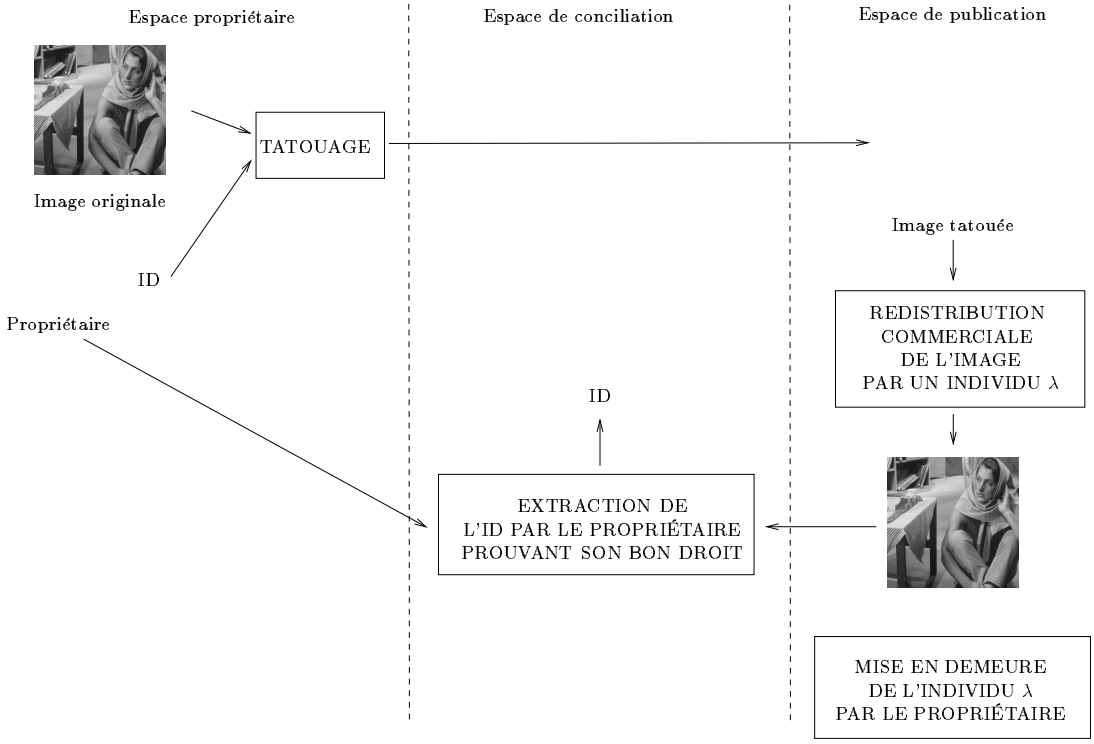


FIG. 5 – *Service de protection de la propriété intellectuelle par tatouage d'image*

1.2 Protection des droits d'auteur

Remplir ce service fut un des premiers thèmes d'étude du tatouage d'image, il est cependant toujours d'actualité et concerne encore la majorité des publications. L'objectif est d'offrir la possibilité à l'auteur ou au propriétaire d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi quelques modifications par rapport à l'originale (fig. 5). Ce problème s'érige autour des trois contraintes ci-après :

- préserver la qualité originale de l'image ;
- garantir la non-ambiguïté de la preuve ;
- assurer la robustesse des éléments de preuve (tatouage).

Détaillons à présent ces trois points fondamentaux.

Qualité de l'image

Le tatouage d'image n'échappe pas aux grands principes généraux de sécurité. Un de ces principes stipule que les services de sécurité doivent être assurés avec un impact minimum sur le service original (non sécurisé). Dans le cas présent, la qualité visuelle de l'image tatouée par rapport à l'image d'origine est un élément prépondérant. Beaucoup d'auteurs sont en effet très réticents à l'idée de détériorer leur oeuvre même afin de protéger

leurs droits d'auteur. La notion d'invisibilité du tatouage et donc de qualité de l'image signée est malheureusement très délicate à évaluer et encore plus délicate à modéliser. En effet, une évaluation « rigoureuse » de la qualité d'une image nécessite la mise en place de tests psychovisuels. Ces tests sont très lourds à mettre en oeuvre, de plus, ils ne peuvent rendre compte de la diversité des conditions dans lesquelles l'image va être observée. Un autre point délicat est de déterminer un critère psychovisuel qui englobe la diversité des types d'images. En effet les critères de qualité rattachés à l'observation d'une image médicale de type échographie ou à une photo de paysage sont bien entendu totalement différents. Pour un même type d'image, la notion d'invisibilité du tatouage est intimement liée à la qualité de l'image originale (cf. § 4.1). Meilleure est la qualité de l'image, plus grande est la difficulté de dissimuler une information supplémentaire de telle sorte que celle-ci soit imperceptible.

Non-ambiguïté de la preuve

L'extraction du tatouage devant constituer une preuve irréfutable de la propriété de l'image, la conception du tatouage et des protocoles rattachés doit exclure l'apparition de toute ambiguïté. Des contestations sont susceptibles de surgir à deux niveaux :

Date de dépôt : la personne malintentionnée ne nie pas le fait que l'image a été effectivement tatouée, cependant elle met en cause la date de dépôt qui est un élément essentiel pour la constitution de la preuve de propriété. Nous aurons une discussion plus approfondie de ce type de conflit au paragraphe 8.3 du chapitre 3 en abordant le problème dit du « dead lock ».

Création d'ID similaires : il convient notamment de s'assurer qu'il n'est pas possible ou tout au moins très difficile de créer un tatouage identique à partir d'une clé d'insertion de tatouage différente.

Robustesse du tatouage

La robustesse du tatouage fait référence à la capacité de la méthode d'extraction de récupérer le tatouage y compris après que l'image aura subi des perturbations. Il convient de distinguer deux familles d'attaques et par conséquence deux types de robustesse :

la robustesse face à des attaques passives : Des modifications de l'image du type conversion de format d'image peuvent éventuellement entraîner la perte du tatouage sans qu'il y ait pour autant une intention délibérée de retirer le tatouage. Dans ce contexte, on parlera d'attaque passive.

la robustesse face à des attaques actives : Ici, le but ultime pour le corrupteur est de rendre le tatouage inopérant. Les manipulations de l'image sont ciblées sur cet objectif, et cherchent à tirer parti au maximum des connaissances a priori sur l'algorithme de tatouage. C'est pourquoi, la plupart des algorithmes prétendus robustes à ce type d'attaques basent leur sécurité sur une information secrète de type clé et font l'hypothèse que seul l'algorithme est connu.

Il est à noter que la frontière entre ces deux types de robustesse est parfois ténue bien qu'il soit potentiellement plus difficile de résister à des attaques malintentionnées. Un simple décalage horizontal de quelques pixels intervient dans de nombreuses chaînes de traitement, cette opération prend en défaut de nombreux algorithmes requérant un positionnement spatial parfait. Cette faiblesse connue, une telle manipulation peut être effectuée dans le seul but de neutraliser l'algorithme de tatouage.

Nous verrons plus en avant dans cette thèse que ces trois points sont indissociables et qu'ils sont à la base de compromis qu'il convient d'arbitrer en fonction des exigences de l'application.

1.3 Non répudiation de l'accès à une image, traçage de copies illicites

Ce service est une bonne illustration de la complémentarité existant entre les méthodes de cryptage et les méthodes de tatouage (fig. 6). Soit l'acheminement d'une image réalisée sous une forme chiffrée, interdisant qu'une personne puisse avoir accès au contenu de l'image lors du transport de celle-ci. Au niveau du destinataire de l'image, il est procédé simultanément au déchiffrage et au tatouage de l'image de telle sorte que si l'utilisateur remet illégalement en circulation l'image, il est possible de tracer la provenance de l'acte délictueux. Notons que contrairement au problème précédent (cf. § 1.2) dans lequel on associe un unique tatouage (identifiant le propriétaire) à une image donnée, il existe ici plusieurs tatouages différents pour une même image originale. En effet, chaque client est bien entendu identifié par un tatouage personnel. Ceci n'est pas sans poser d'importants problèmes de sécurité en cas de collusion entre plusieurs clients malhonnêtes. Si chacun d'eux possède une image tatouée différente I_{T_n}, sous l'hypothèse que l'ensemble des contributions des tatouages soit à moyenne nulle, ils peuvent par exemple tenter de reconstruire l'image originale en calculant l'image moyenne :

$$I_{\text{orig}} = \lim_{n \to \infty} \frac{1}{n} \sum n I_{T_n}$$

1.4 Gestion du nombre de copies d'une image

Contrairement aux données de type analogique pour lesquelles une succession de reproductions entraîne rapidement une perte de qualité, les données numériques peuvent être dupliquées pratiquement sans limite. En effet, dès lors qu'une personne a accès aux données, elle est potentiellement capable de les reproduire bit à bit en préservant ainsi intégralement la qualité originale. Néanmoins, dans des systèmes fermés ou propriétaires destinés au grand public, bien que cette reproduction reste toujours possible, il est envisageable d'en freiner l'ampleur. Un exemple est constitué par les systèmes DVD (Digital Versatile Disk) [11, 64] pour lesquels on se propose d'introduire un tatouage spécifiant si la vidéo a le droit d'être lue et éventuellement recopiée. Les systèmes de lecture examinent l'indicateur de copie avant de procéder à une lecture ou une reproduction de la vidéo. Ce système n'est bien entendu pas totalement sûr dans la mesure où il est toujours possible

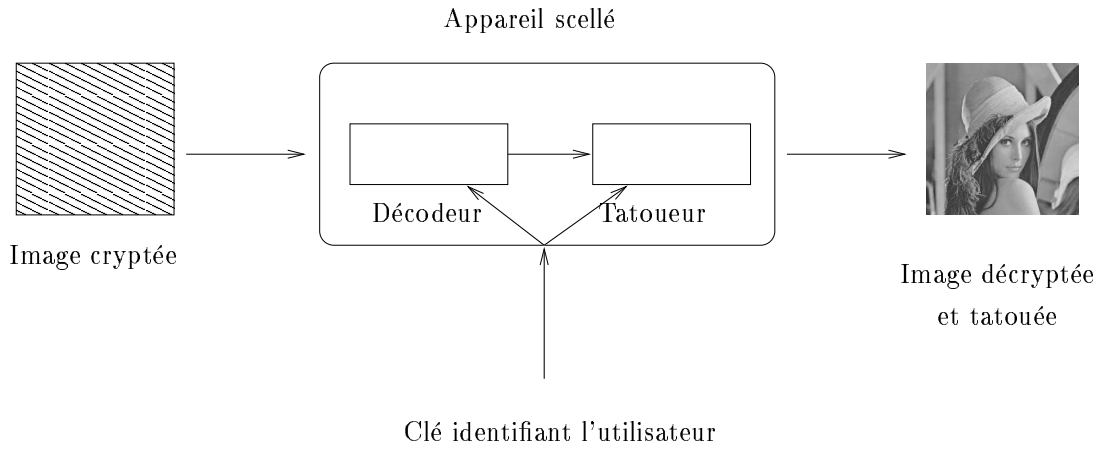


FIG. 6 – *Couplage d'un système de tatouage et de confidentialité en vue d'assurer un service de non répudiation de l'accès à une image*

de concevoir son propre lecteur qui ne tiendra pas compte de l'indicateur de copie. On visera donc ici une protection grand public, il est donc inutile d'exiger une robustesse du tatouage face à des attaques malintentionnées.

1.5 Masquage partiel d'une image en vue d'en limiter et contrôler l'accès

Nous nous plaçons ici dans un contexte proche de celui du chapitre 1. L'objectif est d'ôter tout intérêt à l'image en superposant un tatouage. Seules les personnes à qui l'on désire accorder l'accès sont capables d'inverser le processus afin de reconstituer l'image originale. Contrairement à un cryptage plus classique où l'image est totalement inintéligible, l'intérêt du tatouage réside dans le fait qu'il peut être lui même le support d'une information relative à l'image. Par exemple, on peut faire figurer l'addresse où commander l'image en clair, le nom de la société etc. (fig. 7).

1.6 Notariat électronique

Il s'agit, dans le cadre d'une procédure de commerce électronique d'images via Internet par exemple de permettre à deux entités, un vendeur et un acheteur de créer une preuve réciproque de leur implication dans la transaction d'une image donnée. L'intérêt du tatouage d'image réside dans le rattachemment direct de la preuve à l'objet de la vente (l'image). On peut faire une analogie de ce service avec le rôle du notaire qui est le garant d'une transaction entre individus.

1.7 Autres services

La liste précédente n'est pas exhaustive, de plus, elle se restreint exclusivement aux services de sécurité bien que le tatouage d'image puisse présenter un grand intérêt pour

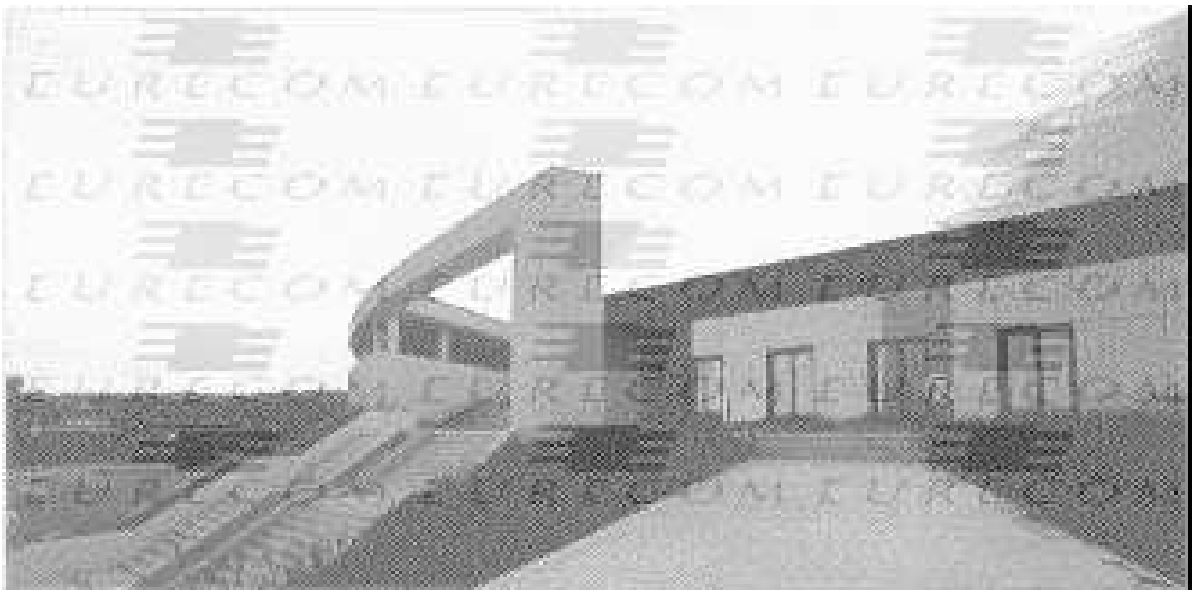


FIG. 7 – *Masquage partiel d'une image par tatouage*

d'autres types de services. On peut par exemple entrevoir des applications dans la gestion des bases de données multimédia. Les problèmes de recherche par le contenu dans de telles bases sont fort complexes ; les moteurs de recherche existant présentent des lacunes qui pourraient être atténuées par l'ajout d'un tatouage spécifiant par exemple quelques mots clés constituant ainsi une aide pour d'éventuelles recherches. Le grand avantage du tatouage d'image par rapport à d'autres formes de marquage, par le biais de fichiers d'en-tête par exemple, réside dans son indépendance vis-à-vis du support et d'éventuelles manipulations.

1.8 Récapitualtif des différentes formes de tatouage et de leurs propriétés

Dans la littérature, plusieurs types de tatouage dont le potentiel applicatif diffère sont référencés [65]. Dans ce paragraphe, nous en faisons un rapide tour d'horizon avant de nous focaliser principalement sur les tatouages invisibles, robustes, à la base des applications visant à protéger les droits d'auteur.

Tatouage visible, réversible Comme son nom l'indique, ce tatouage est parfaitement visible dans l'image. Il présente de plus la propriété d'être indélébile sauf pour les personnes disposant d'une clé secrète. Pour ces dernières, il est parfaitement réversible, il est alors possible de reconstruire intégralement l'image originale.

Tatouage invisible, fragile Il s'agit typiquement d'une forme de tatouage adaptée au contrôle de l'intégrité de l'image (cf. § 1.1). Lors de manipulations de l'image, le tatouage subit des transformations révélatrices de la corruption de l'image, en ce sens, il est dit fragile.

	Invisibilité	Robustesse passive	Robustesse active
Intégrité	×	×	
Protection des droits d'auteur	×	×	×
Non répudiation, traçage de copies illicites	×	×	×
Gestion du nombre de duplications	×	×	×
Contrôle d'accès		×	×
Notariat électronique	×	×	×

TAB. 1 – *Récapitulatif des différents services et des propriétés des tatouages associés*

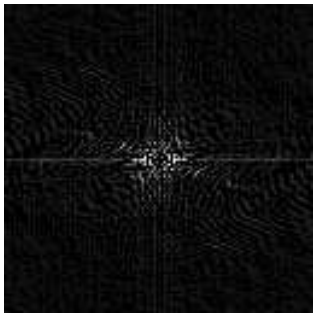
Tatouage invisible, robuste Cette appellation fait référence au tatouage le plus étudié, en particulier dans le cadre de la défense des droits d'auteur.

Nous dressons un tableau récapitulatif (tab. 1) reprenant les différents services de sécurité auxquels peut être associée la notion de tatouage d'image. Ce tableau fait également état des propriétés requises par le tatouage pour remplir ces services.

2 Tour d'horizon des manipulations des images

Dans cette section, nous ne prétendons pas faire un inventaire exhaustif des transformations pouvant être appliquées à une image. Nous nous efforcerons simplement d'attirer l'attention du lecteur sur l'étendue des manipulations intervenant dans les problèmes de tatouage d'image. Il est clair que toute notion de robustesse d'un tatouage est intimement liée à la prise en considération de l'impact des différentes manipulations de l'image. Une bonne connaissance de ces manipulations joue également un rôle majeur lors de l'évaluation de la robustesse d'un système. Les transformations envisagées ont toutes en commun de préserver de l'intérêt à l'image manipulée, nous n'avons pas pris en considération les manipulations engendrant des dégradations jugées inacceptables même si elles sont bien entendu susceptibles de conduire à la neutralisation du tatouage.

Image originale



Module du spectre de Fourier

FIG. 8 – *Répartition de l'énergie au niveau du spectre de fréquence*

2.1 Manipulations par filtrage

Filtrage passe-bas

L'analyse spectrale d'une image « naturelle » montre que la plus grande partie de l'énergie est concentrée au niveau des basses fréquences (fig. 8). L'énergie contenue dans les très hautes fréquences correspond principalement à du bruit. Cette répartition de l'énergie est particulièrement bien vérifiée pour les images de qualité médiocre. Réaliser un filtrage passe-bas de telles images peut être intéressant afin de « restaurer » ces images. De plus, si l'on se place du point de vue du tatouage d'image, le filtrage passe-bas peut également conduire à la suppression du tatouage dans la mesure où, pour des considérations psychovisuelles le tatouage est souvent associé aux hautes fréquences de l'image. Le fitrage passe-bas appartient donc bien à la classe des manipulations qui nous intéresse dans la mesure où il préserve (voire améliore parfois) la qualité de l'image tout en rendant potentiellement difficile la récupération du tatouage pour un certain nombre de méthodes. Notons également que la mise en oeuvre de ce filtrage est très facile, on peut le réaliser soit directement dans le domaine spatial de l'image en utilisant un masque de convolution soit dans le domaine fréquentiel aprés calcul de la transformée de Fourier (nous nous sommes bien évidemment placés dans le cas de filtres linéaires).

Filtrage réhaussant le contraste

Le réhaussement des contours d'une image peut facilement être obtenu suivant le schéma proposé à la figure 9. Il consiste à soustraire les composantes passe-hauts à l'image originale [56]. Une mise en oeuvre possible est obtenue par convolution puis soustraction de l'image avec le Laplacien numérique dont le masque est défini par l'équation 1.

$$D^2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix} \tag{1}$$

L'intérêt de cette technique pour tenter d'attaquer les systèmes de tatouage réside d'une part dans la perturbation des hautes fréquences où figure très souvent le tatouage ce qui peut entraîner sa perte, d'autre part dans l'augmentation de la « satisfaction visuelle »

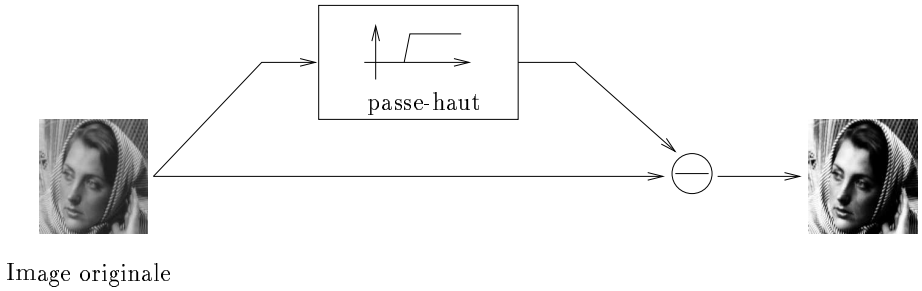


FIG. 9 – *Schéma de réhaussement du contraste par filtrage*

procurée par des contours réhaussés. On conjugue donc ainsi une suppression potentielle du tatouage avec le maintien (voire une amélioration) de la qualité subjective de l'image. Cette opération peut constituer une manipulation à part entière ou faire suite à un filtrage passe-bas dont l'objectif est de réduire préalablement le bruit présent dans les hautes fréquences des images de qualités médiocres.

2.2 Manipulations géométriques

On distingue les manipulations géométriques globales et locales dans la mesure où les techniques pour contrecarrer de telles attaques diffèrent. Dans le premier cas, on dispose d'une nombre d'échantillons élevé pour estimer la transformation, dans le second cas on doit se contenter d'un nombre réduit d'échantillons puisque l'estimation doit être réalisée localement. Nous reviendrons sur ces problèmes dans le paragraphe 7 du chapitre 4 consacré aux problèmes de resynchronisation.

Globales

Une rotation de quelques degrés est pour la plupart des images imperceptible si l'on ne dispose pas de l'image originale comme élément de comparaison. Ceci est particulièrement vrai si la rotation est suivie d'une opération de recadrage afin d'éliminer les effets de bords (triangles noirs). Parmi les transformations géométriques globales les plus courantes, il figure également les translations de quelques pixels, les changements de résolution et les opérations de recadrage. De tels décalages interviennent fréquemment au cours d'une chaîne de traitements. Nous terminons ce tour d'horizon des manipulations géométriques globales en mentionnant la symétrie axiale de l'image par rapport à son axe médian vertical (« effet miroir »). Cette dernière constitue une transformation géométrique particulièrement intéressante dans la mesure où, en l'absence de texte, l'intelligibilité de l'image est souvent intégralement préservée.

Locales

Les transformations locales appliquées peuvent dépendre soit de la position du pixel dans l'image soit d'un processus pseudo aléatoire annexe. Afin de maintenir une certaine continuité dans l'image, des interpolations de type bilinéaire par exemple sont mises en place au niveau des frontières entre les régions contiguës subissant des transformations

différentes. On trouve de telles transformations parmi la panoplie de manipulations mises en jeu par Stirmark (cf. § 2.4).

2.3 Manipulations par requantification

Jusqu'à présent, nous avons examiné les transformations par filtrage permettant d'atténuer ou de supprimer certaines composantes du signal où est disposé le tatouage et les transformations géométriques entraînant une perte d'information sur la localisation des pixels nécessaires à la reconstruction du tatouage. Nous nous proposons à présent d'aborder les manipulations basées sur une re-quantification des grandeurs décrivant l'image (par exemple les niveaux de gris). En effet, toutes les images numériques font l'objet d'une quantification de la valeur des pixels lors de leur acquisition. Il s'agit généralement d'un codage sur 256 niveaux (8 bits) pour les images dites en niveaux de gris et de 2^{24} tons pour les images couleurs.

Changement de table de couleurs, égalisation d'histogramme

En imagerie numérique, on fait largement appel à la notion de table de couleurs par exemple pour associer une couleur affichée sur un écran à des niveaux numériques. Une table de couleurs consiste à définir une correspondance entre une couleur et un ensemble de niveaux. Le format de compression avec pertes « Gif » recalcule une table de couleurs optimales permettant de passer d'un codage sur 24 bits à 8 bits pour une image couleur. Malgré une réduction d'un facteur 3 de la quantité de données on constate que la qualité de l'image est parfaitement acceptable en partie parce que l'oeil humain possède de médiocres performances en termes de résolution et de définition dans le domaine des couleurs. Les tables de couleurs intervenant dans la compression « Gif » ont été déterminées de façon empirique suivant des tests psychovisuels.
Pour les images en niveaux de gris, la manipulation d'histogramme constitue une technique adaptée pour modifier les niveaux de gris tout en préservant la qualité de l'image. Généralement on procède à une égalisation de l'histogramme pour donner un poids équivalent à tous les niveaux de gris. Cette opération a pour effet d'augmenter le contraste de l'image, ce qui est très souvent synonyme pour l'utilisateur d'un plus grand confort visuel. De plus, suite à l'égalisation, certains pixels voient leur niveau changer pour un niveau inférieur ou supérieur proche, ceci s'apparente à une requantification et est succeptible d'éliminer le tatouage.

Requantification des coefficients DCT

Une opération de requantification peut être réalisée dans le domaine spatial mais elle peut également être pratiquée dans un espace transformée. A ce titre, la norme de compression pour image fixe JPEG parvient à un facteur de compression important notamment grâce à une quantification adaptée des coefficients de la Transformée en Cosinus Discrète (DCT). La table de quantification néglige les très hautes fréquences et quantifie de plus en plus finement les moyennes et les basses fréquences. La compression JPEG se rapproche

d'ailleurs en première approximation d'un filtrage passe-bas. Sur le même principe la future norme de compression JPEG-2000 réalisera vraisemblablement une quantification adéquate dans le domaine ondelette.

Conversion Numérique/Analogique/Numérique

Pour des images fixes, ce type de conversion consiste principalement en une impression suivie d'une digitalisation à l'aide d'un scanner. Les effets sur l'image sont multiples et dépendent très largement de la qualité des appareils d'impression et de digitalisation. Néanmoins, on peut considérer que l'image subit un double ré-échantillonnage, l'imprimante introduisant généralement un sous-échantillonnage alors que le scanner pratique un sur-échantillonnage (les capteurs d'un scanner sont généralement plus performants en termes de résolution que les impressions) ; la sensibilité des capteurs introduit quant à elle un bruit de quantification.

Pour ce qui est des données vidéo, la conversion N/A/N consiste par exemple en un double transcodage de la norme MPEG-2 à la norme VHS puis à nouveau à la norme MPEG-2.

2.4 Manipulations spécifiques

Au cours de ces dernières années, faisant suite aux développements des premières méthodes de tatouage, sont apparus deux tests de robustesse : UnZign [89] et surtout Stirmark [54]. Ces outils de recherche constituent actuellement les deux tests les plus sévères. Il s'agit d'attaques mixtes, modifiant l'image tant au niveau géométrique qu'au niveau des composantes de luminance et de couleurs (fig. 10). Les évaluations menées [70] sur les logiciels de tatouage parmi lesquels on compte les logiciels commerciaux des sociétés Digimark, Blue Spike, Mediasec, ont conclu à une suppression quasi systématique du tatouage.

2.5 Mosaïque d'images

Nous terminons ce tour d'horizon des opérations de manipulations d'image par la notion de mosaïque d'images. Bien qu'il ne s'agisse pas à proprement parler d'une manipulation au sens du traitement d'image, la décomposition d'une image sous forme de mosaïque doit être prise en compte dans la mesure où elle pose de graves problèmes aux systèmes automatiques de détection de tatouage [70]. Une mosaïque est formée par un partitionnement de l'image originale en sous images (fig. 11), chaque sous image étant juxtaposée afin de reconstituer l'image d'origine. La mosaïque est réalisée de telle sorte que la taille de chacune des sous images soit insuffisante pour contenir un tatouage robuste. Prenons l'exemple d'une mosaïque de ce type réalisée dans une page « HTML », un système automatique de vérification de tatouage [9](« sipder » ou robot traqueur) doit commencer par identifier les images puis procède à la détection du tatouage. Dans ce cas, il sera très probablement dupé par la mosaïque car il sera incapable de considérer l'image dans son intégralité.

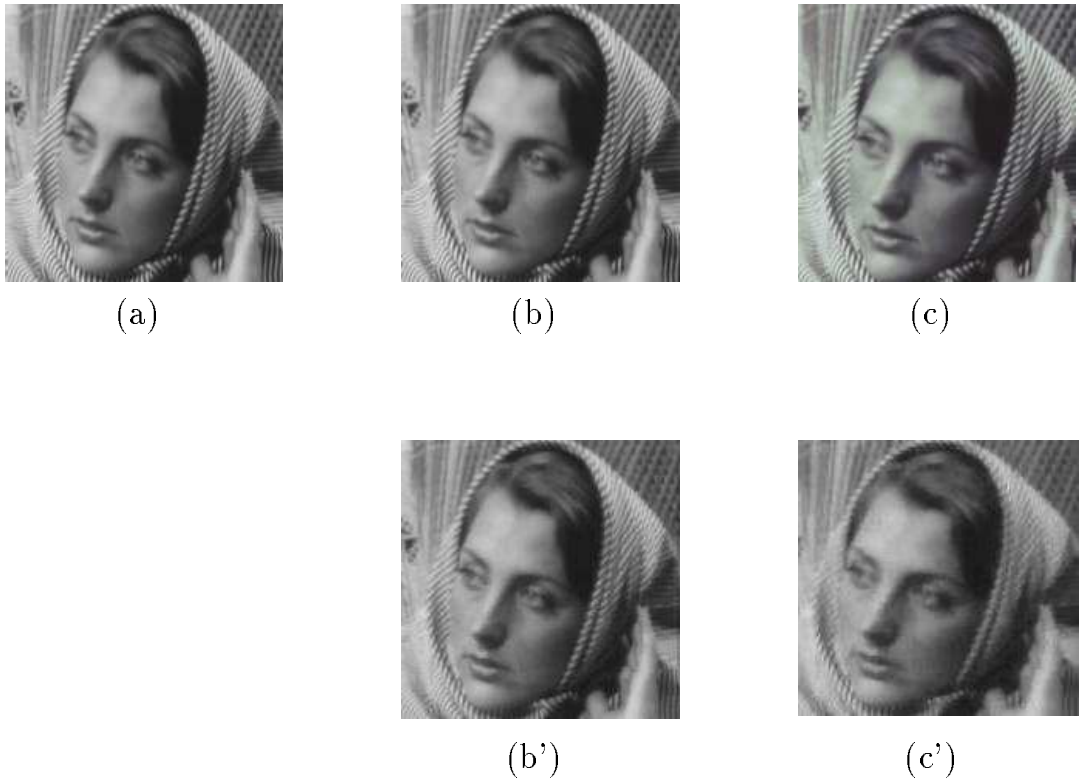


FIG. 10 – *Déformations engendrées par les tests Stirmark et Unzign.*
(a) image originale,
(b) image consécutivement à une itération de Stirmark,
(c) image consécutivement à cinq itérations de Stirmark,
(b') image consécutivement à une itération de UnZign,
(c') image consécutivement à cinq itérations de UnZign

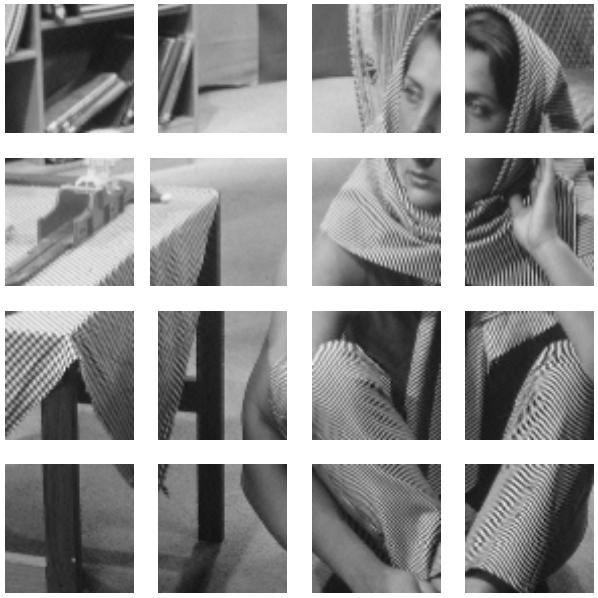


FIG. 11 – *La mosaïque d'image, une parade aux détecteurs automatiques de tatouage*

3 Modélisation des systèmes de tatouage : aspects protocoles

Nous avons vu au paragraphe 1 que les différents services auxquels se proposent de répondre les systèmes de tatouages font intervenir plusieurs acteurs et consistent en l'établissement d'un certain nombre de preuves : preuve de la propriété du copyright, preuve de l'intégrité de l'image, etc. Dès lors, il est clair que des protocoles rigoureux spécifiant à la fois les informations à transmettre et les modes d'échanges doivent être définis afin de garantir le bon fonctionnement des services. Dans ce paragraphe, nous ne saurions proposer des protocoles complets et « définitifs », d'une part parce que les besoins se précisent au fur et à mesure que les services se développent, d'autre part parce qu'il existe autant de protocoles que d'applications. Notre objectif est de mettre en valeur les différents choix qui peuvent se poser lors de la définition d'un système. Nous renvoyons le lecteur au chapitre 6 pour des protocoles détaillés dans le cadre d'applications davantage définies.

3.1 Protocoles usuels en sécurité

Nous rappelons ici les trois types de protocoles fondamentaux en sécurité. Pour plus de simplicité, nous nous limitons au cas d'un échange entre deux individus Alain et Claire où une troisième personne Julien joue éventuellement le rôle de juge.

- Protocole arbitré : Il s'agit d'un protocole dans lequel Julien, une personne intègre et désintéressée (le juge) veille au bon déroulement de la transaction entre Alain et Claire (fig. 12a). Aucune phase du protocole ne se déroule hors du contrôle de Julien. Si l'on admet l'hypothèse que Julien est par définition intègre et qu'il ne

peut pas être corrompu par l'une des deux parties, un protocole basé sur ce mode de fonctionnement possède vraisemblablement un haut niveau de sécurité. Néanmoins il est souvent considéré comme très lourd dans la mesure où le juge doit prendre part à chaque transaction.

- Protocole avec juge-arbitre : Il s'agit d'un protocole arbitré dans lequel l'intervention de Julien, le juge se limite aux phases de conflit. Dans un déroulement « normal » de la communication entre Alain et Claire, on se dispense de l'approbation de Julien (fig. 12b).

- Protocole à discipline intrinsèque : Ce type de protocole est le plus satisfaisant dans la mesure où il assure lui-même son bon déroulement (fig. 12c). Aucun juge n'est nécessaire, ni dans le cadre d'une déroulement normal du protocole, ni même pour dénouer les conflits. Chacun des protagonistes du protocole peut se rendre compte immédiatement d'une fraude de l'autre partie et peut alors stopper l'exécution du protocole. Malheureusement, un protocole de ce type ne peut être mis en place dans toutes les situtations.

3.2 Informations et individus impliqués dans l'établissement des preuves

Nous limitons notre étude aux services de protection du copyright et d'intégrité d'une image. Dans les deux cas, nous distinguons un protocole de dépôt associé à l'opération de tatouage de l'image et un protocole de vérification correspondant à l'extraction ou à la vérification du tatouage.

Protection du copyright

Les protocoles à discipline intrinsèque semblent totalement inadaptés à ce problème dans la mesure où l'arrêt du protocole ne constitue pas une parade à une tentative de manoeuvre frauduleuse. En effet, le protocole ne vise pas à établir les conditions préalables à une communication « sûre » mais à garantir la véracité d'une preuve. Alain veut pouvoir affirmer à Claire ou devant un tribunal (si Claire est malhonnête) qu'il dispose effectivement de la propriété d'une image. Nous sommes typiquement dans un contexte où l'intervention d'un juge (Julien) est nécessaire. On s'oriente donc vers un protocole arbitré ou tout au moins un protocole avec juge-arbitre. Pour étayer son affirmation quant à la propriété de l'image, Alain dispose de l'information introduite dans l'image sous la forme d'un tatouage. On supposera ce tatouage parfaitement robuste aux traitements de l'image, seuls les aspects liés aux protocoles nous incombent pour l'instant. Les problèmes à résoudre par les protocoles sont, d'une part de prouver l'antériorité d'un tatouage par rapport à un autre afin de démasquer si un individu tente de s'approprier les droits d'auteur en sur-tatouant l'image, et d'autre part, d'attester que le tatouage identifie bien la personne à l'origine de la protection de l'image. Les protocoles se doivent d'assurer l'impartialité du jugement en n'étant ni favorable à Alain ni à Claire. Etudions les rôles pouvant être joués par Julien.

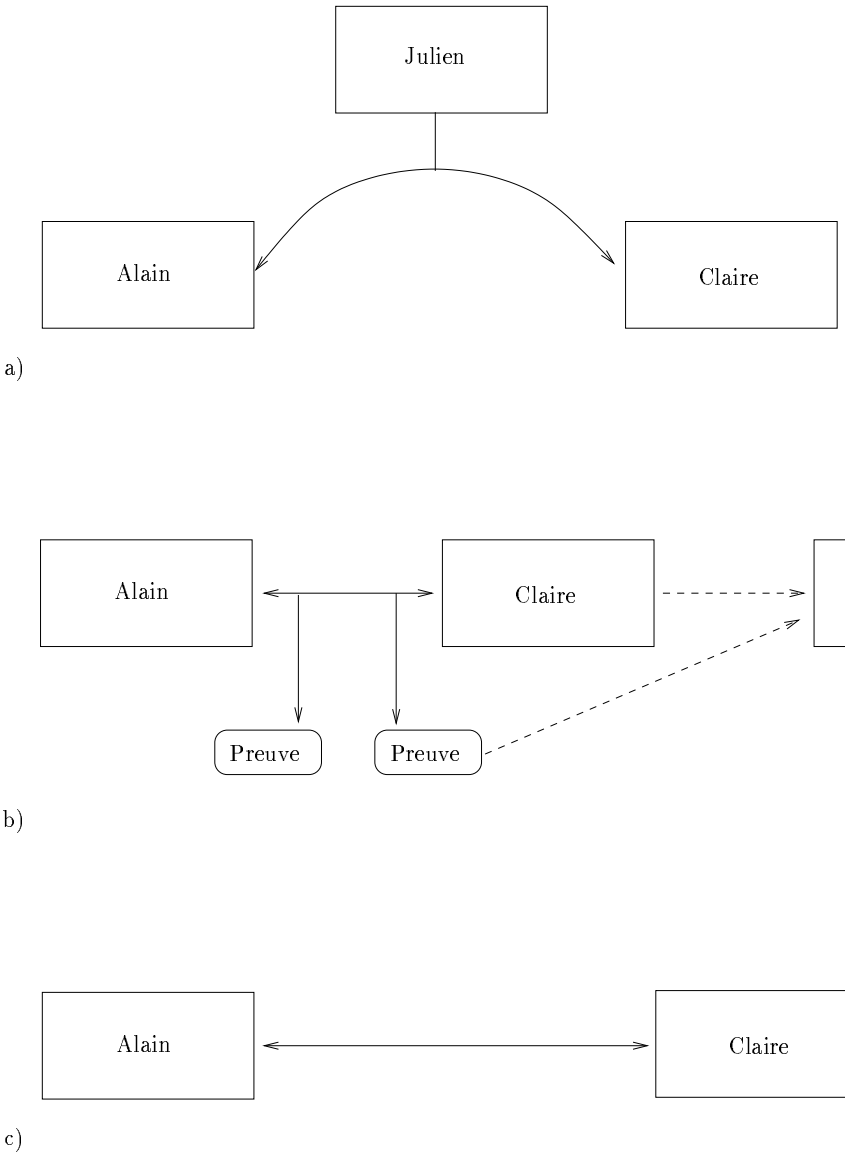


FIG. 12 – *(a) protocole arbitré, (b) protocole avec juge-arbitre, (c) protocole à discipline intrinsèque*

Une première possibilité est d'imaginer Julien intégralement en charge de toutes les opérations, dépôt et vérification du tatouage. Alain communique simplement à Julien l'image qu'il souhaite voir tatouée en prenant soin de la crypter afin qu'Isabelle , une intruse n'ait aucun intérêt à l'intercepter. Julien réalise alors le tatouage de l'image pour le compte d'Alain et lui retourne l'image tatouée ainsi qu'une information secrète nécessaire à l'extraction du tatouage. Le rôle de Julien peut ne pas se limiter à la procédure de dépôt du tatouage, il est sans doute souhaitable que Julien soit directement impliqué dans l'établissement de la preuve. Alain transmet à Julien l'image tatouée pour laquelle il veut prouver sa propriété ainsi que l'information secrète nécessaire à l'extraction du tatouage qui lui a été attribuée lors du dépôt de l'image. Julien effectue alors l'opération d'extraction du tatouage, vérifie la date de dépôt et informe Claire que l'image appartient à Alain depuis la date « t ». Dans le but de protéger les intérêts de Claire, il peut être intéressant d'imposer qu'Alain ne puisse pas directement procéder à l'extraction du tatouage. En effet, de nombreux algorithmes de tatouage sont basés sur un système cryptographique à clé secrète. Autrement dit, si Alain dispose de la clé secrète, il peut pratiquer n'importe quelle opération sur le tatouage, et tenter de le falsifier, y compris extraire un tatouage d'une image et le réintroduire dans une autre image en court-circuitant Julien (si l'on postule que l'algorithme mis en place par Julien est public). Un des intérêts pouvant motiver la réalisation de l'opération d'extraction par Julien, réside dans la possibilité d'assurer la vérification du copyright tout en ne permettant pas à Alain d'avoir accès au tatouage. En effet, Julien peut mettre en place une étape intermédiaire telle que l'information secrète communiquée à Alain ne permette pas d'extraire directement le tatouage mais pointe vers une autre information qui, elle, est directement utilisée par l'algorithme de vérification. Cette solution garantit une certaine équité entre Alain et Julien puisque ni l'un ni l'autre n'a *a priori* la possibilité d'intervenir sur le tatouage.

Néanmoins, il est toujours gênant de concentrer tous les pouvoirs entre les mains d'une seule personne, dans le cas précédent Julien. Si celui-ci devient corrompu, le système s'écroule et ni Alain ni Claire n'ont de moyen pour se défendre. Nous envisageons ici une deuxième possibilité dans laquelle à la fois Alain et Julien sont impliqués de manière indissociable, tant dans le protocole de dépôt que dans celui de vérification. Alain applique une fonction de hachage à l'image originale, le message obtenu est envoyé à Julien. Julien intègre une information identifiant Alain et une relative à la date puis retourne à Alain le message ainsi formé qui constituera le tatouage. Le protocole peut certes imposer que le tatouage contienne une information relative à l'image afin que les tatouages ne soient plus interchangeables d'une image à l'autre. Cette solution est cependant difficilement applicable à notre contexte où l'image à vérifier est susceptible d'être modifiée.

Nous souhaitons soulever un dernier point fondamental quant aux protocoles et plus particulièrement aux données intervenant dans le cadre de la protection du copyright par tatouage. Il est impératif de ne pas mettre en circulation l'image originale, seule la version tatouée doit être rendue publique. Ceci pose un problème majeur pour les « oeuvres anciennes » qui certes font l'objet d'une protection du copyright sur le plan juridique mais pour lesquelles aucune protection par tatouage n'a été mise en place préalablement à leur diffusion.

Remarque

Dans la littérature et dans cette thèse, on considère le tatouage comme une solution pour prouver le copyright d'une image, il s'agit la plupart du temps d'un abus de langage. Les techniques de tatouage permettent uniquement de trancher des situations conflictuelles dans lesquelles deux personnes, Alain et Claire revendiquent le copyright d'une même image. Ces techniques ne prouvent pas qu'il n'existe pas une troisième personne inconnue Thérèse disposant du copyright de très longue date. La condition pour prouver strictement le copyright d'une image nécessiterait pour chaque nouveau dépôt de s'assurer que l'image n'a pas été déjà déposée. Cette contrainte semble peu réaliste tant sur le plan technique que juridique car elle impliquerait que toutes les images soient déposées chez un même juge ou tout au moins qu'il existe des systèmes coopérants, gérant une base de données de toutes les images déposées et qui soit rapidement interrogeable.

Protection de l'intégrité d'une image

L'exigence d'un protocole arbitré pour ce service apparaît beaucoup moins immédiate que pour la protection du copyright. Il semble *a priori* que l'on puisse se satisfaire d'un protocole à discipline intrinsèque. Seule la contrainte de ne pas avoir recours à l'image originale (qui fait justement l'objet du contrôle) lors de la procédure d'extraction du tatouage apparaît incontournable. Soient Alain le propriétaire de l'image et Claire la cliente à qui se destine cette image. Si Alain et Claire partagent une clé secrète (pouvant éventuellement être utilisée pour plusieurs images), Alain procède au tatouage de l'image à l'aide de cette clé puis fait parvenir à Claire l'image tatouée. Claire disposant de la clé, elle peut extraire le tatouage et s'assurer ainsi de l'intégrité de l'image. Si Isabelle s'introduit dans la transaction entre Alain et Claire en procèdant à une retouche de l'image, Claire sera *a priori* capable de détecter ces manipulations. Des variantes de ce protocole sont envisageables. Par exemple pour supprimer l'échange de clé, un système cryptographique à clé publique peut être adopté si celui-ci est compatible avec le procédé de tatouage (cf. §2.2 chap.3). Ce premier protocole très simple repose sur une confiance réciproque de Alain envers Claire, ce qui autorise de se dispenser de juge. Malheureusement, tel n'est pas toujours le cas. En effet, il est légitime de penser qu'Alain n'est pas le seul à diffuser ses propres images, même s'il en est l'auteur. Supposons par exemple que la mise en circulation de l'image soit prise en charge par Isabelle, elle a la possibilité de modifier l'image puis de la retatouer comme bon lui semble. Dans ce nouveau contexte, Claire n'a pas obligatoirement connaissance de l'existence d'Alain , Isabelle peut se présenter comme l'unique interlocuteur de Claire. Claire est alors invitée à vérifier l'intégrité de l'image qu'elle reçoit par rapport à l'image retouchée par Isabelle et non vis-à-vis de l'image originale créée par Alain. La notion d'intégrité est relative à la définition d'une image de référence, il apparaît naturel de considérer l'image créée par Alain comme devant remplir cette fonction. Pour satisfaire cette requête, un protocole arbitré semble de nouveau nécessaire. Nous proposons la création d'un organisme de certification indépendant, dirigé par Julien. Le rôle de Julien est de gérer une liste d'images pour lesquelles il se porte garant de l'intégrité. Isabelle le distributeur d'images fait preuve de sa bonne foi en déclarant que les images qu'elle diffuse sont certifiées par Julien, créant ainsi une

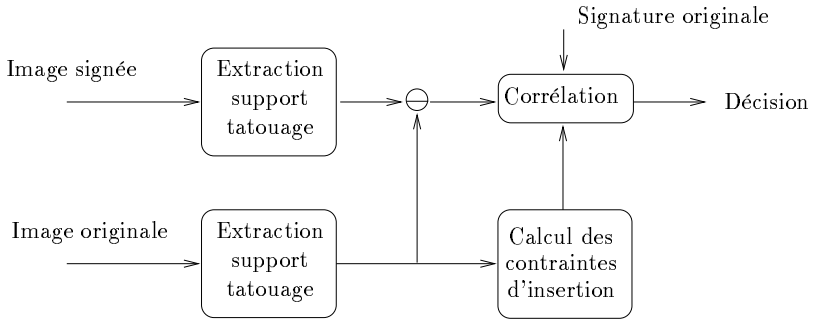


FIG. 13 – *Mode d'extraction assisté (non aveugle)*

sorte de label de qualité. Claire, une cliente d'Isabelle est alors libre de contacter Julien si elle souhaite réellement vérifier l'intégrité de l'image qu'elle souhaite acquérir. Alain n'est pas sollicité à chaque fois que Claire demande la certification d'une de ses images, il se trouve simplement impliqué lorsqu'il décide de faire enregistrer une nouvelle image auprès de Julien. L'organisme garde la trace d'Alain qui communique l'image dite de référence et assure ainsi parallèlement un service de non-répudiation, s'il s'avère qu'Alain était un imposteur, Claire et Julien pourront se retourner contre lui.

Les différents protocoles envisagés ont conduit à définir plusieurs modes pour l'extraction du tatouage : mode non-aveugle, mode semi-aveugle et mode aveugle. Ces modes spécifient l'information *a priori* dont dispose le module d'extraction pour la vérification du tatouage. Nous les avons classés par ordre de connaissances *a priori* décroissantes, impliquant un niveau de robustesse de plus en plus faible. Nous discuterons de ce dernier point au paragraphe 4 relatif aux aspects de traitements d'image du tatouage.

Mode non-aveugle : Le récepteur dispose de l'image ainsi que du tatouage original (fig. 13). Ce contexte est bien évidemment incompatible avec des applications visant à vérifier l'intégrité de l'image, ou à assurer la vérification en temps réel du copyright (pas de délai pour interroger une base contenant les données originales).

Mode semi-aveugle : Le tatouage original est supposé connu lors de l'extraction (fig. 14) et utilisé le plus souvent *via* un score de corrélation.

Mode aveugle : Il s'agit du seul mode où l'on peut réellement parler d'extraction (par opposition à la vérification intervenant dans les deux précédents modes) du tatouage puisque l'on ne présuppose ni la connaissance du tatouage, ni la connaissance de l'image originale (fig. 15).

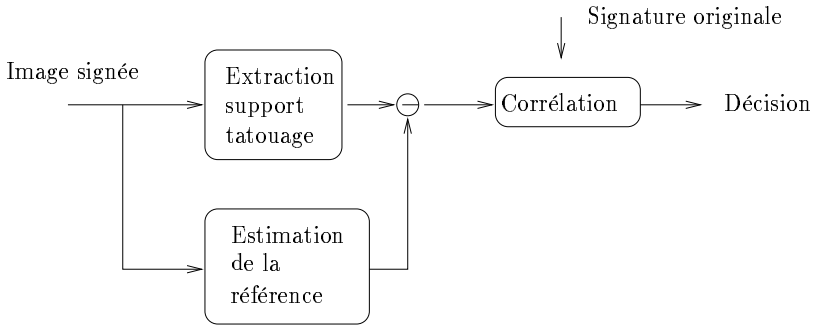


FIG. 14 – *Mode d'extraction semi-aveugle*

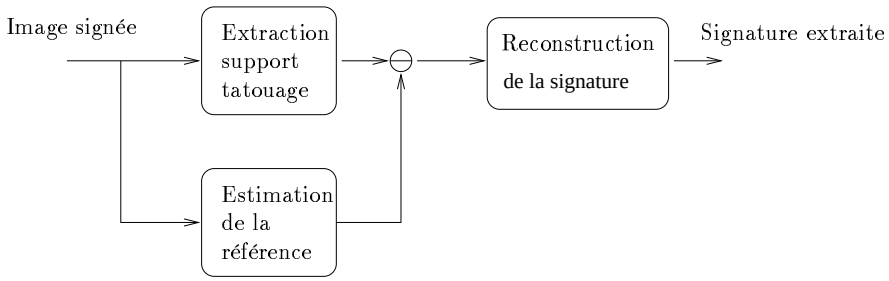


FIG. 15 – *Mode d'extraction aveugle*

4 Modélisation des systèmes de tatouage : aspects traitements d'image

Du point de vue du traitement d'image, la problématique du tatouage [78] s'articule autour des trois points clés suivants :

- Visibilité,
- Robustesse,
- Capacité d'insertion (volume relatif du tatouage et de l'image).

La robustesse du tatouage est un élément essentiel à prendre en considération lors de la conception d'un système de tatouage dans la mesure où l'image tatouée subira très probablement des manipulations parmi celles présentées au paragraphe 2. Il s'agit là d'une différence fondamentale entre les systèmes de tatouage d'images et les procédés stéganographiques. Les techniques stéganographiques se préoccupent de gérer le compromis visibilité *vs.* capacité d'insertion. En ce point elles se rapprochent des problèmes rencontrés en tatouage d'image bien que, dans ce dernier cas il soit *a priori* exclu de répartir le tatouage sur plusieurs images notamment pour revendiquer le copyright d'une image. Cette restriction n'apparaît pas dans les systèmes stéganographiques où l'on peut envisager de transmettre un message secret à l'aide de plusieurs images.

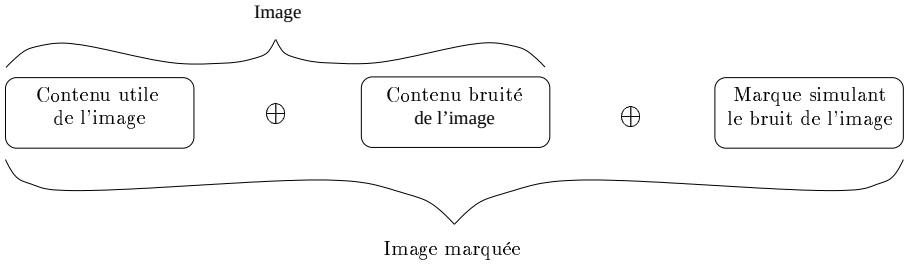


FIG. 16 – *Modélisation du problème de tatouage : point de vue perceptif*

Les diverses transformations présentées au paragraphe 2 ne permettent pas d'identifier un modèle de transformation apte à englober l'ensemble de ces transformations possibles. Il s'agit là d'un problème majeur. Les attributs extraits servant de support au tatouage doivent présenter une invariance pour la classe des manipulations préservant la qualité de l'image exposées au paragraphe 2.

Le rapport entre le volume d'information du tatouage et le volume d'information du média sur lequel s'applique le tatouage joue un rôle primordial dans la problématique. En effet, il est clair que si l'on conçoit l'image comme un canal de transmission (cf. § 4.1) plus l'image a une taille importante, plus la capacité du canal sera élevée. Ce point est parfaitement illustré par le traitement de la vidéo.

4.1 Rapport Signal à Bruit et tatouage d'image

Nous montrons comment l'introduction de deux rapports signal à bruit différents est révélatrices du compromis visibilité, robustesse, capacité d'insertion caractéristique des systèmes de tatouage d'image. Chacun des rapports S/B introduit est représentatif de l'angle sous lequel on examine le problème.

Point de vue visibilité du tatouage

Matsui et Tanaka [62] appréhendent le tatouage d'image d'un point de vue stéganographique en considérant qu'une image est la superposition d'une partie structurée contenant l'information « utile » et d'un bruit psychovisuellement imperceptible dans le cas d'images de bonne qualité. L'objectif d'un système de tatouage est alors de créer une marque présentant toutes les caractéristiques d'un bruit afin qu'elle soit confondue avec le bruit « naturel » de l'image. Ce bruit « naturel » a des origines diverses, il peut être notamment engendré par les systèmes d'acquisition (capteurs CCD), les conversions analogiques / numériques lors d'un transfert d'une pellicule photo sur un support numérique, par la compression d'une image générant un bruit de quantification, etc. Suivant ce formalisme, la visibilité du tatouage est naturellement évaluée en termes de rapport signal à bruit. L'image originale constitue le signal (utile) alors que le tatouage représente le bruit (parasite du point de vue de la visibilité). Il apparaît qu'un PSNR de l'ordre de 38 dB (classiquement exigé par les industriels) confère à l'image tatouée une qualité comparable à un facteur de qualité 87 dans la norme de compression Jpeg qui est bien supérieur au facteur 75 préconisé par défaut.

Point de vue robustesse du tatouage

La théorie des communications a largement recours à la notion de rapport signal à bruit pour mesurer la difficulté de retrouver un signal noyé dans un autre signal ou dans un signal composite. On entrevoit ici clairement le parallèle pouvant exister avec la notion de robustesse du tatouage. La force de marquage peut en effet être exprimée comme le PSNR entre le signal constitutif du tatouage et l'image qui dans ce cas de figure est assimilée à un bruit parasite. Certains auteurs [85, 60] ont proposé d'étendre cette analogie en modélisant également les attaques par un bruit perturbant l'extraction du tatouage. On est donc amené à considérer un rapport signal à bruit où le signal reste constitué par le tatouage mais où le bruit est composite. Il s'agit de la superposition de deux bruits, l'un systématique représentant l'image, l'autre fluctuant, dépendant de l'attaque pratiquée. L'extraction du tatouage est bien évidemment potentiellement plus aisée si le rapport signal à bruit est élevé. Il nous semble important d'apporter quelques remarques quant à l'opportunité de mesurer la « force » d'une attaque par le rapport signal à bruit. En effet, une simple rotation de l'image de 0.7 degré conduit à un PSNR de l'ordre de 22.5 dB qui est bien inférieur aux 28 dB résultant d'une compression Jpeg qualité 5% bien que la dégradation semble beaucoup plus forte dans le second cas. De plus la définition du PSNR ne nous semble pas immédiate pour bon nombre d'attaques. Comment le définir par exemple si l'on recadre l'image ou si l'on change sa résolution ?

Ces deux points de vue nous permettent de percevoir l'antagonisme existant entre les deux requêtes, d'une part l'invisibilité du tatouage, d'autre part la robustesse de celui-ci.

4.2 Modèle projectif basé sur la séparation de sources

Le tatouage d'image peut être appréhendé comme une opération de fusion entre deux sources. La première, l'image est essentielle en terme de visibilité alors que la seconde, le tatouage est prépondérante dès lors que l'on s'attache à la notion de robustesse. Suivant ce point de vue, l'extraction du tatouage apparaît comme un problème de séparation de sources en milieu bruité. Le bruit jouant ici le rôle d'élément perturbateur représente les diverses manipulations de l'image.

Exposé du modèle

Soit S, une signature formée par une séquence de N bits : $\{s_0, s_1, \ldots, s_{N-1}\}$ avec $s_i \in \{-1; 1\}$. Soit I l'image orginale que l'on souhaite protéger à l'aide de S. Nous désignons par C le canal de transmission du tatouage défini par :

$$C = X(I)$$

où X est une transformation de l'image qu'il conviendra de préciser. Nous munissons l'espace engendré par X d'une base orthogonale $\{\phi_i\}$ dans laquelle le tatouage w s'exprime par :

$$w = \sum_{i=0}^{N-1} s_i \alpha(x, y) \phi_i(x, y)$$

où $\alpha(x, y)$ est un masque permettant d'adapter l'énergie du tatouage aux caractéristiques psychovisuelles des régions de l'image considérée.

Le canal de transmission tatoué est alors défini par :

$$\hat{C} = C + w$$

L'image tatouée s'exprime comme la transformée inverse du canal tatoué :

$$\hat{I} = X^{-1}(\hat{C})$$

La récupération des bits de signature est interprétée comme une projection du canal tatoué $\hat{C}$ sur les fonctions de base $\{\phi_i\}$

$$r_i =< \epsilon(\hat{C}), \phi_i >$$

Nous désignons par ϵ une opération de pré-détection visant à accroître les performances du détecteur, nous donnons un exemple d'une telle opération dans l'état de l'art au paragraphe 6.1. Sous l'hypothèse que ϵ puisse être implémenté par filtrage linéaire, si h désigne la réponse impulsionnelle de ce filtre, on a :

$$\begin{aligned} r_i &= < \hat{C} * h, \phi_i > \\ &= < (C + w) * h, \phi_i > \\ &= < w * h, \phi_i > + < C * h, \phi_i > \end{aligned}$$

Développons à présent l'expression précédente en substituant w :

$$r_i =< \sum_{i=0}^{N-1} s_i \alpha(x, y)\phi_i(x, y), \phi_i(x, y) > + < C * h, \phi_i > \quad (2)$$

D'après le formalisme développé, la construction d'un système de tatouage requiert la définition :

- de la transformation X définissant l'espace dans lequel va être réalisée l'opération d'insertion du tatouage. Nous verrons dans le chapitre 3 sur l'état de l'art qu'il peut s'agir par exemple de l'espace de Fourrier ou d'un de ses dérivés.

- du masque psychovisuel $\alpha(x, y)$;

- de la base orthogonale $\phi_i(x, y)$;

- du filtre de prédétection ϵ défini par sa réponse impulsionnelle h.

Modèle projectif et modes d'extraction

Le modèle projectif venant d'être présenté donne un éclairage sur les implications du mode d'extraction vis-à-vis de la robustesse du tatouage. Reprenons l'équation 2, la linéarité du produit scalaire nous a permis de décomposer r_i en deux termes. Il est clair que dans l'optique d'extraire les bits s_i représentant la signature, seul le premier terme $< \sum_{i=0}^{N-1} s_i \alpha(x,y)\phi_i(x,y), \phi_i(x,y) >$ est porteur d'information, le second $< C * h, \phi_i >$ est un terme perturbateur qu'il convient de maîtriser. Plusieurs stratégies ont vu le jour, elles sont directement reliées au mode d'extraction envisagé.

mode aveugle on ne dispose d'aucune information *a priori*, on va chercher à rendre négligeable le terme perturbateur par un filtrage de prédétection. Ce filtrage tend à modifier la distribution statistique de C de telle sorte qu'elle se rapproche d'une courbe gaussienne à moyenne nulle et à faible écart type. Nous illustrons cette stratégie dans le chapitre sur l'état de l'art paragraphe 6.1. D'autres procédés sont présentés dans l'article [7, 99].

mode semi aveugle On distingue deux cas de figure : le premier où la connaissance de l'image originale I permet le calcul de C, on peut donc déterminer le terme $< C * h, \phi_i >$ et ainsi s'en affranchir [86]. Dans le second cas la connaissance *a priori* est constituée par la signature originale. Une corrélation entre la signature extraite et la signature originale permet généralement la mise en valeur d'un pique caractéristique de la coïncidence des deux signaux. Le terme $< C * h, \phi_i >$ peut amoindrir l'amplitude de ce pique mais généralement il n'empêche pas de le détecter.

mode non aveugle On cumule ici les facilités d'extraction du tatouage constituées par les deux sous modes semi aveugles, ce qui en fait naturellement le mode d'extraction [2] le plus robuste.

5 Les difficultés pour estimer les performances des algorithmes

Tout algorithme, et particulièrement ceux destinés à des services de sécurité, doit faire l'objet d'une évaluation de performance. Cet aspect du problème de tatouage d'image a été négligé jusqu'à une période très récente où des publications [59, 36, 70, 32] et un projet international de recherche [74] ont vu le jour. Ce manque d'évaluation des algorithmes proprosés est en partie dû à la jeunesse du domaine, mais aussi à la difficulté de procéder à une évaluation rigoureuse. La plupart des tests relèvent de méthodes empiriques. En effet, un certain nombre d'aspects critiques pour la conception des systèmes se révèle également critique pour leur évaluation. La prise en compte de critères psychovisuels est par exemple déterminante pour estimer les performances d'une méthode, tout comme la connaissance d'un critère analytique de robustesse du tatouage. Même si de nombreux travaux se préoccupent de ces deux points [42, 1], les solutions proposées ne sont pas

2. pour ce mode on parle parfois de vérification plutôt que d'extraction puisque l'information à extraire (la signature) est connue, il est donc plus correcte d'employer le terme de vérification.

encore capables de gérer la complexité des problèmes (facteur subjectif humain pour la vision, multiplicité des attaques pour la robustesse). Nous soulevons un dernier point à propos des difficultés d'évaluation des méthodes de tatouage, il s'agit de la confidentialité des algorithmes proprement dits. En effet, de nombreux algorithmes ne sont pas encore divulgués par leurs auteurs, ni même mis à disposition pour des tests, ceci ne permet pas la conduite d'une évaluation rigoureuse. En effet, les systèmes connus ont fait l'objet d'un « acharnement » particulier qui très souvent a conduit à faire apparaître leurs faiblesses, néanmoins selon le principe de Kerckhoffs [52], il serait dangereux de considérer un algorithme secret comme sûr.

Sans préjuger des résultats des tests qui sont en cours, on peut d'ores et déjà affirmer que les systèmes de tatouage ne peuvent être considérés comme intrinsèquement sûrs, la robustesse d'un système est bien entendu relative aux attaques qu'il peut supporter sans dommage, or il est clair que l'ensemble des attaques est difficilement dénombrable.

6 Conclusion

Ce chapitre nous a permis d'apprécier l'étendue du champ d'application des systèmes de tatouage d'image, depuis les problèmes de protection des droits d'auteur ayant motivé l'apparition de ces techniques, jusqu'aux services plus récents visant à assurer l'intégrité, ou le notariat électronique des images. Cette diversité dans les applications a induit le développement de plusieurs types de tatouage dont nous avons explicité les propriétés spécifiques. Nous avons montré que la problématique inhérente aux systèmes de tatouage peut être formulée autour du compromis visibilité/robustesse/capacité d'insertion. La définition de ce compromis passe par un inventaire des manipulations des images pour lesquelles le tatouage doit subsister, ainsi que par la définition d'un critère capable d'apprécier la qualité de l'image tatouée par rapport à l'image originale. Notons enfin que la jeunesse de ce domaine d'étude justifie une problématique encore incomplète. Nous avons souligné, outre les problèmes de traitement d'image, l'existence de difficultés relatives à l'intégration des techniques de tatouage dans des systèmes complets.

Chapitre 3

Etat de l'art des techniques de tatouage d'image

Parmi les services de sécurité requis par les systèmes multimédia, il convient de distinguer : la confidentialité, la non répudiation tant du point de vue de l'acheteur que du vendeur, la protection des droits d'auteur, la vérification de l'intégrité d'un document. Les deux derniers cités constituent le champ d'investigation privilégié des techniques de « watermarking » que l'on peut traduire par tatouage ou filigrane. Dans ce chapitre en partie extrait de [81, 25, 29], nous dressons un panorama des différentes méthodes de tatouage de documents numériques présentes dans la littérature, ainsi que des critiques qu'elles suscitent. La protection des droits d'auteur des images fixes occupe une place prépondérante dans la littérature relative au tatouage, elle apparaît par conséquent également en bonne place dans ce chapitre.

1 Organisation du chapitre

Nous avons délibérément décidé de ne pas présenter successivement l'ensemble des méthodes dans leur intégralité[3]. En effet, de nombreuses solutions présentent des recouvrements les unes avec les autres. Nous avons donc opté pour un canevas général dans lequel l'ensemble des phases clés d'un système de tatouage est discutée au travers des différentes options et solutions proposées dans la littérature. Ce canevas s'articule autour des sept points suivants :

- les méthodes adoptées pour la sélection des pixels ou blocs de pixels contenant l'information sur le tatouage ;
- le choix d'un espace transformé dans lequel on va réaliser l'opération de dissimulation du tatouage (DCT, ondelettes ...) ;
- les méthodes de mise en forme du tatouage et en particulier d'ajout de redondance dans la signature initiale ;
- le type de modulation adoptée pour introduire la signature dans l'image ;
- les stratégies liées à la récupération ou à la vérification de la signature ;
- l'adaptation des algorithmes de base pour satisfaire au traitement de la vidéo.

Nous terminons ce chapitre par une présentation de quelques contre-mesures afin de prendre en défaut certains systèmes de tatouage exposés.

2 Choix des éléments de l'image recevant l'information de signature : aspects cryptographiques et psychovisuels

Nous avons vu lors de l'étude de la problématique du tatouage d'image qu'il est primordial que seules les personnes habilitées (propriétaire de l'oeuvre, instance supérieure) puissent avoir accès à la localisation exacte des bits du tatouage. Cet aspect de confidentialité est requis afin que le tatouage ne puisse pas être supprimé de façon triviale par des modifications ciblées des pixels de l'image. La plupart des méthodes remplissent cette fonction cryptographique grâce à des générateurs aléatoires initialisés par une clé secrète. Nous donnons un exemple de tels algorithmes au paragraphe 2.1 dans le cadre de schéma à clé privée et au paragraphe 2.2 dans le cadre de schéma à clé publique. Le choix des éléments supportant l'information de signature est également guidé par des considérations visuelles. Nous exposerons au paragraphe 2.3 une famille de techniques restreignant un tel choix directement sur des caractéristiques de l'image par opposition à celles opérant dans des espaces transformés (cf. § 3).

3. Pour un exposé complet d'une méthode donnée, le lecteur est renvoyé aux références bibliographiques qui s'y rattachent.

2.1 Clé secrète et générateur aléatoire

Selon le principe énoncé par Kerckhoff [52], un système de sécurité ne doit pas baser sa sûreté sur la confidentialité de sa méthode. Les hypothèses admises en sécurité présument l'algorithme du système connu et considèrent que l'élément de secret est apporté par une clé paramétrant l'algorithme. De nombreuses méthodes octroient une clé secrète aux personnes habilitées. Cette même clé est nécessaire à la fois pour insérer le tatouage et pour l'extraire, on parle alors d'algorithme cryptographique symétrique. Nous présentons brièvement l'algorithme du « patchwork » qui repose sur le choix d'une clé secrète.

Algorithme du « Patchwork »

Cette technique appartient à la famille des méthodes de tatouage à réponse binaire. Elle permet de répondre par **oui** ou **non** à la question : une personne est-elle en possession de l'information secrète ayant permis de générer le tatouage ? Dans cette méthode, on ne cherche en aucun cas à extraire le tatouage lui même. Détaillons à présent cet algorithme proposé par Bender [4] en 1995 et connu sous le nom d'algorithme du « Patchwork ». On considère une séquence aléatoire S_a générée à partir d'un germe K_s constituant une clé secrète et indépendante de l'image à traiter I. Cette séquence permet de sélectionner des couples de pixels (A_i, B_i) auxquels sont associés les niveaux de gris (a_i, b_i). Considérons la somme des différences de luminance des couples de pixels sélectionnés :

$$S = \sum_{i=1}^{n} a_i - b_i$$

Les auteurs émettent l'hypothèse selon laquelle cette somme tend vers 0 quand n devient suffisamment grand pour conférer à S un caractère statistique.

Le principe du Patchwork est de modifier très légèrement l'image en augmentant d'une unité le niveau de gris des pixels de type A_i et en diminuant d'un niveau de gris les pixels de type B_i. Cette opération a pour effet de rendre dépendant la séquence aléatoire S_a de l'image modifiée I', la somme S devient alors :

$$S = 2 \times n$$

où n est le nombre de couples (A_i, B_i) issus de la séquence aléatoire S_a. Une personne ne disposant pas de la clé K_s est incapable de régénérer la séquence S_a et obtiendra $S = 0$. Seule la personne disposant de K_s est en mesure d'obtenir la « bonne valeur » de S, c'est à dire $2 \times n$. Ces propos doivent être modérés par l'objection suivante : un individu malveillant peut tout à fait appliquer le même algorithme et ainsi créer une nouvelle image signée permettant d'obtenir $S' = 2 \times n$ à partir d'une clé $K_s' \neq K_s$. On tombe ici sur un problème de multi-signatures qui dépasse largement le cadre de cet algorithme. Nous reviendrons plus largement sur ces problèmes au paragraphe 8.3 ainsi qu'au chapitre 5 où nous proposons une alternative au tatouage d'image principalement afin de résoudre ces problèmes.

Cette méthode de base n'est bien sûr pas très robuste, cependant différentes extensions de cet algorithme ont vu le jour [8, 75]. Elles permettent par exemple d'accroître la

résistance du système à des opérations de filtrage sur l'image en considérant non plus des couples de pixels (A_i, B_i) mais des couples de blocs. L'emploi de plusieurs séquences aléatoires orthogonales dans le but de dissimuler plusieurs bits (1 bit par séquence aléatoire) a également été proposé.

2.2 Vérification publique du tatouage

Les algorithmes de tatouage basés sur un système cryptographique à clés secrètes peuvent être inadaptés à certaines applications, ou très contraignants. En effet, ils nécessitent l'implication du propriétaire de l'oeuvre originale, tant lors de la procédure d'insertion que lors du processus d'extraction du tatouage, puisqu'une clé secrète (souvent identique) est requise pour chacun de ces processus. Un tel fonctionnement est par exemple peu adapté avec une utilisation du tatouage visant à garantir l'intégrité d'une image. L'image est en effet susceptible d'être contrôlée par toute personne autre que son propriétaire mais paradoxalement, seul le propriétaire possède la clé secrète nécessaire à l'extraction du tatouage. La solution consistant à communiquer la clé secrète à la personne désirant vérifier l'intégrité de l'image peut s'avérer très dangereuse dans la mesure où cette personne peut alors facilement corrompre l'image et retransmettre une image falsifiée qui prendra en défaut le système de tatouage.

Dans le cadre d'algorithmes de tatouage basés sur la notion d'étalement de spectre par séquence directe (cf. § 4.1), Hartung et Girod [41] ont montré que cette technique était propice à l'introduction d'une vérification publique du tatouage. La séquence d'étalement (séquence aléatoire) constitue l'information indispensable à l'insertion et à la récupération du tatouage. Cependant, du fait de la très grande redondance du tatouage, une partie de la séquence d'étalement peut s'avérer suffisante pour reconstruire l'intégralité de la signature. Pratiquement, la séquence d'étalement originale $\mathrm{SE}_{\mathrm{orig}}$ est dégradée aléatoirement par un bruit annexe, il en résulte qu'en moyenne, la séquence publique $\mathrm{SE}_{\mathrm{pub}}$ présente un bit sur N identique à la séquence d'étalement originale, les autres prennent des valeurs aléatoires dépendantes d'un bruit annexe.

$$SE_i{}^{\mathrm{pub}} = \begin{cases} SE_i{}^{\mathrm{orig}} & \text{aléatoirement avec une probabilité } \frac{1}{N} \\ \mathrm{rand}\{-1, 1\} & \text{sinon} \end{cases}$$

La récupération publique du tatouage est bien entendu moins robuste que la récupération du tatouage connaissant entièrement la séquence d'étalement puisque la signature est reconstruite avec N fois moins d'information. D'autres systèmes à clé publique sont donnés en référence [97, 63]. Pour la critique des systèmes de tatouage public, le lecteur est renvoyé à la référence [12].

Nous abordons à présent un autre aspect concernant le choix des pixels contenant l'information de signature, il s'agit de celui garantissant la minimisation de l'impact visuel.

2.3 Codage prédictif

Les modèles prédictifs utilisés en codage de source font l'hypothèse que les échantillons ou pixels contenus dans un même voisinage sont fortement corrélés. On réalise alors généralement une combinaison linéaire des pixels contenus dans le voisinage du pixel courant

pour estimer sa valeur. L'erreur résiduelle correspondant à la différence entre la prédiction linéaire et la valeur réelle du pixel courant est propice à un codage efficace par exemple de type Huffman. En effet, l'intérêt de la prédiction réside dans la dynamique des erreurs obtenues qui est beaucoup plus faible que celle de l'image elle-même. Les erreurs possèdent généralement une distribution statistique dont la moyenne est proche de zéro et la variance faible, à l'exception des régions à fort contraste tels que les contours. L'étude des caractéristiques psychovisuelles fait apparaître des phénomènes de masquage dans les régions à fort contrastes alors que l'oeil présente une grande sensibilité dans les régions uniformes. Cette particularité du système psychovisuel jointe aux propriétés du codage prédictif a conduit certains auteurs [62] à proposer d'introduire l'information de signature par le biais d'une quantification non linéaire des erreurs. Dans le cadre des systèmes de tatouage aveugle ou semi-aveugle (cf. § 3.2 chap. 2), cette technique est également employée pour calculer un support de référence autorisant à se dispenser de l'image originale lors de l'extraction du tatouage [58]. La valeur du bit de signature rattaché à un pixel de l'image est donnée par le signe de la différence entre la valeur du pixel prédit et la valeur observée. L'hypothèse sous-jacente à une telle détection est d'admettre que les manipulations de l'image originale, induites à la fois par la présence du tatouage et des manipulations de l'image, auront surtout un impact sur l'amplitude des erreurs résiduelles et non sur leur signe.

$$b_i = \text{sign}\{\sum_{j \in \mathcal{P}} x_j - x_i\} \text{ avec } \mathcal{P} \text{ ensemble des pixels de la prédiction}$$

3 Réaliser l'insertion du tatouage dans un espace transformé

Comme nous venons de le présenter, l'algorithme du Patchwork ou les méthodes basées sur le codage prédictif, réalisent le tatouage de l'image directement au niveau des pixels de l'image, néanmoins de nombreuses méthodes optent pour des espaces transformés. Le choix d'un espace transformé pour effectuer l'opération de tatouage repose sur deux idées fortes. On espère : d'une part, tirer parti des phénomènes de masquage déjà étudiés en codage de source, d'autre part extraire des invariants afin d'anticiper d'éventuelles manipulations de l'image.

3.1 Le domaine DCT

Les motivations ayant conduit aux approches par DCT sont de deux ordres :

- l'une se réfère à des questions de visibilité ; les quelques notions psychovisuelles actuellement disponibles sont souvent exprimées en termes de fréquences orientées.
- l'autre a trait à l'utilisation massive de codeurs JPEG basés sur la transformée DCT pour compresser les images. Un algorithme de tatouage construit sur la base de la DCT devrait donc plus facilement prendre en compte la contrainte de robustesse du tatouage face à l'utilisation de JPEG.

Rappels sur la transformée DCT et la compression JPEG

Dans le cadre d'une application aux images, par exemple, pour le codage, il est d'usage, pour des raisons principalement liées à la complexité de calcul de considérer une transformation par blocs de 8×8 pixels. La transformée DCT 2-D par bloc utilisée dans la norme JPEG se définit par :

$$p_{ij} = \frac{2K(i)}{\sqrt{N}} \times \cos \frac{(2j+1) \times i \times \pi}{2N} \qquad (i, j = 0, 1, ..., 7)$$

$$\text{avec N=8 et } K(i) = \begin{cases} \frac{1}{\sqrt{2}} & (i = 0) \\ 1 & (i = 1, 2, ..., 7) \end{cases}$$

La propriété d'orthogonalité de la transformée DCT, permet de calculer la matrice des coefficients DCT $[A]$ simplement :

$$[A] = [a_{ij}] = [p_{ij}] \times [s_{ij}] \times [p_{ij}]^t \qquad (i, j = 0, 1, ..., 7)$$

où s_{ij} est le niveau de gris associé au pixel (i, j) du bloc considéré.

Dans la norme de compression JPEG, une quantification des coefficients fait suite au calcul de la transformée. Les tables de quantification ont été élaborées sur la base de tests psychovisuels. En première approximation, on peut considérer que le pas de quantification est d'autant plus faible que les coefficients DCT sont rattachés à des basses fréquences. Pour un complément d'information sur la norme JPEG, le lecteur est renvoyé aux références [93, 69].

Application au tatouage d'images

La robustesse du tatouage vis-à-vis de la compression JPEG implique de ne pas utiliser les coefficients DCT associés aux hautes fréquences bien qu'ils présentent un impact visuel réduit conforme à l'exigence d'invisibilité du tatouage. Selon le compromis visibilité *vs.* robustesse souhaité, on opte généralement pour l'utilisation des coefficients de basses et/ou de moyennes fréquences. Nous renvoyons le lecteur au paragraphe 5.4 concernant les détails de mixage du tatouage et de l'image originale.

3.2 L'espace engendré par la transformée de Fourier-Mellin

Des transformations géométriques de l'image tatouée conduisent fréquemment à l'impossibilité d'extraire le tatouage pour de nombreux algorithmes. Ce constat a conduit à envisager l'implantation du tatouage dans un espace transformé présentant une invariance aux opérations géométriques usuelles de l'image. Dans l'article [67], Ó Ruanaidh *et al.* préconisent l'usage de la transformée de Fourier-Mellin pour assurer la restitution du tatouage après que l'image a subi une translation et/ou une rotation et/ou un changement d'échelle. Les auteurs mentionnent que cette transformée est également utilisée dans le produit commercial PictureMarc de la société Digimarc. L'espace transformé de

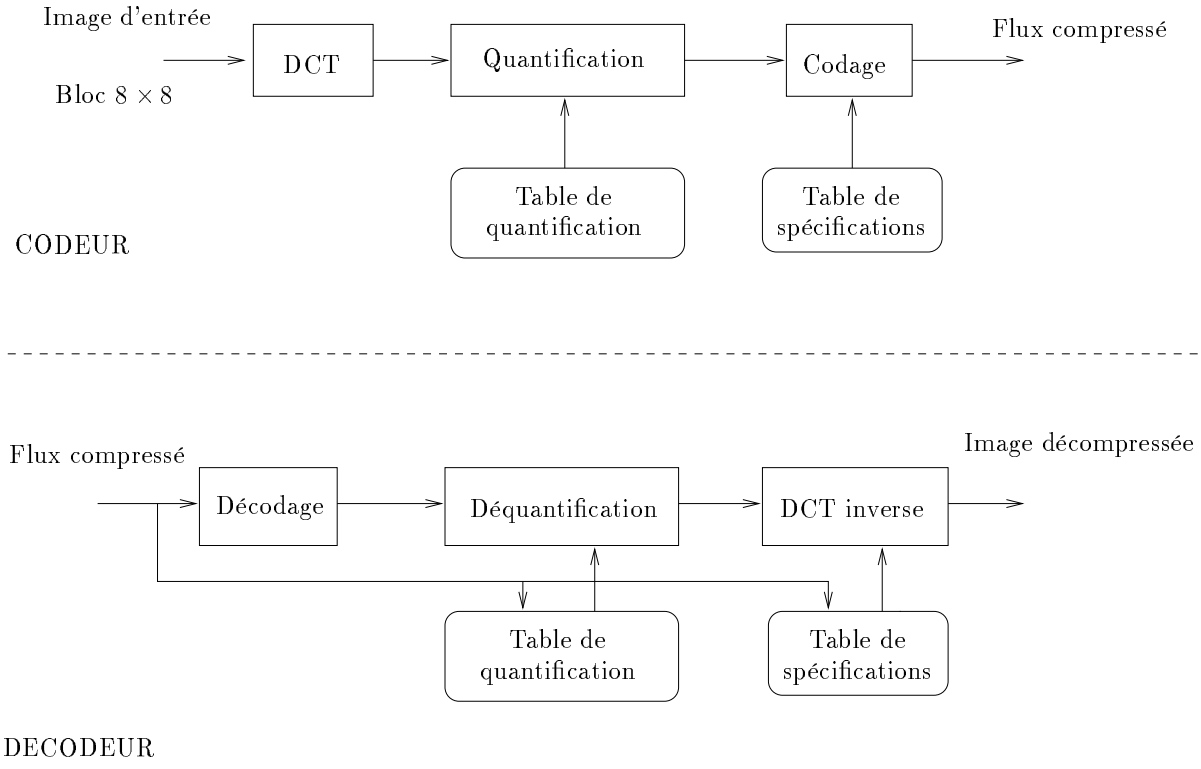


FIG. 1 – *Schéma de principe de la compression JPEG*

Fourier-Mellin est construit sur la base de la propriété de translation de la transformée de Fourier.

$$f(x_1 + a, x_2 + b) \leftrightarrow F(k_1, k_2)e^{[-j(ak_1+bk_2)]}$$

On constate immédiatement que seule la phase (dans le domaine de Fourier) est affectée par la translation. En conséquence si l'on restreint l'espace dans lequel on introduit le tatouage à l'espace engendré par l'amplitude de la transformée de Fourier, on obtient un espace invariant vis-à-vis d'une translation de l'image. Pour satisfaire les propriétés d'invariance par rotation et changement d'échelle, considérons la transformation Log-Polaire (LPT) définie ci-après :

$$(x, y) \mapsto \begin{cases} x = \exp\mu \ \cos\theta \\ y = \exp\mu \ \sin\theta \end{cases} \quad \text{avec } \mu \in \mathbb{R} \quad \text{et} \quad \theta \in [0, 2\pi] \tag{1}$$

Il est clair qu'une rotation du point de coordonnées (x, y) exprimées dans le repère cartésien, se traduit par une translation de θ dans le repère en coordonnées logarithmique-polaire. De même, un changement d'échelle dans le repère cartésien correspond à une translation de μ dans le repère polaire. Par un changement de repère adéquat, une rotation et un changement d'échelle sont ramenés tous deux à une translation, on peut alors utiliser la propriété d'invariance par translation de l'amplitude de la transformée de Fourier pour construire un espace invariant par rotation ou changement d'échelle de l'image originale.

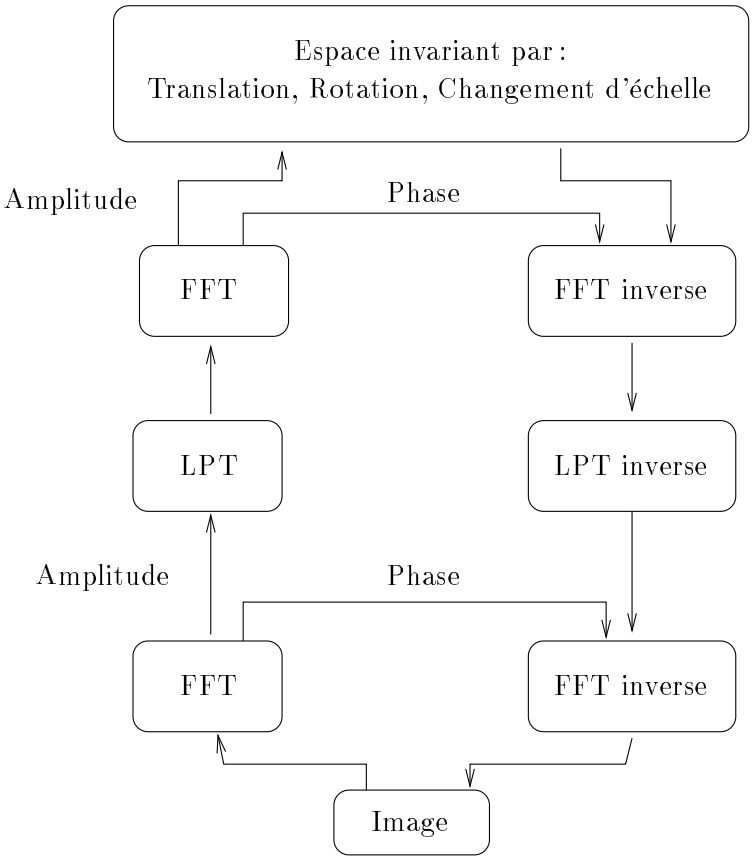


FIG. 2 – *Construction d'un espace invariant par translation, rotation et changement d'échelle*

3.3 Le domaine ondelette

Rappels sur les transformées ondelettes

Nous donnons ici quelques rappels concernant la transformation ondelette tirés du livre de M. Vetterli et J. Kovačević [91], nous insisterons plus particulièrement sur les aspects multirésolution. Pour la clarté de l'exposé nous aborderons les équations sous leur forme unidimensionnelle. L'image est décomposée en une composante passe-haut (respectivement passe-bas) à l'aide de deux filtres suivants :

$$H(\omega) = \sum_k h_k e^{-jk\omega} \qquad \text{passe-haut}$$

$$G(\omega) = \sum_k g_k e^{-jk\omega} \qquad \text{passe-bas}$$

Cette opération est réitérée sur la composante passe haut obtenue à l'étape précédente, on construit ainsi un processus pyramidal (cf. fig. 3,4) conduisant à une décomposition récursive du signal $x[n]$.

$$c_{j-1,k} = \sum_n h_{n-2k} c_{j,n}$$

$$d_{j-1,k} = \sum_n g_{n-2k} c_{j,n}$$

Pour $j = J+1, J, \ldots, J_0$ avec $c_{J+1,k} = x[k], k \in \mathbb{Z}, J+1$ est le niveau de résolution le plus élevé et J_0 est le niveau le plus bas.

Sous réserve que les deux filtres H et G soient orthogonaux, il est possible de reconstruire itérativement l'image à partir de la relation :

$$c_{j,n} = \sum_k h_{n-2k}\ c_{j-1,k} + \sum_k g_{n-2k} d_{j-1,k}$$

Application au tatouage d'image

Les transformées en ondelettes qui tout comme la transformée DCT ont fait l'objet de nombreuses études dans le contexte du codage ont également trouvé un écho dans la communauté du tatouage d'image [94, 98, 55, 99]. Cet intérêt repose d'une part sur les analyses en termes psychovisuels menées afin d'optimiser les tables de quantifications des codeurs, d'autre part sur l'aspect multi-échelle de telles transformées propice à une répartition plus robuste du tatouage. Ce gain en robustesse apporté par l'usage d'une transformée ondelette est particulièrement significatif si l'on considère les algorithmes de compression de type EZW (Embedded Zero-tree Wavelet) qui seront vraisemblablement intégrés dans la nouvelle norme de compression JPEG-2000.

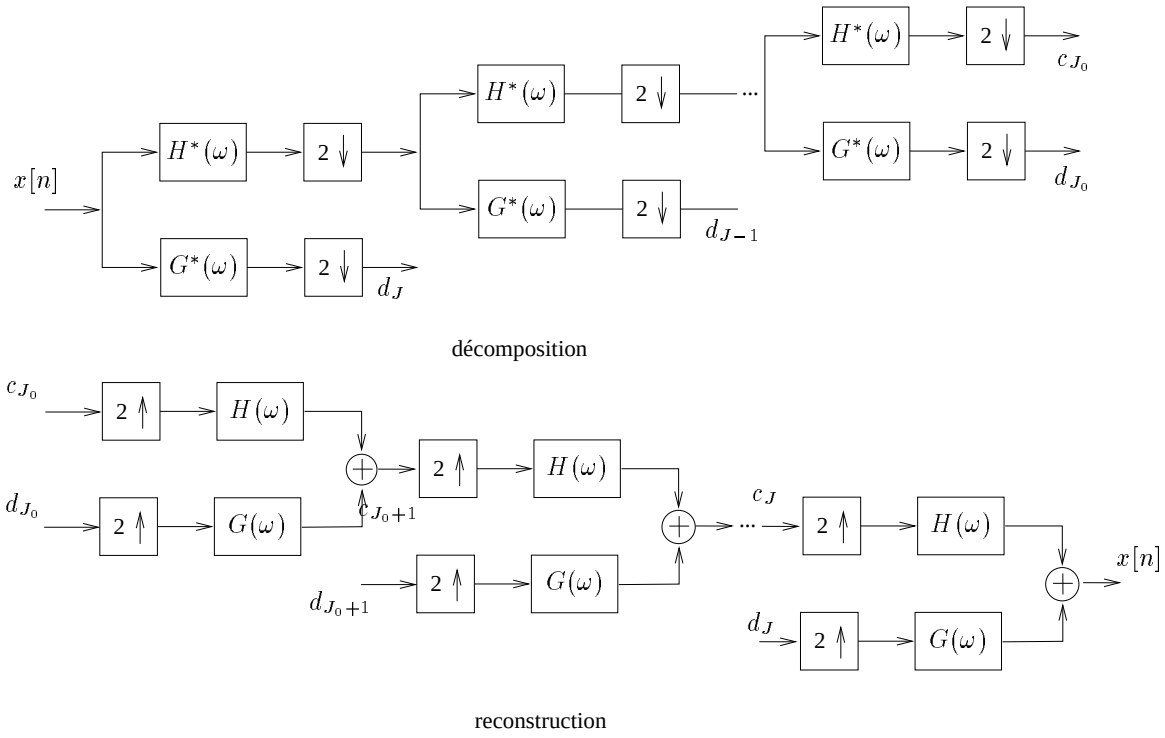


FIG. 3 – *Décomposition et reconstruction multi-échelle*

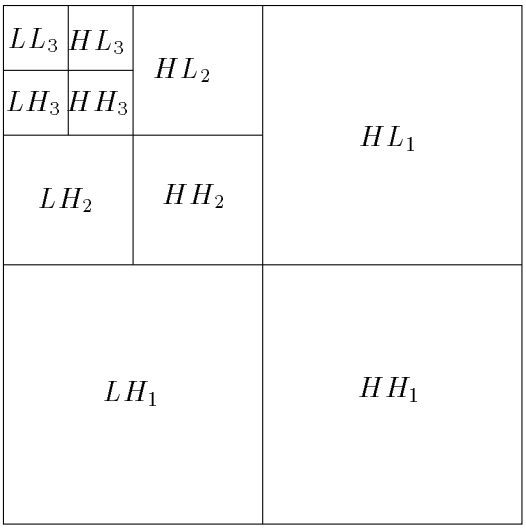


FIG. 4 – *Décomposition multi-échelle 2-D*

3.4 Décomposition de l'image en canaux perceptifs

L'évaluation de la qualité des images est une préoccupation constante des systèmes de traitements d'image ; elle est par exemple cruciale dans les techniques de compressions avec pertes. Les modèles psychovisuels introduits pour évaluer cette qualité considèrent généralement le système visuel humain comme un ensemble de canaux [95, 96, 17] par lesquels sont transmis différents types d'information au cerveau. Les techniques de tatouage d'image, dans le but d'améliorer l'invisibilité du tatouage ont cherché à utiliser ces travaux et en particulier les effets de masquages [3]. Delaigle *et al.* [16, 18] de l'Université Catholique de Louvain ont développé un modèle perceptif permettant d'évaluer analytiquement la visibilité ou l'invisibilité d'une marque afin de pouvoir éventuellement rétroagir sur l'algorithme de tatouage. L'algorithme de l'UCL réalise une décomposition de l'image originale en canaux. La détermination de chaque canal est faite sur la base de caractéristiques fréquentielles (module et phase) ainsi que de la localisation dans le champ de vision. Toute la difficulté consiste à identifier des canaux en adéquation avec les critères perceptifs humains. L'hypothèse sous-jacente consiste à admettre que tout signal ayant des composantes proches de celles d'un canal ne pourra être distingué de celui-ci par l'oeil humain. Dans le modèle retenu par l'UCL, on dispose de 21 canaux définis sur la base de 5 fréquences et de 4 orientations [37]. Ce modèle a fait l'objet d'un test sur des données vidéo par la société Thomson-CSF, nous renvoyons au rapport [45] pour les détails de son évaluation. Notons simplement que ce modèle ne tient pas compte intrinsèquement de la continuité temporelle présente dans les données vidéo.

Remarque

Les modèles de masquage sont très utilisés dans le cadre des traitements audio [87, 3] et donnent de très bons résultats, néanmoins il existe une différence fondamentale entre les données audio et image : dans le cas de l'audio, l'observateur a une position fixe par rapport à la source alors que pour les images, l'observateur est libre de parcourir l'image selon n'importe quel « chemin » ; de plus ce chemin peut varier en fonction de l'observateur etc, il apparaît donc très difficile de tenir compte de ces paramètres pourtant prépondérants.

4 Ajout de redondance à la signature initiale

La taille des signatures nécessaires à identifier sans ambiguïté un individu sont de l'ordre de quelques octets, or une image et a fortiori une vidéo constituent un volume d'information binaire bien supérieur. Il est donc légitime d'ajouter de la redondance à la signature originale afin d'accroître la robustesse du tatouage face à des manipulations de l'image. Ce type de solutions consistant à augmenter la redondance d'un message afin de le rendre plus robuste à des erreurs de transmission a été et est largement étudié dans le domaine des communications numériques. Les solutions proposées ci-après s'en sont d'ailleurs très largement inspirées.

4.1 Etalement de spectre

Très tôt, les techniques d'étalement de spectre sont apparues comme des techniques privilégiées dans les systèmes de tatouage [90, 10, 85, 40]. Bien que quelques restrictions soient apparues à leur encontre [42, 35], ces techniques continuent d'être une pièce maîtresse de nombreux systèmes [66].

Idées motivant l'utilisation de l'étalement de spectre pour le tatouage d'image

1. La marque que l'on souhaite dissimuler dans l'image présente une bande passante très étroite relativement à la bande passante de l'image ;

2. Les fréquences de l'image psychovisuellement non significatives (très hautes fréquences) ne peuvent être utilisées pour dissimuler le tatouage car il ne présenterait pratiquement aucune robustesse vis-à-vis d'un filtrage passe bas qui ne dégraderait pourtant pas significativement l'image ;

3. Malheureusement, les fréquences susceptibles de présenter une plus grande robustesse vis-à-vis d'attaques ont également un impact visuel majeur et une modification significative de ces fréquences entraînerait une dégradation inacceptable de l'image.

Les deux derniers points constituent le compromis robustesse *vs.* visibilité que l'on rencontre dans la plupart des systèmes proposés.

Notions sur l'étalement de spectre

Les techniques d'étalement de spectre ont été introduites pour résoudre les problèmes de communications sur des canaux bruités entre plusieurs utilisateurs [73]. En complément du gain en robustesse que procurent ces techniques vis-à-vis des imperfections du canal de transmission, elles permettent d'assurer la confidentialité entre les différentes communications circulant sur le même canal de transmission.

Etalement par séquence directe : Cette technique réalise l'étalement directement dans le domaine temporel (ou spatial). Un signal à bande étroite S peut être étalé spectralement par modulation à l'aide d'un signal à large spectre PN (s'apparentant à un bruit blanc). Cette modulation confère au signal résultant S_e les caractéristiques spectrales de PN. Si le canal de transmission présente un évanouissement dans la bande étroite où se situe le signal à transmettre S, la technique d'étalement permettra d'assurer une bonne transmission de ce signal. La connaissance du signal PN permet de démoduler le signal S_e et de reconstruire le signal S comme l'illustre la figure 5.

Etalement par saut de fréquence (frequency hopping) : Le principe consiste à moduler le signal original par une porteuse dont la fréquence varie de façon aléatoire. Le signal résultant est ainsi réparti dans l'ensemble de la gamme de fréquence où est choisie la porteuse. Cette technique permet également d'assurer un cryptage du

FIG. 5 – *Principe d'étalement de spectre par séquence directe*

message. En effet, la démodulation du signal nécessite la connaissance de la porteuse utilisée pour moduler le signal or celle-ci est aléatoire puisque sa fréquence dépend d'une clé secrète. Seule la personne disposant de cette clé est en mesure de démoduler le signal.

Exemple pratique d'étalement de spectre par séquence directe

A partir d'un signal binaire $a_j, a_j \in \{-1, 1\}$, il est créé un signal dérivé w_i qui constitue le signal introduit dans la séquence vidéo originale v_i afin de constituer la séquence vidéo tatouée $\hat{v}_i$. La construction de w_i s'attache à garantir que le signal binaire original a_j puisse être extrait de la séquence $\hat{v}_i$ même si celle-ci a subi des manipulations. Cette robustesse de a_j est obtenue en appliquant des techniques basées sur l'étalement de spectre. De manière pratique, le signal binaire original est tout d'abord étalé par un facteur cr appelé période d'étalement (chip rate) afin d'obtenir la séquence étalée b_i.

$$b_i = a_j, j\ cr \leq i < (j+1)\ cr$$

La séquence étalée est alors amplifiée puis modulée par un signal aléatoire présentant un large spectre afin d'obtenir le tatouage directement introduisible dans l'image :

$$w_i = \alpha \times b_i \times p_i$$

Les deux signaux v_i et w_i sont mélangés par simple addition pixels à pixels.

$$\hat{v}_i = v_i + \alpha\ b_i\ p_i$$

Les auteurs [39, 40] prétendent que cette modification de v_i ne devrait pas entraîner de dégradation notable de l'image car la marque ajoutée présente des caractéristiques similaires au bruit naturel de l'image et devrait ainsi se confondre avec celui-ci. La parenté de la marque à un bruit découle directement de l'opération de modulation par un signal aléatoire p_i. En outre, le choix d'un facteur d'amplification α réduit contribue à maintenir le niveau d'énergie de la marque en dessous du seuil de visibilité. La récupération de la séquence binaire a_j est réalisée à partir de la séquence vidéo signée $\hat{v}_i$ par démodulation de la marque et reconcentration de l'énergie du signal démodulé. Pour démoduler le signal, il est bien évident que le récepteur dispose de la séquence aléatoire p_i.

$$s_j = \sum_{i=j\ cr}^{(j+1)\ cr-1} p_i\ \hat{v}_i\ = \sum_{i=j\ cr}^{(j+1)\ cr-1} p_i\ v_i + \sum_{i=j\ cr}^{(j+1)\ cr-1} p_i^2\ \alpha\ b_i$$

Sous les hypothèses que p_i soit à moyenne nulle et statistiquement indépendant de la séquence v_i, l'équation précédente se simplifie et l'on obtient :

$$s_j = cr\ \alpha b_i = cr\ \alpha a_j$$

Les valeurs des bits du signal binaire sont ainsi données par :

$$a_j = sign(s_j)$$

Remarque

Le facteur d'amplification α a été choisi constant et indépendant de l'indice i, néanmoins les auteurs suggèrent qu'il est possible d'améliorer le schéma en rendant ce facteur dépendant des caractéristiques locales de l'image. Ceci offre ainsi l'opportunité d'introduire des considérations liées au système visuel humain (HSV).

4.2 Codes correcteurs

De nombreux articles [15, 14, 44, 16] font référence à une utilisation potentielle de codes correcteurs d'erreurs afin d'augmenter les performances en termes de robustesse de tels ou tels algorithmes de tatouage. L'emploi de tels codes apparaît en effet naturel si l'on examine le problème de la robustesse du tatouage sous l'angle de la communication d'un signal sur un canal bruité (cf. § 4.1 Chap. 2). Cependant, les travaux actuellement publiés proposant par exemple l'emploi de codes BCH et Reed-Muller ne démontrent pas totalement la pertinence de faire usage de tels codes. Nous attribuons cet échec relatif à plusieurs facteurs.

- Contrairement aux applications habituelles du codage canal où l'hypothèse d'une perturbation de type bruit blanc gaussien est très souvent valide, le contexte du tatouage d'image n'apparaît pas favorable à admettre une telle hypothèse. La nature des perturbations est tellement diverse (cf. § 2 Chap. 2) et par conséquent leurs modélisations délicates qu'il est difficile de concevoir un unique code qui soit efficace simultanément pour toutes ces attaques.

- Le support du tatouage est borné, spécialement si l'on considère des images. Il est donc souvent impossible d'étendre le volume initial des données constitutives du tatouage afin d'y adjoindre un code correcteur sans pour autant dégrader les performances initiales de l'algorithme de tatouage. Cette situation est sensiblement différente pour la vidéo et l'audio dans la mesure où nous avons alors la possibilité d'étendre la présence du tatouage sur les trames ou les échantillons suivants. On perçoit bien ici le rôle important joué par le rapport entre le volume d'information du tatouage et des données support à traiter.

L'usage des codes correcteurs pour le tatouage d'image est donc encore un problème ouvert, requérant la conception de codes compacts capables de prendre en compte la diversité des attaques.

5 Fusion des données : signature et image

Le double objectif est de minimiser l'impact visuel du tatouage et de maximiser la robustesse de celui-ci.

5.1 Modulation de phase

La transformée de Fourier d'une image réelle est généralement de nature complexe ; elle possède donc un module et une phase. Des études expérimentales ont montré que l'in-

formation contenue dans la phase était prépondérante sur celle contenue dans l'amplitude dans la représentation d'une image. Cette constatation conduit les auteurs à introduire le tatouage au niveau de la phase pour, d'une part s'assurer qu'une tentative de suppression du tatouage engendrera inévitablement des dégradations importantes dans l'image, d'autre part utiliser les techniques de modulations de phase qui sont reconnues plus robustes au bruit qu'une modulation d'amplitude[4]. Un tel système privilégie donc a priori l'aspect robustesse sur l'aspect visibilité.

5.2 Modulation d'amplitude

Dans l'article [58], il est proposé de réaliser l'insertion de la signature par une modulation d'amplitude de la composante bleue d'une image couleur (RGB). Le choix de la composante bleue est motivé selon les auteurs par une moindre sensibilité de l'oeil humain dans les longueurs d'onde proches du bleu. Considérons une image $I = R, G, B$, $p = (i, j)$ une position aléatoire dans cette image et s le bit que l'on souhaite tatouer. La modulation de la composante B afin d'obtenir la composante signée $\tilde{B}$ est réalisée suivant la formule ci-après :

$$\tilde{B}_{ij} \leftarrow B_{ij} + (2s - 1)L_{ij}q$$

où $L = 0.299R + 0.587G + 0.114B$ désigne la luminance ; q est une constante qui détermine l'amplitude de la modulation, plus q a une valeur élevée, plus le tatouage est robuste, malheureusement, celui-ci est également plus visible. Le point clé de ce type de modulation réside donc dans le choix adéquat du paramètre q pour satisfaire le compromis robustesse/visibilité. La restitution du bit s se fait sur la base d'une prédiction linéaire. Cette prédiction permet d'estimer la valeur initiale de la composante B avant tatouage :

$$\hat{B} = \frac{1}{4c}(\sum_{k=-c}^{k=c} B_{i+k,j} + \sum_{k=-c}^{k=c} B_{i,j+k} - 2B_{i,j})$$

On obtient alors la valeur du bit s en regardant le signe de δ :

$$\delta = \tilde{B}_{i,j} - \hat{B}_{i,j}$$

Il est important de noter que cette technique de démodulation ne nécessite pas l'image originale.

Dans l'article [98], Xia *et al.* proposent de moduler l'amplitude du signal de signature en fonction de l'énergie des coefficients de la transformée ondelette $y[m, n]$ voir paragraphe 3.3. Mathématiquement, la formule d'insertion présente la forme suivante :

$$\tilde{y}[m, n] = y[m, n] + \alpha y^2[m, n]N[m, n]$$

où N est un bruit de moyenne nulle et de variance un ; α est une constante offrant la possibilité de régler le compromis robustesse, visibilité. Les auteurs préconisent d'exclure les coefficients basses résolutions de cette formule d'insertion, ceci se justifie par le fait

4. Notons que cette approche est en contradiction avec celle proposée au paragraphe 3.2

qu'une modification de ces coefficients entraînerait des effets de plages désastreux, l'oeil étant très sensible dans les composantes uniformes (basse résolution). A contrario, les composantes de plus hautes résolutions associées aux contours et aux zones texturées, sont favorables d'un point de vue psychovisuel à recevoir la signature mais sont moins robustes. La superposition à l'image de la signature est d'autant moins perçue que les contrastes ou les textures sont marqués, ce qui correspond à de fortes valeurs d'énergie ($y^2[m,n]$).

5.3 Fusion préservant la luminosité moyenne : algorithme rsppmc

Cette méthode proposée dans [6] par O. Bruyndonckx *et al.*, repose sur la classification de l'image en régions homogènes. L'algorithme d'insertion du tatouage binaire procède comme suit.

Insertion

1. Choix des blocs constituant le support de l'information de tatouage. Ce choix est effectué via une clé secrète initialisant un générateur aléatoire.

2. Classification des pixels de chaque bloc comme appartenant soit à une région à fort contraste soit à une région à variation de contraste progressif. On définit ainsi pour chaque bloc deux régions : R_1 et R_2 pour lesquelles on calcule la luminance moyenne m_1 et m_2.

3. Subdivision de R_1 et R_2 en zones labellisées A ou B selon une grille prédéfinie. On définit ainsi les sous régions : R_{1A}, R_{1B}, R_{2A} et R_{2B} comprenant respectivement n_{1A}, n_{1B}, n_{2A} et n_{2B} pixels dont la luminance moyenne est respectivement : m_{1A}, m_{1B}, m_{2A} et m_{2B}.

4. Soit b le bit du tatouage à introduire dans un bloc donné. L'opération de fusion est définie par la règle suivante ; $\begin{array}{lrcl} \text{if } b=0 & \tilde{m}_{1A}-\tilde{m}_{1B} & = & -l \\ & \tilde{m}_{2A}-\tilde{m}_{2B} & = & -l \\ \text{if } b=1 & \tilde{m}_{1A}-\tilde{m}_{1B} & = & l \\ & \tilde{m}_{2A}-\tilde{m}_{2B} & = & l \end{array}$ où l désigne l'intensité avec laquelle on tatoue l'image.

   La conservation de la luminance moyenne des régions R_1 et R_2 induit :

$$\begin{aligned} \frac{n_{1A}\times\tilde{m}_{1A}+n_{1B}\times\tilde{m}_{1B}}{n_{1A}+n_{1B}} &= m_1 \\ \frac{n_{2A}\times\tilde{m}_{2A}+n_{2B}\times\tilde{m}_{2B}}{n_{2A}+n_{2B}} &= m_2 \end{aligned}$$

Les six dernières équations permettent de déterminer les valeurs de $\tilde{m}_{1A}$, $\tilde{m}_{1B}$, $\tilde{m}_{2A}$ et $\tilde{m}_{2B}$ suivant la valeur du bit b du tatouage à dissimuler. Chaque pixel appartenant à une même région se voit modifier par ajout d'un « offset » calculé comme suit :

$$\delta_{ij} = \tilde{m}_{ij} - m_{ij}$$

où $i = 1, 2$ et $j = A, B$

Extraction L'algorithme d'extraction reprend les phases 1, 2 et 3 définies lors de l'insertion, et rajoute la phase de décision ci-dessous :
on calcule $\sigma_1 = \hat{m}_{1A} - \hat{m}_{1B}$ et $\sigma_2 = \hat{m}_{2A} - \hat{m}_{2B}$

Le signe de σ_1 et σ_2 permet de déduire la valeur du bit b. L'amplitude de σ_1 et σ_2 donne une indication sur le degré de certitude avec lequel on récupère la valeur du bit b. Dans le cadre d'une application de type protection du copyright, la quantité d'information nécessaire à l'identification d'un individu est de l'ordre de quelques dizaines de bits, l'algorithme proposé permet donc d'ajouter beaucoup de redondance. Cet algorithme est de plus propice à la mise en place d'une fonction coût, inversement proportionnelle au degré de certitude avec lequel on récupère chaque bit.

5.4 Ajout du tatouage par quantification des coefficients DCT

Modification de la fonction d'arrondi

Dans l'une de leurs méthodes, Matsui et Tanaka [62] proposent d'introduire la signature binaire lors de l'étape de quantification des coefficients fréquentiels (DCT). Plus précisément, ils modifient la définition de la fonction d'arrondi. Par rapport à la fonction classiquement utilisée dans un codeur JPEG, on ne considère plus l'entier le plus proche mais l'entier pair le plus proche lorsque l'on désire introduire un bit de signature à 1 et l'entier impair le plus proche dans le cas d'un bit de signature à 0. L'erreur de quantification ainsi créée est donc directement corrélée avec la signature. Les auteurs admettent que la dégradation engendrée par cette erreur est suffisamment faible pour ne pas entraîner de gêne visuelle. Si tel n'est pas le cas, il est possible de réduire le pas de quantification des tables de coefficients DCT pour se positionner à un niveau de dégradation acceptable. Malheureusement, cette opération conduit parallèlement à une moindre résistance du tatouage. Le pas de quantification fournit donc un paramètre de réglage du compromis robustesse visibilité.

Définition d'une relation d'ordre entre N-uplet de coefficients

La technique exposée précédemment introduit un bit de tatouage au niveau de chaque coefficient DCT en ne tenant pas compte des coefficients voisins. Koch et Zhao [53, 100] ont cherché à rétablir une notion de voisinage en proposant une modulation différentielle des coefficients DCT.
Soit $N(k_1, l_1, k_2, l_2) = |Y_Q(k_1, l_1)| - |Y_Q(k_2, l_2)|$ le signal différentiel formé à partir des coefficients DCT quantifiés Y_Q associés aux fréquences spatiales horizontales et verticales k_1, l_1, (respectivement k_2, l_2) de l'image. Le tatouage T est introduit en imposant les contraintes :

$$T = 1 \quad \Longrightarrow \quad N(k_1, l_1, k_2, l_2) > 0$$

$$T = 0 \quad \Longrightarrow \quad N(k_1, l_1, k_2, l_2) < 0$$

La conformité de N avec la valeur du bit de T est obtenue en forçant si nécessaire le signe de N. Cette opération nécessite la modification des coefficients $Y_Q(k_1, l_1)$ et $Y_Q(k_2, l_2)$ génèrant bien entendu une erreur, cependant celle-ci est répartie sur deux coefficients contrairement à la méthode proposée au paragraphe précédent. On peut faire une analogie de ces deux méthodes avec une quantification scalaire *vs.* vectorielle. Cette analogie est d'autant plus marquée que la modulation différentielle initialement proposée par Zaho et Koch peut être étendue en considérant des triplets ou des quadruplets de coefficients DCT.

Apportons à présent quelques remarques sur les caractéristiques du signal N. Au niveau local ($k_1 \approx k_2$ et $l_1 \approx l_2$), N présente une moyenne nulle et une variance faible ; à un niveau global, N se caractérise par des non-stationnarités apparaissant lors des changements de régions matérialisés par des contours. La moyenne nulle du signal N pour des valeurs de fréquences proches garantit l'équi-probabilité quant à la possibilité d'insérer le symbole 0 ou 1. Les hypothèses sur le signal N (non-stationnarité à long terme, moyenne nulle et variance faible à court terme) sont d'autant mieux vérifiées si l'on se place au niveau des fréquences intermédiaires. De plus, ces fréquences présentent le double avantage de ne pas être trop sensibles à un filtrage de type passe bas qui constitue une première approximation de la compression JPEG, et de présenter un faible impact psychovisuel si elles sont légèrement modifiées, en raison de la faible variance de N.

Superposition des coefficients DCT de l'image et du tatouage

Cette technique inspirée des méthodes stéganographiques [49, 50] est particulièrement indiquée lorsque le tatouage est de même nature que les données à tatouer. Autrement dit, dans le cadre des images, si le tatouage est lui-même une image, il peut s'agir par exemple d'un logo.

5.5 Ajout du tatouage par substitution de blocs : codage fractal

La plupart des méthodes de tatouage introduisent la signature dans l'image par le biais d'une perturbation de la quantification de certaines grandeurs caractéristiques de l'image. Cette perturbation est fonction de la valeur du bit de la signature désirant être introduit. Les approches précédemment exposées basées sur la quantification de certains coefficients DCT de l'image en sont un bon exemple. Les effets visuels résultant des perturbations de la quantification initiale sont parfois difficilement maîtrisables. Le laboratoire de Traitement des Signaux de l'EPFL propose une nouvelle approche de ce problème reposant sur le codage fractal [76]. Nous avons vu que le codage fractal est basé sur la définition d'une association entre différentes régions de l'image. Cette association est réalisée selon un critère d'auto-similitude fondé sur la minimisation de l'erreur quadratique entre les blocs cibles et les blocs sources transformés (cf. § 3 Chap. 1). Pour un bloc cible donné, la recherche du bloc source associé s'effectue dans une fenêtre de recherche centrée sur le bloc cible. La méthode de tatouage proposée modifie cette recherche en définissant deux sous fenêtres comme il apparaît dans la figure 6. L'insertion de la signature consiste à :

- tirer aléatoirement $N = r \times L$ blocs cibles dans l'image. L est le nombre de bits de la signature et r le coefficient de redondance pour chacun de ces bits ;

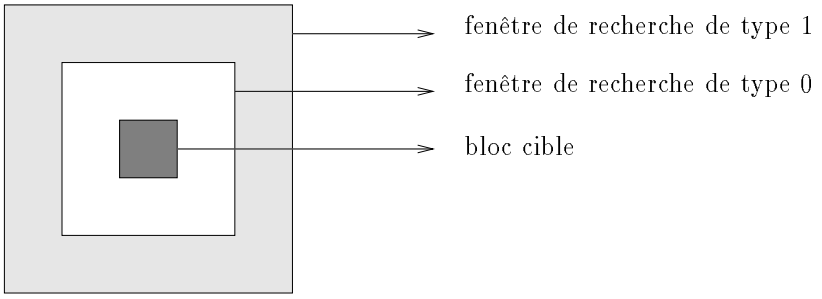


FIG. 6 – *Bloc cible et les deux sous fenêtres de recherche associées*

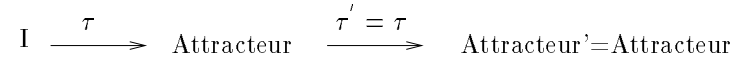


FIG. 7 – *Invariance d'un attracteur et de sa transformée associée*

- pour chacun des N blocs cibles, effectuer la recherche du bloc source associé dans la fenêtre de recherche de type 0 (respectivement de type 1) si le bit associé de la signature à pour valeur 0 (respectivement 1) ;
- pour chacun des blocs cibles non précédemment traités, la recherche du bloc source s'effectue sans contrainte sur la fenêtre de recherche. En d'autres termes, la recherche est effectuée dans la fenêtre constituée par l'union des fenêtres de type 0 et 1 ;
- à partir du code ifs obtenu lors des deux précédentes étapes, effectuer le processus de décodage standard aux techniques de codage fractal afin d'obtenir l'attracteur qui constitue l'image signée.

L'extraction de la signature procède de manière duale à l'insertion.

- Grâce à une clé secrète on régénère le signal aléatoire donnant accès aux N blocs cibles potentiellement porteurs de la signature ;
- Pour chacun des blocs cibles on fait une recherche du bloc source associé par minimisation de l'erreur quadratique (procédé habituel du codage fractal). Cette recherche s'effectue dans la région définie par l'union des fenêtres 0 et 1 ;
- La décision sur la valeur du bit extrait se prend en fonction de la région d'appartenance du bloc source. Si le bloc source appartient à la fenêtre 0 le bit associé est considéré comme valant 0, sinon le bit prend la valeur 1.

L'algorithme d'extraction utilise la propriété clé du codage fractal selon laquelle un attracteur est un invariant, ce qui signifie qu'il est codé sans erreur et que la transformée identifiée pour le coder reste inchangée (cf. fig. 7).

L'application directe de cette propriété à notre problème est à relativiser dans la mesure où l'image signée est potentiellement sujette à des manipulations de type compression par exemple, dès lors, on ne dispose plus rigoureusement de l'attracteur au moment de l'extraction de la signature.

6 Techniques visant à accroître les performances de restitution de la signature lors de la phase d'extraction

L'extraction de la signature est composée d'opérations duales de l'insertion, auxquelles il faut ajouter diverses techniques propres à la phase d'extraction visant à accroître la robustesse du tatouage. Cette partie est dédiée à ces dispositifs.

6.1 Préfiltrage de l'image et blanchiment de l'image

Usuellement, le tatouage introduit dans l'image possède certaines propriétés statistiques. Pour un tatouage binaire, la répartition des bits à « 0 » et à « 1 » est par exemple généralement équiprobable. Dans le cadre de la technique d'étalement de spectre exposée au paragraphe 4.1, F. Hartung propose de moyenner l'image tatouée avant de procéder à l'extraction du tatouage proprement dit, afin de mieux vérifier l'hypothèse initiale :

$$\sum_{i=j\ cr}^{(j+1)\ cr-1} p_i = 0$$

Suivant une démarche similaire, M. Kutter [57] suggère, pour les techniques basées sur une modulation d'amplitude, de filtrer l'image tatouée par convolution avec le masque ci-dessous.

$$h = \frac{1}{12}\begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

Ce filtrage a pour effet de rapprocher le signal reçu le plus possible d'une courbe gaussienne à moyenne nulle et à variance faible, ce type de courbe étant plus propice à la prise de décision. Des informations complémentaires concernant le préfiltrage de l'image en vue d'augmenter les performances du détecteur de tatouage peuvent être obtenues dans l'article de Kalker [51].

6.2 Seuillage adaptatif

De nombreuses méthodes utilisent des seuils afin de décider de la valeur des bits reçus. Ce choix peut s'avérer déterminant pour la bonne réception de la signature or il est clair que des modifications de l'image signée peuvent entraîner un déplacement de la valeur optimale de ce seuil définie lors de l'insertion de la signature. L'article [58] dont nous avons extrait la figure 8 propose d'introduire des bits de tests en complément des bits de signature. Ces bits dont les valeurs sont prédéfinies constituent ainsi une référence et sont utilisés pour estimer le seuil optimal lors de la réception.

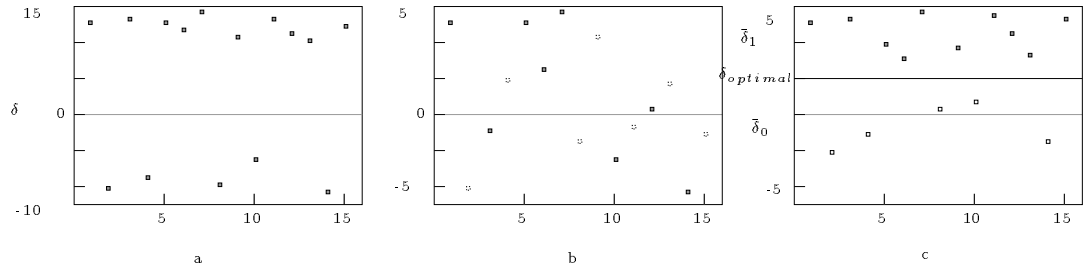


FIG. 8 – *Seuillage adaptatif: a) sans attaque, le seuil de décision est idéalement placé en 0. b) confusion entre les amplitudes associées aux bits 1 et celles associées à 0. c) seuil de décision adaptif optimal calculé à partir des bits de test.*

Il est clair que la modulation d'amplitude utilisée par cette méthode et décrite au paragraphe 5.2 conduit à un seuil optimal de décision initialement égal à 0. L'algorithme peut être jugé irrémédiablement défaillant lorsque les amplitudes associées aux bits à 1 sont enchevêtrées avec celles associées aux bits à 0, dans le cas contraire, on peut espérer prendre une décision exacte à condition de ré-estimer le seuil de décision. Le nouveau seuil optimal est calculé en considérant l'amplitude moyenne des bits tests à 1 noté $\bar{\delta}_1$ et l'amplitude moyenne des bits tests à 0 noté $\bar{\delta}_0$. On commet statistiquement le moins d'erreur en choisissant :

$$\delta_{optimale} = \frac{\bar{\delta}_1 + \bar{\delta}_0}{2}$$

6.3 Estimation et compensation d'attaques géométriques sans image originale

Les manipulations géométriques sur les images signées font partie des attaques les plus sévères sur lesquelles butent de nombreux algorithmes, en particulier lorsque l'on impose la récupération de la signature sans l'aide de l'image originale. L'article [58] tire parti des bits de tests introduits pour déterminer le niveau de seuillage optimal afin d'estimer la transformation inverse de celle qu'a probablement subie l'image. En effet, l'écart entre les amplitudes moyennes $\bar{\delta}_1$ et $\bar{\delta}_0$ donne une idée sur la confiance avec laquelle on va réaliser l'extraction des bits de la signature. Plus cet écart est faible plus l'ambiguïté sur la récupération des bits est importante. On peut penser que si l'image subie une transformation géométrique, cette ambiguïté sera maximale. Soit G la transformation géométrique subit par l'image signée I et H la transformation à identifier que l'on espère le plus proche possible de G^{-1}. Soit J l'image I à laquelle on a appliqué la transformation G et I_H l'image J à laquelle on a appliqué la transformation H. On construit le critère :

$$q(H) = \bar{\delta}_1 - \bar{\delta}_0$$

Cette fonction est maximale si $H = G^{-1}$. Malheureusement, elle n'est pas régulière ce qui ne permet pas la mise en place d'algorithme à descente de gradient afin d'identifier la transformation H. L'optimisation du critère q passe donc par une recherche exhaustive

et nécessite que l'on fasse décrire à H l'ensemble des transformations possibles. Ceci n'est bien évidemment pas très réaliste et l'on doit se limiter à un nombre réduit de transformations. Les auteurs ont appliqué cette méthode afin d'estimer une rotation de l'image et obtiennent de bons résultats en considérant l'ensemble des rotations de 0 à 360 degrés avec un incrément de 5 degrés.

Nous remarquons qu'étant donné l'étendue de l'ensemble des transformations H possibles, cette méthode peut difficilement être appliquée en dehors de transformations globales de l'image.

6.4 Test d'hypothèses

Les tests d'hypothèses font partie des outils usuels dans le cadre de problèmes où une prise de décision intervient [68, 43]. Le tatouage d'image appartient à cette famille de problèmes, particulièrement lorsque le tatouage inséré est connu et qu'il s'agit de vérifier sa présence dans telle ou telle image. On est alors naturellement conduit à formuler les deux hypothèses suivantes :

H1) Le tatouage T est présent dans l'image I.
H2) Le tatouage T n'est pas contenu dans l'image I.

auxquelles on associe les deux types d'erreurs :

Type I : Affirmer la présence du tatouage dans l'image alors qu'il n'y a jamais figuré (erreur favorable au pseudo propriétaire).
Type II : Rejeter la présence du tatouage dans l'image bien qu'il y soit dissimulé (erreur bénéficiant au client).

Classiquement, le problème de décision conduit à un arbitrage entre ces deux types d'erreurs. Il est clair que pour des applications visant à prouver le copyright d'une image, les erreurs de type I doivent être fortement minimisées dans le souci de ne pas favoriser l'entité à l'origine de la demande du service (i.e. le propriétaire). Il s'agit ici de respecter le principe de présomption d'innocence.

Suivant ce modèle, I. Pitas et T. H. Kaskalis proposent dans [75] un raffinement de la méthode du patchwork présentée au paragraphe 2.1 en incluant un test statistique pour discerner le cas $S = 2 \times n$ (présence du tatouage) du cas $S = 0$ (absence du tatouage).

D'autres types de tests sont envisagés [44], notamment si l'on considère l'ensemble des tatouages originaux connus. Un score de corrélation peut alors être calculé entre le tatouage extrait et l'ensemble des tatouages originaux. La distribution des coefficients de corrélation doit présenter un pic plus ou moins marqué correspondant au tatouage effectivement présent dans l'image. L'allure de la distribution reflète le degré de certitude de l'extraction et est propice à une décision basée sur un test d'hypothèses.

7 Adaptation des algorithmes proposés en image fixe aux séquences vidéo

7.1 Les nouvelles contraintes

Le tatouage de séquences vidéo amène de nouvelles contraintes en termes de : stratégie de tatouage, volume d'information traitée, critères psychovisuels, attaques à envisager.

En ce qui concerne la stratégie de tatouage, on doit déterminer s'il est souhaitable de protéger chacune des trames qui sont alors appréhendées comme des images fixes ou bien si l'on peut se contenter de protéger la vidéo dans sa globalité.

Repositionnons le problème de la vidéo dans le cadre général du tatouage en considérant les trois points fondamentaux que sont : la visibilité, la robustesse et la capacité d'insertion.

Les problèmes de visibilité en vidéo sont sensiblement différents de ceux rencontrés en image fixe. La dimension temporelle est caractérisée par une forte continuité liée généralement à la présence importante de fonds statiques dans la scène, à l'exception des trames matérialisant un changement de plan. Cette continuité ne doit pas être brisée par la superposition du tatouage. En outre, la notion de régions d'intérêts prend tout son sens en vidéo. Une personne visionnant une image fixe fait généralement une lecture à plusieurs niveaux, elle est d'abord captée par une région d'intérêt puis elle s'éloigne de cette région et peut faire une analyse détaillée de l'image, la situation est tout autre en vidéo puisque le regard est contraint par le déroulement de la scène, il ne peut s'attarder sur une région spécifique dans une même trame. La différenciation entre les régions d'intérêts et les autres régions est donc plus marquée en vidéo.

Les contraintes de robustesse du tatouage se trouvent modifiées par l'existence de nouvelles manipulations autorisées par le nouveau degré de liberté constitué par la dimension temporelle. On peut par exemple imaginer que la suppression d'une trame est relativement peu pénalisante visuellement bien qu'elle pose d'importants problèmes de resynchronisation lors de l'extraction du tatouage. Parmi les autres transformations susceptibles de poser des problèmes à l'extraction du tatouage, on mentionnera : le moyennage entre deux ou plusieurs trames successives, l'inversion entre deux trames présentant peu d'activité temporelle, la compression MPEG et la notion de trame prédite.

Au niveau de la capacité d'insertion la situation semble plus favorable pour la vidéo. En effet, le rapport (taille du support / taille du tatouage) est beaucoup plus élevé dans le cas d'une vidéo que dans celui d'une image fixe puisque l'on dispose de plus de données support.

Nous soulevons un dernier point quant aux spécificités liées au tatouage de la vidéo, il s'agit du coût calculatoire des opérations de tatouage. Le temps réel est une notion plus fréquente en vidéo qu'en image fixe, cependant peu d'études se sont portées sur ce sujet dans le contexte du tatouage de la vidéo.

7.2 Système de tatouage utilisant un modèle perceptif dédié à la vidéo

Le modèle perceptif doit être en mesure de déterminer les régions d'une image pour lesquelles l'acuité visuelle humaine est faible, ces régions étant les mieux adaptées à recevoir le tatouage. L'originalité de la méthode développée dans [87] par Swanson *et al.* réside dans la définition de trois types de masquage. Les deux premiers : masquage spatial et masquage fréquentiel sont analogues à ceux développés en image fixe [3], le troisième type de masquage prend en compte l'activité temporelle de la vidéo. Par exemple, des discontinuités dans le mouvement peuvent être notamment très pénalisantes pour la qualité de la vidéo et on cherchera par conséquent à les minimiser.

Les auteurs posent la question : est-il plus judicieux de traiter indépendamment chaque trame de la vidéo ou bien est-il préférable de déposer le même tatouage dans plusieurs trames successives ? Les avantages et les inconvénients de cette alternative sont les suivants : introduire un tatouage identique dans plusieurs trames successives entraîne une difficulté supplémentaire pour assurer l'invisibilité du tatouage. En effet, il est par exemple reconnu que les régions de contours sont appropriées à recevoir un tatouage de forte amplitude du fait de la relative faiblesse du système visuel humain dans ce type de région or, dans une région en mouvement, les contours se déplacent et il est donc très difficile d'exploiter ces régions au maximum de leur capacité sans risquer de rendre le tatouage visible. La seconde alternative consistant à fabriquer un tatouage différent pour des trames consécutives peut créer une faille de sécurité importante. En effet, dans une vidéo, de nombreuses régions restent plus ou moins invariantes au cours du temps (fonds), un utilisateur malveillant est susceptible, soit de faire une étude statistique pour plusieurs trames contiguës, soit de remplacer les régions quasi fixes de ces trames par une moyenne entre celles-ci. Il aura alors potentiellement supprimé le tatouage sans nuire à la qualité de la vidéo. Les auteurs ont ainsi mis en évidence la nécessité d'utiliser un tatouage composite, les deux composantes correspondant respectivement aux régions à fortes et à faibles variations temporelles. Pour déterminer ces régions, les auteurs ont recours à une décomposition des trames successives en ondelettes temporelles.

8 Critiques et faiblesses inhérentes aux approches de type tatouage

8.1 Les faiblesses face aux attaques de traitements d'image

D'une manière générale, on constate qu'il existe un certain nombre d'algorithmes dédiés, dans le sens où la résistance du tatouage qu'ils dissimulent a fait l'objet d'une optimisation pour un type bien particulier d'attaques. Cette approche n'est malheureusement pas satisfaisante si l'on considère la multiplicité des attaques. On peut en effet combiner une attaque photométrique (compression) à une attaque géométrique (légère rotation) pour piéger les algorithmes dédiés. Ceci est d'ailleurs le principe de base des outils de test Unzign [89] et Stirmark [72, 54, 71].

8.2 Evolution conjointe des algorithmes de compression et de tatouage d'image

En raison des volumes d'information que constituent les images et les vidéos, de nombreux travaux de recherches ont vu le jour dans le but de réduire la quantité de bits nécessaires tant au stockage qu'à la transmission de ces données. Les techniques de compression développées sont basées sur :

- l'élimination des données redondantes ;
- la suppression des données non significatives.

Si le premier point ne constitue pas un danger vis-à-vis des systèmes de tatouage puisqu'il n'entraîne aucune perte d'information, il en est tout autrement du deuxième point. En effet, les techniques de compression dites « avec pertes » consistent à modéliser le système visuel humain puis, d'après ce modèle à négliger les données non pertinentes. Par exemple, la norme de compression pour image fixe JPEG réalise une quantification plus fine des coefficients DCT liés aux basses fréquences et néglige les coefficients très hautes fréquences. L'hypothèse sous-jacente à l'introduction d'une quantification adaptative réside dans les performances du système visuel humain qui est plus tolérant vis-à-vis d'imperfections au niveau des contours ou des régions texturées correspondant à des coefficients hautes fréquences. Il apparaît clairement que les progrès dans les domaines du tatouage et de la compression d'images sont très largement liés à une meilleure connaissance et modélisation du système visuel humain, cependant les finalités sont divergentes. Les techniques de tatouage visent à identifier les composantes de l'image psychovisuellement négligeables afin de disposer d'un canal de transmission invisible pour le tatouage, les techniques de compression ont pour objectif de supprimer ce canal. Les progrès accomplis en compression d'image et en tatouage d'image sont donc antagonistes. Dans le cas d'un système de compression idéal (ne conservant que les composantes psychovisuellement significatives) on peut d'ailleurs remettre en cause la faisabilité d'un système de tatouage invisible et robuste, puisque l'application de l'algorithme de compression sur l'image tatouée entraînera la suppression du tatouage.

8.3 Le tatouage peut-il résoudre les problèmes de droit d'auteur ?

Cette question fondamentale est posée dans l'article [13]. Les auteurs remettent tout au moins en cause la formulation du problème en soulignant son caractère incomplet. Les contraintes de robustesse du tatouage face à des traitements d'image et de maintien de la qualité de l'image originale sont présentées comme nécessaires mais non suffisantes. En effet, si l'objectif est d'apporter une preuve du droit d'auteur, il est impératif d'introduire la dimension temporelle. Non seulement le tatouage doit pouvoir être extrait de l'image mais il faut également apporter une preuve sur la date de tatouage de l'image. Après avoir précisé les notations des auteurs, nous décrirons les attaques illustrant ce propos.

Notations adoptées par les Auteurs

I	image originale

S	tatouage à introduire dans l'image
$\hat{I}$	version tatouée de I
$\mathcal{E}$	codeur réalisant l'insertion de S dans I
$\mathcal{D}$	décodeur réalisant l'extraction de S à partir de $\hat{I}$
$\mathcal{C}$	fonction de décision

Problème de multisignature

Alain a une image I, il la marque et génère ainsi l'image $\hat{I}$ qu'il rend publique. Isabelle marque à son tour l'image $\hat{I}$ et obtient ainsi $\hat{I}'$. Il est alors clair qu'à la fois Alain et Isabelle peuvent réclamer la paternité de l'image $\hat{I}'$, il existe alors une parfaite symétrie dans le problème. On peut objecter que cette symétrie peut être facilement rompue si l'on a recours à l'image originale tatouée $\hat{I}$ ou à l'image originale I elle-même. En effet à partir de $\hat{I}$ ou I Isabelle n'est pas en mesure d'extraire sa signature alors qu'*a contrario*, Alain peut exhiber sa signature à partir des images $\hat{I}$ et $\hat{I}'$ détenues par Isabelle. La remarque précédente suscite une première interrogation : Est-il bien nécessaire de mettre en oeuvre des techniques de tatouage ? Etant donné qu'il est nécessaire de recourir à une image de référence pour tester une image ? Est-ce que les lois de protection des droits d'auteur en vigueur ne peuvent pas s'appliquer directement ? La seconde objection encore plus critique, découle de la possibilité de créer une pseudo image originale conduisant au problème connu sous le nom de « dead lock ».

Attaque : SWICO (Single-Watermarked-Images Counterfeit-Original) conduisant au problème du « Dead Lock »

Le paragraphe précédent a montré que l'ultime rempart de sécurité des systèmes de tatouage consiste pour la personne victime d'une fraude (ici Alain) à exhiber les images originales (tatouée ou non) et à démontrer que sa signature est également présente dans les images exhibées par Isabelle alors qu'Isabelle ne peut en faire de même avec les images I ou $\hat{I}$.

Afin de prendre en défaut la protection mise en oeuvre par Alain , la stratégie d'Isabelle peut être de fabriquer une pseudo image originale $\tilde{I}$ à partir de $\hat{I}$ tel que $\hat{I}$ et I contiennent sa marque. On rétablirait ainsi une parfaite symétrie entre les deux candidats réclamant la propriété de l'image. La tâche d'Isabelle paraît au premier abord délicate puisqu'elle n'a à aucun moment accès à la véritable image originale I, comment pourrait-elle donc y introduire sa propre marque ? Le principe est de créer un processus de tatouage inverse. Isabelle ne cherche plus à dissimuler une marque S' dans l'image I' mais à la soustraire, créant ainsi une pseudo-image originale $\tilde{I}$. Isabelle a donc créé une nouvelle (fausse) image

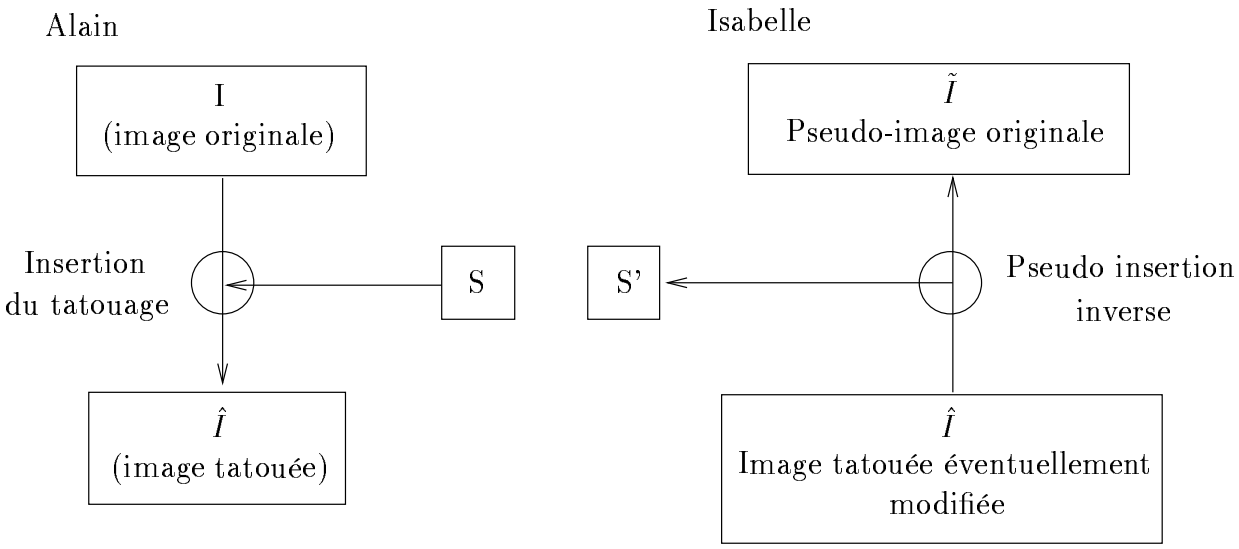


FIG. 9 – *Schéma d'attaque par pseudo-tatouage inverse conduisant à un problème indécidable (deadlock) même en ayant recours à l'image originale*

originale et n'a pas modifié l'image signée $\hat{I}$ mais est néanmoins en mesure de prouver que sa signature est présente à la fois dans $\hat{I}$ et I, ceci conduisant à un problème indécidable.

8.4 Nouvelles contraintes à imposer aux algorithmes de tatouage

Notion de système de tatouage non inversible

Dans l'attaque conduisant au problème du « dead-lock » présentée au paragraphe précédent, Isabelle est capable de créer une pseudo-image originale $\tilde{I}$ respectant les deux conditions ci-après :

$$\mathcal{E}^{-1}(\hat{I}, S') = \tilde{I}$$

et

$$\mathcal{E}(\tilde{I}, S') = \hat{I}$$

un système $(\mathcal{E}, \mathcal{D}, \mathcal{C})$ pour lequel il est possible d'exhiber un codeur $\mathcal{E}^{-1}$ vérifiant les deux conditions ci-dessus est dit inversible. Dans le cas contraire, $(\mathcal{E}, \mathcal{D}, \mathcal{C})$ est dit non-inversible [92].

Notion de système de tatouage quasi-inversible

Un système de tatouage $(\mathcal{E}, \mathcal{D}, \mathcal{C})$ est quasi-inversible si pour toute image $\hat{I}$ il existe un opérateur $\mathcal{E}^{-1}$ tel que :

$$\mathcal{E}^{-1}(\hat{I}) = (\tilde{I}, S')$$

$\mathcal{E}^{-1}$ peut être obtenu en un temps de calcul raisonnable. $\hat{I}$ et $\tilde{I}$ sont perceptuellement proches et

$$\mathcal{C}(\mathcal{D}(\hat{I}, \tilde{I}), S') = 1$$

sinon $(\mathcal{E}, \mathcal{D}, \mathcal{C})$ est dit non-quasi-inversible.

9 Conclusion

Cet état de l'art nous a permis de dégager les grandes lignes conduisant à la conception d'un système de tatouage et a révélé la variété des techniques mises en oeuvre. Néanmoins, la robustesse du tatouage semble surtout vérifiée vis-à-vis des standards compressions (Jpeg, Mpeg), elle n'est pas assurée face à une combinaison d'attaques, notamment lorsqu'il s'agit d'attaques par filtrage passe bas suivies de manipulations géométriques. Les problèmes liés aux protocoles de dépôt et de vérification sont encore peu abordés dans la littérature. La plupart des efforts se sont portés vers une gestion appropriée du compromis robustesse *vs.* visibilité, le plus souvent au détriment d'autres aspects comme la capacité d'insertion ou le mode d'extraction. Très peu d'algorithmes réalisent l'extraction dans un mode aveugle.

Chapitre 4

Proposition d'un algorithme de tatouage

Ce chapitre est dédié à l'algorithme de tatouage développé au cours de cette thèse et ayant fait l'objet des dépôts de brevets [19, 27]. Le cadre fixé pour cette étude consistait d'une part à ne pas avoir recours à l'image originale lors la procédure d'extraction du tatouage, d'autre part à être capable de dissimuler un nombre suffisant de bits pour permettre de couvrir un large champ d'applications, depuis la protection des droits d'auteur par dissimulation d'un identificateur de quelques bits jusqu'à des applications plus exigentes en termes de volumes d'informations à dissimuler pour assurer l'intégrité d'une image par exemple. Dans ce chapitre, nous nous focaliserons sur les aspects algorithmiques et en particulier sur les procédures mises en place pour s'accommoder de manipulations de l'image tatouée. L'aspect applicatif de cet algorithme sera abordé ultérieurement au chapitre 6.

1 Introduction à la méthode

Nous avons poursuivi pour le tatouage d'image l'approche adoptée au chapitre 1 dans le cadre du CA et consistant à dériver des algorithmes de codage de source afin d'assurer des services de sécurité. Soit une image originale I_{orig}, on peut considérer que tout algorithme de codage avec pertes décompose cette image en une somme de deux images. L'une, I_{codage} destinée à se substituer à l'image d'origine représente au mieux celle-ci, l'autre, l'image résiduelle I_{erreur} est dans le cas d'un codage de bonne qualité psychovisuellement négligeable.

$$I_{\text{orig}} = I_{\text{codage}} + I_{\text{erreur}} \tag{1}$$

L'image I_{erreur} apparaît naturellement comme un support favorable à la dissimulation d'un tatouage invisible car toute modification de cette image par le biais d'une modulation avec le tatouage que l'on souhaite dissimuler devrait rester imperceptible. Il convient de nuancer ce propos en notant que, dans le cas d'un codage de bonne qualité, l'exigence de robustesse du tatouage n'est pas remplie puisque, par exemple, l'emploi d'un algorithme de compression avec perte est susceptible de ne conserver que la composante I_{codage} entraînant rapidement la suppression du tatouage. Une possibilité pour rendre le tatouage plus robuste est d'employer un codeur générant une image I_{codage} de qualité médiocre augmentant ainsi l'énergie de I_{erreur} et donc la robustesse du tatouage transmis sur ce support. Cette approche garantit qu'un algorithme de compression visant à supprimer le tatouage devra générer une image de qualité proche de I_{codage} et donc inacceptable, pour espérer rendre le tatouage inopérant. Dans la proposition précédente, nous avons admis l'hypothèse selon laquelle la personne ne dispose pas de l'information secrète utilisée lors de l'insertion du tatouage. Sous cette hypothèse, il est donc nécessaire de manipuler l'ensemble de I_{erreur} en aveugle pour espérer supprimer le tatouage. Cette approche n'échappe bien évidemment pas au compromis robustesse *vs.* visibilité classique à tous les systèmes de tatouage. En effet, plus l'énergie de I_{erreur} est élevée, plus le tatouage présent dans cette composante devrait être robuste mais ce au prix d'un impact visuel plus important. Néanmoins, l'utilisation de techniques de codage de source pour gérer le compromis robustesse *vs.* visibilité apparaît comme une piste prometteuse car ces techniques contiennent intrinsèquement la notion de « psychovisuellement significatif » et sont totalement adaptées au media image. Nous allons à présent développer ces notions dans le cadre du codage par IFS.

2 Tatouage d'image basé sur un modèle affine d'ifs

L'algorithme de tatouage développé durant cette thèse s'inspire des principes précédents, en les transposant à un codeur fractal [28] qui présente en outre des propriétés d'invariances intéressantes et exposées au paragraphe 3 de ce chapitre. Considérons un modèle de transformée affine similaire à celui utilisé en codage :

$$W(I) = A\ I + O_{\text{moy}} \tag{2}$$

La matrice A représente les opérations d'amplification de contraste ainsi que les transformations géométriques reliant les blocs sources et les blocs cibles au cours d'une itération du processus de décodage. Le vecteur O_{moy} représente le réhaussement ou l'abaissement du niveau de gris moyen entre deux blocs en correspondance, les valeurs de ce vecteur sont donc constantes sur un bloc. Pour plus de détails, le lecteur est renvoyé au chapitre 1 ou peut consulter un article de base relatif au codage fractal tel que [48, 34]. Le théorème du collage stipule que :

$$I_{\text{orig}} \approx A\, I_{\text{orig}} + O_{\text{moy}} \tag{3}$$

Dans le contexte d'un codage par ifs, I_{codage} porte le nom d'attracteur noté I_{attract} et est défini comme la limite du processus itératif (processus de décodage) suivant :

$$\begin{aligned} I_{\text{attract}} &= A\,(\cdots A(A\, I_{\text{init}} + O_{\text{moy}}) + O_{\text{moy}} \cdots) + O_{\text{moy}} \\ &= \sum_{i=0}^{\infty} A^i\, O_{\text{moy}} \end{aligned} \tag{4}$$

En conséquence, $I_{\text{orig}} = I_{\text{attract}} + I_{\text{erreur}}$.

2.1 Détermination du support du tatouage

Modifions le modèle de code IFS défini par l'équation 2 en ajoutant un terme correctif O_{correc} à O_{moy}. Ce terme est calculé *a posteriori* de telle sorte que l'on obtienne l'égalité stricte au niveau du théorème du collage, soit :

$$O_{\text{correc}} = I_{\text{orig}} - (A\, I_{\text{orig}} + O_{\text{moy}}) \tag{5}$$

O_{correc} est à moyenne nulle par bloc car la composante continue O_{moy} a été soustraite. Les composantes positives et négatives de O_{correc} sont de plus équi-réparties. Ecrivons à présent la nouvelle équation régissant le processus de décodage :

$$\begin{aligned} I_{\text{orig}} &= A\,(\cdots(A\, I_{\text{init}} + O_{\text{moy}} + O_{\text{correc}})\cdots) + O_{\text{moy}} + O_{\text{correc}} \\ &= \sum_{i=0}^{\infty} A^i\, O_{\text{moy}} + \sum_{i=0}^{\infty} A^i\, O_{\text{correc}} \\ &= I_{\text{attract}} + I_{\text{erreur}} \end{aligned} \tag{6}$$

On constate que le premier terme s'identifie à l'attracteur initialement calculé pour coder l'image alors que le second terme s'identifie à l'image d'erreur [21]. Une écriture sous la forme :

$$I_{\text{erreur}} = \sum_{i=0}^{\infty} A^i\, O_{\text{correc}} \tag{7}$$

permet d'interpréter I_{erreur} comme l'attracteur du processus itératif défini par A et O_{correc}. Il vérifie donc le théorème du collage

$$I_{\text{erreur}} = A\, I_{\text{erreur}} + O_{\text{correc}} \tag{8}$$

d'où

$$O_{\text{correc}} = I_{\text{erreur}} - A\, I_{\text{erreur}} \tag{9}$$

Dans notre approche, le vecteur O_{correc} constituera le support du tatouage.

Remarque

La discrétisation de l'espace des transformées entraîne que deux images légèrement différentes seront néanmoins représentées par le même attracteur I_{attract} qui constitue ainsi une référence.

2.2 Codage du tatouage sur le support

Pour introduire la signature dans l'image, on procède à la modification de O_{correc} suivant les valeurs des bits de la signature binaire T_{bin}. Différentes formes de codage peuvent être envisagées. Nous présentons successivement une approche directe, réalisant un codage bit à pixel, puis une évolution basée sur un codage bit à ensemble de pixels.

Codage direct, bit à pixel

On établit une correspondance directe entre la valeur du bit que l'on souhaite coder et la valeur de O_{correc} rattachée à un pixel de l'image. Soit T_{bin} le vecteur de symboles binaires constituant le tatouage. On procède à une comparaison terme à terme de O_{correc} et T_{bin}.

$$\begin{array}{rcl} \text{Si } T_{\text{bin}} = 1 \text{ et } O_{\text{correc}} > 0 \quad \text{alors} & \quad & O_{\text{mod}} = O_{\text{correc}} \\ \text{si } T_{\text{bin}} = 0 \text{ et } O_{\text{correc}} < 0 \quad \text{alors} & \quad & O_{\text{mod}} = O_{\text{correc}} \\ \text{sinon} & \quad & O_{\text{mod}} = 0 \end{array} \tag{10}$$

O_{mod} constitue le vecteur substitué au vecteur O_{correc} initial pour le calcul de $I_{\text{tatouée}}$.

Généralisation et autres types de codage proposés

D'autres types de codage peuvent bien entendu être envisagés. On peut par exemple introduire une modulation dérivée de celle proposée par Zhao sur des triplets de coefficients DCT (cf. Chap. 3 § 5.4). Un bit de la signature T_{bin} est par exemple codé grâce à trois pixels de O_{mod}. Dans ce cas, plusieurs configurations de O_{mod} contribuent à la représentation d'un bit de T_{bin}. Ceci peut présenter de multiples avantages :

- D'une part, on peut choisir parmi les configurations possibles, celle qui présente un impact visuel minimum.
- D'autre part, on peut adopter une représentation binaire, telle que la distance de Hamming, entre deux configurations de O_{mod} représentant des valeurs différentes de T_{bin}, soit maximale.

– Et enfin, une priorité peut être octroyée à la configuration de O_{mod} entraînant une plus grande stabilité dans l'estimation de A et O_{moy} lors de la phase d'extraction du tatouage.

2.3 Recombinaison du support : obtention de l'image tatouée

Quel que soit le codage adopté pour « fixer » la signature T_{bin} sur le support, l'image tatouée est obtenue en substituant O_{mod} au vecteur initial O_{correc}. On obtient ainsi :

$$I_{\text{tatouée}} = \sum_{i=0}^{\infty} A^i \, (O_{\text{moy}} + O_{\text{mod}}) \tag{11}$$

La richesse du dictionnaire de transformées conditionne la qualité de l'image codée, c'est-à-dire de l'attracteur I_{attract} par rapport à l'image originale I_{orig}. On dispose donc d'un paramétrage pour augmenter ou diminuer l'énergie de l'image d'erreur en fonction du compromis robustesse *vs.* visibilité requis.

2.4 Approximations réalisées lors de l'extraction du tatouage

Nous nous plaçons ici dans un contexte sans attaque. Autrement dit, l'image ne subit aucune modification entre la phase de tatouage et la phase d'extraction de celui-ci. Néanmoins, le codage du tatouage T_{bin} sur le support O_{correc} implique bien évidemment que l'image tatouée est différente de l'image originale, même si elle en est très proche sur le plan psychovisuel. Ceci a des conséquences importantes quant à l'extraction du tatouage, en particulier si l'on se place dans un mode aveugle. La première étape vers l'extraction du tatouage nécessite la détermination de la référence I_{attract}. Ceci implique l'estimation de A et O_{moy} à partir de $I_{\text{tatouée}}$ et non plus de I_{orig}.

Si l'on considère T_{bin} et O_{correc} comme des variables aléatoires équi-réparties et indépendantes alors, par le biais des règles de modulation définies par les équations 10 on obtient :

$$\begin{aligned} I_{\text{tatouée}} &= I_{\text{orig}} \text{ avec une probabilité } p = 1/2 \\ &= I_{\text{attract}} \text{ avec une probabilité } q = 1/2 \end{aligned}$$

50 % des pixels de l'image tatouée sont donc différents de ceux de l'image originale, ceci peut donc paraître incompatible avec une estimation correcte de A et O_{moy} (y compris sans attaque). Néanmoins, il convient de ne pas perdre de vue la nature discrète du dictionnaire de transformation autrement dit de A et O_{moy}. Appréhendons le codage fractal sous l'angle d'une classification. L'espace des images est partitionné en classes dont chaque centroïde est constitué par l'un des attracteurs (fig. 1). Le codage fractal consiste à déterminer à quelle classe appartient l'image originale que l'on souhaite coder puis à représenter l'image par le centroïde (attracteur) de la classe. L'image tatouée $I_{\text{tatouée}}$ doit donc appartenir à la même classe que l'image originale I_{orig} afin que lors de l'extraction du tatouage on lui associe le bon attracteur. En substituant les valeurs de certains pixels originaux par des pixels de l'attracteur, on se rapproche de celui-ci et on assure ainsi la stabilité dans l'estimation de A et O_{moy}.

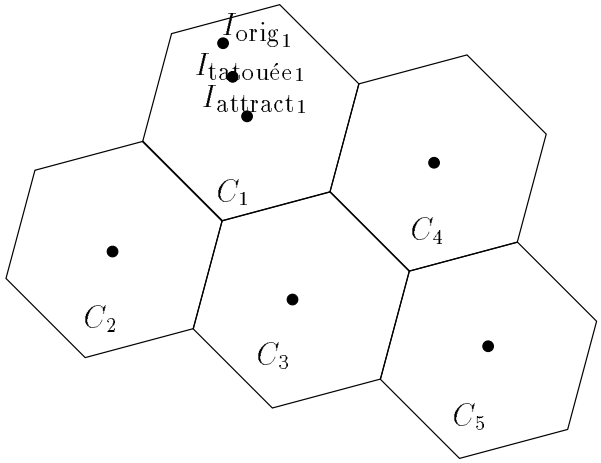


FIG. 1 – *Point de vue classification du codage fractal (la figure ne représente pas fidèlement la géométrie des frontières)*

3 Etude des invariances propres au codage fractal

La robustesse du tatouage est directement fonction de la stabilité de I_{erreur} ou plus exactement des signes de I_{erreur}. Dans cette section, nous étudions le comportement de I_{erreur} en fonction de modifications de l'image.

3.1 Invariance par réhaussement du niveau de gris moyen

Soit $I_{\text{tatouée}}$ l'image tatouée originale, on considère un éclaircissement ou un assombrissement de cette image d'une valeur ℓ. On a donc $\hat{I}_{\text{tatouée}} = I_{\text{tatouée}} + \ell \times \vec{u}$ où $\vec{u}$ est un vecteur unité de l'espace des images. Soient A et O_{moy} les paramètres du code fractal estimés lors du tatouage de l'image à partir de I_{orig}, on vérifie :

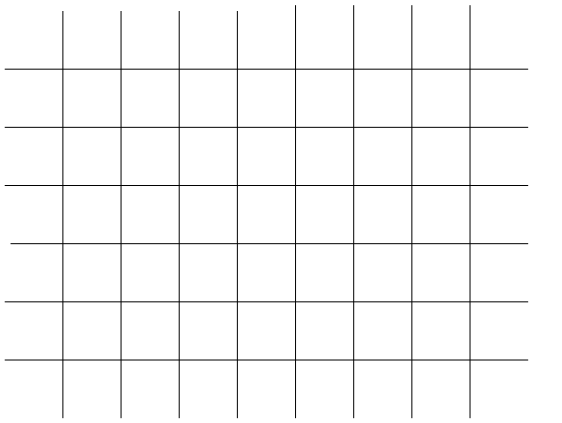
$$I_{\text{attract}} = A\, I_{\text{attract}} + O_{\text{moy}} \tag{12}$$

Etudions à présent les modifications que subissent ces paramètres lorsqu'ils sont estimés à partir de $\hat{I}_{\text{tatouée}}$. En minimisant l'erreur quadratique entre $\hat{I}_{\text{tatouée}}$ et $\hat{A}\, I_{\text{attract}} + \hat{O}_{\text{moy}}$ on va affecter exclusivement le paramètre O_{moy} de la façon suivante : $\hat{O}_{\text{moy}} = O_{\text{moy}} + \ell\vec{u}$. Au niveau de l'image d'erreur il n'y a aucune modification puisque la variation de $\hat{I}_{\text{tatouée}}$ est entièrement compensée par le code fractal.

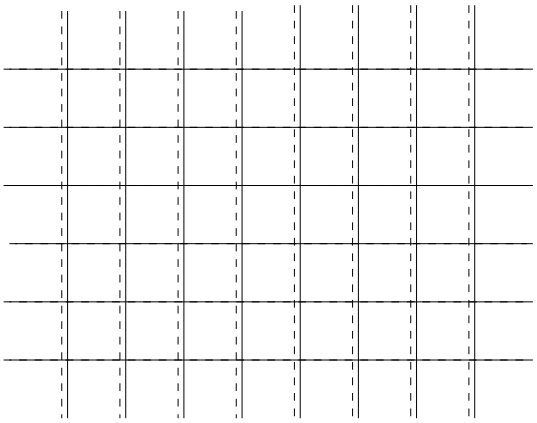
3.2 Invariance par réhaussement du contraste

Soit $I_{\text{tatouée}}$ l'image tatouée originale, on considère un réhaussement ou un affaiblissement de contraste d'un facteur α. La nouvelle image est de la forme :

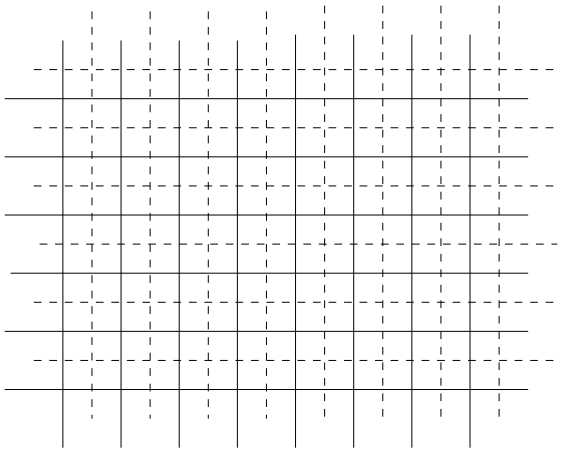
$$\hat{I}_{\text{tatouée}} = \alpha\, I_{\text{tatouée}}$$



a).



b).



c).

FIG. 2 – *Les différents cas relatifs à la translation de l'image tatouée*

où α est appliqué scalairement à chaque pixel de l'image. La procédure d'estimation des paramètres A et O_{moy} par minimisation de l'erreur quadratique va répercuter le réhaussement du contraste exclusivement sur la matrice A qui devient :

$$\hat{A} = \alpha\, A$$

L'image d'erreur reste inchangée.

3.3 Pseudo-invariance par translation

Nous étudions ici les effets d'un décalage de l'image tatouée sur la robustesse du support du tatouage. Trois cas sont à considérer :

– Le premier se réfère à un décalage d'une valeur égale à un multiple de la taille des blocs cibles. I_{erreur} est alors préservée à l'exception bien évidemment des bords où

l'information est perdue. Le support extrait $\hat{Supp}$ présente un décalage qu'il conviendra de compenser avant de procéder à la reconstruction de la signature (fig. 2.a).

- Le second cas est une approximation du précédent. Il n'y a plus superposition exacte entre les grilles des blocs cibles avant et après la translation (fig. 2.b), cependant, on peut admettre en première approximation que le contenu de chaque bloc n'est pas fondamentalement changé. Ce type de translation n'entraînera donc pas de profondes perturbations dans l'appariement bloc source, bloc cible.

- Le dernier cas, que l'on peut considérer comme le plus critique, se caractérise par une translation telle que la nouvelle grille de blocs cibles est en demi décalage (fig. 2.c) par rapport à la grille originale. En pratique, la stabilité est préservée pour les blocs cibles présentant un voisinage dont le contenu est proche des blocs eux-mêmes. Heureusement, cette configuration est très fréquente pour des images réelles.

Les simulations réalisées ont montré que, y compris dans le cas le plus défavorable, la redondance du tatouage conférait à la méthode une robustesse suffisante vis-à-vis de translations pour se dispenser de mettre en place des techniques plus élaborées. Néanmoins, nous proposons au paragraphe 3.5 des extensions afin d'octroyer de nouvelles invariances à la méthode. Ces extensions ont de surplus permis de rendre la méthode strictement invariante par translation.

3.4 Pseudo-invariance par changement d'échelle

Les systèmes de fonctions itérées contiennent intrinsèquement la notion d'invariance par changement d'échelle comme l'atteste les applications du codage fractal réalisant des zooms sur des images [23]. Dans ce contexte, l'invariance par changement d'échelle signifie qu'un code estimé à un niveau de résolution donné permet d'obtenir des images à des niveaux différents. La résolution de l'image décodée est exclusivement fixée par la taille de l'image initialisant le processus de décodage et non par le code lui-même. Pour notre propos, où seule l'invariance de I_{erreur} nous préoccupe, on peut montrer [34] que les propriétés d'invariance se traduisent par un sur- ou un sous-échantillonnage de I_{erreur}. En d'autres termes le sous-échantillonnage entraîne des pertes d'information au niveau du tatouage qu'il convient de prévenir, par exemple en sur-échantillonnant le tatouage initial.

3.5 Extension des invariances

Les paragraphes précédents nous ont permis de montrer que les techniques de codage fractal présentaient intrinsèquement de nombreuses invariances capitales pour des applications de tatouage d'image. Nous montrons dans ce paragraphe comment ces invariances de bases peuvent être étendues afin d'accroître la robustesse du tatouage. Les faiblesses restreignant la gamme des invariances sont de deux ordres :

- le premier est lié au choix de la primitive définissant les blocs cibles et sources,

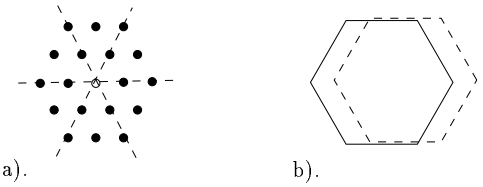


FIG. 3 – *Primitive hexagonale glissante autorisant des transformations plus fines, favorable à une extension des invariances*

– le second dépend de la nature des transformations inclues dans le dictionnaire des transformées.

Nous proposons de remplacer la grille de blocs cibles par une primitive glissante centrée sur chaque pixel (fig. 3). Tous les pixels de la primitive sont alors utilisés lors du critère d'appariement du codage, cependant contrairement à la méthode initiale, le résultat du codage est reporté uniquement sur le pixel central de la primitive et non plus sur l'ensemble de la primitive. Nous faisons glisser la primitive de pixel en pixel (et non plus de bloc en bloc) afin d'obtenir un codage de toute l'image. Ceci présente deux avantages. D'une part, le recouvrement, résultant de la technique glissante, permet de s'affranchir des problèmes dus à la variation du contenu des blocs cibles, rencontrés par exemple lors d'une translation de l'image (cf. § 3.3). D'autre part, le choix d'une primitive plus complexe (fig. 3) offre plus de degrés de liberté pour enrichir le dictionnaire de codage fractal et ainsi obtenir de nouvelles invariances, la primitive hexagonale proposée octroie ainsi de nouvelles invariances pour la rotation.

Remarque

Nous avons étudié le comportement de I_{erreur} pour des modifications globales de l'image $I_{\text{tatouée}}$. Cependant ces résultats restent valables localement. En effet, la recherche de similarités pour la détermination du code fractal est réalisée dans le voisinage de chaque bloc cible. On peut donc considérer que si le voisinage de chaque bloc reste invariant ou si les modifications sont homogènes à l'intérieur du voisinage, les propriétés d'invariance de I_{erreur} sont vérifiées.

4 Schéma global de notre méthode

Les premiers paragraphes de ce chapitre ont donné lieu à une présentation du coeur de notre algorithme, basé sur le codage fractal. Nous nous proposons à présent d'intégrer cette technique dans un schéma complet. Nous reprenons pour sa description l'architecture proposée dans le chapitre 3 sur l'état de l'art.

4.1 L'algorithme d'insertion

La figure 4 montre les trois grandes étapes de notre algorithme d'insertion. On distingue :

- le module de **mise en forme & sécurisation du tatouage**, faisant l'objet du paragraphe 5 ;
- le module de **détermination du support du tatouage**, dont les principes ont été exposés aux paragraphes 2 et 3 ;
- et enfin le module de **fusion des données tatouage et image** exposé au paragraphe 2.2.

4.2 L'algorithme d'extraction

L'algorithme d'extraction décrit à la figure 5 peut se décomposer en trois grandes parties :

- la première est dédiée à la **séparation des signaux** image et support du tatouage (cf. § 2.4 et § 3), elle est réalisée dans un mode totalement aveugle puisque ne nécessitant ni l'image originale ni le tatouage original ;
- la seconde procède au **décryptage et à la resynchronisation** entre le bruit d'étalement PN et les données reçues (cf. § 5.4 et § 7) ;
- la dernière partie prend en charge l'exploitation de la **redondance** afin de reconstruire le tatouage (cf. § 8.2).

5 Mise en forme de la signature

5.1 Types de signature supportés par l'algorithme

L'unité d'insertion de la signature dans l'image est le bit. Ceci découle directement de la modulation adoptée pour fusionner la signature et l'image ainsi que du critère décisionnel basé sur la détermination du signe de O_{mod}. Pour illustrer la mise en forme de la signature, nous avons choisi des logos binaires qui, outre leur aspect pratique pour le copyright d'image, permettent une visualisation claire des différentes étapes de la mise en forme. Néanmoins, il convient de noter que les principales contraintes de notre algorithme vis-à-vis du choix d'un type de signature sont de nature volumique. En effet, il convient de maintenir un rapport : volume du tatouage / volume de l'image, suffisament grand pour préserver une robustesse maximale à la signature.

Le module de fusion de données (signature image) admet comme paramètre d'entrée un signal binaire 2D $\hat{T}_{\text{sed}}$ de même résolution que l'image à signer ; or la signature binaire originale T_{bin} présente un nombre de bits quelconques de l'ordre de quelques dizaines à quelques centaines de bits.

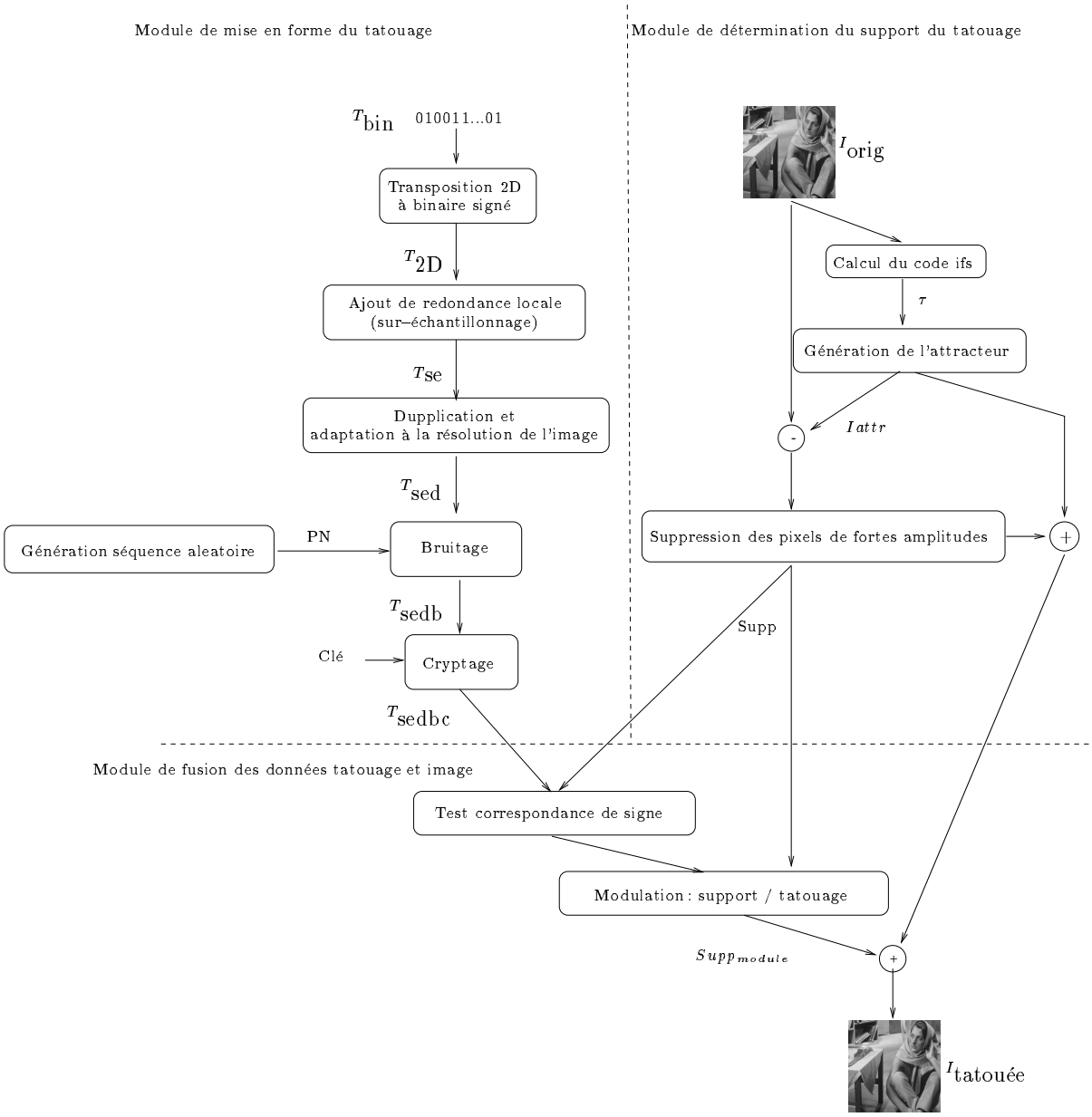


FIG. 4 – *Schéma d'insertion du tatouage*

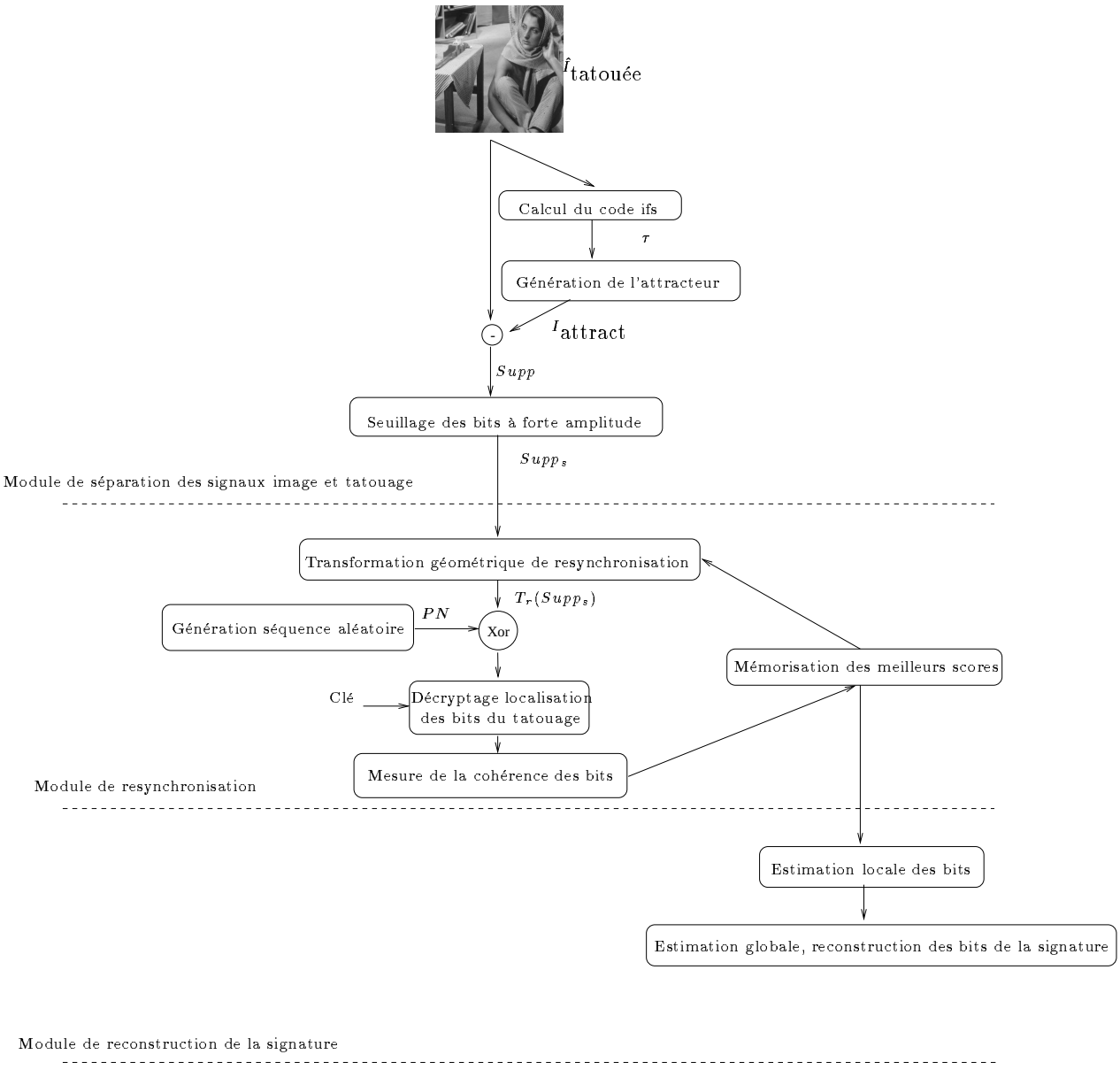


FIG. 5 – *Schéma d'extraction du tatouage*

FIG. 6 – *Types de signature supportés*

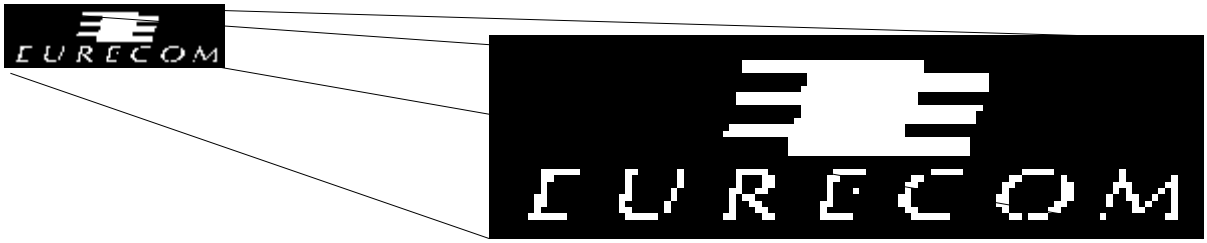


FIG. 7 – *Sur-échantillonnage du logo*

Ces opérations sont à rapprocher des adaptations au canal rencontrées en théorie des communications. En effet, l'image peut être considérée comme un canal de transmission par lequel on désire faire transiter de l'information constituée par la signature. Ce canal est susceptible d'être perturbé et l'adaptation des données brutes de signature aura pour objectif d'accroître l'immunité de la signature à ces perturbations ainsi que d'assurer une confidentialité de ces données.

5.2 Sur-échantillonner ($T_{\mathbf{se}}$) et dupliquer ($T_{\mathbf{sed}}$)

L'ajout de redondance est un moyen classique pour se prémunir contre une perte partielle d'information. L'étude des différentes manipulations susceptibles d'être appliquées à une image sans pour autant lui ôter tout intérêt a fait apparaître qu'il pouvait être pertinent d'ajouter de la redondance à deux niveaux distincts :

Le premier local (au sens spatial de l'image) : est constitué par un sur-échantillonnage de la signature originale T_{bin} original. Ce sur-échantillonnage est réalisé suivant les directions verticale et horizontale. Il a été déterminé, au regard des filtrages passe-bas ne dégradant pas outrageusement la qualité de l'image, qu'un facteur 3 de sur-échantillonnage constituait un paramétrage correct. Ce sur-échantillonnage entraîne un décalage vers les basses fréquences du logo original, puisque le niveau d'un bit est maintenu à la même valeur pendant toute la période de sur-échantillonnage. Ce décalage fréquentiel est cohérent avec l'idée que les basses fréquences seront faiblement détériorées si l'image conserve une qualité acceptable et qu'a contrario, les hautes fréquences risquent de disparaître lors d'un filtrage de type passe-bas qui n'entraîne pas une dégradation très importante de l'image, ce qui est classiquement admis dans le domaine du codage avec pertes.

Le second global : consiste à dupliquer la signature sur-échantillonnée T_{se} constituant ainsi un pavage de l'image. Cette forme de redondance est recommandée pour pallier une défaillance locale de l'algorithme. Il peut s'avérer que des régions de l'image se révèlent inadéquates pour recevoir de l'information, il serait donc fortement préjudiciable que toute l'information permettant de reconstituer un bit de la signature soit contenue dans une région unique de l'image. En effet, d'une part, des régions peuvent être inadaptées pour dissimuler de l'information (i.e. : problèmes de visibilité liés au contenu de la région de l'image) et d'autre part, des régions peuvent

FIG. 8 – *Duplication du logo*

disparaître au cours de certaines manipulations de l'image tel qu'un recadrage, un montage d'images.

5.3 Bruiter

A ce stade de la description de notre méthode, nous disposons d'une marque binaire de la signature dont la taille est égale à celle de l'image. Cependant elle est encore inadaptée à un codage sur le support *Supp via* les méthodes de modulation proposées au paragraphe 2.2. Les raisons motivant des opérations complémentaires préalablement au codage sont les suivantes :

– Il est nécessaire de garantir un service équivalent à tous les clients. En d'autres termes, les performances de l'algorithme doivent être similaires quel que soit le logo considéré ou plus généralement la signature. Ce n'est pas le cas actuellement car de

nombreux logos présentent une répartition de « 0 » et de « 1 » bien particulière pouvant entraîner un comportement marginal de l'algorithme notamment concernant la robustesse.

- Il est souhaitable de disposer d'une signature dont la statistique est proche de celle du support $Supp$, c'est-à-dire à moyenne nulle et équirépartie au niveau des signes. En effet, si tel n'est pas le cas, la technique de modulation de la signature sur le support conduit à privilégier les valeurs positives (ou négatives) de $Supp$ pour supporter l'information, et ceci est préjudiciable à la robustesse du tatouage.

- De nombreuses études psychovisuelles [88, 38] ont montré que le système visuel humain identifie très clairement la présence de motifs réguliers dans une image, même si ceux-ci sont noyés parmi d'autres signaux. La périodicité introduite par la duplication du logo peut contribuer à la création de tels motifs susceptibles d'avoir un impact visuel gênant qu'il convient de prévenir.

- Dans la plupart des applications de tatouage, en particulier en vue d'assurer la protection du copyright, l'information à dissimuler dans l'image n'est pas secrète. Un logo représentant une société, ou une adresse e-mail en sont des exemples. En effet, l'objectif n'est pas de transmettre un message secret contrairement à la stéganographie [49] mais de prouver qu'un message connu identifiant le propriétaire est bien présent dans le document.

Pour remédier à ces possibles faiblesses, nous appliquons une opération de Xor (ou exclusif) entre T_{sed} et un signal aléatoire PN généré par un algorithme à clé secrète.

Cette opération présente un double avantage. D'une part elle supprime toute périodicité dans l'information que nous allons introduire dans l'image à condition que le bruit soit lui-même non périodique. D'autre part elle permet d'uniformiser la répartition de l'information dans l'image quel que soit le logo que l'on désire incruster. En effet, par le biais de ce bruit, l'information dissimulée dans l'image est rendue parfaitement aléatoire et statistiquement indépendante du logo. Pour chaque pixel de l'image, il y aura donc une probabilité $\frac{1}{2}$ qu'il y ait correspondance entre le bit d'information T_{sed} (i.e. : "0 " ou "1") et le signe du support de la signature $Supp$.

Choix du type de bruit : Un bruit uniforme sur l'intervalle a été adopté. La fréquence maximale est imposée par la période adoptée lors du sur-échantillonnage du logo. En effet, nous savons qu'il est préjudiciable d'introduire un signal de fréquence supérieure à $\frac{1}{\text{période de sur-échantillonnage}}$ car il serait très sensible au filtrage passe bas de l'image.

5.4 Cryptage et incertitude sur la localisation du tatouage

L'opération « ou exclusif » réalisée précédemment, place toute personne ne disposant pas de la séquence PN, dans l'incapacité de connaître la valeur des bits de la signature cachée. Néanmoins, ceci ne signifie en aucune façon que le tatouage est protégé contre une attaque visant à le rendre irrécupérable. Etudions cette faiblesse en détails. Chaque bit de la signature est codé sous une forme redondante grâce à une multitude de pixels de l'image. La valeur de chaque bit de la signature extraite est attribuée par maximisation d'un

critère de vraisemblance. Pour certaines signatures, par exemple constituées d'un simple numéro, la perte d'un seul bit de la signature originale entraîne l'invalidité de l'algorithme. Dans ces conditions, une attaque triviale mais cependant efficace pourrait par exemple consister à choisir un bit quelconque de la signature et à perturber l'ensemble des pixels utilisés pour sa reconstruction. Cette perturbation peut consister à ajouter et à retrancher alternativement quelques niveaux de gris aux pixels. Dans le cas où le tatouage est codé sur le support par modulation d'amplitude, une telle manipulation rend la reconstruction du bit inefficace. Notons que cette attaque n'introduit pas obligatoirement une dégradation outrancière de l'image dans la mesure où un nombre relativement réduit de pixels a été touché. Il est nécessaire de mettre en place un système cryptographique permettant de « casser » l'association directe entre un bit de la signature et les pixels le représentant (cf. fig. 9). Le choix du procédé cryptographique doit se faire en tenant compte des nombreuses erreurs pouvant survenir dans le message (tatouage avant reconstruction) reçu. En effet, la plupart des procédés cryptographiques sont basés sur le principe de confusion-diffusion. Autrement dit, si l'on considère le chiffrement d'une page de texte, la notion de confusion correspond au mélange de l'ordre des caractères alors que la diffusion assure une inégalité entre la fréquence des caractères du texte chiffré vis-à-vis de ceux du texte clair. Le principe de diffusion implique que la modification d'un caractère du texte clair entraîne la modification de l'ensemble du texte chiffré, de façon similaire le changement d'un caractère du texte chiffré induit une modification de l'ensemble du message déchiffré résultant. Les conséquences de ce principe sont catastrophiques dans notre cas où des erreurs sont introduites au niveau du tatouage (avant reconstruction). En effet, des manipulations de l'image donneront inévitablement naissance à un phénomène de propagation d'erreurs rendant impossible la récupération du tatouage.

En conclusion, le processus pseudo-aléatoire en charge de l'association bit de tatouage, pixel de l'image doit être totalement indépendant d'éventuelles modifications de l'image. Ceci ne va pas sans poser d'importants problèmes de robustesse du processus cryptographique si de nombreuses images sont signées par la même personne avec la même clé. Nous préconisons par exemple d'indexer la séquence aléatoire en fonction du temps.

6 Paramétrisation de l'algorithme et problèmes de visibilité

Il est essentiel de pouvoir influer sur des paramétres de l'algorithme afin de positionner le compromis robustesse *vs.* visibilité au niveau souhaité. En effet, certaines images de qualité médiocre peuvent supporter un tatouage important sans dégradation perceptible, *a contrario* des images de haute qualité doivent être tatouées modérément pour préserver leur qualité originale. En outre, certains auteurs peuvent tolérer une légère dégradation de leurs images au profit d'une protection accrue, contrairement à d'autres auteurs qui souhaiteront maintenir à tout prix la qualité originale de l'image. Il s'agit d'autant d'exemples mettant en valeur la nécessité de proposer un algorithme paramétrable afin de satisfaire aux différentes demandes. Dans notre algorithme, le compromis robustesse *vs.* visibilité est géré à plusieurs niveaux. Le premier présenté au paragraphe 6.1 est propre à l'utilisation

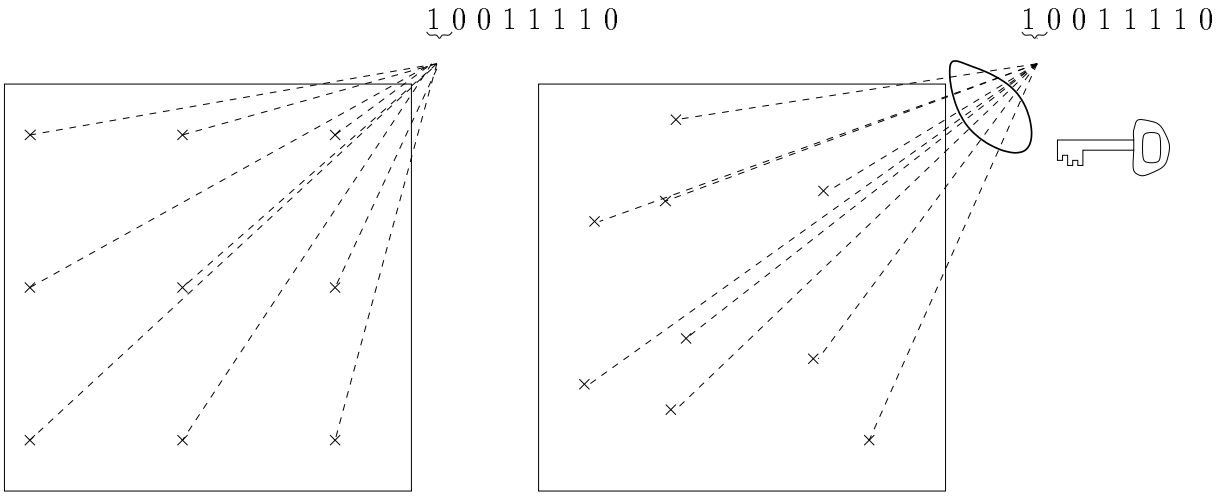


FIG. 9 – *Association entre les bits de signature*

de techniques de codage fractal et tient compte de la nature des régions de l'image. Le second présenté au paragraphe 6.2 est une paramétrisation directement liée à la technique de fusion du tatouage sur le support.

6.1 Discrétisation du dictionnaire de codage

Le codage fractal nécessite la définition d'un dictionnaire de transformations dans lequel sont choisies les fonctions décrivant le processus itératif représentant l'image (cf. § 3 Chap. 1). Dans le contexte du codage de source, la détermination du dictionnaire s'effectue en fonction du compromis : qualité de l'image, taux de compression. Pour notre propos, nous montrerons que la notion de compression disparaît au profit de celle de robustesse du tatouage.

Le choix d'un dictionnaire riche améliore sensiblement la qualité de l'image reconstruite. En d'autres termes, l'attracteur I_{attract} se trouve d'autant plus proche de l'image originale I_{orig} au sens d'une distance donnée (généralement la distance quadratique) que le dictionnaire est complet. Ceci se vérifie immédiatement en examinant la borne supérieure de l'erreur de reconstruction proposée par le théorème du collage. Ce résultat est confirmé d'un point de vue pratique comme l'illustre la figure 10

La règle de modulation stipule que l'erreur maximale est de la forme $I_{\text{orig}} - I_{\text{attract}}$, il est clair que plus le dictionnaire de codage est riche plus I_{attract} se rapproche de $Iorig$ et donc plus cette erreur diminue. La contrepartie d'un tel choix est la perte de robustesse du tatouage. En effet, l'image d'erreur $Iorig - Iattr$ constitue le support du tatouage.

6.2 Modulation de la signature sur le support

L'opération de mixage de la signature avec le support du tatouage (cf. § 2.2) est propice à un paramètrage : visibilité, robustesse. Ce paramétrage est réalisé en termes de densité de pixels marqués et d'amplitude des modifications par rapport à l'image originale.

Image originale

Attracteur très basse qualité

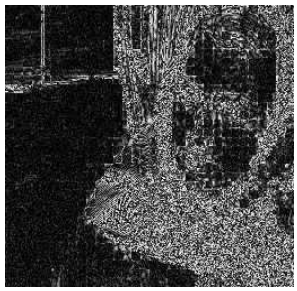


Image d'erreur amplifiée × 10

Attracteur basse qualité

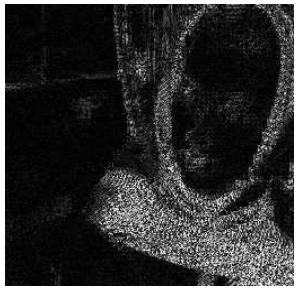


Image d'erreur amplifiée × 10

FIG. 10 – *Discrétisation du dictionnaire et erreur de reconstruction*

7 Resynchronisation des données reçues

7.1 Le problème

La nature étalée du tatouage permet de compenser certaines imperfections dans le positionnement relatif de $\hat{Supp}_{module}$ par rapport au bruit de la séquence d'étalement PN, cependant cet étalement ne peut pas corriger des transformations dont l'amplitude dépasse quelques pixels. A titre d'exemple, une translation horizontale supérieure à 5 pixels ne peut être compensée par ce dispositif. Il est donc nécessaire de mettre en place un dispositif capable d'effectuer le repositionnement. Ce problème revêt deux aspects :

- le premier consiste à proposer un modèle de transformées suffisamment riche pour pouvoir englober en première approximation l'ensemble des transformations potentiellement subies par l'image.
- le second est relatif au critère permettant de déterminer pour une image à authentifier donnée, quelle transformation ou quelles valeurs des paramètres du modèle sont les plus appropriées à compenser la transformation réellement appliquée à l'image.

7.2 Méthode directe

La première difficulté consiste à définir de façon précise l'espace des solutions, c'est-à-dire l'ensemble des transformations d'une image. D'un point de vue théorique, si l'on

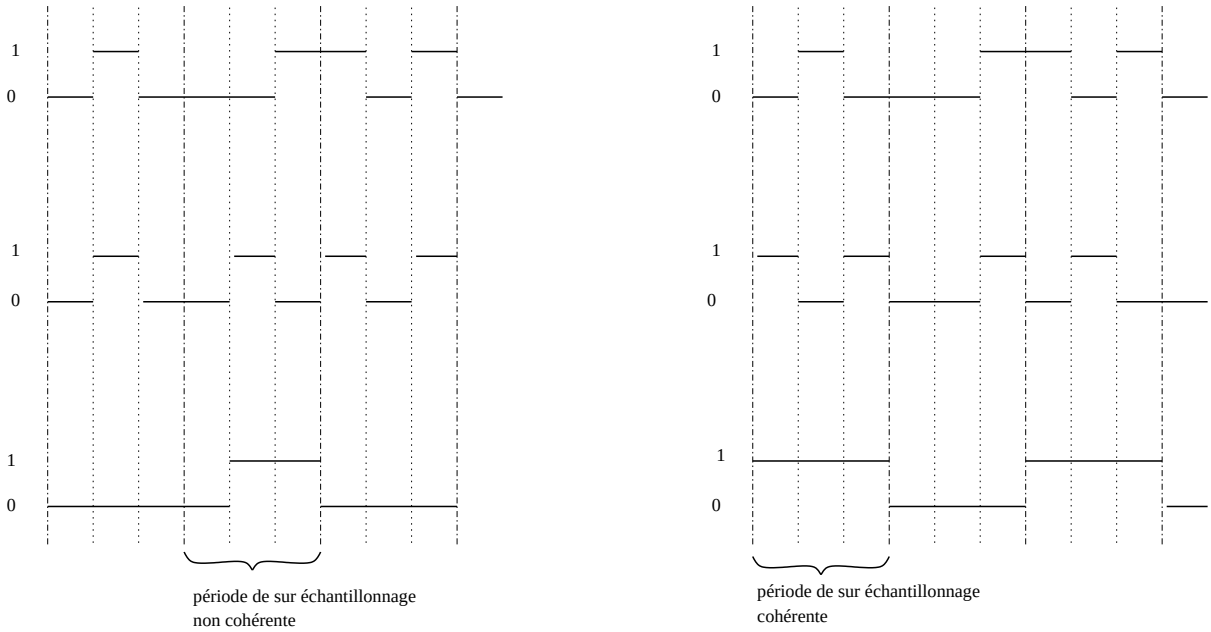


FIG. 11 – *Principe du recalage par maximisation de cohérence. a) la valeur du bit n'est pas constante sur la période de sur-échantillonnage (ici 3), le bruit n'est pas correctement recalé. b) après un décalage vers la droite du bruit, les valeurs des bits deviennent constantes sur la période de sur-échantillonnage ; on en conclut à un recalage correct du bruit. Le principe de maximisation de cohérence s'applique également au niveau global en considérant la duplication du tatouage.*

considère une image comme un ensemble de points, une transformation est une permutation de tous ou certains de ces points. L'espace des transformations obtenues bien que très riche ne correspond pas à nos besoins. D'une part, il considère un grand nombre de transformations qui ne préservent aucunement l'intelligibilité de l'image (l'image issue de la transformation ne présente aucun intérêt), d'autre part, il ne prend pas en compte les transformations tel que le changement de résolution dans lesquelles l'espace d'arrivée est distinct de l'espace d'origine. Nous sommes donc contraint de définir l'espace des manipulations géométriques des images de façon empirique. La procédure de resynchronisation est basée sur une maximisation de la cohérence des bits extraits de l'image et contribuant à la reconstruction d'un bit du tatouage. La maximisation est effectuée en décrivant l'espace des manipulations géométriques.

7.3 Tentative d'optimisation par une approche hiérarchique

Le principal problème rencontré dans la méthode directe est inhérent à la nature exhaustive de la recherche de solution. L'espace des solutions à parcourir est en effet considérable.

Première approche : orthogonaliser l'espace des solutions. Ceci permettrait d'estimer chaque type de transformée indépendamment.

Deuxième approche : sous-échantillonner l'espace des solutions, avec la possibilité de mettre en place une procédure de raffinement successif.

7.4 Méthode utilisant l'image tatouée standard

Précisons tout d'abord le terme d'image tatouée standard qui ne doit pas être confondu avec l'image originale (non tatouée). L'image tatouée standard est l'image directement issue de l'algorithme de tatouage. Cette image n'a donc subi aucune modification qu'elle soit de type bienveillante (compression) ou malveillante, elle est cependant dotée d'une protection visant à protéger ses droits d'auteur et peut par conséquent faire l'objet d'une diffusion publique contrairement à l'image originale qui ne doit en aucun cas être mise en circulation.

Nous disposons d'une image de référence contrairement aux deux autres méthodes précédemment proposées.

8 Exploitation de la redondance et reconstruction de la signature

8.1 Réjection des bits à faible taux de cohérence

Nous avons défini la cohérence locale d'un bit par son taux de variabilité sur une période de sur-échantillonnage.

Après des modifications de l'image signée, il arrive très fréquemment qu'un bit ne soit pas cohérent sur une période de sur-échantillonnage bien que le recalage du bruit ait été

réalisé avec succès. Dès lors, il est intéressant d'exclure ces bits avant de procéder à la reconstruction du logo.

Nous considérons donc l'ensemble des bits contribuant à la reconstruction d'un pixel du logo et les classons par ordre de cohérence locale décroissante. Pour chaque pixel du logo, seuls les N bits présentant les taux de cohérence locaux les plus forts seront considérés par la suite.

Remarque :
Outre le rejet de bits basé sur la cohérence locale, il est possible d'introduire une notion de certitude liée à la validité des bits du voisinage. Un bit entouré de bits supposés erronés devra être considéré avec « précautions ».

8.2 Exploitation de la duplication de la signature par vote

Pour un bit de la signature donné, parmi les bits considérés valides (non exclus par le processus précédent), on organise un vote. Si le score obtenu est supérieur à un seuil, c'est-à-dire que l'on arrive à dégager une majorité suffisamment large, le pixel du logo prend la valeur du groupe dominant.

8.3 Cas d'une signature de type logo : post filtrage

Des connaissances a priori sur la signature peuvent être utilisées en dernier recours pour prendre une décision quant à la valeur du bit extrait. Cette aide à la décision est particulièrement utile dans les cas où le système d'extraction octroie un niveau de certitude faible, autrement dit si le vote (cf. § 8.2) n'a pas permis de dégager une majorité suffisamment large. A titre d'exemple, un filtrage par hystérésis permet de diminuer le taux d'erreur de 10 % dans le cas où la signature est constituée d'un logo binaire. Lors de nos simulations, nous avons considéré qu'une majorité inférieure à trois voix ne constituait pas une majorité suffisante et qu'il était alors préférable de réaliser une prédiction pour déterminer la valeur du bit. Cette prédiction consiste à utiliser un voisinage 3×3 centré sur les pixels défectueux et à affecter à ce pixel la valeur dominante des pixels contenus dans le voisinage. Ce type de filtrage est uniquement adapté à des signatures possèdant une stationnarité suffisamment forte pour que la prédiction soit valide. Les signatures de type logo sont donc particulièrement bien adaptées, cependant il convient d'attirer l'attention du lecteur sur le fait que ce procédé de restauration par filtrage prédictif est susceptible d'introduire des disparités quant à la robustesse des différentes signatures. Ceci est contraire au principe d'égalité entre les différents utilisateurs, qu'il est légitime d'exiger.

9 Evaluation de la robustesse de l'algorithme face aux traitements de l'image

De nombreux algorithmes de tatouage ont vu le jour au cours de ces dernières années. Malheureusement aucune évaluation commune n'a été réalisée. Il est très difficile à l'heure actuelle de cerner les forces et les faiblesses de chacune des méthodes. Dans cette section,

nous proposons un test qui s'articule autour de trois points que nous avons jugés essentiels. Le premier est relatif à la qualité de l'image signée ; le second concerne la capacité de l'algorithme à cacher un tatouage de volume informationnel important ; le troisième mesure la robustesse du tatouage face à des attaques sur l'image. En termes de robustesse, il nous est apparu intéressant de noter l'évolution des phénomènes au-delà d'une réponse binaire de la forme : robuste / non robuste.

Pour mesurer ces trois paramètres nous avons défini le protocole suivant.

9.1 Protocole du test

La première partie du test consiste à déterminer la capacité maximale de l'algorithme à dissimuler un tatouage. La qualité entre l'image tatouée et l'image originale est fixée à une valeur supérieure à 38 dB, on considère une séquence aléatoire binaire de longueur L constituant le tatouage. Le paramètre L est fixé de telle sorte que l'on récupère (sans attaque de l'image) la séquence binaire avec un taux d'erreur de l'ordre de 1 %. On est ainsi placé aux limites de la robustesse de l'algorithme.

La seconde partie du test consiste, à partir de l'image tatouée définie lors de la première phase à faire subir des manipulations à cette image et à observer l'évolution du taux d'erreur de la séquence binaire restituée.

Nous étudions le comportement de notre algorithme face à une compression Jpeg. On considère l'évolution de la robustesse en fonction du facteur de qualité de la compression 1. Le tableau 2 présente la robustesse de l'algorithme face à un large éventail d'attaque par traitement d'image. Pour cette évaluation, nous avons considéré différents tatouages et différentes images. Nous avons ainsi pu vérifier que l'introduction d'une opération Xor entre le tatouage et un bruit (cf. § 5.3) permet bien l'obtention de résultats similaires quel que soit le tatouage considéré (principe d'égalité de service). Ces résultats ont fait l'objet d'une démonstration présentée à IEEE-Multimedia Signal Processing Workshop [79].

Une évaluation complémentaire sera présentée au chapitre 6 dans un contexte plus applicatif, il sera plus particulièrement discuté des problèmes liés aux protocoles de dépôt et de vérification du tatouage comparativement à la deuxième approche proposée dans cette thèse décrite au chapitre 5.

10 Conclusion

Nous avons proposé un système de tatouage robuste capable de fonctionner dans les différents modes d'extraction. L'accent a néanmoins été porté sur le mode aveugle, ouvrant ainsi les portes au plus large champ d'applications. Au niveau de la robustesse, nos travaux se sont particulièrement attachés à résoudre les problèmes découlant de manipulations géométriques complexes et/ou de la combinaison de transformations telles que celles constituées par les attaques Stirmark et Unzign qui au regard de l'état de l'art 3 semblent poser le plus de difficultés. Bien qu'il n'existe pas de preuve formelle de la robustesse de l'algorithme, les simulations réalisées ont révélé un très bon comportement de celui-ci dans des configurations de tatouages et d'images variées. Ces résultats ont été

	PSNR	récupéré succès
image originale / image tatouée	37.6	oui
image tatouée / image tatouée, compressée Jpeg Q75	39.46	oui
image tatouée / image tatouée, compressée Jpeg Q65	38.44	oui
image tatouée / image tatouée, compressée Jpeg Q55	37.63	oui
image tatouée / image tatouée, compressée Jpeg Q45	36.95	oui
image tatouée / image tatouée, compressée Jpeg Q35	36.08	oui
image tatouée / image tatouée, compressée Jpeg Q25	34.82	oui
image tatouée / image tatouée, compressée Jpeg Q15	32.81	oui[5]
image tatouée / image tatouée, compressée Jpeg Q5	27.97	non[6]

TAB. 1 – *Résistance du tatouage face à des niveaux croissant de compression JPEG. (Les tests présentés ont été réalisés sur l'image Fruits)*
La première ligne de ce tableau donne une mesure analytique (L_2) de la dégradation engendrée par le tatouage. Les lignes suivantes donnent une évaluation du comportement de l'algorithme lors de compressions JPEG de plus en plus fortes.

obtenus sans sacrifier la capacité d'insertion de notre algorithme puisque nous sommes capables d'insérer jusqu'à 900 bits tout en obtenant des taux d'erreurs faibles.

Attaque	**Type de tatouage**	**Type d'image**	**Tatouage extrait**
Jpeg Q40%	ascii : "Eurecom"	Lena 512 × 512, 256 niveaux de gris	"Eurecom"
Jpeg Q40%	ascii : "IEEE"	US Airforce jet 512×512, couleur 24 bits	« IEEE »
Petite rotation 0.7 degré	ascii : "Lena"	Lena 512×512, 256 niveaux de gris	"Lena"
Translation horizontale de 7 pixels	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Recadrage 10%	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Effet miroire	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Etirement horizontal 105 %	séquence aléatoire 900 bits	House 256×256, couleur 24 bits	97 % bits récupérés
Inclinaison verticale 1 degré	séquence aléatoire 900 bits	House 256×256, couleur 24 bits	82 % bits récupérés
Imprimer & Scanner couleurs 600dpi	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »
Imprimer & Scanner niveaux de gris 1200 dpi	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »
conversion RAW2GIF	séquence aléatoire 900 bits	Fruit 512×512, couleur 24 bits	74 % bits récupérés
Unzign cracker	ascii : "Eurecom"	US Airforce jet 512×512, couleur 24 bits	« Eurecom »
Stirmark cracker	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »

TAB. 2 – *Exemples de tests de robustesse de l'algorithme de tatouage face à diverses manipulations de l'image. La qualité de l'image tatouée par rapport à l'image originale est dans tous les cas maintenue supérieure à 37/38 dB. Les images correspondant à ces tests figurent en annexe*

Chapitre 5

Proposition d'une alternative au tatouage : l'empreinte externe

Les approches par tatouage butent sur la difficulté de concevoir un tatouage respectant le compromis robustesse vs. visibilité. En effet, l'information ajoutée doit être d'une part invisible car il n'est pas tolérable de dégrader la qualité de l'oeuvre originale, mais néanmoins fortement présente car cette information doit pouvoir être restituée même après que l'image a subi diverses manipulations de nature ne dégradant pas outrageusement sa qualité (robustesse). L'approche proposée dans ce chapitre et ayant fait l'objet du dépôt de brevets [30, 26] s'inscrit en marge de ces méthodes dans la mesure où aucune information n'est dissimulée dans l'image elle-même. Nous proposons de créer une empreinte externe à l'image, cette empreinte est archivée dans une base de données et utilisée a posteriori pour apporter la preuve de la propriété de l'image.

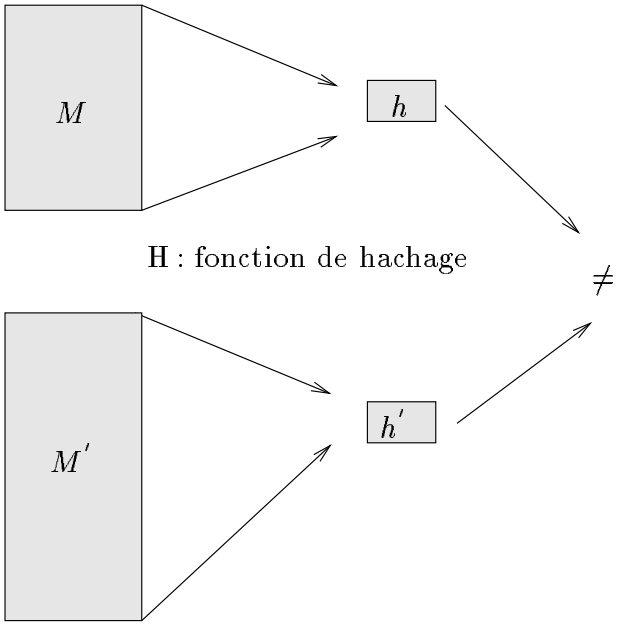


FIG. 1 – *Fonction de hachage*

1 Rappel sur les fonctions de hachage à sens unique

Les fonctions de hachage à sens unique sont largement utilisées en sécurité dès lors qu'il s'agit de signer un fichier informatique. Ces fonctions sont utilisées tant pour s'assurer de l'intégrité d'un fichier que pour attester de la provenance ce fichier. En s'appuyant sur la figure 1, nous nous proposons de clarifier la notion de fonction de hachage.

Définition 3 (Fonction de hachage à sens unique) *Une fonction de hachage, $H(M)$ s'applique à n'importe quel message M de longueur quelconque et retourne un message $h = H(M)$ de longueur fixe m. La fonction H vérifie de plus les propriétés suivantes :*

- *étant donné M, il est facile de calculer h ;*
- *étant donné h, il est très difficile de trouver un message M tel que $H(M) = h$;*
- *étant donné un message M, il est très difficile de trouver un autre message M' tel que $H(M) = H(M')$*

La difficulté d'appliquer de telles fonctions à notre contexte provient des manipulations que peut subir l'image. L'utilisation de fonctions de hachage pour prouver l'origine d'un document nécessite que ce document n'ait pas été retouché de quelque façon que ce soit car ces fonctions sont instables et modifient intégralement leur résultat si le message d'entrée change même d'un seul bit. Ceci est incompatible avec le propos du tatouage d'image qui est justement de prouver l'origine d'une image même lorsque celle-ci a été contrefaite. Nous tenterons dans la suite de ce chapitre de résoudre cette incompatibilité.

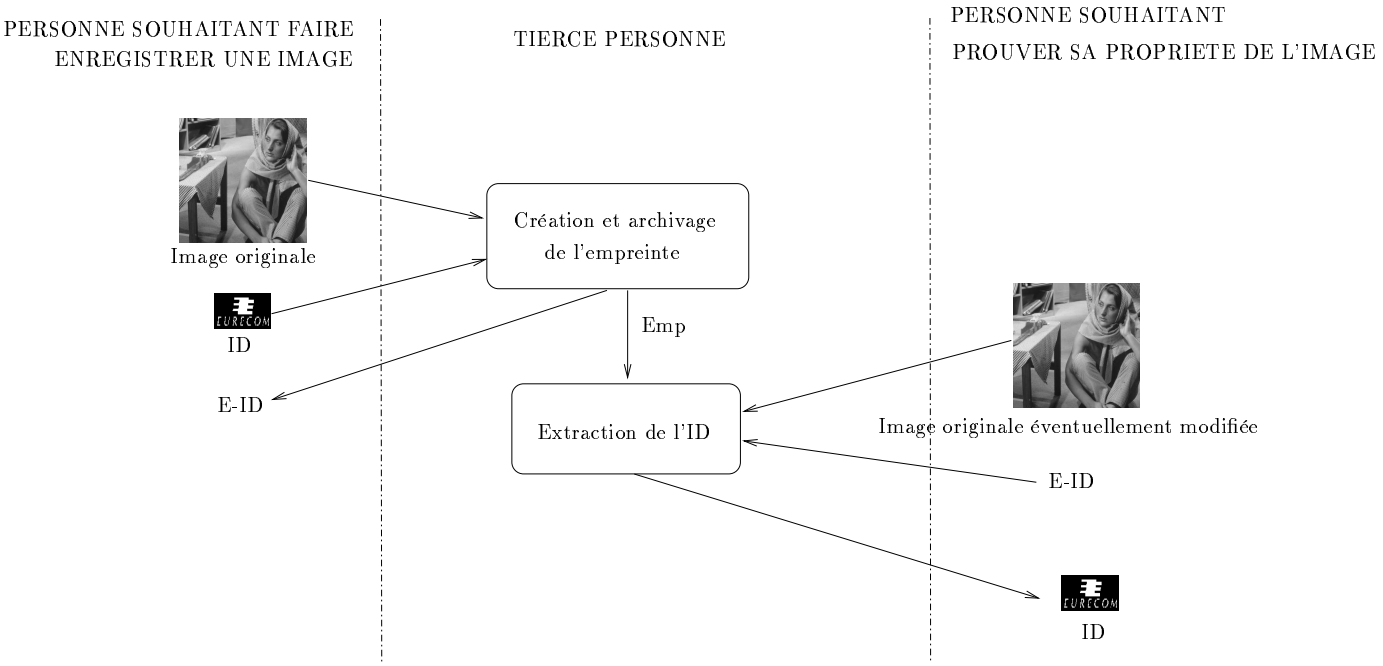


FIG. 2 – *Principe de l'empreinte externe*

2 Du tatouage vers l'empreinte externe

L'analyse au niveau des protocoles de la problématique relative à la protection des droits d'auteur (cf. § 3 Chap. 2) a fait apparaître que contrairement aux premières espérances, il ne semble pas possible de faire «l'économie» d'une tierce personne pour gérer les conflits entre deux individus se disputant la propriété d'une image. L'approche envisagée ici postule donc d'emblée l'existence de cette tierce personne et cherche à en tirer le meilleur parti.

Notre nouveau schéma repose sur la définition d'une empreinte qui soit à la fois dépendante de l'image et de son propriétaire (similairement à une fonction de hachage) tout en restant opérationnelle face à des manipulations de l'image.

Une empreinte externe est une information générée à partir d'une image et d'un ID utilisateur (logo) permettant de prouver par exemple la dépendance image-utilisateur (fig. 2). Le mot utilisateur est à prendre dans un sens générique et peut tout aussi bien signifier propriétaire de l'image, que couple vendeur-acheteur ou tout autre groupement d'individus impliqué dans la mise en place de services de sécurité appliqués aux images. Les empreintes sont archivées dans une base de données d'où le choix de la terminologie d'empreinte externe (à l'image). Il s'agit là d'une différence fondamentale par rapport aux systèmes de tatouage classique puisque, l'empreinte étant externe, la notion d'image tatouée devient caduque, seule l'image originale subsiste, excluant ainsi tout problème de visibilité. Afin qu'une empreinte externe puisse permettre la constitution d'une preuve de propriété du copyright pour régler les conflits entre deux tiers, elle doit présenter les

caractéristiques suivantes :

Dépendante de l'image : L'empreinte générée doit être fortement dépendante de l'image afin que la même empreinte ne soit pas engendrée pour deux images distinctes.

Dépendante de l'auteur : Elle doit être également fortement dépendante de l'auteur, pour assurer que deux entités différentes ne puissent de génèrer la même empreinte à partir d'une même image. Ou tout au moins que la probabilité d'y parvenir soit négligeable.

Robuste : Tout comme dans le schéma de tatouage « classique », l'empreinte doit permettre d'exhiber le logo identificateur, y compris après que l'image a subi des manipulations non-destructives.

2.1 Algorithme de génération de l'empreinte

Nous allons à présent décrire en détail l'algorithme d'empreinte externe (fig. 3) qui reprend en partie l'algorithme de tatouage présenté au chapitre 4.

Les entrées de l'algorithme sont :

- l'image originale ;
- le logo de l'utilisateur (user-ID), société ;
- une clé secrète associée à un dateur générant un signal pseudo-aléatoire.

Le nouvel algorithme diffère de celui-ci de tatouage classique par la suppression de la phase d'insertion dans l'image du tatouage mis en forme T_{sedbc}. En effet, dans l'algorithme initial, nous modifions l'image originale selon le critère de correspondance de signe entre l'information binaire T_{sedbc} que nous souhaitons dissimuler et l'image originale moins l'attracteur (cf. Chap. 4). Lorsqu'il y avait correspondance de signe, le pixel associé prenait la valeur du pixel original alors qu'en l'absence de correspondance, la valeur de ce pixel prenait la valeur de l'attracteur. Dans ce nouvel algorithme, cette dernière modification de l'image originale est supprimée au profit de la création d'une carte de correspondance de signe Emp. Cette carte binaire est obtenue en notant pour chaque pixel s'il satisfait au critère de correspondance de signe développé ci-dessus. Cette information de correspondance de signe que nous appelons carte des correspondances constitue l'empreinte externe qui est archivée dans une base de données et sera ré-utilisée lors de « l'extraction » de l'ID.

2.2 Algorithme d'extraction de l'ID à partir de l'image et de l'empreinte

Les entrées de l'algorithme sont :

- l'image dont l'on revendique le copyright ;
- l'E-ID identifiant l'empreinte attribué lors du dépôts de l'image ;

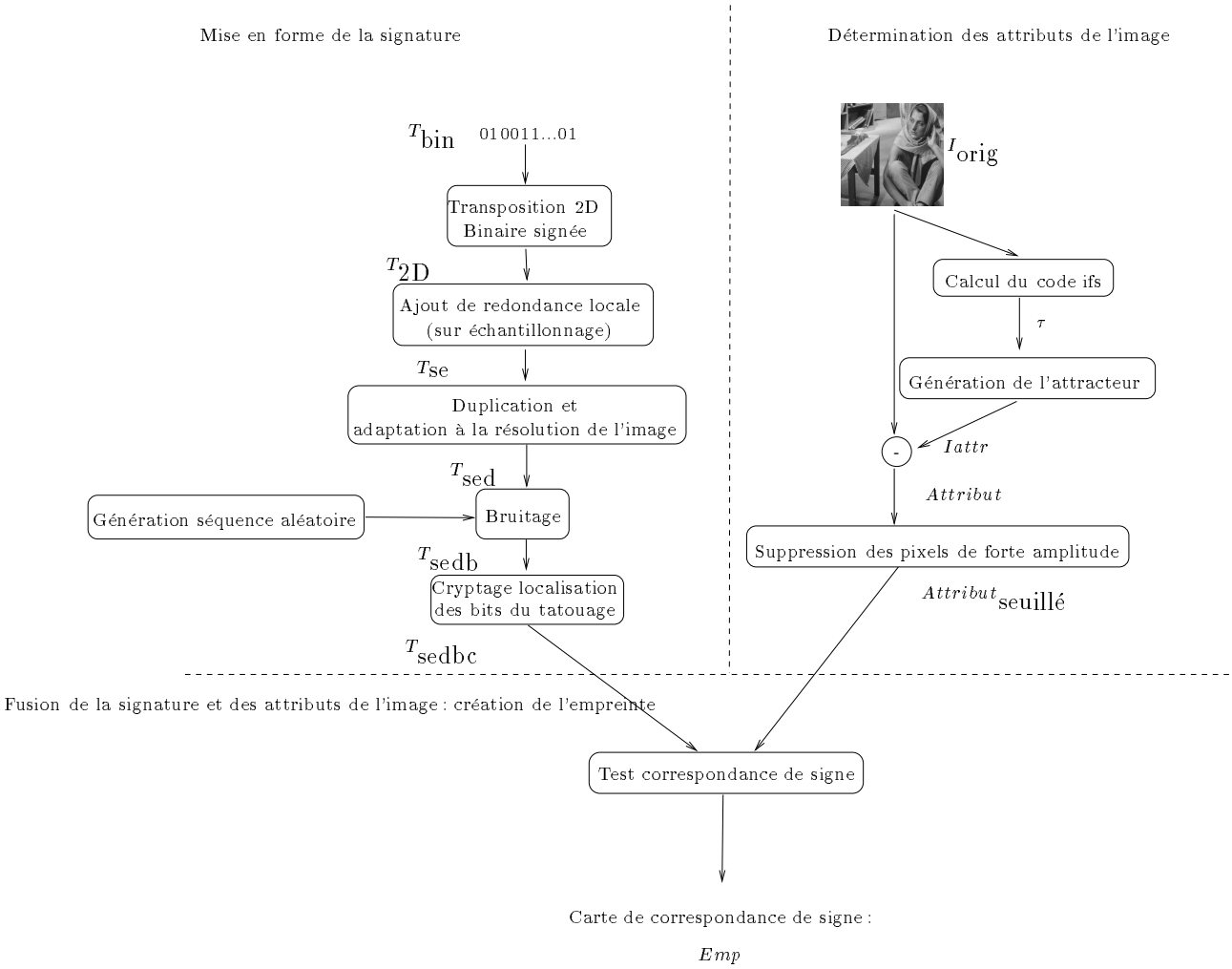


FIG. 3 – *Algorithme de création de l'empreinte*

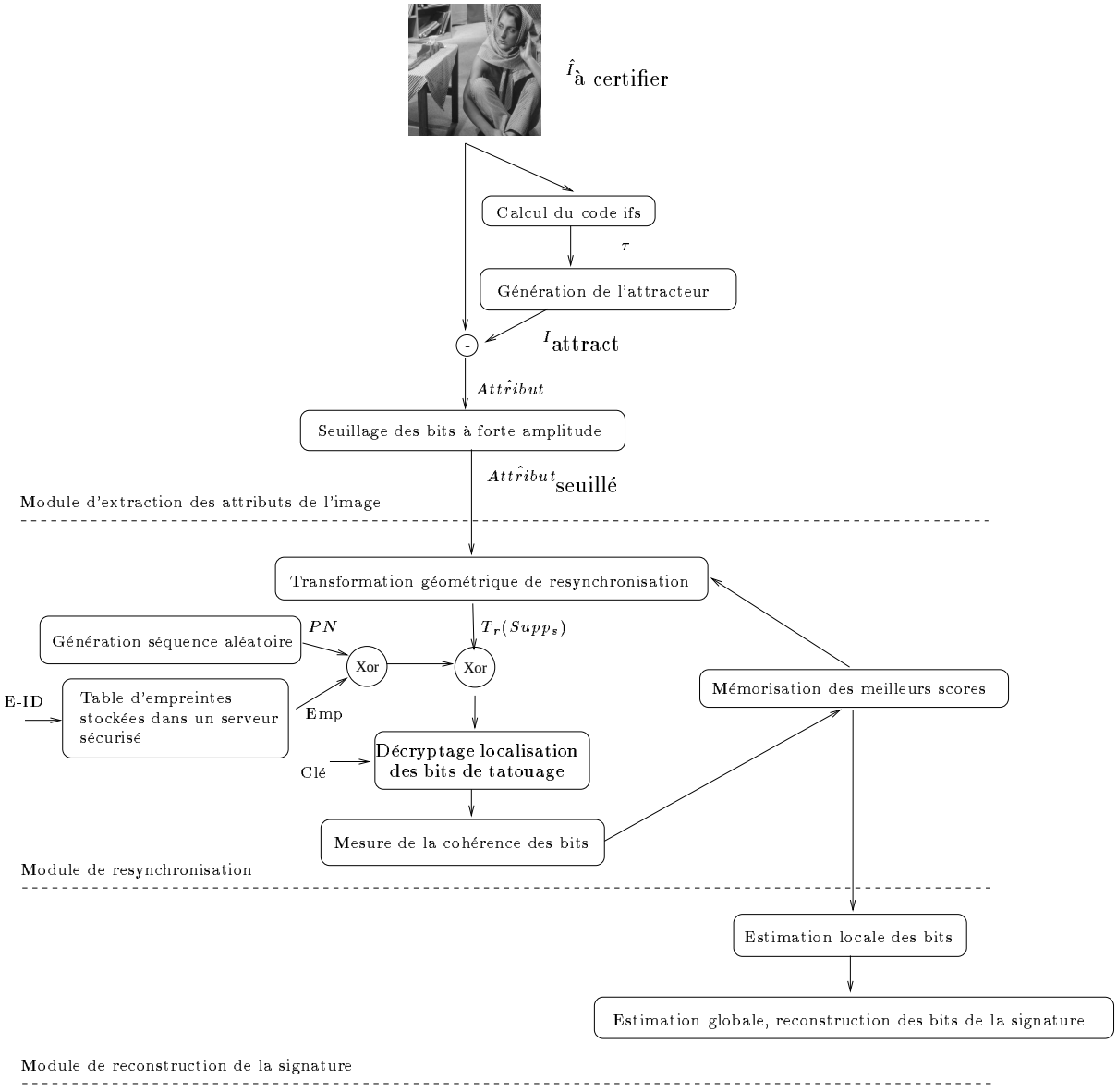


FIG. 4 – *Algorithme de vérification de l'empreinte*

- la clé secrète du générateur aléatoire donnant naissance au bruit PN attribuée lors du dépôt de l'image ;
- la clé secrète permettant de décrypter les positions du tatouage.

L'algorithme de vérification de l'ID (fig. 4) est très proche de celui décrit au chapitre 4. L'unique différence réside dans l'ajout d'une opération Xor réalisée entre l'empreinte enregistrée *Emp* et le signal PN issu du générateur aléatoire. Notons que l'utilisation du bruit PN est maintenue, bien qu'il perde sa fonction dédiée à la diminution de l'impact visuel du tatouage (suppression des motifs du tatouage) puisque la notion d'image tatouée a disparu et que seule subsiste l'image originale. PN demeure cependant nécessaire afin de garantir une équité de service entre les différents tatouages et donc les différents utilisateurs. Par rapport à l'algorithme initialement proposé où seulement un pixel sur deux en moyenne est porteur de l'information du tatouage (contrainte de correspondance de signe entre la marque binaire à introduire et l'image support), cette nouvelle opération permet de s'affranchir de cette limitation. Chaque pixel de l'image est maintenant pleinement porteur d'information et contribue à la reconstruction du logo, puisque l'empreinte rétablit la correspondance de signe si elle n'est pas présente initialement. La quantité d'information disponible pour reconstruire le logo est donc doublée ce qui bien entendu permet d'accroître considérablement la robustesse du système lors de manipulations de l'image.

3 Insertion de notre algorithme dans un protocole complet assurant la protection des droits d'auteurs

Comme mentionné au paragraphe 2, les protocoles font partie intégrantes de la méthode d'empreinte externe. Nous exposons ici les protocoles d'enregistrement et de vérification du copyright puis discutons les différentes options choisies.

3.1 Protocole d'enregistrement du copyright d'une image

Le protocole d'enregistrement (fig. 5) distingue trois phases :

- Une phase d'initialisation 1,2,3,4 au cours de laquelle, la personne désirant enregistrer un copyright sur une image prouve son identité,
- une phase de soumission des images à protéger 5,5',
- une phase au cours de laquelle le serveur notifie au propriétaire que l'opération de dépôt a été réalisée et lui fait parvenir les numéros d'identification des empreintes (E- ID) correspondant au dépôt de chacune des images 6,6'.

3.2 Protocole de vérification du copyright

Ce protocole (fig. 6) est très simple et ne nécessite pas de phase d'identification de l'utilisateur. Le demandeur communique simplement au serveur l'E-ID ainsi que l'image

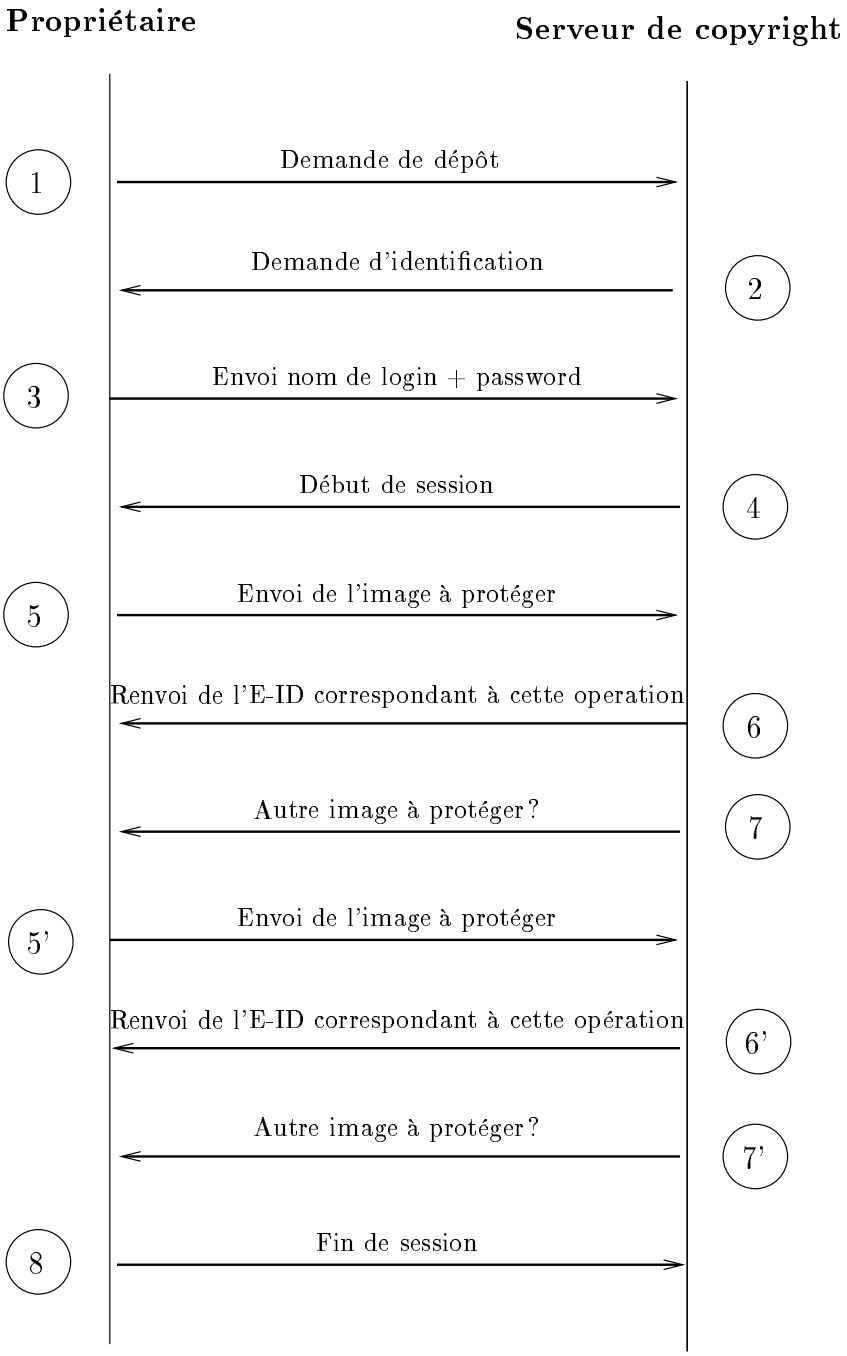


FIG. 5 – *Protocole d'enregistrement du copyright d'une image*

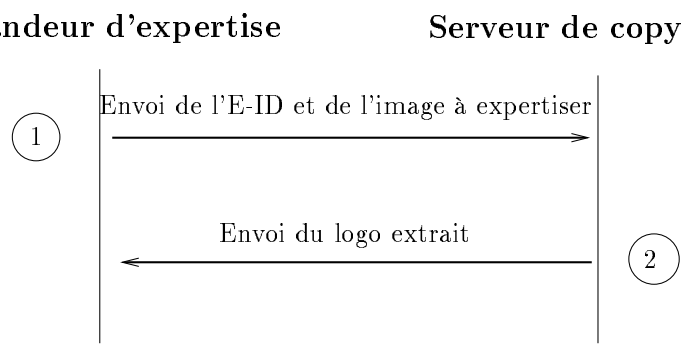


FIG. 6 – *Protocole de vérification du copyright d'une image*

pour laquelle il demande la vérification du copyright ; le serveur retourne alors le logo résultant de l'algorithme de vérification.

3.3 Justifications des choix effectués lors de la définition des protocoles

Mode « logger » lors du dépôt du copyright d'une image La phase d'enregistrement du copyright d'une image auprès du serveur est réalisée selon un mode de communication de type : « login + password » ; ceci permet :

- d'une part de se prémunir contre des dépôts de copyright illicites destinés à ternir l'image d'une société. Supposons par exemple qu'un individu dépose de façon anonyme le copyright d'une image dont il sait qu'elle a déjà fait l'objet d'un dépôt. Si la personne malveillante utilise lors de cette opération le logo d'une société qu'elle souhaite discréditer, cette dernière risque de se trouver impliquée à son insu.
- d'autre part, indépendamment des problèmes liés à la sécurité, la phase d'initialisation permet de gérer l'aspect facturation du service.

Présence de l'E-ID dans l'en-tête de l'image L'ajout de l'E-ID dans l'en-tête de l'image permet à n'importe quel utilisateur de vérifier le copyright de l'image qu'il souhaite acquérir. Notons que la falsification de l'E-ID n'entraîne aucun avantage pour une personne malveillante (cf. § 2.2 Chap. 6)

Non divulgation des empreintes, preuve indirecte Notons que les algorithmes décrits aux paragraphes 2.1 et 2.2 associés aux protocoles de dépôts et de vérifications sont exécutés dans un espace protégé (le serveur ou tierce personne) de telle sorte que l'empreinte générée ne soit jamais rendue publique, seul le serveur (tierce personne) est détenteur de cette information (fig. 2). Cette structure rend difficile la mise en place d'attaques de type : « à texte clair choisi ». En effet, une personne externe au serveur n'a aucun moyen d'observer les relations de dépendance entre une image et une empreinte, elle ne peut pas soumettre un ensemble d'images et observer les modifications des empreintes générées afin de tenter de casser l'algorithme.

La seule information retournée par le serveur est le logo (user-ID) or la correspondance : modification de l'empreinte, modification du logo extrait n'est absolument pas triviale du fait des mécanismes de très forte redondance impliqués dans cette relation, beaucoup de modifications de l'empreinte préservent le logo intact. On pourrait d'ailleurs envisager de retourner systématiquement le logo original (stocké dans la base de données) si le taux d'erreur du logo extrait n'est que de quelques pixels et une mire générique : document pas enregistré dans le cas contraire. Par un tel processus la relation : modification de l'empreinte, modification du logo extrait disparaît complètement pour une personne externe au serveur. La non divulgation des empreintes est rendue possible grâce à la mise en place d'un algorithme de vérification (dépendance utilisateur-image) fonctionnant dans un mode de preuve indirecte. En effet, le serveur utilise l'information contenue dans l'empreinte pour reconstruire l'user-ID (logo) à partir de l'image à expertiser ; et seul ce logo est exhibé pour attester de l'appartenance du copyright.

4 Evaluation de l'algorithme : un nouveau compromis robustesse / collision d'identification

L'une des approches pour discréditer la méthode consiste à créer des collisions afin d'alimenter une équivoque quant à la preuve apportée par l'empreinte externe. Avant de discuter le compromis robustesse / collision d'identification proprement dit, nous énumérons les différentes formes de collisions possibles.

1. Deux images distinctes, à partir d'une même empreinte génèrent un ID identique.

2. Une même image, à partir de deux empreintes différentes révèle le même ID.

3. Une même image, à partir de deux empreintes différentes révèle deux ID valides et distinctes.

Le premier type de collisions est dans une certaine mesure souhaitée puisqu'il garantit la robustesse de la méthode d'extraction même si l'image originale a subi des manipulations. Il faut néanmoins veiller à ce que deux images totalement différentes ne créent pas de collisions. On voit ici apparaître le nouveau compromis robustesse / collision d'identification qui malheureusement présente une part de subjectivité au même titre que le compromis robustesse / visibilité. En effet la notion d'images distinctes au sens sémantique est très délicate à définir et dépend de nombreux facteurs, en particulier du type d'images considérées et de l'utilisation qui en est faite. A ce délicat problème, nous nous contenterons d'apporter les précisions suivantes : la qualité de l'attracteur généré par le codage fractal donne une limite inférieure au delà de laquelle il n'est plus possible de retrouver l'ID puisque le support de celui-ci aura été intégralement supprimé. En conséquence, les paramètres du codeur IFS peuvent être utilisés pour ajuster le compromis robustesse / collision. Plus le codeur est de bonne qualité, plus les risques de collisions seront faibles mais moins la robustesse de ID sera assurée si l'on retouche l'image tatouée.

Examinons à présent les risques de collisions liées à deux empreintes distinctes. Nous devons envisager deux types d'attaques. Un premier constitué par une collision fortuite qui est très improbable étant donnée la combinatoire du système. Pour une image de taille donnée, nous pouvons paramétrer ce risque de collisions en augmentant ou en diminuant la taille de l'ID de sorte qu'il existe une correspondance plus ou moins biunivoque entre l'empreinte et l'ID. Plus cette correspondance se rapproche d'une bijection plus les risques de collisions sont faibles. Pour une image 512×512, la combinatoire est de $2^{512\times512} = 2^{262144}$! Encore une fois, le compromis robustesse / collision existe, nous préconnisons l'utilisation d'un ID binaire de 64×64 bits pour disposer d'un juste compromis. Concernant les attaques par collisions à enpreintes distinctes, nous avons également prêté attention à d'éventuelles attaques malveillantes qui par des tests successifs s'attacheraient à modifier l'image ou à chercher une empreinte pré-enregistrée tel que l'ID révèlé soit favorable au faussaire. Notre réponse face à ce type d'attaques consiste à la mise en place d'un procédé de preuve indirecte proposé au paragraphe 3.3 qui permet d'évacuer ce problème.

Abordons à présent le problème de la robustesse. Nous avons mené testé la pérénité du tatouage face à différentes manipulations de l'image tatouée. Les résultats de ces tests sont rapportés dans les tableaux 1 et 2. Ils comprennent : l'addition de bruit à l'image, le décalage de l'image (translation), l'extraction de région d'intérêt jusqu'à $\frac{1}{4}$ de la taille originale de l'image, une symétrie de l'image par rapport à l'axe médian vertical (effet miroir), le montage avec d'autres images ont été pratiqués pour évaluer la robustesse du système. Tous ces tests concluent à une extraction satisfaisante de l'ID.

5 Conclusion

Dans ce chapitre nous avons décrit une nouvelle approche pour assurer la protection des droits d'auteur sur des images. Cette nouvelle méthode transforme le compromis robustesse / visibilité en un compromis robustesse / collision d'identification. Au regard des expériences menées, le nouveau problème posé apparaît plus facile à résoudre. D'un part parce que la robustesse est considérablement accrue en supprimant la limitation de tatouage d'un pixel sur deux (correspondance de signe), d'autre part parce que les collisions d'identification sont peu probables étant donné la combinatoire du problème (taille d'empreinte suffisament grande). De plus,nous avons démontré que ce danger de collision face à des attaques intentionnelles peut être considérablement amoindri si l'accès à l'empreinte n'est autorisé qu'au travers une table via un identifiant (E_ID). Une discussion approfondie sur les potentialités comparées des méthodes par empreinte externe et par tatouage classique est menée au chapitre suivant.

Attaque	**Type d'identificateur**	**Type d'image**	**Identificateur extrait**
Jpeg Q40%	ascii : "Eurecom"	Lena 512×512, 256 niveaux de gris	"Eurecom"
Jpeg Q40%	ascii : "IEEE"	US Airforce jet 512×512, couleur 24 bits	« IEEE »
Petite rotation 0.7 degré	ascii : "Lena"	Lena 512×512, 256 niveaux de gris	"Lena"
Translation horizontale de 7 pixels	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Recadrage 50%	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Effet miroire	Logo binaire : Eurecom 4096 bits	Fruit 512×512, couleur 24 bits	Logo intégralement récupéré
Etirement horizontal 105 %	séquence aléatoire 900 bits	House 256×256, couleur 24 bits	100 % bits récupérés
Inclinaison verticale 1 degré	séquence aléatoire 900 bits	House 256×256, couleur 24 bits	100 % bits récupérés
Imprimer & Scanner couleurs 600dpi	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »
Imprimer & Scanner niveaux de gris 1200 dpi	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »
conversion RAW2GIF	séquence aléatoire 900 bits	Fruit 512×512, couleur 24 bits	92 % bits récupérés
Unzign cracker	ascii : "Eurecom"	US Airforce jet 512×512, couleur 24 bits	« Eurecom »
Stirmark cracker	ascii : "Eurecom"	Fruit 512×512, couleur 24 bits	« Eurecom »
Double itération de Stirmark	ascii : "Eurecom"	Airplane 512×512, couleur 24 bits	« Eurecom »

TAB. 1 – *Exemples de tests de robustesse de l'algorithme d'empreinte externe face à diverses manipulations de l'image.*

	PSNR	récupéré succès
image tatouée / image tatouée, compressée Jpeg Q75	39.46	100%
image tatouée / image tatouée, compressée Jpeg Q65	38.44	100%
image tatouée / image tatouée, compressée Jpeg Q55	37.63	100%
image tatouée / image tatouée, compressée Jpeg Q45	36.95	100%
image tatouée / image tatouée, compressée Jpeg Q35	36.08	99%
image tatouée / image tatouée, compressée Jpeg Q25	34.82	98%
image tatouée / image tatouée, compressée Jpeg Q15	32.81	95%
image tatouée / image tatouée, compressée Jpeg Q10	32.81	94%
image tatouée / image tatouée, compressée Jpeg Q5	27.97	92%

TAB. 2 – *Résistance de l'identificateur face à des niveaux croissants de compression JPEG. (Les tests présentés ont été réalisés sur l'image Peppers).*

Chapitre 6

Application aux services de sécurité des algorithmes de tatouage et d'empreinte externe : une étude comparative

La dissimulation d'une information dans une image peut être utile dans un grand nombre d'applications. Les recherches en tatouage ont été initiées pour résoudre les droits de propriété d'oeuvres multimedia et en particulier d'image ; nous sommes ici placés dans le cadre d'oeuvres publiques, pour lesquelles, l'auteur souhaite simplement être reconnu. A contrario, une demande existe pour assurer la sécurité d'oeuvres multimedia dont la diffusion s'adresse à un nombre d'individus limités et clairement identifiés. Les techniques de tatouage interviennent ici afin de déceler un utilisateur tentant de rediffuser le document qui lui a été remis. La troisième application majeure du tatouage est constituée par la vérification de l'intégrité d'un document. Le tatouage robuste inséré dans l'image joue le rôle de référence par rapport à laquelle on va pouvoir la comparer. L'image est ainsi auto-protégée.

1 Critiques de la méthode par empreinte externe, comparativement à une approche par tatouage ou autre stratégie

1.1 Avantages sur les techniques de tatouage

Impact du système de copyright sur la qualité du document

Le principal reproche fait aux techniques de « watermarking » concerne leur inefficacité à résoudre le compromis robustesse / visibilité inhérent à ces approches. Une question concernant la faisabilité même du « watermarking » reste d'ailleurs ouverte. En effet, est-il possible de modifier une image en insérant une information sans que :

- cette opération soit visible,
- personne ne puisse effectuer une autre opération d'insertion (toujours non perceptible) qui rendrait la récupération de l'information dissimulée impossible ?

En d'autres termes, quelle « supériorité » a la personne créant un tatouage sur un éventuel pirate pour dissimuler une information dans une image ? La plupart des algorithmes présentant un niveau minimum de robustesse acquièrent cette robustesse au prix d'une dégradation notable de la qualité du document. Dans notre approche, la notion de dégradation tolérable de l'image (qui par ailleurs est très subjective et par conséquent difficile à définir analytiquement) disparaît puisqu'il n'y a qu'un seul document mis en circulation : l'image originale.

Double archivage

A partir de l'image originale, les systèmes de watermarking créent un deuxième document (l'image signée) qu'ils mettent en circulation. Même pour les techniques ne nécessitant pas le document original lors de la phase de vérification, il apparaît peu probable que le propriétaire détruise le document original. Dans ces conditions, il est nécessaire de mettre en place un double archivage : image originale et image signée. Cette discussion est caduque dans notre système puisqu'il ne subsiste qu'un seul document : l'image originale.

Entité certificatrice

Pour résoudre les conflits liés aux attaques par multi-signatures, les analyses convergent et on s'accorde à penser qu'il n'est pas possible de faire l'économie d'une entité certificatrice afin de dater le dépôt du copyright, cette entité devant de plus conserver la trace de chaque dépôt. Dans ces conditions, la présence dans notre schéma d'une entité dédiée à la gestion de la base de données des marques ne peut être considérée comme un surcoût inhérent à notre méthode, dès lors que l'on souhaite remédier aux problèmes de sur-signatures.

Accès des utilisateurs à l'information redondante

Pour garantir un niveau de robustesse élevé du tatouage face à des manipulations de l'image, toutes les techniques de tatouage sont contraintes d'ajouter une redondance très importante au niveau du tatouage. Ceci est contraire aux principes de sécurité élémentaire énoncés par Shannon qui stipulent que : « la sécurité est inversement proportionnelle à la redondance du message » . Notre algorithme s'affranchit de ces problèmes car l'information redondante (assurant la robustesse) n'est en aucun cas laissée accessible aux utilisateurs (l'empreinte est locale au serveur), (cf. § 3.3 Chap. 5).

1.2 Avantages sur l'enregistrement du document original lui-même

Dans ce paragraphe, nous présentons les avantages que peut présenter l'approche proposée par rapport à une approche plus classique qui consisterait simplement à déposer directement, auprès d'un organisme de certification, le document (i.e. l'image) lui-même.

Quantité d'informations à archiver

Si l'on considère que le propriétaire souhaite déposer une image couleur 24-bits, cette approche permet au certificateur de conserver uniquement une empreinte binaire (définie en fonction de l'image et du propriétaire), plus éventuellement une clé secrète, soit dans ce cas précis 24 fois moins d'informations.

Procédures d'enregistrement et de récupérations automatiques

La procédure proposée permet de traiter de manière numérique et automatique les différentes phases du processus de certification et de communication : dépôt, génération d'une clé, récupération,... Par rapport à une approche dite classique : d'enregistrement de document, d'arbitrage,... la procédure proposée permet de traiter de manière rapide (voire quasi immédiate), efficace et fiable une masse importante de documents à un coût donc (sans doute) très faible.

Critères objectifs

Si le document original a été modifié, sans la procédure proposée dans ce document, le certificateur devra alors de manière subjective comparer deux documents dont un original remis précédemment par le propriétaire et archivé par le certificateur, avec un second document identique, ou éventuellement manipulé. Si les personnes concernées par l'arbitrage sont toutes de bonne foi (i.e. demande d'information par ex.) un jugement subjectif du certificateur sera sans doute suffisant. Par contre, si certaines des personnes concernées sont de mauvaise foi, ont réalisé des opérations « complexes » sur le second document, revendiquent des droits sur le document, il sera difficile, sur la base d'un critère subjectif de similarité visuelle, de faire valoir les droits du propriétaire sans s'exposer à des polémiques ou de longues procédures. Entre autres, s'agissant de documents numériques, on peut tout à fait concevoir que les personnes souhaitent qu'on leur présente des preuves objectives et quantitatives. Or, les techniques actuelles ne permettent pas d'établir un

lien analytique entre images proches au sens visuel et proches au sens numérique, sans utiliser une procédure préalable comme celle décrite dans ce document (i.e. génération d'une marque datée, propre au couple document-propriétaire).

1.3 Limites de l'application de l'empreinte externe

Bien que la robustesse de l'empreinte externe face à des manipulations de l'image soit bien supérieure à celle du tatouage, ce dernier conserve un intéret pour résoudre certains problèmes pour lesquels l'empreinte externe est inopérante. Considérons par exemple, l'ensemble des applications où l'on souhaite mettre en circulation différentes versions d'une même image. On peut rapprocher ce cas de figure de la notion de licence dans le domaine du logiciel informatique. Chaque utilisateur ou groupe d'utilisateurs dispose de son propre numéro de licence. Il est alors possible de tracer d'éventuelles versions délictueuses d'un logiciel et de remonter à la source de la fuite. Il est clair que notre système ne peut pas être utilisé dans ce contexte dans la mesure où l'on ne différencie pas plusieurs versions de l'image.

2 Comment l'empreinte externe peut répondre à différents scénarii dans le contexte de la protection du copyright

2.1 Conflit direct entre deux individus

Le propriétaire de l'image qui a pris soin de faire enregistrer son copyright auprès du serveur de certification, «demande» à ce serveur d'exécuter l'algorithme de certification en lui fournissant l'image pour laquelle il existe un conflit ainsi que l'E-ID qu'il a reçu lors du dépôt de cette image. Si la personne a effectivement déposé l'image comme elle le prétend, le serveur le confirmera en exhibant le logo de la personne et la date de dépôt.

2.2 Vérification du copyright d'une image par un individu quelconque

A partir de l'E-ID présent dans l'en-tête de l'image, n'importe quel individu peut s'assurer auprès du serveur que le copyright appartient effectivement à la personne qui le prétend. Notons qu'une personne malveillante n'a aucun intérêt à falsifier l'E-ID, car la vérification d'un copyright avec un E-ID corrompu ne donne aucun résultat ce qui alerte sur l'origine douteuse de l'image, de plus, de par la structure du schéma (l'empreinte de copyright reste secrète) il n'est en aucun cas capable de fabriquer un E-ID susceptible de révéler son propre logo en utilisant l'empreinte d'une image qu'il aurait préalablement déposée.

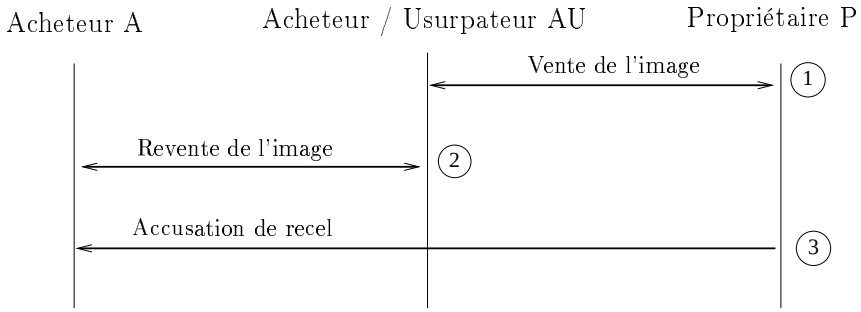


FIG. 1 – *Cas conflictuel d'un acheteur victime d'un usurpateur*

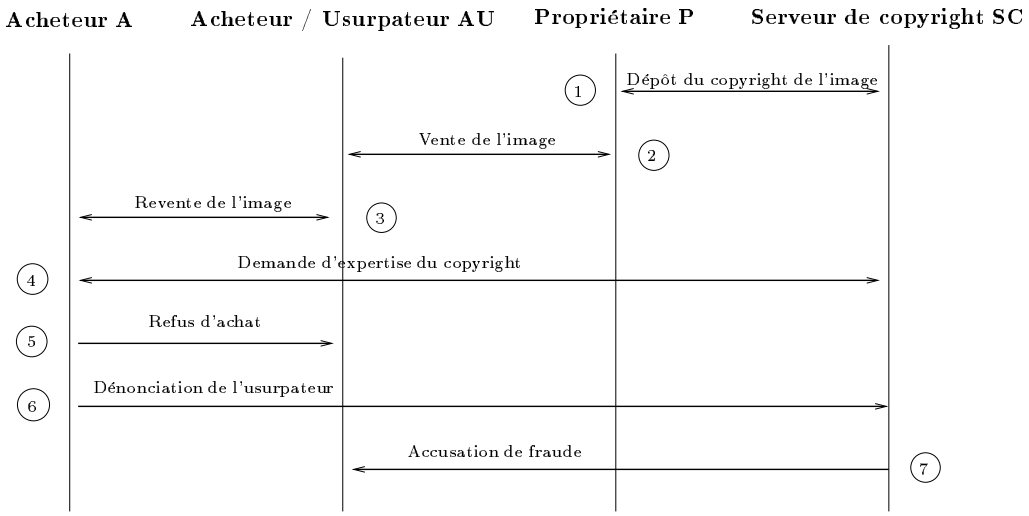


FIG. 2 – *Résolution du conflit si seul P a protégé l'image*

2.3 Echec à la mise en place de réseaux de ventes parallèles et recèles

Tout acheteur de document multimédia souhaite obtenir des garanties sur la provenance du document qu'il souhaite acquérir afin notamment d'être en mesure de se défendre contre d'éventuelles accusations de recèles. La figure 1 constitue un exemple simple dans lequel un acheteur de bonne foi « A » est victime d'un réseau de vente parallèle « AU » et est accusé de recèle par le propriétaire légitime « P ». Le précédent conflit peut être résolu si le propriétaire légitime P a pris soin d'enregistrer son image auprès du serveur de copyright {étape 1}. Lorsque l'acheteur A désire effectuer un achat auprès de AU, il peut s'assurer au préalable de la validité du copyright en transmettant une requête d'authentification auprès du serveur de copyright {étape 4}. Lors de cette requête, A communique au serveur l'E-ID présent dans l'en-tête de l'image. Si l'E-ID a été modifié par AU, le serveur n'exhibera aucun logo et l'image sera qualifiée de « douteuse ». Si l'E-ID est laissé intact, le logo exhibé sera celui du propriétaire légitime P et AU sera donc confondu. Considérons maintenant le cas où AU a sur-signé l'image {étape 3} et placé un nouvel

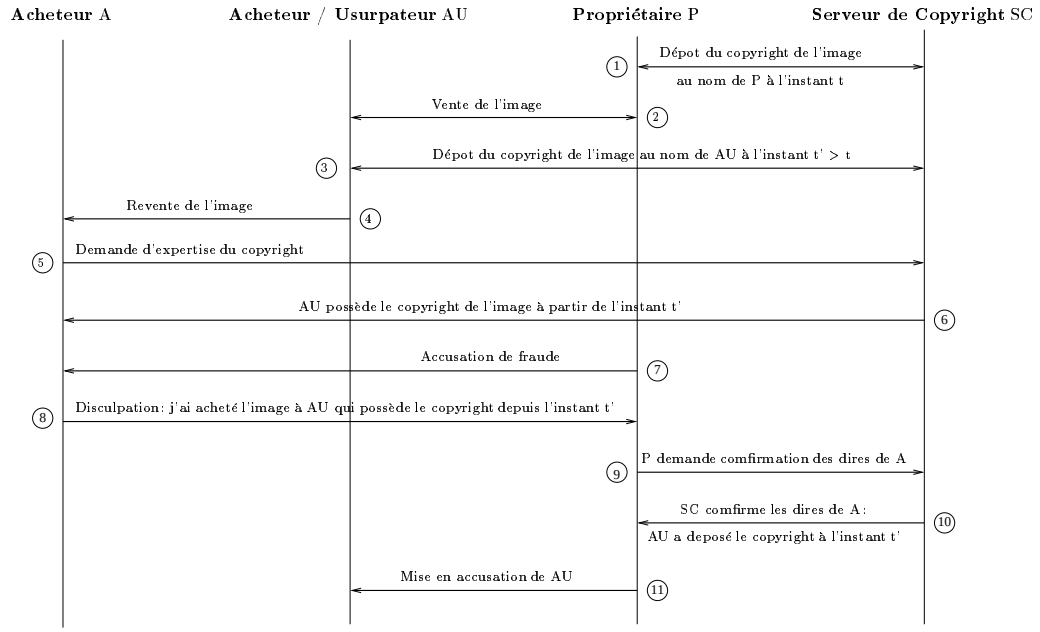


FIG. 3 – *Résolution du conflit si AU a également protégé l'image*

identificateur E-ID' dans l'en-tête de l'image. A qui demande une expertise du copyright de l'image en communiquant au serveur l'E-ID' recevra en réponse que AU a déposé le copyright à compter de la date t'. A se trouve alors en position d'être accusé de fraude par le propriétaire légitime P {étape 7}. Cependant A peut facilement se disculper et prouver son bon droit en montrant à P que l'image lui a été vendue par AU qui prétendait posséder le copyright de cette image {étape 8}. Le propriétaire légitime P se retournera alors contre AU et montrera qu'il possède le copyright depuis la date t avec t <t'.

3 Notariat électronique par empreinte externe

Nous pouvons d'ores et déjà envisager de rendre l'empreinte dépendante de la personne ou de l'ensemble des personnes à qui l'image a été transmise. D'une façon plus générale, l'empreinte peut servir à certifier le canal par lequel l'image a été transmise. Cette empreinte sera donc dépendante du propriétaire, de l'image, d'un ou plusieurs clients, ou encore du moyen de diffusion utilisé. A partir de là, de multiples combinaisons, autres que (propriétaire, image) peuvent être envisagées comme (propriétaire, image, client) ou (image, client), ou bien encore (propriétaire, image, support de diffusion/acquisition) et par voie de conséquence remplir d'autres fonctionnalités de sécurité que celles précitées. En particulier, le développement du commerce électronique pose de nouveaux problèmes pour la gestion des contrats en l'absence de documents papiers attestant des transactions. Dans ce contexte il est intéressant de réfléchir à des applications capables de gérer ce nouveau type de transactions et de jouer implicitement le rôle de notaire électronique (fig. 4). Le concept de notariat électronique implique que les entités ne puissent nier avoir effectué une transaction avec telles et telles clauses dans le contrat. Le contrat peut conte-

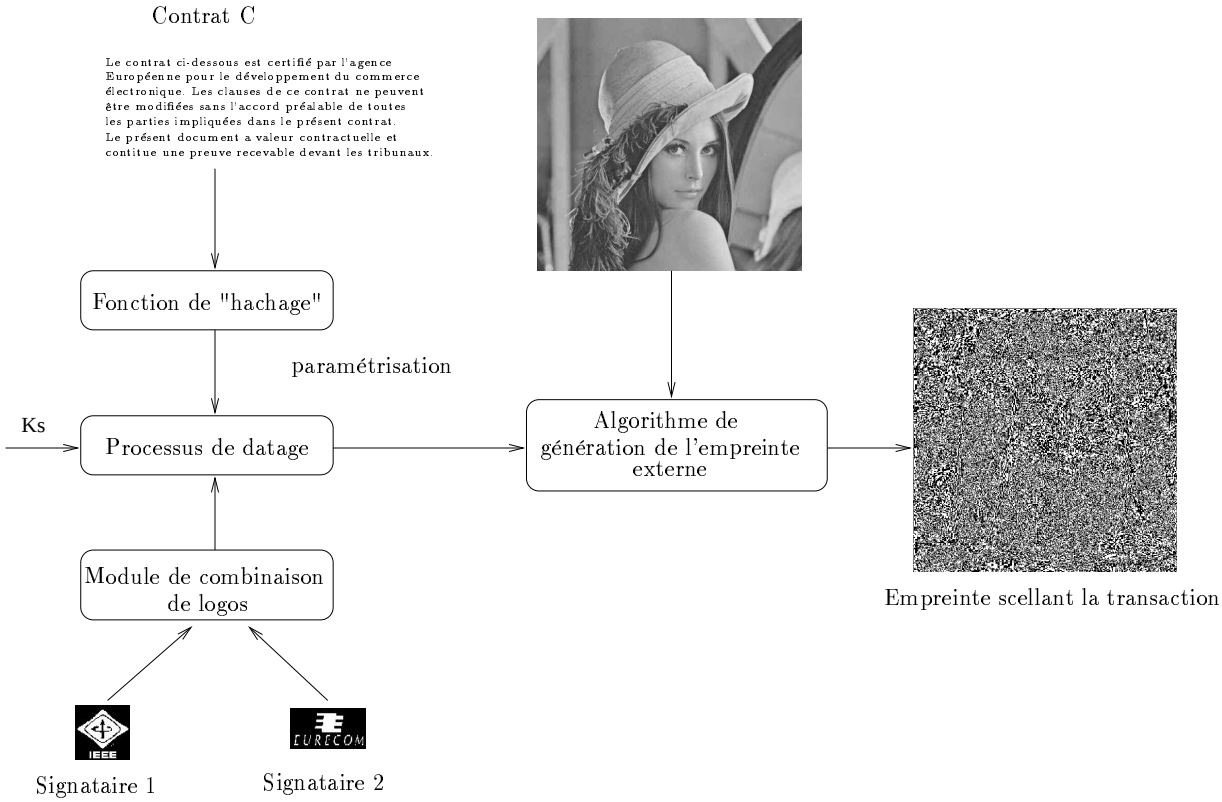


FIG. 4 – *Signature de contract électronique pour l'achat d'une image*

nir des clauses de divulgation de l'image du type : utilisation privée uniquement, droit de diffusion mais non monnayable, droit de vente de l'image etc. En termes de sécurité, le notariat électronique s'apparente à la mise en place de mécanismes de non-répudiation. Dans notre système, ils reposent :

- d'une part sur le fait que l'accès au serveur pour le dépôt de document se fait en mode « loggé » avec un processus d'identification par mot de passe par exemple,

- d'autre part sur la garantie que l'empreinte ne peut être prédite par une personne extérieure au serveur de sorte qu'il ne peut y avoir ambiguïté. Une personne malveillante ne peut pas corrompre un E-ID dans le but d'utiliser une empreinte déjà présente dans la base de données et qui pourrait à tort mettre en cause une personne.

Dans le schéma ci-dessus, le contrat est approuvé par les deux parties par un processus de va-et-vient via le serveur qui authentifie ainsi que les deux parties ont bien pris connaissance des termes du contrat. A l'issue de la signature du contrat, les deux parties qui possèdent chacune le même E-ID (retourné par le serveur) peuvent à tout moment prouver que le contrat C a été signé en communiquant au serveur, le présent contrat, l'image sur lequel porte le contrat et l'E-ID ; le serveur exhibera alors le logo mixte (IEEE, Eurecom dans notre exemple) si le contrat a effectivement été passé.

4 Service d'intégrité par tatouage d'image

Nous présentons dans cette partie de la thèse des résultats préliminaires concernant le service d'intégrité tel qu'il a été introduit au chapitre 2. Nous considérons les deux options pouvant conduire à protéger l'intégrité d'une image grâce à son tatouage et étudions le comportement de notre algorithme de tatouage pour ces deux approches [24, 80, 5].

4.1 Service d'intégrité par tatouage fragile

La difficulté et la qualité de reconstruction du tatouage peuvent constituer un indicateur sur le niveau de modification de l'image. On constate par exemple que l'ensemble des dégradations « bienveillantes » résultant d'une phase de compression se répartit plus ou moins uniformément dans l'image alors que les dégradations malveillantes, montage d'image par exemple se caractérisent par une dégradation locale très forte. Nous proposons donc d'adapter l'algorithme de tatouage développé pour la protection des droits d'auteur afin d'analyser la fragilité du tatouage et ainsi repérer les zones manipulées. Contrairement au contexte de protection du copyright, nous considérons ici que le tatouage est connu a priori, il s'agit non plus d'un identifiant de propriété mais d'une mire de référence. Avant élimination de la redondance, l'algorithme de tatouage extrait trois types d'information :

- les points conformes à la valeur attendue de la mire ;
- les points résolument faux ;
- les points indécis pour lesquels on ne peut rien affirmer.

La proportion locale de ces différents types de point doit permettre d'analyser l'image. Par exemple, si l'image à été retouchée, les points résolument faux seront majoritaires. Différents paramètres influencent la prise de décisions. Tout d'abord les seuils fixant à partir de quels taux de points exactes, erronés ou indécis, une région donnée est validée ou rejetée. Un deuxième paramètre a considérer est la taille des fenêtres de décision, c'est à dire le nombre de pixels que l'on va considérer pour faire l'analyse locale de l'image. Plus ce nombre est grand plus le seuil de fausse alarme (détection d'une région erronée alors qu'elle était effectivement intègre) sera bas. Cependant des fenêtres de décision de grande taille ne permettent pas d'avoir une résolution précise sur la région manipulée ; de plus une manipulation très locale mais néanmoins de première importance comme la modification des caractères indiquant le copyright de l'image, risque de ne pas être détectée. Nos premiers tests ont conclu qu'une fenêtre de dimension 8×8 pixels est optimale.

4.2 Service d'intégrité par contrôle d'attributs de l'image

Nous rappelons que cette approche consiste à dissimuler sous la forme d'un tatouage des attributs caractéristiques de l'image et non plus une mire de référence comme dans l'approche précédente. La vérification de l'intégrité de l'image s'effectue en contrôlant la conformité des attributs recalculés à partir de l'image reçue par rapport à ceux figurant dans le tatouage. Les problèmes pour mettre en place cette approche sont assez similaires à

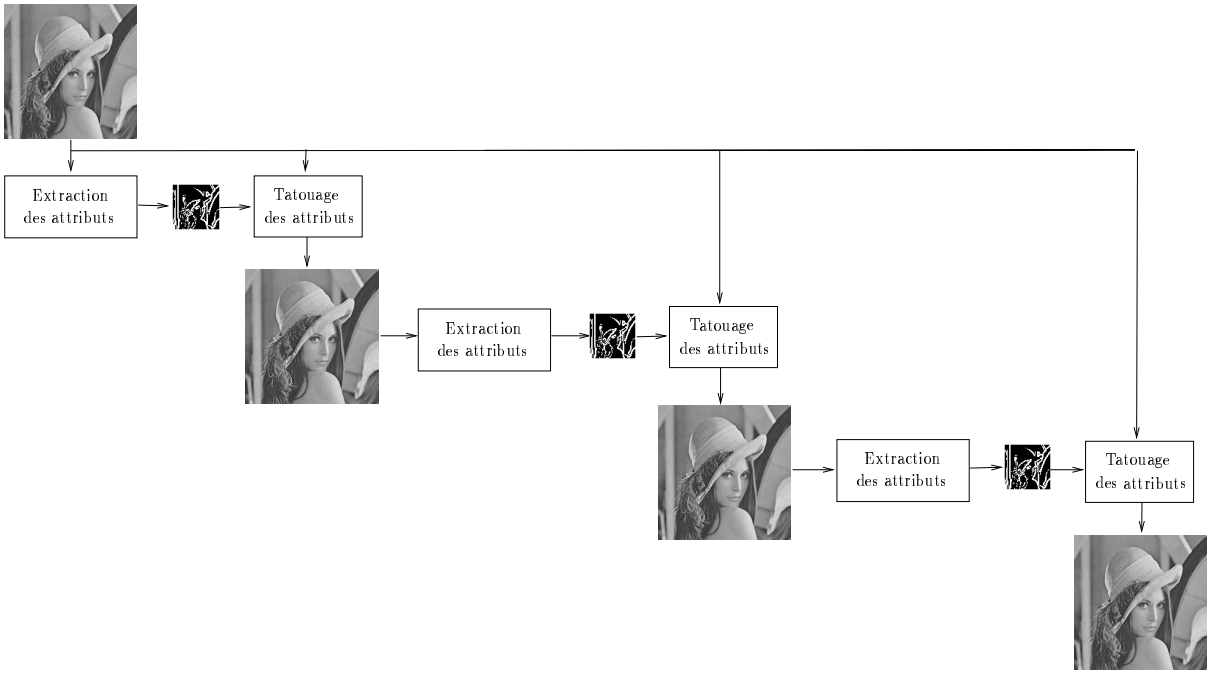


FIG. 5 – *Tatouage itératif d'attribut de l'image*

ceux rencontrés dans les problèmes de droit d'auteur car il faut impérativement disposer d'un tatouage robustesse la contrainte de capacité de tatouage élevée est primordiale. En effet pour dissimuler des attributs binaires significatifs il est souhaitable de disposer d'un tatouage binaire dont la taille minimum est de 64 par 64 pixels. Dans la méthode proposée, nous avons implicitement fait l'hypothèse que les attributs extraits à partir de l'image originale (constituant le tatouage) et ceux extraits à partir de l'image tatouée (utilisés pour la vérification) sont identiques. Cette hypothèse est motivée par le fait que l'image originale et l'image tatouée sont proches sur le plan visuel. Même si cette hypothèse reste grossièrement vérifiée au niveau numérique, il est possible d'améliorer de façon significative la méthode en proposant un tatouage itératif (fig. 5). Le procédé consiste à effectuer un premier tatouage en considérant les attributs calculés à partir de l'image originale, puis à calculer de nouveaux attributs à partir de l'image venant d'être tatouée. Ces nouveaux attributs sont alors utilisés pour tatouer l'image originale. On constate que pour cette seconde image tatouée les attributs insérés et ceux recalculés à partir de l'image sont plus proches que lors du tatouage initial. Pratiquement à la suite de quelques itérations (généralement trois) les attributs contenus dans le tatouage et ceux extraits à partir de l'image tatouée deviennent identiques. La figure 6 est un exemple de résultats obtenus avec cette méthode.

FIG. 6 – *Résultats d'intégrité par tatouage :*
a) image originale ; b) image tatouée ;
c) image attaquée ; c) détection des attaques.

5 Conclusion

Dans ce chapitre, nous avons donné un aperçu des applications possibles des algorithmes de tatouage et d'empreinte externe développés au cours de cette thèse. Une étude parallèle entre ces deux techniques a montré que l'empreinte externe est plus favorable pour résoudre les problèmes de copyright malgré les contraintes que nécessite la maintenance permanente d'un serveur. En outre, ce type d'environnement (serveur) est très favorable par exemple pour gérer des contracts et constituer ainsi un notaire électronique. Les différents scénarii d'attaques étudiés plaident en faveur d'un environnement de sécurité global intégrant des protocoles pour faire échec à une apropriation illicite d'une image. Malgré les nombreux avantages qui motivent un recours à la technique d'empreinte externe, le tatouage d'image classique présente encore un intérêt, en particulier pour gérer un service d'intégrité ou lorsqu'il n'est pas envisageable de recourir à un serveur. Dans ce dernier cas, une technique de tatouage couplée à une protection physique peut constituer une solution.

Chapitre 7

Conclusions et Perspectives

Dans ce chapitre, nous apportons une conclusion à nos travaux tant concernant le contrôle d'accès que le tatouage et l'empreinte externe. Nous tenterons également de dégager les différentes voies qui pourraient avantageusement être explorées pour d'une part améliorer les services existant d'autre part en proposer de nouveaux.

1 Conclusions

Partis des techniques de stégonographie définissant la façon d'assurer la confidentialité d'un message en le dissimulant dans un autre message, les techniques de tatouage se sont d'abord focalisées sur les problèmes de dégradation du media liés à l'ajout d'une information supplémentaire. Les progrès se sont ensuite portés dans l'intégration progressive de critères de robustesse. La multiplicité des manipulations possibles nous incite d'ailleurs à penser que cette quête est loin d'être terminée. Au fur et à mesure que les systèmes de tatouage deviennent crédibles sur le plan de la robustesse du tatouage face à des manipulations des images ainsi que du point de vue de l'invisibilité, de nouvelles préoccupations directement liées à l'application visée apparaissent. Il s'agit principalement des problèmes de protocole qui ont été totalement occultés dans les premières recherches. Sur un plan juridique que se passe-t-il si les images piratées sont hébergées sur un serveur domicilié dans un pays qui n'a pas signé les accords internationnaux sur le copyright ? Malgré les réserves mentionnées précédemment, les techniques de tatouage commencent à faire partie intégrante des fonctionnalités des nouveaux produits (DVD, Photoshop etc) et sont inscrites au cahier des charges des futurs standards de codage d'image ou de vidéo (Jpeg-2000, Mpeg-4).

Au cours de cette thèse, nous avons proposé deux approches dans le but d'assurer des services de sécurité à des images, la première est,

sur la base de simulations, une étude de la robustesse des deux approches a été réalisée, notamment face aux outils de test que sont Stirmark et Unzign sur lesquels butent tous les schémas commercialisés à l'heure actuelle.

Une analyse des protocoles liés à la mise en place des deux applications phares du tatouage d'image que sont actuellement la protection du copyright et l'intégrité a été conduite. La conclusion principale de cette analyse est que contrairement aux premiers systèmes envisagés où l'on mentionnait uniquement la présence de deux protagonistes (le propriétaire de l'image et un imposteur) nous sommes convaincus qu'il est nécessaire d'avoir recours à une tierce personne au moins pour le service de protection du copyright.

2 Perspectives

2.1 Algorithmes capables d'intégrer de nouvelles attaques

Etant donnée la multiplicité des attaques pouvant être mise en oeuvre sur des images, il est fort probable que, quel que soit le soin apporté à la conception du système de tatouage, ce système sera un jour pris en défaut. Il serait donc intéressant, faute de pouvoir devancer cette attaque, de concevoir un algorithme capable d'intégrer de nouvelles attaques *a posteriori*. Par exemple, s'il s'agit d'une nouvelle attaque géométrique, le modèle de transformée géométrique pourrait être enrichi en évaluant une correspondance entre l'image tatouée attaquée et l'image tatouée initiale.

2.2 Tatouage à résistance aléatoire

Constituer une preuve irréfutable de l'usurpation de droit d'auteur peut discréditer gravement une société ou un individu et ainsi lui être préjudiciable. Il peut donc être intéressant de proposer un système « jouant » sur la peur d'être pris même s'il ne peut garantir un succès de façon systèmatique. En effet, nous avons mis en évidence la difficulté de concevoir un système permettant de résister à l'ensemble des attaques simultanément. Cependant, on pourrait donc imaginer un algorithme sélectionnant aléatoirement les attaques pour lesquelles il serait robuste. De telle sorte, on crée un doute chez l'usurpateur potentiel qui ne souhaitera pas encourir le risque d'être démasqué.

2.3 Intégrité

Les premiers résultats obtenus dans le cadre de l'intégrité des images ne sont pas entièrement satisfaisants. Nous parvenons à détecter et localiser des régions ayant fait l'objet d'un montage mais la sensibilité de notre système est encore trop importante pour accepter une compression Jpeg faible (Qualité $>75\%$) de l'image sans détecter des malversations. En effet certes le tatouage est robuste pour ces facteurs de compression, cependant les caractèristiques de l'image sont elles-même affectées. Les prochaines études devront donc à la fois accroître la robustesse du système face à une compression Jpeg tout en préservant la capacité de détecter et localiser des attaques modifiant le contenu de l'image. On peut penser qu'il sera nécessaire de combiner plusieurs attributs de l'image déjà étudiés individuellement par exemple les contours et la moyenne. Etant donnée la complémentarité de ces attributs, il est envisageable de les discrétiser plus largement de façon à ne conserver pour chacun d'eux que l'information essentielle qu'ils caractérisent au mieux.

2.4 Extension à la vidéo et à d'autres media

Dans le cadre du contrôle d'accès, nous avons montré la possibilité d'étendre à la vidéo les algorithmes développés sur image fixe en considérant des cubes comme primitive de base en remplacement des blocs. Une approche similaire est envisageable pour adapter nos algorithmes de tatouage ou d'empreinte externe, cependant, cette extension devra prendre en compte de nouveaux critères psychovisuels adaptés à la dimension temporelle de la vidéo, de plus, si le tatouage en temps réel est requis, une maîtrise du coût calculatoire du codage fractal sera nécessaire. Pour les autres données numériques, en particulier pour le signal audio, il est nécessaire d'une part d'étudier précisément les manipulations et attaques propres à chaque type de media, d'autre part de définir un dictionnaire de codage satisfaisant simultanément les contraines psycho-acoustiques et la robustesse de la marque.

Annexe A

Images extraites des simulations sur l'algorithme de tatouage

Cette annexe vient en complément de l'évalution numérique de l'algorithme de tatouage réalisée au chapitre 4. Sous réserve de la qualité d'impression du présent document, sur la base d'exemples réels, cette annexe donne une idée de l'impact du tatouage sur la qualité de l'image. Nous donnons également quelques exemples représentatifs des attaques pour lesquelles notre algorithme est robuste.

1 Images originales et images tatouées

a)

b)

Image originale House et la version tatouée avec une séquence aléatoire de 900 bits.

a)

b)

Image originale Lena et la version tatouée avec la chaîne de caractères ASCII Eurecom.

a)

b)

Image originale Us Air Force et la version tatouée avec la chaîne de caractères ASCII IEEE.

a)

b)

Image originale Fruits et la version tatouée avec la chaîne de caractères ASCII IEEE.

2 Résistance du tatouage face à une compression Jpeg

a)

b)

Image tatouée et après compression Jpeg de qualité a) 75 %, b) 65 %

c)

d)

Image tatouée et après compression Jpeg de qualité c) 55 %, d) 45 %

e)

f)

Image tatouée et après compression Jpeg de qualité e) 35 %, f) 25 %

g)

h)

Image tatouée et après compression Jpeg de qualité g) 15 %, h) 5 %

3 Résistance du tatouage face à des manipulations géométriques

a)

b)

Image tatouée et après rotation de 0.7 degré

a)

b)

Image tatouée et après translation de 7 pixels

a)

b)

Image tatouée et après recadrage de 10 %

a)

b)

Image tatouée et après symétrie axiale

a)

b)

Image tatouée et après verticale de 1 % degré

a)

b)

Image tatouée et après étirement horizontal de 105 %

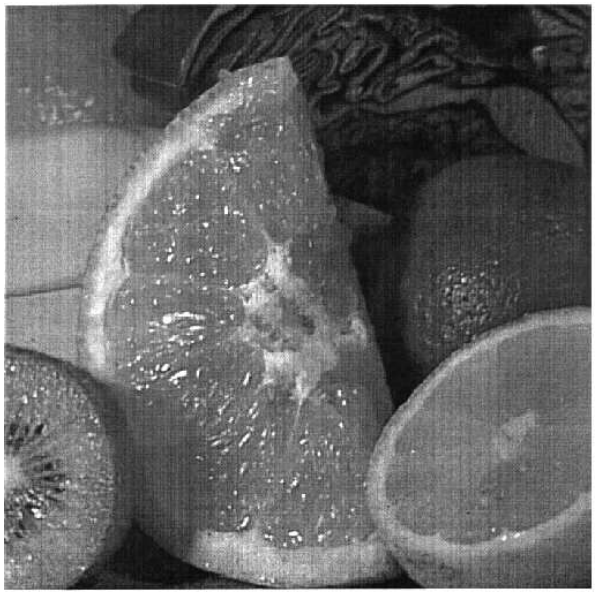
4 Résistance du tatouage face à des requantifications

a)

b)

Image tatouée et après impression et re-digitalisation couleurs.

a)



b)

Image tatouée et après impression et re-digitalisation niveaux de gris

5 Résistance du tatouage face à Stirmark et Unzign

a)

b)

Image tatouée et après une itération de Stirmark

a)

b)

Image tatouée et après une itération d'Unzign

Bibliographie

[1] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva. Dwt-based technique for spatio-frequency masking of digital signatures. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[2] Michael F. Barnsley, Arnaud Jacquin, Francois Malassenet, Laurie Reuter, and Alan D. Sloan. Harnessing chaos for image synthesis. *Computer Graphics*, 22(4) :131–140, August 1988.

[3] F. Bartolini, M. Barni, V. Cappellini, and A. Piva. Mask building for perceptually hiding frequency embedded watermarks. In *Proc. of the Int. Conf. on Image Processing (ICIP'98)*, volume 1, pages 450–454, Chicago, Illinois, US, Oct. 1998. IEEE Signal Processing Society.

[4] W. Bender, D. Gruhl, and N. Morimoto. Techniques for data hiding. In *Proceedings of the SPIE*, volume 2420, pages 40–51, San Jose, CA, Feb. 1995.

[5] G. Blondel, M. Crépaux, and P. Portal. Tatouage pour l'intégrité des images. Master's thesis, Institut Eurecom, Apr. 1999. Rapport confidentiel.

[6] O. Bruyndonckx, J.-J. Quisquater, and B. Macq. Spatial method for copyright labeling of digital images. In *Nonlinear Signal Processing Workshop*, pages 456–459, Thessaloniki, Greece, 1995.

[7] J. J. Chae and B. S. Manjunath. Extracting hidden data without knowing host source. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[8] G. C.Langelaar, J.C.A. Van der Lubbe, and R. L. Lagendijk. Robust labeling methods for copy protection of images. In *Proceedings of SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases*, San Jose, California, Feb. 1997.

[9] Digimarc Corporation. Identify, manage and track your images. http ://www.digimarc.com/, 1998.

[10] I. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. Technical report, NEC Research Institute, 1995.

[11] I. Cox and J.-P. Linnartz. Some general methods for tampering with watermarks. *IEEE Journal on Selected Areas in Communications (Special issue on Copyright and Privacy Protection)*, 16(4) :587–593, May 1998.

[12] I. J. Cox and J-P. M.G. Linnartz. Public watermarks and resistance to tampering. In *IEEE Int. Conf. on Image Processing (ICIP'97)*, Oct. 1997. Pages not in proceedings, in CDrom only.

[13] S. Craver, N. Memon, B.L. Yeo, and M. Yeung. Can invisible watermarks resolve rightful ownerships? In *Proceedings of SPIE*, volume 3022, pages 310–321, 1997.

[14] V. Darmstaedter, J.-F. Delaigle, D. Nicholson, and B. Macq. A block based watermarking technique for MPEG-2 signals : Optimization and validation on real digital TV distribution links. In *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'98)*, May 1998.

[15] J.-F. Delaigle, J.-M Boucqueau, J.-J. Quisquater, and B. Macq. Digital images protection techniques in a broadcast framework : overview. In *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'96)*, pages 711–728, Louvain-la-Neuve, Belgium, May 1996.

[16] J.-F Delaigle, C. De Vleeschouwer, and B. Macq. Watermarking using a matching model based on he human visual system. Ecole thématique CNRS GDR-PRC ISIS : Information Signal Images Marly le Roi, Apr. 1997.

[17] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq. Psychovisual approach for digital picture watermarking. *Journal of Electronic Imaging*, 7(3) :628–640, Jul. 1998.

[18] J.-F. Delaigle, C. De Vleeschouwer, and B. Macq. Watermarking algorithm based on a human visual model. *Signal Processing*, 66(3) :319–336, May 1998.

[19] J-L. Dugelay. Procédé de dissimulation d'informations dans une image numérique. brevet inpi fr 98-04083 (eurecom 09-fr) mars 1998 pending patent pct/fr99/00485 (eurecom 09-pct) mars 1999.

[20] J.-L. Dugelay and M. Barakat. Image sequence coding using 3-d i.f.s. In *IEEE International Conference on Image Processing (ICIP'96)*, pages 141–145, Lausanne, Switzerland, September 1996.

[21] J.-L. Dugelay and A. Gersho. Enhanced fractal image coding by combining ifs and vq. In *Proc. IEEE Int. Conf. on Image Processing*, 1997.

[22] J.-L. Dugelay, E. Majdandzic, and S. Roche. Fractal-based video coding and slow motion replay. In *proc. of Picture Coding Symposium (PCS'99)*, pages 49–52. IEEE, Apr. 1999.

[23] J.-L. Dugelay, E. Polidori, and S. Roche. Iterated function systems for still image processing. In *proc. of the third international workshop on image and signal processing*, Manchester, United Kingdom, Nov. 1996.

[24] J.-L. Dugelay, C. Rey, and S. Roche. Contrôle de l'intégrité d'une image à l'aide d'un tatouage invisible et robuste, dépendant de l'image. Technical Report RR-99-050, Institut Euréecom, Mai 1999.

[25] J.-L. Dugelay, C. Rey, and S. Roche. Introduction au tatouage d'images - etat de l'art. In *Compression et Représentation des Signaux Audiovisuels (CORESA'99)*, Juin 1999.

[26] J-L. Dugelay and S. Roche. Process for marking a multimedia document, such an image, by generating a mark. pending paptent ep 99480075.3 (eurecom 11/12 ep) july 1999.

[27] J-L. Dugelay and S. Roche. Signature d'images par dissimulation d'une information binaire. brevet en cours inpi fr 98-07607 (eurecom 11-fr) juin 1998.

[28] J.-L. Dugelay and S. Roche. Fractal transform based large digital watermark embedding and robust full blind extraction. In *proc. of IEEE Multimedia Systems (ICMCS'99)*, pages 1003–1004, Florence Italy, June 1999.

[29] J.-L. Dugelay and S. Roche. Introduction au tatouage d'images. *to appear in Annales des Télécoms*, 1999.

[30] J.-L. Dugelay and S. Roche. Procédé de marquage d'un document multimedia, tel qu'une image par génération d'une empreinte externe. brevet en cours inpi fr 99-02154 (eurecom 12-fr), Fév. 1999.

[31] J.-L. Dugelay and J.-M. Sadoul. Moving picture fractal coding using a mixed approach i.f.s. and motion. In *European Signal Processing Conference (EUSIPCO'96)*, volume 2, pages 1363–1367, Trieste Italy, 1996.

[32] F. Petitcolas et al. Attacks on copyright marking systems. In *Second workshop on information hiding*. http://www.cl.cam.ac.uk/ fapp2/papers/ih98-attacks/, Apr. 1998.

[33] Eutelsat. Multimedia via satellite services in the DVB era with EUTELSAT. http://www.eutelsat.com/multimedia_service/emp98.pdf, 1998.

[34] Yuval Fisher, editor. *Fractal Image Compression : Theory and Application*. Springer-Verlag, New York, 1995.

[35] J. Fridrich, A. C. Baldoza, and R. J. Simard. Robust digital watermark based on key-dependent basis functions. In David Aucsmith (Ed), editor, *Information Hiding, Second International Workshop, IH'98*, LNCS 1525, ISBN 3-540-65386-4, Portland, Oregon, USA, Apr. 1998. Springer-Verlag.

[36] J. Fridrich and M. Goljan. Comparing robustness of watermarking techniques. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[37] F. Goffin, J.F. Delaigle, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater. A low cost perceptive digital picture watermarking method. In *Proc. of SPIE Electronic Imaging*, pages 264–277, San Jose, Feb. 1997.

[38] S.S. Hacisalihzade, L.W. Stark, and J.S. Allen. Visual perception and sequences of eye movement fixations : a stochastic modeling approach. *IEEE Trans on Systems, Man and Cybernetics*, 22(3) :474—481, may/june 1992.

[39] F. Hartung and B. Girod. Digital watermarking of raw and compressed video. In *Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies*, Berlin, Germany, Oct. 1996.

[40] F. Hartung and B. Girod. Digital watermarking of MPEG-2 coded video in the bitstream domain. In *Proc. of the IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP'97)*, volume 4, pages 2621–2624, Munich, Germany, Apr. 1997.

[41] F. Hartung and B. Girod. Fast public-key watermarking of compressed video. In *IEEE Signal Processing Society 1997 Int. Conf. on Image Processing (ICIP'97)*, Santa Barbara, California, Oct. 1997.

[42] F. H. Hartung, J. K. Su, and B. Girod. Spread spectrum watermarking : malicious attacks and counterattacks. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[43] C. W. Helstrom. *Statistical Theory of Signal Detection*. Pergamon Press, New York, 2 edition, 1968.

[44] J.R. Hernández, F. Pérez-González, J. M. Rodríguez, and G. Nieto. The impact of channel coding on the performance of spatial watermarking for copyright protection. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'98)*, volume 5, pages 2973–2976, 1998.

[45] S. Heulin. Tatouage d'images : le problème de la visibilité. Master's thesis, Institut Eurecom, Juil. 1997. Rapport confidentiel.

[46] J.E. Hutchinson. Fractals and self similarity. *Indiana University Mathematics Journal*, vol 30(number 3), 81.

[47] Arnaud Jacquin. A novel fractal block-coding technique for digital images. In *Proceedings of ICASSP*, volume 4, pages 2225–2228, 1990.

[48] Arnaud E. Jacquin. Image coding based on a fractal theory of iterated contractive image transformations. *IEEE Transactions on Image Processing*, 1(1) :18–30, January 1992.

[49] N.F. Johnson and S. Jajodia. Exploring steganography : Seeing the unseen. *Computer*, 31(2) :26–34, Feb. 1998.

[50] N.F. Johnson and S. Jajodia. Steganalysis of images created using current steganography software. In *Proc. Second Int. Workshop on Information Hiding*, pages 273–289, Apr. 1998.

[51] T. Kalker, J.-P. Linnartz, and M. van Dijk. Improved watermark detection reliability using filtering before correlation. In *Proc. IEEE Int. Conf. on Image Processing*, Oct. 1998.

[52] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, 9 :5–38, Jan. 1883.

[53] E. Koch and J. Zhao. Towards robust and hiden image copyright labeling. In *IEEE Workshop on Nonlinear Signal and Image Processing*, Thessaloniki, Greece, Oct. 1995.

[54] M. Kuhn. Stirmark - image watermarking robustness test. http ://www.cl.cam.ac.uk/ mgk25/stirmark.html, 1998.

[55] D. Kundur and D. Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. In *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, volume 6, pages 2969–2972, 1998.

[56] M. Kunt. *Traitement numérique des images*, volume 2 of *Traitement de l'information.* Presses polutechniques et universitaires romandes, 1 edition, 1993.

[57] M. Kutter. Watermarking resisting to translation, rotation and scaling. In *Proc. of SPIE*, volume 3528, pages 423–431, Boston USA, Nov. 1998.

[58] M. Kutter, F. Jordan, and F. Bossen. Digital signature of color images using amplitude modulation. In *Proc. of SPIE storage and retrieval for image and video databases*, pages 518–526, San Jose, USA,, Feb 1997.

[59] M. Kutter and F. A. P. Petitcolas. Fair benchmark for image watermarking systems. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[60] J.-P. Linnartz, T. Kalker, and G. Depovere. Modeling the false alarm and missed detection rate for electronic watermarks. In *Proc. Second Int. Workshop on Information Hiding*, pages 329–343, Apr. 1998.

[61] E. Majdandzic. Compression de séquences vidéo par I.F.S et fonctionnalités. Master's thesis, DEA Systèmes de Télécommunications Numériques : Ecole Nationale Supérieure des Télécommunications, 1997.

[62] K. Matsui and K. Tanaka. Video-steganography : How to secretly embed a signature in a picture. *Journal of the interactive Multimedia Association Intellectual Property Project*, 1 :187–206, 1994.

[63] N. Memon and P. W. Wong. Buyer-seller watermarking protocol based on amplitude modulation and the el gamal public-key cryptosystem. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[64] M. Miller, I. Cox, and J. Bloom. Watermarking in the real world : an application to dvd. In *in Proc. of the Workshop "Multimedia and Secutiy" at ACM Multimedia 98*, Bristol UK, Sept. 1998.

[65] F. Mintzer, G.W. Braudaway, and m. M. Yeung. Effective and ineffective digital watermarks. In *IEEE Int. Conf. on Image Processing*, volume 3, pages 9–12, Santa-Barbara, CA, Oct. 1997.

[66] B. G. Mobasseri. Exploring cdma for watermarking of digital video. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[67] J. J.K. Ó Ruanaidh and T. Pun. Rotation, translation and scale invariant digital image watermarking. In *IEEE Signal Processing Society 1997 Int. Conf. on Image Processing (ICIP'97)*, volume 1, pages 536–539, Santa Barbara, CA, Oct. 1997.

[68] A. Papoulis. *Probability, Random Variables, and Stochastic Processes.* McGraw-Hill Series in Electrical Engineering, 3 edition, 1991.

[69] W. B. Pennebaker and J. L. Mitchell. *JPEG still image data compression standard.* Van Nostrand Reinhold Company, New York, 1992.

[70] F. A. P. Petitcolas and R. J. Anderson. Weaknesses of copyright marking systems. In *Multimedia and Security – Workshop at ACM Multimedia'98*, volume 41, pages 55–61, Bristol, United Kingdom, Sept. 1998. ACM.

[71] F. A. P. Petitcolas and R. J. Anderson. Evaluation of copyright marking systems. In *To be presented at IEEE Multimedia Systems (ICMCS'99)*, Florence Italy, June 1999.

[72] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. Attacks on copyright marking system. In David Aucsmith (Ed), editor, *Information Hiding, Second International Workshop, IH'98*, LNCS 1525, ISBN 3-540-65386-4, Portland, Oregon, USA, Apr. 1998. Springer-Verlag.

[73] R. L. Pickholtz, D. L. Schilling, and L. B. Millstein. Theory of spread spectrum communications - a tutorial. *IEEE Trans. on Communications*, pages 855–884, 1982.

[74] L. Piron, M. Kutter, and J. M. Boucqueau. Octalis benchmarking : comparisons of three watermarking techniques. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[75] I. Pitas and T.H. Kaskalis. Applying signatures on digital images. In *IEEE Workshop on Nonlinear Signal and Image Processing*, pages 460–463, Thessaloniki, Greece, Oct. 1995.

[76] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In *Proceedings of SPIE Photonics East Symposium*, volume 1, Boston, USA, Nov. 18-22 1996.

[77] S. Roche and J.-L. Dugelay. Improvements in i.f.s. formulation for its use in still image coding. In *proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Halkidiki, Greece, June 1995.

[78] S. Roche and J.-L. Dugelay. Mécanismes de securité liés à la transmission des images. In *Journées COmpression et REprésentation des Signaux Audiovisuels (CORESA'97)*, Cnet Issy-les-Moulineaux, France, Mar. 1997.

[79] S. Roche and J.-L. Dugelay. Image watermarking based on the fractal transform. In *proc. of IEEE Multimedia Signal Processing Worshop (MMSP'98)*, pages 358–363, Redondo Beach CA USA, Dec. 1998.

[80] S. Roche and J.-L. Dugelay. A fractal-inspired approach to data embedding in digital images for authentication services. In *proc. of IEEE Multimedia Signal Processing Worshop (MMSP'99)*, pages 565–566, Sep. 1999.

[81] S. Roche and J.-L. Dugelay. *Information hiding techniques for steganography and digital watermarking*, chapter 6 : A survey of current watermarking techniques. Artech Housse Inc., 1999.

[82] S. Roche, J.-L. Dugelay, and R. Molva. Multi-resolution access control algorithm based on fractal coding. In *proc. of 1996 IEEE Int. Conf. on Image Processing*, volume 3, pages 235–238, Lausanne, Switzerland, Sep. 1996. EPFL, IEEE.

[83] B. Schneier. *Applied Cryptography, Protocols, Algorithms, and Source Code in C.* J. Wiley and Sons Inc., 1994.

[84] C. E. Shannon. Communication theory of secret systems. *Bell System Technical Journal*, 28(4) :656–715, 1948.

[85] J. Smith and B. Comiskey. Modulation and information hiding in images. In *Proc. of the First International Workshop on Information Hiding*, volume 1174 of *Springer Lecture Notes in Computer Science*, pages 207–227. Springer, 1996.

[86] Q. Sun and J. Wu. Recovering modified watermarked images with reference to original image. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[87] M. D. Swanson, B. Zhu, and A. Tewfik. Multiresolution scene-based video watermarking using perceptual models. *IEEE journal on Selected areas in communications*, 16(4) :540–550, May 1998.

[88] P. Thompson. The coding of velocity of movement in the human visual system. *Vision Res.*, 24(1) :41—45, 1984.

[89] Unzign. Is your watermark secure? http ://www.cl.cam.ac.uk/users/fapp2/steganography/image_wa 1997.

[90] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne. A digital watermark. In *Int. Conf. on Image Processing (ICIP'94)*, volume 2, pages 86–90, Austin, Texas, USA, 1994. IEEE.

[91] M. Vetterli and J. Kovačević. *Wavelets and Subband Coding.* Prentice Hall, Englewood Cliffs, NJ, 1995.

[92] G. Voyatzis and I. Pitas. Protecting digital-image copyrights : A framework. *IEEE Computer Graphics and Applications*, 19(1) :18–24, Jan. 1999.

[93] G. K. Wallace. The jpeg still picture compression standard. *Communications of the ACM*, 34(4) :40–44, Apr. 1991.

[94] H.-J. Wang and C.-C. Jay Kuo. Image protection via watermarking on perceptually significant wavelet coefficients. In *proc. of IEEE Multimedia Signal Processing Worshop (MMSP'98)*, pages 279–284, Redondo Beach CA USA, Dec. 1998.

[95] S. Westen, R. Lagendijk, and J. Biemond. Perceptual image quality based on a multiple channel hvs model. In *Proc. of the IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP'95)*, volume 4, pages 2351–2354, 1995.

[96] S. Winkler. A perceptual distortion metric for digital color images. In *Proc. of the Int. Conf. on Image Processing (ICIP'98)*, volume 1, pages 399–403, Chicago, Illinois, US, Oct. 1998. IEEE Signal Processing Society.

[97] P. W. Wong. A public key watermark for image verification and authentication. In *Proc. of the Int. Conf. on Image Processing (ICIP'98)*, volume 1, Chicago, Illinois, US, Oct. 1998. IEEE Signal Processing Society.

[98] X.-G. Xia, C. G. Boncelet, and G. R. Arce. Wavelet transform based watermark for digital images. *Optics Express*, 3(12) :497–511, Dec. 1998.

[99] W. Zeng, B. Liu, and S. Lei. Extraction of multiresolution watermark images for claiming rightful ownership. In *Proc. of Spie, Electronic Imaging'99, Security and Watermarking of Multimedia Contents*, volume 3657, Jan. 1999.

[100] J. Zhao. A WWW service to embed and prove digital copyright watermarks. In *Proc. European Conference on Multimedia Applications, Services and Techniques (ECMAST'96)*, 1996.

Mes publications et brevets

[1] J.-L. Dugelay and S. Roche. Introduction au tatouage d'images. *to appear in Annales des Télécoms*, 1999.

[2] S. Roche and J.-L. Dugelay. *Information hiding techniques for steganography and digital watermarking*, chapter 6 : A survey of current watermarking techniques. Artech Housse Inc.,ISBN 1-58053-035-4, 1999.

[3] S. Roche and J.-L. Dugelay. A fractal-inspired approach to data embedding in digital images for authentication services. In *proc. of IEEE Multimedia Signal Processing Worshop (MMSP'99)*, Sep. 1999.

[4] J.-L. Dugelay, C. Rey, and S. Roche. Introduction au tatouage d'images - etat de l'art. In *Compression et Représentation des Signaux Audiovisuels (CORESA'99)*, Juin 1999.

[5] J.-L. Dugelay and S. Roche. Fractal transform based large digital watermark embedding and robust full blind extraction. In *proc. of IEEE Multimedia Systems (ICMCS'99)*, Florence Italy, June 1999.

[6] J.-L. Dugelay, E. Majdandzic, and S. Roche. Fractal-based video coding and slow motion replay. In *proc. of Picture Coding Symposium (PCS'99)*. IEEE, Apr. 1999.

[7] J.-L. Dugelay and S. Roche. Procédé de marquage d'un document multimedia, tel qu'une image par génération d'une empreinte externe. patent pending fr 99 02154, Mar. 1999.

[8] S. Roche and J.-L. Dugelay. Image watermarking based on the fractal transform. In *proc. of IEEE Multimedia Signal Processing Worshop (MMSP'98)*, pages 358–363, Redondo Beach CA USA, Dec. 1998.

[9] J-L. Dugelay and S. Roche. Procédé de signature d'un document numérique par dissimulation d'une information binaire. patent pending fr 9807607, Aug. 1998.

[10] S. Roche and J.-L. Dugelay. Mécanismes de securité liés à la transmission des images. In *Journées COmpression et REprésentation des Signaux Audiovisuels (CORESA'97)*, Cnet Issy-les-Moulineaux, France, Mar. 1997.

[11] J.-L. Dugelay, E. Polidori, and S. Roche. Iterated function systems for still image processing. In *Proceedings of the third international workshop on image and signal processing*, Manchester, United Kingdom, Nov. 1996.

[12] S. Roche, J.-L. Dugelay, and R. Molva. Multi-resolution access control algorithm based on fractal coding. In *proc. of 1996 IEEE Int. Conf. on Image Processing*, volume 3, pages 235–238, Lausanne, Switzerland, Sep. 1996. EPFL, IEEE.

[13] S. Roche and J.-L. Dugelay. Improvements in i.f.s. formulation for its use in still image coding. In *proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Halkidiki, Greece, June 1995.