

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique



UNIVERSITÉ FERHAT ABBAS - SETIF1

FACULTÉ DE TECHNOLOGIE

THÈSE

Présentée au Département d'Electronique

Pour l'obtention du diplôme de

DOCTORAT

Domaine : Sciences et Technologie

Filière: Electronique

Option: Electronique

Par

SAHIR Mourad

THÈME

Sécurisation des fichiers multimédia par tatouage numérique

Soutenue le 16 / 12 / 2025 devant le Jury:

BOUZIT Nacerdine	Professeur	Univ. Ferhat Abbas Sétif 1	Président
AMARDJIA Nourredine	Professeur	Univ. Ferhat Abbas Sétif 1	Directeur de thèse
BOUGUEZEL Saad	Professeur	Univ. Ferhat Abbas Sétif 1	Examineur
AIDEL Salih	Professeur	Univ. BBA	Examineur
KHEDROUCHE Djamel	Professeur	Univ. M'sila	Examineur
AIT KAKI Abdelaziz	MCA	Univ. Oum El Bouaghi	Examineur
BEKKOUCHE Tewfik	Professeur	Univ. BBA	Invité

Remerciements

Je tiens tout d'abord à exprimer mes sincères remerciements à **Monsieur le Professeur AMARDJIA Nourredine**, Mon directeur de thèse, pour son encadrement, pour son aide et ses conseils très précieux tout au long de ce travail. Merci ne suffira jamais à vous témoigner toute ma reconnaissance. Infiniment reconnaissant.

Je tiens aussi à exprimer ma profonde gratitude et mes meilleurs respects à Messieurs les membres de jury pour avoir accepté de juger mon travail et de m'honorer par leur présence et je suis très reconnaissant pour le temps et l'intérêt qu'ils ont accordé à cette recherche, et pour la qualité de leurs remarques, suggestions et critiques constructives qui ont permis d'en améliorer la qualité :

Monsieur BOUZIT Nacerdine, Professeur à l'Université Ferhat Abbas Sétif 1, à l'intérêt accordé à mon travail et qui m'a fait le grand honneur de présider ce jury. **Monsieur BOUGUEZEL Saad**, Professeur à l'Université Ferhat Abbas Sétif 1, **Monsieur AIDEL Salih**, Professeur à l'Université Mohamed El Bachir El Ibrahimi de Bordj Bou Arréridj, **Monsieur KHEDROUCHE Djamel**, Professeur à l'Université Mohamed Boudiaf de M'sila, **Monsieur AIT KAKI Abdelaziz**, Maître de conférences à l'Université d'Oum El Bouaghi, et **Monsieur BEKKOUCHE Tewfik**, Professeur à l'Université Mohamed Boudiaf de M'sila qui me font aussi le grand honneur en acceptant de participer à ce jury et de lire et d'évaluer ce travail. Ceux qui viennent de loin m'honorent de leurs présence malgré la distance.

Mes remerciements et reconnaissances sont également adressés à tous qui de près ou de loin m'ont aidé et encouragé dans ce travail :

Ma famille, mes parents et mon frère koceila.

Mr Bekkouche Tewfik.

Que tous les enseignants qui ont contribué à ma formation à l'Université de Sétif 1 trouvent en ce modeste travail, le témoignage de ma profonde gratitude en particulier les enseignants du département d'électronique.

Table des matières

Remerciements	
Introduction générale	1
Chapitre 1: Etat de l'art sur le tatouage numérique	
1.1. Introduction.....	6
1.2. Les techniques de protection.....	6
1.2.1. La cryptographie.....	7
1.2.2. La stéganographie.....	8
1.2.3. Le tatouage numérique.....	8
1.3. Principes généraux d'une méthode de tatouage.....	8
1.3.1. La phase d'insertion.....	9
1.3.2. La phase de transmission ou d'attaques.....	10
1.3.2.1. Attaques de bonne foi (bienveillante).....	10
1.3.2.2. Attaques malveillantes	11
1.3.3. La phase d'extraction.....	12
1.4. Les contraintes d'un schéma de tatouage efficace.....	13
1.4.1. Imperceptibilité.....	13
1.4.2. Capacité.....	14
1.4.3. Robustesse	14
1.4.4. Sécurité	15
1.4.5. La complexité.....	15
1.5. Classification des méthodes de tatouage selon le Domain d'application.....	15
1.5.1. Protection des droits d'auteurs.....	15
1.5.2. L'intégrité et l'authentification de contenu	16
1.5.3. Contrôle de copie.....	16
1.5.4. Indexation	16
1.6. Classification des algorithmes du tatouage numérique.....	16
1.6.1. Classification selon la technique d'insertion de la marque.....	17
1.6.2. Classification selon le domaine d'insertion.....	20

1.6.2.1. Domaine Spatial.....	20
1.6.2.1.1. Représentation spatiale de l'image.....	20
1.6.2.1.2. Insertion de la marque dans le domaine spatial.....	21
1.6.2.2. Domaine fréquentiel.....	23
Dans la transformée en cosinus discrète (DCT).....	23
Dans la transformée en ondelettes discrète (DWT).....	24
Dans la transformée de Fourier discrète (DFT)	24
Dans La décomposition en valeurs singulières (SVD).....	25
1.6.2.3. Domaine hybride.....	26
1.6.3. Classification selon la robustesse.....	27
A) Tatouage robuste.....	27
B) Tatouage fragile.....	27
C) Tatouage semi-fragile.....	27
1.6.4. Classification selon la perception de la marque.....	27
1.6.5. Classification selon la préservation de l'image originale.....	28
1.7. Critères d'évaluation des performances des algorithmes de tatouage d'images.....	28
1.7.1. Evaluation de la qualité visuelle d'une image tatouée.....	28
A) Dans le cas d'une image en niveaux de gris et binaire.....	28
B) Dans le cas d'une image couleur RVB.....	29
1.7.2. Critère de performance de robustesse.....	30
A) Dans le cas d'une image en niveaux de gris et binaire.....	30
B) Dans le cas d'une marque c'est une image couleur RVB.....	30
1.8. Conclusion.....	31

Chapitre 2: Tatouage numérique d'images dans le domaine transformées

2.1. Introduction	32
2.2. La Transformée de Fourier discrète (DFT).....	32
2.3. Transformée en Cosinus Discrète (DCT).....	34
2.3.1. La comparaison entre la DFT et la DCT.....	36
2.4. La transformée en ondelette discrète (DWT).....	37
2.4.1. Comparaison entre DWT et DCT.....	39
2.5. Décomposition en valeurs singulières (SVD).....	41
2.5.1. Algorithmes de Tatouage numérique Basés sur la décomposition SVD.....	42

A) Algorithme SVD de Chandra.....	42
B) Algorithme de R.Liu et T.Tan.....	43
C) Tatouage d'images en couleurs utilisant la transformée SVD	45
2.6. Décomposition de Hessenberg.....	47
2.7. Transformée d'Arnold.....	49
2.8. Domaine hybrides.....	50
1) La méthode DWT-DCT-SVD appliquée sur les images en niveau de gris	50
2) La méthode FRT-DWT-SVD appliquée sur les images couleurs RVB 24 Bits/pixels	52
3) La méthode DWT-HD-SVD appliquée sur les images couleurs RVB 24 Bits/pixels.....	56
2.9. Conclusion.....	59

Chapitre 3: Utilisation de l'algorithme ABC en tatouage numérique

3.1. Introduction	60
3.2. Les méthodes de résolution de problème d'optimisation.....	61
3.2. 1. Les méthodes hybrides.....	62
3.2. 2. Les méthodes exactes.....	62
3.2.3. Les méthodes approchées.....	62
3.2.3.1. Les méthodes heuristiques.....	62
3. 2.3.2. Les méthodes méta-heuristiques	63
3. 2.3.2.1. Les méthodes méta-heuristiques à base de solution unique.....	63
3. 2.3.2.2. Les méta- heuristiques à base de population de solutions	63
3. 2.3.2.2.1. L'intelligence par essaim.....	64
3.3. Optimisation par l'algorithme de colonie d'abeilles artificielles.....	64
3. 3.1. Principe du fonctionnement de l'algorithme d'abeilles artificielles.....	64
3. 3.2. Algorithme de colonie d'abeilles artificielles.....	66
Partie A. Résumé des étapes principales de l'algorithme.....	66
Partie B. Description détaillée de l'algorithme	67
Partie C. Le pseudo-code de l'algorithme ABC	70
3.4. Optimisation des facteurs d'insertion dans un algorithme de tatouage par l'algorithme ABC.....	72
3.5. Conclusion.....	76

Chapitre 4: Algorithme développé DWT-HD-SVD et comparaison des résultats

4.1. Introduction	77
4.2. Le schéma de tatouage proposé.....	78
4.2.1.Algorithme d’insertion de la marque	79
4.2.2. Algorithme d’extraction de la marque.....	83
4.2.3.Optimisation des facteurs d'insertion à l'aide d'algorithme (ABC).....	86
4.3. Résultats expérimentaux et discussions.....	88
4.3.1. Résultats d'imperceptibilité et analyse comparative.....	89
4.3.2. Résultats de la robustesse.....	94
4.3.2.1. Attaques non géométriques.....	95
4.3.2.2. Attaques géométriques.....	98
4.3.3. Conclusion	101
4.4. Analyse comparative.....	101
4.4.1.Comparaison avec schémas tatouage couleur la marque une image en niveaux de gris	101
4.4.2.Comparaison avec les schémas de tatouage couleur, la marque une image en couleur..	103
4.4.3.Attaques combinatoires.....	104
4.4.4. Analyse de la capacité d'intégration.....	105
4.5. Conclusion.....	106
Conclusion générale.....	107
Bibliographie	
Résumé	

Liste des figures

Chapitre 1: Etat de l'art sur le tatouage numérique

Figure 1.1 : Schéma générique de la cryptographie.....	7
Figure 1.2 : Schéma général du tatouage numérique.....	9
Figure 1.3 : Contraintes du tatouage numérique.....	14
Figure 1.4 : Classification des algorithmes de tatouage d'images.....	17
Figure 1.5 : Récupération du tatouage par la modulation dither (DM)	19

Chapitre 2: Tatouage numérique d'images dans le domaine transformées

Figure 2.1 : Image Lena et son module de TFD.....	33
Figure 2.2 : Distribution des fréquences des coefficients d'amplitude d'une DFT.....	34
Figure 2.3 : Différentes bandes de fréquences dans un bloc DCT 8x8.....	35
Figure 2.4 : La lecture fréquentielles en zig-zag dans un bloc DCT 8x8.....	36
Figure 2.5 : Principe de décomposition 2D par filtrage passe - bas ($g(n)$) et passe - haut ($h(n)$) dans le sens horizontal (Ligne) et vertical (Colonne).....	38
Figure 2.6 : Exemple d'une décomposition en ondelettes à 2 niveaux de résolution de l'image Barbara.....	39
Figure 2.7 : Application de la transformée d'Arnold directe et inverse sur l'image Lena après 15 itérations.....	49

Chapitre 3: Utilisation de l'algorithme ABC en tatouage numérique

Figure 3.1 : Classification des méthodes de résolution de problèmes d'optimisation.....	61
Figure 3.2 : Le processus d'optimisation des facteurs d'insertion (α).....	75

Liste des figures

.Chapitre 4: Algorithme développé DWT-HD-SVD et comparaison des résultats

Figure 4.1 : Le schéma bloc du processus d'insertion de la marque.....	82
Figure 4.2 : Le schéma bloc du processus d'extraction de la marque.....	85
Figure 4.3 : Le processus d'optimisation des facteurs d'insertion (α).....	87
Figure 4.4 : Images couleur hôtes (a-e).....	88
Figure 4.5 : Marques à insérer respectivement (f) et (g)	89
Figure 4.6 : Images tatouées avec la marque Peugeot logo: (a) Image Lena tatouée, (b) Image Baboon tatouée, (c) Image Peppers tatouée, (d) Airplane tatouée, (e) Image Sailboat tatouée, (f) marque extraite de (a), (g) marque extraite de (b), (h) marque extraite de (c), (i) marque extraite de (d) et (j) marque extraite de (e) sans présence d'attaques sur les images tatouées.....	90
Figure 4.7 : Images tatouées avec la marque 8- color image : (a) Image Lena tatouée, (b) Image Baboon tatouée, (c) Image Peppers tatouée, (d) Image Airplane tatouée, (e) Image Sailboat tatouée , (f) marque extraite de (a), (g) marque extraite de (b), (h) marque extraite de (c), (i) marque extraite de (d) et (j) marque extraite de (e) sans présence d'attaques sur les images tatouées.....	90
Figure 4.8 : PSNR sous différents facteurs d'insertion α pour les différentes images hôtes.....	92
Figure 4.9 : PSNR sous différents facteurs d'insertion α pour les différentes images hôtes.....	92
Figure 4.10 : NCC sous différents facteurs d'insertion α pour image Lena.....	93
Figure 4.11 : NCC sous différents facteurs d'insertion α pour image Sailboat.....	94
Figure 4.12 : L'évolution d'ABC après tatouage l' image Lena avec la marque Peugeot lego.....	95
Figure 4.13 : Image tatouée et marque extraite (Peugeot logo) après application d'attaques non géométriques: (a) JPEG(Q = 10), (b) JPEG2000 (CR= 5), (c) Salt and Pepper noise (0.05), (d) Gaussian noise (0.05), (e) Speckle noise (0.05), (f) Median filter (5×5), (g) Gaussian filter (5×5), (h) Mean filter (5×5), (i) Gamma correction (0.8), (j) Motion Blur (angle = 4, length = 7), (k) Sharpning (Radius = 2, Amount = 1), (l) Histogram Equalization (64 Bins).....	98
Figure 4.14 : Image tatouée (Lena) et la marque extraite (Peugeot logo) après application d'attaques géométriques : (a) Cropping (25 %), (b) Cropping (50 %), (c) Rotation (15°), (d) Rotation (30°), (e) Translation (10,10), (f) Translation (20,20), (g) Cut (20,20), (h) Scaling (0.5), (i) Scaling (2)	100
Figure 4.15 : Résultats d'attaques multiples sur l'image tatouée Baboon avec la marque Peugeot logo intégrée sous (a) compression JPEG (30) + rotation(1°), (b) filtre médian (2×2) + translation (20, 20), et (c) bruit sel et poivre (0,02) + découpage (10 ,10).....	105

Liste des tableaux

Chapitre 4: Algorithme développé DWT-HD-SVD et comparaison des résultats

Tableau 4.1 : Les valeurs des paramètres de l'algorithme ABC.....	88
Tableau 4.2 : Résultats d'imperceptibilité (PSNR) entre l'image hôte d'origine et tatouée, ainsi que la robustesse (NCC) entre la marque d'origine et la marque extraite pour le schéma de tatouage proposé sans attaques.....	89
Tableau 4.3 : Analyse comparative du schéma proposé avec divers autres schémas de tatouage pour l'imperceptibilité utilisant le PSNR (dB).....	91
Tableau 4.4 : Résultat du NCC de la marque extraite pour le schéma proposé utilisant Peugeot logo et 8-color image comme marques sous diverses attaques non géométriques.....	97
Tableau 4.5 : Résultat du NCC de la marque extraite pour le cas du schéma proposé utilisant Peugeot logo et 8-color image comme marques sous diverses attaques géométriques.....	100
Tableau 4.6 : Comparaison de la robustesse entre schéma proposé et ceux de [4, 5, 6], basée sur les valeurs de NCCs.....	102
Tableau 4.7 : Comparaison la robustesse du schéma proposé et des schémas de [7, 8], basée sur les valeurs NCCs.....	103
Tableau 4.8 : Comparaison des valeurs du NCC sous plusieurs attaques en utilisant la marque Peugeot logo.....	104
Tableau 4.9: La capacité d'intégration de diverses méthodes de tatouages numériques.....	105

Introduction générale

Introduction générale

En raison de la diffusion rapide et généralisée de grandes quantités de fichiers numériques, tels que des fichiers audio, des images, et des vidéos, via les systèmes de communication à haut débit, il est impératif de vérifier leur originalité et la propriété de leurs droits d'auteur. Par conséquent, pour protéger les données multimédia, nous devons concevoir un système de protection du droit d'auteur robuste, sécurisé, fiable et efficace. De nombreux systèmes de sécurité de l'information, tels que la stéganographie, la cryptographie, et le tatouage numérique, ont été proposés [1,2]. Le tatouage numérique représente l'une des meilleures solutions parmi toutes celles-ci [3].

Le tatouage numérique (ou filigrane numérique) consiste à intégrer une information confidentielle appelée marque ou tatouage et aussi filigrane tels que : un texte, logo, image, etc. dans un contenu hôte, à titre d'exemple une image, à l'aide de clés confidentielles. Cette marque peut être extraite ultérieurement pour prouver l'authenticité et la propriété du créateur [4].

Les schémas de tatouage numérique sont classés en trois classes [5,6], lors de l'extraction de la marque : schémas non aveugles, semi-aveugles et aveugles. Dans un schéma non aveugle, l'image hôte non tatouée (originale) est requise pour extraire la marque secrète intégrée (insérée). Dans un schéma semi-aveugle, la technique nécessite des informations supplémentaires et l'image tatouée pour extraire la marque. Dans un schéma aveugle, la marque secrète intégrée est extraite sans référence à l'image hôte.

Le schéma de tatouage est souvent divisé en deux classes en fonction de la perception humaine, telles que les schémas de tatouage visible et non visible. Dans le schéma de tatouage visible, la marque est insérée dans l'image hôte de manière à ce que l'utilisateur puisse la voir sur l'image tatouée [7]. Dans le schéma de tatouage invisible, la marque est insérée dans l'image hôte de manière à ce que seul l'utilisateur autorisé puisse y accéder [8].

Le tatouage numérique d'images repose principalement sur le processus d'insertion de la marque, qui s'effectue dans deux domaines clés (domaine spatial et domaine fréquentiel). Dans les approches du domaine spatial, le tatouage est directement intégré aux pixels [9]. L'intégration du tatouage dans le domaine spatial est une méthode directe. Elle présente plusieurs avantages, comme un coût de calcul réduit, une capacité élevée, une meilleure qualité perceptuelle, mais une moindre robustesse. Elle est principalement adaptée aux applications d'authentification. Dans les approches du domaine de transformation, une transformation mathématique est appliquée à l'image originale pour intégrer le tatouage aux

coefficients de transformation, puis l'application de la transformation inverse permet d'obtenir le tatouage intégré. Cette méthode est plus robuste.

Les méthodes les plus fréquemment utilisées reposent sur la transformée en cosinus discrète (DCT) [10], la transformée de Fourier discrète (DFT) [11], la transformée en ondelettes discrète (DWT) [12], la décomposition en valeurs singulières (SVD) [13] et la décomposition de Hessenberg (HD) [14]. Elles offrent une grande imperceptibilité et une bonne robustesse aux traitements d'images courants, et surtout, sont plus robustes que les techniques spatiales. L'imperceptibilité dépend de la similarité entre l'image hôte et l'image tatouée. La robustesse mesure la difficulté à supprimer ou à détruire le tatouage (la marque) de l'image tatouée [15], lors du processus d'extraction, la marque intégrée est extraite de l'image tatouée, puis comparée à la marque d'origine. Si elle est identique, les données sont authentifiées.

De nombreux chercheurs ont implémenté le tatouage numérique basé sur la SVD dans différents domaines tels que la DCT, la DFT et la DWT, etc. Le changement de domaine contribue à l'imperceptibilité et à la robustesse [16].

La technologie du tatouage numérique a fait des progrès considérables au cours des dix dernières années. Cependant, les schémas de tatouage conventionnels sont principalement conçus pour les images en niveaux de gris ou des images binaires, tandis que les schémas de tatouage des images couleur n'ont pas été suffisamment explorés. Cela s'explique principalement par le fait que les images en niveaux de gris sont faciles à traiter et ne contiennent que des informations sur la luminance. Contrairement aux images binaires et en niveaux de gris, les images couleur peuvent considérablement améliorer la capacité et la fidélité des informations. Dans le tatouage couleur, la perception des couleurs repose sur la luminance et la chrominance. Les images couleur peuvent être divisées en trois canaux de couleurs primaires, contrairement aux images en niveaux de gris à canal unique, le tatouage des images couleur est donc plus complexe.

Les techniques de tatouage dans les espaces couleur RVB, YIQ, YUV et YCbCr ont été étudiées et leurs performances comparées ont été analysées. Il a été démontré que l'intégration du tatouage dans l'espace couleur YCbCr était plus robuste que dans les espaces couleur RVB et YUV [17]. Par conséquent, nous avons choisi l'espace couleur YCbCr dans notre recherche. L'invisibilité (l'imperceptibilité) et la robustesse sont deux paramètres essentiels pour le tatouage numérique d'images, et le compromis entre elles constitue toujours un défi. Récemment, plusieurs algorithmes bio-inspirés ont été utilisés pour résoudre ce problème, tels

que l'évolution différentielle (DE) [18], l'algorithme génétique (GA) [19], l'optimisation par essaim de particules (PSO) [20] et la colonie d'abeilles artificielle (ABC) [21]. La méthode ABC a été largement adoptée en raison de ses nombreux avantages, tels qu'une convergence rapide, un nombre réduit de paramètres initiaux et une mise en œuvre simple [22]. Dans ce travail, la méthode ABC est utilisée pour trouver les facteurs d'insertion appropriés qui optimisent le compromis robustesse-imperceptibilité.

Objectif de la thèse

Dans la présente thèse de doctorat, qui traite le sujet sécurisation des fichiers multimédia par tatouage numérique, nous nous sommes concentrés sur deux principaux défis majeurs :

Le premier défi est la proposition d'une méthode de tatouage numérique des images couleurs robuste et sécurisée, qui intègre une marque qui est une image couleur dans une image couleur hôte, toutes les deux de la même taille en offrant une meilleure imperceptibilité, une capacité d'intégration élevée et surtout une grande robustesse, ainsi qu'une résistance réaliste aux attaques géométriques et non géométriques, afin d'assurer la protection des droits d'auteur et l'identification de la propriété.

Dans le but d'améliorer la sécurité et la robustesse de la marque intégrée, la transformée d'Arnold avec plusieurs itérations comme clé de sécurité est utilisée pour brouiller la marque. Dans le schéma proposé, si la clé secrète utilisée lors du brouillage est inconnue, personne ne peut récupérer l'image secrète du tatouage. Cette méthode est basée sur la décomposition de Hessenberg (HD) et la décomposition en valeurs singulières (SVD) dans le domaine de la transformée en ondelettes discrètes (DWT). Dans un premier temps, l'image couleur hôte et l'image du tatouage couleur dans l'espace RVB sont converties dans l'espace YCbCr, puis les données du tatouage sont intégrées au canal de luminance (Y) de l'image hôte. Dans ce travail, la composante principale de la luminance (Y) du tatouage est insérée dans la valeur singulière de l'image hôte avec un facteur d'insertion. Ce facteur d'insertion utilisé pour l'intégration de la marque permet de gérer le compromis entre l'imperceptibilité de la marque (le filigrane) et sa robustesse. Ce paramètre est choisi manuellement, pour chaque image couleur utilisée. Toutefois, ce choix n'aboutit pas forcément à une solution optimale et nécessite beaucoup de temps de tests. Il est donc essentiel de se disposer d'une technique pour automatiser le processus de sélection du facteur d'insertion optimal.

Le second défi est une amélioration de notre technique basée sur les DWT-HD-SVD. Dans cet algorithme, le choix d'un facteur d'insertion adéquat est la clé d'une conception

optimale. En l'occurrence, il est essentiel de maximiser l'imperceptibilité et la robustesse, ce qui nécessite donc l'utilisation d'une approche d'optimisation. En utilisant l'algorithme de la colonie d'abeilles artificielles (ABC), il est possible de déterminer les facteurs d'insertion optimaux pour avoir les meilleures performances en termes d'imperceptibilité et de robustesse. De plus, cette approche facilite l'automatisation de la sélection des facteurs d'insertion optimaux. Cette combinaison nous a conduits à l'aboutissement au développement d'une nouvelle technique de tatouage d'images couleur optimisée, basée sur la décomposition de Hessenberg et la SVD dans le domaine des ondelettes. Le schéma de tatouage proposé offre une grande capacité d'insertion, une bonne imperceptibilité de l'image tatouée et une grande robustesse face aux attaques géométriques (rotation, mise à l'échelle, recadrage, découpe,..., etc.), aux attaques non géométriques (filtrage, ajout de bruit, compression JPEG,..., etc.) et aux attaques combinatoires (géométriques et non géométriques en même temps).

Organisation de la thèse

Afin de réaliser ces objectifs, cette thèse est structurée autour de quatre chapitres :

Le chapitre 1, est dédié à la revue de la littérature sur le tatouage numérique. Après avoir exposé les différentes techniques de dissimulation de l'information, nous avons présenté le tatouage numérique et le principe de base du fonctionnement d'un système de tatouage (procédure d'insertion et d'extraction), les différents schémas qui mènent à l'intégration de la marque (sous forme d'additif ou substitutif). Une vue d'ensemble de la classification des différentes techniques de tatouage est ensuite donnée. Par la suite, nous avons mis en évidence les différentes attaques que peut subir le tatouage des images et nous avons abordé l'évaluation des performances d'un algorithme de tatouage qui regroupe (imperceptibilité et la robustesse).

Le chapitre 2, présente les différentes transformées discrètes souvent employées dans le domaine fréquentiel dans le cas du tatouage numérique des images fixes, et met l'accent sur l'usage de la SVD dans le cadre du tatouage numérique des images. Il présente également quelques méthodes très connues qui se servent de cette transformée pour intégrer des marques numériques. Il expose également différentes techniques de tatouage associées à la SVD dans le domaine fréquentiel, appliquées sur des images en niveaux de gris et couleur.

Le chapitre 3, se focalise sur l'optimisation en introduisant l'algorithme de la colonie d'abeilles artificielles. Cette méta-heuristique d'optimisation est inspirée du comportement astucieux des abeilles dans leur quête de nourriture. Elle a pour but d'être utilisée dans la recherche des

facteurs d'insertion optimaux pour un algorithme de tatouage numérique d'images fixes (en niveau de gris et couleur).

Le chapitre 4, est consacré à la présentation de notre contribution. Développement d'une nouvelle technique de tatouage d'images couleur optimisée, basée sur la décomposition de Hessenberg et la SVD dans le domaine des ondelettes. La technique est testée avec plusieurs images couleurs et le schéma de tatouage proposé a démontré une grande capacité d'insertion, une bonne imperceptibilité de l'image tatouée et une grande robustesse face aux attaques géométriques, aux attaques non géométriques et aux attaques combinatoires (géométriques et non géométriques simultanément) avec des comparaisons aux schémas de tatouage d'images développés récemment.

Cette thèse se termine par une conclusion générale qui résume notre méthode, rappelant les conclusions tirées et offre des perspectives pour cette recherche.

Chapitre 1

Etat de l'art sur le tatouage numérique

1.1. Introduction

Dans l'ère du numérique, avec l'émergence des technologies de l'information et de la communication (TIC) sur Internet, la diffusion massive de contenus numériques (images, vidéos et sons) est devenue omniprésente. Cette évolution a fait émerger des problématiques cruciales liées à la protection des droits d'auteur, à l'authentification des documents et à la lutte contre la contrefaçon. Dans ce cadre, le tatouage numérique s'impose comme une technique de sécurisation incontournable.

L'intérêt de ce chapitre est de présenter un aperçu général sur le tatouage numérique et ses applications dans différents domaines. Après avoir donné un aperçu sur les méthodes de camouflage (dissimulation) des informations, nous aborderons le sujet du tatouage numérique et le principe de base d'un système de tatouage (phase d'insertion et phase d'extraction), les différents schémas qui mènent à l'intégration de la marque (additive ou substitutive). Nous donnerons ensuite une vision de la classification des différentes techniques de tatouage. Ensuite, nous décrirons les différentes attaques que peut subir le tatouage des images et nous aborderons l'évaluation de la performance d'un algorithme de tatouage qui regroupe (imperceptibilité et la robustesse).

1.2. Les techniques de protection

La transmission sécurisée des informations repose sur un ensemble de techniques et de protocoles visant à protéger les données tout au long de leur parcours, depuis l'émetteur jusqu'au récepteur [1]. Parmi ces techniques, on trouve notamment la cryptographie, la stéganographie, le tatouage numérique et aussi appelé filigrane numérique. Dans l'univers de la sécurisation des informations, on admet que la cryptographie est l'art des codes secrets, elle vise à créer une représentation indéchiffrable d'un message ou d'une information (qui devient alors secrète). En revanche, la stéganographie cherche à dissimuler un message au sein d'un contenu pour qu'il ne soit pas simplement indéchiffrable, mais aussi indiscernable. Pour ce qui est du tatouage, cet autre principe de camouflage propose des approches techniques pour aborder les enjeux de protection des droits d'auteurs et de reproduction.

1.2.1. La cryptographie

La cryptographie est l'art de rendre **indéchiffrable** un message et ceci au sus de toute personne tierce [2,3]. La cryptographie est une méthode couramment employée pour sécuriser le contenu numérique des médias. Avant d'être transmis, le message est crypté puis décrypté à la destination de réception en utilisant une clé spécifique. Il est impossible d'accéder au contenu sans posséder la clé appropriée. On désigne le message à encoder sous le terme de texte en clair, tandis que le message une fois encodé est appelé texte chiffré (cipher text). La figure 1.1 illustre schématiquement la cryptographie. Elle satisfait les exigences des utilisateurs concernant la sécurité [4], telles que la protection de la vie privée, l'intégrité et l'identification.

1. L'intégrité : Le message que l'expéditeur envoie doit correspondre exactement au message que le destinataire déchiffre.
2. La confidentialité : L'objectif est qu'un individu interceptant les cryptogrammes ne soit pas en mesure de les déchiffrer.
3. L'authentification : Le destinataire doit être en mesure de confirmer sans aucun doute que le message vient bien de l'expéditeur prévu.

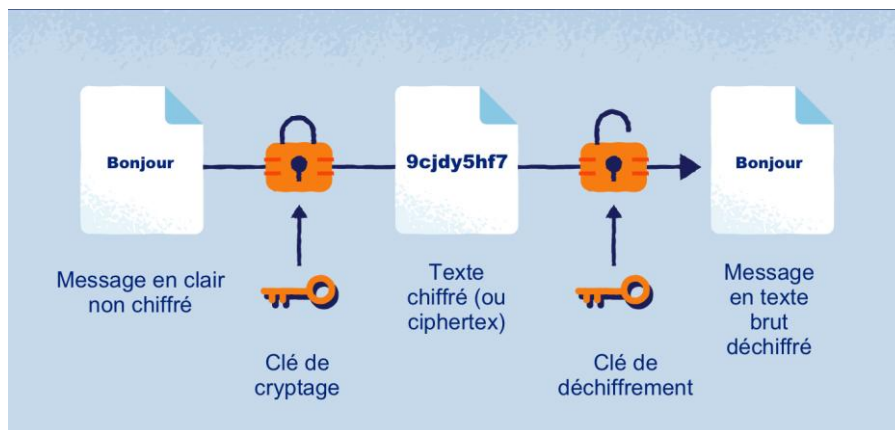


Figure 1.1 : Schéma générique de la cryptographie.

L'information est sécurisée jusqu'au moment de la transmission, mais une fois déchiffrée, elle devient non protégée et peut être reproduite et diffusée. Actuellement, deux des méthodes les plus couramment employées sont l'algorithme symétrique DES (qui fait appel à une clé de chiffrement et de déchiffrement identique, aussi connue sous le nom de clé privée) et l'algorithme asymétrique RSA (qui utilise deux clés distinctes, la clé privée pour le chiffrement et la clé publique pour le déchiffrement).

1.2.2. La stéganographie

La stéganographie consiste à dissimuler des informations en insérant un message dans un contenu anodin tel qu'une image, une vidéo ou un son [5], afin d'appliquer un processus de dissimulation inobservable. En d'autres termes, le but est de rendre ardu, voire impossible, de distinguer un document original d'un document altéré contenant le message caché. À la différence de la cryptographie, la stéganographie empêchera de suspecter l'existence de l'information elle-même (C'est l'art de la communication secrète).

1.2.3. Le tatouage numérique

Le **tatouage numérique** (ou filigrane numérique) est une technique qui consiste à insérer un message appelé marque ou tatouage et aussi appelé filigrane (**watermark** en anglais) dans un contenu numérique tel qu'une image, une vidéo, un son ou un document texte [6]. Ce tatouage ou marque et aussi appelé filigrane peut contenir des informations sur le propriétaire, des données d'authentification, ou encore des éléments de traçabilité, dont l'objectif principal est de protéger les droits d'auteur, de vérifier l'intégrité des données ou d'assurer le suivi de l'utilisation d'un contenu, tout en veillant à maintenir la qualité perceptible de l'original. Contrairement à la stéganographie, qui vise à dissimuler l'existence d'un message secret, le tatouage numérique cherche principalement à associer durablement une information au contenu, de manière robuste face aux modifications éventuelles (compression, recadrage, bruit,..., etc.). Le tatouage peut être **visible** (par exemple un logo) ou **invisible** (non perceptible à l'œil ou à l'oreille humaine dans le cas d'un son).

1.3. Principes généraux d'une méthode de tatouage

Comme mentionné précédemment, le tatouage numérique est une procédure qui consiste à intégrer une marque numérique (ou filigrane) W , généralement imperceptible dans un **signal original**, également appelé **signal hôte** I_0 . Ce filigrane contient des informations pouvant être utilisées dans une variété d'applications, telles que la défense des droits d'auteur, le suivi de diffusions, l'authenticité des données ou encore la transmission sécurisée [7]. Sa présence est signalé lorsqu'un **détecteur** approprié détecte le média tatoué. Le **filigrane (marque numérique)**, qui peut être défini comme une séquence aléatoire, un logo binaire ou une image en niveaux de gris ou en couleur, est inséré dans le signal d'origine, réalisé par le biais de l'encodeur. Par conséquent, un **encodeur** dispose de deux entrées : la première est le filigrane W (souvent

accompagné d'une clé secrète K) et la seconde est le signal d'origine I_o (qui peut correspondre à une image, un extrait vidéo ou un enregistrement audio, etc.). Le **signal tatoué** I_w , qui ne peut pas être perceptuellement différencier du signal original, est obtenu à la sortie de l'encodeur. Le décodeur identifie la présence d'un filigrane (ou marque) dans le média analysé, et s'il en détecte un, il sera extrait. Lorsque l'on envisage le codeur de filigrane (du tatouage) en tant qu' émetteur au sein d'une chaîne de communication, l'extracteur de filigrane peut être assimilé à un récepteur. Ainsi, le processus de filigrane numérique peut être composé de trois phases fondamentales : l'insertion, la transmission (éventuellement sujette à des attaques) et la détection (ou extraction). La Figure 1.2 présente de manière générale l'application du tatouage numérique à une image.

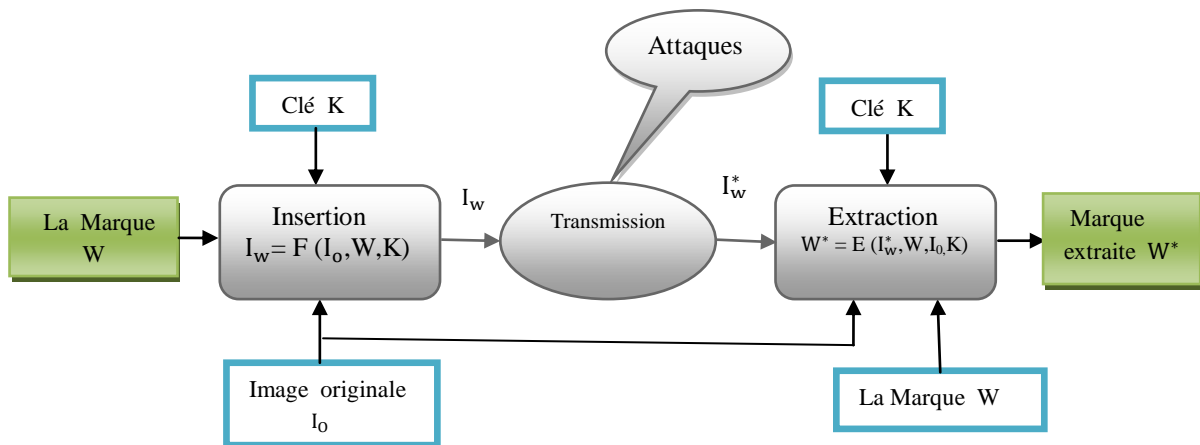


Figure 1.2 : Schéma général du tatouage numérique.

1.3.1. La phase d'insertion

Lors de l'étape d'intégration (d'insertion) du filigrane (la marque), également dénommée phase de codage, le processus d'intégration prend en entrée une marque W , une image hôte originale I_o et une clé secrète K qui est exclusive au tatoueur. Celle-ci est employée pour améliorer la sécurité de l'ensemble du système de tatouage. L'image filigranée (tatouée) I_w est le résultat de l'intégration de la marque W dans l'image originale I_o via une fonction d'insertion F . Cette étape est représentée par la fonction ci-dessous [8] :

$$I_w = F(I_o, W, K) \quad (1.1)$$

1.3.2. La phase de transmission ou d'attaques

L'image tatouée I_w est par la suite copiée et attaquée, ce qui est représenté par la transmission à travers un canal affecté par un bruit. L'image reçue filigranée (tatouée) et attaquée est appelée I_w^* . Les attaques de tatouage numérique sont caractérisées comme toutes les procédures qui pourraient rendre la marque invisible ou illisible. On distingue deux principales sortes d'attaques, à savoir les bienveillantes et les malveillantes.

1.3.2.1. Attaques de bonne foi (bienveillantes)

Toutes les actions ou interventions réalisées dans le but est d'altérer ou de dissimuler quelques propriétés de l'image sans le but d'éliminer le filigrane, sont catégorisées comme des attaques bienveillantes. Il n'est pas facile de réaliser une analyse détaillée de l'ensemble de ces attaques en raison de leur nombre important. Cependant, nous nous limiterons à présenter les traitements les plus fréquemment utilisés.

- 1) **La compression** : Toute méthode de tatouage robuste devrait être capable de supporter jusqu'à un certain degré de compression. L'intérêt de la compression est de minimiser au maximum le volume des données contenues dans un document. Ce processus vise à supprimer les éléments moins significatifs sur le plan perceptif tout en conservant les éléments clés du document.
- 2) **Le filtrage** : Le filtrage est une technique fondamentale en traitement d'images, souvent employée pour l'élimination du bruit. Ce genre de filtrage tend à réduire les éléments haute fréquence de l'image, ce qui entraîne une dégradation des éléments du filigrane inséré dans ces fréquences.
- 3) **Les transformations valométriques** : Des modifications courantes dans le domaine du traitement d'images comprennent, entre autres, l'étalonnage, l'égalisation de l'histogramme, et la transformation Gamma,..., etc. Elles visent à modifier l'intensité de chaque pixel de la luminance de l'image au moyen d'une fonction linéaire ou non, dans le but de perfectionner l'apparence visuelle de l'image.
- 4) **Le bruit** : L'introduction accidentelle d'un bruit de grande ampleur peut entraîner un impact de la dissimulation du filigrane et donc entraver son identification. A titre d'exemple une impression d'image accompagnée d'une numérisation.

5) Transformations géométriques

Ce type de modification n'a pas un but pour supprimer le filigrane, mais plutôt à le rendre invisible même si il est toujours présent dans l'image. Ces transformations provoquent une désynchronisation entre le filigrane inséré dans l'image et le décodeur. Pour la plupart des algorithmes de tatouage, le décodeur doit savoir précisément où se trouve le filigrane dans l'image. On peut mentionner plusieurs types de transformations géométriques, telles que les transformations affines (translation, rotation et modification d'échelle), le recadrage (cropping en anglais), qui vise à éliminer une portion de l'image. On trouve également des modifications géométriques telles que l'attaque StirMark, cette agression implique une série de déformations géométriques choisies au hasard et utilisées sur place à divers points de l'image [9].

a) Rotation :

De légers changements d'angle appliqués à l'image tatouée peuvent faire en sorte que le filigrane ne soit pas indétectable.

b) Stirmark :

Il s'agit d'une série de déformations géométriques aléatoires faites sur plusieurs pixels d'une image, soit de manière globale, soit locale.

c) Cropping (rognage) :

Utilisé pour supprimer ou sectionner une partie de l'image tatouée.

d) Scaling (mise à l'échelle) :

On applique cette méthode sur une image numérique dans le but de modifier ces dimensions.

1.3.2.2. Attaques malveillantes

C'est des opérations spécifiques destinées à détruire volontairement le filigrane (la marque) ou à entraver son extraction/détection. On peut utiliser l'ensemble des attaques évoquées auparavant dans cet objectif. On mentionne également l'attaque par marquage excessif ou par plusieurs tatouages. Cette attaque vise à un sur-marquage d'une image déjà marquée, classant ce genre d'attaques dans la classe des ambiguïtés ou de confusion [10].

La première catégorisation a été proposée par Hartung et al. [11] : elle concerne les attaques qui n'altèrent pas de façon significative la qualité de l'image d'origine. Cette catégorisation identifie les quatre classification ci-dessous :

1) Attaques basiques : Elles visent à compromettre le filigrane incorporé en manipulant l'intégralité des informations de l'image tatouée, sans chercher à localiser et séparer spécifiquement le filigrane (la marque). Parmi les possibles opérations, on peut citer le filtrage,

l'ajout de bruit, la correction gamma, la compression JPEG, et la quantification dans le domaine spatial.

- 2) Attaques de détection impossibles : également appelées attaques de synchronisation, elles visent à rendre le processus de détection irréalisable, principalement par des transformations géométriques .
- 3) Attaques d'ambiguïté : Aussi appelées de confusion. Ces attaques cherchent à créer une confusion en générant des images contrefaites et filigranées (tatouées). Un cas illustratif en introduisant une ou plusieurs filigranes supplémentaires, rendant ainsi complexe l'identification du filigrane d'origine.
- 4) Attaques d'enlèvement : Ce sont des attaques qui essaient d'examiner les images filigranées (tatouées), et après de séparer l'image originale et le filigrane (la marque) qui sera éliminé(e).

1.3.3. La phase d'extraction

La détection/extraction reçoit en entrée l'image filigranée (marquée) et potentiellement attaquée I_w^* , la clé secrète K , l'image originale I_o et le filigrane (la marque) original W .

L'étape d'extraction implique le calcul d'une estimation W^* de W . Elle est représentée par la fonction :

$$W^* = E (I_w^*, W, I_o, K) \quad (1.2)$$

La lettre E représente la fonction d'extraction.

En fonction des informations nécessaires à l'extraction de la marque, les systèmes de tatouage numérique sont classés en trois schémas [12] : aveugle, semi-aveugle et non aveugle. Si I_w n'est pas modifiée (attaquée), alors la marque extraite W^* correspond exactement à la marque originale W .

A) La détection dans le cas du schéma aveugle : Est la forme de tatouage la plus ancienne. L'extracteur ne demande pas de connaître l'image originale, ni du tatouage (la marque) au moment de l'extraction, il ne doit rester que l'image tatouée et la clé secrète K . L'extraction est modélisée de la manière suivante :

$$W^* = E (I_w^*, K) \quad (1.3)$$

On peut mentionner les recherches de [13, 14] dans cette catégorie de méthodes.

B) La détection dans le cas du schéma semi-aveugle : une détection semi-aveugle n'utilise pas l'image originale, tandis que, la marque originale est nécessaire. Des informations complémentaires sont nécessaires pour faciliter la détection ou l'extraction. L'extraction est représentée par le modèle suivant :

$$W^* = E(I_w^*, W, K) \quad (1.4)$$

Parmi les méthodes de cette catégorie, on peut mentionner les études [15, 16].

C) La détection dans le cas du schéma non-aveugle : On dit que la détection est non-aveugle lorsqu'elle utilise l'image originale et la clé secrète (K) pour effectuer la détection. Voici comment l'extraction est représentée par le modèle suivant :

$$W^* = E(I_w^*, W, I_o, K) \quad (1.5)$$

On peut mentionner les études [17, 18] parmi les méthodes de cette catégorie.

Généralement la robustesse des schémas **non-aveugle et semi-aveugle** est plus importante que celles des schémas **aveugles**.

1.4. Les contraintes d'un schéma de tatouage efficace

Les techniques de tatouage nécessitent diverses caractéristiques en fonction de leurs domaines d'utilisation et de leurs objectifs. Dans un document, la marque dissimulée doit se conformer à certaines conditions fondamentales. Généralement, il existe quatre critères clés fréquemment utilisés pour évaluer l'efficacité d'une méthode de tatouage. Ces éléments incluent l'invisibilité (l'imperceptibilité), la robustesse, la capacité et la sécurité [19].

1.4.1. Imperceptibilité

La qualité de l'image d'origine ne devrait pas être altérée après qu'elle ait été tatouée par le filigrane (la marque). Selon les auteurs [19], l'imperceptibilité est décrite comme la ressemblance visuelle entre l'image originale et l'image marquée. Le filigrane inséré doit être totalement invisible pour le système visuel humain (SVH). L'intégration ne doit pas dégrader de manière perceptible l'image originale, en d'autres termes, l'image tatouée doit être identique visuellement à l'image d'origine. Il est essentiel de préserver la pureté de l'image et si la marque est visible, son élimination pourrait être relativement aisée. L'attribut d'invisibilité concerne uniquement le tatouage numérique imperceptible.

1.4.2. Capacité

La capacité peut être déterminée par la quantité d'informations que l'on est en mesure d'incorporer dans l'image hôte originale. Effectivement, l'intégration de la marque est conditionnée par le nombre de pixels susceptibles d'être modifiés. Il est démontré qu'en général, plus la dimension de la marque est importante, plus l'image tatouée sa détérioration est significative (la marque est davantage est visible).

1.4.3. Robustesse

La robustesse fait référence à la faculté du filigrane à tenir bon face aux modifications du contenu sur lequel il est inséré. Ces modifications englobent toutes les attaques, de type intentionnelles ou non. Le premier cherche à éliminer la marque intégrée dans un contenu, alors que le second vise à modifier la marque plutôt qu'à la supprimer. Par exemple, dans beaucoup de systèmes qui nécessitent le sauvegarde et la diffusion d'images, une méthode de compression avec pertes est mise en œuvre pour diminuer la dimension des données et par conséquent améliorer l'efficacité du système. La compression est donc considérée comme une agression envers la marque. Par ailleurs, les images numériques peuvent être facilement manipulées (par exemple, zoomer, filtrage,...,etc.) grâce à l'utilisation de logiciels très courants. Ces changements peuvent alors poser un risque pour la qualité du tatouage. Les créateurs des schémas de tatouages cherchent donc à rendre leur marque robuste face à la multitude d'épreuves.

Ces trois exigences (imperceptibilité, capacité et robustesse) sont en opposition. Par exemple, si l'on augmente le facteur d'insertion (la force du marquage) pour rendre le tatouage plus résistant, cela aura pour conséquence inverse de le rendre plus visible. En d'autres termes, si on augmente la quantité d'information du tatouage à intégrer, cela se traduira par un tatouage plus apparent et moins résistant. Ainsi, une solution doit être trouvée en équilibrant ces trois critères pour mettre en place une technique de tatouage numérique. J. Fridrich [20] illustre la relation compromis entre l'invisibilité, la robustesse et la capacité à travers un triangle mis en lumière par la figure (1.3).

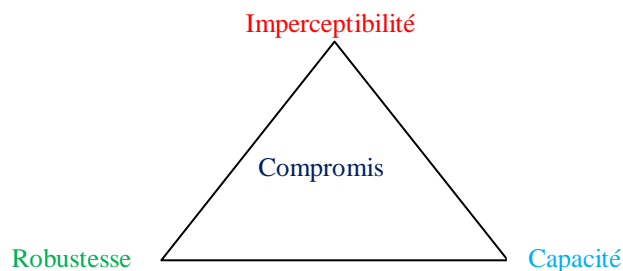


Figure 1.3 : Contraintes du tatouage numérique.

1.4.4. Sécurité

Dans un grand nombre d'applications, le processus d'intégration doit être sécurisé afin qu'un adversaire ne puisse pas extraire ou supprimer la marque. Le dispositif de sécurité est inviolable à moins que l'utilisateur dispose de la clé secrète permettant d'insérer la marque. Ainsi, un modèle de tatouage est réellement sécurisé lorsque la connaissance précise de la méthode d'intégration du marquage ne permet pas à un individu non autorisé d'extraire cette marque. Les exigences de sécurité évoluent en fonction des applications, les plus strictes étant celles utilisées dans le domaine des communications [21].

1.4.5. La complexité

Pour certaines applications de tatouage, le coût du calcul occupe une importance considérable. Habituellement, la durée nécessaire pour le calcul doit être inférieure à un certain seuil. A titre d'exemple, au sein du domaine du contrôle et de diffusion, il est nécessaire d'effectuer l'intégration et la détection en temps instantané. En revanche, pour les applications de protection des droits d'auteur, le délai n'est pas un critère essentiel pour l'exécution pratique.

1.5. Classification des méthodes de tatouage selon le Domain d'application

Les schémas de tatouage numérique sont élaborés en tenant compte de diverses applications, parmi celle-ci on peut citer :

1.5.1. Protection des droits d'auteurs

L'application initiale considérée en matière de tatouage des images a été la protection des droits d'auteur. Malgré tout, ce service est toujours en vigueur et concerne la plupart des publications. Le but est de permettre, en présence du conflit, au détenteur d'une image de démontrer qu'il est véritablement le propriétaire, malgré que l'image en question a été altérée par rapport à l'originale [22].

1.5.2. L'intégrité et l'authentification de contenu

Pour assurer la validité du contenu, toute modification ou intervention sur celui-ci doit être identifiée, et il est nécessaire de s'assurer que l'image n'a pas été altérée par rapport à l'image originale tout en respectant l'identité du patient ou du médecin [23]. Cela peut être accompli en utilisant un tatouage fragile ou semi-fragile qui présente une faible résistance aux altérations de l'image hôte. Le but de l'évaluation de la qualité peut être réalisée en utilisant un tatouage semi-fragile. La marque extraite peut non seulement signaler une éventuelle dégradation de l'image originale, mais aussi apporter des renseignements supplémentaires sur la détérioration de celle-ci.

1.5.3. Contrôle de copie

En raison de paiements différenciés pour cet objet, les utilisateurs peuvent bénéficier de privilèges distincts (contrôle de la lecture/copie) sur celui-ci. Certains systèmes prévoient d'intégrer un dispositif de duplication et de vérification pour détecter la contrefaçon du contenu ou restreindre le nombre de copies autorisées. On peut utiliser la marque dans ce but.

1.5.4. Indexation

Il est désormais possible d'incorporer des données explicatives dans une image, à titre d'exemple, un médecin pourrait intégrer de manière discrète les informations du patient soigné, son diagnostic et ses notes dans une radiographie. On fait référence à ce genre de documents comme des documents auto-indexés, parce que la marque inclut sa propre description, facilitant ainsi son archivage dans une base de données sans problème lié au changement de format [24].

1.6. Classification des algorithmes du tatouage numérique

Divers schémas de filigrane numérique ont été élaborés pour différentes utilisations. Ces schémas semblent à première vue très dissemblables les uns des autres. Cette partie est consacrée à la catégorisation des techniques de tatouage numérique pour les images. Cette catégorisation peut être réalisée en fonction de plusieurs critères, tels que :

- Le domaine d'insertion (spatial, fréquentiel, hybride).
- La robustesse (robuste, fragile, semi-fragile).
- Technique d'intégration de la marque (schéma additif, schéma substitutif).
- Le mode d'extraction de la marque, la perception de la marque et la préservation de l'image originale. L'organigramme de cette classification (catégorisation) est illustré dans la Figure 1.4.

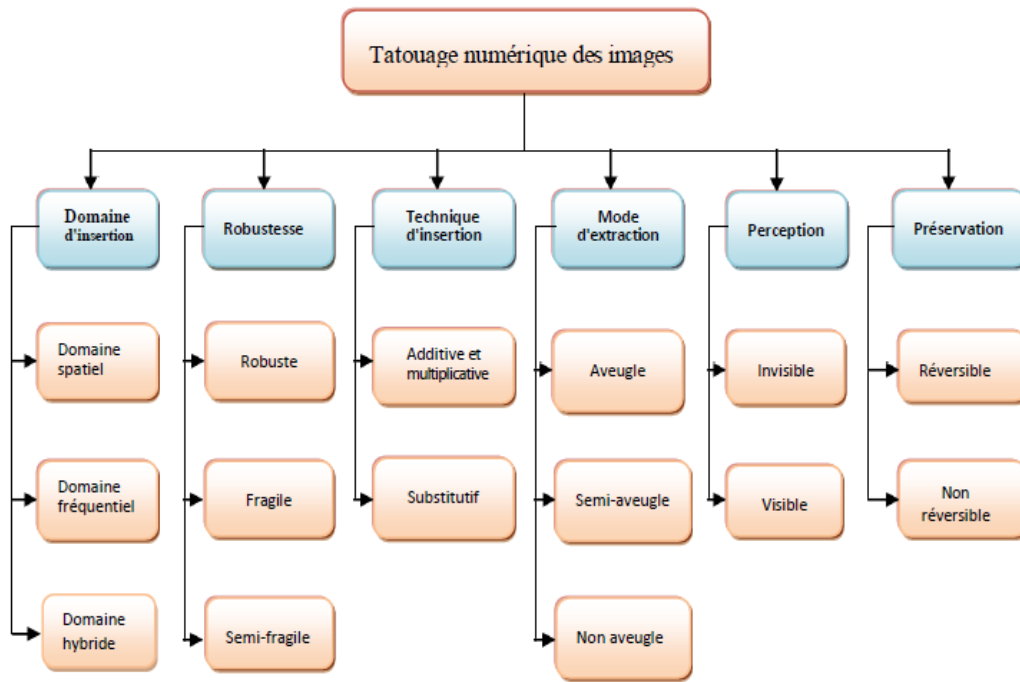


Figure 1.4 : Classification des algorithmes de tatouage d'images.

1.6.1. Classification selon la technique d'insertion de la marque

Les méthodes de tatouage numérique sont classées en deux schémas distinctes : les schémas additifs et les schémas substitutifs.

A) Schéma additif

Dans le cadre de l'approche additive, l'intégration peut se faire, directement sur l'image, dans le domaine spatial, ou bien dans un domaine fréquentiel. La méthode des techniques additives implique l'incorporation de la marque dans les composants du document à tatouer, en suivant l'une des trois équations suivantes [25]:

$$1) \text{ Principe d'additif} \quad I_w(i, j) = I_o(i, j) + \alpha \times W(i, j) \quad (1.6)$$

$$2) \text{ Principe multiplicatif} \quad I_w(i, j) = I_o(i, j) \times (1 + \alpha \times W(i, j)) \quad (1.7)$$

$$2) \text{ Principe exponentiel} \quad I_w(i, j) = I_o(i, j) \times e^{\alpha \times W(i, j)} \quad (1.8)$$

avec $I_w(i, j)$ et $I_o(i, j)$ illustrant l'élément perceptif de l'image tatouée et originale à la position (i, j) . α est un paramètre positif contrôlant le niveau d'intégration de la marque W , connu sous le nom du facteur d'insertion.

B) Schéma substitutif

Le tatouage n'est pas inséré, mais plutôt remplacé par les éléments de l'image originale hôte (pixels, coefficients des transformées : DCT, DFT, DWT, ..., etc.) qui sont déterminés grâce à une clé secrète pour les faire correspondre à la marque. De nombreuses méthodes substitutives ont été suggérées dans les publications scientifiques. La première technique implique l'échange des bits les moins significatifs des pixels d'une image contre ceux de la marque. Cette technique a été employée dans [26] pour les images en couleur. La deuxième, la quantification par la modulation d'index (QIM), suggérée par Chen et Wornell [27], est une méthode largement employée dans le tatouage des images. Cette méthode repose sur le principe de quantifier l'image grâce à un groupe de quantificateurs indexés selon la marque à intégrer. Par conséquent, chaque composant de la marque est associé à un quantificateur distinct, et l'opération de tatouage se réalise par la quantification de l'image en utilisant le quantificateur spécifique à la marque.

➤ Quantification par modulation d'indices

Dans le but de régler le problème lié à la méthode de tatouage additif à spectre étalé [28], Chen et Wornell ont suggéré une nouvelle classe de méthodes d'intégration, nommée modulation d'indice de quantification (QIM). La QIM consiste à moduler un signal avec les informations intégrées. La quantification est ensuite effectuée à l'aide du quantificateur associé. L'une des techniques QIM présentée est la modulation dither (DM). L'algorithme de base de la DM quantifie le vecteur de caractéristiques x à l'aide d'un quantificateur q choisi parmi une famille de quantificateurs basés sur le bit de message w à intégrer. Le vecteur de caractéristiques tatoué y est ensuite obtenu par :

$$y = s(x; w) = q(x + d(w)) - d(w) \quad (1.9)$$

où $q(\cdot)$ est une fonction de quantification avec le pas Δ défini comme :

$$q(x) = \text{round}\left(\frac{x}{\Delta}\right) \times \Delta \quad (1.10)$$

$d(w)$ est une valeur de dither correspondant au bit de w

$d(0)$ sélectionnée de manière pseudo-aléatoire en suivant une distribution uniforme sur $[-\frac{\Delta}{2}, \frac{\Delta}{2}]$

$$d(1) = \begin{cases} d(0) + \frac{\Delta}{2}, & d(0) < 0 \\ d(0) - \frac{\Delta}{2}, & d(0) \geq 0 \end{cases} \quad (1.11)$$

par exemple si on choisit le bit $w = 0$, $d(0) = -\frac{\Delta}{4}$, et $d(1) = +\frac{\Delta}{4}$ pour le bit $w = 1$.

Pour déterminer le bit de message intégré \tilde{w} au décodeur, le signal tatoué est requantifié à l'aide de la même famille de quantificateurs que celle présentée dans la figure 1.5. Ensuite, le décodeur à distance minimale est exécuté selon l'équation suivante :

$$\tilde{w} = \underset{w \in \{0,1\}}{\operatorname{argmin}} |y - s(y; w)| \quad (1.12)$$

QIM offre une capacité d'intégration élevée et des réalisations peu complexes. De plus, la procédure d'extraction de QIM est aveugle, ce qui la rend adaptée à un tatouage numérique robuste.

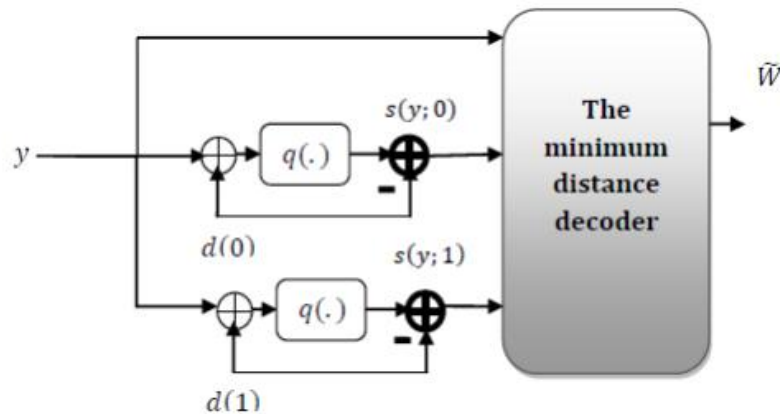


Figure 1.5 : Récupération du tatouage par la modulation dither (DM) .

1.6.2. Classification selon le domaine d'insertion

Selon la littérature, les méthodes de tatouage peuvent être classées en deux catégories : celles qui agissent dans le domaine spatial ou dans le domaine transformées (DFT, DCT, DWT ou SVD). Toutefois, on trouve des méthodes qui recourent à la combinaison de multiples domaines, connues sous le nom de techniques hybrides [29]. On retrouve fréquemment ces algorithmes dans les publications. La fiabilité de la méthode, en matière de robustesse et de capacité, est directement influencée par le choix du domaine. La sélection de la technique est conditionnée par l'application ciblée, étant donné que chaque domaine présente ses particularités distinctes.

1.6.2.1. Domaine Spatial

1.6.2.1.1. Représentation spatiale de l'image

Une image numérique I_o est une matrice de taille $M \times N$ de valeurs entières. Elle est constituée de pixels. Une valeur $I_o(i, j)$ est associée à chaque pixel (i, j) de cette image. On peut exprimer cette valeur de diverses manières. Un pixel d'une image en niveaux de gris est représenté par sa luminance, qui est codée sur 8 bits, il est donc compris entre 0 et $2^8 - 1$ (un entier entre 0 (noir) et 255 (blanc)). Tandis que un pixels d'une image couleur en codage RVB est représenté par trois composantes (rouge(R),vert(V) et bleu(B)). Chaque pixel de l'image est une combinaison de rouge, de vert et de bleu. Chaque couleur est représentée par un octet, soit 8 bits. Chaque pixel est codé sur 3 octets, soit 24 bits : le rouge de 0 à 255, le vert de 0 à 255 et le bleu de 0 à 255. La méthode se fonde sur la synthèse additive des couleurs : il est possible de créer n'importe quelle couleur en combinant ces trois couleurs primaires en proportions appropriées. En combinant ces éléments RVB à différentes proportions, on peut reproduire une vaste gamme de couleurs. L'œil humain est plus réceptif aux éléments V (vert) et R (rouge) qu'à la composante B (bleu). C'est pourquoi la majorité des techniques de tatouage numérique pour les images en couleur incorporent la marque à travers la composante B, pour garantir une invisible optimale.

La plupart des recherches scientifiques utilisent l'espace colorimétrique RVB pour les méthodes de tatouage d'images [30, 31], en utilisant chaque composante R, V ou B ou en les combinant pour l'intégration du tatouage. Cependant, l'espace colorimétrique RVB n'est pas très efficace pour les images Réels [32], car les couleurs et l'intensité de l'image sont séparées, ce qui entraîne une perte de teinte lors d'une modification, telle qu'une compression ou un filtrage, où l'énergie de chaque composante est réduite. De plus, la redondance d'information entre les trois

composantes est relativement faible. Ainsi, l'image d'origine est d'abord convertie de l'espace colorimétrique RVB vers l'espace colorimétrique YCbCr à l'aide de l'équation (1.13) [33] :

$$\begin{cases} Y = 0.299 R + 0.587 V + 0.114 B \\ Cb = -0.169 R - 0.331 V + 0.500 B \\ Cr = 0.500R - 0.419 V - 0.081 B \end{cases} \quad (1.13)$$

2) Le modèle YCbCr éventuellement, représenté comme une transformation inverse en termes mathématiques du modèle RVB. Dans ce modèle, la composante Y désigne la luminance tandis que les deux composantes Cb et Cr illustrent la composante de la chrominance bleu et rouge. Le lien linéaire entre l'espace YCrCb et l'espace RVB est donné par [33] :

$$\begin{cases} R = Y - 0.001 Cb + 1.402 Cr \\ V = Y - 0.344 Cb + 0.714 Cr \\ B = Y + 1.722 Cb + 0.001 Cr \end{cases} \quad (1.14)$$

Le système visuel humain présente une sensibilité moindre à la luminance Y par rapport à la chrominance (Cb et Cr). L'analyse perceptuelle qui se base sur la manipulation spatiale de l'image présente des limites, rendant difficile la prédiction de l'effet des attaques sur les images contenant des tatouages. A titre d'exemple, la compression JPEG impacte surtout les fréquences élevées, qui sont moins perceptibles par l'œil humain. Cependant, lorsqu'il s'agit de tatouages numériques dans le domaine spatial, isoler ces hautes fréquences devient complexe, car elles sont susceptibles d'être davantage plus touchées et ont donc besoin d'un traitement spécifique pendant les étapes d'intégration et d'extraction. C'est ici que réside l'intérêt de travailler dans le domaine fréquentiel, qui permet d'isoler les différentes fréquences (basses, moyennes et hautes) de l'image. A titre d'exemple, on peut utiliser les transformées telles que: la DFT, la DWT, la DCT, ..., etc.

1.6.2.1.2. Insertion de la marque dans le domaine spatial

Dans le cas des méthodes d'insertion dans le domaine spatial, la marque est intégrée en altérant directement les pixels de l'image hôte d'origine, notamment pour les images en niveaux de gris. Toutefois, pour le cas des images couleur, il est possible de modifier un canal ou plusieurs d'un espace colorimétrique donné [34]. En général, ces pixels sont choisis à l'aide d'une clé secrète

ou en fonction d'un système psycho-visuel. Les premières tentatives de développement de filigrane numérique ont été initiées en raison de la simplicité de ce domaine. La première technique de tatouage spatial a été introduite par Tanaka et ses collaborateurs [35]. Cette technique implique l'insertion de chaque composant de filigrane dans le bit de poids faible de chaque pixel de l'image hôte. Le principal avantage de ce domaine réside dans son coût de calcul peu élevé, ce qui encourage son intégration dans les applications de tatouage en temps réel. Ils présentent des vulnérabilités telles que les attaques de la compression avec perte et le filtrage. C'est pourquoi de nombreuses techniques de tatouage recourent à l'incorporation en utilisant d'autres domaines, fondés sur les transformations. Les techniques les plus fréquemment employées dans ce domaine comprennent : le LSB (Least Significant Bit), la méthode du Patchwork, le codage par blocs de texture et l'étalement du spectre.

a) Méthode de Patchwork

La méthode du Patchwork, introduite par Bender et al. [37] concernant le tatouage d'images dans le domaine spatial, est une approche statistique. Son principe fondamental réside dans la sélection pseudo-aléatoire de deux sous-groupes A et B, du signal d'origine par le biais d'une clé secrète. L'incorporation du tatouage s'effectue en modifiant ces deux sous-groupes dans des directions opposées, en augmentant de 1 les amplitudes des échantillons du sous-groupe A et en soustrayant la même valeur du sous-groupe B comme suit :

$$a_i = a_i + 1 \quad (1.15)$$

$$b_i = b_i - 1 \quad (1.16)$$

(a_i et b_i) les échantillons (pixels) des sous-groupes A et B avec $i = 1, 2, \dots, N$.

Pour l'extraction, on déterminera les N couples de pixels depuis la clé secrète et on calculera :

$$S = \sum_{i=1}^N (\hat{a}_i - \hat{b}_i) = \sum_{i=1}^N (a_i - b_i) + 2N \quad (1.17)$$

Puisque les couples sont choisis arbitrairement et, si nous prenons en compte N suffisamment grand, la somme des différences ($a_i - b_i$) est insignifiant en comparaison avec N et nulle en moyenne. Donc, si à la détection de S est proche de la valeur 2N, il sera possible d'affirmer

qu'incontestablement la marque est présente, néanmoins, on conclura dans le cas contraire que l'image n'est pas tatouée.

b) Yeo et Kim [38] ont suggéré une version englobante de la technique Patchwork. Concernant l'intégration, les méthodes additives et multiplicatives Patchwork sont fusionnées et les facteurs d'intégrations sont définis de manière adaptative. Cette variante de la méthode présente une résistance face au filtrage gaussien, au filtrage médian, à l'amélioration de la netteté, à la compression. Le principal inconvénient de la méthode est sa capacité d'intégration limitée et sa vulnérabilité face à la compression JPEG en présence d'un facteur de qualité plus élevé.

1.6.2.2. Domaine fréquentiel

les méthodes de filigrane numérique élaborées pour opérer dans le domaine fréquentiel sont plus robustes et plus complexes mais couramment employées. La marque est intégrée dans quelques coefficients de ce spectre de fréquence. On peut mentionner plusieurs types de transformées employées dans les techniques de filigrane numérique d'images, tels que : la transformée discrète en cosinus (DCT), la transformée discrète en ondelettes (DWT), la transformée de Fourier discrète (DFT) et la décomposition en valeurs singulières (SVD). Dans l'espace transformées (DWT, DCT, etc.), l'énergie du signal est focalisée sur les éléments de basse fréquence. L'intégration du tatouage au sein de ces fréquences offre une robustesse appréciable, toutefois elle engendre des dégradations visibles dans le domaine spatial. Cependant, l'intégration dans les éléments de haute fréquence ne détériore pas la qualité du signal, par contre rend la marque vulnérable à des attaques comme le filtrage passe-bas et la compression. Par conséquent, la gamme de fréquences intermédiaires (moyennes fréquences) est souvent la plus appropriée pour le tatouage, puisque elle répond à la nécessité d'un équilibre entre la résistance et l'invisibilité.

Dans la transformée en cosinus discrète (DCT)

Hsu et al. [39] ont proposé un système de tatouage numérique semi - aveugle dans le but d'améliorer la qualité visuelle des images tatouées. L'image en premier est divisée en blocs non superposés, puis une DCT est appliquée à chaque bloc non superposé. Dans cet algorithme, le tatouage est appliqué sur les coefficients DCT de fréquence moyenne, laissant intacts les coefficients de basse fréquence. L'algorithme proposé s'est avéré peu robuste tout en améliorant la qualité visuelle de l'image tatouée.

Cox et al. [40] ont proposé un algorithme de tatouage numérique non aveugle dans le domaine DCT, Cet algorithme se base sur le concept de dispersion du spectre dans le domaine des fréquences. La marque à intégrer W , une séquence produite par une distribution normale de moyenne zéro et de variance unitaire. L'intégration de la marque s'effectue en ajustant les coefficients DCT présentant les amplitudes les plus élevées, dans la partie des basses fréquences qui représentent les éléments perceptuels les plus importants de l'image. Cela permet d'obtenir une grande robustesse, car ces coefficients sont capables de résister à divers traitements d'image, ainsi qu'aux certaines attaques géométriques. Bien que non aveugle, l'algorithme proposé reste inadapté à de nombreuses applications du filigrane numérique.

Dans la transformée en ondelettes discrète (DWT)

Hsu et al. [41] ont utilisé les coefficients DWT des détails des sous-bandes (HL, LH et HH) de l'image hôte et de la marque pour proposer un algorithme de tatouage numérique multirésolution. Les auteurs ont proposé une méthode dans laquelle l'image hôte et la marque numérique ont été décomposées hiérarchiquement par les ondelettes, puis les bandes détails de la marque ont été ajoutées aux bandes détails de l'image hôte. Les résultats pratique montrent que la technique de tatouage proposée produit une différence quasi invisible entre l'image d'origine et tatouée, et qu'elle est robuste aux traitements d'images courants et à la compression JPEG avec perte, mais les attaques géométriques restent difficiles à réaliser avec cette méthode.

Xia et al. [42] suggèrent un schéma de tatouage numérique qui s'appuie sur l'utilisation de la DWT de Haar. L'image hôte est décomposée en deux niveaux d'ondelettes. La marque employée est une suite pseudo aléatoire (bruit gaussien) : elle est intégrée aux éléments des six sous bandes, à l'exception, les coefficients de la basse fréquence (sous bande LL). L'identification de la marque s'effectue durant l'extraction par le biais d'une technique d'intercorrélacion entre l'image hôte et tatouée. Les essais effectués indiquent que cette technique présente une bonne résistance face à l'addition de bruit et à la compression.

Dans la transformée de Fourier discrète (DFT)

Kim et al. [43] ont présenté un algorithme d'intégration d'une marque qui est une image binaire dans une autre image hôte. La marque est modulée par une matrice de pseudo-bruit binaire (P). Ce pseudo-bruit permet d'étaler uniformément la marque et constitue la clé de sa récupération. La marque obtenue ensuite est intégrée dans le domaine de Fourier de l'image de couverture en

modifiant les composantes d'amplitude ($m_{ij} = m_{ij} + S * P_{ij} * w_{ij}$). Le facteur d'insertion S est une constante qui détermine la force du tatouage. La récupération peut être effectuée sans connaître l'image d'origine. Ce processus commence par une approximation de l'amplitude des coefficients de Fourier de l'image d'origine. Cela peut être réalisé en calculant la moyenne des coefficients d'amplitude autour de chaque point de l'image tatouée. La différence entre la valeur prédite et la valeur réelle dans la version de l'image tatouée est divisée par le pseudo-bruit utilisé lors de l'insertion (peut être régénéré à l'aide de la clé). Les résultats de simulations démontrent que ce schéma offre une grande robustesse aux distorsions telles que le flou et la compression avec perte.

Solachidis et al. [44] proposent une méthode de tatouage robuste à la rotation et à la mise à l'échelle. La marque est une séquence 2D circulaire prenant les valeurs 1 et -1. Sa valeur moyenne est nulle. La région dans laquelle le tatouage est intégré doit être un anneau couvrant les fréquences moyennes. Cet anneau est divisé en S secteurs et en cercles homocentriques. Chaque secteur reçoit la même valeur (1 et -1). Le tatouage est ajouté directement à la magnitude du domaine DFT. Si la magnitude devient négative, elle est arrondie à 0. La propriété de symétrie conjuguée de la DFT doit être préservée. L'image originale n'est pas requise pour la détection. La détection se fait en trouvant la corrélation entre les coefficients éventuellement de l'image tatouée et la marque originale, puis en comparant cette corrélation à un seuil. L'algorithme il a présenté une robustesse à la compression, au filtrage, au recadrage, à la translation et à la rotation.

Dans la décomposition en valeurs singulières (SVD)

Vaishnavi [45] a proposé une méthode conçue pour un tatouage d'image robuste et invisible dans l'espace colorimétrique RVB. L'image hôte est divisée en canaux de couleurs (R, V et B), ensuite la composante bleu de l'image hôte est sélectionnée pour insérer la marque, qui est une image en niveaux de gris, Après décomposition en matrices U , S et V en utilisant la SVD. Les SVs de la marque sont multipliées par un scalaire et ensuite ajoutées aux SVs de la composante bleu de l'image hôte. L'image tatouée est ensuite reconstruite à partir des nouveaux éléments du canal bleu, rouge et vert de couleur restantes non modifiées. La performance de la technique est évaluée avec les mesures de corrélation normalisée (NC) et de PSNR. La méthode proposée offre une bonne robustesse aux attaques par flou de mouvement et filtrage médian, par contre n'est pas robuste face aux distorsions géométriques, à la rotation d'image.

1.6.2.3. Domaine hybride

Les techniques qui intègrent directement la marque dans le domaine spatial ou qui se basent sur une unique transformée fréquentielle ont souvent des performances réduites. Des algorithmes hybrides ont donc été suggérés[10]. S'appuyer exclusivement sur un unique domaine, qu'il soit spatial ou fréquentiel, dans une technique de filigrane numérique des images peut présenter deux inconvénients :

- 1) Dans l'espace spatial ou fréquentiel, la qualité de l'image se détériore considérablement à mesure que la dimension de la marque s'accroît.
- 2) La marque intégrée dans les éléments fréquents subit de légères modifications durant la transition du domaine fréquentiel au domaine spatial, à cause de la transformation des nombres réels en nombres entiers [46].

Le concept d'hybride peut faire référence à la combinaison de deux domaines distincts: L'association de l'un des deux domaines (spatial ou fréquentiel) avec une transformation matricielle, et la combinaison de plusieurs transformées fréquentielles.

1. Le domaine spatial combiné avec le domaine fréquentiel. On peut mentionner [47, 48] comme exemples de travaux combinant les domaines spatial et fréquentiel. Un schéma a été présenté par Su et Kuo [47] qui insère deux marques numériques, l'une dans le domaine spatial et l'autre dans le domaine fréquentiel de l'image hôte (intégrée à la magnitude de la transformée de Fourier discrète (TFD)). L'insertion est basée sur l'approche d'étalement du spectre pour offrir une plus grande robustesse face à la rotation et à la mise à l'échelle. Shih et Wu [48] proposent une technique de tatouage numérique combinant à la fois le domaine spatial et fréquentiel. L'image du tatouage est séparée en deux parties W_1 et W_2 . W_1 est intégrée dans le Domaine spatiale de l'image hôte et W_2 dans le domaine fréquentielle de l'image hôte après application de la DCT dans le but d'améliorer l'imperceptibilité et pour renforcer la robustesse du filigrane .

2. Il est possible de combiner le domaine spatial ou fréquentiel avec une transformation matricielle. Il convient de mentionner les recherches de Liu et Tan [49] qui ont introduit une méthode spatiale fondée sur la SVD. Il convient de mentionner que cette méthode présente une grande probabilité de fausses détections positives, comme le souligne [50]. Mohammad et ses collaborateurs [51] ont fait des ajustements à cet algorithme [49] pour remédier à ce problème. Huang et Guan [52] ont suggéré un algorithme hybride et non aveugle en combinant la DCT et la SVD. L'article [53] a combiné la factorisation en matrices non négatives (NMF) avec la DWT.

3. Il est possible de combiner deux ou plusieurs transformées. Pour illustration, on peut mentionner les recherches d'Abdallah et al. [54]. Ils suggèrent un modèle Fondé sur la transformation de Hadamard et la DWT. Singh et al. [55] ont présenté un schéma de tatouage robuste basé sur des transformations multiples (DWT, DCT et SVD), une 2D-DWT de niveau 1 a été appliquée à l'image hôte afin de la décomposer en sous-bandes. La sous-bande HH est choisit, une DCT suivie d'une SVD ont été appliquées pendant le processus d'intégration pour obtenir l'image tatouée.

1.6.3. Classification selon la robustesse

Cette classification conduit à l'identification de trois catégories de tatouage numérique : robuste, fragile et semi-fragile.

A) **Tatouage robuste** : On considère qu'un schéma de tatouage est robuste, dès que la détection de la marque demeure efficace, même en cas de modifications ou d'attaques sur le document tatoué. Il doit être capable de résister à des opérations légalles effectuées sur le fichier numérique (comme la compression, la conversion analogique-numérique, le filtrage, etc.) ainsi qu'à des activités illégales (telles que les cyberattaques). On se sert de ce genre de tatouage pour protéger les droits d'auteur [56].

B) **Tatouage fragile** : Dans le cas d'un filigrane fragile, la marque réagit de manière très sensible aux changements apportés au contenu tatoué. Cette méthode est utilisée pour certifier l'authenticité et la véracité d'un contenu tatoué. Une méthode de tatouage délicate devrait identifier avec une probabilité élevée de toute modification du contenu tatoué. Une analyse comparative est réalisée entre la marque extraite et la marque originale dans le but d'évaluer l'authenticité du document [57,58].

C) **Tatouage semi-fragile** : Il associe les traits du tatouage résistant et fragile afin d'atteindre une condition intermédiaire, où le marquage est résistant à un ensemble spécifique des altérations, mais fragile face à d'autres. Ce type de tatouage est employé pour authentifier des images [59].

1.6.4. Classification selon la perception de la marque

On peut classer les méthodes de tatouage d'images numériques en deux catégories : visibles et invisibles.

a) **Le tatouage visible** : implique l'insertion d'une marque, elle peut s'agir d'un logo, d'un texte de copyright, d'un texte avec le nom de l'entreprise sur une zone d'intérêt de l'image d'origine, le

tatouage est visible sur l'image tatouée (il est facile de faire la différence entre l'image originale et l'image tatouée) [60].

b) Le tatouage invisible : il s'agit d'incorporer une marque de manière à modifier l'image originale, afin que la marque soit imperceptible pour l'utilisateur, donc il est difficile de distinguer entre l'image d'origine et l'image tatouée.

1.6.5. Classification selon la préservation de l'image originale

Les méthodes de tatouage peuvent être catégorisées en fonction de leur capacité à préserver l'image originale, en méthodes réversibles et non réversibles.

- 1) Les techniques réversibles peuvent restituer toutes les caractéristiques initiales de l'image hôte suite à l'extraction de la marque (tatouage) [61, 62].
- 2) Dans les méthodes irréversibles, l'image d'origine est définitivement modifiée par le processus d'insertion et la matrice de pixels originale ne peut pas être récupérée. La majorité des techniques existantes ne sont pas réversibles.

1.7. Critères d'évaluation des performances des algorithmes de tatouage d'images

Les algorithmes de tatouage numérique sont évalués par deux critères (l'imperceptibilité et la robustesse).

1.7.1. Evaluation de la qualité visuelle d'une image tatouée

Le critère de l'imperceptibilité est mesuré entre l'image originale I_o et son image tatouée I_w par deux mesures objectives : Le rapport signal sur bruit de crête (PSNR) et la similarité structurelle (SSIM).

A) Dans le cas d'une image en niveaux de gris et binaire

- Le rapport signal sur bruit de crête PSNR (Peak Signal to Noise Ratio en anglais) est donné par [63] :

$$\text{PSNR}(I_o, I_w)\text{dB} = 10 \times \text{Log}_{10} \left(\frac{X_{\max}^2}{\text{EQM}(I_o, I_w)} \right) \quad (1.18)$$

où X_{\max} représente la valeur maximale de l'intensité de pixel de l'image originale notée I_o . Par exemple, dans le cas des images en niveaux de gris codées sur 8 bits / pixel on a la valeur de $X_{\max} = 2^8 - 1 = 255$. pour une image codée sur 5 bits/pixel on aura $X_{\max} = 2^5 - 1 = 31$.

où EQM est l'erreur quadratique moyenne entre l'image originale hôte I_o et l'image tatouée I_w . Elle est définie par :

$$\text{EQM}(I_o, I_w) = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N ((I_o(i, j) - I_w(i, j))^2) \quad (1.19)$$

les deux images sont de la même taille $M \times N$. $I_o(i, j)$ et $I_w(i, j)$: représentent les valeurs des pixels d'image originale et tatouée.

- La similarité structurelle (SSIM) est donnée par [64] :

$$\text{SSIM}(I_o, I_w) = \left(\frac{2\mu_{I_o} \times \mu_{I_w} + c_1}{\mu_{I_o}^2 + \mu_{I_w}^2 + c_1} \right) \times \left(\frac{2S_{I_o} \times S_{I_w} + c_2}{S_{I_o}^2 + S_{I_w}^2 + c_2} \right) \times \left(\frac{S_{I_o I_w} + c_3}{(S_{I_o} \times S_{I_w} + c_3)} \right) \quad (1.20)$$

où μ_{I_o} et μ_{I_w} est la moyenne des images I_o et I_w . S_{I_o} et S_{I_w} indiquent respectivement l'écart type des images I_o et I_w . $S_{I_o I_w}$ indique la covariance entre les images I_o et I_w et c_1, c_2 et c_3 des valeurs positives constantes.

B) Dans le cas d'une image couleur RVB

Le calcul du PSNR entre une image couleur RVB originale I_o^{RVB} et son image couleur tatouée I_w^{RVB} est donné par l'équation (1.21). Après séparation de l'image couleur RVB originale et son image couleur tatouée en canaux rouge, vert et bleu.

- On calcul le PSNR de chaque composante R(rouge), V(vert) et B(bleu) séparément entre l'image originale et tatouée comme le cas d'une image en niveaux de gris [65], ensuite on calcule la moyenne du PSNR des trois composantes (R, V et B) selon l'équation (1.21).

$$\text{PSNR(dB)}_{\text{Moyen}} = \frac{\text{PSNR}(R_o, R_w)\text{dB} + \text{PSNR}(V_o, V_w)\text{dB} + \text{PSNR}(B_o, B_w)\text{dB}}{3} \quad (1.21)$$

- La similarité structurelle (SSIM) entre une image couleur RVB originale I_o^{RVB} avec son image couleur RVB tatouée I_w^{RVB} est donnée par :

$$SSIM(I_o^{RVB}, I_w^{RVB})_{Moyen} = \frac{SSIM(R_o, R_w) + SSIM(V_o, V_w)dB + SSIM(B_o, B_w)}{3} \quad (1.22)$$

1.7.2. Critère de performance de robustesse

Il est essentiel qu'un système de tatouage soit robuste. Afin d'évaluer la ressemblance entre le tatouage d'origine W et le tatouage extrait W^* , nous avons recours à la corrélation normalisée (NC) et au taux de correction binaire (BCR) en cas d'une marque binaire. Ces métriques impliquent une comparaison pixel par pixel des valeurs des deux marques pour évaluer la similarité dans le cas où la marque est une image.

A) Dans le cas d'une marque c'est une image en niveaux de gris ou binaire

- La corrélation normalisée (NC) est donnée par [66] :

$$NC(W, W^*) = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i,j) \times W^*(i,j)}{\sum_{i=1}^M \sum_{j=1}^N W(i,j)^2} \quad (1.23)$$

elle évalue le degré de similarité entre la marque d'origine W et la marque extraite W^* . $W(i, j)$ est la valeur du pixel à la position (i, j) de la marque, $W^*(i, j)$ représente la valeur du pixel à la position (i, j) de la marque extraite. $M \times N$: est la taille de la marque .

- Le taux de correction de bit (BCR) est défini par [67] :

$$BCR(W, W^*) = \frac{\sum_{i=1}^M \sum_{j=1}^N \overline{W(i,j) \oplus W^*(i,j)}}{M \times N} \times 100 \% \quad (1.24)$$

Avec \oplus fait référence à l'opération d'addition bit à bit selon le modulo 2. (M, N) est la taille de la marque. $W(i, j)$ représente la position de la valeur binaire de la marque et $W^*(i, j)$ la valeur binaire du tatouage extrait.

Remarque: il existe une forte corrélation entre W et W^* lorsque NC ou le BCR se situe près de 1.

B) Dans le cas d'une marque c'est une image couleur RVB

- La corrélation croisée normalisée (NCC) pour évaluer la robustesse entre l'image originale et extraite couleur est donnée par l'équation (1.25) [65] :

$$NCC = \frac{\sum_{k=1}^3 \sum_{i=1}^P \sum_{j=1}^Q (W(i,j,k) \times W^*(i,j,k))}{\sqrt{\sum_{k=1}^3 \sum_{i=1}^P \sum_{j=1}^Q [W(i,j,k)]^2} \times \sqrt{\sum_{k=1}^3 \sum_{i=1}^P \sum_{j=1}^Q [W^*(i,j,k)]^2}} \quad (1.25)$$

k : représente la composante (canal) du rouge (R), du vert (V) et du bleu (B) de l'image marque insérée et extraite.

$W(i, j, k)$, $W^*(i, j, k)$ représentent la valeur du pixel (i,j) dans la composante k de l'image marque originale et celle de l'image marque extraite.

W et W^* présentent respectivement la marque originale et la marque extraite et P, Q désignent la largeur et la hauteur des images de taille $P \times Q$.

1.8. Conclusion

Au sein de ce chapitre, on a commencé par les techniques de dissimulation de l'information à savoir la cryptographie et la stéganographie, puis nous avons présenté une vue générale des techniques de marquage (tatouage) numérique d'images existants. Après la présentation et de la classification générale des méthodes de tatouage numérique des images, nous avons mis en place une classification basée sur le domaine d'insertion, qui peut être spatial, fréquentiel ou combiné pour la marque et aussi nous avons mis en évidence le bénéfice lié à chaque domaine. Dans la partie suivante, nous avons exposé la classification des algorithmes de tatouage numérique en fonction de leur robustesse, distinguant le tatouage robuste, fragile et semi-fragile, les différentes attaques que peut subir un algorithme de tatouage d'images. Ensuite, nous avons exposé la classification des modèles de filigrane numérique en fonction de leurs méthodes d'insertion. On y distingue les schémas additifs et substitutifs. Par la suite, nous avons détaillé la catégorisation en fonction du mode d'extraction de la marque (aveugle, semi-aveugle et non aveugle), de la visibilité de la marque (visible ou non visible) et de la conservation de l'image d'origine (réversible ou irréversible). Pour finir, nous avons exposé les critères d'évaluation des performances d'un système de tatouage numérique.

Chapitre 2

Tatouage numérique d'images dans le domaine transformées

2.1. Introduction

Les méthodes de tatouage utilisées dans le domaine spatial sont trop fragiles, ne résistent pas à certaines attaques de traitement d'images telles que la compression JPEG, filtrage et l'ajout de bruit [1]. Elles sont beaucoup moins robustes face à différents types d'attaques. Ces inconvénients ont attiré l'attention sur la recherche de techniques de tatouage par domaine de transformation [2]. Les systèmes de tatouage numérique basés sur ce domaine sont des systèmes dans lesquels une transformation fréquentielle est appliquée à l'image hôte et le tatouage numérique (la marque) est intégré aux coefficients transformés en tenant compte des caractéristiques du système visuel humain (SVH). Les techniques de domaine de transformation se sont avérées plus performantes que les techniques du domaine spatial [39]. Dans la littérature, diverses techniques de transformation, telles que la transformée en cosinus discrète (DCT), la transformée de Fourier discrète (DFT), la transformée en ondelettes discrète (DWT), certaines méthodes de transformation d'algèbre linéaire comme la décomposition en valeurs singulières (SVD), la décomposition QR[3], la décomposition de Hessenberg (HD) et bien d'autres, démontrent une meilleure robustesse, une meilleure sécurité et une meilleure imperceptibilité face à diverses attaques, telles que la compression, le bruit, le filtrage, la découpe et la rotation. Cette section passe en revue certaines de ces études, qui ont principalement utilisé des transformées dans le domaine fréquentiel, telles que DCT, DFT, DWT et SVD, et aborde les méthodes hybrides qui ont déjà été mises en œuvre pour assurer l'imperceptibilité et la robustesse des systèmes de tatouage numérique.

2.2. La Transformée de Fourier discrète (DFT)

La Transformée de Fourier discrète (DFT) désigne la technique la plus populaire pour convertir les images du domaine spatial en domaine fréquentiel [4]. Elle propose une plus grande résistance face aux attaques géométriques. La transformation de Fourier implique la décomposition d'un signal ou d'une image en une série de signaux élémentaires, caractérisés par leur facilité de manipulation et d'observation. Ces signaux de base sont à la fois périodiques et complexes, ce qui facilite l'analyse en amplitude et en phase des systèmes [5, 44]. La définition de la transformée de Fourier discrète d'une image $I(m, n)$ qui possède une dimension $(M \times N)$ est donnée par :

$$f(u, v) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m, n) e^{-j2\pi\left(\frac{u \times m}{M} + \frac{v \times n}{N}\right)} \quad (2.1)$$

(u et v) représentent les fréquences spatiales associées à une position m et n . En se basant sur la transformée de Fourier, il est envisageable de reconstituer de manière précise l'image d'origine en effectuant la transformée inverse :

$$I(m, n) = \frac{1}{M \times N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} f(u, v) e^{j2\pi \left(\frac{u \times m}{M} + \frac{v \times n}{N} \right)} \quad (2.2)$$

Les images issues de la transformation de Fourier discrète sont complexes. Habituellement, pour illustrer cette forme complexe, nous calculons le module M et la phase P à l'aide des équations ci-dessous :

$$M(u, v) = |f(u, v)| = \sqrt{(\text{Re}(u, v))^2 + (\text{Im}(u, v))^2} \quad (2.3)$$

$$P(u, v) = \arg(f(u, v)) = \tan^{-1} \left(\frac{\text{Im}(u, v)}{\text{Re}(u, v)} \right) \quad (2.4)$$

Les symboles Im et Re désignent, dans ce contexte, les composantes imaginaire et réelle de la DFT de l'image I . De manière générale, seule l'amplitude du spectre est représentée, comme le montre la répartition fréquentielle illustrée dans la figure 2.1 dans le cas de l'image de Lena.



Figure 2.1 : Image Lena et son module de TFD.

La figure 2.2 explique la répartition fréquentielle (basses, moyennes et hautes) dans le spectre du module de la transformée de Fourier discrète de l'image Lena. En fonction des propriétés de symétrie hermitienne de la Transformée de Fourier Discrète (DFT), les coefficients du module situés dans le quadrant 1 et 2 haut sont équivalents à ceux des coefficients présents dans le quadrant 3 et 4 du bas.

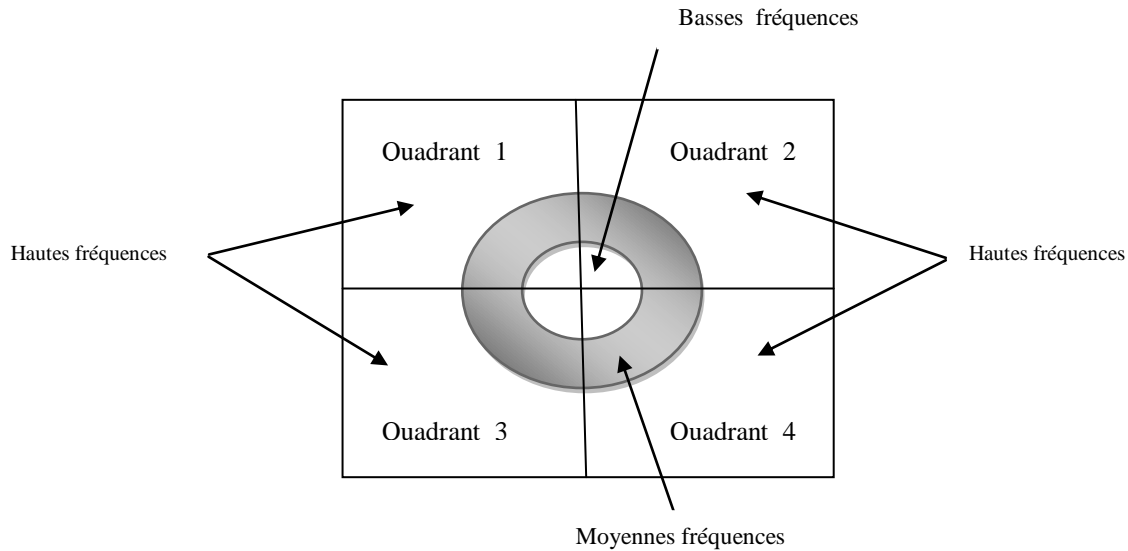


Figure 2.2 : Distribution des fréquences des coefficients d'amplitude d'une DFT.

2.3. Transformée en Cosinus Discrète (DCT)

La transformée en cosinus discrète (DCT) convertit un signal du domaine spatial au domaine fréquentiel. La transformée DCT est à valeurs réelles et fournit une meilleure approximation d'un signal avec peu de coefficients. C'est l'une des transformées linéaires les plus populaires et un outil de compression pour le traitement numérique du signal [6]. Cette procédure sans perte est largement utilisée en raison de sa bonne capacité de compression d'énergie et de décorrélation. La transformation Cosinus discrète de l'image I de taille $(M \times N)$ est définie comme suite [7,8] :

$$f(u,v) = \frac{2}{\sqrt{M \times N}} \times C(u) \times C(v) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I(i,j) \times \cos \left[\frac{\pi \times u}{2 \times M} (2 \times i + 1) \right] \times \cos \left[\frac{\pi \times v}{2 \times N} (2 \times j + 1) \right] \quad (2.5)$$

Et la transformation inversée de DCT sur l'image est définie comme suit :

$$I(i,j) = \frac{2}{\sqrt{M \times N}} \times \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} C(u) \times C(v) \times f(u,v) \times \cos \left[\frac{\pi \times u}{2 \times M} (2 \times i + 1) \right] \times \cos \left[\frac{\pi \times v}{2 \times N} (2 \times j + 1) \right] \quad (2.6)$$

$$\text{avec } \begin{cases} C(u) = C(v) = \frac{1}{\sqrt{2}} & \text{pour } u = v = 0. \\ C(u) = C(v) = 1 & \text{autres } u \neq 0, v \neq 0. \end{cases} \quad (2.7)$$

N et M : représentant dimension de l'image.

$I(i,j)$: valeur du pixel en la ligne i et colonne j de l'image I .

$f(u,v)$: valeur du coefficient DCT en ligne u et colonne v .

Dans la plupart de cas, avant d'appliquer la DCT 2D, il est nécessaire de décomposer une image en plusieurs sous-images non superposées (en blocs) de taille fixe. Par exemple, l'image d'entrée est divisée en blocs de taille 8×8 , 4×4 .

La transformation DCT d'un blocs 8×8 d'image est donné comme suit :

$$f(u,v) = \left(\frac{1}{4}\right) \times C(u) \times C(v) \sum_{i=0}^7 \sum_{j=0}^7 I(i,j) \times \cos\left[\frac{\pi \times u}{16} (2 \times i + 1)\right] \times \cos\left[\frac{\pi \times v}{16} (2 \times j + 1)\right] \quad (2.8)$$

Et la transformation inversée de DCT sur le même blocs 8×8 d'image est définie comme suivant :

$$I(i,j) = \left(\frac{1}{4}\right) \times \sum_{u=0}^7 \sum_{v=0}^7 C(u) \times C(v) \times f(u,v) \times \cos\left[\frac{\pi \times u}{16} (2 \times i + 1)\right] \times \cos\left[\frac{\pi \times v}{16} (2 \times j + 1)\right] \quad (2.9)$$

$$\text{avec } \begin{cases} C(u) = C(v) = \frac{1}{\sqrt{2}} & \text{pour } u = v = 0 . \\ C(u) = C(v) = 1 & \text{autres } u \neq , 0 \neq v . \end{cases}$$

La transformée DCT est utilisée pour convertir l'image spatiale en informations spectrales afin de sélectionner les bandes spectrales appropriées pour l'insertion de la marque (tatouage). La DCT permet de séparer une image en composantes spectrales d'importance variable : les composantes basse fréquence apparaissent en haut à gauche et les composantes haute fréquence en bas à droite comme illustré à la figure 2.3. Pour la plupart des images, la majeure partie de l'énergie se situe à basse fréquence, ce qui est une perception humaine élevée. À l'inverse, les signaux haute fréquence ont une énergie d'image mineure et doivent être peu perceptibles par l'homme.

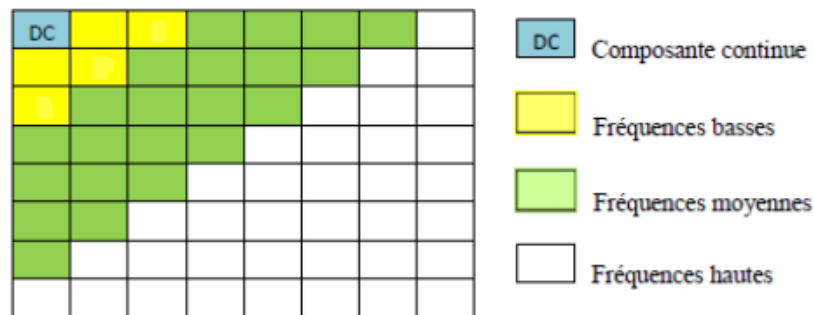


Figure 2.3 : Différentes bandes de fréquences dans un bloc DCT 8×8 .

La lecture des blocs se fait d'une manière en Zig-Zag (balayage depuis les basses fréquences jusqu' au hautes fréquences on ordre) comme le montre la figure 2.4. La majorité des algorithmes basés sur cette transformation dissimulent le message secret dans les fréquences moyennes.

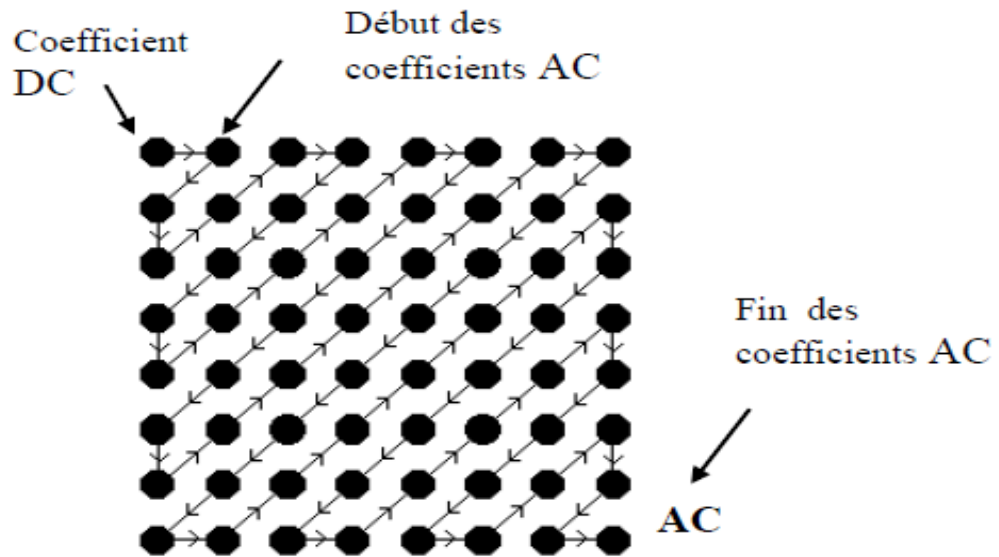


Figure 2.4 : La lecture fréquentielle en zig-zag dans un bloc DCT 8x8.

2.3.1. La comparaison entre la DFT et la DCT

1) La DCT présente cependant une meilleure compaction énergétique que la DFT, seuls quelques coefficients de transformée représentant la plupart de l'énergie de l'image ou du bloc. Cette propriété de la DCT la rend utile dans des applications telles que les communications de données et le codage de signaux (compression).

2) La DCT est similaire à la DFT car elle décompose un signal en une série de fonctions cosinus harmoniques. La DCT est en fait une version simplifiée : seule la partie réelle de la DFT est prise en compte donc nécessite moins de calcul par rapport à la DFT.

3) La Symétrie :

- La DFT ne présente pas de propriétés de symétrie spécifiques en raison de sa base exponentielle complexe.

- La DCT exploite la symétrie paire des fonctions cosinus, ce qui permet une compression et une représentation plus efficaces des signaux.

4) DFT peut gérer des séquences d'entrée complexes et produire des résultats complexes mais pas la DCT qui peut gérer que des séquences d'entrée réelles et produire des résultats réelles.

2.4. La transformée en ondelette discrète (DWT)

La transformée en ondelette discrète (DWT) est une transformée fréquentielle qui fournit une représentation temps-fréquence d'un signal numérique. La DWT bidimensionnelle (2D-DWT) décompose une image en un ensemble de quatre sous bandes, qui peuvent être réassemblées par sa procédure inverse (2D-IDWT) pour reconstruire l'image d'origine. Cette transformation repose sur deux phases : le filtrage et l'échantillonnage. Le filtrage rend possible la décomposition de l'image en sous-bandes haute et basse fréquence, tandis que l'échantillonnage permet de réduire la résolution de chaque sous bande [9].

L'image est premièrement traitée horizontalement (Ligne), puis sous-échantillonnée par un facteur de 2. Par la suite, elle est traitée verticalement (Colonne) et également sous-échantillonnée par un facteur de 2. Par conséquent, nous obtenons quatre sous-bandes (sous-images : LL, LH, HL et HH) dans le domaine des fréquences. Comme illustré à la figure 2.5 [10], ces sous-bandes constituent des matrices dont les dimensions sont diminuées par un facteur de 2.

1) La sous-bande LL (obtenue après filtrage par deux filtres passe-bas) correspond aux basses fréquences de l'image originale, ses coefficients sont donc les plus significatifs, elle est appelée aussi sous-bande d'approximation. La majorité des données de l'image originale se trouvent dans cette sous-bande.

2) La sous-bande LH (obtenue après passage par un filtre passe-bas et un filtre passe-haut), on obtient une image qui met en avant les détails verticaux qui correspondent aux bords horizontaux de l'image originale.

3) La sous-bande HL (obtenue après passage par un filtre passe-haut puis un passe-bas), on obtient une image qui met en avant les détails horizontaux et relatifs aux bords verticaux de l'image originale.

4) La sous-bande HH (obtenue après passage par deux filtres passe-haut) est une image qui met en avant les détails diagonaux de l'image originale qui contient les composantes hautes fréquences de l'image originale.

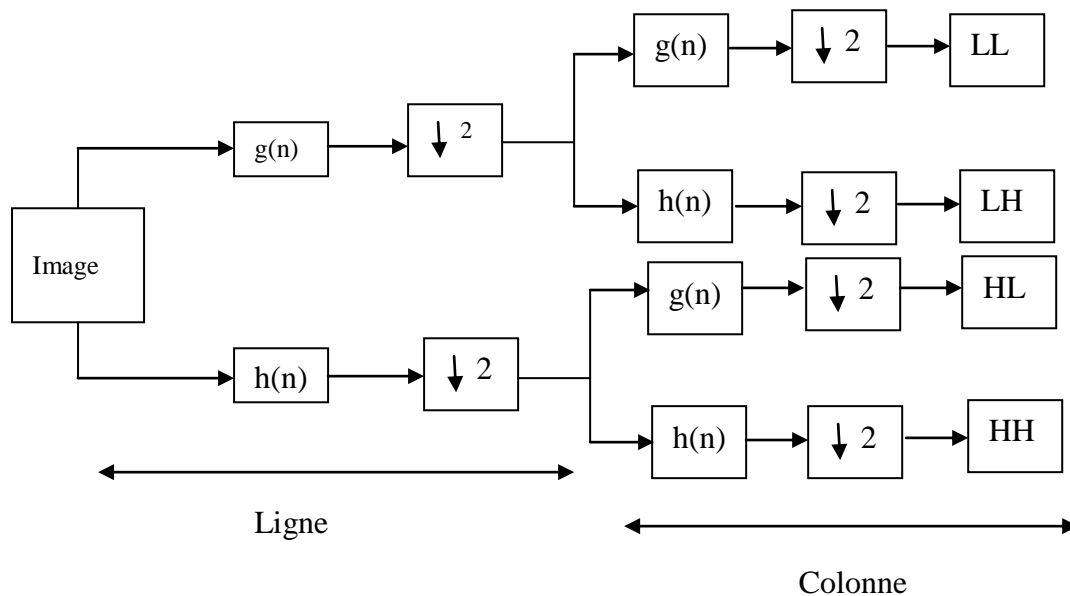


Figure 2.5 : Principe de décomposition 2D par filtrage passe - bas ($g(n)$) et passe - haut ($h(n)$) dans le sens horizontal (Ligne) et vertical (Colonne).

$\downarrow 2$: Sous-échantillonnage d'un facteur de deux (suppression d'un échantillon sur deux).

On arrive donc à obtenir, le premier stade de décomposition en ondelettes. Afin d'avoir une décomposition en ondelettes à plusieurs niveaux, il suffit de subdiviser la sous-bande LL de la même manière. Cela nous donnera alors un second niveau de décomposition, et ce processus peut être répété [11].

Un exemple de l'image Barbara décomposée en deux niveaux de résolution par la décomposition en ondelettes est illustré visuellement dans la figure 2.6.

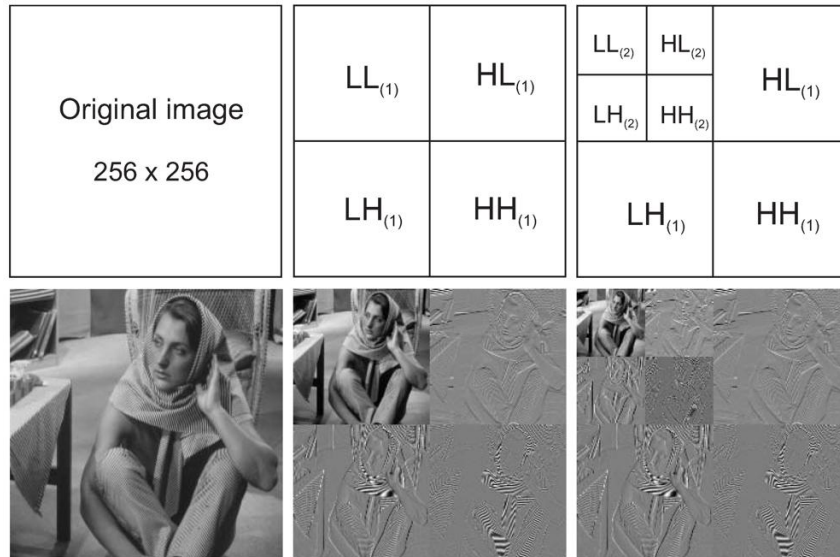


Figure 2.6 : Exemple d'une décomposition en ondelettes à 2 niveaux de résolution de l'image Barbara.

L'image est transformée à l'aide de filtres de la transformée en ondelettes. De nombreux filtres sont proposés, les plus utilisés dans ce domaine du tatouage comprennent les filtres de Haar, les filtres orthogonaux de Daubechies (2 et 4), ainsi que les filtres bi-orthogonaux et de Morlet. Chaque filtre décompose l'image en multiples fréquences.

2.4.1. Comparaison entre DWT et DCT [12]

1) Caractéristiques de transformation :

a) DWT : Décompose une image en différentes composantes fréquentielles à l'aide d'ondelettes. Fournit une localisation temporelle et fréquentielle, ce qui la rend efficace pour capturer les détails de l'image à différentes échelles. Permet une analyse multi-résolution, ce qui peut être utile pour intégrer des marques dans différentes zones de l'image. La DWT offre une description plus détaillée des propriétés du système visuel humain (HSV) par rapport à la DCT et à la DFT.

b) DCT : Transforme une image en une somme de fonctions cosinus de grandeurs et de fréquences variables. Principalement utilisée en compression JPEG, elle accentue les basses fréquences par rapport aux hautes fréquences. présente cependant une meilleure compaction énergétique, seuls quelques coefficients de transformée représentant la majorité de l'énergie de l'image (la majeure partie de l'énergie se situe à basse fréquence). Moins efficace pour l'analyse multi-résolution que la DWT.

2) Robustesse :

a) DWT : Généralement plus robuste face à diverses attaques telles que la compression, le recadrage et l'ajout de bruit en raison de sa nature multi-résolution. Les marques peuvent être intégrées dans les composantes haute, basses et moyennes fréquences, qui sont moins susceptibles d'être affectées par ces attaques.

b) DCT : Bien que la DCT puisse être robuste, elle est plus vulnérable aux attaques par compression (comme la compression JPEG), car la marque est souvent intégrée aux composantes de basse fréquence, qui peuvent être considérablement altérées lors de la compression. Les tatouages basés sur la DCT peuvent être plus facilement supprimés si les attaquants savent où chercher.

3) Capacité :

a) DWT : Offre une capacité de tatouage numérique supérieure grâce à la possibilité d'intégrer des informations dans plusieurs bandes de fréquences. Cette capacité peut être ajustée en fonction du niveau de décomposition en ondelettes utilisé.

b) DCT : Offre généralement une capacité de tatouage numérique inférieure, car elle se concentre sur un nombre réduit de bandes de fréquences, principalement les composantes basse fréquence. La quantité de données pouvant être intégrée est limitée par rapport à la DWT.

4) Qualité de l'image Tatouée :

a) DWT : Tend à maintenir une meilleure qualité visuelle de l'image tatouée, car le processus d'intégration peut être réalisé de manière à minimiser la distorsion perceptuelle. L'influence du tatouage numérique peut être moins perceptible à l'œil nu.

b) DCT : Peut introduire des artefacts plus visibles dans l'image tatouée, surtout si le processus de tatouage numérique n'est pas géré avec soin. La dégradation de la qualité peut être plus prononcée, notamment avec des niveaux de tatouage numérique élevés.

5) Complexité de calcul :

a) DWT : Nécessite généralement davantage de ressources de calcul en raison de la complexité des transformées en ondelettes et de leur nature multirésolution. L'implémentation peut être plus complexe que la DCT.

b) DCT : Généralement plus rapide et moins gourmande en ressources, elle facilite son implémentation dans les applications temps réel. Largement utilisée dans les normes de compression d'images existantes (comme JPEG), ce qui simplifie l'intégration.

Conclusion

En résumé, la technologie DWT est souvent privilégiée pour le tatouage d'images numériques en raison de sa robustesse, de sa capacité supérieure et de sa meilleure préservation de la qualité. La technologie DCT, bien que plus rapide et plus simple, peut être plus vulnérable aux attaques et à la dégradation de la qualité. Le choix entre la technologie DWT et la technologie DCT dépend en fin de compte des exigences spécifiques de l'application de tatouage, telles que la robustesse, la capacité et l'efficacité de calcul.

2.5. Décomposition en valeurs singulières (SVD)

La décomposition en valeurs singulières (SVD) est une technique mathématique utilisée pour extraire les caractéristiques géométriques d'une image. L'image est une matrice réelle non négative du point de vue de l'algèbre linéaire [13]. Soit P une image de taille $n \times n$. La SVD de P peut être décrite comme suit :

$$P = U \times S \times V^T \quad (2.10)$$

On a:

$$U^T \times U = I_n \quad (2.11)$$

$$V^T \times V = I_n \quad (2.12)$$

I_n : est une matrice identité de taille $n \times n$.

Les matrices U et V sont appelées vecteurs singuliers gauche et droit, sont des matrices orthogonales de dimensions $n \times n$ chacune et S est une matrice diagonale rectangulaire de taille $n \times n$, les éléments de S sont des valeurs non négatives sur la diagonale représentant des valeurs singulières de P . Les éléments diagonaux de la matrice $S = \text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ satisfont l'ordre : $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n$ [14].

P : peut être également écrite comme suit :

$$P = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + \dots + \lambda_n U_n V_n^T. \quad (2.13)$$

Il est important de noter que:

- Les composantes non négatives de S représentent la valeur de luminance de l'image.

- Les modifier légèrement n'affecte pas la qualité de l'image et elles ne changent pas beaucoup après les attaques, les algorithmes de tatouage utilisent ces propriétés.
- Elle se révèle utile dans diverses applications comme la compression d'images et le tatouage numérique.
- Une propriété utile dans les schémas de tatouage numérique. En multipliant U par S, on obtient la matrice de composante principale :

$$PC = U \times S \quad (2.14)$$

La composante principale contient les caractéristiques particulières de toute image .

2.5.1. Algorithmes de Tatouage numérique Basés sur la décomposition SVD

L'outil mathématique très employé dans le traitement d'images numériques est la SVD. Cette méthode est employée pour le tatouage d'images numériques, et les résultats obtenus montrent une grande efficacité en termes de robustesse et d'invisibilité.

On va présenter trois algorithmes de tatouage non aveugles qui s'appuient sur cette transformée. La marque est insérée en sélectionnant la matrice diagonale S. La SVD est mise en œuvre soit sur l'image entière, soit sur des parties (blocs) de celle-ci.

A) Algorithme SVD de Chandra

D.V. Satish Chandra [15] a suggéré une méthode non aveugle qui utilise l'application de la transformation SVD à l'image complète (Global-SVD) ainsi qu'à la marque. On multiplie les valeurs singulières (SVs) provenant de la marque par un facteur scalaire, puis on les combine avec les SVs de l'image initiale. Lors de l'étape d'extraction, nous devons recourir aux trois matrices : celle diagonale de l'image initiale et les matrices orthogonales de la marque d'origine.

A1) Algorithme d'insertion

I_0 : image hôte de taille $n \times m$.

W : marque originale de taille $n \times m$.

L'intégration de la marque se fait selon les étapes ci-dessous :

1) Décomposer l'image originale hôte I_0 avec la SVD :

$$I_0 = U \times S \times V^T$$

2) Effectuer la SVD sur la marque W :

$$W = U_w \times S_w \times V_w^T$$

3) Création d'une nouvelle matrice diagonale S_Y en se basant sur la formule ci-dessous :

$$S_Y = S + \alpha \times S_w$$

Où α représente un scalaire (facteur d'insertion, également connu sous le nom de force de tatouage) sélectionné pour préserver la qualité visuelle de l'image tatouée.

4) Restituer l'image marquée I_w à l'aide de la matrice S_Y et des matrices orthogonales (U, V) de l'image hôte comme ceci :

$$I_w = U \times S_Y \times V^T$$

5) Sauvegarder α et les matrices : S, U_w et V_w comme clés secrètes pour l'extraction de la marque :

S : matrice diagonale de l'image hôte.

U_w, V_w : Les matrices orthogonales de la marque originale.

α : facteur d'insertion.

A2) Algorithme d'extraction

Le procédé d'extraction se déroule de la manière suivante :

1) Décomposer l'image I_w^* tatouée et éventuellement attaquée avec la SVD :

$$I_w^* = U^* \times S^* \times V^{T*}$$

2) Calculer de la matrice diagonale S_w^* en utilisant la matrice S (clé secrète) et le facteur d'insertion α :

$$S_w^* = (S^* - S) / \alpha$$

3) Reconstruire la marque W^* en se basant sur les matrices suivantes : S_w^*, U_w et V_w :

$$W^* = U_w \times S_w^* \times V_w^T$$

B) Algorithme de R.Liu et T.Tan

l'article [14] propose une technique de tatouage non aveugle. La marque est multipliée par un scalaire appelé facteur d'insertion et ensuite ajoutée à la matrice des valeurs singulières de l'image hôte. Les analyses expérimentales indiquent que cette technique est résistante à diverses attaques, telles que les filtres passe-bas, la compression,..., etc. Toutefois, le principal

inconvenient de cette technique découle de l'étape d'extraction de la marque qui nécessite la connaissance de trois matrices. Voici le principe de fonctionnement de cet algorithme :

B1) Algorithme d'insertion de la marque

I_o : image hôte de taille $n \times m$.

W : la marque originale de taille $n \times m$.

L'insertion de la marque est décrite selon ces étapes suivantes :

1) Décomposer l'image hôte I_o avec la SVD :

$$I_o = U \times S \times V^T$$

2) Ajouter la marque à la matrice diagonale S de l'image hôte comme suit :

$$A = S + \alpha \times W$$

3) Décomposer la matrice A avec la SVD :

$$A = U_w \times S_w \times V_w^T$$

4) L'image tatouée est produite en employant la matrice S_w de l'image d'origine comme suit :

$$I_w = U \times S_w \times V^T$$

5) Sauvegarder α et les matrices: S , U_w et V_w comme clés secrètes pour l'extraction de la marque :

S : matrice diagonale de l'image hôte I_o .

U_w , V_w : matrices orthogonales de la marque originale W .

α : facteur d'insertion.

B2) Algorithme d'extraction de la marque

La procédure d'extraction est décrite comme suit :

I_w^* : L'image tatouée et attaquée.

Les matrices clés :

– S : Valeurs singulières de l'image hôte .

– U_w , V_w : Vecteurs singulières gauche et droit de la marque originale.

1) Décomposer l'image I_w^* avec la SVD :

$$I_w^* = U^* \times S^* \times V^{T*}$$

2) Calculer la matrice A^* en employant les clés secrètes U_w et V_w de la manière suivante :

$$A^* = U_w \times S^* \times V_w^T$$

3) La marque est récupérée en employant le facteur d'insertion (α) et la matrice clé S de l'image hôte comme suit :

$$W^* = (A^* - S) / \alpha .$$

C) Tatouage d'images en couleurs utilisant la transformée SVD

Dans [16], Cet article propose un système de tatouage couleur basé sur la SVD par bloc. Le tatouage est une image couleur de taille 64×64 pixels (24bits/pixel) à insérer dans l'image hôte couleur 512×512 pixels(24bits/pixel). La taille du bloc peut être ajustée en fonction de la quantité de tatouage à intégrer. Un pixel de chaque canal de couleurs RVB du tatouage est enfoui dans la valeur singulière (SV) maximal du bloc correspondant du canal (de la composante) RVB de l'image couleur hôte. L'étape d'extraction de la marque nécessite une connaissance de l'image hôte. L'algorithme est expliqué comme suit.

C1) Algorithme d'insertion de la marque

I_o : Image hôte, une image couleur RVB de taille $N \times N$ ou $N = 2^n$.

W : La marque originale, une image couleur de taille $M \times M$, $M = 2^m$ et $n \geq m$.

La procédure d'intégration de la marque se déroule en respectant les étapes suivantes :

1) Séparez l'image hôte I_o en trois composantes de couleurs : Rouge (I_{oR}), Vert (I_{oV}) et Bleu (I_{oB}) et la marque W aussi en composantes Rouge(W_R), Vert (W_V) et Bleu (W_B).

L'idée est d'insérer la composante du Rouge de la marque dans la composante du Rouge (I_{oR}) de l'image hôte et la composante du Vert de la marque dans la composante du Vert (I_{oV}) de l'image hôte et la Bleu de la marque dans la Bleu (I_{oB}) aussi de l'image hôte.

2) Pour chaque composante (canal) de couleur de l'image hôte $\{I_{oR}, I_{oV}, I_{oB}\}$ faire :

- Procéder à la division de la composante en blocs L_i de taille: $\frac{N}{M} \times \frac{N}{M}$.
- Concernant chaque bloc L_i , effectuer la SVD au bloc :

$$L_i = U_i \times S_i \times V_i^T$$

- Sélectionner la matrice diagonale S_i du bloc L_i , un pixel de la marque W_i est ajouté à la plus grande valeur singulière (SV) de cette matrice S_i comme suit :

$$\lambda_1^{iw} = \lambda_1^i + \alpha \times W_i$$

Où α est un scalaire (facteur d'insertion ou aussi appelé la force de tatouage).

- S_{iw} est la matrice diagonale du bloc marqué L_{iw} avec le premier élément λ_1^{iw} . Construire le bloc tatoué L_{iw} comme suit :

$$L_{iw} = U_i \times S_{iw} \times V_i^T$$

- Reconstituer la composante du rouge (I_{oRw}), du Vert (I_{oVw}) et du Bleu (I_{oBw}) tatouées à partir des blocs tatoués.

3) Reconstituer l'image hôte couleur tatouée I_w à partir des trois composantes tatouées du $\{I_{oRw}, I_{oVw}, I_{oBw}\}$.

C2) Algorithme d'extraction de la marque

I_w^* : L'image tatouée et probablement attaquée.

I_o : image hôte de taille $n \times m$.

Le processus d'extraction est décrit comme le suivant :

1) Séparez l'image hôte I_w^* tatouée et probablement attaquée en trois composantes de couleurs: Rouge (I_{oRw}^*), Vert (I_{oVw}^*), et Bleu (I_{oBw}^*).

1) Concernant chaque composante (canal) de couleur $\{I_{oRw}^*, I_{oVw}^*, I_{oBw}^*\}$ faire :

- Procéder à la division de la composante en blocs L_{iw}^* de taille : $\frac{N}{M} \times \frac{N}{M}$.
- Concernant chaque bloc L_{iw}^* . Décomposer le bloc avec la SVD :

$$L_{iw}^* = U_i^* \times S_i^* \times V_i^{*T}$$

– La valeur du pixel de la composante couleur de la marque W_i^* est obtenue à partir de la plus grande valeur singulière de S_i^* , qui est (λ_1^{*iw}) du bloc L_{iw}^* et celle du bloc original L_i de S_i , qui est (λ_1^i) comme suit :

$$W_i^* = \frac{(\lambda_1^{*iw} - \lambda_1^i)}{\alpha}$$

– Reconstruire la composante du Rouge (W_R^*), du Vert (W_V^*) et du bleu (W_B^*) de la marque extraite à partir des valeurs des pixels extraits.

2) Reconstruire la marque W^* extraite : image couleur RVB à partir des trois composantes couleur extraites W_R^* , W_V^* et W_B^* .

2.6. Décomposition de Hessenberg

La décomposition de Hessenberg [17,18] est la factorisation d'une matrice carrée B par des transformations de similarité orthogonales sous la forme :

$$B = Q \times H \times Q^T \quad (2.15)$$

Où Q est une matrice orthogonale et H est une matrice de Hessenberg supérieure, ce qui signifie que $h_{ij} = 0$ lorsque $i > j + 1$. La décomposition de Hessenberg est généralement calculée par des matrices de Householder. La matrice de Householder (P) est une matrice orthogonale de la forme:

$$P = (I_n - 2\mu\mu^T) / \mu^T\mu \quad (2.16)$$

Où μ est un vecteur non nul dans R^n et I_n est la matrice identité de taille $n \times n$. La procédure globale comporte $n-2$ étapes lorsque B est de taille $n \times n$. Par conséquent, la décomposition de Hessenberg se calcule comme suit :

$$H = (P_1 P_2 \dots P_{n-3} P_{n-2})^T B (P_1 P_2 \dots P_{n-3} P_{n-2}) \quad (2.17)$$

$$H = Q^T \times B \times Q \quad (2.18)$$

$$B = Q \times H \times Q^T$$

$$\text{Où } Q = P_1 P_2 \dots P_{n-3} P_{n-2}.$$

À titre d'illustration, on prend une matrice de pixels B de taille 4×4 comme suit :

$$B = \begin{bmatrix} 143 & 164 & 152 & 133 \\ 129 & 167 & 177 & 158 \\ 129 & 153 & 172 & 177 \\ 131 & 146 & 158 & 158 \end{bmatrix}$$

Lorsque B est décomposée par la décomposition de Hessenberg, sa matrice orthogonale Q et sa matrice de Hessenberg supérieure H sont données respectivement comme suit :

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -0,5744 & -0,4086 & -0,7093 \\ 0 & -0,5744 & -0,4162 & 0,7049 \\ 0 & -0,5833 & 0,8123 & 0,0043 \end{bmatrix}$$

$$H = \begin{bmatrix} 143,0000 & -259,0750 & -22,2510 & -8,6043 \\ -224,5952 & 488,5263 & 0,5495 & -16,7245 \\ 0,0000 & 22,3807 & 3,8942 & -1,5683 \\ 0,0000 & 0,0000 & 16,4508 & 4,5796 \end{bmatrix}$$

La méthode proposée [19] offre une plus grande robustesse aux attaques que la DCT, la DFT et de nombreuses méthodes spatiales. Cette technique s'avère très résistante à un large éventail d'attaques synchrones (non géométriques) et asynchrones (géométriques), et le tatouage est toujours présent dans l'image attaquée. L'article présente une nouvelle méthode de tatouage utilisant un nouveau domaine pour la représentation d'images et l'intégration du tatouage : la transformation mathématique de Hessenberg. De plus, la méthode proposée est aveugle et l'utilisation de l'image hôte n'est pas nécessaire pour la détection du tatouage.

Remarque : On désigne la notation HD à l'avenir comme abréviation de la décomposition de Hessenberg.

2.7. Transformée d'Arnold

Dans le but de renforcer la robustesse de la technique du filigrane numérique et de la sécurité de la marque à insérer, la marque peut être préalablement traitée (cryptée) avant son intégration à l'image d'origine. On peut y parvenir en utilisant la transformée d'Arnold, par le

biais de son mécanisme de périodicité qui modifie les positions des pixels d'une image carrée de dimension $N \times N$ selon le modèle suivant [20] :

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \bmod N \quad (2.19)$$

avec (u,v) et $(u',v') \in \{1,2, \dots, N\}$.

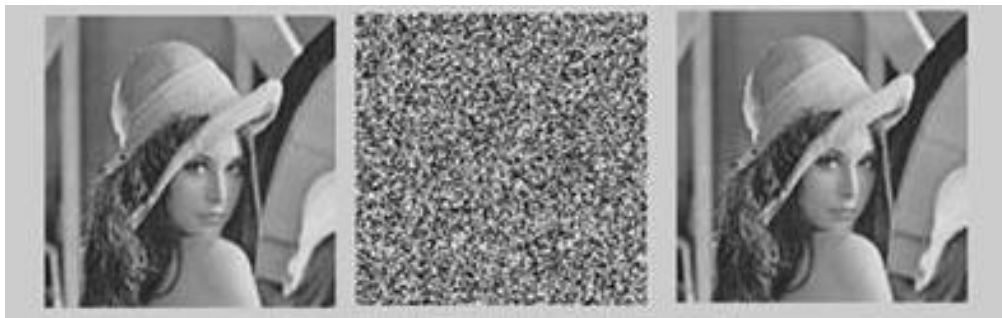
Où (u,v) représente les coordonnées des pixels de l'image d'origine et (u',v') celles de l'image brouillée qui présentent les nouvelles coordonnées des pixels de la transformation d'Arnold, après calcul itératif et N est la hauteur ou la largeur de l'image carrée traitée.

$\bmod N$: représente l'opérateur modulo N .

Pour restituer la marque d'origine, la formule de transformation d'Arnold inverse correspondante peut être définie comme suit :

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} u' \\ v' \end{pmatrix} \bmod N \quad (2.20)$$

En utilisant la transformée d'Arnold sur l'image Lena, on remarque qu'après 15 itérations, l'image devient totalement brouillée, telle qu'elle a été illustrée à la figure 2.7.



(a) Lena

(b) Lena brouillée

(c) Lena restituée

Figure 2.7 : Application de la transformée d'Arnold directe et inverse sur l'image Lena après 15 itérations.

2.8. Domaine hybrides

Toutes les techniques de tatouage d'images qui ont été développées dans les divers domaines de la représentation d'image, notamment le domaine spatial et le domaine fréquentiel avec toutes les transformations dérivées (DCT, DFT, DWT, ..., etc.). Chaque

méthode a ses propres avantages et inconvénients en fonction des exigences spécifiques au domaine d'application ou laquelle la marque elle est intégrée. Ces contraintes proviennent du fait que chaque méthode est résistante à certaines distorsions et attaques spécifiques, mais vulnérable face à d'autres. Aucune de ces méthodes ne montre une résistance face à une vaste gamme d'attaques synchrones et asynchrones, sauf en utilisant des combinaisons d'insertion de multiples domaines ou transformées. Il est donc nécessaire de proposer des domaines plus robustes pour surmonter ces limites et respecter tous les critères de tatouage (capacité, invisibilité et robustesse) qui est le domaine Hybride .

Dans la suite nous donnons trois exemples des algorithmes qui sont basés sur le domaine Hybride : Deux ou plusieurs transformées peuvent être combinées.

1) La méthode DWT-DCT-SVD appliquée sur les images en niveau de gris

Une technique hybride robuste de tatouage d'images numériques basée sur les techniques DWT, DCT et SVD. Nous proposons un algorithme sécurisé combinant les avantages des trois transformations fréquemment utilisées : La DWT, la DCT et la SVD. En vue de renforcer la sécurité du schéma suggéré, la transformée d'Arnold est utilisée pour crypter l'image du tatouage numérique. Un niveau de DWT est d'abord appliqué à l'image hôte d'origine, puis la sous-bande LL est sélectionnée pour le traitement. Celle-ci est divisée en blocs (4×4) et la DCT est appliquée à chacun de ces blocs. Le premier coefficient DC de chaque bloc est ensuite sélectionné pour former une matrice à laquelle la SVD est appliquée, puis les valeurs singulières sont modifiées avec un tatouage numérique crypté avec un facteur d'insertion α sélectionné.

Nous supposons que la dimension de l'image hôte I est de (512×512) pixels et celle de la marque, une image de taille 64×64 pixels. Nous allons d'abord intégrer le tatouage dans l'image hôte à l'aide de l'algorithme d'intégration, puis l'extraire à l'aide de l'algorithme d'extraction. l'image hôte et de la marque sont des images en niveaux de gris de 8bits / pixels.

1.1) Processus d'intégration de la marque

Le processus d'intégration suit ces étapes, décrites ci-dessous :

1) Appliquez la méthode DWT à l'image hôte I de taille 512×512 pixels pour la décomposer en quatre sous-bandes : LL, HL, LH et HH, chacune de taille 256×256 pixels.

2) Choisissez la sous-bande LL, puis divisez-la en blocs carrés (4×4) non superposés, puis appliquez la méthode de la 2D-DCT à chaque bloc carrés (4×4).

3) Récupérer la composante continue (DC) de tous les blocs pour former une matrice B de dimensions 64×64 .

4) Décomposer la matrice B avec la SVD pour obtenir U_1 , S_1 et V_1 :

$$\text{SVD}(B) = U_1 \times S_1 \times V_1^T$$

5) Brouiller l'image du tatouage de taille 64×64 avec la transformée d'Arnold et modifier les valeurs singulières de S_1 avec l'image de la marque brouillée W :

$$S_m = S_1 + \alpha \times W$$

où α est un facteur d'insertion et sa valeur peut varier entre 0 et 1.

6) Décomposer la matrice S_m avec la SVD pour obtenir U_2 , S_2 et V_2 , et stocker U_2 , S_1 et V_2 comme clés secrètes pour l'extraction de la marque :

$$\text{SVD}(S_m) = U_2 \times S_2 \times V_2^T$$

7) Calculer la matrice B^* modifiée, $B^* = U_1 \times S_2 \times V_1^T$, qui contient les informations de la marque .

8) Restaurer chaque valeur DC de la matrice B^* à sa position appropriée dans les blocs de la sous-bandes LL.

9) Appliquez la DCT inverse à tous les blocs pour générer la sous-bande basse fréquence marquée LL^* .

10) Appliquez la DWT inverse à LL^* , HL, LH et HH pour obtenir l'image tatouée I_w .

1.2) Processus d'extraction de la marque

Le procédé d'extraction se déroule de la manière suivante :

1) Appliquer la méthode DWT à l'image Tatouée attaquée dans le but d'obtenir les sous-bandes: LL_w , HL^* , LH^* et HH^* .

2) Choisissez la sous-bande LL_w , puis divisez-la en blocs carrés de 4×4 , puis appliquez la DCT à chaque bloc.

3) Collecter la composante continue (DC) de tous les blocs pour former une matrice DC_w de dimensions 64×64 .

4) Appliquez la SVD à DC_w , pour obtenir U_w , S_w et V_w :

$$\text{SVD}(DC_w) = U_w \times S_w \times V_w^T$$

5) Utilisez S_w avec (U_2 et V_2 stockés côté insertion) pour obtenir S_m^* :

$$S_m^* = U_2 \times S_w \times V_2^T.$$

6) Utilise S_1 (stocké côté insertion) pour extraire l'image de la marque brouillée comme suit :

$$W^{**} = (S_m^* - S_1) / \alpha .$$

7) Appliquez la transformée d'Arnold inverse pour restaurer la marque d'origine W^* .

2) La méthode FRT-DWT-SVD appliquée sur les images couleurs RVB 24 Bits/pixels

Dans [21], les auteurs ont proposé une technique robuste de tatouage d'images semi-aveugle, basée sur la transformée en ridgelet finie (FRT) [22], la DWT, la SVD, l'optimisation par essaim de particules (PSO) et la transformée d'Arnold, afin de protéger les droits d'auteur et de vérifier l'authenticité des images couleur. Tout d'abord, l'image en couleur est convertie de l'espace colorimétrique RVB à l'espace colorimétrique YCbCr, et la composante de luminance (Y) est prise en compte pour l'insertion des données du tatouage. Dans cette étude, la composante principale (PC) de l'image du tatouage est directement insérée dans la valeur singulière correspondante de l'image hôte par le facteur d'insertion α . Pour améliorer encore la sécurité, la transformée d'Arnold est appliquée pour traiter le canal Y de l'image du tatouage avant son insertion dans l'image de couverture (hôte). Par ailleurs, PSO optimise le facteur d'insertion α . Des facteurs d'évaluation qualitatifs tels que (PSNR) et la similarité structurelle (SSIM) sont utilisés pour évaluer la qualité visuelle entre l'image hôte et tatouée, tandis que la corrélation croisée normalisée (NCC) permet d'évaluer la ressemblance entre la marque et la marque extraite (restituée). Les performances du schéma proposé sont évaluées à l'aide d'attaques géométriques, non géométriques et combinatoires, et sa robustesse est démontrée par une comparaison avec différents schémas de tatouage d'images.

Voici comment sont présentées les étapes pour l'intégration et l'extraction de la marque :

1. L'image hôte est une image couleur RVB d'une résolution de 512×512 pixels, de 24 bits par pixels.
2. La marque est une image couleur RVB d'une résolution de 512×512 pixels, de 24 bits par pixels.
3. La dimension de l'image du tatouage (la marque) est identique à celle de l'image de hôte, ce qui améliore la capacité d'intégration de la marque dans l'image hôte.
4. Le schéma proposé utilise également l'optimisation par essaim de particules (PSO) pour obtenir le facteur d'insertion optimal (α) dans le but d'atteindre un meilleur équilibre entre l'invisibilité (PSNR) et la robustesse (NCC). Dans la procédure d'optimisation du schéma de

tatouage d'images proposé. La fonction fitness du PSO utilisée par le schéma proposé est définie comme suit [23] :

$$f = \frac{n}{(\text{PSNR} + \sum_{i=1}^n \text{NCC}_i)}$$

Où f représente la fonction fitness, PSNR permet de calculer l'invisibilité entre l' image hôte et l'image tatouée , et NCC_i permet de calculer la ressemblance (robustesse) entre la marque image originale et la marque, les images extraites. Tandis que n représente le nombre d'attaques effectuées sur l' image tatouée lors de l'optimisation du facteur d'insertion α par le PSO.

2.1) Algorithme d'insertion de la marque

Les étapes du processus d'intégration de la marque sont décrites ci-dessous :

Étape 1 : l'image couleur hôte (I_{RVB}) et la marque une image couleur (W_{RVB}) sont converties dans l'espace couleur YCbCr pour obtenir les composantes $I_Y, I_{\text{Cb}}, I_{\text{Cr}}$ et $W_Y, W_{\text{Cb}}, W_{\text{Cr}}$, respectivement.

Étape 2 : Sélectionnez W_Y , la composante de luminance de la marque, et randomisez-la en appliquant la transformée d'Arnold pour obtenir W'_Y .

Étape 3 : La FRT [24] est utilisée pour transformer le canal de luminance I_Y de l'image hôte comme suit :

$$\text{RI}_Y = \text{FRT}(I_Y)$$

Étape 4 : Appliquez la 2D-DWT à un niveau de décomposition à la composante RI_Y Pour obtenir quatre sous-bandes fréquentielles distinctes, à savoir la sous-image RI_{YLL} et trois sous-images $\text{RI}_{\text{YLH}}, \text{RI}_{\text{YHL}}$ et RI_{YHH} (détails verticaux, détails horizontaux et diagonaux) et à la composante W'_Y pour obtenir quatre sous-bandes fréquentielles aussi distinctes, à savoir la sous-image W'_{YLL} et trois sous-images $W'_{\text{YLH}}, W'_{\text{YHL}}$ et W'_{YHH} (détails verticaux, détails horizontaux et diagonaux) , respectivement.

$$[\text{RI}_{\text{YLL}}, \text{RI}_{\text{YLH}}, \text{RI}_{\text{YHL}}, \text{RI}_{\text{YHH}}] = \text{DWT}(\text{RI}_Y)$$

$$[W'_{\text{YLL}}, W'_{\text{YLH}}, W'_{\text{YHL}}, W'_{\text{YHH}}] = \text{DWT}(W'_Y)$$

Étape 5 : Sélectionnez la sous-bande RI_{YHL} pour l'intégration de la marque et effectuez la décomposition en valeurs singulières sur cette sous-bande pour obtenir les matrices U,S et V:

$$\text{SVD}(\text{RI}_{\text{YHL}}) = U \times S \times V^T$$

Étape 6 : Sélectionnez la sous-bande de détails horizontaux de la marque W'_{YHL} et effectuez la SVD sur cette sous-bande pour obtenir les matrices U_1, S_1 et V_1 et extraire la composante principale (PC) de la sous-bande comme suit :

$$\begin{aligned} \text{SVD}(W'_{YHL}) &= U_1 \times S_1 \times V_1^T \\ \text{PC} &= U_1 \times S_1 \end{aligned}$$

Étape 7 : La composante principale (PC) de l'image de la marque couleur obtenue à l'étape 6 est multipliée par un facteur α . Les valeurs résultantes sont ensuite ajoutées aux valeurs singulières S obtenues à l'étape 5. Cette phase est mathématiquement définie comme suit :

$$S^* = S + \alpha \times \text{PC}$$

α désigne le paramètre d'insertion qui gère l'équilibre entre invisibilité et robustesse .

Étape 8 : La SVD inverse (ISVD) est appliquée pour obtenir la sous-bande RI^*_{YHL} marquée de détails horizontaux d'ondelettes ensuite La DWT inverse de premier niveau (IDWT) est appliquée à la sous-image RI^*_{YHL} modifiée et aux trois autres sous-images RI_{YLL}, RI_{YLH} et RI_{YHH} pour obtenir la composante de coefficients de la FRT (RI^*_Y) marquée comme suit :

$$\begin{aligned} RI^*_{YHL} &= U \times S^* \times V^T \\ RI^*_Y &= \text{IDWT}[RI_{YLL}, RI_{YLH}, RI^*_{YHL}, RI_{YHH}] \end{aligned}$$

Étape 9 : La FRT inverse (IFRT) est appliquée aux coefficients de la composante RI^*_Y pour obtenir la composante de luminance tatouée I^*_Y , définie comme suit :

$$I^*_Y = \text{IFRT}(RI^*_Y)$$

Étape 10 : Combinez la luminance marquée I^*_Y avec la chrominance I_{Cb}, I_{Cr} pour obtenir l'image couleur tatouée I_{wRVB} dans l'espace RVB comme suit :

$$I_{wRVB} = \text{YCbCr2RGB}[I^*_Y, I_{Cb}, I_{Cr}]$$

2.2) Algorithme d'extraction de la marque

Les étapes d'extraction de la marque sont décrites ci-dessous en utilisant la procédure inverse de l'opération d'insertion de la marque :

Étape 1 : Transformez l'image couleur tatouée et éventuellement attaquée I_{wRVB}^* de l'espace RVB en espace YCbCr pour obtenir les composantes I_{wY} , I_{Cb}^* and I_{Cr}^* :

$$[I_{wY}, I_{Cb}^*, I_{Cr}^*] = \text{RGB2YCbCr}(I_{wRVB}^*)$$

Étape 2 : La FRT est utilisée au canal de luminance (I_{wY}) de l'image couleur tatouée et attaquée afin d'obtenir les coefficients de ridgelet. Elle peut être définie comme suit :

$$RI_{wY} = \text{FRT}(I_{wY})$$

Étape 3 : Appliquez la 2D-DWT à un niveau de décomposition à la composante RI_{wY} Pour obtenir quatre sous-bandes fréquentielles distinctes, à savoir la sous-image RI_{wYLL} et trois sous-images $RI_{wY LH}$, $RI_{wY HL}$ et $RI_{wY HH}$ (détails verticaux, détails horizontaux et diagonaux) :

$$[RI_{wYLL}, RI_{wY LH}, RI_{wY HL}, RI_{wY HH}] = \text{DWT}(RI_{wY})$$

Étape 4 : Sélectionnez la sous-bande $RI_{wY HL}$ et effectuez la décomposition en valeurs singulières sur cette sous-bande afin d'avoir les matrices U_w , S_w et V_w :

$$\text{SVD}(RI_{wY HL}) = U_w \times S_w \times V_w^T$$

Étape 5 : Utilisez la clé S (stockée dans le schéma d'intégration) et extrayez le composante principale de la marque comme suivant:

$$PC_w = \frac{(S_w - S)}{\alpha}$$

Étape 6 : Utilisez la clé V_1^T , enregistrée lors de la procédure d'insertion de la marque, pour obtenir la sous-bande marquée W_{YHL}^* :

$$W_{YHL}^* = PC_w \times V_1^T$$

Étape 7 : La DWT inverse d'un niveau de reconstruction (IDWT) est appliquée à la sous-image W'_{YLL} et aux trois autres sous-images $W'_{Y LH}$, W_{YHL}^* et $W'_{Y HH}$ pour obtenir la composante de luminance marquée brouillée $W_Y^{* '}$ comme suit :

$$W_Y^{* '} = \text{IDWT}[W'_{YLL}, W'_{Y LH}, W_{YHL}^*, W'_{Y HH}]$$

Étape 8 : Effectuez la transformée inverse d'Arnold sur $W_Y^{* '}$ pour obtenir la composante de luminance marquée non brouillée W_Y^* .

Étape 9: Combinez la luminance de la marque extraite W_Y^* avec la chrominance de la marque W_{Cb} et W_{Cr} qui sont obtenues lors de la phase d'insertion pour obtenir l'image couleur extraite dans l'espace RVB comme suit :

$$W_{RVB}^* = YCbCr2RGB[W_Y^*, W_{Cb}, W_{Cr}]$$

3) La méthode DWT- HD - SVD appliquée sur les images couleurs RVB 24 Bits/pixels

Dans [25], les auteurs ont proposé un système de tatouage adaptatif d'images couleur haute performance basé sur la DWT, la décomposition de Hessenberg (HD) et la SVD. Afin d'améliorer la sécurité du tatouage, une cartographie chaotique logistique a été utilisée pour chiffrer l'image du tatouage. En calculant de manière adaptative le facteur d'insertion via l'entropie de l'image hôte. L'image du tatouage est intégrée dans la composante Y de l'espace de couleur YCbCr, afin d'améliorer l'imperceptibilité de l'algorithme. De plus, la robustesse de l'algorithme a été améliorée grâce à des méthodes de correction des valeurs singulières. Comparé à d'autres schémas de tatouage hybrides, le schéma proposé est capable de résister efficacement à de multiples attaques avec une grande robustesse, bien que le schéma ait une meilleure robustesse globale, sa robustesse aux attaques de rotation et de recadrage est relativement faible.

Voici comment sont décrites les phases d'insertion et d'extraction :

1. L'image hôte est une image couleur RVB d'une résolution de 512×512 pixels, de 24 bits par pixels.
2. La marque est une image en niveaux de gris d'une résolution de 256×256 pixels, de 8 bits par pixels.

3.1) Algorithme d'insertion de la marque

L'espace couleur YCbCr est choisit pour ces avantages d'améliorer la transparence visuelle de l'image tatouée, et la composante Y est retenue car elle est plus robuste à l'intégration du tatouage que les composantes Cb et Cr. Une décomposition en ondelettes discrètes de la composante Y et une décomposition de Hessenberg (HD) de la sous-bande LL résultante pour obtenir la matrice supérieure H. Par la ensuite une SVD est appliquée sur la matrice supérieure H. Le facteur d'insertion (α) est calculé à partir de l'entropie visuelle et de l'entropie de bord de l'image hôte afin d'intégrer le tatouage.

Les étapes de l'intégration du tatouage sont présentées selon la procédure ci-dessous :

Étape 1 : La marque est une image en niveaux de gris est cryptée par cartographie chaotique logistique comme suit :

$$W' = \text{Logistique}(W)$$

Étape 2 : À l'aide de la SVD, l'image W' est décomposée en trois matrices U_w , S_w et V_w :

$$[U_w, S_w, V_w] = \text{SVD}(W')$$

Étape 3 : L'image hôte couleur (I_{RVB}) est convertie de l'espace couleur RVB vers l'espace couleur YCbCr, pour obtenir les composantes I_Y , I_{Cb} , I_{Cr} , ensuite sélectionner la composante de luminance I_Y :

$$[I_Y, I_{Cb}, I_{Cr}] = \text{RGB2YCbCr}(I_{RVB})$$

Étape 4 : Une décomposition en ondelettes de Haar à un niveau sur la composante I_Y de luminance est effectuée pour la décomposer en quatre sous-bandes : LL, HL, LH et HH :

$$[LL, HL, LH, HH] = \text{DWT}(I_Y)$$

Étape 5 : Appliquer la décomposition de la matrice de Hessenberg (HD) sur la sous-bande LL pour obtenir la matrice supérieure H :

$$LL = Q \times H \times Q^T$$

Étape 6 : Décomposer La matrice de Hessenberg supérieure H par la SVD pour obtenir les trois matrices U_H , S_H et V_H :

$$[U_H, S_H, V_H] = \text{SVD}(H)$$

Étape 7 : Incorporation de la matrice S_w obtenue à l'étape 2 et S_H obtenue à l'étape 6 par la méthode de mélange (α) :

$$S'_H = \alpha \times S_w + (1-\alpha) \times S_H$$

Étape 8 : Reconstruction de La matrice de Hessenberg supérieure H' par décomposition en valeurs singulières inverses à partir des matrices U_H , S'_H et V_H :

$$H' = U_H \times S'_H \times V_H^T$$

Étape 9 : Reconstruire la sous-bande LL' selon les matrices Q et H' , en utilisant la décomposition de Hessenberg inverse :

$$LL' = Q \times H' \times Q^T$$

Étape 10 : Une transformée en ondelettes discrète inverse est effectuée sur les quatre sous-bandes LL' , HL, LH et HH, dans le but d'obtenir l'image du canal I'_Y marquée comme suit :

$$I'_Y = \text{IDWT} [LL', HL, LH, HH]$$

Étape 11 : Combinez la luminance marquée I'_Y avec la chrominance I_{Cb} et I_{Cr} pour obtenir l'image couleur tatouée I_{wRVB} dans l'espace RVB comme suit :

$$I_{wRVB} = \text{YCbCr2RGB} [I'_Y, I_{Cb}, I_{Cr}]$$

3.2) Algorithme d'extraction de la marque

Lors du processus de récupération de la marque, l'image tatouée et probablement attaquée est initialement transformée dans l'espace colorimétrique YCbCr, puis une décomposition en ondelettes discrètes est appliquée à la composante Y. La sous-bandes LL est sélectionnée pour la décomposition matricielle de Hessenberg (HD) afin d'obtenir la matrice supérieure H. La SVD est ensuite appliquée sur H pour obtenir la matrice des valeurs singulières. La matrice des valeurs singulières de la marque est ensuite extraite. Enfin, l'image tatouée chiffrée est obtenue par décomposition par valeurs singulières inverse, puis l'image tatouée est restaurée par déchiffrement.

Étape 1 : Lire l'image couleur tatouée et probablement attaquée I_{wRVB}^* de l'espace RVB et la convertir dans l'espace couleur YCbCr, pour obtenir les composantes I_{wY} , I_{Cb}^* et I_{Cr}^* , puis sélectionner la composante de luminance I_{wY} comme suit :

$$[I_{wY}, I_{Cb}^*, I_{Cr}^*] = \text{RGB2YCbCr}(I_{wRVB}^*)$$

Étape 2 : Sélectionner la composante I_{wY} et effectuez une décomposition en ondelettes de Haar à un niveau :

$$[LL_{wM}, HL_{wM}, LH_{wM}, HH_{wM}] = \text{DWT}(I_{wY})$$

Étape 3 : Sélectionner la sous-bandes LL_{wM} et effectuez la décomposition matricielle de Hessenberg sur cette sous-bandes pour obtenir la matrice supérieure H_{wM} :

$$LL_{wM} = Q_{wM} \times H_{wM} \times Q_{wM}^T$$

Étape 4 : Effectuer la SVD sur la matrice supérieure H_{wM} pour obtenir les matrices U_{wM} , S_{wM} et V_{wM} de la façon suivante:

$$[U_{wM}, S_{wM}, V_{wM}] = \text{SVD}(H_{wM})$$

Étape 5 : La matrice des valeurs singulières de la marque chiffrée peut être obtenue par le facteur d'insertion α et la matrice des valeurs singulières S_H (clé secrète) :

$$S'_w = \frac{S_{wM} - (1 - \alpha) \times S_H}{\alpha}$$

Étape 7 : Récupérer la marque chiffrée en effectuant une décomposition en valeurs singulières inverses des matrices U_w , S'_w et V_w :

$$W'_E = U_w \times S'_w \times V_w^T$$

Étape 8 : Déchiffrer l'image à l'aide de la cartographie chaotique logistique et obtenir la marque (tatouage) extraite W_E .

2.9. Conclusion

Dans cette présentation du chapitre, nous avons commencé par exposer les transformées les plus couramment employées dans le cadre du tatouage numérique des images en domaine fréquentiel telles que la DCT, la DFT, la DWT, la SVD et la décomposition de Hessenberg (HD), et pour renforcer la sécurité de la marque à insérer on a présenté, la transformée d'Arnold qui peut être appliquée sur le tatouage avant son intégration dans l'image hôte, ensuite, nous avons analysé et exposé les techniques du marquage (tatouage) numérique non aveugle fondées sur la SVD en abordant les méthodes d'insertion et de l'extraction de la marque dans la matrice diagonale S , qui offre de nombreux bénéfices tels que la facilité des calculs et l'imperceptibilité de la marque de l'image tatouée, la résistance aux attaques d'effacement, notamment, la compression JPEG, l'addition du bruit et le filtrage, ..., etc. Mais, pour ce qui concerne la robustesse par rapport aux attaques géométriques est réduite. Et par la suite on a abordé les méthodes hybrides, présentons trois méthodes de tatouage, qui associent la SVD avec les transformées, telle que la DWT-DCT-SVD, la FRT-DWT-SVD et la DWT-HD-SVD. Nous avons étudié et présenté ces algorithmes de tatouage numérique non aveugle en détails qui sont conçus pour le cas des images couleurs et en niveaux de gris. Dans le chapitre suivant, nous allons aborder l'optimisation dans le but de présenter en détails l'algorithme de la colonie d'abeilles artificielles, qui est une méta-heuristique d'optimisation inspirée du comportement intelligent des abeilles, afin de l'utiliser dans le but de la recherche des facteurs d'insertion optimaux dans les algorithmes de tatouage numérique des images fixes dans le but d'obtenir une grande invisibilité de l'image tatouée et une robustesse maximale de la marque extraite .

Chapitre 3

Utilisation de l'algorithme ABC en tatouage numérique

3.1. Introduction

Pendant les dix dernières années, les techniques d'optimisation sont devenues un sujet d'étude et de recherche important. L'utilisation croissante de l'optimisation a été stimulée par la disponibilité des ordinateurs numériques et la nécessité de les utiliser pour l'étude de grands systèmes. Il existe deux catégories d'algorithmes qui se démarquent ou méthodes d'optimisation : exactes et approchées. On utilise des méthodes exactes pour régler des problèmes en un temps limité. Elles conduisent systématiquement à une solution identique. Elles aboutissent toujours à la même solution idéale à condition que les conditions initiales ainsi que les variables de contrôle soient identiques. En revanche, les techniques approchées (stochastiques) se servent de processus probabilistes susceptibles de pouvoir aboutir, après de nombreux essais, à des résultats divergents peuvent être obtenus, et ce, même en maintenant les mêmes conditions initiales ainsi que les paramètres de contrôle. On utilise ce genre d'algorithme d'optimisation pour s'attaquer aux problèmes dits complexes d'optimisation pour lesquels les méthodes traditionnelles ne sont pas disponibles. Les méthodes stochastiques comportent les méthodes dites heuristiques et méta-heuristiques. Les algorithmes heuristiques sont spécifiques à un problème, tandis que les algorithmes méta-heuristiques sont indépendants du problème, permettant ainsi de résoudre une grande variété de problèmes réels. Le mot méta-heuristique provient du grec et il est constitué de deux éléments : « méta » qui veut dire après ou plus loin, et « heuristique » qui signifie la découverte de. Au fur et à mesure, les chercheurs ont suggéré des méthodes autonomes inspirées de phénomènes biologiques et bio-sociologiques. Ces techniques ou méthodes sont efficaces et polyvalentes, elles peuvent être ajustées et/ou personnalisées pour répondre aux besoins d'une problématique particulière.

L'intelligence en essaim est une sous-discipline des algorithmes bio-inspirés de la nature, qui étudie le comportement des insectes sociaux tels que les abeilles et les fourmis. Elles sont la source d'inspiration, qui, malgré leur comportement individuel simple, parviennent à accomplir des tâches extrêmement complexes grâce à leur collaboration. Cette approche de résolution des problèmes a conduit à la création de méta-heuristiques robustes et très performantes.

L'objectif de ce chapitre est d'offrir un aperçu général sur l'optimisation, et ensuite de présenter en détails l'algorithme de la colonie d'abeilles artificielles qui est une méta-heuristique d'optimisation inspirée du comportement intelligent des abeilles au cours de la quête de nourriture. Elle fait partie de la famille des algorithmes à base de l'intelligence par

essaim. Dans notre travail on l'utilisera en vue de la recherche des facteurs d'insertion optimaux dans une technique de tatouage numérique des images fixes (couleurs et en niveau de gris) dans le but d'obtenir une qualité meilleure de l'image tatouée et une robustesse maximale de la marque extraite.

3.2. Les méthodes de résolution de problème d'optimisation

Plusieurs méthodes pour résoudre des problèmes de diverses complexités ont été suggérées (Figure 3.1). Par conséquent, on a constaté une diversité considérable et des disparités notables en termes de principe, de stratégie et de résultats. Ces diversités et distinctions ont conduit à la catégorisation des diverses techniques de résolution de problèmes en deux grandes classes : la classe des méthodes exactes et celle des méthodes approchées. La combinaison des techniques de ces deux catégories a produit une pseudo classe qui comprend des méthodes qualifiées d'hybrides.

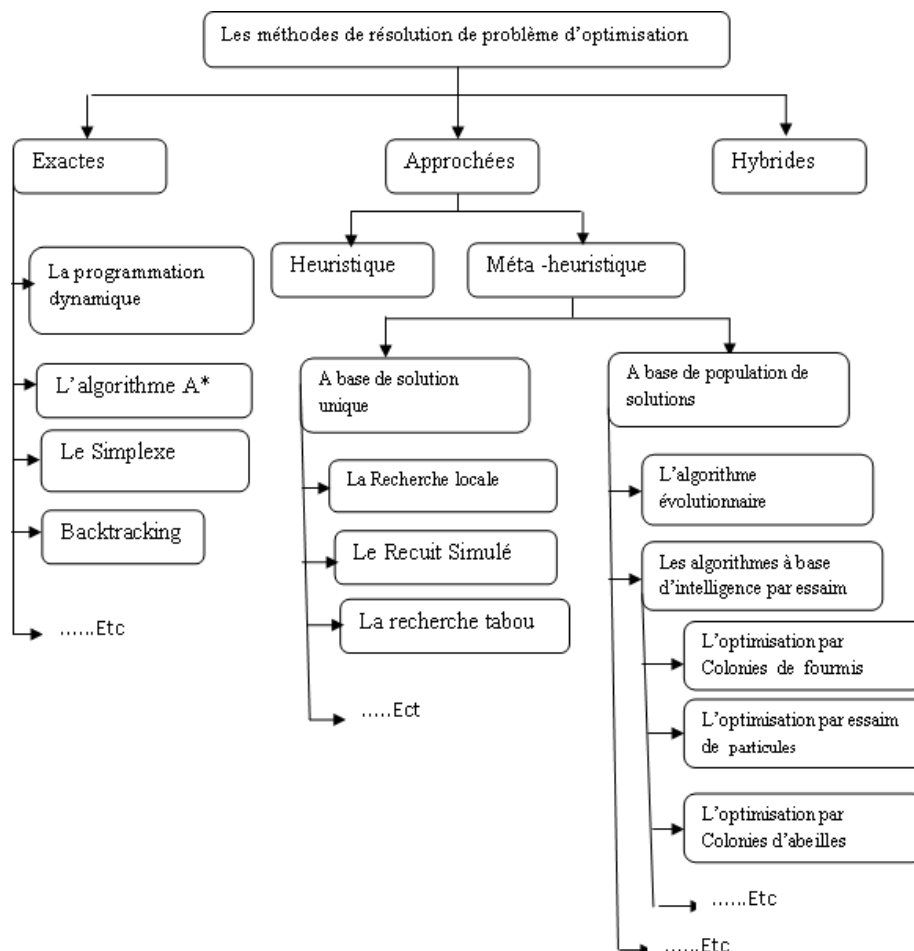


Figure 3.1: Classification des méthodes de résolution de problèmes d'optimisation.

3.2. 1. Les méthodes hybrides

Une méthode hybride combine deux ou plusieurs algorithmes, permettant d'exploiter les avantages de ces méthodes pour pallier les inconvénients d'un algorithme unique [1]. Chaque méthode, déjà suggérée, présente des points forts qu'on veut améliorer et des manques qu'on veut remplir. Sur cette base, de nombreux chercheurs ont proposé l'association des méthodes de résoudre les problèmes dans le but d'exploiter les avantages propres à chacune et aussi de suggérer des options plus efficaces et meilleures.

3.2. 2. Les méthodes exactes

L'atout des méthodes exactes est qu'elles garantissent de trouver la meilleure solution optimale pour le problème en question. Les méthodes exactes sont souvent critiquées pour leur coût élevé en ce qui concerne les ressources nécessaires. Effectivement, La durée de temps nécessaire pour la recherche et/ou la capacité de stockage en mémoire requise pour obtenir la solution idéale via une méthode précise est habituellement importante, surtout en ce qui concerne les problèmes de grande ampleur. Ainsi, la complexité de ce genre d'algorithmes croît de façon exponentielle en fonction de la dimension de l'instance à gérer. Elle s'avère particulièrement élevée dans le cas de problèmes impliquant plusieurs variables. On trouve de nombreux algorithmes exacts, parmi elle l'algorithme du simplexe, la programmation dynamique, l'algorithme A*, l'algorithme de retour arriéré (Backtracking),..., etc. [2] [3].

3.2.3. Les méthodes approchées

Différentes méthodes approchées suggérées, sont adaptées pour résoudre des problèmes complexes et pour trouver facilement des solutions dans un délai court. On classe généralement ces techniques en deux classes : les méthodes heuristiques et les méthodes méta-heuristiques (Figure 3.1).

3.2.3.1. Les méthodes heuristiques

Les méthodes qualifiées d'heuristiques sont des approches propres à une problématique spécifique. Elles requièrent une compréhension du domaine lié au problème abordé. Il s'agit effectivement de règles empiriques fondées sur l'expérience et les résultats obtenus dans le but d'optimiser les recherches à venir. Une heuristique est une méthode algorithmique qui offre une solution approximative et pratique, sans forcément être la meilleure, pour un problème

complexe d'optimisation. Cette approche approximative s'oppose à un algorithme précis qui fournit une solution optimale pour une problématique spécifique. On peut citer parmi ces algorithmes : Nearest Neighbor, Hill Climbing, Beam Search, Branch and Bound,..., etc.

3. 2.3.2. Les méthodes méta-heuristiques

Les méta-heuristiques des méthodes d'optimisation utilisées pour trouver des solutions à des problèmes complexes impossibles à résoudre par des approches standard [4]. Ces algorithmes sont basés sur des processus naturels, qu'ils soient issus de la physique (comme le recuit simulé), de la biologie de l'évolution (comme les algorithmes génétiques) ou de l'éthologie (comme les algorithmes de colonies de fourmis ou l'optimisation par essaims particuliers). On peut catégoriser ces techniques méta-heuristiques en deux catégories : les approches à solution unique telles que le recuit simulé et les approches reposant sur une population de solutions.

3. 2.3.2.1. Les méthodes méta-heuristiques à base de solution unique

Elles commencent la recherche en se basant sur une seule solution de départ, et utilisent le concept du voisinage dans le but d'optimiser la solution actuelle. En réalité, la solution initiale est modifiée plusieurs fois en se basant sur son entourage. L'objectif de ces modifications locaux visent à examiner autour de la solution actuelle pour l'améliorer petit à petit à chaque itération. Le voisinage de la solution comprend toutes les modifications possibles qui peuvent être apportées à la solution en question. La qualité du produit final est particulièrement influencée par les ajustements réalisés par les opérateurs de voisinage. Plusieurs approches basées sur une solution unique ont été suggérées dans les publications. Dans celles-ci figurent la descente, le recuit simulé, la recherche tabou et la recherche à voisinage [5].

3. 2.3.2.2. Les méta-heuristiques à base de population de solutions

Les méta-heuristiques basées sur la population commencent leur recherche avec une variété de solutions. Elles sont mises en œuvre sur un ensemble de solutions dans le but d'en déterminer la meilleure solution (l'optimum global), qui constituera la solution au problème examiné [5]. Le recours à un éventail de solutions plutôt qu'à une unique solution stimule la diversité dans la recherche et accroît les chances d'apparition de solutions de haute qualité. De nombreuses méthodes utilisant un groupe de solutions ont été proposées, allant des

algorithmes évolutionnaires aux algorithmes génétiques, puis aux algorithmes basés sur l'intelligence par essaims comme l'optimisation par essaim de particules, les colonies de fourmis et d'abeilles [6].

3. 2.3.2.2.1. L'intelligence par essaim

Les algorithmes qui utilisent l'intelligence collective (par essaim) constituent une catégorie d'algorithmes tirés des phénomènes naturels[5]. Ces algorithmes tirent généralement leur inspiration des comportements de groupe de quelques espèces pour résoudre leurs problèmes [7]. On utilise souvent le mot "essaim" pour désigner un ensemble ou un groupe limité de particules (comme l'oiseau, l'abeille, la fourmi,... ,etc.) ou d'entités interactives. Les oiseaux qui volent en essaims, les colonies de fourmis, les bancs de poissons, les ruches d'abeilles, et ainsi de suite. Par conséquent, en s'inspirant du comportement social des particules qui parviennent à une auto-organisation en essaims, plusieurs algorithmes ont été suggérés au cours des dernières décennies tels que : l'optimisation par essaim de particules (PSO) [8], l'algorithme des colonies de fourmis (ACO) [9], l'algorithme des colonies d'abeilles artificielles,..., etc.

3.3. Optimisation par l'algorithme de colonie d'abeilles artificielles

La technique d'optimisation par colonie d'abeilles est relativement nouvelle. Elle s'inspire du comportement naturel des abeilles pour son principe. Dervis Karaboga a élaboré l'algorithme en 2005 [10]. Dans cette perspective, nous allons d'abord détailler la structure d'une colonie d'abeilles, ensuite expliquer le comportement des abeilles quand elles recherchent de la nourriture. Et pour finir, exposer l'algorithme d'optimisation par colonie d'abeilles artificielle.

3. 3.1. Principe du fonctionnement de l'algorithme d'abeilles artificielles

Dans l'algorithme des colonies d'abeilles artificielles (ABC), la population de membres est représentée comme une colonie d'abeilles et on identifie trois types d'abeilles : les abeilles **employées** qui retrouvent les sources de la nourriture, les abeilles **spectatrices** (observatrices) sont chargées à évaluer les sources trouvées et les **scoutes** (éclaireuses ou exploratrices) sont tenues de chercher de nouvelles sources de nourriture [11].

L'algorithme ABC part du principe qu'il existe une unique abeille employée pour chaque source de nourriture. L'emplacement (la position) où se trouve une source de nourriture est

une solution possible au problème à optimiser. La quantité de nectar dans une source de nourriture témoigne de la qualité de la solution (une valeur fitness). Au début, la colonie ne compte que quelques abeilles éclaireuses (exploratrices) et observatrices (spectatrices). Les abeilles éclaireuses sont envoyées à la découverte des sources de nourriture potentielle de nectar, tandis que les observatrices attendent d'être recrutées près de la ruche. Si une abeille éclaireuse trouve une source de nectar, elle enregistre sa position actuelle dans sa mémoire et devient une abeille employée [12].

Dans la **phase des abeilles employées**, les abeilles employées sont celles qui ont déjà été assignées à une source de nourriture. Chacune d'elles enregistre sa position et sélectionne une autre source de nourriture chez sa voisine, puis choisit celle qui offre le meilleur nectar. Elles retournent ensuite à la ruche et commencent à danser en fonction de la qualité du nectar de la source de nourriture qui leur est associée (elle présente une danse nommée danse frétillante, afin de partager avec les autres abeilles la position de la source en nourriture).

Lors de la **phase des observatrices**, une abeille observatrice observe la danse des abeilles employées à la ruche et sélectionne une abeille employée en fonction des danses observées, de sorte que la probabilité de choisir une abeille employée soit proportionnelle à la qualité du nectar de cette abeille employée. L'abeille observatrice reçoit ensuite les informations relatives à la source de nourriture choisie (position de la source et qualité du nectar) et devient une abeille employée associée à cette source.

Dans la **phase des éclaireuses**, les éclaireuses ce sont des abeilles libres qui doivent trouver de nouvelles sources de nourriture et ensuite évaluer leur nectar. Dans cette phase, l'une des abeilles employées est sélectionnée et classée comme éclaireuse (explorent l'environnement autour de la ruche à la recherche de nouvelles sources de nourriture). Le choix est contrôlé par un paramètre de contrôle nommé (Limite). Lorsqu'une solution représentant une source de nourriture ne montre pas d'amélioration après un nombre déterminé d'essais, cette source de nourriture est abandonnée par son abeille employée et celle-ci devient éclaireuse. Le nombre de tentatives pour libérer une source de nourriture correspond à la valeur Limite, un critère de contrôle important dans l'algorithme ABC.

3. 3.2. Algorithme de colonie d'abeilles artificielles

L'algorithme de la colonie d'abeilles artificielles (ABC : Artificial Bee Colony (En anglais)) est une méta- heuristique d'optimisation inspirée du comportement intelligent des abeilles dans le cadre de la quête de nourriture. Proposé par **Derviş Karaboğa** en 2005 [10], il est particulièrement efficace dans le but de régler les problèmes d'optimisation continus et combinatoires.

Afin de rendre la compréhension de l'algorithme plus aisée, on donne dans la partie A son résumé, dans la partie B l'algorithme et dans la partie C le Pseudo-code de l'algorithme.

Partie A : Résumé des étapes principales de l'algorithme.

Les phases clés du fonctionnement de l'algorithme ABC sont résumées ci-dessous :
Au début, on introduit les paramètres de l'algorithme, ensuite on passe à la phase de l'initialisation.

1. Initialisation :

- Génération aléatoire des solutions initiales.
- Calcul de la fonction fitness pour chaque solution.
- Initialisation d'un compteur d'essais (trial) pour chaque solution.

2. Boucle principale (répéter pour chaque itération jusqu'au critère d'arrêt la phase des abeilles employées, observatrices et éclaireuses) :

- **Phase des abeilles employées :**
 - Chaque solution est modifiée localement (recherche de voisinage). quand la nouvelle solution demeure meilleure, elle prend la place de l'ancienne si non elle garde l'ancienne.
- **Phase des abeilles observatrices :**
 - Les abeilles observatrices attendent dans la ruche et décident des sources de nourriture à explorer en fonction des informations partagées par les abeilles employées.
 - La probabilité qu'une abeille observatrice choisisse une source de nourriture est proportionnelle à la qualité (fitness) de cette source de nourriture. Les sources de meilleure qualité attirent davantage d'observatrices.
 - Modification similaire à la phase des abeilles employées.

- **Phase des abeilles éclaireuses :**
 - Remplacement des solutions stagnantes (celles qui n'ont pas été améliorées après un certain nombre d'essais).
 - Une nouvelle solution est générée aléatoirement

3. Critère d'arrêt :

- Arrêt après un nombre fixé d'itérations ou si la solution ne s'améliore plus.

Partie B : Description détaillée de l'algorithme.

Etape 1. Définir les paramètres de l'algorithme ABC.

Les paramètres clés qui définissent l'algorithme ABC sont les suivants [12] :

- Taille de la colonie ou la population de la colonie (TC) : Il s'agit du total des abeilles employées et des abeilles observatrices. On choisit cette taille selon le problème à optimiser.
- $NS=TC/2$: Nombre de sources de nourriture (taille de la population des solutions). Elle est toujours choisie la moitié de la Taille de la colonie.
- Nombre d'abeilles employées = NS : La moitié de la population des abeilles se trouve désignée comme employées, tandis qu'un nombre équivalent est affecté comme nombre de sources de nourriture.
- Nombre d'abeilles observatrices = NS : Les observatrices sont attribuées au même nombre que les employées (moitié de la taille de la colonie).
- Nombre d'abeilles exploratrices (éclaireuses) = variable (Toute abeille employée qui arrive à la limite de tentative d'amélioration sans résultat, est transformée en éclaireuse pour découvrir de nouveaux endroits où se nourrir).
- Nmax : Nombre maximal d'itérations.
- Bornes supérieure ($x_{max,j}$) et inférieure ($x_{min,j}$) de chaque variable : Intervalle des solutions (espace de recherche).
- d : Dimension du problème.
- Limite (Limite d'abondant) : Il s'agit du nombre maximal de tentatives (itérations) accordé à une abeille employée pour améliorer sa valeur fitness.

Etape 2. Phase d'initialisation :

L'algorithme ABC produit une population initiale de NS solutions (sources de nourriture) distribuées de manière aléatoire. Chaque solution x_i ($i = 1, 2, \dots, NS$) qui est initialisée par les éclaireuses, représente un vecteur de solution au problème d'optimisation. Les variables contenues dans tout vecteur doivent faire l'objet d'une optimisation.

Soit $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,d})$ la i -ième source de nourriture et d , la dimension du problème d'optimisation. La population initiale de NS solutions est générée aléatoirement à partir de l'équation (3.1) :

$$x_{i,j} = x_{\min,j} + \text{rand}(0,1) (x_{\max,j} - x_{\min,j}) \quad (3.1)$$

Pour $i = 1, 2, \dots, NS$ et $j = 1, 2, \dots, d$.

Où $x_{i,j}$ est la solution comprise entre $x_{\min,j}$ et $x_{\max,j}$ dans la j -ième direction de dimension d .

$x_{\min,j}$, $x_{\max,j}$: limite inférieure et supérieure du j -ième direction de la dimension d de la solution x_i .

$\text{rand}(0, 1)$ est une variable aléatoire dont la valeur est comprise entre 0 et 1.

La fonction objectif f_i et sa fonction $fitness_i$ associée pour chaque solution x_i est donnée par la fonction suivante [16] :

$$fitness_i = \begin{cases} \frac{1}{f(x_i)+1} & \text{si } (f(x_i) \geq 0) \\ 1 + \text{abs}(f(x_i)) & \text{si } (f(x_i) < 0) \end{cases} \quad (3.2)$$

Ici, $f(x_i)$ représente la valeur de la fonction objectif à l'emplacement source de nourriture x_i .

De plus, un compteur d'essais (trial) est initialisé à 0 pour chaque source de nourriture (solution).

Après l'étape d'initialisation, la population des solutions est soumise à des cycles successifs. $C = 1, 2, \dots, C_{\max}$, ces cycles correspondent à des processus de recherche effectués par les abeilles employées, observatrices et éclaireuses.

Étape 3. Phase des abeilles employées :

Au cours de cette phase, chacune des abeilles employées x_i ($i = 1, 2, \dots, NS$) produit une nouvelle source de nourriture S_i dans le voisinage de sa position actuelle au moyen de l'équation ci-après :

$$S_{i,j} = x_{i,j} + \Phi_{(i,j)}(x_{i,j} - x_{k,j}) \quad (3.3)$$

Avec :

k : indice sélectionné aléatoirement de l'intervalle $[1, NS]$.

j : indice attribué aléatoirement de $[1, d]$.

$i \neq k$ et $i, k \in (1, 2, \dots, NS)$.

$\Phi_{(i,j)}$: un facteur aléatoire prend une valeur entre $[-1, 1]$.

$x_{k,j}$ est une abeille voisine de $x_{i,j}$.

Une fois que la solution S_i est obtenue, elle sera vérifiée si elle est dans l'intervalle des solutions [13] :

pour $j=1$ à d .

Si $S_{i,j} > x_{\max,j}$ alors $S_{i,j} = x_{\max,j}$ et Si $S_{i,j} < x_{\min,j}$ alors $S_{i,j} = x_{\min,j}$.

Une comparaison entre (x_i et s_i), c'est à dire entre la valeur de *fitness* ($fitness(x_i)$ et $fitness(s_i)$). Si $fitness(s_i) > fitness(x_i)$ l'abeille employée mémorise la nouvelle position et oublie l'ancien et le compteur d'essais (trial) est remis à 0. Sinon, la position précédente est conservée x_i et le compteur d'essais (trial) est incrémenté de 1.

Etape 4. Phase des abeilles observatrices :

Une fois que l'ensemble des abeilles employées finissent leurs recherches, elles communiquent aux abeilles observatrices, sur la piste de danse, les données concernant les quantités de nectar (valeur fitness) ainsi que les emplacements de leurs sources.

La valeur de probabilité p_i pour la i -ième source de nourriture avec laquelle une abeille employée x_i est choisie par une abeille spectatrice peut être calculée en utilisant l'expression donnée dans l'équation (3.4) :

$$p_i = \frac{fitness(x_i)}{\sum_{k=1}^{NS} fitness(x_k)} \quad (3.4)$$

Pour chaque source de nourriture x_i , un nombre réel aléatoire r est généré dans l'intervalle $[0,1]$. Si la valeur de probabilité p_i dans l'équation (3.4) associée à cette source est supérieure à ce nombre r aléatoire, alors l'abeille observatrice génère une mise à jour de la position de cette source de nourriture avec de l'équation (3.3). Après que la source est estimée, l'abeille observatrice, ou bien elle retient la nouvelle position et oublie l'ancienne (Si la solution nouvellement proposée est supérieure, elle supprime l'ancienne) et son compteur d'essais (trial) est remis à 0. Si la solution ne peut pas être améliorée, elle garde l'ancienne solution et le compteur d'essais (trial) augmente de 1. Ce processus est répété pour toutes les sources de nourriture x_i ($i=1, 2, \dots, NS$).

Étape 5. Phase des abeilles éclaireuses :

Un compteur d'essais (trial) est associé à chaque source de nourriture, indiquant le nombre d'essais pendant lesquels la source de nourriture ne peut être améliorée. Lorsque la source de nourriture ne peut être améliorée pendant un nombre d'essais prédéterminé (limite), l'abeille employée appartient à cette source de nourriture se transforme à une abeille éclaireuse. L'abeille éclaireuse trouve ensuite une nouvelle source de nourriture d'une façon aléatoire en utilisant l'équation (3.1).

Étape 6. Critère d'arrêt :

Contrôler le processus de calcul jusqu'à l'arrivée du nombre d'itérations à la valeur maximale prédéfinie, ou jusqu'à ce qu'une solution satisfaisante de la fonction objectif soit identifiée ou si la solution ne s'améliore plus.

Partie C : Le pseudo-code de l'algorithme ABC.

Conformément à la description ci-dessus, les étapes de : l'initialisation de la population, la phase d'abeille employée, calculer la probabilité, la phase d'abeille observatrice et la phase d'abeille éclaireuse, sont résumés dans le pseudo-code de l'ABC suivant [14].

STEP I Initialisation des paramètres de l'algorithme ABC :

- 1: Introduire les paramètres (TC, NS, Nmax , Limite).
- 2: Définie la fonction objectif (f) et l'intervalle des solutions .
- 3: Compteur d'essais (trial) initialisé à 0 pour chaque solution générée (NS).

STEP II Initialisation de la population

- 1: **pour** $i = 1$ à NS **faire**
- 2: **pour** $j = 1$ à d **faire**
- 3: Générer des solutions $x_{i,j}$ à l'aide de l'équation (3.1)
- 4: **Fin pour**
- 5: Évaluer la fitness de chaque solution x_i à l'aide de la fonction (3.2)
- 6: **Fin pour**

STEP III Phase des abeilles employées:

- 1: **pour** $i = 1$ à NS **faire**
- 2: choisir aléatoirement k , ou $k \in \{1,2,\dots,NS\}$ et $k \neq i$
- 3: choisir aléatoirement j , ou $j \in \{1,2,\dots,d\}$
- 4: Produire une nouvelle source de nourriture s_i avec de l'équation (3.3)
- 5: **Si** ($fitness(s_i) > fitness(x_i)$) **alors**
- 6: $x_i = s_i$
- 7: $fitness(x_i) = fitness(s_i)$
- 8: $trial_i = 0$

```

9:   Sinon
10:       $x_i = x_i$ 
11:       $trial_i = trial_i + 1$ 
12:   FinSi
13: Fin pour

```

STEP IV Calculer la probabilité p_i de chaque solution :

```

1:  $Somme\_probabilite = 0$ 
2: pour  $i = 1$  à NS faire
3:    $Somme\_probabilite = Somme\_probabilite + fitness(s_i)$  .
4: Fin pour
5: pour  $i = 1$  à NS faire
6:    $p_i = fitness(s_i) / Somme\_probabilite$ .
7: Fin pour

```

STEP V Phase des abeilles observatrices :

```

1: pour  $i = 1$  à NS faire
2:    $rnd = rand(0, 1)$ 
3:   Si ( $rnd < p_i$ )
4:     sélectionner aléatoirement  $k$ , ou  $k \in \{1, 2, \dots, NS\}$  et  $k \neq i$ 
5:     sélectionner aléatoirement  $j$ , ou  $j \in \{1, 2, \dots, d\}$ 
6:     Générer une nouvelle source de nourriture  $s_i$  à l'aide de l'équation (3.3)
7:     Si ( $fitness(s_i) > fitness(x_i)$ ) alors
8:        $x_i = s_i$ 
9:        $fitness(x_i) = fitness(s_i)$ 
10:       $trial_i = 0$ 
11:     Sinon
12:        $x_i = x_i$ 
13:        $trial_i = trial_i + 1$ 
14:     Fin Si
15: Fin pour

```

STEP VI Phase des abeilles éclaireuses :

```

1: pour  $i = 1$  à NS faire
2:   Si ( $trial_i \geq limite$ ) alors
3:     pour  $j = 1$  à  $d$  faire
4:       Produire une solution  $x_i$  avec de l'équation (3.1)
5:     Fin pour
6:      $trial_i = 0$ 
7:   Fin Si
8: Fin pour

```

STEP VII Programme principal :

```

1: Mettre  $iter = 1$ 
2: Tantque ( $iter \leq Nmax$ ) faire
3:   répéter STEP III à STEP VI
4:    $iter = iter + 1$ 
5: Fin Tantque
6: Mémoriser la meilleure solution ( La meilleure source de nourriture atteinte ).

```

3.4. Optimisation des facteurs d'insertion dans un algorithme de tatouage numérique par l'algorithme ABC .

Les algorithmes de tatouage numériques sont différenciés en fonction de la façon par laquelle la marque est insérée dans un document hôte, soit par ajout ou par substitution. L'insertion selon le principe additif est effectuée conformément à l'équation ci-dessous :

$$I_W = I_o + \alpha \times W \quad (3.5)$$

L'image tatouée I_W se crée en additionnant la marque W multipliée par un paramètre d'insertion (α) à l'image hôte I_o .

La qualité d'image ainsi que la robustesse d'un système de tatouage numérique dépendent principalement du facteur d'insertion (α). Un paramètre (facteur) d'insertion élevé garantit une robustesse importante de la marque tout en entraînant une dégradation significative de la qualité visuelle de l'image tatouée. En revanche, un petit paramètre d'insertion garantit une excellente qualité visuelle de l'image tatouée, tandis que la robustesse de la marque est plus fragile. Il est donc nécessaire de rechercher la meilleure valeur du facteur d'insertion (α), qui assure un équilibre entre invisibilité et robustesse. Les facteurs d'insertion sont sélectionnés manuellement dans la plupart des recherches existantes sur le tatouage d'images, sans tenir compte du fait que le facteur d'insertion dépend de l'image. En d'autres termes, chaque image nécessite un facteur d'insertion différent pour offrir une qualité visuelle de l'image tatouée et une robustesse optimale. L'utilisation des algorithmes d'optimisation méta-heuristiques permettent de déterminer les facteurs d'insertion les plus pertinents pour surmonter le conflit entre invisibilité et robustesse.

Dans ce travail, on a préféré l'utilisation de l'algorithme ABC pour trouver automatiquement les facteurs d'insertion optimaux permettant d'insérer la marque dans l'image (l'équation (3.5)), dans le but de surmonter le conflit entre invisibilité et robustesse. Dans cette partie, nous détaillons l'application de l'algorithme de colonie d'abeille artificielle dans le contexte de l'algorithme de tatouage numérique des images. La figure 3.2 illustre le schéma bloc de l'optimisation, lequel constitue un système asservi en boucle fermée.

On définit d'abord les paramètres de l'algorithme ABC :

- Taille de la colonie (TC) : (nombre d'abeilles employées et observatrices généralement prend comme valeur $TC/2$ chacune).
- L'intervalle des facteurs d'insertion à optimiser.

- $NS = TC/2$: Nombre de sources de nourritures (les solutions).
- Limite : Nombre maximal d'échecs avant abandon.
- d : Dimension du problème.
- Nombre maximal d'itérations : N_{max} .

On passe ensuite à l'étape d'initialisation :

1. Initialisation :

- Générer la population initiale $\alpha_i, i = 1, \dots, NS$.
- Examiner la fitness de chaque solution.
- Initialiser le compteur d'essais (trial) de chaque solution à 0.

On a comme variables d'entrée les facteurs d'insertion $\alpha_i (i = 1, \dots, NS)$.

L'intégration de la marque est réalisée pour chaque facteur d'insertion $\alpha_i (i = 1, \dots, NS)$ de la population (Insertion de NS fois la marque W dans NS même copies image hôte I_0 et on obtient ainsi NS images tatouées I_{W_i}) selon l'équation suivante :

$$I_{W_i} = I_0 + \alpha_i \times W_i \quad (3.6)$$

On a pour chaque image tatouée I_{W_i} d'indice $i (i = 1, \dots, NS)$:

(1) On calcule l'invisibilité (PSNR) entre l'image originale I_0 et l'image marquée I_{W_i} correspondante :

$$PSNR (I_0, I_{W_i}).$$

(2) Ensuite on effectue un nombre P des attaques choisies sur l'image marquée I_{W_i} . On arrive donc à obtenir P images qui sont tatouées et attaquées $\tilde{I}_{W_i,j}$, avec $j = \{1,2,\dots, p\}$.

(3) En se basant sur le processus d'extraction de la marque et en calculant la corrélation normalisée (NC) entre la marque originale W et les marques $\tilde{W}_{i,j}$ extraites à partir de chaque image marquée et attaquée $\tilde{I}_{W_i,j}$: $NC_j(W, \tilde{W}_{i,j})$ avec $j = \{1,2,\dots, p\}$.

On a comme variables de sortie une fonction fitness qui prend la forme générale suivante :

$$fitness(\alpha_i) = f (\sum_j^p NC_j(W, \tilde{W}_{i,j}) , PSNR (I_0, I_{W_i})) \quad (3.7)$$

où p représente le nombre d'attaques qui sert à évaluer les facteurs d'insertion $\alpha_i (i = 1, \dots, NS)$ dans le but de trouver la meilleure valeur de la fonction fitness (parmi toutes les solutions) et la mémoriser comme meilleure solution. Cette estimation objective est déterminée sur la base de l'image originale I_0 , l'image tatouée I_{W_i} , la marque originale W et les p marques extraites $\tilde{W}_{i,j}$, avec $j = \{1, 2, \dots, p\}$ après application de différentes p attaques

sur l'image tatouée aux choix selon l'objectif fixé. A titre d'exemple, la compression JPEG en utilisant un facteur de qualité Q, le filtrage médian, le recadrage, le bruit poivre et sel, la correction gamma, l'égalisation d'histogramme,...., etc.

Lorsque la condition d'arrêt n'est pas remplie, une mise à jour de la position des abeilles (les facteurs d'insertion α_i) pour maximiser la fonction fitness est effectuée à chaque itération selon le principe suivant :

itération = 0.

2. Répéter (Étape 1 à Étape 3) pour un nombre maximal d'itérations (Nmax) :

itération = itération +1.

Étape 1. Phase des abeilles employées :

A . Pour chaque solution α_i ($i=1,2,\dots,NS$) :

- Générer une solution voisine s_i autour de α_i .
- Si s_i est meilleure que α_i , remplacer α_i par s_i et réinitialiser trial[i] à 0.
- Sinon, incrémenter trial[i] avec 1.

B. Calculer la probabilité p_i pour chaque solution α_i ($i=1,2,\dots,NS$) (sélectionnée avec une probabilité proportionnelle à sa fitness) :

$$p_i = \text{fitness}[i] / \text{somme}(\text{fitness})$$

Étape 2. Phase des abeilles observatrices :

Pour chaque abeille observatrice α_i : un nombre réel r aléatoire est produit pour chaque source.

Dans le cas où la probabilité p_i associée à cette source est plus élevée que le nombre aléatoire donné, alors :

- Générer une solution voisine s_i autour de α_i .
- Si s_i est meilleure que α_i , remplacer α_i par s_i et réinitialiser trial [i] à 0.
- Sinon, incrémenter trial[i] avec 1.

Étape 3. Phase des abeilles éclaireuses :

Pour chaque solution α_i :

Si trial[i] \geq Limite :

- Remplacer α_i par une nouvelle solution aléatoire.
- Réinitialiser trial[i] à 0.

Condition satisfaite : Quand le nombre d'itérations atteint la valeur maximale prédéfinie ou si la solution ne s'améliore plus. Enregistrer la valeur de la meilleure solution finale (le facteur d'insertion (α) optimal).

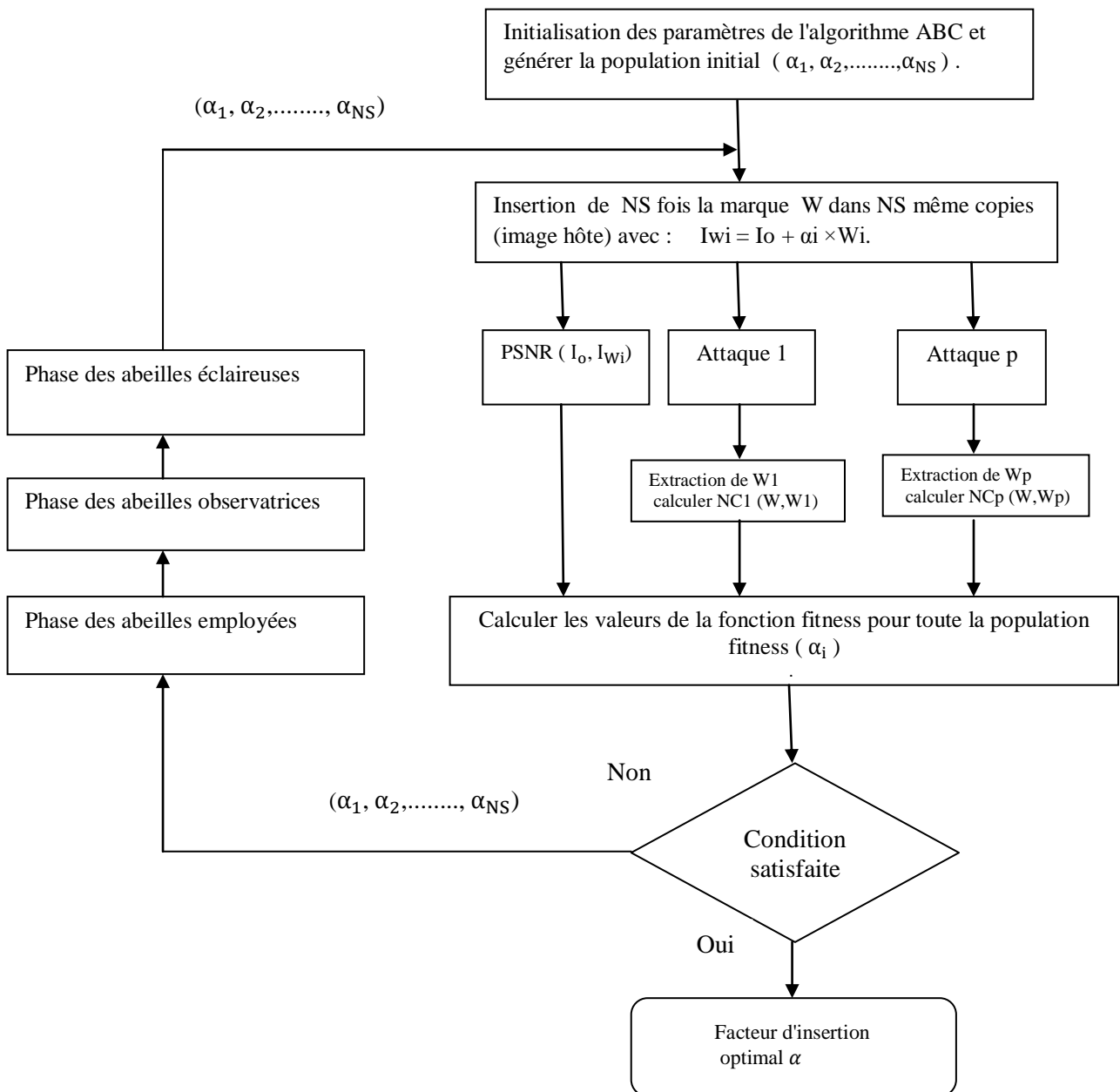


Figure 3.2: Le processus d'optimisation des facteurs d'insertion (α) .

3.5. Conclusion

Ce chapitre offre un panorama général des diverses techniques de résolution des problèmes d'optimisation exposées dans la littérature, allant des méthodes exactes aux solutions approchées, ensuite nous nous sommes concentrés sur les méthodes méta-heuristiques et nous avons focalisé sur les techniques utilisant l'intelligence par essaim qui ont gagné en popularité ces dernières décennies. Un choix a été fait sur la méthode d'optimisation par colonie d'abeilles artificielles pour plusieurs raisons : Il s'agit d'une des techniques d'optimisation récentes pouvant être utilisée pour divers problèmes d'optimisation. Le concept de base de cette méthode est de créer aléatoirement une population initiale, et de mener ensuite une recherche stochastique en s'appuyant principalement sur deux actions. La recherche autour des sources choisies, ainsi qu'une recherche d'exploration en intégrant de nouvelles sources après plusieurs tentatives d'amélioration. Ce processus, d'une part, favorise une recherche plus rapide et, d'autre part, permet une exploration approfondie de l'espace de recherche. Ensuite nous avons montré en détails comment appliquer l'algorithme(ABC) pour optimiser les facteurs d'insertion dans le cas d'un algorithme de tatouage numérique des images fixes. L'objectif du prochain chapitre est d'utiliser cette technique sur le tatouage numérique des images couleur, et d'examiner les résultats qui nous aident à trouver un équilibre entre l'invisibilité (ou imperceptibilité) et la robustesse.

Chapitre 4

Développement d'une nouvelle technique de tatouage d'images couleur optimisée, basée sur la décomposition de Hessenberg et la SVD dans le domaine des ondelettes.

4.1. Introduction

Le Tatouage numérique est considéré comme une solution fiable pour protéger les droits d'auteur et prouver la propriété de documents multimédias numériques tels que les fichiers audio, image et vidéo. Les performances d'invisibilité et de robustesse sont deux paramètres essentiels pour le tatouage d'images, et trouver le compromis entre elles constitue un enjeu majeur. Une solution proposée consiste à utiliser une méta-heuristique d'optimisation tel que la colonie d'abeilles artificielles (ABC), pour résoudre ce problème. De plus, ces dernières années, le tatouage d'images couleur est devenu un sujet de recherche prometteur. Un défi majeur consiste à concevoir une technique de tatouage intégrant une marque d'image couleur dans une image couleur hôte, dans lequel l'image hôte et la marque sont des images couleur, et les dimensions de la marque sont égales à celles de l'image hôte, ce qui augmente la capacité d'intégration de la marque dans l'image hôte. Car la plupart des systèmes de tatouage décrits dans la littérature utilisent des images binaires, en niveaux de gris, ou couleur et leurs dimensions sont inférieures à celles de l'image hôte.

Le but de ce présent travail est de développer une nouvelle technique de tatouage intégrant une marque qui est une image couleur dans une image couleur hôte, toutes les deux de la même taille et offrant une meilleure imperceptibilité, une capacité d'intégration élevée et surtout une grande robustesse, ainsi qu'une résistance réaliste aux attaques non géométriques et géométriques, afin d'assurer la protection des droits d'auteur et l'identification de la propriété.

Dans ce travail, nous utilisons la décomposition de Hessenberg (HD) et la SVD dans le domaine DWT. La HD agit comme une transformée matricielle, présente une bonne invariance rotationnelle, permet d'augmenter significativement la robustesse, pour résoudre le problème de la faible robustesse des algorithmes de tatouage numérique contre les attaques géométriques [1].

Les principaux apports de notre schéma proposé sont les suivants :

- 1) Au lieu de sélectionner manuellement les facteurs d'insertion. Nous avons appliqué l'algorithme ABC basé sur des conditions prédéfinies, le PSNR cible et la robustesse afin de trouver automatiquement les meilleures valeurs des facteurs d'insertion, car ces derniers dépendent de l'image et ne doivent pas être identiques pour toutes les images hôtes.
- 2) L'algorithme proposé utilise la décomposition de Hessenberg, elle présente une bonne invariance rotationnelle, ce qui lui confère une forte robustesse face aux attaques géométriques et améliore l'imperceptibilité.

3) Pour renforcer la sécurité et la robustesse de la marque intégrée, un niveau de protection supplémentaire a été ajouté : avant l'intégration, la marque est randomisée à l'aide d'une permutation chaotique appelée transformée d'Arnold.

4) Le schéma de tatouage proposé offre une capacité d'intégration élevée, une bonne imperceptibilité de l'image tatouée et une plus grande robustesse face aux attaques géométriques (rotation, mise à l'échelle, recadrage et découpe), aux attaques non géométriques (filtrage, netteté, ajout de bruit, compression JPEG) et aux attaques combinatoires (géométriques et non géométriques) par rapport aux schémas de tatouage d'images récents .

4.2. Le schéma de tatouage proposé

Il convient de préciser que l'image couleur destinée au tatouage est convertie du format RVB (Rouge, Vert et Bleu) vers le format YCbCr (Y: luminance, Cb : chrominance bleue, Cr : chrominance rouge), et que l'intégration s'opère au niveau de la composante de luminance Y de cette image couleur.

Dans le schéma proposé, l'image couleur hôte (I_{RVB}) et la marque une image couleur (W_{RVB}) sont converties de l'espace RVB vers l'espace YCbCr, et la composante de luminance (Y) de l'espace colorimétrique YCbCr de l'image hôte et de la marque sont sélectionnées. La composante de luminance Y de la marque est brouillée par la transformée d'Arnold. Ensuite, la composante de luminance brouillée est décomposée par DWT à un niveau de résolution et la sous- bande HL est choisit pour calculer la composante principale(CP) de la marque. La DWT à un niveau de résolution est aussi appliquée à la composante Y de l'image hôte, ce qui produit différentes sous-bandes ou sous-images multirésolution, la sous-image LL est sélectionnée pour l'insertion de la marque tout en conservant les autres bandes intactes et une décomposition de Hessenberg (HD) sur la sous-bande LL est appliquée pour obtenir la matrice supérieure H. Nous effectuons ensuite une décomposition en valeurs singulières de la matrice H. Dans ce travail, la composante principale(CP) de la luminance (Y) de la marque est insérée dans les valeurs singulières associées à l'image hôte avec un facteur d'insertion α approprié qui optimise le compromis robustesse-imperceptibilité. L'algorithme de colonie d'abeilles artificielles (ABC) est utilisé pour trouver les facteurs d'insertion α appropriés.

Pour extraire la marque, l'image tatouée est d'abord convertie à l'espace colorimétrique YCbCr. La composante de luminance Y est sélectionnée. Ensuite, la composante de luminance est décomposée par DWT à un niveau pour obtenir la sous-bande basse fréquence

LL tatouée, et la HD est appliquée sur cette dernière et la matrice supérieure H est sélectionnée, en suite la SVD est appliquée pour extraire la composante principale. La composante de luminance intégrée de la marque est récupérée, la transformée d'Arnold inverse est appliquée à cette dernière et le résultat est fusionné avec les autres composantes de couleur. Enfin, la marque extraite de l'espace colorimétrique YCbCr est transformée en espace colorimétrique RVB pour obtenir la marque extraite (W_{RVB}^*).

La méthode de tatouage numérique proposée se compose de trois parties, décrites dans cette section : l'insertion de la marque dans l'image hôte, l'extraction de la marque et l'optimisation des facteurs d'insertion à l'aide de l'algorithme (ABC).

Remarque : Le type d'ondelette choisit dans notre algorithme est l'ondelette de Haar.

4.2.1. Algorithme d'insertion de la marque

Le schéma bloc du processus d'insertion est illustré à la figure 4.1. Les étapes du processus d'insertion de la marque sont décrites ci-dessous :

1) Image hôte

Étape 1 : Tout d'abord, convertissez l'image couleur hôte (I_{RVB}) de l'espace colorimétrique RVB en espace colorimétrique YCbCr, ce qui permet d'obtenir les composantes de luminance I_Y , de chrominance bleue I_{Cb} et de chrominance rouge I_{Cr} :

$$[I_Y, I_{Cb}, I_{Cr}] = RVB2YCbCr(I_{RVB}) \quad (4.1)$$

Étape 2: Sélectionnez I_Y , la composante de luminance et appliquez la DWT à un niveau pour la décomposer en quatre sous-bandes I_{YLL} , I_{YHL} , I_{YLH} et I_{YHH} :

$$[I_{YLL}, I_{YLH}, I_{YHL}, I_{YHH}] = DWT(I_Y) \quad (4.2)$$

Étape 3 : Sélectionnez la sous-bande basse fréquence I_{YLL} pour l'insertion de la marque. Cette sous-bande contient la plupart des informations nécessaires pour résister à différents types d'attaques, et effectuer la décomposition en Hessenberg HD sur elle :

$$I_{YLL} = Q \times H \times Q^T \quad (4.3)$$

Étape 4: Sélectionnez la matrice de Hessenberg supérieure H et appliquez la SVD et enregistrez la matrice (S) pour la phase de l'extraction (clé secrète) :

$$\text{SVD}(H) = U \times S \times V^T \quad (4.4)$$

2) La marque W_{RVB} une image couleur dans l'espace colorimétrique RVB

Étape 5 : Convertissez l'image couleur W_{RVB} en espace colorimétrique YCbCr, ce qui permet d'obtenir les composantes $W_Y, W_{\text{Cb}}, W_{\text{Cr}}$, respectivement. Puis appliquez la transformée d'Arnold (TA) à la composante de luminance W_Y pour obtenir W'_Y :

$$[W_Y, W_{\text{Cb}}, W_{\text{Cr}}] = \text{RVB2YCbCr}(W_{\text{RVB}}) \quad (4.5)$$

$$W'_Y = \text{TA}(W_Y) \quad (4.6)$$

Étape 6 : Sélectionnez la composante de luminance brouillée W'_Y et appliquez la DWT à un niveau pour la décomposer en quatre sous-bandes : $W'_{\text{YLL}}, W'_{\text{YHL}}, W'_{\text{YLH}}$ et W'_{YHH} :

$$[W'_{\text{YLL}}, W'_{\text{YLH}}, W'_{\text{YHL}}, W'_{\text{YHH}}] = \text{DWT}(W'_Y) \quad (4.7)$$

Étape 7: Appliquez la SVD sur la sous-bande W'_{YHL} et extrayez la composante principale (PC_{water}) de la sous-bande et enregistrez la matrice V_{water}^T pour le schéma d'extraction de la marque (clé secrète) :

$$\text{SVD}(W'_{\text{YHL}}) = U_{\text{water}} \times S_{\text{water}} \times V_{\text{water}}^T \quad (4.8)$$

$$\text{PC}_{\text{water}} = U_{\text{water}} \times S_{\text{water}} \quad (4.9)$$

3) Insertion de la composante principale (PC_{water}) de la marque

Étape 8 : Insérer la PC_{water} de la marque dans la matrice diagonale (S) de la matrice de Hessenberg supérieure H de l'image hôte en utilisant le facteur d'insertion (α) optimal obtenu par l'utilisation de l'algorithme de colonie d'abeilles artificielle (ABC) comme suit :

$$\text{PC}_{\text{mark}} = S + \alpha \text{PC}_{\text{water}} \quad (4.10)$$

Étape 9 : Effectuez la SVD sur PC_{mark} et enregistrez les matrices U_{mark} et V_{mark}^T pour le schéma d'extraction de la marque comme suit :

$$\text{SVD}(\text{PC}_{\text{mark}}) = U_{\text{mark}} \times S_{\text{mark}} \times V_{\text{mark}}^T \quad (4.11)$$

Étape 10 : La matrice de Hessenberg supérieure tatouée H^* de l'image hôte est générée à l'aide de la SVD inverse :

$$H^* = U \times S_{\text{mark}} \times V^T \quad (4.12)$$

Étape 11 : Une nouvelle sous-bande d'approximation basse fréquence I_{YLL}^* est reconstruite à partir de la décomposition de Hessenberg inverse, donnée par :

$$I_{YLL}^* = Q \times H^* \times Q^T \quad (4.13)$$

Étape 12 : Appliquez la DWT inverse à un niveau à I_{YLL}^* , I_{YHL} , I_{YLH} et I_{YHH} pour obtenir la composante de luminance tatouée I_Y^* :

$$I_Y^* = IDWT [I_{YLL}^*, I_{YLH}, I_{YHL}, I_{YHH}] \quad (4.14)$$

Étape 13 : Fusionnez la composante de luminance I_Y^* tatouée avec les composantes de chrominance (I_{Cb} et I_{Cr}) dans l'espace colorimétrique YCbCr, ensuite Convertissez-la en espace colorimétrique RVB pour obtenir l'image couleur tatouée I_{wRVB} :

$$I_{wRVB} = YCbCr2RGB [I_Y^*, I_{Cb}, I_{Cr}] \quad (4.15)$$

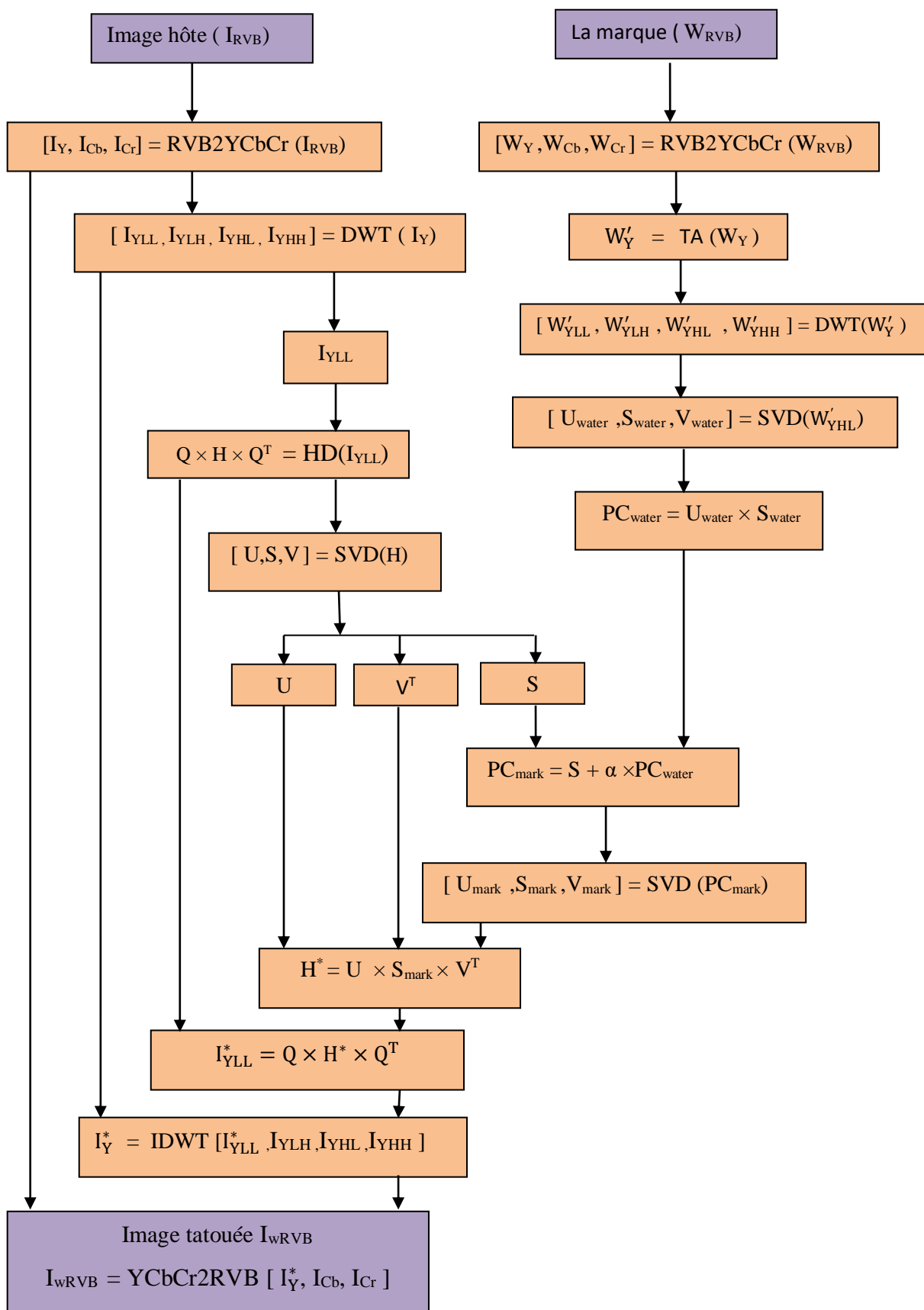


Figure 4.1 : Le schéma bloc du processus d'insertion de la marque.

4.2.2. Algorithme d'extraction de la marque

L'extraction est le processus inverse de l'intégration, dans lequel la marque intégrée est extraite à l'aide des informations connues uniquement de l'utilisateur légitime et obtenues lors de l'intégration. La procédure d'extraction est mise en œuvre comme illustrée à la figure 4.2 et elle est décrite selon les étapes suivantes :

Étape 1 : Tout d'abord, convertissez l'image couleur tatouée supposée attaquée ou modifiée I_{WRVB}^* vers l'espace colorimétrique YCbCr, ce qui permet d'obtenir les composants I_{wY} , I_{Cb}^* et I_{Cr}^* :

$$[I_{wY}, I_{Cb}^*, I_{Cr}^*] = RVB2YCbCr (I_{WRVB}^*) \quad (4.16)$$

Étape 2 : Sélectionner la composante I_{wY} de luminance et effectuez la DWT sur elle (une décomposition en ondelette de Haar à un niveau) pour obtenir les sous-bandes : I_{wYLL} , I_{wYLH} , I_{wYHL} et I_{wYHH} :

$$[I_{wYLL}, I_{wYLH}, I_{wYHL}, I_{wYHH}] = DWT (I_{wY}) \quad (4.17)$$

Étape 3 : Sélectionnez la sous-bande I_{wYLL} et effectuez la décomposition de Hessenberg sur elle, comme suit :

$$I_{wYLL} = Q_w \times H_w \times Q_w^T \quad (4.18)$$

Étape 4 : Sélectionnez la matrice de Hessenberg supérieure H_w et appliquez la SVD comme suit :

$$SVD(H_w) = U_w \times S_w \times V_w^T \quad (4.19)$$

Étape 5 : Utilisez les matrices clés : U_{mark} et V_{mark}^T (stockées dans le schéma d'intégration) pour obtenir :

$$PC_{Smark}^* = U_{mark} \times S_w \times V_{mark}^T \quad (4.20)$$

Étape 6 : Utilisez la clé S (stockée dans le schéma d'intégration) et extrayez la composante principale de la marque comme suit :

$$PC_{water}^* = \frac{(PC_{Smark}^* - S)}{\alpha} \quad (4.21)$$

Étape 7 : Utilisez la matrice clé V_{water}^T (stockée dans le schéma d'intégration) pour obtenir l'extraction de la sous-bande de la marque W_{YHL}^* comme suit :

$$W_{YHL}^* = PC_{water}^* \times V_{water}^T \quad (4.22)$$

Étape 8: Appliquez la DWT inverse à un niveau de résolution aux quatre sous-bandes W'_{YLL} , W'_{YLH} , W^*_{YHL} et W'_{YHH} pour obtenir la composante de luminance tatouée est brouillée $W_Y^{*'}$:

$$W_Y^{*' } = \text{IDWT}[W'_{YLL}, W'_{YLH}, W^*_{YHL}, W'_{YHH}] \quad (4.23)$$

Étape 9: Effectuez la transformée d'Arnold inverse sur $W_Y^{*'}$ pour obtenir la composante de luminance de la marque non brouillée W_Y^* :

$$W_Y^* = \text{TA inverse} (W_Y^{*' }) \quad (4.24)$$

Étape 10: Fusionnez la composante de luminance W_Y^* avec les composantes de chrominance (W_{Cb}, W_{Cr}) pour reconstruire l'image tatouée dans l'espace YCbCr, puis convertissez-la dans l'espace RVB pour obtenir l'image couleur de la marque extraite W_{RVB}^* :

$$W_{RVB}^* = \text{YCbCr2RVB}[W_Y^*, W_{Cb}, W_{Cr}] \quad (4.25)$$

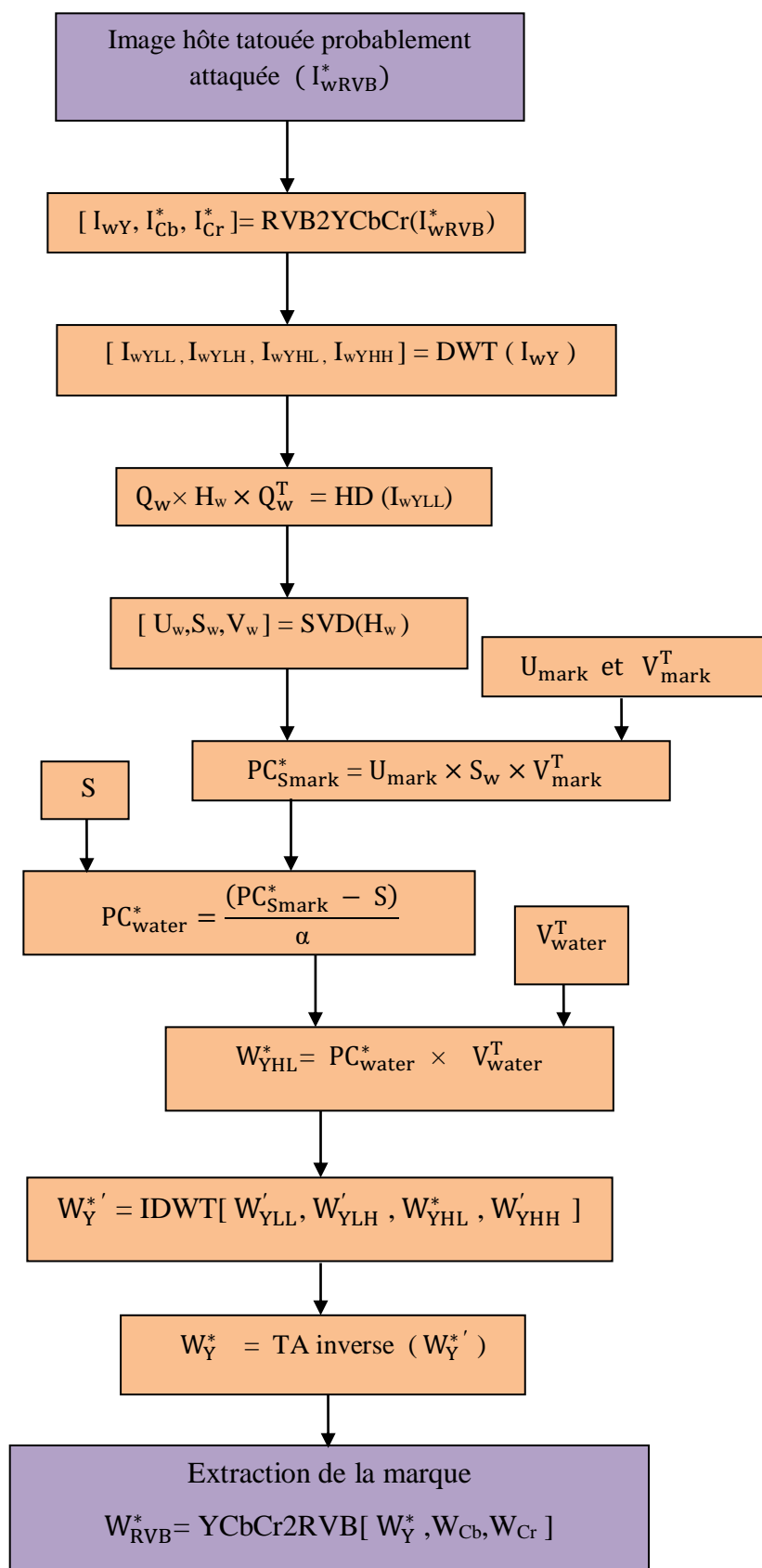


Figure 4.2 : Le schéma bloc du processus d'extraction de la marque.

4.2. 3. Optimisation des facteurs d'insertion à l'aide d'algorithme (ABC)

L'imperceptibilité et la robustesse du schéma proposé dépendent fortement de la valeur du facteur d'insertion (α). Une faible valeur offre une meilleure imperceptibilité, mais au prix d'une faible robustesse du schéma, une valeur élevée, quant à elle, entraîne une imperceptibilité faible, mais offre une grande robustesse. Il est donc nécessaire de trouver une valeur optimale du facteur d'insertion, assurant un équilibre entre imperceptibilité et robustesse pour chaque intégration en valeurs singulières. L'imperceptibilité (invisibilité) est mesurée avec le rapport signal/bruit de crête (PSNR) entre l'image hôte et son image tatouée et la robustesse avec la corrélation croisée normalisée (NCC) entre la marque originale et la marque extraite.

L'idée principale est d'obtenir une plus grande robustesse pour les attaques multiples, sous condition de satisfaire l'imperceptibilité.

Le processus d'optimisation des facteurs d'insertion (α) est présenté à la figure 4.3.

Les valeurs des paramètres de l'algorithme ABC sont présentées dans le tableau 4.1.

Nous appliquons sept (07) différents types d'attaques sur l'image tatouée I_{wRVB} à savoir le Bruit gaussien de moyenne = 0 et de variance = 0,003, une rotation d'image avec un angle de 15 degrés dans le sens des aiguilles d'une montre (rotation (15°)), filtre gaussien (3×3), filtre médian (3×3), recadrage (25%), translation (20, 20) et une correction gamma de valeur de 0,7.

La robustesse moyenne de ces sept (07) différents types d'attaques est la fonction objective que l'on cherche à maximiser. Elle est définie comme suit :

$$\text{Robustesse}_{\text{moyenne}} = \frac{\sum_{i=1}^P \text{NCC}(W, W_i^*)}{P} \quad (4.26)$$

Avec condition de maintenir le PSNR égal ou supérieur à un seuil ($\text{PSNR} \geq \text{PSNR}_{\text{cible}}$).

P : représente le nombre d'attaques, dans notre cas on a choisit sept (07) types d'attaques.

W : la marque originale image couleur type RVB.

W_i^* : les marques extraites à partir de chaque image hôte tatouée et attaquée.

La fonction fitness (Ft) de l'algorithme ABC à minimiser est définie comme suit :

$$\text{Ft} = \frac{1}{\text{Robustesse}_{\text{moyenne}}} \quad (4.27)$$

Plus la robustesse est élevée, plus la marque extraite est similaire à la marque d'origine.

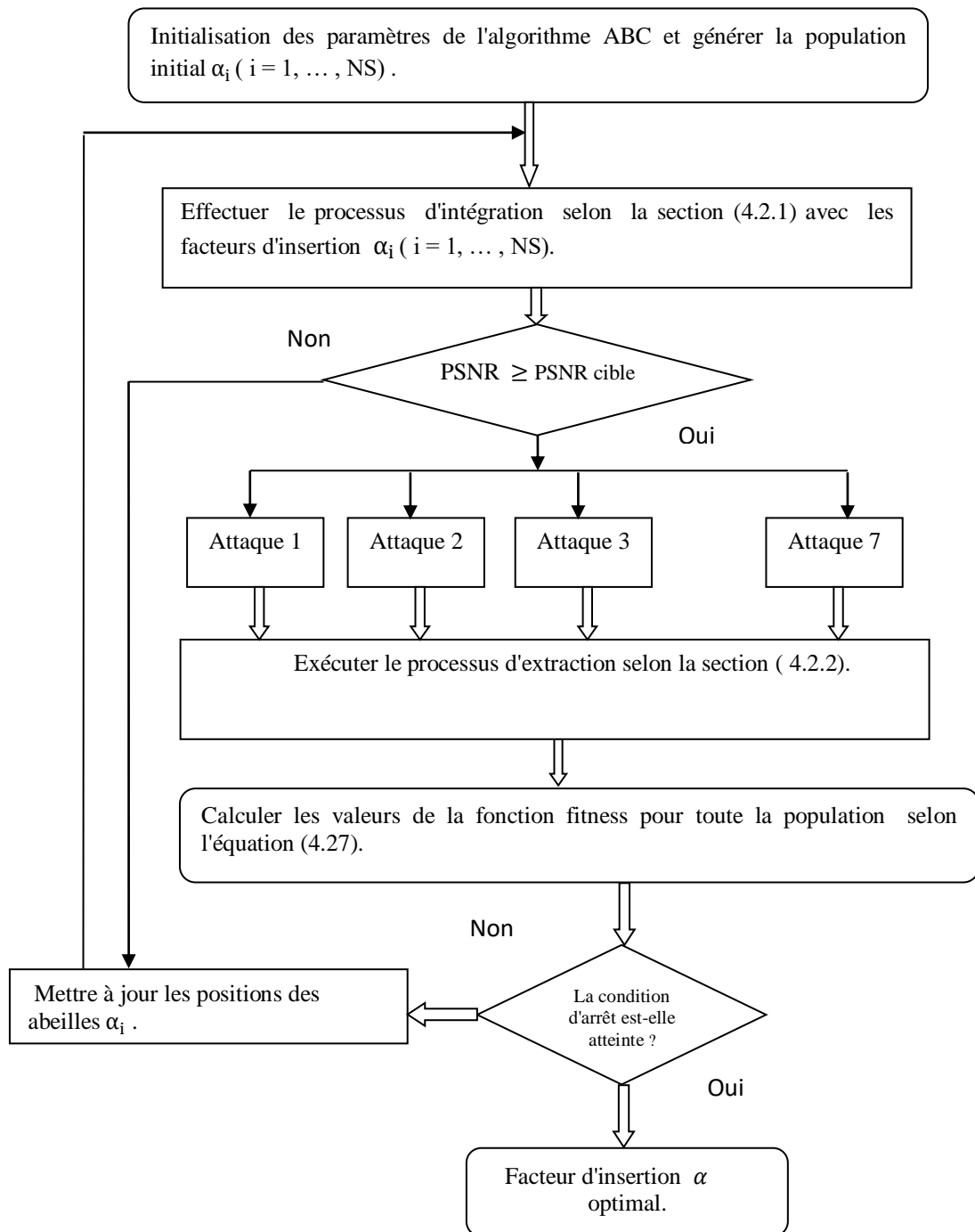


Figure 4.3 : Le processus d'optimisation des facteurs d'insertion (α).

Tableau 4.1 : Les valeurs des paramètres de l'algorithme ABC.

Paramètres de l'algorithme d'optimisation ABC	valeurs
Taille de la colonie	20
Nombre maximal d'itérations	12
Limite d'abondant	12
Intervalle des solutions	[0 , 1]
Nombre d'abeilles employées	50 % de la taille de la colonie
Nombre d'abeilles observatrices	50 % de la taille de la colonie
Nombre d'abeilles exploratrices	Variable
Sept (07) Attaques	Gaussian noise ($M = 0$, $\text{var} = 0.003$), rotation (15°), gaussian filter (3×3), median filter (3×3), cropping (25%) , translation (20, 20) , gamma correction (0.7).

4.3. Résultats expérimentaux et discussions

Toutes les expériences du schéma de tatouage proposé sont réalisées sur un ordinateur équipé d'un processeur Intel core i5-5200U à 2,20 GHz et de 8 Go de RAM, utilisant la version R2017a de MATLAB. Dans le but d'évaluer les performances du schéma proposé, cinq images hôtes en couleur de 24 bits/pixel de taille 512 x 512 pixels, à savoir Lena, Baboon, Peppers, Airplane et Sailboat, sont sélectionnées dans la base de données [2], sont présentées dans la figure 4.4, ainsi que deux images en couleur de 24 bits/pixel de taille de 512 x 512 pixels, à savoir le logo Peugeot et 8-color image comme deux marques, voir la figure 4.5.



(a) Lena

(b) Baboon

(c) Peppers

(d) Airplane

(e) Sailboat

Figure 4.4: Images couleur hôtes (a-e) .



(f) Peugeot logo.



(g) 8-color image.

Figure 4.5 : Marques à insérer respectivement (f) et (g) .

4.3.1. Résultats d'imperceptibilité et analyse comparative

Lorsque le PSNR est supérieur à 35 dB, l'image tatouée est considérée comme imperceptible [3]. L'analyse expérimentale du schéma proposé en terme de PSNR et NCC est présenté dans le tableau 4.2. D'après ce tableau, les valeurs de PSNR (calculée entre l'image couleur hôte d'origine et son image tatouée) obtenues sont supérieures à 46 dB pour les cinq images hôtes avec les deux marques (Peugeot logo et 8- color image) utilisées, ce qui indique que notre schéma présente une imperceptibilité élevée. La valeur de NCC est égal à 1, indiquant que la marque est entièrement récupérée pour le schéma de tatouage proposé dans le cas sans attaques. A partir des figures (4.6 et 4.7), on voit qu'il est difficile de distinguer entre les images originales et leurs images tatouées .

Tableau 4.2 : Résultats d'imperceptibilité (PSNR) entre l'image hôte d'origine et l'image tatouée, ainsi que la robustesse (NCC) entre la marque d'origine et la marque extraite pour le schéma de tatouage proposé sans attaques.

Images hôtes	Les marques			
	Peugeot logo		8- color image	
	PSNR(db)	NCC	PSNR(db)	NCC
Lena	46.3095	1	46.8579	1
Baboon	46.0233	1	46.5473	1
Peppers	46.5200	1	47.1339	1
Airplane	46.4928	1	47.1122	1
Sailboat	47.0590	1	47.5427	1

Nous avons comparé le schéma proposé avec la marque Peugeot logo intégrée aux différents schémas de tatouage présentés dans la littérature [4, 5, 7, 8, 9], voir dans le tableau 4.3. Il ressort du tableau 4.3 que les résultats d'imperceptibilité (valeurs de PSNR) du schéma proposé sont supérieurs à ceux des schémas présentés dans [4, 5, 7, 8, 9].

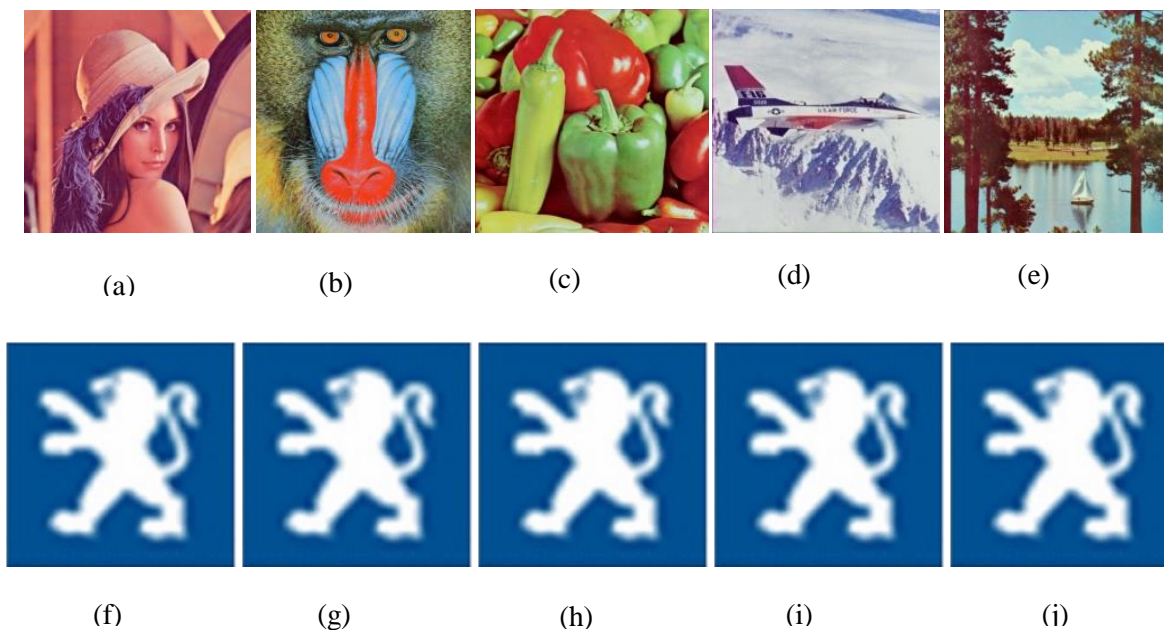


Figure 4.6 : Les images tatouées avec la marque Peugeot logo: (a) Image Lena tatouée, (b) Image Baboon tatouée, (c) Image Peppers tatouée, (d) Image Airplane tatouée, (e) Image Sailboat tatouée, (f) marque extraite de (a), (g) marque extraite de (b), (h) marque extraite de (c), (i) marque extraite de (d) et (j) marque extraite de (e) sans présence d'attaques sur les images tatouées .

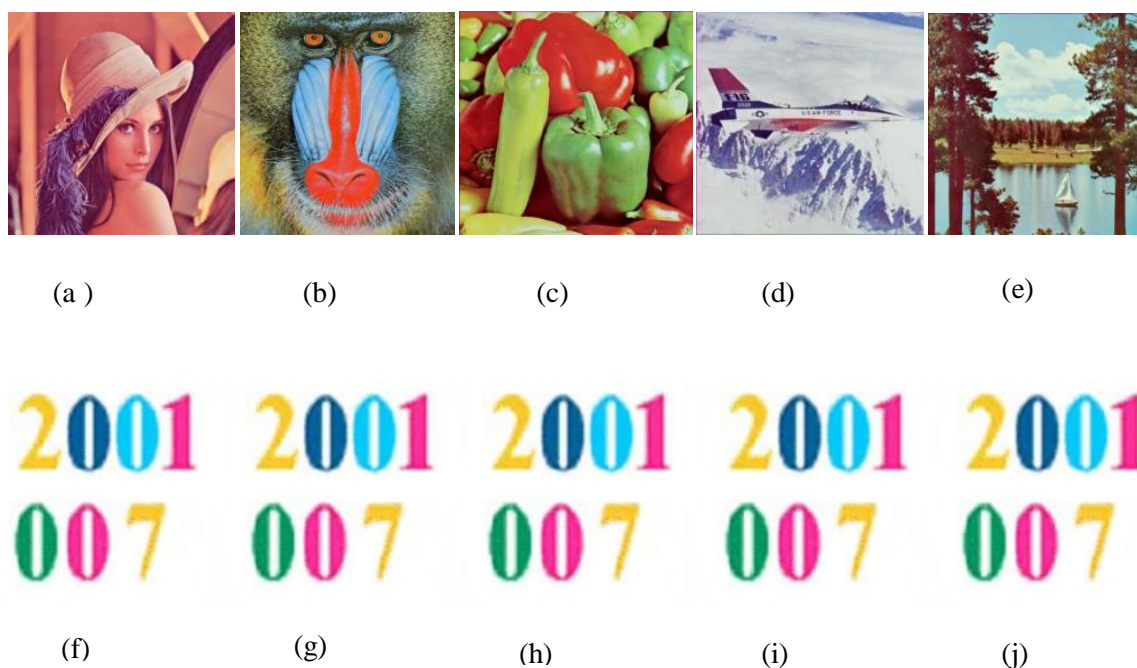


Figure 4.7 : Les images tatouées avec la marque 8- color image : (a) Image Lena tatouée, (b) Image Baboon tatouée, (c) Image Peppers tatouée, (d) Image Airplane tatouée, (e) Image Sailboat tatouée, (f) marque extraite de (a), (g) marque extraite de (b), (h) marque extraite de (c), (i) marque extraite de (d) et (j) marque extraite de (e) sans présence d'attaques sur les images tatouées.

Tableau 4.3: Analyse comparative du schéma proposé avec divers autres schémas de tatouage pour l'imperceptibilité utilisant le PSNR (dB) .

Image tatouée	PSNR (dB)					
	[4]	[5]	[7]	[8]	[9]	proposé
Lena	-	-	41.2072	44.3830	45.5728	46.3095
Baboon	46.1830	45.7047	-	-	45.3375	46.0233
Peppers	45.8709	45.6135	-	-	45.6712	46.5200
Airplane	45.3999	44.4467	40.0748	44.2744	45.0533	46.4928
Sailboat	46.0233	45.7167	-	-	45.2016	47.0590

Les figures 4.8 et 4.9 présentent les résultats du PSNR pour différentes valeurs du facteur d'insertion α , qui prend ces valeurs dans l'intervalle de 0.02 à 0.4 avec un pas de 0.02 pour les cinq images hôtes de tests. D'après les résultats des figures, il apparaît que plus la valeur du facteur d'insertion α est élevée, plus le PSNR est diminué. Il est bien clair que les valeurs du PSNR obtenues dans le cas de la marque Peugeot lego insérée varient entre 38dB à 52 dB (figure 4.8) et pour le cas de la marque 8-color image insérée varient entre 43 dB à 52 dB (figure 4.9). Ces valeurs du PSNR sont grandement appréciées dans le domaine du tatouage d'images, ce qui nous autorise à qualifier l'algorithme proposé d'imperceptible dans cette marge d'intervalle.

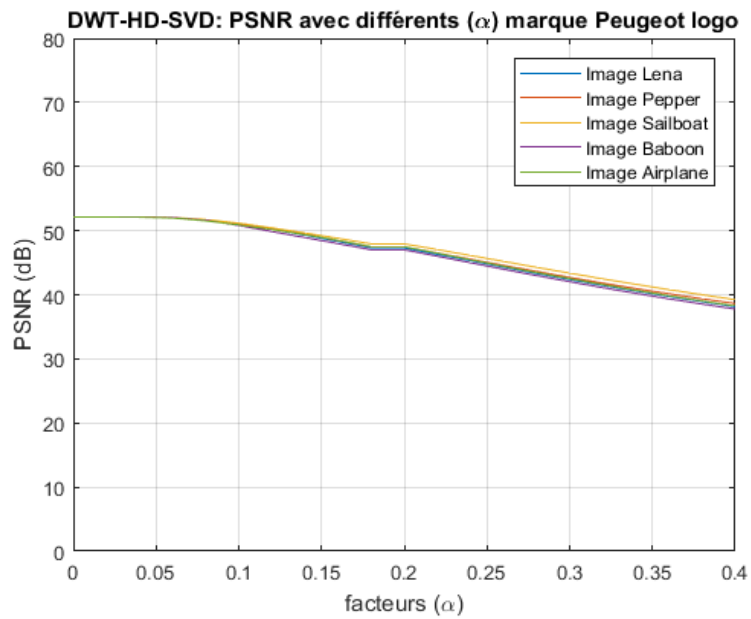


Figure 4.8 : PSNR sous différents facteurs d'insertion α pour les différentes images hôtes .

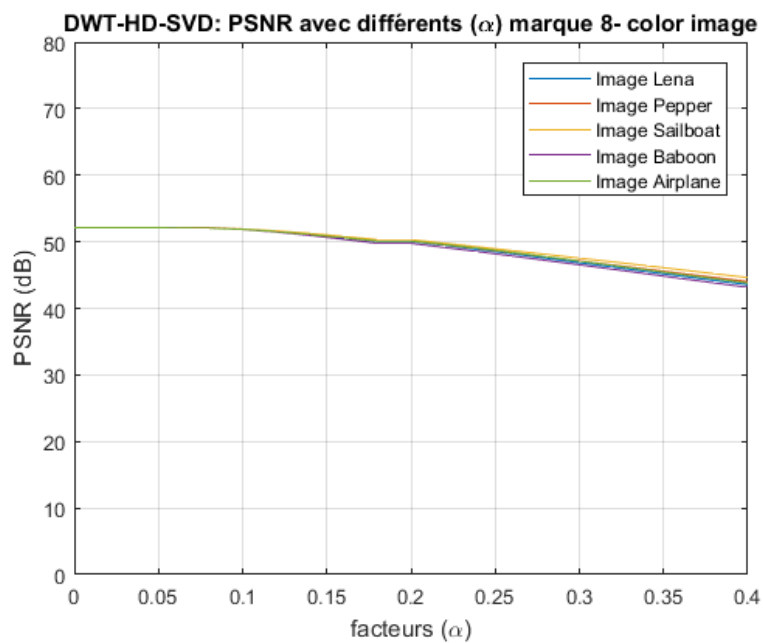


Figure 4.9 : PSNR sous différents facteurs d'insertion α pour les différentes images hôtes .

Les figures 4.10 et 4.11 présentent les résultats du NCC pour différentes valeurs du facteur d'insertion α , qui prend ces valeurs dans l'intervalle de 0.02 à 0.4 avec un pas de 0.02. Pour chaque valeur du facteur d'insertion α , nous appliquons sept (07) différents types d'attaques séparément sur l'image tatouée et ensuite on extrait la marque insérée pour chaque attaque, à savoir Le Bruit gaussien de moyenne = 0 et de variance = 0,003, une rotation de l'image avec un angle de 15 degrés dans le sens des aiguilles d'une montre Rotation (15°), Filtre gaussien (3×3), Filtre médian (3×3), Recadrage (25%), translation (20, 20) et une correction gamma de valeur de 0,7 et les résultats de la robustesse NCC entre la marque originale W et extraite W^* de chaque attaque est rapporté sur ces figures (l'image tatouée Lena avec la marque Peugeot logo et l'image tatouée Sailboat avec la marque 8- color image). D'après ces résultats, on remarque que plus la valeur du facteur d'insertion α est élevée, plus le NCC est élevée et sa valeur se rapproche de 1. Cela signifie qu'un facteur d'insertion α élevé fournit une robustesse élevée et inversement.

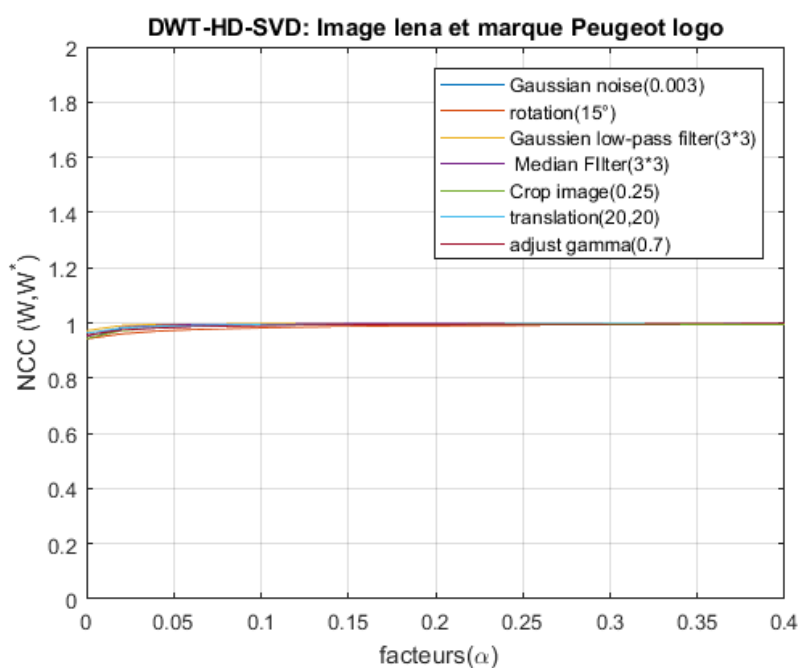


Figure 4.10: NCC sous différents facteurs d'insertion α pour image Lena.

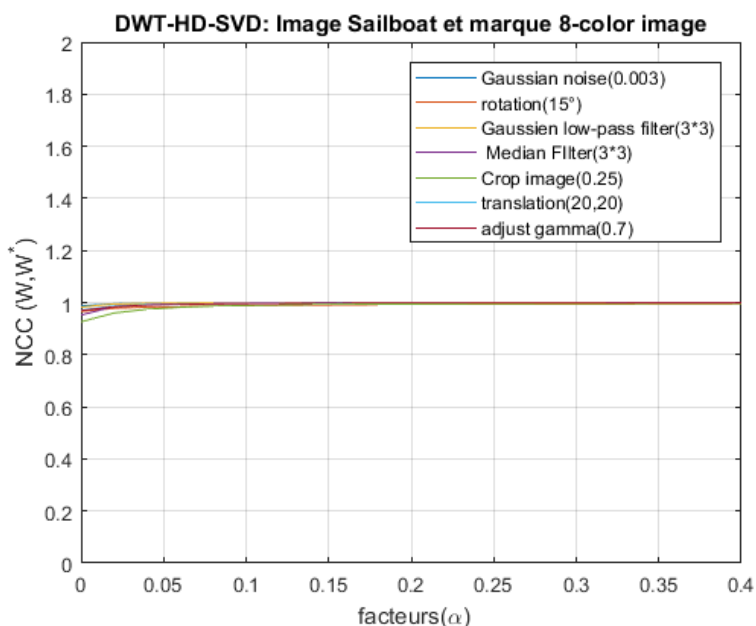


Figure 4.11: NCC sous différents facteurs d'insertion α pour image Sailboat.

Conclusion

- La différence de la valeur du PSNR obtenue entre les différentes images tatouées des tests avec la même marque d'insertion et avec le même facteur d'insertion α , revient à la nature des images (riche en contenu basse fréquence ou en haute fréquence ou constitue un mélange des deux, présente des contours et ou de la texture) qui diffèrent d'une image à l'autre et aussi en cas de changement de la marque (figure 4.8 et 4.9).

- D'après les figures (4.8 à 4.11), nous constatons de ces résultats que plus la valeur du facteur d'insertion α est élevée, plus le PSNR est diminué et plus le NCC est élevée se rapprochant de 1, ce qui veut dire que la marque extraite est très semblable à celle intégrée. Cela se résume qu'un facteur d'insertion α élevé fournit une faible imperceptibilité mais une robustesse élevée et inversement.

4.3.2. Résultats de la robustesse

La robustesse du schéma proposé est examinée en appliquant différentes attaques sur l'image tatouée et en mesurant la ressemblance entre la marque extraite et la marque originale (NCC). La corrélation croisée normalisée (NCC) est utilisée pour mesurer cette robustesse. Dans les expériences spécifiques suivantes, nous avons appliqué des attaques non géométriques (filtrage, ajout de bruit et compression JPEG et JPEG2000), et des attaques

géométriques (rotation, mise à l'échelle, recadrage, découpe et translation) sur différentes images tatouées .

Un exemple d'application de l'algorithme d'optimisation (ABC) sur l'image Lena est montré sur la figure 4.12. Il est bien clair, d'après la figure 4.12 que la méthode d'ABC tente toujours à chercher le meilleur facteur d'insertion α pour chaque itération et par conséquent, la recherche de la valeur minimale de la fonction fitness. La meilleure valeur α étant pour l'image Lena avec la marque Peugeot logo intégrée est obtenue à partir de la 8^{ème} itération pour une solution, un facteur d'insertion $\alpha = 0.22$ et comme résultat d'un PSNR de 46.3095 dB pour l'image tatouée Lena .

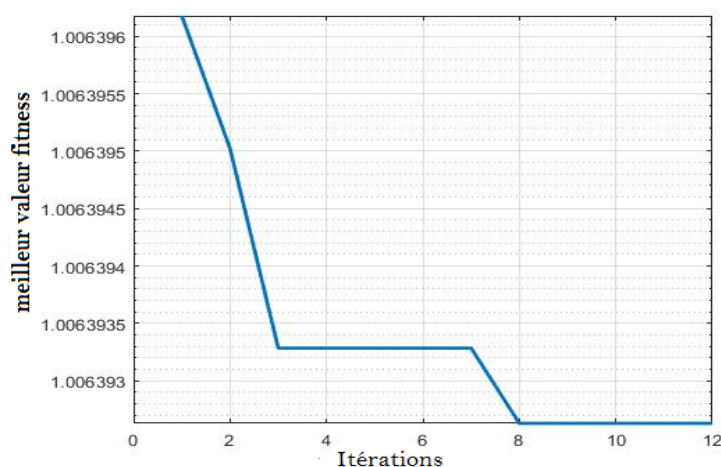


Figure 4.12 : L'évolution d'ABC après tatouage de l'image Lena avec la marque Peugeot logo.

4.3.2.1. Attaques non géométriques

Le tableau 4.4 présente les résultats des valeurs des NCCs des marques extraites (Image : Peugeot logo et 8-color image) suite à différentes attaques non géométriques avec des paramètres variables sur les images de tests (Lena, Airplane et Peppers) tatouées avec la marque Peugeot logo et 8-color image .

D'après ce tableau, on remarque que les valeurs des NCCs obtenues sont élevées pour toutes les images tatouées de tests avec les deux marques utilisées et les valeurs des NCCs des différentes attaques avec différents paramètres, montrent que, à mesure que la force de l'attaque augmente, les valeurs des NCCs affichent une tendance à la baisse, mais qui est faible. Cependant, cette tendance est relativement stable dans le cas de la compression JPEG et JPEG200.

La robustesse est testée sous compression JPEG avec différents facteurs de qualité Q , avec la valeur de $Q = 10, 70$ et 90 . Plus Q est petit, plus l'image tatouée est fortement compressée et plus Q est grand, plus l'image est faiblement compressée.

La robustesse est testée aussi sous compression JPEG2000 avec trois taux de compression CR (Compression ratio), avec la valeur de $CR = 10, 70$ et 90 . Plus CR est petit, plus l'image tatouée est faiblement compressée et Plus le CR est grand, plus l'image est fortement compressée.

L'efficacité du système de tatouage proposé est testé aussi sur trois types de bruits : Le bruit sel et poivre (Salt and Pepper noise), avec différentes valeurs de densité (density) de bruit de $0,01$ (1%), de $0,03$ (3%) et $0,05$ (5%) respectivement. Par ailleurs, le bruit gaussien (Gaussian noise) avec une moyenne nulle et des valeurs de variance (var) fixées à $0,01$ (1 %), à $0,03$ (3 %) et $0,05$ (5 %) est l'un des bruits les plus répandus susceptibles de corrompre l'image tatouée. De plus, les images tatouées sont également examinées en ajoutant le bruit de speckle (Speckle noise) avec une moyenne nulle et de variance(var) de valeur $0,01$ (1 %), de $0,03$ (3 %) et de $0,05$ (5 %).

Le filtrage généralement utilisé pour débruitage d'image, est une autre catégorie d'attaques. Les performances du schéma de tatouage proposé sont également testées à l'aide de trois types d'attaques de filtrage, filtre médian (Median filter), avec un filtre gaussien (Gaussian filter), et avec un filtre moyen (Mean filter) tous en utilisant des tailles de fenêtres différentes de : 2×2 , 3×3 et de 5×5 .

D'autres attaques non géométriques sont la correction gamma (GC), le flou de mouvement (Motion Blur), l'amélioration de la netteté (Sharpening) et l'égalisation d'histogramme (Histogram Equalization), qui sont également utilisées pour analyser les performances du schéma de tatouage proposé. La correction gamma (GC) est l'une des méthodes d'amélioration d'image les plus connues pour corriger une mauvaise qualité d'image. Les tests effectués avec une valeur de gamma de $0,3$, $0,5$ et de $0,8$. Dans l'opération de flou de mouvement (Motion Blur), le flou pour attaquer l'image tatouée est choisi avec l'angle = 4 et length = 7 . Dans l'opération de l'amélioration de la netteté (Sharpening) d'image, les paramètres choisis, Radius = 2 et Amount = 1 .

L'égalisation d'histogramme (HE) est une technique d'amélioration d'image. Les performances du système de tatouage proposé sont également évaluées grâce à la modification de l'histogramme avec 60 Bins et 150 Bins .

Tableau 4.4 : Résultat du NCC de la marque extraite pour le schéma proposé utilisant Peugeot logo et 8-color image comme marques sous diverses attaques non géométriques.

Attaques	Paramètres	Avec la marque Peugeot logo			Avec la marque 8-color image		
		Lena	Airplane	Pepper	Lena	Airplane	Pepper
JPEG	Q =10	0.9985	0.9984	0.9984	0.9991	0.9991	0.9991
	Q =70	0.9985	0.9985	0.9985	0.9992	0.9992	0.9991
	Q = 90	0.9985	0.9986	0.9985	0.9992	0.9992	0.9992
JPEG 2000	CR=5	0.9985	0.9985	0.9985	0.9992	0.9992	0.9992
	CR=10	0.9985	0.9985	0.9985	0.9992	0.9992	0.9992
	CR=40	0.9984	0.9984	0.9983	0.9991	0.9991	0.9991
Salt and Pepper noise	Density = 0.01	0.9978	0.9978	0.9977	0.9989	0.9989	0.9989
	Density = 0.03	0.9947	0.9944	0.9941	0.9980	0.9980	0.9978
	Density = 0.05	0.9907	0.9902	0.9890	0.9968	0.9966	0.9963
Gaussian noise	Var = 0.01	0.9949	0.9948	0.9947	0.9981	0.9981	0.9979
	Var = 0.03	0.9833	0.9844	0.9822	0.9946	0.9948	0.9942
	Var = 0.05	0.9712	0.9742	0.9702	0.9908	0.9915	0.9899
Speckle noise	Var = 0.01	0.9979	0.9968	0.9978	0.9990	0.9987	0.9989
	Var = 0.03	0.9959	0.9916	0.9952	0.9983	0.9970	0.9981
	Var = 0.05	0.9934	0.9860	0.9920	0.9976	0.9955	0.9972
Median filter	2×2	0.9982	0.9981	0.9982	0.9991	0.9992	0.9991
	3×3	0.9978	0.9977	0.9980	0.9990	0.9990	0.9990
	5×5	0.9955	0.9949	0.9966	0.9984	0.9982	0.9987
Gaussian filter	2×2	0.9980	0.9979	0.9980	0.9990	0.9990	0.9990
	3×3	0.9982	0.9981	0.9982	0.9991	0.9991	0.9991
	5×5	0.9982	0.9981	0.9982	0.9991	0.9991	0.9991
Mean filter	2×2	0.9980	0.9979	0.9980	0.9990	0.9990	0.9990
	3×3	0.9961	0.9956	0.9964	0.9985	0.9984	0.9986
	5×5	0.9891	0.9867	0.9905	0.9967	0.9960	0.9971
Gamma correction	0.3	0.9700	0.9553	0.9909	0.9875	0.9819	0.9957
	0.5	0.9865	0.9755	0.9956	0.9944	0.9905	0.9980
	0.8	0.9978	0.9944	0.9986	0.9992	0.9978	0.9993
Motion Blur	angle = 4 length = 7	0.9891	0.9893	0.9916	0.9966	0.9967	0.9974
Sharpening	Radius=2, Amount=1	0.9948	0.9954	0.9969	0.9967	0.9983	0.9987
Histogram Equalization	64 Bins	0.9819	0.9483	0.9919	0.9921	0.9774	0.9965
	150 Bins	0.9827	0.9495	0.9928	0.9930	0.9781	0.9969

La figure 4.13, présente les images de Lena qui sont tatouées avec la marque Peugeot logo et les marques extraites, suite à l'application de différents types d'attaques non géométriques : compression JPEG, compression JPEG2000, bruit Salt and Pepper, bruit gaussien, le bruit de speckle, filtre médian, filtre gaussien, filtre moyen, la correction gamma, le flou de mouvement (Motion Blur), l'amélioration de la netteté (Sharpening) et l'égalisation d'histogramme. D'après cette figure, il apparaît clairement que la marque a été récupérée parfaitement pour tous les types d'attaques.



Figure 4.13 : L'image tatouée (Lena) et la marque extraite (Peugeot logo) après application d'attaques non géométriques : (a) JPEG(Q = 10), (b) JPEG2000 (CR= 5), (c) Salt and Pepper noise (0.05), (d) Gaussian noise (0.05), (e) Speckle noise (0.05), (f) Median filter (5×5), (g) Gaussian filter (5×5), (h) Mean filter (5×5), (i) Gamma correction (0.8), (j) Motion Blur (angle = 4, length = 7), (k) Sharpening (Radius = 2, Amount = 1), (l) Histogram Equalization (64 Bins).

4.3.2.2. Attaques géométriques

Pour l'analyse des performances du système de tatouage proposé, cinq types de distorsions géométriques sont appliquées aux images tatouées : le recadrage (Cropping), le redimensionnement ou la mise à l'échelle (Scaling), la rotation (Rotation), la translation (Translation) et la découpe (CUT). Le tableau 4.5 présente les résultats des valeurs des NCCs des marques extraites (Peugeot logo et 8-color image) après application différentes attaques géométriques avec des paramètres variables sur les images de tests (Lena, Airplane et Peppers) tatouées avec la marque Peugeot logo et 8-color image. D'après ce tableau on

remarque que les valeurs NCCs sont dans la majorité élevées pour toutes les images tatouées avec les deux marques. D'après le tableau, on peut remarquer que les valeurs des NCCs de différentes attaques avec différents paramètres, montrent que, à mesure que la force de l'attaque augmente, les valeurs NCCs affichent une tendance à la baisse, mais qui reste relativement faible pour toutes les types d'attaques .

Le premier type de distorsion géométrique est le recadrage d'image (Cropping), qui consiste à supprimer une partie d'une image tatouée, généralement à partir des bordures. Le test est effectué avec une zone de recadrage de 20% , 25 % et 50 %.

Le deuxième type de distorsion géométrique est appelé rotation d'image (Rotation). Les performances du schéma de tatouage proposé sont testées en appliquant une attaque de rotation de 5°, 15° et 30° dans le sens anti - horaire afin d'en vérifier la robustesse.

Le troisième type de distorsion c'est la translation (TR), consiste à déplacer l'image tatouée horizontalement, verticalement ou les deux en même temps, déplaçant ainsi l'image de sa position d'origine. Des attaques par translation de (10, 10) ,(20, 20) et de (80, 80) sont effectuées .

Le quatrième type de distorsion est la découpe (CUT), qui consiste à éliminer des lignes de pixels sur l'image tatouée du côté gauche ou du côté droit et aussi dans les deux côtés en même temps. Afin de démontrer la robustesse du schéma de tatouage proposé, des attaques par découpe, de 10 lignes de pixels coté gauche et droite et aussi de 20 lignes de pixels coté gauche et droite sont effectuées .

Le cinquième type de distorsion est le redimensionnement ou la mise à l'échelle (Scaling), qui consiste à en modifier la taille d'image, que ce soit pour l'agrandir ou pour la rétrécir. Dans ce cas, les images tatouées sont vérifiées pour une attaque de mise à l'échelle, qui consiste à les redimensionner à une réduction d'échelle de 0.25, de 0.5 et à une augmentation d'échelle de 2 de leur taille d'origine.

La figure 4.14, présente les images de Lena qui sont tatouées avec la marque Peugeot logo et les marques extraites, suite à l'application de différents types d'attaques géométriques : le recadrage (Cropping), la Rotation, la Translation, la découpe (CUT), la mise à l'échelle (Scaling). D'après cette figure, comme nous pouvons le constater, les marques qui sont extraites semblent, identiques à celle intégrée, et cela pour tous les types d'attaques.

Tableau 4.5 : Résultat du NCC de la marque extraite pour le schéma proposé utilisant Peugeot logo et 8-color image comme marques sous diverses attaques géométriques.

Attaques	Paramètres	Avec la marque Peugeot logo			Avec la marque 8-color image		
		Lena	Airplane	Pepper	Lena	Airplane	Pepper
Cropping	20 %	0.9954	0.9983	0.9910	0.9981	0.9993	0.9967
	25 %	0.9853	0.9881	0.9872	0.9945	0.9954	0.9947
	50 %	0.9718	0.9614	0.9651	0.9908	0.9856	0.9863
Rotation	5°	0.9932	0.9867	0.9950	0.9970	0.9938	0.9981
	15°	0.9900	0.9766	0.9910	0.9956	0.9889	0.9961
	30°	0.9888	0.9710	0.9894	0.9947	0.9869	0.9954
Translation	(10,10)	0.9980	0.9984	0.9978	0.9990	0.9991	0.9989
	(20,20)	0.9968	0.9979	0.9960	0.9986	0.9990	0.9983
	(80,80)	0.9830	0.9913	0.9769	0.9934	0.9966	0.9909
Cut (left,right)	(10,10)	0.9979	0.9983	0.9980	0.9990	0.9991	0.9990
	(20,20)	0.9968	0.9978	0.9967	0.9986	0.9989	0.9986
Scaling	0.25	0.9887	0.9864	0.9902	0.9966	0.9960	0.9971
	0.5	0.9977	0.9975	0.9977	0.9989	0.9989	0.9971
	2	0.9985	0.9985	0.9984	0.9991	0.9991	0.9971

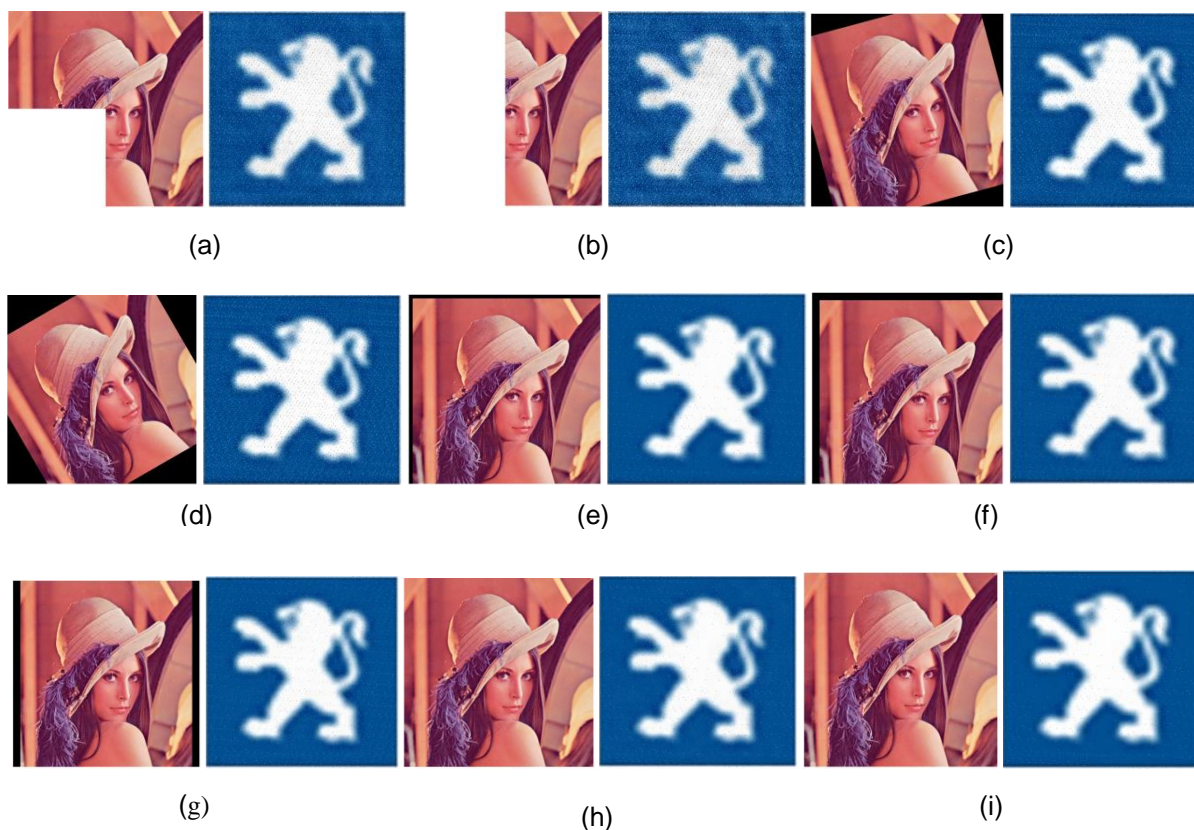


Figure 4.14 : L'image tatouée (Lena) et la marque extraite (Peugeot logo) après application d'attaques géométriques : (a) Cropping (25 %), (b) Cropping (50 %), (c) Rotation (15°), (d) Rotation (30°), (e) Translation (10,10), (f) Translation (20,20), (g) Cut (20,20), (h) Scaling (0.5), (i) Scaling (2).

4.3.3. Conclusion

Au vu des résultats des tests expérimentaux que nous avons obtenus, la méthode proposée démontre une excellente imperceptibilité (voir figure 4.6 et figure 4.7). Les valeurs PSNRs des images tatouées dépassent 46 dB pour les deux marques utilisées (tableau 4.2). En ce qui concerne la robustesse, nous avons mis en œuvre des attaques géométriques et non géométriques sur les images tests tatouées, avec les deux marques utilisées. Il est facile de conclure que le schéma de tatouage suggéré présente une robustesse élevée, comme l'illustre la figure 4.13 et la figure 4.14. Les valeurs des NCCs obtenues dans le contexte des deux marques utilisées sont en grande majorité largement supérieures à 0,9900.

4.4. Analyse comparative

Dans le but de démontrer la robustesse du schéma proposé face à différentes attaques de tatouage, les résultats obtenus dans le présent travail sont comparés à ceux des autres schémas de tatouage similaires dans la littérature :

4.4.1. Comparaison avec les schémas de tatouage couleur avec la marque une image en niveaux de gris

L'algorithme proposé a été testé avec diverses attaques d'images, incluant des attaques non géométriques et géométriques. Une analyse comparative en termes de la robustesse avec les schémas récents présentés dans [4,5,6], sous les mêmes attaques et paramètres, en utilisant l' image couleur Airplane tatouée avec la marque Peugeot logo est faite. Les résultats de la comparaison avec les valeurs des NCCs sont présentés dans le tableau 4.6. Selon les résultats des NCCs du tableau 4.6, montrent facilement qu'il est évident que notre méthode surpasse les méthodes citées, en termes de robustesse dans la majorité des situations d'attaques sur l'image Airplane. Donc on peut dire que l'algorithme proposé est très robuste. Mais reste à noter que quelques résultats sont légèrement supérieur à les nôtres, dans le cas d'ajout du bruit gaussien (Gaussien noise) avec la variance de 0.01 et en présence de la Rotation d'image avec un angle de cinq degrés (5°) dans [6], et aussi la compression JPEG avec un facteur de qualité $Q=90$ dans [5] et en présence de Bruit de sel et de poivre (Salt and Pepper noise) avec une densité de 0.05 dans [4] .

Dans les schémas [4, 5, 6], une image en niveaux de gris de taille 256×256 pixels de 8 bits/pixel, comme marque est utilisée de taille inférieure à celle de l'image couleur hôte de taille de 512×512 pixels de 24bits/pixel. L'image couleur hôte est d'abord convertie de

l'espace couleur RVB vers l'espace couleur YCbCr, et la composante de luminance (Y) est prise en compte pour l'insertion des données du tatouage.

Dans [4], le schéma de tatouage d'images proposé est basé sur la transformée en ondelettes discrète (DWT), la transformée en cosinus discrète (DCT) et la décomposition en valeurs singulières (SVD). Dans le schéma [5], l' algorithme de tatouage est basé sur la DWT, la décomposition de Hessenberg (HD) et la SVD. Par contre dans [6], le schéma de tatouage d'images présenté est basé sur la transformée en ondelettes entières, la décomposition de Hessenberg (HD) et la SVD.

Le schéma proposé dans ce travail est basé sur l' utilisation de la décomposition en Hessenberg (HD) et de la SVD dans le domaine de la DWT. La marque utilisée est une image couleur ayant les mêmes dimensions que l'image couleur hôte, soit 512×512 pixels avec une profondeur de 24 bits par pixel, ce qui offre un haut niveau d'intégration. De plus, il utilise l'algorithme ABC qui peut accélérer la recherche du facteur d'insertion optimal.

Tableau 4.6 : Comparaison de la robustesse entre le schéma proposé et des schémas de [4, 5 et 6], basée sur les valeurs de NCCs.

Attaques	Paramètres	Méthodes avec image hôte Airplane			
		[4]	[5]	[6]	Proposée
JPEG compression	Q = 70	-	-	0.9959	0.9985
	Q = 90	0.9986	0.9988	-	0.9986
Salt and Pepper noise	Density = 0.01	-	0.9920	0.9922	0.9978
	Density = 0.05	0.9918	0.9337	-	0.9902
Gaussien noise	Var = 0.01	-	0.9772	0.9956	0.9948
	Var = 0.05	0.9146	0.8380	-	0.9742
Speckle noise	Var = 0.01	-	0.9841	0.9917	0.9968
	Var = 0.05	0.9822	0.8653	-	0.9860
Median filter	3×3	-	-	0.9952	0.9977
Gaussian filter	3×3	0.9960	0.9963	0.9962	0.9981
	5×5	-	0.9932	-	0.9981
Sharpening	Radius=2, Amount=1	0.9745	0.9733	0.9935	0.9954
Mean filter	3×3	0.9944	0.9948	0.9941	0.9956
	5×5	-	0.9818	-	0.9867
Cropping	0.20	0.8871	0.9239	-	0.9983
Rotation	10°	0.8182	0.8445	-	0.9805
	5°	-	0.8984	0.9930	0.9867
Scaling	0.5	-	-	0.9962	0.9975
	2	-	-	0.9970	0.9985
Gamma correction	0.8	-	0.9800	-	0.9944

4.4.2. Comparaison avec les schémas de tatouage couleur avec la marque une image en couleur

Les résultats comparatifs de la robustesse entre le schéma proposé et ceux de [7, 8], en se basant sur les valeurs des NCCs sont présentées dans le tableau 4.7. D'après ce tableau, on peut constater que notre technique surpasse les deux autres techniques pour le cas de l'image Airplane tatouée avec la marque 8-color image et aussi pour l'image Lena tatouée avec la marque Peugeot logo, sauf exception dans le cas de l'attaque avec une compression JPEG 2000 pour les deux images tatouées, le résultat du NCC du schéma proposé est légèrement inférieur à celui de [8]. Pour les attaques géométriques, l'algorithme proposé présente un degré d'amélioration plus important que ceux décrits dans la littérature [7,8], notamment pour les attaques par rotation, translation et recadrage. l'algorithme proposé atteint systématiquement des valeurs NCCs supérieures à celles décrites par [7,8].

Dans le schéma [8], le tatouage est une image couleur de taille 128×128 pixels de 24 bits/pixel est utilisé pour l'intégrer à l'image couleur hôte de taille 512×512 pixels de 24bits/pixel. La marque est insérée dans la composante de couleur bleue de l'image hôte avec un facteur d'insertion optimisé dans le but d'atteindre un bon compromis entre robustesse et imperceptibilité. Dans le schéma [7], un algorithme de tatouage aveugle est développé. La marque utilisée est une image couleur de taille 32×32 pixels de 24bits/pixel, et l'image couleur hôte de taille 512×512 pixels de 24bits/pixel.

Tableau 4.7: Comparaison de la robustesse du schéma proposé avec les schémas de [7, 8], basée sur les valeurs NCCs.

Attaques	Paramètres	image hôte Aiplane avec la marque 8-color image			image hôte Lena avec la marque Peugeot logo		
		[7]	[8]	Proposé	[7]	[8]	Proposé
JPEG compression	Q = 30	0.7541	0.9881	0.9992	0.8577	0.9808	0.9985
JPEG 2000	CR=10	0.8405	0.9998	0.9992	0.9383	0.9995	0.9985
Gaussien noise	Var = 0.003	0.6478	0.9965	0.9990	0.7623	0.9935	0.9979
Salt and Pepper noise	Density = 0.01	0.9251	0.9872	0.9989	0.9478	0.9912	0.9978
Median filter	2×2	0.7009	0.9992	0.9992	0.8439	0.9983	0.9983
Cropping	50 %	0.9625	0.8200	0.9856	0.8398	0.9632	0.9718
Zoom-out	1:2	0.7999	0.9989	0.9991	0.9833	0.9968	0.9985
Rotation	30°	0.8224	0.8274	0.9869	0.9062	0.7251	0.9888
Translation	(-40,-20)	0.9873	0.8196	0.9985	0.9404	0.7251	0.9974

4.4.3. Attaques combinatoires

Les combinaisons de plusieurs attaques simultanées sur l'image tatouée sont appelées attaques multiples. Une personne non autorisée tente systématiquement d'appliquer plusieurs attaques pour détruire la marque intégrée, d'où l'importance d'expérimenter plusieurs attaques sur le schéma proposé. L'analyse comparative du schéma de tatouage proposé en termes de valeur de NCC en utilisant une combinaison d'attaques géométriques et non géométriques simultanément est faite. Le tableau 4.8 montre que les valeurs des NCCs obtenues par notre schéma sont supérieures à celles de [9] pour toutes les attaques multiples avec les mêmes paramètres en utilisant les mêmes images hôtes couleur (Lena, Baboon et Pepper) avec la marque Peugeot logo intégrée. D'après le tableau, on constate que le schéma de tatouage proposé est robuste face à ces attaques (les valeurs NCCs pour toutes les attaques multiples sont supérieures à 0,9800). Certains résultats de ces attaques sur l'image tatouée Baboon sont présentés dans la figure 4.15 avec la marque extraite. Nous pouvons observer que la récupération de la marque est totale.

Tableau 4.8 : Comparaison des valeurs du NCC sous plusieurs attaques en utilisant la marque Peugeot logo.

Attaques combinatoires	Images tatouées avec la marque Peugeot logo					
	Lena		Baboon		Peppers	
	[9]	proposé	[9]	Proposé	[9]	Proposé
Gaussian noise (0.01) + Cropping (25%)	0.9088	0.9885	0.9045	0.9934	0.8990	0.9861
Median filter (2×2) + Translation (20,20)	0.9958	0.9961	0.9923	0.9952	0.9918	0.9953
Salt and Pepper noise(0.02) +Rotation (1°)	0.9715	0.9976	0.9699	0.9973	0.9685	0.9970
JPEG compression (Q=90) + Translation (10,10)	0.9755	0.9980	0.9710	0.9983	0.9700	0.9977
Salt and Pepper noise(0.02) + Cropping (25%)	0.9715	0.9879	0.9699	0.9922	0.9685	0.9868
JPEG compression (Q=30) + Rotation(1°)	0.9245	0.9976	0.9045	0.9966	0.9130	0.9972
Salt and Pepper noise(0.1) + Scaling(0.25)	0.9588	0.9847	0.9455	0.9568	0.9570	0.9849
Salt and Pepper noise(0.02) + Cutting(10,10)	0.9015	0.9958	0.8990	0.9978	0.9090	0.9956

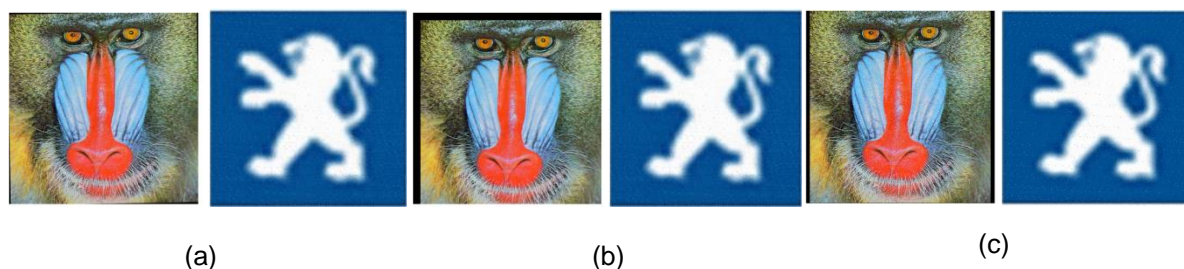


Figure 4.15 : Résultats d'attaques multiples sur l'image tatouée Baboon avec la marque Peugeot logo intégrée sous : (a) compression JPEG (30) + rotation (1°), (b) filtre médian (2×2) + translation (20, 20), et (c) bruit sel et poivre (0,02) + découpage (10 ,10).

4.4. 4. Analyse de la capacité d'intégration

La capacité d'intégration peut être calculée à partir du nombre de bits de la marque intégrée et du nombre de pixels de l'image hôte. La capacité d'intégration est également un facteur important pour mesurer la qualité de l'algorithme de tatouage. La capacité d'intégration mesure le nombre de bits d'information pouvant être insérés dans l'image hôte [10]. Comme le montre le tableau 4.9. Dans notre schéma, l' image couleur hôte et la marque (une image couleur), toutes les deux de taille 512×512 pixels, par conséquent, la capacité d'intégration de notre schéma est de $(512 \times 512 \times 24) / (512 \times 512 \times 3) = 8$ bpp. Il s'agit d'une capacité d'intégration élevée par rapport aux schémas de tatouage qui utilisent une marque est une image en niveaux de gris avec 8 bits / pixel et l' image couleur hôte de taille 512×512 pixels de capacité d'intégration $(256 \times 256 \times 8) / (512 \times 512 \times 3) = 0.6667$ bpp pour le cas des articles [4,5,6], $(32 \times 32 \times 24) / (512 \times 512 \times 3) = 0,03125$ bpp dans le cas de l'article présenté dans [7], et $(128 \times 128 \times 24) / (512 \times 512 \times 3) = 0,5$ bpp pour le cas de l'article présenté dans [8] .

Tableau 4.9 : La capacité d'intégration de diverses méthodes de tatouages numériques.

Méthodes	Taille de la marque en bits	Image hôte en pixel	Capacité d'intégration en bit/pixel
[4]	$256 \times 256 \times 8$	$512 \times 512 \times 3$	0,6667 bpp
[5]	$256 \times 256 \times 8$	$512 \times 512 \times 3$	0,6667 bpp
[6]	$256 \times 256 \times 8$	$512 \times 512 \times 3$	0,6667 bpp
[7]	$32 \times 32 \times 24$	$512 \times 512 \times 3$	0.03125 bpp
[8]	$128 \times 128 \times 24$	$512 \times 512 \times 3$	0.5 bpp
[9]	$512 \times 512 \times 24$	$512 \times 512 \times 3$	8 bpp
proposée	$512 \times 512 \times 24$	$512 \times 512 \times 3$	8 bpp

4.5. Conclusion

La technologie de tatouage numérique requiert un équilibre entre imperceptibilité, robustesse et capacité d'insertion, sans négliger le facteur de sécurité. Dans ce travail, nous avons cherché à obtenir ces propriétés en proposant une configuration de tatouage numérique semi-aveugle optimisée pour les images couleur. La marque utilisée est une image couleur de même dimensions que l'image couleur hôte, de taille 512×512 pixels et de 24 bits/pixel, ce qui présente l'avantage d'une capacité d'intégration élevée.

La technique proposée repose sur la décomposition de Hessenberg (HD) et la décomposition en valeurs singulières (SVD) dans le domaine de la transformée en ondelettes discrètes (DWT), car le tatouage numérique dans ce domaine offre une grande robustesse. La HD nous a permis d'augmenter significativement le facteur d'imperceptibilité et de robustesse. En particulier, nous avons utilisé l'algorithme de colonie d'abeilles artificielles (ABC) pour trouver les meilleurs facteurs d'insertion, ce qui nous a permis de trouver le juste équilibre entre imperceptibilité et robustesse. Pour renforcer la sécurité, l'image de la marque a été brouillée à l'aide de la transformée d'Arnold. Les résultats ont montré que le système de tatouage proposé était hautement imperceptible et offre une capacité d'intégration élevée. Sa résistance aux manipulations courantes de traitement d'images, telles que le filtrage, ajout de bruit, et la compression JPEG, les attaques géométriques telles que la rotation, mise à l'échelle, recadrage et découpe et diverses combinaisons d'attaques telles que l'ajout de bruit et la rotation, le filtrage et la découpe, le filtrage et la translation ou la compression JPEG et la rotation, a également été testée.

De plus, une évaluation comparative avec les dernières techniques avancées de tatouage d'images a démontré sa supériorité en termes d'imperceptibilité, de robustesse et de capacité d'insertion.

Conclusion générale

1. Conclusion

Dans le cadre de la thèse de doctorat, qui traite le sujet de la sécurisation des fichiers multimédia par tatouage numérique, nous avons fixé un objectif majeur de développer une méthode robuste de tatouage numérique incorporant une marque c'est une image en couleur dans une image en couleur hôte, dans laquelle l'image hôte et la marque sont toutes les deux de mêmes dimensions. Cela augmente la capacité d'intégration des données dans l'image hôte.

Après avoir présenté l'état de l'art sur le tatouage numérique des images, nous avons suggéré une classification des diverses techniques de tatouage d'images que l'on peut trouver dans les publications. Ensuite on a présenté en détail l'algorithme d'optimisation par colonie d'abeilles artificielles, dans le but de l'exploiter pour trouver les facteurs d'insertion optimaux, dans le cas des méthodes de tatouage numérique des images fixes afin d'obtenir une grande imperceptibilité de la qualité de l'image tatouée et une robustesse maximale de la marque extraite.

Par la suite, nous avons présenté notre première contribution qui consiste en le développement d'une nouvelle technique de tatouage numérique des images couleur robuste et sécurisée, qui intègre une marque qui est une image couleur dans une image couleur hôte, toutes les deux de la même taille, en offrant une meilleure imperceptibilité, une capacité d'intégration élevée et surtout une grande robustesse.

Le schéma suggéré tire parti des caractéristiques avantageuses de chaque transformée utilisée, à savoir la DWT, la décomposition de Hessenberg (HD) et la SVD pour atteindre un meilleur compromis entre imperceptibilité, robustesse et capacité. Les résultats expérimentaux démontrent que cette technique possède à la fois une bonne imperceptibilité, une grande robustesse face aux attaques géométriques, non géométriques et aux attaques combinatoires (géométriques et non géométriques simultanément). En outre, cette méthode assure un processus d'extraction sécurisé (la transformée d'Arnold avec plusieurs itérations comme clé de sécurité est utilisée pour brouiller la marque. Dans le schéma proposé, si la clé secrète utilisée lors du brouillage est inconnue, personne ne peut récupérer l'image secrète du tatouage), ce qui démontre son efficacité pour le cas des applications de la protection des droits d'auteur et l'identification de la propriété.

Toutefois, le principal défi de cette méthode réside dans la recherche du facteur d'insertion adéquat optimal pour chaque image hôte. En effet, dans cette méthode, le facteur d'insertion est choisi manuellement après plusieurs essais.

Ainsi, en second apport, nous avons suggéré un algorithme de sélection automatique des facteurs d'insertion optimaux à l'aide de l'algorithme d'optimisation par colonie d'abeilles artificielles (ABC). Les résultats de l'expérimentation ont démontré une amélioration des performances de la méthode DWT-HD-SVD optimisée, en termes d'imperceptibilité et de robustesse. Aussi, une comparaison avec les techniques récentes de tatouage d'images en niveaux de gris et en couleur a mis en évidence son avantage en termes d'invisibilité, de résistance aux attaques et de capacité d'intégration.

2. Perspectives

Lors de la décennie écoulée, les modèles tridimensionnels (3D) ont suscité un intérêt croissant dans divers domaines d'applications tels que les jeux vidéo, le domaine médical et l'industrie cinématographique en 3D. Il est donc primordial de protéger ces modèles contre toute copie, distribution et modification non autorisées. Pour notre contribution nous envisagerons l'extension de cette contribution, au tatouage des images 3D.

Bibliographie

Introduction générale

- [1] K. J. Giri and R. Bashir, " A block based watermarking approach for color images using discrete wavelet transformation," *International Journal of Information Technology*. 2018.
- [2] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan, and N. N. Xiong, "A robust watermarking scheme in YCbCr color space based on channel coding," *IEEE Access*, vol. 7, pp. 25026-25036, 2019.
- [3] P. Vaidya S. and C. Mouli P. V. S. S. R., " A robust semi-blind watermarking for color images based on multiple decompositions," *Multimedia Tools Appl.*, vol. 76, no. 24, pp. 25623-25656, Dec. 2017.
- [4] V. M. Potdar, S. Han and E.Chang, " A survey of digital image watermarking techniques, " *INDIN '05.2005 3rd IEEE International Conference on Industrial Informatics,2005*.pp.709 - 716, Aug, 2005, doi: 10.1109 / INDIN. 2005. 1560462. *Applications*, vol. 41, no.17, pp.7858-7867,Dec.2014, <https://doi.org/10.1016/j.eswa.2014.06.011>.
- [5] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan and N. N. Xiong, "A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding," *IEEE Access*, vol. 7, pp. 25026-25036, Jan, 2019, doi: 10.1109/ACCESS.2019.2896304.
- [6] P. Vaidya S. and C. Mouli P. V. S. S. R., " A robust semi-blind watermarking for color images based on multiple decompositions," *Multimedia Tools and Applications*, vol. 76, no. 24, pp. 25623-25656, Dec. 2017,<https://doi.org/10.1007/s11042-017-4355-0>.
- [7] D. R. Denslin Brabin, S. Bojjagani and D.R. Denslin Braja, " A Visible Watermarking Scheme for JPEG Images Based on Modification of Frequency Coefficients," *Automatic Control and Computer Sciences*,vol.55, pp. 444–453, Nov.2021, <https://doi.org/10.3103/S0146411621050023>.
- [8] A. K. Singh, M. Dave, and A. Mohan, " Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8381-8401, Jul. 2016, <https://doi.org/10.1007/s11042-015-2754-7>.
- [9] N. Nikolaidis and I. Pitas," Robust image watermarking in the spatial domain, " *Signal Processing*, vol. 66, no. 3, pp. 385-403,May ,1998, [https://doi.org/10.1016/S0165-1684\(98\)00017-6](https://doi.org/10.1016/S0165-1684(98)00017-6).
- [10] S. W. Byun, H. -S. Son and S. -P. Lee, " Fast and Robust Watermarking Method Based on DCT Specific Location,"*IEEE Access*, vol.7, pp. 100706-100718, 2019, <https://ieeexplore.ieee.org/document/8772033>.
- [11] V. Solachidis and L. Pitas, " Circularly symmetric watermark embedding in 2-D DFT domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753, Nov., 2001, doi: 10.1109/83.967401.

-
- [12] S. Roy and A. Pal, "A hybrid domain color image watermarking based on DWT-SVD," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 2, pp. 201-217, July, 2019, <https://doi.org/10.1007/s40998-018-0109-x>.
- [13] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, March, 2002, doi: 10.1109/6046.985560.
- [14] Q. Su, G. Wang, G. Lv, X. Zhang, G. Deng and B. Chen, "A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition," *Multimedia Tools and Applications*, vol. 76, pp. 8781-8801, Apr, 2017, <https://doi.org/10.1007/s11042-016-3522-z>.
- [15] H. Tao, L. Chongmin, J. Mohamad Zain and A. Abdalla, "A Robust Image Watermarking Theories and Techniques: A Review," *Journal of Applied Research and Technology*, vol. 12, no. 1, Feb 1, 2014, [https://doi.org/10.1016/S1665-6423\(14\)71612-8](https://doi.org/10.1016/S1665-6423(14)71612-8).
- [16] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26845-26879, Oct. 2018, <https://doi.org/10.1007/s11042-018-5891-y>.
- [17] Y. Tan, J. Qin, X. Xiang, W. Ma, W. Pan and N. N. Xiong, "A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding," in *IEEE Access*, vol. 7, pp. 25026-25036, 2019, doi: 10.1109/ACCESS.2019.2896304.
- [18] M. Ali, C.W. Ahn and P. Siarry, "Differential evolution algorithm for the selection of optimal scaling factors in image watermarking," *Engineering Applications of Artificial Intelligence*, vol. 31, no. 31, pp. 1526, May, 2014, <https://doi.org/10.1016/j.engappai.2013.07.009>.
- [19] B. Jagadeesh, S. S. Kumar and K. R. Rajeswari, "Image Watermarking Scheme Using Singular Value Decomposition, Quantization and Genetic Algorithm," *2010 International Conference on Signal Acquisition and Processing*, 2010, pp. 120-124, doi : 10.1109/ ICSAP. 2010.71.
- [20] A. Bassel, M. J. Nordin, and M. B. Abdulkareem, "An invisible image watermarking based on modified particle swarm optimization (PSO) algorithm," *International Journal of Security and Its Applications*, vol. 12, no. 2, pp. 1-8, Mar. 2018, <http://dx.doi.org/10.14257/ijisia.2018.12.2.01>.
- [21] M. Gupta, G. Parmar, R. Gupta, and M. Saraswat, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *International Journal of Computational Intelligence Systems*, vol. 8, no. 2, pp. 364-380, Mar. 2015, <https://doi.org/10.1080/18756891.2015.1001958>.
- [22] D. Karaboga, B. Akay, A comparative study of Artificial Bee Colony algorithm, *Appl. Math. Comput.* 214 (2009) 108-132.

Chapitre 1 : Etat de l'art sur le tatouage numérique

- [1] A.Moez,M.S.Bouhlef and L.Kamoun," Nouvelle technique de crypto-compression pour la sécurisation de la transmission es images médicales",Sciences Electronique, ” Technologies de l'information et des Télécommunications ,M.S.Bouhlef,B.Solaiman et L.Kamoun ISBN 9973-41-85-6,Mar.2003.
- [2] C.Chang.M.S.Hwang and T-S Chen." A new encryption algorithm for image cryptosystems," *The Journal of Systems and Software*,Vol.58 .pp.83-91,2001.
- [3] J.C.Borie," Sécurisation d'images par cryptage :application aux images méicales," thèse de doctorat, université de Nimes ,2004.
- [4] L. Besson, " Conception, analyse et implémentation d'algorithmes de chiffrement symétrique sur FPGA," thèse de doctorat,université Paris-Saclay , Aug. 12, 2021.
- [5] Chandreyee Maiti, Debanjana Bakshi, Ipsita Zamider, Pinky Gorai, and Dakshina Ranjan Kisku,“ Data Hiding in Images Using Some Efficient Steganography Techniques,” *Communications in computer and information science*, pp. 195–203, Jan. 2011, doi: https://doi.org/10.1007/978-3-642-27183-0_21.
- [6] D. Kundur and D. Hatzinakos, “ Digital watermarking using multiresolution wavelet decomposition,” *International Conference on Acoustics, Speech, and Signal Processing*, volume 5, pp, 2969–2972.May 1998, doi: <https://doi.org/10.1109/icassp.1998.678149>.
- [7] M. Praveen Kumar and C. S. K. Shastri, “A Review on Watermarking Techniques of Digital Image,” *Lecture Notes in Electrical Engineering*, pp. 155–162, 2024, doi: https://doi.org/10.1007/978-981-97-4657-6_12.
- [8] F. Hartung and M. Kutter, " Multimedia watermarking techniques," in *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079-1107, Jul. 1999, doi: 10.1109/5.771066.
- [9] M. Kutter and Fabien, " Fair benchmark for image watermarking systems," *Proceedings of SPIE*, Apr. 1999, doi: <https://doi.org/10.1117/12.344672>.
- [10] Khaled Loukhaoukha," *Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multiobjective*," thèse de Doctorat , Université Laval,2010.
- [11] F. HARTUNG, J.K. SU et B. GIROD," Spread spectrum watermarking : malicious attacks and counter attacks," In SPIE Conference on Security and Watermarkinci of Multimedia Contents, vol. 3657, pp. 147-158, San Jose, États-Unis, jan.1999.
- [12] S. Katzenbeisser, F. Petitcolas," *Information Hiding Techniques for Steganography and Digital Watermarking*," Artech House, 2000.
- [13] M. A. Dorairangaswamy, " Protecting digital-image copyrights: A robust and blind watermarking scheme," *2009 First International Conference on Networked Digital Technologies*, Ostrava, Czech Republic, pp. 423-428, 2009, doi: 10.1109/NDT.2009.5272151.

-
- [14] R. Sinhal and I. A. Ansari, "A blind and secured image watermarking method using DWT-DCT techniques," *2018 Conference on Information and Communication Technology (CICT)*, Jabalpur, India, pp. 1-6, 2018, doi: 10.1109/INFOCOMTECH.2018.8722400.
- [15] D. K. Thind and S. Jindal, "A Semi Blind DWT-SVD Video Watermarking," *Procedia Computer Science*, vol. 46, pp.1661–1667, 2015, doi: <https://doi.org/10.1016/j.procs.2015.02.104>.
- [16] R. Kaur and S. Jindal, "Semi-blind Image Watermarking Using High Frequency Band Based on DWT-SVD," *6th International Conference on Emerging Trends in Engineering and Technology*, Nagpur, India, pp. 19-24, 2013, doi: 10.1109/ICETET.2013.5.
- [17] R. K. Arya, S. Singh and R. Saharan, "A secure non-blind block based digital image watermarking technique using DWT and DCT," *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Kochi, India, pp. 2042-2048, 2015, doi: 10.1109/ICACCI.2015.7275917.
- [18] N. V. Dharwadkar, B. B. Amberker and A. Gorai, "Non-blind watermarking scheme for color images in RGB space using DWT-SVD," *International Conference on Communications and Signal Processing*, Kerala, India, pp. 489-493, 2011, doi: 10.1109/ICCSP.2011.5739368.
- [20] J. Fridrich, "Applications of data hiding in digital images," *ISSPA . Proceedings of the Fifth International Symposium on Signal Processing and its Applications*, Brisbane, QLD, Australia, Nov. 1999, doi: 10.1109/ISSPA.1999.818099.
- [21] R. Wazirali, R. Ahmad, A. Al-Amayreh, M. Al-Madi, and A. Khalifeh, "Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview," *Electronics*, vol.10,no.14,p. 1744, Jul. 2021, doi: <https://doi.org/10.3390/electronics10141744>.
- [22] F. M. Boland, J. J. K. O'Ruanaidh and C. Dautzenberg, "Watermarking digital images for copyright protection," *Fifth International Conference on Image Processing and its Applications*, 1995., Edinburgh, pp. 326-330, 1995, doi: 10.1049/cp:19950674.
- [23] P. Bandyopadhyay, S. Das, S. Paul, A. Chaudhuri and M. Banerjee, "A Dynamic Watermarking Scheme for Color Image Authentication," *International Conference on Advances in Recent Technologies in Communication and Computing*, Kottayam, India, pp. 314-318, doi: 10.1109/ARTCom.2009.94.
- [24] J. Abraham and V. Paul, "Imperceptible Image Indexing Using Digital Watermarking," *Communications in computer and information science*, pp. 110–116, Jan..2012, doi: https://doi.org/10.1007/978-3-642-34135-9_11.
- [25] I. J. Cox, J. Kilian, Frank Thomson Leighton, and T. G. Shamoan, "A secure, robust watermark for multimedia," *Lecture Notes in Computer Science*, pp. 185–206, May. 1996, doi: https://doi.org/10.1007/3-540-61996-8_41.
- [26] Dharwadkar, N. V. and B. Amberker, "Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution," *Journal of Computing - Vol.1, Issue 1, Dec. 2009*.

-
- [27] B. Chen and G. W. Wornell, " Quantization index modulation : a class of provably good methods for digital watermarking and information embedding,"*IEEE Transaction on information theory*, Vol. 47, No. 4, pp. 1423–1443, May. 2001.
- [28] I. Nouioua, " Développement et Implémentation d'Algorithmes de Tatouage Numérique des Données Multimédia ," thèse de doctorat, département d'électronique, Université Ferhat Abbas, Sétif, 2019.
- [29] Der-Chyuan Lou and Chia-Hung Sung, " Robust image watermarking based on hybrid transformation," *IEEE 37th Annual International Carnahan Conference on Security Technology, Proceedings.*, Taipei, Taiwan, pp.394-399,2003,doi: 10.1109/CCST.2003.1297592.
- [30] SHI, Hongqin, LV, Fangliang, et CAO, Yiqin," A Blind Watermarking Technique for Color Image based on SVD with Circulation," *J. Softw.*, vol. 9, no 7, pp. 1749-1756, 2014.
- [31] G. Sun and Y. Yu, " DWT Based Watermarking Algorithm of Color Images," *2nd IEEE Conference on Industrial Electronics and Applications*, Harbin, China, pp. 1823-1826, 2007 doi: 10.1109/ICIEA.2007.4318725.
- [32] G. S. Kalra, R. Talwar, and Harsh Sadawarti, "Adaptive digital image watermarking for color images in frequency domain," vol. 74, no. 17, pp. 6849–6869, Mar. 2014, doi: <https://doi.org/10.1007/s11042-014-1932-3>.
- [33] Youssra Lakrissi, Abderrahim Saaidi, and Abdelouahed Essahlaoui, " Novel dynamic color image watermarking based on DWT-SVD and the human visual system,"*Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13531–13555, Jul. 2017, doi: <https://doi.org/10.1007/s11042-017-4974-5>.
- [34] C.-H. CHOU et K.-C Liu ,"Performance analysis of color image watermarking schemes using perceptually redundant signal spaces," *Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*,Pasadena, États-Unis, pp. 651-654, Déc .2006.
- [35]K. Tanaka, Y. Nakamura and K. Matsui, " Embedding secret information into a dithered multi-level image," *IEEE Conference on Military Communications*, Monterey, CA, USA, pp. 216-220 ,vol.1, 1990, doi: 10.1109/MILCOM.1990.117416.
- [36] Emami, M. S., K. Omar, S. Sahran and S. N. H. S. Abdullah, " Spatial Domain Approaches for Real-Time Ownership Identification, " *JAIT-Journal of Advances in Information Technology*, Vol.5, No. 1, Feb. 2014.
- [37] W. Bender, D. Gruhl, N. Morimoto and A. Lu, " Techniques for data hiding," in *IBM Systems Journal*, vol. 35, no. 3, pp. 313-336, 1996, doi: 10.1147/sj.353.0313.
- [38] I.-K. Yeo and H. J. Kim, " Generalized patchwork algorithm for image watermarking," *Multimedia Systems*,vol.9, no. 3, pp. 261–265, Sep. 2003, doi: <https://doi.org/10.1007/s00530-003-0097-0>.
- [39] Chiou-Ting Hsu and Ja-Ling Wu, " Hidden digital watermarks in images," in *IEEE Transactions on Image Processing*,vol.8, no. 1, pp. 58-68, Jan. 1999, doi: 10.1109/83.736686.

-
- [40] I. J. Cox, J. Kilian, Frank Thomson Leighton, and T. G. Shamoan, "A secure, robust watermark for multimedia," *Lecture Notes in Computer Science*, pp. 185–206, May. 1996, doi: https://doi.org/10.1007/3-540-61996-8_41.
- [41] Chion-Ting Hsu and Ja-Ling Wu, "Multiresolution watermarking for digital images," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 8, pp. 1097–1101, 1998, doi: <https://doi.org/10.1109/82.718818>.
- [42] X.-G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," *IEEE Xplore*, vol. 1, pp. 548-551, Oct. 01, 1997.
- [43] Kim W. G., Lee J. C., and Lee W. D., "An Image Watermarking Scheme with Hidden Signature," *IEEE Proceeding of the International Conference on Image Processing*, Japan, pp. 206-210, Oct. 1999.
- [44] Solachidis V. and Pitas I., "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," in *Proceedings of the International Conference on Acoustics, Speech and Signal Processing, IEEE Signal Processing Society*, Phoenix, Arizona, USA, vol. 6, pp. 1653-1656, Mar. 1999, doi: <https://doi.org/10.1109/icassp.1999.757589>.
- [45] D. Vaishnavi and T. S. Subashini, "Robust and Invisible Image Watermarking in RGB Color Space Using SVD," *Procedia Computer Science*, vol. 46, pp. 1770–1777, 2015, doi: <https://doi.org/10.1016/j.procs.2015.02.130>.
- [46] Y.-T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique," *Pattern Recognition*, vol. 37, no. 12, pp. 2349–2359, Dec. 2004, doi: <https://doi.org/10.1016/j.patcog.2004.05.003>.
- [47] P.-C. Su and C.-C.J. Kuo, "Image watermarking scheme to resist generalized geometrical transformations," *Proceedings of SPIE, the International Society for Optical Engineering/Proceedings of SPIE*, vol. 4209, pp. 354–365, Mar. 2001, doi: <https://doi.org/10.1117/12.420838>.
- [48] F. Y. Shih and S. Y. T. Wu, "Combinational image watermarking in the spatial and frequency domains," *Pattern Recognition*, vol. 36, no. 4, pp. 969 – 975, Apr. 2003, doi: [https://doi.org/10.1016/s0031-3203\(02\)00122-x](https://doi.org/10.1016/s0031-3203(02)00122-x).
- [49] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," in *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, Mar. 2002, doi: [10.1109/6046.985560](https://doi.org/10.1109/6046.985560).
- [50] R. Rykaczewski, "Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership"," in *IEEE Transactions on Multimedia*, vol. 9, no. 2, pp. 421-423, Feb. 2007, doi: [10.1109/TMM.2006.886297](https://doi.org/10.1109/TMM.2006.886297).
- [51] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," *Signal Processing*, vol. 88, no. 9, pp. 2158 –2180, Sep. 2008, doi: <https://doi.org/10.1016/j.sigpro.2008.02.015>.
- [52] F. Huang and Z.-H. Guan, "A hybrid SVD-DCT watermarking method based on LPSNR," *Pattern Recognition Letters*, vol. 25, no. 15, pp. 1769 –1775, Nov. 2004, doi: <https://doi.org/10.1016/j.patrec.2004.07.003>.

-
- [53] W. Lu, W. Sun, and H. Lu, "Robust watermarking based on DWT and nonnegative matrix factorization," *Computers & Electrical Engineering*, vol. 35, no. 1, pp. 183–188, Jan. 2009, doi: <https://doi.org/10.1016/j.compeleceng.2008.09.004>.
- [54] E.E. ABDALLAH, A. Ben HAMZA et P. BHATTACHARYA," Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms," *Journal of Electronic Imaging*,vol.13.no. 3.pp.1-9, Jul. 2007.
- [55] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible dual watermarking using error correcting codes for application in telemedicine," *International Journal of Electronic Security and Digital Forensics*, vol. 6, no. 4,pp. 285-305, 2014, doi: <https://doi.org/10.1504/ijesdf.2014.065739>.
- [56] D. Xiao, Q. Tang, A. Zhao and M. Li, "Robust Watermarking Scheme in Encrypted Domain Based on Integer Lifting Wavelet Transform and Compressed Sensing," *ICASSP IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Rhodes Island, Greece, pp. 1-5, 2023, doi: 10.1109/ICASSP49357.2023.10095228.
- [57] Yuning Hua, Bo Wu and Gang Wu, "A color image fragile watermarking algorithm based on DWT-DCT," *2010 Chinese Control and Decision Conference*, Xuzhou, pp. 2840-2845, 2010, doi: 10.1109/CCDC.2010.5498711.
- [58] Y. Du and T. Zhang, "A Reversible and Fragile Watermarking Algorithm Based on DCT," *International Conference on Artificial Intelligence and Computational Intelligence*, Shanghai, China, pp. 301-304, 2009, doi: 10.1109/AICI.2009.30.
- [59] E.T.Lin, C. I. Podilchuk, and E.J. Delp, "Detection of Image Alterations Using Semi-Fragile Watermarks," in proceedings of Security and Watermarking of Multimedia Contents II (SPIE), May .9,2000.
- [60] Tali Dekel, M. Rubinstein, C. Liu, and W. T. Freeman, "On the Effectiveness of Visible Watermarks," pp. 6864–6872, Jul. 2017, doi: <https://doi.org/10.1109/cvpr.2017.726>.
- [61] Z. Zhang, Q . Sun, and W.C. Wong," A Novel Lossy-to-lossless Watermarking Scheme for JPEG2000 Images," In *International Conference on Image Processing, ICIP'04*, vol. 1, pp. 573–576, 2004.
- [62] LI, C.-T. "Reversible watermarking scheme with image-independent embedding capacity," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 152, no 6, p. 779-786, 2005.
- [63] Zhou Wang and A. C. Bovik, "Mean squared error: Love it or leave it? A new look at Signal Fidelity Measures," *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 98–117, Jan. 2009, doi: <https://doi.org/10.1109/msp.2008.930649>.
- [64] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, Apr.2004, doi: 10.1109/TIP.2003.819861.

[65] Q. Su, Y. Niu, X. Liu, and Y. Zhu, "Embedding color watermarks in color images based on Schur decomposition," *Optics Communications*, vol. 285, no. 7, pp. 1792–1802, Apr. 2012, <https://doi.org/10.1016/j.optcom.2011.12.065>.

[66] T. Q. Nguyen, D. M. Duong, and D. M. Duong, " Robust and high capacity watermarking for image based on DWT-SVD," *IEEE RIVF*, Can Tho, Vietnam, pp. 83-88, 2015, doi: 10.1109/RIVF.2015.7049879.

[67] C-C. CHANG, C-C. LIN et Y.-S. Hu , "An SVD oriented watermark embedding scheme with high qualities for the restored images", *International Journal of Innovative Computing, Information & Control*, vol.3,no.3,pp.609-620, Jun. 2007.

Chapitre 2 : Tatouage numérique d'images dans le domaine des transformées

[1] L. M. Cheng, L. L. Cheng, C. K. Chan and K. W. Ng, " Digital watermarking based on frequency random position insertion," *ICARCV 2004 8th Control, Automation, Robotics and Vision Conference, 2004.*, Kunming, China, 2004, pp.977-982, Vol.2, doi:10.1109/ICARCV .2004.1468975.

[2] M. Begum and M. S. Uddin, " Digital Image Watermarking Techniques: A Review," *Information*, vol. 11, no. 2, p. 110, Feb. 2020, doi: <https://doi.org/10.3390/info11020110>.

[3] P. T. Nha, T. M. Thanh and N. -T. Huynh, "An improved QR decomposition for color image watermarking," *International Conference on Knowledge and Systems Engineering (KSE)*, Ho Chi Minh City, Vietnam, pp. 56-60, 2018, doi: 10.1109/KSE.2018.8573423.

[5] R. Rabia, " Tatouage robuste d'images imprimées," *Thèse de doctorat*, <https://theses.fr/2015ORLE2068> , Université d'Orléans , France, 2015.

[6] A.B. Watson, " Image Compression Using the Discrete Cosine Transform ", *Mathematica Journal*, pp. 81-88, 1994.

[7] X. Kang, Y. Chen, F. Zhao, and G. Lin, " Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain," *Soft Computing*, vol.24,no.14,pp.10561–10584,Nov. 2019, doi: <https://doi.org/10.1007/s00500-019-04563-6>.

[8] W.H Chen, C.H. Smith, and S.C. Fralick, " A fast computational algorithm for the discrete cosine transform," *IEEE Trans. Commun.*, vol. COM-25, pp.1004-1009. 1977.

[9] D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13001–13024, Jul. 2016, doi: <https://doi.org/10.1007/s11042-016-3706-6>.

[10] M. SAHIR, " Compression des images numériques par la technique des ondelettes ", *Thèse de magister*, université Ferhat Abbas-Setif .Algérie. 2011.

[11] S.G. Mallat, " A theory for multi resolution signal decomposition: The wavelet representation," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol.11 ,no.7,pp. 674–693,Jul.1989.

-
- [12] A. Kumari, Harshek Madhukar, S. A. Haider, A. Majumder, and S. Kundu, " Digital Watermarking Strategies for Healthcare Data Security: A Comprehensive Review and Analysis," May 21, 2024.
- [13] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection," *Expert Systems with Applications: An International Journal*, vol.39,no.1,pp.673–689,Jan.2012,<https://doi.org/10.1016/j.eswa.2011.07.059>.
- [14] R. Liu and T. Tan," An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002, doi: <https://doi.org/10.1109/6046.985560>.
- [15] D. V. S. Chandra, " Digital image watermarking using singular value decomposition," in *45th Midwest Symposium on Circuits and Systems. MWSCAS-2002.*, vol. 3, pp. 1264–267, 2002. doi: <https://doi.org/10.1109/mwscas.2002.1187023>.
- [16]Y. Xing and J. Tan, "A Color Watermarking Scheme Based on Block-SVD and Arnold Transformation," *Second Workshop on Digital Media and its Application in Museum & Heritages (DMAMH 2007)*, pp. 3–8, Dec. 2007, doi: <https://doi.org/10.1109/dmamh.2007.15>.
- [17] Q. Su," Novel blind colour image watermarking technique using Hessenberg decomposition," *IET Image Processing*, vol. 10, no. 11, pp.817–829, Nov. 2016, <https://doi.org/10.1049/iet-ipr.2016.0048>.
- [18] Q. Su and B. Chen, "A novel blind color image watermarking using upper Hessenberg matrix," *Aeu-international Journal of Electronics and Communications*, vol. 78, pp. 64–71, Aug. 2017, doi: <https://doi.org/10.1016/j.aeue.2017.05.025>.
- [19] H. Seddik, M. Sayadi, F. Fnaiech et M. Cheriet," Image Watermarking Based on the Hessenberg Transform" *The International Journal of Image andGraphics*, Volume: 9, Issue: 3, pp .411- 433,Jul. 2009.
- [20] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm,"*First International Conference on Information Science and Engineering*,Nanjing, China, pp.1164–1167, 2009, <https://doi.org/10.1109/ICISE.2009.347>.
- [21] A. M. Cheema, S. M. Adnan, and Z. Mehmood, "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," *IEEE Access*, vol.8, pp. 169525–169547, 2020, <https://doi.org/10.1109/ACCESS.2020.3024181>.

[22] S. AlZubi, N. Islam, and M. Abbod, " Multiresolution Analysis Using Wavelet, Ridgelet, and Curvelet Transforms for Medical Image Segmentation," *Int. Journal of Biomedical Imaging*, vol. 2011, pp. 1–18, 2011, doi: <https://doi.org/10.1155/2011/136034>.

[23] L. Zhang and D. Wei," Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization," *Multimedia Tools Appl.*,vol. 78, no. 19, pp. 28003_28023, Oct. 2019.

[24] R. Thanki and S. Borra, "A color image steganography in hybrid FRT–DWT domain,"*Journal of Information Security and Applications*, vol. 40, pp. 92–102, Jun. 2018, doi: <https://doi.org/10.1016/j.jisa.2018.03.004>.

[25] Y. Dong, R. Yan, and C. Yin, " An adaptive robust watermarking scheme based on chaotic mapping," *Scientific Reports*, vol. 14, no.1,Oct. 2024,Art. no. 24735, <https://doi.org/10.1038/s41598-024-76101-w>.

Chapitre 3 : Utilisation de l’algorithme ABC en tatouage numérique

[1] Beatriz Flamia Azevedo, A. Maria, and A. I. Pereira, “ Hybrid approaches to optimization and machine learning methods: a systematic literature review,” *Machine Learning*, Jan. 2024, doi: <https://doi.org/10.1007/s10994-023-06467-x>.

[2] M. Cavazzuti, “ Deterministic Optimization,” *Springer eBooks*, pp. 77–102, Sep. 2012, doi: https://doi.org/10.1007/978-3-642-31187-1_4.

[3] A. E. Dor, “ Perfectionnement des algorithmes d’optimisation par essaim particulière : applications en segmentation d’images et en électronique,” *Hal.science*, Dec. 2012, doi: <https://theses.hal.science/tel-00788961>.

[4] S. M. Almufti, Awaz Ahmad Shaban, Rasan Ismael Ali, and J. A. Dela, “ Overview of Metaheuristic Algorithms,” *Polaris Global Journal of Scholarly Research and Trends*, vol. 2, no. 2, pp. 10–32, Apr. 2023, doi: <https://doi.org/10.58429/pgjsrt.v2n2a144>.

[5] V. Tomar, M. Bansal, and P. Singh, “ Metaheuristic Algorithms for Optimization : A Brief Review,” *Engineering Proceedings*, vol. 59, no. 1, p. 238, 2024, doi: <https://doi.org/10.3390/engproc2023059238>.

[6] S. M. Almufti, Awaz Ahmad Shaban, Rasan Ismael Ali, and J. A. Dela, “ Overview of Metaheuristic Algorithms,” *Polaris Global Journal of Scholarly Research and Trends*, vol. 2, no. 2, pp. 10–32, Apr. 2023, doi: <https://doi.org/10.58429/pgjsrt.v2n2a144>.

[7] Bansal, J., Singh, P., & Nikhil, R. “ Evolutionary and swarm intelligence algorithms ,” *Studies In Computational intelligence*. Springer, 2018.

[5] V. Tomar, M. Bansal, and P. Singh, “ Metaheuristic Algorithms for Optimization: A Brief Review,” *Engineering Proceedings*, vol.59, no. 1, p. 238, 2024, doi: <https://doi.org/10.3390/engproc2023059238>.

[6] S. M. Almufti, Awaz Ahmad Shaban, Rasan Ismael Ali, and J. A. Dela, "Overview of Metaheuristic Algorithms," *Polaris Global Journal of Scholarly Research and Trends*, vol. 2, no. 2, pp. 10–32, Apr. 2023, doi: <https://doi.org/10.58429/pgjsrt.v2n2a144>.

[7] Bansal, J., Singh, P., & Nikhil, R. Evolutionary and swarm intelligence algorithms. Studies In *Computational intelligence*. Jagdish Chand Bansal, Pramod Kumar Singh, and N. R. Pal, "*Evolutionary and Swarm Intelligence Algorithms*". Springer, 2018.

[8] J. KENNEDY et R. EBERHART : Particle swarm optimization. In IEEE International Conference on Neural Networks, vol. 4, p. 1942-1948, Perth, Australie, octobre-décembre 1995.

[9] M. DORIGO, V. MANIEZZO et A. COLORNI : The Ant System : Optimization by a colony of cooperating agents. IEEE Transactions on Systems, Man, and Cybernetics-Part B, 26(1):29-41, février 1996.

[10] Karaboga, D., "An Idea Based on Honey Bee Swarm for Numerical Optimization," Technical Report-TR06, Department of Computer Engineering, Engineering Faculty, Erciyes University. (2005).

[11] A. Yurtkuran and E. Emel, " An Enhanced Artificial Bee Colony Algorithm with Solution Acceptance Rule and Probabilistic Multisearch," *Computational Intelligence and Neuroscience*, vol. 2016, pp. 1–13, 2016, doi: <https://doi.org/10.1155/2016/8085953>.

[12] Y. Yan, Y. Zhang, and F. Gao, " Dynamic artificial bee colony algorithm for multi-parameters optimization of support vector machine-based soft-margin classifier," *EURASIP Journal on Advances in Signal Processing*, vol. 2012, no. 1, Jul. 2012, doi: <https://doi.org/10.1186/1687-6180-2012-160>.

[13] B. Akay and D. Karaboga, " A modified Artificial Bee Colony algorithm for real-parameter optimization," *Information Sciences*, vol. 192, pp. 120–142, Jun. 2012, doi: <https://doi.org/10.1016/j.ins.2010.07.015>.

[14] M. A. Awadallah, M. A. Al-Betar, A. L. Bolaji, E. M. Alsukhni, and H. Al-Zoubi, "Natural selection methods for artificial bee colony with new versions of onlooker bee," *Soft Computing*, vol. 23, no. 15, pp. 6455–6494, Jun. 2018, doi: <https://doi.org/10.1007/s00500-018-3299-2>.

Chapitre 4 : Algorithme développé DWT-HD-SVD et comparaison des résultats

[1] T. Huang, J. Xu, Y. Yang, and B. Han, " Robust Zero-Watermarking Algorithm for Medical Images Using Double-Tree Complex Wavelet Transform and Hessenberg Decomposition," *Mathematics*, vol.10,no.7,p.1154,Apr.2022,doi:<https://doi.org/10.3390/math10071154>.

[2] SIPI Image Database: <https://sipi.usc.edu/database/database.php?volume=misc>.

[3] Q. Zheng, N. Liu, and F. Wang, " An Adaptive Embedding Strength Watermarking Algorithm Based on Shearlets' Capture Directional Features," *Mathematics*, vol. 8, no. 8, Aug. 2020, Art. no. 1377, <https://doi.org/10.3390/math8081377>.

-
- [4] Y. Dong, R. Yan, Q. Zhang, and X. Wu, " A Hybrid Domain Color Image Watermarking Scheme Based on Hyperchaotic Mapping," *Mathematics*, vol. 12, no. 12, Jun. 2024, Art. no. 1859, <https://doi.org/10.3390/math12121859>.
- [5] Y. Dong, R. Yan, and C. Yin," An adaptive robust watermarking scheme based on chaotic mapping," *Scientific Reports*, vol. 14, no. 1, Oct. 2024,Art. no. 24735, <https://doi.org/10.1038/s41598-024-76101-w>.
- [6] R. Dwivedi and V. K. Srivastava, " IWT based robust and secure color image watermarking using Hessenberg decomposition and SVD,"*Journal of Optics*, Aug. 2024, <https://doi.org/10.1007/s12596-024-02141-0>.
- [7] H. Wang, Z. Yuan, S. Chen, and Q. Su, " Embedding color watermark image to color host image based on 2D-DCT, " *Optik*, vol. 274, Mar. 2023, Art. no. 170585, <https://doi.org/10.1016/j.ijleo.2023.170585>.
- [8] B. Latreche, H. Naimi, and S. Saadi, " A secure and robust color image watermarking method using SVD and GAT in the multiresolution DCHWT domain," *The Journal of Engineering and Exact Sciences*, vol.9, no. 10, pp. 17317–01e, Nov. 2023, <https://doi.org/10.18540/jcecv19iss10pp17317-01e>.
- [9] A. M. Cheema, S. M. Adnan, and Z. Mehmood, " A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," *IEEE Access*, vol. 8, pp. 169525–169547, 2020, <https://doi.org/10.1109/ACCESS.2020.3024181>.
- [10] Z. Yuan, D. Liu, X. Zhang, H. Wang, and Q. Su, " DCT-based color digital image blind watermarking method with variable steps," *Multimedia Tools and Applications*, vol.79, no. 41–42, pp. 30557–30581, Aug. 2020, doi: <https://doi.org/10.1007/s11042-020-09499-w>.

ملخص

في هذه الرسالة، نُقدّم مساهمتين في مجال إضافة العلامات المائية للصور الملونة. في المساهمة الأولى، نقترح تقنية جديدة لإضافة العلامات المائية للصور الملونة، تعتمد على تحليل هيسنبرغ (HD) و SVD في مجال (DWT). يُتيح تضمين علامة ملونة في صورة ملونة رئيسية، كلاهما بنفس الحجم، عدم إدراك أفضل، وقدرة تضمين عالية، ومثانة عالية ضد الهجمات. يُستخدم عامل تضمين للتحكم في التوازن بين عدم إدراك العلامة ومثانتها. يُختار هذا العامل يدويًا لكل صورة ملونة مستخدمة. مع ذلك، لا يؤدي هذا الاختيار بالضرورة إلى الحل الأمثل، ويتطلب وقتًا طويلًا للاختبار. تُظهر النتائج التجريبية أن هذه الطريقة تُقدّم عدم إدراك جيد ومثانة عالية ضد الهجمات الهندسية وغير الهندسية والهجمات التجميعية (الهندسية وغير الهندسية في نفس الوقت). المساهمة الثانية هي تحسين تقنيتنا القائمة على DWT-HD-SVD وذلك من خلال استخدام خوارزمية مستعمرة النحل الاصطناعي (ABC) من جهة، تتيح هذه الخوارزمية تحديد عوامل الإدخال الأمثل للحصول على أفضل أداء من حيث عدم الإدراك والمثانة، ومن جهة أخرى، تسهّل استخدام التقنيه من خلال أتمتة عملية اختيار عامل الإدخال الأمثل لكل صورة اختبار. وقد أظهرت مقارنتها بأحدث تقنيات وضع العلامات المائية على الصور ميزتها من حيث عدم الرؤية ومقاومة الاختراق وسعة التضمين.

الكلمات المفتاحية : علامة مائية صورة ملونة؛ تحلل هيسنبرغ (HD) ؛ تحلل القيمة المفردة (SVD) ؛ تحويل الموجات المنفصلة (DWT)؛ مستعمرة النحل الاصطناعي (ABC).

Abstract

In this thesis, we present two contributions in the field of color image watermarking. In the first contribution, we propose a new color image watermarking technique, based on Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD) in DWT Domain, which embedding a color image watermark into a host color image, both of the same dimension, provides better imperceptibility, high embedding capacity and exhibits high robustness against attacks. An embedding factor is used to control the trade-off between watermark invisibility and robustness. This factor is manually selected for each color image used. However, this selection does not necessarily guarantee the optimal solution and requires a lot of testing time. Experimental results demonstrate that this technique provides high-quality imperceptibility and strong robustness against geometric, non-geometric, and combinatorial attacks (geometric and non-geometric at the same time). The second contribution is an improvement of our technique based on DWT-HD-SVD. By exploiting the Artificial Bee Colony (ABC) algorithm. On the one hand, this algorithm allows finding the optimal insertion factors in order to obtain the best performances in terms of invisibility and robustness and on the other hand, it facilitates the use of the watermarking technique by automating the process of selecting the optimal insertion factor for each test image. A comparison with the most recent image watermarking techniques highlighted its advantage in terms of invisibility, resistance to attacks and embedding capacity.

Keywords: Color image watermark; Hessenberg decomposition (HD); Singular value decomposition (SVD); Discrete wavelet transform (DWT); Artificial bee colony (ABC).

Résumé

Dans cette thèse, nous présentons deux contributions dans le domaine du tatouage d'images couleur. Dans la première contribution, nous proposons une nouvelle technique de tatouage d'images couleur, basée sur la décomposition de Hessenberg (HD) et la SVD dans le domaine des transformées en ondelettes discrètes (DWT), qui intègre une marque qui est une image couleur dans une image couleur hôte, toutes les deux de la même taille, offrant une meilleure imperceptibilité, une capacité d'intégration élevée et présentant une grande robustesse contre les attaques. Un facteur d'insertion est employé pour contrôler le compromis entre l'invisibilité de la marque et sa robustesse. Ce facteur est sélectionné manuellement, pour chaque image couleur utilisée. Toutefois, cette sélection ne garantit pas forcément la solution optimale et exige beaucoup de temps de tests. Les résultats expérimentaux démontrent que cette technique offre une imperceptibilité de qualité ainsi qu'une forte robustesse face aux attaques géométriques, non géométriques et aux attaques combinatoires (géométriques et non géométriques en même temps). La deuxième contribution est une amélioration de notre technique de tatouage basée sur DWT-HD-SVD. En exploitant l'algorithme de la colonie d'abeilles artificielles (ABC). D'une part, cet algorithme permet de trouver les facteurs optimaux d'insertion dans le but d'obtenir les meilleures performances en termes d'invisibilité et de robustesse et, d'autre part, il facilite l'utilisation de la technique de tatouage en automatisant le processus de sélection du facteur d'insertion optimal pour chaque image de test. Une comparaison avec les techniques de tatouage d'images les plus récentes a mis en évidence son avantage en termes d'invisibilité, de résistance aux attaques et de capacité d'intégration.

Mots clés : Marque une image couleur ; Décomposition de Hessenberg (HD) ; Décomposition en valeurs singulières (SVD) ; Transformée en ondelettes discrètes (DWT) ; Colonie d'abeilles artificielles (ABC).