الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ HADJ LAKHDAR BATNA

Faculté de Technologie
Département d'Electronique

THESE

En vue de l'obtention du diplôme de

DOCTORAT EN SCIENCES
Option : Electronique

Présentée par :

Ammar Dahmani
Magister en électronique

Thème

CONTRIBUTION AU DEVELOPPEMENT D'UNE TECHNIQUE DE WATERMARKING POUR IMAGES

Soutenue le 16/10/ 2014
Devant le Jury composé de :

N. Benoudjit	Professeur	Université de Batna	Président
A. Louchene	Professeur	Université de Batna	Rapporteur
D. Saigaa	Professeur	Université de Msila	Examinateur
S. Bouguezel	Professeur	Université Sétif	Examinateur
M. Taibi	Professeur	Université d'Annaba	Examinateur
R. Benzid	Maitre de conférence. A	Université de Batna	Examinateur

ANNEE UNIVERSITAIRE :2014/2015

Je tiens en premier lieur à exprimer toute ma gratitude et à adresser mes plus vifs remerciements à mon directeur de thèse le professeur ***Louchene Ahmed****.*

Mes remerciements vont également aux membres de jury :

- *Professeur* ***Benoudijt Nabil*** *de l'université de BATNA pour l'honneur qu'il m'a fait d'être président de mon jury de thèse.*
- *Professeur* ***Saigaa Djamel*** *de l'université de MSILA pour avoir accepté d'être parmi les membres de jury, sa présence est un grand honneur pour moi.*
- *Professeur* ***Bouguezel Saad*** *de l'université de SETIF que je tiens à remercier à la fois pour son rôle de membre de jury et sa collaboration au cours de la réalisation de ce travail.*
- *Docteur Mahmoud* ***Taibi*** *de l'université d'ANNABA qui ma honoré par sa présence et son acceptation de juger ce travail.*
- *Docteur* ***Benzid Ridha*** *de l'université de BATNA pour avoir bien voulu juger ce travail et pour ces remarques constructives.*

Enfin je remercie toutes les personnes qui m'ont aidé de prés ou de loin pour achever ce travail.

Sommaire

Introduction générale…… 1

Chapitre I : Etat de l'art du domaine de watermarking des documents numériques…….. 5

I.1. Introduction…….. 5

I.2.Droits d'auteurs…… 5

I.3 Systèmes numériques de gestion des droits d'auteur (SNGD)…… 7

I.4 Cadre juridique de la protection des droits d'auteur…….. 8

I.5 Cryptographie, stéganographie et watermarking…….. 10

I.5.1 La cryptographie…….. 11

I.5.2 La stéganographie…….. 12

I.5.3 Le watermarking ou tatouage numérique…….. 14

I.6. Les éléments d'un système de watermarking…….. 15

I.6.1 insertion du message…….. 16

I.6.2 diffusion du document marqué et attaques……... 21

I.6.3 Récupération de la signature (watermark) …….. 22

I.7 Contraintes d'un système de watermark……... 23

I.7.1 Imperceptibilité……... 23

I.7.2 Robustesse……... 24

I.7.3 Capacité……... 26

I.7.4 Complexité…….. 27

I.8 Domaines d'application du watermarking……... 27

I.8.1 Protection des droits d'auteurs……... 28

I.8.2 Le suivie de copie ou Fingerprinting…….. 28

I.8.3 Contrôle de copie……... 29

I.8.4 Vérification de l'authenticité et l'intégrité d'un document numérique…... 32

I.8.5 Combler le fossé entre les objets analogiques et numériques (indexation 33

I.8.6 Watermark visible…….. 33

I.8.7Autres applications…….. 34

I.9 Considération protocolaires……... 34

I.10 Conclusion…….. 37

Chapitre II : Domaine du watermarking d'images fixes…….. 38

II.1 Introduction……... 38

II.2 Contexte du tatouage d'image…….. 38

II.3 Principe général d'un schéma de tatouage d'images……... 38

II.3.1 Définition…….. 38

II.3.2 Schéma général d'une méthode de tatouage d'images…….. 39
II.3.2.1 Phase d'insertion …….. 39
II.3.2.2 Phase d'extraction…….. 44
II.4. Evaluation des algorithmes de tatouage…….. 47
II.4.1 Evaluation de la distorsion introduite par l'insertion de la marque…… 47
II.4.1.1 wPSNR (le PSNR pondéré)…… 48
II.4.1.2 Mesure de Watson…….. 48
II.4.2 Les attaques et la robustesse…….. 49
II.4.2.1 Classification des attaques…….. 49
II.4.2.1.1. Les attaques innocentes…….. 50
II.4.2.1.2. Les attaques malveillantes…….. 56
II.5. Conclusion…….. 62
Chapitre III : Points clés et état de l'art des méthodes de watermarking d'images fixes. 64
III.1 Introduction…….. 64
III.2. Le type de schéma d'insertion de la signature …….. 65
III.2.1 Schémas additifs…… 65
III.2.2 Schémas substitutifs…….. 67
III.3. Le choix de l'espace de travail…….. 69
III.3.1 le domaine spatial…… 69
III.3.2 le domaine transformé…….. 70
III.3.2.1. La transformée en cosinus discrète (DCT)…….. 70
III.3.2.2. La transformée de Fourier discrète (DFT)…….. 72
III.3.2.3. La transformée de Fourier-Mellin…….. 74
III.3.2.3. La transformée en ondelettes discrète (DWT)…….. 80
III.3.3 Décomposition de l'image en canaux perceptifs…….. 82
III.3.3.1 Modélisation mono-canal…….. 83
III.3.3.2. Modélisation multi-canal…….. 84
III.4. La stratégie d'insertion de la marque…….. 86
III.4.1 Masquage psychovisuel…… 86
III.4.1.1. Masques spatiaux…….. 86
III.4.1.2. Masques fréquentiels…… 88
III.5. La manière de fusionner la marque avec l'image…… 90
III.5.1 Fusionnement par modulation…….. 90
III.5.2 Fusionnement par quantification des coefficients DCT…….. 91
III.5.2.1. Modification de la fonction d'arrondi…… 91

III.5.2.2. Définition d'une relation de N-uplet de coefficients…….. 91
III.5.2.3. Superposition des coefficients DCT de l'image et de la marque…….. 92
III.5.3. Fusionnement par substitution de blocs…… 92
III.5.4. Fusionnement par quantification vectorielle spatiale…… 92
III.5.5. Fusionnement par quantification des coefficients des ondelettes…… 92
III.6. Les méthodes utilisées pour détecter ou extraire la marque…… 93
III.6.1. Détection par corrélation…… 93
III.6.2. Estimation par filtrage Wiener …….. 94
III.6.3. Estimation par filtrage Passe-haut …….. 95
III.6.4. Estimation par décision optimale …….. 95
III.7. La catégorie d'attaques visées…… 96
III.8. Etat de l'art des méthodes de watermarking d'image fixe…… 96
III.8.1. Les méthodes spatiales…….. 96
III.8.1.1 Méthode du bit le moins significatif (LSB)…….. 98
III.8.1.2 Méthode du Patchwork…….. 99
III.8.1.2 Méthode de l'étalement de spectre…….. 100
III.8.1.3 Méthode de quantification…… 101
III.8.2. Les méthodes fréquentielles…… 103
III.8.2.1. insertion dans le domaine DCT…….. 103
III.8.2.2. insertion dans le domaine DWT…….. 106
III.8.2.3. insertion dans le domaine DFT…….. 108
III.9. Conclusion…….. 108
Chapitre IV : les méthodes de watermarking développées…… 109
IV.1. Tatouage D'image Fixe en Utilisant la Variance Local des Blocs…… 110
IV.1.1. Description de la méthode développée…… 111
IV.1.1.1. Insertion de la marque…….. 111
IV.1.1.2. Extraction de la marque…… 114
IV.1.2. Résultats et interprétations…….. 115
IV.1.2.1. Test de l'invisibilité de la marque…….. 115
IV.1.2.2. Test de la robustesse vis-à-vis la compression…….. 121
IV.1.2.3. Test de la robustesse vis-à-vis changement de format…….. 123
IV.1.3. Conclusion…….. 124
IV.2. Méthode Hybride DWT-DCT de Tatouage d'image Fixe…… 125
IV.2.1. Description de la méthode développée…….. 126
IV.2.1.1. Insertion de la marque…….. 126

IV.2.1.2. Extraction de la marque.…… 129

IV.2.2. Tests et interprétation des résultats …….. 130

IV.1.2.1. Test de l'invisibilité de la marque.…….. 130

IV.2.2.2. Test de la robustesse vis-à-vis la compression.…… 137

IV.2.2.3. Test de la robustesse vis-à-vis l'ajout de bruit Gaussien.…….. 145

IV.2.3. Conclusion.…….. 146

IV.3.Méthode de Watermarking Résistante aux Transformations Géométriques (RST) et la Compression, Basée sur la DWT, LPM et la Corrélation de Phase 147

IV.3.1. Introduction.…… 148

IV.3.2. Travaux en relation avec l'approche développée.…….. 148

IV.3.3.Rappel de quelques transformées en relation avec l'approche développée 150

IV.3.4. Description de la méthode développée.…….. 156

IV.3.4.1. Insertion de la marque.…….. 156

IV.3.4.2. Extraction de la marque.…….. 158

IV.3.5. Tests et interprétation des résultats …….. 160

IV.3.5.1. Test de l'invisibilité de la marque.…….. 161

IV.3.5.2. Test de la robustesse vis-à-vis la translation.…… 161

IV.3.5.3. Test de la robustesse vis-à-vis le changement d'échelle.…….. 163

IV.3.5.4. Test de la robustesse vis-à-vis la rotation.…….. 165

IV.3.5.5. Test de la robustesse vis-à-vis la rotation et le changement d'échelle 167

IV.3.5.5. Test de la robustesse vis-à-vis la compression JPEG.…….. 171

IV.3.5.5. Test de la robustesse vis-à-vis l'addition du bruit Gaussien.…….. 172

IV.3.6. Conclusion.…… 173

IV.4. Méthode de Watermarking Basée sur la DWT Multi-Niveaux et une Nouvelle Classe de Transformées Paramétriques Orthogonales-Réciproques (ROPT) 174

IV.4.1. Introduction.…….. 175

IV.4.2. Travaux en relation avec l'approche développée.…… 175

IV.4.3. Rappel sur la ROPT.…….. 177

IV.4.4. Description de la méthode développée.…….. 178

IV.4.4.1. Insertion de la marque.…….. 179

IV.4.4.2. Extraction de la marque.…… 180

IV.4.5. Tests et interprétation des résultats.…… 182

IV.4.5.1. Test de l'invisibilité de la marque.…… 183

IV.4.5.2. Test de la robustesse vis-à-vis la compression.…….. 185
IV.4.5.3. Test de la robustesse vis-à-vis l'ajout de bruit.…….. 187
IV.4.5.4. Test de la robustesse vis-à-vis le filtrage passe-bas.…….. 190
IV.4.6. Conclusion.…….. 192
V. Conclusion et perspectifs.…… 193
VI. Annexes.…… 196
VII. Bibliographie.…… 202

Table des figures

Figure I.1. *Schéma général d'un système de watermarking.…… 15*

Figure I.2. *Insertion du watermark via l'extraction de caractéristiques inversible.…... 20*

Figure I.3. *Exemple d'insertion du watermark dans l'amplitude de DFT.…… 20*

Figure I.4. *Les deux formes du module de récupération de la signature.…… 22*

Figure I.5. *Compromis entre robustesse, imperceptibilité et capacité.…... 27*

Figure I.6*. CSS empêche seulement que les données légales ne soient pas transmises…. 31*
aux appareils non-conformes, alors que l'inverse est encore possible (lignes pointillées)

Figure I.7. *L'utilisation du watermarking sépare le monde conforme du monde non….. 31*
conforme

Figure I.8. *Compromis entre robustesse et capacité du watermark pour différentes.…… 34*
applications

Figure I.*9 Le premier exemple d'attaques SWICO …….. 36*

Figure I.*9 Le deuxième exemple d'attaques SWICO.…….. 36*

Figure II.1. *Dispositif générique d'un système de tatouage d'image …….. 39*

Figure II.2. *Insertion et extraction d'une signature.…….. 40*

Figure II.3. *mode d'extraction non aveugle.…….... 45*

Figure II.4. *mode d'extraction semi-aveugle.…….. 46*

Figure II.5. *mode d'extraction aveugle.…….... 46*

Figure II.6. *Exemple d'une image compressée.…….... 51*

Figure II.7*. Quelques opérations de filtrage : a) lissage et b) rehaussement ……. 52*

Figure II.8. *Les transformations géométriques élémentaires.…….. 55*

Figure II.9. *Effacement de la marque par estimation.…….... 57*

Figure II.10. *Effacement de la marque par remodulation.…….... 57*

Figure II.11. *Attaque par copiage « Copy attack ».…….... 58*

Figure II.12*. Principe de l'attaque IBM ou deadlock.…….... 60*

Figure II.13. *Attaque par mosaïques.…….... 62*

Figure III.1. *Insertion de la marque pour des schémas additifs.…… 66*

Figure III.2. *Extraction de la marque pour des schémas additifs.…….. 67*

Figure III.3. *Schéma d'insertion par substitution.…….. 68*

Figure III.4. *Détection de la marque pour les schémas substitutifs.…….... 69*

Figure III.5*. Répartition des fréquences dans un bloc DCT.…….... 71*

Figure III.6. *Les valeurs des coefficients d'un bloc DCT.…… 71*

Figure.III.7*. Répartition fréquentielle des coefficients de l'amplitude d'une DFT.…… 73*

Figure. III.8. *Les deux images originales avant permutation de phases.…….... 74*

Figure. III.9. *Les deux images originales après permutation de phases.…….... 74*

Figure III.10. *Le passage du domaine cartésien au domaine log-polaire…….. 75*

Figure III.11. *Construction d'un espace invariant aux transformations géométriques… 76*

Figure III.12. *Exemple d'une image translate par (50, 50)…… 78*

Figure III.13. *Exemple d'une image réduite par X et pivotée d'un angle α…… 79*

Figure III.14. *Exemple de décomposition d'une image en ondelettes à 3 niveaux …….. 80*

Figure III.15. *Décomposition de l'image Lena en ondelette niveau 1…….. 81*

Figure III.16. *Modélisation du comportement des parties périphériques du HVS…….. 85*

Figure III.17. *Création de masque par le schéma de Bartolini …… 89*

Figure III.18. *Schéma de détection de la marque par corrélation…….. 94*

Figure III.19. *Processus d'insertion pour la méthode spatiale…….. 97*

Figure III.20. *Détection de la marque par corrélation…… 98*

Figure III.21. *Insertion de la marque par étalement de spectre selon l'approche de…… 101*
Hartung et Girot

Figure III.22. *Quantification Scalaire…….. 102*

Figure III.23. *Quantification vectorielle avec pas uniforme…….. 102*

Figure III.24. *Numérotation de bloc DCT dans l'algorithme de Zhao et Koch…….. 104*

Figure III.25. *Mécanisme d'insertion de la méthode de Kundur…….. 106*

Figure III.26. *Insertion de la marque selon le schéma de Barni…… 107*

Figure IV.1. *Schéma d'insertion de la marque…….. 111*

Figure IV.2. *Répartition des fréquences dans un bloc DCT…… 113*

Figure IV.3. *Emplacement des coefficients supportant la marque…… 113*

Figure IV.4. *Schéma d'extraction de la marque…… 114*

Figure IV.5. *Vérification de la contrainte invisibilité de la marque …… 116*

Figure IV.6. *Dégradation de la qualité de l'image après insertion de la marque …….. 117*

Figure IV.7. *Vérification de l'invisibilité de la marque pour les deux cas extrêmes …… 118*

Figure IV.8. *Vérification de l'invisibilité de la marque pour différentes valeurs de NR.. 119*

Figure IV.9. *Variation Du PSNR en fonction du nombre de redondance NR…….. 120*

Figure IV.10. *Variation du PSIM en fonction du taux de compression pour NR=11…… 122*

Figure IV.11. *Variation du PSIM en fonction du taux de compression pour NR=512….. 122*

Figure IV.12. *Robustesse vis-à-vis le changement de format…….. 123*

Figure IV.13. *Robustesse vis-à-vis la conversion en niveau de gris…….. 124*

Figure IV.14. *Schéma d'insertion de la marque…… 127*

Figure IV.15 *Disposition des coefficients concernés par la modification…….. 128*

Figure IV.16. *Schéma d'extraction de la marque…….. 129*

Figure IV.17. *Insertion de la marque [0 0 0 0 0 0 0 0] dans la position P0 avec NR=1.. 131*
et NR=110

Figure IV.18. *Insertion de la marque [1 1 1 1 1 1 1 1] dans la position P0 avec NR=1.. et NR=110* 132
Figure IV.19. *Insertion de la marque [0 0 0 0 0 0 0 0] dans la position P8 avec NR=1.. et NR=110* 133
Figure IV.20. *Insertion de la marque [1 1 1 1 1 1 1 1] dans la position P8 avec NR=1. et NR=110* 134
Figure IV.21. *Variations du PSNR en fonction de la position de la marque pour NR=1.* 135
Figure IV.22. *Variations du PSNR en fonction de la position de la marque pour……. NR=10* 136
Figure IV.23. *Variations du PSNR en fonction de la position de la marque pour……. NR=20* 136
Figure VI.24. *Variations du PSNR en fonction de la position de la marque pour……. NR=40* 137
Figure IV.25. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P2, NR=20* 138
Figure IV.26. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P3, NR=20* 138
Figure IV.27. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P4, NR=20* 139
Figure IV.28. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P5, NR=20* 139
Figure IV.29. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P6, NR=20* 140
Figure IV.30. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P7, NR=20* 140
Figure IV.31. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P8, NR=20* 141
Figure IV.32. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P2, NR=100* 141
Figure IV.33. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P3, NR=100* 142
Figure IV.34. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P4, NR=100* 142
Figure IV.35. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P5, NR=100* 143
Figure IV.36. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P6, NR=100* 143
Figure IV.37. *Robustesse de la marque vis-à-vis la compression JPEG pour la…….. position P7, NR=100* 144
Figure IV.38. *Robustesse de la marque vis-à-vis la compression JPEG pour la position P8, NR=100* 144
Figure IV.39. *Robustesse de la marque vis-à-vis l'attaque par bruit Gaussien……* 145
Figure IV.40. *Exemple de décomposition d'une image par la DWT……* 150
Figure IV.41. *Exemple d'interpolation Bilinéaire……* 156
Figure IV.42. *La région choisie pour l'insertion de la marque……* 157
Figure IV.43. *Diagramme du processus d'insertion de la maque……* 158
Figure IV.44. *Diagramme du processus d'extraction de la marque……* 159

Figure IV.45. *Vérification de la contrainte invisibilité.…… 161*

Figure IV.46. *Exemple d'une translation par (50, 50).…… 162*

Figure IV.47. *Conservation de l'information de l'image.…… 163*

Figure IV.48. *Exemple d'une image réduite d'un facteur X.…… 164*

Figure IV.49. *Le pourcentage de similarité PSIM pour différents facteurs d'échelles.… 165*

Figure IV.50*. Exemple d'une image marquée et tournée d'un angle inconnu α.…… 166*

Figure IV.51*. Corrélation de phase entre le LPM de l'image originale et celui de.…... 167*
l'image marquée et tournée d'un angle α

Figure IV.52. *Le PSIM pour différentes valeurs de rotation de l'image marquée.…… 167*

Figure IV.53. *Exemple d'une image réduite et tournée en même temps.…….... 169*

Figure IV.54. *Corrélation de phase entre le LPM de l'image originale et celui de.…... 170*
l'image marquée réduite de X et tournée de α

Figure IV.55. *Variation du PSIM pour α=65°/ X= [0.3,…..,1].…… 171*

Figure IV.56*. Variation du PSIM pour X=0.8 / α = [0.…..180].…….... 171*

Figure IV.57. *Variation du PSIM en fonction du facteur de qualité.…… 172*

Figure IV.58. *Variation du PSIM en fonction du niveau d'énergie d'un bruit Gaussien. 173*

Figure IV.59. *Organigramme du processus d'insertion de la marque.…… 180*

Figure IV.60. *Organigramme du processus d'extraction de la marque.…….... 182*

Figure IV.61. *Imperceptibilité de la marque.…….... 183*

Figure IV.62. *Variation du PSNR en fonction de λ pour d=0,1 et 2.…… 184*

Figure IV.63. *Variation de NC en fonction de λ pour d=0,1 et 2.…….... 184*

Figure IV.64. *Marques extraites pour les différents niveaux dans le cas Q=50 et λ= 0.1 185*

Figure IV.65. *Variation de NC en fonction de Q pour λ= 0.1.…… 186*

Figure IV.66. *Variation de NC en fonction de Q pour λ= 0.06.…….... 186*

Figure IV.67*. a- Image tatouée attaquée par un bruit blanc Gaussienne V=0.001.…..... 187*
b- La marque extraite

Figure IV.68. *La marque extraite dans les cas des bruits Gaussien blanc, Speckel et….. 188*
Salt-Pepper

Figure IV.69. *Variation de NC en fonction de la variance du bruit Gaussien blanc pour 189*
différents niveaux de décomposition d

Figure IV.70. *Variation de NC en fonction de la variance du bruit Speckel pour.…… 189*
différents niveaux de décomposition d

Figure IV.71. *Variation de NC en fonction de la densité du bruit Salt-Pepper pour.…… 190*
différents niveaux de décomposition d

Figure IV.72. *Les marques extraites dans les cas des filtres Gaussien, average et disk... 191*
de taille 3x3

Figure IV.73. *Variation de NC en fonction de la déviation standard du filtre Gaussien.. de taille 5x5* *191*

L'information est une donnée précieuse. Elle a toujours eu un rôle primordial au cours de l'histoire. C'est pour cela que son contrôle est synonyme de pouvoir et de puissance.

Avec l'évolution des nations et dans le but de faciliter les relations sociales, économiques et scientifiques voir même politiques, le droit à l'information était devenu de grande importance. En effet, la promulgation et la déclaration de ce droit a eu lieu en décembre 1948 au niveau de l'assemblée générale de l'ONU dans l'article 19 de sa déclaration des droits de l'homme. Il stipule que « Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit ». Cela bien sûr avec la préservation des droits des producteurs de ces informations comme il a été mentionné dans l'article 27 « Chacun a droit à la protection des intérêts moraux et matériels découlant de toute production scientifique, littéraire ou artistique dont il est l'auteur ».

L'avènement de l'ère numérique, les développements d'Internet et plus généralement de nouveaux moyens de communication ont rendu l'accès à l'information bien plus aisé que le passé. En plus, la disponibilité des réseaux, des supports numériques de grande capacité et l'engouement sans cesse grandissant du grand public pour les nouvelles technologies de l'information entraînent une circulation accrue des documents multimédia (images, vidéos, son, textes, etc.…). De par leur nature numérique et en plus des facilités qu'offrent les ordinateurs à traiter et manipuler les données numériques, ces documents multimédia sont en effet très faciles à pirater : on peut les stocker, les dupliquer, les transformer et les diffuser illégalement sans qu'ils perdent de leur qualité. Dans ce contexte, il est très difficile de concilier le libre accès à l'information et le respect des droits d'auteur, le contrôle des copies et l'intégrité d'un document. Il s'est donc avéré nécessaire pour les créateurs de contenus numériques de rechercher les solutions pour empêcher ou tout du moins freiner le piratage de ces œuvres multimédia.

Pour répondre à ces besoins, un nouvel axe de recherche est apparu au début des années 90 et ne cesse de prendre de l'importance au sein de la communauté scientifique. Issu de la cryptographie et la stéganographie, le tatouage numérique appelé en anglais watermarking (filigrane en français) est une approche qui a émergée ces dernières années et se présente comme une solution alternative ou complémentaire pour renforcer la sécurité des documents numériques. Le principe de cette technique consiste à enfouir au sein même du

document numérique (image, son, vidéo, etc.…) une signature (appelée marque ou aussi watermark) indélébile et imperceptible tout en lissant le document signé exploitable. Cette signature, qui est intimement liée au document hôte et non pas associée comme en-tête, augmente la fonctionnalité du document et permet de résoudre des problèmes de copyright, d'authentification, de traçabilité, etc. Ceci, à condition qu'elle soit robuste aux différents traitements et attaques (innocents ou malveillants) que peut subir le document. Le degré de cette robustesse varie selon l'application envisagée. Beaucoup d'efforts ont été exploités par les chercheurs dans ce domaine de watermarking et jusqu'à présent plusieurs méthodes ont été proposées [1], [2], [3], [4] et [5].

Le travail présenté dans cette thèse va dans la même optique et a pour objectif de proposer des méthodes hybrides de tatouage des images numériques fixes. Ces méthodes sont basées sur l'utilisation combinée des domaines transformés obtenus par la transformée en cosinus discrète (*DCT*), la transformée en ondelettes discrète (*DWT*) et d'une nouvelle classe de transformée appelée *ROPT* (Reciprocal- Orthogonal Parametric Transforms).

Cette thèse est organisée en quatre chapitres :

Dans le premier chapitre, nous avons présentés un état de l'art du domaine du watermarking des données multimédias d'une façon générale. En premier lieu nous avons abordé la question des droits d'auteur ou le copyright qui a été l'origine de l'émergence de ce domaine. Puis, nous avons évoqué l'aspect juridique et technique de cette discipline. Par la suite, nous avons parlé de la conception des systèmes de watermarking, des contraintes en relation ainsi que des domaines d'application.

Dans le deuxième chapitre, notre étude est focalisée en particulier sur le watermarking (ou tatouage) d'images fixes. Dans le but de la protection du copyright des images fixes, nous avons présenté les principaux modules composants le système de watermarking. Les contraintes relatives aux phases d'insertion et de détection sont discutées. Ensuite, nous avons abordé la question d'évaluation des algorithmes de tatouage d'images fixes. Cette évaluation est étroitement liée aux différentes attaques, présentées en détail dans la fin de ce chapitre, que peut subir une image.

Le troisième chapitre est consacré exclusivement aux méthodes de watermarking d'images fixes. Les différents paramètres distinctifs sont présentés, à savoir :

- le type de schéma d'insertion de la marque (additif ou substitutif),
- la stratégie d'insertion ainsi que son fusionnement avec les données de l'image à marquer (les caractéristiques du système visuel humain *HVS* sont prises en compte),

- la catégorie d'attaques visées par l'application,
- les méthodes d'amélioration de la détection et de l'extraction de la marque,
- le choix de l'espace d'insertion de la marque.

Ensuite, un état de l'art des méthodes de watermarking d'images, séparées en méthodes spatiales et transformées, est présenté.

Le quatrième chapitre, divisé en quatre parties, est réservé à la présentation de nos contributions et travaux dans le domaine de watermarking d'image fixe [6][7][8][9][10]. Dans la première partie de ce chapitre, nous avons présenté la première méthode développée. Il s'agit d'une méthode de watermarking basée sur la transformée en cosinus discrète (*DCT : Discreet Cosin Transform).* L'insertion de la marque se fait dans des blocs *DCT* de 8x8, et qui sont sélectionnés selon leurs variances locales de luminance. Le travail réalisé dans cette partie était un travail de base et représentait nos premiers pas d'investigation dans le domaine de watermarking. Ça nous a aidé à focaliser la lumière sur de nombreux problèmes en relation avec l'invisibilité de la marque et sa robustesse vis-à-vis de la compression, l'ajout du bruit et le filtrage. Donc, la recherche des solutions à ces problèmes nous a conduits à développer une nouvelle approche hybride. Cette méthode, qui a fait l'objet de la deuxième partie de ce chapitre, est basée sur la combinaison de deux transformées qui sont la *DCT* et *DWT* (*Discreet Wavelet Transform*). En effet, l'utilisation de la sous-bande basse fréquences (*LL*) obtenue par la *DWT* permet la mise à disposition d'un espace très robuste à la compression mais il remit en cause l'invisibilité de la marque et bien sûre la qualité de l'image. L'application de la *DCT* à la sous-bande (*LL*) permet de cerner ce problème.

Dans la troisième partie, nous nous sommes intéressés à d'autres types d'attaques qui représentent un grand challenge aux méthodes de watermarking. Il s'agit en fait des transformations géométriques à savoir la translation, la rotation et le changement d'échelle. La principale difficulté dans ces attaques géométriques est la perte de synchronisation dans la détection de la marque. Ainsi, cette dernière échoue même si la marque subsiste encore dans l'image marquée. La méthode développée est aussi hybride, mais cette fois elle combine la *DWT*, la transformée de Fourier Discrète (*DFT*) et la représentation logo-polaire (*LPM* : Logo-Polar Mapping) à travers la transformée de Fourier-Mellin (*FMT*). Le choix de la *DWT* revient aux raisons citées précédemment qui concerne surtout la robustesse à la compression. L'amplitude de la transformée *DFT* appliquée à la sous-bande (*LL*) est un espace qui est invariant seulement à la translation. Donc, pour résoudre le problème de rotation et de changement d'échelle, on a fait recours à la transformée *FMT*, appliquée à l'amplitude de la *DFT*, qui permet d'avoir un espace invariant à ces transformations. Pour l'extraction ou la

détection de la marque, nous avons utilisé la corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée. Cette corrélation permet de connaitre la nature de la transformation subite par l'image, de corriger le déplacement correspondant et par conséquent synchroniser la détection de la marque.

La dernière partie de ce chapitre est consacrée à la présentation d'une autre approche traitant en particulier l'aspect sécuritaire des méthodes de watermarking. Pour répondre à cette exigence, nous avons fait recours à un nouveau type de transformation loin des transformées habituelles. En fait, Il s'agit d'une nouvelle classe de transformée appelée « *ROPT* » (*Reciprocal-Orthogonal Parametric Transforms*) [11]. L'idée de base derrière la méthode proposée consiste à utiliser une nouvelle méthode de génération de clés. Ceci, en exploitant le grand nombre de paramètres indépendants (3N/2) fournis par la *ROPT* comme clé supplément de tatouage ajouté à celle utilisée pour l'insertion du watermark. Pour contourner l'inconvénient de la *ROPT*, qui donne une répartition non uniforme des fréquences, nous avons opté à l'exploitation de la sous-bande des basses fréquences (*LL*) obtenue par la *DWT*. De cette façon nous assurerons d'une part que les fréquences de la région dans laquelle le watermark sera inséré sont tous de la même gamme, d'autre part la robustesse du watermark contre certaines attaques.

Enfin nous avons terminé cette thèse par une conclusion où nous avons dégagé les points clés en relation avec les systèmes de watermarking d'image, ainsi que les perspectifs offertes par ces systèmes.

I.1 INTRODUCTION

Depuis la seconde moitié des années 1990, la dissimulation des données numériques « digital data hiding » a reçu une attention croissante de la part de la communauté des technologies de l'information. Le tatouage ou le watermarking qui fait partie de ce domaine scientifique très récent présente de multiples intérêts. Il trouve son origine dans le manque de techniques fiables de protections des documents numériques qui sont devenus volatiles et faciles à pirater.

Nous présentons dans ce chapitre les enjeux offerts par le watermarking. Au début, nous abordons la question de la protection des droits d'auteurs qui a été la cause principale de la naissance de cette discipline de watermarking. Les outils techniques et juridiques relatif à cette technique seront également présentés. Ensuite, nous passons en revue les techniques en relation directe avec le watermarking, à savoir la cryptographie et la stéganographie, tout en présentant les similitudes et complémentarités. La section (I.6) sera réservée à la présentation des différents éléments constitutifs d'un système de watermarking par analogie avec les systèmes de communication. Avant de donner quelques domaines d'application, nous parlerons des contraintes principales à prendre en considération lors de la conception d'un système de watermarking. Finalement, pour l'implémentation de ces systèmes dans des applications réelles, des considérations protocolaires doivent être prises en compte.

I.2 Droits d'auteurs

Deux systèmes de protection des œuvres existent dans le monde : le droit d'auteur utilisé en France et le copyright utilisé aux Etats-Unis. La principale différence entre ces deux systèmes réside dans les conditions de protection. En France, elle est implicite dès l'invention (pas de dépôt formel), aux USA l'invention doit être tangible (durable) et pour permettre une action en justice, elle doit être déposée au *Copyright Office*. En France, le droit d'auteur est né à la suite de la révolution en 1791, autour du concept de personnalité unique de l'auteur d'une œuvre [12]. L'auteur y acquiert un droit de représentation et de reproduction sur son œuvre. On différencie le droit moral (respect de l'intégrité de l'œuvre, droit de retrait), et les droits patrimoniaux (reproduction, distribution), qui perdure 70 ans après le décès de l'auteur. Les exceptions à la protection sont la liberté d'information (analyses courtes de l'œuvre, reproduction dans une revue de presse) et la liberté de création (parodie). La législation française actuelle s'appuie sur le code de la propriété intellectuelle qui comprend la propriété littéraire et artistique (droits d'auteur) et la propriété industrielle (brevets). Les critères de

protection d'une œuvre sont sa concrétisation intellectuelle (d'une idée non protégeable, à une œuvre) et matérielle, mais surtout son originalité.

La spécificité du système des droits d'auteurs est illustrée par la bataille dont font l'objet les logiciels informatiques au Parlement Européen en 2006. Le logiciel est, en effet, protégé en France par le droit d'auteur depuis 1985, bien que ces droits reviennent automatiquement à l'employeur. Aux USA, les logiciels font l'objet de brevets, système que la commission européenne propose d'imposer en Europe. En effet, un brevet doit être explicitement déposé, éventuellement tenu secret et est payant pendant toute la durée de protection [13]. L'ampleur de la controverse souligne la différence fondamentale entre ces deux systèmes de protection. Par son caractère implicite, le système du droit d'auteur empêche le dépôt d'une œuvre par quelqu'un d'autre que son auteur. D'autre part, le système du droit d'auteur permet l'existence du « logiciel libre » : l'auteur peut signer une licence (par exemple sur le modèle *GPL*, pour *General Public License*) dans laquelle il exprime le souhait de ne pas être protégé dans l'exploitation de son œuvre, tout en conservant son droit moral. Sur ce modèle, commence à se développer le courant dit de l' « art libre », avec les licences *Creative Commons* ou les Licences Art Libre.

Cas particulier des documents numériques

Les œuvres numériques posent cependant un problème d'application du droit d'auteur. Une œuvre numérique peut être distribuée de manière légale sous forme concrète (*CD*, *DVD*), ou via des plates-formes payantes de téléchargement qui permettent la rémunération de l'auteur. Cependant, il est très facile de fabriquer une copie absolument identique à l'œuvre numérique originale, ainsi que de la distribuer. La contrefaçon ne nécessite pas de moyen technique particulier. Le problème est devenu particulièrement aigu avec l'apparition du système *P2P*. Il s'agit d'un système d'échange de fichiers d'ordinateur à ordinateur qui réunit près de 10 millions d'utilisateur dans le monde. Si la technologie elle-même n'est pas illicite, le fait de partager des fichiers protégés par le droit d'auteur l'est, puisque les ayants-droits ne sont pas rémunérés lors de l'échange. Le téléchargement est légal, mais la mise en ligne (*upload*) est soumise à autorisation, or dans le *P2P* est à la fois émetteur et récepteur. Le droit français ajoute une complication supplémentaire en autorisant la copie privée. Son détournement à des fins de piratage a conduit à la création d'une taxe sur les supports *CD* et *DVD* vierges, destinés aux auteurs. En 2006, une nouvelle loi sur les « droits d'auteur dans la société de l'information » a été votée suite à une directive de 2001 du Parlement Européen, et rénove en profondeur la question des droits d'auteurs numériques [14].

I.3 Systèmes numériques de gestion des droits d'auteur (*SNGD*)

Les systèmes numériques de gestion des droits d'auteur *SNGD*, en anglais (*DRMS : Digital Rights Management Systems*) appelés aussi « verrous numériques », ont pour fonctions essentielles de permettre aux titulaires de droit d'autoriser ou d'interdire la représentation et la reproduction des œuvres et ainsi d'exercer les droits exclusifs reconnus par la loi sur leurs œuvres. De tels systèmes ne sont concevables que dans l'environnement numérique, renforcés par la possibilité de communications par réseaux. Les principales sociétés qui commercialisent ces systèmes sont *Microsoft, Sony, Thomson, Philips, IBM, HP*.

Avec ces systèmes, l'exercice des droits des titulaires se fait sur un ensemble de licences d'utilisations octroyées aux consommateurs d'œuvres culturels. En contrepartie de l'octroi de licences, l'utilisateur consent à un paiement. Un système automatisé de rémunération constitue une partie des *SNGD* mais le but des *SNGD* est d'automatiser toute la chaîne de contrôle de la reproduction et de la représentation de l'œuvre. Les systèmes de *DRMS* utilisent les techniques de watermarking et forment des bases de données qui contiennent des renseignements sur le contenu, dans la plupart des cas sur l'auteur et les autres titulaires de droits. Cette information permet au système d'autoriser des tiers à utiliser les œuvres en question. Un système de gestion du droit d'auteur comporte généralement deux modules fondamentaux, l'un servant à l'identification du contenu et l'autre à l'octroi d'une licence (ou, rarement, aux autres transactions portant sur le droit, telles qu'une cession complète).

S'ils peuvent être considérés comme un ensemble organisé et cohérent de mesures de protection, les *DRMS* assurent toutes les fonctions permettant à des contenus numériques d'être commercialisés dans des conditions juridiques de protection et d'exploitation particulières. Distribuer à un large public une œuvre numérique comporte des contraintes bien supérieures que celles nécessaires pour commercialiser un produit ordinaire. Cela tient à la protection particulière accordée aux œuvres culturelles par le droit de la propriété intellectuelle.

Aussi les systèmes numériques de gestion de droits ont besoin pour fonctionner dans des conditions qui respectent les droits de titulaires de droit sur les œuvres, de délimiter un "espace de confiance". C'est seulement dans cet espace que pourra se réaliser la distribution de contenus numériques d'œuvre diverses. Dans un espace de confiance, le titulaire des droits peut avoir confiance dans l'utilisateur. Il le connaît (authentification), et peut limiter les droits octroyés sur l'œuvre en les décrivant précisément grâce à un système de description des droits. De plus, il pourra être rémunéré immédiatement par l'utilisateur. Pour créer un espace de

confiance, le titulaire de droits et son utilisateur doivent pourvoir échanger des informations en toute confidentialité sans qu'une tierce ne puisse connaître d'éléments de leur dialogue. Cet espace doit s'étendre dans tous les environnements où pourrait se situer l'œuvre, depuis le fournisseur (titulaire des droits), en passant par le distributeur (réseaux) jusqu'au consommateur (utilisateur). Pour suivre l'œuvre, il va donc falloir la marquer afin que des outils techniques puissent garantir une sécurité des transactions de l'amont (fournisseurs) à l'aval (consommateur).

Ces outils devront assurer la continuation de l'espace de confiance entre trois environnements:

- celui des titulaires de droits qui comprend les auteurs, les artistes, les interprètes et les producteurs qui sont titulaires des droits exclusifs des œuvres, et pour les derniers propriétaires des supports de fixation des œuvres,
- celui du distributeur qui doit assurer l'encodage des œuvres et les droits pour les diffuser au public,
- celui de l'utilisateur acheteur des licences d'exploitation et du matériel analogique ou numérique.

I.4 Cadre juridique de la protection des droits d'auteur

La convention de Berne et de nombreuses lois nationales contiennent un inventaire des composantes de la propriété intellectuelle. Il existe deux grandes catégories : le droit moral et les droits économiques. Dans la première, on trouve le droit de paternité de l'œuvre et le droit de s'opposer à sa mutilation. Dans la seconde, les droits les plus importants sont le droit de reproduction, le droit de communication au public (qui comprend, d'après l'article 8 du Traité de l'*OMPI* (Organisation Mondiale de la Propriété Intellectuelle) sur le droit d'auteur, le droit de "mise à disposition") et le droit d'adaptation. Un système de *DRMS* se préoccupe principalement des droits qui peuvent aisément faire l'objet d'une licence ou d'une cession : les droits économiques se prêtent donc mieux à la gestion électronique qu'au droit moral.

L'application à l'échelle mondiale des traités de l'*OMPI* sur le droit d'auteur et sur les interprétations et exécutions et les phonogrammes devraient garantir que les données relatives à la gestion du droit d'auteur ne sont pas délibérément modifiées. C'est ainsi que l'*OMPI* a défini un cadre particulier de la protection juridique des documents numériques. Un traité sur le droit d'auteur a été signé le 20 décembre 1996, entrant dans le cadre de la convention de berne révisée le 2 mars 1997. L'article 12 de ce traité discute les « informations relatives au régime des droits d'auteur de documents sous forme électronique » :

1- les parties contractantes doivent prévoir des sanctions juridiques appropriées et efficaces contre toute personne qui accomplit l'un des actes suivants en sachant, ou, pour ce qui relève des sanctions civiles, en ayant des raisons valables de penser que cet acte va entraîner, permettre, faciliter ou dissimuler une atteinte à un droit prévu par le présent traité ou la Convention de Berne :

   i) supprimer ou modifier, sans y être habilitée, toute information relative au régime des droits se présentant sous forme électronique ;

   ii) distribuer, importes aux fins de distribution, radiodiffuser ou communiquer au public, sans être habilitée, des œuvres ou des exemplaires d'œuvres en sachant que des informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

2- dans le présent article, l'expression **« information sur le régime des droits »** s'entend des informations permettant d'identifier l'œuvre, l'auteur de l'œuvre, le titulaire de tout droit sur l'œuvre ou des informations sur les conditions et modalités d'utilisation de l'œuvre, et de tout numéro ou code représentant ces informations, lorsque l'un de ces éléments d'information est joint à l'exemplaire d'une œuvre ou apparaît en relation avec la communication d'une œuvre au public.

Même si le terme tatouage ou watermarking n'est pas mentionner directement, le deuxième point de l'article souligne l'utilisation d'une information sous forme d'une entête de fichier ou encore d'une signature numérique.

Cette volonté de protéger les documents numériques et d'interdire les modifications des informations concernant les droits d'auteurs a fait l'objet de plusieurs lois. En France, La loi relative au droit d'auteur et aux droits voisins dans la société de l'information, dite loi DADVSI, est une loi issue de la transposition en droit français de la directive européenne 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information [15]. Ce texte a été adopté par l'Assemblée nationale et le Sénat le 30 juin 2006, avant d'être examiné par le Conseil constitutionnel qui en a supprimé certaines dispositions. Le texte, publié au Journal officiel le 3 août 2006, prévoit des amendes d'un montant de 300 000 euros ainsi que 3 ans de prison pour toute personne éditant un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés, et jusqu'à 6 mois de prison et 30 000 euros d'amende pour toute personne diffusant ou facilitant la diffusion d'un logiciel permettant de casser les mesures techniques de protection (*DRMS*) qui selon ses défenseurs visent à empêcher la contrefaçon.

Aux Etats-Unis, une loi sur la protection des documents numériques à été signée par le président Bill Clinton en octobre 1998. Elle porte le nom de « *Digital Millennium Copyright Act* » [16]. Cette loi interdit la modification des moyens numériques (tatouage, cryptage) protégeant la propriété intellectuelle. Elle interdit aussi le développement ou la vente d'outils permettant d'enlever ces protections numériques. Toute personne violant la loi pourra recevoir une amende allant jusqu'à 2500$.

En Algérie, c'est l'office national des droits d'auteur et des droits voisins (*ONDA*) qui s'en charge des problèmes des droits d'auteurs [17]. C'est un établissement public à caractère industriel et commercial. Il est régi par les dispositions pertinentes de l'Ordonnance 03-05 du 19 juillet 2003 relative aux droits d'auteur et aux droits voisins ainsi que par le décret exécutif 05/356 du 21/09/2005 portant ses Statuts. Conformément à l'article 5 des dits Statuts, l'*ONDA* a pour mission :

- la protection des intérêts moraux et matériels des auteurs ou de leurs ayants droit et des titulaires des droits voisins. Cette protection est assurée dans le cadre de la gestion collective à travers la simple protection,
- la protection des œuvres du Patrimoine culturel traditionnel et des œuvres nationales tombées dans le domaine public,
- la protection sociale des auteurs et des Artistes interprètes ou exécutants.
- la promotion culturelle, telle que définie à l'article 4 de l'annexe au décret 05/356. Dans ce cadre, l'*ONDA* exerce toutes les attributions lui permettant la prise en charge de ces missions.

L'*ONDA* étant membre de confédération internationales, agissant dans les domaines de sa compétence, (*CISAC* et *SCAPR*) il adopte, dans le cadre de son fonctionnement, les règles professionnelles, normes et standards arrêtés par ces dites associations.

I.5 Cryptographie, stéganographie et watermarking

La cryptographie, la stéganographie et le watermarking sont des techniques qui traitent de la protection et de la sécurisation de l'information, mais leurs premiers objectifs sont différents. Ce besoin de sécurisation est motivé par des problèmes de confidentialité et d'intégrité. Bien que la cryptographie et la stéganographie, qui font partie des sciences du secret, ont été utilisées avant le commencement de notre ère à des fins militaires et diplomatique, le watermarking est un domaine qui a émergé récemment et qui s'apparente beaucoup plus à la stéganographie. L'objectif de cette section est de passer en revue ces différents domaines en précisant les similitudes et complémentarités.

I.5.1 La cryptographie.

La cryptologie est une science qui existe depuis des siècles et plus précisément depuis l'invention de l'écriture. C'est une discipline qui regroupe d'une part : la cryptographie, mot grec signifiant écriture secrète, qui désigne l'art de chiffrer le contenu d'un message et le rendre inexploitable. D'autre part : la cryptanalyse, la technique opposée à la cryptographie et qui consiste à casser le code protégeant un message chiffré. Pour la petite histoire, au cinquième siècle avant J.C les habitants de Sparte ont laissé les premières traces de procédé cryptographique : une bandelette de parchemin était enroulée en spirale de manière très serrée le long d'un bâton. Le message était sur le bâton enveloppé puis le parchemin était détaché. Une personne qui ne possédait pas un bâton de même diamètre (faisant office de clé) ne pouvait pas enrouler correctement la bandelette et lire le message [18]. Ce furent les armées de Jules César qui utilisèrent le premier procédé de substitution : le message est crypté en substituant chaque lettre par une autre lettre d'un alphabet décalé. La clé représentait le nombre de lettres de décalage [19].

Avec l'avènement de l'ère numérique et notamment avec l'apparition de l'ordinateur, cette science de cryptologie a considérablement évolué. Elle est devenue une discipline de recherche publique de l'informatique théorique basée sur des outils mathématiques sophistiqués.

La cryptographie, qui est étroitement lié aux systèmes de communication, fut une première proposition pour sécuriser les documents numériques. Elle offre des outils permettant d'assurer la confidentialité (chiffrement), l'intégrité (hachage, signature) ou encore l'authentification (protocoles de type défi-réponse). Les procédés utilisés dans les algorithmes de chiffrage sont publiques, le secret réside uniquement dans la connaissance de la clé secrète. Cette dernière doit avoir une taille importante pour pouvoir éviter les attaques combinatoires. Seule la connaissance de cette clé et du moyen de cryptage peut permettre de décoder le message et le rendre accessible. Mais une fois décrypté, le document ne présente alors aucune protection et peut être distribué malhonnêtement. En plus, il est impossible d'exposer librement les documents protégés. Par exemple, ce type de protection serait inapproprié pour une galerie en ligne.

Deux schémas algorithmiques sont utilisés dans les techniques de la cryptographie :

- les algorithmes symétriques qui utilisent la même clé dans les procédés de cryptage et décryptage du document,

- les algorithmes asymétriques dont lesquels deux clés différentes sont utilisées : une clé privée pour crypter et une autre clé publique pour décrypter.

L'un des schémas les plus connus est le procédé *RSA* utilisé pour crypter de nombreuses transactions sur Internet (voir annexe A).

Avec l'arrivée des réseaux et des œuvres multimédias des problèmes sont apparus que la cryptographie ne pouvait résoudre seule. Les solutions sont portées par les techniques de dissimulation de données ou « data hiding », qui depuis une dizaine d'années constitue un domaine de recherche de plus en plus important. Ces techniques ont pour objectif de cacher un message utile dans un message de couverture. Selon le contexte on distingue : la stéganographie et le tatouage (watermarking).

I.5.2 La stéganographie.

Le mot stéganographie vient du grec '*steganos*' (caché ou secret) et '*graphy*' (écriture ou dessin) et signifie littéralement 'écriture cachée'. Si la cryptographie est l'art de secret, la stéganographie est l'art de dissimulation : son objet est de faire passer inaperçu un message secondaire dans un message primaire. Le message primaire reste lisible à tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires d'une information secrète. L'apparition de la stéganographie est très ancienne et elle est à peu près contemporaine de celle de la cryptographie. La première trace écrite se trouve dans les histoires de l'historien grec Hérodote, parues vers 445 av J.-C, à travers deux récits. Le premier relate l'histoire d'Histiée, ancien tyran de Milet, qui incite son gendre d'Aristagoras, le nouveau tyran de Milet, à se révolter contre son roi Darius. Pour transmettre son message à Aristagoras, il eut l'idée de raser la tête de son esclave le plus fidèle, de lui tatouer son message sur le crâne et d'attendre que les cheveux repoussent avant d'envoyer l'esclave pour Milet, avec pour consigne de se faire raser les cheveux. Un autre passage des histoires relate l'histoire de Demarate, ancien roi de Sparte réfugié auprès du roi des Perses, Xerxès Ier, qui a succédé à Darius. Demarate fut mis au courant d'un projet d'invasion de la Grèce. Il décida alors de prévenir Sparte en toute discrétion en utilisant le stratagème suivant : « il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis » Les tablettes étant arrivées à Sparte, la reine Gorgô fit gratter la cire et découvrit ainsi le message de Démarate. [20].

Ces histoires racontées par Hérodote illustrent déjà les deux principales méthodes de stéganographie utilisées au cours des siècles. On pourra essayer de cacher physiquement

l'existence d'un message, comme sur le crâne d'un esclave. Ou alors on dissimulera le message sur un support qui transmet déjà de l'information, comme les tablettes de cire. Ces deux méthodes ont toujours cohabité, même si la seconde fut sans doute plus populaire.

Une autre technique de stéganographie est l'utilisation d'encres sympathiques ou invisibles. Cette technique était très utilisée au moyen âge pour envoyer des messages secrets. On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait, de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message [21].

Durant la seconde guerre mondiale, en plus des techniques de l'encre invisible, des méthodes plus sophistiquées furent utilisées à l'aide de moyens modernes, comme les microfilms cachés sous des timbres postes ou sur des couvertures de magazine. Les microfilms sont de toutes petites photographies (de la taille d'un caractère), mais qui peuvent contenir l'équivalent d'une page de livre. Cette technique était très appréciée par les Allemands [22].

Donc la stéganographie se distingue de la cryptographie dans la mesure où l'objectif principal de la cryptographie est de rendre illisible le message à toute personne ne possédant pas l'information secrète adéquate. De plus, alors la cryptographie offre une sécurité plutôt a priori (par exemple, contrôle d'accès), la stéganographie offre une sécurité plutôt a posteriori, dans la mesure où le message secondaire est supposé rester accessible après recopies et manipulations du message primaire.

Avec l'avènement de l'informatique et le développement des échanges électroniques, les possibilités de cacher un message se sont multipliées : on peut cacher un message dans un texte, une image, un site internet, un programme ou une musique. La stéganographie a aussi trouvé des applications commerciales avec l'émergence d'un nouvel axe de recherche qui est le tatouage numérique ou « digital watermarking ».

I.5.3 Le watermarking ou tatouage numérique.

Le tatouage (appelé aussi filigrane en anglais watermark) est une technique qui trouve ces origines dans le marquage des documents papier et des billets. Cette technique a longtemps servi comme preuve d'originalité et d'un mécanisme pour prévenir la contrefaçon. En effet, on peut trouver les premiers filigranes sur des papiers du treizième siècle, dans le but de garantir leur qualité. Sur un billet de banque, les fibres sont marquées au moment de la sortie du bain d'eau, ce qui est à l'origine du terme anglais « *water mark* ».

Aujourd'hui, et avec la prolifération des documents numériques, le tatouage numérique (digital watermarking) se présente comme solution alternative ou complémentaire aux techniques précédentes pour résoudre les problèmes de sécurisation de ces documents. Comme la stéganographie, le tatouage numérique se propose de dissimuler ou d'enfouir au sein d'un document une signature (marque ou watermark) indélébile et imperceptible, tout en lissant le document marqué exploitable. Cette signature, qui est intrinsèquement liée aux données du document, permet de résoudre des problèmes de droits d'auteur ou augmenter la fonctionnalité du document. Dans le contexte de la protection des droits d'auteurs, la marque insérée correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelque soient les traitements (innocents ou malveillants) que subit le document marqué, la marque doit rester détectable tant que le document est exploitable et ceci uniquement par les personnes autorisées possédant la clé privée de détection.

Les premiers articles traitant ce sujet de watermarking sont apparus au début des années 90 avec l'article de Tanaka sur une méthode pour cacher de l'information dans une image [23]. Le terme digital watermarking (tatouage numérique) fut pour la première fois employé en 1992 par Andrew Tirkel et Charles Osborne [24]. En fait, le terme utilisé par Tirkel et Osborne est originaire du Japon : denshi sukashi qui se traduit en anglais par "electronic watermark". Paul Levinson parle également de tatouage numérique. Il préconise dans son ouvrage l'utilisation de numéros de brevets intelligents, en embarquant dans chaque élément technologique une puce électronique qui donnerait la liste des inventeurs [25]. Ingmar Cox popularisa les techniques d'étalement de spectre pour le tatouage numérique [26]. Depuis 1995, l'explosion du nombre de publications et de brevets à ce sujet a fait du watermarking un domaine majeur surtout en traitement d'image. Très vite, de nombreux laboratoires et industriels se sont intéressés à ce domaine. Ce qui est concrétisé par la création de l'atelier *IHW (Information Hiding Workshop*) en 1996, d'une conférence spécifique au sein de *SPIE* en 1999 et de l'atelier *IWDW* (*International Workshop on Digital Watermarking*) en 2002. Quatre journaux dédiés aux problématiques de sécurité de l'information ont été crées : *IEEE Trans. on Information Forensics and Security* et *IEE Proc. Information Security en 2005, LNCS Transactions on Data Hiding and Multimedia security* et *EURASIP Journal on Information Security en 2006*. Cette dynamique a induit une prolifération d'entreprises dans le domaine du watermarking. Digimarc, firme pionnière et leader sur le marché, rassemble des brevets de base sur le tatouage notamment celui de l'estampillage dont elle vend la licence.

Elle est également auteur du module de tatouage des logiciels de traitement d'image bien connus comme *Adobe Photoshop*, *Paint Shop Pro* ou bien encore *Corel Draw*. Son concurrent *Verance* fournit les outils de contrôle de flux audiovisuel *Broadcast Verification* et *ConfirmMedia*. La compagnie *Liquid Audio* fournit également un système de tatouage audio. Le *SDMI* (*Secure Digital Music Initiative*) est un consortium de compagnies pour un projet de tatouage audio. Les associations japonaises *JASRAC* et *RIAS* sont également actives dans ce domaine. En France, *Nextamp* et *MediaSec*, filiales de Thomson, s'intéressent au suivi et à la sécurité vidéo. Notamment, l'institut National de l'audiovisuel (*INA*) utilise le système de tatouage vidéo de Thomson pour une application de suivi des transactions : le document téléchargé contient le nom de l'acheteur. L'institut Fraunhofer (créateur du *MP3*) a annoncé en 2006 avoir développé un logiciel de tatouage audio commercialisable [14]. On outre, le mot clé « watermarking » a fait son apparition dans les instances internationales relatives à *JPEG-2000* [27], *MPEG-4* [28], ou encore *DVD* [29].

I.6. Les éléments d'un système de watermarking

Selon un point de vue généralisé, un système de watermarking est un peu comme un système de communication composé de trois éléments principaux: un émetteur, un canal de communication, et un récepteur. Pour être plus précis, l'insertion de l'information à cacher dans le signal hôte joue le rôle de transmission de données; tout traitement appliqué au signal hôte après la dissimulation de l'information, ainsi que l'interaction entre les données de l'information cachée et ceux du signal hôte lui-même, représente la transmission à travers un canal de communication, la récupération de l'information cachée à partir des données de l'hôte joue le rôle de récepteur. Par analogie aux systèmes de communication, tout système de watermarking prend la forme donnée sur la figure (I.1) [1].

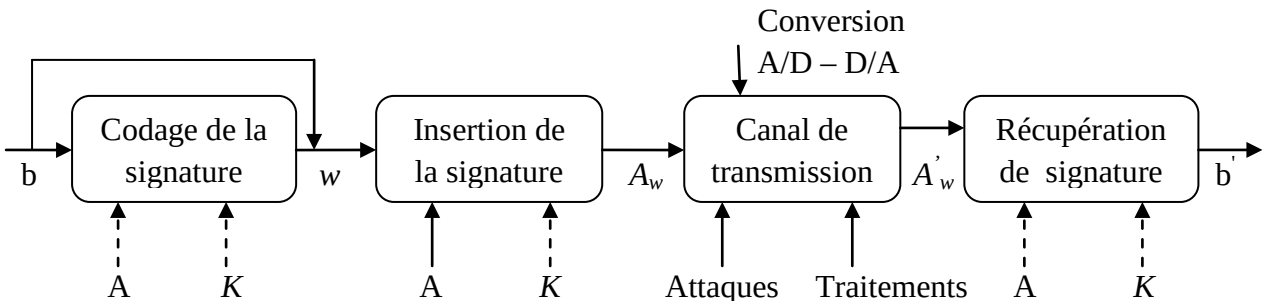


Figure I.1 Schéma général d'un système de watermarking

L'information de la signature à cacher au sein des données du signal hôte représente l'entrée même du système. Sans perdre de généralité, nous supposerons que cette information est donnée sous la forme d'une chaîne binaire

$$b = (b_1, b_2, ..., b_k) \qquad (I.1)$$

Avec $b_i \in \{1,0\}$. Nous nous référerons à la chaîne **b** comme étant le code de watermark (à ne pas confondre avec le signal de watermark qui sera présenté plus tard).

Du côté de l'émetteur, un module d'insertion incruste la chaîne **b** dans les données du signal hôte. Ce dernier peut être un fichier audio, une image fixe, une séquence vidéo, etc.….

Il est généralement désigné par le symbole (*A*) sauf lorsque sa nature exacte ne peut être négligée. Dans ce cas, les images fixes et les vidéos sont désignés par le symbole (*I*) et l'audio par (*S*). Le module d'insertion peut accepter une clé secrète *K*, en tant qu'entrée supplémentaire. Une telle clé, dont l'objectif principal est d'introduire un certain secret pendant la phase d'insertion, est généralement utilisée pour paramétrer le processus d'intégration et rendre la reprise ou la détection du watermark impossible pour les utilisateurs non autorisés qui n'ont pas accès à *K*.

Donc transmettre un message par le support d'un document comporte trois phases : l'insertion du message dans le support, la diffusion du document marqué et enfin l'extraction du message. Les briques de cet enchaînement résumé par la figure (I.1) seront détaillées dans les sections suivantes.

I.6.1 insertion du message

La fonctionnalité du module d'insertion du message ou de la signature peut être subdivisée en trois tâches principales:

a- codage de la signature.

b- insertion de la signature.

c- dissimulation de la signature.

a- Codage de la signature

Dans de nombreux systèmes de tatouage, le message d'information **b** n'est pas incorporé directement à l'intérieur du signal hôte. En effet, avant l'insertion le code du watermark (**b**) est transformé en un signal watermark **(*w*)** plus approprié pour l'incorporation.

$$w = (w_1, w_2, ..., w_n) \qquad (I.2)$$

Cette transformation ou ce codage consiste en l'ajout de (*k*) bits de redondance aux (*n*) bits d'information de la signature, les (*k*) bits supplémentaires servant à corriger les perturbations du canal de transmission. Le choix du code à employer dépend de ses performances, c'est à dire de la faculté à corriger les perturbations du signal d'entrée. Ce choix doit prendre en compte les propriétés du bruit qui perturbe le canal de transmission. Les méthodes présentées ci-dessous s'inspire de la théorie de l'information et des techniques utilisées dans le domaine des communications numériques.

- **Etalement de spectre**

En s'appuyant sur l'observation que les communications numériques par des canaux très bruités, susceptibles d'être affectés par des perturbations intentionnelles tels que le brouillage ou les interférences, sont généralement basés sur les techniques d'étalement de spectre, plusieurs algorithmes de tatouage ont été développés et qui utilisent une technique similaire pour coder l'information de la signature à dissimuler dans le document hôte. 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 via un même canal de transmission [30] [31].

- **Etalement par séquence direct** : l'étalement de spectre est réalisé directement dans le domaine spatial ou temporal. Le spectre du message *M*, qui est basse fréquence, est étalé par modulation à l'aide d'un signal large bande *PN* (possédant les caractéristiques d'un bruit blanc). Cette modulation permet d'obtenir un signal M_e possédant les mêmes caractéristiques spectrales de *PN*.
- **Etalement par saut de fréquence (frequency hopping) :** le principe de cette technique consiste à moduler le signal signature par une porteuse dont la fréquence varie de manière aléatoire. Le signal résultant est ainsi réparti dans l'ensemble de la gamme de fréquence où est choisie la porteuse. Donc cette technique permet d'assurer en plus un cryptage du message. En effet, la connaissance de la porteuse qui dépend éventuellement d'une clé secrète est indispensable pour la récupération du signal signature.

- **Codes correcteurs d'erreurs**

Le codage de la signature peut s'effectuer en utilisant des codes correcteurs d'erreurs. Les travaux présentés dans les articles [32][33][34][35] font références à une utilisation potentielle de ces codes correcteurs d'erreurs pour améliorer la robustesse des algorithmes de tatouage. L'emploi de tels codes apparaît en effet naturel si le problème de la robustesse du tatouage est

pris de point de vue communication d'un signal sur un canal bruité. L'usage des codes correcteurs dans le cadre du tatouage reste un sujet ouvert, nécessitant la conception de codes compacts capables de prendre en compte la diversité des attaques. Plusieurs catégories de ces codes correcteurs, utilisés dans le processus de mise en forme de la signature, sont présentées dans [36] dont quelques un sont cités ci-dessous :

- **les codes en blocs linéaires** (n,k) sont composés de $M=2^k$ séquences binaires de longueur *n*. Toute combinaison linéaire de mots du code forme également un mot de code,
- **les codes linéaires cycliques** représentent la classe la plus importante des codes en blocs linéaire. Toute permutation circulaire à gauche de *j* éléments binaires d'un mot de code redonne un mot de code. Pour ces codes, on utilise généralement une représentation polynomiale des mots du code plutôt qu'une représentation vectorielle. Les codes (*BCH*) et les codes de Reed-Solomon sont des exemples de ces codes linéaires cycliques,
- **les codes convolutifs** constituent une seconde famille de codes correcteurs d'erreurs au moins aussi importante que les codes en blocs. Pour être générer, ils utilisent des registres à mémoires. Un code généré selon un symbole dépend aussi de la valeur du symbole précédent. Le codage de Viterbi [37] et celui de Fano [38] sont les plus connus des codes convolutifs,
- **les Turbo Codes** représentent une autre façon de construire des codes avec une distance minimale élevée en partant de codes simples et moins performants. Plus précisément, dans leur forme de base, les turbo-codes sont construits par la concaténation parallèle de deux (ou plusieurs) codes convolutifs. Le principal avantage de turbo-codes est la possibilité de décoder de manière itérative à un coût de calcul qui est à peu près le même que le coût de décodage des codes constitutifs.

- **Codes à répétition**

Il s'agit d'un moyen intuitif pour protéger un message, puisqu'il consiste à répéter *n* fois chacun de ses éléments binaires. A chaque bit du message est associé un mot de code de taille *n*. Le décodage peut simplement s'effectuer par moyennage et seuillage des mots reçus. Ce principe de codage est très simple à mettre en œuvre et s'avère souvent efficace lorsque le canal est tés perturbé (capacité très faible).

- **Concaténation de codes**

La concaténation permet d'associer des types de codes différents. Les codes utilisés peuvent être un code à répétition et des codes linéaires ou convolutifs. L'intérêt majeur de la concaténation des codes réside dans l'obtention d'un code de distance minimale élevée, donc puissant, tout en maintenant une complexité de codage et surtout de décodage raisonnable. On distingue généralement deux types de concaténations :

- Série : en premier lieu le message est codé par le code externe, ensuite le code résultant est codé par un codeur interne.
- Parallèle : le message est codé par le code C_1 donnant une séquence S_1 et parallèlement, après un entrelacement facultatif, il est codé par un code C_2 produisant une séquence S_2. Le mot de code résultant est le couple (S_1, S_2).

Finalement, **b** peut être laissé tel quel, conduisant ainsi à un schéma dans lequel le code de watermark est directement insérée dans (*A*). Dans ce cas, le signal de watermark (***w***) coïncide avec le code watermark (**b**).

b- Insertion de la signature

L'opération d'insertion de la marque peut être modélisée par une fonction $\mathcal{E}$ qui prend en entrée le document hôte (à tatouer), le signal watermark (***w***) et une clé (*K*) pour générer en sortie le document marqué ou tatoué A_w :

$$\mathcal{E}(A, w, K) = A_w \qquad \text{(I.3)}$$

Il est à noter que l'équation (I.3) reste valable même lorsque le code de watermark est inséré directement dans *A*, car dans ce cas, nous avons simplement ***w*** = **b**. La définition de $\mathcal{E}$ passe en général par la sélection d'un ensemble de caractéristiques (ou de points d'intérêts) du document hôte, qui sont modifiées en fonction du signal watermark. Cet ensemble de caractéristiques est désigné par $F(A)= f_A = \{f_1, f_2,.....f_m\} \in \mathbb{F}^m$ et l'insertion du watermark revient à définir un opérateur d'insertion (*) qui transforme $F(A)$ en un ensemble de caractéristiques marquées $F(A_w)$ c'est à dire :

$$F(A_w) = F(\mathcal{E}(A, w, K)) = F(A) * w \qquad \text{(I.4)}$$

En général m, qui est le cardinal de l'ensemble des caractéristiques à marquer, ne doit pas nécessairement être égale à la longueur du signal du watermark.

Bien que les équations (I.3) et (I.4) décrivent principalement le même processus, à savoir l'insertion du watermark dans le document (*A*), elles ont tendance à considérer le problème de l'insertion sous deux angles différents. Selon (I.3), l'insertion est plus

naturellement réalisée en agissant sur le document hôte, c'est à dire modifie (A) de sorte que lorsque la fonction d'extraction F est appliquée à A_w, l'ensemble des caractéristiques marquées $f_{Aw} = \{f_{w1}, f_{w2}, \ldots..f_{wm}\}$ est obtenu.

L'équation (I.4) tend à décrire le processus d'insertion comme étant une modification directe de l'ensemble des caractéristiques f_A par l'opérateur (*). Selon cette formulation, le processus d'insertion du watermark prend la forme indiquée sur la figure (I.2) suivante.

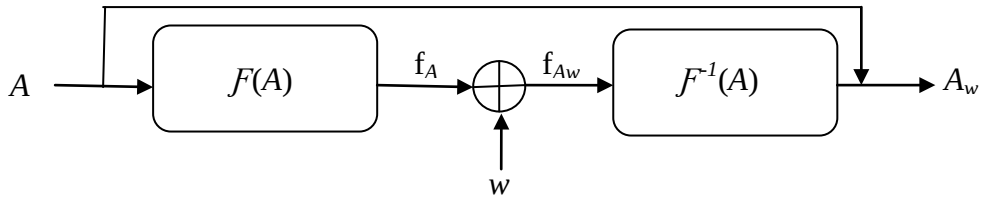


Figure I.2 Insertion du watermark via l'extraction de caractéristiques inversible

En premier lieu, l'ensemble des caractéristiques f_A est extrait du document hôte (A), ensuite l'application de l'opérateur (*) produit f_{Aw} , et enfin le processus d'extraction est inversé pour obtenir A_w.

$$A_w = F^{-1}(f_{Aw}) \qquad \text{(I.5)}$$

La nécessité d'assurer que F^{-1} soit inversible peut être assouplie en permettant à F^{-1}d'exploiter la connaissance de (A) pour obtenir (A_w). Il s'agit dans ce cas d'une faible inversibilité.

$$A_w = F^{-1}(f_{Aw,}\, A) \qquad \text{(I.6)}$$

A titre d'exemple, considérant un système de watermarking dont lequel le watermark est inséré dans les coefficients de l'amplitude *DFT* (la transformé de Fourier discrète) du document hôte. La procédure d'extraction des caractéristiques (points d'intérêts) n'est pas strictement inversible du moment qu'elle écarte l'information de la phase de la *DFT*. Cependant, l'information de phase peut être facilement récupérée à partir du document hôte original, une possibilité admise par la formulation (I.6). Une description schématique de la procédure est donnée sur la figure (I.3).

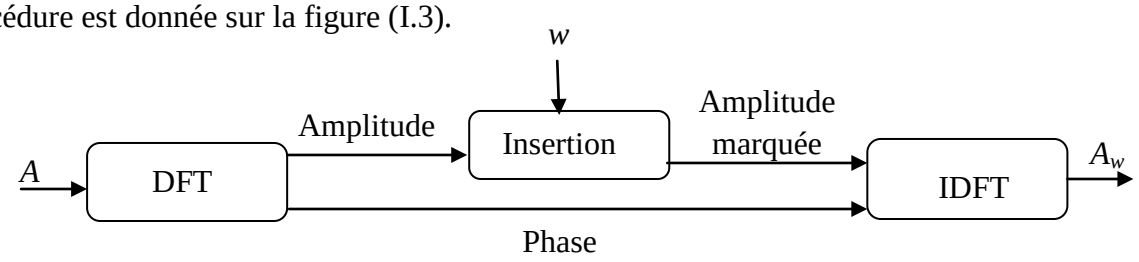


Figure I.3 Exemple d'insertion du watermark dans l'amplitude de *DFT*

Il est à noter que ni l'inversibilité stricte, ni faible de F n'est demandée en général, puisque $\mathcal{E}$ peut être définie comme une fonction opérant directement dans le domaine spatial (équation (I.3)).

c- dissimulation de la signature

La préoccupation principale de la partie insertion d'un système de dissimulation des données est de rendre les données cachées imperceptible. Cette tâche peut être réalisée soit implicitement, en choisissant correctement l'ensemble des caractéristiques (points d'intérêts) et la règle d'enfouissement, ou explicitement par l'introduction d'une étape d'occultation après l'insertion du watermark. Dans ce but, les propriétés des sens humains doivent être soigneusement étudiés, du moment que l'imperceptibilité repose en fin de compte sur les imperfections de ces sens. Ainsi, le tatouage des images fixes et les séquences vidéo s'appuient sur les caractéristiques du système visuel humain (*HVS*), tandis que le tatouage des documents audio exploite les propriétés du système auditif humain (*HAS*).

Donc, avoir une idée claire des mécanismes sur lesquels repose la perception des stimuli visuels et auditifs peut aider au bon contrôle et réglage de la phase d'insertion du watermark et en particulier de son invisibilité.

I.6.2 diffusion du document marqué et attaques

Après l'insertion de la marque le document marqué est diffusé dans le canal, c'est à dire qu'il subit une série de manipulations ou de modifications. Il est parfois nécessaire de changer de format, de passer par des canaux analogiques (qui nécessite une transformation numérique/analogique)….etc. On distingue les attaques involontaires (ou innocentes) des attaques malveillantes (ou malicieuses). La compression avec perte (*JPEG* pour image et *MP3* pour la musique), les conversions A/N et N/A ou encore les traitements courants des documents (filtrage, égalisation, transformations géométriques….) sont des exemples de ces attaques involontaires. Par contre, les attaques malveillants ont pour but soit de détecter la marque et la supprimé ou la remplacer par une autre, soit empêcher complètement son extraction. Plusieurs travaux ont proposé de telles attaques adaptées à un type de tatouage précis [39], [40], [41]. Ces attaques sont indépendantes de la clé utilisée lors de l'insertion. Les lois de Kerckhoffs [42] enseigne que la sécurité d'un système repose sur la clé et non pas sur le secret de l'algorithme. De ce fait, même si l'attaquant connaît parfaitement l'algorithme de tatouage utilisé, la présence d'une clé secrète empêche la connaissance de la forme exacte

du signal watermark (*w*) inséré. Il est clair que des attaques qui entraînent des dégradations trop importantes, rendant le document inexploitable, auraient très peu d'intérêt, même si elles étaient susceptibles de conduire à la neutralisation du tatouage. On distingue principalement trois types d'attaques : les attaques liées au signal, les attaques de nature cryptographique et les attaques de protocoles. Nous nous reviendrons sur ce problème d'attaques avec une présentation détaillée dans le chapitre (II) concernant le tatouage d'image fixe.

I.6.3 Récupération de la signature (watermark)

Le module de récupération ou d'extraction de signature peut avoir deux formes différentes. Selon le schéma donné sur la figure (I.4.a), le détecteur du watermark utilise le document tatoué et attaqué (A'_w) et le code watermark (b) pour décider si (A'_w) contient (b) ou non. Le détecteur peut exiger la connaissance de la clé (*K*) utilisée pour l'insertion de la signature. En plus, le détecteur peut réaliser cette tâche en comparant (A'_w) avec le document original (*A*) comme il peut prendre la décision sans faire recours à (*A*).

Alternativement, le module d'extraction peut fonctionner selon le schéma de la figure (I.4.b). Dans ce cas le code watermark (b) n'est pas connu d'avance. L'objectif du module d'extraction est d'extraire (b) de (A'_w). Cette opération, comme pour le cas précédant, exige la connaissance apriori de (*A*) et de (*K*).

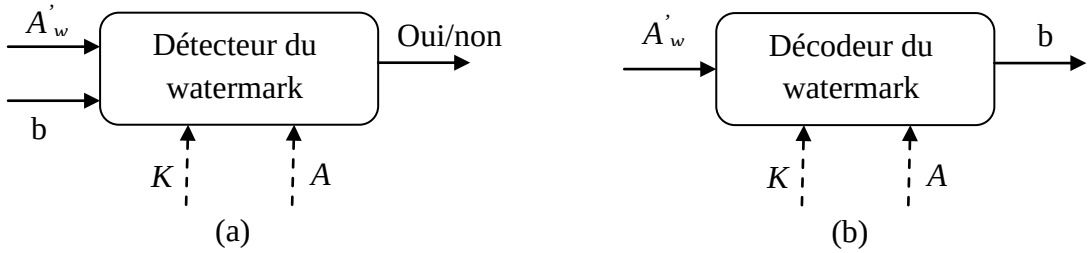


Figure I.4 Les deux formes du module de récupération de la signature

La distinction entre le watermark lisible et détectable peut être en outre mis en évidence en considérant les différentes formes prises par la fonction de décodage / détection (*D*) caractérisant le système. Par conséquent, plusieurs modes d'extraction de la signature sont envisageables et le choix du modèle dépendra de l'application visée et des protocoles utilisés :

Mode non-aveugle : (ou tatouage privé) dans ce cas de situation la présence du document originale est nécessaire. Si la fonction (*D*) extrait la signature, il s'agit d'un watermark lisible. La fonction (*D*) accepte en entrée trois arguments.

$$D(A'_w, A, K) = b \qquad (I.7)$$

Si la fonction (D) détecte la présence de la signature, il s'agit d'un watermark détectable. La fonction (D) accepte en entrée quatre arguments (sa sortie sera 1 si la signature est détectée 0 si non)

$$D(A'_w, A, b, K) = \text{oui/non (1/0)} \qquad (I.8)$$

La présence du document original à la détection facilite la création du schéma général de tatouage (implémentation et détection) et apporte beaucoup de robustesse à ce schéma. Cependant, ce contexte est bien évidement incompatible avec des applications visant à vérifier l'intégrité d'un document, ou à assurer la vérification en temps réel du copyright (problème de temps d'accès à la base de données contenant les informations originales).

Mode semi-aveugle : (ou tatouage semi-privé) le document original n'est pas connu apriori contrairement à la signature originale supposée connu lors de l'extraction et utilisée le plus souvent via un score de corrélation

$$D(A'_w, b, K) = \text{oui/non (1/0)} \qquad (I.9)$$

Mode aveugle : (ou tatouage public) il s'agit du seul mode où l'on peut réellement parler d'extraction de la signature, puisque l'on ne présuppose ni la connaissance du document original, ni la connaissance de la signature. La robustesse du schéma ne repose ici que sur la connaissance de la clé.

$$D(A'_w, K) = b \qquad (I.10)$$

C'est le mode d'extraction le plus intéressant, mais également le plus difficile à mettre en œuvre. Il faut donc apporter beaucoup de soin à anticiper les attaques possibles. Ce mode est - utilisable dans tous les cas de tatouage nécessitant une clé privée.

Mode asymétrique : la détection par algorithmes asymétriques ou à clé publique peut être schématisée comme une détection aveugle, la clé secrète de détection étant connue de tous. Une des principales difficultés de ce type de tatouage est d'empêcher la destruction de la marque ou son invalidation alors que tous les utilisateurs connaissent l'algorithme employé et la clé. C'est pour cela que l'on utilise des algorithmes asymétriques où la clé d'implantation de la marque n'est pas la clé de détection.

I.7 Contraintes d'un système de watermarking

Les principales contraintes techniques à prendre en compte pour concevoir un algorithme de tatouage performant sont les suivantes : Imperceptibilité, Robustesse, Complexité et Capacité.

I.7.1 Imperceptibilité

Le tatouage numérique consiste à insérer un tatouage ou une signature dans un document numérique (image, son vidéo….). La modification s'effectue dans les composantes perceptibles (comme la luminance des pixels d'une image), et non dans l'en-tête d'un fichier par exemple. Ce tatouage doit pouvoir être détecté et décodé, mais aussi doit être imperceptible, c.-à-d. que la déformation doit être suffisamment faible pour que l'utilisateur ne puisse pas différencier le document tatoué de l'originale. Cette propriété est importante pour deux raisons. La première est évidente : le marquage ne doit pas empêcher la compréhension de l'œuvre, celle-ci doit garder toute sa qualité artistique ou commerciale. Une autre raison est, qu'ainsi cachée la marque est plus difficilement détruite par piratage. Prenons deux exemples très simples pour souligner son importance. Imaginons une image en niveau de gris avec une large zone uniforme. Si l'on rajoute un peu de bruit, ceci va immédiatement se voir dans cette zone. Il faut plutôt mettre le tatouage dans des zones de fort gradient (contour de formes, zones fortement texturées,…) où l'œil est moins sensible. Un autre exemple vient du marquage des images couleurs. Il est connu que l'œil humain n'est pas sensible de la même façon à toutes les longueurs d'onde. On peut ainsi dissimuler plus ou moins d'informations suivant la teinte considérée.

Dans la plupart des algorithmes de tatouage proposés, l'imperceptibilité du tatouage s'obtient en utilisant diverses propriétés du Système Visuel Humain (*SVH*). Ces propriétés souvent trouvées à partir d'heuristiques, proposent des modélisations du comportement psychovisuel humain.

I.7.2 Robustesse

Le document tatoué est destiné à être distribué à grande échelle, il est donc amené à subir des déformations ou des attaques. Celles-ci peuvent être involontaires (innocentes) ou volontaires (malveillantes : pirate voulant endommager le tatouage). La robustesse à de telles attaques est l'une des propriétés importantes d'une méthode de tatouage. On pourrait séparer cette rubrique en deux parties : la *robustesse* et la *sécurité*. Ces deux caractéristiques sont souvent confondues surtout dans le cas du watermarking.

On parle de robustesse pour définir la résistance du tatouage surtout à des attaques innocentes. Dans le cas d'une image, ces attaques ou transformations peuvent être de type géométrique (rotation, zoom, découpage …). Elles peuvent modifier certaines caractéristiques de l'image (histogramme des couleurs, saturation…). Il peut aussi s'agir de tous les types de dégradations fréquentielles de l'image (compression avec pertes, filtres passe haut ou passe bas, conversion A/N ou N/A etc.…).

La sécurité caractérise la façon dont le tatouage va résister à des attaques malveillantes. On peut faire des parallèles avec la cryptanalyse. Le pirate va chercher à laver le document tatoué de façon intelligente. Il est sensé connaître l'algorithme et va, en général, chercher la clé qui lit le tatouage. Cela demande souvent une analyse approfondie de la technique de marquage employée. Comme dans toutes les disciplines proches de la cryptographie, c'est uniquement la confidentialité de la clé (K) qui assure la sûreté du système car la confidentialité des algorithmes mis en œuvre n'est pas garantie. Cette exigence correspond au deuxième principe de Kerckhoffs [42]. Donc l'utilisation d'une clé secrète (K) rend le schéma irréversible : il est impossible d'extraire la signature sans la clé secrète.

Même si le niveau exact de la robustesse que doit avoir la signature ou la marque à insérer ne peut être spécifié sans tenir compte d'une application particulière, on peut considérer quatre niveaux de robustesse qualitatifs englobant la plupart des situations rencontrées en pratique :

- **Watermark sécurisé** : dans ce cas, qui traitent principalement avec la protection du droit d'auteur, la vérification de la propriété ou d'autres applications axées sur la sécurité. Le watermark doit survivre aux attaques innocentes et malveillantes. En watermarking sécurisé, la perte des données cachées devrait être obtenue au détriment d'une dégradation importante de la qualité du signal hôte. Il est, cependant, important de souligner que même le système le plus sûr n'a pas besoin d'être parfait, au contraire, il est seulement nécessaire qu'un degré assez élevé de sécurité est atteint. En d'autres termes, la destruction du watermark n'a pas besoin d'être impossible (ce qui ne sera probablement jamais le cas), mais seulement assez difficile.
- **Watermark robuste** : dans ce cas, il est nécessaire que le watermark soit résistant seulement contre les manipulations innocentes. Bien sûr, le watermarking robuste est moins exigeant que le watermarking sécurisé. Les domaines d'application du tatouage robuste comprennent toutes les situations dans lesquelles il est peu probable que quelqu'un manipule les données du document hôte avec l'intention de supprimer le

watermark. En même temps, le scénario d'application est telle que l'utilisation, pour ainsi dire, normale de données comprend plusieurs types de manipulations qui ne doivent pas endommager les données cachées. Même dans des applications de protection du droit d'auteur, l'adoption du watermarking robuste au lieu de watermarking sécurisé peut être autorisée en raison de l'utilisation d'un protocole de protection du droit d'auteur dans lequel tous les acteurs concernés ne sont pas intéressés à enlever le watermark.

- **Watermark semi-fragile** : Dans certaines applications la robustesse n'est pas une exigence majeure, principalement parce que le signal hôte n'est pas destiné à subir des manipulations, mais un nombre très limité de modifications mineures telles que la compression avec perte modérée, ou l'amélioration de la qualité. C'est le cas, par exemple, des données d'étiquetage pour améliorer l'archivage, dans lequel les données cachées sont seulement nécessaire pour récupérer les données document hôte d'une archive, et de ce fait il peut être écartée une fois que les données ont été consultée correctement. Il est probable, cependant, que les données sont archivées dans un format compressé, et le watermark est inséré avant la compression. Dans ce cas, le watermark doit être robuste contre la compression avec pertes. En général, nous disons que le watermark est semi-fragile s'il survit seulement à un nombre limité, voir bien défini, de manipulations qui laissent la qualité du document hôte virtuellement intact.
- **Watermark fragile** : le watermark est dit fragile si l'information cachée dans les données du document hôte est perdue ou altéré irrémédiablement dès qu'une modification est appliquée au signal hôte. Une telle perte d'information peut être globale, c'est à dire aucune partie du watermark ne peut être récupéré ou locale c'est à dire seulement une partie du watermark est endommagé. La principale application du watermarking fragile est l'authentification des données. En effet, la perte ou l'altération du watermark sera prise comme une preuve que les données ont été falsifiées, alors que la récupération de l'information du watermark contenue dans les données est utilisée pour certifier l'originalité du document.

I.7.3 Capacité

La troisième contrainte importante du tatouage est la capacité du watermark (*payload ou ratio*). C'est la quantité d'informations que l'on espère cacher par rapport à la quantité d'informations associée au document hôte. Bien qu'en général la capacité du watermark ne dépend pas de l'algorithme particulier utilisé, mais elle est plutôt lié aux caractéristiques du

signal hôte, de la distorsion induite par l'insertion du watermark et de la force des attaques que le document tatoué peut subir. Il est également judicieux de parler de la capacité d'une technique donnée, comme étant la quantité de bits d'information qu'elle est capable de transmettre d'une manière plus ou moins fiable. Donc il est très facile de comprendre que la capacité est une propriété fondamentale de tout algorithme de tatouage qui détermine très souvent si une technique peut être utilisée avec profit dans un contexte donné ou non. Une capacité plus élevée est toujours obtenue au détriment soit de la robustesse soit de l'imperceptibilité ou les deux ensembles. Il faut nécessairement faire un compromis entre ces trois contraintes robustesse, imperceptibilité et capacité et ceci en tenant compte de l'application visée figure (I.5).

La capacité du watermark dans le contexte de la protection des droits d'auteurs n'est pas primordiale : l'insertion d'un numéro d'identification codé sur 64 bits suffit dans la plupart des applications de protection des contenus. Un seul bit est nécessaire pour la protection des copies. La capacité devra cependant être plus importante dans le cas d'applications du tatouage pour la transmission de données cachées, par exemple à des fins d'augmentation ou d'enrichissement des contenus multimédias.

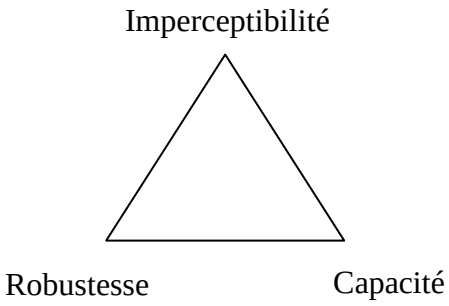


Figure I.5 compromis entre robustesse, imperceptibilité et capacité

I.7.4 Complexité

Dans la pratique, la plupart des opérations de tatouage doivent pouvoir s'effectuer en temps réel (surtout la détection, pour des films par exemple). Ceci implique une contrainte supplémentaire sur la complexité des opérations utilisées pour le marquage et pour la détection.

I.8 Domaines d'application du watermarking

Les applications du tatouage numérique (digital watermarking) sont nombreuses : leur diversité fait que les contraintes qu'elles imposent varient selon l'application envisagée. Les

contradictions existantes entre ces contraintes citées dans la section précédente rendent impossible la création d'un algorithme universel adaptable à toutes les applications.

Il paraît donc nécessaire que la première étape de la conception d'un algorithme de watermarking comprenne la définition des applications auxquelles la méthode sera destinée puisque celles-ci définiront les besoins du watermark. La littérature relative au watermarking décrit abondamment les utilisations possibles du watermarking [1][43][44][45] on distingue :

I.8.1 Protection des droits d'auteurs

La protection des droits d'auteurs est le scénario le plus classique servie par le watermarking. Ce dernier offre une alternative intéressante à la cryptographie car il permet de protéger le document même lorsque celui-ci est diffusé. Ce service reste cependant toujours d'actualité et fait l'objet de la majorité des publications. L'objectif est d'offrir, en cas de litige, la possibilité à l'auteur ou bien le propriétaire d'une œuvre d'apporter la preuve qu'il est effectivement ce qu'il prétend être. Pour ce faire, dès qu'il crée l'œuvre, il intègre également une signature l'identifiant sans ambiguïté. Malheureusement, ce schéma simple ne peut pas fournir une preuve valable devant un tribunal, à moins que la non-inversibilité de l'algorithme de watermarking soit démontrée.

Une façon courante de confier à la procédure de vérification du copyright une valeur juridique, est d'introduire la présence d'une tierce partie de confiance (*TTP*) dans le protocole de watermarking. Le watermark identifiant l'auteur peut lui être attribué par une Autorité de l'enregistrement de confiance. De cette façon, en fait, il serait plus difficile à inverser l'opération de watermarking, surtout quand le tatouage aveugle est utilisé. Et par conséquent, le pirate ne peut pas concevoir une ad hoc fausse originale œuvre.

En ce qui concerne les exigences qu'un algorithme de watermarking, utilisé pour la vérification du copyright, doit satisfaire : le watermark doit être sécurisé, étant donné que les pirates sont évidemment intéressés à le supprimer, éventuellement au moyen de procédures de calcul intensives. En outre, le tatouage privé est préférable, en raison de sa sécurité intrinsèquement supérieure. Enfin, les besoins en capacité dépendent du nombre de différents codes d'identification de l'auteur que le système peut supporter.

I.8.2 Le suivie de copie ou Fingerprinting

Une deuxième application classique de tatouage numérique est la protection contre la copie. Deux scénarios sont possibles: selon le premier, un mécanisme est prévu pour le rendre impossible, ou tout au moins très difficile, de faire des copies illégales d'une œuvre protégée (voir la section I.8.3 pour une discussion sur le mécanisme de contrôle de copie). Dans le

deuxième scénario, un mécanisme que l'on appelle la dissuasion contre la copie est adopté pour empêcher la duplication et la distribution non autorisée. La dissuasion de copie est habituellement obtenue en prévoyant un mécanisme permettant de retracer des copies non autorisées au propriétaire original de l'œuvre. Dans le cas le plus fréquent, le traçage de la distribution est rendue possible en laissant le vendeur (propriétaire) insérer un watermark distinct, appelé dans ce cas *Fingerprint* identifiant l'acheteur ou tout autre destinataire de l'œuvre, dans toutes les copies distribués. Si, plus tard, une copie non autorisée de l'œuvre protégée est trouvé, son origine peut être récupérée en récupérant le watermark unique qu'elle contient. Bien sûr, le watermark doit être sécurisé afin de prévenir toute tentative de l'enlever et lisible pour faire son extraction plus facile. L'identification d'un pirate peut conduire à des poursuites judiciaires. Mais il est difficile de conférer au *Fingerprinting* le statut juridique de preuve. De plus à cause du délai d'aboutissement d'une telle action, le *Fingerprinting* a plutôt une valeur dissuasive.

Un exemple concret d'application est le « paiement à la séance » sur les chaînes numériques et Internet. L'acheteur peut avoir l'intention de copie le document (film ou musique) pendant sa lecture pour le mettre ensuite à sa disposition. Savoir que le document est tatoué d'un numéro de série unique permettant aux ayants droits de remonter jusqu'à lui pourra éventuellement le dissuader de le pirater. Un autre exemple concernant les opérateurs de télévision à péage, qui rencontrent des difficultés dans l'identification des systèmes pirates et sont soumis à des coûts de renouvellement important des cartes à puce. Une identification des œuvres par *Fingerprinting* est intéressante à des fins techniques, comme la contribution au maintien de la protection par la révocation des systèmes pirates et le renouvellement des clés ou des systèmes compromis.

Le cadre le plus adapté à une telle application est celui des services interactifs, pour lesquels il est possible d'appliquer le *Fingerprinting* à la source, avant diffusion. Cela fait du *Fingerprinting* un outil très complémentaire de la cryptographie.

I.8.3 Contrôle de copie

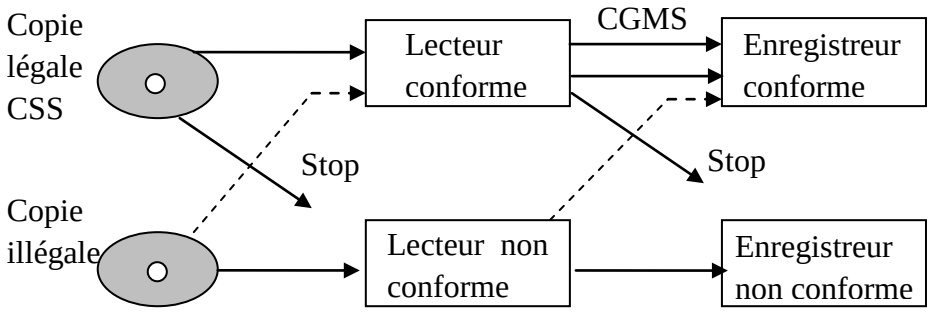
Contrairement aux données de nature analogique pour lesquelles une succession de reproductions entraîne rapidement une perte significative de la qualité, les données numériques peuvent être dupliquées quasiment à l'infini. Le cryptage d'un document ne suffit pas à assurer la protection de la copie : la sécurité est assurée le long du canal de transmission qui relie le vendeur à l'acheteur sous certaines hypothèses de robustesse ; mais une fois décrypté, le document n'est plus protégé et rien n'empêche le client de le copier. Face à cette

nouvelle situation, certaines instances proposent d'utiliser des techniques de watermarking afin de limiter l'ampleur de ce phénomène. Deux informations relatives à la copie et à l'utilisation sont encodées dans le watermark : il peut s'agir d'autorisations du type « pas de copies », « une seule copie », « plus de copies disponibles », ou encore « copie sans restrictions ». Le dispositif chargé de la lecture et/ou de la copie interroge le support en refusant de le lire ou de le copier si les données encodées ne le permettent pas.

La protection de la copie des *DVD* représente un exemple de ce genre d'applications [1][46][47]. En effet, les professionnels du cinéma et de la vidéo ont lancé une réflexion sur les différents moyens de protéger ce support. La coalition de nombreuses entreprises importantes appartenant aux domaines de la vidéo et du watermarking telles que *IBM, NEC,* Sony, Hitachi, Pioneer, Signafy, Philips, Macrovision et Digimarc, a proposée un schéma de protection de *DVD*. Son mécanisme se base sur la distinction entre les lecteurs et enregistreurs *DVD* conformes et non conformes. Les appareils conformes utilisent trois systèmes liés à des brevets permettant de restreindre la copie des *DVD* :

- Le *CSS* (*Content Scrambling System*) c'est un système de cryptage qui utilise deux clés, l'une propre au support *DVD* et l'autre au fichier de la vidéo enregistrée. Les deux clés sont stockées sur la zone d'entrée du *DVD*, une zone qui est seulement lu par les appareils conformes.
- Le *CGMS* (*Copy Generation Management System*), gère les droits de copie des *DVD*. Chaque *DVD* possède une information codée sur deux bits appelée *CCI* (*Copy Control Information*). Les deux bits sont stockées dans l'en-tête d'un flux *MPEG*, codant l'une des trois indications suivantes : copie libre (*copy-freely*), pas de copie (*copy-never*), une seule copie (*copy-once*). Par exemple, le résultat de l'indication une seule copie (*copy-once*) est que la vidéo peut être copié mais après la copie, les bits *CGMS* seront changées à l'état pas de copie (*copy-never*).

La figure (I.6) décrit le cas d'utilisation du système *CSS*. Un *DVD* protégé ne peut être lu est enregistré que par les appareils conformes. En effet, il n'est pas possible que la sortie d'un lecteur conforme soit connectée à un enregistreur non conforme, puisque d'une part les appareils conformes ne sont pas autorisés à dialoguer avec des périphériques non conformes, de l'autre côté, l'enregistrement au moyen d'appareils conforme est régi par le *CGMS*.



0 **Figure I.6**. *CSS* empêche seulement que les données légales ne soient pas transmises aux appareils non-conformes, alors que l'inverse est encore possible (lignes pointillées)

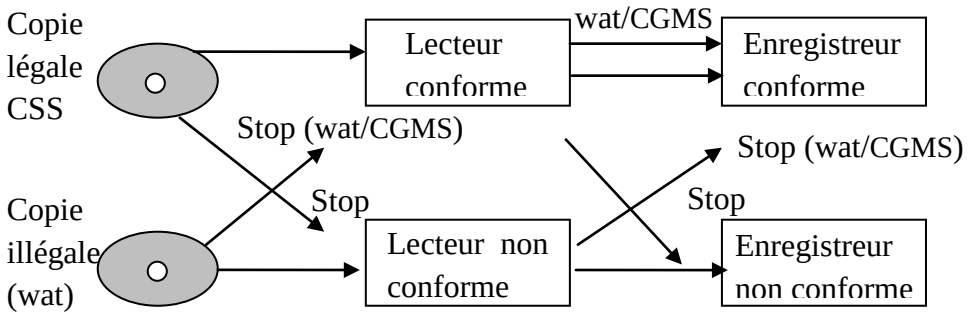


Figure I.7. L'utilisation du watermarking sépare le monde conforme du monde non conforme

Comme on peut le constater sur la figure (I.6), le *CSS* et le *CGMS* empêchent le flux du monde conforme envers le monde non conforme. Néanmoins, afin de décourager la copie illégale l'inverse doit aussi être vrai, c'est à dire, il ne devrait pas être possible d'utiliser un dispositif conforme pour lire ou enregistrer un disque illégal. Sinon, le mécanisme de protection ne ferait que favoriser la diffusion des dispositifs conformes. Dans ce but, le *CSS* seul n'est pas suffisant. Considérons, par exemple, le cas d'un pirate utilisant la sortie analogique *RGB* d'un lecteur conforme pour faire une copie non cryptée de la vidéo à l'aide d'un *enregistreur* non conforme. Une telle copie peut être lue et enregistrée aussi sur les dispositifs conformes car la vidéo illégale est confondue à une vidéo gratuite sans protection (absence de *CSS* et *CGMS*).

L'utilisation du watermarking permet de combler ces failles en insérant un watermark sécurisé au sein du flux *MPEG2*. Ce watermark se compose de deux informations : l'une contient les données *CCI* de *CGMS* permettant le contrôle de l'enregistrement sur les

enregistreurs conformes, l'autre indique si le *DVD* d'origine utilise le procédé *CSS*. Ainsi, les lecteurs conformes sont capables de lire uniquement les *DVD* légaux, et les lecteurs non conformes uniquement les DVD illégaux comme il est montré sur la figure (I.7).

I.8.4 Vérification de l'authenticité et l'intégrité d'un document numérique

Un des effets (indésirables) de la disponibilité de plus en plus efficace des outils de traitement du signal, et de leur utilisation possible de modifier le contenu visuel ou audio de documents numériques sans laisser de traces perceptibles de la modification, est la perte de crédibilité de données numérique. Car des doutes existent toujours qu'ils ont été altérés, d'une manière qui modifie substantiellement le contenu des données initiales. Une telle perte de crédibilité est dramatique si les données numériques doivent être utilisées légalement, par exemple comme preuve devant un tribunal. Toutefois, il peut avoir un impact important dans notre vie quotidienne. Pour surmonter un tel problème, il est nécessaire que des contre-mesures appropriées soient prises pour authentifier les signaux enregistrés sous forme numérique, c'est à dire de veiller à ce que les signaux n'ont pas été altérés (intégrité des données) et de prouver leur véritable origine.

Bien que la cryptographie puisse fournir un moyen précieux pour l'authentification des documents numériques, le développement d'approches alternatives est souhaitable afin de faire face à certaines faiblesses potentielles de la méthode cryptographique. L'authentification des données à travers le tatouage numérique (*Digital Watermarking*) représente une solution faisable et très élégante aux problèmes ci-dessus. D'une façon générale l'authentification d'un document numérique peut être réalisée soit par watermarking fragile, semi-fragile ou robuste.

Avec le watermarking fragile, l'information cachée est perdu ou modifié dès que le document hôte subit une modification: la perte du watermark ou son altération sera prise comme une preuve que les données ont été falsifiées, alors que la récupération du watermark contenu dans les données est utilisée pour démontrer l'intégrité des données et, si nécessaire, pour remonter à l'origine des données. D'autres modèles possèdent la capacité de localiser l'endroit de l'altération ou de discriminer entre les manipulations malveillantes et innocentes (par exemple la compression d'image modérée). Dans ce dernier cas, un système de tatouage semi-fragile doit être utilisé, car le watermark survit uniquement à un certain type de manipulations permises.

L'utilisation du tatouage robuste pour l'authentification des données repose sur un mécanisme différent: un résumé du document hôte est calculé ensuit associé aux informations sur l'origine des données, il est inséré dans le document lui-même au moyen de tatouage

robuste. Pour prouver l'intégrité des données, l'information véhiculée par le watermark est récupérée et comparée avec le contenu réel de la séquence: leur disparité est considéré comme une preuve de la modification des données. La capacité de localiser les manipulations dépendra de l'exactitude du résumé inséré.

Un système d'authentification des pièces d'identité basé sur le watermarking a été présenté par *Kutter et al*. [48]. Le watermark est inséré automatiquement dans la photo de la personne lors de sa prise. Ce watermark est unique et étroitement lié au numéro d'identité de la carte. En cas de falsification par changement de photo par exemple, la tentative de détection du watermark à partir du numéro d'identité permet de vérifier son absence dans la photo substituée et par conséquent la pièce d'identité a été falsifiée.

I.8.5 Combler le fossé entre les objets analogiques et numériques (indexation)

Une façon intelligente d'exploiter le tatouage numérique, consiste à relier un support de travail analogique au monde numérique en vue de l'obtention d'information sur le support. Le concept d'images intelligentes (*Smart images*) du système *MediaBridge* développé par la société « *Digimarc* » [49], est un exemple d'une telle vision de tatouage numérique. Selon le paradigme des images intelligentes, un watermark (jouant le rôle d'un pointeur) est inséré dans l'image. Ce watermark permet de lier l'utilisateur à l'information supplémentaire concernant cette image et stockée sur Internet. Par exemple, un tel watermark peut être utilisée pour lier une image sur un journal pour une page web pour explorer davantage le sujet de l'article dont lequel l'image est apparaît. Le lien à l'Internet est activé en montrant l'image imprimée à une webcam connectée à un PC, lors de l'extraction du watermark l'*URL* du site Web avec les informations pertinentes sont extraites et la connexion est établie.

I.8.6 Watermark visible

Pour certaines applications, l'insertion d'un watermark visible peut être envisagée. C'est le cas par exemple des petit logos qui apparaissent en haut à droite des images de journaux télévisés. Cette marque sert d'information aux consommateurs mais aussi d'argument dissuasif. Dans ce sens Craver et al. [50] ont développé une méthode pour la protection des images digitales, en insérant un logo translucide qui recouvre la totalité de l'image et sans gêner sa compréhension. Les avantages de cette méthode sont la facilité d'implémentation et de détection du watermark, les inconvénients sont évidemment une très grande fragilité aux attaques. En effet, il est très facile de supprimer la partie marquée de l'image et en reconstruisant l'image par interpolation. De plus, cette solution ne convient pas

par exemple pour la vente d'images hautes qualités, et devient ridicule si l'on travaille sur des signaux audio.

I.8.7 Autres applications

Bien évidemment il existe d'autres applications possibles en dehors de celles décrites précédemment. A titre d'exemple on peut citer l'exploitation d'un canal de communication caché, offerte par le watermarking, pour une meilleure transmission surtout la transmission vidéo qui gagne de plus en plus de consensus. La dissimulation de données (*data hiding*) peut être utile pour la transmission vidéo de plusieurs façons. De point de vue codage source, il peut aider à concevoir des systèmes de compression plus puissants où une partie de l'information est transmise en se cachant dans le flux binaire codé. Par exemple, les données de chrominance peuvent être insérées à l'intérieur du train de bits de transport des informations de luminance. Comme, les données audio peuvent être transmises en les cachant à l'intérieur de la séquence d'images vidéo (audio dans vidéo). Du point de vue codage du canal, la dissimulation de données peut être exploitée pour améliorer la résilience du flux de bits codés en ce qui concerne les erreurs de canal (auto-correction). De ce fait, les informations redondantes sur la vidéo transmise pourraient être cachées dans le train de bits codé et utilisé pour la reconstruction de la vidéo en cas où les erreurs du canal altèrent le flux de bits transmis.

Pour terminer cette section on peut dire qu'il est utopique d'espérer avoir un watermark imperceptible, de grande capacité et qui soit aussi robuste à une très grande variété d'attaques et de traitements. Il faut nécessairement chercher un compromis entre les trois contraintes citées précédemment en tenant compte des exigences de l'application visée c.-à-d. la fonctionnalité du watermark comme il est indiqué sur la figure (I.8).

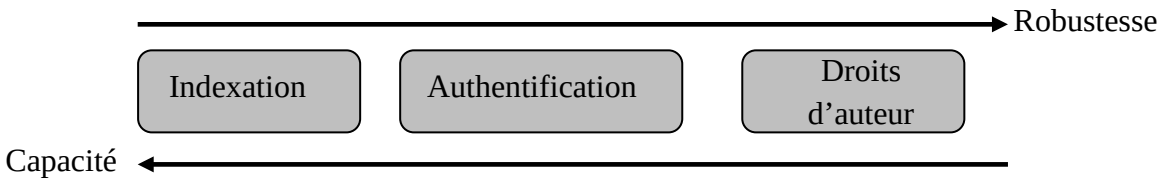


Figure I.8 Compromis entre robustesse et capacité du watermark pour différentes applications

I.9 Considération protocolaires

L'utilisation du watermarking dans des applications réelles, comme par exemple la protection des droits d'auteurs ou l'authentification des données, ne peut pas être achevée sans considérations protocolaires. En outre, il est instructif d'analyser les exigences que les

problèmes de protocole imposent sur la technologie du watermarking et vice versa comment les limitations technologiques du watermarking impactent la conception du protocole.

L'utilisation du watermarking pour la protection du droit d'auteur est un bon exemple de clarifier l'interaction étroite entre la dissimulation des données (*data hiding*) et l'analyse au niveau du protocole. Supposons, par exemple, que le watermark doit être utilisé pour identifier sans ambiguïté le propriétaire d'un document multimédia. On peut simplement insérer dans le document un code watermark avec l'identité du propriétaire du document. Bien sûr, le watermark doit être aussi robuste que possible, sinon un attaquant pourrait le supprimer et le remplacer par un nouveau watermark contenant son identité. Cependant, des attaques plus subtiles peuvent être considérées, appelant ainsi à une utilisation plus intelligente du watermarking. Supposons, par exemple, qu'au lieu de tenter de supprimer le watermark du propriétaire, l'attaquant ajoute simplement son watermark au document tatoué. Même, en supposant que le nouveau watermark n'efface pas le premier, la présence dans le document de deux watermarks différents rend impossible de déterminer le véritable propriétaire du document en lisant simplement le watermark (s) qu'il contient.

Pour être précis, nous supposons que pour protéger son œuvre (A), le propriétaire (X) ajoute un watermark avec son code d'identification (W_X), produisant ainsi un document tatoué $A_{WX} = A + W_X$, puis il le met à la disposition du public. Pour des raisons de piratage, (Y) prend le document tatoué et y ajoute son propre watermark (W_Y), en produisant un nouveau document tatoué $A_{WXWY} = A + W_X + W_Y$. Il est maintenant impossible de décider si A_{WXWY} appartient à (X) ou (Y), car il contient à la fois les watermarks des deux. Pour résoudre l'ambiguïté, (X) et (Y) peuvent être invités à montrer s'ils sont en mesure de présenter une copie du document qui contient leur filigrane mais ne contient pas le filigrane de l'autre candidat. (X) peut facilement satisfaire la demande, car il détient le document initial sans le code d'identification de (Y), alors que cela ne devrait pas être possible pour (Y), étant donné que le document entre ses mains est une copie du document tatoué de (X). Cependant, des précautions doivent être prises, pour ne pas être sensible à une attaque plus subtile connue comme l'attaque *SWICO* (*Single-Watermarked-Image-Counterfeit-Original*). Supposons, en effet, que la technique de tatouage utilisé par (X) n'est pas aveugle, c'est à dire pour révéler la présence du watermark le détecteur a besoin de comparer le document tatoué avec l'original (par exemple par une simple opération de soustraction). (X) peut utiliser le document original pour montrer que celui de (Y) contient son watermark et qu'il possède une copie du document A_{WX} contenant W_X mais pas W_Y, en fait:

$$A_{WXWY} - A = A + W_X + W_Y - A = W_X + W_Y \qquad \text{(I.11)}$$

$$A_{WX} - A = A + W_X - A = W_X \qquad \text{(I.12)}$$

Le problème est que (Y) peut faire la même chose en construisant un faux original document (A_f) pour être utilisé au cours de la procédure de vérification de la propriété. En se référant aux figures (I.9) et (I.10), il suffit que (Y) soustrait son filigrane de (A_{WX}), soutenant que le document original est $A_f = A_{WX} - W_Y = A + W_X - W_Y$. De cette façon ($Y$) peut prouver qu'il possède un document tatoué (A_{WX}), mis à la disposition du publique, qui contient W_Y mais ne contient pas W_X :

$$A_{WX} - A_f = A + W_X - (A + W_X - W_Y) = W_Y \qquad \text{(I.13).}$$

Comme on peut le constater, le tatouage en mode non-aveugle (privé) d'un document par un simple ajout d'un watermark n'est pas suffisant pour prouver la propriété, même si le watermark ne peut être enlevée sans détruire le document tatoué.

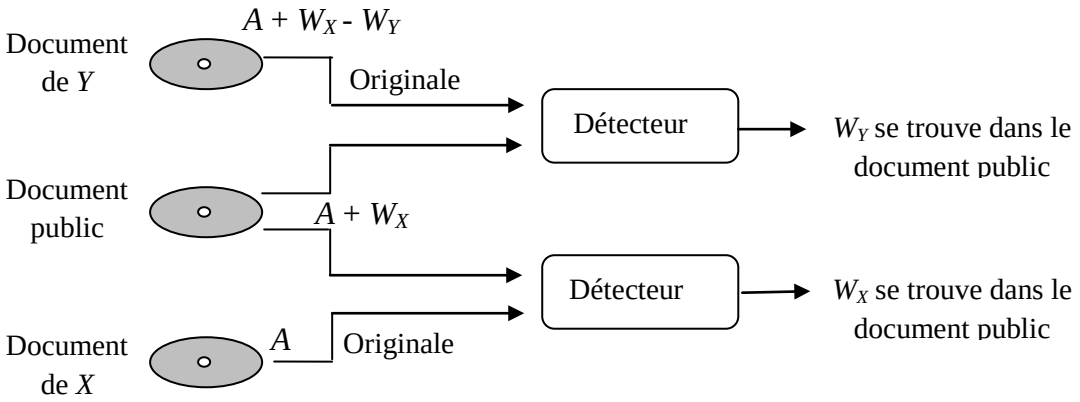


Figure. I.9. Le premier exemple d'attaques SWICO

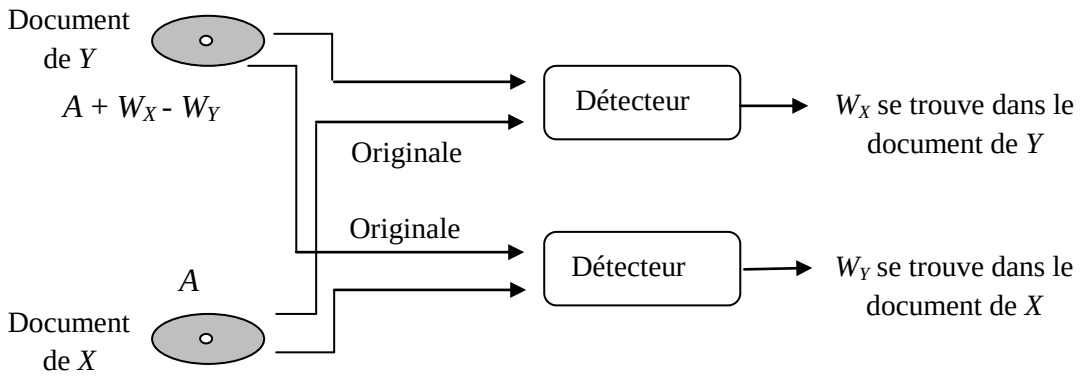


Figure. I.10. Le deuxième exemple d'attaques SWICO

I.10 Conclusion

Nous nous sommes intéressés dans ce chapitre à présenter les principes du tatouage (ou watermarking) des données multimédias d'une façon générale. Cette jeune discipline trouve ses origines dans des sciences utilisées depuis longtemps comme la cryptographie et la stéganographie. Malgré sa modernité, elle a bénéficié d'un cadre juridique bien particulier défini par différentes conventions et lois, ceci est en relations avec les solutions que porte cette nouvelle technique aux problèmes de sécurisation des données numériques face au piratage et à la contrefaçon.

En tirant partie des connaissances acquises dans les domaines de la théorie de l'information et des communications numériques (capacité, codes orthogonaux, codes correcteurs, multiporteuses *OFDM*, partage de canaux- *TDMA*, *FDMA* et *CDMA*, interférences), le traitement du signal (représentation temps-échelle, transformations multirésolutions orthogonales ou redondantes, filtrage et estimation des paramètres, segmentation, détection), les statistiques (décision, tests d'hypothèses, mesure de confiance, fusion, reconnaissance) et la cryptographie (gestion de clés publiques et privées); le watermarking s'impose comme solution efficace, en termes de sécurité et de recherche d'information, dans plusieurs domaines. Dans ce contexte, beaucoup d'applications trouve un intérêt à ce qu'un watermark visible ou non, soit entrelacé aux données multimédia numériques, afin d'assurer des services aussi variés que la protection des droits d'auteurs, le contrôle de copie, le Fingerprinting, l'indexation, l'authentification, la traçabilité…etc. La conception d'un schéma de watermarking doit prendre en compte, en plus des considérations protocolaires, les détailles de l'application visée en vue de réaliser un compromis entre les contraintes d'imperceptibilité, de robustesse et de capacité.

La protection des droits d'auteurs est la discipline qui semble offrir au watermarking diverses applications industrielles telles la protection du *DVD* et des images fixes. Le chapitre qui suit sera consacré aux systèmes de watermarking propres aux images fixes qui représente l'axe de notre recherche.

II.1 Introduction

Dans ce chapitre, nous parlerons du contexte du tatouage d'images numériques fixes. Nous donnons ensuite le principe général d'un système de tatouage d'image, pour la protection du copyright, en décrivant notamment les différentes étapes d'insertion et de détection de la marque (ou signature). Dans la section (II.3) nous revenons en détails sur les différentes attaques, mentionnées brièvement dans le chapitre (I), que peut subir une image marquée.

II.2 Contexte du tatouage d'image

Les développements d'Internet et plus généralement des nouveaux moyens de communication ont fait entrer le monde dans une ère où le numérique prend une place de plus en plus importante ; petit à petit les appareils photo numériques supplantent les anciennes pellicules chimiques, les lecteurs DVD remplacent les magnétoscopes comme les Compact Discs ont pu le faire avec les disques vinyles.

L'intérêt que le grand public porte à ces nouveaux supports numériques provient notamment des facilités qu'offrent les ordinateurs à traiter et manipuler les données numériques. Cette nouvelle ère pose de ce fait de sérieux problèmes de droits d'auteurs : l'image – avec les photos de presse –, le son – avec les Compacts Discs – et la vidéo – avec les DVD – sont les premiers supports touchés par le piratage.

Chercheurs et industriels ont donc étudié diverses méthodes pour empêcher ou tout du moins freiner la copie de ces œuvres multimédia. L'une d'elles est le tatouage d'images.

II.3 Principe général d'un schéma de tatouage d'images

II.3.1 Définition

Le principe général d'une méthode de tatouage d'une image numérique en vue de la protection du copyright, que l'on peut sommairement décrire à l'aide de la figure (II.1), consiste à introduire une information de copyright en modifiant imperceptiblement la valeur des échantillons de l'image. L'extraction de l'information de copyright doit être possible tant que l'image, qui a éventuellement subi des manipulations de natures variées, est de qualité proche de celle de l'image originale. Dans la plupart des algorithmes de tatouage, le marquage est protégé par un code secret. Seules les personnes ou les organismes autorisés peuvent savoir si une image a été marquée et le cas échéant lire cette marque. Cette exigence se concrétise dans les algorithmes de tatouage par l'usage d'une clé privée cryptographique appartenant au propriétaire de l'image.

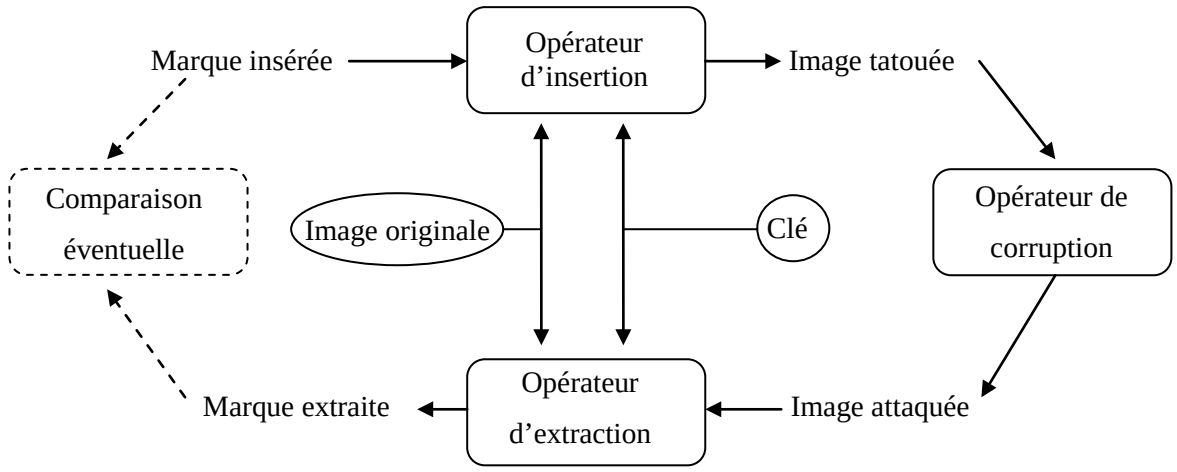


Figure II.1. Dispositif générique d'un système de tatouage d'image

II.3.2 Schéma général d'une méthode de tatouage d'images

Le schéma de tatouage d'images, qui est un cas particulier des schémas de watermarking évoqués précédemment dans le chapitre (I), se décompose en deux étapes distinctes illustrées par la figure (II.2) :

II.3.2.1 Phase d'insertion

Elle consiste en l'insertion d'une marque (w) dans une image (I) pour obtenir une image marquée (I_w), en vue d'identifier son propriétaire (le nom de l'auteur ou de l'entreprise par exemple). Cette insertion peut se faire soit dans le domaine spatial et dans ce cas la fonction de marquage, en se référant à l'équation (I.1), peut s'exprimer par :

$$\mathcal{E}(I, w, K) = I_w \qquad \text{(II.1)}$$

Soit dans un domaine transformé obtenu par une transformation inversible (T) telle que la transformée en cosinus discrète (TCD), la transformée de Fourier discrète (TFD), la transformée de Fourier Mellin (TFM) ou encore la transformée en ondelettes discrète (DWT). Dans ce cas de situation la fonction de marquage s'exprime par :

$$\mathcal{E}(T(I), w, K) = I_w \qquad \text{(II.2)}$$

La marque insérée (w) dépend d'une clé secrète (K) mais aussi du message que l'on désire insérer $b=\{b_0,b_1,\ldots\ldots,b_k\}$(pour plus de détails voir section 1-6 du chapitre I).

Donc l'opération d'insertion de la marque peut être définie comme une application ($\mathcal{E}$) de l'espace des watermarks ($\mathcal{W}$), de l'espace des clés ($\mathcal{K}$) et de l'espace des images($\mathcal{I}$) dans ce dernier. Elle fait correspondre à un watermark (w), une clé (K) et une image hôte (I), une image tatouée (I^*) [51].

$$(\mathcal{W}, \mathcal{K}, \mathcal{I}) \rightarrow \mathcal{I}$$

$$(w, K, I) \rightarrow I^* \qquad \text{(II.3)}$$

Ce formalisme, très général, représente le processus d'insertion de la marque pour tous les processus de tatouage. Nous allons maintenant préciser les propriétés que l'application ($\mathcal{E}$) doit satisfaire et définir les espaces de départ et d'arrivée $\mathcal{W}$, $\mathcal{K}$ et $\mathcal{I}$.

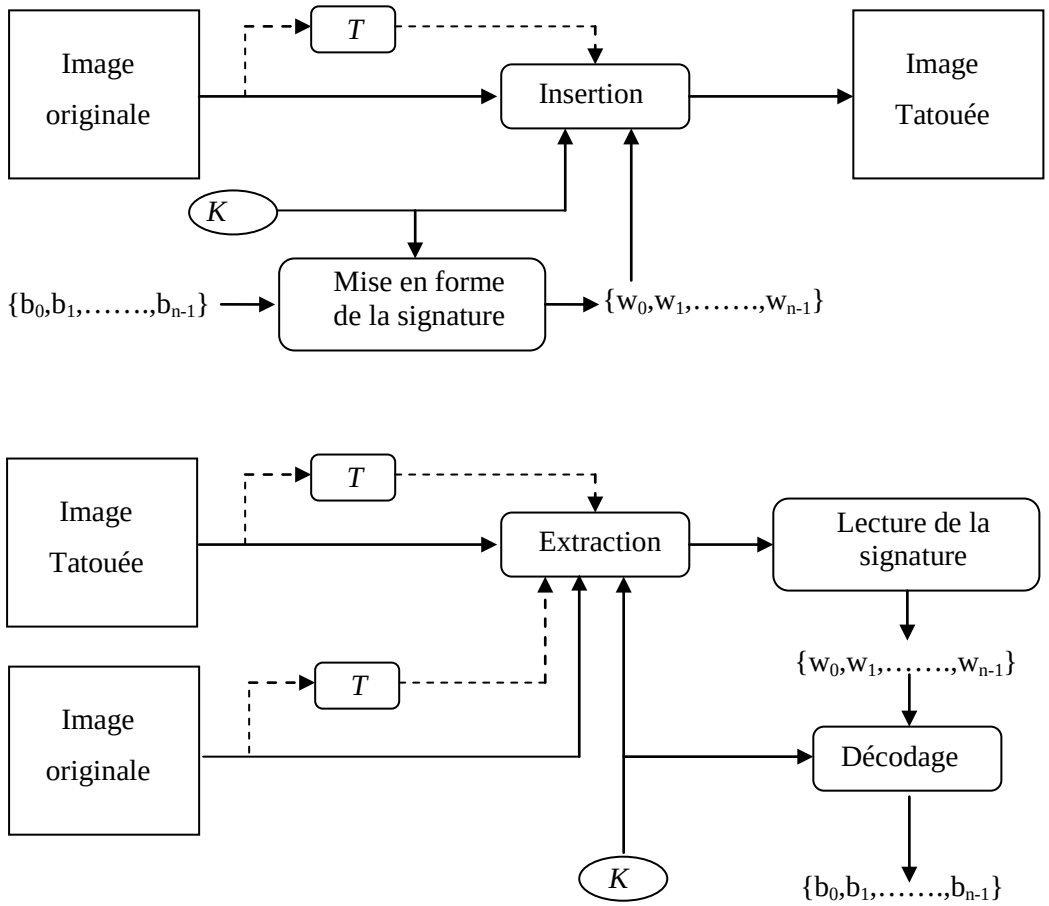


Figure II.2 Insertion et extraction d'une signature

a. La fonction d'insertion

Contrainte d'imperceptibilité

Le marquage doit être imperceptible, c'est-à-dire qu'un utilisateur quelconque ne doit pas pouvoir différencier visuellement l'image marquée de l'image originale. Cette propriété est importante pour deux raison. La première est évidente : le marquage ne doit pas empêcher la compréhension de l'œuvre, celle-ci doit garder toute sa qualité artistique ou commerciale. Une autre raison est, qu'ainsi cachée, la marque est plus difficilement détruite par piratage.

Dans la plus part des algorithmes proposés, l'imperceptibilité du tatouage s'obtient en utilisant diverses propriétés du Système Visuel Humain (SVH. Ces propriétés, souvent trouvées à partir d'heuristiques, proposent des modélisations du comportement psycho-visuel humain. En général, un seuil de perceptibilité est calculé à partir de l'image originale, les modifications de l'image ne peuvent se faire qu'à concurrence de ce seuil.

Cette contrainte pose un problème d'évaluation. En effet, une fois l'image tatouée, on doit pouvoir assurer que les distorsions causées sont imperceptibles. On utilise couramment le *PSNR* (pour *Peak Signal to noise Ratio*) pour quantifier ces dégradations.

Sûreté du tatouage, inversibilité de $\mathcal{E}$

Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est assurée uniquement par la confidentialité de la clé *K*. En effet, on ne peut pas garantir la confidentialité des algorithmes mis en œuvre. Si *K* est inconnu, aucun utilisateur ne doit pouvoir retrouver l'image originale. Cette contrainte est souvent remplacée par la suivante, plus réaliste : Ne connaissant pas la clé secrète, un pirate ne doit pas pouvoir retrouver l'image originale sans pour cela mettre en œuvre des moyens plus coûteux que ceux correspondant à l'achat des droits de copyright.

L'inversibilité de l'application $\mathcal{E}$ est donc conditionnée par la connaissance de la clé. Cette inversibilité n'est pas obligatoire. Elle peut être recherchée si les ayant-droits de l'image veulent enlever la marque pour en ajouter une autre (si par exemple, le statut de copyright a changé). L'inversibilité de $\mathcal{E}$ est impossible si des informations inhérentes à l'image originale ont disparu dans la version tatouée. Certains processus d'insertion de la marque sont par exemple fondés sur une substitution ou une quantification des valeurs de l'image qui sont alors irrémédiablement modifiées. Ces derniers schémas assurent plus de sécurité dans le cas

où la clé est divulguée et peuvent alors servir pour des algorithmes dits à clé publique, où aucun secret n'est requis pour la détection de la marque [52].

Injectivité de l'application $\mathcal{E}$

Si une image marquée correspond à deux propriétaires différents, c'est-à-dire deux couples (W, K), on se retrouve dans la position dite de l'impasse : On ne peut pas conclure sur l'appartenance de l'image à l'un ou l'autre des propriétaires. On se retrouve dans une telle situation si l'application $\mathcal{E}$ n'est pas injective.

La solution proposée pour éviter ce problème est de restreindre les espaces de départs, c'est-à-dire en imposant une structure fixée à la clé et à la marque. Si on impose de plus que la clé soit fonction de l'image originale, l'attaquant aura alors beaucoup plus de mal à générer le faux triplet solution (W_f, K_f, I_f). En général, un tiers de confiance intervient dans le protocole de tatouage, il délivre par exemple la clé privée, pour chaque image.

Surjectivité de l'application $\mathcal{E}$

$\mathcal{E}$ est surjective si et seulement si, il existe pour toute image I, un triplet (W, K, I) tel que $I = \mathcal{E}$ (W, K, I). Ceci signifie que toutes les images (originales ou non) possèdent une marque à l'état naturel. Il suffirait à un pirate de trouver le code et la marque pour s'approprier les images originales en circulation. Le danger de cette attaque, très proche de celle mentionnée ci-dessus est évité de la même manière : On restreint les ensembles de départs et on introduit un tiers de confiance dans le protocole de watermarking ou tatouage.

b- Espaces d'entrée

Espace des watermarks

L'ensemble $\mathcal{W}$ est l'ensemble de toutes les marques possibles. Son cardinal doit être le plus grand possible, c'est-à-dire que la longueur de la marque W doit être la plus grande possible. Cette longueur est pourtant limitée par plusieurs contraintes. D'une part, elle dépend de la taille de l'image hôte. En effet, on ne peut pas inscrire trop d'informations dans un petit support. De plus, la contrainte d'invisibilité impose une marque de petite taille. Il est évident que plus la marque est petite, plus il est facile de cacher. Enfin, pour assurer la robustesse du processus de tatouage, W est fortement redondant. Cette redondance s'exprime de plusieurs manières, ce peut être de la redondance pure (la même information est répétée plusieurs fois), l'emploi de code correcteur d'erreurs ou l'emploi de techniques dites d'étalement de spectre.

Dans certains algorithmes, la marque a une structure prédéfinie, comme par exemple une succession de M-séquences. La taille de la marque est ainsi toujours supérieure à celle de l'information qu'elle porte.

Pour l'instant aucune norme n'a été adoptée concernant la taille de chaque marque et donc le cardinal de l'ensemble $\mathcal{W}$. Dans la plupart des contributions, la marque est fixée à une centaine de bits pour une image 512x512 codée sous 8 bits.

Dans certaines méthodes dites additives à étalement de spectre, la présence de la marque est détectée sur 1 bit. L'algorithme de détection signale uniquement la présence d'un motif correspondant à un tatouage de l'image. Ce motif dépendant de la clé *K*, c'est la connaissance de cette clé qui joue le rôle d'identifiant. Il faut alors que le cardinal de K soit très grand, pour caractériser le maximum de propriétaires.

Espace des clés

C'est sur la connaissance de la clé *K* que repose toute la sécurité du tatouage. En effet si *K* est divulgué, tout le monde peut détecter et lire la marque. Dans la plupart des schémas à clé privée, la connaissance de la clé permet de retrouver l'image originale ou d'invalider la détection du tatouage. Ainsi, un pirate ne doit pas pouvoir retrouver la clé. Toute tentative de recherche exhaustive de la clé doit être impossible ou trop coûteuse à réaliser. Pour cela, la taille de la clé doit être grande et sa structure compliquée. Inversement, la clé privée doit être facilement stockée par le propriétaire et le tiers de confiance, sa taille doit donc être raisonnable. Si par exemple, la taille de la clé est proche de celle de l'image originale, le tatouage pour la protection du copyright n'a plus lieu d'être : il serait alors plus simple que le tiers de confiance stocke directement l'image originale.

La clé *K*, issue d'un processus cryptographique, contient des informations qui permettent par exemple de piloter les endroits d'insertion du watermark. Dans d'autres schémas dits à étalement de spectre, la clé génère un motif qui sera utilisé comme vecteur du watermark.

Espace des images hôtes

A priori, n'importe quelle image doit pouvoir être tatoué. Cependant, il est évident qu'on ne peut pas marquer les images de trop petite taille (quelques pixels sont insuffisants pour contenir le watermark). En général, les processus de watermarking fixent la taille minimale des images hôtes à 512x512 pixels ou plus rarement à 256x256 pixels. Ce dernier choix paraît raisonnable puisque les industriels appellent les images de 256x256 pixels « imagettes » et ne leur confèrent pas de valeur commerciale. Les schémas de watermarking

excluent donc de l'espace des images hôtes les images de petite taille. Cette restriction de l'espace de départ entraîne des problèmes de robustesse. En effet, une attaque dite mosaïque utilise cette restriction pour invalider la détection du marquage.

Afin de pouvoir cacher la marque, il est clair que le support doit respecter d'autres contraintes, si par exemple l'image est trop monotone, le schéma d'insertion de la marque ne pourra pas fonctionner ou le tatouage sera trop visible. C'est le problème posé par certaines images synthétiques comme les dessins qui contiennent de grandes zones uniformes. Les applications concernant les images médicales commencent à être étudiées spécifiquement. La plupart des schémas de watermarking s'intéressent cependant à des images hôte de type « cinéma » ou photographie. Celles-ci représentent en effet la majorité des images en circulation.

Formellement, une image est une application I de l'espace des coordonnées spatiales dans un ensemble de valeurs quantifiées : à chaque couple de coordonnées (x, y) de l'image (appelé usuellement pixel), on associe une valeur $I(x, y)$. Selon les modes de représentation, la valeur d'un pixel peut être exprimée de différentes façons : pour les images couleurs, la valeur d'un pixel est contenue dans un triplet (R, G, B) ou (Y, U, V). Dans la première représentation, R désigne la quantité de rouge, G celle de vert et B celle de bleu, dans la seconde, Y est la luminance du pixel, U et V étant des paramètres de chrominance. Les images dites à niveau de gris ne sont représentées que par les valeurs de luminance Y. Le système visuel humain étant moins sensible à la luminance qu'aux chrominances, les algorithmes de watermarking ne modifient que ce paramètre.

II.3.2.2 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 watermarking. Certains algorithmes [53] pratiquent un filtrage de l'image tatouée avant d'entreprendre la vérification du tatouage. D'autres algorithmes [4] confectionnent un tatouage comprenant des bits dont les valeurs sont prédéfinies afin de permettre une première estimation de l'attaque qu'a pu subir l'image. Ces derniers algorithmes sont propices à la mise en place de seuils de décisions adaptatifs. Enfin, les tests d'hypothèses font également parti des outils usuellement utilisés dans le cadre de problèmes où une prise de décision intervient. En tatouage d'image, ils trouvent particulièrement leur intérêt lorsque la signature est connue et qu'il s'agit de vérifier sa présence dans telle ou telle image, le plus souvent par corrélation. Donc l'opération d'extraction comprend deux parties :

d'une part, la détection de la signature (watermark) et d'autre part, s'elle est présente, son décodage. La phase de détection consiste à prouver la présence de la signature dans l'image marquée et attaquée, grâce à la clé *K*. La phase de décodage consiste à calculer une estimation du message contenu dans la signature (figure II.2).

Comme nous l'avons évoqué au premier chapitre de ce document (sec I.6.3), il existe plusieurs modes d'extraction de la marque. Selon les différents schémas, l'image originale peut être utilisée ou non lors de l'extraction de la marque. Donc le choix du modèle dépendra de l'application visée et des protocoles utilisés. On distingue :

- **Le mode non-aveugle** (ou tatouage privé) figure (II.3) : dans ce cas l'image et la marque originale sont nécessaires. Si le détecteur extrait la marque, il est dit de *type I*, on a alors :

$$(K, I, I') \rightarrow W' \qquad \text{(II.1)}$$

Si le détecteur est une mesure de présence de la marque (sa sortie sera 1 si la marque est détectée 0 sinon), la détection est alors une application de *type II* avec :

$$(W, K, I, I') \rightarrow 0,1 \qquad \text{(II.2)}$$

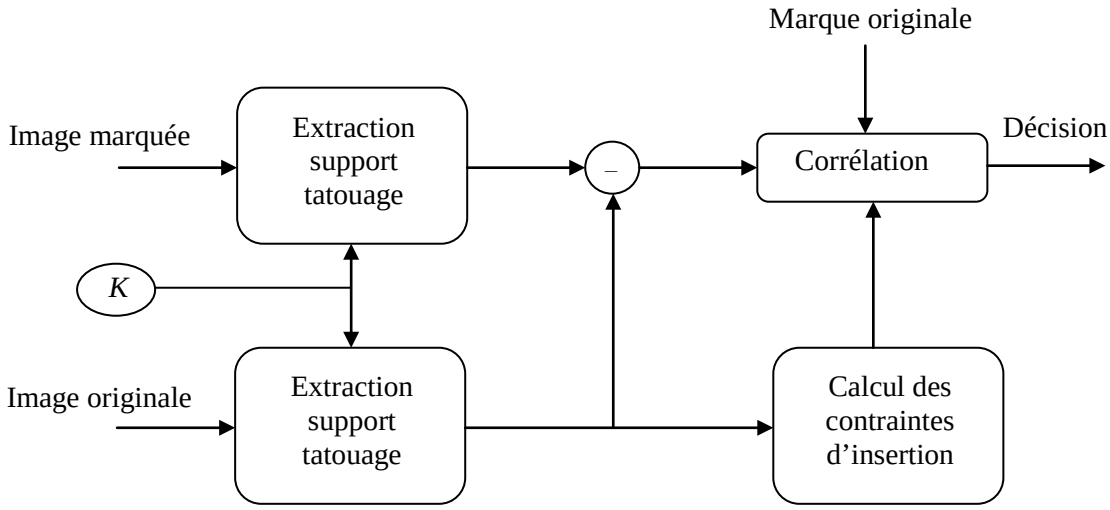


Figure II.3 mode d'extraction non aveugle

L'image originale fournit une référence pouvant servir à améliorer l'estimation de la signature ou encore à identifier les divers traitements subis par l'image marquée.

- **Le mode semi-aveugle** (ou tatouage semi-privé) figure (II.4) : ce type de détection n'utilise pas l'image originale mais seulement la marque originale en donnant une réponse sur sa présence dans l'image marquée :

$$(K, W, I') \rightarrow 0,1 \qquad \text{(II.3)}$$

- **Le mode aveugle** (ou tatouage public) figure (II.5) : dans ce cas l'extraction de la marque se fait en absence de l'image et de la marque originales. La robustesse du schéma ne repose ici que sur la connaissance de la clé.

$$(K, , I') \rightarrow W \qquad \text{(II.4)}$$

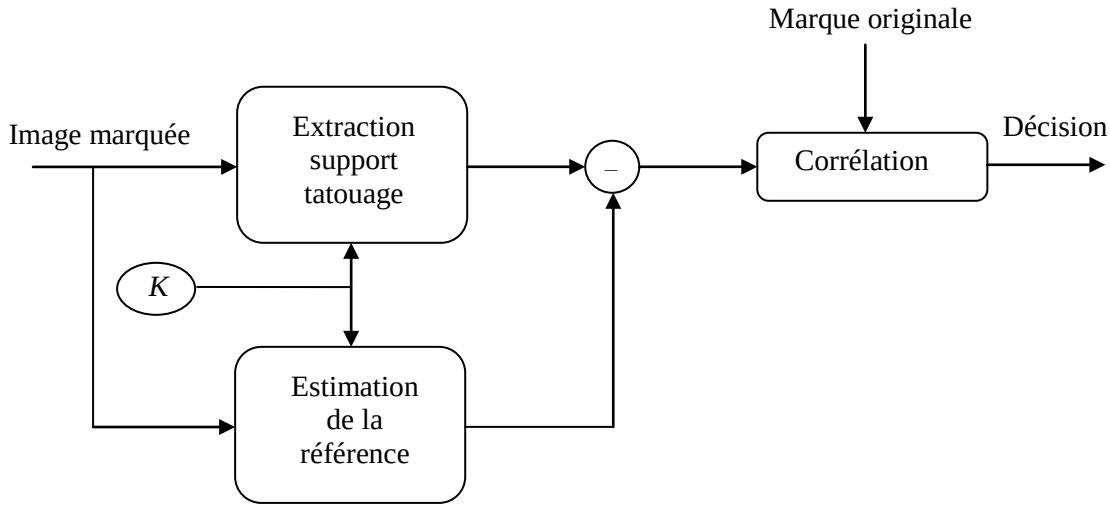


Figure II.4 mode d'extraction semi-aveugle

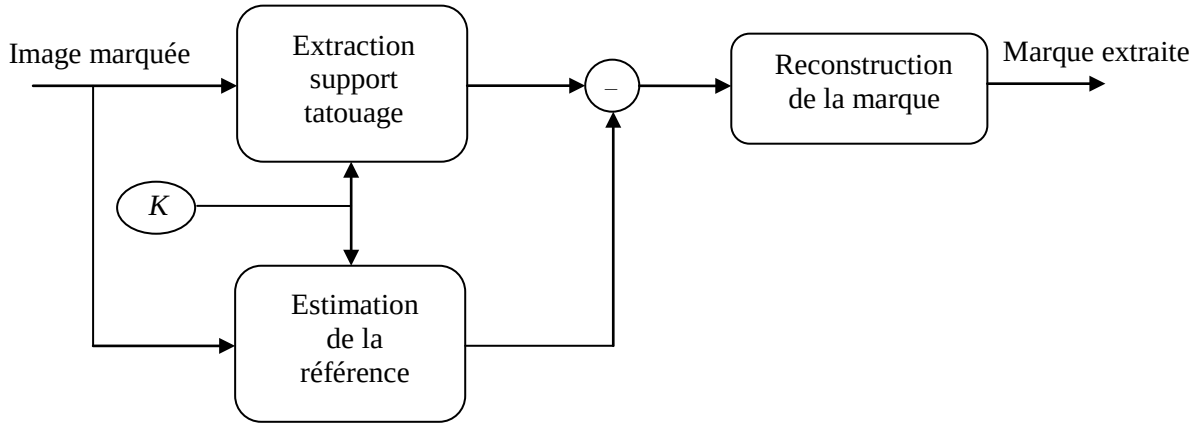


Figure II.5 mode d'extraction aveugle

Pour la protection du copyright, la marque originale est supposée connue, les algorithmes de détection par extraction sont alors suivis d'une étape de vérification. La marque extraite est comparée à la marque originale par mesure de corrélation. Cette mesure est finalement seuillée pour obtenir la valeur de décision : 1 si l'image est considérée tatouée, 0 sinon.

II.4. Evaluation des algorithmes de tatouage

Les contraintes essentielles du tatouage d'image sont l'invisibilité de la marque sa taille (ou capacité) et sa robustesse vis-à-vis aux différentes attaques ou manipulations. Evaluer les processus de watermarking n'est pas une chose immédiate. En effet, comme nous l'avons évoqué dans le chapitre précédent, aucun cahier des charges ne donne des valeurs fixées pour la taille de la marque, la qualité du watermarking (son imperceptibilité) ou l'ensemble des attaques auxquelles le watermarking ou tatouage doit être robuste. Donc un compromis entre ces trois contraintes est réalisé selon l'application envisagée.

II.4.1 Evaluation de la distorsion introduite par l'insertion de la marque

Il n'existe aucune méthode automatique pour mesurer la qualité absolue d'une image. Aucun algorithme n'est capable, sans image de référence, de dire qu'une image est de bonne ou mauvaise qualité. Cependant, dans le cadre de nos applications, cette contrainte n'est restrictive puisque l'image originale peut nous servir de référence. La mesure de qualité des images est donc une mesure de distance entre deux images.

Les mesures de distances les plus simples comparent les deux images pixels par pixels. Elles sont fondées sur la différence entre les deux images ou sur des corrélations entre ces images. Les mesures de distorsion les plus populaires en traitement d'images et compression étant tout simplement le rapport signal sur bruit (*SNR : Signal to Noise Ratio*) et le (*PSNR : Peak Signal to Noise Ratio*). Ils sont mesurés en décibel (dB) à partir des relations suivantes :

$$(SNR)_{dB} = 10log_{10}\left(\sum_{m=1}^{M}\sum_{n=1}^{N} I_{m,n}^2 \,/\, \sum_{m=1}^{M}\sum_{n=1}^{N}\left(I_{m,n} - I_{m,n}^*\right)^2\right) \quad \text{(II.5)}$$

$$(PSNR)_{dB} = 10log_{10}\left(\max_{m,n} I_{m,n}^2 \,/MSE\right) \quad \text{(II.6)}$$

Avec *MSE* (mean square error) donnée par :

$$MSE = \frac{1}{M.N}\sum_{m=1}^{M}\sum_{n=1}^{N}[I(m,n) - I^*(m,n)]^2 \quad \text{(II.7)}$$

Où *I(m, n)* est la valeur du pixel *(m, n)* de l'image de référence et $I^*(m, n)$ celle de l'image à tester, les deux images étant de taille [M x N].

Malheureusement, le *PSNR*, qui est la mesure la plus couramment utilisée (comme l'ensemble des métriques basées pixel) ne tient absolument pas compte du contenu fréquentiel de l'image. Bien que servant toujours de référence, le PSNR n'est pas la métrique la plus appropriée au contexte du tatouage d'image. Certains auteurs préconisent alors l'utilisation d'autres métriques plus adaptées, telles que le *wPSNR* (*weigted PSNR ou PSNR pondéré*) [54], le *MPSNR* (*masked PSNR*) [55] ou bien encore la mesure de Watson [56].

II.4.1.1 wPSNR (le PSNR pondéré)

La définition du *PSNR* donnée précédemment (équa. II.6) pénalise l'ajout du bruit (le tatouage) de la même manière quelles que soient les régions de l'image. Alors qu'en raison des phénomènes de masquage, la perception d'un bruit est plus importante dans les régions uniformes que dans les zones texturées ou les contours. Le *wPSNR* donné par l'équation (II.9) se distingue du *PSNR* en différenciant des régions visuellement différentes. Une manière simple d'attribuer un poids à une zone de l'image en fonction de son contenu fréquentiel est d'utiliser la fonction *NVF* (*Noise Visibility Function*). Cette fonction, dans le cas où on considère que l'image suit un modèle non stationnaire gaussien, est donnée par la formule (II.8) suivante :

$$NVF(i,j) = \frac{1}{1+\sigma_x^2(m,n)} \qquad \text{(II.8)}$$

Où $1 + \sigma_x^2(m,n)$ représente la variance locale de l'image dans une fenêtre centrée sur le pixel de coordonnées *(m, n)*.

$$(wPSNR)_{dB} = 10log_{10}\left(\frac{\max_{m,n} I^2}{\|NVF(I-I^*)\|^2}\right) \qquad \text{(II.9)}$$

II.4.1.2 Mesure de Watson

Le modèle de Watson [56], [57] a été développé à l'origine pour évaluer la qualité des images compressées par *JPEG*. Ce modèle estime la distorsion perceptible par l'œil humain dans le domaine *TCD* (Transformée en Cosinus Discrète). Son application s'effectue sur des blocs *DCT* 8x8 de l'image. L'erreur de quantification est pondérée par un seuil de visibilité qui dépend essentiellement de trois facteurs : un modèle de sensibilité de l'œil (c.-à-d. table déterminée expérimentalement donnant les réponses de l'œil à des stimuli isolés), ainsi que deux modèles de masquage l'un adapté à la luminance et l'autre au contraste. Pour obtenir une mesure globale de l'erreur perceptible, les erreurs de quantification pondérées pour

chaque couple de fréquences sont sommées sur chacun des blocs constituant l'image. Les résultats sont ensuite sommés sur l'ensemble de l'espace *TCD* en utilisant la sommation de Minkowski. La distorsion est exprimée en termes de nombre différences perceptibles (*JNDs*).

II.4.2 Les attaques et la robustesse

Les attaques tiennent une place très importante dans le cahier des charges d'un processus de watermarking puisqu'elles définissent la robustesse et la sécurité de la marque. Une attaque peut être considérée comme un traitement ou une manipulation qui contourne l'objectif visé par la technique de watermarking pour une application donnée. Selon cette définition, les attaques relatives au watermarking d'image comprennent d'une part des opérations normales de traitement liées à l'utilisation ou à la diffusion de l'image telles que la compression avec perte, les conversions A/N et N/A et la conversion de fréquence d'échantillonnage qui peuvent involontairement détruire la marque ; et d'autre part des attaques dites malveillantes, plus spécifiques, dont le but est de détruire ou d'empêcher l'extraction de la marque. La notion de robustesse d'un tatouage est intimement liée à l'impact visuel engendré par les différentes manipulations subie par l'image. Il est clair que des attaques qui entraîneraient des dégradations importantes, rendant l'image totalement inexploitable, auraient très peu d'intérêt, même si elles étaient capables de détruire la marque. Par contre, une attaque est dite réussie si elle défait la technique du watermarking tout en conservant la qualité de l'image.

II.4.2.1 Classification des attaques

Avant de commencer à décrire les différentes attaques, que peut subir une image marquée, il est utile d'esquisser une classification permettant d'identifier facilement ces attaques. En effet, un classement de ces derniers en plusieurs groupes permet à la fois au concepteur d'un algorithme de watermarking et à l'utilisateur du système de watermarking l'identification des exigences de sécurité, ainsi que de juger de la facilité d'utilisation de la technologie de watermarking. A ce sujet, plusieurs classifications ont été adoptées parmi les quelles on peut citer :

- une classification qui se base sur l'intention du manipulateur de l'image marquée. Dans ce cas on distingue les attaques innocentes et les attaques malveillantes,
- une classification établie selon l'étape du watermarking mis en défaut. En effet, si des pirates tentent par exemple d'enlever la marque, c'est l'étape d'insertion qui est visée. Ils peuvent aussi vouloir invalider le marquage, en noyant par exemple le message

dans du bruit, c'est alors l'étape de détection qui est visée,

- une classification qui tien compte du niveau d'intervention du manipulateur, dans ce cas on distingue principalement trois types d'attaques : les attaques liées au signal, les attaques de nature cryptographique, et les attaques de protocoles,
- une autre classification établie selon l'effet de l'attaque sur la position ou l'emplacement de la marque dans l'image. De ce fait, on distingue d'une part les attaques synchrones qui ne modifient pas la position spatiale ou temporelle du signal tels que la compression, le lissage, l'ajout de bruit, ..., et d'autre part les attaques asynchrones qui modifient la position spatiale ou temporelle du signal, et introduisent donc une désynchronisation : transformations géométriques, ...

Malgré que ces classifications ont été élaborées selon des points de vue différents, mais elles englobent presque les mêmes attaques. Pour nous, nous avons opté à la première classification et selon laquelle nous allons présenter dans ce qui suit les différentes attaques que peut subir une image marquée.

II.4.2.1.1. Les attaques innocentes

Tous les traitements ou les manipulations utilisées par les traiteurs d'images qu'ils soient scientifiques, photographes ou infographistes sont classés comme étant des attaques innocentes. L'objectif de ces traitements c'est de modifier ou masquer certaines caractéristiques de l'image. Il est impossible de dresser un inventaire exhaustif de ces traitements parce qu'ils sont nombreux mais nous nous contenterons de présenter les plus couramment utilisés.

- **La compression** : la taille brute importante d'une image numérique pose de grands problèmes de transmission ou de sauvegarde par exemple, la raison pour laquelle de nombreux utilisateurs font recours à des outils de compression pour réduire la taille du fichier. Les algorithmes de compression sont particulièrement dangereux pour les processus de watermarking. En effet, l'objectif d'utilisation de ces algorithmes est de compacter autant que possible la représentation de l'image en éliminant les données jugées perceptuellement moins importantes et garder les composantes essentielles de l'image. C'est pourquoi Cox et al. [26] proposent d'insérer la marque dans des endroits « perceptuellement significatifs » de l'image. Ces endroits sont souvent choisis dans les domaines utilisés par les algorithmes de compression. Tous les algorithmes de compression avec perte suivent un schéma de trois étapes. La première

étape consiste en l'application d'une transformation mathématique pour les échantillons de l'image pour les projeter dans un espace où les coefficients obtenus peuvent être considérés comme presque indépendants, et où la modélisation de la perception est plus facile; les transformations les plus courantes sont la *DCT* (par exemple dans le *JPEG* standard) ou la *DWT* (par exemple dans la norme *JPEG2000*). Cette première étape n'entraine (du moins en principe) aucune perte d'information étant la transformation réversible. La seconde étape consiste en la quantification des coefficients transformés: c'est dans ce processus que les informations de détails (composante haute fréquence de l'image) sont perdues en raison de la nature irréversible du processus de quantification ainsi que l'apparition de la géométrie des blocs pour des taux de compression élevés. Enfin, dans la troisième étape, les coefficients quantifiés subissent un codage entropique (par exemple par le codage de Huffman ou le codage arithmétique) sans perte d'information.

Figure II.6. Exemple d'une image compressée

- **Le filtrage** : en fait, du point de vue traitement de signal, l'opération de filtrage ni plus ni moins qu'un produit de convolution du signal (ici l'image) avec une fonction dont la transformé de Fourier est une Gaussienne, une fonction porte etc. … Donc les filtres sont un des outils de base du traitement d'image utilisés principalement pour améliorer son aspect. Par exemple pour rendre une image plus douce par une opération de lissage ou atténuer un bruit présent dans l'image, un filtre passe bas est utilisé. Cela a pour effet d'atténuer les composantes hautes fréquences de l'image et par conséquent dégrader les composantes hautes fréquences de la marque comme il est indiqué sur la

figure (II.7.b). Un autre exemple concernant le rehaussement de l'image qui devient plus contrastée et les détails et les contours sont beaucoup plus visibles. Par conséquent, les composantes hautes fréquences de la marque sont augmentées (voir figure II.7.c).

a. Image originale

b. Image lissée

c- Image contrastée

Figure II.7. Quelques opérations de filtrage : a) lissage et b) rehaussement

- **Les transformations valumétriques**, fréquentes en traitement d'images, incluent par exemple l'égalisation d'histogramme. Cette opération consiste à appliquer une transformation sur chaque pixel de l'image, et donc d'obtenir une nouvelle image à partir d'une opération

indépendante sur chacun des pixels. Cette égalisation est intéressante pour les images dont la totalité, ou seulement une partie, est de faible contraste (l'ensemble des pixels sont d'intensité proches). En plus de l'égalisation d'histogramme, on trouve aussi l'étalement d'histogramme et la correction gamma.

- **Ajout de bruit (gaussien, aléatoire uniforme)**, l'ajout involontaire ou délibéré, et avec des proportions importantes, d'un bruit dans une image peut masquer la marque et par conséquent gêner son extraction.
- **Transformation en niveaux de gris** : la conversion d'une image couleur en niveaux de gris consiste à éliminer les composantes couleurs. Par conséquent, la perte de la marque sûr si celle-ci est insérée dans l'une des composantes couleurs (par exemple le bleu). Pour faire face à ce genre d'attaque il est préférable d'insérer la marque dans la luminance.
- **Transformations géométriques** : en général, l'édition des images nécessite constamment de modifier leur géométrie. Ces manipulations géométriques, même très simples, sont des attaques particulièrement sévères face auxquelles beaucoup d'algorithmes de watermarking d'image se révèlent inefficaces, en particulier lorsque l'on impose une extraction en mode aveugle. L'effet de ce type de transformations sur la marque insérée dépend du domaine d'insertion. En effet, si la marque est insérée dans le domaine spatial, elle subira les mêmes transformations que subit l'image. Alors que, dans le domaine transformé les effets de ces transformations sur la marque seront très différents. Dans tous les cas, ces transformations géométriques provoquent une perte de synchronisation entre la marque contenue dans l'image et le détecteur qui a besoin de connaître la position exacte de la marque dans l'image. parmi ces transformations géométriques on peut citer les suivantes :
  - *Les transformations de base dites affines*, qui englobe les translations, les rotations et les changements d'échelle voir (figure. II.8).
  - *Recadrage (en anglais cropping)*, dans certains cas, les personnes ne sont intéressées que par un morceau de l'image (par exemple le centre). Alors l'image sera recadrée à cet endroit. Cette opération a deux effets : le premier est la perte d'une partie du watermark et le deuxième c'est que le watermark subit une transformation similaire à celle produite par une translation. Pour être résistant à ce type d'attaque, le watermark doit être présent sur toute l'image.
  - *Symétrie horizontale*, certaines images peuvent être "flipper" sans perdre de leur sens (par exemple un paysage). Bien qu'il ne s'applique qu'à peu d'images, lorsqu'il

se produit, très peu de marquages lui survivent.

- *Suppression de lignes et de colonnes*, ce type de manipulations sont généralement imperceptibles, mais leur effet est suffisant pour induire une désynchronisation et rendre difficile l'extraction de la marque.

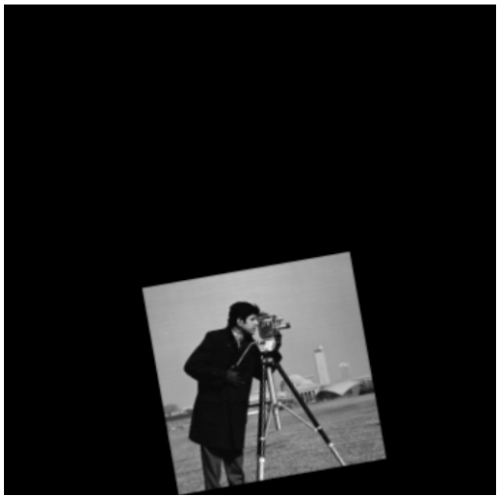
- **Conversions numérique-analogique-numérique** : la possibilité de la récupération de la marque, même après une conversion au format analogique (qui est le cas extrême du changement de format possible) d'une image numérique, est l'une des particularités attractives du watermarking. Pour récupérer une marque insérée dans une image analogique (imprimée), une numérisation de celle-ci est indispensable et ceci est réalisé par un scanner par exemple. Ces conversions numérique/analogique ensuite analogique/numérique constituent une attaque intéressante. Cette dernière peut être modélisée par une combinaison d'un ajout de bruit (due à l'acquisition), d'un double ré-échantillonnage et de légères déformations géométriques liées au positionnement de l'image lors de ces conversions.

b- Image originale

a- Translation

c- Rotation

d- Changement d'échelle



e- Changement d'échelle, rotation et translation

Figure. II.8 Les transformations géométriques élémentaires

II.4.2.1.2. Les attaques malveillantes

La plupart des transformations évoquées précédemment sont des traitements qui peuvent être appliqué à une image dont le but est d'améliore la qualité (manipulation d'histogramme, réduction du bruit, filtrage), de sauvegarde (compression, changement de format) et d'édition (transformations géométriques). Malheureusement, ces manipulations peuvent être utilisées dans un but malveillant, en visant explicitement à détruire délibérément la marque ou à empêcher son extraction. Donc, tous ces traitement et d'autres qui entravent la bonne récupération de la marque, soit par effacement ou désynchronisation ou encore par exploitation d'une faille propre à un schéma de watermarking particulier, sont qualifiés d'attaques malveillantes. Celles-ci peuvent être réalisées soit d'une manière dite aveugle (sans connaître l'algorithme particulier utilisé pour le watermarking), soit d'une façon dite informée (exploitant des informations sur l'algorithme de watermarking utilisé pour le tatouage de l'image). Parmi les attaques malveillantes les plus courantes, dans le domaine du watermarking des images, on citera les suivantes :

- **Les attaques d'effacement par débruitage** : La marque insérée dans l'image ressemble souvent à du bruit, c'est donc tout naturellement que les pirates appliquent au document marqué des méthodes classiques de débruitage (filtres de Wiener, filtre de Kalman, estimation du maximum a posteriori, ondelettes, multifractal) pour lui retrancher l'estimation de la marque. Sous certaines conditions, le signal résultant sera proche du signal original. Langelaar *et al.* [58] ont par exemple proposé une attaque, basée sur le filtrage non linéaire, spécifique aux méthodes de watermarking d'images utilisant l'étalement de spectre. L'idée générale consiste à estimer le watermark a partir de l'image marquée I_w. Dans ce cas spécial, un filtre médian 3x3 déterminé expérimentalement, est utilisé pour produire l'image filtrée I'_w.

$$I'_w = med_{3x3}(I_w) \qquad \text{(II.10)}$$

La différence entre l'image marquée et l'image filtrée donne une première approximation du watermark équation (II.11).

$$w' = I_w - I'_w \qquad \text{(II.11)}$$

Avant sa soustraction, le watermark estimé est filtré une deuxième fois, par un filtre passe haut, ensuite pondéré par un facteur d'échelle, déterminé expérimentalement, pour donner l'approximation finale $\hat{w}$ du watermark (voir figure II.9)

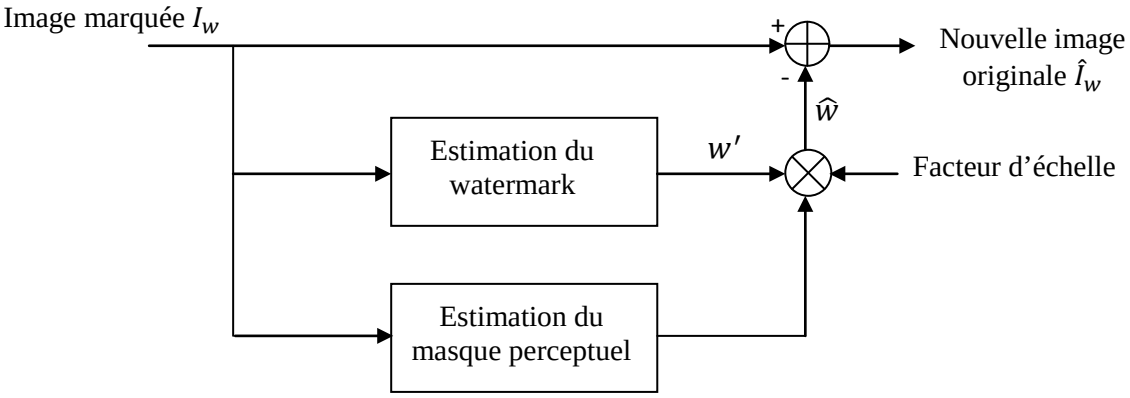


Figure II.9. Effacement de la marque par estimation

Toujours dans le même contexte, les attaques d'effacement par remodulation est un cas spécial des attaques d'effacement de la marque par estimation. Ce type d'attaque consiste en une modulation inverse de l'opération d'insertion de la marque ; en tentant de faire face d'une part aux différentes exigences de qualité de l'image marquée et d'autre part à la suppression de la marque. Les travaux de Voloshynovsky *et al.* [59] s'inscrivent dans cette optique. En effet, les auteurs ont cherché à estimer la marque par la méthode du maximum à posteriori (*MAP*). L'estimation de la signature est alors soustraite à l'image marquée et une version modulée de la prédiction est ajoutée à nouveau sur l'image afin de conserver une information haute fréquence.

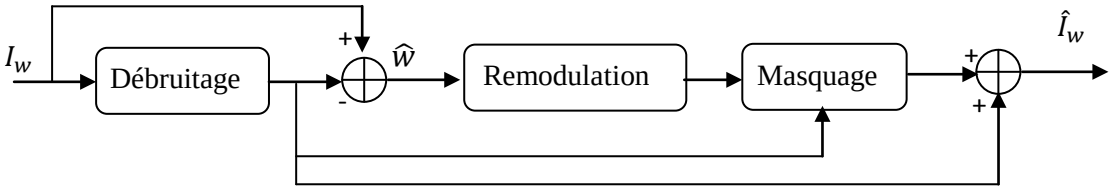


Figure II.10. Effacement de la marque par remodulation

- **L'attaque par copiage ou « Copy Attack »** : le but de ce type d'attaque consiste à copier le watermark contenu dans une image marquée dans une autre image. Cette attaque est réalisée essentiellement en trois étapes comme il est indiqué sur la figure (II.11). Dans la première étape une estimation, basée sur le processus de débruitage vu précédemment, du watermark dans l'image marquée est calculée. Dans la seconde étape, un masque perceptuel est déterminé pour pouvoir adapté le watermark estimé à

l'image cible. La dernière étape consiste à insérer le watermark obtenu dans l'image cible pour obtenir une version tatouée. La présentation originale de ce type d'attaque revient à Kutter *et al.* [48]. Dans leur travaux, les auteurs proposent une méthode basée sur la prédiction dans le domaine spatial pour effectuer une copie du watermark sans connaissances à priori. Le but est toujours de créer un litige lors de l'authentification du propriétaire : en effet lors de la confrontation avec le propriétaire, le pirate pourra répondre que le logiciel de détection retrouve la marque sur beaucoup d'autres images qui n'appartiennent cette fois qu'au pirate.

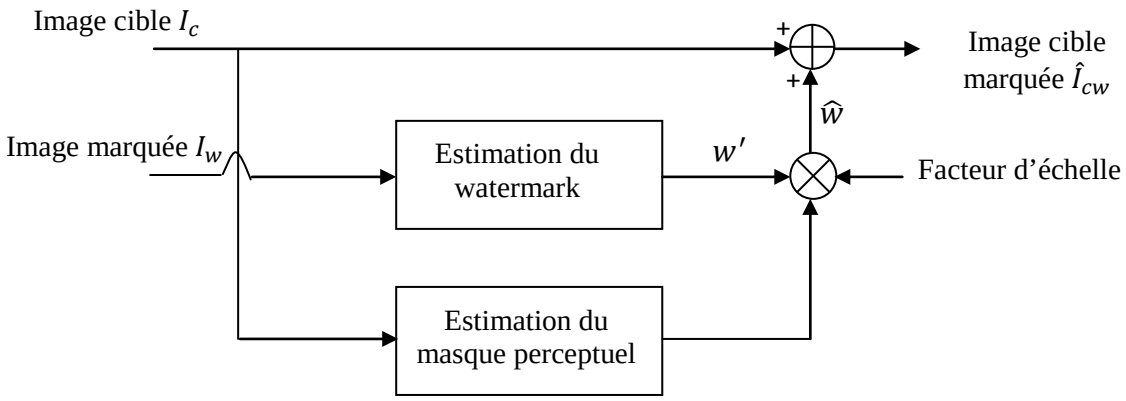


Figure II.11. Attaque par copiage « Copy attack »

- **L'attaque par sur-marquage « Overmarking »** : le sur-marquage est une opération qui consiste à tatouer une image déjà marquée et contenant un watermark. Les watermarks peuvent être détectés indépendamment si, par exemple, l'endroit où l'information sera cachée est déterminé par une clé secrète. Cette opération peut toujours être effectuée si l'attaquant possède l'accès aux modules d'insertion et de détection du système de watermarking. Si l'intention du watermark est la protection du droit d'auteur, les deux parties (le propriétaire du droit d'auteur et l'attaquant) peuvent prétendre la propriété de l'image. Le problème de la propriété serait résolu dans ce cas, si l'ordre d'insertion du watermark peut être prouvé de manière faible. Le seul avantage que possède le propriétaire du droit d'auteur comparativement à l'attaquant c'est bien son accès à la vraie image originale. Du moment que l'attaquant a seulement accès à l'image déjà marquée, la séquence de l'insertion serait déterminé par le fait que les deux parties ont à lire le watermark à

partir de leur images présumées originales. Un problème se pose donc si chacune des deux parties peut lire son watermark à partir de l'image originale de l'adversaire. Dans ce cas, un stand-off est créé, où le propriétaire du droit d'auteur n'a pas de véritable avantage sur l'adversaire. Ce type d'attaque mène à une situation d'impasse « *deadlock* » connue aussi sous le nom d'attaque *IBM*.

- **Attaque *IBM* ou « *deadlock* »** : différentes formes de l'attaque *IBM* sont possibles en fonction de la possibilité d'accès de l'attaquant à l'image originale. Pour faire la distinction entre le watermark du propriétaire du droit d'auteur et *celui* de l'attaquant, les lettres *c* et *a*, respectivement, seront utilisés. L'hypothèse de base de cette attaque est que la corrélation entre les deux watermarks est très faible (ce qui est probable).

$$C_\tau(W_c, W_a) \approx 0 \qquad \text{(II.12)}$$

En outre, l'image marquée I_W et la fausse image originale I_a sont créées selon les équations suivantes :

$$I_w = E_{K^c}(I_o, W_c) = I_o + W_c \qquad \text{(II.13)}$$

$$I_a = E_{K^a}^{-1}(I_w, W_a) = I_w - W_a \qquad \text{(II.14)}$$

$$\Rightarrow I_w = E_{K^a}(I_a, W_a) \qquad \text{(II.15)}$$

L'image marquée I_W est obtenue par l'intermédiaire d'un processus d'insertion ordinaire tandis que la création de la fausse image originale I_a est basée sur l'inversion du processus d'insertion d'un système de watermarking. Dans le cas de la détection non-aveugle (*informed detection*), le propriétaire du copyright peut démontrer que W_C se trouve dans I_W ainsi que dans la fausse image originale I_a par la construction de la différence qui devrait être proche de W_C pour une méthode robuste:

$$C_\tau(I_w - I_o, W_c) = 1 \qquad \text{(II.16)}$$

$$C_\tau(I_a - I_o, W_c) = C_\tau(W_c, W_c) - \underbrace{C_\tau(W_a, W_c)}_{=0} = 1 \qquad \text{(II.17)}$$

Néanmoins, l'attaquant peut aussi prouver la présence de son watermark W_a dans l'image marquée I_W et dans l'image originale I_O.

$$C_\tau(I_w - I_a, W_a) = 1 \qquad \text{(II.18)}$$

$$C_\tau(I_o - I_a, W_a) = -\underbrace{C_\tau(W_c, W_a)}_{=0} + C_\tau(W_a, W_a) = 1 \qquad \text{(II.19)}$$

Ce type d'attaque a été proposé par Craver *et al.* [60] dans un rapport du groupe *IBM* où ils ont introduit la notion du watermarking ou tatouage inversible. Ils ont démontré cette attaque sur les systèmes de watermarking dont la détection est non-aveugle en utilisant l'algorithme de Cox [5]. La force de la détection mesurée par C_τ était presque identique. Pour remédier à ce type d'attaque, les auteurs de ce rapport proposent l'utilisation des tatouages non inversibles en liant *W* par une fonction de hachage *H(I_O)* dépendant uniquement de l'image originale. Ce qui signifie en terme de tatouage d'image : d'une part qu'il devient alors impossible de soustraire une signature à une image marquée et d'autre part qu'il ne doit pas être possible d'extraire une signature depuis une image qui n'est pas été marquée.

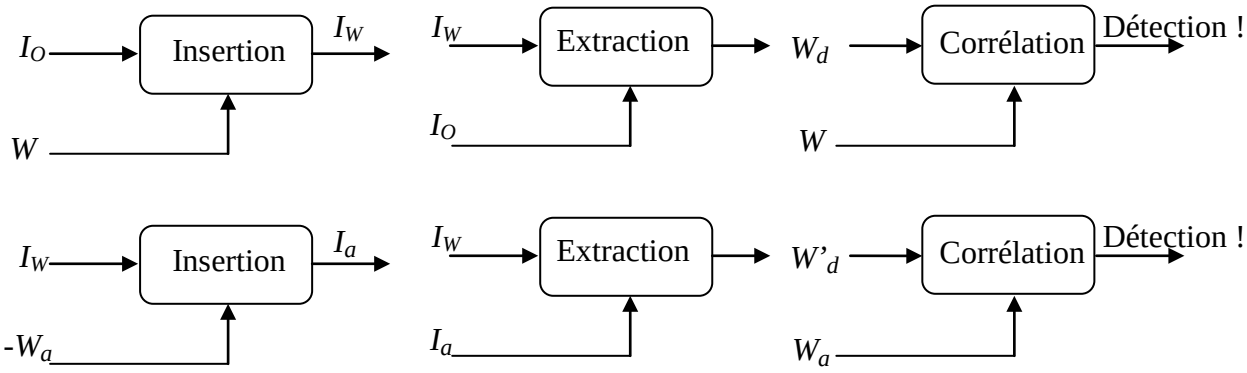


Figure II.12 : Principe de l'attaque IBM ou *deadlock*

- **Attaques par collusion** : les attaques par collusion [61] sont sans doute les attaques cryptographiques les plus difficiles à se prémunir en tatouage d'image. Ces attaques ont lieu lorsque plusieurs sont en possession des mêmes images portant différentes watermarks. La mise en commun de ces images permet de nombreuses opérations : moyenne, recherche de propriétés statistiques communes dans différents domaines, recherche d'informations sur la localisation de la marque…, afin de produire illégalement des images non marquées. On distingue généralement deux cas :
  - dans le premier cas, toutes les images disponibles contiennent le même watermark. Dans cette situation, la collusion consiste à estimer le watermark dans chacune des images marquées, puis une optimisation du watermark est

obtenue par une combinaison linéaire des différentes estimations. Ensuite par l'une des attaques d'effacement vues précédemment (par exemple attaque par remodulation), le watermark est effacé de toutes les images marquée. La seule contre-mesure pour ce type d'attaque est de rendre le watermark fortement lié au contenu de l'image, de telle sorte qu'il serait impossible d'avoir le même watermark dans les différentes images marquées (ce qui est réalisable, par exemple, par l'adaptation perceptuelle du watermark),

- dans le deuxième cas, nous supposons que nous disposons de plusieurs copies d'une image marquée mais qui contiennent des watermarks différents. Cette situation est commune pour les applications de suivie de copy (*fingerprinting*) où chaque image distribué est marquée avec l'identifiant du destinataire. L'image résultante de la moyenne des images marquées sera de la même qualité que ces dernières. Elle contiendra tous les watermarks des images utilisées, mais leurs énergies sont fortement amorties. En générale, si l'on moyenne N copies marquées différemment, l'énergie de chaque watermark dans l'image résultante est réduite par $(1/N^2)$. La détection sera alors perturbée à la fois par cette baisse d'énergie et de possibles interférence entre les marques.

- **Attaque par mosaïques** Ce type d'attaque qui a été proposé par Petitcolas [62] est très simple, mais imparable est pose de graves problèmes aux systèmes automatiques de détection du watermark. Son principe consiste à décomposer l'image marquée en petites imagettes, qui sont ensuite juxtaposées les unes aux autres afin de reconstituer visuellement l'image d'origine (voir figure II.13). on peut donc aisément la regarder sans s'apercevoir de la manipulation, mais le tatouage est totalement désynchronisé si sa détection est automatisée. Donc ce morcellement de l'image marquée provoque une perte de synchronisation et la faible taille des imagettes réduit toute chance de détecter la marque.

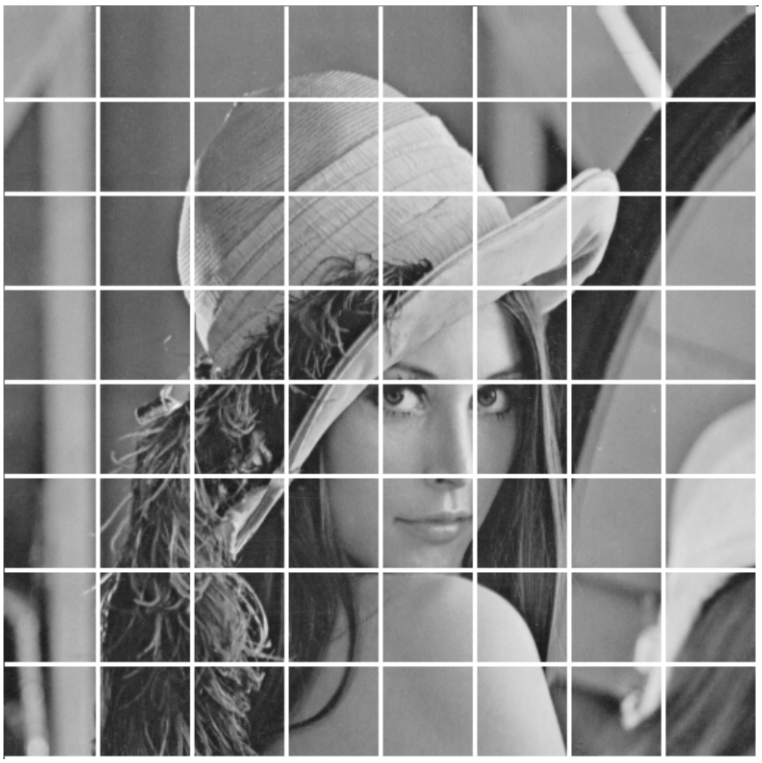


Figure II.13. Attaque par mosaïques

- **Attaques d'évaluation des performances ou « Benchmarking »**

  La conception d'un système d'évaluation efficace est une tâche difficile, en raison de la nécessité de normaliser les attaques contre lesquelles les algorithmes doivent être testés, le niveau désiré de discrétion et de sécurité, et ainsi de suite. Jusqu'au jour, plusieurs efforts ont été faits pour concevoir un bon système d'évaluation, mais la recherche dans ce domaine est toujours en cours. Ces bancs de tests ou logiciels permettent de mettre à disposition des manipulations spécifiques dont le but est de détruire directement le watermark contenu dans l'image. Parmi les logiciels, les plus référencés, réalisant de telles attaques on peut citer les suivant :

  - Stirmark benchmark: développé par Petitcolas et Kuhn [63].
  - Checkmark benchmark: proposé par Pereira [64].
  - Optimark benchmark : réalisé par Solachidis [65].

II.5. Conclusion

Nous nous somme intéressés dans ce chapitre au contexte technique qui entoure le domaine du watermarking d'images fixes. Un système de tatouage d'image se compose

généralement de deux modules qui sont le module insertion et le module extraction ou détection. Pendant la conception on doit opter une approche globale, c'est-à-dire en apportant un soin particulier à la phase de détection de la marque et ceci dès la conception du module d'insertion.

Bien que les techniques de watermarking d'image aient, d'un point de vue algorithmique, atteint une certaine maturité mais il reste toujours associé à un éventail extrêmement large de contraintes. De ce fait le cahier des charges n'est pas fixe ce qui rend impossible de certifier qu'un algorithme puisse faire face à toutes les attaques possibles. Ces différentes attaques, que nous avons présentés, montre la nécessité de penser la conception de l'algorithme en termes d'applications : une fois ces applications sont définies, il devient possible d'anticiper les attaques et de les contrer.

III.1 Introduction

Les premières méthodes de tatouage proposées dès 1995 étaient empiriques. Elles reposaient sur des techniques de substitution, consistant par exemple à inverser une certaine propriété d'un ensemble de sites choisis dans un signal hôte X, telle qu'une relation d'ordre, en fonction du bit du message m à cacher. Ces méthodes relativement simples nécessitent, pour être robustes, l'utilisation de codes correcteurs d'erreurs spécifiques, ou de répéter les substitutions plusieurs fois sur différents segments du signal hôte. La sécurité du tatouage est ainsi diminuée.

Le tatouage s'est ensuite appuyé sur les principes théoriques de la communication numérique, sur la théorie de l'information et la théorie des jeux [66][67]. Deux grandes approches du tatouage ont été proposées, reposant sur des méthodes additives ou substitutives à base de dictionnaires (méthodes issues des travaux de Costa [68].

Les méthodes de tatouage tirent également partie de modèles psychologiques et physiologiques de perception des dégradations des signaux et des images, pour pondérer le signal de tatouage *W* et définir des mesures perceptuelles des distorsions engendrées sur le document hôte par l'insertion et l'attaque du tatouage.

Les schémas de tatouage que l'on peut rencontrer dans la littérature scientifique sont très variés. Autant de paramètres permettent de les distinguer, parmi les quels on peut citer :

- le type de schéma d'insertion de la marque **:** soit un schéma additif (la marque est ajoutée à des composantes de l'image originale), soit un schéma substitutif (ou la marque prend la place de quelques composantes de l'image),
- la stratégie d'insertion de la marque : la manière de transformer la signature (ou le message) en marque numérique et la mise en forme de celle-ci vis-à-vis de l'image à marquer (redondance, codes correcteurs, utilisation d'un masque psycho visuel adaptant la marque à l'image à tatouer**)**,
- la manière de fusionner ou de mélanger intimement la marque avec l'image (modulation), l'idée de base consiste le plus souvent à imposer une relation binaire entre les bites du message et des caractéristiques choisies de l'image porteuse.
- le choix de l'espace de travail : la marque peut soit être insérée dans le domaine spatial, soit dans le domaine transformée (*DCT, TFD*, Ondelettes, fractales, etc.…**).**
- la méthode utilisée pour détecter ou extraire la marque,
- la catégorie d'attaques visées (compression *JPEG*, transformations géométriques, etc.…).

Dans ce chapitre, nous allons parler en premier lieu de ces différents paramètres de distinction des schémas de watermarking. Ensuite, séparées en méthodes spatiales et fréquentielles, nous donneront un état de l'art de quelques techniques utilisées dans le domaine du watermarking d'images fixes.

III.2. Le type de schéma d'insertion de la signature

La phase d'insertion désigne l'opération qui consiste à passer d'une image *I* et d'une marque *W* à une image tatouée I_W. On identifie ici trois principaux types d'insertion : l'insertion additive, substitutive avec dictionnaire et substitutive avec contraintes. Ils diffèrent également par le principe de codage qui leur est associé.

III.2.1 Schémas additifs.

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter une marque *W* qui représente le signal à des composantes de l'image *I* correspondant au bruit. Afin de respecter la contrainte d'imperceptibilité, l'énergie de *W* est très inférieure à celle de l'image *I*. Donc, nous somme en face d'un système de transmission très fortement bruité. Dans un tel contexte, la difficulté consiste à mettre en forme le signal de telle manière qu'il puisse être détecté malgré le bruit causé d'une part par l'image et d'autre par les attaques.

Dans le tatouage additive, l'opération d'insertion est décrite par :

$$I_W = I + W \qquad \text{(III.1)}$$

Le schéma illustré par la figure (III.1) donne les différentes étapes constituants ce type de tatouage et qui sont come suite :

1- extraction des composantes caractéristiques de l'image I. cette opération peut se faire directement a partir de l'image elle-même ou a partir d'une transformation fréquentielle (*DCT, TFD, DWT,…*). Dans le but de donner un caractère secret au domaine d'insertion noté *C(K)* crée par ces caractéristiques, ces dernières sont aménager et réordonnées en utilisant une clé secrète *K*,

2- génération de la marque à insérer, en utilisant le message *M* et la clé secrète *K*, par opérateur de génération que nous appellerons **G** :

$$W = G(M, K) \qquad \text{(III.2)}$$

L'image I peut cependant intervenir dans la génération de W, soit par l'emploi d'un masque perceptuel, soit dans une adaptation au tatouage informé alors :

$$\mathrm{W} = \mathrm{G}(\mathrm{M}, \mathrm{K}, I) \qquad \text{(III.3)}$$

3- la marque W est ajoutée sur les composantes caractéristiques de l'image $C_K(I)$ pour obtenir les composantes $C_K(I_W)$ de l'image marquée :

$$C_K(I_w) = C_K(I) + W(M, K, I) \qquad \text{(III.4)}$$

4- l'image marquée est reconstruite à partir des composantes $C_K(I_W)$

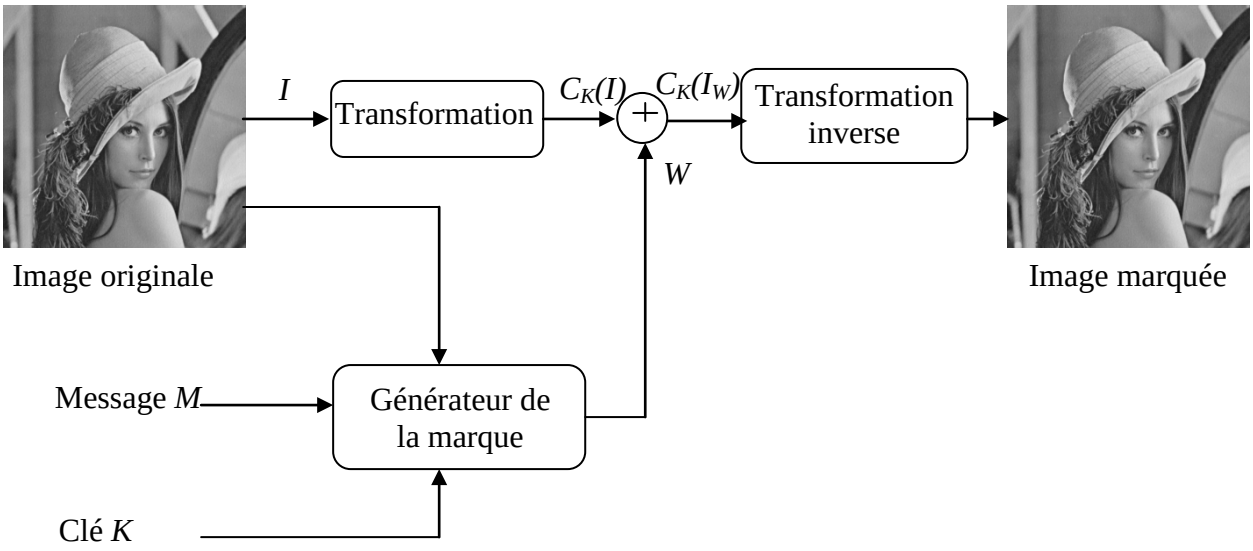


Figure III.1 Insertion de la marque pour des schémas additifs

L'opération de détection (ou extraction) de la marque est l'inverse de l'opération d'insertion. La détection se base essentiellement sur l'utilisation de la corrélation ou les techniques d'estimation par filtrage (par exemple filtrage passe haut, filtre de Wiener voir chapitre 2) ou encore la technique de décision optimale. Ces techniques seront détaillées d'avantage dans la section (III.6). Donc la procédure permettant la détection de la marque, illustrée sur la figure (III.2), se compose des étapes suivantes :

1- en utilisant les mêmes paramètres d'insertion (clé *K* et domaine d'insertion), les composantes caractéristiques marquées sont extraites,
2- extraction de la marque soit par estimation soit par corrélation des composantes caractéristiques tatouées avec la marque originale,
3- décodage du message si la marque contient un message codé.

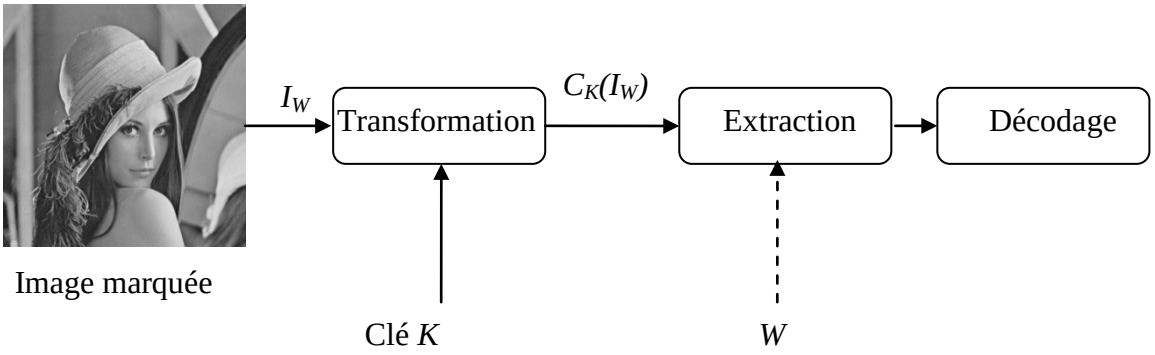


Figure III.2 Extraction de la marque pour des schémas additifs

III.2.2 Schémas substitutifs.

Le principe des schémas substitutifs consiste à substituer la marque à des composantes de l'image, ce qui correspond principalement à deux comportements :

- le premier, que nous appellerons tatouage substitutif avec dictionnaire, consiste à remplacer le signal original par un mot issu d'un dictionnaire noté $\mathcal{D}$: $\mathcal{D}$ est découpé en sous-dictionnaires $\mathcal{D}_M$, chacun correspondant à un message possible *M*. Afin de respecter la contrainte d'imperceptibilité et d'incruster un message, le mot de code inséré doit dépendre à la fois du message secret et de l'image originale (équation. III.3). Ici l'opérateur de génération est un opérateur de choix :

$$\mathrm{G}(\mathrm{M}, \mathrm{K}, I) \in \mathcal{D}_M \qquad \text{(III.5)}$$

- le second type de schémas substitutifs consiste à imposer un ensemble de contraintes aux données marquées, nous le nommerons tatouage substitutif avec contraintes.

Ces définitions sont bien entendu non –exclusives. Par exemple, on peut considérer qu'un tatouage substitutif avec dictionnaire impose la contrainte d'appartenance à un dictionnaire donné. Au niveau purement algorithmique, toute technique substitutive peut également s'interpréter comme une insertion additive. Plus généralement la phase d'insertion des schémas substitutifs, donnée par la figure (III.3), peut être décrite par les étapes présentées ci-dessous :

1- en utilisant la clé privée *K*, des composants caractéristiques $C_K(I)$ de l'image sont sélectionnées. Elles peuvent être des pixels, des coefficients issus des différentes transformations (*DCT*, *DWT*, …), ou encore des propriétés géométriques de l'image,
2- le watermark *W* est exprimé en modifiant les caractéristiques des composantes pointées par la clé *K*. Cela se fait selon une contrainte $\mathcal{F}$ donnée et qui peut être une

relation d'ordre, un critère de similarité, une propriété géométrique de l'image ou encore l'appartenance à un certain espace fonctionnel,

3- les composantes caractéristiques marquées sont obtenues à l'étape de substitution :

$$C_K(I_W) = \mathcal{F}\,(C_K(I),\, W(K)) \qquad \text{(III.6)}$$

4- ces composantes marquées sont ensuite réintégrées pour obtenir l'image marquée.

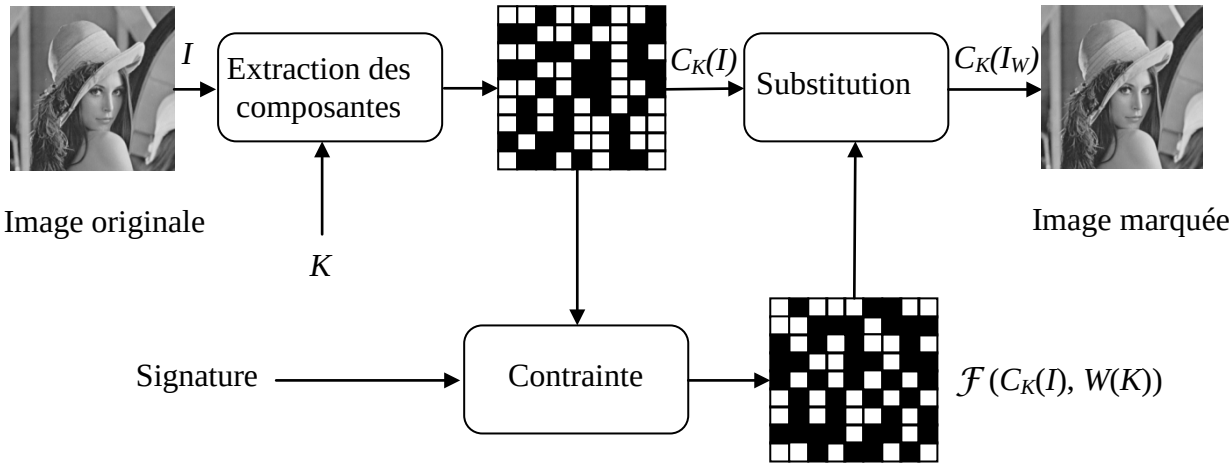


Figure III.3. Schéma d'insertion par substitution

La détection du message inséré, s'il existe, s'effectue directement à partir des composantes extraites de l'image marquée. Cette lecture ne peut pas affirmer que la signature est présente dans l'image. La composante substituée $\mathcal{F}\,(C_K(I),\, W(K))$ doit donc posséder des caractéristiques remarquables. Un préambule, composé d'une séquence prédéfinie, peut par exemple être inséré pour être utilisé lors de la détection [47]. Donc la phase de détection, pour un schéma substitutif donnée sur la figure (III.4), peut se décomposer en quatre étapes :

1- En utilisant la clé secrète K, les composantes caractéristiques $C_K(I_W)$ de l'image marquée I_W.
2- La lecture du message se fait à partir de la contrainte $\mathcal{F}$ utilisée lors de la phase d'insertion de la marque.
3- La détection de la signature s'effectue en comparant le degré de similitude entre le préambule retrouvé et le préambule utilisé lors de l'insertion.

4- La dernière étape consiste à décoder le message.

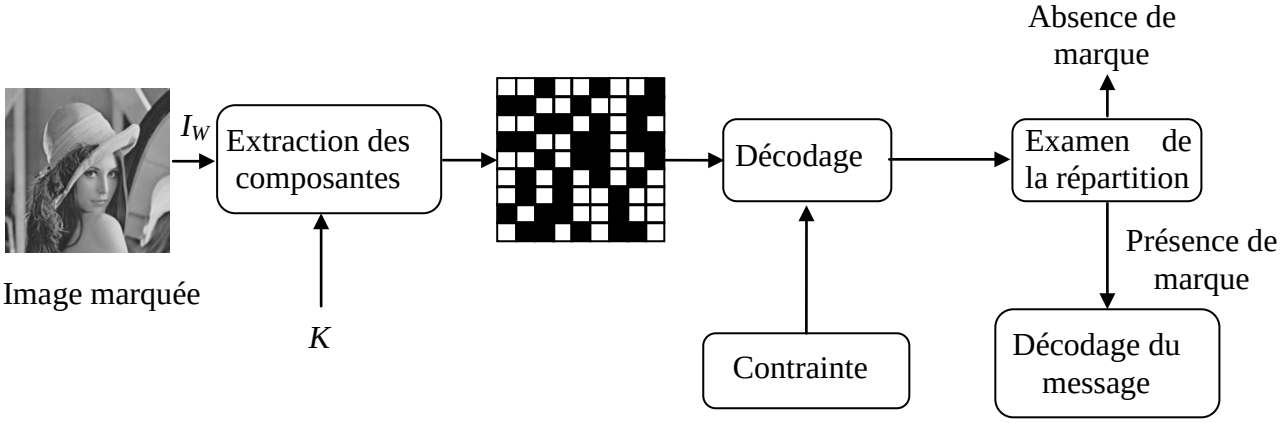


Figure III.4. Détection de la marque pour les schémas substitutifs

Donc pour finir cette section, on peut conclure que les schémas additifs font que le signal hôte (l'image à marquer) est un bruit limitant la performance de la transmission : même en l'absence d'attaque, il est possible d'avoir des erreurs d'extraction. Par contre, dans le cas des schémas substitutifs, les données hôtes n'interférent pas dans le décodage. En l'absence d'attaque, on est certain de décoder correctement le message inséré.

III.3. Le choix de l'espace de travail

Le choix de l'espace ou du domaine de travail nous conduit à définir la nature des éléments de l'image recevant l'information de la marque (signature). Cette nature dépend essentiellement de l'espace de représentation de l'image à marquer. Comme nous le verrons par la suite, chaque espace apporte diverses possibilités en termes de performance et de robustesse. On distingue principalement deux domaines : **spatial** et **transformé**.

III.3.1 le domaine spatial

Le moyen le plus simple d'obtenir un vecteur de données est de considérer directement les valeurs des échantillons de l'image : il s'agit de tatouage dans le domaine spatial où les pixels de l'image sont qualifiés d'abriter l'information de la marque. Bien que les méthodes spatiales ont l'avantage d'être facilement implantables et peu couteuse en temps de calcul, mais la représentation spatiale se prête mal à l'analyse perceptuelle et à la modélisation des attaques. En effet, il est difficile de prévoir l'impacte des attaques sur les données marquées. Ainsi, les compressions telle que *JPEG*, par exemple, modifient principalement les composantes hautes fréquences qui sont peu influentes perceptuellement. Dans le cas d'un tatouage spatial, il est difficile d'isoler ces hautes fréquences, qui seront potentiellement plus

attaquées et qui nécessitent donc un traitement particulier lors des phases d'insertion est d'extraction.

III.3.2 le domaine transformé

Le domaine transformé est un espace d'insertion de la marque obtenu après une transformation inversible (*DCT, DFT, DWT,…*). Donc ces transformations, qui changent l'état de représentation des données de l'image et les transfèrent dans un domaine fréquentielle, permettent d'analyser plus finement l'image à marquée et d'obtenir une représentation plus adaptée au tatouage robuste. De ce fait, les méthodes de tatouage d'image, qui utilisent le domaine fréquentielle comme domine d'insertion, peuvent être d'avantage robuste face aux opérations de compression puisqu'elles utilisent le même espace que celui qui sert au codage de l'image. En plus, le calcul de la transformée d'une image est devenu peu couteux en temps grâce aux algorithmes de transformation rapides. Dans la suite de cette section nous présenterons les transformées les plus utilisées dans le domaine de watermarking.

III.3.2.1. La transformée en cosinus discrète (*DCT*)

Depuis quelques années, la transformée en cosinus discrète (*DCT*) est la représentation de choix pour la compression (*MP3*, *JPEG* et *MPEG*), grâce à son compromis intéressant entre pouvoir de décorrélation, proche de l'optimale, et complexité algorithmique. Elle est utilisée dans les algorithmes de compression *JPEG* et *MPEG* par blocs de taille 8x8. Cette technique est très souvent reprise dans les techniques de tatouage utilisant la *DCT*.

La *DCT* d'une image I(N,N) est donnée par l'équation suivante :

$$C(u,v) = c(u)c(v)\frac{2}{N}\sum_{i=0}^{N-1}\sum_{k=0}^{N-1} I(i,k)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(k+\frac{1}{2}\right)\right) \quad \text{(III.7)}$$

$$\text{Avec :}\begin{cases} c(w) = 2^{-1/2} & w = 0 \\ c(w) = 1 & w > 0 \end{cases} \quad \text{(III.8)}$$

La transformée *DCT* inverse se calcule comme suite :

$$I(i,k) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)C(u,v)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(k+\frac{1}{2}\right)\right) \quad \text{(III.9)}$$

Cette transformée souvent calculée sur des blocs de l'image de taille 8x8, soit 64 coefficients. Ces coefficients sont répartis sur trois zones : basses, moyennes et hautes fréquence, comme il est indiqué sur la figure (III.5).

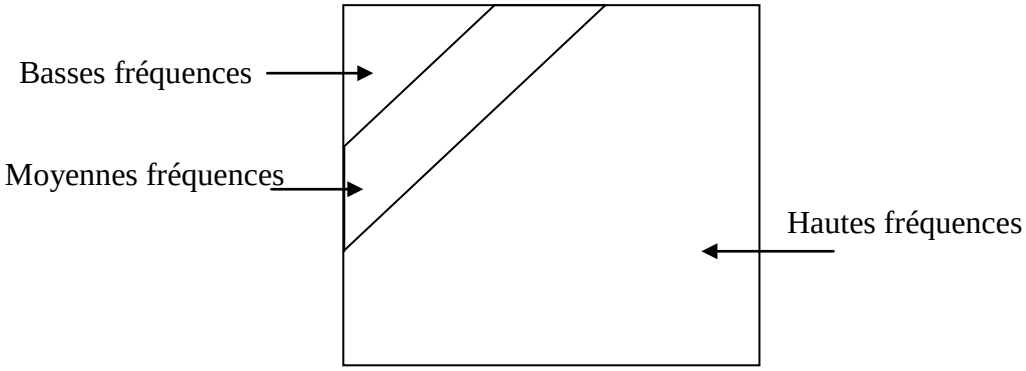


Figure III.5. Répartition des fréquences dans un bloc DCT

Une autre propriété importante de la transformée *DCT* est la décroissance rapide de l'amplitude des coefficients lorsque *u* et *v* augmentent voir (figure.III.6). La raison pour laquelle cette transformée est très utile pour la compression d'images.

149.8	-37.2	0.6	-7.4	-2.0	-5.7	3.5	-3.0
23.9	5.9	0.2	4.5	-1.8	-0.6	-2.0	3.5
0.9	-2.2	-3.4	-5.1	-2.1	1.0	-0.6	0.4
5.2	-0.2	0.3	0.1	-3.1	-1.5	-1.7	0.5
1.0	-0.3	-0.7	0.8	1.3	1.4	-1.6	0.0
-0.9	1.7	3.0	-0.4	0.9	-1.1	2.3	0.2
-2.5	-1.1	0.9	-0.2	0.1	-2.0	1.9	2.5
3.2	1.1	-1.4	3.2	0.0	-1.7	1.0	1.6

Figure III.6 Les valeurs des coefficients d'un bloc DCT

Le dernier point opérant en faveur d'un tatouage utilisant le domaine DCT est qu'il est possible de bénéficier, au moins en partie, des études psychovisuelles pour gérer les problèmes de visibilité de la marque.

Par contre l'utilisation de la *DCT* comme espace d'insertion ne permet pas de localiser avec précision, dans le domaine spatial, les transformations géométriques que la marque peut subir. En effet, celles-ci ont pour effet de modifier considérablement la valeur des coefficients *DCT* d'une manière qui n'est pas facilement modélisable.

III.3.2.2. La transformée de Fourier discrète (*DFT*)

La transformée de Fourier ne sert pas uniquement à l'application des filtres, mais permet par exemple, de traiter directement les fréquences des images (à la manière des signaux) ou encore de compresser des images.

La *DFT* (transformée de Fourier discrète), ainsi que sa transformée inverse *IDFT*, d'une image *I(x, y)* de taille *M* x *N* sont données comme suite :

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \qquad \text{(III.10)}$$

$$f(x,y) = \frac{1}{M.N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi(\frac{ux}{M}+\frac{vy}{N})} \qquad \text{(III.11)}$$

Les images que l'on obtient en appliquant une *DFT* donne une image complexe. On pourrait se demander comment les représenter. En général, on calcule le module F_m et la phase F_p données par les équations suivantes :

$$F_m = |F(u,v)| = [R^2(u,v) + I^2(u,v)]^{1/2} \qquad \text{(III.12)}$$

$$F_p = \emptyset(u,v) = tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \qquad \text{(III.13)}$$

Avec : *R* (*u*, *v*) et *I* (*u*, *v*) sont respectivement les parties réelles et imaginaire de *F* (*u*, *v*).

En général, pour représenter la transformée, on représente uniquement le module dont la répartition fréquentielle est illustrée sur la figure (III.7) Il est à noter qu'en raison des propriétés de symétrie du spectre *DFT*, le nombre effectif de coefficients *DFT* est moins que N^2. En notant que les amplitudes des coefficients dans le premier et le deuxième quadrant sont égales à celles des coefficients du troisième et quatrième quadrant. Donc, on obtient $N^2/2$ coefficients indépendants qui peuvent être utilisés pour insérer le watermark. En outre, comme pour le cas de la *DCT*, afin de trouver un compromis entre la visibilité et la robustesse seuls les coefficients de fréquence moyenne (la zone de couleur grise sur la figure III.7) sont habituellement exploités.

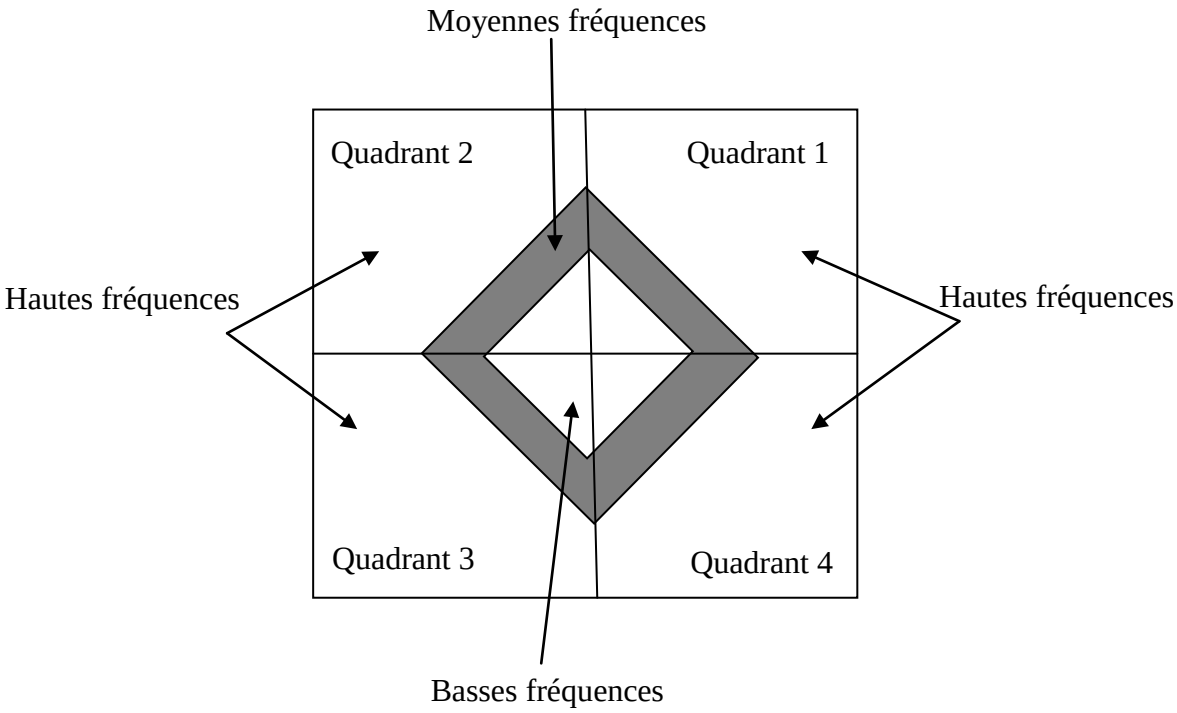


Figure.III.7. Répartition fréquentielle des coefficients de l'amplitude d'une *DFT*

L'utilisation de la phase de l'image complexe pour l'insertion de la marque est possible mais avec précaution. En fait, la phase dispose de beaucoup d'informations pertinentes de l'image. L'exemple qu'on donnera montre l'importance des informations contenues dans la phase d'une *DFT* d'une image. On calcul la transformée *DFT* des deux images données sur la figure (III.8). Ensuite, comme il indiqué sur la figure (III.9), on reconstruit les deux images avec permutation de leurs phases.

Dans le domaine de la *DFT*, une translation de l'image se répercute exclusivement sur la phase et laisse invariant l'amplitude comme il est indiqué par l'équation (III.14).

$$I(x+a, y+b) \rightarrow F(u,v)e^{-j(a.u+b.v)} \qquad \text{(III.14)}$$

Donc, en travaillant sur le module, le tatouage est robuste à cette attaque. Mais les transformations géométriques ce n'est pas uniquement la translation, il y a aussi la rotation et le changement d'échelle. Donc, pour faire face aux problèmes de désynchronisation causée par toutes ces transformations géométriques, il faut trouver un espace complètement invariant à ces transformations. C'est ce que nous allons présenter dans la section qui suit.

Figure. III.8. Les deux images originales avant permutation de phases

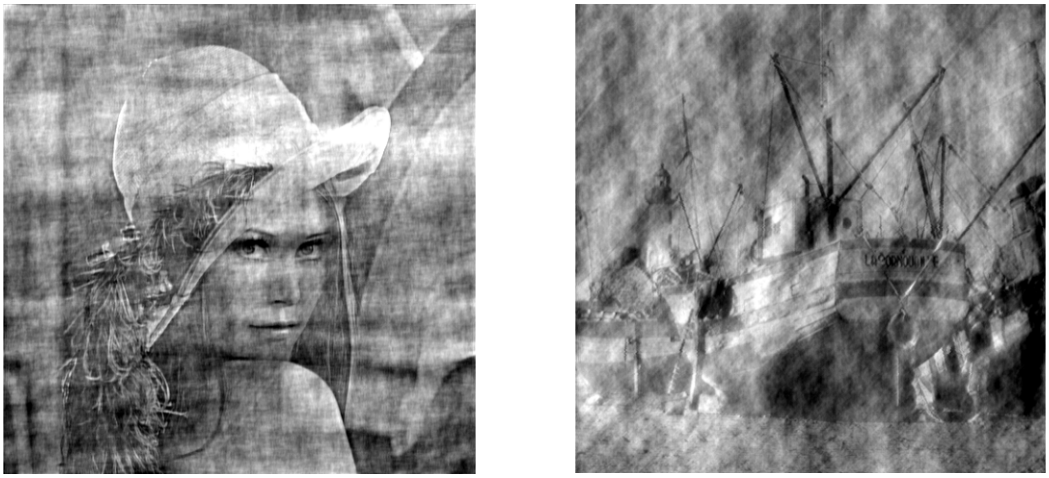


Figure. III.9. Les deux images originales après permutation de phases

III.3.2.3. La transformée de Fourier-Mellin.

Les transformations géométriques sont actuellement les attaques les plus efficaces pour empêcher la détection de la signature dans l'image marquée. Ce constat a conduit les tatoueurs d'images à chercher un espace transformée invariant aux transformées géométriques. Comme nous l'avons vu dans la section précédente, le module de la transformée de Fourier possède une invariance aux translations (qui sont en réalité des translations spatiales circulaires). Maintenant, concernant la rotation et le changement d'échelle, le spectre d'amplitude est affecté par ces transformations. En effet, l'extension des

axes d'une image, avec un facteur (σ) dans le domaine spatial provoque une mis à l'échelle inverse dans le domaine fréquentiel, comme il est décrit par l'équation (III.15). En outre, la rotation de l'image d'un angle (θ) dans le domaine spatial se traduit par une rotation du même angle du spectre d'amplitude de la transformé de Fourier (équation III.16).

$$I(\sigma.x, \sigma.y) \rightarrow \frac{1}{\sigma} F(\frac{u}{\sigma}, \frac{v}{\sigma}) \quad \text{(III.15)}$$

$$I(x.\cos\theta - y.\sin\theta\,, x.\sin\theta + y.\cos\theta) \rightarrow F(u.\cos\theta - v.\sin\theta\,, u.\sin\theta + v.\cos\theta) \quad \text{(III.16)}$$

Pour faire face aux problèmes de rotation et de changement d'échelle, O Ruanaidh *et al.* [69] préconisent l'usage de la transformée de Fourier-Mellin. Les auteurs étendent les propriétés d'invariance par translation cyclique de la transformée de Fourier en utilisant le changement de variable pour chaque couple (*x, y*). Ce changement permet de passer d'un repère cartésien (x, y) vers un autre logarithmique-polaire (ρ, θ) comme il est indiqué sur la figure (III.10).

$$\begin{cases} x = e^{\rho}\cos\theta \\ y = e^{\rho}\sin\theta \end{cases} \quad \text{(III.17)}$$

Avec : $\begin{cases} \rho = \log \mathrm{r} = [(x - x_c)^2 - (y - y_c)^2]^{1/2} \\ \theta = tan^{-1}.\frac{y - y_c}{x - x_c} \end{cases}$ (III.18)

Où (r, θ) sont les coordonnées polaires, et (x_c, y_c) est le centre du plan log-polaire de l'image.

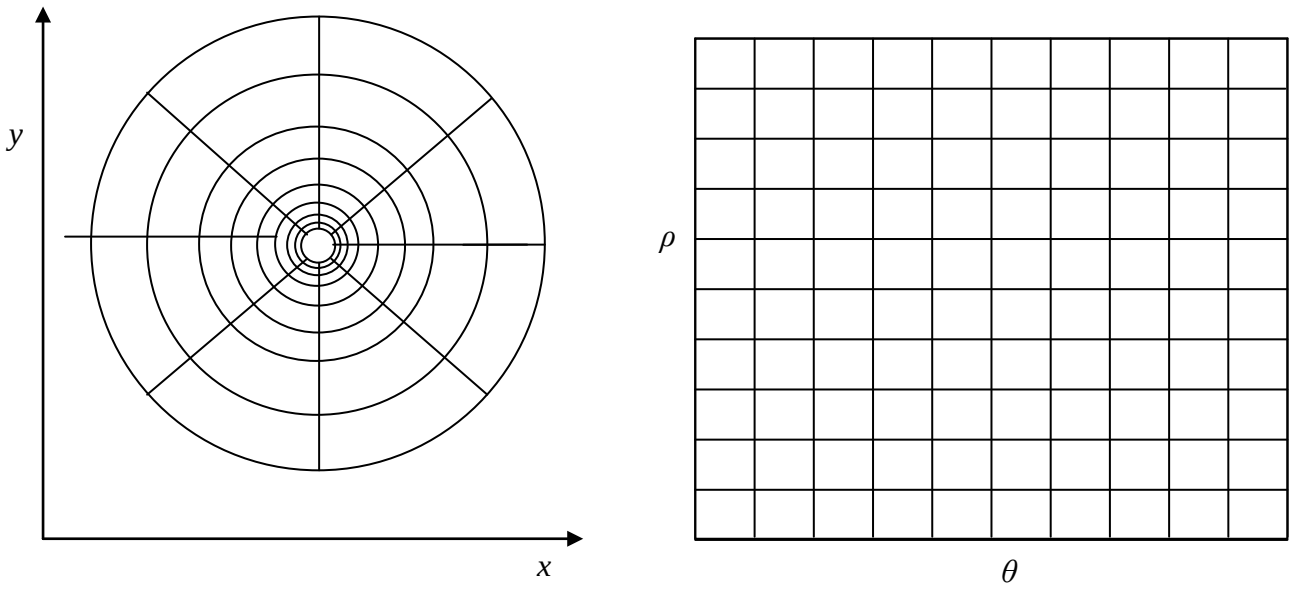


Figure III.10. Le passage du domaine cartésien au domaine log-polaire

Ce passage, du domaine cartésien au domaine log-polaire, ramène les opérations de rotation et de changement d'échelle à une translation (équations III.19 et III.20) :

$$(\sigma.x, \sigma.y) \leftrightarrow (\rho + log\sigma, \theta) \quad \text{(III.19)}$$

$$(x\cos(\theta+\alpha) - y\sin(\theta+\alpha), x\sin(\theta+\alpha) + y\cos(\theta+\alpha)) \leftrightarrow (\rho, \theta+\alpha) \quad \text{(III.20)}$$

Le calcul de la transformée de Fourier, après ce changement de variable, donne un espace invariant aux rotations et aux changements d'échelles. Cette transformée s'appelle la transformée de Fourier-Mellin. La figure (III.11) donne les différentes étapes de transformations nécessaires à la construction d'un espace d'insertion de la marque invariant aux transformations géométriques (translation, rotation et changement d'échelle). Cette transformation de l'image du domaine spatial au domaine invariant se compose d'une transformée de Fourier suivie d'une transformée de Fourier-Mellin. Pour que la transformation soit inversible, la phase de l'image originale est conservée et réutilisée lors du retour au domaine spatial.

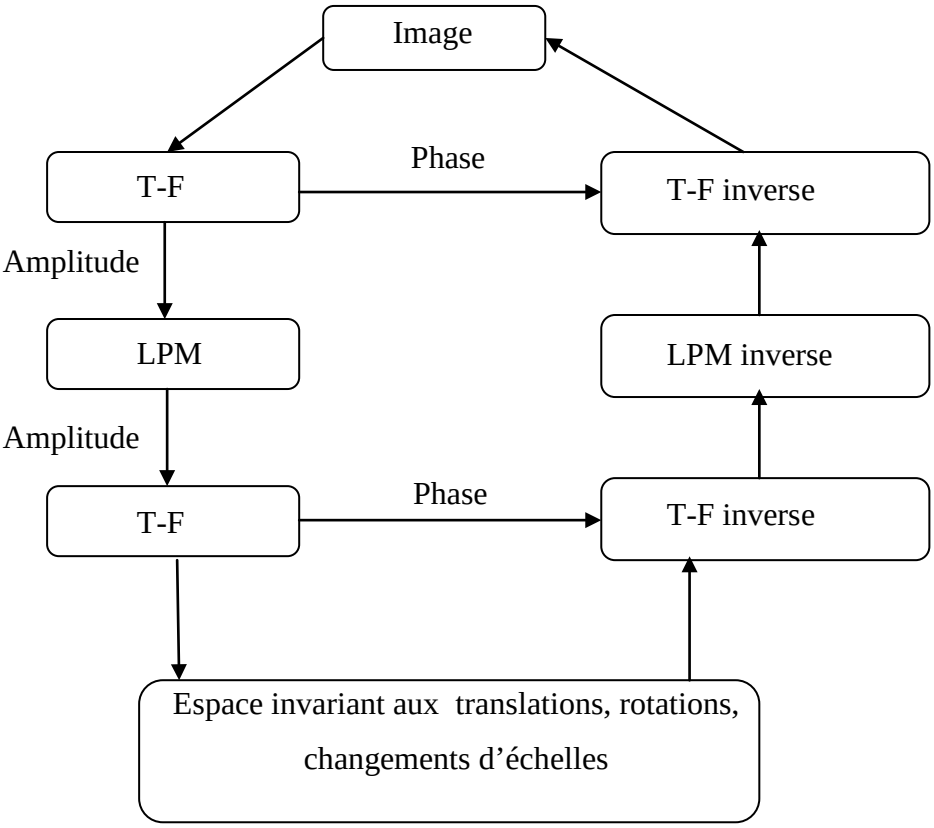


Figure III.11. Construction d'un espace invariant aux transformations géométriques

Donc l'invariance à la translation est assurée par l'utilisation du module de la transformée de Fourier insensible aux translations. Par contre, l'invariance à la rotation et au changement d'échelle est obtenue par :

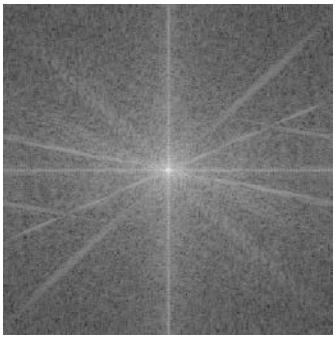
- une transformation en coordonnées log-polaires du module de la transformée de Fourier, cette opération permet de transformer les rotations et les changements d'échelles en simples translations.
- L'application d'une deuxième transformée de Fourier permet d'annuler l'effet de ces translations et par conséquent un espace invariant à la translation, rotation et changement d'échelle.

Le passage des coordonnées euclidiennes aux coordonnées polaires implique des approximations numériques dans le cas discret, liées à un problème de changement de grille d'échantillonnage. Ces approximations font que l'enchaînement transformée de Fourier-Mellin et transformée inverse n'est pas sans part : la transformée n'est pas parfaitement inversible en pratique et introduit une distorsion supplémentaire si elle est utilisée dans un schéma de watermarking. Il convient donc d'utiliser une interpolation qui ne dégradera pas trop la reconstruction de l'image.

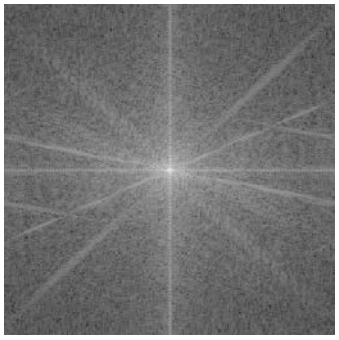
L'insertion et la détection de la marque se font de façon classique dans le domaine transformé de l'image. Les figures (III.12) et (III.13) illustrent un exemple de l'application de cette transformée.

a-image originale

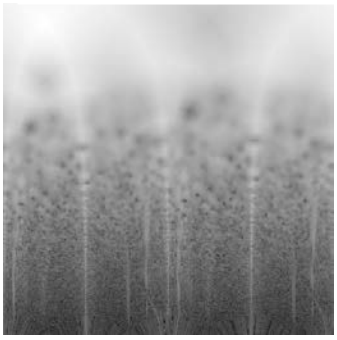
b-image translatée



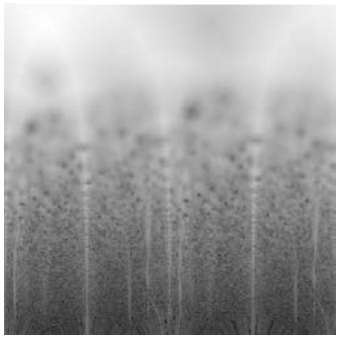
c- Spectre d'amplitude de l'image originale



d- Spectre d'amplitude de l'image translatée



e- Log-polaire de l'image originale

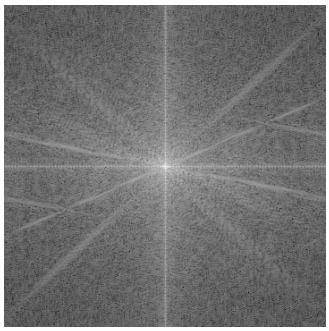


f- Log-polaire de l'image translatée

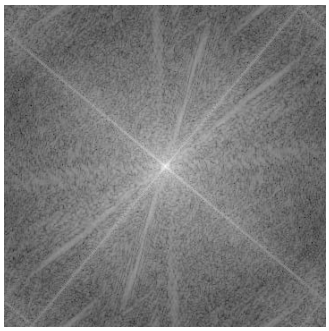
Figure III.12. Exemple d'une image translatée par (50,

a. image originale

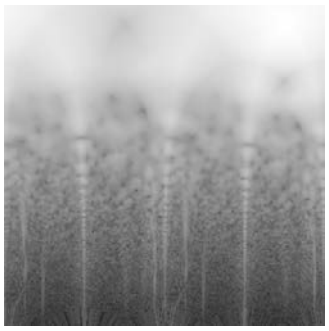
b. image réduite par X et pivotée d'un angle α



c- Spectre d'amplitude de l'image originale



d- Spectre d'amplitude de l'image transformée



e- Log-polaire de l'image originale

f- Log-polaire de l'image transformée

Figure III.13. Exemple d'une image réduite par X et pivotée d'un angle α

III.3.2.3. La transformée en ondelettes discrète (*DWT*)

La transformation en ondelettes est née de la convergence des travaux théoriques déjà anciens, notamment ceux de Haar (1910), de Littlewood et Paley (1930), de Zygmund (1930), de Gabor (1940), puis vers 1960 de Calderon, et des idées récentes mises en avant propos; pour le traitement numérique de certains signaux par Morlet (le premier à avoir proposé le nom d'ondelettes, 1982), ou pour le développement d'outils mathématiques utilisés en physique théorique par Grossmann (1983). Dés lors de nombreux chercheurs apportèrent des bases mathématiques solides en faisant apparaître la notion de base orthogonale (Meyer, 1985), d'analyse multi-résolution (Mallat, 1989), et d'ondelettes à support compact (Daubechies, 1988).

La transformée en ondelettes qui, tout comme la transformée *DCT*, fait l'objet de nombreuses études dans le contexte du codage. En effet, elle représente la pierre angulaire du récent format de compression d'image *JPEG 2000*. Elles ont également trouvé un écho dans la communauté du tatouage d'image.

La transformée en ondelettes discrète (*DWT*) bidimensionnelle repose sur la notion d'analyse multi-résolution d'une image. Donc elle permet de transformer un signal discret en sous –bandes directionnelles, assimilables à une décomposition fréquentielle récursive. Cette décomposition est réalisée à l'aide d'une paire de filtres *QMF* (filtres quadratiques miroirs), l'un étant passe haut (*H*) et l'autre passe bas (*L*). Ces deux filtres sont successivement appliqués sur toute l'image qui à leur sortie subit un sous échantillonnage par un facteur de 2. Nous obtenons ainsi une sous bande basses fréquences (*LL*), et trois sous bandes hautes fréquences présentant des orientations spatiales caractéristiques (diagonale, horizontale et verticale) : (*HH*), (*HL*) et (*LH*) respectivement comme il est indiqué sur la figure (III.14).

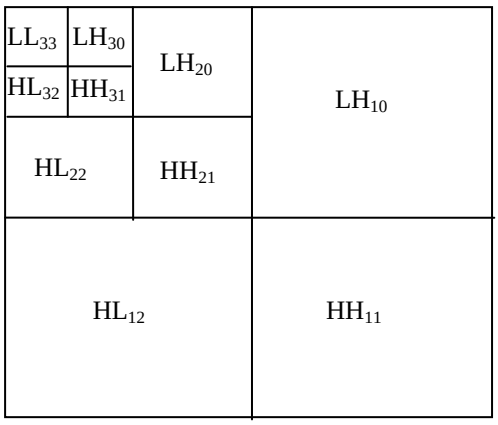


Figure. III.14 Exemple de décomposition d'une image en ondelettes à 3 niveaux

Outre l'interprétation fréquentielle des sous-bandes, on remarque que la structure spatiale de l'image est conservé (au contraire des transformées de Fourier et *DCT*) : on a un aspect spatio-fréquentiel comme on peut le constater sur l'exemple donné sur la figure (III.15). Les sous-bandes représentent l'information portée par l'image source à différents niveaux de résolution : l'image d'approximation (*LL*) est une version réduite et lissée de l'image initiale tandis que les images de détails horizontale (*LH*), verticale (*HL*) et diagonale (*HH*) contiennent uniquement des informations relatives à la texture locale et aux contours des régions de l'image, à une résolution donnée et selon une direction donnée.

Donc la décomposition d'une image en sous-bandes permet d'en isoler les composantes basse-fréquences. Celles-ci constituent en espace d'insertion qui est moins sensible que l'image elle-même. D'autre part, la décomposition de l'image en sous-bandes est souvent proche d'une décomposition en canaux perceptifs et facilite l'utilisation d'un modèle psycho- visuel.

Figure III.15. Décomposition de l'image Lena en ondelette niveau 1

La transformée *DWT* présente deux inconvénients qui sont :

- Le manque d'invariance au décalage, ce qui signifie des petits changements dans le signal d'entrée peuvent provoquer de grands changements dans les coefficients d'ondelettes

- Une mauvaise sélectivité directionnelle des caractéristiques diagonales.

Parmi les alternatives possibles on trouve la transformée *UDWT* (*Undecimated Discrete Wavelet Transform*) qui est invariante au décalage mais elle est très redondante et a encore une faible sélectivité pour les caractéristiques diagonales. Une autre alternative c'est l'ondelette complexe (*CWT*) qui, au prix d'une redondance modérée, offre une invariance au décalage.

Il existe plusieurs types d'ondelettes, parmi les quelles on peut citer : les ondelettes de Haar, utilisées dans notre étude, celles de Daubechies, Coiflets, Symlets… (Voir annexe *B*).

Outre les transformée *DCT, DFT* et *DWT* précédemment évoquées, les transformations inversibles classiques en traitement d'image sont la transformation de Karhunen-Loève (*KLT*), de Hadamard, de Slant et la décomposition en valeurs singulières (*SVD*) [70]. Ces quatre domaines ont été utilisés en tatouage d'images, sans apporter de différence significative de performance et pâtissant d'une étude perceptuelle complexe. De nombreux autres domaines transformés ont été envisagés, sans apporter en pratique une amélioration significative des performances ou des invariances géométriques : transformée de Fourier fractionnelle, transformation de Radon-Wigner, transformée de Laguerre Discrète, transformation Mojette (cas particulier de transformée de Radon [71]) et même la phase des images [72].

III.3.3 Décomposition de l'image en canaux perceptifs

Pour satisfaire les deux contraintes conflictuelles que sont l'invisibilité et la robustesse aux attaques, les schémas de watermarking s'orientent de plus en plus vers l'exploitation des modèles du système visuel humain *HVS*. En effet, la sensibilité du *HVS* aux fréquences spatiales est exploitée pour déterminer les sites propices à l'insertion de la marque. Ceci on considérant le *HVS* comme un ensemble de canaux par lesquels sont transmis différents types d'informations au cerveau [73], [74], [75]. Les techniques de watermarking, dont le but est d'améliorer l'invisibilité de la marque dans l'image, ont cherché à utiliser ces travaux et en particulier les effets de masquage que nous détaillerons dans la section (III.4.1). Delaigle et al. [76], [77] 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 watermarking. L'algorithme proposé 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 deux signaux à l'intérieur d'un même canal ne pourront être distingués par l'œil humain.

La sensibilité du système visuel humain (*HVS*) dépend principalement de trois paramètres : la fréquence spatiale, la couleur et l'intensité lumineuse (la luminosité). La réponse perceptuelle en fonction de la fréquence spatiale correspond à la sensibilité au contraste. Cette réponse définie la fonction de sensibilité au contraste (*CSF*), étudiée dans [78]. Celle-ci quantifie la faculté de l'œil à percevoir un signal périodique dans l'espace mais aussi dans le temps. Le *HVS* est sensible aux contrastes moyens, et peu stimulé par les contrastes très for ou très faibles. De plus, la sensibilité varie selon l'orientation de cette fréquence : l'œil est plus sensible aux motifs horizontaux et verticaux, plutôt qu'aux motifs à 45 degrés. Le second paramètre est la fréquence spectrale, c'est-à-dire la couleur. Le *HVS* n'est en effet pas sensible de la même manière aux différentes longueurs d'onde du spectre visible. Dans le cas d'une représentation de la couleur sous la forme de trois canaux {rouge, vert, bleu}, le canal bleu est celui qui a le moins d'importance (le *HVS* y est moins sensible). Enfin, le dernier paramètre est la luminosité. L'œil peut remarquer de plus petites variations de luminosité quand la luminosité moyenne est faible.

Ces paramètres doivent être prises en compte dans la conception des modèles perceptuels afin qu'ils soient proches de la réalité.

III.3.3.1 Modélisation mono-canal

Afin de déterminer la sensibilité au contraste du *HVS*, plusieurs études ont été menées. Le principe général consiste à afficher des stimuli spatiaux, mono fréquentiels, monodimensionnels, à variation de luminance donnée par :

$$L(x) = L(1 + c\sin(2\pi f x)) \qquad \text{(III.21)}$$

où L est la luminance de fond et à déterminer la valeur minimale du contraste « c » permettant de détecter la fréquence f. Le contraste obtenu C_{jn} (Just Noticeable Contrast) est appelé « contraste seuil » ou « seuil de visibilité ».

$$C_{jn} = \frac{\Delta L_{jn}}{L} \qquad \text{(III.22)}$$

L'inverse de ce contraste représente la fonction de sensibilité aux contrastes :

$$CSF = \frac{1}{C_{jn}} = \frac{L}{\Delta L_{jn}} \qquad \text{(III.23)}$$

Le premier modèle de la fonction de sensibilité aux contrastes (*CSF*) a été proposé dans les années 70 par Mannos et Sakrison [78] et s'écrit :

$$CSF(f) = a\left(b + \frac{f}{f_0}\right)\exp\left(-\frac{f}{f_0}\right)^c \quad \text{(III.24)}$$

a, *b*, *c* et f_0 représentent les paramètres du modèle. L'expression donnée par l'équation (III.25) a été utilisée par les auteurs, dans le cadre de l'évaluation de la qualité des images dégradées, pour pondérer le spectre de l'image d'erreur.

$$CSF(f) = 2.6(0.192 + 0.114f)\exp(-0.114)^{1.1} \quad \text{(III.25)}$$

Bien que cette modélisation soit largement admise, diverses études sont menées pour prendre en compte les différents paramètres expérimentaux. Ainsi la *CSF* proposée par Barten [79] tient compte de la variation de la luminance de fond L et des conditions d'observation. Cette *CSF* s'écrit :

$$CSF(f, L) = a(L, f, \omega)f\sqrt{1 + 0.06\exp[b(L)f]}\,.\exp\,[-b(L)f] \quad \text{(III.26)}$$

Avec :

L : représente la luminance de fond et est exprimée en candelas par mètre carré.

f : représente la fréquence radiale et s'exprime en cycles par degré.

Les paramètres du modèle $a(L, f, \omega)$ et $b(L)$ sont donnés par :

$$a(L, f, \omega) = \frac{540(1+\frac{0.7}{L})^{-0.2}}{1+\frac{12}{\omega(1+\frac{f}{3})^2}} \quad \text{(III.27)}$$

$$b(L) = 0.3(1 + \frac{100}{L})^{0.15} \quad \text{(III.28)}$$

L'angle solide ω, exprimé en degrés, est donné par

$$\omega = \frac{180}{\pi}\frac{\sqrt{A}}{D} \quad \text{(III.29)}$$

Avec *A* représente la taille de l'image et *D* la distance d'observation.

Cette *CSF* a été modifiée pour rendre compte du caractère non isotropique de la sensibilité visuelle [80]:

$$CSF(f, L, \theta) = a(L, f, \omega)f\sqrt{1 + 0.06\exp[b(L)f]}\,.\exp\,[-b(L)f\Gamma(\theta)] \quad \text{(III.26)}$$

Avec : $\Gamma(\theta) = 1 - 0.079[\cos(4\theta) - 1]$.

III.3.3.2. Modélisation multi-canal

Bien que souvent utilisée, la modélisation « mono-canal » ne suffit pas toutefois à expliquer le comportement du *HVS* vis-à-vis de stimuli complexes [81][82]. Il est admis que le HVS utilise pour l'analyse des signaux d'entrée un ensemble de canaux dont chacun est sensible à une orientation et une fréquence spatiale donnée [83]. Les caractéristiques de ces canaux, séparables dans une représentation polaire, on fait l'objet de plusieurs études [84][85][86].

Pour ce qui est de la sélectivité radiale, différentes valeurs de largeur de bande existent. Une largeur de bande constante égale à l'octave est donnée dans [87][88] alors que Georgeson et Harris [89] relèvent une valeur de 1.33 octaves. Une bande passante de 2 octaves dépendante de la fréquence spatiale est également donnée dans [90] pour un canal centré sur 8 cycles/degré.

Concernant la sélectivité angulaire, celle-ci varie avec la fréquence centrale du canal visuel considéré. Pour les faibles fréquences radiales (autour de 1cy/d°), la largeur de bande angulaire mesurée dans [89] est de l'ordre de 50 degrés. Pour les moyennes fréquences radiales (autour de 4 cy/d°), cette largeur de bande varie selon les auteurs entre 35 et 40 degrés [86]. Enfin, pour les moyennes-hautes fréquences (8 à 12 cy/d°), la bande passante est d'environ 30 degrés [90], [86].

La modélisation en canaux perceptuels décrite dans [91] est donnée sur la figure (III.16). Elle consiste en quatre bandes radiales appelées couronnes. La couronne I (basses fréquences) est non sélective en orientation. Les largeurs de bandes des couronnes II, III et IV sont respectivement de 1.9 octaves, 1.3 octaves et 1 octave. Chacune de ces couronnes est sélective en orientation. Cette sélectivité angulaire dépend de la fréquence spatiale et vaut 45 degrés pour la couronne II et 30 degrés pour les couronnes III et IV.

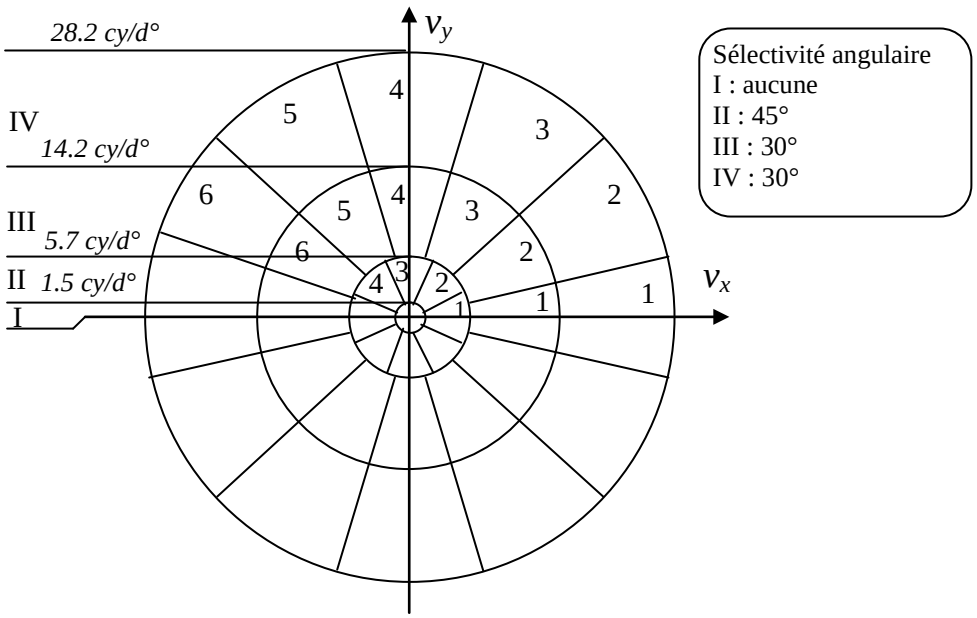


Figure III.16. Modélisation du comportement des parties périphériques du *HVS*

III.4. La stratégie d'insertion de la marque

Comme nous l'avons présenté à la section (I.6.1) du premier chapitre, l'insertion de la marque dans un document peut nécessiter le passage par ces trois phases : codage, insertion et dissimulation. Pour le codage et l'insertion, nous avons détaillé suffisamment ces points dans la même section. En ce qui concerne la dissimulation, qui se base essentiellement sur le masquage psychovisuels, la section ci-dessous portera plus de détailles et d'explications.

III.4.1 Masquage psychovisuel

La contrainte d'imperceptibilité impose aux tatoueurs d'insérer une marque suffisamment faible et dans les composantes les moins perceptibles. L'utilisation de modèles psychovisuels permet d'augmenter la puissance de la marque sans que le gain soit visuellement perceptible. L'objectif de ces techniques est de prendre en défaut le système visuel humain *HVS* et d'exploiter les différentes propriétés de masquage. C'est quoi le masquage ? Pour répondre à cette question nous nous référerons à la section précédente. En accord avec la modélisation perceptuelle présentée, les signaux ayant des caractéristiques voisines sont traités par les même canaux visuels et suivent donc le même cheminement de l'œil jusqu'au cortex. Il apparaît en effet que de tels signaux interagissent entre eux et sont soumis à des effets non linéaires. L'effet non linéaire le plus considéré est l'effet de masquage. Ce dernier traduit la variation du seuil de détection d'un stimulus due à la présence d'un signal, qualifié de signal masquant, ayant des caractéristiques voisines et un niveau plus fort. De nombreux modèles de masques psychovisuels ont été proposés pour le tatouage d'images [92][93]. Ils utilisent des propriétés empiriques du système visuel humain, combinées avec une analyse statistique. Ces masques sont classés en deux catégories : les masques spatiaux et les masques fréquentiels.

III.4.1.1. Masques spatiaux

La méthode la plus intuitive et facile à mettre en œuvre consiste à tenir en compte de l'activité de l'image. En effet, la conception des masques spatiaux se base sur les trois règles suivantes :

1- Les perturbations sont beaucoup moins visibles sur les régions fortement texturées que sur les surfaces uniformes.
2- Les contours sont plus sensible à l'ajout du bruit que les régions fortement texturées mais moins sensible comparativement aux zones uniformes.

3- Les perturbations sont beaucoup moins visibles dans les régions très sombre ou fortement éclairées.

Donc les masques spatiaux sont calculés à partir de la luminance et favorisent les contours et les régions de forte texture. L'approche la plus pratique pour prendre en compte les règles citées précédemment et les caractéristiques du *HVS* vues dans la section (III.3.3) est l'introduction d'une pondération perceptuelle. On peut donc se contenter d'une pondération par un facteur de masquage (ψ) qui limite la puissance du watermark (W). Il est cependant préconisé d'utiliser un masque mesurant les variations locales de luminance, car l'œil est moins sensible aux modifications d'amplitude situées prés des contours et dans les régions fortement texturées. Ce modèle psychovisuel très simple s'appelle « loi de Weber » : la sensibilité du *HVS* est inversement proportionnelle à l'intensité lumineuse (voir section 5.1.1 de [1]). Ces masques spatiaux conduisent souvent à des tatouages passe-haut, ce qui peut nuire à la robustesse. Le masquage de contour n'est efficace que si le masque a la même orientation que l'image. C'est pourquoi le masquage de texture est souvent privilégié. L'un des masques spatiaux les plus courants est appelé « filtre Laplacien », car il annule les dérivées secondes horizontales, verticales et diagonales de l'image [94] : le masque (ψ) est obtenu en prenant les valeurs absolues de l'image I convoluée par un masque Laplacien (h):

$$\psi_{k_1,k_2} = h_\psi \otimes I(k_1, k_2) \qquad \text{(III.27)}$$

$$h_\psi(k,l) = \frac{1}{9}\begin{bmatrix} -1 & -1 & -1 \\ -1 & 8 & -1 \\ -1 & -1 & -1 \end{bmatrix} \qquad \text{(III.28)}$$

Les travaux de l'équipe de T. Pun [95] s'appuient sur une pondération calculée à partir d'une constatation simple : l'œil agit comme un filtre débruiteur. Plus le filtre supprime de bruit, et moins le *HVS* sera sensible à ce bruit. Les auteurs définissent alors une mesure, notée NVF (*noise visibility function*), d'une forme similaire à celle de la pondération d'un filtre de Winner. La fonction de visibilité du bruit (*FVB*) est calculée à partir des variances locales de l'image et du bruit :

$$FVB = \frac{p.\sigma_n^2}{p.\sigma_n^2 + \sigma_x^2} \qquad \text{(III.29)}$$

Où σ_x et σ_n représentent respectivement les variances locales de l'image et du bruit, p représente un facteur de pondération.

L'insertion de la marque s'effectue alors de la façon suivante :

$$I_w = I + S(1 - FVB).W \qquad \text{(III.30)}$$

Où *S* est une constante qui représente la force d'insertion de la marque.

Ce masque permet donc d'insérer une marque de dynamique importante dans les régions de l'image correspondant aux textures et aux contours. Par contre, la marque insérée dans les zones uniforme est très faible car la fonction *FVB* est proche de 1.

III.4.1.2. Masques fréquentiels

Les masques spatiaux concentrent le watermark sur les textures er les contours de l'image. Cependant, les contours d'une image concernent peu de ponts, ce qui réduit la taille du watermark à insérer et la robustesse. De plus, une modification d'un contour peut générer des artefacts perceptibles. Cette limitation est mise en avant par Delaigle et al. [96] qui ont été les premiers à proposer un schéma de tatouage liant étroitement le Système Visuel Humain et l'insertion de la marque dans l'image. Ils préconisent l'utilisation de filtres de contraste et de motif, beaucoup plus complexes et faisant intervenir le domaine fréquentiel. Dans le domaine fréquentiel, les masques sont beaucoup plus efficaces et indispensables afin de ne pas modifier les basses fréquences (composantes les plus perceptibles) ou les hautes les hautes fréquences (les plus vulnérables aux attaques).

Bartolini et *al*. proposent d'améliorer un schéma utilisant la transformation en cosinus discrète (*DCT*) par l'utilisation d'un masque qui exploite les propriétés du *HVS* [97]. Le masque *M* crée contient des valeurs appartenant à l'intervalle [0, 1]. Il permet de pondérer l'image originale *I* et l'image marquée sans masque I_w pour obtenir une autre image tatouée I_{wm} en tenant compte des propriétés du masque :

$$I_{wm} = (1 - M)I + MI_w = I + MW \qquad \text{(III.31)}$$

Où W représente la marque insérée : $W = I_w - I$

Les auteurs comparent trois méthodes différentes afin de créer des masques psychovisuels. La première est basée sur un calcul d'activité de l'image à partir de la variance locale de l'image. La seconde utilise un modèle du système visuel humain. La dernière est la méthode qui offre le meilleurs compromis invisibilité / robustesse, elle s'appuie sur une analyse des moyennes fréquences de l'image. Ces composantes moyennes fréquences, après une décomposition *DCT*, sont isolées et utilisées pour l'insertion de la marque. Les auteurs prennent aussi en compte les composantes sombres et très lumineuses de l'image, ainsi que les composantes correspondant aux contours de l'image. Le principe de la création du masque est illustré sur la figure (III.17).

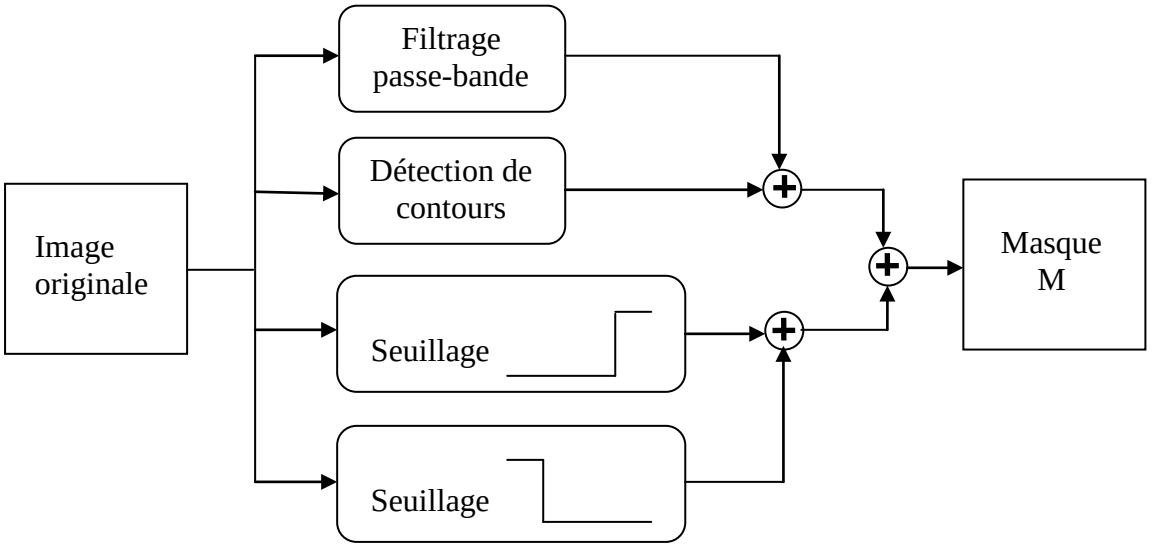


Figure III.17. Création de masque par le schéma de Bartolini

Une autre façon de prendre en compte le *HVS* est d'utiliser des seuils de perception. Ce type de seuil ne mesure pas une distorsion, mais indique la distorsion maximale autorisée sans que la modification soit visible. Au dessous de ce seuil, la modification ne pourra pas être remarquée, mais au dessus elle pourra être perçue. Ce niveau de distorsion maximal est noté *JND* (Just Noticeable Difference). Watson [98] a déterminé expérimentalement des seuils de perception du bruit pour les coefficients *DWT*, utilisés afin de calculer des matrices de quantification pour faire de la compression d'images.

Cette notion de seuil de différence juste visible a été employée par Wolfgang et al. qui ont proposés une pondération dans deux domaines transformés, l'un après transformation *DCT* sur des blocs de 8x8, l'autre après une transformation par ondelettes [99]. Dans les deux domaines, l'insertion de la signature, représentée par une séquence aléatoire de répartition gaussienne est calculée par addition :

$$Y(u,v) = \begin{cases} X(u,v) + J(u,v)W(u,v) & si\ |X(u,v)| > J(u,v) \\ X(u,v) & si\ |X(u,v)| < J(u,v) \end{cases} \qquad \text{(III.32)}$$

Ce seuil *JND* représenté par *J(u, v)* est utilisé pour déterminer les pas de quantification des coefficients *DCT* lors de la compression *JPEG*

Sadaane et al. propose une approche qui exploite une modélisation du *HVS* en canaux séparables polairement [100]. La sélection des sites propices au watermarking est effectuée sur l'image des luminances. Cette sélection exploite la décomposition en canaux perceptuels de la figure (III.16). Pour chacun des sites retenus un modèle de visibilité des erreurs permet

de déterminer la force maximale au-delà de laquelle le watermark inséré engendre des dégradations visibles. Cette force maximale est ensuite utilisée pour pondérer le watermark avant son insertion.

III.5. La manière de fusionner la marque avec l'image

Le fusionnement des données de l'image et la marque est l'un des points clé d'un système de watermarking. En effet, c'est cette stratégie de fusionnement qui fait la différence entre une approche et une autre de point de vue sécurité, robustesse, capacité et voir même visibilité. Dans la littérature des méthodes de watermarking des images plusieurs techniques de fusionnement sont utilisées. Parmi les quelles on cite les suivantes :

III.5.1 Fusionnement par modulation

En télécommunication, pour pouvoir transmettre un signal on fait recours à une porteuse qui s'en charge de porter ce signal. Ce transport se fait soit à travers son amplitude, sa fréquence ou sa phase. Donc on parle d'une modulation d'amplitude, de fréquence et de phase.

En watermarking, l'image (qui représente la porteuse) est sensée de porter la marque (le signal à transmettre). Et comme la transformée de Fourier d'une image possède une amplitude et une phase, donc la possibilité de la modulation d'amplitude ou de phase est envisageable. Si l'aspect robustesse est privilégie sur l'aspect invisibilité, la modulation de phase sera favorisée par rapport à la modulation d'amplitude. Car, en plus que les techniques de modulation de phase sont reconnues comme étant plus robustes au bruit, des études expérimentales ont montré que l'information contenue dans la phase est prépondérante sur celle contenue dans l'amplitude dans la représentation d'une image. De ce fait, l'insertion de la marque au niveau de la phase assure que la tentative de suppression de la marque entrainera inévitablement des dégradations importantes de l'image. Maintenant, si l'aspect invisibilité a plus d'importance que l'aspect robustesse, c'est le cas du watermarking fragile, l'insertion de la marque est réalisé par une modulation d'amplitude. Dans le cas d'une image couleur il est préférable de moduler la composante bleue plutôt que de moduler la composante luminance. Ce choix peut sembler, à première vue, injustifié dans la mesure où l'œil humain est particulièrement sensible aux variations de tons de bleu (le pouvoir de discrimination des couleurs du *HVS* n'est pas uniforme). L'explication est que l'œil est plus sensible à des variations de luminosité et de contraste qu'à des variations de nuances de couleur. En effet, la contribution des composantes (rouge, vert et bleu) dans la composition de la luminance est donnée par la formule suivante :

$$L = 0.299.R + 0.587.G + 0.114.B \quad \text{(III.33)}$$

On peut constater que l'apport de la composante bleu dans la composition de la luminance est le plus faible. De ce fait, la répercussion de la modulation de la composante bleue, en termes de distorsion, sera plus faible que si l'on avait modulé directement la luminance.

III.5.2 Fusionnement par quantification des coefficients *DCT*

La manipulation des coefficients *DCT* obtenus après une transformation en cosinus discrète de l'image à marquer, en vue de fusionner les données image et marque, a fait l'objet de plusieurs propositions telle que la modification de la fonction d'arrondi, la définition d'une relation de N-uplet de coefficients, superposition des coefficients de l'image et de la marque,…etc. Chacune de ces approches, dont nous nous parlerons brièvement dans les sections ci-dessous, essaye de réalise ce fusionnement de données image-marque en respectant un certain compromis invisibilité-robustesse.

III.5.2.1. Modification de la fonction d'arrondi

La fonction utilisée classiquement dans un codeur *JPEG* considère l'entier le plus proche. Inspiré de cette technique, Matsui et Tanaka [101] proposent d'introduire la marque binaire lors de l'étape de quantification des coefficients *DCT*. Leur approche considère l'entier pair (respectivement impair) le plus proche pour l'insertion d'un bit 1 de la marque (respectivement 0). L'erreur de quantification ainsi crée est donc directement corrélée avec la marque. En cas de dégradation de la qualité de l'image, l'approche offre la possibilité de réduire le pas de quantification des tables de coefficients *DCT* pour se positionner à un niveau de dégradation acceptable. Malgré que cette opération provoque une moindre résistance du watermark, mais le pas de quantification présente un paramètre de réglage du compromis robustesse / invisibilité.

III.5.2.2. Définition d'une relation de N-uplet de coefficients

Koch et Zhao [102][103] ont proposés une approche qui cherche à rétablir une notion de voisinage en utilisant une modulation différentielle des coefficients *DCT*. Contrairement à la technique proposé par Matsui et Tanaka et qui permet d'insérer un seul bit au niveau de chaque coefficient mais sans tenir compte des coefficients voisins.

III.5.2.3. Superposition des coefficients *DCT* de l'image et de la marque

Cette technique est particulièrement utilisée lorsque le document à marquer et la marque sont de même nature. Dans le contexte du watermarking des images, le watermark ou la marque est lui-même une image.

III.5.3. Fusionnement par substitution de blocs

Le fusionnement des données de l'image et de la marque par les méthodes vues dans la section précédente se base sur la perturbation de la quantification de certains coefficients *DCT*. Les effets visuels résultant de cette manipulation sont parfois difficilement maîtrisables. Une approche différente proposée par J. Puate et *al*. [104] et basée sur le codage fractal qui est lui-même 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. Pour un bloc cible donné, la recherche du bloc source associé s'effectue dans deux fenêtres de recherche centrées sur le bloc cible.

L'intérêt de cette approche est de mettre à profit certaines propriétés d'invariance propres aux fractales afin de pouvoir prévenir certaines attaques et récupérer la marque d'une manière aveugle c.-à-d. sans avoir recours à l'image originale.

III.5.4. Fusionnement par quantification vectorielle spatiale

Une méthode de watermarking fondée sur le principe de codage par quantification vectorielle a été proposée par Chen *et al.* [52]. La quantification vectorielle consiste à remplacer des blocs de l'image par d'autres appartenant à un dictionnaire prédéfini (le choix des blocs minimise les distorsions infligées à l'image). Le nombre de dictionnaires est fonction de la quantité d'informations contenues dans la marque. Selon la valeur de la marque, un dictionnaire sera choisi. Dans chaque dictionnaire, la taille et la variété des blocs détermine la distorsion produite par l'insertion de la marque.

III.5.5. Fusionnement par quantification des coefficients des ondelettes

Cette approche substitutive a été proposée par Kundur *et al.* [105]. Elle consiste à calculer la *DWT* de l'image jusqu'à un niveau l. A chaque résolution j (niveau de la décomposition en ondelettes), on choisi aléatoirement (avec une clé K) trois coefficients de détails appartenant à trois orientations fréquentielles distinctes (horizontales, verticales et diagonales). Ces coefficients sont d'abord classés selon leur valeur : $C_1 \leq C_2 \leq C_3$, puis le coefficient médian C_2 est modifié. Les modifications se font par quantification. Le segment $[C_1, C_2]$ est divisé en $2Q - 1$ segments de longueur Δ (Q est la force du watermark)

- Si $W_i = 1$, $C_2^* = C_3 - p_3\Delta : C_2$ est quantifié sur un grille passant par C_3
- Si $W_i = 0$, $C_2^* = C_1 + p_1\Delta : C_2$ est quantifié sur un grille passant par C_1

Les coefficients entiers p_1 et p_3 minimisent les distorsions.

Cette technique a pour avantage de permettre de transmettre une marque de grande taille ((N^2-1)/3 pour une image de taille N^2), sa robustesse peut donc être fortement augmentée par redondance ou emploi de code correcteurs d'erreurs.

III.6. Les méthodes utilisées pour détecter ou extraire la marque

L'extraction ou la détection de la marque est un élément distinctif pour comparer ou évaluer l'efficacité des systèmes de watermarking. Comme nous l'avons évoqué au premier chapitre (sec. I.6.3) et détaillé au deuxième chapitre (sec. II.3.2), la détection de la marque peut se faire soit en mode non-aveugle, semi-aveugle, aveugle ou asymétrique. Cela dépend essentiellement de l'application visée, du type de schéma de watermarking (additive ou substitutif), de la disponibilité de l'image et de la marque originale…etc. L'utilisation de l'image originale permet d'améliorer l'estimation de la marque insérée, mais aussi l'utilisation des techniques de prédiction permet d'optimiser sa détection. Ces techniques sont surtout utilisées dans le cas des schémas additifs. Par contre les schémas substitutifs n'ont pas besoin de l'image originale pour augmenter les performances de la détection de la marque. Ce type de schéma peut avoir recours à l'utilisation de codes correcteurs d'erreurs pour améliorer les performances de décodage du message [106]. Dans les sections qui suivent nous nous intéressons particulièrement à présenter quelques techniques d'amélioration de la détection de la marque.

III.6.1. Détection par corrélation

Les tests d'hypothèses font parti des outils usuellement utilisés dans le cadre de problèmes où une prise de décision intervient. Dans le contexte du watermarking d'image, ils trouvent particulièrement leur intérêt lorsque la marque est connue et qu'il s'agit de vérifier sa présence dans une image, le plus souvent par corrélation. Donc la corrélation est l'une des méthodes les plus couramment utilisées dans un procédé de détection en mode aveugle. Elle consiste à mesurer la similarité entre deux groupes de données. Bien sûre un taux de corrélation élevé indique une plus grande similitude. Lors de la détection, la corrélation entre l'image tatouée I_W et la marque de référence permet d'obtenir une information révélatrice de la présence de la marque. Cette corrélation est donnée par l'équation suivante :

$$Z =< W;\ I_W >= \sum_i \sum_j W_{i,j} I_{i,j} \quad \text{(III.34)}$$

Z : vecteur d'observation représentant la valeur de corrélation

Deux hypothèses sont envisageables :

1- Présence de la marque :

$$Z_1 =< W; I + W >=< W; I > \ +< W; W > \cong < W; W > \quad \text{(III.35)}$$

2- Absence de la marque :

$$Z_2 =< W; I > \ll Z_1 \quad \text{(III.36)}$$

La procédure de détection de la marque est représentée sur la figure (III.18) ci-dessous.

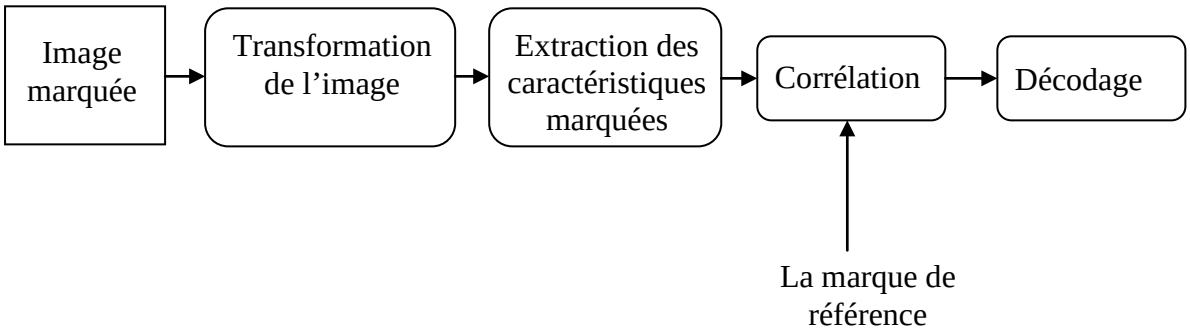


Figure III.18. Schéma de détection de la marque par corrélation

III.6.2. Estimation par filtrage Wiener

Hernandez et al. ont utilisé le filtrage de Wiener, fondé sur la minimisation par les moindres carrés obtenue à partir de l'erreur de prédiction, pour améliorer la détection de la marque [107]. La prédiction $\widehat{W}$ du watermark est exprimée comme suite :

$$\widehat{W} = \alpha . I_W + \beta . I_d \quad \text{(III.37)}$$

Où I_d représente la matrice identité et α et β sont deux inconnues à déterminer à partir de deux conditions. La première est que par définition l'espérance de $\widehat{W}$ doit être nulle ce qui implique :

$$\alpha . E[I_W] + \beta = 0 \quad \text{(III.38)}$$

La deuxième condition est que l'erreur d'estimation doit être orthogonale à I_W ce qui donne :

$$E\left[\left(\widehat{W} - W\right) I_W\right] = 0 \quad \text{(III.39)}$$

En supposant que l'image originale *I* et le watermark *W* sont indépendant (*E [I.W]*=0), la résolution de ce système donne l'expression de $\widehat{W}$:

$$\widehat{W} = \frac{E[W^2]}{E[W^2]+E[I^2]}(I_W - E[I_W]) \qquad \text{(III.40)}$$

Pratiquement, le calcul de $\widehat{W}$ s'effectue en évaluant les moyennes et les variances de façon locale, c.-à-d. dans un voisinage entourant chaque composante de l'image marquée.

III.6.3. Estimation par filtrage Passe-haut

L'estimation $\widehat{W}$ du watermark W permet d'augmenter les performances de la corrélation en calculant :

$$Z' = < W;\ \widehat{W} > = \sum_i \sum_j w_{i,j}\widehat{w}_{i,j} \qquad \text{(III.41)}$$

L'utilisation d'un filtrage passe-haut rend possible l'élimination d'une partie des composantes propres à l'image et ainsi l'augmentation de la corrélation [47]. C'est ainsi que Kutter a utilisé un filtrage par un masque *h* de taille 7x7 afin de prédire la signature [4]. La forme de *h* est donnée par :

$$h = \begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ -1 & -1 & -1 & 12 & -1 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix} \qquad \text{(III.42)}$$

III.6.4. Estimation par décision optimale

Lorsque le signal est perturbé par une séquence gaussienne blanche et additive, le critère du maximum de vraisemblance permet d'obtenir la règle de décision optimale. Donc elle consiste à trouver l'élément du message qui est le plus proche du signal reçu. Dans le contexte du watermarking et dans le cas d'une insertion binaire par étalement de spectre, la décision est prise à partir du résultat d'un seuillage sur la valeur de la corrélation. Ce qui donne :

- Si $< \widehat{W}; W >$ est positive, le bit détecté est égal à 1.
- Si $< \widehat{W}; W >$ est négative, le bit détecté est égal à 0.

III.7. La catégorie d'attaques visées

Comme nous l'avons présenté, en détail, au deuxième chapitre (sec. II.4.1), une image marquée peut subir une variété d'attaques. Ces attaques sont classées en deux catégories :

- Les attaques innocentes : qui représentent les traitements d'image usuelle telle que la compression, le filtrage, les transformations géométriques, les conversions A/N et N/A…etc.
- Les attaques malveillantes : dont l'objectif est d'entraver la bonne récupération de la marque soit par effacement ou désynchronisation ou par exploitation d'une faille propre au schéma de watermarking.

Ces attaques tiennent une place très importante dans le cahier des charges d'un processus de watermarking puisqu'elles définissent la robustesse et la sécurité de la marque. Malheureusement, ce cahier des charges n'est pas fixe ce qui rend impossible de certifier qu'un algorithme puisse faire face à toutes les attaques possibles. De ce fait, il est nécessaire de penser la conception du schéma de watermarking en termes d'applications visées : une fois ces applications définies, il devient possible d'anticiper les attaques qui seront utilisées et de les contrer. Donc chaque schéma de watermarking s'attache à une catégorie d'attaques bien spécifiques.

III.8. Etat de l'art des méthodes de watermarking d'image fixe.

III.8.1. Les méthodes spatiales.

Les méthodes spatiales consistent à insérer la marque directement dans l'image. Elles ont l'avantage d'être facilement implantables mais sont peu robustes.

L'insertion et la détection dans le domaine spatial suivent dans la majorité des algorithmes le schéma classique décrit ci-dessous :

- D'une part on génère une Séquence Binaire Pseudo Aléatoire S (une m-séquence ou une gold séquence par exemple) à l'aide d'une clé secrète, uniquement connue du propriétaire. Cette séquence est composée uniquement de +1 et de –1 et a une moyenne nulle (c'est à dire autant de –1 que de +1).
- Le message à insérer composé de +1 et –1 (par exemple M = {+1, -1, -1, +1}) est ensuite modulé par la Séquence S puis transformé en un signal à deux dimensions : pour cela on remplit ligne par ligne ce signal 2D. Pour une image 12*12, il faudra donc une séquence S de 144 échantillons. Cette marque est ensuite ajoutée directement à l'image comme le décrit la figure (III.19).

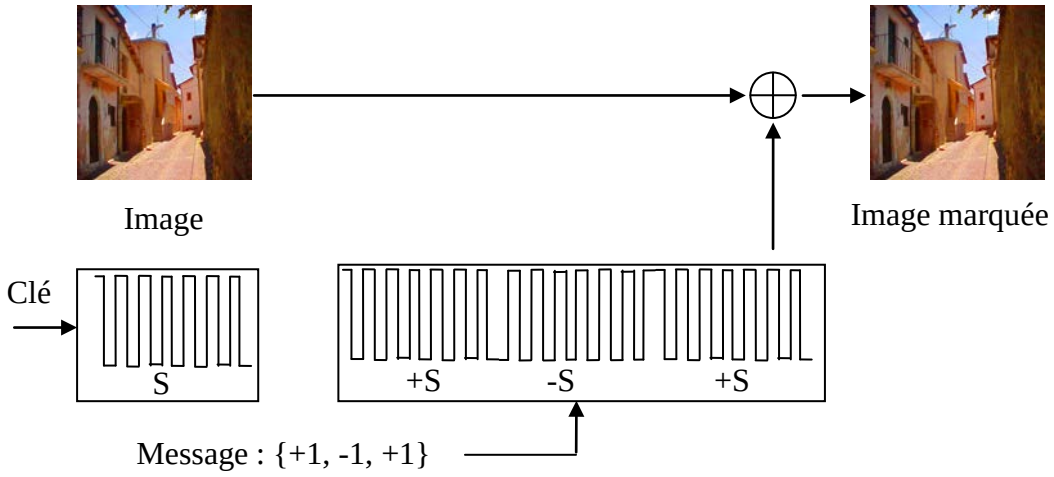


Figure III.19 Processus d'insertion pour la méthode spatiale

- La détection se fait le plus souvent par corrélation : en effet la marque de moyenne nulle, on peut considérer que l'inter-corrélation de la marque avec l'image est négligeable par rapport à l'auto-corrélation de marque. Pour détecter la signature, il suffit donc de calculer l'inter-corrélation de la marque avec l'image marquée. Ce calcul se fait simplement en multipliant pixel par pixel les deux images et en faisant ensuite la somme des produits. Le processus est répété pour chaque bit inséré pour obtenir à la fin le message détecté.

Appelons I l'image initiale, W la marque, W_d une marque différente et I_W l'image marquée et supposons que toutes ces images sont de taille 100*100. La détection suit alors le schéma ci-dessous :

- On forme l'image marquée $I_W = I + W$
- On calcule l'inter-corrélation $< I_W, W > = < I+W, W > = < I, W > + < W, W >$

$= \varepsilon + 10\,000$ (avec $\varepsilon << 10\,000$)

- Pour une marque différente on aurait $< I_W, W_d > = < I, W > + < W_d, W >$

$= \varepsilon + \varepsilon << < I_W, W >$

On prend donc une décision sur la présence ou non d'une marque si l'inter-corrélation est supérieure à un seuil préalablement fixé, comme le résume le schéma de la figure (III.20).

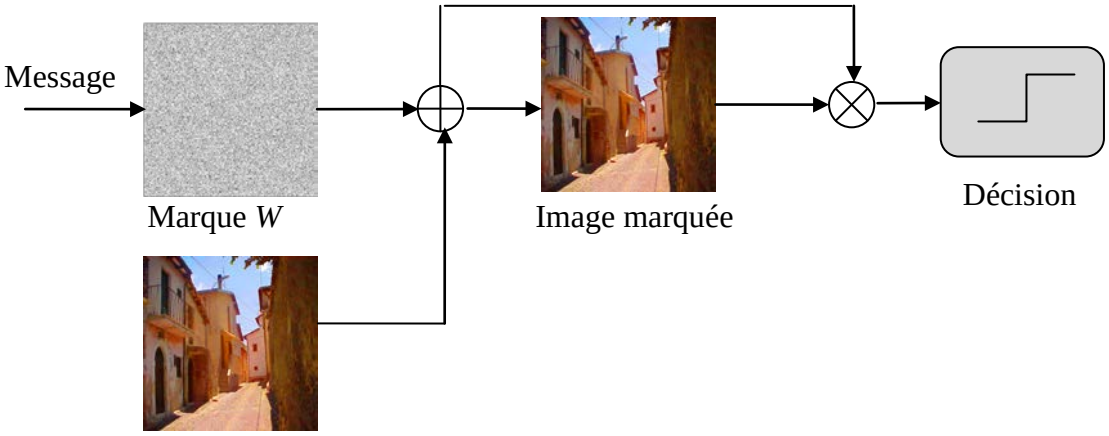


Figure III.20. Détection de la marque par corrélation

Dans cette section nous présenterons un résumé non exhaustif des divers travaux de watermarking d'images dans le domaine spatial.

III.8.1.1 Méthode du bit le moins significatif (*LSB*)

Les premières techniques de watermarking (1993) remplaçaient directement les bits de poids faibles *LSB* (*Least Significant Bit*) de l'image par le message. Bien que cette méthode permette d'insérer des marques de grande taille, mais cette capacité se paye par une très faible robustesse. En effet, de simples attaques telles que la compression *JPEG* ou le bruit peuvent modifier les *LSB* et donc rendre l'extraction de la marque impossible. Donc son champ d'application se limite à la stéganographie ou au watermarking fragile.

Parmi les travaux utilisant cette technique on cite à titre d'exemple ceux de P.G. Van Schyndel *et al.* [108] qui ont proposé deux méthodes. Les deux méthodes utilisent des m-séquences pour obtenir un pseudo-code (PN) (le watermark). La première est basée sur la manipulation du plan binaire du *LSB*, en insérant la séquence m sur le bit de poids faible des données de l'image. Ceci offre un décodage simple et rapide. La seconde procédure utilise l'addition linéaire du watermark aux données de l'image et elle est plus difficile à décoder, ce qui offre une sécurité inhérente. Le processus de décodage fait appel à la fonction d'auto-corrélation unique et optimale de m-séquences. Le principal problème rencontré avec l'addition du watermark est le maintient du rang dynamique de l'image originale ainsi que la sortie d'auto-corrélation. Le watermark est robuste de la moyenne, et potentiellement compatible avec la compression *JPEG*.

R. B. Wolfgang et E. J. Delp [109], présente une autre approche dont le watermark est une extension à deux dimensions de celui de [108]. Leur premier watermark est robuste aux

opérations de filtrage (moyen et médian). Le second est robuste à la compression *JPEG*. Ce type de watermark à deux dimensions permet de localiser exactement l'endroit où l'image a subie des changements.

III.8.1.2 Méthode du Patchwork

Cette méthode, très classique, est introduite par Bender et al [110] ensuite étudié en détail par Pitas et Kaskalis [111] [112]. Elle opère directement dans le domaine spatial (au niveau des pixels) et elle part d'une approche statique de l'image. Elle se base sur le fait suivant : si l'on prend un grand nombre de fois deux points au hasard et qu'on soustrait leur luminance l'une à l'autre, la probabilité que cette différence soit nul est très importante. Donc l'insertion de la marque suit les étapes suivantes :

- Une clé *K* est utilisée pour sélectionner pseudo-aléatoirement deux ensembles, disjointes et de même cardinal, de pixels *A* et *B* (d'où l'appellation patchwork).
- Les valeurs des luminances des pixels appartenant à *A* et *B* sont alors modifiées selon les formules suivantes :

$$a_i^* = a_i + 1 \qquad \text{(III.43)}$$

$$b_i^* = b_i - 1 \qquad \text{(III.44)}$$

A la détection, la somme *S* des différences entre les valeurs de luminances de ces deux groupes de pixels, est calculée comme suite :

$$S^* = \sum_{i=1}^{N}(a_i^* - b_i^*) \qquad \text{(III.45)}$$

Si l'on connait la clé définissant les deux ensembles *A* et *B* et en supposant que l'image satisfait certaines propriétés statistiques, la valeur attendue de la somme est *2N*.

Si l'on ne connait pas cette clé, on ne peut pas retrouver les deux ensembles, on peut que générer deux ensembles différents. Si ces ensembles sont générés pseudo-aléatoirement (avec une autre clé *K'*), l'espérance de la somme est alors nulle.

Ce principe de détection est fondé sur le résultat statistique suivant : si l'on choisi pseudo-aléatoirement deux ensembles de pixels de même cardinal, l'espérance mathématique de la somme de leur différence est nulle :

$$E(S) = \sum_{i=1}^{N}[E(a_i) - E(b_i)] = 0 \qquad \text{(III.46)}$$

Les deux sous-ensembles sélectionnés par les clés doivent être grandes et bien répartis dans l'image pour que cette propriété soit vérifiée.

On peut remarquer que l'insertion de la marque peut se résumer à l'addition de l'image avec une matrice de watermark *W*, de même taille que l'image et contenant la valeur 1 pour les pixels de l'ensemble *A*, -1 pour ceux de *B*, 0 sinon.

Cette méthode de base, appartenant à la famille des méthodes de watermarking à réponse binaire, n'est bien évidemment pas très robuste ; cependant, différentes extensions de cette approche ont vu le jour [113]. Elles permettent par exemple d'accroitre la résistance du système à des opérations de filtrage sur l'image en considérant non plus des couples de pixels mais des couples de blocs. L'emploi de plusieurs séquences aléatoires orthogonales dans le but de dissimuler plusieurs bits (1 par séquence aléatoire) a également été proposé [114].

III.8.1.2 Méthode de l'étalement de spectre

Une des techniques utilisées largement en télécommunication est l'étalement de spectre. Son principe consiste à étaler le spectre d'un message sur toute la bande passante du canal. Le message ainsi étalé sera donc présent sur toutes les fréquences et sera résistant aux altérations de cette bande. De plus, le message ressemble à un bruit blanc et donc très difficile à intercepter par un utilisateur non autorisé. Par analogie à la définition du watermarking, qui consiste à insérer (transmettre) une marque (message) dans une image (canal de transmission) exposée à des attaques (bruit), on constate que l'étalement de spectre peut jouer un rôle important dans les applications du watermarking.

Effectivement, Tirkel *et al*. [24][108] ont été les premiers auteurs à utiliser cette technique d'étalement de spectre pour insérer une marque dans une image. ils proposent d'ajouter des M-séquences sur les bits de poids faible de l'image. La détection de la marque s'obtient par le calcule de l'inter-corrélation entre la M-séquence et l'image marquée. L'apparition des pics de corrélation témoignent de la présence de la marque.

Cette technique a également été utilisée par Hartung et Girot [115] pour développer un schéma similaire permettant d'insérer un message de plusieurs bits au sein d'une image ou une séquence d'image. Chaque bit à insérer, associé à (+1) ou à (-1), est étalé sur une fenêtre. Le message étalé est modulé par une séquence pseudo aléatoire *PN* pour obtenir le watermark *W* qui est une matrice de même cardinal que l'image. Le watermark *W* est ensuite pondéré par un masque qui tient compte de l'activité de l'image. La séquence résultante est ajoutée à l'image à marquer, selon l'équation (III.47), comme il illustré sur la figure (III.21).

$$I_W = I + \alpha . W \qquad \text{(III.47)}$$

Si on l'image originale est accessible, la détection extrait W puis le message m, PN étant connu. Si on dispose uniquement de la séquence pseudo aléatoire, la détection

s'effectuera par corrélation entre l'image marquée et la séquence pseudo aléatoire. Le signe de corrélation donne la valeur du bit inséré. Les performances de la corrélation peuvent être améliorées en utilisant un filtre passe-haut pour l'estimation de la marque.

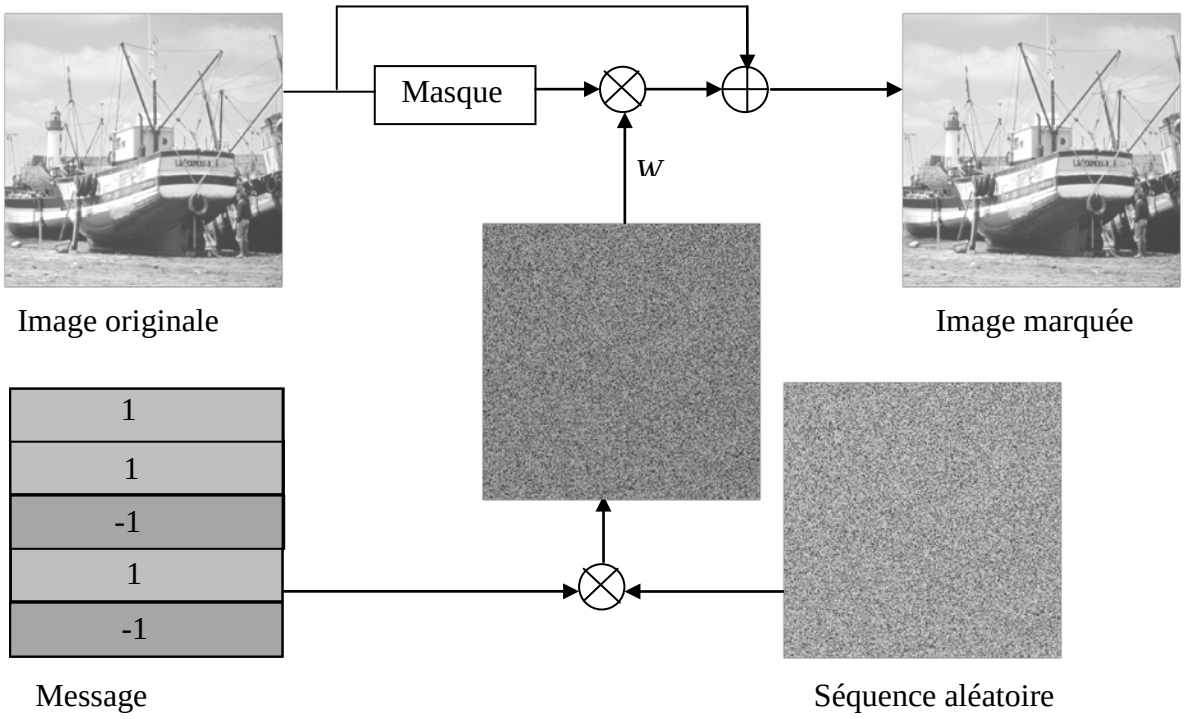


Figure III.21. Insertion de la marque par étalement de spectre selon l'approche de Hartung et Girot

La particularité de ces méthodes réside dans l'emploi du pseudo-bruit permettant d'étaler le spectre du message. Même si toutes les séquences aléatoires peuvent à priori convenir, certaines (m-séquences, code de Gold) possèdent des propriétés d'auto-corrélation permettant une meilleur réception du message et une minimisation des interférences. La robustesse de ce type de méthode varie selon l'attaque envisagée. En général, ces méthodes donnent d'assez bons résultats sauf pour les attaques de désynchronisation.

III.8.1.3 Méthode de quantification

Le principe du watermarking par quantification consiste à substituer les données de l'image par des états de quantification. L'extraction de la marque se fait en prenant l'état le plus proche des données reçues. On distingue la quantification scalaire (figure III.22) et vectorielle (figure III.23). Parmi les méthodes quantificatives les plus connues on cite : la

modulation D'indices de quantification (*QIM*) de Chen et Wornell [116] et le Schéma de Costa Scalaire (*SCS*) d'Eggers et al. [117].

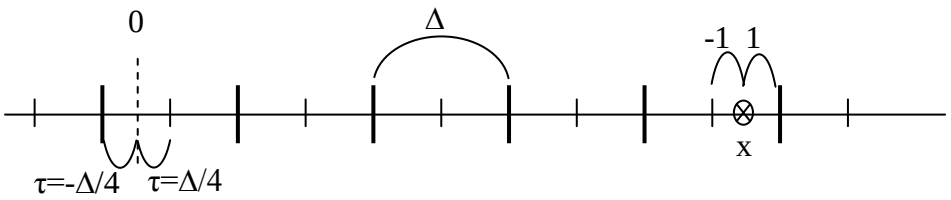


Figure III.22. Quantification Scalaire

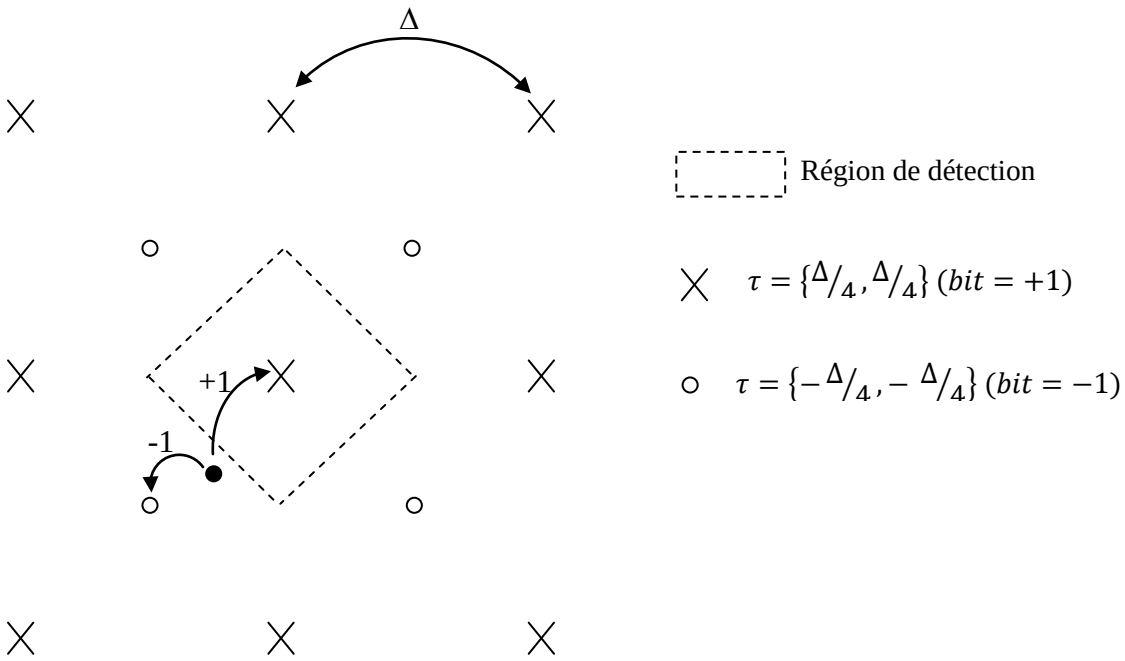


Figure III.23. Quantification vectorielle avec pas uniforme

- **Modulation d'indices de quantification (*QIM*)**

Le watermarking quantificatif a été introduit par Chen et Wornell sous le nom de *QIM* (*Quantization Index Modulation*). Cette appellation généralise explicitement la technique historique du *LSB*, qui peut être considérée comme une substitution d'un pixel d'une image par le résultat de deux quantificateurs grossiers : celui pour le quel le plan *LSB* vaut toujours 0, et celui pour lequel il vaut toujours 1. Dans le *QIM*, on étend ce principe à d'autre quantités scalaires *x*, d'autres quantificateurs *Q* et à la quantification vectorielle. Le choix des quantificateurs utilisés est déterminé, parmi un ensemble donné, par le message à insérer,

d'où l'appellation « Modulation d'Indices de Quantification ». Le pas de quantification Δ résulte d'un compromis entre les distorsions provoquées par l'insertion, la performance de détection et le nombre de mots contenus dans le dictionnaire. Les méthodes de la classe *QIM* sont optimales en performance au décodage et de capacité d'insertion dans certain scénarios d'attaque.

- **Schéma de Costa Scalaire (*SCS*)**

Eggers et al. ont exploité le lien entre *QIM* et le schéma de Costa pour proposer une implantation sous-optimale explicite du schéma de Costa. Elle est connue sous le nom de Schéma de Costa Scalaire *SCS* (*Scalar Costa Scheme*). Ce schéma suppose que les attaques sont exclusivement basées sur l'ajout de bruit gaussien.

En plus des méthodes spatiales citées ci-dessus, il existe encore d'autres telles que : la méthode de substitution d'histogramme proposé par Coltuc *et al*. [118], la substitution des caractéristiques géométriques de Maes *et al*. [119], ….etc.

III.8.2. Les méthodes fréquentielles

Le principe des méthodes fréquentielles consiste à insérer la marque non pas directement dans l'image mais dans un domaine transformé. Ce dernier est obtenu par une transformation inversible qui peut être une *DCT*, *DFT*, *DWT*, …etc. Pour retrouver l'image marquée, on effectue la transformée inverse. Ces méthodes résistent mieux aux attaques géométriques. Les figures (III.1, 2, 3, 4) décrivent les procédures d'insertion et de détection de la marque.

III.8.2.1. insertion dans le domaine *DCT*

L'algorithme développé par Zhao et Koch en 1995 [120] est l'un des premiers algorithmes de watermarking d'image publié dans la littérature scientifique. Il permet d'incruster la marque dans les coefficients *DCT* des blocs de l'image. En effet, l'image est divisée en blocs de 8x8, ensuite ces blocs subissent une transformation *DCT*. Les coefficients des moyennes fréquences sont sélectionnés et numéroté comme il est indiqué sur la figure (III.24)

Partant de ces 8 coefficients moyens fréquences, 18 sous-ensembles contenant chacun 3 coefficients différents sont formés comme l'illustre le tableau (III.1). L'insertion de la marque correspondant à laisser les amplitudes des coefficients dans l'un de ces 18 sous-ensembles ayant un ordre prédéfini. Le sous-ensemble exact qui transportera effectivement la marque est déterminé selon une clé secrète *K*. Un exemple possible de la correspondance

entre les bits d'information et l'ordre des coefficients est donné dans le tableau (III.2) (L = la plus faible amplitude, H=la plus haute amplitude, M=moyenne amplitude). Lorsque en essaye d'insérer un bit, trois situations sont possibles. Si les coefficients sélectionnés présentent déjà l'ordre souhaité, les coefficients restent inchangés. Si les coefficients ne sont pas dans l'ordre désiré, ils sont modifiés de manière que cet ordre soit obtenu. Si la modification nécessaire pour atteindre l'ordre désiré est trop grande, les coefficients peuvent être modifiés de sorte que l'une des combinaisons non valides soit atteinte. Dans ce dernier cas, aucun bit d'information n'est caché dans le bloc *DCT*. Afin d'augmenter la robustesse du watermark, la possibilité d'ajouter des bits de redondance à la chaîne d'information est envisagée. Le décodage de la marque est simple, puisqu'il suffit de récupérer les séquences de coefficients marqués selon la clé *K* et comparer l'ordre de coefficients *DCT*.

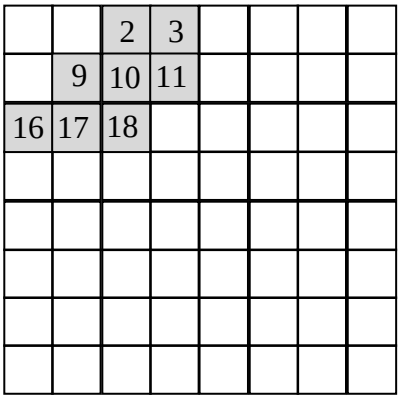


Figure III.24. Numérotation de bloc DCT dans l'algorithme de Zhao et Koch

Set N°	P1	P2	P3
1	2	9	10
2	9	2	10
3	3	10	1
…..	…	…	…
18	17	10	18

Tableau.III.1.Sous-ensembles des coefficients DCT pour l'insertion de la marque

P1	P2	P3	Bit	P1	P2	P3	Bit
H	M	L	1	L	L	H	0
M	H	L	1	H	L	M	Invalide
H	H	L	1	L	H	M	Invalide
M	L	H	0	M	M	M	Invalide
L	M	H	0				

Tableau III.2. Correspondance entre les bits d'information et l'ordre des coefficients

Cox et al. [5][121] proposent une méthode qui utilise la transformée en cosinus discrète (*DCT*) pour insérer la marque dans l'image. Ils appliquent la *DCT* à toute l'image et insèrent la signature dans les basses fréquences, c'est à dire dans les composantes les plus

significatives. Ils modifient les *n* coefficients *DCT* de plus grande amplitude, à l'exception de la composante continue, suivant l'une des formules suivantes :

$$V_i' = V_i + \alpha . W_i \quad \text{(III.48)}$$

$$V_i' = V_i(1 + \alpha . W_i) \quad \text{(III.49)}$$

$$V_i' = V_i e^{\alpha . W_i} \quad \text{(III.50)}$$

avec :

V_i' : Coefficient DCT de l'image marquée

V_i: Coefficient DCT de l'image originale

α : Coefficient d'invisibilité

W_i : Coefficient réel issu d'une distribution gaussienne centrée normée.

L'extraction se fait en inversant le processus d'insertion et en utilisant l'image originale pour retrouver la marque. La suite $W_i{}'$ extraite est comparée à la suite W_i par un calcul de similitude donné par :

$$s = \frac{W'W}{\sqrt{W'W}} \quad \text{(III.51)}$$

Cette méthode est très robuste et donne de bonne résultats face aux attaques de type changement d'échelle, compression *JPEG*, conversion *A/N* et *N/A*, et attaque par collision. Le principal désavantage de cette méthode est que l'image originale doit être connue pour permettre l'extraction de la marque.

La solution à ce problème a été portée par Piva et al. [122] qui utilisent le même principe d'insertion, mais la détection de la marque s'effectue sans l'image originale. En effet, la marque *W* est ajoutée aux composantes *DCT* choisis suivant la formule :

$$V_i' = V_i + \alpha . |V_i| . W_i \quad \text{(III.52)}$$

La détection s'effectue en évaluant la corrélation *Z* des coefficients *DCT* marqués et de la marque :

$$Z = \frac{v'W}{M} \quad \text{(III.53)}$$

Où *M* représente le nombre de coefficients marqués.

Bors et Pitas utilisent la quantification scalaire et vectorielle des coefficients *DCT* pour l'insertion de la marque [123]. Cette insertion est réalisée en contraignant les valeurs des coefficients *DCT* se trouvant dans la gamme de moyenne fréquence des blocs. La détection de la marque se fait en étudiant la répartition des blocs sélectionnés satisfaisant la contrainte utilisée lors de l'insertion.

III.8.2.2. insertion dans le domaine *DWT*

Kundur et Hatzinakos [105] proposent une méthode de watermarking d'image utilisant le domaine multi-résolution obtenu par la *DWT*. La marque, qui est une matrice binaire, est décomposée par la *DWT* en quatre sous-marques (niveau 1). Quand à l'image à marquée, elle est décomposée en ondelettes jusqu'à un niveau L (en pratique L=4). Les coefficients de détails de tous les niveaux sont alors modifiés par quantification. Le choix de ces coefficients est déterminé de façon à ce que les données insérées soient étalées spatialement et sur toutes les résolutions. La quantification de ces coefficients suivant les données à insérer s'effectue en découpant l'espace des réels suivant un pas de quantification. A chaque pas est associée, alternativement la valeur 0 ou 1. Ainsi, si au coefficient d'ondelettes correspond la valeur binaire à insérer, le coefficient n'est pas modifié. Par contre, si les valeurs ne correspondent pas, le coefficient est modifié. L'image marquée est alors reconstruite par transformation inverse. La détection de la marque se fait d'une manière non aveugle (watermarking informé). En effet, l'image originale est utilisée pour extraire les valeurs de la marque à chaque niveau. La marque extraite finale étant la moyenne des valeurs obtenues. Cette méthode est très robuste à la compression et à l'ajout de bruit blanc mais reste sensible au filtrage.

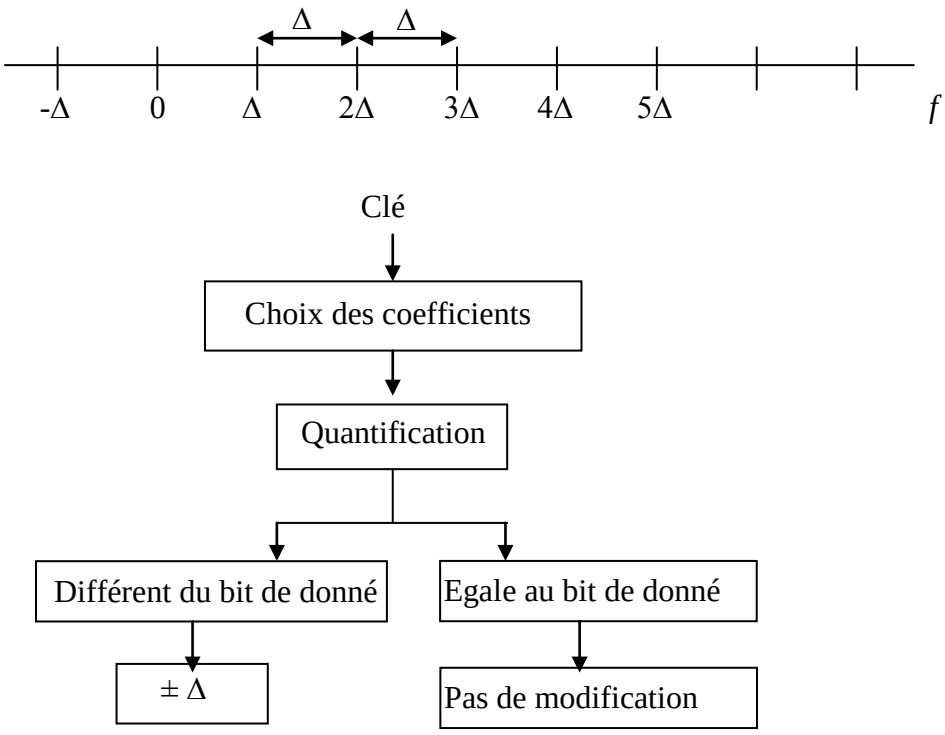


Figure III.25. Mécanisme d'insertion de la méthode de Kundur

Barni et al. [124] proposent un schéma de tatouage fondé sur le même principe, mais à détection semi-privée. Le watermark sous forme d'un bruit blanc est ajouté, d'une manière adaptative, dans chacune des trois sous bandes de détails (LH_0, HL_0, HH_0) du niveau 1 de la *DWT* comme il est indiqué sur la figure (III.26). Les coefficients des trois sous-bandes sont modifiés selon les équations suivantes :

$$I_w^{LH}[i,j] = I_0^{LH}[i,j] + \alpha.\lambda^{LH}[i,j].W[iN+j] \quad \text{(III.54)}$$

$$I_w^{HL}[i,j] = I_0^{HL}[i,j] + \alpha.\lambda^{HL}[i,j].W[MN+iN+j] \quad \text{(III.55)}$$

$$I_w^{HH}[i,j] = I_0^{HH}[i,j] + \alpha.\lambda^{HH}[i,j].W[2MN+iN+j] \quad \text{(III.56)}$$

Où α est un paramètre global désignant la force de la marque, λ est un facteur de pondération local qui prend en compte les caractéristiques du système visuel humain (*HVS*), et *W* est une séquence binaire pseudo-aléatoire. La détection de la marque se fait par le calcul de la corrélation entre les coefficients marqués de la *DWT* et la séquence du watermark *W*. Les auteurs proposent aussi une méthode pour choisir le seuil qui minimise la probabilité de fausse alarme.

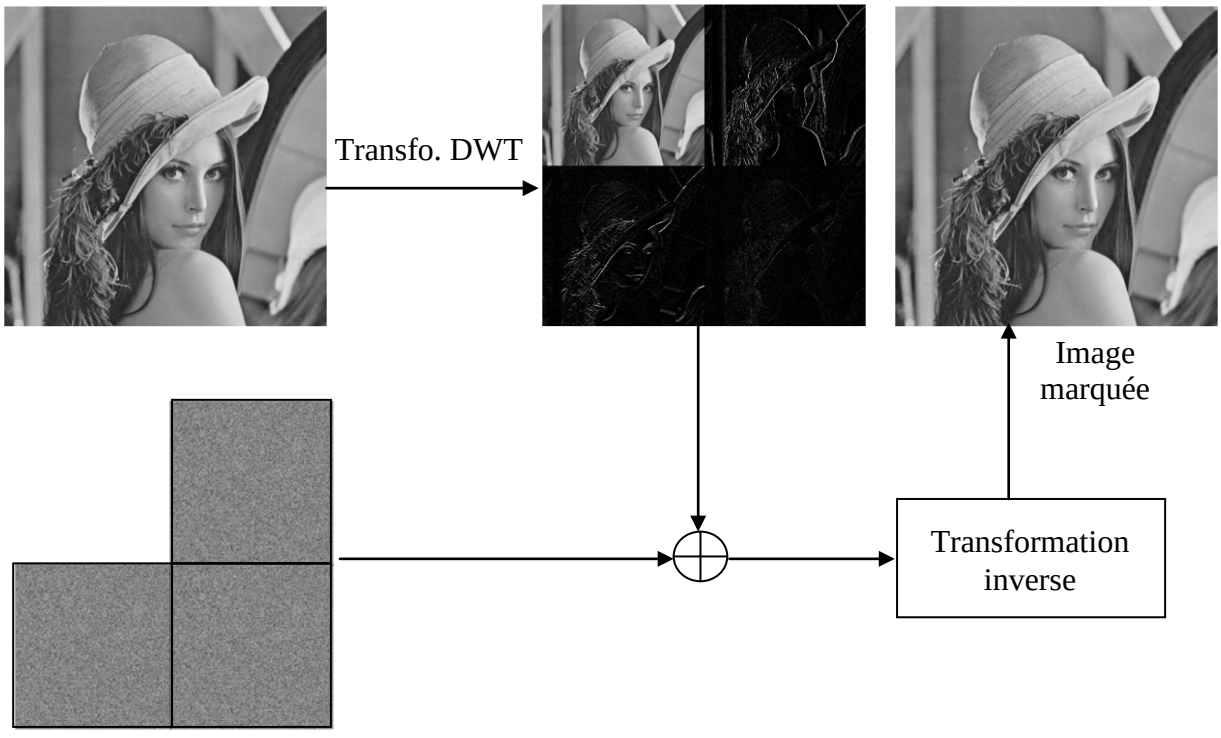


Figure III.26. Insertion de la marque selon le schéma de Barni

Des techniques similaires ont été proposées par d'autres auteurs comme par exemple H. Inoue *et al.* [125], et H. Wang *et al.* [126]. Un résumé des différents algorithmes de watermarking, utilisant le domaine transformé engendré par la *DWT*, est donné par P. Meerwald et A. Uhl dans [127].

III.8.2.3. insertion dans le domaine *DFT*

Certaines transformations ne sont intrinsèquement pas affectées par les transformations géométriques spécifiques. Par exemple, le remplacement de la transformation *DCT* par une transformation invariante comme le logo- polaire (*LPM*), qui est aussi appelé la transformée de Fourier - Mellin, tel que décrit par O Ruanaidh et Pun [69] et détaillée dans la section (III.3.2.3), présente certains avantages théoriques. Après l'application de la *TFD*, un passage du domaine cartésien au domaine log-polaire est effectué. Ce passage ramène les opérations de rotation et de changement d'échelle à une translation (équations III.19 et III.20). Le schéma d'intégration est illustré à la figure (III.11). En raison de problèmes pratiques, les auteurs suggèrent l'insertion du watermark dans le domaine invariant *DFT* et en ajoutant un deuxième watermark appelé (*Template).* Une autre approche qui utilise les propriétés du domaine invariant *LPM* a été proposée par Lin et al. [128], [129].

III.9. Conclusion

Nous avons présenté dans ce chapitre et en premier lieu les différents paramètres distinctifs des schémas de watermarking d'images. En effet, ces schémas peuvent être classés selon le type d'insertion de la marque où on distingue les schémas additifs et les schémas substitutifs plus performants. La stratégie d'insertion de la marque, la manière de fusionner les données de cette dernière avec les données de l'image à marquée, les méthodes utilisées pour améliorer la détection et l'extraction de la marque, et la catégorie d'attaques visées sont aussi des paramètres de classification des méthodes de watermarking. Un autre paramètre clé est le choix de l'espace d'insertion de la marque. En effet, chaque espace apporte diverses possibilités en termes de performance et de robustesse. On distingue principalement deux domaines : spatial opérant directement sur les pixels de l'image et transformé obtenu par une transformation inversible telle que *DCT, DWT, DFT*…etc. Donc, ce choix de l'espace de travail nous a amené à présenter un état de l'art des méthodes de watermarking divisées en méthodes spatiales et méthodes transformées (fréquentielles).

Introduction

Dans ce chapitre, organisé en quatre parties, nous allons présenter nos différents travaux et contributions dans le domaine de watermarking d'images fixes.

En premier lieu une méthode de watermarking, utilisant la variance locale des blocs, est présentée [6]. Une amélioration de cette approche constitue l'objet de la deuxième partie de ce chapitre. Cette amélioration est réalisée en développant une méthode de watermarking hybride basée sur la combinaison des deux transformées *DCT* et *DWT* [7]. Une autre approche, visant en particulier la robustesse vis-à vis les transformations géométriques élémentaires à savoir la rotation, la translation et le changement d'échelle, a été présentée dans la troisième partie [8]. La dernière partie de ce chapitre est consacrée à la présentation d'une autre approche traitant en particulier l'aspect sécuritaire des méthodes de watermarking [9][10]. Pour répondre à cette exigence on a fait recours à un nouveau type de transformation loin des transformées habituelles. En fait, Il s'agit d'une nouvelle classe de transformée appelée « *ROPT* » (*Reciprocal-Orthogonal Parametric Transforms*) [11].

IV.1. TATOUAGE D'IMAGE FIXE EN UTILISANT LA VARIANCE LOCALE DES BLOCS

IV.1.1. Description de la méthode développée

La méthode développée appartient à la catégorie des schémas substitutifs avec contraintes, c.-à-d. le tatouage ou le watermarking de l'image se fait en imposant des contraintes aux données marquées. Elle opère dans un domaine transformée obtenu par l'application de la transformée *DCT*. Elle se base d'une part sur l'étude de la variance locale de la luminance des blocs *DCT* pour sélectionner les blocs à marquer. D'autre part, elle se base sur le développement d'une stratégie de marquage assurant un compromis entre l'invisibilité et la robustesse de la marque. Cette dernière est une séquence binaire insérée dans l'image d'une façon redondante. Elle est récupérée sans faire recours à l'image originale, ce qui qualifie le tatouage d'être non informé (*Blind watermarking*). Le processus de tatouage se compose de deux phases : la phase d'insertion de la marque et celle de sa détection.

IV.1.1.1. Insertion de la marque

La phase d'insertion de la marque comporte plusieurs étapes comme il est indiqué sur la figure (IV.1). En premier lieu on sépare les couleurs de base (R, G, B) de l'image à marquer. Ensuite, les paramètres luminance et chrominance sont calculés comme suite :

$$Y = 0.299.R + 0.387.G + 0.114.B \quad \text{(IV.1)}$$

$$Cr = 0.5.R - 0.4187.G - 0.0813.B + 128 \quad \text{(IV.2)}$$

$$Cb = -0.1687.R - 0.3313.G + 0.5.B + 128 \quad \text{(IV.3)}$$

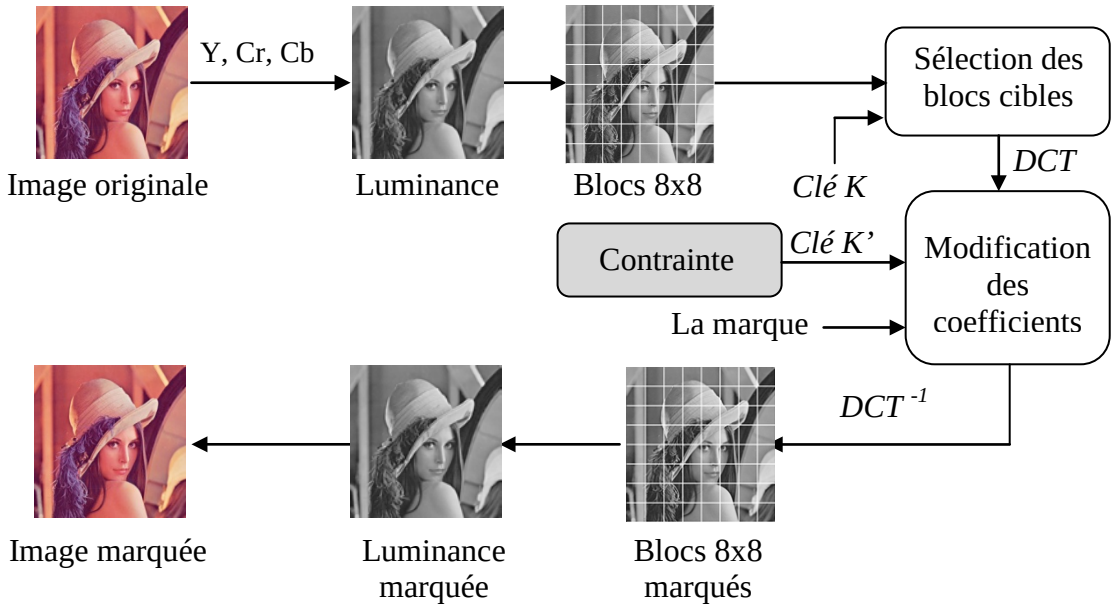


Figure IV.1. Schéma d'insertion de la marque

Après avoir divisé l'image luminance en blocs de 8x8, un calcul de la variance locale de la luminance de chaque bloc est effectué. Ceci permettra de sélectionner les blocs aptes à

abriter la marque. Après une transformation *DCT*, un certain nombre de coefficients des blocs sélectionnés sont modifiés selon une stratégie qui représente la clé d'insertion de la marque.

- ***Sélection des blocs à marquer***

Comme nous l'avons mentionné dans la section (III.3.3) du chapitre (III), le système visuel humain (*HVS*) est sensible aux contrastes moyens, et peu stimulé par les contrastes très forts ou très faibles. Par conséquent, les perturbations dans une image sont invisibles dans les régions fortement éclairées, très sombres ou texturées. En se basant sur cette constatation et pour assurer que les modifications portées aux coefficients *DCT* ne soient pas perceptibles, il faut que les blocs aux quels appartiennent soient situés dans l'une des trois régions citées précédemment. Donc chaque bloc sera caractérisé par un paramètre appelé variance locale de la luminance, elle est calculée par la formule (IV-4) suivante:

$$\sigma_B^{\,2} = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[I(i,j)-\mu_B]^2 \qquad \text{(IV.4)}$$

Avec: *B* est un bloc de 8x8 pixels, N=8 et μ_B est la moyenne du même bloc calculée selon la formule (IV.5) :

$$\mu_B = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}I(i,j) \qquad \text{(IV.5)}$$

En effet, un seuillage de ce paramètre de variance locale permet de sélectionner les blocs concernés par le marquage.

- ***Modification des coefficients DCT***

La transformée *DCT* d'un bloc de 8x8 pixels est un bloc de 8x8 coefficients réparties sur trois zones de fréquences comme il est indiqué sur la figure (IV.2) : basses, moyennes et hautes fréquences. Si on se propose d'insérer la marque dans les coefficients de la zone des hautes fréquences, on risquera la perdre à cause par exemple d'une compression *JPEG* ou un bruitage ou encore un filtrage passe-bas. Si la marque est insérée dans la région des basses fréquences, la qualité de l'image résultante sera dégradée. Donc pour faire un compromis entre l'invisibilité de la marque et sa robustesse on a envisagé de l'insérer dans la zone des moyennes fréquences. Parmi les cinq coefficients concernés par le test comme il est indiqué sur la figure (IV.3), on cherche les deux coefficients dont la valeur absolue de leur différence est minimale, soit coef1 et coef2. Ensuite, si le bit de la marque est un (1) les cinq coefficients seront augmentés de la même valeur et qui est égale à la valeur moyenne de coef1 et coef2. Si

le bit est un zéro, les coefficients seront diminués de la même valeur. Cette manière de marquage permet d'assurer que les deux coefficients coef1 et coef2 seront toujours les seuls à vérifier la condition de la valeur absolue de leur différence minimale.

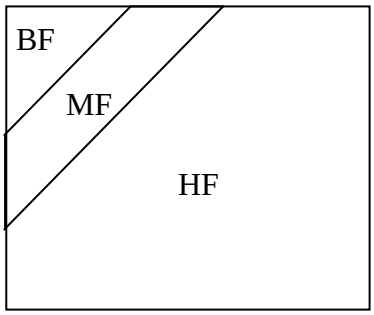


Figure IV.2. Répartition des fréquences dans un bloc DCT

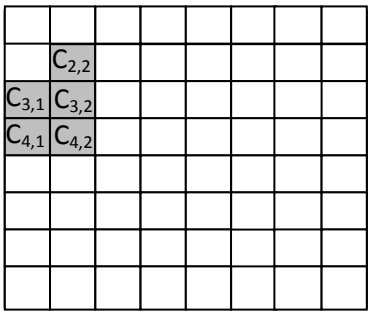


Figure IV.3. Emplacement des coefficients supportant la marque

- ***Algorithme d'insertion de la marque***

1. soit une séquence de n bits (b_1, b_2, ……., b_n) qui constitue la marque à insérer,
2. séparer les trois couleurs de base *R, G, B* de l'image,
3. calculer les paramètres luminance Y et chrominance *Cb, Cr*,
4. diviser la luminance en blocs de 8x8,
5. sélectionner, selon une clé *K* (seuillage de la variance locale), les blocs concernés par le marquage,
6. calculer la DCT de chaque bloc sélectionné,
7. calculer la différence absolue, deux à deux, entre les coefficients $C_{2,2}$, $C_{3,1}$, $C_{3,2}$, $C_{4,1}$, $C_{4,2}$ du bloc *DCT* sélectionné. Les coefficients dont la différence est minimale sont notés respectivement coef1 et coef2,
8. la modification des deux coefficients se fait selon l'état du bit b_i de la marque

- Si b_i=1, $\begin{cases} C_{2,2}^m = C_{2,2} + \frac{coef1+coef2}{2} \\ C_{3,1}^m = C_{3,1} + \frac{coef1+coef2}{2} \\ C_{3,2}^m = C_{3,2} + \frac{coef1+coef2}{2} \\ C_{4,1}^m = C_{4,1} + \frac{coef1+coef2}{2} \\ C_{4,2}^m = C_{4,2} + \frac{coef1+coef2}{2} \end{cases}$

- Si b_i=0, $\begin{cases} C^m_{2,2} = C_{2,2} - \frac{coef1+coef2}{2} \\ C^m_{3,1} = C_{3,1} - \frac{coef1+coef2}{2} \\ C^m_{3,2} = C_{3,2} - \frac{coef1+coef2}{2} \\ C^m_{4,1} = C_{4,1} - \frac{coef1+coef2}{2} \\ C^m_{4,2} = C_{4,2} - \frac{coef1+coef2}{2} \end{cases}$

9. une fois tous les blocs concernés par le marquage sont marqués, on calculer la DCT inverse de chaque bloc,
10. reconstitution de la matrice luminance à partir des blocs 8x8,
11. reconstitution des couleurs de base RGB, à partir des paramètres luminances marqués et chrominances conservés,
12. reconstitution de l'image marquée.

Remarque: La marque est insérée plusieurs fois (redondance de la marque) pour augmenter la possibilité de sa détection.

IV.1.1.2. Extraction de la marque

L'extraction de la marque se fait d'une manière aveugle, c'est-à-dire sans utilisé l'image originale. Donc pour accéder aux endroits d'extraction de la marque on suit les étapes illustrées sur la figue (IV.4).

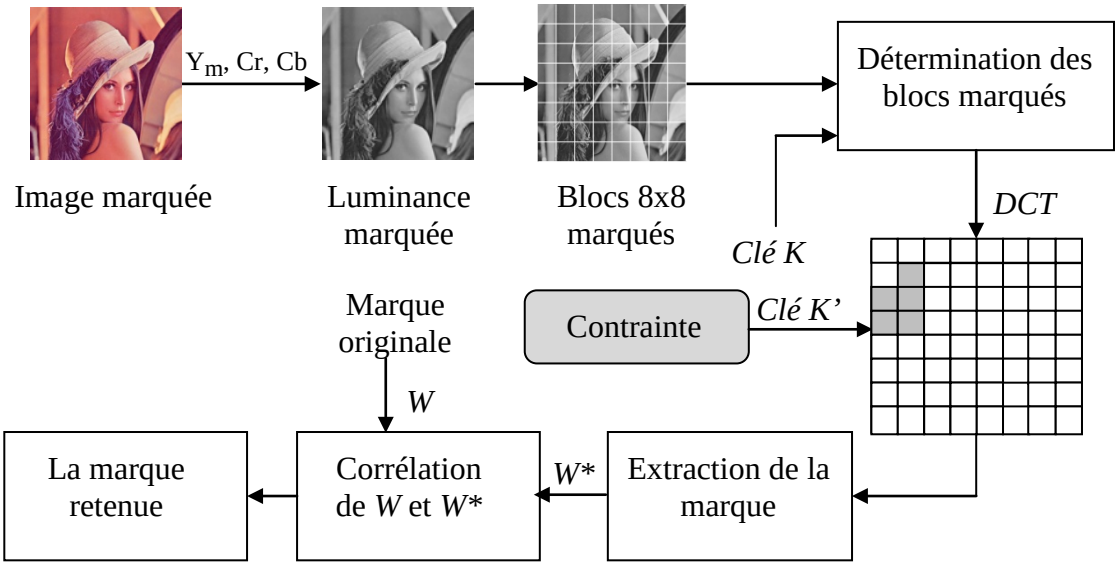


Figure IV.4. Schéma d'extraction de la marque

- ***Algorithme de détection de la marque***

1. séparer les trois couleurs de base *R, G, B* de l'image marquée,
2. déterminer la luminance marquée *Ym*,
3. retrouver les blocs marqués grâce à la clé secrète *K*,
4. déterminer les cinq coefficients *DCT* associé à chaque bloc sélectionné,
5. déterminer les deux coefficients *DCT* marqués, coef1m et coef2m, dont la valeur absolue de leur différence est minimale,
6. calculer la valeur moyenne : valmoym = (coef1m+coef2m)/2,

- Si valmoym = 0, le bit est un zéro
- Si non le bit est un 1

7. calculer la corrélation de la marque originale avec les différentes marques extraites,
8. à partir des résultats de corrélation, retenir la marque la plus corrélative.

IV.1.2. Résultats et interprétations

Pour tester l'approche développée nous avons utilisé l'image Lena 512x512. La marque insérée est une séquence binaire de 8 bits. Sa redondance est étroitement liée au seuil choisi pour la sélection des blocs susceptibles à être marqué. L'ensemble des tests effectués touchent essentiellement l'invisibilité de la marque et la robustesse vis-à-vis la compression, le changement de format et la conversion en niveau de gris.

IV.1.2.1. Test de l'invisibilité de la marque

La contrainte invisibilité est vérifiée parce qu'on a veillé sur la vérification des deux points suivants:

1- les coefficients à modifier se situent dans la région des moyennes fréquences,

2- les quantités, ajoutées ou soustraites aux coefficients lors de leurs modifications, n'altèrent pas la qualité de l'image.

La figure (IV.5) montre l'effet du respect des deux points ci-dessus et le bon choix du seuil de sélection des blocs dont les quels la marque sera insérée. En effet, la qualité de l'image est préservée et aucune différence n'est perceptible entre l'image originale et l'image

marquée. Par contre l'image de la figure (IV.6) illustre clairement les dégradations provoquées par le non respect des points cités précédemment.

Image Originale

Image Marquée

Figure IV.5. Vérification de la contrainte invisibilité de la marque

Image Originale

Image Marquée

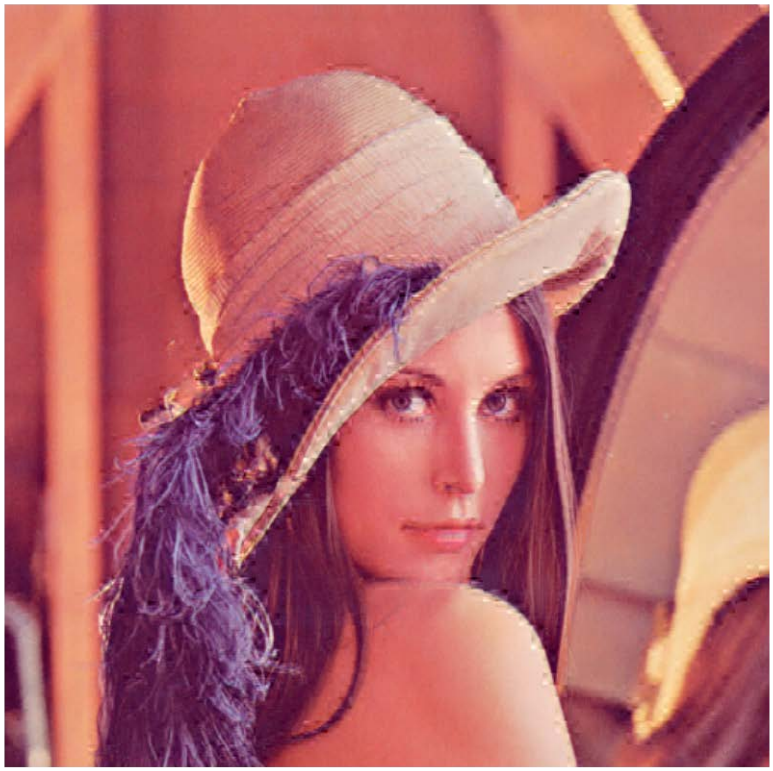
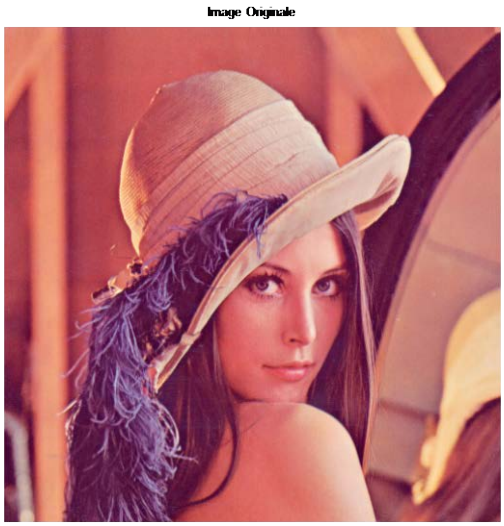


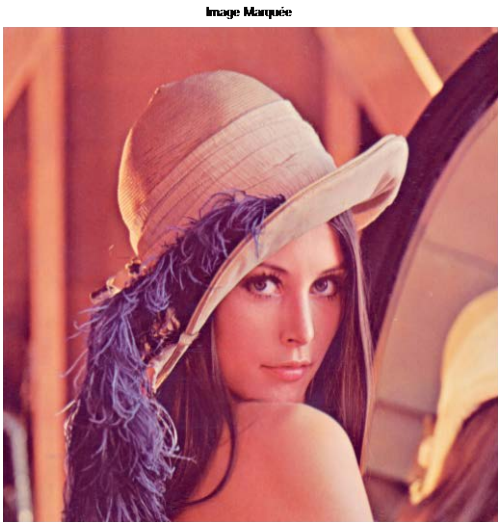
Figure IV.6. Dégradation de la qualité de l'image après insertion de la marque

La figure (IV.7) montre les résultats d'insertion des combinaisons [1 1 1 1 1 1 1 1] et [0 0 0 0 0 0 0 0] de la marque. En effet, ces deux combinaisons correspondent aux modifications maximales que peut subir les coefficients *DCT* des blocs sélectionnés. Comme on peut le constater la contrainte invisibilité est vérifiée et aucune différence perceptible entre l'image originale et l'image marquée.

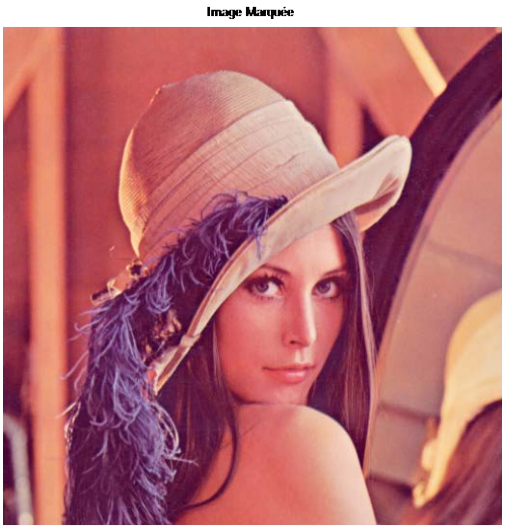
Un autre test de la contrainte invisibilité est donné sur la figure (IV.8). Il montre qu'elle est vérifiée quelque soit le nombre de redondance de la marque (*NR*). Cela est dû au fait que dans notre approche c'est le seuillage de la variance locale des blocs qui détermine le nombre de bits à insérer et non pas l'inverse.



a. Image originale



c. Image marquée W=[11111111]



b. Image marquée W=[00000000]

Figure IV.7. Vérification de l'invisibilité de la marque pour les deux cas extrêmes

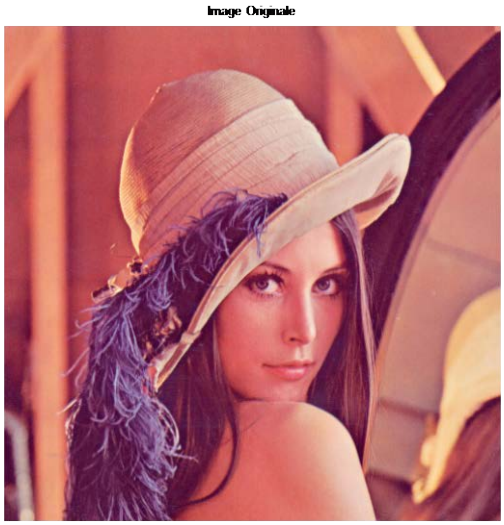


Image originale

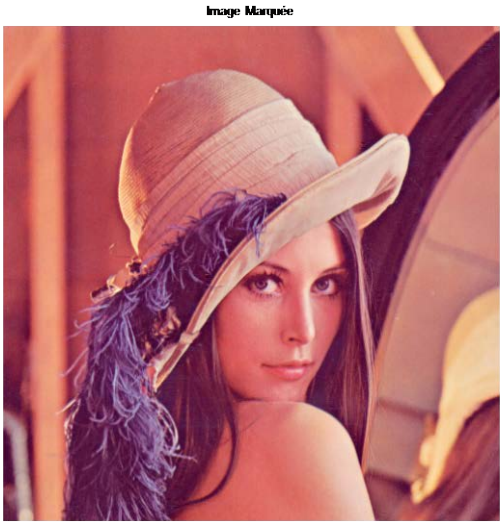


Image marquée, cas NR=23

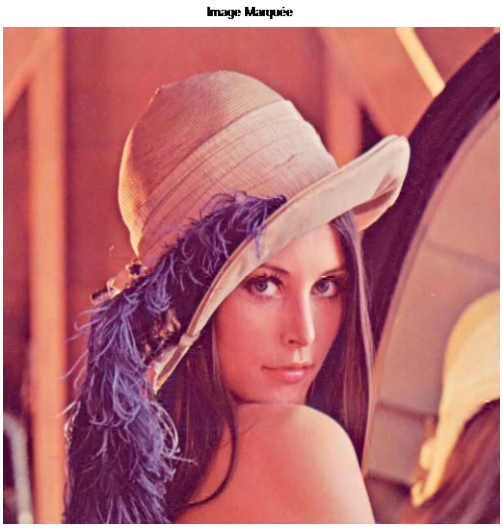


Image marquée, cas NR=91

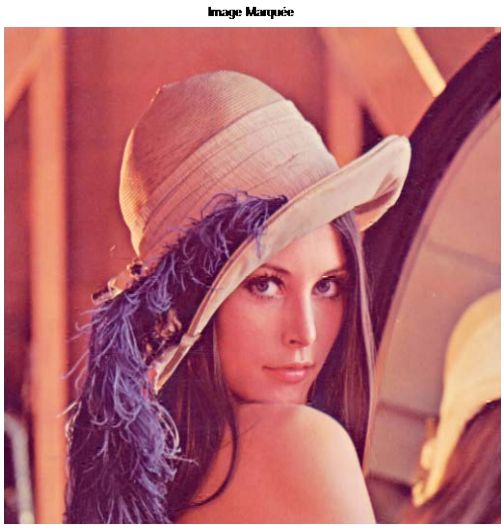


Image marquée, cas NR=160

Image marquée, cas NR=200

Image marquée, cas NR=243

Figure IV.8. Vérification de l'invisibilité de la marque pour différentes valeurs de NR

Quand on parle de l'invisibilité de la marque c'est certainement la qualité de l'image qui est visée. Donc pour évaluer la distorsion engendrée à cause de l'insertion de la marque on a utilisé un des paramètres les plus populaires en traitement d'image. Il s'agit du *PSNR* (*Peak Signal to Noise Ratio*) pour plus de détails voire sec (II.4.1) du chapitre (II). La courbe de la figure (IV.9) illustre les variations du *PSNR* en fonction du nombre de redondance de la marque (*NR*)

$$MSE = \frac{1}{m.n}\sum_{i=1}^{m}\sum_{j=1}^{n}[I(i,j) - I^{*}(i,j)]^{2} \qquad \text{(IV.6)}$$

$$PSNR = 10\log\left(\frac{I^{2}_{\max}}{MSE}\right) = 20\log\left(\frac{I_{\max}}{\sqrt{MSE}}\right) \qquad \text{(IV.7)}$$

Avec :

MSE : c'est l'erreur quadratique moyenne,

I : image original

*I** : image marquée

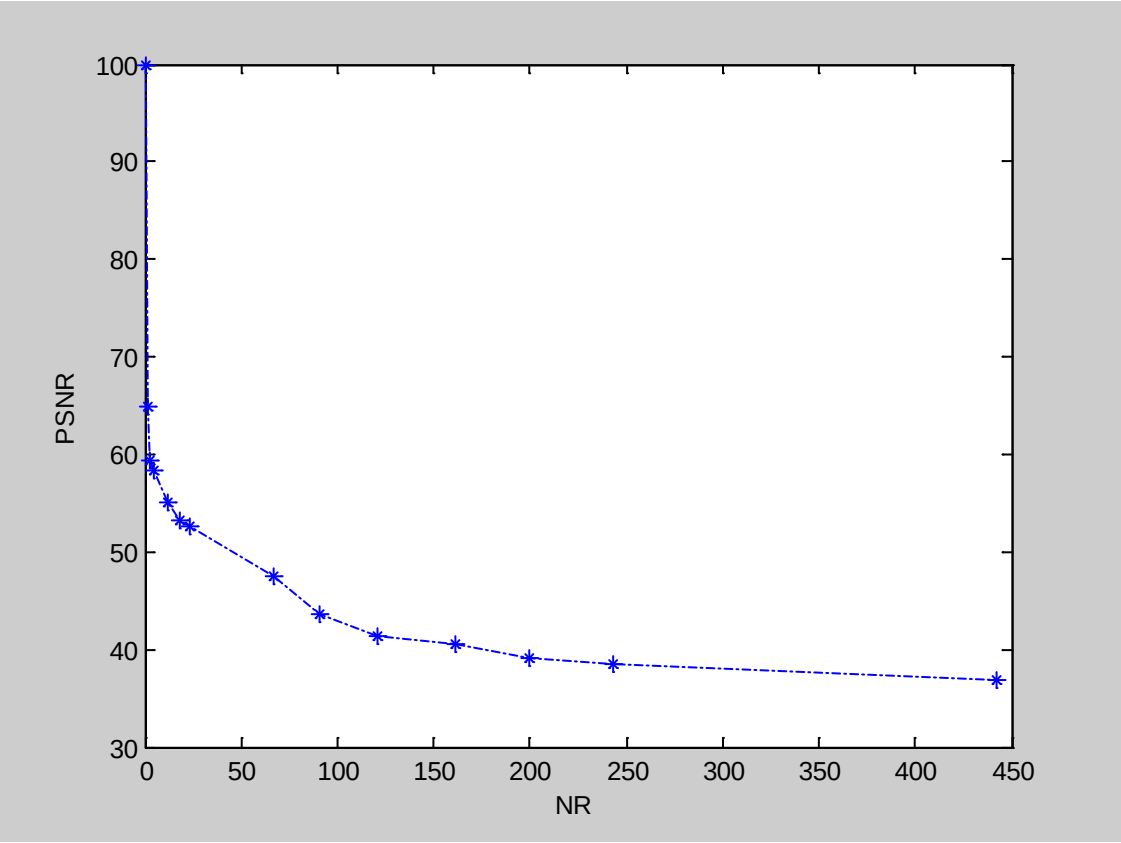


Figure IV.9. Variation Du *PSNR* en fonction du nombre de redondance *NR*

De la figure (IV.9) on constate que lorsque le nombre de redondance de la marque (*NR*) est augmenté, le nombre de blocs concernés par la modification de leurs coefficients augmente. Ce qu'explique la diminution du *PSNR*, mais il reste toujours dans un intervalle de valeurs très acceptables.

IV.1.2.2. Test de la robustesse vis-à-vis la compression

Pour les tests de robustesse vis-à-vis la compression, nous avons compressé l'image marquée avec différents taux de compression (taux de qualité). Ensuite, pour chaque taux de compression et selon le nombre de redondance (*NR*), la marque la plus proche de la marque originale est extraite. Pour mettre cette opération en évidence nous calculons le pourcentage de similarité (*PSIM*). C'est est un paramètre qui donne le taux de ressemblance entre les marques récupérées et la maque originale et il est donné par la formule (IV.8) :

$$PSIM = \max_i^T \left(\frac{NBS_i}{NBM} \right) * 100 \qquad \text{(IV.8)}$$

- T : Nombre de marques récupérées.
- NBS_i : Nombre de bits, de la i^{ème} marque récupérée, similaire aux bits de la marque originale.
- NBM : Nombre de bits de la marque originale.

Les figures (IV.10) et (IV.11) donnent les variations du rapport de similarité (*PSIM*), entre la marque originale est celle extraite, en fonction du taux de compression pour *NR*=11 et *NR*=521 respectivement.

A partir des courbes des figures (IV.10) et (IV.11) on peut constater l'effet de la redondance de la marque sur sa détection. Pour *NR*=11, on remarque que pour des taux de compression allant jusqu'à 30% la similarité entre la marque originale et celle extraite est de 80%. Mais pour des taux de compression supérieurs à 30%, le rapport de similarité chute à des valeurs moins importantes indiquant l'échec de l'extraction de la marque. Par contre pour un *NR*=512, la similarité entre la marque originale et celle extraite est entre 80% et 100% pour des taux de compression allant jusqu'à 90%. Ceci s'explique par le fait que plus NR est grand plus le nombre de marques extraites augmente et plus est la chance d'avoir parmi celles-ci une marque similaire à la marque originale.

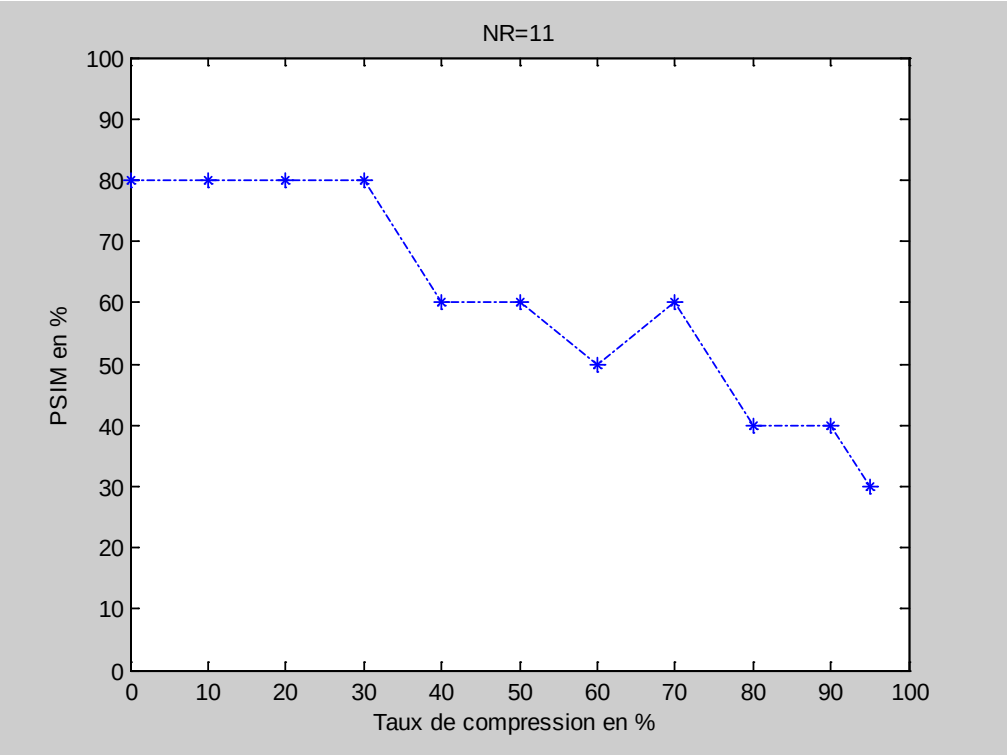


Figure IV.10. Variation du *PSIM* en fonction du taux de compression pour *NR*=11

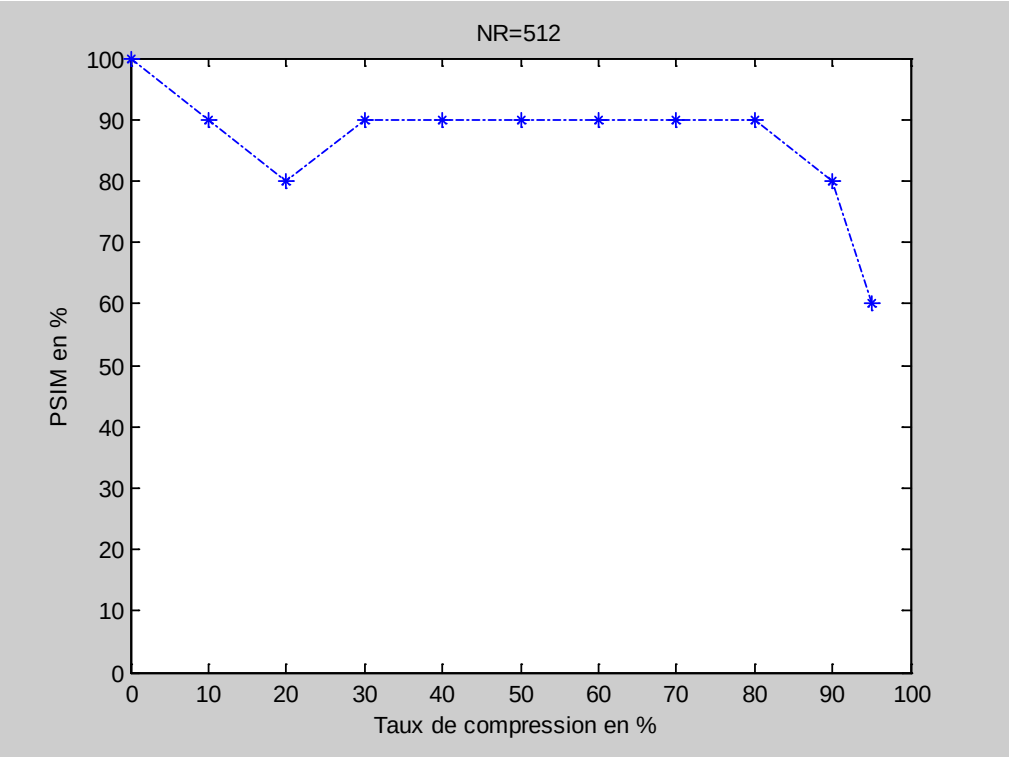


Figure IV.11. Variation du *PSIM* en fonction du taux de compression pour *NR*=512

IV.1.2.3. Test de la robustesse vis-à-vis changement de format

Pour le test de la robustesse de la marque vis-à-vis le changement de format, l'image marquée est sauvegardée sous différents type de formats tel que JPEG, BNP, TIFF et PNG comme il est indiqué sur la figure (IV.12). L'extraction de la marque est réussie pour les quatre types de format. Ceci se justifié par le fait que lors de l'insertion de la marque, ces données sont intimement liées aux données de l'image et non pas attachées entant que entête ou fichier.

Format Tiff | JPEG qualité 100%

Format BMP | Format PNG

.

Figure IV.12. Robustesse vis-à-vis le changement de format

IV.1.2.4. Test de la robustesse vis-à-vis la conversion en niveau de gris

L'opération de conversion de l'image couleur marquée en niveau de gris, donnée sur la figure (IV.13), n'altère pas l'extraction de la marque. C'est tout simplement parce qu'au

cours de ce passage en niveau de gris c'est les composants chrominance qui disparaissent. La composante luminance, qui comporte la marque, est conservée.

Image marquée en couleurs

Image en niveau de gris

Figure .IV.13. Robustesse vis-à-vis la conversion en niveau de gris

IV.1.3. Conclusion

Dans cette première partie de ce chapitre nous avons présenté notre première contribution dans le domaine du watermarking d'image fixe. L'approche développée appartient aux schémas substitutifs non informé (aveugle). Comme il est clair des résultats des tests effectués, elle possède certaines performances en terme d'invisibilité et de robustesse vis-à-vis la compression, le changement de format et la conversion en niveau de gris. Cependant, plusieurs problèmes restent à résoudre parmi lesquels on cite les suivant :

- La robustesse de la marque à des taux de compression élevés.
- La difficulté de modéliser les variations des coefficients DCT. Ceci perturbe la procédure d'extraction de la marque basée sur la stratégie utilisée lors de la phase d'insertion.
- La méthode n'est pas robuste aux attaques d'ajout de bruits ou de filtrage.
- La limitation de l'espace d'insertion de la marque aux zones fortement texturée (hautes fréquences).

Une analyse de ces problèmes nous a conduits à développer une approche hybride qui fera l'objet de la deuxième partie de ce chapitre.

IV.2. Méthode Hybride DWT-DCT de Tatouage d'image Fixe

IV.2.1. Description de la méthode développée

Le travail que nous présentons ici est une amélioration de l'approche présentée dans la première partie de ce chapitre. La méthode développée se base sur la combinaison de deux transformées qui sont la *DWT* et la *DCT*. L'utilisation de la *DWT* permet de séparer complètement les basses fréquences dans la sous bande *LL*, appelée aussi approximation, des hautes fréquences qui représente les détails de l'image et qui sont données par les sous bandes *LH*, *HL* et *HH*. Ensuite, on s'intéresse uniquement à la sous bande *LL* puisque elle représente les basses fréquences. Un endroit d'insertion très sûre pour que la marque soit robuste surtout vis-à-vis les opérations de compression, de filtrage passe bas et d'ajout de bruit…etc. Mais, un endroit non sûr pour l'invisibilité de la marque. Pour résoudre ce problème on a fait recours à la *DCT* qu'on applique uniquement à la sous-bande basse fréquences (*LL*). Ceci permet de séparer les basses, les moyennes et les hautes fréquences de *LL*. Par conséquent, et en comparaison avec l'approche de la première partie, le nombre de coefficients *DCT* aptes à supporter la marque devient très important.

Contrairement à la plupart des techniques de tatouage qui marquent la totalité des blocs, notre méthode marque un nombre limité de blocs déterminé par trois paramètres à savoir la variance locale de chaque bloc, la taille de la marque à insérer et le nombre de redondance de la marque. Cette stratégie permet de minimiser considérablement les altérations de la qualité de l'image et assure un compromet entre l'invisibilité et la robustesse de la marque.

L'extraction de la marque se fait d'une manière aveugle, c'est-à-dire sans faire recours à l'image originale, ce qui qualifié le tatouage d'être non informé (*Blind watermarking*).

IV.2.1.1. Insertion de la marque

La méthode proposée fait partie des schémas substitutifs à contrainte. La procédure d'insertion de la marque passe par plusieurs étapes comme il est indiqué sur la figure (IV.14). Après avoir séparé les couleurs de base (R, G, B) de l'image à marquer, en calcul les paramètres luminance et chrominance selon les équations (IV.1, IV.2 et IV.3). Les paramètres chrominances sont conservés, par contre la luminance, qui est l'objectif du tatouage, subit une transformation *DWT* de Haar de niveau 1. La sous-bande basse fréquences (*LL*) est divisée en blocs de 8x8 qui seront sélectionnés selon leurs variances locales, et pour enfin insérer la marque par modification de leurs coefficients.

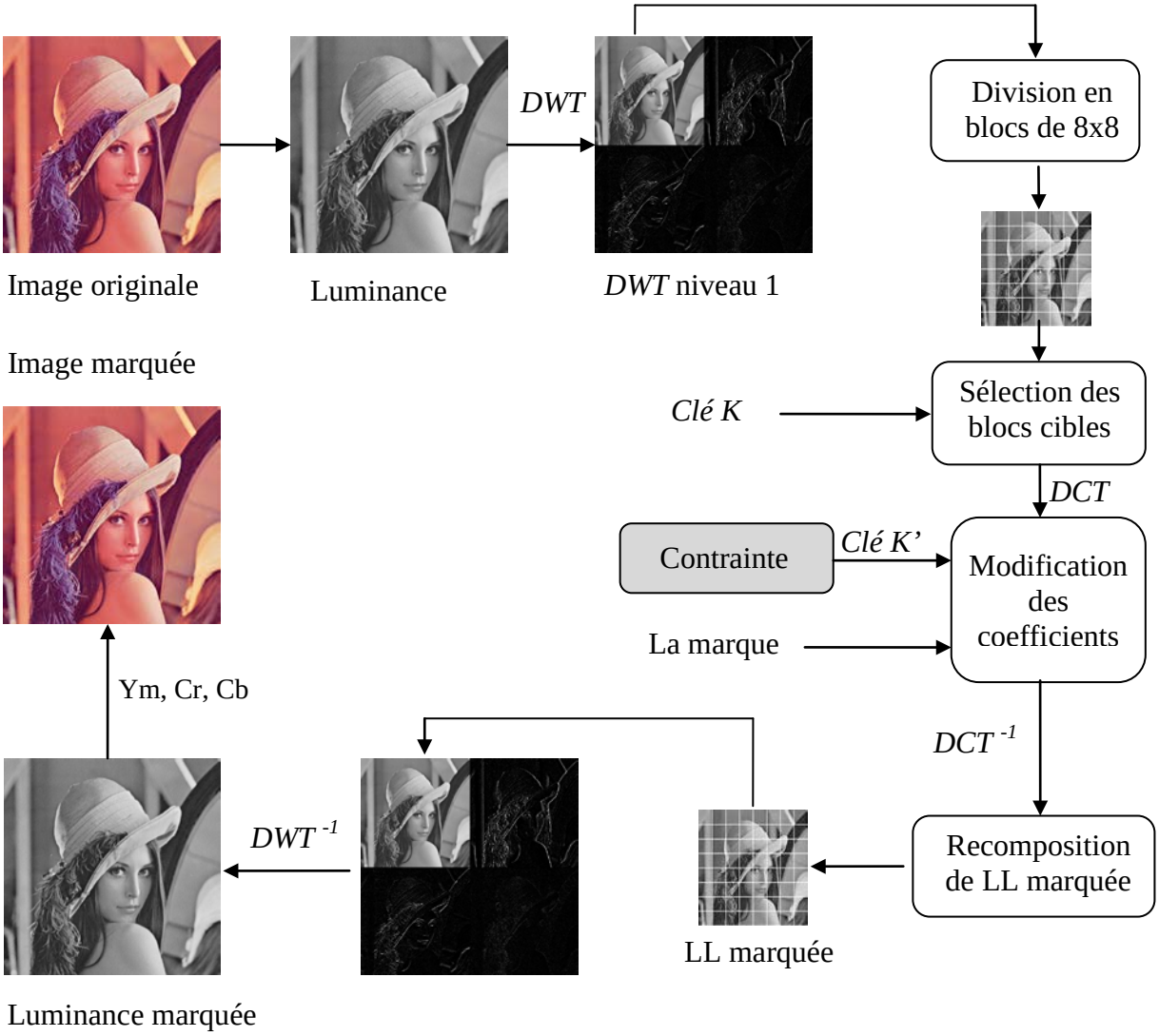


Figure IV.14. Schéma d'insertion de la marque

.

- ***Sélection des blocs à marquer***

La sélection des blocs susceptibles d'être marqués se fait presque de la même manière que pour la méthode de la première partie. On calcul les variances locales des blocs, ensuite un seuillage de ce paramètre permet de sélectionner les blocs concernés par le marquage. A la différence que dans cette approche le seuil est déterminé en fonction de la taille de la marque à insérée et de son nombre de redondance. Une fois les blocs concernés par le marquage sont sélectionnés, on procède à l'insertion de la marque selon

une stratégie également différente de celle de la première méthode. Ce qui est expliqué dans la section ci-dessous.

- ***Modification des coefficients DCT***

Les coefficients concernés par la modification sont ceux situés sur la ligne en zigzag, modèle utilisé dans la compression *JPEG*, comme il est indiqué sur la figure (IV.15). Ce choix est justifié par la faible variance des coefficients appartenant à chaque ligne (continué) des matrices de quantification utilisées lors de la compression. Cette structure nous offre (9) positions possibles pour l'insertion de la marque. Les coefficients choisis de chaque position sont modifiés selon l'état du bit de la marque. Ainsi, la contribution de ce changement sur la totalité du bloc doit être négligeable.

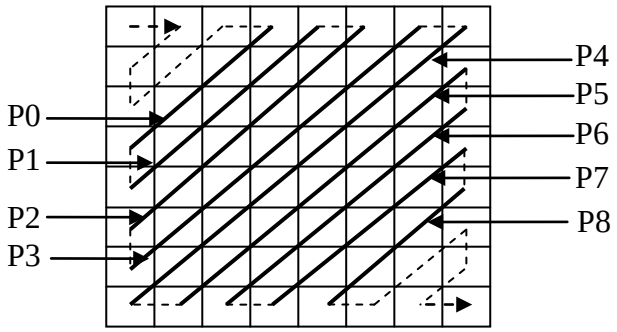


Figure .IV.15 Disposition des coefficients concernés par la modification

- ***Algorithme d'insertion de la marque***

1. soit une séquence de n bits (b_1, b_2, ……., b_n) qui constitué la marque à insérer.
2. Séparer les trois couleurs de l'image et calculer la matrice luminance concernée par le marquage.
3. Calculer la *DWT* de la luminance.
4. Diviser l'approximation LL en blocs de 8x8.
5. Calculer la *DCT* de chaque bloc.
6. sélectionner selon une clé (seuillage de la variance locale), les blocs concernés par le marquage.
7. Sélectionner une position, parmi les 9 possibilités, et choisir les coefficients à modifier.

8. Modifier l'ordonnancement des coefficients selon l'état du bit b_i de la marque
9. une fois tous les blocs concernés par le marquage sont marqués, calculer la *DCT* inverse de chaque bloc.
10. reconstitution de la matrice approximation (*LL*) marquée à partir des blocs 8x8.
11. Calculer la *DWT* inverse.
12. reconstitution des couleurs de base RGB, à partir des paramètres luminances marqués et chrominances conservés.
13. reconstitution de l'image marquée

IV.2.1.2. Extraction de la marque

L'extraction de la marque se fait sans recours à l'image originale. L'enchaînement des étapes de cette extraction sont donnée sur la figure (IV.16).

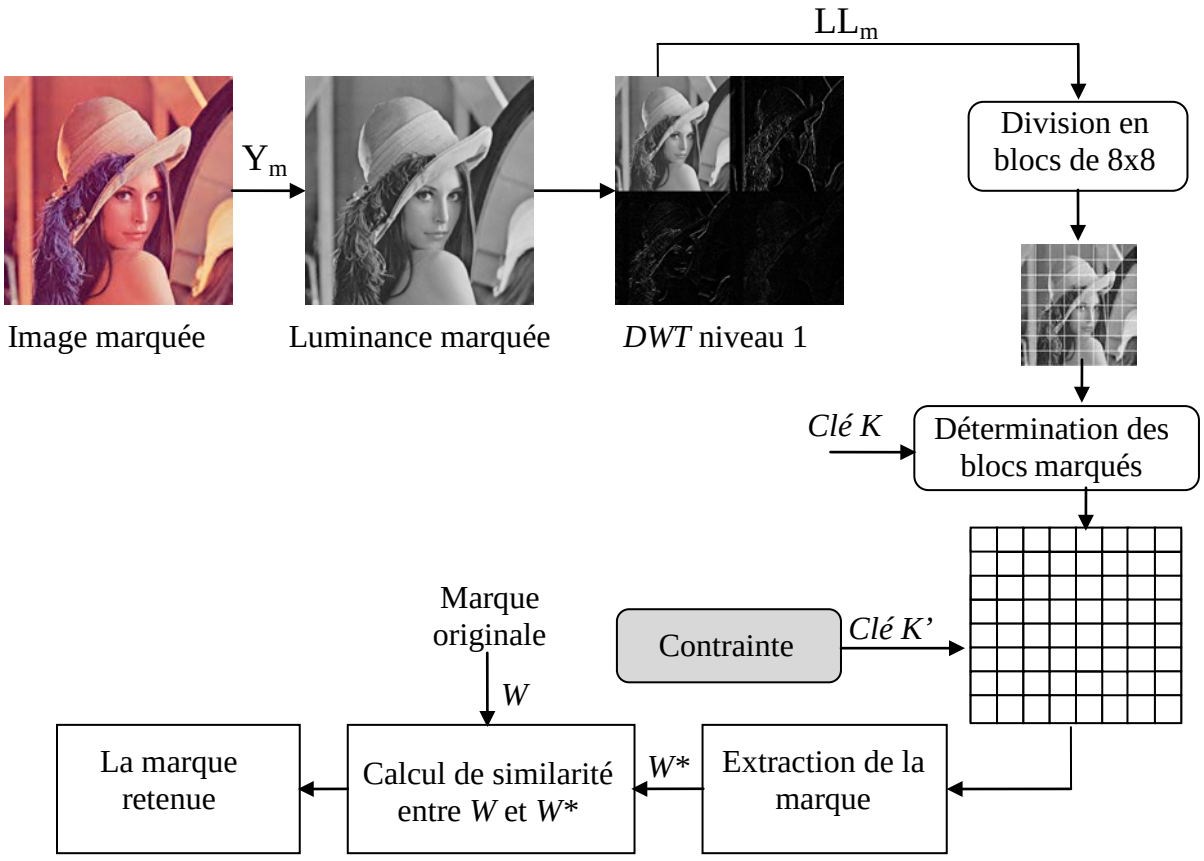


Figure IV.16. Schéma d'extraction de la marque

- ***Algorithme d'extraction de la marque***

1. Séparer les trois couleurs de l'image marquée.
2. Calculer la luminance marquée *Ym*.

3. Calculer la *DWT* de la luminance marquée.
4. Diviser l'approximation (*LL*) marquée en blocs de 8x8.
5. Calculer la *DCT* de chaque bloc.
6. Trouver les blocs marqués en utilisant la même stratégie de seuillage utilisée lors de l'insertion (la clé *K*).
7. L'état de l'ordonnancement des quatre coefficients appartenant à la même position (clé *K'*) détermine si le bloc est marqué par 1 ou 0.
8. Un calcul de similarité entre les marques récupérées et la marque originale permet de dégager la meilleure marque détectée avec son pourcentage de similitude.

IV.2.2. Tests et interprétation des résultats

Dans ce qui suit nous allons présenter des résultats de tests comparatifs et qui mettent en relief les performances de la méthode développée (utilisant la *DWT* et la *DCT*) par rapport à l'utilisation de la *DCT* seule. Ces performances, en terme de qualité et de robustesse vis-à-vis la compression *JPEG* et l'ajout de bruit Gaussien, sont le *PSNR* (*Peak Signal to Noise Ratio*) et le *PSIM* (pourcentage de similarité).

L'implantation de l'approche développée a été faite à l'aide d'un programme réalisé en MATLAB. Les tests ont été effectués sur l'image Lena de résolution 512x512 pixels et de 24 bits par pixel.

IV.1.2.1. Test de l'invisibilité de la marque

La contrainte invisibilité de la marque a été garantie pour les raisons suivantes :

1- les coefficients à modifier se situent sur une ligne en zigzag, modèle utilisé dans la compression *JPEG*, comme il est indiqué sur la figure (IV.15).
2- Cette disposition montre une faible variance des valeurs des coefficients de la même position.
3- La stratégie utilisée pour modifier ces coefficients lors de l'insertion du bit de la marque (modification de l'ordonnancement) n'altère plus la qualité de l'image. c'est justement parce que leur variance est faible.

Pour montrer l'efficacité de la méthode développée en termes d'invisibilité de la marque, on a choisi d'effectuer des tests concernant les situations les plus délicates. En effet,

pour voire les dégradations qui peuvent être provoquées par les plus importantes modifications possibles, on a choisi d'insérer les marques [0 0 0 0 0 0 0 0] et [1 1 1 1 1 1 1 1] correspondantes à ces modifications pour des redondances *NR*=1 et *NR*=100. Ces marques sont insérées dans les deux positions extrêmes *P0* et *P8*, qui représentent respectivement les très basses et les très hautes fréquences, du bloc sélectionné pour le marquage et appartenant à la sous-bande basses fréquence (*LL*).

a. Image originale

b. Image marquée *W*=[00000000] et *NR*=1

c. Image marquée *W*=[00000000] et *NR*=110

Figure IV.17. Insertion de la marque [0 0 0 0 0 0 0 0] dans la position *P0* avec *NR*=1 et *NR*=110

a. Image originale

b. Image marquée
W=[11111111] et *NR*=1

c. Image marquée
W=[11111111] et *NR*=110

Figure IV.18. Insertion de la marque [1 1 1 1 1 1 1 1] dans la position *P0* avec *NR*=1 et *NR*=110

Les figures (IV.17) et (IV.18) montrent respectivement l'insertion des marques [0 0 0 0 0 0 0 0] et [1 1 1 1 1 1 1 1] dans la position *P0*. Dans les deux cas d'insertion on constate que la marque est invisible pour *NR*=1 (figure (IV.17.b) et (IV.18.b)), par contre son effet est clairement visible pour *NR*=110 (figure (IV.17.c) et (IV.18.c)). Ceci s'explique par le fait que la position *P0* correspond aux très basses fréquences. Par conséquent, dans le cas de *NR*=1, le nombre de coefficients basses fréquences modifiés est très faible et égale à 32, c'est pourquoi l'effet de l'insertion de la marque n'est pas visible. Par contre dans le cas de *NR*=110, le nombre est de l'ordre de 3520, la raison pour laquelle la dégradation est très importante.

a. Image originale

b. Image marquée
W=[00000000] et *NR*=1

c. Image marquée
W=[00000000] et *NR*=110

Figure IV.19. Insertion de la marque [0 0 0 0 0 0 0 0] dans la position *P8* avec *NR*=1 et *NR*=110

Dans les figures (IV.19) et (IV.20), qui illustrent les deux cas d'insertion de la marque en modifiant les coefficients *DCT* de la position *P8* pour des redondances *NR*=1 et *NR*=110, on constate que la qualité de l'image est conservée et aucune distorsion n'est perceptible. Ceci est dû au faite que la position *P8* correspond aux hautes fréquences de la sous-bande basses fréquences (*LL*). Donc quelque soit le nombre de coefficients modifiés, l'effet de cette modification reste imperceptible. Mais, au contraire pour le *PSNR* qui est sensible aux nombre de coefficients modifiés, donc il est influencé par NR et voir même par la position d'insertion de la marque.

a. Image originale

b. Image marquée
W=[11111111] et NR=1

b. Image marquée
W=[11111111] et NR=110

Figure IV.20. Insertion de la marque [1 1 1 1 1 1 1 1] dans la position *P8* avec *NR*=1 et *NR*=110

Dans ce qui suit nous allons présenter les résultats donnant les variations du *PSNR* en fonction des positions d'insertion de la marque (*P0, P1, P2, P3, P4, P5, P6, P7, P8*). Les courbes des figures (IV.21), (IV.22), (IV.23) et (IV.24) illustrent ces résultats pour différents nombre de redondance (*NR*) et pour les deux méthodes (*DWT-DCT*) et (*DCT* seule).

De ces résultats, on constate que l'augmentation du nombre de redondances *NR* engendre une diminution du *PSNR*.

- Dans le cas du tatouage par la *DCT* seule, cette diminution est très faible et ca concerne uniquement les positions *P0, P1, P2, P3* qui correspondent aux basses fréquences de chaque

bloc *DCT*. Le *PSNR* des positions *P4, P5, P6, P7, P8,* qui correspondent aux hautes fréquences de chaque bloc *DCT*, reste inchangé.

- Par contre, dans le cas du tatouage par la méthode *DWT+DCT*, la diminution du *PSNR* est très importante pour les cas des positions *P0, P1, P2, P3* correspondantes aux très basses fréquences de chaque bloc *DCT* de la sous bande basses fréquences (*LL*). Cette diminution devient de plus en plus moins importante en passant aux positions supérieures correspondantes aux hautes fréquences de chaque bloc *DCT* de la sous bande basses fréquences (*LL*).

Ceci s'explique par le fait que : dans le cas de la *DCT*, l'effet des modifications portées aux coefficients *DCT* est réparti sur l'information pertinente de l'image (composantes basses fréquences) et les détails de l'image. Par contre dans le cas de la *DWT+DCT*, la totalité de l'effet est concentrée sur l'information pertinente de l'image seule (sous bande *LL*). Malgré ces diminutions, les valeurs du *PSNR* restent toujours dans l'intervalle des valeurs très acceptables et cela pour de grandes valeurs de *NR* permettant d'augmenter la possibilité de la détection de la marque.

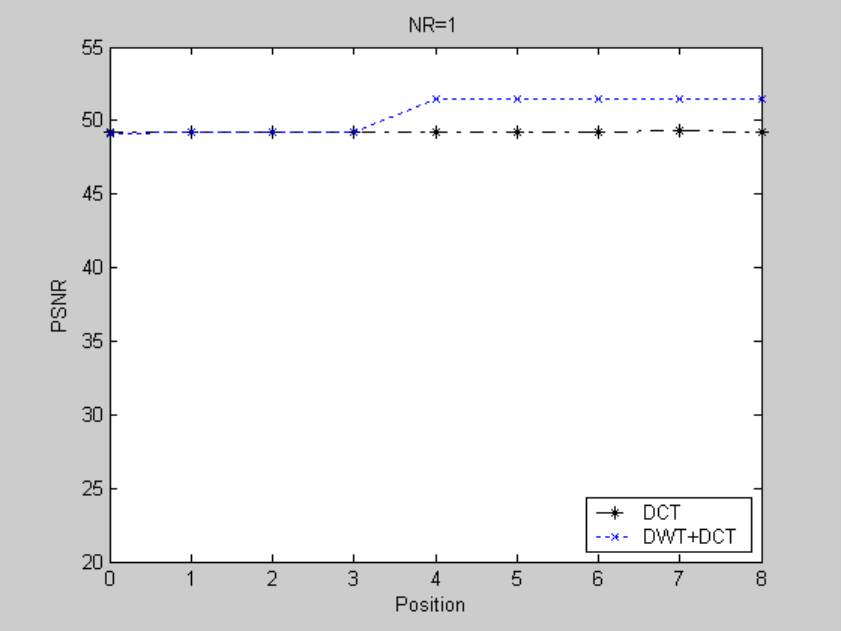


Figure .IV.21. Variations du *PSNR* en fonction de la position de la marque pour *NR*=1

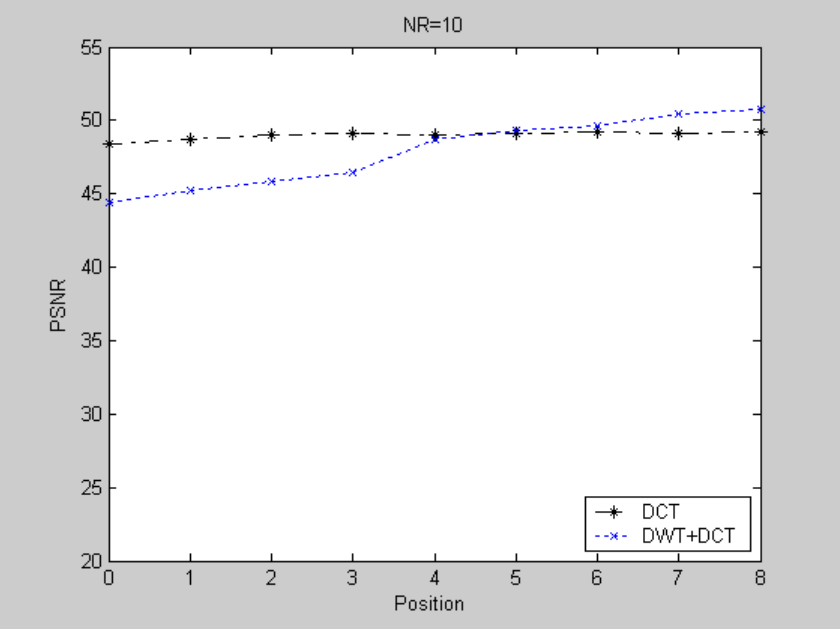


Figure .IV.22. Variations du *PSNR* en fonction de la position de la marque pour *NR*=10

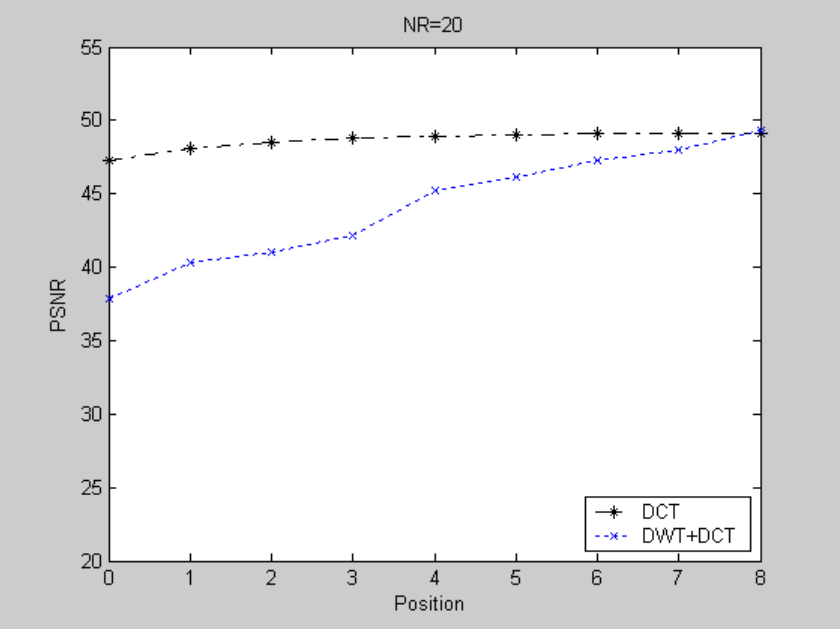


Figure IV.23. Variations du *PSNR* en fonction de la position de la marque pour *NR*=20

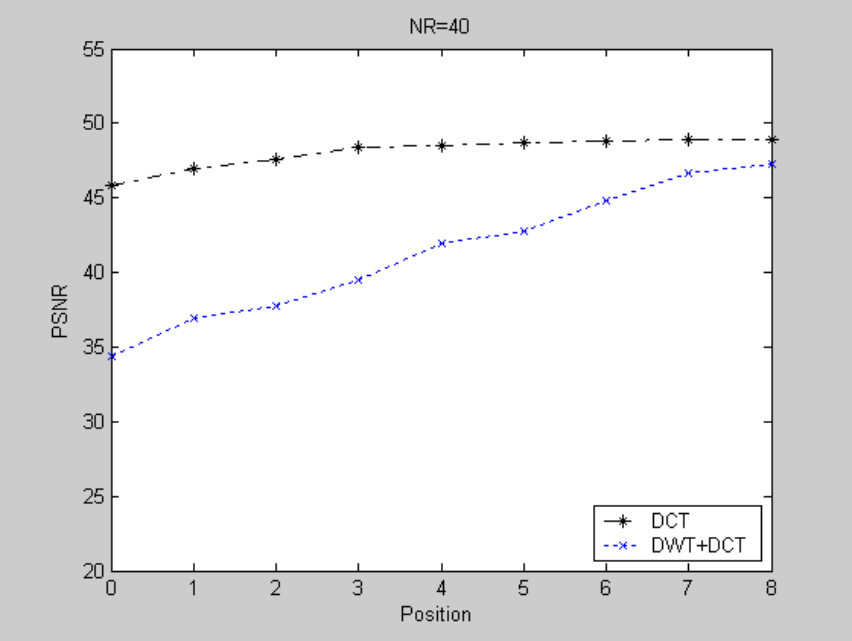


Figure VI.24. Variations du *PSNR* en fonction de la position de la marque pour *NR*=40

IV.2.2.2. Test de la robustesse vis-à-vis de la compression

Nous présentons dans ce deuxième test les résultats mettant en évidence les performances de la méthode hybride proposée (*DWT+DCT*) par rapport à la *DCT* seule, en terme de robustesse de la marque vis-à-vis de la compression *JPEG*. Les images marquées aux positions *P2, P3, P4, P5, P6, P7 et P8* (concernant les moyennes et les hautes fréquences) et avec un nombre de redondance *NR*=20, sont attaquées par une compression *JPEG* à des niveaux de qualité différents. Ensuite, la marque est extraite de l'image marquée et le pourcentage de similitude entre la marque originale et la marque extraite est calculé. Les résultats des figures (IV.25), (IV.26), (IV.27), (IV.28), (IV.29), (IV.30), (IV.31) et (IV.32) montrent clairement l'apport de la méthode développée. On constate que, pour la méthode *DWT+DCT*, la marque est récupérable à 100% pour des niveaux de qualités très bas allant jusqu'à 20 (taux de compression 80%).

Par contre, dans le cas de la *DCT* seule, le *PSIM* est à 100% uniquement pour des niveaux de qualités supérieurs ou égales à 70. En changeant la position d'insertion de la marque vers des positions supérieures, le *PSIM* diminué. On peut expliquer ça comme suite :

- Dans le cas de la *DCT* seul, les positions *P3, P4, P5, P6, P7 et P8* correspondent aux hautes fréquences.

- Dans le cas de *DWT+DCT*, les positions *P3, P4, P5* correspondent aux moyennes fréquences, et *P6, P7 et P8* correspondent aux hautes fréquences, de la sous-bande basses fréquences (LL).

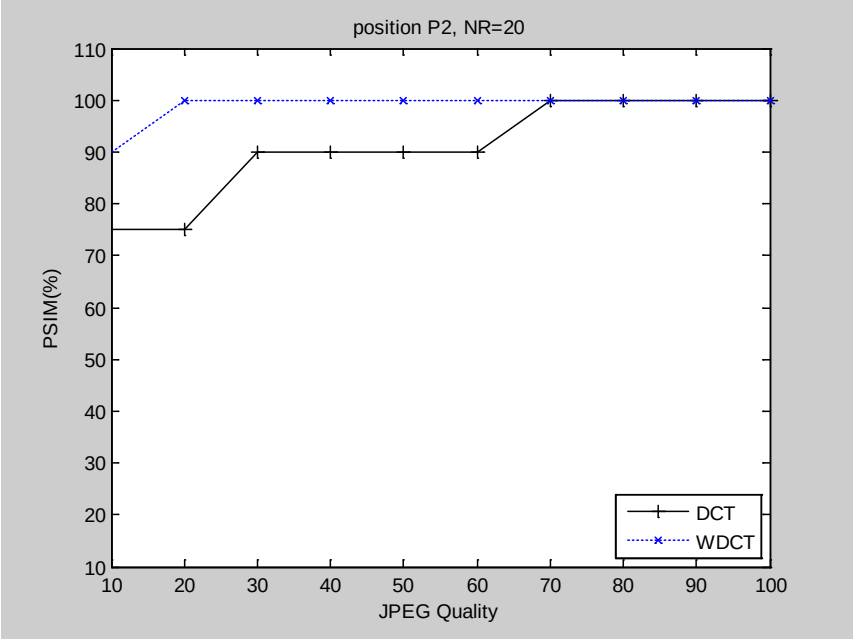


Figure .IV.25. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P2*, *NR*=20

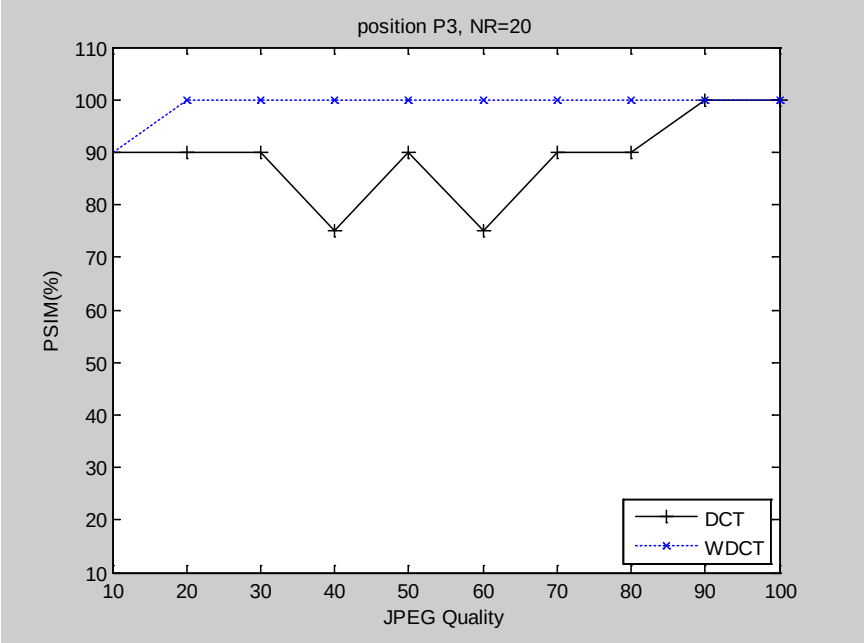


Figure .IV.26. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P3*, *NR*=20

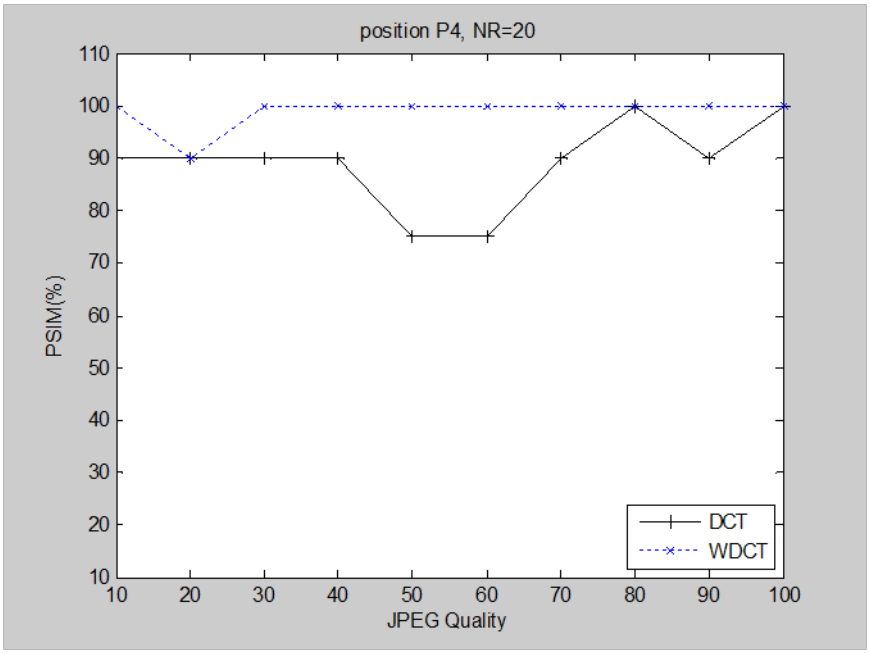


Figure .IV.27. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P4*, *NR*=20

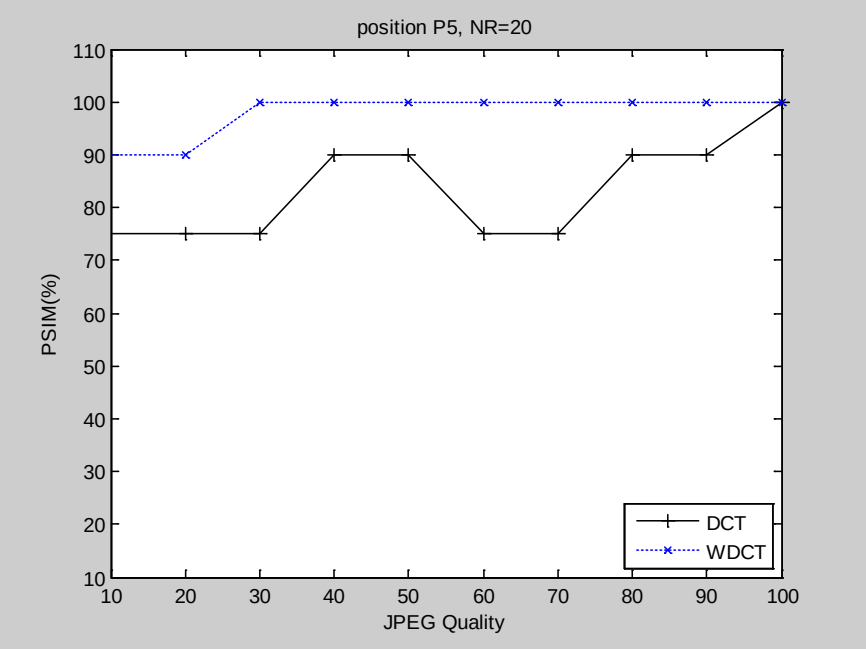


Figure .IV.28. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P5*, *NR*=20

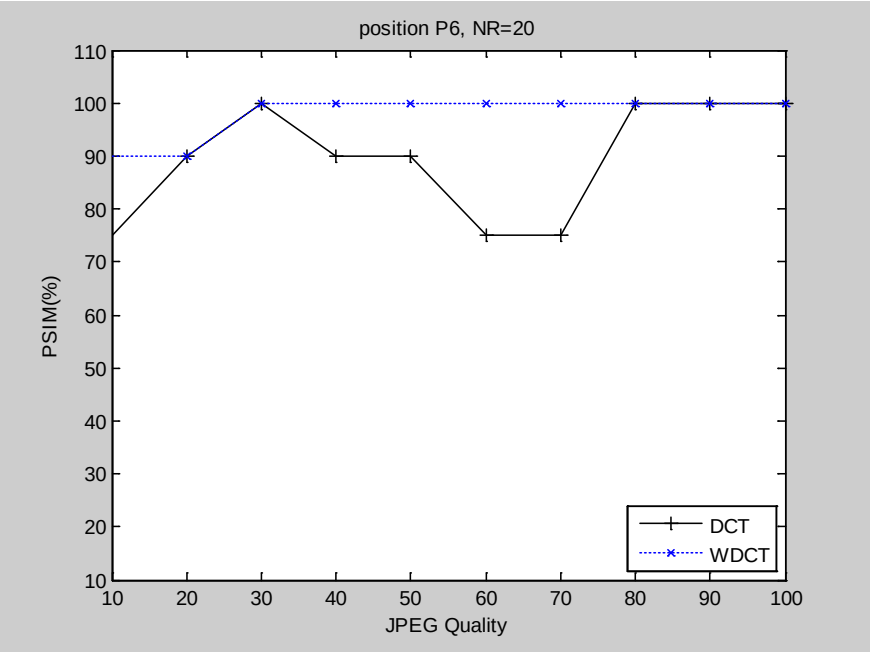


Figure .IV.29. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P6*, *NR*=20

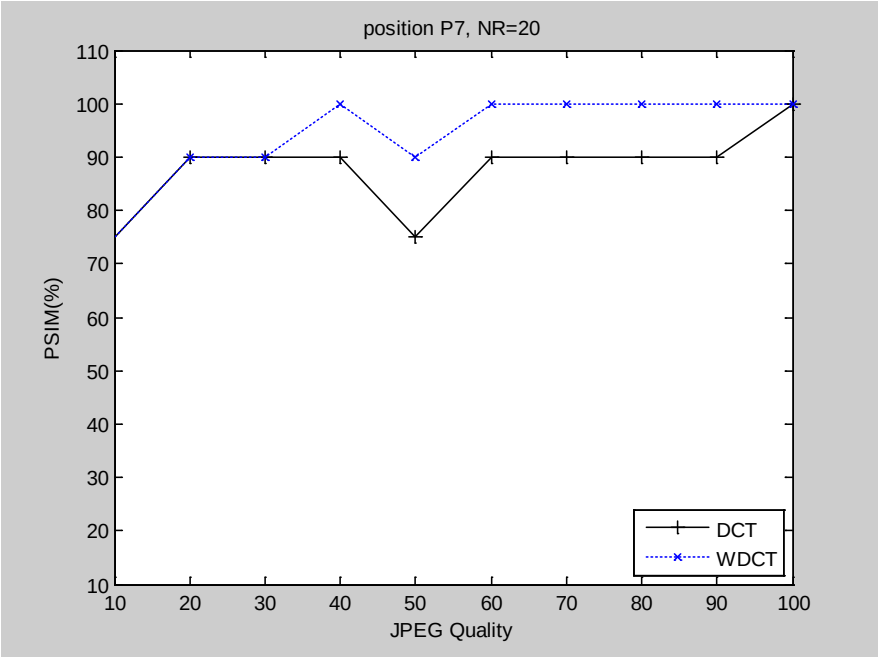


Figure .IV.30. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P7*, *NR*=20

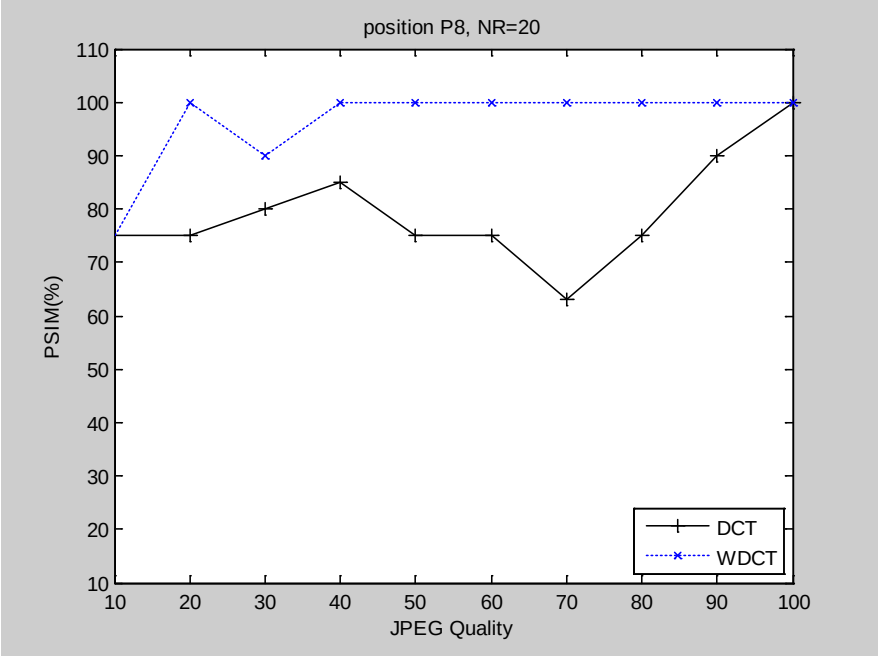


Figure .IV.31. Robustesse de la marque vis-à-vis de la compression *JPEG* pour la position *P8*, *NR*=20

Pour voir l'effet du nombre de redondance de la marque insérée (*NR*) sur l'extraction de la marque (*PSIM*), nous avons fait subir l'image marquée, avec *NR*=100, aux mêmes tests de compression. Nous avons recueilli les résultats illustrés sur les figures (de IV.32 à IV.38).

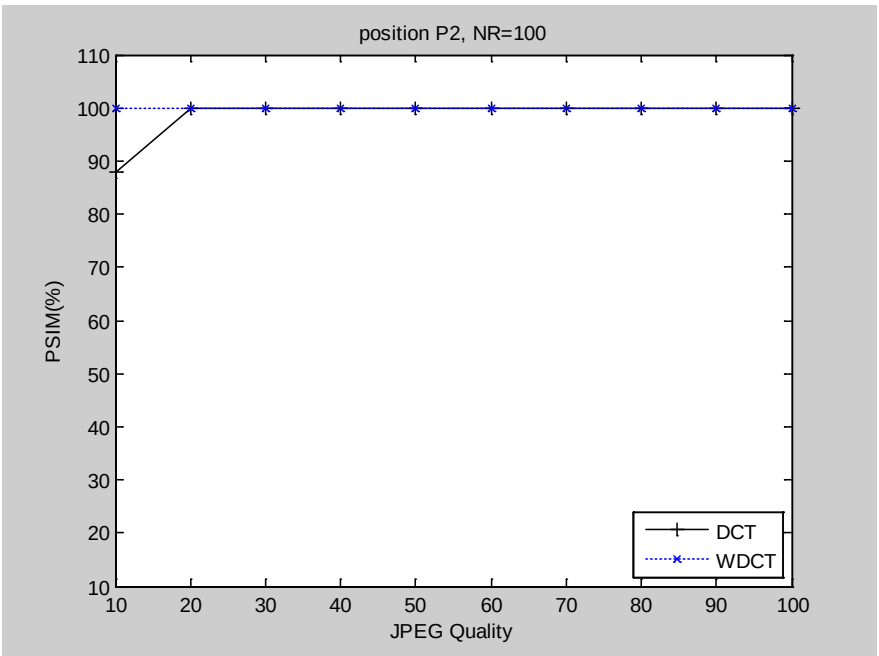


Figure .IV.32. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P2*, *NR*=100

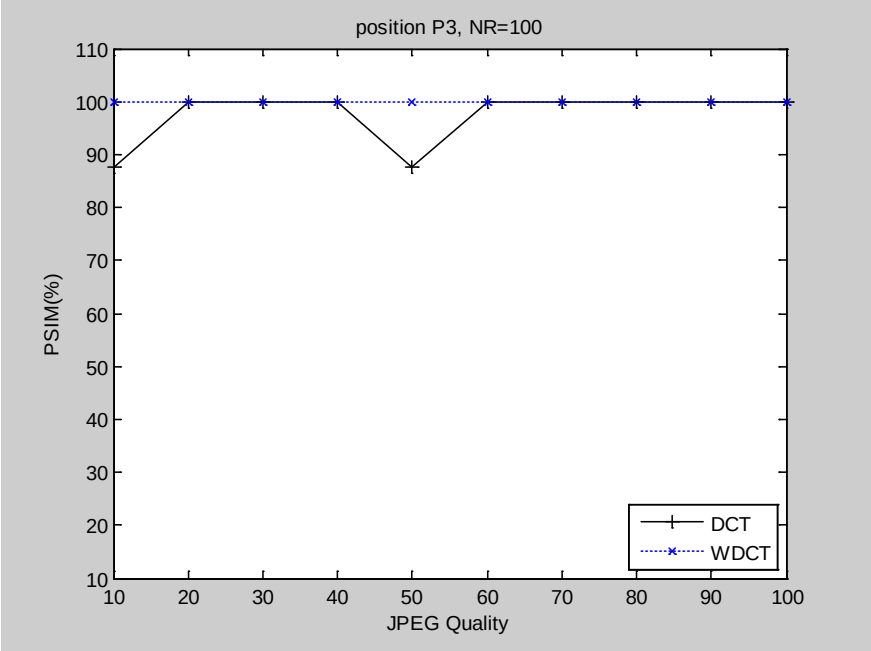


Figure .IV.33. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P3*, *NR*=100

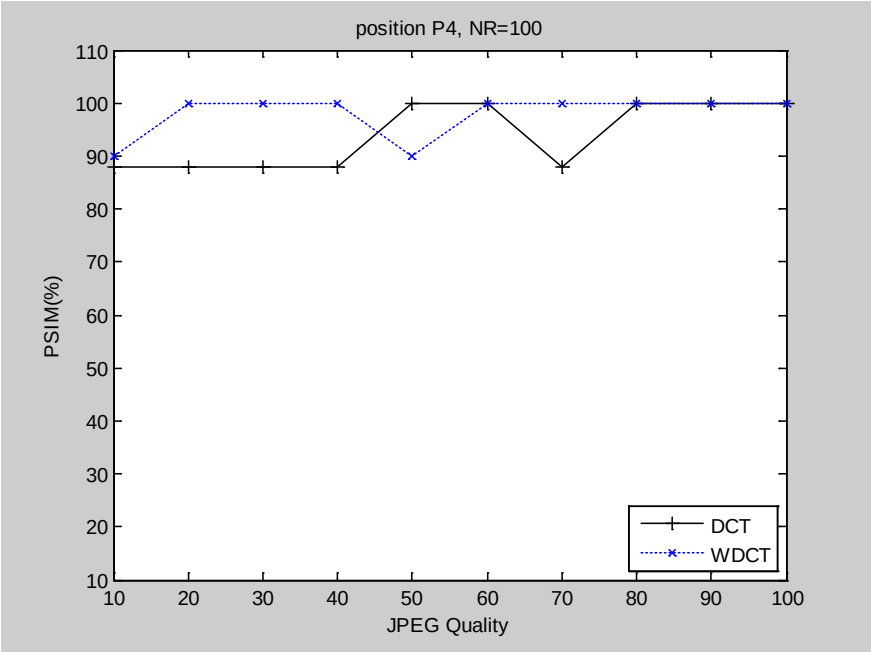


Figure .IV.34. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P4*, *NR*=100

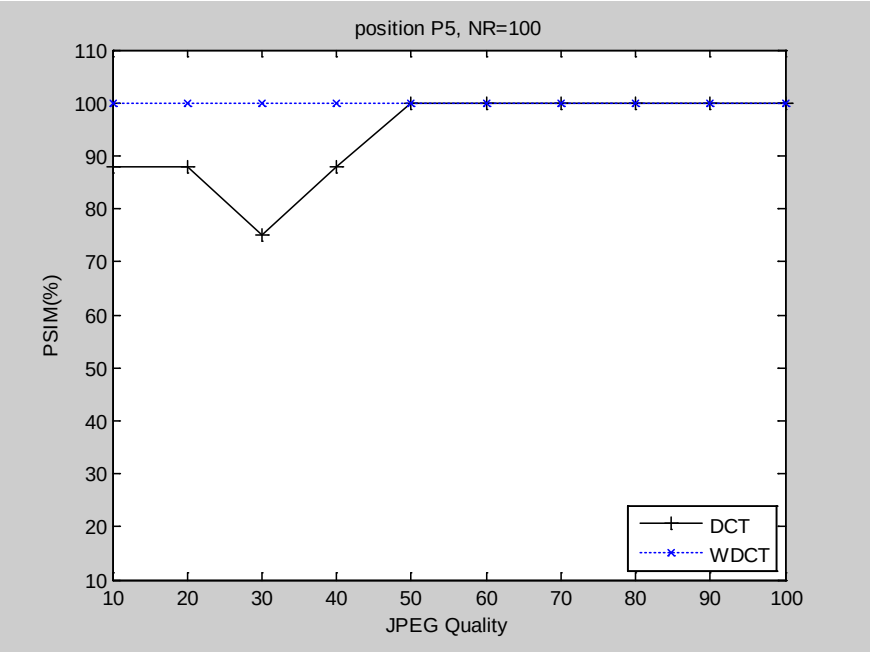


Figure .IV.35. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P5*, *NR*=100

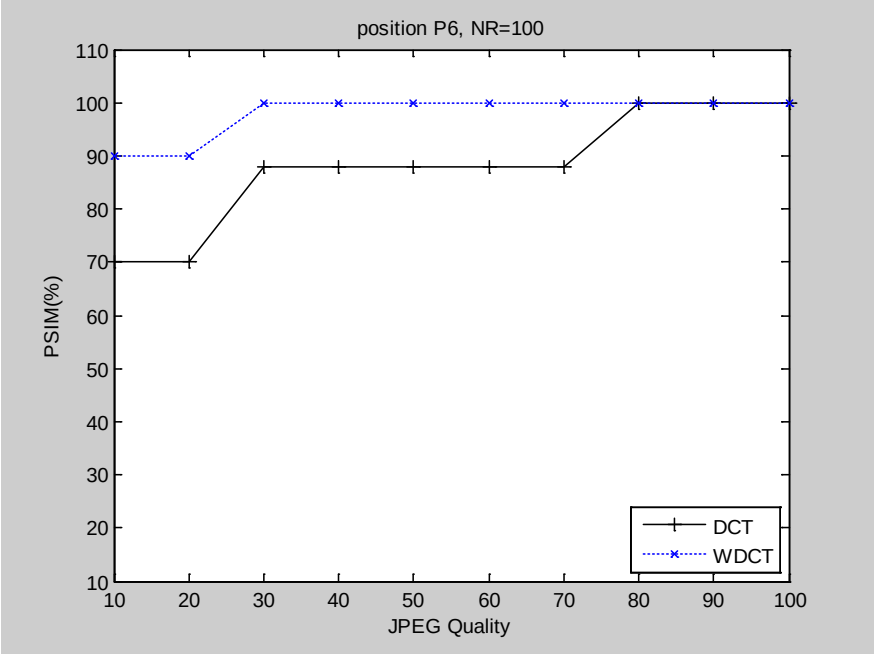


Figure .IV.36. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P6*, *NR*=100

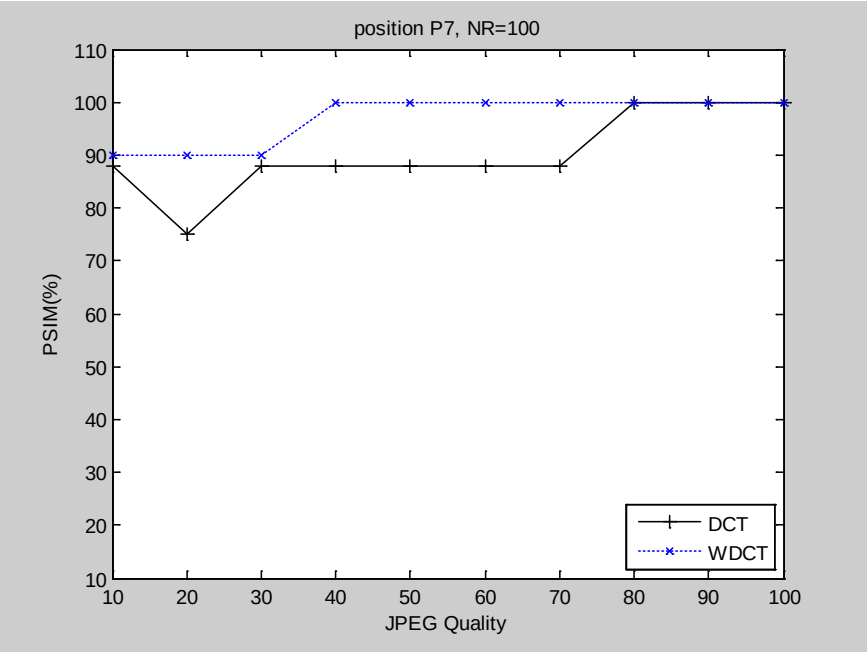


Figure .IV.37. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P7*, *NR*=100

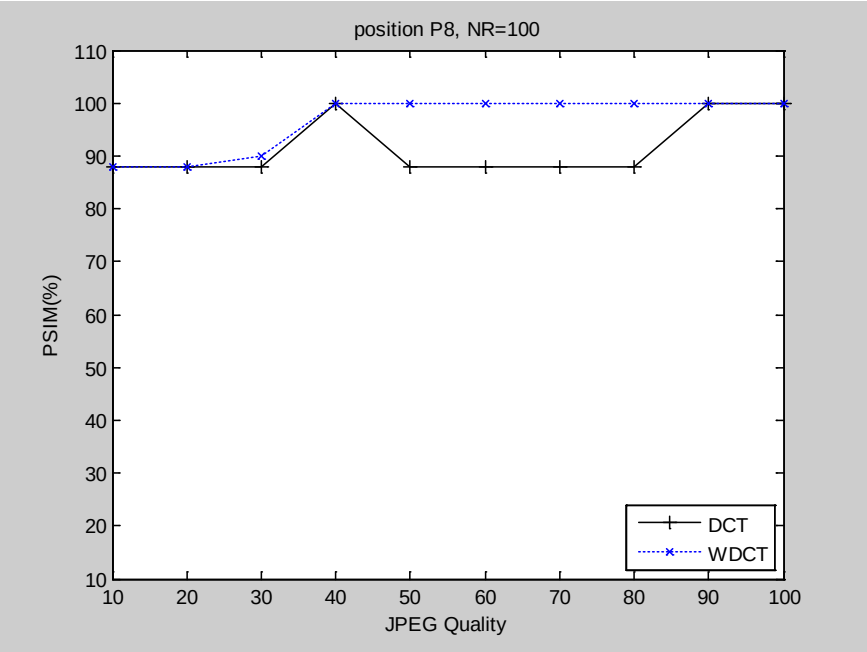


Figure .IV.38. Robustesse de la marque vis-à-vis la compression *JPEG* pour la position *P8*, *NR*=100

En comparant ces résultats à ceux obtenus pour *NR*=20, on peut constater l'apport de l'augmentation de *NR* sur l'amélioration du *PSIM* pour différents taux de compression. C'est tout à fait normal, parce que l'augmentation de *NR*, induit une augmentation de la présence de

la marque dans l'image et par conséquent une croissance de la chance d'avoir une similaire à la marque originale. Mais cette augmentation de *NR* ne doit pas se faire au détriment de la qualité de l'image. En effet, en se référent aux résultats des figure (IV.17) et (IV.18), on peut constater qu'on doit éviter d'insérer la marque, avec de grandes valeurs de *NR*, dans les positions *P0* et *P1* correspondantes aux très basses fréquences.

IV.2.2.3. Test de la robustesse vis-à-vis de l'ajout de bruit Gaussien

Cette fois ci, nous allons étudier la robustesse de la marque vis-à-vis de l'ajout d'un bruit. L'image marquée à la position *P2* (*P2* est l'une des positions optimales d'insertion de la marque) est attaquée par un ajout de bruit Gaussien de valeur moyenne nulle et à des niveaux d'énergie différents. Ensuite la marque extraite de l'image bruitée est comparée à la marque originale. La figure (IV.39) illustre les résultats donnant le *PSIM* pour différentes variances du bruit Gaussien additif. Comme nous pouvons le constater, les images marquées par la méthode *DWT+DCT* sont plus robustes à l'ajout d'un bruit Gaussien que celles marquées par la *DCT* seule. C'est tout à fait logique, parce que dans le cas de la *DWT+DCT*, les blocs marqués font partie de la sous bande (*LL*) qui représente les basses fréquences de l'image. Par contre dans le cas *DCT* seule, les blocs marqués appartiennent à l'image complète avec toutes ses composantes fréquentielles.

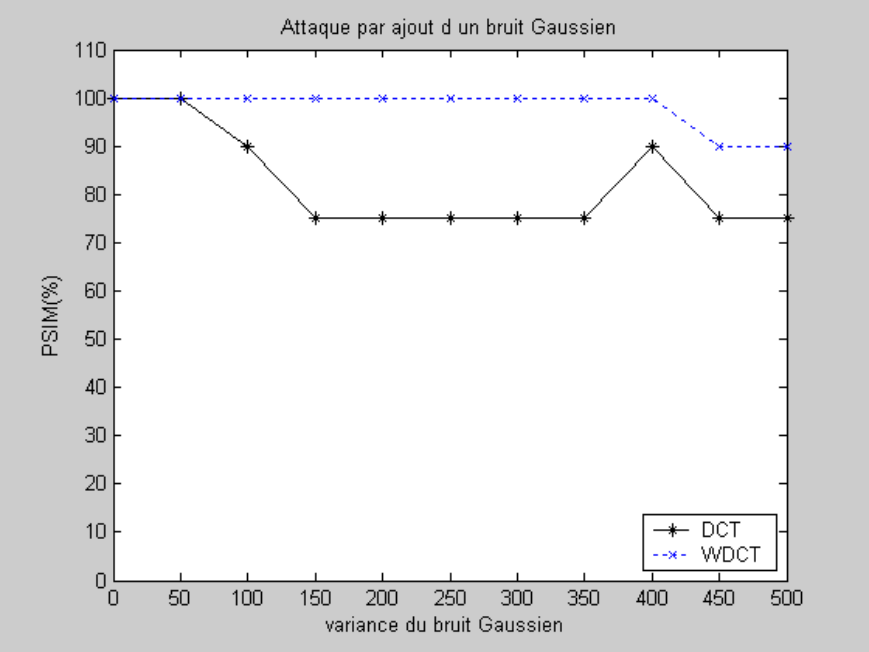


Figure .IV.39. Robustesse de la marque vis-à-vis de l'attaque par bruit Gaussien

IV.2.3. Conclusion

Ce travail est une amélioration de la méthode qu'on a déjà présenté dans la première partie et qui se base uniquement sur la *DCT*. Nous avons développé une méthode hybride combinant deux transformées la *DWT* et la *DCT*. En effet, cette approche permet la mise à disposition d'un espace transformé adéquat pour l'insertion de la marque. Cet espace est formé de la sous-bande basse fréquences (*LL*), obtenue par la *DWT* et assurant la robustesse vis-à-vis des taux de compression élevés ainsi que l'ajout de bruit Gaussien. L'objectif de l'application de la deuxième transformée *DCT* c'est de séparer les basses, les moyennes et les hautes fréquences de la sous-bande (*LL*) d'origine basse fréquences. De cette façon nous avons élargi le champ d'insertion de la marque qui était très limité dans la première méthode. Cet élargissement procure 9 positions d'insertions disposées en zigzag (principe utilisé en compression *JPEG*). D'après les testes effectués, les positions P2, P3, P4 et P5 sont jugées d'être optimales pour l'insertion de la marque et assurant un compromis entre l'invisibilité et la robustesse. Les résultats obtenus témoignent des performances de la méthode développée en termes de robustesse vis-à-vis la compression *JPEG* et l'ajout de bruit Gaussien. Cette méthode est aussi robuste au changement de formats et à la conversion de l'image marquée en niveaux de gris. Cependant, la méthode proposée peut être améliorée par exemple :

- Utilisation de la *DWT* à plusieurs niveaux.
- Insertion d'une marque sous forme d'une image binaire.
- Extension à d'autres attaques.

IV.3. Méthode de Watermarking Résistante aux Transformations Géométriques (RST) et la Compression, Basée sur la DWT, LPM et la Corrélation de Phase.

IV.3.1. Introduction

Alors que de nombreuses méthodes de watermarking fonctionnent bien dans le cas des attaques de compression, mais elles manquent de robustesse vis-à-vis les transformations géométriques. La rotation et la mise à l'échelle sont considérées parmi les attaques les plus difficiles. En effet, la principale difficulté dans ces attaques géométriques est la perte de synchronisation dans la détection de la marque. Ainsi, la détection échoue même si la marque existe encore dans l'image marquée.

Le travail présenté dans cette partie propose une autre approche hybride de watermarking pour des images fixes. Elle vise en particulier la robustesse vis-à-vis la compression et les transformations géométriques élémentaires (*RST* : Rotation, Changement d'échelle et Translation). Elle est basée sur l'utilisation de la transformée en ondelette discrète (*DWT*), la transformée logo-polaire et la corrélation de phase. Afin d'être robuste à la compression, la marque est insérée dans l'amplitude de la transformée de Fourier discrète (*DFT*) de la sous-bande basse fréquences (*LL*) obtenue par la *DWT*. En outre, pour être robuste aux transformations géométriques (RST), on a utilisé un espace invariant à ces transformations obtenu par la transformée de Fourier-Mellin (*FMT*). Pour l'extraction de la marque, et à travers une corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée, on calcule le déplacement causé par les transformations géométriques (*RST*). La correction de ce déplacement permet de synchroniser la détection de la marque.

Dans ce qui suit nous présenterons quelques travaux en relation avec notre approche, puis nous rappellerons quelques notions théoriques en relation avec le travail réalisé. Ensuite, et après avoir décrire la méthode développée, nous discuterons les résultats de tests effectués.

IV.3.2. Travaux en relation avec l'approche développée

Récemment, de nombreuses techniques de tatouage numérique ont été proposées qui sont orientés vers des attaques géométriques. Dans certaines approches un motif supplémentaire est inséré dans l'image en même temps que le watermark de manière à être en mesure de revenir à l'attaque géométrique. Il existe également des méthodes de watermarking, où les processus d'insertion et de détection ont lieu dans un domaine qui est invariant aux transformations géométriques.

Pour faire face aux problèmes de rotation et de changement d'échelle, O Ruanaidh et al. [69] préconisent l'usage de la transformée de Fourier-Mellin (*FMT*). Dans leur approche, la transformée de Fourier discrète (*DFT*) d'une image est calculée et ensuite la transformée de Fourier-Mellin est réalisée sur l'amplitude, le watermark est inséré dans l'amplitude de la

transformée résultante. L'image marquée est reconstruite en effectuant les transformations inverses, à savoir une *DFT* inverse et *FMT* inverse, après avoir utilisé la phase initiale. Le watermark inséré peut être extrait en transformant l'image marquée dans le domaine invariant aux *RST*. Depuis lors, les difficultés liées à la mise en œuvre pratique des idées contenues dans [69] ont été expérimenté par de nombreux chercheurs.

Pereira *et al* ont proposé dans [130] l'insertion de deux watermark, un modèle et un message à étalement de spectre contenant les informations. Le modèle en lui-même ne contient aucune information, mais sert à détecter les transformations subies par l'image. La dégradation de la qualité de l'image est l'un des problèmes major de cette approche.

Lin *et al.* [128] ont proposé un algorithme de tatouage basé sur la *FMT* qui peut être effectivement appliqué à des situations concrètes. Ce système appartient à la classe des techniques du domaine transformé détectables. En effet, pour réaliser une robustesse vis-à-vis les transformations géométriques sans passer par leur identification et inversion, ils proposent d'insérer le watermark dans un signal unidimensionnel et invariant à la translation et aux changements d'échelle. Ce signal est obtenu de la manière suivante : en premier lieu une *DFT* est appliquée à l'image, puis suivie d'une conversion en coordonnées logo-polaire des valeurs de l'amplitude. Enfin, une sommation d'une fonction de ces grandeurs sur l'axe du logarithme du rayon. L'inconvénient de ce système est la recherche exhaustive qui prend du temps.

B. Kim *et al.* [131] ont proposé un schéma de tatouage qui est mis en œuvre par l'amélioration de la normalisation de l'image fondée sur le watermarking (*INW : Image Normalization Based Watermarking*). La normalisation d'image est basée sur les moments de l'image, ainsi le centroïde invariant (*IC*) est proposé et seule la région centrale (R), qui a moins de possibilité de recadrage par *RST*, est utilisée pour la normalisation.

Dans [132], J. et H. Zhang Xuan ont proposé une méthode de watermarking robuste aux transformations géométriques (*RST*). L'insertion de la marque se fait dans un domaine invariant aux RST. Cette invariance est basée d'une part sur les propriétés de translation et de rotation de la transformée de Radon, et d'autre part sur l'invariance à la translation de l'amplitude de la transformée de Fourier.

L'approche de Z. Dong [133] utilise aussi le principe de l'espace invariant. Elle consiste en l'insertion de la marque dans le *LPM* du spectre d'amplitude de la transformée de Fourier de l'image originale.

F.K. Mohamed et R. Abbes ont proposé dans [134] un schéma de tatouage basé sur le logo insertion, dans le domaine transformé *DCT*, en utilisant des techniques de normalisation de l'image. Le watermark n'est pas inséré directement dans l'image normalisée. Cependant,

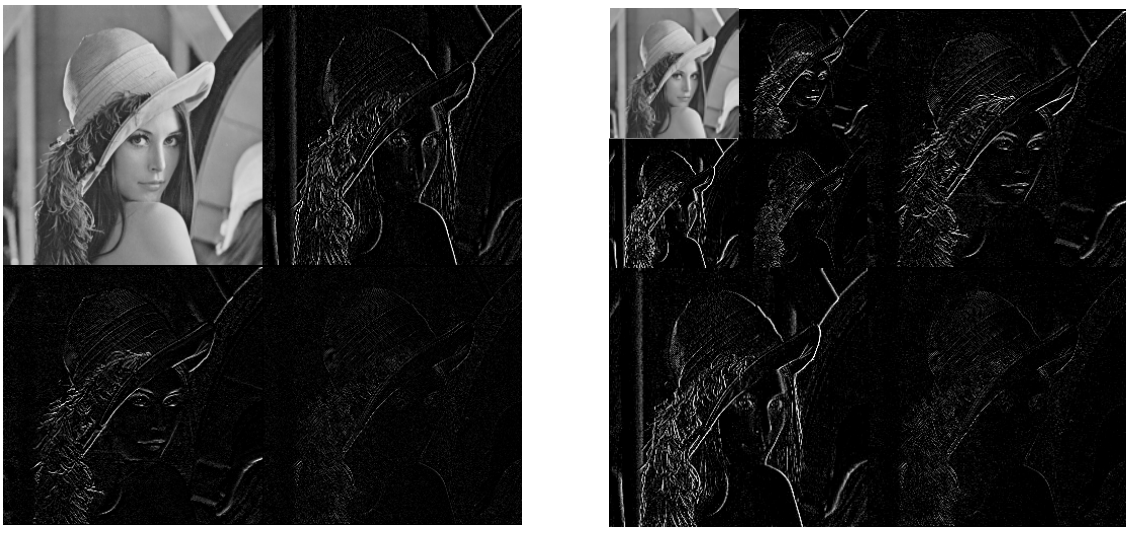
cette normalisation d'image est simplement utilisée pour calculer les paramètres de la transformation affine de telle sorte que l'incrustation du watermark et sa détection soient effectuées dans le système de coordonnées initial.

IV.3.3. Rappel de quelques transformées en relation avec l'approche développée

Dans cette section nous rappellerons quelques notions et transformées utilisées pour le développement de la méthode de watermarking proposé. Pour plus de détails voir la section (III.3.2) du chapitre 3.

a. La transformé en ondelettes discrète *DWT*

L'application de la *DWT* à une image consiste en sa décomposition en quatre sous-bandes. La sous-bande (*LL*) est le résultat de l'application d'un filtrage passe-bas dans les deux directions horizontale et verticale. Les deux sous-bandes de détails (*LH*) et (*HL*) sont obtenues en appliquant un filtrage passe-bas (haut) dans la direction horizontale et un filtrage passe-haut (bas) dans la direction verticale. La sous-bande (*HH*) est le résultat d'un filtrage passe-haut effectue horizontalement et verticalement. Cette procédure est appliquée, d'une manière itérative, à la sous-bande (*LL*) jusqu'à l'obtention de niveau de décomposition désiré comme il est indiqué sur l'exemple de la figure (IV.40).



a. Niveau 1 b. Niveau 2

Figure IV.40. Exemple de décomposition d'une image par la *DWT*

b. Transformée de Fourier Discrète *DFT*

Dans la pratique une image est obtenue par échantillonnage et elle est de taille finie. La *DFT* (transformée de Fourier discrète), ainsi que sa transformée inverse *IDFT*, d'une image *f(x, y)* de taille *M* x *N* sont données comme suite [135]:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\, e^{-j2\pi(ux/M+vy/N)} \quad ..(IV.39)$$

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v)\, e^{j2\pi(ux/M+vy/N)} \quad ..(IV.40)$$

Le spectre d'amplitude et l'angle de phase sont données par :

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \quad .....(IV.41)$$

$$\phi(u,v) = \tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right] \quad .....(IV.42)$$

Où *R (u, v)* et *I(u, v)* sont respectivement les parties réelle et imaginaire de *F(u, v)*

Dans ce qui suit nous donnons quelques propriétés de la *DFT* vis-à-vis les transformations géométriques effectués dans le domaine spatial.

1. Supposant que l'image $f_1(x, y)$ est le résultat d'une rotation, d'un angle θ dans le domaine spatial, de l'image originale $f_0(x, y)$:

$$f_1(x,y) = f_0((x\cos\theta + y\sin\theta),(-x\sin\theta + y\cos\theta)) \quad ..(IV.43)$$

$F_1(u, v)$ et $F_0(u, v)$, qui sont respectivement les transformées de Fourier de $f_1(x, y)$ et $f_0(x, y)$, sont reliés par la relation suivante :

$$F_1(u,v) = F_0((u\cos\theta + v\sin\theta),(-u\sin\theta + v\cos\theta)) \quad ..(IV.44)$$

De l'équation (IV.44), on peut constater que la rotation d'une image d'un angle θ dans le domaine spatial engendre une rotation du même angle dans le domaine fréquentiel.

2. Un changement d'échelle dans le domaine spatial se traduit par un effet inverse dans le domaine fréquentiel :

$$TF[f(ax,by)] = \frac{1}{|a.b|}F\left(\frac{u}{a},\frac{v}{b}\right) \quad .....(IV.45)$$

Où *a* et *b* sont respectivement les facteurs de changement d'échelle le long des axes *X* et *Y*.

3. Supposant que *F(u,v)* est la transformée de Fourier d'une image *f(x, y)*. La translation dans le domaine spatial de cette image entrainera un décalage linéaire de la phase de *F(u ,v)* par contre son amplitude est conservée comme il est indiqué par l'équation (IV.46) :

$$TF\left[f(x+x_0, y+y_0)\right] = F(u,v)\, e^{j2\pi(x_0\frac{u}{M}+y_0\frac{v}{N})} .(IV.46)$$

Maintenant, considérons les trois transformations géométriques ensemble (une translation, une rotation et un changement d'échelle) dont les paramètres sont respectivement (x_0, y_0), α et σ. Supposons que $F_0(u, v)$ est la transformée de l'image originale $f_0(x, y)$ et $F_1(u, v)$ celle de l'image transformée $f_1(x, y)$. La relation entre les amplitudes des deux transformées est donnée par [69][128] :

$$\left|F_1(u,v)\right| = \left|\sigma\right|^{-2}\left|F_0(\sigma^{-1}(u\cos\alpha + v\sin\alpha), \sigma^{-1}(-u\sin\alpha + v\cos\alpha)\right| .....(IV.47)$$

Comme on peut le constater le module de $F_1(u, v)$ ne dépend pas des paramètres de translation (x_0, y_0), ce que assure l'invariance à la translation.

c. Le passage au domaine logo-polaire ou *LPM*

Dans une représentation logo-polaire les pixels d'une image sont indexés par un numéro d'anneau *R* et un numéro de rayon *W* qui sont liés aux coordonnées ordinaires x, y par les relations suivantes [136] :

$$r = \left[(x-x_c)^2 + (y-y_c)^2\right]^{1/2} .....(IV.48)$$

$$\theta = \tan^{-1}\frac{y-y_c}{x-x_c}$$

$$R = \frac{(n_r - 1)\log(r/r_{\min})}{\log(r_{\max}/r_{\min})} .....(IV.49)$$

$$W = \frac{n_w\theta}{2\pi}$$

Avec : (r, θ) représentent les coordonnées polaires.

(x_c, y_c) la centre du modèle d'échantillonnage logo-polaire.

n_r et n_w sont respectivement le nombre d'anneaux et de côtes.

r_{min} et r_{max} correspondent respectivement au plus petit et au plus large rayon des anneaux. Nous définissons le rayon logo-polaire par :

$$\rho = \ln r \text{.....} (IV.50)$$

Pour garantir l'invariance à la rotation et au changement d'échelle, l'amplitude $|F_1(u,v)|$ de la *DFT* de l'image est échantillonnée en utilisant les coordonnées polaire définies par :

$$u = e^{\rho} \cos\theta \text{.....} (IV.51)$$
$$v = e^{\rho} \sin\theta \text{.....} (IV.52)$$

Où $\rho \epsilon R^+$ et$0 \leq \theta \leq 2\pi$

En substituant les équations ci-dessus dans l'équation (IV.47) nous obtenons :

$$|F_1(u,v)| = |\sigma|^{-2} |F_0(\sigma^{-1} e^{\rho} \cos(\theta - \alpha), \sigma^{-1} e^{\rho} \sin(\theta - \alpha)\ |...(IV.53)$$

L'équation (IV.53) peut être facilement rendue sous la forme :

$$|F_1(\rho,\theta)| = |\sigma|^{-2} |F_0(\rho - \log\sigma, \theta - \alpha)|...(IV.54)$$

Comme on peut le constater, dans le système de coordonnées (ρ, θ), le changement d'échelle et la rotation se sont convertis à des translations de ρ et θ respectivement. Le changement d'échelle se traduit par un décalage, le long de l'axe du rayon logo-polaire ρ, d'une quantité logσ. Quand à la rotation elle se traduit par un décalage cyclique, le long de l'axe des angles θ, d'une quantité α. Par contre, la translation n'a aucun effet dans le domaine logo-polaire.

d. La transformée de Fourier-Mellin (*FMT*)

L'application d'une deuxième *DFT* à l'amplitude de la première *DFT*, représentée dans le plan logo-polaire (ρ, θ), permet de contourner les translations dans ce plan. Cette opération est connue sous le nom de la transformée de Fourier-Mellin. Maintenant si nous appliquons la transformée de Fourier aux deux termes de l'équation (IV.54), et selon la propriété de translation de cette transformée, nous obtiendrons :

$$I_1(\omega_\rho, \omega_\theta) = |\sigma|^{-2} e^{-j(\omega_\rho . \log\sigma + \omega_\theta . \alpha)} I_0(\omega_\rho, \omega_\theta) (IV.55)$$

L'amplitude de la transformée de Fourier des deux *LPM* est relié par :

$$\left|I_1(\omega_\rho,\omega_\theta)\right| = |\sigma|^{-2}\left|I_0(\omega_\rho,\omega_\theta)\right| \text{.....} (IV.56)$$

La différence de phase entre les deux LPM est étroitement lié à leur déplacement, elle est donnée par :

$$e^{j(\omega_\rho.\log\sigma+\omega_\theta.\alpha)} \text{.....} (IV.57)$$

L'équation (IV.56) démontre que l'amplitude de la transformée de Fourier-Mellin est invariante à la rotation et la translation. Mais elle est multipliée par un facteur $|\sigma|^{-2}$ causé par le changement d'échelle. Ce facteur n'aura pas d'effet si on utilise une corrélation normalisé lors de la détection des déplacements provoqué par les transformations *RST*.

e. La corrélation de phase

La corrélation de phase est l'une des approches les plus efficaces permettant la rectification de la position du watermark tout en évitant les recherches exhaustives. C. D. Kuglin et D. C. Hines ont proposé dans [137] une corrélation de phase basée sur la propriété de la transformée de Fourier donnée par le théorème de décalage. Etant donnée l'image f_0 et sa version transformée f_1 translatée de (x0, y0) :

$$f_1(x,y) = f_0(x-x_0, y-y_0) \text{.....} (IV.58)$$

Donc la relation entre leurs transformées de Fourier F_0 et F_1 est la suivante :

$$F_1(u,v) = e^{-j(ux_0+vy_0)}F_0(u,v) \text{.....} (IV.59)$$

Le spectre cross-power (*Cross-Power Spectrum*) des deux images est donnée par :

$$C = \frac{F_1(u,v).F_0^*(u,v)}{\left|F_1(u,v).F_0^*(u,v)\right|}e^{j(ux_0+vy_0)} \text{.....} (IV.60)$$

Avec *F** c'est le conjugué complexe de *F*.

La propriété de translation garantie que la phase du spectre du cross-power est équivalente à la différence de phase entre les images. En plus, si nous représentons la phase du spectre du cross-power dans sa forme spatiale, c.-à-d. en prenant la transformée de Fourier inverse de la représentation dans le domaine fréquentiel :

$$D = IDFT(angle(C)) \quad \text{.....(IV.61)}$$

Où *angle (C)* c'est la phase de *C*, et *IDFT* c'est la transformée de Fourier inverse.

L'une des propriétés de la transformée de Fourier stipule que : la transformée de Fourier de la fonction $\delta(x-d)$ est $e^{-j\omega d}$. L'équation (IV.61) donne deux fonctions δ centrées à l'endroit de déplacement. Donc *D* est une impulsion nulle partout sauf à l'endroit de déplacement.

f. L'interpolation

L'interpolation est une opération permettant d'estimer des valeurs en prenant la moyenne des valeurs connues aux points voisins. De nombreuses méthodes sont utilisées pour l'interpolation, tel que :

1. La méthode du plus proche (nearest) : la valeur d'un point interpolé est la valeur du point le plus proche.
2. Bilinéaire : la valeur d'un point interpolé est une combinaison des valeurs des quatre points les plus proches.
3. Bicubique : la valeur d'un point interpolé est une combinaison des valeurs des seize points les plus proches.

La méthode bilinéaire est plus rapide et moins nécessiteuse en mémoire que bicubique, et produit une surface plus lisse que la méthode du plus proche. Par conséquent, la plupart des applications utilisent une interpolation bilinéaire. Ici, nous donnons un exemple sur l'interpolation bilinéaire utilisée lors du passage au *LPM*. Chaque point dans le spectre d'amplitude log-polaire est calculé à partir d'une moyenne pondérée de quatre points du spectre d'amplitude représenté dans le plan cartésienne comme il est indiqué par l'équation (IV.62) et la figure (IV.41)

$$\begin{aligned} P(\rho,\theta) = {} & C(x,y).(1-a).(1-b) \\ & + C(x,y+1).(1-a).b \\ & + C(x+1,y).a.(1-b) \\ & + C(x+1,y+1).a.b \end{aligned} \qquad \text{(IV.62)}$$

C(x, y), C(x, y+1), C(x+1, y) et *C(x+1, y+1)* sont quatre points du plan cartésienne, $P(\rho,\theta)$ (*P* dans la figure (IV.41)) est le point correspondant à l'intérieur de carré spécifié par les quatre points, a et b représente la différence de coordonnée entre les points *P* et *C(x, y)* sur les axes *X* et *Y* respectivement.

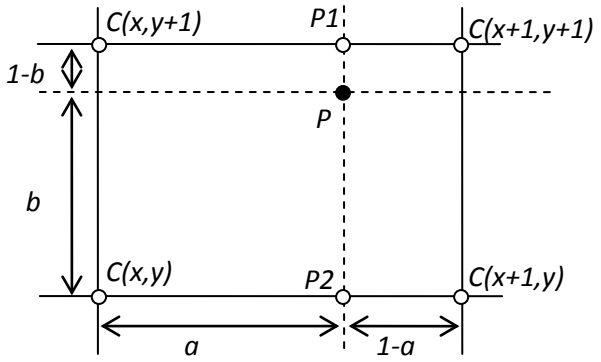


Figure IV.41 Exemple d'interpolation Bilinéaire

IV.3.4. Description de la méthode développée

L'approche que nous présentons dans cette partie est aussi hybride et basée sur l'utilisation de plusieurs transformées. En premier lieu, une *DWT* est appliquée à l'image à marquer, puis seule la sous-bande (*LL*) est utilisée et subie une transformation *DFT*. L'amplitude de cette dernière est transformée dans un plan logo-polaire en subissant une *LPM*. L'insertion se fait d'une manière substitutive ce qui classe la méthode proposée dans la catégorie des schémas substitutifs. La détection de la marque passe par une étape de correction qui se base sur l'utilisation de la corrélation de phase. Cette correction permet de synchroniser l'image marquée et l'image originale et par conséquent l'extraction de la marque.

Donc comme tout système de watermarking, la méthode proposée se compose de deux phases qui sont : la phase d'insertion de la marque et la phase de sa détection.

IV.3.4.1. Insertion de la marque

Pour assurer la robustesse vis-à-vis la compression, on a choisi de travailler sur l'amplitude de la *DFT* de la sous-bande (*LL*) obtenue par une *DWT*. En plus, et en vue de résister aux transformations géométrique (*RST*), l'endroit d'insertion de la marque est calculé par une approximation logo-polaire inverse (*ILPM*) des positions choisis dans le domaine *LPM* de l'amplitude *DFT* de la sous-bande (*LL*). Comme il est illustré sur la figure (IV.42), pour chaque point choisi dans le domaine *LPM* correspond quatre points (*FCP*) dans le domaine cartésienne de l'amplitude *DFT* obtenue par l'approximation *ILPM* (équation IV.62). Donc, l'insertion de la marque par le changement des valeurs des quatre points dans le domaine *DFT* conduit à un changement de la valeur du point correspondant dans le domaine *LPM*. Dans le but de maintenir la symétrie de l'amplitude *DFT*, les points symétriques (*SP*) des quatre points calculés doivent être changés de la même manière.

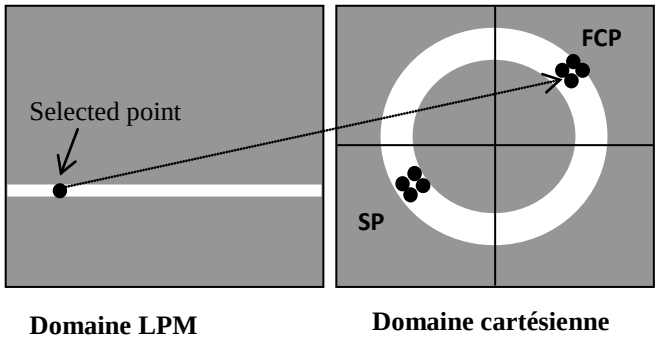


Figure VI.42 La région choisie pour l'insertion de la marque

L'invisibilité de la marque est assurée par le choix de la région des moyennes fréquences de l'amplitude de la transformée *DFT* de la sous-bande basse fréquences (*LL*).

Donc la procédure d'insertion de la marque, comme il indiqué sur la figure (IV.43), se compose des étapes suivantes :

1. choisir une marque, sous forme de séquence de bits, dont la taille déterminera le nombre de points nécessaires à son insertion,
2. calculer la transformée *DWT* de l'image originale (niveau de gris),
3. calculer la transformée *DFT* de la sous-bande (LL_0),
4. transformer l'amplitude de la *DFT* du domaine cartésienne au domaine *LPM*,
5. selon la taille de la marque sélectionner un ensemble de points dans le domaine *LPM*,
6. pour chaque point choisi dans le domaine *LPM*, et en utilisant l'approximation logo-polaire inverse (*ILPM*), calculer les quatre points (*FCP*) correspondant dans le domaine cartésienne de l'amplitude de la *DFT* ainsi que leurs points symétriques (*SP*),
7. insérer la marque, dans l'amplitude *DFT*, en effectuant un changement des valeurs correspondantes aux points (*FCP*) et (*SP*) et ceci selon l'état de bit de la marque,
8. calculer la transformée de Fourier inverse *IDFT*, en utilisant l'amplitude obtenue dans l'étape 7 et la phase originale. Le résultat est la sous-bande marquée (LL_M),
9. appliquer la transformée en ondelette inverse *IDWT* pour obtenir l'image marquée.

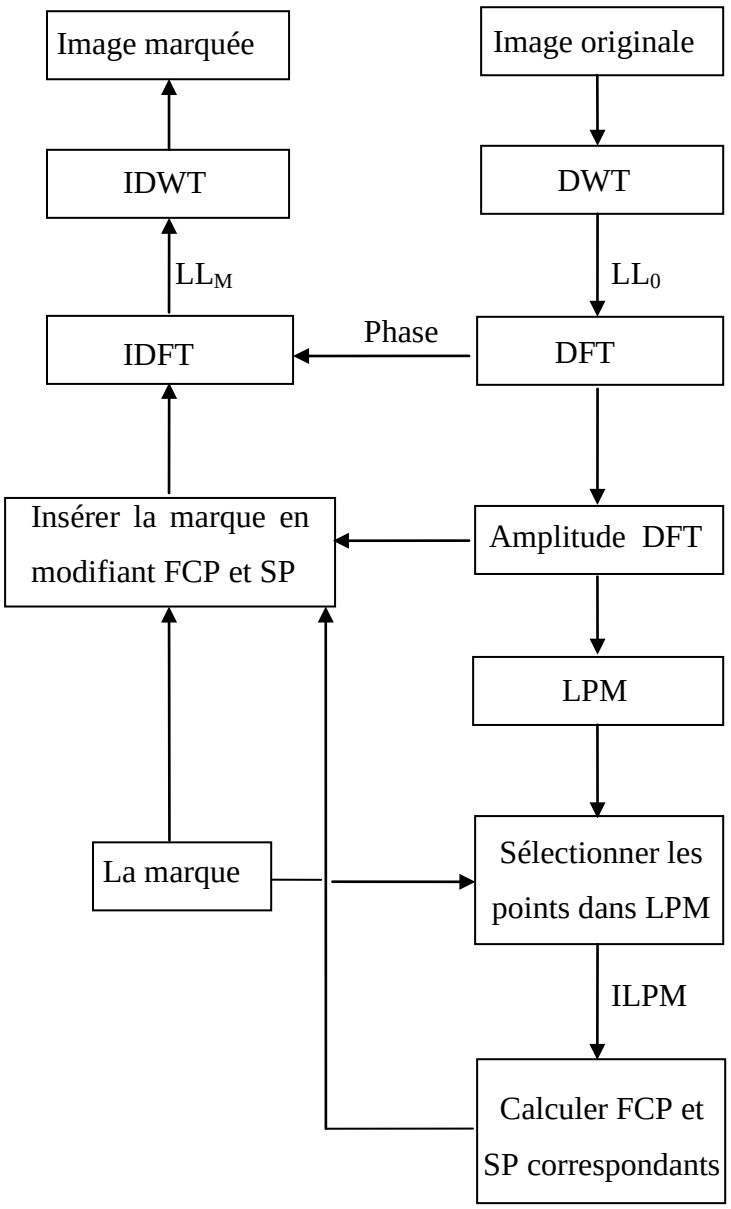


Figure VI.43 Diagramme du processus d'insertion de la maque

IV.3.4.2. Extraction de la marque

La méthode développée fait partie des schémas substitutifs informés c.-à-d. la nécessité de la présence de l'image originale lors de l'extraction ou la détection de la marque. En effet, une corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée, qui a éventuellement subie des transformations géométriques (*RST*), est calculée. Le résultat de la corrélation de phase permet de connaitre les déplacements qui identifient la ou les transformations que l'image ait subies. La correction de ces déplacements procure une synchronisation de la détection de la marque.

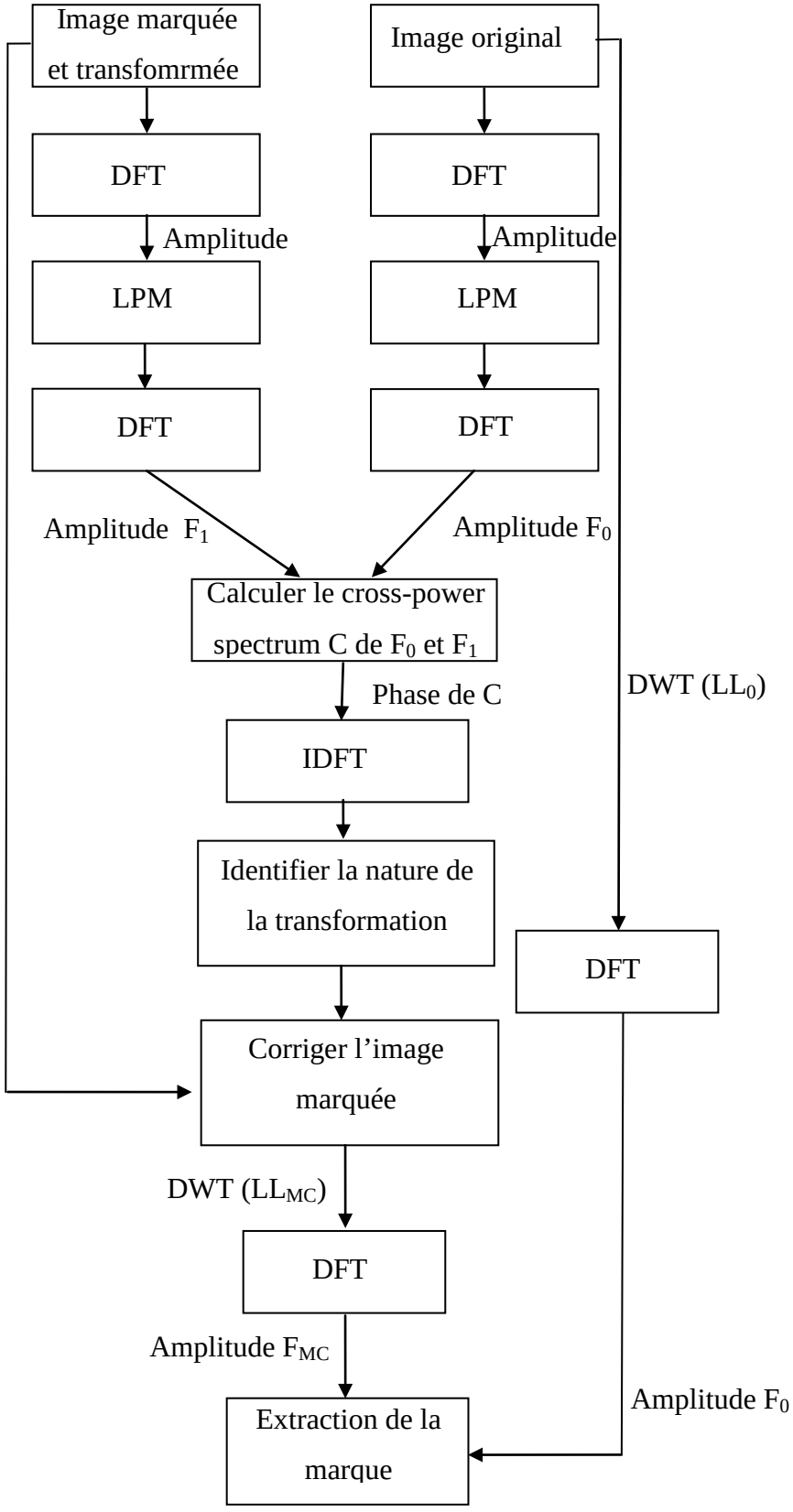


Figure IV.44 Diagramme du processus d'extraction de la marque

Les différentes étapes du processus d'extraction de la marque, illustré sur la figure (IV.44), sont comme suite :

1. appliquer la transformée *DFT* à l'image originale ainsi que l'image marquée (qui a éventuellement subi des transformations *RST*,
2. appliquer le *LPM* aux amplitudes des transformées obtenues dans 1,
3. appliquer une deuxième *DFT* aux résultats obtenus dans 2,
4. en utilisant l'équation (IV.60), calculer le spectre du cross-power *C* des deux *DFT* obtenues dans 3,
5. calculer la transformée *IDFT* de C donnée par l'équation (IV.61),
6. calculer le déplacement entre le *LPM* de l'image originale et celui de l'image marquée (transformée),
7. identifier la ou les transformations subies par l'image marquée,
8. corriger l'image marquée selon les déplacements calculés dans 6,
9. effectuer la transformée *DWT* pour l'image originale ainsi pour celle marquée et corrigée,
10. calculer la *DFT* des sous-bandes (LL_{MC}) et (LL_0),
11. à l'aide de la clé utilisé lors de l'insertion, déterminer les point concernés par le marquage,
12. à l'aide de la deuxième clé (façon de modifier les valeurs des points *FCP*) déterminer l'état de bit,
13. vérifier la similarité entre la marque originale et la marque extraite en utilisant la corrélation normalisée donnée par l'équation (IV.63). Si la valeur de cette corrélation est supérieure à un seuil on dira que la marque est extraite correctement si non la marque n'existe pas ou on n'arrive pas à l'extraire.

$$sim = \frac{W_0 x W_1^T}{\sqrt{\left(W_0 x W_0^T\right)\left(W_1 x W_1^T\right)}} \text{.....} (IV.63)$$

W_0 et W_1 sont respectivement la marque originale et la marque extraite

IV.3.5. Tests et interprétation des résultats

Dans cette section nous allons illustrer les performances de l'approche développée en termes de robustesse vis-à-vis les transformations géométrique élémentaires (translation, rotation et changement d'échelle) ainsi que d'autres attaques telles que la compression et

l'ajout du bruit. L'algorithme proposé, réalisé sous MATLAB, a été testé sur l'image en niveau de gris cameraman de taille 256x256.

IV.3.5.1. Test de l'invisibilité de la marque

Comme il est indiqué sur la figure (IV.45). L'image marquée de la figure (IV.45.a) est obtenue en insérant dans l'image originale figure (IV.45.b) une marque sous forme de séquence binaire de 10 bits. Par conséquent, le nombre de coefficient susceptibles d'être changer est de 80. La contrainte invisibilité est vérifiée parce que l'insertion de la marque est effectuée dans les coefficients moyens fréquences de l'amplitude de la *DFT* de la sous-bande (*LL*). Aucune différence n'est perceptible entre les deux images et la valeur du *PSNR* qui est de l'ordre de 62.32 témoigne de la très bonne qualité de l'image marquée.

a. Image originale Padded b. Image marquée

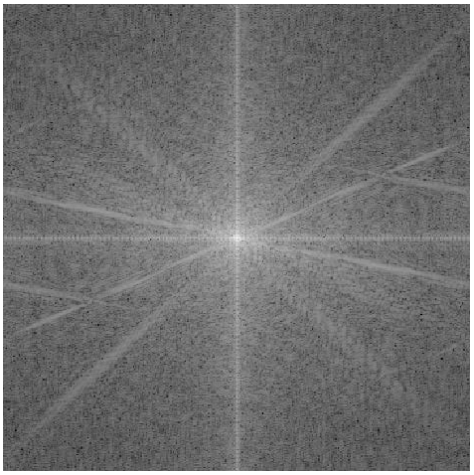
Figure VI.45. Vérification de la contrainte invisibilité

IV.3.5.2. Test de la robustesse vis-à-vis de la translation

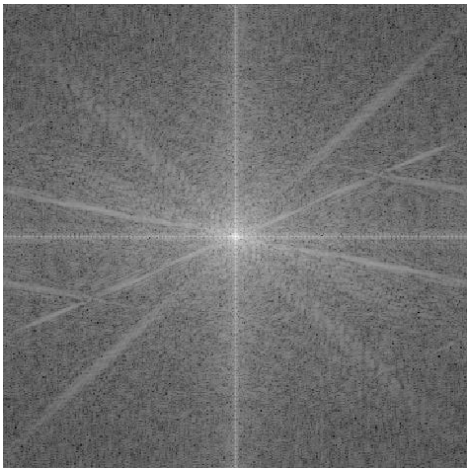
Comme nous l'avons déjà mentionné au début de cette partie, la méthode développée procure un domaine invariant à la translation. Cela est dû à la propriété de la transformée de Fourier (équation IV.47). Cela peut être constaté clairement sur la figure (IV.46), où l'image marquée (a) et celle marquée et translaté (b) possèdent le même spectre d'amplitude (c, d). Par conséquent, leurs transformées *LPM* sont identiques (e, f). L'image translatée est le résultat d'un décalage cyclique de l'image marquée. Donc, la totalité de l'information est conservée, voire figure (IV.47), et la marque est extraite avec succès quelque soit la translation subite par l'image.

a- Image marquée

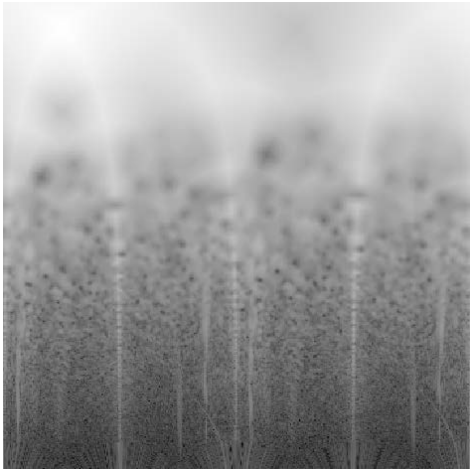
b- Image marquée et translatée



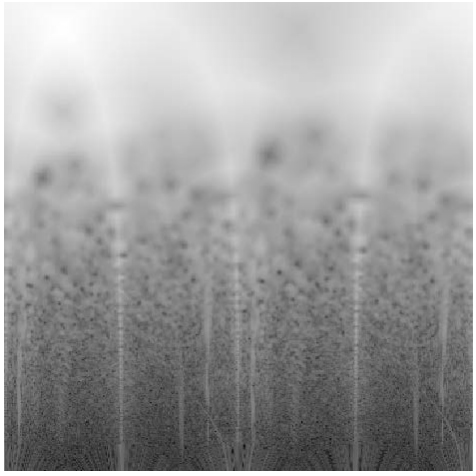
c- Spectre d'amplitude de l'image marquée



d- Spectre d'amplitude de l'image marquée translatée



e- *LPM* de l'image marquée



f- *LPM* de l'image marquée translatée

Figure IV.46 Exemple d'une translation par (50, 50)

Figure IV.47 Conservation de l'information de l'image

IV.3.5.3. Test de la robustesse vis-à-vis le changement d'échelle

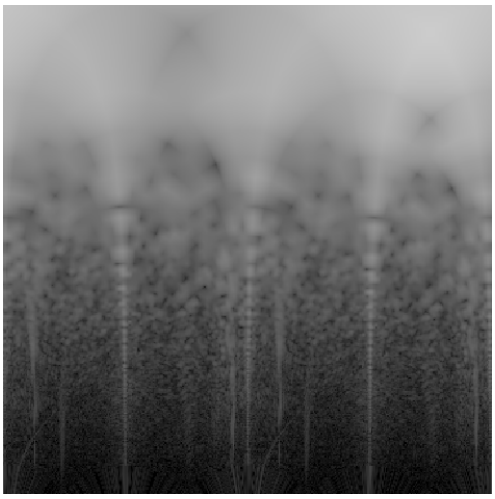
La figure (IV.48) illustre un exemple de changement d'échelle. L'image marquée de la figure (IV.48.a) a été réduite par un facteur de changement d'échelle *X* comme il est indiqué sur la figure (IV.48.b). Les transformées logo-polaires (*LPM*) des deux images sont données sur les figures (IV.48.c) et (IV.48.d) respectivement. La corrélation de phase entre les deux *LPM* est indiquée sur la figure (IV.48.e). Donc le problème consiste à déterminer la valeur de X pour pouvoir corriger l'image.

Comme on le constate sur les figures (IV.48.c, d), une transformation de type changement d'échelle se traduit par un décalage vertical dans le domaine *LPM*. L'évaluation du facteur d'échelle *X* se fait en calculant le déplacement des deux pics détectés dans le spectre de corrélation de phase (dans le cas de changement d'échelle, le déplacement a lieu uniquement sur les lignes). Pour l'exemple de la figure (IV.48), les deux pics sont détectés aux emplacements (41, 1) et (321, 1) ce que correspond à X=0.5.

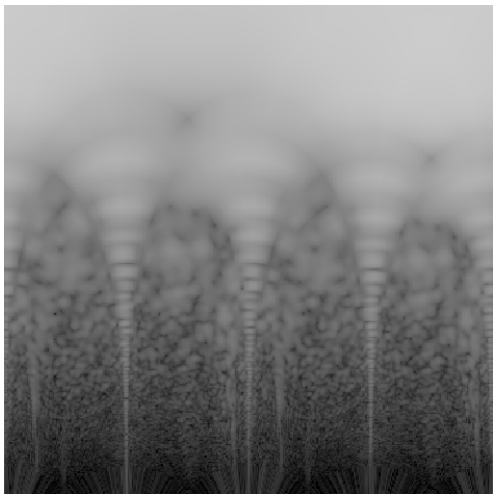
Pour synchroniser l'extraction de la marque, l'image transformée doit subir la transformation inverse qui consiste à l'agrandir d'un facteur égale à $1/X$. Dans le cas de l'exemple précédent, la similarité entre la marque originale et celle extraite est de 90%. La figure (IV.49) donne les résultats du pourcentage de similarité (*PSIM*) obtenus pour différents facteurs d'échelle.

a. Image originale

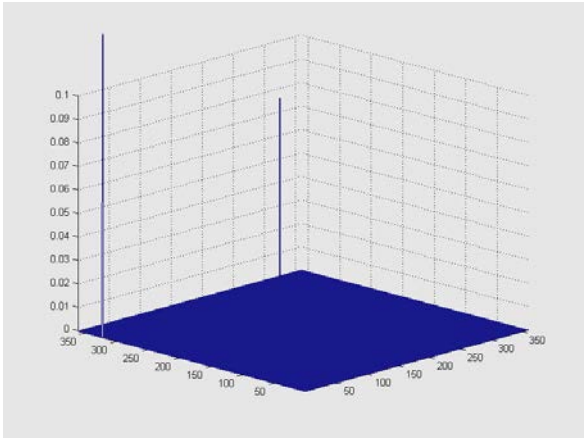
b. Image marquée et réduite par *X*



c- *LPM* de l'image originale



d- *LPM* de l'image marquée et réduite



e- Spectre de corrélation de phase entre les deux *LPM*

Figure IV.48 Exemple d'une image réduite d'un facteur *X*

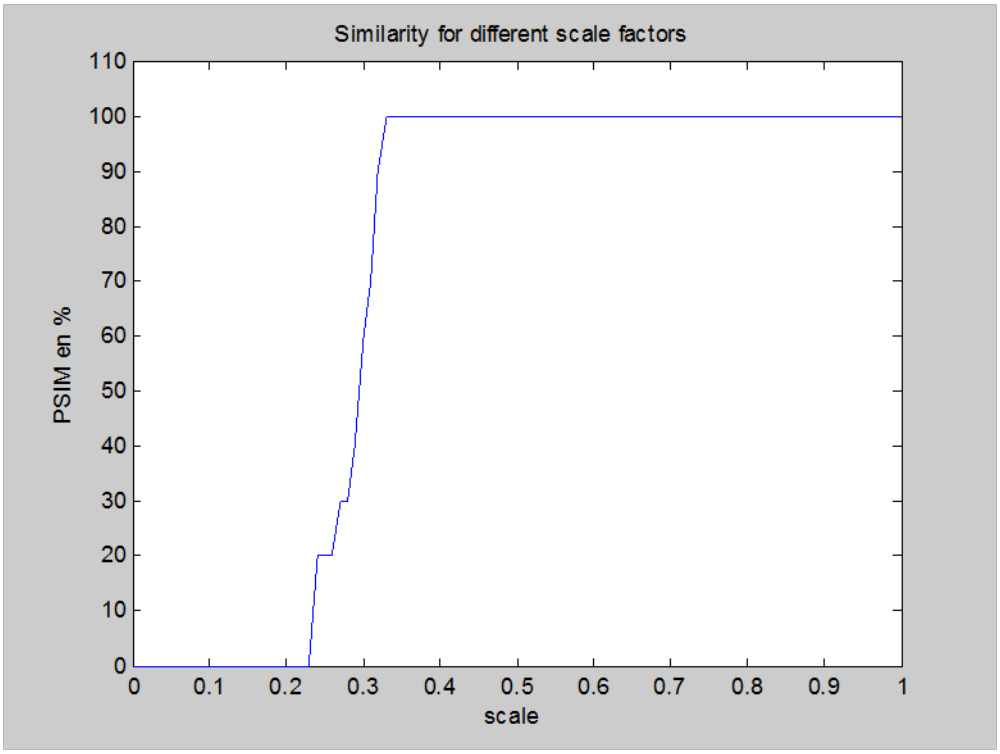


Figure IV.49 Le pourcentage de similarité *PSIM* pour différents facteurs d'échelles

IV.3.5.4. Test de la robustesse vis-à-vis de la rotation

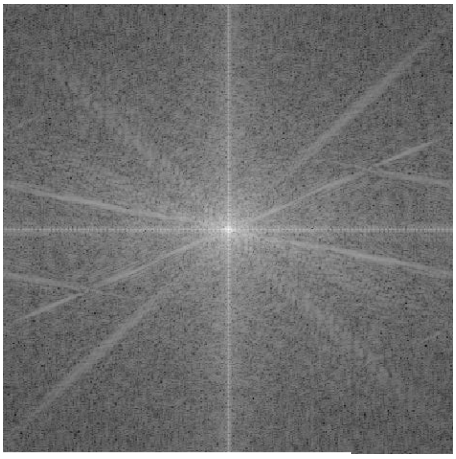
Comme l'image est délayée (*padded*) en fonction de sa taille, sa rotation avec recadrage et même avec un grand degré n'affectent pas sa taille et sa forme initiales. En d'autres termes, l'ensemble des informations de l'image est conservé. L'exemple donné dans la figure (IV.50) montre une image marquée (a) qui est entraîné en rotation avec un angle α inconnus (b). Nous devons donc déterminer cet angle à partir du déplacement calculé par la corrélation de phase entre le *LPM* de l'image originale et celui de l'image qui a subit la rotation (g). La marque sera extraite après avoir corrigé l'image tournée en appliquant la rotation inverse en conséquence à l'angle déterminé α.

Comme il est montré dans la figure (IV.50) (c, d), la rotation de l'image induit un spectre qui est tourné par le même angle. Cette rotation est transformée en une translation horizontale cyclique dans le domaine du *LPM* (voir la figure (IV.50) (e, f)). L'angle de rotation est évalué par le calcul du déplacement des deux pics détectés dans le spectre de la corrélation de phase (le déplacement n'a lieu que sur les colonnes comme illustré sur la figure (IV.51)). Pour l'exemple donné dans la figure (IV.50), les deux pics sont situés à (1, 71) et (1, 291) qui correspond à $\alpha = 70$ °. L'image pivotée subit une rotation de 70 ° dans le sens

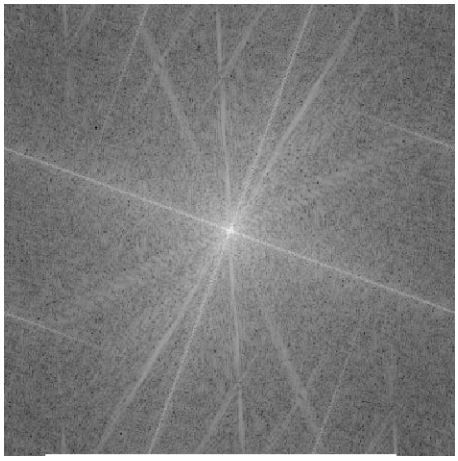
horaire. Ceci permet d'obtenir une synchronisation entre l'image originale et l'image marquée. Pour cet exemple, la similitude entre la marque originale et celle extraite est de 100%.

a. Image originale

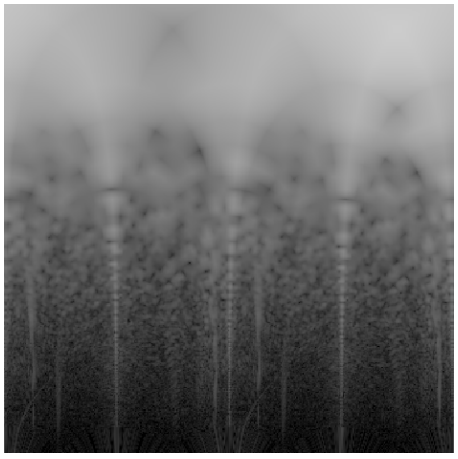
b. Image marquée et tournée d'un angle α



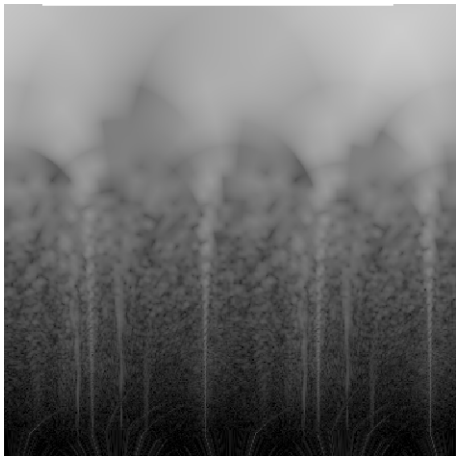
c- Spectre d'amplitude de l'image originale



d- Spectre d'amplitude de l'image pivotée de α



e- LPM de l'image originale



f- LPM de l'image tournée de α

Figure IV.50. Exemple d'une image marquée et tournée d'un angle inconnu α

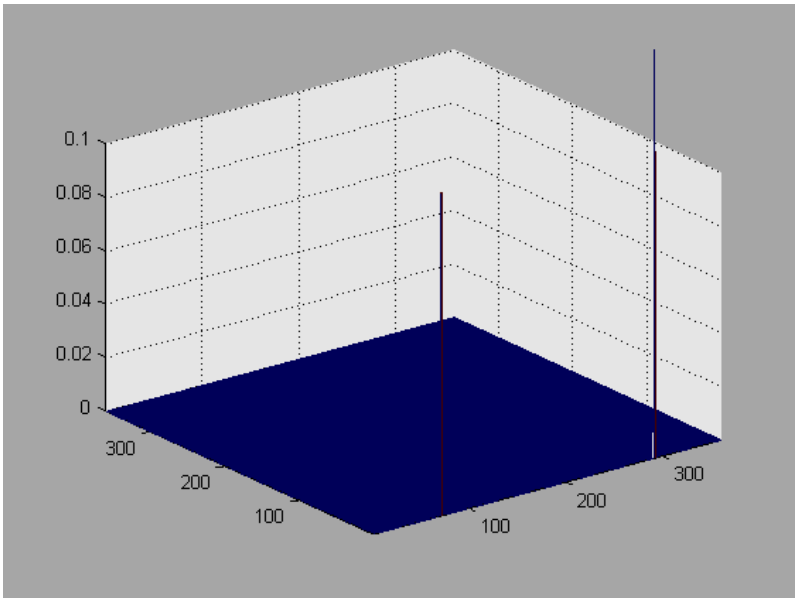


Figure IV.51. Corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée et tournée d'un angle α

Il est intéressant de noter que: en raison de la symétrie du domaine obtenue par la *DFT*, le déplacement induit dans la corrélation de phase d'un angle α est le même que celui produit par (α + π). Pour cette raison, la figure (IV.52) donne les résultats de similarité, entre la marque originale et celle extraite, pour des valeurs α allant de 1 ° à 180 °.

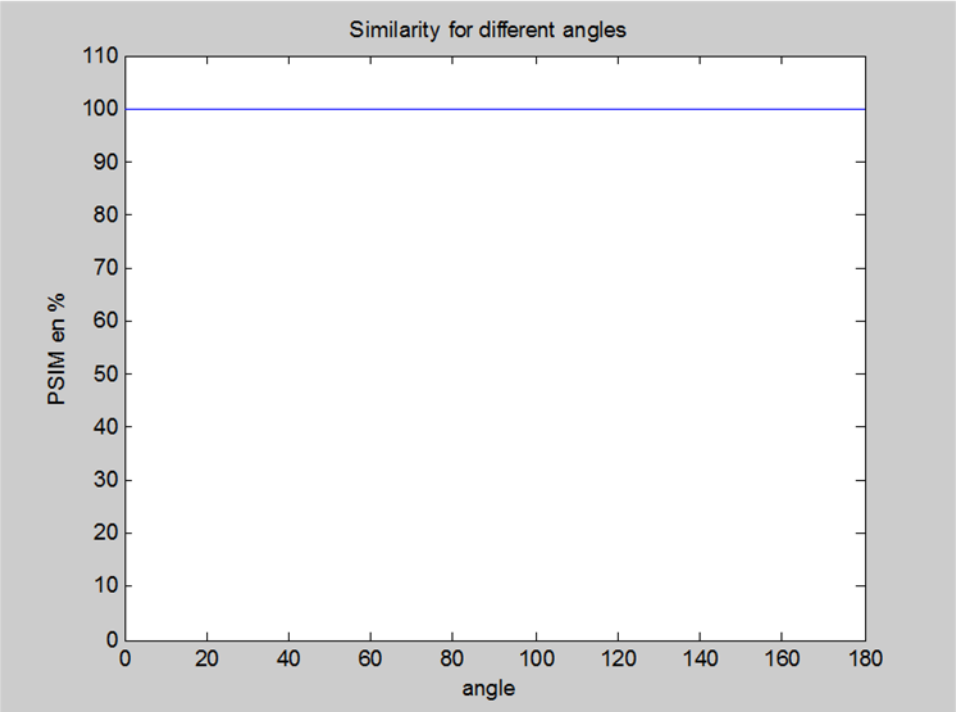


Figure IV.52 Le *PSIM* pour différentes valeurs de rotation de l'image marquée

Les résultats de la figure (IV.52) témoignent de la robustesse de l'approche développée vis-à-vis la rotation. En effet, la marque est extraite à 100% quelque soit l'angle de rotation.

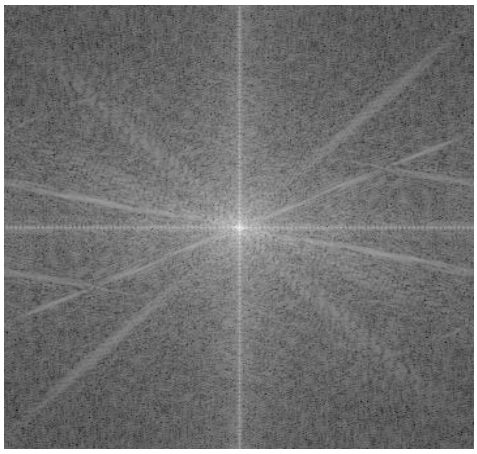
IV.3.5.5. Test de la robustesse vis-à-vis la rotation et le changement d'échelle

Dans ce type de test, nous avons à extraire la marque de l'image marquée et qui a subi des transformations combinées. En effet, elle est réduite d'un facteur de changement d'échelle X et tournée d'un angle α comme il est montré sur la figure (IV.53.b). Comme on peut le constater sur les figures (IV.53.e) et (IV.53.f), les transformations de changement d'échelle et de rotation sont converties à des translations cycliques le long des axes vertical et horizontal respectivement. Donc, à partir de l'emplacement des deux pics dans le spectre de corrélation de phase de la figure (IV.54), on peut déduire que l'image a subi deux transformation : une de type changement d'échelle et l'autre de type rotation. Les deux pics sont localisés aux endroits (22, 51) et (340, 311) et ceci correspond à un facteur d'échelle X=0.7 et à un angle de rotation α=50°.

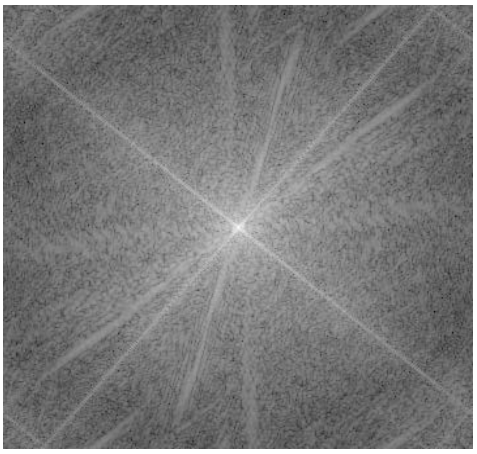
Pour synchroniser l'extraction de la marque on doit faire subir à l'image les transformations inverses à savoir : un changement d'échelle de facteur 1/0.7 et une rotation d'un angle α=50° dans le sens des horaire.

a. Image originale

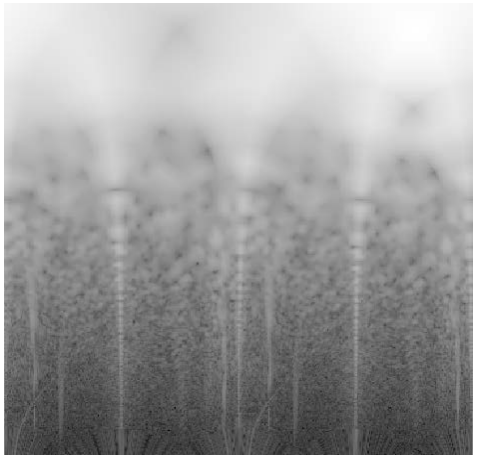
b. Image marquée réduite par *X* et tournée de α



c- Spectre d'amplitude de l'image originale



d- Spectre d'amplitude de l'image transformée par *X* et α



e- *LPM* de l'image originale

f- *LPM* de l'image marquée et transformée par X et α

Figure IV.53 Exemple d'une image réduite et tournée en même temps

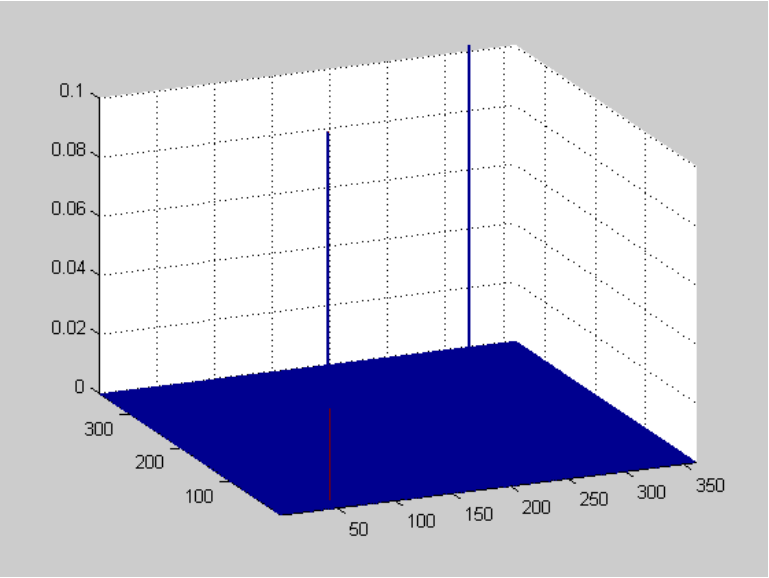


Figure IV.54 Corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée réduite de *X* et tournée de α

Pour l'exemple précédent la similarité entre la marque originale et celle extraite après correction est de 100%. Les figures (IV.55) et (IV.56) illustrent les résultats de tests de similarité entre les deux marques originale et extraite, pour les deux exemples suivant :

1- une image tournée d'un angle de 65° et réduite par des facteurs d'échelle allant de 0.3 à 1,
2- une image réduite par un facteur d'échelle égale à 0.8 et tournée d'angles allant de 0° à 180°.

A partir des résultats obtenus on peut conclure que : dans le cas des transformées combinées, la similarité entre la marque originale et celle extraite après correction est affectée uniquement par le niveau de changement d'échelle.

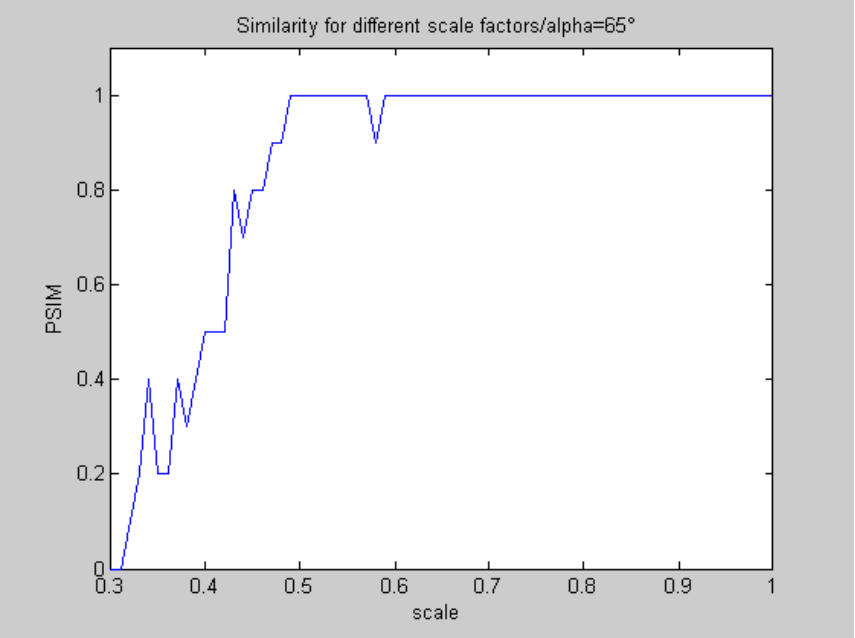


Figure IV.55. Variation du *PSIM* pour α=65°/ X= [0.3,..…,1]

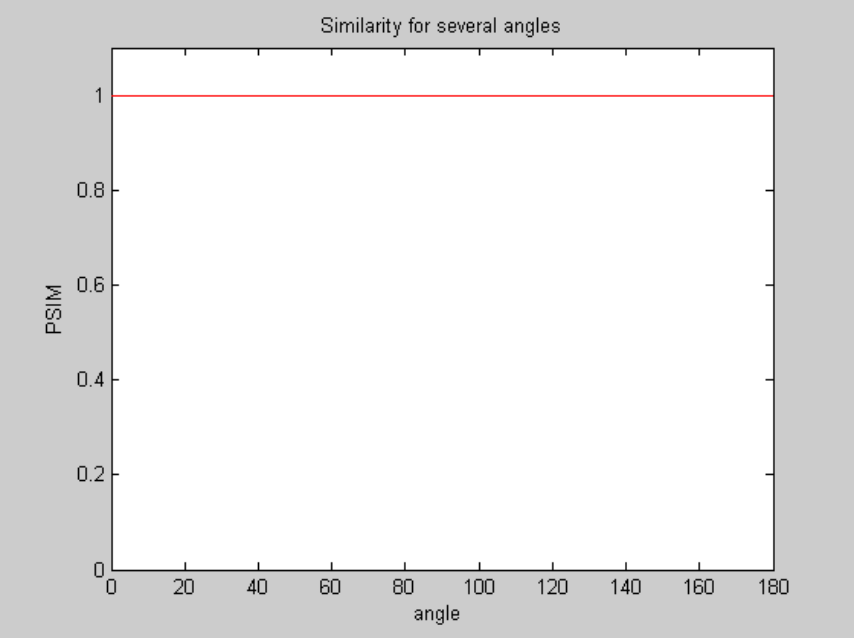


Figure IV.56. Variation du *PSIM* pour *X*=0.8 / α = [0…….180]

IV.3.5.5. Test de la robustesse vis-à-vis de la compression *JPEG*

Dans cette section nous allons montrer les performances de l'approche développée en termes de robustesse vis-à-vis de la compression JPEG. En effet, l'image marquée Cameraman est compressée avec différents facteurs de qualité. Les résultats de la figure

(IV.57) donnent les variations du pourcentage de similarité entre la marque originale et celle extraite après compression de l'image marquée. De ces résultats on peut conclure que notre approche est robuste à la compression. Cela est dû à la stratégie utilisée pour l'insertion de la marque, et qui consiste à modifier les coefficients moyens fréquences de l'amplitude *DFT* de la sous-bande basse fréquences (*LL*).

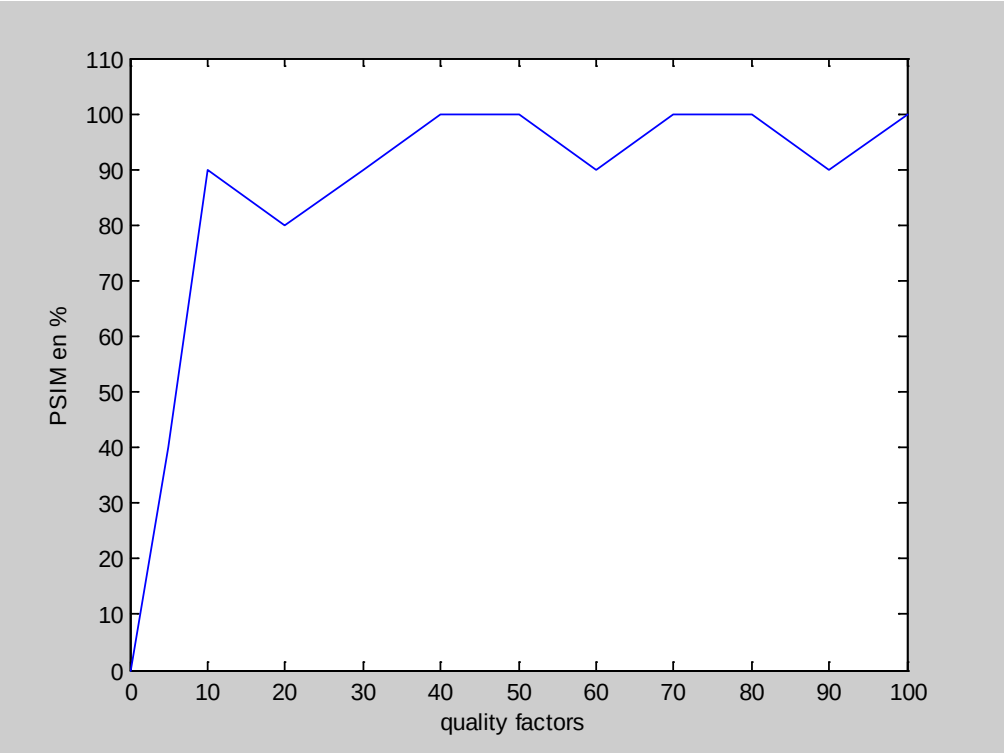


Figure IV.57. Variation du *PSIM* en fonction du facteur de qualité

IV.3.5.5. Test de la robustesse vis-à-vis l'addition du bruit Gaussien

Dans cette expérience, l'image marquée est attaquée par l'ajout d'un bruit Gaussien de différents niveaux d'énergie. La marque extraite pour chaque niveau d'énergie de bruit est comparée à la marque originale. Les résultats de la figure (IV.58), qui donne l'allure de la variation du *PSIM* en fonction de l'énergie du bruit Gaussien, montre que la méthode est robuste à l'ajout du bruit Gaussien. C'est tout a fait logique, parce que la stratégie d'insertion adoptée consiste à travailler sur les coefficients moyens fréquences de l'amplitude *DFT* de la sous-bande (LL). Une zone loin d'être influencer par le bruit.

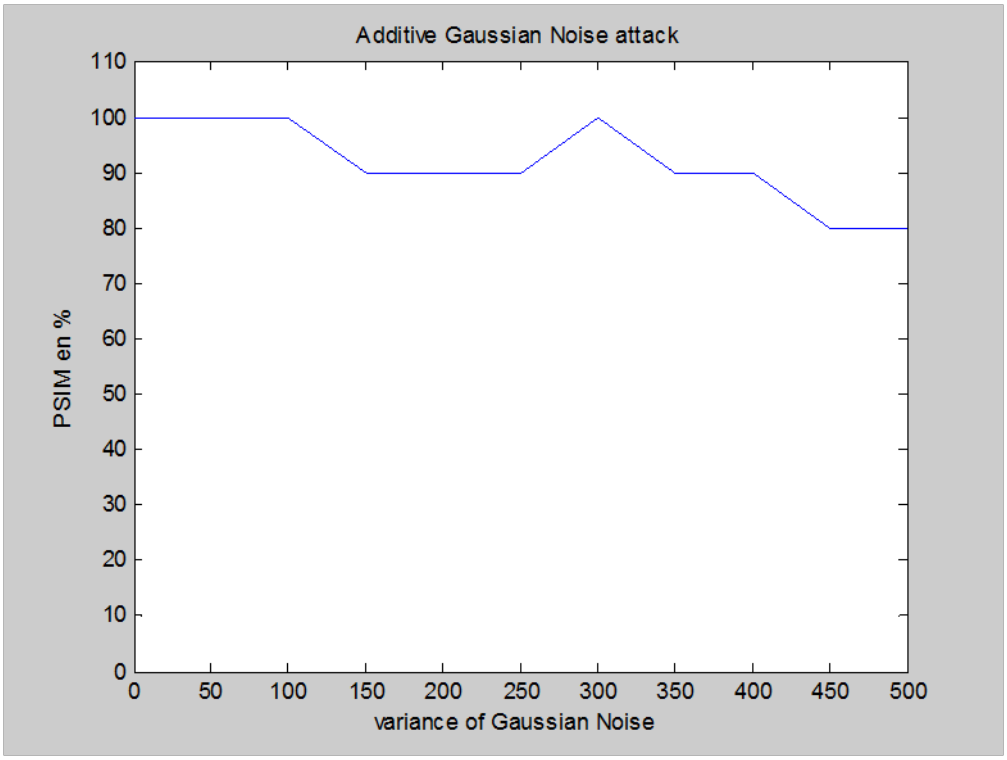


Figure IV.58. Variation du *PSIM* en fonction du niveau d'énergie d'un bruit Gaussien

IV.3.6. Conclusion

Dans cette partie, nous avons présenté une autre approche hybride. L'objectif principal visé est la robustesse vis-à-vis les transformations géométriques élémentaires qui sont : la translation, la rotation et le changement d'échelle (*RST*). La marque est insérée dans une image rembourrée (*padded*) selon une stratégie qui permet : d'une part, en utilisant la *DWT*, d'avoir un espace robuste à la compression et l'ajout du bruit. D'autre part, l'utilisation de la transformée de Fourier-Mellin (*FMT*) fournit un domaine transformé invariante pour *RST* . L'extraction de la marque est synchronisée par le calcul de la corrélation de phase entre le *LPM* de l'image originale et celui de l'image marquée et transformée. Les résultats des tests prouvent que la méthode présentée est robuste contre les transformations géométriques (*RST*), l'ajout du bruit Gaussien et la compression *JPEG* voir même les attaques combinées.

Enfin, nous envisageons une amélioration de la méthode mise au point en particulier par l'utilisation d'une marque sous forme d'une image à la place de la séquence binaire.

IV.4. Méthode de Watermarking Basée sur la *DWT* Multi-Niveaux et une Nouvelle Classe de Transformées Paramétriques Orthogonales-Réciproques (ROPT)

IV.4.1. Introduction

A travers le travail présenté dans cette partie, nous proposons une autre approche hybride de watermarking pour des images fixes en niveau de gris. L'approche développée, et à la différence des méthodes vues dans les parties précédentes, s'inscrit dans le contexte sécuritaire du domaine de watermarking d'image et utilise une marque sous forme d'image. Elle combine deux transformées, à savoir la transformée *DWT* multi-niveaux et une nouvelle classe de Transformées Paramétrique Orthogonale-Réciproque (*ROPT* : *reciprocal-orthogonal parametric transforms*). L'idée de base de la méthode développée consiste à exploiter le grand nombre des paramètres indépendants, (*3N/2*) procurés par la *ROPT*, pour générer une clé supplémentaire qui s'ajoute à celle utilisée pendant l'insertion de la marque. Cependant, l'utilisation de la *ROPT* seule rend difficile la vérification de la contrainte invisibilité de la marque, à cause de la répartition non uniforme des fréquences offerte par cette transformée. C'est pourquoi nous avons choisi d'appliquer la *ROPT* à la sous-bande basse fréquences obtenue par la *DWT*. De cette façon nous avons assuré d'une part que les fréquences de la région dans laquelle le watermark sera inséré sont toutes de la même gamme, d'autre part la robustesse du watermark contre certaines attaques telles que la compression *JPEG*, le filtrage passe bas, l'ajout de bruit ainsi que les combinaisons de ces attaques.

Dans les sections qui suivent nous présenterons quelques travaux en relation avec notre approche, puis nous donnerons un rappel sur la *ROPT*. Ensuite, et après avoir décrire la méthode développée, nous discuterons les résultats des différents tests effectués.

IV.4.2. Travaux en relation avec l'approche développée

Falkowski et Lim ont proposé une technique de tatouage basée sur les transformées multi-résolution et complexes de Hadamard [138]. Initialement, la transformation multi-résolution de Hadamard est appliquée à l'image pour la décomposer en différentes bandes de fréquences. Ensuite, la transformation de Hadamard complexe 2D est appliquée à la bande des basses fréquences après l'avoir divisée en blocs de 8x8. Le watermark est inséré dans ce domaine en modifiant les éléments des composantes les plus significatives de l'image. Le système proposé s'avère robuste contre plusieurs attaques comme la compression *JPEG*, redimensionnement, recadrage et les tatouages successifs.

Dans l'approche développée par Gilani et Skodras [139], l'insertion du watermark se fait en modifiant les coefficients haute fréquence de la transformée de Hadamard. Une image subit une transformée en ondelettes de Haar puis une transformation de Hadamard. Cela entraîne le domaine fréquentiel multi-résolution de Hadamard. La transformation de

Hadamard concentre la majeure partie de l'énergie dans le coin supérieur gauche, et par conséquent, il est choisi pour incorporer l'information du watermark. Les auteurs estiment que les bandes de hautes fréquences de la transformation de Hadamard sont robustes contre le bruit et peuvent donc résister à des attaques de compression *JPEG* à faible facteur de qualité.

Bogdan J. Falkowski a révélé une façon d'incorporer un watermark dans une image en niveaux de gris en utilisant d'une part la transformée multi-résolution et multipolarité modifiée de Walsh-Hadamard et d'autre part la transformée complexe de Hadamard [140]. Le processus consiste à extraire les pixels bruts à partir du bitmap de l'image et les stockées dans un tableau bidimensionnel. Puis la transformation de Walsh-Hadamard multipolarité est appliquée pour décomposer l'image en structure pyramidale avec divers sous-bandes. La sous bande basse fréquence est sélectionnée et segmentée en blocs de 8x8 pour subir par la suite une transformation de Hadamard complexe unidimensionnelle appliquée sur les lignes puis les colonnes. L'insertion du watermark est réalisée en modifiant les coefficients de la transformée complexe de Hadamard. Cette technique est robuste à la compression *JPEG*, redimensionnement de l'image, les distorsions de bruit, la netteté, recadrage et le tatouage successive.

Gaurav Bhatnagar et Balasubramanian Raman ont proposé une version plus récente de la transformée de Walsh-Hadamard appelée la transformée de Walsh-Hadamard multi-résolution (*MR-WHT*). En outre, un schéma de tatouage robuste est proposé pour la protection du droit d'auteur en utilisant la *MR-WHT* et la décomposition en valeur singulière [141]. L'idée de base du système proposé est de décomposer une image en utilisant la *MR-WHT*. Ensuite, les valeurs singulières médianes de la sous-bande haute fréquence sont modifiées avec les valeurs singulières du watermark. Enfin, ils ont développé un système fiable qui permet l'extraction du watermark a partir de l'image déformée. Cette technique permet une meilleure imperceptibilité visuelle et elle est robuste vis-à-vis plusieurs attaques intentionnelles et non-intentionnelles.

Marjuni, A.; Logeswaran, R.; Ahmad Fauzi, M.F.; ont proposé un nouveau système de tatouage d'image basé sur l'utilisation de la transformation de Walsh Hadamard rapide (*FWHT*) combinée avec la transformée en cosinus discrète (*DCT*) [142]. La *DCT* est appliquée à chaque bloc 8x8 de l'image originale pour obtenir les coefficients DC où le watermark original, qui subit la *FWHT*, est inséré Ensuite, la *DCT* inverse est appliquée sur la composante DC marquée pour reconstruire l'image tatouée. Ce système produit une grande transparence perceptive du watermark inséré et il a prouvé sa robustesse contre quelques attaques.

Franklin Rajkumar.V, Manekandan.GRS et V.Santhi ont présenté un nouvel algorithme de tatouage dont lequel la technique de transformation de Hadamard est combiné avec un modèle d'entropie. Ce modèle d'entropie mesure le contenu d'informations de chaque bloc qui est utilisé comme critère pour la sélection de blocs [143]. La technique proposée peut cacher un watermark, sous forme d'une image entière ou d'un motif, directement dans l'image originale. Comme la qualité de l'image est à conserver la totalité de l'image n'est pas modifiée au cours de l'insertion. Seulement quelques blocs sont utilisés et ceci en fonction de la taille du watermark et les informations du contenu d'un bloc de l'image. La complexité de calcul de l'algorithme proposé est réduite par l'utilisation de la transformation de Hadamard, qui convertit l'image de couverture du domaine spatial au domaine transformé. Le schéma proposé est robuste à l'ajout du bruit aléatoire, aux attaques de redimensionnement et recadrage.

IV.4.3. Rappel sur la *ROPT*

Le travail proposé par S. Bouguezel dans [11], traite une nouvelle classe de transformées paramétriques orthogonales-réciproques (ROPT). L'idée est basée sur la combinaison d'un nouveau noyau paramétrique avec celui de la transformée de Walsh-Hadamard. Le résultat est un opérateur de matrice paramétrique carrée d'ordre *N* avec des propriétés très intéressantes. Une des propriétés les plus importantes de cette transformation est que l'inverse de l'opérateur de la matrice est la transposée de la matrice dont les coefficients sont les inverses des éléments de la matrice directe. Cet opérateur de matrice d'ordre *N* et sa version normalisée ont respectivement *3N/2* et *N/2-1* paramètres indépendants, pour une séquence dont la longueur *N* est une puissance de deux.

La *ROPT* d'une séquence complexe *x(k)* d'ordre $N=2^r$ est définie comme suite :

$$X(n) = \sum_{k=0}^{N-1} x(k) a_{k,s(n)} (-1)^{kon} \ldots\ldots n = 0,1,\ldots\ldots,N-1 \qquad (IV.64)$$

Où $k\ o\ n = k_0 n_0 + k_1 n_1 + \ldots\ldots\ldots + k_{r-1} n_{r-1}$, $s(n) = (-1)^{(N-1)on}$.

La transformée inverse est donnée par l'équation :

$$x(k) = \frac{1}{N} \sum_{n=0}^{N-1} X(n) \frac{1}{a_{k,s(n)}} (-1)^{kon} \ldots\ldots k = 0,1,\ldots\ldots,N-1 \qquad (IV.65)$$

Où $a_{k,1}$ et $a_{k,-1}$ sont des paramètres complexes non nuls est satisfaisants la relation :

$$a_{k,1} a_{N-1-k,-1} = a_{k,-1} a_{N-1-k,1} \qquad (IV.66)$$

Nous supposons que les séquences d'entrée et de sortie *x (k)* et *X (n)* sont donnés respectivement par les vecteurs colonnes *x* et *X* de dimension *Nx1*. Ensuite, la formulation sous forme matricielle de la transformée ROPT directe et inverse, proposée par (*IV.64*) et (*IV.65*), peut être exprimé en utilisant les nouvelles matrices paramétriques ayant des structures simples avec des propriétés intéressantes. Elle est donnée comme suit:

$$X=P_N.x \qquad (IV.67)$$

$$x=P_N^{-1}.X \qquad (IV.68)$$

Où P_N et P_N^{-1} sont respectivement les matrices des transformées directes et inverse. Mis à part le facteur d'échelle de *1/N*, il est clair à partir de (IV.64) et (IV.65) que le (*k, n*) ième élement de la matrice P_N^{-1} est l'inverse (c'est à dire réciproque) de la (n, k) ième élément de la matrice P_N. Par conséquent, la matrice inverse P_{N-1} est facile à obtenir à partir de la matrice directe P_N. Elle est donnée par :

$$P_N^{-1}= 1/N.(P_N^R)^T \qquad (IV.69)$$

Où la matrice P_N^R est obtenue en prenant l'inverse de chaque élément de P_N et $(.)^T$ représente la transposition de la matrice associée. Compte tenu du fait que P_N satisfait la relation $P_N^{-1}=1/N\ (P_N^R)^T$ et contient tous les paramètres indépendants de la transformée, elle est appelé une matrice de *ROP*. Une matrice *ROP* est dite normalisée si tous les éléments de la première ligne et la première colonne sont égaux à l'unité.

Dans le cas où N=8, la matrice *ROP* directe est donnée comme suite :

$$P_8 = \begin{bmatrix} a_{0,1} & a_{1,1} & a_{2,1} & a_{3,1} & a_{4,1} & a_{5,1} & a_{6,1} & a_{7,1} \\ a_{0,-1} & -a_{1,-1} & a_{2,-1} & -a_{3,-1} & \frac{a_{3,-1}.a_{4,1}}{a_{3,1}} & -\frac{a_{2,-1}.a_{5,1}}{a_{2,1}} & \frac{a_{1,-1}.a_{6,1}}{a_{1,1}} & -\frac{a_{0,-1}.a_{7,1}}{a_{0,1}} \\ a_{0,-1} & a_{1,-1} & -a_{2,-1} & -a_{3,-1} & \frac{a_{3,-1}.a_{4,1}}{a_{3,1}} & \frac{a_{2,-1}.a_{5,1}}{a_{2,1}} & -\frac{a_{1,-1}.a_{6,1}}{a_{1,1}} & -\frac{a_{0,-1}.a_{7,1}}{a_{0,1}} \\ a_{0,1} & -a_{1,1} & -a_{2,1} & a_{3,1} & a_{4,1} & -a_{5,1} & -a_{6,1} & a_{7,1} \\ a_{0,-1} & a_{1,-1} & a_{2,-1} & a_{3,-1} & -\frac{a_{3,-1}.a_{4,1}}{a_{3,1}} & -\frac{a_{2,-1}.a_{5,1}}{a_{2,1}} & -\frac{a_{1,-1}.a_{6,1}}{a_{1,1}} & -\frac{a_{0,-1}.a_{7,1}}{a_{0,1}} \\ a_{0,1} & -a_{1,1} & a_{2,1} & -a_{3,1} & -a_{4,1} & a_{5,1} & -a_{6,1} & a_{7,1} \\ a_{0,1} & a_{1,1} & -a_{2,1} & -a_{3,1} & -a_{4,1} & -a_{5,1} & a_{6,1} & a_{7,1} \\ a_{0,-1} & -a_{1,-1} & -a_{2,-1} & a_{3,-1} & -\frac{a_{3,-1}.a_{4,1}}{a_{3,1}} & \frac{a_{2,-1}.a_{5,1}}{a_{2,1}} & \frac{a_{1,-1}.a_{6,1}}{a_{1,1}} & -\frac{a_{0,-1}.a_{7,1}}{a_{0,1}} \end{bmatrix} \qquad (IV.68)$$

IV.4.4. Description de la méthode développée

Dans l'approche de tatouage proposé dans cette partie, deux transformations sont utilisés. À savoir, la transformée en ondelettes discrètes (*DWT*) et la nouvelle classe de transformations paramétriques orthogonales-réciproques (*ROPT*) qui est adapté à notre application. En effet, au lieu d'utiliser des séquences comme entrée et sortie on utilise des matrices. Par conséquent, la *ROPT* et la *ROPT* inverse sont données par (IV.69) et (IV.70)

respectivement. On suppose que les matrices d'entrée et de sortie *y (i, j)* et *Y (u, v)* sont de taille *NxN*.

$$Y = (P_N . y . (P_N{}^R)^T)/N \quad (IV.69)$$

$$y = ((P_N{}^R)^T . Y . P_N)/N \quad (IV.70)$$

La première transformation permet d'obtenir un endroit approprié pour l'insertion du watermark, dans notre cas, la sous-bande basses fréquences (*LL*) est utilisée, ce qui conduit à vérifier les critères de robustesse. La seconde fournit une clé de sécurité supplémentaire ajoutée à celle(s) utilisées pour insérer le watermark. En effet, le choix des paramètres de la matrice donnée par (*IV.68*) pour appliquer la *ROPT* à la sous-bande (*LL*) de l'image hôte sont différents de ceux utilisés en appliquant la *ROPT* au watermark.

IV.4.4.1. Insertion de la marque

La phase d'insertion de la marque, illustrée par l'organigramme de la figure (IV.59), se compose des étapes données par l'algorithme suivant :

- **Algorithme d'insertion de la marque**

1- Convertir l'image en niveau de gris si elle est en couleur.

2- Appliquer à l'image la transformée *DWT* au niveau désiré (*d*).

3- Diviser la sous-bande (LL_d), obtenue dans l'étape 2, en blocs B_{ij} de taille 8x8.

4- Après avoir choisi les paramètres appropriés, qui forment la première clé, appliqué à chaque bloc la *ROPT* de la manière suivant :

$$\text{ROPT}\,[B_{ij}] = RB_{ij} = (P_N . B_{ij} . (P_N{}^R)^T)/N, \quad N=8.$$

5- Diviser le marque, qui est une image et doit être de même taille que la sous-bande (LL_d), en blocs W_{ij} de taille 8x8.

6- Après avoir choisi les paramètres appropriés, qui forment la deuxième clé, appliqué à chaque bloc W_{ij} la *ROPT* de la manière suivant :

$$\text{ROPT}\,[W_{ij}] = R\,W_{ij} = (P_N . W_{ij} . (P_N{}^R)^T)/N, \quad N=8.$$

7- Insérer la marque en combinant RB_{ij} et $R\,W_{ij}$ pondéré par un paramètre (λ), qui d'une part assure l'invisibilité de la marque et d'autre part joue le rôle d'une troisième clé. Soit RY_{ij} le résultat de cette insertion.

8- Appliquer la *ROPT* inverse à chaque bloc : $\text{ROPT}^{-1}[RY_{ij}] = Y_{ij} = ((P_N{}^R)^T . RY_{ij} . P_N)/N$

9- Intégrer les blocs Y_{ij} pour composer la sous-bande marquée (LL_{Md}).

10- Appliquer la transformée inverse IDWT pour obtenir l'image marquée en niveau de gris.

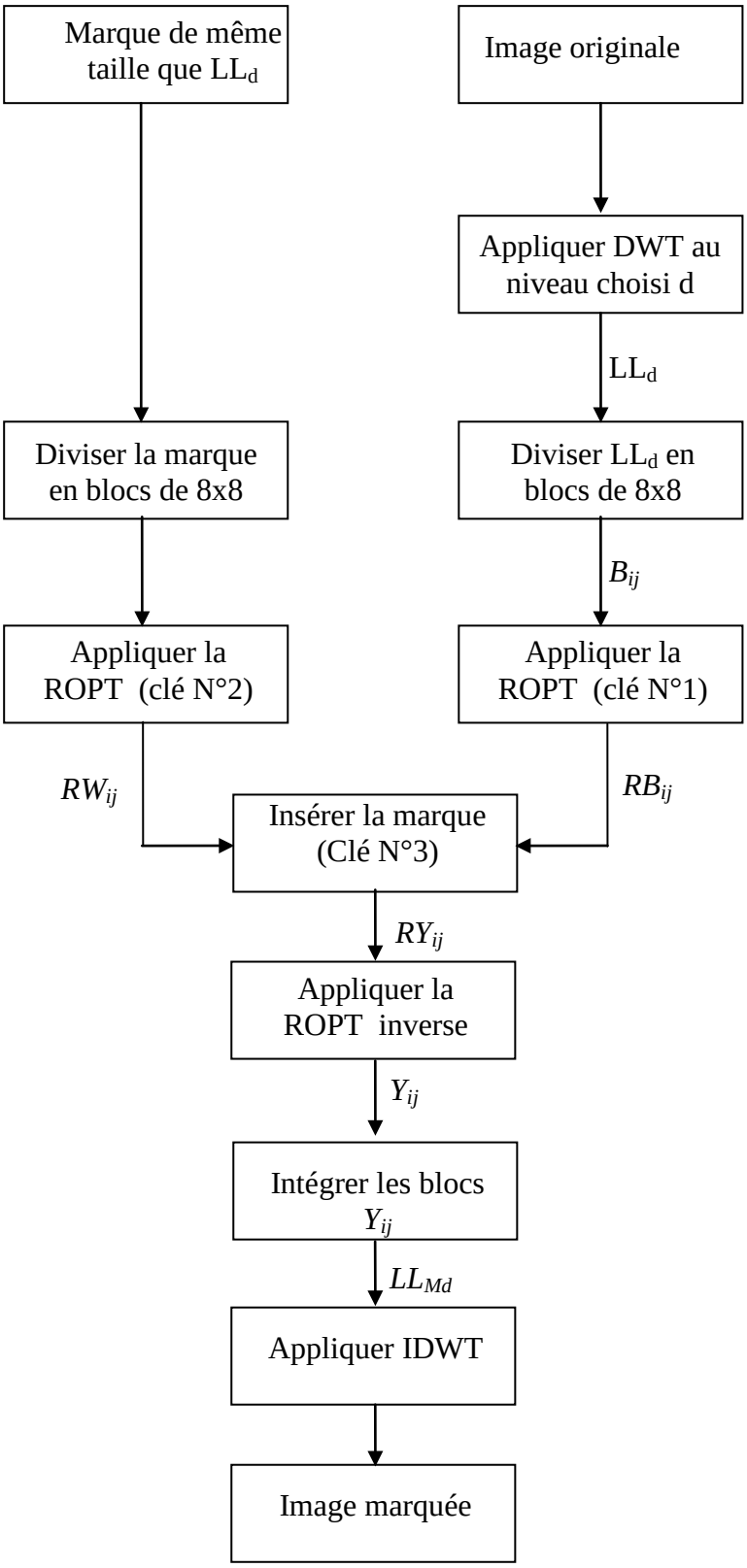


Figure IV.59. Organigramme du processus d'insertion de la marque

IV.4.4.2. Extraction de la marque

L'extraction de la marque se fait d'une manière non aveugle (watermarking informé), ce qui implique l'utilisation de l'image originale. L'enchaînement des étapes de cette extraction, illustré sur la figure (IV.60), est donné par l'algorithme suivant :

- **Algorithme d'extraction de la marque**
  1- Convertir l'image originale et celle marquée en niveau de gris si celles-ci sont en couleurs.
  2- Appliquer la *DWT*, au niveau décomposition fixé d, aux résultats précédents.
  3- Diviser à la fois les sous-bandes (LL_d) et (LL_{Md}), obtenues dans l'étape 2, en blocs de taille 8x8 B_{Oij} et B_{Mij} respectivement.
  4- En utilisant la première clé, appliquer la ROPT pour chaque bloc B_{Oij} et B_{Mij} :
  RB_{Oij}= ROPT [B_{Oij}] = (P_N. B_{Oij}. (P_N^R)^T)/N
  RB_{Mij}= ROPT [B_{Mij}] = (P_N. B_{Mij}. (P_N^R)^T)/N, N=8.
  5- A partir des blocs B_{Oij} et B_{Mij} et en utilisant la troisième clé (λ), extraire les blocs de la marques soient RW_{Eij}.
  6- En utilisant la deuxième clé, appliquer pour chaque bloc RW_{Eij} la *ROPT* inverse. Soit W_{Eij}= ((P_N^R)^T. RW_{Eij}. P_N)/N.
  7- Intégrer les blocs W_{Eij} pour composer la marque extraite.
  8- Vérifier la similitude entre la marque originale et celle extraite à l'aide de la corrélation normalisée donnée par l'équation (IV.71) ci-dessous. Si la valeur de similarité est supérieure à un seuil, la marque est extraite avec succès, si non elle n'existe pas ou nous n'arrivons pas à détecter.

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} W(i,j) * W_E(i,j)}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{M} W^2(i,j) * \sum_{i=1}^{N}\sum_{j=1}^{M} W_E^2(i,j)}} \qquad \text{(IV.71)}$$

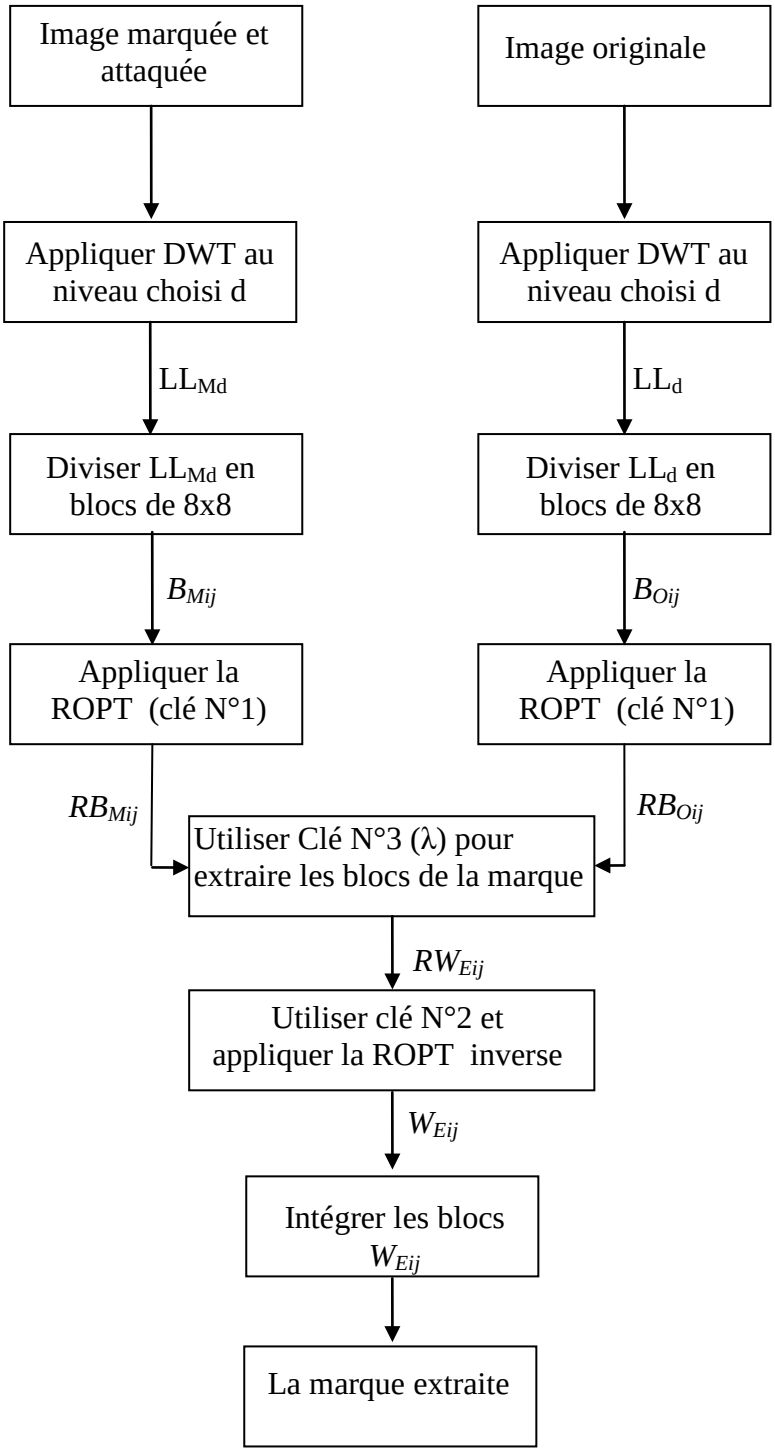


Figure IV.60. Organigramme du processus d'extraction de la marque

IV.4.5. Tests et interprétation des résultats

Dans cette section, nous illustrons les performances de la méthode proposée contre des attaques telles que la compression *JPEG*, le filtrage passe-bas et l'ajout de bruit. L'algorithme proposé a été simulé en utilisant le logiciel Matlab. L'image en niveaux de gris Lena de taille

512x512 et des marques de taille 256x256, 128x128, 64x64 ont été utilisés comme référence pour tester les performances de l'algorithme.

IV.4.5.1. Test de l'invisibilité de la marque

La figure (IV.61.c) montre l'image marquée obtenu en insérant la marque montrée par la figure (IV.61.b) dans l'image originale de la figure (IV.61.a). Comme on peut le voir, la marque est imperceptible et la qualité de l'image a été préservée. Cela a également été vérifié par le calcul du *PSNR* (Signal to Noise Ratio) entre l'image originale et celle marquée. La figure (IV.62) donne une idée sur la variation des valeurs du *PSNR* par rapport aux valeurs du paramètre de force de marquage (λ). Ceci pour chaque niveau de décomposition (LL_d) utilisé pour l'insertion de la marque.

a- Image originale

c- Image marquée

b- La marque

Figure IV.61. Imperceptibilité de la marque

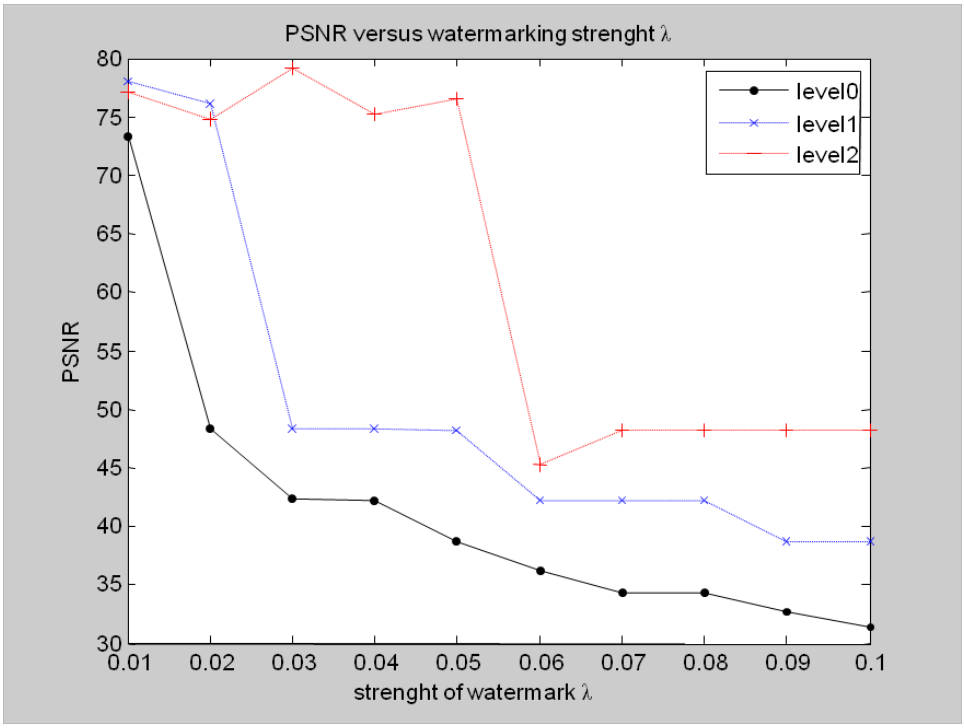


Figure IV.62. Variation du *PSNR* en fonction de λ pour d=0,1 et 2

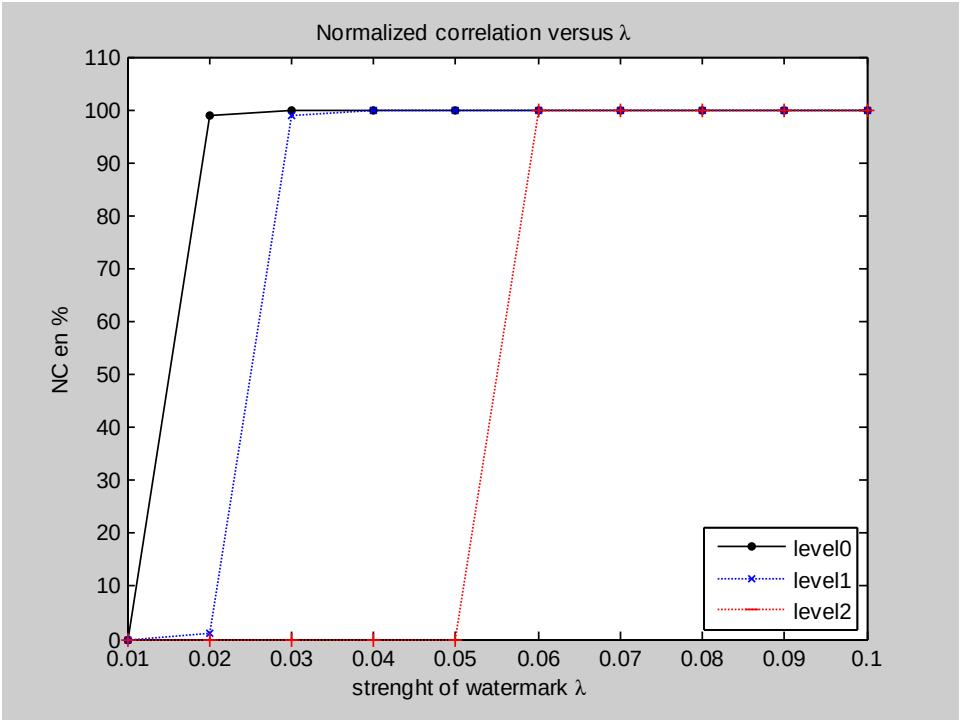
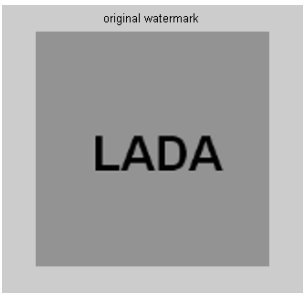


Figure IV.63. Variation de *NC* en fonction de λ pour d=0,1 et 2

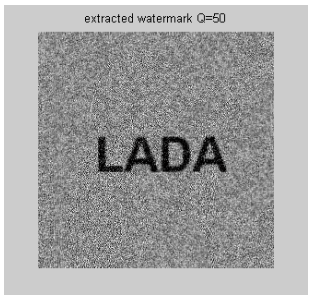
Des figures (IV.62) et (IV.63) on peut conclure que le *PSNR* obtenu, dans les trois cas d'insertion de la marque, est très acceptable pour les valeurs de λ allant de 0.01 à 0.1. Alors que l'extraction de la marque est limitée, dans le cas de niveau de décomposition d=2, aux valeurs $0.06 \leq \lambda \leq 0.1$. Dans le cas d=1 et d=0, elle est limitée aux valeurs $0.02 \leq \lambda \leq 0.1$ et $0.03 \leq \lambda \leq 0.1$ respectivement. Donc, pour les tests qui suivent λ est choisi entre 0.06 et 0.1.

IV.4.5.2. Test de la robustesse vis-à-vis de la compression

Dans ce type de test, l'image marquée est compressée avec différents facteurs de qualité *Q*. Les résultats illustrés par la figure (IV.64) montrent la marque extraite dans le cas d'une compression *Q*=50, λ =0.1 et pour les trois niveaux de décomposition d=0,1 et 2.

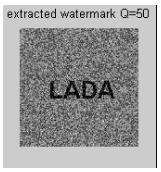


Marque originale
de taille 256x256
Pour d=0



Marque extraite
de taille 256x256
Pour d=0

Marque originale
de taille 128x128
Pour d=1



Marque extraite
de taille 128x128
Pour d=1

Marque originale
de taille 64x64
Pour d=2

Marque extraite
de taille 64x64
Pour d=2

Figure IV.64. Marques extraites pour les différents niveaux dans le cas *Q*=50 et λ = 0.1

Pour vérifier la similitude entre la marque extraite et celle d'origine; la corrélation normalisée (*NC*) donnée par l'équation (IV.71) a été utilisée. Les Résultats des figures (IV.65) et (IV.66) montrent la tendance de (*NC*) par rapport aux facteurs de qualité.

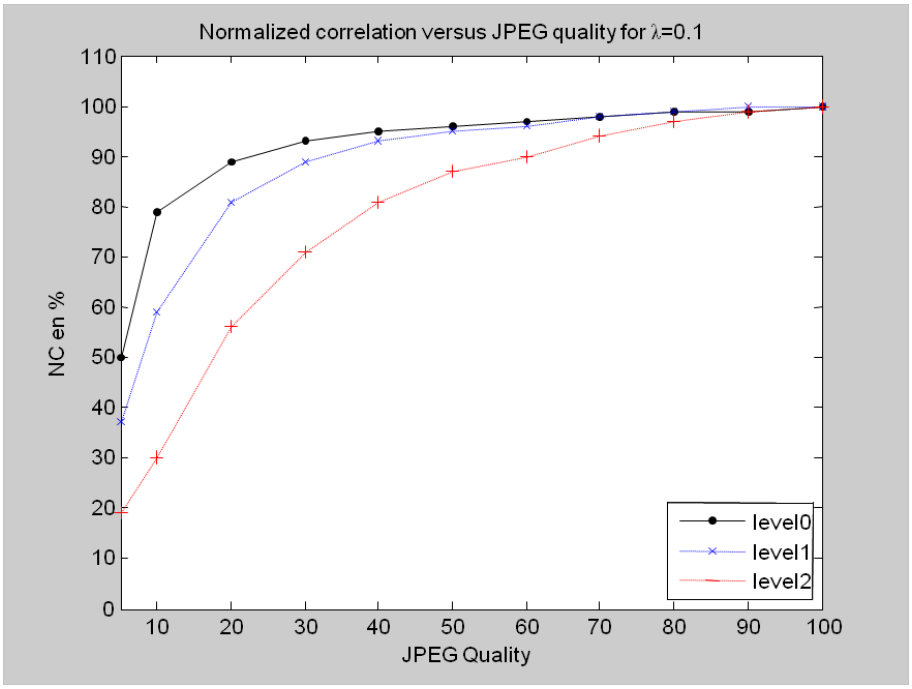


Figure IV.65. Variation de *NC* en fonction de *Q* pour λ= 0.1

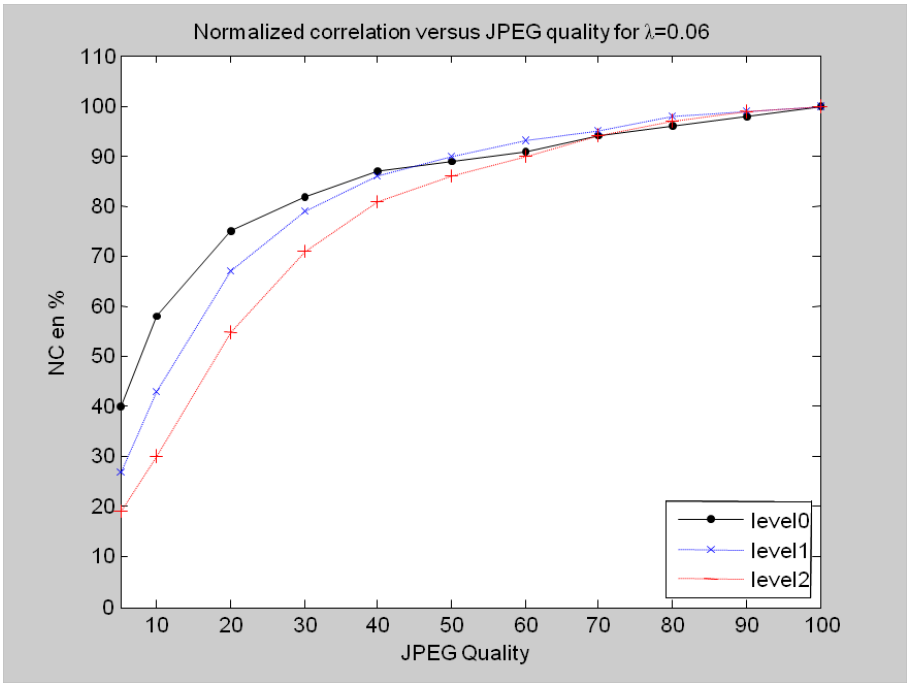
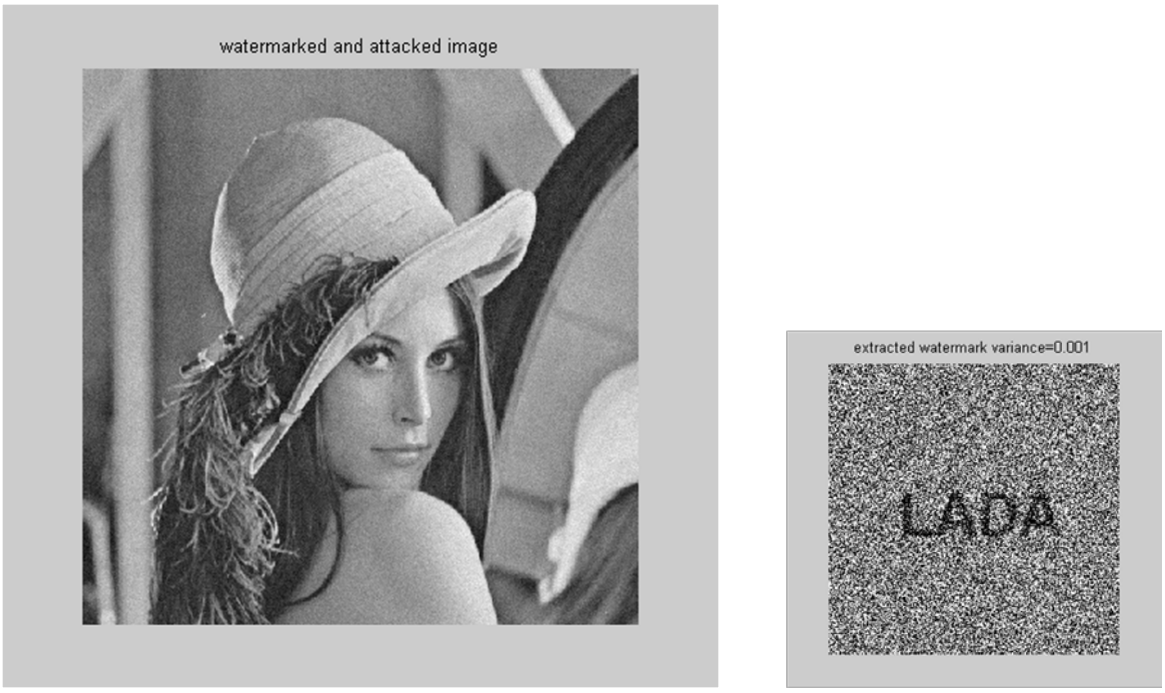


Figure IV.66. Variation de *NC* en fonction de *Q* pour λ= 0.06

La qualité de la marque extraite est considéré comme bonne si la valeur du (*NC*) est au-dessus de 50%. Par conséquent, les résultats de la figure (IV.65) et (IV.66) témoignent de la robustesse de la méthode proposée contre la compression *JPEG*. En effet, la marque peut être extraite même pour une valeur plus basse du coefficient de qualité *Q*.

IV.4.5.3. Test de la robustesse vis-à-vis de l'ajout de bruit

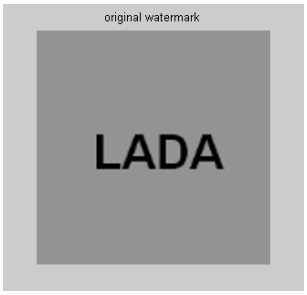
Dans cette expérience, l'image tatouée est attaqué par des bruits divers tels que le bruit blanc gaussien, Speckel et Salt-Pepper. La figure (IV.67) donnée ci-dessous montre un exemple d'image tatouée ajouté à un bruit blanc gaussien de moyenne 0 et de variance (V) égale à 0,001 ainsi que la marque extraite correspondante.



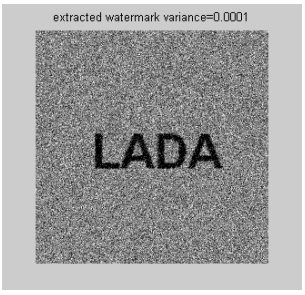
-a- - b-

Figure IV.67. a- Image tatouée attaquée par un bruit blanc Gaussienne V=0.001
b- La marque extraite

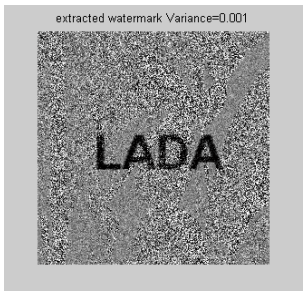
Les résultats représentés sur la figure (IV.68) illustrent la marque extraite pour certaines variances de bruit gaussien blanc, Speckel et Salt-Pepper. Le niveau de décomposition est d = 0 et $\lambda = 0,1$.



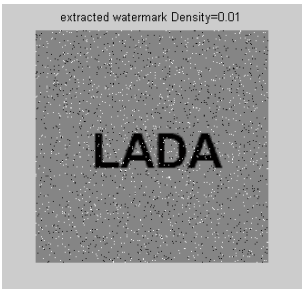
La marque originale



Cas du bruit Gaussien blanc V=0.001



Cas du bruit Speckel V=0.001



Cas du bruit Salt-Pepper D=0.01

Figure IV.68. La marque extraite dans les cas des bruits Gaussien blanc, Speckel et Salt-Pepper

La marque extraite est comparé à l'originale en utilisant la corrélation normalisée (*NC*). Les courbes des figures (IV.69), (IV.70) et (IV.71) donnent les variations de (*NC*) en fonction de la variance du bruit et selon le niveau de décomposition utilisée pour insérer la marque.

Comme on peut le constaté à partir des résultats ci-dessus la méthode proposée est robuste contre les attaques de nature ajout de bruit. En particulier lorsque le niveau 0 est utilisé, la marque peut être détectée pour des valeurs de variance allant de 0 à 0,01

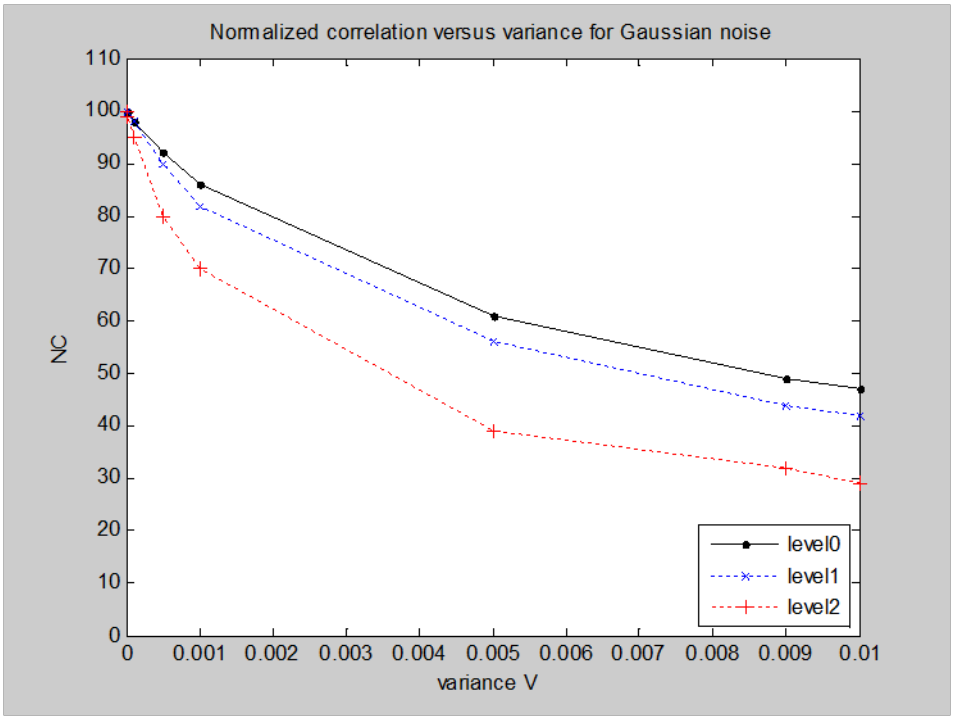


Figure IV.69. Variation de *NC* en fonction de la variance du bruit Gaussien blanc pour différents niveaux de décomposition *d*

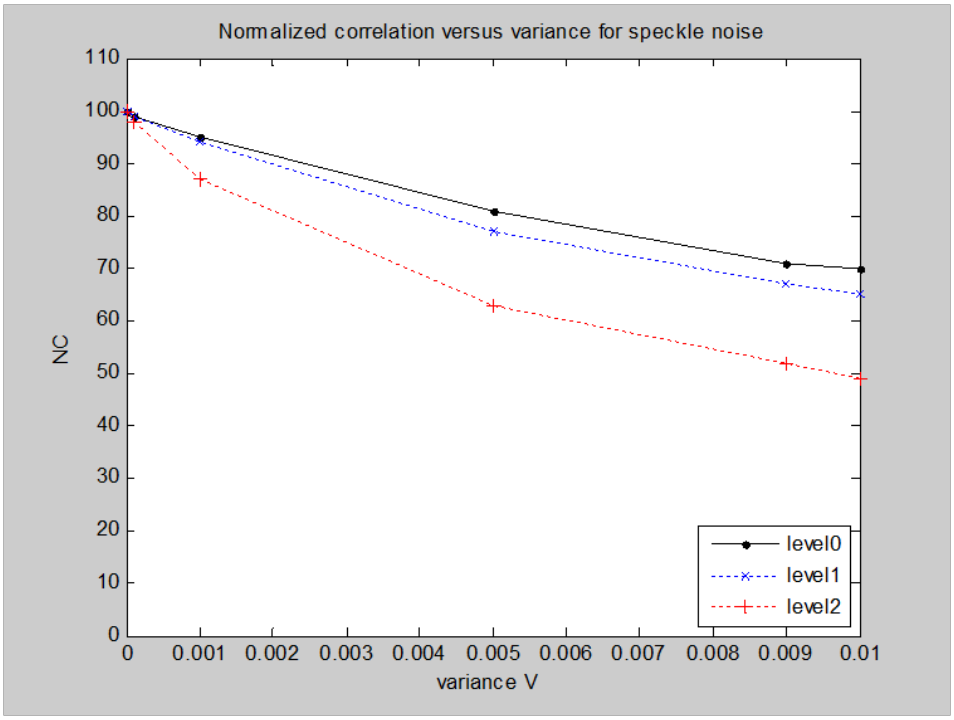


Figure IV.70. Variation de *NC* en fonction de la variance du bruit Speckel pour différents niveaux de décomposition *d*

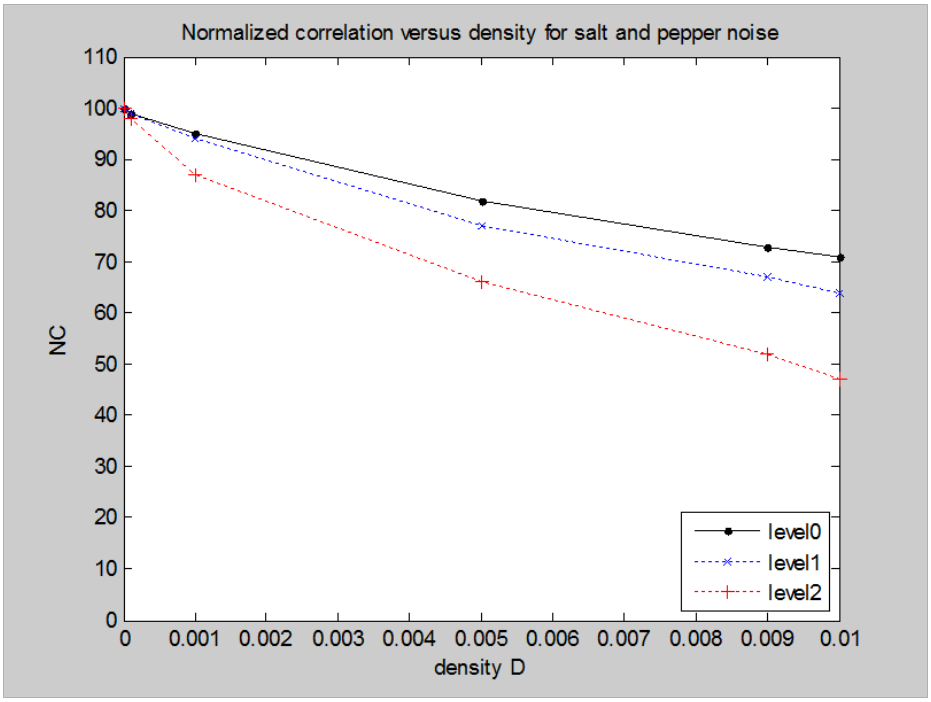
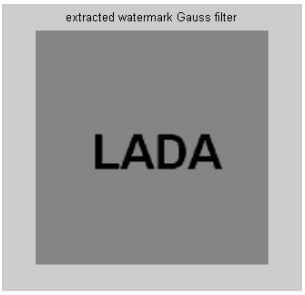


Figure IV.71. Variation de *NC* en fonction de la densité du bruit Salt-Pepper pour différents niveaux de décomposition *d*

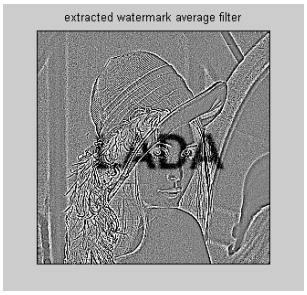
IV.4.5.4. Test de la robustesse vis-à-vis le filtrage passe-bas

Dans ce cas d'attaques l'image marquée est filtrée par trois types de filtre à savoir Gauss, average et disk. La figure (IV.72) montre la marque extraite, pour chaque type de filtre de taille 3x3 dans le cas d'une décomposition en niveau d=0. Comme on peut le voir, la marque extraite, dans le cas du filtre de Gauss, est meilleure que les autres. Cela est dû à sa nature qui est un filtre passe-bas gaussien à rotation symétriques, contrairement aux deux autres qui sont respectivement des filtres moyenne et moyenne circulaire.

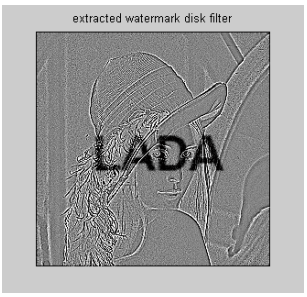
La figure (IV.73) donne l'allure de la corrélation normalisée (*NC*) en fonction de l'écart type (déviation standard) du filtre Gaussien de taille 5x5 pour les trois niveaux de décomposition. Du moment que (*NC*) est supérieure à 50% quelles que soient les valeurs de déviation standard pour les cas de niveaux de décomposition d=0 et d=1, et pour la majorité des valeurs pour le cas d=2, alors nous pouvons conclure que la méthode proposée est robuste aux attaques de filtrage passe-bas. En effet, la marque est insérée au sein de la sous-bande basse fréquences (LL_d) de *DWT*.



a- Filtre Gaussien



b- Filtre Average



c- Filtre disk

Figure IV.72. Les marques extraites dans les cas des filtres Gaussien, average et disk de taille 3x3

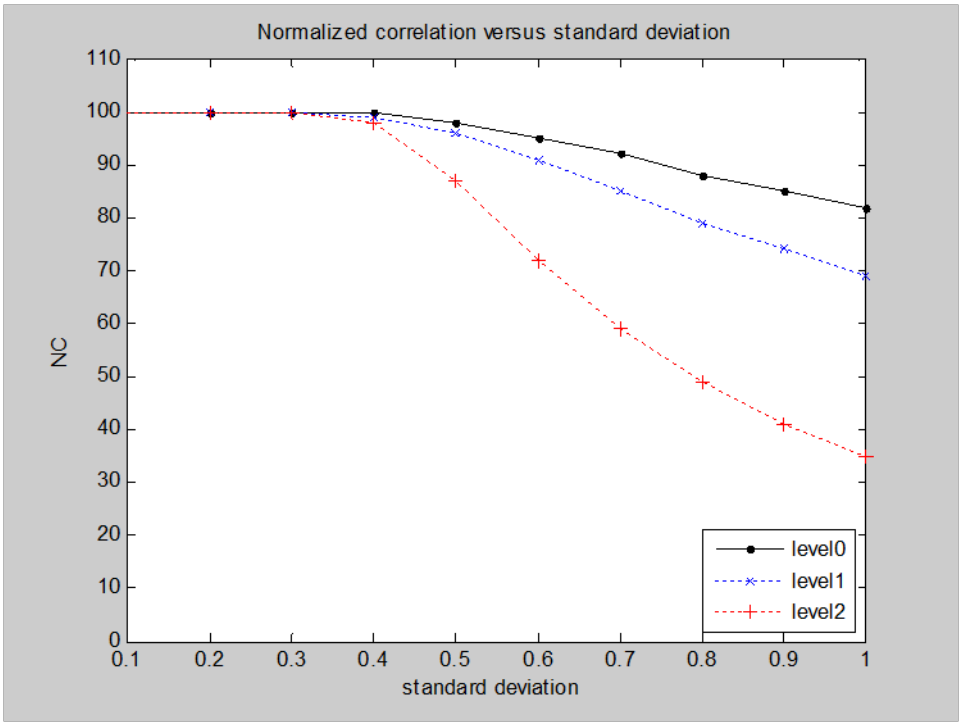


Figure IV.73. Variation de *NC* en fonction de la déviation standard du filtre Gaussien de taille 5x5

IV.4.6. Conclusion

Dans cette partie, nous avons proposé une méthode de tatouage hybride basé d'une part sur l'utilisation de la transformée *DWT,* permettant la décomposition en plusieurs niveaux de l'image à marquée, et d'autre part sur une nouvelle classe de transformations paramétriques orthogonales-réciproques (*ROPT*). Cette dernière est appliquée à la fois à la sous-bande (*LLd*), obtenue pour un niveau de décomposition donné *d*, et la marque qui doit être de même taille que la sous-bande (LL_d). Notre objectif est d'accroître la sécurité du procédé de tatouage, ce qui augmente la robustesse du watermark contre les attaques malveillantes visant par exemple sa détection et la suppression ou la modification. Pour faire, une nouvelle méthode pour générer la clé est utilisée. Nous avons exploité le grand nombre de paramètres indépendants (*3N/2*) fournis par la (*ROPT*) comme clé supplément de tatouage ajoutée à celle utilisé pour l'insertion du watermark. L'utilisation de la décomposition multi-niveaux *DWT* permet de contourner l'inconvénient de la *ROPT* qui donne une partition non uniforme des fréquences. En effet, l'utilisation de la sous-bande basse fréquences assure que les composantes à marquées appartiennent toutes à la même gamme de fréquences.

En plus de la sécurité offerte par la mis à disposition de plusieurs clés obtenues par l'application de la ROPT à la sous-bande (*LLd*) et à la marque, la méthode proposée est jugée robuste contre plusieurs attaques telles que la compression *JPEG*, le filtrage passe-bas, et l'ajout du bruit et même des attaques combinées.

Enfin, nous envisageons l'amélioration de la méthode développée en étendant sa robustesse à d'autres attaques en particulier les transformations géométriques (RST).

Conclusion générale

Nous avons introduit le travail présenté dans cette thèse par un état de l'art du domaine du watermarking des documents numériques. Nous avons évoqué les aspects juridique et technique relatifs à ce domaine. Après avoir souligné les similitudes et les complémentarités avec d'autres techniques déjà existantes, la cryptographie et la stéganographie, nous avons présenté la structure générale des systèmes de watermarking, ainsi que les contraintes principales à prendre en considération lors de la conception de ces systèmes. Ensuite, un intérêt particulier a été accordé aux systèmes de watermarking d'image fixes qui représente l'axe de notre recherche. Après avoir présenté une étude des différents paramètres distinctifs, nous avons passé en revue quelques méthodes de tatouage d'images fixes.

Notre contribution dans ce domaine de watermarking d'image fixe est marquée par le développement de quatre méthodes [6][7][8][9][10] :

- La première méthode, qui représentait nous premiers pas d'exploration du domaine de watermarking, est basée sur l'utilisation de la transformée en cosinus discrète (*DCT*). L'idée de base consiste à choisir des endroits fortement éclairées, très sombres ou texturée pour insérer la marque. Le seuillage de la variance locale de la luminance permet de sélectionner les blocs aptes à abriter la marque L'approche mis au point possède certaines performances en terme d'invisibilité et de robustesse vis-à-vis la compression, le changement de format et la conversion en niveau de gris. Cependant, plusieurs problèmes restent à résoudre parmi lesquels on cite les suivant : manque de robustesse à des taux de compression très élevés et la limitation de l'espace d'insertion de la marque.

- La deuxième méthode est le résultat d'analyse des insuffisances de la méthode précédente. En effet, nous avons proposé une méthode hybride qui combine deux transformées à savoir : la Transformée en Ondelette Discrète (*DWT*) et la *DCT*. La transformée *DWT* permet de séparer complètement les basses fréquences dans la sous bande *LL*, appelée aussi approximation, des hautes fréquences qui représente les détails de l'image et qui sont données par les sous bandes *LH*, *HL* et *HH*. Ensuite, on s'intéresse uniquement à la sous bande *LL* puisque elle représente les basses fréquences. Un endroit d'insertion très sûre pour que la marque soit robuste surtout vis-à-vis les opérations de compression, de filtrage passe bas et d'ajout de bruit…etc. Mais, un endroit non sûr pour l'invisibilité de la marque. Pour résoudre ce problème on a fait recours à la *DCT* qu'on applique uniquement à la sous-bande

basse fréquences (*LL*). Ceci permet de séparer les basses, les moyennes et les hautes fréquences de *LL*. Par conséquent, et en comparaison avec l'approche de la première partie, le nombre de coefficients *DCT* aptes à supporter la marque devient très important.

- En plus de la robustesse vis-à-vis les attaques vues précédemment, la troisième méthode, a comme objectif principal de faire face aux problèmes de désynchronisation causés par les transformations géométriques (translation, rotation et changement d'échelle). Pour répondre à ce cahier de charge, nous avons opté à une combinaison de la *DWT*, la Transformée de Fourier Discrète (*DFT*) et la transformée de Fourier-Mellin (*FMT*). En effet, la première transformée offre un espace d'insertion de la marque intouchable par les effets de compression et de bruitage. La deuxième transformée (*DFT*) possède une amplitude insensible à la translation et la troisième (*FMT*) procure un domaine invariant à la rotation et au changement d'échelle. La synchronisation de l'extraction de la marque passe par la correction des déplacements, causés par des éventuelles transformations géométriques, localisés dans le spectre d'amplitude de la corrélation de phase entre les transformées logo-polaire (*LPM*) de l'image originale et celle marquée et transformée.
- Dans la quatrième approche et en plus de la nature du watermark qui est prise sous forme d'image, nous nous somme intéressé à l'aspect sécuritaire de la méthode de watermarking. La méthode développée est aussi hybride, mais qui combine avec la *DWT* une nouvelle classe de transformée appelée « *ROPT* » (*Reciprocal-Orthogonal Parametric Transforms*) [11]. L'idée de base derrière la méthode proposée consiste à utiliser une nouvelle méthode de génération de clés. Ceci en exploitant le grand nombre de paramètres indépendants (*3N/2*) fournis par la *ROPT* comme clé supplément de tatouage ajouté à celui utilisé pour l'insertion du watermark.

Donc nos travaux ont principalement porté sur deux aspects : l'invisibilité et la robustesse de la marque. L'étude comparative, présentée dans la deuxième partie du chapitre IV, entre la méthode basé *DCT* et celle basé *DWT+DCT* montre l'apport de la combinaison des transformées. En effet, cette combinaison porte une complémentarité entre les transformées *DWT* et *DCT*. Par conséquent les inconvénients d'une transformée sont couvert

par les avantages de l'autre transformée. C'est dans cette même optique de complémentarité que nous avons développé la troisième et la quatrième méthode.

Bien que les méthodes présentées possèdent des performances considérables et réalisent un compromis très acceptable entre l'invisibilité et la robustesse de la marque, mais plusieurs problèmes restent à résoudre. Ceci offre d'autres perspectifs d'amélioration et de développement.

Perspectives :

L'avantage du watermarking par rapport à la cryptographie c'est qu'il assure une circulation transparente des données sur les réseaux. Mais il ne possède pas encore la robustesse que peuvent procurer les outils de nature cryptographique. Car c'est un domaine récent et en plein période de croissance en comparaison avec la cryptographie qui est déjà mure, et ses techniques sont éprouvées depuis plusieurs décennies et largement utilisé. De nos jours aucun système de watermarking n'a prouvé son universalité

Les perspectives ouvertes par nos travaux peuvent être résumés dans les points suivants :

- Afin d'augmenter la possibilité d'insertion et de permettre une meilleur maitrise de la force de la marque, nous envisageons de développer de nouvelles techniques de modulation de la marque avec le contenu de l'image.
- Etendre les méthodes développées à la vidéo considérée comme étant une succession d'images.
- Dans le but de sécuriser la méthode de watermarking, nous envisageons de faire appel à la cryptographie asymétrique.
- S'orienter vers d'autres applications, en dehors du contexte sécuritaire du watermarking, telles que l'augmentation ou l'enrichissement des contenus (indexation multimédia, canal caché), la création de méta-documents,….etc.
- Afin d'améliorer le processus d'extraction de la marque qui nécessite une prise de décision dans un environnement altéré par les attaques, nous envisageons de faire appel aux techniques de la logique flou et les réseaux de neurones.

Bibliographie

[1]. M. Barni, F. Bartolini. "Watermarking Systems Engineering, Enabling Digital Assets Security and Other Applications", Signal Processing and Communications Series, Copyright 2004 By Marcel Dekker, Inc. New York. USA

[2]. M. Arnold, M. Schmucker, S.D. Wolthusen. " Techniques and Applications of Digital Watermarking and Content Protection". Computer Security Series, Copyright by Artech House, Boston. London

[3]. Vidyasagar M.Potdar, Song Han, Elizabeth Chang « A Survey Of Digital Image Watermarking Techniques », 3rd International Conference on Industrial Informatics (INDIN 2005). Copyright IEEE.

[4] M. Kutter. « Watermarking resisting to translation, rotation and scaling ». *In Proceedings* of SPIE, vol. 3528, pp. 423-431, Boston, USA, Nov. 1998.

[5]. I.Cox, J.Killian, T.Leighton, and T.Shamoon. "Secure spread spectrum watermarking for multimedia". IEEE Transactions On Image Processing. 6(12): 1673-1687, December 1997.

[6] A.Dahmani, A. Louchene, " Tatouage d'Image Fixe en Utilisant la Variance Locale des Blocs", 2nd International Conference on Electronics Systems CISE'09, 25-26 October 2009, Batna, Algeria.

[7] A.Dahmani, A. Louchene," Méthode Hybride DWT-DCT de Tatouage d'Image fixe ", Revue des Sciences et de la Technologie –RST- Vol 1, No. 2, 2010. pp. 28-39, Batna.

[8] A. Louchene, and A. Dahmani, "Watermarking Methode Resilient to RST and Compression Based on DWT, LPM and Phase Correlation", International Journal of Computers and Applications – ACTA Press- Vol. 35 No 1, pp. 1-8, 2013.

[9] A.Dahmani, A. Louchene, " A Watermarking Methode Based on Multi-Level DWT and New Class of Reciprocal-Orthogonal Parametric Transforms ROPT " , Revue des Sciences et de la Technologie –RST- Vol 3, No. 1, 2012. pp. 27-42, Batna.

[10] A.Dahmani, A. Louchene, "A Novel Digital Watermarking Methode Based on Multi-Level DWT and New Class of Reciprocal-Orthogonal Parametric Transforms ROPT ", The 2nd International Conference on Electronics and Oil, (ICEO'13) : From Theory to Applications March 05-06, 2013 university of Ouargla.

[11] S. Bouguezel, M. Omair Ahmed, " A New Class of Reciprocal-Orthogonal Parametric Transforms". IEEE Transactions on Circuits and Systems, Regular Papers, Vol. 56, No. 4, pp. 795- 805, April 2009.

[12] T. Pasquier, P. Treguer, C. Bareille, S. Bois, S. Martin, and A. Couillaud. « Rencontre avec le droit d'auteur », livre d'accompagnement de l'Exposition, Espace Mendès France de Poitiers, 2005.

[13] C. Crampes and J. Larrieu, « Aspects économiques et juridiques de la propriété intellectuelle », Formation CIES, Université des Sciences Sociales de Toulouse, 2004.

[14] V. Martin « Contribution des Filtres LPTV et des Techniques D'Interpolation au Tatouage Numérique » Thèse de Doctorat soutenue le 28 novembre 2006, Institut National Polytechnique de Toulouse.

[15] Webzine L'internaute, « Le projet de loi sur les droits d'auteurs adopté par l'assemblée : ce qu'il faut retenir ». *http:linternaute.com*, mars 2006.

[16] Dvd audio copyright specs merge.http://www.nytimes.com/library/tech/98/10/cyber/articles/29wipo.html, October 1998

[17] Office National Des Droits d'Auteur et des droits Voisins (ONDA) www.algerieinfo.biz/administration-algerie/onda-algerie.htm

[18] D. Kahn. « The code breakers ». Macmillan Publishing, 1967.

[19] G. Dubertret. « Initiation à la cryptographie ». Vuiber, 1998.

[20] G. Simmons. « The History of Subliminal Channels ». IEEE Journal on Selected Areas in Communications, Vol 16, No. 4 : pp.452-462. May 1998.

[21] D. Kahn. « The History of Steganography », Proc. Of First Int. Workshop on Information Hiding, Cambridge, UK, May 30-June1 1996. Lecture notes in Computer Science. Vol. 1174. Ross Anderson (Ed.).

[22] F.A.P.Petitcolas, R.J.Anderson, and M.G.Kunh. « Information Hiding- a Survey ». Proceedings of the IEEE, Vol 87, No. 7 : pp. 1062-1078. USA, July 1999.

[23] K. Tanaka, Y. Nakamura, and K. Matsui « Embedding Secret information into a Dithered Multi-level Image » in Proceedings of IEEE Military Communication Conference. pp.216-220. September 1990.

[24] C. F. Osborne, A. Z. Tirkel, G. A. Rankin, R. van Schyndel, W. J. Ho, and N. R. A. Mee « Electronic Water mark ». In Digital Image Computing Technology and Application, pp. 666-672, Austin (TX), USA, December, 1993.

[25] Paul Levinson, The Soft Edge : A Natural History and Future of the Information Revolution (1997).

[26] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoun, « Secure Spread Spectrum Watermarking for Multimedia », IEEE Trans. On Image Processing. Vol. 6, No. 12, pp. 1673-1687. (1997).

[27] JPEG 2000. http://www.jpeg.org/JPEG2000.html

[28] MPEG-4 Requirements Group-CfP for Identification and Protection of Content in MPEG-4. ISO document JTC1/SC29/WG11 N1714, 1997.

[29] Watermarking for DVD- CfP- http://www.dvcc.com/dhsg/, 1997.

[30] R.L. Pickholtz, D.L. Schilling and L.B. Millstein, "Theory of Spread Spectrum communications" a tutorial. IEEE Transactions on Communications, pp. 855-884, 1982.

[31] J.G. Proakis and M. Salehi. "Communication Systems Engeneering", Prentice Hall International Edition. 1994.

[32] V.Darmstaedter, J-F. Delaigle, D. Nicholson and B. Macq. « A Block Based Watermarking Technique for MPEG-2 Signals : Optimisation and Validation on real Digital TV Distribution Links ». In Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST'98), May 1998.

[33] J-F. Delaigle, C. De Vleeschouwer and B. Macq. « Watermarking Using a Matching Model Based on The Humain Visual System ». Ecole Thématique CNRS GDR-PRC ISIS : Information Signal Images Marly le Roi, Apr. 1997.

[34] J-F. Delaigle, J-M. Boucqueau, J-J. Quisquarter and B. Macq. « Digital Images Protection Techniques in a Broadcast Framework : Overview ». In Proceeding of European Conference on Multimedia Applications, Services and Techniques (ECMAST'96), pp. 711-728, Louvain-la-Neuve, Belgium, May 1996.

[35] J.R. Hernandez, F. Pérez-Gonzalez, J.M. Rodriguez and G. Nieto. « The impact of Channel Coding on The Performance of Spatial Watermarking for Copyright Protection » In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'98), vol. 5, pp. 2973-2976, 1998.

[36] H.Maître and S.Baudy. « Modèles Théoriques de Prédiction de Performance » Technical Report, Réseau National de la Recherche en Télécommunication, Projet Aquamars, Paris, -August 1999. Vit Fan

[37] A.J. Viterbi. « Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm » IEEE Transactions on Information Theory, vol. IT-13, pp. 260-269, April 1967.

[38] R. M. Fano. « A Heuristic Discussion of Probabilistic Decoding » IEEE Transactions on Information Theory, vol. IT-9, pp. 64-73, 1963.

[39] S. Voloshynovskiy, F. Deguillaume, and T. Pun. « Multibit Digital Watermarking Robust Against Local Nonlinear Geometrical Distortions » . In Pro. Int. Conf. On Image Processing, pages 999-1002, Thessaloniki, Greece, Oct.2001.

[40] A. Herrigel, S. Voloshynovskiy, and Y. Rytsar. « The Watermark Template Attack ». In Proc. SPIE, San Jose, CA, Jan. 2001.

[41] J. K. Su, J. J. Eggers, and B. Girod. « Optimum Attack on Digital Watermarks and its Defencse ». In Proc. Conf. On Signals, System and Computers, Asilomar, CA, Oct. 2001.

[42] A. Kerckhoffs. « La Cryptographie Militaire ». Journal des Sciences Militaires, vol. 9, pp. 5-38, 1883.

[43] F. A. P. Petitcolas. R. J. Anderson. And M. G. Kuhn. « Information Hiding- a survey ». Proceeding of the IEEE (USA). 87(7) : 1062-1078, 1999.

[44] S. Karzenbeisser and F. A. P. Petitcolas. « Information Hiding Techniques for Steganography and Digital Watermarking ». Artech House, 1999.

[45] F. Hartung and M. Kutter. « Multimedia Watermarking Techniques ». Proceeding of the IEEE. 87(7) : 1079-1107, July 1999.

[46] M. Maes, T. Kalker, J.P. Linnartz, J. T. F. G. Depovere, and J. Haitsma, « Digital Watermarking for DVD Video : Copy Protection », IEEE Signal Processing Magazine, 17(2000), no. 5, pp. 47-57.

[47] P. Bas. « Méthodes de tatouages d'images fondées sur le contenu ». PhD Thesis. Thèse de l'institut national Polytechnique de Grenoble, France 2000.

[48] M. Kutter, S. Voloshynovskiy, and A. Herrigel. « Watermark copy attack ». In Ping Wah Wong and Edward J. Delp, editors, *IST/SPIE's 12th Annual Symposium, Electronic Imaging 2000 ; Security and Watermarking of Multimedia Content II, volume 3971 of SPIE Proceedings*, San Joes, California USA, 23-28 jan 2000.

[49] A.M. Alattar. « Smart images using digimarc's watermarking technology ». In SPIE, editor, *Security and Watermarking of multimedia contents*, volume 3971, pp. 246-263, San Joes, California USA, january 2000.

[50] S. Craver, N. Mernon, B.L. Yeo and M.M. Yeung. « Can invisible watermarks resolve rightful ownerships ». Technical report 20509, IBM Reaserch Division, Yorktown Heights, NJ, July 1996.

[51] A. Manoury. « Tatouage D'Images Numériques par Paquets D'Ondelettes » thèse de Doctorat. Soutenue à l'Ecole Centrale de Nantes, le 21 Décembre 2001.

[52] B.Chen and G. Wornell. « An information-theoretic approach to the design of robust digital watermarking systems ». In *International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, Phoenix, AZ, March 1999.

[53] T. Kalker and J-P. Linnartz. « Improved watermark detection reliability using filtering before correlation ». *In Proceeding IEEE International Conference on Image Processing*, Chicago, USA, Oct. 1998.

[54] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun. « Attack modeling : towards a second generation watermarking benchmark ». *IEEE Transactions on Signal Processing N 81(2001)*, pp. 1177-1214, 2001.

[55] C.J. van den Branden Lambrecht and J.E. Farrell. « Perceptual quality metric for digitally coded color images ». *In Proceeding of EUSIPCO*, pp. 1175-1178, Trieste, Italy, Sep. 1996.

[56] A.B. Watson. « DCT quantization matrices visually optimized for individual images ». *Human Vision, Visual Processing and Digital Display IV, Bernice E. Rogowitz Editor, Proc. SPIE 1913-14*, 1993.

[57] I.J Cox, M.L. Mille and J.A. Bloom. « Digital Watermarking ». *Morgan Kaufmann Publishers*, 2001.

[58] Langelaar, G. C., R. L. Lagendijk, and J. Biemond, « Removing Spacial Spread Spectrum Watermarks by Non-Linear Filtering » *Ninth European Signal Processing Conference*, Island of Rhodos, Greece, September 1998, pp. 2281-2284.

[59] Voloshynovskiy, S., et al., « Generalized Watermarking Attack Based on Watermark Estimation and Perceptual Romodulation » in P. W. Wong and E. J. Delp, (eds), *Proceedings of Electronic Imaging 2000, Security and Watermarking of Multimedia Contents II*, San Jose, CA, January 2000.

[60] S. Craver, N. Mernon, B.L. Yeo and M.M. Yeung. « Resolving rightful ownership with invisible watermarking techniques : Limitations, attacks and implication ». Technical report, IBM Reaserch Report RC 20755, March 1997.

[61] D. Boneh and J. Shaw. « Collusion- Secure Fingerprinting for Digital Data ». *IEEE Transactions on Information Theory*, vol. 44, No 5, 1998.

[62] F. A. P. Petitcolas. R. J. Anderson. « On the limits of steganography ». *IEEE Transactions on Selected Areas in Communications*, 16(4) :474-481, May 1998.

[63] M. Kutter, and F. A. P. Petitcolas. « A Fair Benchmark for Image Watermarking System ». in P. W. Wong and E. J. Delp, (eds), *Proceedings of Electronic Imaging 1999, Security and Watermarking of Multimedia Contents*, San Jose, CA, January 1999, pp.226-236.

[64] S. Pereira et al. « Second Generation Benchmarking and Application Oriented Evaluation ». in I.S. Moskowitz, (ed.), *Information Hiding : 4th International Workshop, vol. 2137 of Lecture Notes in Computer Science*, Pittsburgh : Springer-Verlag, October 2001, pp. 340-353.

[65] V. Solachidis et al. « A Benchmarking Protocol for Watermarking Methods ». *Proceedings of the IEEE International Conference on Image Processing (ICIP'01),* Thessaloniki, Greece, October 2001, pp. 1023-1026.

[66] A.S. Cohen and A. Lapidoth, « The Gaussian Watermarking Game », *IEEE Transactions on Information Theory*, 48(6) :1693-1667, June 2002.

[67] P. Moulin and J.A. O'Sullivan, « Information-Theoretic Analysis of Information Hiding » *IEEE Transactions on Information Theory*, 49(3), March 2003.

[68] M. Costa, « Writing on Dirty Paper », *IEEE Transactions on Information Theory*, 29(3) :439-441, May 1983.

[69] J. O Ruanaidh and T. Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", in Proc. 4th IEEE Int. Conf. on Image Processing, ICIP'97, vol. I, Santa Barbara, CA, USA, October 1997, pp.536-539.

[70] A.K. Jain. "*Fundamentals of Digital Image Processing*". Prentice-Hall International. 1989.

[71] F. Autrusseau. "*Tatouage d'images fondé sur la modélisation du système visuel humain et sur la transformation Mojette*". These PhD, Ecole polytechnique de l'Université de Nantes, 2002.

[72] J.J. O Ruanaidh. W.Dowling. and F.Boland. "*Phase watermarking of digital images*". Proc. Of ICIP, 3:239-242, 1996.

[73] J-F. Delaigle, C. De Vleeschouwer and B. Macq. « Psychovisual approach for digital picture watermarking ». *Journal of Electronic Imaging*, 7(3) :319-336, May 1998.

[74] S. Winkler. " A perceptual distortion metric for digital color images". In Proceedings of the International Conference on Image Processing (ICIP'98), vol. 1, pp. 399-403, Chicago, Illinois, USA, Oct. 1998.

[75] S. Western, R. Lagendijk and J. Biermond. "Perceptual image quality based on a multiple channel HVS model". *In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'95)*, vol. 4, pp. 2351-2354, 1995.

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

[77] 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.

[78] J. L. Mannos and J. J. Sakrison. " The effects of a visual fidelity criterion on the encoding of images". *IEEE Transactions on Information Theory*, vol. IT-20, pp. 525-536, July 1974.

[79] P. Barten. " Evaluation of subjective image quality with the square-root integral method". Journal of Optical Society of America 7, pp. 2024-2031, 1990.

[80] A. De Rosa, M. Barni, F. Bartolini and A. Piva, " Watermark capacity measure incorporating in a model of the human visual system", *IST/SPIE's 13th International Symposium Electronic Imaging: Multimedia Processing and applications (Security and watermarking of multimedia contents III)*, 2001.

[81] D. J. Sakrison, " On the role of the observer and a distorsion measure in image transmission", *IEEE trans, on Com.*, Vol. 25, No 11, pp. 1251-1267, 1977.

[82] J.N. Graham, "Detection of gratting patterns containing two spatial frequencies; A compararison of a single channel and multiple channels models", *Vis, Research*, Vol. 11, pp. 251-259, 1971.

[83] R. Valois and K. Valoi, "Spatial vision", *Oxford Univ. Press*, 1988.

[84] C. D. Burr and S. A. Wiijensundra, "Orientation discrimination depends on spatial frequency", *Vis. Res*., Vol. 31, No7/8, pp. 1449-1452, 1991.

[85] S.J. Anderson, Burr D.C. and M. Morrone, "Two dimensional spatial frequency selectivity of motion sensitive mechanisms in human vision", *J.O.S.A.*, Vol. 8, pp. 1340-1351, 1991.

[86] G. C. Philips and H. Wilson, "Orientation bandwidths of spatial mechanisms measured by masking", *J.O.S.A.*, Vol. 1, No 2, pp. 226-232, 1984.

[87] S. Daly, " The visibility difference predictor: An algorithm for the assessment of image fidelity", *Proc. Of SPIE, Human Vision, Visual Processing and Digital Display*, Vol. III, pp. 2-15, 1992.

[88] A. Watson, " The cortex transform: rapid computation of simulated neural images", *Computer Vision and Image Processing*, 39, pp. 311-327, 1987.

[89] M. A. Georgeson and M. Harris, " Spatial selectivity of contrast adaptation: Models and data", *Vision Research*, Vol. 24, pp.729-749, 1984.

[90] J. G. Daugman, " Spatial visual channels in the Fourier plane", *Vision Research*, Vol. 24, No 9, pp. 891-910, 1984.

[91] A. Saadane, D. Barba and H. Senane, " The estimation of visual bandwidths and their impact in image decomposition and coding", *Proceedings of Visual Communications and Image Processing*, 1993.

[92] J.M. Foly, "Human luminance pattern mechanisms: Masking experiments require a new model", *J.O.S.A.* A 11(6), pp. 1710-1719, 1994.

[93] P.C. Theo and D.J. Heeger, "Perceptual image distorsion" *Proc. of SPIE*, vol. 2179, pp. 127-141, 1994.

[94] T. Kalker and A. Janssen, " Analysis of SPOMF detection". *Proc. Of IEEE conference on ICIP*, 1:316-319, 1999.

[95] S. Voloshynovskiy, A. Herrigel, N. Baumgartner, and T. Pun "A stochastic approach to content adaptive digital image watermarking". *International Workshop on Information Hiding*, pp. 212-236, 1999.

[96] J. F. Delaigle, C. De Vleeschouwer, B. Macq, and L. Langendijk. “Human visual system features enabling watermarking”. *Multimedia and Expo, 2002, ICME’02. Proceedings, 2002 IEEE International Conference.* vol. 2, pp. 26-29, 2002.

[97] F. Bartolini, M. Barni, V. Cappellini, and A. Piva. “Mask building for perceptually hiding frequency embedded watermarks”. In IEEE-ICIP’98, vol. I, pp. 450-454, Chicago (IL, USA), October 1998.

[98] A. B. Watson, G. Y. Yang, J. A. Solomon, and J. Villasenor. “Visibility of wavelet quantization noise”, IEEE Trans. Image Proc., 6(8): 1164-1175, 1997.

[99] E. J. Delp R. B. Wolfgan, C. I. Podilchuk. “Perceptual watermarks for digital images and video”, Proceedings of the IEEE, 87(7), pp. 1108-1126, july 1999.

[100] A. Saadan, F. Autrusseau. “Adaptive and perceptual watermarking of still image”. Traitement du signal- Volume 19- N° 4- Spécial 2001.

[101] K. Matsui and K. Tanaka. “Video-steganography: how to secretly embedded a signature in a picture”. Journal *of the interactive Multimedia Association Intellectual Property Project*, vol. 1, pp. 187-206, 1994.

[102] E.Koch and J. Zhao. “Towards robust and hidden image copyright labeling”. *IEEE Workshop on Nonlinear Signal and Image Processing*. Thessaloniki, Greece, 1995.

[103] J. Zhao. “A WWW service to embed and prove digital copyright watermarks”. *In Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST’96)*, 1996.

[104] J. Puate and F. Jordan. “Using fractal compression scheme to embed a digital signature into an image”. *In proceedings of SPIE Photonics East Symposium*, vol. 1, pp. 18-22, Boston, USA, November, 1996.

[105] D. Kundur and D. Hatzinakos. “Digital watermarking using multirésolutions wavelet decomposition”. *In International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, volume 5, pp. 2969-2972, Seattle, Washington, USA, May 1998. IEEE.

[106] H. Maître and S. Baudry. “Modèles théoriques de prediction de performance”. *Technical report, Réseau National de la Recherché en Télécomunication, Project Aquamars*, Paris, August 1999.

[107] J. R. Hernandez and F. Perez-Gonzalez. “Statistical analysis of watermarking schemes for copyright protection of images”. *Proceedings of the IEEE*, 87(7), pp. 1142-1143, July 1999.

[108] R. G. Van Schyndel, A.Z. Tirkel, and C.F. Osborne. “A digital Watermark”. *In IEEE, editor, ICIP’94*, vol. 2, pp.86-90, Austin (TX), USA, 1994.

[109] R. G. Wolfgang and E. J. Delp, "A Watermark for Digital Images", ICIP-96, vol. 3, pp 219-222.

[110] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, 35 (3&4), pp. 313-336, 1996.

[111] I. Pitas and T. Kaskalis, "Applying signature on digital images", *In IEEE Workshop on Nonlinear Signal and Image Processing*, pp. 460-463, Neos Marmaras, Greece, June 1995.

[112] I. Pitas," A Method for signature casting on digital images", *In Proceedings of the ICIP-96*, vol. 3, pp. 215-218, 1996.

[113] O, Bruyndonekx, J.J. Quisquater and B. Macq," Spatial Method for Copyright Labeling of Digital Images", *IEEE Workshop on Nonlinear Signal and Image Processing-NSIP'95*, pp. 456-459, 1995.

[114] C. Rey, "Tatouage d'image: Gain en robustesse et intégrité des images", Thèse de Doctorat de l'Université d'Avignon et des Pays de Vaucluse, Février 2003.

[115] F. Hurtung and B. Girot. "Watermarking for uncompressed and compressed video". *Signal Processing*, Vol. 66, N°.3, pp. 283-333,Mai 1998.

[116] B.Chen and G. Wornell. « Quantization index modulation : A class of provably good methods for digital watermarking and information embedding ». *IEEE Trans. on Information Theory*, pp. 1423-1443, 2001.

[117] J.J Eggers, R. Bauml, R. Tzschoppe, and B. Girod. "Scalar Costa Scheme for Information Embedding". *IEEE Trans. On Signal Processing*. Vol. 51(4), pp. 1003-1019, 2003.

[118] D. Coltuc and P. Bolon. "Watermarking by histogram specification", In Ping Wab Wong and Edward J. Delp, editors, *IS&T/SPIE's 11th Annual Symposium, Electronic Imaging '99 : Security and Watermarking of Multimedia Contents, volume 3657 of SPIE Proceeding*, pp. 252-263, San Jose, California USA, 23-29 January 1999.

[119] M.J.J Maes and C.W.A. M. van Overveld. "Digital watermarking by geometric warping". In IEEE- ICIP'98, volume II, pp. 424-429, Chicago, USA, October 1998.

[120] J. Zhao and E. Koch, « Embedding robust labels into images for copyright protection », In Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, KnowRight'95, Vienna, Austria, August 1995, pp. 242-251.

[121] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoun, « Secure Spread Spectrum Watermarking for Multimedia », *IEEE Transactions on Image Processing*, vol. 6(12), pp.1673-1687, December 1997.

[122] A. Piva, M. Barni, F. Bartolini, and V. Cappellini. «DCT based watermark recovering without resorting to the uncorrupted original image », *In Proc. ICIP*, pp. 520-523, 1997.

[123] A. Bors and I. Pitas. « Image watermarking using DCT domain constraint ». In Proc. ICIP, volume 3, pp. 231-234, Lausanne, 1999.

[124] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, and A. Piva, " A DWT-based technique for spatio-frequnecy masking of digital signatures", In Ping Wab Wong and Edward J. Delp, editors, *IS&T/SPIE's 11th Annual Symposium, Electronic Imaging '99 : Security and Watermarking of Multimedia Contents, volume 3657 of SPIE Proceeding*, pp. 31-39, San Jose, California USA, 23-29 January 1999.

[125] H. Inoue, et al., "A Digital Watermarking Technique Based on the Wavelet Transform and its Robstness on Image Compression and Transformation", *Proceedings of the 1998 IEEE International Conference on Image Processing (ICIP-98),* Vol. 2, pp.391-395, Chicago, October 1998.

[126] Wang, H.-J. M., P.-C. Su; and C.-C. J. Kuo,"Wavelet-Based Digital Image Watermarking". Optics Express 491, Vol. 3, N°. 12, December 1998.

[127] P. Meerwald, and A. Uhl. "A Survey of Wavelet-Domain Watermarking Algorithms", In Ping Wab Wong and Edward J. Delp, editors, *Proceeding of Electronic Imaging 2001, Security and Watermarking of Multimedia Contents III*, pp. 505-516, San Jose, California USA, January 2001.

[128]. C. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, Rotation, Scale, and Translation Resilient Watermarking for Image, IEEE Transaction on Image Processing, Vol.10, No.5, pp. 767-782, 2001. .

[129] Lin, C.-Y., et al., "Rotation, Scale and Translation Resilient Public Watermarking for Images", In Ping Wab Wong and Edward J. Delp, editors, *Proceeding of Electronic Imaging 2000, Security and Watermarking of Multimedia Contents II*, pp. 90-98, San Jose, California USA, January 2000.

[130] S. Pereira and T. Pun, "Robust Template Matching for Affine Resistant Image Watermark", IEEE Transactions on Image Processing, Vol. 9 No. 6, 2000, pp. 1123-1129.

[131] B. Kim, J. Choi, K. Park, F. Petitcolas, K. Hyoung Joong," Image Normalization Using Invariant Centroid for RST Invariant Digital Image Watermarking", First International workshop on digital watermarking, Seoul, Vol. 2613, 2002, pp. 202-211.

[132] J. Xuan, H. Zhang and L. Wang, "Rotation, Scaling and Translation Invariant Image Watermarking Based on Radon Transform", Visual Communication and Image Processing, edited by Li, Shipeng; Pereira, Fernando; Shum, Heung-Yeung; Tescher, Andrew G., Proceedings of the SPIE, Vol.5960, 2005,pp. 1499-1505.

[133] D. Zheng, J. Zhao. "A novel RST-Invariant Digital Image Watermarking Scheme", Third International Symposium on Multispectral Image Processing and Pattern Recognition, edited by Lu, Hanqing; Zhang, Tianxu, Proceedings of the SPIE, Vol. 5286, pp. 477-480, 2003.

[134] F. K. Mohamed and R. Abbes," RST Robust Watermarking Scheme Based on Image Normalization and DCT Decomposition", Malaysian Journal of Computer Science, Vol. 20(1), 2007, pp. 77-90.

[135]. R. Bracewell, "The Fourier Transform and Its Applications", McGraw-Hill, 2000, ISBN:0-07-303938-1.

[136]. R. Gonzalez and R. Woods, Digital Image Processing, Prentice-Hall, 2002, ISBN:0-201-18075-8.

[137]. C. D. Kuglin and D.C. Hines, The Phase Correlation Image Alignment Method, In Proc of The IEEE 1975 International Conference on Cybernetrics and Society (Sept.), pages 163-165,1975.

[138] Falkowski, B.J., Lim, L.S. "Image Watermarking Using Hadamard Transform". In IEEE Electronics Letters, United Kingdom, vol. 36, no.3, pp. 211-213, February 2000.

[139] Gilani, A.M. Skodras, A.N, "Watermarking by Multi-resolution Hadamard Transform", in Proceedings Electronic Imaging and Visual Arts (EVA 2001), pp. 73-77. Florence, Italy, March 26-30, 2001.

[140] Bogdan J. Falkowski, "Muli-Polarity Complex Hadamard Transforms for Phase Watermarking Algorithm", 6th International Conference on Information Communication and Signal Processing, pp. 1-5, December 2007.

[141] Gaurav Bhatnagar and Balasubramanian Raman, "Robust Watermarking in Multi resolution Walsh-Hadamard Transform", Proc. Of IEEE International Advance computing Conference (IACC2009), Patiala, India, 6-7 March 2009, pp. 894-899.

[142] Marjuni, A.; Logeswaran, R.; Ahmad Fauzi, M.F. " An Image Watermarking Scheme Based on Fast Walsh Hadamard Transformation and Discrete Cosine Transformation", International Conference on Networking and Information Technology, pp.289-293, June 2010.

[143] Franklin R.V, Manekandan.GRS, V.Santhi. "Entropy Based Robust Watermarking Scheme Using Hadamard Transformation Technique". International Journal of Computer Applications (0975-8887), Volume 12-No.9, January 2011.

Annexe A

L'algorithme *RSA*

Le procédé de cryptage *RSA* repose sur le fait que la factorisation d'un nombre composé du produit de deux nombres premiers est un calcul extrêmement complexe lorsque les nombres sont suffisamment grands. Les différentes étapes qui constituent ce procédé de cryptage sont les suivantes :

- La création des clés s'effectue en prenant deux nombres premiers *p* et *q*. On calcule le produit $n = p \times q$ de ces deux nombres.
- On trouve ensuite un nombre *e* tel qu'il soit premier avec *p-1* et *q-1*.
- On calcul enfin *d* tel que : $(d \times e)\ MOD\ (p - 1)(q - 1) = 1$.
- La clé publique est représentée par le couple [*e*, *n*].
- La clé privée est représentée par le couple [*d*, *n*].

Soit *m* le nombre à crypter et *c* le nombre décrypté :

- Pour crypter *m* on calcule $c = m^e\ MOD(n)$.
- Pour décrypter *c* on calcule $m = c^d\ MOD(n)$

La taille des clés *RSA* utilisées pour le commerce électronique est actuellement de 512 bits. Cependant la cryptographie est toujours confrontée à la puissance des calculateurs et à l'ingéniosité des cryptanalystes. A l'heure actuelle, l'utilisation d'une clé de taille 512 bits rend le système de cryptage *RSA* vulnérable, et les prochains schémas dédiés au commerce électronique utiliseront une clé de 1024 bits.

Annexe B

B.1 Les ondelettes

Les ondelettes, famille de fonctions déduites d'une même fonction, appelée ondelette mère, par opérations de translations et dilatations, ont trouvé, de par la puissance de leur théorie, des applications dans de nombreux domaines aussi variés que les mathématiques (analyse, probabilités), le traitement du signal (compression, astronomie, sismique), la physique (mécanique quantique, turbulence). En effet, cet outil permet la représentation de fonctions de $L2$, dans une base bien localisée en espace et en fréquence, offrant les avantages de l'analyse de Fourier et s'affranchissant des inconvénients du manque de localisation de cette dernière.

Lorsque le signal est analysé avec une grande fenêtre, le signal est de faible résolution : la forme générale du signal est alors obtenue. Plus la largeur de la fenêtre diminue, plus la résolution croît et présente ainsi les détails du signal.

B.2. Transformée en ondelettes continues

La transformée en ondelettes continue (CWT) s'écrit :

$$\gamma(s,\tau) = \int f(t).\Psi^{*}_{s,\tau}(t).dt \qquad (B.1)$$

La fonction f (t) (correspondant à un signal à analyser) est décomposée en une série de fonctions de base $\psi^{*}_{s,\tau}$ .Les ondelettes sont générées à partir d'une ondelette mère Ψ (t), par translation et dilatation :

$$\Psi_{s,\tau}(t) = \frac{1}{\sqrt{s}}\Psi\left(\frac{t-\tau}{s}\right) \qquad (B.2)$$

Avec S facteur de dilatation (ou coefficient d'échelle), et τ est le facteur de translation.

B.3. Transformée en ondelettes discrètes

La transformée discrète fait intervenir des dilatations et translations discrètes :

$$\Psi_{j,k}(t) = \frac{1}{\sqrt{s_0^j}} \Psi\left(\frac{t - k\tau_0 . s_0^j}{S^j{}_0} \right) \qquad (B.3)$$

Où ***j*** et ***k*** sont des entiers. En général, on prend τ_0 =0 et S_0 =0. Ces valeurs sont normalisées pour avoir de bases orthonormées d'ondelettes, donc décorréler les coefficients afin de réduire le volume d'information redondant.

B.3.1 Exemples d'ondelettes orthogonales

Les premières ondelettes qui sont nées des travaux de Meyer et Mallat, sont les ondelettes orthogonales. Il existe un certain nombre de familles d'ondelettes orthogonales couramment utilisées. Les plus connues sont sans doute les ondelettes de Haar et les ondelettes de Daubechies.

B.3.1.1. Ondelette de Haar

Un premier exemple d'ondelette orthogonale est l'ondelette de Haar. La fonction d'échelle dans ce cas est :

$$\phi_{haar} = x_{[0,1]}(t) \qquad (B.4)$$

et l'ondelette correspondante :

$$\psi_{haar} = x_{[0,1/2]}(t) - x_{[1/2,1]}(t) \qquad (B.5)$$

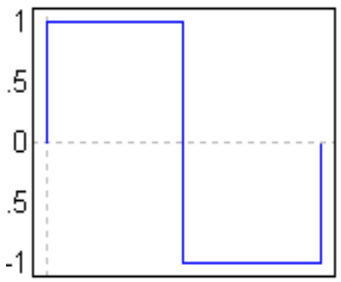


Figure B.1. Ondelette de Haar

B.3.1.2. Ondelette de Shannon

$$\psi_{SH} = \frac{\sin 2\pi - \sin \pi . t}{\pi t} \qquad (B.6)$$

Dont la fonction d'échelle est

$$\Phi_{SH} = \sin c(\pi.t) \qquad (B.7)$$

La fonction (B.7) n'est pas beaucoup utilisée en raison de sa très faible décroissance à l'infini. En effet, $\boldsymbol{\phi}_{SH}$ est très mal localisé en temps $\boldsymbol{\Delta\hat{\phi}_{SH} = \infty}$**.** La raison de cette mauvaise localisation en temps vient du fait que dans le domaine fréquentiel, $\boldsymbol{\hat{\phi}_{SH}(W) = \infty}$ comporte deux discontinuités à $\boldsymbol{-\pi}$ et $\boldsymbol{\pi}$ .En conséquence, dans le domaine temporel la fonction décroît en $\boldsymbol{1/t}$ et donc $\boldsymbol{\Delta\phi_{SH} = \infty}$**.**

B.3.1.3. Ondelette de Meyer

Meyer a construit une fonction d'échelle de telle sorte que sa transformée de Fourier soit lisse aux endroits de discontinuité de $\boldsymbol{\hat{\phi}_{SH}(W)}$ (voir ondelettes de Shannon). En temps, cela se traduit par une décroissance plus rapide à l'infini par rapport à l'ondelette de Shannon. La fonction d'échelle et l'ondelette sont symétriques respectivement par rapport à 0 et -1/2. Les ondelettes de Meyer sont des ondelettes indéfiniment dérivables, de support infini. Leur implémentation se fait plutôt dans le domaine fréquentiel.

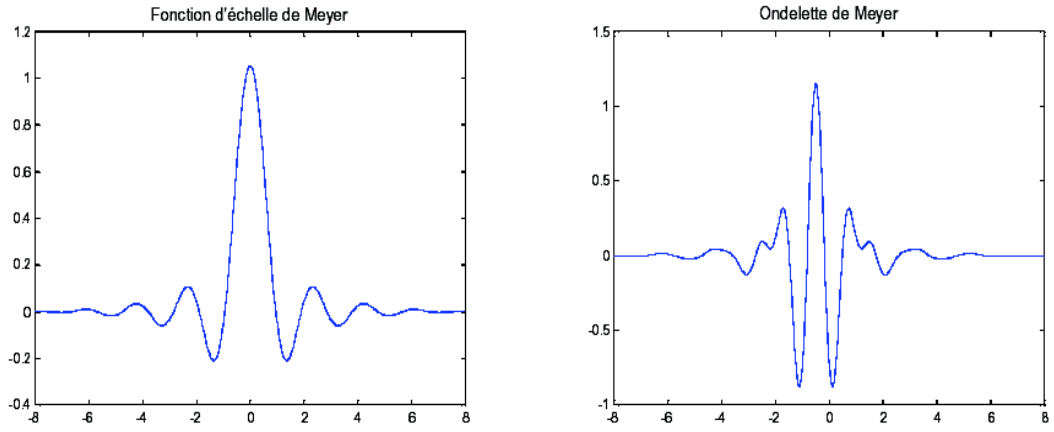


Figure B.2. Fonction d'échelles et ondelettes de Meyer**.**

B.3.1.4. Ondelette de Daubechies :

Les ondelettes de Daubechies sont probablement les plus utilisées en ce qui concerne les ondelettes orthogonales. Elles sont à support compact. Ces ondelettes seront notées **dbN, où** : **db** est le symbole donné pour Daubechies, et N est le nombre de moments nuls de l'ondelette. Les ondelettes de Daubechies sont supportées sur un intervalle de longueur **2N-1.** Ces ondelettes présentent l'inconvénient de ne pas être symétriques ou antisymétriques, excepté quand **N=1** ce qui correspond à l'ondelette de Haar. La figure (B.3) ci dessous représente les fonctions d'échelle et ondelettes pour N=2, N=4, et N=8.

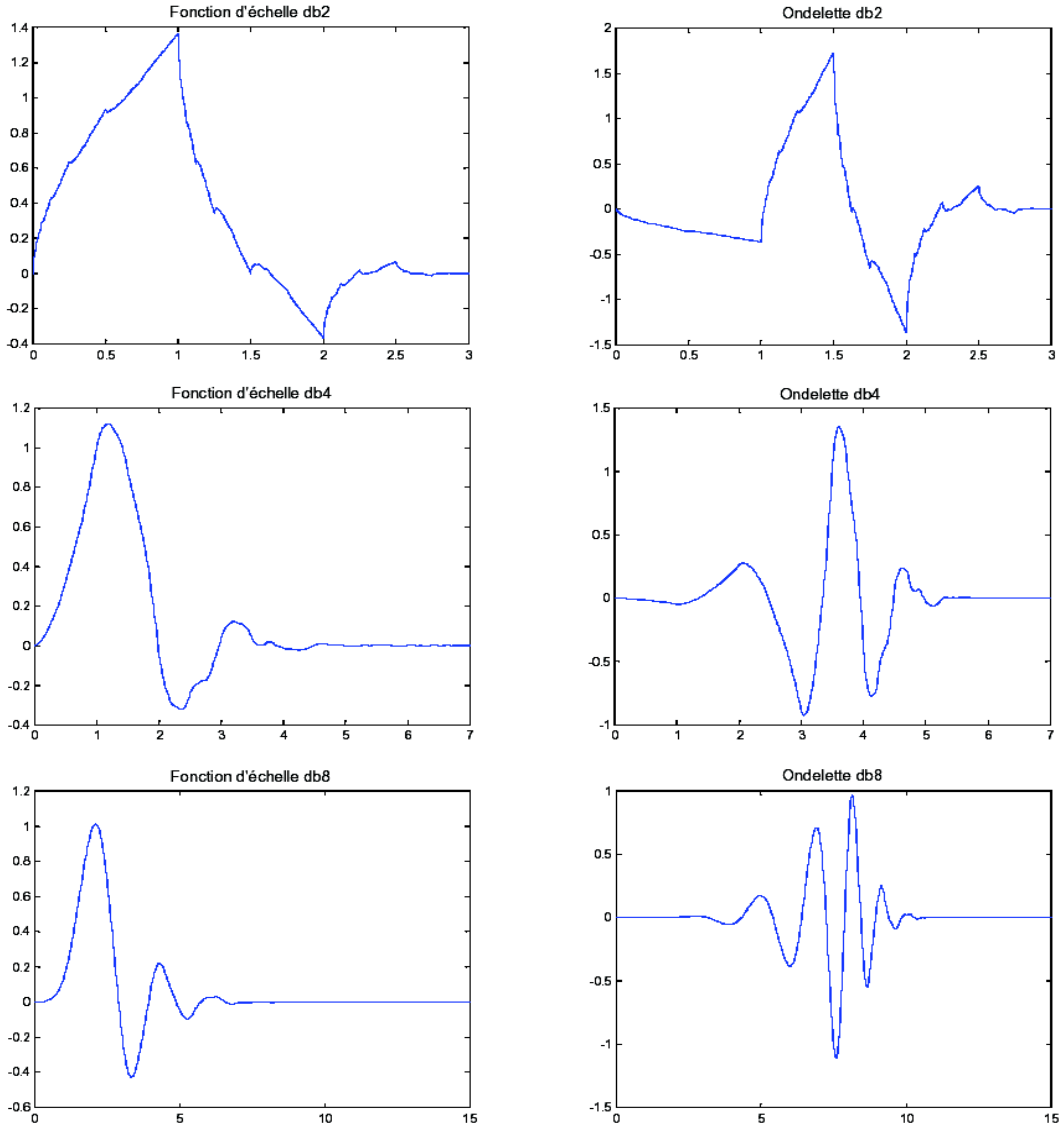


Figure B.3. Fonctions d'échelles et ondelettes de Daubechies pour *N=2, 4,8.*

B.3.1.5. Ondelette de Symlets

Pour obtenir une ondelette symétrique ou antisymétrique, le filtre ***h1*** doit être symétrique ou antisymétrique par rapport au centre de son support. Les Symlets sont des ondelettes de Daubechies construites de telle sorte que la phase de $\hat{h}_1(w)$ soit la plus linéaire possible. Le support des Symlets est *2N+1*. La figure (B.4) ci-dessous représente la fonction d'échelle et l'ondelette pour *N=8*. Une meilleure symétrie par rapport à l'ondelette de Daubechies (*N=8*) peut être remarquée.

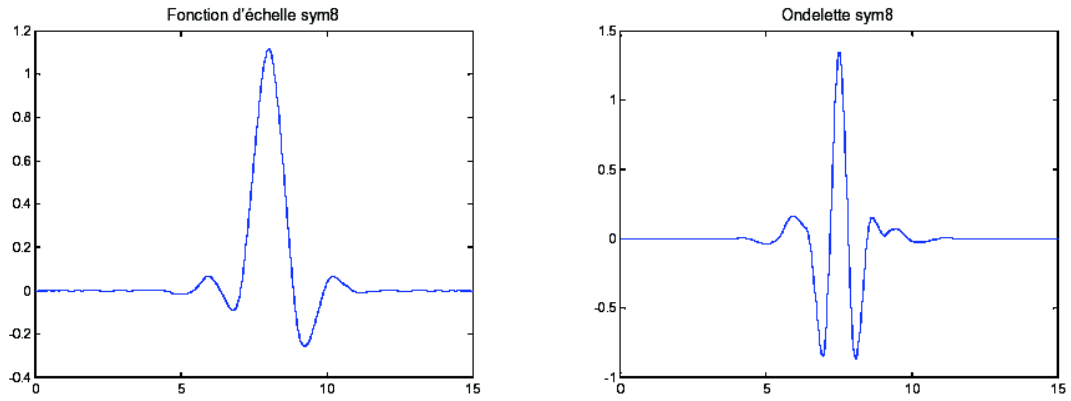


Figure B.4. Fonctions d'échelles et ondelettes de Symlets pour *N=8.*

B.3.1.6. Ondelette de Coiflets

Pour une application en analyse numérique, Coiflets a demandé à Daubechies de construire une famille d'ondelettes avec *N* moments nuls et un support de taille minimum, et dont la fonction d'échelle vérifie :

$$\int_{-\infty}^{+\infty}\phi(t)dt = 1 \quad et \quad \int_{-\infty}^{+\infty}t^{k}\phi(t)dt = 0 \quad pour \quad 1 \le k \le N \qquad (B.8)$$

Le résultat est l'ondelette coiflets dont la taille du support est *3N-1* au lieu de *2N-1* pour une ondelette de Daubechies. La figure (B.5) ci dessous représente la fonction d'échelle et l'ondelette pour *N=5*.

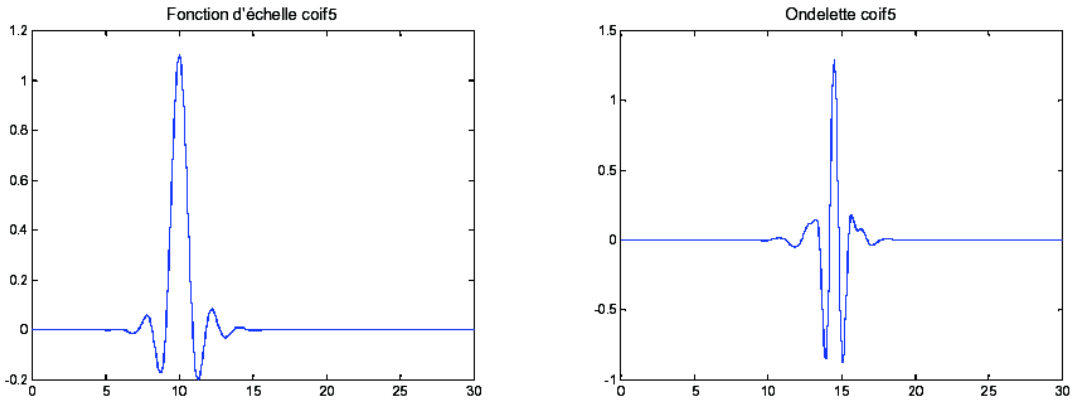


Figure B.5. Fonction d'échelle et ondelettes de Coiflets pour *N=5*.

Résumé

Le travail présenté dans cette thèse a pour objectif de proposer des méthodes hybrides de tatouage d'images numériques fixes. Ces méthodes sont basées sur l'utilisation combinée des domaines transformés obtenus par différentes transformées à savoir : la DCT, la DWT et une nouvelle classe de transformée appelée ROPT (Reciprocal- Orthogonal Parametric Transforms).

Summary

The work presented in this thesis proposes hybrid watermarking methods for still and digital images. These methods are based on the combined use of transformed domains obtained by different transforms namely: DCT, DWT and a new class of transforms called ROPT (Reciprocal- Parametric Orthogonal Transforms).

ملخص

يهدف العمل المقدم في هذه الأطروحة إلى اقتراح أساليب مختلطة للوشم الرقمي الخاص بالصور الرقمية الثابتة. وتعتمد هذه الطرق على الاستخدام المشترك للمجالات المحولة و الناتجة عن مختلف التحويلات مثل :DCT, DWT ونوع جديد يسمى تحويل (ROPT (Reciprocal- Parametric Orthogonal Transforms