

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



Université Hadj Lakhdar Batna
Faculté de Technologie
Département d'Électronique



THÈSE

Présentée pour l'obtention du diplôme de
DOCTORAT en SCIENCES en Électronique

OPTION

Microélectronique

Par

Mme Samia BELKACEM

Thème

Chaos based image watermarking

Soutenue devant le jury composé de :

Dr. BENATIA Djamel	Prof.	Université Batna	Président
Dr. BOURIDANE Ahmed	Prof.	Université Northumbria	Rapporteur
Dr. DIBI Zohir	Prof.	Université Batna	Co-rapporteur
Dr. FORTAKI Tarek	Prof.	Université Batna	Examineur
Dr. BOUTOUT Farid	Prof.	Université Bordj Bou-Arredj	Examineur
Dr. MESSAI Abderraouf	Prof.	Université Constantine 1	Examineur

Remerciements

Tout d'abord je remercie le Bon Dieu, le tout puissant, de nous avoir donné la santé, le courage, la patience et surtout la raison.

Ce travail a été effectué au laboratoire d'Electronique Avancée de l'université de Batna.

Je tiens à exprimer ma profonde gratitude à monsieur Ahmed BOURIDANE, Professeur à l'université de Northumbria, UK, pour avoir dirigé ce travail, pour ses nombreuses remarques qui ont montré une très vaste connaissance du sujet, pour les conseils scientifiques et les encouragements qu'il m'a prodigués.

J'adresse mes remerciements les plus sincères à mon co-directeur de thèse Professeur Zohir DIBI, Vice Recteur de l'université de Batna, pour son encadrement constant et efficace tout au long de l'élaboration de ce travail de recherche au cours duquel j'ai pu apprécier ses qualités tant humaines que professionnelles. Vous m'avez toujours réservé le meilleur accueil, malgré vos obligations professionnelles.

Je tiens à remercier les membres de jury, à commencer par le Professeur Djamel BENATIA de l'université de Batna, pour l'honneur qu'il m'a fait en présidant le jury de cette thèse. Mes remerciements vont également au Professeur Tarek FORTAKI de l'université de Batna pour avoir accepté de juger ce travail. Au Professeur Farid BOUTOUT du département d'électronique de l'université de Bordj Bou-Arredj, le Professeur Abderraouf MESSAI du département d'Electronique de l'université de Constantine 1 j'exprime ma profonde gratitude pour m'avoir honoré en acceptant de juger ce travail.

Enfin, je remercie tous ceux qui m'ont soutenu, encouragé et donné l'envie de mener à terme ce travail.

Mme. BELKACEM Samia

Résumé

L'objectif de cette thèse était de concevoir des nouvelles approches de tatouage d'images numériques permettant d'obtenir le meilleur compromis entre la robustesse et l'invisibilité. Nous avons proposé des méthodes de tatouage chaotique des images numériques ; les domaines d'insertion adoptés sont le domaine spatial et le domaine transformé tel que la DCT et la DWT.

Les points de faiblesse de l'œil humain ont été exploités pour la conception des masques perceptuels pour la pondération de la marque. Il s'agit de la détermination des zones texturées et la modélisation de l'effet de la luminance. L'utilisation de ces masques dans le domaine spatial et fréquentiel, ont permis l'obtention d'un système robuste aux attaques et en même temps ne dégrade pas la qualité de l'image tatouée.

Dans le domaine DCT, l'insertion de la marque est faite par l'exploitation des masques visuels proposés. L'étude de performance de ces schémas en terme de qualité et de robustesse est effectuée.

Le domaine des ondelettes est également introduit, en vue d'élaboration des systèmes de tatouage chaotique des images numériques par l'utilisation des masques proposés. Nous avons fait appel dans cette thèse à la notion de l'image de référence. Les deux systèmes de détection semi aveugle et non aveugle ont été utilisés pour la détection du filigrane.

Une modélisation des coefficients DCT a été faite par l'utilisation de la distribution GFD . L'évaluation de leur paramètres est basée sur l'utilisation de la méthode des moments ; où les statistiques de l'image est prise en considération pour la conception d'un système de détection. L'étude des performances a permis de mettre en évidence les avantages des approches proposées en termes d'invisibilité et de robustesse face aux différentes attaques avec une détection aveugle.

Mot clefs : Carte chaotique, tatouage d'image, détection du filigrane, HVS, domaine fréquentiel, domaine spatial, Modélisation de la DCT, méthodes des moments.

Abstract

The objective of this thesis was to design new approaches for digital image watermarking in the goal to obtain the best compromise between robustness and invisibility. These methods involve the chaotic watermarking of digital images. The areas of the watermark insertion are adopted to both spatial and transform domain such as DCT and DWT.

The weakens points of the human eye are exploited for the design of the perceptual masks for the weighting of the watermark. It is about the determination of the textured areas and modeling of the effect of brightness. The use of these masks in the spatial domain and frequency domain, have allows obtaining a robust system against to the attacks and in the same time which does not degrade the image quality.

In the DCT domain, the insertion of the watermark was made by the operation of the proposed visual masks, and these schemes performance is studies in terms of quality and robustness.

The wavelet domain is also investigated for the chaotic watermarking images using the proposed masks. The concept of the reference image was used. Blind and not blind systems are used for the watermark detection.

Modeling the DCT coefficients was made by using the *GFD* distribution, and evaluation of their parameters is based on the use of the moment method; where the statistics of the image is taken into account for the design of a detection system. The performance study has highlighted the benefits of the proposed approaches in terms of invisibility and robustness against various attacks with blind detection.

Key-words: Chaotic map, image watermarking, watermark detection, HVS, transform domain, spatial domain, DCT modeling, moment method.

يتمثل الهدف من هذه الرسالة في تصميم مناهج جديدة لوشم الصور الرقمية للحصول على أفضل حل بين الجودة و المتانة باستعمال خرائط الفوضى، والتي تعتمد على المجال المساحي و التواتري.

أستغلت نقاط ضعف النظام البصري لتصميم الأقنعة البصرية، وذلك بتعيين المناطق المركبة ونمذجة النقاط المضيئة لوزن الوشم. هذه الأقنعة تم تطبيقها في المجال المساحي و التواتري لوشم الصور الرقمية، للحصول على نظام قوي ضد الهجمات بدون أن نفقد الصورة الرقمية جودتها.

في مجال DCT، تم إدخال الوشم باستعمال الأقنعة البصرية المقترحة، وقد تم تحليل هذه الدراسة من حيث الجودة و المتانة.

استخدمنا أيضا مجال الموجات المتقطع لوشم الصور باستعمال خرائط الفوضى عن طريق استعمال الأقنعة المقترحة مع اللجوء الى نظام الكشف الأعمى و الغير الأعمى للتعرف عن الوشم. وقد استخدم أيضا مفهوم الصورة المرجعية.

نمذجة معاملات DCT تم إجراؤها باستخدام التوزيع GFD، ويستند تقييم المعاملات باستخدام طريقة العزوم؛ حيث يتم أخذ الإحصاءات من الصورة في الحسبان لتصميم نظام الكشف الذي لا يعتمد على الصورة الأصلية. وقد أبرزت الدراسة التي قمنا بها فوائد النهج المقترح من حيث الجودة و المتانة ضد هجوم الضغط مع استعمال الكشف الأعمى.

كلمات مفتاحية: خرائط الفوضى، وشم الصور، كشف الوشم، HVS، المجال التواتري، المجال المساحي، نمذجة DCT، طريقة العزوم.

Liste des figures

Figure I. 1 : Echantillon de 2D de la carte skew tent produite lorsque $\mathbf{b0} = \mathbf{0.01}$; (a) : $\mathbf{a}=0.2$, (b) : $\mathbf{a} = \mathbf{0.9}$	11
Figure I. 2 : 300 points d'une trajectoire typique du système de la carte skew tent, pour $\mathbf{a} = 0.63$	12
Figure I. 3 : Watermak généré par la carte de Bernoulli ;(a) : $n=3$;(b) : $n=7$	13
Figure I. 4 : Filigrane généré par la carte logistique (a) : $y_0=0.001$ et $\lambda=3.83$, (b) : $y_0=0$ et $\lambda=4$, (c) : $y_0=0.1$ et $\lambda=3.98$	14
Figure I. 5 : Sensibilité de la carte logistique à la valeur initiale (0.1, 0.1001 et 0.2).....	15
Figure I. 6 : (a) : Fonction d'autocorrélation, (b) : Fonction de corrélation croisée des séquences chaotiques d'une longueur 2000. (Carte logistique).....	16
Figure I. 7 : Diagramme de bifurcation de la carte logistique (λ entre 0 et 4).....	16
Figure I. 8 : Diagramme de bifurcation de la carte logistique (λ entre 3.4 et 4).....	17
Figure II. 1 : Transmission d'un message par le tatouage d'un document.....	22
Figure II. 2 : Modèle général du processus d'insertion et de détection.....	23
Figure II. 3 : Image de logo :(a) : Logo de l'université de Batna ;(b) : Logo d'Air Algérie ;(c) : Logo de la Télévision Algérienne.....	23
Figure II. 4 : (a) : La carte Skew tent (0.9); (b) : La carte logistique ($y_0=0.1$ et $\lambda=3.98$) ; (c) : La carte de Bernoulli ($n=3$).....	24
Figure II. 5 : Les éléments contradictoires d'un système de tatouage.....	26
Figure II. 6 : Tatouage additive dans le domaine spatial : (a) : Le logo de l'université de Batna ; (b) : Image originale Watch ;(c) : Image tatouée avec $\alpha = \mathbf{0.2}$;(d) : Image tatouée avec $\alpha = \mathbf{0.7}$	28
Figure II. 7 : Tatouage multiplicative dans le domaine spatial : (a) : Le logo de l'université de Batna ; (b) : Image originale Watch ;(c) : Image tatouée avec $\alpha = \mathbf{0.2}$;(d) : Image tatouée avec $\alpha = \mathbf{0.7}$	29
Figure II. 8 : Etapes du procédé d'insertion du filigrane [11].....	32
Figure II. 9 : Etapes du procédé d'extraction [11].....	32
Figure II.10 : Les transformations géométriques ; (a) : Image originale ;(b) : La rotation ;(c) : La translation ;(d) : Le découpage.....	35
Figure III. 1 : La fonction de sensibilité au contraste.....	41
Figure III. 2 : Le filigrane produit ($X_0 = 0.1$ & $\lambda=3.98$), taille= 256×256	44
Figure III. 3 : Fonction de visibilité de bruit pour l'image peppers (a, b) et l'image f16 (c, d).....	45
Figure III. 4 : Diagramme proposé pour l'insertion de filigrane.....	46
Figure III. 5 : (a) : Image originale (b) : Image tatouée sans masque avec PSNR = 70.7608dB (c) : Image tatouée avec l'utilisation du masque pour PSNR=87.4980dB (d) : La différence entre l'image tatouée et l'image originale (les grandeurs sont amplifiées par un facteur de 100 pour le but de visionnement, le nombre maximum de l'information qui peut être insérée dans l'image est 7941 bits).....	47
Figure III. 6 : Variation de PSNR de l'image tatouée avec et sans masque pour les images Lena, peppers, boat et baboon.....	48
Figure III. 7 : Valeurs de masque proposé.....	49

Figure III. 8 : (a) :L'image originale ; (b) : L'image masque basée sur le HVS.....	49
Figure III. 9 : Réponse du détecteur de l'image tatouée dans la figure (III.9c) à 1000 filigranes produits.....	50
Figure III. 10 : Comparaison des images, (a): Image originale, (b): Image tatouée sans masque PSNR=31.3682dB (c) : Image tatouée avec masque PSNR=43.8767dB ($\alpha=0.03$)	51
Figure III. 11 : Variation de PSNR de l'image tatouée peppers avec et sans masque.....	51
Figure III. 12 : Réponse de détecteur à la compression JPEG de l'image peppers	52
Figure III. 13 : Filigranes présentés en forme binaire créés par la même clef ($\lambda= 3.98$, $X_0=0.01$), (a) : Balayage raster, (b) : Balayage de Peano	53
Figure III. 14 : Exemple de mélange, (a) : L'image originale, (b), (c), et (d) L'itération du mélange de (a) après un, deux, et dix itérations, respectivement.....	54
Figure III. 15 : Valeurs de masque.....	55
Figure III. 16 : Le masque visuel proposé, (a) : Le masque du texture M1;(b) : Le masque de luminance M2 ;(c) Le masque proposé M amplifié par un facteur de 5 pour le visionnement.....	56
Figure III. 17 : Réponse du détecteur pour l'image watch.....	56
Figure III. 18 : Images après l'insertion du watermark ; (a) : Image tatouée avec le masque proposé PSNR=40.2252dB ; (b) : Image tatouée sans masque PSNR=27.6461dB ; (c) et (d) La différence entre l'image tatouée et originale amplifiée par un facteur 100 pour le visionnement.	57
Figure III. 19 : Variation de PSNR de l'image tatouée avec et sans masque	58
Figure III. 20 : La réponse du détecteur :(a, b) : Compression JPEG (Q=20), (c, d) : Filtrage médian (fenêtre 3×3), (e, f) : Ajout de bruit (100%), (g, h) : Le découpage diagonal (50%)	60
Figure IV. 1 : Ordre des coefficients DCT.....	64
Figure IV. 2 : Amplitude des coefficients DCT	65
Figure IV. 3 : Calcul de la 2D-DCT par l'utilisation de la séparabilité.....	66
Figure IV. 4 : Les coefficients DCT où le watermark est inséré.....	68
Figure IV. 5 : Comparaison d'invisibilité par l'insertion du filigrane dans le DC et les coefficients moyens, (a) : Image originale Watch, (b) : Image tatouée en utilisant les coefficients DC ($\alpha=0.1$), (c) : Image tatouée en utilisant les coefficients moyens ($\alpha=0.022$)	70
Figure IV. 6 : Test de robustesse (a) : Compression JPEG, (b) : Filtrage médian	70
Figure IV. 7: (a) : Le masque obtenu par l'image boat ; (b) : Watermark de la taille 32×32	71
Figure IV. 8 : Comparaison des images, (a) : Image originale, (b) : Image tatouée sans masque PSNR=40.7620dB, (c) : Image tatouée avec masque PSNR = 43.7202dB.....	73
Figure IV. 9 : Comparaison de PSNR entre le système proposé avec le masque et sans masque pour l'image boat.....	73
Figure IV. 10 : Valeur de masque.....	74
Figure IV. 11: Le masque visuel proposé, (a) : L'image originale ; (b) : Fonction de visibilité de bruit de f16 ; (c) : Le masque de texture ;(d) : Le masque de luminance proposé ;(e) : Le masque final obtenu.....	74
Figure IV. 12: Comparaison des images, (a) : Image tatouée avec le masque ML PSNR=40.1958dB, (b) : Image tatouée par le masque MT PSNR=35.3071dB, (c) ; (d) : La différence entre l'image tatouée et l'image originale amplifiée par un facteur de 100 pour le but de visionnement	76

Figure IV. 13 : Comparaison de PSNR entre les deux méthodes	76
Figure IV. 14 : Test de robustesse (a) : Compression JPEG, (b) : L'ajout du bruit.....	77
Figure V. 1 : Décomposition d'une image par DWT :(a) : Image à décomposer, (b) : Niveau 1 ;(c) : Niveau 2 ; (d) : Niveau 3	83
Figure V. 2 : Décomposition en ondelette niveau 2 pour l'image boat	84
Figure V. 3 : Schéma fonctionnel de la méthode proposée.....	85
Figure V. 4 : La réponse du détecteur	86
Figure V. 5 : (a) : Image originale, (b) : Le filigrane utilisé 64× 64.....	87
Figure V. 6 : Comparaison des méthodes d'insertion ; (a) : L'image boat tatouée dans le DWT PSNR=40.4808dB, (b) : Image tatouée dans le domaine spatial PSNR = 38.2891dB, (c), (d) : La différence entre l'image tatouée et l'image originale amplifiée par un facteur de 20 pour le but de visionnement.....	87
Figure V. 7 : Comparaison de PSNR entre les deux méthodes	88
Figure V. 8 : Comparaison de robustesse, (a), (b) et (c) : Image compressée avec un facteur de qualité Q=20, (d), (e) et (f) : Filtrage médian avec une fenêtre de taille de 5× 5	89
Figure V. 9 : (a) : Image originale baboon ;(b) : Le masque obtenu [1], [2] (amplifié par 10) ; (c) : Le masque proposé obtenu par le choix du minimum (amplifié par 10).....	90
Figure V. 10 : Comparaison de PSNR entre les deux méthodes.....	90
Figure V. 11 : Comparaison de robustesse entre le schéma proposé et celui de [1], (a), (b) et (c) : Images compressées avec le facteur de qualité Q=20, (d), (e) et (f) : Image tatouée attaquée par le filtrage médian avec une fenêtre de taille de 5× 5 et la réponse du détecteur	91
Figure V. 12 : Procédure d'insertion proposée	92
Figure V. 13 : Procédure de détection proposée	94
Figure V. 14 : (a) : Image de test; (b) : Image de référence; (c) : Image tatouée PSNR=36.91dB ($\alpha=0.03$).....	94
Figure V. 15 : Réponse de détecteur à 200 filigranes produits.....	95
Figure V. 16 : Variation du PSNR de l'image tatouée	95
Figure V. 17 : Réponse de détecteur au JPEG pour (Q=30)	96
Figure V. 18 : Graphique de ROC.....	98
Figure V. 19 : Réponse du détecteur à la compression JPEG avec alpha=0.09	99
Figure VI. 1 : Histogramme des coefficients de DCT de l'image Bridge [19]	104
Figure VI. 2 : La fonction de la densité de probabilité de GGD avec $\sigma^2 =1$	105
Figure VI. 3 : Sensibilité de GFD à ses paramètres pour l'image watch	107
Figure VI. 4 : Le Pdf empirique et ses modèles statistiques.....	107
Figure VI. 5 : Comparaison de la qualité de l'ajustement.....	113
Figure VI. 6 : Comparaison visuelle de la qualité des images tatouées : le haut sont les images originales, et le bas sont les images tatouées.....	113
Figure VI. 7 : Comparaison de PSNR entre les ac et les coefficients bas du ac.....	114
Figure VI. 8 : Réponse du détecteur pour l'image tatouée.....	115
Figure VI. 9 : Réponse du détecteur face à la compression JPEG pour l'image baboon ..	116

Liste des tableaux

Tableau II. 1: Métriques de distorsion basées sur la différence entre l'image originale et tatouée.....	34
Tableau V. 1: Mesure de qualité en PSNR.....	88
Tableau VI. 1: Test d'ajustement pour différentes images.....	111
Tableau VI. 2: Paramètre γ estimé pour différentes images de test.....	112
Tableau VI. 3: Comparaison de la qualité de l'ajustement.....	112
Tableau VI. 4: Amélioration du CR.....	116

Liste des abréviations

P2P : Peer To Peer

HVS : Human Visual System

JPEG : Joint Photographic Experts Group

DCT : Discret Cosine Transform

GGD : Generalized Gauss Distribution

GFD : Generalized Gamma distribution

DFT : Discret Fourier Transform

MPEG: Moving pictures Experts Group

PSNR : Peak signal to Noise Ratio

MSE : Mean Square Error

dB : Decibel

NVF : Noise Visibility Function

ROC : Receiving Operating Characteristics

Pdf : Probability Density Function

Liste des conférences & publications

1. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Efficient Image Watermarking Using Noise Visibility Function*", Fourth International Multi-Conference on Systems, Signals & Devices, March 19-22, Hammamet, Tunisia, 2007.
2. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Masking Model For Image Watermarking*", The 4th International Summer School on Signal Processing & it's Applications, 30 June-4 July Boumerdes (UMBB) Algeria, 2007.
3. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*A Comparative Study Of DCT Image Watermarking Algorithms*", 3^{èmes} Journées Internationales sur l'Informatique Graphique, Constantine, Algeria, October-29-30, 2007.
4. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Luminance-Model For Spread Spectrum Image Watermarking*", 4th International Conference on Computer Integrated Manufacturing CIP'2007, Setif, Algeria November 03-04, 2007.
5. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Robust Color Image Watermarking Scheme*", 4th International Conference on Computer Integrated Manufacturing, Setif, Algeria November 03-04, 2007.
6. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Chaos-Based Image Watermarking Scheme In The DWT*", Les Journées sur les Signaux et Systèmes, Guelma, Algeria Novembre 14-15, 2007.
7. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*Image Watermarking Using Visual Model Based Discrete Wavelet Transform*", 2^{ème} Conférence sur la Vision Artificielle, Tizi-Ouzou, November 18-20, Algeria, 2007.
8. S. BELKACEM, Z. DIBI, A. BOURIDANE, "*A Masking Model Of HVS For Image Watermaking In The DCT Domain*", IEEE, International Conference on Electronics, Circuits and Systems, Marrakech, 330-334, Morocco, December 11-14, 2007.
9. S. BELKACEM, Z. DIBI, A. BOURIDANE & M. LAADJEL, "*Color Image Watermarking Based On Chaotic Map*", IEEE, International Conference on Electronics, Circuits and Systems, Marrakech, 343-346, Morocco, December 11-14, 2007.
10. S. BELKACEM, S. KHALDI, Z. DIBI, & A. BOURIDANE, Z. AMRANI, "*Image Watermarking Algorithm Based On Perceptual Masking And Chaotic Map*", 10th Maghrebian Conference on Information Technologies, MCSEAI, April 28-30, Oran, Algeria, 2008.
11. S. BELKACEM, S. KHALDI, Z. DIBI, & A. BOURIDANE, "*Image Watermarking Scheme Based On Self-Reference Image*", La journée des Jeunes Chercheurs en Informatique, 20 Mai, Guelma, Algérie, 2008.

12. S. BELKACEM, Z. DIBI, & A. BOURIDANE, "*Watermarking Scheme Based On Image Statistics*", The 9th International Summer School on Signal Processing & it's Applications, 3-7 October, Oran Algeria, 2009.
13. S. BELKACEM, Z. DIBI, & A. BOURIDANE, "*Chaos Watermarking Scheme Based on Wavelet Domain*", International Conference on Electrical Engineering, Electronics and Automatics, 2-3 November Bejaia, Algeria, 2010.
14. S. BELKACEM, Z. DIBI, & A. BOURIDANE, "*DCT coefficients modelling for image watermarking*", International Journal of Computers and Applications, Acta Press, 36, 155-163, 2014.

Table des matières

Remerciements	i
Résumé	ii
Abstract	iii
ملخص	iv
Liste des figures	v
Liste des tableaux	viii
Liste des abréviations	ix
Liste des conférences & publications	x
Table des matières	xii
Introduction générale	1
Problématique.....	1
Solution	2
Organisation de la thèse	5
Bibliographie	6
Chapitre I : La théorie des systèmes chaotiques	9
Introduction	9
1. Historique de la théorie du chaos	9
2. Les systèmes dynamiques.....	10
3. Les cartes chaotiques les plus utilisées	11
3.1. La carte Skew tent	11
3.2. La carte de Bernoulli	12
3.3. La carte logistique	13
3.3.1. Sensibilité aux conditions initiales.....	14
4. Les propriétés de corrélation des séquences chaotiques.....	15
5. Diagramme de bifurcation	16
6. Application du Chaos dans le domaine du tatouage numérique.....	18
7. Avantage des séquences chaotiques	18
8. Filigrane à base de cartes chaotiques.....	18
Conclusion.....	19
Bibliographie	19
Chapitre II : Généralités sur le tatouage d'images numériques	21
Introduction	21

1. Historique du tatouage.....	21
1.1. Le tatouage numérique.....	22
1.2. Eléments d'un système de tatouage.....	22
1.3. Le processus du tatouage.....	22
2. Types de filigrane.....	23
2.1. Logos et images.....	23
2.2. Filigranes pseudo-aléatoires.....	24
2.3. Filigranes chaotiques.....	24
3. Les propriétés d'un filigrane.....	24
4. Les contraintes d'un système de tatouage.....	26
4.1. Transparence (invisibilité).....	27
4.2. Robustesse.....	27
4.3. Capacité.....	27
5. Les techniques du tatouage.....	27
5.1. Méthodes d'insertion d'un filigrane.....	27
5.2. Méthode de détection du filigrane.....	29
5.3. Domaines de tatouage.....	30
5.3.1. Domaine spatial.....	30
5.3.2. Domaine transformé.....	30
5.3.3. Domaine hybride.....	33
6. Evaluation des algorithmes du tatouage.....	33
7. Classification des attaques.....	35
8. Applications du tatouage numérique.....	36
Conclusion.....	37
Bibliographie.....	37

Chapitre III : Les algorithmes développés de tatouage des images dans le domaine spatial..... 40

Introduction.....	40
1. Le système visuel humain (HVS).....	40
1.1. Masques psychovisuels.....	41
2. Etat de l'art sur la modélisation du HVS pour le tatouage d'image.....	42
3. Notre système de tatouage.....	43
4. Tatouage d'image numérique par l'utilisation de la fonction de visibilité de bruit (NVF).....	43
4.1. Construction de filigrane.....	44
4.2. Génération du masque.....	44
4.3. Procédure d'insertion.....	46

4.4.	Résultats de simulation	46
5.	Modèle de luminance pour le tatouage d'image.....	48
5.1.	Le masque spatial proposé	48
5.2.	Insertion du filigrane.....	49
5.3.	Détection de filigrane.....	50
5.4.	Résultats de simulation	51
6.	Algorithme de tatouage d'image basé sur le <i>NVF</i> et la luminance	52
6.1.	Génération du filigrane.....	53
6.2.	Le masque spatial proposé	54
6.3.	Etude de performance du masque proposé	55
6.3.1.	Insertion du filigrane.....	55
6.3.2.	Détection de filigrane	56
6.4.	Résultats et discussion	57
6.4.1.	Mesure de qualité.....	57
1.1.1.	Test de robustesse.....	58
	Conclusion.....	59
	Bibliographie	60
Chapitre IV: Les algorithmes développés de tatouage des images dans le domaine DCT		63
	Introduction	63
1.	La transformée en cosinus discrète	63
1.1.	La forme mathématique de la DCT	63
1.2.	Distribution des coefficients DCT	64
1.3.	Propriétés de la DCT.....	65
1.3.1.	La décorrélation	65
1.3.2.	Concentration de l'information	65
1.3.3.	Séparabilité	65
1.3.4.	Réversibilité.....	66
1.4.	Pour quoi la DCT?	66
2.	Etat de l'art sur le tatouage d'image dans la DCT.....	66
3.	Etude comparative des algorithmes de tatouage d'image dans le domaine DCT..	68
3.1.	Etude comparative entre DC et les coefficients moyens	68
3.1.1.	Insertion du watermark.....	68
3.1.2.	Extraction de filigrane.....	69
3.1.3.	Comparaison visuelle	70
3.1.4.	Test de robustesse.....	70

3.2.	Algorithme du tatouage d'image basé sur le DC et le HVS.....	71
3.2.1.	Insertion du filigrane.....	71
3.2.2.	La procédure de détection.....	72
3.2.3.	Résultats de tatouage basé sur DC	72
4.	Modèle de HVS pour le tatouage d'image dans le domaine DCT.....	73
4.1.	Conception du masque	74
4.2.	Stratégie d'insertion	74
4.3.	Procédure d'extraction du filigrane.....	75
4.4.	Evaluation des performances	75
4.5.	Test de robustesse.....	77
	Conclusion.....	78
	Bibliographie	78
	Chapitre V : Les algorithmes développés de tatouage des images dans le domaine DWT.....	80
	Introduction	80
1.	La théorie des ondelettes	80
2.	Les propriétés d'ondelettes.....	81
3.	Représentation des coefficients d'ondelettes.....	82
4.	Quelques algorithmes de tatouage d'image utilisant la transformée en ondelettes	84
5.	Tatouage d'image basé sur le modèle visuel dans le domaine des ondelettes.....	85
5.1.	Algorithme d'insertion du filigrane	85
5.2.	Détection du filigrane.....	86
5.3.	Résultats de simulation	87
5.3.1.	Mesure de la qualité perceptuelle	87
5.3.2.	Test de robustesse.....	88
6.	Schéma de tatouage d'image dans le DWT basé sur la valeur minimale.....	89
7.	Schéma de tatouage d'image basé sur l'image d'auto référence.....	91
7.1.	Insertion du filigrane.....	93
7.2.	Détection de filigrane.....	93
7.3.	Résultats de simulation	94
8.	Schéma de tatouage dans le domaine des ondelettes basé sur les statistiques d'image.....	96
8.1.	Insertion du filigrane.....	96
8.2.	Détection de filigrane.....	97
8.2.1.	Seuil de décision.....	97
8.3.	Graphique de la caractéristique opérationnelle de récepteur (ROC).....	98

8.4. Compression de JPEG.....	98
Conclusion.....	99
Bibliographie	99
Chapitre VI : Modélisation des coefficients DCT :Application au tatouage d'image.....	102
Introduction	102
1. Etat de l'art sur la modélisation des coefficients DCT.....	102
2. Distribution de Gauss Généralisée GFD	104
2.1. Evaluation de paramètre de forme et d'écart type.....	105
3. La distribution GFD	106
3.1. Distribution GFD à quatre paramètres.....	106
3.2. Distribution GFD à trois paramètres.....	106
3.2.1. Sensibilité de la distribution GFD à ses paramètres	107
3.2.2. Pdf des coefficients de DCT	107
4. Modélisation des coefficients DCT : Application au tatouage d'image	108
4.1. Evaluation des paramètres de la distribution GFD	108
4.2. Stratégie de tatouage d'image.....	108
4.3. Détecteur de filigrane.....	109
4.4. Résultats de simulation	111
4.4.1. Qualité d'ajustement.....	111
4.4.2. Mesure de qualité.....	113
4.4.3. Test de robustesse.....	114
Conclusion.....	116
Bibliographie	117
Conclusion générale	120
Annexe A: Les techniques de balayage	125
1. Le balayage Zig-Zag	125
2. Le balayage raster	125
3. Le balayage de Kutter	126
4. Le balayage de Peano.....	126
Bibliographies	127
Annexe B : Démonstration mathématique.....	128
Annexe B.0 : Calcul du moment <i>kth</i>	128
Annexe B.1 : Détermination des paramètres de GFD	129
Annexe B.2 : Calcul de la moyenne et de la variance.....	130

Introduction générale

Problématique

Une œuvre numérique peut être distribuée de manière légale sous forme concrète (CD, DVD), ou via des plates formes payantes de téléchargement qui permettent la rémunération de l'auteur. Cependant, il est très aisé de fabriquer une copie absolument identique à l'œuvre numérique originale, ainsi que de la distribuer. La contrefaçon ne nécessite pas de moyens techniques particulier. Le problème est devenu particulièrement aigu avec l'apparition du système P2P (Peer to Peer) [1], comme Kazaa, Limewire, Exceem et eMule permettant de copier facilement le contenu des utilisateurs du Web pour accéder et partager des Terabyte des médias numériques. Cette technologie réduit également de manière significative les efforts des pirates pour enregistrer illégalement, au disque, vente, copie et distribution du matériel copyright-protection sans compenser les propriétaires de leur copyright juridiques [2].

Les documents numériques quels qu'ils soient sont donc soumis au problème du piratage (copie des documents sans acquittement de droits d'auteur). Le piratage peut avoir une répercussion économique non négligeable. Selon une étude publiée par l'organisation professionnelle de lutte contre la piraterie IIPA (International Intellectual Property Association), près de 10 millions de jeux vidéo ont été piratés en décembre 2009 [3]. L'IIPA est une organisation regroupant plus de 1900 entreprises qui produisent et distribuent du matériel protégé par les droits d'auteur à travers le monde [4].

Une étude réalisée en mois de Mars 2010 par TERA Consultants, un cabinet de conseil indépendant basée à Paris, a porté essentiellement sur l'effet de la piraterie numérique qui recouvre les différentes formes de piratage en ligne, dont l'échange de fichiers P2P. Cette étude avait pour objectif d'évaluer les conséquences économiques du piratage numérique sur les industries créatives et a visée en particulier son impact sur la perte de chiffre d'affaires et d'emplois [3].

Solution

Le tatouage numérique ou le watermarking cherche de résoudre le problème de la protection des droits d'auteur ou copyright. Le tatouage numérique est une technique issue d'un art appelé la stéganographie. Il s'agit d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message caché dans le signal hôte, généralement appelé le watermark ou le filigrane (est un ensemble de bits, dont le contenu dépend de l'application). Le filigrane peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte [5].

Dans la littérature, plusieurs méthodes efficaces de tatouage sont développées et satisfont certains conditions selon le problème traité, mais la majorité des watermarks sont générés par les générateurs pseudo-aléatoire [6], [7]. Le filigrane à base de carte chaotique suscite un intérêt accru récemment, et s'est avéré une alternative à cette technique. La notion du chaos est introduite pour la sécurité des systèmes de transmission en général et dans les systèmes de tatouage numérique en particulier. La génération de filigrane par l'utilisation de la carte chaotique a été présentée vers les années 90 par Voyatzis et al. [8]. Ces itérations sont modélisées sous la forme d'un système dynamique et sont étudiées dans le cadre de la théorie mathématique du chaos.

Vu les propriétés des séquences chaotiques telles que : distribution uniforme, hyper sensibilité à la clef secrète et reproductibilité à l'identique (déterministe), ses dernières propriétés sont d'excellentes candidates pour sécuriser efficacement l'accès aux positions du filigrane et de répartir spatialement de façon uniforme le tatouage ou le filigrane dans toute l'image [9].

La discipline de l'évaluation de la qualité des images a permis la mise en œuvre de plusieurs études approfondies du Système Visuel Humain (HVS). Dans plusieurs algorithmes de tatouage numérique le filigrane est inséré par une petite modification sur les données originales. Cette modification est effectuée en ajoutant ou en soustrayant des éléments du filigrane. Avant le processus d'insertion, le filigrane est pondéré par un facteur. Le problème ici est de trouver une valeur optimale de ce facteur qui est calculé en exploitant des modèles de HVS. L'utilisation des masques perceptuels,

qui tiennent compte des propriétés du système visuel humain (HVS), s'avère être une manière efficace d'améliorer la robustesse d'un filigrane sans affecter la qualité d'image [10].

Les trois clefs d'un système de tatouage sont : la méthode de la génération du filigrane, l'algorithme d'insertion du filigrane et l'algorithme de la détection ou l'extraction du filigrane. La détection de filigrane dépend de la manière de l'insertion de filigrane, et aussi des propriétés statistiques des coefficients d'image.

Selon la théorie de la détection du signal, le modèle mathématique des données originales est important, et possède une influence pertinente sur les performances du détecteur. La connaissance de la distribution statistique du signal hôte est une donnée indispensable pour modéliser d'une façon rigoureuse le système du tatouage [11].

Plusieurs travaux ont étudiés les méthodes de tatouage basées sur la modélisation des coefficients de l'image numériques dans le domaine transformé tel que la DCT (Discret Cosine Transform), et les techniques de détection du filigrane inséré [11], [12], [13], [14], [15]. Les coefficients à haute fréquence de la DCT ont été modélisés par la distribution GGD par Hernandez et al. [12], et l'insertion du filigrane est basée sur l'image masque, le détecteur optimum a été développé.

La modélisation des coefficients DCT par la distribution de Weibull a été étudié par [13] d'une manière multiplicative, et l'étape de détection était semblable à celle du Hernandez et al. [12]. Une comparaison entre les différents types de détecteurs pour l'insertion multiplicative et additive du filigrane dans les coefficients d'image est proposée par [14] pour les distributions de Weibull et de GGD.

La modélisation des coefficients DCT par la distribution α –stable est proposée par [15], mais la détection est basée sur la distribution de Cauchy, et la connaissance de la valeur de la force d'insertion du filigrane est indispensable comme dans [12]. Cette contrainte constitue une limitation pour une détection aveugle du filigrane. Wu et al. [16] ont modélisé les coefficients DCT d'une manière semblables à Briassouli et al. [15], mais le détecteur était construit sur la base de la même distribution.

L'objectif de ce travail consiste à étudier et de développer des algorithmes de tatouage d'image numériques basés sur les séquences chaotiques dans le cadre de la protection des droits d'auteur, en tenant compte des possibilités d'attaques sur les schémas proposés, sans dégrader leur qualité perceptuelle.

Quatre algorithmes de tatouage d'image sont proposés dans le domaine spatial qui sont présentés dans les travaux [17], [18], [19], [20]. Dans une première étape, on a proposé l'exploitation de la fonction NVF (Noise Visibility Function) comme une image de pondération et au même temps comme un filtre pour l'insertion du watermark afin d'obtenir des valeurs élevées de PSNR [17]. Puis on a conçu dans un autre travail [18] un masque perceptuel pour la pondération du filigrane par la modélisation de l'effet de luminance sur le HVS. Vient par la suite, les travaux qui se trouve dans [19], qui utilisent les deux idées au même temps pour la génération d'un nouveau masque, et l'étude de performance en terme de visibilité et robustesse du schéma de tatouage est étudié dans [20].

Les travaux [21], [22] sont proposés dans le cadre du tatouage d'image dans le domaine transformé DCT. Une comparaison entre les coefficients de la transformée DCT est faite [21], il s'agit des coefficients DC et les coefficients de fréquence moyenne, et ceci est testé sur un système de tatouage complet. Vu les résultats obtenus par les coefficients DC en terme de qualité visuelle de l'image tatouée et de robustesse ; ils sont alors choisis par notre système de tatouage. Dans le même travail, on a utilisé le masque développé dans le domaine spatial [19] pour la pondération du filigrane dans le domaine DCT. Dans ce domaine on a développé aussi un masque qui exploite les propriétés visuelles [22], mais cette fois d'une manière linéaire dans le domaine spatial, puis on l'a exploité dans le domaine transformé. Les performances de ce système en terme de qualité et de robustesse sont étudiées.

Quatre travaux sont fait dans le domaine des ondelettes. Dans un premier lieu on utilise le masque proposé dans le travail de [19] pour faire l'insertion dans le domaine d'ondelette en choisissant la bande basse fréquence [23]. Puis un nouveau masque est conçu, basé sur la sélection de la valeur minimale entre la texture et la luminance [24]. Dans le troisième travail [25] une nouvelle méthode basée sur l'image d'auto référence

est utilisée. Enfin, de la même façon d'insertion que dans [23], le système de détection utilisé est semi aveugle basé sur les statistiques de l'image tatouée [26].

Le quatrième travail a porté sur la modélisation des coefficients DCT. On a prouvé par simulation que les coefficients bas du ac de la transformée DCT sont bien modélisés par la distribution *GFD* (Generalized Gamma Distribution) ; et leur paramètres sont déterminés à partir de la méthode des moments. Ces coefficients sont choisis pour l'insertion du watermark chaotique. Pour l'étape de la détection on a développé un détecteur basé sur le maximum de la vraie semblance afin de montrer la robustesse de notre algorithme face à la compression JPEG (Joint Photographic Experts Groups) [27].

Organisation de la thèse

La thèse est composée de deux parties et organisée comme suit:

La première partie établit un état de l'art des différentes terminologies dans lesquelles s'inscrivent nos travaux de thèse, il s'agit du chaos et du watermarking d'image. Cette partie se décompose aussi en deux chapitres:

- Puisque le filigrane est l'élément essentiel dans les différents schémas de tatouage des images proposés dans cette thèse, nous avons consacré le premier chapitre à la notion du signal chaotique et son utilisation à la génération des séquences pseudo aléatoire, ainsi que les propriétés statistiques du signal généré sont présentées. L'étude théorique approfondie du chaos est loin d'être l'objectif de cette thèse.
- En chapitre 2 on présente une littérature sur les algorithmes du tatouage des images numériques. L'histoire du tatouage numérique sera donnée. On discutera aussi les éléments de base d'un système de tatouage numérique et les différentes contraintes qu'on devrait considérer. L'état de l'art sur les méthodes de tatouage basées sur les séquences chaotiques est exposé également dans cette partie. Les attaques possibles et l'évaluation de la qualité perceptuelle des images.

La seconde partie est composée de quatre chapitres, qui présente les quatre méthodes de tatouage développées avec l'essentielle des résultats de simulation dans le

cadre du tatouage chaotique des images numériques. On commence par l'état de l'art au début de chaque chapitre, et les algorithmes développés seront ensuite expliqués.

- Nous donnons dans le chapitre 3, les algorithmes développés de tatouage d'image numérique dans le domaine spatial et les masques visuels proposés. La validation des masques obtenus seront ensuite testé dans des schémas de tatouage dans le domaine spatial.
- Différents algorithmes proposés de tatouage basés sur la transformée DCT par l'utilisation des masques perceptuels sont discutés au chapitre 4.
- Au chapitre 5, les algorithmes de tatouage proposés dans le domaine transformé d'ondelette, qui sont basés sur les masques perceptuels sont évalués, et leur robustesse sont comparées les uns avec les autres.
- Au chapitre 6, nous décrivons les étapes nécessaires à l'élaboration d'un modèle pour les coefficients d'images dans le domaine transformé DCT par l'utilisation de la Distribution Gamma Généralisée (*GFD*). On décrit aussi l'algorithme proposé pour l'insertion et l'extraction du watermark dans les images numériques, ainsi que leurs résultats de simulation pour l'évaluation de leur performance.

Une conclusion générale suit immédiatement le chapitre 6 pour conclure le travail, on cite quelques perspectives de ce travail.

Quelques méthodes de balayage du filigrane, que nous avons utilisées lors des différents schémas de tatouage sont données en annexe A.

L'annexe B insérée en fin de cette thèse décrit la démonstration mathématiques des équations : de moment, d'estimation des paramètres de la distribution *GFD*, et le calcul de la variance et la moyenne du détecteur.

Bibliographie

[1] V. Martin, Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique, Thèse de Doctorat, Polytechnique de Toulouse, 2006.

- [2] C. Obimbo, B. Salami, Using digital watermarking for copyright protection, watermarking, 2, Dr. Mithun Das Gupta (Ed.), ISBN: 978-953-51-0619-7, InTech, 2012.
- [3] M. Koubaa, Tatouage robuste de vidéo basé sur la notion de régions d'intérêt, Thèse de Doctorat, Université Bordeaux 1, 2010.
- [4] <http://www.iipa.com>
- [5] M. Eyadat, Comparative performance evaluation of practical digital watermarking embedding schemes, Thèse de Doctorat, University of California 2003.
- [6] L. Kocarev and G. Jakimoski, Pseudorandom bits generated by chaotic maps, IEEE Transactions On Circuits And Systems—I: Fundamental Theory And Applications, 50(1), 123-126, January 2003.
- [7] C.W.H.Fung, A. Gortan, W.G. Junior, A review study on image digital watermarking, The Tenth International Conference on Networks, The Netherlands Antilles, 24-28, 23-28 January 2011.
- [8] G. Voyatzis and I. Pitas, Chaotic watermarks for embedding in the spatial digital image domain, IEEE International Conference on Image Processing, 2, 432–436, 1998.
- [9] A. Mooney, The Generation and detection of chaos-based watermarks, Thèse de Doctorat, Nuimaynooth University, 2005.
- [10] G.I. Karybali, K. Berberidis, Efficient spatial image watermarking via new perceptual masking and blind detection schemes, IEEE Transactions on Information Forensics and security, 1(2), 256 – 274, June 2006.
- [11] G. Guelvouit, Tatouage robuste par étalement de spectre avec prise en compte de l'information adjacente, Thèse de Doctorat, INSA DE RENNES, 2003.
- [12] J.R. Hernandez, M. Amado, and F.P. Gonzalez, DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure, IEEE Transaction Image Processing, 9(1), 55–68, Janvier 2000
- [13] M. Barni, F. Bartolini, A.D. Rosa, and A. Piva, Optimum decoding and detection of multiplicative watermarks, IEEE Transaction Signal Processing, 51(4), 1118–1123, April 2003.
- [14] Q. Cheng and T.S. Huang, Robust optimum detection of transform domain multiplicative watermarks, IEEE Transaction Signal Processing, 51(4), 906–924, April 2003.
- [15] A. Briassouli, P. Tsakalides, and A. Stouraitis, Hidden messages in heavy-tails: DCT-domain watermark detection using alpha-stable models, IEEE Transaction Multimedia, 7(4), 700–715, August 2005.

- [16] J. Wu, Z. Sun, Robust detection of DCT-domain watermarks using alpha-stable models, 4th IEEE Conference on Industrial Electronics and Applications, 3787-3790, 2009.
- [17] S. Belkacem, Z. Dibi, A. Bouridane, Efficient image watermarking using noise visibility function, Fourth International Multi-Conference on Systems, Signals & Devices, March 19-22, Hammamet, Tunisia, 2007.
- [18] S. Belkacem, Z. Dibi, A. Bouridane, Luminance-model for spread spectrum image watermarking, 4th International Conference on Computer Integrated Manufacturing CIP, November 03-04, Setif Algeria, 2007.
- [19] S. Belkacem, Z. Dibi, A. Bouridane, Masking model for image watermarking, The 4th International Summer School on Signal Processing & its Applications, 30 June-4 July, Boumerdes (UMBB) Algeria, 2007.
- [20] S. Belkacem, S. Khaldi, Z. Dibi, & A. Bouridane, Z. Amrani, Image watermarking algorithm based on perceptual masking and chaotic map, 10th Maghrebian Conference on Information Technologies, MCSEAI, April 28-30, Oran, Algeria, 2008 .
- [21] S. Belkacem, Z. Dibi, A. Bouridane, A comparative study of DCT image watermarking algorithms, 3^{èmes} Journées Internationales sur l'Informatique Graphique, JIG'2007, Constantine, Algeria, October-29-30, 2007.
- [22] S. Belkacem, Z. Dibi, A. Bouridane, A masking model of HVS for image watermarking in the DCT domain, IEEE, 14th International Conference on Electronics, Circuits and Systems, Marrakech, Morocco December, 330 – 334, 11-14, 2007.
- [23] S. Belkacem, Z. Dibi, A. Bouridane, Image watermarking using visual model based discrete wavelet transform, 2^{ème} Conférence sur la Vision Artificielle, Tizi-Ouzou, Algeria Nov 18-20, 2007.
- [24] S. Belkacem, Z. Dibi, A. Bouridane, Chaos-based image watermarking scheme in the DWT, Les Journées sur les Signaux et Systèmes, JSS, Guelma, Algeria Novembre 14-15, 2007.
- [25] S. Belkacem, S. Khaldi, Z. Dibi, & A. Bouridane, Image watermarking scheme based on self-reference image, La journée des Jeunes Chercheurs en Informatique, 20 Mai, Guelma, Algérie, 2008.
- [26] S. Belkacem, Z. Dibi, & A. Bouridane, Chaos watermarking scheme based on wavelet domain, International Conference on Electrical Engineering, Electronics and Automatics'10 Bejaia, Algeria, 2-3 November 2010.
- [27] S. Belkacem, Z. Dibi, & A. Bouridane, DCT coefficients modelling for image watermarking, International Journal of Computers and Applications, Acta Press, 36, 155-163, 2014.

Chapitre I : La théorie des systèmes chaotiques

Introduction

Les cartes chaotiques peuvent être utilisées, dans les applications liées à la sécurité de l'information, pour la génération des clés secrètes dans les algorithmes de cryptage, de stéganographie, et de tatouage numérique. Dans ce chapitre, on donne en bref la théorie des systèmes chaotiques, et les différentes cartes utilisées pour produire une nouvelle classe des signaux, appelée les séquences chaotiques. Ce travail se concentre principalement sur l'application de la théorie de chaos pour la conception du filigrane pour les systèmes du tatouage de l'image numérique. Ainsi que les différentes cartes chaotiques utilisées pour la génération du filigrane numérique qui sont également étudiés, avec leurs propriétés.

1. Historique de la théorie du chaos

En 1963 le météorologue Edward Lorenz expérimentait une méthode lui permettant de prévoir les phénomènes météorologiques. C'est par pur hasard qu'il observa qu'une modification minime des données initiales pouvait changer de manière considérable ses résultats. Lorenz venait de découvrir le phénomène de sensibilité aux conditions initiales. Les systèmes répondant à cette propriété seront à partir de 1975 nommés : systèmes chaotiques [1].

Vers la fin du XIXe siècle le mathématicien, physicien et philosophe français Henri Poincaré avait déjà mis en évidence le phénomène de sensibilité aux conditions initiales lors de l'étude astronomique du problème des trois corps. On trouve dans le calcul des probabilités de Henri Poincaré l'affirmation suivante [2] :

«Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. Si nous connaissions exactement les lois de la nature et la situation de l'univers à l'instant initial, nous pourrions prédire exactement la situation de ce même univers à un instant ultérieur. Mais, lors même que les lois naturelles n'auraient plus de secret pour nous, nous ne pourrions connaître la situation qu'approximativement. Si cela nous permet de

prévoir la situation ultérieure avec la même approximation, c'est tout ce qu'il nous faut, nous disons que le phénomène a été prévu, qu'il est régi par des lois ; mais il n'en est pas toujours ainsi, il peut arriver que de petites différences dans les conditions initiales engendrent de très grandes dans les phénomènes finaux ; une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit. »

2. Les systèmes dynamiques

Un système dynamique chaotique est un système déterministe qui montre un comportement aléatoire par sa dépendance et sa sensibilité à ses conditions initiales. Puisque, dans la pratique, les conditions initiales ne peuvent jamais être spécifiées avec une précision infinie, le comportement d'un système chaotique est imprévisible, et donc, comme un bruit [1].

Les applications diverses de cette théorie dans divers domaines de recherche s'accroissent progressivement. Pour obtenir une appréciation d'être à la base du système dynamique non linéaire, la théorie chaotique considère trois types de systèmes dynamiques [3]:

1. Systèmes dynamiques autonomes;
2. Les systèmes dynamiques non autonomes diffèrent des systèmes autonomes parce que le champ de vecteur est une fonction de X et de t , et l'état initial ne peut pas être arbitrairement placé à zéro ;
3. Des systèmes dynamiques de temps discret sont définis par l'équation d'état, $X_{k+1} = g(X_k)$, $k = 0, 1, 2, \dots$, où $X_k \in R^n$ s'appelle l'état, et g trace l'état X_k au prochain état X_{k+1} . Commencant par un état initial X_0 les applications répétées de la carte g provoquent une séquence des points $\{X_k : k = 0, 1, 2, \dots\}$ appelée une orbite du système à temps discret.

La théorie chaotique est basée sur le troisième type du système dynamique lorsqu'elle fonctionne dans l'état chaotique.

3. Les cartes chaotiques les plus utilisées

Un certain nombre de fonctions chaotiques ont été proposé dans la littérature pour la génération de filigrane ; les trois cartes les plus utilisées sont la carte skew tent, la carte de Bernoulli et la carte logistique.

3.1. La carte Skew tent

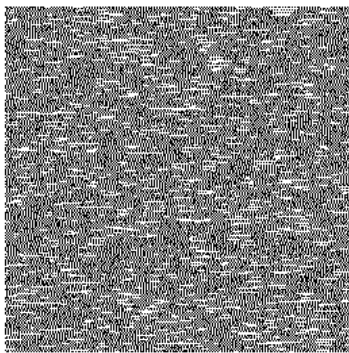
Dans cette section la carte skew tent sera examinée pour l'usage dans le domaine de tatouage, qui peut être exprimée comme suit [4] :

$$h: [0, 1] \rightarrow [0, 1]$$

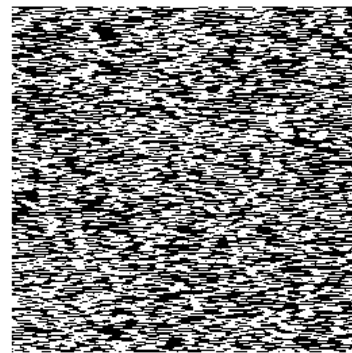
$$h(b) = \begin{cases} \left(\frac{1}{a}\right)b, & 0 \leq b \leq a \\ \left(\frac{1}{1-a}\right)b + \left(\frac{1}{1-a}\right), & a \leq b \leq 1 \end{cases} \quad a \in [0, 1] \quad (I.1)$$

Avec une valeur initiale b_0 , et en variant le paramètre a , des séquences peuvent être produites. On place un seuil, et si un élément de la séquence est plus grand que le seuil, nous remplaçons cet élément par 1 ; autrement, le remplacer par 0. Alors le filigrane bidimensionnel (2D) est constitué en considérant l'une des méthodes de balayage, pour plus d'information consulter l'annexe A.

Sur la figure (I.1) on donne un échantillon bidimensionnel de la carte skew tent produit avec une valeur initiale $b_0 = 0.01$, pour $a = 0.2$ et $a = 0.9$.



a



b

Figure I. 1 : Echantillon de 2D de la carte skew tent produite lorsque $b_0 = 0.01$; (a) : $a=0.2$, (b) : $a = 0.9$.

La séquence est produite lors de l'itération de la fonction chaotique, avec une valeur initiale et une valeur de graine. La séquence produite est alors quantifiée à une séquence

binaire selon un seuil. L'utilisation du balayage Peano (annexe A) à cette séquence peut la convertir en image bidimensionnelle qui peut être utilisée comme un filigrane.

La trajectoire typique $h(k)$ du système dynamique obtenu par l'itération de la carte skew tent, est montrée sur la figure (I.2), pour $a = 0.63$.

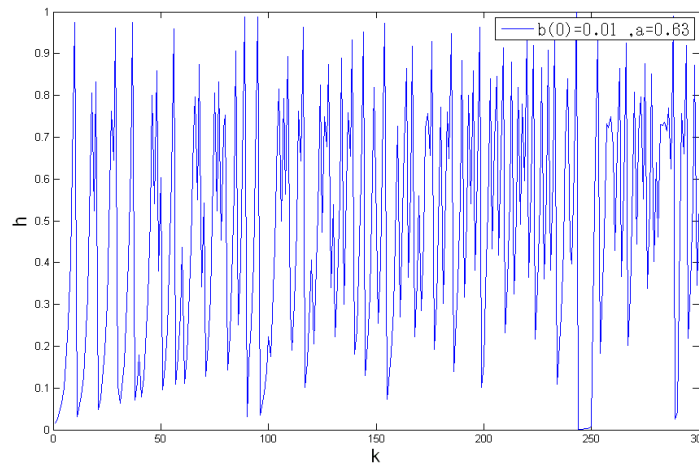


Figure I. 2 : 300 points d'une trajectoire typique du système de la carte skew tent, pour $a = 0.63$

Sa forme d'onde est irrégulière et ça signifie que le système est chaotique. La propriété la plus importante d'un système chaotique est, cependant, la sensibilité aux conditions initiales.

3.2. La carte de Bernoulli

L'utilisation de la carte de Bernoulli à décalage pour la génération de filigrane a été présentée comme alternative aux générateurs pseudo-aléatoires généralement utilisés pour la conception de filigrane. La carte de Bernoulli n-way est définies dans l'intervalle $[0, 1]$ par l'expression suivante [5] :

$$x_{n+1} = Bx_n(\text{mod}1) \quad (I.2)$$

Un exemple de filigrane généré par la carte de Bernoulli pour les deux cas de B ($B = 3$ et $B = 7$) est montré sur la figure (I.3).

Lorsque la valeur de $B = 2$, la carte est désignée sous le nom de la carte de Bernoulli à décalage binaire. La carte de Bernoulli à décalage [6] est définie par l'équation suivante:

$$D(x) = \begin{cases} 2x & \text{si } 0 \leq x \leq \frac{1}{2} \\ 2x - 1 & \text{si } \frac{1}{2} \leq x \leq 1 \end{cases} \quad (I.3)$$

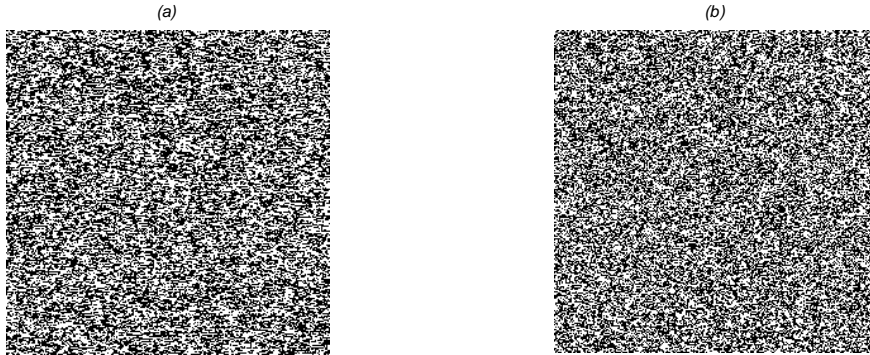


Figure 1.3 : Watermak généré par la carte de Bernoulli ;(a) :n=3 ;(b) :n=7

De la même façon comme les autres cartes chaotiques, une séquence chaotique de filigrane est produite par l'itération de la carte de Bernoulli à décalage. La séquence obtenue à partir de la carte de Bernoulli à décalage est non distingué du bruit blanc, bien que le processus soit complètement déterministe. Pour des petites valeurs de B , les séquences de Bernoulli produites sont caractérisés par les filigranes passe-bas, alors qu'à mesure que B augmente, les caractéristiques passe-bas des séquences de Bernoulli s'affaiblissent et elles tendent vers un spectre blanc, de ce fait convergeant vers des filigranes aléatoires. On peut conclure, donc, que n commande les propriétés spectrales des filigranes chaotiques de Bernoulli. Les séquences les plus passe-bas qui peuvent être produites par l'utilisation des cartes de Bernoulli sont obtenus lorsque $B = 2$. Ceci souvent serait choisi si le système de tatouage va être soumis aux attaques passe-bas [7].

3.3. La carte logistique

La carte logistique est proposée pour modéliser la dynamique d'une population des organisations qui apparaissent dans les générations discrètes, telles que les insectes. La valeur de carte X_{n+1} dépend de son X_n actuel de densité de population avec l'équation logistique donnée par [8] :

$$X_{n+1} = \lambda X_n(1 - X_n) \quad (I.4)$$

Où λ (Lambda) est la fonction de graine, et X_0 est la valeur initiale de la fonction. L'intervalle des valeurs initiales pour la fonction qui doit être utilisée pour produire des

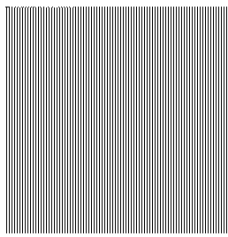
filigranes chaotiques est $[3.5699 \leq \lambda \leq 4]$, souvent connu comme « région chaotique ». Des filigranes peuvent être produits de l'itération de la carte logistique. La séquence résultante est quantifiée pour donner un filigrane binaire-évalué.

On donne sur la figure (I.4) un exemple de la carte logistique générée par les paramètres suivants :

- La région périodique est obtenue lorsque $\lambda = 3.83$ et $X_0 = 0.001$.
- La région à point fixe.

Pour déterminer les points fixes de la carte chaotique $X_n = X_{n+1} \Rightarrow X_n = \lambda X_n(1 - X_n)$

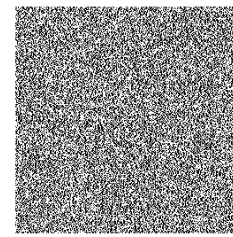
$$\Rightarrow X_n[1 - \lambda(1 - X_n)] = 0 \Rightarrow \begin{cases} X_n = 0 \\ \text{ou} \\ X_n = 1 - \frac{1}{\lambda} \end{cases} \quad (I.5)$$



(a)



(b)



(c)

Figure I. 4 : Filigrane généré par la carte logistique (a) : $y_0=0.001$ et $\lambda=3.83$, (b) : $y_0=0$ et $\lambda=4$, (c) : $y_0=0.1$ et $\lambda=3.98$

Au contraire de la carte skew tent et Bernoulli n-way, la carte logistique demande une précaution lors du choix de la valeur de graine pour la génération du filigrane, dans le sens d'une fausse sélection de la graine peut entraîner la génération d'un filigrane périodique qu'est pas souhaitable.

3.3.1. Sensibilité aux conditions initiales

Une autre propriété importante émerge dans le chaotique, supposant qu'on a trois points initiales qui sont proches, l'évolution de $X(k)$ en fonction de n est montrée sur la figure ci dessous.

Sur la figure (I.5), on remarque, qu'après un certain nombre d'itération les trois courbes se divergent l'une de l'autre. La sensibilité aux conditions initiales est le

problème majeur du chaos, elle empêche toute prédiction sur l'évolution du système au delà d'un certain temps.

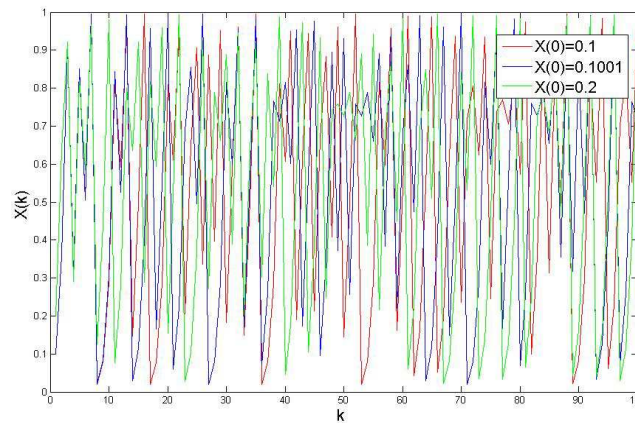
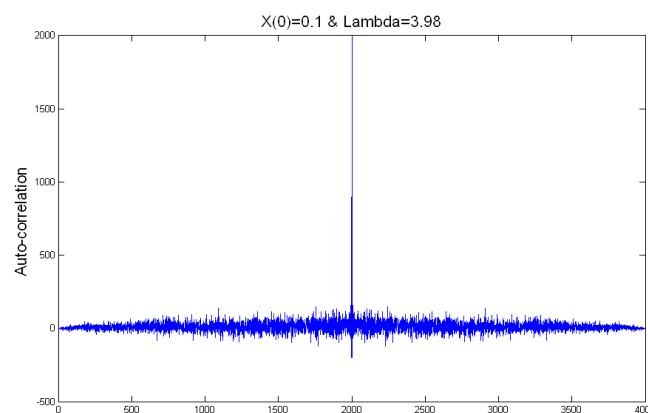


Figure I.5 : Sensibilité de la carte logistique à la valeur initiale (0.1, 0.1001 et 0.2)

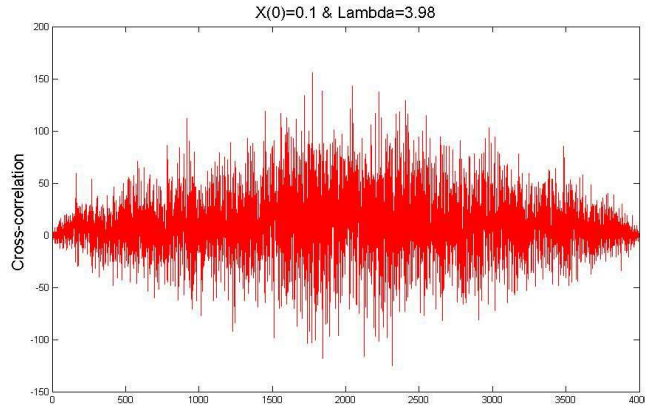
4. Les propriétés de corrélation des séquences chaotiques

Les séquences chaotiques ont des valeurs très faibles de la fonction de corrélation croisée. Les séquences chaotiques permettent également aux utilisateurs dans les systèmes de communication d'obtenir des systèmes de grande sécurité.

Sur la figure (I.6) on montre l'allure de la fonction d'autocorrélation, et de la fonction corrélation croisée pour la séquence générée par les paramètres suivants ($\lambda = 3.98$ et $X(0) = 0.1$).



(a)



(b)

Figure I. 6 : (a) : Fonction d'autocorrélation, (b) : Fonction de corrélation croisée des séquences chaotiques d'une longueur 2000. (Carte logistique)

On remarque que, les signaux chaotiques ont des propriétés fortes d'autocorrélation, avec des corrélations croisées faibles.

5. Diagramme de bifurcation

Qu'est ce que une bifurcation ? Un diagramme de bifurcation est un résumé visuel de la succession du doublement de période produite à mesure que λ s'augmente. La figure suivante montre le diagramme de bifurcation de la carte logistique, le long de l'axe des abscisses λ . Pour chaque valeur de λ le système est d'abord permis de s'installer et alors les valeurs successives de X sont tracées pour quelques centaines d'itérations [5].

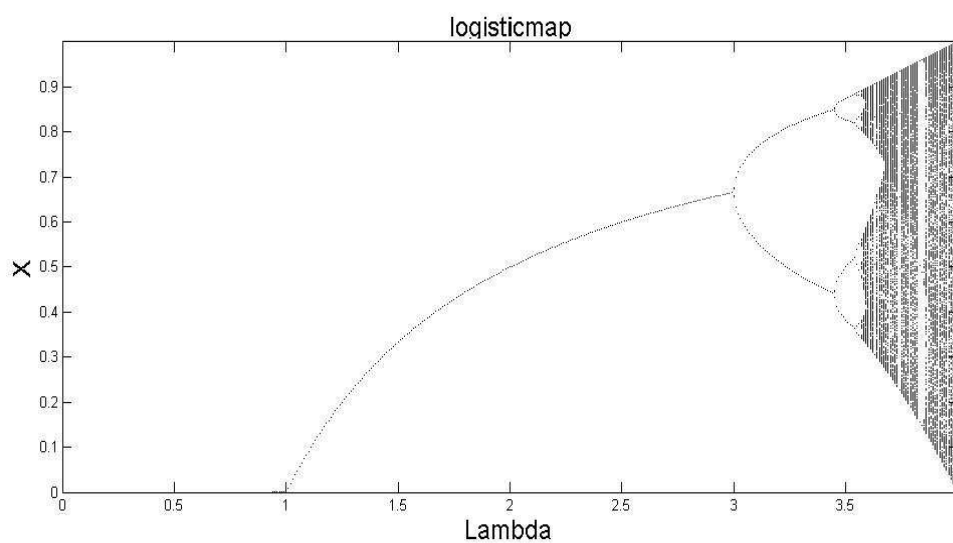


Figure I. 7 : Diagramme de bifurcation de la carte logistique (λ entre 0 et 4)

On remarque que :

- ✓ Pour λ est inférieur à 1, tous les points sont tracés à zéro. Zéro est un point attracteur.
- ✓ Pour λ entre 1 et 3, nous avons un attracteur à un-point, mais la valeur de l'attracteur X s'augmente lorsque la valeur de λ augmente aussi.
- ✓ La bifurcation se produise à $\lambda = 3$, et $\lambda = 3.45, 3.54, 3.564, 3.569$ (approximativement).
- ✓ Jusqu'à 3.57, le système est chaotique.
- ✓ Cependant, le système n'est pas chaotique pour toutes les valeurs de λ supérieur à 3.57. Lorsque la valeur de λ est supérieur à 3.57, un nombre restreint de valeur de X sont visités. Ces régions produisent « l'espace blanc » dans le diagramme.
- ✓ Autour $\lambda = 3.83$ on trouve un attracteur à trois points.
- ✓ En fait, entre 3.57 et 4 il y a un interfoliage (interleaving) riche de chaos et de séquence.

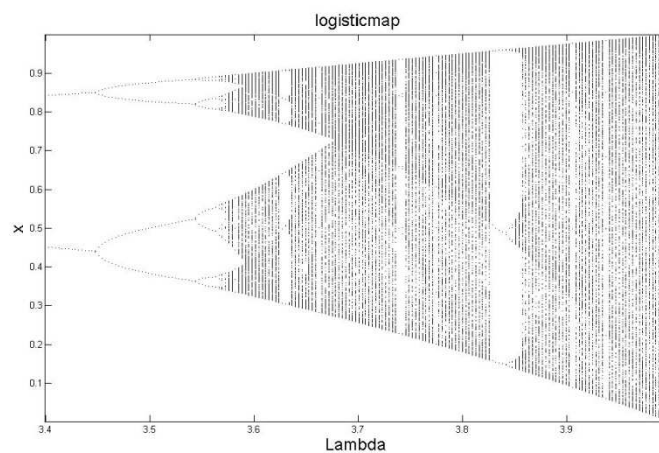


Figure I. 8 : Diagramme de bifurcation de la carte logistique (λ entre 3.4 et 4)

En conclusion, un petit changement de la valeur de λ peut rendre le système stable chaotique, et vice versa.

6. Application du Chaos dans le domaine du tatouage numérique

L'idée d'utiliser les signaux chaotiques pour transmettre l'information est apparue dans le début des années 90 [1]. La majorité des filigranes présentés dans la littérature jusqu'à présent sont produites à base des générateurs de nombre pseudo-aléatoire. Cependant, les séquences produites par l'itération des cartes chaotiques constituent une alternative efficace aux séquences pseudo-aléatoires de filigrane. Les séquences peuvent être produites par l'itération d'une fonction chaotique, qui a été définie avec une fonction de graine (seed function) et une valeur initiale, et cette séquence peut être quantifiée pour construire un filigrane binaire.

Ces dernières années, des cartes chaotiques ont été utilisées pour le tatouage numérique, pour augmenter la sécurité de ces systèmes [7], [8], [9]. Les propriétés les plus importantes du chaos dans la dissimulation de l'information sont sa sensibilité extrême aux conditions initiales. Ces caractéristiques spéciales font appel aux cartes chaotiques présentant d'excellents candidats pour le tatouage et la cryptographie, basés sur la condition du Shannon classique de la confusion et de la diffusion.

7. Avantage des séquences chaotiques

Les séquences chaotiques sont faciles à produire et à stocker, l'expression mathématique de la carte chaotique et un état initial sont nécessaires pour leur génération, ainsi il signifie qu'il n'y a aucun besoin de stockage de la longue séquence. L'avantage principal des séquences chaotiques est qu'elles sont facilement contrôlables les propriétés spectrales/corrélation, dans la réalité, fait une bonne alternative aux signaux pseudo-aléatoires utilisés couramment [10].

Les filigranes chaotiques peuvent être insérées dans le domaine temporel/spatial ou dans un domaine transformé où leur corrélation/propriétés spectrales peut être exploitée plus efficacement pour obtenir des séquences robustes de tatouage.

8. Filigrane à base de cartes chaotiques

La majorité des générateurs de séquences utilisent un générateur de nombre pseudo-aléatoire pour produire un filigrane. Le filigrane à base de carte chaotique s'est avéré une alternative à cette.

Les systèmes chaotiques peuvent être utilisés pour produire des nombres pseudo-aléatoires. Dans plusieurs articles, les auteurs ont proposé un générateur de nombre pseudo-aléatoire dérivé par chaos [11].

La génération de filigrane par l'utilisation de la carte chaotique a été présentée vers les années 90 par Voyatzis et al. [12]. En 2000, Nikolaidis et al. [8] ont utilisé deux fonctions chaotiques, à savoir, la carte de n-way de Bernoulli et n-way séquence de la queue (tailed sequence). La première carte chaotique est utilisée pour mélanger l'image binaire du filigrane avant qu'il soit inséré dans l'image numérique. La deuxième fonction chaotique est appliquée pour la génération des séquences du filigrane. Une comparaison entre les différentes cartes chaotiques avec leurs applications au tatouage d'image a été faite par Nikolaidis et al. [8]. Tefas et al. [9] ont introduit la carte skew tent dans leur système de tatouage. Après cette période, l'utilisation de la carte chaotique a trouvé une grande utilisation dans le domaine de la génération du filigrane [13].

Conclusion

Dans ce chapitre nous avons abordé un certain nombre de notions de base de la théorie des systèmes chaotiques. Quelques cartes chaotiques qui permettent la génération du filigrane ont été citées, et on a discuté les propriétés les plus importantes telles que ; la sensibilité aux conditions initiales et l'aspect aléatoire ; qui sont les points attirant des chercheurs afin de les utiliser dans divers domaines comme le traitement du signal, d'image pour le cryptage et le tatouage numérique...etc.

Bibliographie

- [1] T. Schimming, Statistical analysis and optimization of chaos based broadband communications, Thèse de Doctorat, Ecole Polytechnique Fédérale de Lausanne, 2002.
- [2] M.W. Lee, Etude des comportements chaotiques en modulation de cohérence et application à la cryptographie, Thèse de Doctorat, Université de Franche-Comté, 2002.
- [3] A. Mooney, The generation and detection of chaos-based watermarks, Thèse de Doctorat, Nuimaynooth University, 2005.
- [4] A. Tefas, N. Nikolaidis, I. Pitas, Chaotic watermark sequences for correlation-based schemes, In Proceedings of 12th European signal processing conference EUSIPCO, Vienna, Austria, 1891–1894, 2004.

- [5] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, I. Pitas, Statistical analysis of a watermarking system based on Bernoulli chaotic sequences, *Signal Processing*, 81, 1273-1293, 2001.
- [6] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, and I. Pitas, Bernoulli shift generated watermarks: Theoretic investigation, *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, 3, 1989–1992, 2001.
- [7] Z. Dawei, C. Guanrong, and L. Wenbo, A chaos based robust wavelet domain watermarking algorithm, *Chaos, Solitons & Fractals*, 22, 47–54, 2004.
- [8] A. Nikolaidis and I. Pitas, Comparison of different chaotic maps with application to image watermarking, *IEEE International Symposium on Circuits and Systems*, 5, 509–512, 2000.
- [9] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, Markov chaotic sequences for correlation based watermarking schemes, *Proceedings of Chaos, Solitons and Fractals*, 17, 567–573, 2003.
- [10] C.P. Silva and A.M. Young, Introduction to Chaos-Based Communications and Signal Processing, *IEEE Aerospace Conference Proceedings*, 1, 279-299, 2000.
- [11] L. Kocarev and G. Jakimoski, Pseudorandom bits generated by chaotic maps, *IEEE Transactions On Circuits And Systems—I: Fundamental Theory And Applications*, 50(1), 123-126, January 2003.
- [12] G. Voyatzis, I. Pitas. Chaotic watermarks for embedding in the spatial digital image domain, *IEEE Proceedings of Image Processing*, 432–436, 1998.
- [13] J. Zhang and L. Tian, A new watermarking method based on chaotic maps, *IEEE Proceedings of Multimedia and Expo Conference*, 2, 939–942, 2004.

Chapitre II : Généralités sur le tatouage d'images numériques

Introduction

La protection des données numériques et l'application des droits de propriété intellectuelle sont devenues une question pertinente dans le monde numérique lorsque les systèmes sont connectés à l'internet. Le tatouage numérique aide les propriétaires en affirmant leurs droits de propriété intellectuels sur les œuvres d'art qu'ils créent. Il est difficile à imposer ces droits avec des images numériques, puisqu'il est facile de copier et distribuer les copies parfaites d'une image originale. Dans ce chapitre, nous présentons des généralités sur la notion du tatouage. Un état de l'art sur les techniques du tatouage existantes, les principes de conception d'une technique de tatouage, et quelques unes de ses applications, les plus utilisées sont ensuite étudiés. Enfin les méthodes d'évaluation des algorithmes du tatouage en prenant en considération des mesures objectives et subjectives de la qualité de l'image tatouée ainsi que les éventuelles attaques sont exposés.

1. Historique du tatouage

Le tatouage numérique est une technique qui consiste à insérer des informations numériques (marque ou signature) de manière imperceptible et indélébile dans le corps même d'un autre document numérique. Le tatouage des documents est un domaine récent qui s'apparente à la stéganographie [1]. La cryptographie et la stéganographie sont des techniques qui répondent à des problèmes de sécurité. Elles sont destinées à transmettre une information à caractère confidentiel.

La cryptographie consiste à transformer un message pour qu'il devienne illisible. La connaissance de la clef et de l'algorithme de cryptage permet de décoder le message afin de le rendre lisible. Cette technique a pour but de protéger le document pendant sa transmission.

La stéganographie consiste à cacher, de manière subliminale, un message secondaire dans un message primaire. Le message primaire reste lisible à tous, tandis que le

message secondaire n'est pas lisible que par une ou plusieurs personnes propriétaires d'une information secrète [2].

1.1. Le tatouage numérique

Le tatouage numérique est le processus d'inclure ou de cacher un signal, appelé le filigrane, dans un autre signal, d'une manière robuste et au même temps imperceptible. Le signal hôte peut être une image, son, vidéo ou un document de texte (par exemple, code source de programme).

1.2. Éléments d'un système de tatouage

Un système de tatouage est défini comme un système de communication se compose de trois éléments principaux : un émetteur, une voie de transmission, et un récepteur comme le montre la figure (II.1). Pour être plus spécifique, l'insertion d'information à être cachée dans le signal joue le rôle de la transmission de données ; le traitement appliqué aux données de système hôte après la dissimulation de l'information, avec l'interaction entre les données cachées et les données de système, représente la voie de transmission; la détection d'information cachée des données dans le système agit la partie du récepteur. L'information à cacher dans les données de système hôte représente l'entrée même du système [3].

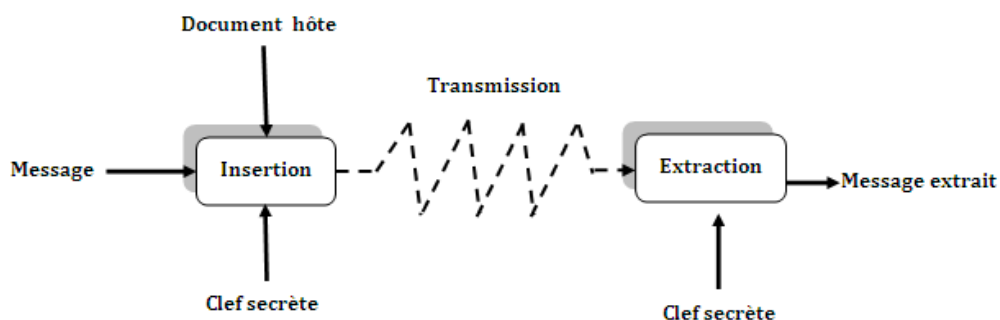


Figure II. 1 : Transmission d'un message par le tatouage d'un document

1.3. Le processus du tatouage

Le schéma du tatouage numérique est résumé sur la figure (II.2) : un message m contenant L bits d'information est transformé selon une clef k en un filigrane w qui est ensuite inséré dans le document x (appelé "hôte") pour donner un document tatoué y . C'est la phase d'insertion. Ici, w est exprimé sous la forme d'un bruit qui est ajouté au document, la déformation dépendant de la puissance du bruit. k est secrète et spécifique

au tatoueur y est ensuite copié et attaqué, ce qui est modélisé par la transmission dans un canal soumis au bruit. Le document reçu est appelé z

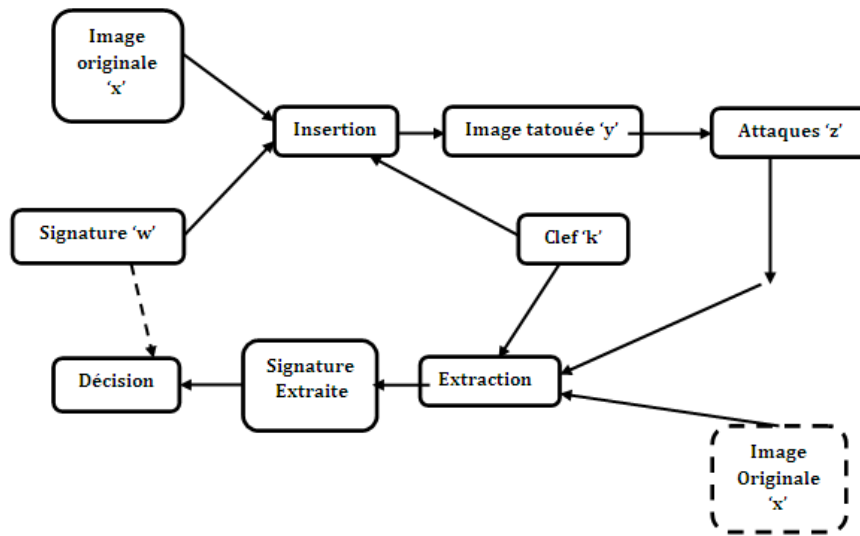


Figure II. 2 : Modèle général du processus d'insertion et de détection

La réception d'un document consiste en deux parties : d'une part, la détection du filigrane et d'autre part, s'il est présent, son décodage. La phase de détection consiste à prouver la présence d'un tatouage dans z grâce à la clef k [4].

2. Types de filigrane

Les types de filigrane les plus utilisés sont discutés dans les sections suivantes. Il y a deux types principaux de filigrane, à savoir : les filigranes visibles et invisibles.

2.1. Logos et images

Les logos et les images sont les filigranes utilisés particulièrement pour les systèmes de tatouage visible. La majorité de stations de télévision utilisent le logo de stations perceptible.



Figure II. 3 : Image de logo : (a) : Logo de l'université de Batna ;(b) : Logo d'Air Algérie ;(c) : Logo de la Télévision Algérienne

2.2. Filigranes pseudo-aléatoires

La majorité des générateurs de séquence de filigrane proposés jusqu'à présent utilisent un générateur de nombre pseudo-aléatoire pour créer une séquence de filigrane [5], [6], [7]. Ces séquences de filigrane sont normalement incluses d'une façon imperceptible dans l'image hôte. Ces séquences peuvent être modélisées en tant que des variables aléatoires indépendants, et identiquement distribuées (I.I.D.) obéissant à une distribution uniforme. Les séquences ont des propriétés comme le bruit blanc. Une seule graine (seed) reproduira la même séquence des nombres à chaque fois. La séquence des nombres produits est habituellement convertie à l'un des deux nombres (0 et 1) pour donner un filigrane binaire.

2.3. Filigranes chaotiques

Les filigranes chaotiques se rapportent à ceux qui sont produits par l'itération récursive d'une certaine fonction chaotique [8], [9]. La génération de filigrane basée sur l'utilisation des fonctions chaotiques a été précédemment suggérée, avec la carte logistique, la carte skew tent, la carte du décalage de Bernoulli, la carte de Henon ...etc. Sur la figure ci-dessous on donne un exemple de quelques filigranes chaotiques.

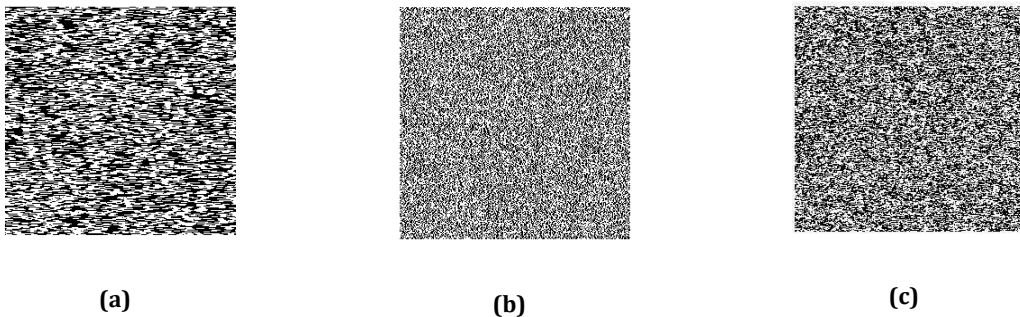


Figure II. 4 : (a): La carte Skew tent (0.9); (b): La carte logistique ($y_0=0.1$ et $\lambda=3.98$) ; (c): La carte de Bernoulli ($n=3$)

3. Les propriétés d'un filigrane

Les caractéristiques désirées des filigranes sont énumérées ci-dessous [10]:

- ✓ Difficile à noter

Les filigranes invisibles, également désignés sous le nom des filigranes imperceptibles, sont invisibles à l'œil humain, et qui ne dégrade pas la qualité du

contenu. Ils ont un avantage par rapport aux filigranes perceptibles du fait leur endroit n'est pas connu à un attaquant.

✓ Robustesse

Généralement un filigrane doit être robuste aux transformations qui incluent les distorsions communes de signal comme les conversions de D/A et de A/D et la compression avec perte. D'ailleurs, pour les images et la vidéo, il est important que le filigrane survive à des distorsions géométriques telles que la translation, le changement d'échelle (scaling) et le découpage (cropping)...etc.

✓ Résistance aux zones altérées (Tamper-resistance)

Aussi le filigrane doit être robuste pour résister aux déformations de signal, un filigrane peut également être soumis au traitement des signaux qui est seulement prévu pour enlever le filigrane.

✓ Filigrane privé

Un filigrane privé où le décodeur exige la connaissance du contenu non tatoué ou la séquence pseudo-aléatoire de bruit qui constitue le filigrane, qu'est seulement connue à l'émetteur et au récepteur, sont plus résistants que les filigranes publics dans lesquels tout le monde est libre de décoder le filigrane.

✓ Encodeur/décodeur asymétriques

Le déplacement d'un filigrane public exige d'inverser le codage, alors il est fortement souhaitable de faire un encodeur complexe le plus possible, particulièrement si le filigrane doit être appliqué seulement une seule fois. Cependant si les décodeurs doivent fonctionner en temps réel, alors il est nécessaire pour que le processus de décodage soit plus simple que le codage.

✓ Débit de bit

Le débit de bit d'un filigrane se rapporte à la quantité de l'information qu'un filigrane peut coder dans un signal. C'est particulièrement important pour les filigranes publics.

✓ Modification et filigranes multiples

Dans quelques circonstances, il est souhaitable d'altérer le filigrane après son insertion. Par exemple, dans le cas des disques de vidéo numérique, un disque peut être tatoué pour permettre seulement une seule copie. Une fois que cette copie a été tirée, il est alors nécessaire d'altérer le filigrane sur le disque original pour interdire d'autres copies. Le changement d'un filigrane peut être accompli : (a) enlevant le 1^{er} filigrane et puis ajoutant un nouveau filigrane ou (b) insérer un 2^{ème} filigrane.

✓ Universel

Le même filigrane numérique devrait s'appliquer à chacun des trois médias à l'étude. C'est potentiellement utile dans le tatouage des produits de multimédia. Egalement cette propriété favorise l'implémentation du tatouage le son/d'image/vidéo sur un matériel commun.

✓ Intervention humaine minimum

L'insertion du filigrane devrait exiger la moindre intervention humaine.

4. Les contraintes d'un système de tatouage

Les contraintes rencontrées dans un système de tatouage sont larges et parfois contradictoires.

Dans chaque système de tatouage il y a une contradiction entre l'imperceptibilité, la robustesse et la capacité du système. Cette contradiction peut être représentée comme le montre la figure suivante [11], [12].

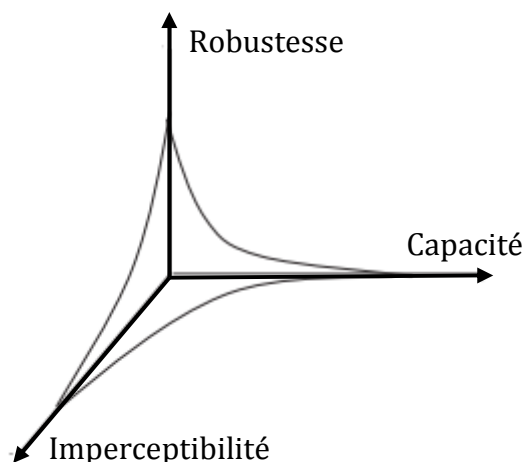


Figure II. 5 : Les éléments contradictoires d'un système de tatouage

4.1. Transparence (invisibilité)

Ceci se rapporte à la similitude perceptuelle entre l'image tatouée et l'image originale. Le filigrane devrait être imperceptible. Il signifie qu'aucun effet visuel ou audio ne devrait être perçu par l'utilisateur. Le filigrane ne devrait pas dégrader la qualité du contenu, mais dans quelques applications nous pouvons accepter un peu de dégradation pour avoir une robustesse plus élevée.

4.2. Robustesse

Le filigrane doit résister aux attaques qui sont visées directement l'information incluse. Il ne doit pas être possible qu'un attaquant supprime le filigrane sans rendre les données de multimédia inutilisables. Particulièrement il ne doit pas être possible de rechercher ou même modifier le filigrane sans connaissance de la clef secrète de filigrane.

4.3. Capacité

Un système de tatouage doit tenir compte d'une quantité de l'information utile pour être inclus dans une image. La capacité utile de données dans le tatouage d'image signifie le nombre de bit codé avec l'image. La capacité utile d'information incluse de filigrane doit être suffisante pour permettre l'application envisagée.

D'une façon générale, la condition de capacité lutte toujours contre deux autres conditions importantes qui sont : l'imperceptibilité de filigrane et la robustesse de filigrane.

5. Les techniques du tatouage

Plusieurs méthodes de tatouage existent, elles diffèrent selon l'application et les contraintes qu'elles exigent.

5.1. Méthodes d'insertion d'un filigrane

Trois formules pour l'insertion du filigrane sont énumérées ci-dessous [11].

L'approche additive, est l'une des méthodes la plus utilisée généralement, le signal tatoué I_w est obtenue en ajoutant tout simplement le filigrane w pondéré avec un facteur α aux échantillons du signal hôte I par l'utilisation de la formule suivante :

$$I_w = I + \alpha w \quad (II.1)$$

Dans l'approche de l'insertion multiplicative, le filigrane est multiplié par le signal hôte et le facteur d'insertion α :

$$I_w = I(1 + \alpha w) \quad (II.2)$$

Enfin, une approche non linéaire de l'insertion définit par la fonction exponentielle est défini comme suit :

$$I_w = Ie^{\alpha w} \quad (II.3)$$

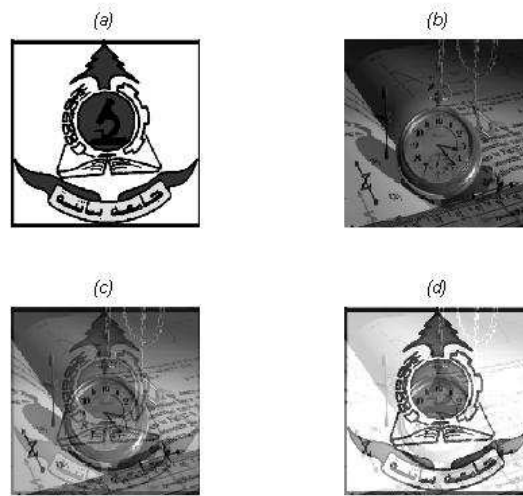


Figure II. 6 : Tatouage additive dans le domaine spatial : (a) : Le logo de l'université de Batna ; (b) : Image originale Watch ;(c) : Image tatouée avec $\alpha = 0.2$;(d) : Image tatouée avec $\alpha = 0.7$

Dans le domaine spatial l'image est représentée par des pixels. Un exemple d'un tatouage spatial de base, qui consiste à placer un logo dans une image pour l'identifier par l'utilisation de l'équation (II.1) avec un facteur d'insertion $\alpha = 0.2$, et $\alpha = 0.7$ est illustré sur la figure (II.7) :

Nous pouvons dire, lorsque la valeur du facteur d'insertion s'augmente, le filigrane devient plus visible.

Dans le cas d'une insertion multiplicative dans le domaine spatial, on peut voir de l'équation (II.2) qu'il y a une très grande dépendance au facteur d'insertion par rapport au cas d'insertion additive.

On remarque sur la figure ci-dessous, qu'il ya une grande différence au niveau de la visibilité du filigrane lorsque la valeur d'insertion est la même, mais les méthodes d'insertion sont différentes. Une valeur basse du facteur d'insertion dans la méthode additif peut donner des résultats similaires à des valeurs plus élevées dans le cas de d'insertion multiplicative.

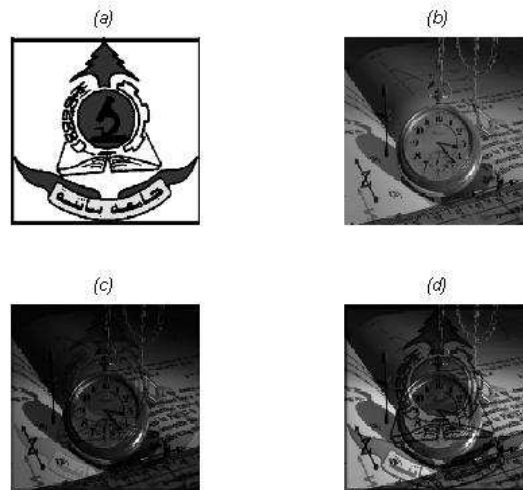


Figure II. 7 : Tatouage multiplicative dans le domaine spatial : (a) : Le logo de l'université de Batna ; (b) : Image originale Watch ;(c) : Image tatouée avec $\alpha = 0.2$;(d) : Image tatouée avec $\alpha = 0.7$

5.2. Méthode de détection du filigrane

Les trois clefs d'un système de tatouage sont: la méthode de la génération du filigrane, l'algorithme d'insertion du filigrane et l'algorithme de la détection ou l'extraction du filigrane. Selon le processus d'extraction du filigrane, les techniques de détection peuvent être divisées en trois types [13]:

- Non aveugle

Les schémas non aveugles de tatouage exigent l'image originale et la clef secrète pour la détection de filigrane, et ce type d'algorithme n'est pas robuste.

- Semi aveugle

Les schémas de semi aveugle exigent la clef secrète et les bits de la séquence du filigrane pour l'extraction ou la détection du filigrane.

- Aveugle

Les schémas aveugles ont besoin seulement des clefs secrètes pour l'extraction ou la détection du filigrane.

5.3. Domaines de tatouage

Il est possible d'ajouter un filigrane à l'image numérique soit dans le domaine spatial ou le domaine transformé par l'utilisation d'une technique additive d'insertion ou multiplicative.

Selon le domaine d'insertion du filigrane, les techniques de tatouage peuvent être divisées en deux types :

- Techniques de tatouage dans le domaine spatial ;
- Techniques de tatouage dans le domaine fréquentiel.

Dans le domaine spatial, les techniques d'insertion du filigrane est fait sur des pixels d'image tandis que dans le domaine fréquentiel les techniques d'insertion sont fait après la prise de la transformée de l'image. Généralement les méthodes de domaine fréquentiel sont plus robustes que les techniques du domaine spatial.

5.3.1. Domaine spatial

C'est la manière la plus simple d'insertion d'un filigrane dans l'image originale. En général une signature pseudo-aléatoire de bruit est produite par une clef. La signature est pondérée puis ajoutée à l'image hôte.

Des filigranes visibles sont habituellement incluent dans le domaine spatial, c.à.d, directement sur les valeurs de pixel d'une image [14], [15].

5.3.2. Domaine transformé

Beaucoup d'approches, pour lesquelles des filigranes sont insérés dans le domaine transformé basé sur la transformée en cosinus discrète (DCT), la transformée de Fourier discrète (DFT), ou la transformée par ondelettes discrète (DWT) sont cités ci dessous.

- Le domaine DCT

L'image dans le domaine transformé est représentée en termes de ses fréquences. Le domaine de DCT est utilisé couramment dans les systèmes du tatouage d'image numérique et de vidéo, en raison de son utilisation dans le JPEG et les normes MPEG.

L'ajout du filigrane aux coefficients de basse fréquence de la DCT peut causer une déformation perceptuelle visible, cependant l'insertion du filigrane dans les coefficients haute fréquence sont vulnérable à la compression JPEG et MPEG. Les coefficients de fréquence moyenne sont le choix dominant pour la plupart des algorithmes existants de tatouage dans le domaine de DCT [16].

Plusieurs schémas basés sur DCT sont présentés dans [11], [17], [18], [19], [20]. L'application d'une DCT sur une image peut facilement être divisée en de pseudo bandes de fréquence de sorte que le filigrane puisse commodément être inséré dans les fréquences de bande moyennes les plus importantes.

Le tatouage dans le domaine de DCT peut être classifié en deux classes : la DCT est appliqué sur l'image complet et lorsque l'image est divisée en des blocs de taille 8×8. Les premiers algorithmes présentés par Cox et al. [11] utilisent une approche globale de DCT noté par étalement du spectre pour l'insertion d'un filigrane robuste dans la partie perceptuel significative du système visuel humain (HVS).

En 1997 Cox et al. ont présenté un article intitulé « Secure Spread Spectrum Watermarking for Multimedia » [11], l'un des articles les plus cités (cité 5815 fois jusqu'à 2013 selon la recherche de Google Scholar), et ensuite la plupart des efforts de recherches sont basés sur ce travail.

La question demeure toujours qu'elles sont les coefficients qui vont changer et comment ?. Cox et autres utilisent les 1000 coefficients de plus grandes valeur pour insérer une séquence de filigrane de longueur 1000. La seule exception est le coefficient DC, située au coordonnés (0.0) de la matrice de DCT, qui ne devrait pas être changé due à son influence perceptible sur la qualité de l'image. D'une part, les coefficients de hautes fréquences sont facilement changés sous des attaques communes telles que la compression. Néanmoins, l'auteur propose de ne pas changer les coefficients proches à DC due à leur influence. Sur la figure (II.8) et (II.9) nous montrons le processus général de l'insertion et de la détection de filigrane qui a été proposé par Cox et al. [11].

Cox et autres donnent l'équation (II.4) pour vérifier la similarité entre le filigrane extrait x^* et la séquence originale x .

$$sim(x, x^*) = \frac{x^*.x}{\sqrt{x^*.x}} \quad (II.4)$$

Lorsque la DCT est appliquée sur l'image complète, alors n'importe quel changement des coefficients de transformation affecte l'image entière ; pour couvrir cet inconvénient l'image originale est divisé en des blocs 8×8 DCT pour l'insertion du filigrane [21].

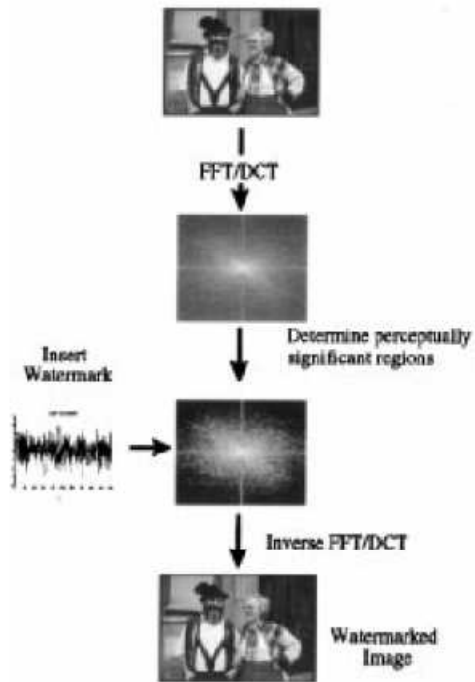


Figure II. 8 : Etapes du procédé d'insertion du filigrane [11]

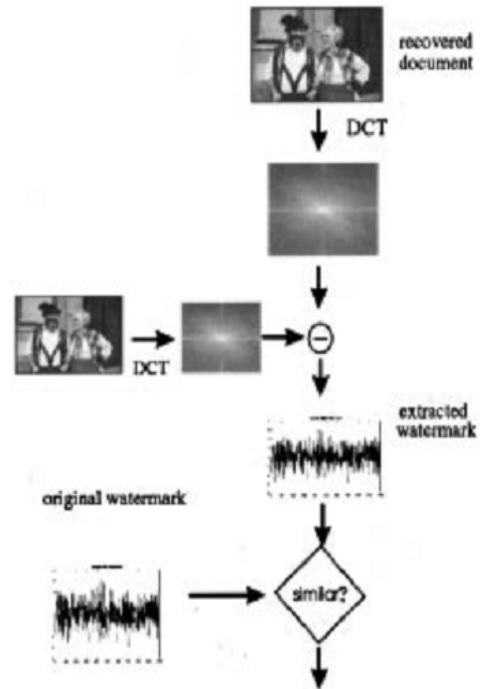


Figure II. 9 : Etapes du procédé d'extraction [11]

- Domaine d'ondelette

DWT a une localité spatiale de fréquence, qui signifie si le signal est inclus il va affecter l'image localement [22]. Il est bien connu que la DWT ait l'avantage de la multi résolution et de la bonne localisation dans le domaine de fréquence spatiale, et elle est également utilisée dans le codage de l'image/vidéo dans la norme JPEG2000 et MPEG7.

Xia, Boncelet, et Arce [23] ont proposé un schéma de tatouage basé sur la transformation par ondelettes discrète (DWT). Le filigrane, modélisé en tant que bruit Gaussien, a été ajouté aux bandes moyennes et à haute fréquence de l'image. Le processus de décodage prenant la DWT de l'image tatouée. Des sections du filigrane ont été extraites et corrélées avec des sections du filigrane original. Si la corrélation croisée était au-dessus d'un seuil, alors le filigrane a été détecté. Autrement, l'image est décomposée en des bandes plus fin jusqu'au filigrane entier et extrait est corrélées avec le filigrane original.

5.3.3. Domaine hybride

Dans ce domaine, les chercheurs se concentrent sur de mixer le domaine spatial et du domaine transformé (c.à.d, combinaisons de DFT, de DWT et de DCT) et appliquer également le modèle mathématique et statistique, et d'autres approches disciplinaires dans le tatouage : par exemple utilisation de la théorie du chaos, le codage d'image fractale ...etc.

Zhao et al. [24] présentent une technique duelle de tatouage de domaine pour l'authentification d'image et la compression d'image. Ils utilisent le domaine de DCT pour la génération de filigrane et le domaine de DWT pour l'insertion de filigrane. Ils utilisent l'orthogonalité du domaine de DCT-DWT pour le tatouage.

6. Evaluation des algorithmes du tatouage

L'évaluation d'un processus de tatouage se fait en mesurant leur tendance vers le cahier de charge idéal, c'est à dire avoir un meilleur compromis robustesse/invisibilité. Donc il faut d'une part que l'image tatouée soit de la même qualité que l'image originale et les attaques pour lesquelles le tatouage doit être robuste, doivent conserver la qualité de l'image [25].

La première constatation est qu'il n'existe aucune méthode automatique pour mesurer la qualité absolue d'une image. Aucun algorithme n'est capable, sans image de référence, de dire qu'une image est de bonne ou de mauvaise qualité. Cependant, dans le cadre de nos applications, cette contrainte n'est pas restrictive puisque l'image originale peut nous servir de référence. La mesure de qualité des images est donc une mesure de distance entre deux images. Les mesures de distances les plus simples comparent les deux images pixels par pixels. Elles sont fondées sur la différence entre les deux images ou sur des corrélations entre ces images. Les mesures de distorsion les plus populaires en traitement d'image et la compression étant tout simplement le rapport signal sur bruit (SNR: Signal to Noise Ratio) et le (PSNR: Peak Signal to Noise Ratio). Ces rapports sont mesurés en décibels (dB) à partir des relations suivantes [26] :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (II.5)$$

MSE (Mean Square Error) est l'erreur carrée moyenne entre les images originales et tatouées est définies comme suit:

$$MSE = \frac{1}{M.N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - I_w(i,j))^2 \quad (II.6)$$

Où $I(i,j)$ est la valeur du pixel (i,j) de l'image référence et $I_w(i,j)$ celle de l'image à tester, les deux images étant de taille $m \times n$.

Si ces mesures quantifient bien les dégradations par ajout de bruit, leurs applications dans notre cadre de travail posent différents problèmes. Les plus évidents concernent par exemple les transformations affines : si on fait subir une symétrie à une image, le PSNR entre l'image modifiée et son original pourra être très bas alors que l'image n'est pas modifiée. On ne peut pas donc utiliser ces mesures de manière systématique. On peut observer aussi que ces mesures n'intègrent pas dans le calcul les comportements des voisinages des pixels traités et qu'aucun comportement fréquentiel n'est pris en compte.

Différents outils psychovisuels permettant de noter la qualité d'une image dégradée par rapport à une image originale existent dans la littérature [27]. Ces outils sont très proches de ceux utilisés en tatouage psychovisuel, ils sont basés sur les mêmes modélisations du Système Visuel Humain (SVH). On peut, en utilisant ces outils, pour assurer qu'une image est de bonne qualité ou non.

Les mesures	Les formules
Différence Maximum	$DM = \max_{m,n} I_{m,n} - I_{m,n}^* $
Différence Moyenne Absolue	$AD = \frac{1}{MN} \sum_{m,n} I_{m,n} - I_{m,n}^* $
Différence Moyenne Absolue Normalisée	$NAD = \frac{\sum_{m,n} I_{m,n} - I_{m,n}^* }{\sum_{m,n} I_{m,n} }$
L ^p -Normal	$L^p = \left(\frac{1}{MN} \sum_{m,n} I_{m,n} - I_{m,n}^* ^p \right)^{1/p}$
Erreur Moyenne Quadratique Laplacien	$LMSE = \frac{\sum_{m,n} (\nabla^2 I_{m,n} - \nabla^2 I_{m,n}^*)^2}{\sum_{m,n} (\nabla^2 I_{m,n}^*)^2}$
Fidélité de l'image	$IF = 1 - \frac{\sum_{m,n} (I_{m,n} - I_{m,n}^*)^2}{\sum_{m,n} I_{m,n}^2}$
Rapport Signal sur Bruit	$SNR = \frac{\sum_{m,n} I_{m,n}^2}{\sum_{m,n} (I_{m,n} - I_{m,n}^*)^2}$

Tableau II. 1: Métriques de distorsion basées sur la différence entre l'image originale et tatouée

Le tableau (II.1) représente d'autres mesures de distorsion utilisées dans la littérature. Ces mesures sont basées aussi sur le calcul de la différence entre l'image originale et tatouée (attaquée ou non attaquée) [27], [28].

7. Classification des attaques

Une attaque est n'importe quelle tentative (malveillante ou coïncidente) d'empêcher un système de tatouage. La sécurité d'un filigrane se rapporte à sa capacité de résister à des attaques hostiles. Selon l'application et les conditions de tatouage, une liste de déformations et les attaques qui peuvent avoir lieu sont cités ci-dessous [29], [30]:

- Compression avec perte

Beaucoup d'algorithmes de compression comme le JPEG et le MPEG peuvent potentiellement dégrader la qualité des données par la perte non récupérable de données.

- Distorsions géométriques

Les distorsions géométriques sont spécifiques aux images et aux vidéos et incluent des opérations telles que la rotation, la translation, et le découpage (cropping), comme le montre la figure ci-dessous :

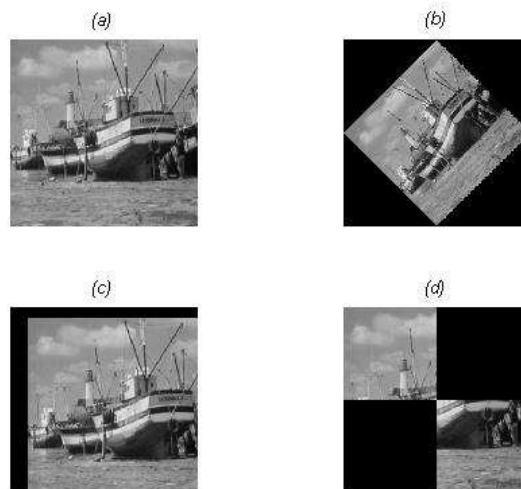


Figure II.10 : Les transformations géométriques ; (a) : Image originale ;(b) : La rotation ;(c) : La translation ;(d) : Le découpage

- Opérations communes de traitement des signaux

Elles incluent :

Conversion de D/A ; Conversion de A/D ; Rééchantillonnage ; Requantization ; Dithring ; Récompression ; Filtrage linéaire tel que le filtrage passe haut et passe bas ; filtrage non

linéaire tel que le filtrage médian ; Réduction de couleur ; Addition de bruit Gaussien et non Gaussien et échange local des pixels.

D'autres attaques intentionnelles ;

- Impression et le rescane (rescanning) ;
- Tatouage d'image tatouée (rewatermarking) ;
- La collusion

Plusieurs utilisateurs malhonnêtes produisent une copie piratée à partir de leurs exemplaires.

- Contrefaçon (forgery).

Un certain nombre de destinataires autorisés de l'image ne devraient pas pouvoir s'entendre pour former une copie d'image tatouée avec le filigrane incorporé valide d'une personne qui n'est pas dans le groupe.

- L'attaque IBM

Il ne devrait pas être possible de produire un original faux qui exécute également comme l'original et a également comme conséquence l'extraction du filigrane comme réclamée par le support de l'original faux.

L'Unzign et le Stirmark ont montré le succès remarquable pour enlever des données incluses par des programmes disponibles dans le commerce [2].

8. Applications du tatouage numérique

Le souci primaire du tatouage numérique était la protection du copyright. Cependant, les avancées récentes dans l'ordinateur et les technologies d'Internet ont forcé des efforts de recherches d'explorer d'autres domaines d'application imprévus pour le tatouage numérique. Nous récapitulerons ci-dessous les applications principales du tatouage numérique [7], [10]:

- ✓ Protection du copyright ;
- ✓ Empreinte digitale ;

- ✓ Surveillance d'émission ;
- ✓ Authentification de multimédia ;
- ✓ Détection et correction de fraude ;
- ✓ Contrôle de copie..

Conclusion

L'objectif de ce chapitre était d'introduire quelques notions sur la technique de tatouage de documents numériques et des images en particulier. Les applications de cette technique sont multiples, et les contraintes qu'elle impose varient selon l'application envisagée. Nous avons donné une brève théorie du tatouage et leurs applications, et la classification des algorithmes qui existe. On a comparé aussi dans ce chapitre les performances des méthodes additives et multiplicatives pour les schémas d'étalement de spectre.

Bibliographie

- [1] R.B. Wolfgang, C.I. Podilchuk, Perceptual watermarks for digital images and video, *Proceedings of the IEEE*, 87(7), 1108 – 1126, July 1999.
- [2] C. Rey, Tatouage d'image : Gain en robustesse et intégrité des images, Thèse de Doctorat, Université d'Avignon et des pays de vaucluse, 2003.
- [3] G.L. Guelvouit, Tatouage robuste par étalement de spectre avec prise en compte de l'information adjacente, Thèse de Doctorat, Institut National des Sciences appliquées de Rennes, 2003.
- [4] V. Singh, Digital watermarking: A tutorial, *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, 10 – 21, January, 2011.
- [5] L. Kocarev, G. Jakimoski, Pseudorandom bits generated by chaotic maps, *IEEE Transactions on Circuits and Systems—I: fundamental theory and applications*, 50(1), 123 – 126, January 2003.
- [6] S. Chen, H. Leung, Ergodic chaotic parameter modulation with application to digital image watermarking, *IEEE Transactions on image processing*, 14(10), 1590–1602, October 2005.

- [7] C.W.H.Fung, A. Gortan, W.G. Junior, A review study on image digital watermarking, The Tenth International Conference on Networks, The Netherlands Antilles, 24-28, 23-28 January 2011.
- [8] G. Voyatzis and I. Pitas, Chaotic watermarks for embedding in the spatial digital image, International Conference on Image Processing, ICIP, 432 - 436, 4-7 Oct 1998.
- [9] A. Nikolaidis, I. Pitas, A region-based technique for chaotic image watermarking, EUSIPCO2000, 2, September 4-8, 2000.
- [10] C. Rafiullah, Digital watermarking for image authentication and recovery, Thèse de Doctorat, Pakistan Institute of Engineering and Applied Sciences, 2010.
- [11] I.J. Cox, J. Kilian, T. Leighton, and T.G. Shamoan, Secure spread spectrum watermarking for multimedia. In Proceedings of the IEEE International Conference on Image Processing, ICIP, 6, 1673 -1687, Santa Barbara, California, USA, October 1997.
- [12] A. Mooney, The generation and detection of chaos-based watermarks, Thèse de Doctorat, University of NUI Maynooth, 2005.
- [13] X.W. Zhu, Research of blind watermark detection algorithm based on generalized Gaussian distribution, Journal of Software, 5(4), 413-420, 2010.
- [14] C.H. Huang, and J.L. Wu, Attacking visible watermarking schemes, In IEEE Transactions on Multimedia, 6, 16-30, February 2004.
- [15] N. Baaziz, Adaptive watermarking schemes based on a redundant contourlet transform, IEEE International Conference on Image Processing ICIP, 11-14 September, 221-224, 2005.
- [16] M. Barni, F. Bartolini, V. Cappellini, A. Piva, A DCT-domain system for robust image watermarking, Signal Processing, 66, 357-372, 1998.
- [17] J. Huang, Y.Q. Shi, and Y. Shi, Embedding image watermarks in DC components, IEEE Transactions on circuits and systems for video technology, 10(6), 974 - 979, September 2000.
- [18] J.R. Hernandez, M. Amado, and F.P. Gonzalez, DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure, IEEE Transaction Image Processing, 9(1), 55-68, Jan. 2000.
- [19] A. Nikolaidis and I. Pitas, Asymptotically optimal detection for additive watermarking in the DCT and DWT domains, IEEE Transaction Image Processing, 12(5), 563-571, May 2003.
- [20] T.M. Ng and H. K. Garg, Maximum likelihood detection in image watermarking using generalized Gamma model, 1680-1684 in Proc. 39th Asilomar Conf. Signals, Systems, Computers, Pacific Grove, CA, 2005.

- [21] M. Barni, F. Bartolini, A.D. Rosa and A. Piva, A new decoder for the optimum recovery of nonadditive watermarks, *IEEE Transaction Image Processing*, 10(5), 755-766, May 2001.
- [22] V.M. Potdar, S. Han, E. Chang, A survey of digital image watermarking techniques, *3rd IEEE International Conference on Industrial Informatics (INDIN)*, 709 – 716, 2005.
- [23] X.G. Xia, C.G. Boncelet, G.R. Arce, A multiresolution watermark for digital images, In the *Proceedings of IEEE International Conference on Image Processing*, 1, 549 – 551, October 1997.
- [24] Y. Zhao, P. Campisi, D. Kundur, Dual domain watermarking for authentication and compression of cultural heritage images, in *IEEE Transactions on image Processing*, 13(3), 430-448, March 2004.
- [25] A. Manoury, *Tatouage d'images numériques par paquets d'ondelettes*, Thèse de Doctorat, L'Ecole Centrale de Nantes et l'Université de Nantes, 2001.
- [26] C.S. Woo, *Digital image watermarking methods for copyright protection and authentication*, Thèse de Doctorat, Queensland University, 2007.
- [27] M.E. Hajji, *La sécurité d'images par le tatouage numérique dans le domaine d'ondelettes*, Thèse de Doctorat, Université Agadir, 2012.
- [28] M. Kutter, F. Petitcolas, A fair benchmark for image watermarking systems, *Electronics Imaging, security and watermarking of multimedia contents, Imaging. Security and Watermarking of Multimedia Contents*, 3657, 1-14, 1999.
- [29] V. Conotter, *Active and passive multimedia forensics*, PhD Dissertation, University of Trento, 2011.
- [30] <http://www.cse.wustl.edu/~jain/cse571-11/ftp/watermrk/index.html>

Chapitre III : Les algorithmes développés de tatouage des images dans le domaine spatial

Introduction

Le but de ce chapitre est de proposer des algorithmes de tatouage d'image dans le domaine spatial afin d'améliorer la qualité perceptuelle et la robustesse des images tatouées. Le contenu d'image est analysé et les propriétés du HVS sont exploitées pour produire un masque visuel de la même taille que l'image hôte. Dans ce chapitre, quelques masques visuels sont proposés, en se basant sur la détermination des zones texturées et la modélisation mathématique de l'effet de la luminance sur le système HVS.

1. Le système visuel humain (HVS)

La sensibilité du système visuel humain (HVS) dépend principalement de trois paramètres : la fréquence spatiale, la couleur et l'intensité lumineuse (la luminosité). La réponse perceptuelle en fonction de la fréquence spatiale correspond à la sensibilité au contraste. Cette réponse définit une fonction notée CSF (Contrast sensitivity Function) [1].

Plusieurs modèles mathématiques ont été proposés pour représenter cette fonction de sensibilité. La plupart des modèles se basent sur le modèle proposé par Mannos et Sakrison [2] qui définissent la fonction de sensibilité du contraste en fonction de la fréquence spatiale comme suit :

$$CSF(f) = K_0(1 + K_1 f) \cdot \exp(-k_2 f)^{k_3} \quad (\text{III.1})$$

où K_0 , K_1 , K_2 et k_3 sont des paramètres à définir.

On choisit les paramètres proposés par [2], on obtient l'équation suivante :

$$CSF(f) = 2,6 (0,0192 + 0,114 f) \cdot \exp(-0,114 f)^{1,1} \quad (\text{III.2})$$

f est la fréquence spatiale exprimée par cycles/degré de l'angle visuel. La courbe de CSF est donnée sur la figure (III.1) [3].

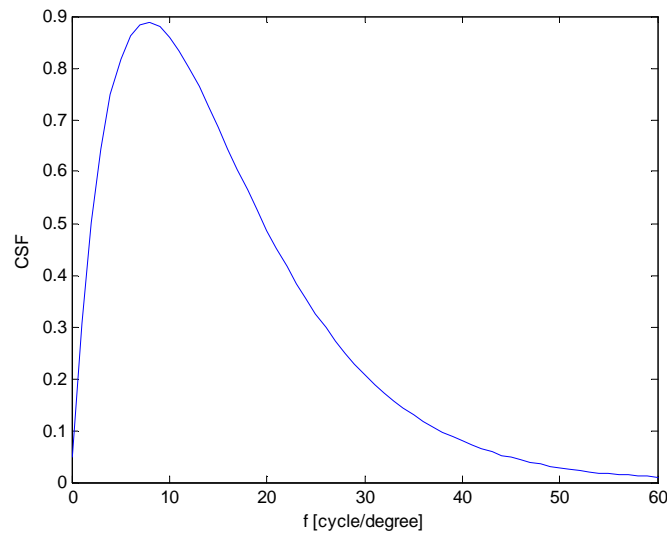


Figure III. 1 : La fonction de sensibilité au contraste

Cette fonction montre que la sensibilité de l'œil humain est maximale pour une fréquence spatiale de 8 *cycles/degree* ; au voisinage de cette valeur, la sensibilité reste élevée mais diminue au fur et à mesure qu'on s'éloigne de la valeur de $f = 8 \text{ cycles/degree}$: elle devient négligeable à partir de $f = 50 \text{ cycles/degree}$ (détails très fin de l'image).

1.1. Masques psychovisuels

De nombreux masques psychovisuels ont été proposés pour le tatouage d'images. Ils utilisent des propriétés empiriques du HVS, combinées avec une analyse statistique. Une approche classique est d'utiliser des techniques de codage existant en compression d'image. On distingue deux types de masques [4] :

- ✓ Les masques spatiaux sont calculés à partir de la luminance et favorisent les contours et les régions de forte variance locale. Ces masques conduisent souvent à des tatouages passe-haut, ce qui peut réduire la robustesse. Le masquage de contour est efficace que si le masque a la même orientation que le signal hôte.
- ✓ Les masques fréquentiels prennent en compte la sensibilité du HVS à une modification de chaque composante fréquentielle, à une modification de la luminance par rapport à un fond constant et réalisent un masquage de contraste prenant en compte la fréquence spatiale.

2. Etat de l'art sur la modélisation du HVS pour le tatouage d'image

Un algorithme de tatouage d'image soit efficace exige plusieurs critères standards. Cependant, il est impossible de répondre à tous ces critères au même temps.

Plusieurs études sur le tatouage d'image dans le domaine spatial ont été rapportées dans la littérature [5], [6], [7], [8], [9], [10]. L'une des premières méthodes proposée, est la technique des bits de poids faibles LSB (Least Significant Bit) [5]. La méthode de tatouage du LSB consiste à forcer le poids faible de chaque pixel à 0 ou 1, selon la valeur du bit de la séquence contenue dans le watermark. L'utilisation des masques perceptuels, qui tiennent compte les propriétés du système visuel humain (HVS), s'avère être une manière efficace pour améliorer la robustesse d'un système de tatouage sans affecter la qualité d'image. Les auteurs dans le travail [6] ont proposé une méthode nommée par Patchwork, qui est basée sur la différence de luminance entre deux ensembles de pixels, déterminée à l'aide d'une clef. Cette méthode utilise des critères visuels pour l'insertion du watermark. Sebé et al. [7], ont décrit deux algorithmes de tatouage d'image dans le domaine spatial pour la protection de copyright d'image. L'un des schémas est robuste au découpage, tandis que, l'autre est robuste au décalage. Le processus de la détection du filigrane exige la connaissance de l'image originale. Nikolaidis et al. [8] ont proposé une méthode d'insertion et de détection dans le domaine spatial basé sur la segmentation d'image qui détermine les régions qui sont robuste à la majorité des attaques, comme la compression le filtrage, le découpage et la rotation. Bangaleea et al. [9], ont présenté un schéma de tatouage dans le domaine spatial pour les images fixes. L'analyse perceptuelle est utilisée pour déterminer l'imperceptibilité du filigrane dans l'image originale. La marque utilisée est à la base des générateurs pseudo-aléatoire et l'insertion se fait d'une manière additive. La technique de détection est basée sur la corrélation. Tefas et al. [10] ont été présenté une analyse statistique des schémas de tatouage basées sur la détection par corrélation utilisant des filigranes produits par la carte skew tente. L'insertion du filigrane a lieu dans le domaine spatial d'une manière additive. La détection de filigrane est effectuée par l'utilisation de corrélation entre l'image à examiner et le filigrane. Afin de décider la présence de la marque, la valeur de corrélation est comparée à un seuil convenablement choisi.

L'utilisation des masques perceptuels, qui tiennent compte des propriétés du système visuel humain (HVS), s'avère être une manière efficace pour améliorer la robustesse d'un système de tatouage sans affecter la qualité d'image.

3. Notre système de tatouage

Notre système de tatouage est défini comme suit :

1. On note l'ensemble d'images numériques d'échelle de gris, pour être protégé, de la taille $m \times n$ par $I = \{I_{ij} \in [0, 1, \dots, 2^{L-1}]\}$, où L note les bits binaire des pixels d'image de niveau gris ;
2. w : est l'ensemble du signal de filigrane : $w = \{w_{ij} \in [0, 1]\}$;
3. I_w : est l'image tatouée ;
4. α : est une constante définie par l'utilisateur ajustée pour assurer l'invisibilité du filigrane ;
5. d : représente la matrice de différence entre l'image tatouée et l'image originale;
6. M_T : désigne le masque des secteurs texturés;
7. M_L : désigne le masque de la luminance;
8. M : note le masque final ;
9. T_w : le seuil ;
10. sim : la valeur de la corrélation.

4. Tatouage d'image numérique par l'utilisation de la fonction de visibilité de bruit (NVF)

Le but de ce travail est d'améliorer les performances d'un système de tatouage numérique dans le domaine spatial, en développant un nouvel algorithme pour l'insertion de ce filigrane dans l'image hôte [11]. En basant sur le NVF (Noise Visibility Function) de l'image hôte, le masque est de la même taille que l'image originale. Son utilisation comme une image de pondération et filtre pendant l'étape d'insertion, nous a permis d'accroître la valeur du facteur d'insertion, pour atteindre le meilleur compromis entre la robustesse et l'invisibilité.

4.1. Construction de filigrane

La plupart des techniques de génération de filigrane disponibles dans la littérature sont produites à partir des séquences de nombre pseudo-aléatoire [12], [13]. Cependant, les séquences produites par l'itération des cartes chaotiques donnent une alternative efficace aux séquences pseudo-aléatoires de filigrane. Une telle séquence peut être produite en réitérant une fonction chaotique, qui a été semée avec une fonction de graine (function seed) et une valeur initiale, et cette séquence peut être quantifiée pour former un filigrane binaire.

Le chaos est connu pour être un système extrêmement sensible à son état initial et un petit changement d'état initial peuvent faire le chaos changé considérablement après quelques itérations [14], [15].

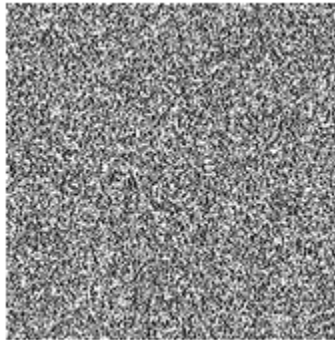


Figure III. 2 : Le filigrane produit ($X_0 = 0.1$ & $\lambda=3.98$), taille=256 ×256

La carte la plus simple et la plus utilisée est la carte logistique écrite sous sa forme récursive $X_{n+1} = \lambda X_n(1 - X_n)$; Ici, $0 \leq X_n \leq 1$ et $0 \leq \lambda \leq 4$ s'appelle le paramètre de bifurcation. Selon la valeur de λ , la dynamique de ce système peut se changer dramatiquement, lorsque $3.57 \leq \lambda \leq 4$ la séquence est non périodique, non convergente, et très sensible à la valeur initiale [16], [17]. Un signal 1D chaotique est au départ produit, puis transformé pour produire un filigrane de 2D. Afin d'obtenir le filigrane de 2D, en utilisant le balayage raster (voir annexe A). Le point de départ de la séquence (l'état initial de la carte) est considéré comme la clef du filigrane.

4.2. Génération du masque

La *NVF* c'est une fonction qui caractérise les propriétés locales d'image, et qui permet l'identification des régions texturées et les régions de bord où le filigrane devrait plus fortement être inséré [18]. L'expression de *NVF* est donnée par l'équation (III.3):

$$NVF(i, j) = \frac{1}{1 + \sigma_x^2(i, j)} \quad (III.3)$$

Un paramètre de réglage θ est inséré dans l'expression du NVF pour l'ajustement de contraste. Ce paramètre est donné par $\theta = \frac{D}{(\sigma_{xmax})^2}$.

où $(\sigma_{xmax})^2$ est la variance locale maximale pour une image donnée, et D est un paramètre expérimentalement déterminé.

alors la fonction NVF devient comme suit :

$$NVF(i, j) = \frac{1}{1 + \theta \cdot \sigma_x^2(i, j)} \quad (III.4)$$

$\sigma_x(i, j)$ note la variance locale de l'image dans une fenêtre centrée sur un pixel avec les coordonnées (i, j) , $i \leq 1, j \leq M$.

La variance locale est donnée par :

$$\sigma_x^2(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^{k=L} \sum_{l=-L}^{l=L} (x(i+k, j+l) - \bar{x}(i, j))^2 \quad (III.5)$$

avec :

$$\bar{x}(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^{k=L} \sum_{l=-L}^{l=L} x(i+k, j+l) \quad (III.6)$$

Une fenêtre de la taille 3×3 est utilisée pour le calcul de NVF . Le NVF pour les images de test nommées peppers et f16 est montré sur la figure (III.3).

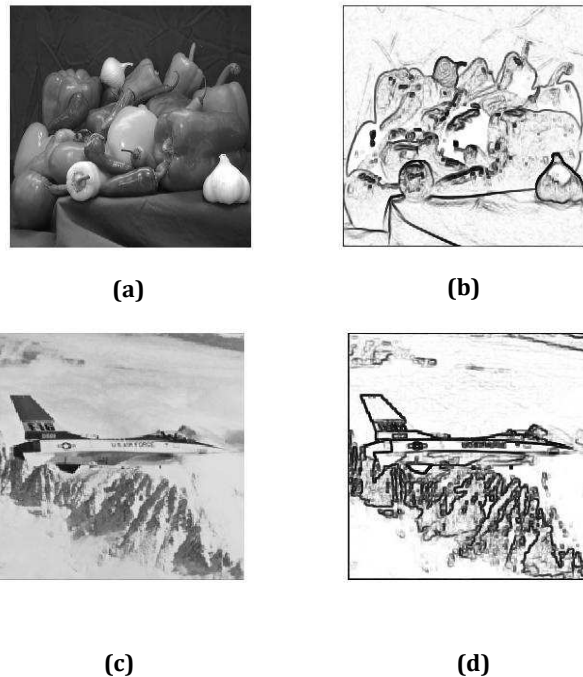


Figure III. 3 : Fonction de visibilité de bruit pour l'image peppers (a, b) et l'image f16 (c, d)

La fonction NVF prend des valeurs entre zéro et un. Les valeurs élevées de NVF correspondent à des régions très lumineuses, qui indiquent des régions plates (flat) ; et les petites valeurs de NVF correspondent à des régions sombres, qui indiquent des régions texturées ou des régions avec des bords (edges).

4.3. Procédure d'insertion

Le processus d'insertion du watermark par l'utilisation de la fonction NVF est représenté sur la figure (III.4).

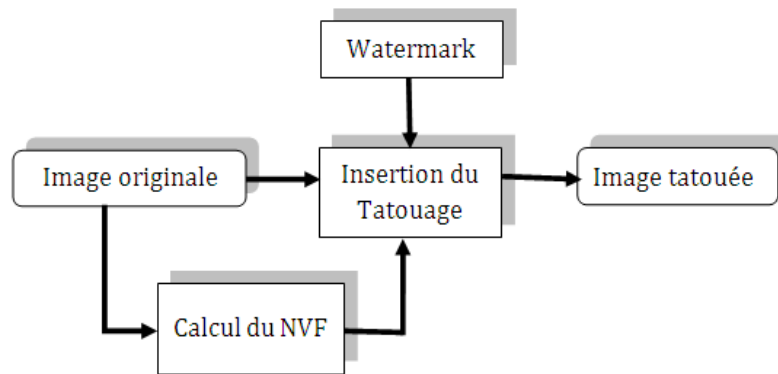


Figure III. 4 : Diagramme proposé pour l'insertion de filigrane

Dans ce travail, nous proposons la fonction NVF comme un filtre et au même temps une image de pondération du watermark, selon l'équation suivante :

$$I_w(i,j) = \begin{cases} I(i,j) + NVF(i,j).w(i,j).\alpha & \text{si } I(i,j) > NVF(i,j) \\ I(i,j) & \text{sinon} \end{cases} \quad (\text{III.7})$$

$I(i,j)$ et $I_w(i,j)$ sont les valeurs des pixels pour l'image originale et tatouée, respectivement, le $w(i,j)$ sont les éléments de filigrane, et $NVF(i,j)$ est le NVF correspondant à l'image $I(i,j)$.

Dans l'équation proposée (III.7), seulement les pixels qui possèdent des valeurs plus grandes que le NVF qui sont tatoués ; cependant les pixels inférieurs au NVF ne sont pas tatoués.

4.4. Résultats de simulation

Pour montrer l'efficacité de l'algorithme proposé, des résultats de simulation sous MATLAB sont donnés dans cette section. Dans la simulation, quatre images de tests de la taille 256×256 , appelées Lena, peppers, boat et baboon sont utilisées ; le filigrane à insérer est de la même taille que l'image originale.

D'abord nous avons évalué la qualité perceptuelle de l'image tatouée avec notre algorithme. On peut voir que les images originales et tatouées avec le masque sont perceptiblement indistinguables, de ce fait en validant la contrainte d'invisibilité pour des algorithmes efficaces de tatouage numérique.

Nous utilisons la valeur de PSNR (Peak Signal to Noise Ratio) pour évaluer la qualité de l'image tatouée par notre méthode. C'est une méthode populaire pour évaluer la différence entre l'image tatouée et son image originale.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (III.8)$$

MSE est l'erreur carrée moyenne entre les images originales et tatouées définie comme :

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i,j) - I_w(i,j))^2 \quad (III.9)$$

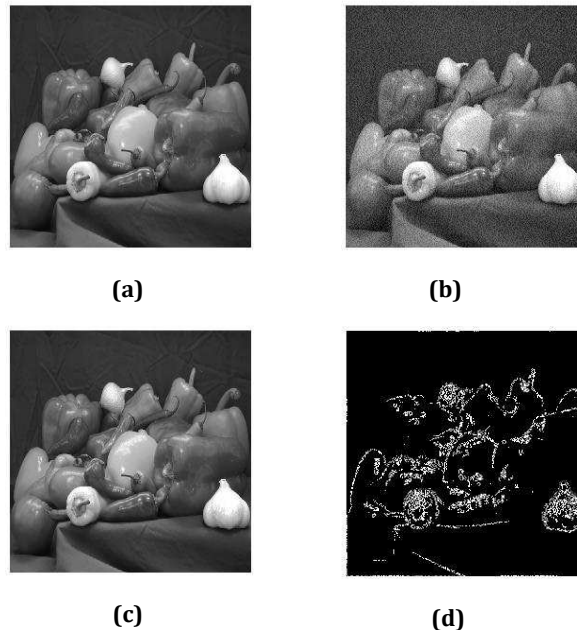


Figure III. 5 : (a) : Image originale (b) : Image tatouée sans masque avec PSNR = 70.7608dB (c) : Image tatouée avec l'utilisation du masque pour PSNR=87.4980dB (d) : La différence entre l'image tatouée et l'image originale (les grandeurs sont amplifiées par un facteur de 100 pour le but de visionnement, le nombre maximum de l'information qui peut être insérée dans l'image est 7941 bits)

En comparant les deux systèmes de tatouage d'image numérique, le système qui possède une valeur très élevée de PSNR a une meilleure qualité visuelle.

Nous présenterons aussi la variation de PSNR de l'image tatouée (Lena, peppers, boat et baboon), pour la valeur de alpha est changé de 0.1→3. La qualité de l'image en terme de PSNR est donnée sur la figure (III.6).

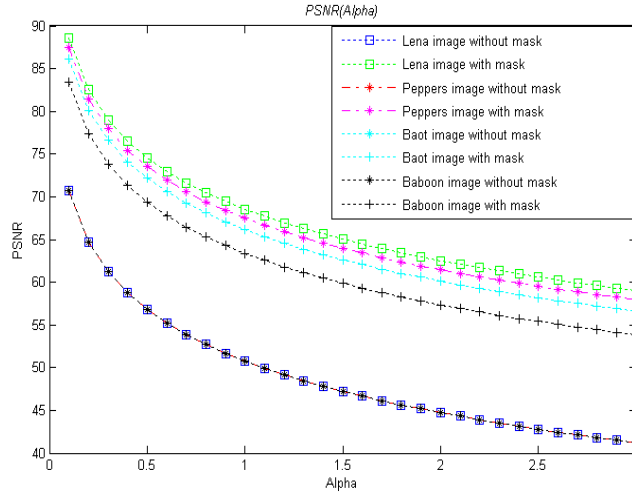


Figure III. 6 : Variation de PSNR de l'image tatouée avec et sans masque pour les images Lena, peppers, boat et baboon

On remarque que les images tatouées, qui sont obtenues par notre schéma proposé, ont la meilleure valeur de PSNR.

5. Modèle de luminance pour le tatouage d'image

Dans cette section, on va décrire un nouveau masque perceptuel spatial proposé dans [19], où l'effet de la luminance sur le HVS est modélisé en basant sur les points de faiblesse de l'œil humain. L'algorithme du tatouage d'image proposé est exécuté dans le domaine spatial.

5.1. Le masque spatial proposé

Afin d'augmenter l'invisibilité du filigrane, les caractéristiques du système visuel humain (HVS) peuvent être exploitées pour adapter le filigrane à l'image à tatouer, que l'œil humain est moins sensible au changement dans les régions avec une forte valeur de luminance comme dans des régions de faible valeur comparées aux régions de valeur moyenne de gris, où la déformation est plus apparente [11].

Dans notre approche proposée, nous prenons en compte les propriétés locales de l'image et les points de faiblesse du HVS.

La valeur du masque proposé à chaque pixel est donnée par l'équation suivante :

$$M_L(i, j) = e^{\left| \frac{I(i, j) - 128}{128} \right|} - 1 \quad (\text{III.10})$$

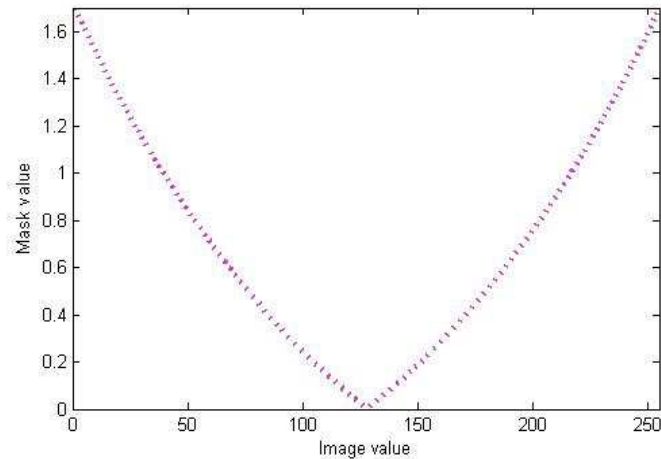


Figure III. 7 : Valeurs de masque proposé

Les valeurs de masque sont tracées sur la figure (III.7), l'image masque M_L possède des valeurs dans l'intervalle $[0,1.7]$, cette technique permet l'insertion d'un filigrane plus fort dans les régions de grande et de petite valeur de luminance, plutôt que dans les régions de valeur moyenne de luminance.

L'image masque obtenue par la modélisation de la luminance pour l'image boat est donnée sur la figure ci dessous.



Figure III. 8 : (a) :L'image originale ; (b) : L'image masque basée sur le HVS

5.2. Insertion du filigrane

L'image tatouée dans le cas le plus simple, où le contenu d'image n'est pas pris en considération (Méthode1) (c.à.d, aucun masque perceptuel n'est utilisé), peut être écrite comme suit :

$$I_w = I + \alpha w \quad (\text{III.11})$$

Si le masque perceptuel spatial est utilisé (Méthode2), l'insertion du filigrane peut être exprimée par l'équation suivante :

$$I_w = I + \alpha w \otimes M_L \quad (\text{III.12})$$

où \otimes désigne la multiplication point par point.

Dans ce cas l'image de filigrane w est multipliée par les éléments du masque M_L élément par élément.

5.3. Détection de filigrane

La présence (ou l'absence) d'un filigrane connu dans un signal reçu est évaluée en utilisant une méthode standard de statistique de détection : il s'agit de la corrélation entre le signal reçu I_w (image tatouée) et le filigrane inclu w . Ce calcul est soutenu par des expériences de Zeng et al. [20]. Si le résultat est plus grand que la valeur du seuil, nous pouvons dire que l'image est tatouée ; autrement, elle n'est pas tatouée.

$$sim = \frac{\sum_m \sum_n (w(i,j) - \bar{w}) \cdot (I_w(i,j) - \bar{I}_w)}{\sqrt{\sum_m \sum_n (w(i,j) - \bar{w})^2 \cdot (\sum_m \sum_n (I_w(i,j) - \bar{I}_w)^2)}} \quad (III.13)$$

où w , I_w sont le filigrane et l'image tatouée respectivement, \bar{w} et \bar{I}_w sont la valeur moyenne du filigrane et l'image tatouée.

Pour qu'un schéma de tatouage soit efficace, il est très important de placer un seuil approprié qui réduit au minimum le nombre de fausse alarme positive et fausse alarme négative. Le seuil devrait être plus grand que la valeur maximum de corrélation entre le filigrane extrait et les filigranes aléatoires, et soient beaucoup moins que celle entre le filigrane extrait et le filigrane inséré [21]. Les résultats expérimentaux suggèrent qu'une valeur de seuil $T_w = 0.01$ devrait être utilisée pour l'image de test.

La figure (III.9) montre la réponse du détecteur pour 1000 filigranes ; seulement le watermark du numéro 100 était inséré.

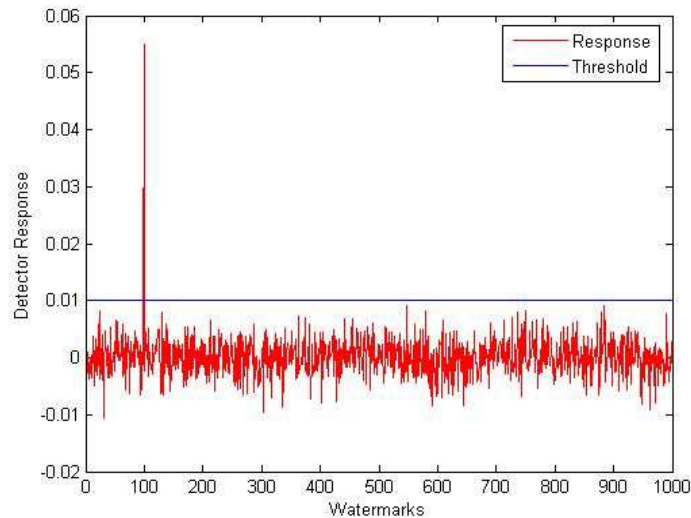


Figure III. 9 : Réponse du détecteur de l'image tatouée dans la figure (III.9c) à 1000 filigranes produits

La réponse du détecteur au filigrane correct est beaucoup plus grande que la réponse aux autres filigranes, le système de tatouage a détecté le filigrane incorporé correct parmi 1000 filigranes différents.

5.4. Résultats de simulation

PSNR pénalise la visibilité du bruit dans une image, une valeur de PSNR de 36dB est acceptable en terme de dégradation, qui signifie qu'aucune dégradation significative n'est observée par l'œil humain [22].

D'abord nous avons évalué la qualité perceptuelle de l'image tatouée avec notre algorithme. On peut voir que l'image originale et l'image tatouée avec le masque sont perceptiblement indistinguables, de cette manière la condition d'invisibilité est validée pour des algorithmes efficaces de tatouage.

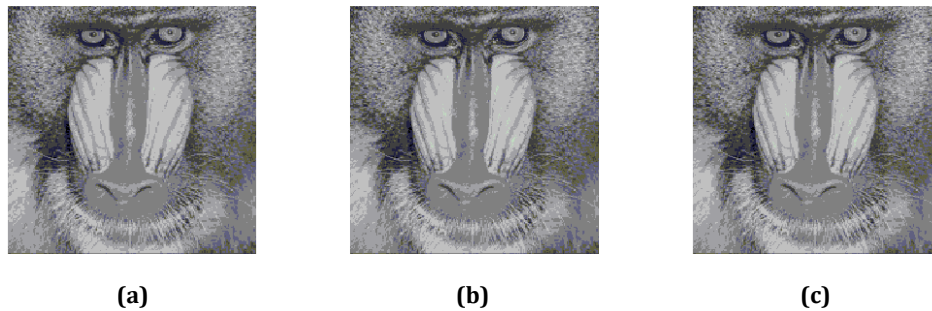


Figure III. 10 : Comparaison des images, (a): Image originale, (b): Image tatouée sans masque PSNR=31.3682dB (c) : Image tatouée avec masque PSNR=43.8767dB ($\alpha=0.03$)

La variation des valeurs de PSNR avec le facteur d'insertion est variable pour l'image peppers pour les deux méthodes, où alpha est varié de 0.01 jusqu'à 0.1.

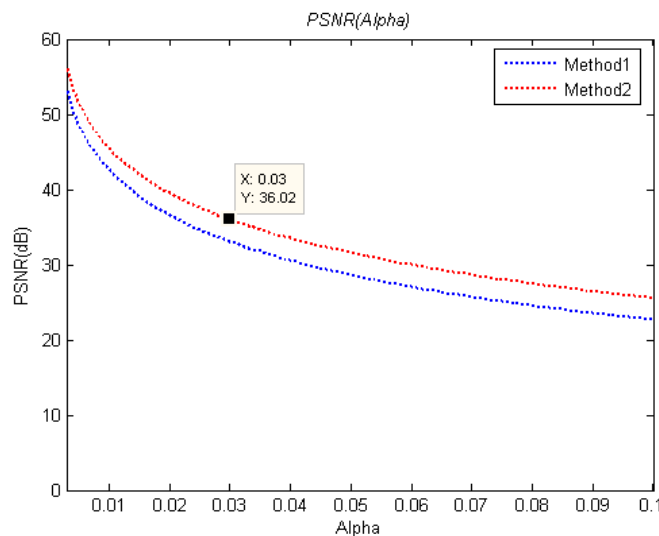


Figure III. 11 : Variation de PSNR de l'image tatouée peppers avec et sans masque

Nous avons trouvé la valeur de PSNR sur la figure (III.11) de l'image tatouée avec notre masque (Method2) possède la valeur supérieure comparée à l'autre schéma de tatouage, où le masque M_L n'est pas pris en considération (Method1). L'espace entre les valeurs suggère les performances supérieures de notre nouvel algorithme.

Nous pouvons dire qu'une plus grande valeur du α peut être utilisée, sans détruire la qualité d'image, tout en utilisant le masque développé.

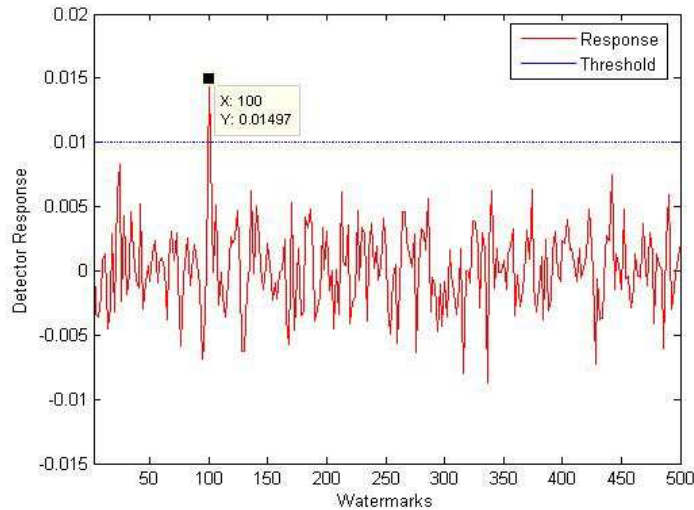


Figure III. 12 : Réponse de détecteur à la compression JPEG de l'image peppers

Puis, nous avons examiné la robustesse de l'algorithme face à la compression JPEG avec un facteur de compression $Q = 60$. La réponse de détecteur est donnée sur la figure (III.12).

Le détecteur est au-dessus du seuil, la technique suggérée réussit à détecter le filigrane après la compression JPEG. Les résultats ont prouvé que, l'utilisation de l'approche du masque, permet d'insérer dans les images numériques des filigranes d'une énergie plus élevée, que lui étaient possibles sans masque.

6. Algorithme de tatouage d'image basé sur le NVF et la luminance

Dans cette section on va proposer une technique pour le tatouage d'image fixe basé sur les concepts de HVS développés dans les travaux [23] et [24]. Le filigrane est produit en utilisant la carte logistique et réorganisé dans le balayage de Peano, puis signé dans le domaine spatial en exploitant les caractéristiques du système visuel humain afin d'atteindre l'invisibilité de filigrane sans diminuer sa robustesse. Dans l'algorithme

proposé, le NVF de l'image est calculé et l'information de luminance est pris en considération.

6.1. Génération du filigrane

Le filigrane bidimensionnel w de la taille $m \times n$ est constitué en considérant une séquence X_n de longueur $m.n$ et d'une technique de balayage [25]. Puis, on mis un seuil T_w . Si un élément de la séquence est plus grand que le seuil, nous remplaçons cet élément par 1 ; autrement, le remplacer par 0, comme le décrit la formule suivante :

$$w(i, j) = \begin{cases} 1 & \text{si } w(i, j) \geq T_w \\ 0 & \text{si } w(i, j) < T_w \end{cases} \quad (\text{III.14})$$

Ainsi, nous obtenons le filigrane désiré.

La figure (III.13) montres quelques filigranes en forme binaire, où les types de balayage raster et Peano sont utilisées. Pour plus d'information sur quelques types de balayage consulter l'annexe A.

Pour obtenir plus de sécurité et plus de robustesse, l'image de filigrane doit être mélangée (scrambling) avant de l'insérer dans l'image [26]. La méthode de mélange est utilisée pour chiffrer une image en commandant à nouveau la position spatiale des pixels.

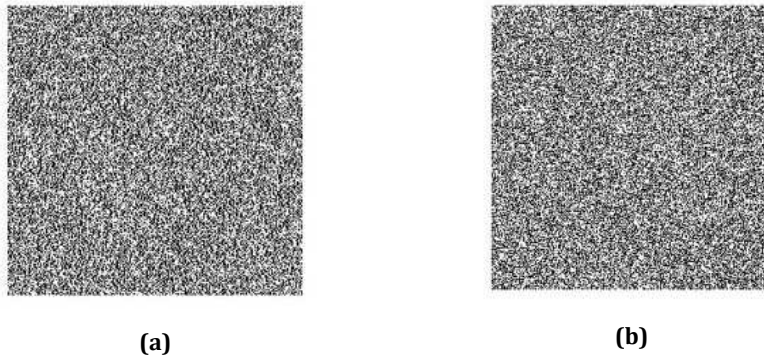


Figure III. 13 : Filigranes présentés en forme binaire créés par la même clef ($\lambda= 3.98, X0=0.01$), (a) : Balayage raster, (b) : Balayage de Peano

Dans cette partie, nous utilisons la transformation à deux-dimension pour mélanger l'image. L'équation du mélange est exprimée par [27], [28] et donné par l'équation (III.15) :

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \text{ mod } n \quad (\text{III.15})$$

n : désigne la largeur de l'image.

Il signifie que chaque pixel aux coordonnées (i, j) de l'image de filigrane est déplacé vers les coordonnées (i', j') par l'utilisation de l'équation (III.15). Le nombre de transformations exécutées sur l'image de filigrane et k sont gardés comme des clés secrètes.

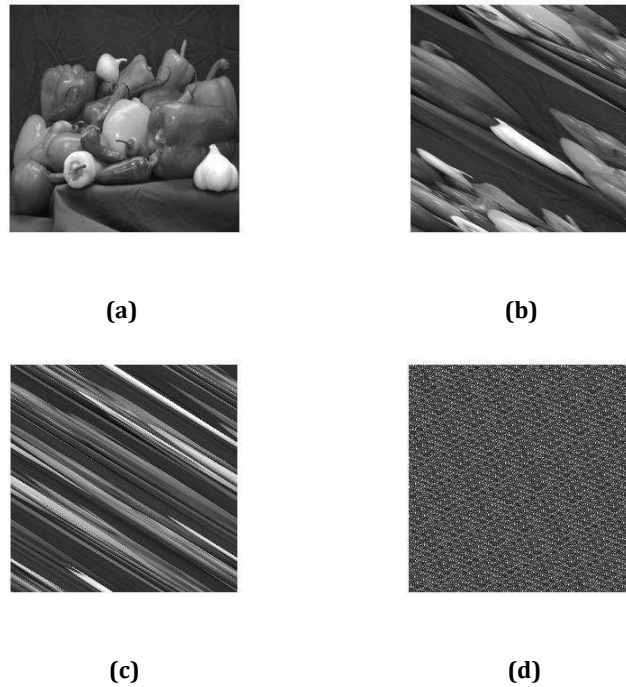


Figure III. 14 : Exemple de mélange, (a) : L'image originale, (b), (c), et (d) L'itération du mélange de (a) après un, deux, et dix itérations, respectivement.

Pour montrer l'effet de la méthode de mélange, nous utilisons comme exemple l'image appelée Peppers, comme le montre la figure (III.14). Le but du mélange dans ce travail est de mélanger l'image de filigrane.

6.2. Le masque spatial proposé

Afin d'améliorer l'invisibilité perceptuelle, les propriétés de l'image originale doivent être considérées, et aussi que les caractéristiques du système visuel humain (HVS) peuvent être exploitées pour adapter le filigrane à l'image qu'on va tatouée. Nous produisons le masque de l'image en utilisant les propriétés suivantes de HVS [29], [30] :

1. L'œil est moins sensible au bruit dans des zones fortement texturés ;
2. La modification autour des bords est très apparente à l'œil ;
3. L'œil est moins sensible au bruit dans les secteurs avec des valeurs élevées et faible de luminance.

Pour l'analyse de texture nous utilisons la fonction de NVF décrite précédemment :

Le masque M_T produit pour les secteurs texturés est défini comme suit :

$$M_T = 1 - NVF \quad (\text{III.16})$$

Le masque M_L proposé, qui tient l'effet de la luminance sur le HVS à chaque pixel avec une normalisation des valeurs dans l'intervalle [0,1] est donné par [23]:

$$M_L(i, j) = \frac{\left| e^{\frac{I(i, j) - 128}{128}} - 1 \right|}{e} \quad (\text{III.17})$$

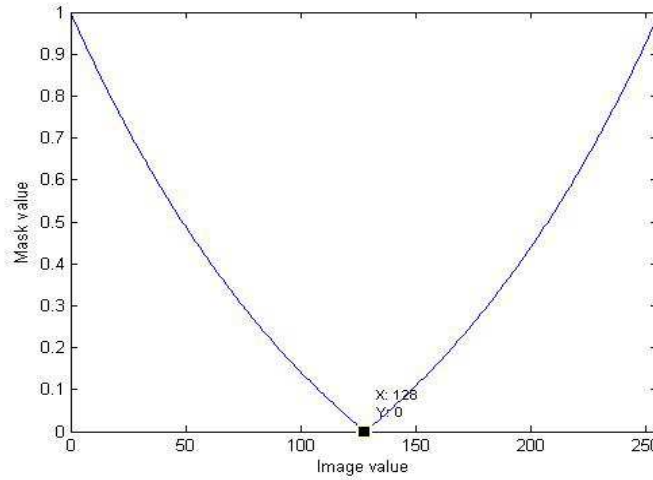


Figure III. 15 : Valeurs de masque

Les valeurs de masque sont tracées sur la figure (III.15), possède des valeurs dans l'intervalle [0,1].

Après l'obtention des deux masques correspondant à la texture M_T et à la luminance M_L , nous produisons le masque final M en utilisant l'équation suivante :

$$M = M_T \otimes M_L \quad (\text{III.18})$$

\otimes désigne une multiplication point par point.

6.3. Etude de performance du masque proposé

6.3.1. Insertion du filigrane

L'image tatouée dans le cas le plus simple, où le contenu d'image n'est pas pris en considération (c.à.d, aucun masque perceptuel n'est utilisé), peut être écrite comme suit :

$$I_w = I + \alpha w \quad (\text{III.19})$$

Si un masque spatial est utilisé, le filigrane w est multiplié élément par élément par le masque M . L'insertion de filigrane peut être exprimée par l'équation suivante :

$$I_w = I + \alpha(w \otimes M) \quad (\text{III.20})$$

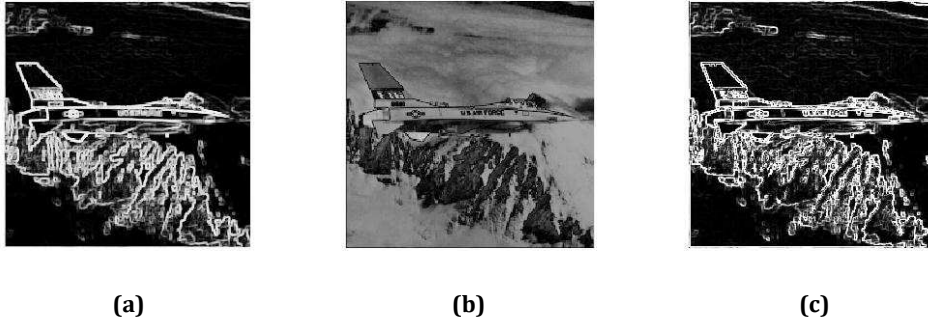


Figure III. 16 : Le masque visuel proposé, (a) : Le masque du texture M1;(b) : Le masque de luminance M2 ;(c) Le masque proposé M amplifié par un facteur de 5 pour le visionnement

6.3.2. Détection de filigrane

La détection et l'extraction de filigrane est une autre étape importante dans l'algorithme du tatouage. Pour détecter la présence ou l'absence du filigrane, la différence ($d = I_w - I$) entre l'image tatouée et l'image hôte est calculée puis corrélée avec le filigrane mélangé, comme le montre l'équation (III.21).

$$sim = \frac{\sum_m \sum_n (w(i,j) - \bar{w}) \cdot (d(i,j) - \bar{d})}{\sqrt{\sum_m \sum_n (w(i,j) - \bar{w})^2 \cdot (\sum_m \sum_n (d(i,j) - \bar{d})^2)}} \quad (\text{III.21})$$

Si le résultat est plus grand que la valeur de seuil, on peut dire que l'image est tatouée ; autrement dit, elle n'est pas tatouée.

Les résultats expérimentaux suggèrent qu'une valeur de 0.015 devrait être utilisée pour l'image de test.

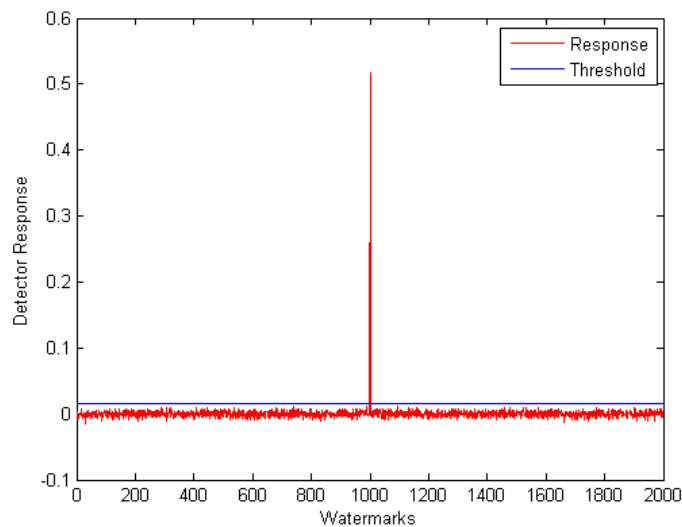


Figure III. 17 : Réponse du détecteur pour l'image watch

La figure (III.17) montre la réponse de détecteur pour les 2000 graines de filigrane, était seulement une seule graine est correcte, et la corrélation est plus forte, qui montre la détection correcte de filigrane. Dans ce schéma la marque correcte est le filigrane de numéro 1000.

6.4. Résultats et discussion

Pour montrer l'efficacité de l'algorithme proposé, des résultats de simulation sous MATLAB sont donnés dans cette section. Dans la simulation, l'image watch de la taille 256×256 est utilisée ; le filigrane à insérer est de la même taille que l'image originale.

6.4.1. Mesure de qualité

Afin de déterminer la dégradation dans une image tatouée nous appliquons le PSNR. Les expériences ont été exécutées pour deux cas, c.à.d, le cas, où le contenu d'image n'est pas pris en considération (c.à.d, aucun masque n'est utilisé), et le cas du tatouage basé sur le masque perceptuel proposé.

D'abord nous avons évalué la qualité perceptuelle de l'image tatouée avec notre algorithme. On peut dire que l'image originale et tatouée avec le masque sont visuellement indistinguable, ceci valide les conditions d'invisibilité pour des algorithmes efficaces de tatouage.

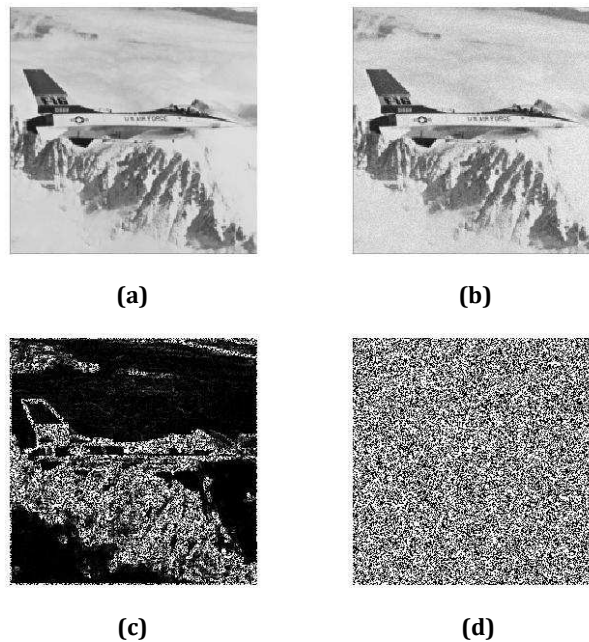


Figure III. 18 : Images après l'insertion du watermark ; (a) : Image tatouée avec le masque proposé PSNR=40.2252dB ; (b) : Image tatouée sans masque PSNR=27.6461dB ; (c) et (d) La différence entre l'image tatouée et originale amplifiée par un facteur 100 pour le visionnement.

La variation des valeurs de PSNR avec le changement du facteur α pour l'image f16 pour les deux méthodes est donnée dans la figure (III.19), alpha est changé de 0.01 \rightarrow 0.1.

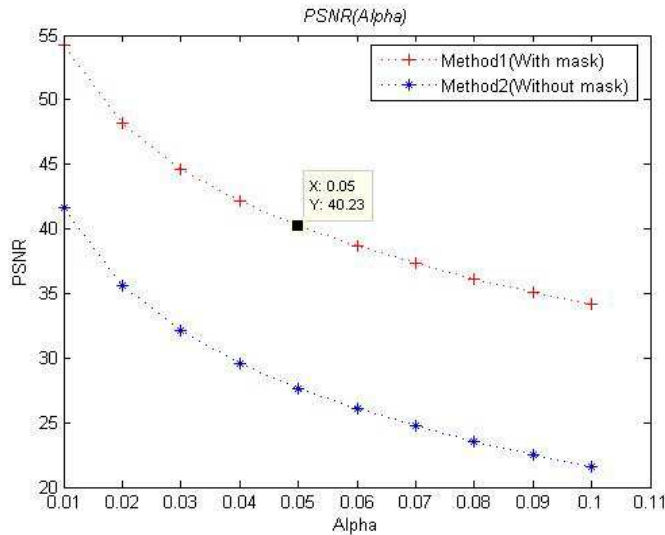


Figure III. 19 : Variation de PSNR de l'image tatouée avec et sans masque

Nous avons trouvé la valeur de PSNR de l'image tatouée avec notre approche possède la valeur supérieure comparée aux autres systèmes de tatouage. La bande entre les valeurs suggère les performances supérieures de notre nouvel algorithme. Nous pouvons dire qu'une plus grande valeur de α peut être utilisée, sans détruire la qualité de l'image, lorsqu'on utilise les techniques des masques.

1.1.1. Test de robustesse

Pour montrer la robustesse de l'algorithme proposé face aux transformations d'image, par la compression JPEG avec un facteur de qualité $Q=20$, le filtrage médian (MF) avec l'utilisation d'une fenêtre de taille 3×3 , et l'ajout de bruit 100% par l'utilisation du logiciel StirMark [31], et finalement le découpage diagonal de 50% de l'image tatouée où les parties absentes de l'image attaquée sont remplacées avec des parties du filigrane comme représenté sur la figure (III.20).

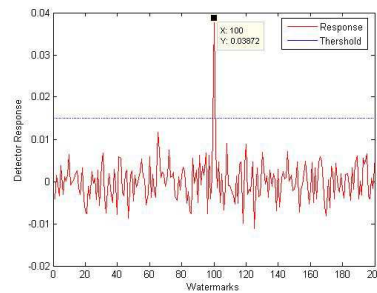
On remarque que la réponse du détecteur face aux attaques pour le vrai filigrane est plus grande par rapport à la valeur de la réponse du détecteur face aux faux filigranes.

Conclusion

Dans ce chapitre la fonction NVF et la propriété de la luminance sont exploitées pour la conception des masques visuels. On a proposé quelques algorithmes de tatouage pour des images numériques à base de ces masques. Le filigrane est inséré dans le domaine spatial en exploitant les caractéristiques du système visuel humain afin d'atteindre l'invisibilité du filigrane sans diminuer sa robustesse. Les résultats de comparaison des images tatouées obtenues sans masque et avec masque conçu montrent l'intérêt de notre approche. Les algorithmes de tatouage dans le domaine spatial résistent très mal à tout type d'attaque géométrique ou fréquentiel. Cet inconvénient a dirigé les chercheurs vers l'utilisation d'autres domaines robustes.



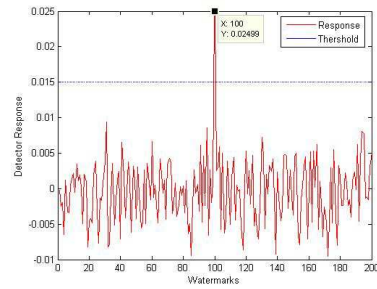
(a)



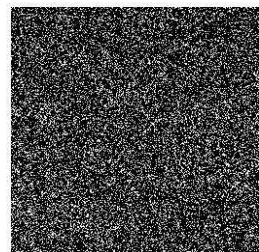
(b)



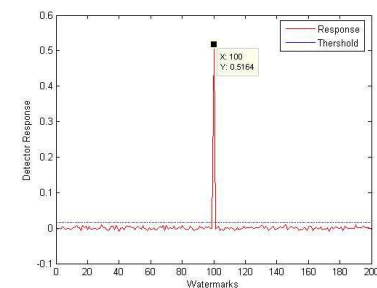
(c)



(d)



(e)



(f)

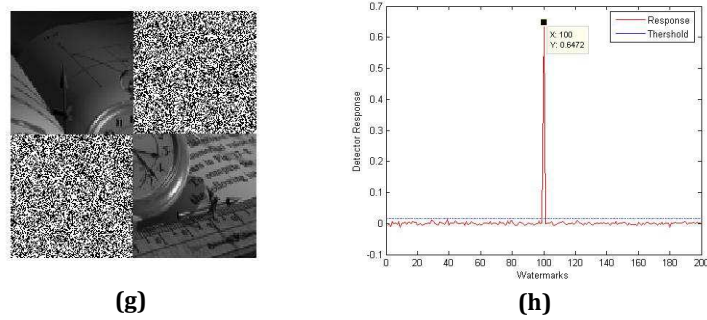


Figure III. 20 : La réponse du détecteur : (a, b) : Compression JPEG (Q=20), (c, d) : Filtrage médian (fenêtre 3×3), (e, f) : Ajout de bruit (100%), (g, h) : Le découpage diagonal (50%)

Bibliographie

- [1] G. Gaetan, Tatouage robuste par étalement de spectre avec prise en compte de l'information adjacente, Thèse de Doctorat, INSA de Rennes, 2003.
- [2] D. Levický, P. Foriš, Human visual system models in digital image watermarking, *Radioengineering*, 13(4), 38 – 43, Decembre 2004.
- [3] A. Beghdadi, M.C. Larabi, A. Bouzerdoum, K.M. Iftikharuddin, A survey of perceptual image processing methods, *Signal Processing: Image Communication*, 28, 811-831, 2013.
- [4] V. Martin, M. Chabert, B. Lacaze, Masques perceptuels reposant sur l'interpolation en tatouage numérique, Colloque GRETSI, 11-14 Septembre, Troyes, 1193-1196, 2007.
- [5] S. Pan, H.C. Huang, and L.C. Jain, *Intelligent watermarking techniques*, World Scientific Publishing Company, Singapore, ISBN: 981-238-757-9, 2004.
- [6] W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, *Proceedings of the SPIE*, 1995.
- [7] F. Sebé, J. Domingo-Ferrer, and J. Herrera, Spatial-domain image watermarking robust against compression, filtering, cropping and scaling, *Proceedings of ISW 2000*, 1975, 44–53, 2000.
- [8] A. Nikolaidis, I. Pitas, Region-based image watermarking, *IEEE Transactions on Image Processing*, 10(11), 1726 – 1740, November 2001.
- [9] R. Bangaleea and H.C.S. Rughooputh, Performance improvement of spread spectrum spatial domain watermarking scheme through diversity and attack characterization, *IEEE, 6th African conference in Africa*, 1, 293–298, 2002.
- [10] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, Performance analysis of correlation-based watermarking schemes employing Markov chaotic sequences, *IEEE Transaction on Signal Processing*, 51, 1979–1994, 2003.
- [11] S. Belkacem, Z. Dibi, A. Bouridane, Efficient Image Watermarking Using Noise Visibility Function, *International Multi-conference on Systems, Signal & Devices-Hammamet, Tunisia* 19-22 March 2007.

- [12] S. Chen, H. Leung, Ergodic chaotic parameter modulation with application to digital image watermarking, *IEEE Transactions on image processing*, 14(10), 1590 – 1602, October 2005.
- [13] L. Kocarev, G. Jakimoski, Pseudorandom bits generated by chaotic maps, *IEEE Transactions on Circuits and Systems—I: fundamental theory and applications*, 50(1), 123 – 126, January 2003.
- [14] P. Stavroulakis, *Chaos Applications in telecommunications*, Published by CRC Press, 2006.
- [15] A. Mooney, J.G. Keating and I. Pitas, A comparative study of chaotic and white noise signals in digital watermarking, *Chaos, Solitons and Fractals*, 35, 913–921, 2008.
- [16] A. Mooney, J. G. Keating and D. M. Heffernan, A detailed study of the generation of optically detectable watermarks using the logistic map, *Chaos, Solitons and Fractals*, 30, 1088-1097, 2006.
- [17] J. Zhang, L. Tian, H. M. Tai, A new watermarking method based on chaotic maps, *IEEE International Conference on Multimedia and expo (ICME)*, 939 - 942, 2004.
- [18] S. Voloshynovskiy, A. Herrige, N. Baumgärtner and T. Pune, A stochastic approach to content adaptive digital image watermarking, *International Workshop on Information Hiding*, Vol. LNCS 1768 of *Lecture Notes in Computer Science*, 212-236. Springer Verlag, Dresden, Germany, 29 September-10 October 1999.
- [19] S. Belkacem, Z. Dibi, A. Bouridane, Luminance-model for spread spectrum image watermarking, *4th International Conference on Computer Integrated Manufacturing CIP'2007*, Setif, Algeria November 03-04, 2007.
- [20] W. Zeng and B. Liu, A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images, *IEEE Transaction Image Process*, 8(11), 1534–1548, Nov. 1999.
- [21] H. Guo, N. D. Georganas, Multi-resolution image watermarking scheme in the spectrum domain, *Proceedings of the IEEE Canadian Conference on Electrical & Computer Engineering*. 2002.
- [22] C.H. Huang, J.L. Wu, Fidelity-controlled robustness enhancement of blind watermarking schemes using evolutionary computational techniques, *International Workshop on Digital Watermarking 2004 (IWDW 2004)*, Seoul, Korea, October, 2004.
- [23] S. Belkacem, Z. Dibi, A. Bouridane, Masking model for image watermarking, *The 4th International Summer School on Signal Processing & it's Applications*, 30 June-4 July Boumerdes (UMBB), Algeria 2007.
- [24] S. Belkacem, S. Khaldi, Z. Dibi, & A. Bouridane, Z. Amrani, Image watermarking algorithm based on perceptual masking and chaotic map, *10th Maghrebian Conference on Information Technologies, MCSEAI*, April 28-30 Oran, Algeria, 2008.

- [25] G. Voyatzis and I. Pitas, Chaotic watermarks for embedding in the spatial digital image, International Conference on Image Processing, ICIP, 432 - 436, 4-7 Oct 1998.
- [26] F. Hartung, M. Kutter, Multimedia watermarking techniques, Proceedings of The IEEE, 87(7), 1079 - 1107, July 1999.
- [27] Y.T. Wu, F.K. Shih, Digital watermarking based on chaotic map and reference register, Elsevier, Pattern Recognition, 40, 3753-3763, 2007.
- [28] W. Xiao, Z. Ji, J. Zhang, W. Wu, A watermarking algorithm based on chaotic encryption, Conference on Computers, IEEE, Communications, Control and Power Engineering TENCON Proceedings, 545-548, 2002.
- [29] D. Taskovski, S. Bogdanova and M. Bogdanov, Adaptive watermarking for digital image protection, XII Telekomunikacioni forum TELFOR 2004, Beograd, Sava Centar, 2004.
- [30] M. Barni, F. Bartolini, Watermarking systems engineering enabling digital assets security and other applications, CRC Press, Boca Raton, 2004.
- [31] StirMark: <http://www.petitcolas.net/fabien/watermarking/stirmark/>

Chapitre IV: Les algorithmes développés de tatouage des images dans le domaine DCT

Introduction

La transformée en cosinus discrète est l'une des techniques permettant la conversion du signal temporel en coefficients fréquentiels. Cette technique est largement utilisée dans le domaine de la compression des données et du traitement d'image. Plusieurs travaux ont été proposés sur des méthodes de tatouage numérique dans la littérature qui sont basées sur le domaine de DCT. Dans ce chapitre, quelques notions de la théorie de la DCT sont données. Une étude comparative entre les coefficients DCT est réalisée. Deux systèmes de tatouage chaotiques des images numériques dans le domaine DCT sont proposés, avec leurs résultats de simulation.

1. La transformée en cosinus discrète

La transformée en cosinus discrète (DCT) est largement utilisée dans le traitement numérique du signal et de l'image. C'est une transformation mathématique qui transforme un ensemble de données du domaine spatial au domaine fréquentiel et inversement par l'IDCT (Inverse Discrete Cosine Transform). Dans ce qui suit on va présenter les équations mathématiques de la DCT et de l'IDCT avec leurs propriétés.

1.1. La forme mathématique de la DCT

La transformée en cosinus discrète (DCT) a été la première fois présentée en 1974 par Ahmed et al. [1]. Dans cette transformation chaque pixel de l'image est transformé en coefficient de DCT. La transformée DCT s'applique sur un signal discret. Les coefficients $F(u, v)$ de DCT, d'une image de pixel $f(i, j)$ est donnée par [2], [3]. Les formules mathématiques de la transformation directe et inverse sont présentées ci-dessous:

- Transformée DCT direct

$$F(u, v) = C(u)C(v) \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} f(i, j) \cos \left[\frac{\pi(2i+1)u}{2m} \right] \cos \left[\frac{\pi(2j+1)v}{2n} \right] \quad (IV.1)$$

- Transformée DCT inverse

$$f(i, j) = \sum_{u=0}^{m-1} \sum_{v=0}^{n-1} C(u)C(v)F(u, v) \cos \left[\frac{\pi(2i+1)u}{2m} \right] \cos \left[\frac{\pi(2j+1)v}{2n} \right] \quad (IV.2)$$

où

$$\begin{cases} C(u) = \frac{1}{\sqrt{m}} \text{ lorsque } u = 0 \\ C(u) = \sqrt{\frac{2}{m}} \text{ lorsque } 0 \leq u \leq m - 1 \end{cases} \quad (IV.3)$$

et

$$\begin{cases} C(v) = \frac{1}{\sqrt{n}} \text{ lorsque } v = 0 \\ C(v) = \sqrt{\frac{2}{n}} \text{ lorsque } 0 \leq v \leq n - 1 \end{cases} \quad (IV.4)$$

m et n représentent le nombre des lignes et de colonnes de l'image respectivement.

1.2. Distribution des coefficients DCT

L'application de la DCT sur un bloc de taille 8×8 pixels est un bloc de 8×8 coefficients, qui donne un total de 64 coefficients de DCT. Le coefficient DC, qui est situé au coin gauche supérieur, tient la majeure partie de l'énergie d'image. Les 63 coefficients restants sont désignés sous le nom des coefficients ac.

Pour illustrer les coordonnées et l'ordre de la distribution des coefficients DCT, nous donnons l'exemple 8×8 de DCT comme il est montré dans la figure(IV.1).

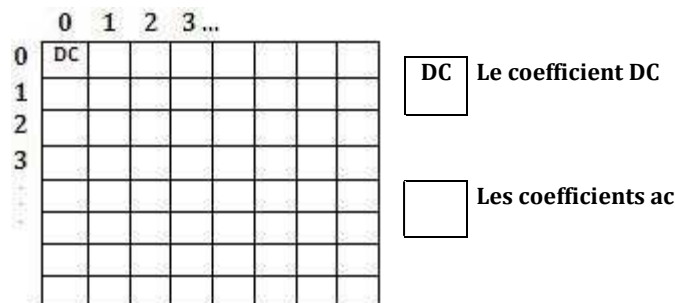


Figure IV. 1 : Ordre des coefficients DCT

Dans la figure (IV.2), nous montrons les amplitudes de DCT pour différentes valeurs de fréquences spatiales pour les images peppers, f16, boat et baboon.

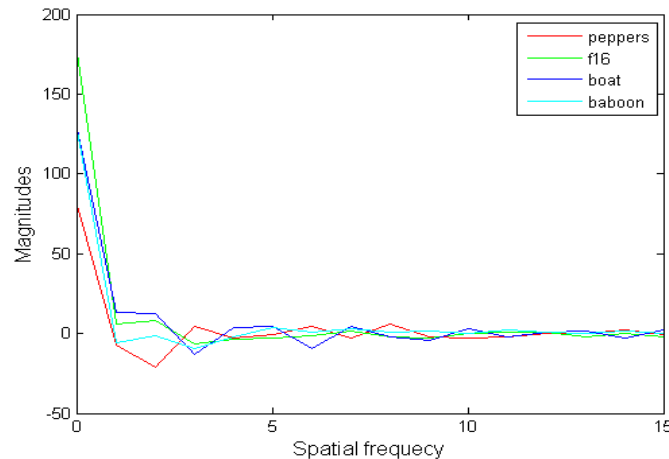


Figure IV. 2 : Amplitude des coefficients DCT

On note que, la distribution d'énergie se concentre aux coefficients de basse fréquence. L'amplitude du coefficient DC est beaucoup plus grande que celle de tous les coefficients ac. En général les composants de basse fréquence contiennent plus d'énergie que les composants à haute fréquence.

1.3. Propriétés de la DCT

La transformée en DCT appliquée en traitement des images possède les propriétés suivantes [4], [5] :

1.3.1. La décorrélation

Les coefficients sont fortement décorrélés dans le domaine transformé.

1.3.2. Concentration de l'information

Dans la transformée DCT, la plus grande partie de l'information contenue dans une image est concentrée dans un nombre réduit de coefficients. C'est-à-dire elle condense tous les coefficients non nuls dans le quart supérieur gauche de la surface du bloc transformé.

1.3.3. Séparabilité

$F(u, v)$ peut être calculé en deux étapes, par les opérations successives unidimensionnelles (1D) sur les lignes et les colonnes de l'image, comme le montre la figure (IV.3).

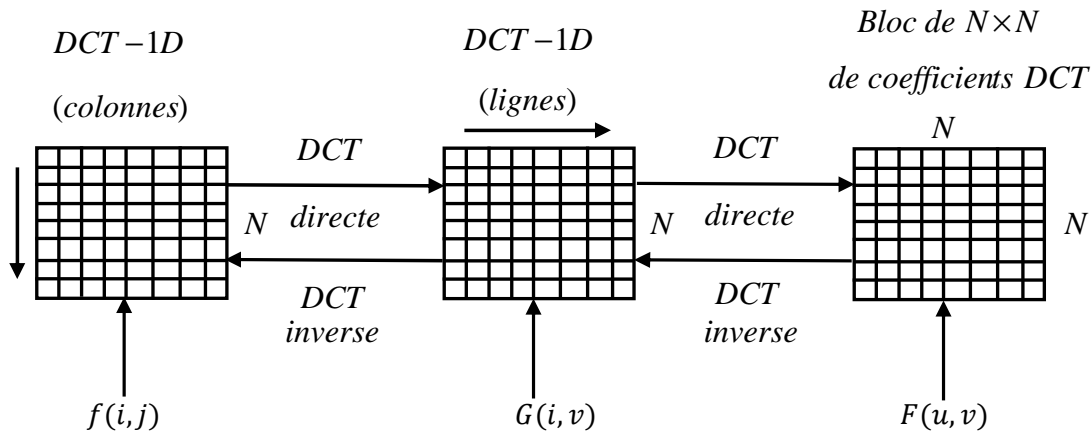


Figure IV. 3 : Calcul de la 2D-DCT par l'utilisation de la séparabilité

1.3.4. Réversibilité

La DCT transforme un tableau de valeurs numériques en un autre de la même taille et d'une façon réversible. Il s'agit le bloc de pixels initiaux est reconstitué par l'application de la transformation inverse au bloc des coefficients.

1.4. Pourquoi la DCT?

Les méthodes de tatouage des images numériques dans le domaine transformé, et particulièrement dans le domaine (DCT), sont plus populaires pour les raisons suivantes [6], [7], [8], [9] :

1. Les propriétés du système visuel humain (HVS) peuvent être insérées au tatouage dans le domaine transformé plus efficacement.
2. L'énergie du signal incluse dans le domaine transformé sera répartie sur tous les pixels dans le domaine spatial. C'est un avantage à l'invisibilité.
3. Ils peuvent être mis en application dans le domaine compressé depuis la plupart des normes internationales de compression d'image et de vidéo, telles que JPEG et MPEG.

2. Etat de l'art sur le tatouage d'image dans la DCT

Les algorithmes de tatouage d'image se regroupent en deux catégories. Le premier groupe de méthodes fonctionne dans le domaine spatial qui consiste à changer les niveaux de gris de quelques pixels. Un autre groupe de techniques modifie les coefficients dans le domaine transformé.

La méthode proposée dans [10] utilise les caractéristiques HVS pour garantir l'invisibilité de la marque. Elle assure l'invisibilité au moyen de filtrage du filigrane à insérer avec un filtre qui rapproche les caractéristiques fréquentielles du HVS. Dans les travaux traités dans [11], la séquence du watermark est insérée dans les 1000 coefficients de la plus grande valeur de la transformée DCT en excluant le coefficient DC. Le processus de détection est basé sur la soustraction entre l'image tatouée et l'image originale. Le choix des coefficients DCT de l'image où l'insertion aura lieu est une autre issue qui a été l'objectif de plusieurs travaux [12], [13]. Barni et al. [12] ont proposé un algorithme de tatouage utilisant les coefficients ac en excluant le coefficient DC. Celui dans [13] choisit les coefficients pour faire l'insertion dans le domaine transformé, tel que la transformée de Fourier discrète (DFT), la transformée en cosinus discret (DCT), transformé en ondelette discrète (DWT), en basant sur le seuil de perception JND (Just Noticeable Difference), le seuil de visionnement des particuliers et des caractéristiques locales d'image. Huang et al. [14], ont proposé un schéma de tatouage où la marque est insérée d'une manière multiplicative dans le coefficient DC de la transformée DCT par l'utilisation d'un masque visuel qui caractérise les zone texturées. La détection du watermark est basée sur l'utilisation de la corrélation. Dans [15], les auteurs ont proposés une méthode qui combine entre la décomposition en valeur singulière (SVD) et la transformée DCT. Dans cette algorithme, seulement les valeurs singulières de la maque qui sont insérées dans les coefficients DCT de l'image originale. Dans les travaux proposés dans [16], les coefficients bas dans le domaine de DCT contiennent la partie majeure d'information portée par l'image. En outre ces coefficients sont moins affectés par la quantification JPEG. A fin de rendre les filigranes imperceptibles au système visuel humain (HVS) l'insertion doit se faire dans les coefficients de haute fréquence de l'image. Dans les travaux présentés dans [17] les informations de la texture, la luminance, corner et les contours sont considérées pour la génération du masque qui permet l'insertion d'un filigrane d'une manière moins perceptible à l'œil humain.

Des améliorations de performance du système du tatouage peuvent être obtenues en exploitant les caractéristiques du HVS dans le processus de tatouage.

3. Etude comparative des algorithmes de tatouage d'image dans le domaine DCT

Dans cette section deux parties sont traitées qui font l'objectif d'un travail étudié dans [8] : la première partie c'est une étude comparative entre le coefficient DC et les coefficients moyens (les coefficients bas du ac) ; et dans la deuxième partie un algorithme du tatouage basé sur le coefficient DC et le système HVS est donné.

3.1. Etude comparative entre DC et les coefficients moyens

Dans ce travail [8] on propose un système de tatouage, où la méthode d'insertion est similaire à [6], et on exploite le masque visuel qu'on a déjà le proposé dans [13] qui contient les deux informations ; la luminance et la texture. De cette manière on augmente la valeur du facteur d'insertion et on ne dégrade pas la qualité de l'image ; la carte logistique est utilisée pour la conception du watermark.

3.1.1. Insertion du watermark

L'algorithme d'insertion du watermark peut s'expliquer comme suit :

Les coefficients d'un bloc 8×8 DCT, qui sont choisis pour l'insertion du watermark doivent vérifier la relation $5 \leq u + v \leq 8$, sont montrées sur la figure (IV.4).

Etape 1 : Produire une séquence de longueur $(\frac{m}{8} \times \frac{n}{8}) \times 22$ selon la carte logistique.

Etape 2 : Dans la deuxième étape, l'image est divisée en des blocs de taille 8×8 , et chaque bloc est indépendamment transformé dans le domaine DCT, afin d'améliorer la robustesse de l'algorithme.

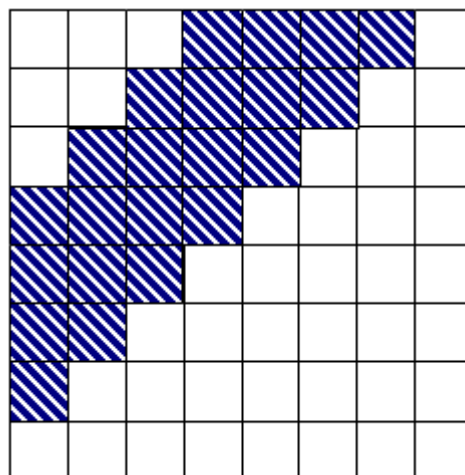


Figure IV. 4 : Les coefficients DCT où le watermark est inséré

Etape 3 : En basant sur la position du pixel, l'insertion du filigrane est faite en utilisant les formules (IV.5) et (IV.6) :

Pour le coefficient DC de chaque bloc, la formule d'insertion est la suivante :

$$I_{w1}(u, v, b) = \begin{cases} I(u, v, b) + \alpha \cdot w & \text{Si } u = v = 0 \\ I(u, v, b) & \text{sinon} \end{cases} \quad (\text{IV.5})$$

Pour les coefficients moyens, la formule d'insertion est donnée par l'équation (IV.6):

$$I_{w2}(u, v, b) = \begin{cases} I(u, v, b) + \alpha \cdot w & \text{Si } 5 \leq u + v \leq 8 \\ I(u, v, b) & \text{sinon} \end{cases} \quad (\text{IV.6})$$

où :

$I_w(u, v, b)$: Représente les coefficients modifiés de DCT dans les coordonnées (u, v) pour le bloc b ;

$I(u, v, b)$: Désigne le coefficient DCT dans les coordonnées (u, v) pour le bloc b ;

Etape 4 : L'inverse de la DCT2 est appliqué à chaque bloc, et enfin on obtient l'image tatouée.

3.1.2. Extraction de filigrane

L'extraction de filigrane est le processus inverse de l'algorithme d'insertion décrit ci-dessus. En cours d'extraction, on doit connaître le filigrane inséré et l'image hôte ; et la détection est effectuée dans le domaine DCT comme suit :

Pour les coefficients de fréquence DC l'extraction est définie par :

$$w' = \frac{I_{w1} - I}{\alpha} \quad \text{si } u = v = 0 \quad (\text{IV.7})$$

Pour les coefficients moyenne l'extraction est définie par :

$$w' = \frac{I_{w2} - I}{\alpha} \quad \text{si } 5 \leq u + v \leq 8 \quad (\text{IV.8})$$

L'étape finale du processus d'extraction est de mesurer la similarité entre le filigrane original w et le filigrane extrait w' . La fonction de similarité est donnée par l'équation suivante:

$$sim = \frac{\sum_m \sum_n (w(i, j) - \bar{w}) \cdot (w'(i, j) - \bar{w}')}{\sqrt{\sum_m \sum_n (w(i, j) - \bar{w})^2 \cdot (\sum_m \sum_n (w'(i, j) - \bar{w}')^2)}} \quad (\text{IV.9})$$

où w, w' sont le filigrane inséré et extrait, et \bar{w} et \bar{w}' représentent la valeur moyenne du filigrane original et extrait, respectivement. Une grande valeur de sim est obtenue, lorsque les deux watermark sont plus semblable.

3.1.3. Comparaison visuelle

Sur la figure (IV.5) on compare l'invisibilité des images tatouées, en utilisant le coefficient DC et les coefficients moyens pour le tatouage, où le PSNR des deux images tatouées est fixé à 40dB.



(a)

(b)

(c)

Figure IV. 5 : Comparaison d'invisibilité par l'insertion du filigrane dans le DC et les coefficients moyens, (a) : Image originale Watch, (b) : Image tatouée en utilisant les coefficients DC ($\alpha=0.1$), (c) : Image tatouée en utilisant les coefficients moyens ($\alpha=0.022$)

Le filigrane n'est pas visible dans les images tatouées. Pour cet exemple, la valeur de $\alpha=0.022$ pour les coefficients moyens, et 0.1 pour les coefficients de DC. Les valeurs de α utilisées dans les coefficients moyens est plus faible comparés à celle utilisé dans les coefficients de DC, pour l'obtention de la même valeur du PSNR.

3.1.4. Test de robustesse

Le système de tatouage devrait être robuste contre aux attaques des données. Il devrait être pratiquement impossible aux utilisateurs non autorisés de l'enlever ou le détecter. Ces attaques incluent la compression JPEG et le filtrage médian, elles sont montrées sur la figure (IV.6).

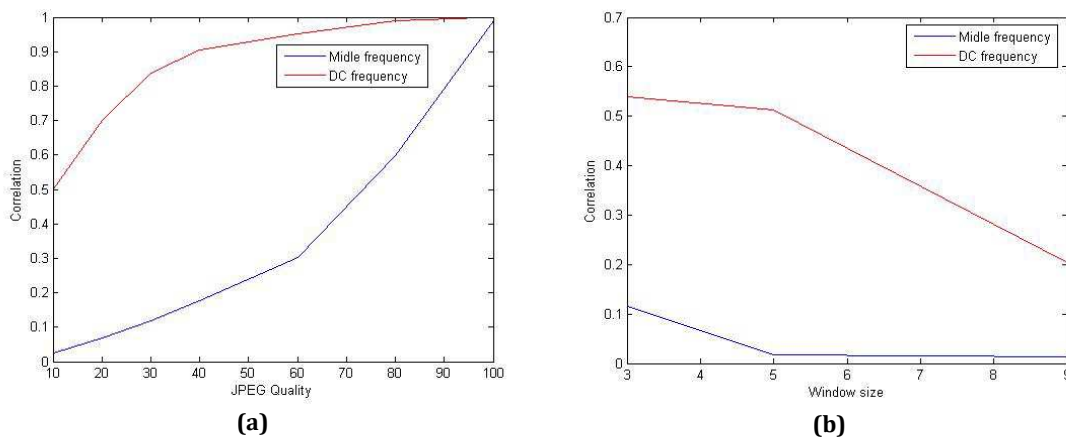


Figure IV. 6 : Test de robustesse (a) : Compression JPEG, (b) : Filtrage médian

Les résultats de simulation ont montré que l'insertion du filigrane dans les coefficients DC porte moins de dégradation perceptuelle et plus de robustesse plutôt que dans les coefficients de fréquence moyenne.

3.2. Algorithme du tatouage d'image basé sur le DC et le HVS

Vu les avantages présentés par les coefficients DC de la transformée DCT, on propose de les utiliser pendant l'étape d'insertion pour le tatouage d'image numérique. Le filigrane est généré par l'utilisation de la carte skew tent, et le système est implémenté en trois étapes:

3.2.1. Insertion du filigrane

L'algorithme d'insertion du filigrane peut être décrit comme suit :

Etape 1 : D'abord, produire d'une séquence de taille $\frac{m}{8} \times \frac{n}{8}$ selon la carte skew tent écrite sous sa forme récursive suivante [18], [19] :

$h: [0,1] \rightarrow [0,1]$

$$h(b) = \begin{cases} \left(\frac{1}{a}\right)b, & 0 \leq b \leq a \\ \left(\frac{1}{1-a}\right)b + \left(\frac{1}{1-a}\right), & a \leq b \leq 1 \end{cases} \quad a \in [0, 1] \quad (\text{IV.10})$$

Etape 2 : Calculer le masque M de l'image dans le domaine spatial [20], et le divisé en des blocs de taille 8×8 , et chaque bloc est indépendamment transformé dans le domaine transformé par 2D-DCT.

Etape 3 : Dans la troisième étape, diviser l'image en des blocs 8×8 et chaque bloc est indépendamment transformé dans le domaine transformé par 2D-DCT.



Figure IV. 7: (a) : Le masque obtenu par l'image boat ; (b) : Watermark de la taille 32×32

Etape 4 : En se basant sur les coordonnées du pixel, le filigrane est inséré dans les coefficients de DC en utilisant le masque M comme suit :

$$I_w(u, v, b) = \begin{cases} I(u, v, b) + \alpha \cdot w \otimes M & \text{si } u = v = 0 \\ I(u, v, b) & \text{sinon} \end{cases} \quad (\text{IV.11})$$

ici :

$I_w(u, v, b)$: est le coefficient modifié de DCT dans les coordonnées (u, v) pour le bloc b ;

$I(u, v, b)$: est le coefficient de DCT dans les coordonnées (u, v) pour le bloc b ;

$M(u, v, b)$: est le masque dans le domaine de DCT dans les coordonnées (u, v) pour le bloc b ;

où \otimes désigne la multiplication point par point.

Etape 5 : Enfin, l'inverse de la DCT2 est appliqué à chaque bloc, pour obtenir l'image tatouée.

3.2.2. La procédure de détection

La procédure d'extraction est le processus inverse de l'algorithme d'insertion (similaire à celle donnée dans la section 3.1.2).

L'étape finale c'est de mesurer la similarité entre la marque originale et la marque extraite par l'utilisation de l'équation (IV.9).

3.2.3. Résultats de tatouage basé sur DC

Comparaison visuelle

D'abord nous avons évalué la qualité perceptuelle, sur la figure (IV.8) on compare l'invisibilité de l'image tatouée dans le domaine de DCT sans et avec masque en utilisant les coefficients de DC de chaque bloc.

On peut noter que les images originales et tatouées avec notre algorithme sont perceptiblement indistinguables, ceci valide la contrainte d'invisibilité pour des algorithmes efficaces de tatouage.



(a) (b) (c)
 Figure IV. 8 : Comparaison des images, (a) : Image originale, (b) : Image tatouée sans masque PSNR=40.7620dB, (c) : Image tatouée avec masque PSNR = 43.7202dB

Variation de PSNR

On peut observer la variation des valeurs de PSNR avec le changement du facteur α qui varie de 0.1 \rightarrow 1 pour l'image boat sur la figure (IV.9).

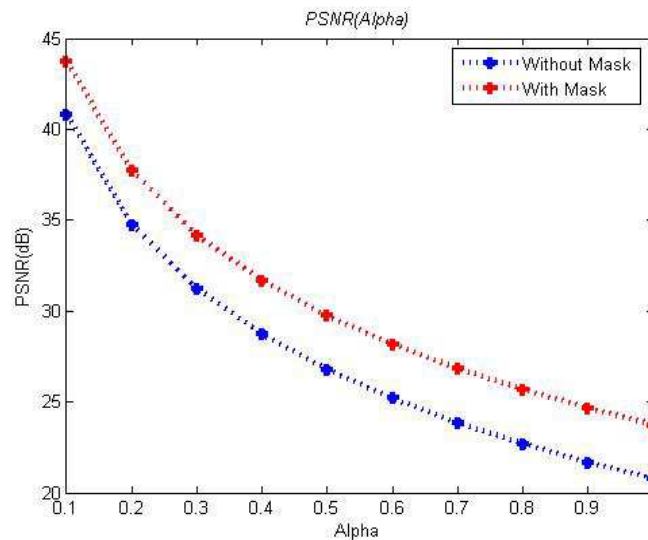


Figure IV. 9 : Comparaison de PSNR entre le système proposé avec le masque et sans masque pour l'image boat

On observe une amélioration apparente du PSNR lorsque la valeur de α change de 0.1 à 1. Pour les images tatouées obtenues par le système proposé lorsqu'on utilise le masque développé, elles ont la meilleure valeur en terme PSNR.

4. Modèle de HVS pour le tatouage d'image dans le domaine DCT

Dans cette approche proposée [21] nous prenons en compte les propriétés locales de l'image et du système visuel humain (HVS), pour le tatouage de l'image numérique dans le domaine DCT.

4.1. Conception du masque

La valeur du masque proposé de luminance à chaque pixel est donnée par l'équation suivante [19]:

$$M_L(i, j) = \left| \frac{I(i, j) - 128}{128} \right| \quad (IV.12)$$

Les valeurs de masque sont tracées sur la figure ci-dessous. Il possède des valeurs dans l'intervalle [0.1].

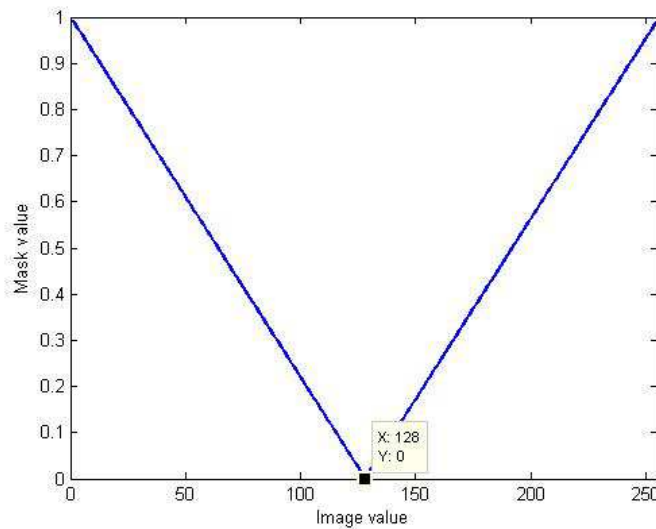


Figure IV. 10 : Valeur de masque

Après l'obtention des deux masques correspondant à la texture M_T (Chapitre III : Section 4) et à la luminance M_L nous produisons le masque final M en utilisant l'équation suivante :

$$M = M_T \otimes M_L \quad (IV.13)$$

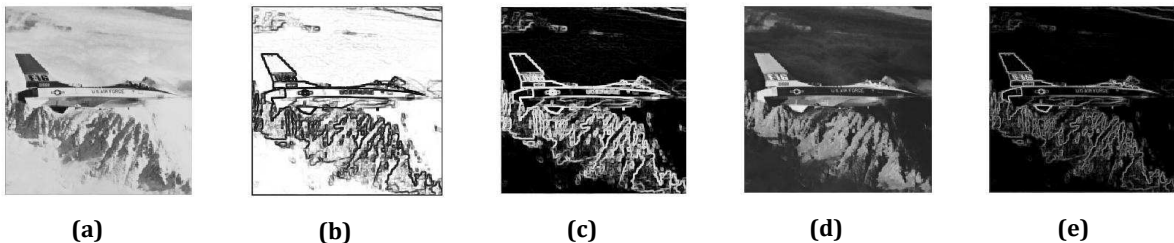


Figure IV. 11 : Le masque visuel proposé, (a) : L'image originale ; (b) : Fonction de visibilité de bruit de f16 ; (c) : Le masque de texture ; (d) : Le masque de luminance proposé ; (e) : Le masque final obtenu

4.2. Stratégie d'insertion

La procédure d'insertion du filigrane est résumée dans les étapes suivantes :

Etape 1 : Générer une séquence d'une taille $m \times n$ (la taille de l'image originale) selon la carte logistique ;

Etape 2 : Puis, calculer le NVF de l'image dans le domaine spatial, pour obtenir le masque de texture, et le divisé en des blocs de taille 8×8 pixels ;

Etape 3 : Dans la troisième étape, l'image est divisée aussi en des blocs de taille 8×8 pixels, et chaque bloc est indépendamment transformé à la 2D-DCT;

Etape 4 : Pour l'image tatouée, lorsque l'information de luminance n'est pas prise en considération (seulement l'information de texture), l'équation de l'insertion du filigrane peut s'écrire comme suit :

$$I_w(u, v, b) = I(u, v, b) + \alpha w(i, j) M_T(i, j, b) \quad (IV.14)$$

Si la luminance et l'information de la texture sont utilisées, l'insertion de filigrane est faite en utilisant l'équation (IV.15) :

$$I_w(u, v, b) = I(u, v, b) + \alpha w(i, j) M(i, j, b) \quad (IV.15)$$

Etape 5 : L'inverse de la DCT2 est appliqué à chaque bloc pour obtenir l'image tatouée.

$M(i, j, b)$: Représente la valeur de masque dans le domaine spatial dans les coordonnées (i, j) pour le bloc b .

4.3. Procédure d'extraction du filigrane

Pour extraire le filigrane inséré, nous calculons la corrélation croisée ($xcorr$) entre l'image tatouée et le filigrane original. Alors la matrice obtenue est comparée à un seuil constant prédéfini ($T_w = 0.03$) pour décider si les éléments du filigrane extrait (w') porte '0' ou '1' en utilisant la formule suivante:

$$w'(i, j) = \begin{cases} 1 & \text{si } xcorr \geq T_w \\ 0 & \text{si } xcorr < T_w \end{cases} \quad (IV.16)$$

L'étape finale du processus d'extraction est de mesurer la similitude entre le filigrane original w et le filigrane extrait w' , par l'utilisation de l'équation (IV.9).

4.4. Evaluation des performances

Les performances de notre schéma proposé de tatouage ont été évaluées à l'aide des images de tests de la taille 256×256 , et le filigrane est de la même taille que l'image hôte. Les simulations sont effectuées dans l'environnement du logiciel MATLAB 7.

Sur la figure (IV.12), on compare l'imperceptibilité des images originales et tatouées dans le domaine transformé DCT, par les deux masques qui sont définis précédemment.

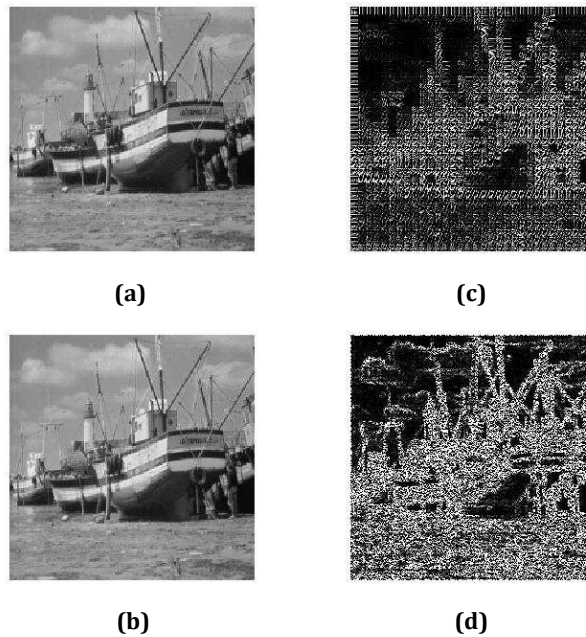


Figure IV. 12 : Comparaison des images, (a) : Image tatouée avec le masque M_L PSNR=40.1958dB, (b) : Image tatouée par le masque M_T PSNR=35.3071dB, (c) ; (d) : La différence entre l'image tatouée et l'image originale amplifiée par un facteur de 100 pour le but de visionnement

On peut observer aussi le changement des valeurs de PSNR lorsque le facteur d'insertion est variable pour les deux méthodes sur la figure (IV.13), lorsque alpha est changé de 0.05→1 pour l'image boat. La variation du PSNR pour la méthode proposée est tracée par la ligne marquée par le symbole de "+", cependant la ligne marquée par "." représente la variation du PSNR lorsqu'on tient compte uniquement de la texture.

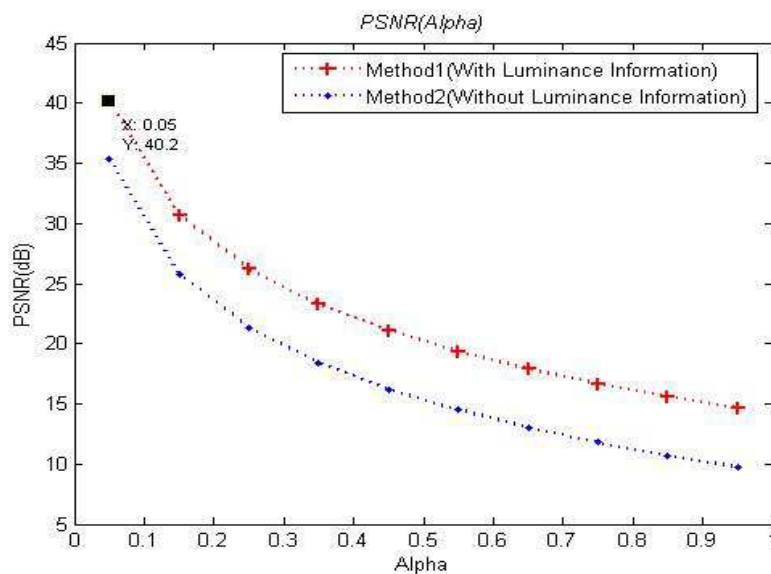


Figure IV. 13 : Comparaison de PSNR entre les deux méthodes

La bande entre les valeurs suggère les performances supérieures de notre nouvel algorithme, et cette amélioration a été observée à partir des expériences multiples.

On note que les images tatouées, qui sont obtenues par notre schéma proposé (texture et luminance), ont la meilleure mesure en terme de PSNR.

L'amélioration en terme de PSNR pour les quatre images de test pour alpha est fixée à 0.05 est donnée dans le tableau ci-dessous.

Image	f16	baboon	Lena	watch
PSNR%	18.5909	15.5925	12.2029	7.6641

Tableau IV. 1 : Le pourcentage d'amélioration en PSNR pour différentes images

L'amélioration obtenue en PSNR% est due à l'efficacité de l'algorithme proposé. D'après les valeurs données par le tableau (IV.1), l'image f16 présente la plus grande valeur d'amélioration en PSNR, nous pouvons dire qu'elle contient beaucoup de valeur de zone texturée et de pixel de valeur 128 que les trois autres images (Lena, watch et baboon). Cet algorithme nous permet d'obtenir une plus grande amélioration en terme de PSNR, lorsque l'image utilisée contient plusieurs pixels de valeurs de 128.

4.5. Test de robustesse

Nous avons évalué la robustesse du système proposé contre quelques attaques sur l'image tatouée telle que l'ajout du bruit, et la compression JPEG, pour chaque attaque les différentes corrélations sont évaluées. La variation de corrélation pour chaque attaque est donnée sur la figure ci-dessous.

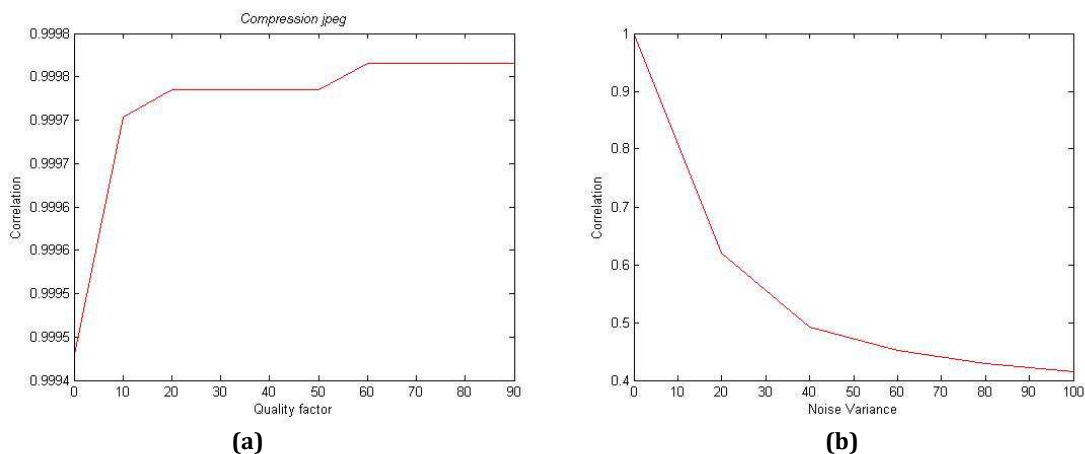


Figure IV. 14 : Test de robustesse (a) : Compression JPEG, (b) : L'ajout du bruit

Des bruits de différentes valeurs de force (10%, 20%, 40%, 60%, 80% et 100%) sont ajoutés à l'image tatouée pour évaluer la robustesse de la méthode. Sur la figure (IV.14b)

on montre le résultat obtenu, on peut dire qu'une augmentation de la valeur de la force de bruit donne une diminution de la valeur de la corrélation. Ceci est prévu, cependant la valeur de la corrélation reste acceptable pour les bruits avec une force inférieure à 10% et présente presque une valeur de corrélation égale à 1.

D'après la figure (IV.14), le schéma proposé est robuste contre les attaques communes, telles que la compression JPEG et l'ajout de bruit.

Conclusion

Les algorithmes que nous avons développés dans ce chapitre sont basés sur l'utilisation des masques conçus pour le tatouage chaotique de l'image dans le domaine DCT. Les résultats de simulation ont prouvé que l'utilisation de l'approche du masque spatial et le choix des coefficients de la transformée DCT à tatouer ; permet d'insérer des filigranes d'une énergie plus élevée et qui ne dégrade pas la qualité de l'image tatouée.

Bibliographie

- [1] N. Ahmed, T. Natarajan, and K.R. Rao, Discrete cosine transform, IEEE Transaction on Computer, C-23, 90-93, Jan.1974.
- [2] N. Roma, L. Sousa, A tutorial overview on the properties of the discrete cosine transform for encoded image and video processing, Signal Processing, 91, 2443-2464, 2011.
- [3] C.H. Yuen, K.W. Wong, A chaos-based joint image compression and encryption scheme using DCT and SHA-1, Applied Soft Computing, 11, 5092-5098, 2011.
- [4] I. Bouklihacene, Compression d'images médicales par ondelettes de seconde génération, Thèse de Doctorat, Université de Tlemcen, 2014.
- [5] N. Brahim, Développement et implémentation des algorithmes de compression d'image basé sur des transformées entières, Mémoire de Magister, Université Ferhat Abbas, 2011.
- [6] J. Huang, Y.Q. Shi, Embedding strategy for image watermarking in DCT domain, Electron. Lett, 34, 748-750, April 1998.
- [7] S. Belkacem, Z. Dibi, A. Bouridane, Efficient image watermarking using Noise visibility Function, Internationnal Multi-conference on Systems, signal & Devices-Tunisia, 19-22 March, 2007.

- [8] S. Belkacem, Z. Dibi, A. Bouridane, A comparative study of DCT image watermarking algorithms, 3^{èmes} Journées Internationales sur l'Informatique Graphique, JIG'2007, Constantine, Algeria, October-29-30, 2007.
- [9] B.Tao, B. Dickinson, Adaptive watermarking in the DCT domain, IEEE International Conference on Acoustics, Speech, and Signal Processing, 4, 2985 – 2988, 1997.
- [10] M.D. Swanson. B. Zhu, A.H. Tewfik, Transparent robust image watermarking, IEEE International Conference On Image Processing, 3, 211-214, 1996.
- [11] I.J. Cox, J. Kilian, T. Leighton, and T.G. Shamoan, Secure spread spectrum watermarking for multimedia, In Proceedings of the IEEE International Conference on Image Processing, ICIP, 6, 1673 –1687, Santa Barbara, California, USA, October 1997.
- [12] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, A DCT-domain system for robust image watermarking, Signal Processing, 66(3), 357–372, 1999.
- [13] R.B. Wolfgang, C.I. Podilchuck and E.I. Delp, Perceptual watermarks for digital images and video, Proc. of IEEE, 87, 1108-1126, July 1999.
- [14] J. Huang, Y.Q. Shi, and Y. Shi, Embedding image watermarks in DC components, IEEE Transactions On Circuits And Systems For Video Technology, 10(6), 974 – 979, September 2000.
- [15] C.H. Huang and J.L. Wu, Attacking visible watermarking schemes, IEEE Transactions on Multimedia, 16–30, 2004.
- [16] I. Retsas, R. Pieper, R. Cristi, Watermark recovery with a DCT Based scheme employing nonuniform imbedding, IEEE Symposium on System Theory, proceedings of the Thirty-Fourth Southeastern, 157 – 161, 2002.
- [17] A.K. Parthasarathy and S. Kak, An improved method of content based image watermarking, IEEE Transactions On Broadcasting, 53(2), 468 – 479, 2007.
- [18] A. Mooney, J. G. Keating and I. Pitas, A comparative study of chaotic and white noise signals in digital watermarking, Chaos, Solitons and Fractals, 35, 913–921, 2008.
- [19] P. Stavroulakis, Chaos applications in telecommunications, Published by CRC Press, 2006.
- [20] S. Belkacem, Z. Dibi, A. Bouridane, Masking model for image watermarking, Summer School. Boumerdes, 30 jun-04 July, Algeria, 2007.
- [21] S. Belkacem, Z. Dibi, A. Bouridane, A masking model of HVS for image watermarking in the DCT domain, IEEE, International Conference on Electronics, Circuits and Systems, Marrakech, Morocco December 11-14, 2007.

Chapitre V : Les algorithmes développés de tatouage des images dans le domaine DWT

Introduction

Dans ce chapitre, on commence par une description de la transformation en ondelette DWT, puis nous présentons les différents algorithmes de tatouage d'images qui sont développés dans ce domaine. Quatre algorithmes sont proposés dans le domaine DWT, dans le premier travail, on utilise le masque qui est déjà développé dans [1] pour le tatouage de l'image dans le domaine DWT [2]. Le second algorithme c'est une amélioration du masque proposé dans [1] par l'utilisation de la notion de la sélection de la valeur minimale [3]. Dans le troisième algorithme, on utilise la notion de l'image auto-référence pour l'insertion du filigrane dans le domaine des ondelettes [4] et dans le quatrième travail, le masque [1] est utilisé, mais la procédure de la détection est basée sur les propriétés statistiques de l'image tatouée [5].

1. La théorie des ondelettes

La question qui peut être posée : « quel est l'avantage d'utiliser une transformation en ondelette plutôt qu'une transformation discrète en cosinus ? » Malgré le grand succès de la TCD (Transformation en Cosinus Discrète), la transformée en ondelettes a pris un grand chemin dans différents domaines de recherche. Celle-ci nous amène à penser qu'elle fournit une réponse correcte au problème du traitement d'images. En effet l'image se trouve, grâce à l'analyse en ondelettes décomposée en informations indépendantes (détails de basses fréquences et détails de hautes fréquences). La décomposition donnée par la transformée d'ondelette augmente la résolution spatio-fréquentielle, mais cette décomposition reste toujours figée car les basses fréquences sont décomposées à chaque fois quelque soit les caractéristiques de l'image [6].

Depuis les travaux de Grossman et Morlet, la transformation en ondelettes est apparue comme un outil performant permettant de résoudre des problèmes relevant de différents domaines d'application. Très tôt, un intérêt soutenu c'est manifesté à l'égard

de la Transformée en ondelettes en traitement d'images. La notion d'ondelettes ou wavelets a été utilisée pour la première fois au début des années 80 par le géophysicien français J. Morlet pour désigner des fonctions mathématiques utilisées dans la représentation des données sismiques [7].

L'analyse par ondelettes est un outil mathématique capable de transformer un signal d'énergie finie dans le domaine spatial en un autre signal d'énergie finie dans le domaine spatio-fréquentiel. Les composantes de ce nouveau signal sont appelées les coefficients d'ondelettes. Ces coefficients renseignent sur la variation locale des niveaux de gris autour d'un pixel donné de l'image. Ils sont d'autant plus grands que cette variation est importante [8].

Les ondelettes, famille de fonctions déduites d'une même fonction, appelée ondelette mère, par opérations de translations, dilatations et rotations, sont nées de l'analyse des signaux sismiques haute résolution. Cet outil puissant a ensuite été développé, tant du point de vue pratique que du point de vue théorique, par des chercheurs tels Y. Meyer, Daubechies, S. Mallat, P.G. Lemarié, Morlet ...etc. pour aboutir à la théorie de l'analyse par ondelettes telle qu'elle existe aujourd'hui [9].

2. Les propriétés d'ondelettes

Dans la section suivante on donne les propriétés de la transformée en ondelettes [10].

- Sélectivité en fréquence

Dans la transformée de Fourier, la fonction utilisée pour analyser le signal étudié est une fonction sinusoïdale de fréquence précise, et quand on la multiplie par le signal, le coefficient obtenu ne se réfère qu'à cette fréquence. En revanche, une ondelette est constituée de plusieurs fréquences. Les coefficients d'ondelettes se réfèrent à ce mélange de fréquences. Plus la gamme de fréquence de l'ondelette est étroite, plus l'ondelette est sélective en fréquence.

- Similarité

Toutes les ondelettes qui appartiennent à la même famille doivent être similaires, c'est à dire se déduire les unes des autres par combinaison linéaire de translations et de dilatations.

- Symétrie

On souhaite parfois que l'ondelette présente des propriétés de symétrie temporelle afin d'éviter le déphasage dans la transformée en ondelettes.

- Orthogonalité

Cette propriété est à l'origine de la popularité des ondelettes qui offrent des bases d'ondelettes orthogonales et non redondantes. Cela conduit à une décomposition unique.

- Régularité

Une ondelette doit être suffisamment régulière car c'est la principale contribution des ondelettes dans le domaine du codage. Elle agit sur la qualité de la reconstruction du signal. Une ondelette est dite régulière si elle est très lisse et on peut l'approximer localement par un polynôme. L'ordre de régularité d'une ondelette est égal au nombre de ses moments nuls.

- Nombre de moments nuls

Pour certaines applications, les ondelettes doivent également avoir un certain nombre de moments nuls, afin d'éliminer la partie polynomiale du signal et être ainsi plus sensible aux fluctuations les moins régulières.

- Facteur d'échelle minimal

Théoriquement le facteur d'échelle, a , qui est strictement positif, peut varier jusqu'à $+\infty$. En pratique, Il convient de se fixer un nombre de points de discrétisation minimum, \min , de telle sorte que les valeurs discrètes de l'ondelette soient représentatives de sa forme continue.

3. Représentation des coefficients d'ondelettes

L'application de la transformée en ondelettes discrète (DWT) sur une image numérique, donne une image divisée en quatre sous-bandes. Il s'agit d'une sous-bande d'approximation LL et trois sous-bandes de détails : LH, HH et HL, correspondant, respectivement aux détails verticaux, diagonaux et horizontaux. La lettre H correspond au filtrage passe haut et la

lettre L à celui du passe bas appliqués de façon séparable sur les lignes et les colonnes. La décomposition de la sous-bande d'approximation LL permet d'obtenir une représentation sous forme pyramidale [11]. Sur la figure (V.1) on donne un exemple de la décomposition d'une image par trois niveaux de décomposition en DWT.

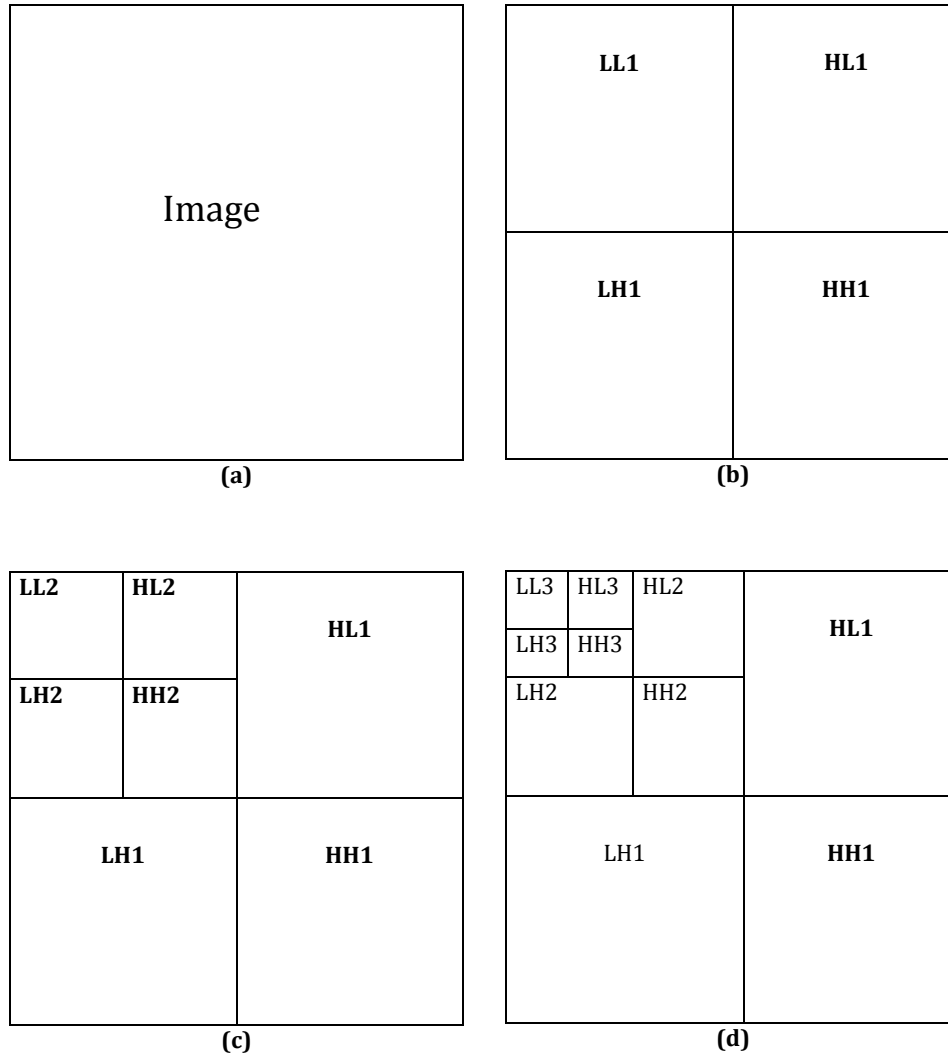


Figure V. 1 : Décomposition d'une image par DWT :(a) : Image à décomposer, (b) : Niveau 1 ;(c) : Niveau 2 ; (d) : Niveau 3

Un exemple de la décomposition en ondelette discrète appliqué en deux niveaux sur l'image de test nommée boat est donné sur la figure (V.2).

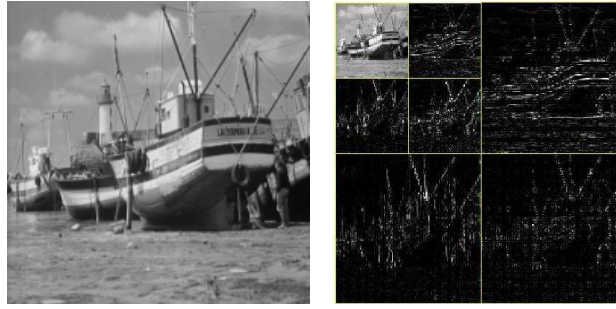


Figure V. 2 : Décomposition en ondelette niveau 2 pour l'image boat

4. Quelques algorithmes de tatouage d'image utilisant la transformée en ondelettes

Les transformées en ondelettes qui, tout comme la transformée DCT fait l'objet de nombreuses études dans le contexte du traitement du signal et de l'image, ont également trouvé un écho dans la communauté du tatouage. Le principe de tatouage numérique dans le domaine d'ondelettes, consiste à décomposer l'image en utilisant la transformée en ondelettes DWT puis à insérer une marque dans une résolution donnée. L'enjeu le plus important dans le tatouage d'image basé sur la DWT est de savoir comment choisir les coefficients à tatouer et de combien d'énergie peut être insérée.

Barni et al. dans leurs travail [12] ont été basé sur les caractéristiques du HVS pour l'insertion du watermark dans le domaine d'ondelettes. Le filigrane a été détecté par le calcul de la corrélation entre les coefficients tatoués et le filigrane inséré. Cette méthode a inclus l'image de filigrane dans la sous-bande de HH du premier niveau, et cette sous-bande n'était pas robuste à certaines attaques comme la compression JPEG, et au filtrage passe bas. Zhang et al. [13] divisent l'image originale en des blocs, puis chaque bloc est transformé par DWT. La moyenne et la variance des sous-bands sont utilisées pour sélectionner les coefficients à modifier. Dans les travaux proposés dans [14] le schéma de tatouage était basé sur le domaine d'ondelettes. L'image à tatouer est obtenue par l'utilisation de deux niveaux de décomposition en ondelettes. L'insertion du filigrane était faite d'une manière multiplicative. La détection est basée sur la méthode de corrélation entre la marque insérée et la marque extraite. McKinnon et al. [15] ont proposé une technique de tatouage basée sur les ondelettes en quantifiant de manière adaptative une paire de famille d'arbres. Les familles d'arbres ont été créés par un groupe de coefficients d'ondelette des différents niveaux de décomposition le long des

mêmes directions spatiales. Chaque bit de filigrane a été inclus dans diverses bandes de fréquence et donc a été écarté sur des grandes régions spatiales. Les travaux de proposés par [16] présentent une méthode de tatouage basée sur la transformée en ondelettes discrètes pour la protection de copyright de l'image numérique. Les éléments de filigrane ont été ajoutés aux coefficients significatifs de chaque sous-bande en considérant les caractéristiques du système visuelles humaines (HVS). Reddy et al. [17], ont proposé une méthode de tatouage dans le domaine d'ondelettes au moyen de l'ondelette de Haar. L'utilisation du modèle de HVS dans le schéma proposé a eu comme conséquence un algorithme efficace de tatouage.

5. Tatouage d'image basé sur le modèle visuel dans le domaine des ondelettes

Dans cette section, le masque spatial développé dans [1] (Chapitre III :Section 6.3), est utilisé pour la conception d'un algorithme de tatouage chaotique dans le domaine des ondelettes [2].

5.1. Algorithme d'insertion du filigrane

Le diagramme de notre algorithme est donné sur la figure (V.3).

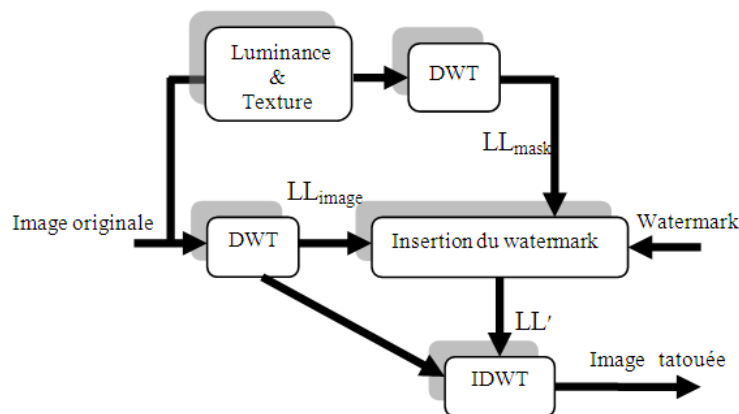


Figure V. 3 : Schéma fonctionnel de la méthode proposée

D'abord nous utilisons une carte logistique pour produire le filigrane. Ensuite, on décompose l'image originale et le masque conçu par DWT en deux niveaux par l'utilisation de l'ondelette de Haar, pour obtenir les coefficients d'ondelettes dans chaque bande ; seulement la bande de basse fréquence (LL) est choisie pour l'insertion du filigrane selon l'équation suivante :

$$LL' = LL_{image} + \alpha w LL_{mask} \quad (V.1)$$

où LL_{image} sont les coefficients d'ondelette de l'image originale, LL_{mask} représente les coefficients d'ondelette du masque produit dans le domaine spatial, w est le filigrane.

L'image tatouée est alors reconstruite en exécutant l'inverse de la transformée en ondelette (IDWT) à toutes les sous-bandes, comme le montre la figure (V.3).

5.2. Détection du filigrane

Le processus de détection se décrit comme suit :

L'image originale et l'image tatouée sont transformées en DWT et décomposées en 2 niveaux en utilisant l'ondelette de Haar. Puis, nous soustrayons les coefficients bas de l'image originale des coefficients bas de l'image tatouée. La valeur de corrélation est calculée entre la différence (d) et le filigrane inséré produit par la clef secrète pour déterminer si l'image contient le filigrane ou non. La formule de la mesure de la valeur de corrélation est donnée par l'équation (III.21) (Chapitre III : Section 5.3)

Les résultats empiriques suggèrent qu'une valeur de seuil de 0.01 devrait être utilisée pour l'image de test.

Une comparaison de la réponse du détecteur dans les deux domaines d'insertions (spatial et DWT) sont données sur la figure (V.4), où nous avons 100 filigranes différents, et le filigrane correcte est désigné par le numéro 10.

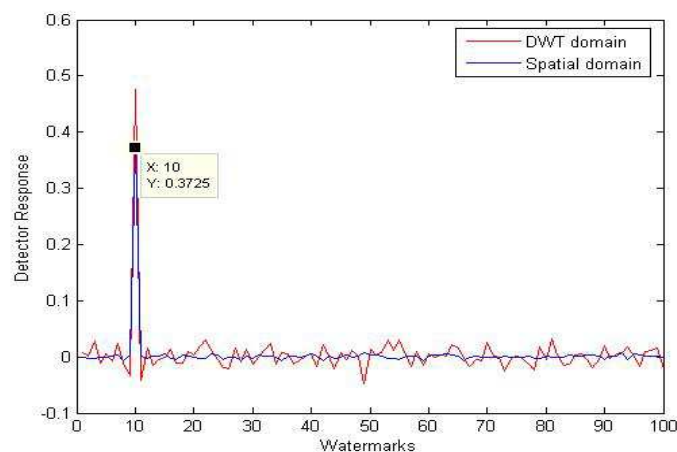


Figure V. 4 : La réponse du détecteur

Il est évident que la valeur de la corrélation dans le domaine DWT pour la méthode proposée soit plus grande que pour la méthode où l'insertion est faite dans le domaine spatial [1].

5.3. Résultats de simulation

Les expériences sont exécutées sur différentes images grises telles que boat, watch, qui sont dans la gamme $[0,1]$, de taille 256×256 . Les données de filigrane sont représentées par l'image binaire 64×64 . Dans les deux techniques, la force de filigrane est ajustée à une valeur de 0.2.



Figure V. 5 : (a) : Image originale, (b) : Le filigrane utilisé 64×64

5.3.1. Mesure de la qualité perceptive

Sur la figure (V.6), on compare l'invisibilité des images tatouées dans le domaine spatial et le domaine transformé (DWT). La différence entre l'image originale et l'image tatouée dans le domaine DWT est donné par la figure (V.6c) ; et sur la figure (V.6d) on donne la différence entre l'image originale et l'image tatouée dans le domaine spatial.

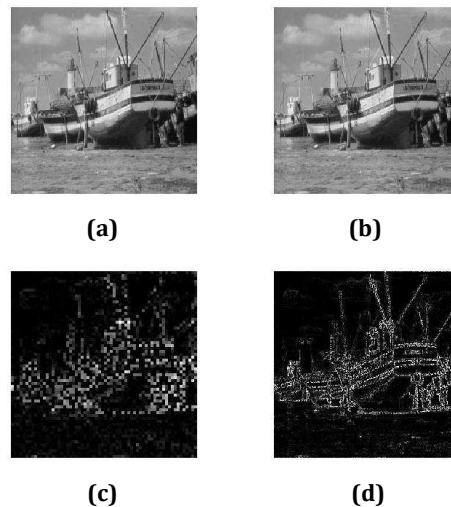


Figure V. 6 : Comparaison des méthodes d'insertion ; (a) : L'image boat tatouée dans le DWT PSNR=40.4808dB, (b) : Image tatouée dans le domaine spatial PSNR = 38.2891dB, (c), (d) : La différence entre l'image tatouée et l'image originale amplifiée par un facteur de 20 pour le but de visionnement

On peut observer le changement des valeurs de PSNR pour l'image boat dans les deux méthodes, lorsque alpha est changé de 0.1 à 0.4 sur la figure (V.7).

L'espace entre les valeurs de PSNR suggère les performances supérieures de notre nouvel algorithme, et cette amélioration a été observée à travers des expériences multiples.

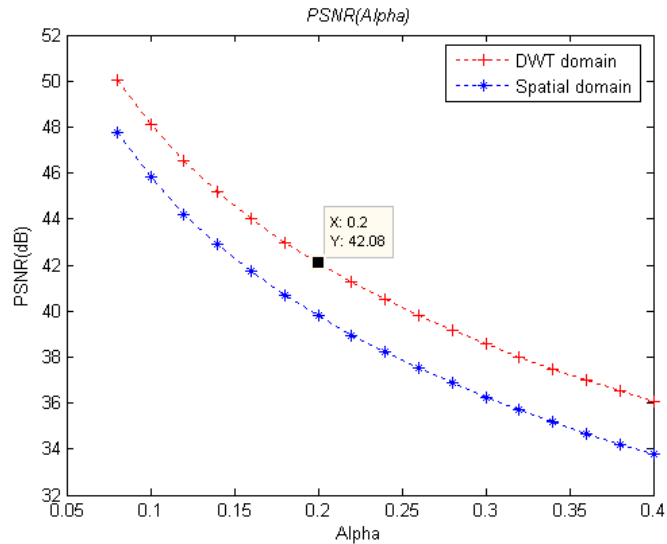


Figure V. 7 : Comparaison de PSNR entre les deux méthodes

Sur le tableau (V.1), on donne les valeurs de PSNR pour la méthode proposée et celle qui se trouve dans [1].

Image	lena	peppers	baboon	f16
PSNR	41.9327	42.0786	40.0879	40.7122
PSNR [1]	39.8590	39.7849	38.6108	38.1745

Tableau V. 1: Mesure de qualité en PSNR

On note que les images tatouées, qui sont obtenues par notre schéma proposé, ont la meilleure valeur en terme de PSNR. L'amélioration obtenue de PSNR est due à l'efficacité de l'algorithme proposé.

5.3.2. Test de robustesse

Nous illustrerons la robustesse de la méthode proposée à plusieurs attaques. Nous avons comparé la robustesse de la méthode développée dans DWT à celle [1], et les résultats du détecteur sont montrés sur la figure (V.8).

Compression JPEG

L'une des attaques les plus importantes auxquelles le filigrane devrait être résistant est la compression JPEG. Pour examiner l'effet de la compression JPEG, nous avons fixé la qualité de compression à 20. La méthode proposée de tatouage maintient une valeur plus élevée de détection que la méthode de [1].

Filtrage médian

L'image tatouée est filtrée avec une fenêtre de taille 5×5 , comme le montre la figure (V.8). La méthode proposée donne un bon résultat en terme de réponse de détecteur comparée à celle proposée dans [1].

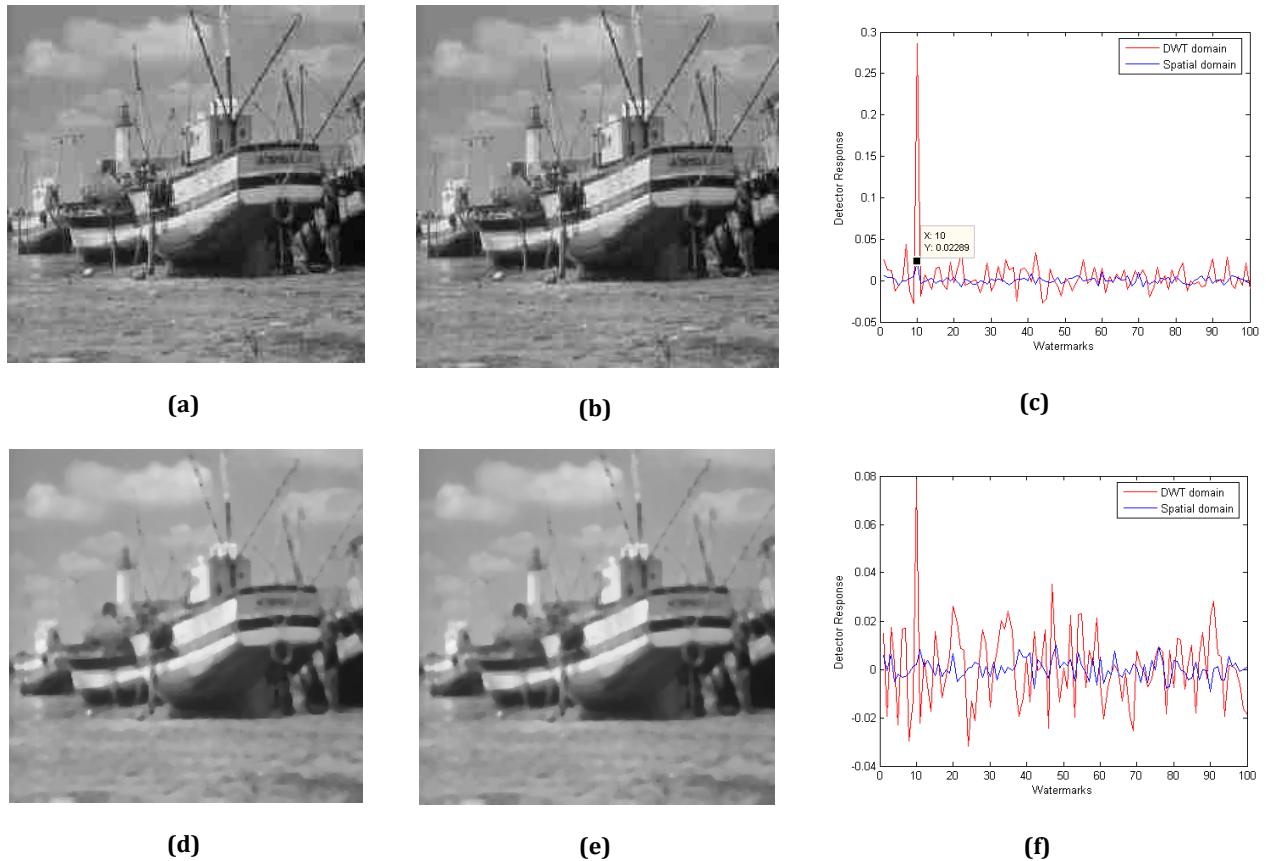


Figure V. 8 : Comparaison de robustesse, (a), (b) et (c) : Image compressée avec un facteur de qualité $Q=20$, (d), (e) et (f) : Filtrage médian avec une fenêtre de taille de 5×5

Il est évident que le coefficient de corrélation pour la méthode proposée soit plus grand par rapport à la méthode de [1], pour le cas de la compression JPEG et du filtrage médian.

6. Schéma de tatouage d'image dans le DWT basé sur la valeur minimale

Dans ce travail [3] le masque de la texture et de la luminance sont développés de la même façon que dans [1], [2] ; où la combinaison entre les deux masques est faite par la multiplication élément par élément pour l'obtention du masque final (*mask1*). Dans ce travail, le masque final (*mask2*) est conçu par le choix de la valeur minimale entre le

masque de la texture et de la luminance. Les procédures d'insertion et de détection sont conçues d'une manière similaire à celle utilisé dans [2]. Une comparaison est faite pour l'évaluation de performance de ce nouveau masque sur un schéma de tatouage complet. La carte de Bernoulli [18] est utilisée pour la conception du filigrane.

Sur la figure (V.9), on représente l'image originale, et le masque obtenu par la méthode proposée dans [1], ainsi que le masque obtenu par la méthode du choix de la valeur minimale successivement.

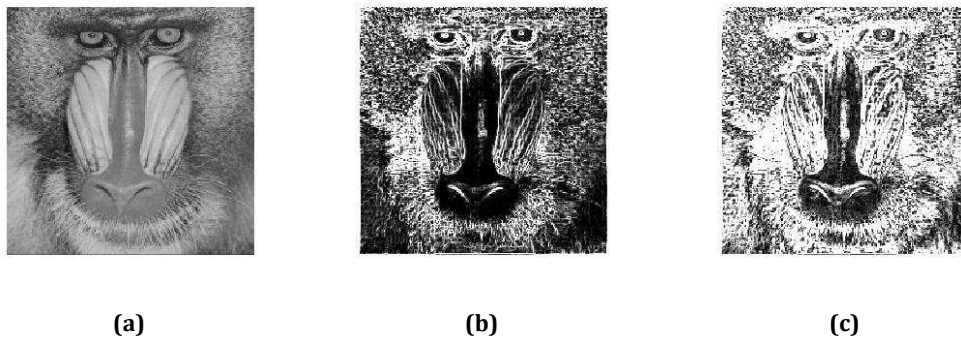


Figure V. 9 : (a) : Image originale baboon ;(b) : Le masque obtenu [1], [2] (amplifié par 10) ; (c) : Le masque proposé obtenu par le choix du minimum (amplifié par 10)

On remarque que le masque de la figure (V.9c) contient plus de régions lumineuses que le masque donné sur la figure (V.9b).

L'évaluation de performance de cet algorithme en terme d'invisibilité et de robustesse sont donnée sur la figure ci-dessous.

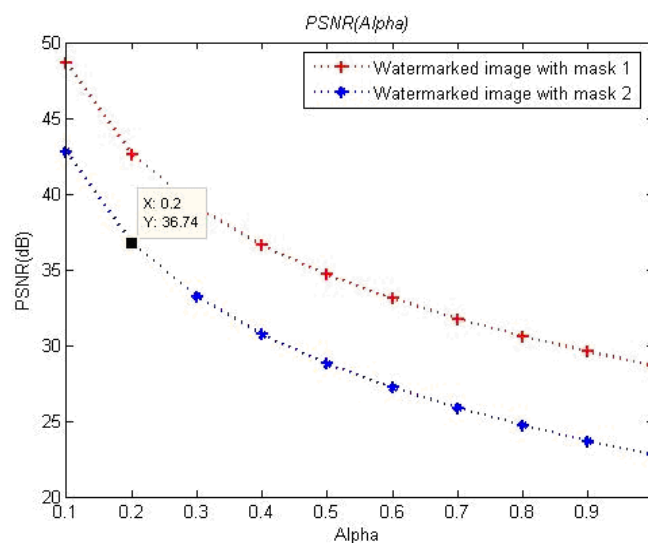


Figure V. 10 : Comparaison de PSNR entre les deux méthodes

Une différence apparente existe entre les deux courbes de *PSNR*. Alors l'image tatouée par mask2 (méthode de choix du minimum) cause une basse dégradation de la qualité de l'image comparée à l'utilisation du mask1 (méthode de multiplication).

Le processus de détection est similaire à celle utilisé dans [2]. Le résultat de la détection est donné sur la figure ci-dessous.

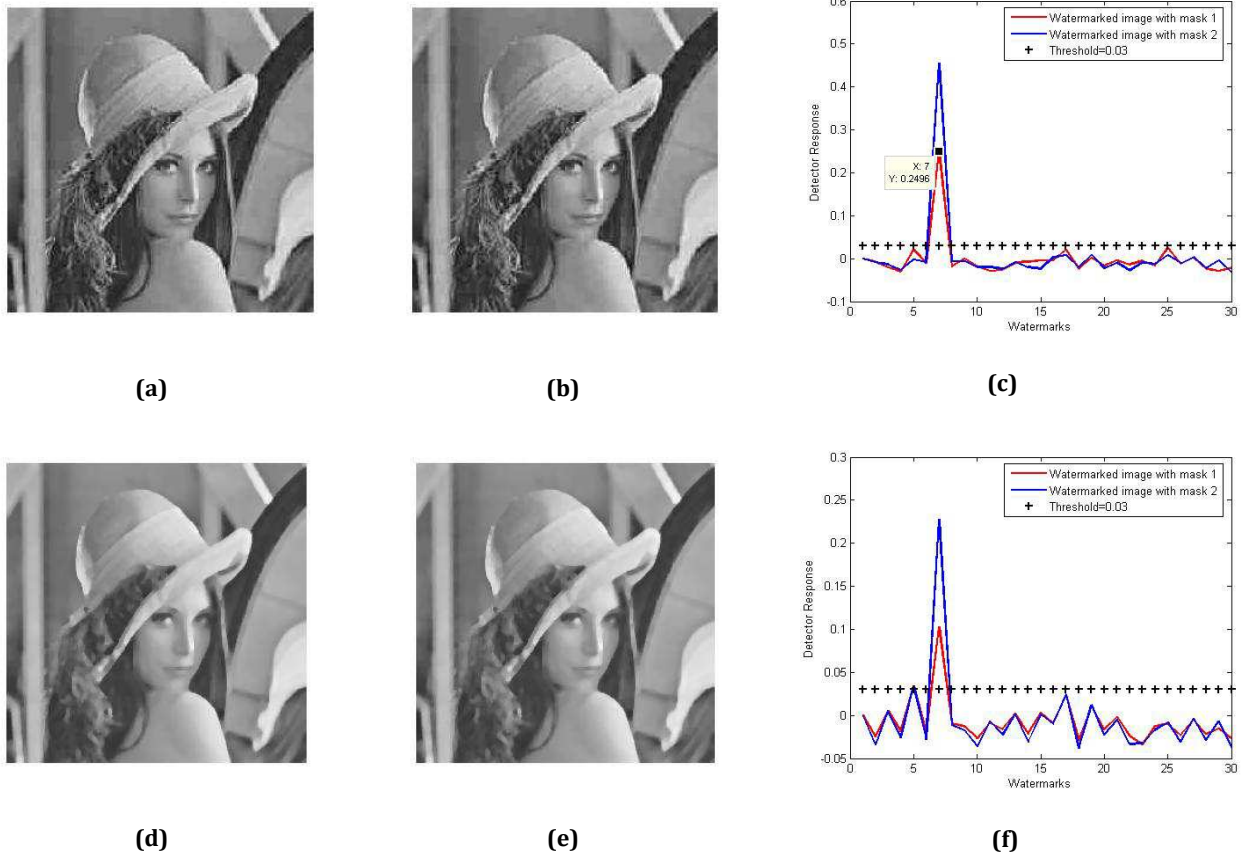


Figure V. 11 : Comparaison de robustesse entre le schéma proposé et celui de [1], (a), (b) et (c) : Images compressées avec le facteur de qualité $Q=20$, (d), (e) et (f) : Image tatouée attaquée par le filtrage médian avec une fenêtre de taille de 5×5 et la réponse du détecteur

On remarque que, les images tatouées par le mask2 présente une valeur de détecteur élevée par rapport aux images tatouée par le mask1, face à la compression JPEG et le filtrage médian. Ceci valide les performances du système proposé en terme d'invisibilité et de robustesse.

7. Schéma de tatouage d'image basé sur l'image d'auto référence

L'image d'auto référence est établie par Liu [19] qui consiste à la mise à zéro les bandes de haute fréquence de la transformation DWT. Dans ce travail, on propose de

mettre les coefficients de basse fréquence à zéro. Le système de détection est le même utilisé dans les travaux précédents [2], [3].

La recherche sur le système visuel humain (HVS) indique que pour une image, la plupart d'énergie est concentrée sur les basses fréquences et l'œil humain est sensible au changement de la bande de basse fréquence. En se basant sur cette idée, dans la nouvelle méthode décrite dans cette partie, nous proposons de mettre la bande de fréquence basse à zéro au lieu de la bande de fréquences élevées, afin d'atteindre la meilleure qualité visuelle.

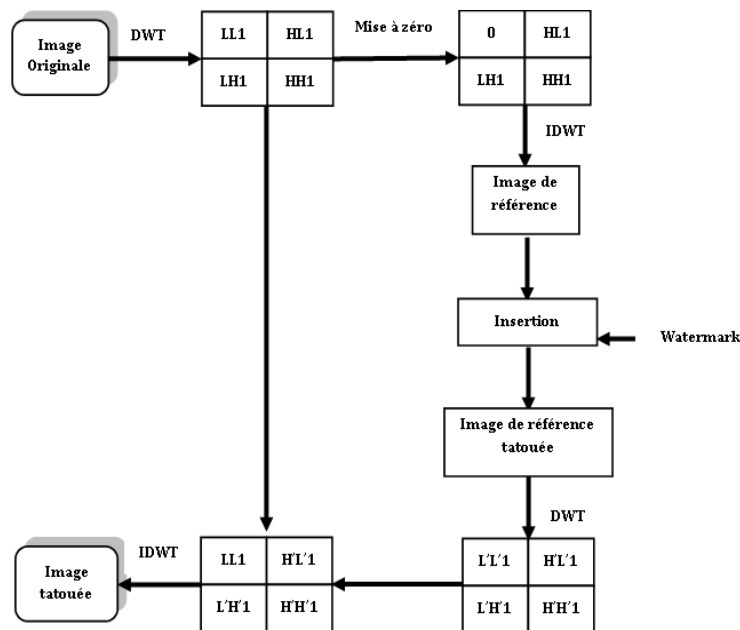


Figure V. 12 : Procédure d'insertion proposée

Dans ce travail on propose un schéma de tatouage d'image basé sur l'image de référence pour l'insertion du filigrane. Le filigrane est construit en utilisant la carte logistique. Dans notre schéma de tatouage, l'image de référence est extraite dans le domaine d'ondelette en mettant la bande de basse fréquence à zéro, puis l'inverse de la DWT est calculé. L'insertion du filigrane est faite dans le domaine spatial dans l'image de référence. L'image de référence tatouée est décomposée en niveau 1, et la bande de fréquence basse est remplacée par la bande basse de l'image originale. Enfin l'inverse de la DWT est calculé pour obtenir l'image tatouée.

Dans l'étape de détection, l'image originale est nécessaire pour l'extraction de l'image de référence à partir de l'image originale et tatouée, puis la corrélation entre l'image de différence et de filigrane est calculée. La comparaison est faite entre les

résultats de notre algorithme proposé avec celle qui n'utilise pas l'image de référence pour montrer les performances supérieures de notre nouvel algorithme, tout en ne dégradant pas les performances de détection du filigrane.

7.1. Insertion du filigrane

Le système de tatouage proposé, qui décrit la procédure d'insertion, est donné sur la figure (V.12).

- La carte logistique est utilisée pour produire un filigrane de la même taille que l'image originale.
- L'image originale est décomposée au niveau 1 en ondelette en quatre bandes LL_1, LH_1, HL_1, HH_1 . Les basses fréquences LL_1 sont mises à zéro et l'inverse de la DWT est appliquée afin d'obtenir l'image de référence.
- Le filigrane est inséré dans l'image de référence dans le domaine spatial d'une manière additive selon l'équation suivante :

$$Ref_w = Ref + \alpha w \quad (V.2)$$

L'image tatouée de référence est décomposée en DWT niveau1, et puis les $L'L'_1$ sont remplacés par LL_1 . L'inverse de la DWT est calculé pour obtenir l'image tatouée.

Ref : est l'image de référence ;

Ref_w : est l'image tatouée de référence ;

α : représente la force d'insertion ;

$L'L'_1$: désigne les coefficients bas de l'image de référence tatouée décomposée en niveau 1.

7.2. Détection de filigrane

L'image originale et l'image tatouée sont transformées en un seul niveau d'ondelette en utilisant l'ondelette de Haar comme le montre la figure (V.13), puis nous extrayons l'image de référence. Ensuite, on calcule la valeur de corrélation (Equation (IV.9)) entre la différence ($d = I_w - I$) et le filigrane inséré produit par la clef secrète pour décider si l'image contient le filigrane ou non.

Dans l'étape de détection on compare la corrélation entre la différence (d) et le filigrane original. Si le résultat est plus grand que la valeur du seuil, nous pouvons dire que l'image est tatouée ; autrement, elle n'est pas tatouée.

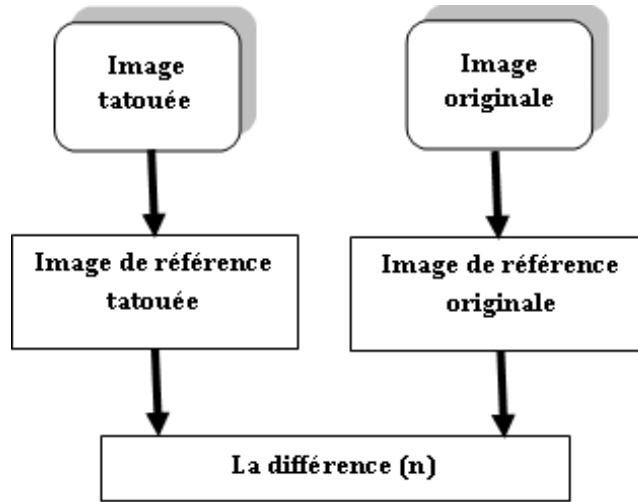


Figure V. 13 : Procédure de détection proposée

7.3. Résultats de simulation

L'étape suivante concerne l'évaluation de l'approche proposée et de son efficacité. Pour cela, nous avons tatoué la même image par l'utilisation de la méthode proposée (method1) et une autre fois sans image de référence (method2). Sur la figure (V.14) on donne l'image boat original qui a été signé avec $\alpha=0.03$, l'image de référence, et l'image tatouée obtenue avec l'utilisation de l'image de référence.

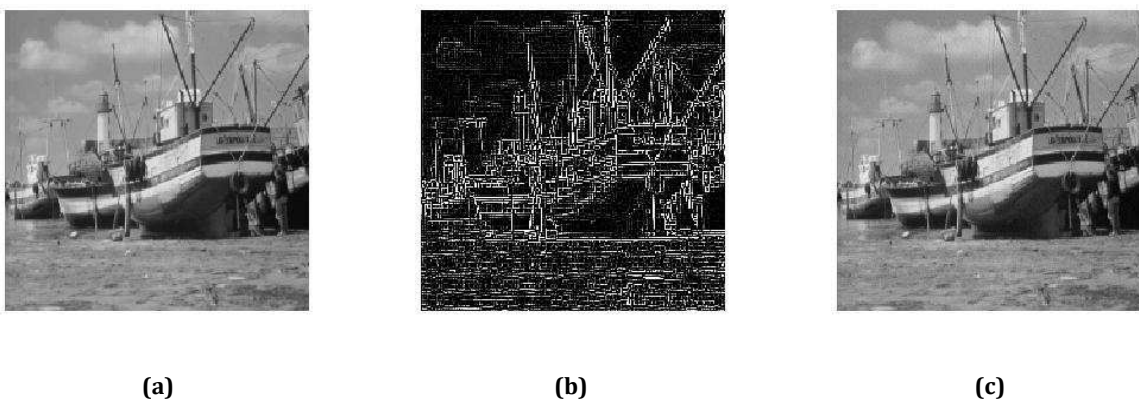


Figure V. 14 : (a) : Image de test ; (b) : Image de référence; (c) : Image tatouée PSNR=36.91dB ($\alpha=0.03$)

La figure (V.15) montre la réponse de détecteur pour 200 graines de filigrane ; seulement le filigrane du numéro 100 qui est inséré. La réponse au filigrane correct est beaucoup plus grande que les réponses aux autres filigranes. Le système de tatouage a détecté le filigrane correct inséré parmi les 200 filigranes différents.

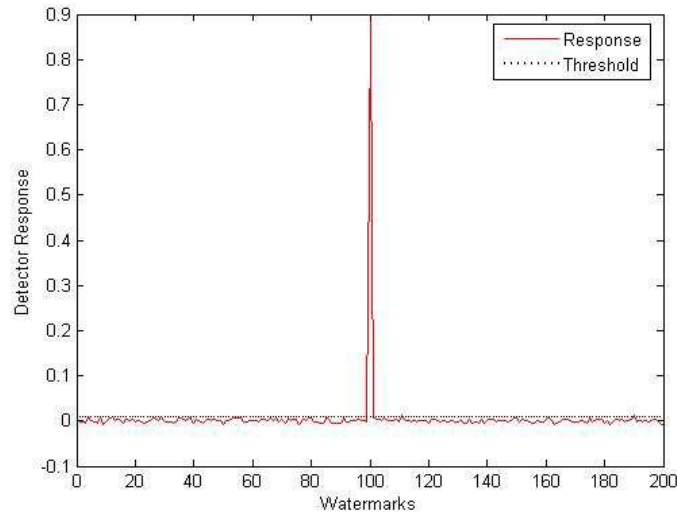


Figure V. 15 : Réponse de détecteur à 200 filigranes produits

Sur la figure (V.16) on donne la variation du PSNR pour les deux méthodes. On remarque que la méthode proposée (Method1) apporte un gain significatif en terme de PSNR.

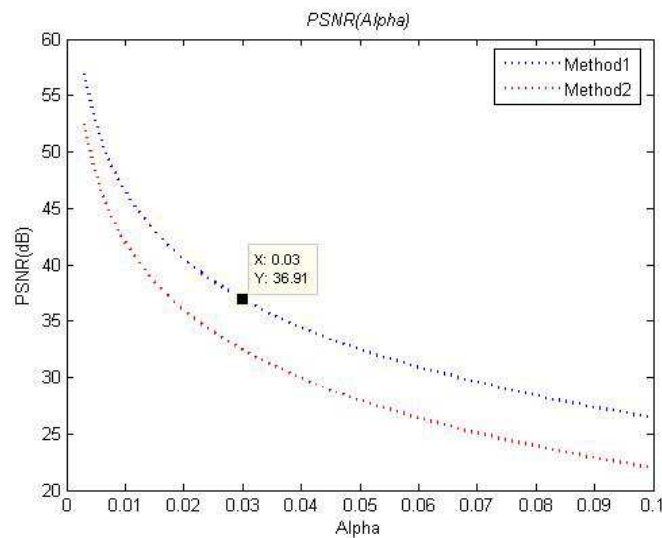


Figure V. 16 : Variation du PSNR de l'image tatouée

Après, nous avons examiné la robustesse de l'algorithme face à la compression JPEG avec un facteur $Q=30$. La réponse du détecteur est donnée dans figure (V.17). Le détecteur est au-dessus du seuil, la technique suggérée réussit à détecter le filigrane après la compression JPEG.

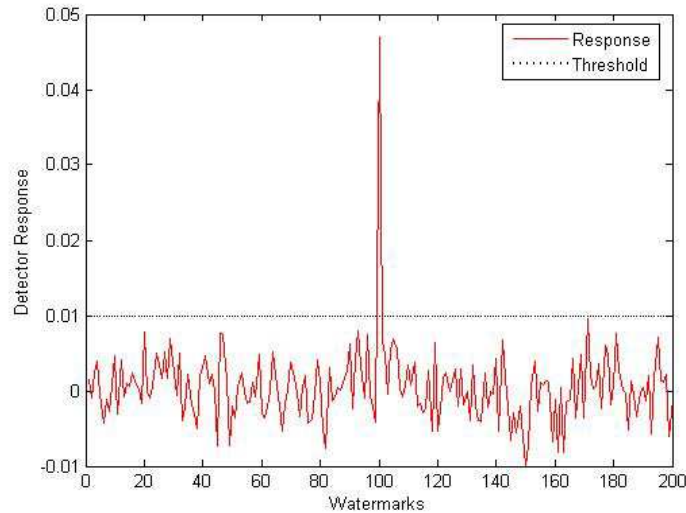


Figure V. 17 : Réponse de détecteur au JPEG pour (Q=30)

8. Schéma de tatouage dans le domaine des ondelettes basé sur les statistiques d'image

L'étape de la conception du masque, et d'insertion du filigrane est similaire à celle donnée dans [1], [2]. Cependant, la procédure de détection dans ce travail [5] est aveugle qui ne nécessite pas la présence de l'image originale. Il s'agit de l'utilisation de la corrélation linéaire LCD (Linear Correlator Detector).

8.1. Insertion du filigrane

La procédure d'insertion du filigrane proposée est montrée dans figure (V.3) (section 2.1). La carte logistique est utilisée pour produire le filigrane. Ensuite, on décompose l'image originale et le masque en DWT, pour obtenir les coefficients d'ondelettes dans chaque bande comme montré sur la figure (V.3), puis on choisit seulement la bande de basse fréquence (LL) pour l'insertion du filigrane d'une manière additive selon l'équation suivante :

$$LL' = LL_{image} + \alpha w \otimes LL_{mask} \quad (V.3)$$

où, LL_{image} représente les coefficients originaux de l'ondelettes et LL_{mask} sont les coefficients d'ondelettes du masque produit dans le domaine spatial, w est le filigrane et α est la force d'insertion. L'image tatouée est alors reconstruite en appliquant l'inverse de l'ondelette (IDWT).

8.2. Détection de filigrane

Le test statistique qui est souvent utilisée dans la détection de filigrane est la corrélation entre le signal à étudier et le filigrane inséré. Pour n'importe quelle séquence tatouée y , la corrélation avec le filigrane w est calculée en utilisant le LCD (détecteur linéaire de corrélation) défini par [20], [21] est donnée par l'équation (V.4) :

$$LCD(y) = \frac{1}{N} \sum_{k=1}^N y_k w_k \quad (V.4)$$

Par conséquent, nous pouvons prendre une décision sur l'image. Si $LCD(y)$ est plus grand qu'un seuil prédéfini, et vice versa. Cette technique est aveugle puisque la détection est effectuée sans présence de l'image originale.

Le test d'hypothèse aura la forme suivante:

$$\begin{cases} H_0: y[k] = x[k] + \alpha w[k] \\ H_1: y[k] = x[k] \end{cases} \quad (V.5)$$

H_0 : Signifie que le filigrane existe.

H_1 : Signifie aucun filigrane n'existe dans l'image ;

8.2.1. Seuil de décision

Pour obtenir le seuil ρ , le critère de Neyman-Pearson est utilisé, est donnée par l'équation (V.6) comme suit :

$$\begin{cases} \frac{1}{N} \sum_{k=1}^N y_k w_k \geq \rho \Rightarrow watermark\ present \\ \frac{1}{N} \sum_{k=1}^N y_k w_k < \rho \Rightarrow watermark\ absent \end{cases} \quad (V.6)$$

Le ρ représente la valeur du seuil choisi de tel façon la probabilité de fausse alarme pf (le filigrane détecté mais n'existe pas réellement) est fixe, et la probabilité manquante (missing) de détection pd (le filigrane existe mais n'est pas détecté) doit être réduite au minimum.

Le Pf et Pd sont calculés d'après [20] comme suit :

$$P_d = Q\left(\frac{\rho - m_1}{\sigma_1}\right), P_f = Q\left(\frac{\rho - m_0}{\sigma_0}\right) \quad (V.7)$$

Où $Q(\cdot)$ est la fonction de distribution cumulative définie par :

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp\left(-\frac{t^2}{2}\right) dt ; m_0, \sigma_0 \text{ et } m_1, \sigma_1 \text{ sont la moyenne et la variance du}$$

détecteur sous l'hypothèse H_0 et H_1 respectivement.

La caractéristique opérationnelle de récepteur (ROC) qui décrit la relation entre le pd et pf est donnée par l'équation (V.8) :

$$P_d = Q\left(\frac{Q^{-1}(P_f)\sigma_0 + m_0 - m_1}{\sigma_1}\right) \quad (\text{V.8})$$

Pour une probabilité donnée de fausse alarme pf , nous pouvons calculer le seuil nécessaire pour qu'un filigrane soit détecté, par l'utilisation de l'équation suivante :

$$\rho = m_0 + \sigma_0 \cdot Q^{-1}(1 - P_f) \quad (\text{V.9})$$

8.3. Graphique de la caractéristique opérationnelle de récepteur (ROC)

La caractéristique opérationnelle de récepteur (ROC) est très utile lorsqu'on évalue le comportement et la fiabilité d'un schéma de tatouage [22].

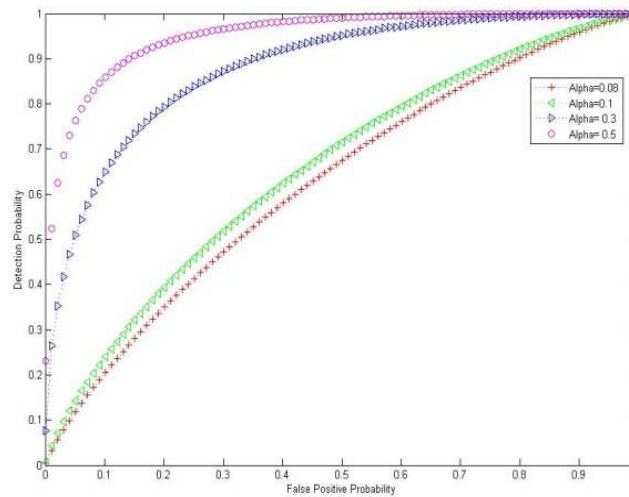


Figure V. 18 : Graphique de ROC

Le facteur alpha est fixé à 0.08, 0.1, 0.3 et 0.5, respectivement. Sur la figure (V.18) on présente le graphique de ROC de l'image watch sans attaque.

On remarque qu'une grande valeur d'insertion correspond à une probabilité plus élevée de détection.

8.4. Compression de JPEG

Dans le cas d'attaque, on met l'image watch en application à la compression JPEG. La force α de filigrane est fixée à 0.012. La probabilité de fausse positive pf est fixée à 10^{-9} , et nous détectons le filigrane par la détection de corrélation linéaire.

On sait que la fidélité d'une image de tatouage diminue lorsque le facteur de qualité diminue [12]. Nous exécutons la compression JPEG avec des facteurs de qualité diminuant de 100 à 0.

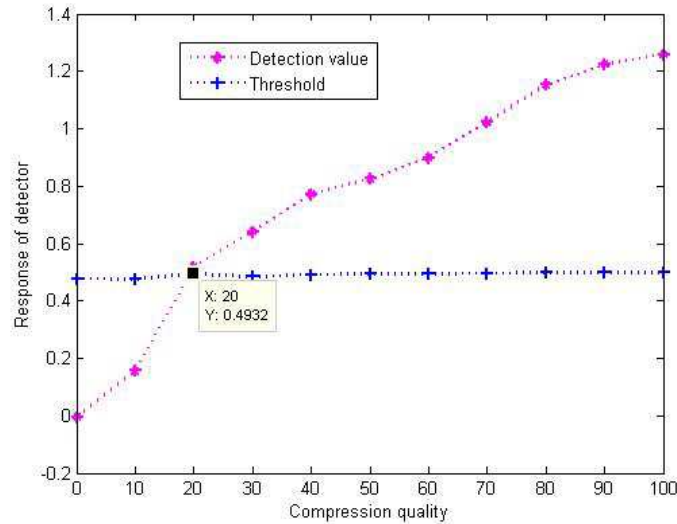


Figure V. 19 : Réponse du détecteur à la compression JPEG avec $\alpha=0.09$

On observe sur la figure (V.19) que la réponse du détecteur de corrélation est inférieure au seuil lorsque le facteur de qualité est inférieure de 20.

Conclusion

Dans ce chapitre, nous avons décrit quatre algorithmes de tatouage d'image dans le domaine DWT qui sont basés sur le masque développé dans le domaine spatial. Deux approches ont été utilisées pour la conception du masque. Il s'agit de la multiplication et du choix de la valeur minimale. La notion de l'image de référence est utilisée dont le but d'insertion du filigrane. Les propriétés statistiques de l'image sont exploitées pour avoir une détection aveugle de la marque. Les résultats prouvent que la technique proposée basée sur HVS dans DWT permet l'augmentation de l'invisibilité, tout en ne dégradant pas les performances de détection du filigrane.

Bibliographie

- [1] S. Belkacem, Z. Dibi, A. Bouridane, Masking model for image watermarking, The 4th International Summer School on Signal Processing & it's Applications, 30 June-4 July Boumerdes (UMBB) Algeria, 2007.

- [2] S. Belkacem, Z. Dibi, A. Bouridane, Image watermarking using visual model based discrete wavelet transform, 2^{ième} Conférence sur la Vision Artificielle, Tizi-Ouzou, Algeria November 18-20, 2007.
- [3] S. Belkacem, Z. Dibi, A. Bouridane, Chaos-based image watermarking scheme in the DWT, Les Journées sur les Signaux et Systèmes, JSS'07, Guelma, Algeria Novembre 14-15, 2007.
- [4] S. Belkacem, S. Khaldi, Z. Dibi, & A. Bouridane, Image watermarking scheme based on self-reference image, La journée des Jeunes Chercheurs en Informatique, 20 Mai, Guelma, Algérie, 2008.
- [5] S. Belkacem, Z. Dibi, & A. Bouridane, Chaos watermarking scheme based on wavelet domain, International Conference on Electrical Engineering, Electronics and Automatics'10 Bejaia, Algeria, 2-3 November 2010.
- [6] J. Mahdjoub, Vers un système de vision auto-adaptatif à base de systèmes multi-agents, Thèse de l'Université Reims Champagne-Ardenne, 2011.
- [7] <http://michel.pourtier.pagesperso-orange.fr/Waves1.htm> (2015).
- [8] S. Abdelmounaime, M.F. Belbachir, I. Tahar, La transformation en ondelettes pour l'extraction de la texture-couleur. Application à la classification combinée des images (HRV) de SPOT, International Journal of Remote Sensing, 27(18), 20 September, 3977–3990, 2006.
- [9] M. Mekouar, Compression d'images médicales par ondelettes et régions d'intérêt, Mémoire de Maîtrise Electronique, Montréal, Ecole de technologie supérieure, 2001.
- [10] R. Benali, Analyse du signal ECG par réseau adaptatif d'ondelettes en vue de la reconnaissance de pathologies cardiaques, Thèse de Doctorat, Université Abou Bekr Belkaid Tlemcen, 2013.
- [11] M.E. Hajji, La sécurité d'images par le tatouage numérique dans le domaine d'ondelettes, Thèse de Doctorat, Université Agadir, 2012.
- [12] M. Barni, F. Bartolini, and A. Piva, Improved wavelet-based watermarking through pixel-wise masking, IEEE Transaction on Image Processing, 10, 783-791, 2001.
- [13] G. Zhang, S. Wang, Q. Wen, An adaptive block-based blind watermarking algorithm, In Proceedings of the IEEE ICSP, 2294–2297, 2004.
- [14] C. H. Lee and H.K. Lee, Geometric attack resistant watermarking in wavelet transform domain, Optics Express, 13,1307–1321, 2005.
- [15] B. McKinnon and X. Qi, Adaptive wavelet-based family tree quantization for digital image watermarking, Proc. of the 8th IASTED International Conference on Signal and Image Processing (SIP'06), Honolulu, Hawaii, August 14-16, 2006.

- [16] A. Zolghadrasli, S. Rezazadeh, Evaluation of spread spectrum watermarking schemes in the wavelet domain using HVS characteristics, *International Journal of Information Science & Technology*, 2, 2007.
- [17] V.P. Reddy, and S. Varadarajan, Human visual system sentient imperceptible and efficient wavelet-based watermarking scheme for copyright protection of digital images, *IJCSNS International Journal of Computer Science and Network Security*, 9(4), 2009.
- [18] P. Stavroulakis, *Chaos applications in telecommunications*, Published by CRC Press, 2006.
- [19] J.L. Liu, D.C. Lou, M.C. Chang, H.K. Tso, A robust watermarking scheme using self-reference image, *Computer Standards & Interfaces*, 28, 356– 367, 2006.
- [20] Q. Cheng, T.S. Huang, Robust optimum detection of transform domain multiplicative watermarks, *IEEE transactions on signal processing*, 51(4), 906 – 924, 2003.
- [21] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, I. Pitas, Statistical analysis of a watermarking system based on Bernoulli chaotic sequences, *Signal Processing*, 81, 1273-1293, 2001.
- [22] M. Kutter, F. Petitcolas, A fair benchmark for image watermarking systems, *Electronic Imaging, security and watermarking of multimedia contents*, *Electronic Imaging. Security and Watermarking of Multimedia Contents*, 3657, 1-14, 1999.

Chapitre VI : Modélisation des coefficients DCT : Application au tatouage d'image

Introduction

Il est important de bien choisir les meilleurs coefficients modélisés de la transformée DCT pour répondre aux exigences d'un algorithme de tatouage. Dans ce chapitre, nous allons montrer que les coefficients bas du ac de la transformée DCT sont bien modélisés lorsqu'on utilise la Distribution Gamma Généralisée (*G Γ D*). Un nouveau estimateur basé sur la méthode des moments a été proposé pour estimer leurs paramètres, et la qualité de l'ajustement (χ^2) est utilisée pour prouver son efficacité. Les coefficients modélisés ont été choisis pour exécuter le processus d'insertion du filigrane. Afin d'augmenter la sécurité de notre schéma, les cartes chaotiques ont été également utilisées. Le modèle des fonctions de densité de probabilité (*pdf*) pour les images tatouées dans le domaine de DCT est dérivé, et le détecteur développé est basé sur la théorie du maximum de la vraisemblance. Les résultats de simulation ont montré que la méthode proposée possède une meilleure imperceptibilité, et extrêmement sensible à la clef et robuste à l'attaque JPEG quand la méthode des moments est utilisée. Avec notre méthode nous pouvons détecter le filigrane lorsque le taux de compression (CR) dépasse 28.5 pour toutes les images tatouées qui sont attaquées par la compression JPEG.

1. Etat de l'art sur la modélisation des coefficients DCT

Les dispositifs d'image numérique permettent de faire un nombre illimité de copies d'un "original" pour être facilement distribué et/ou forgé [1]. Le tatouage a été proposé comme une technologie pour assurer la protection de copyright par l'insertion d'un signal dans le contenu numérique de multimédia tel que des images ou vidéo d'une manière imperceptible, pourtant discernable [2], [3], [4]. Des cartes chaotiques ont été utilisées comme alternative aux séquences pseudo-aléatoires pour le tatouage numérique [5], [6], [7], afin d'augmenter la sécurité de leur schéma ; en raison de sa sensibilité extrême aux conditions initiales. Les algorithmes de tatouage d'image chaotique peuvent se faire dans le domaine spatial en changeant la valeur de quelques

pixels des images ou dans le domaine transformé tel que la DCT, DWT, DFT, ou la transformée en pyramide. Généralement, le tatouage dans le domaine fréquentiel est plus robuste que le domaine spatial.

Jusqu'à présent, il y a eu des efforts considérables dans le domaine de la recherche de la modélisation statistique de l'image numérique pour répondre aux exigences d'un algorithme de tatouage [8], [9]. Plusieurs travaux ont été étudié la distribution des coefficients de DCT d'images. La Distribution Généralisée de Gauss (*GGD*) est largement utilisée dans la littérature pour la modélisation des données numériques dans le domaine transformé DCT. Muller [10] a prouvé que *GGD* est le meilleur modèle pour la modélisation statistique des coefficients DCT. Joshi et Fischer [11] ont comparé les performances des modèles *GGD* et de Laplacian dans l'image. Récemment, ils ont affirmé que (*GFD*) adapte bien les coefficients ac de la transformée DCT est meilleure que la distribution *GGD* [12].

La distribution *GFD* à quatre paramètres a été la première fois présentée par Amoroso 1925. Ci après, les différentes distributions ont émergé comme des sous-classes de ce modèle. Stacy [13] en 1962 a proposé *GFD* avec trois paramètres, qui permet d'approximer le comportement d'un grand nombre de distribution. Shin et al. [14] ont utilisé *GFD* d'abord pour la modélisation statistique du signal audio, et puis pour la distribution de probabilité d'image dans le domaine DCT [12]. NG et Garg [15] ont utilisé cette distribution pour la transformée DFT (Discret Fourier Transform) pour modéliser les coefficients de l'image dont le but de tatouage. Li et al. [16] ont proposé d'utiliser la distribution *GFD* pour la modélisation des images SAR.

La clef de la modélisation statistique par une distribution appropriée consiste à bien évaluer ses paramètres. Tous les chercheurs confirme que, pour estimer les trois paramètres (γ, β et η) de *GFD*, d'une manière analytique par l'utilisation de la méthode de maximum de vraisemblance (Log Likelihood) est difficile, parce que les résultats sont représentés par des équations non-linéaires qui nécessitent des intégrales numériques [12], [17], [18]. En 2005, Chang et al. [12], confirme que ML (Maximum Likelihood) reste compliqué, et dans [14] les auteurs ont confirmé également l'évaluation des trois paramètres *GFD* du *pdf* reste complexe, jusqu'à 2013 Noufaily et al. [18] aient certifié que le ML n'est pas une bonne option pour la distribution *GFD*, ce qui pousse les chercheurs à trouver d'autres méthodes pour l'estimation des paramètres de cette

distribution. Dans [15] la méthode d'évaluation des paramètres de cette distribution est basée sur le calcul de la moyenne et la variance des données. Chang et al. [12], ont proposé une approche basée sur le gradient ascendant pour résoudre les équations de score qui mènent à un système à quatre équations non linéaires, ce qui exige un calcul itératif, et ils n'ont pas abordé l'aspect de zéros des données. Almpandis et Kotropoulos [17] ont utilisé la même méthode d'évaluation que dans [12] pour la segmentation phonémique. Ici on propose une nouvelle méthode d'évaluation basée sur la méthode des moments comme alternative à celle proposée par [12].

2. Distribution de Gauss Généralisée *GGD*

Diverses études ont été faites sur la distribution des coefficients de DCT des images numériques. Cependant, ils ont concentrées sur l'approximation des données empiriques de quelques images standard d'une variété de distribution statistique qui sont bien connue [19]. Sur la figure (VI.1), on donne le *pdf* de l'image Bridge.

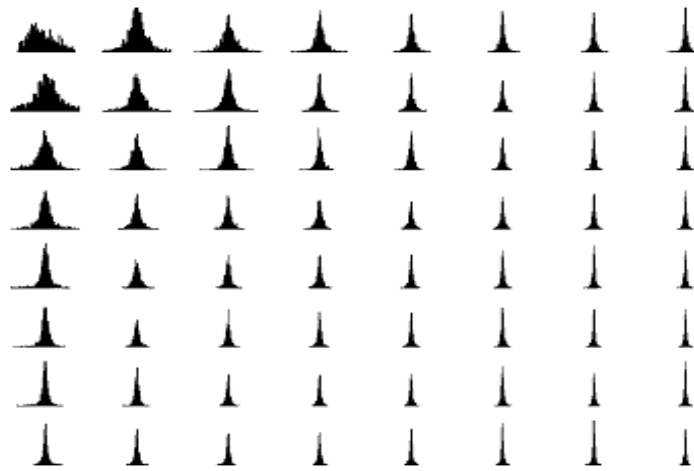


Figure VI. 1 : Histogramme des coefficients de DCT de l'image Bridge [19]

Un grand nombre de distributions symétriques peuvent être suffisamment rapprochées en utilisant la distribution *GGD*. Joshi et Fischer [11] ont approximé les coefficients ac de la DCT en utilisant *GGD* avec une moyenne égale à zéro.

Afin de modéliser le comportement statistique de l'image le mieux possible et d'éviter la limitation du modèle Gaussien, le *GGD* est adopté. Le modèle de *GGD* est largement utilisé dans la littérature pour décrire quelques distributions de probabilité des données numériques dans le domaine transformé. Il fournit fondamentalement une bonne compréhension du comportement statistique des signaux qui sont impulsive et avec des

queues lourdes (heavy tailed) comme les ondelettes et les coefficients DC dans la transformée DCT [20]. Un *GGD* rapproche une grande classe des distributions statistiques comme : Laplacienne ($v=1$), Gaussienne ($v=2$) et la distribution uniforme ($v \rightarrow \infty$).

L'équation analytique de la fonction de densité de probabilité de la distribution *GGD* est donnée par [11], [12], [20], [21] :

$$\begin{cases} P(x|v, \sigma) = \frac{vA(v, \sigma)}{2\Gamma(1/v)} e^{-[A(v, \sigma)|x|]^v}, & -\infty < x < +\infty; v, \sigma > 0 \\ A(v, \sigma) = \sigma^{-1} \sqrt{\frac{\Gamma(3/v)}{\Gamma(1/v)}} \end{cases} \quad (\text{VI.1})$$

ici, $\Gamma(\cdot)$ note la fonction Gamma habituelle définie par $\Gamma(t) = \int_0^{\infty} r^{t-1} e^{-r} dr$; v et σ sont des constantes réelles positives.

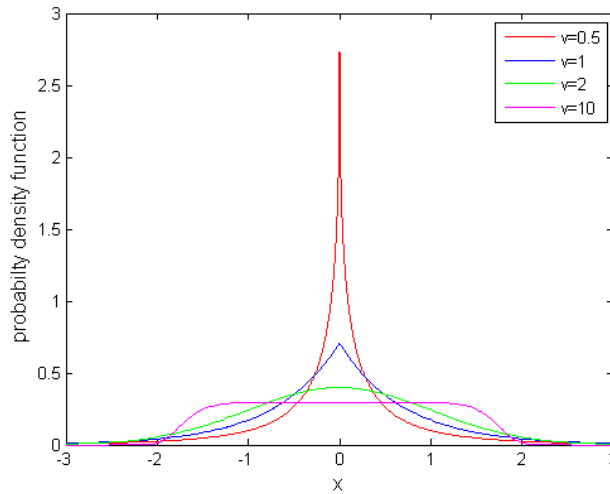


Figure VI. 2 : La fonction de la densité de probabilité de GGD avec $\sigma^2 = 1$

Sur la figure (VI.2), on illustre la distribution de *GGD* lorsque la variance v augmente, et on compare aussi les *pdf* de *GGD* pour différentes valeurs de paramètre de forme v avec l'hypothèse d'une moyenne 0 et $\sigma^2 = 1$.

La distribution Laplacienne et la distribution Gaussienne sont des cas spéciaux du *GGD* pour $v = 1$ et $v = 2$ respectivement.

Notons qu'une petite valeur du paramètre de forme v correspondant à des queues plus lourdes et donc la distribution fait une pointe.

2.1. Evaluation de paramètre de forme et d'écart type

La clef de la modélisation statistique d'une distribution appropriée, c'est d'estimer ses paramètres. Varanasi et al. [22] discutent l'évaluation des paramètres pour le *GGD* en

utilisant la méthode de maximum de vraisemblance et des moments. Le paramètre de forme v est estimé par la méthode de maximum de vraisemblance.

Dans [11] les auteurs ont proposé les équations suivantes pour l'évaluation des paramètres de GGD , tel que \hat{v} et $\hat{\sigma}$:

$$\frac{\psi(1/v+1)+\log(v)}{v^2} + \frac{1}{v^2} \log\left(\frac{1}{n} \sum_{i=1}^n |x_i|^v\right) - \frac{\sum_{i=1}^n |x_i|^v \log(|x_i|)}{v \sum_{i=1}^n |x_i|^v} = 0 \quad (IV.2)$$

ici $\psi(\tau) = -\gamma + \int_0^1 (1-t^{\tau-1})((1-t)^{-1}) dt$, pour \hat{v} connu, l'évaluation de l'écart type est donné par :

$$\begin{cases} \hat{\sigma} = \left[\frac{v\mu(v)^v \sum_{i=1}^n |x_i|^v}{n} \right]^{1/v} \\ \mu(v) = \sqrt{\frac{\Gamma(3/v)}{\Gamma(1/v)}} \end{cases} \quad (IV.3)$$

3. La distribution GFD

Plusieurs formes mathématiques de la distribution GFD sont proposées dans la littérature [12], [17], [23], [24], [25]. Dans cette section on va donner en bref la distribution GFD à quatre paramètres et on s'intéresse à celle avec trois paramètres.

3.1. Distribution GFD à quatre paramètres

Harter [23] a proposé une distribution GFD à quatre paramètres qui inclut un paramètre d'endroit c , paramètre d'échelle a , paramètre b de forme et de puissance p , avec une fonction de densité de probabilité donnée par l'équation (VI.4) :

$$f(x; c, a, b, p) = \frac{p}{a\Gamma(b)} \left(\frac{x-c}{a}\right)^{b-1} \exp\left\{-\left(\frac{x-c}{a}\right)^p\right\}, (x \geq c; a, b, p > 0) \quad (VI.4)$$

Le rôle joué par le paramètre d'endroit c ; est que une augmentation dans la valeur de c fait déplacer la courbe de pdf de la distribution GFD à droite d'une manière horizontale.

3.2. Distribution GFD à trois paramètres

La distribution GFD avec trois paramètres possède la fonction de densité de probabilité définie par [12], [17], [24], [25] comme suit :

$$f_x(x) = \frac{\gamma\beta^\eta}{2\Gamma(\eta)} |x|^{\eta-1} \exp(-\beta|x|^\gamma) \quad (VI.5)$$

$\Gamma(\cdot)$ désigne la fonction Gamma, γ, β et η sont des paramètres positifs réels.

Le moment k^{th} qui suit la distribution GFD est montré dans l'annexe B, et peut s'exprimer comme suit :

$$E(|x|^k) = \frac{\Gamma(\eta + \frac{k}{\beta})}{\beta^k \Gamma(\eta)} \tag{VI.6}$$

3.2.1. Sensibilité de la distribution GFD à ses paramètres

Sur la figure ci-dessous on trace le pdf de l'image watch, pour montrer la sensibilité de la distribution GFD lorsqu'en variant l'une de ses paramètres et on fixe les autres.

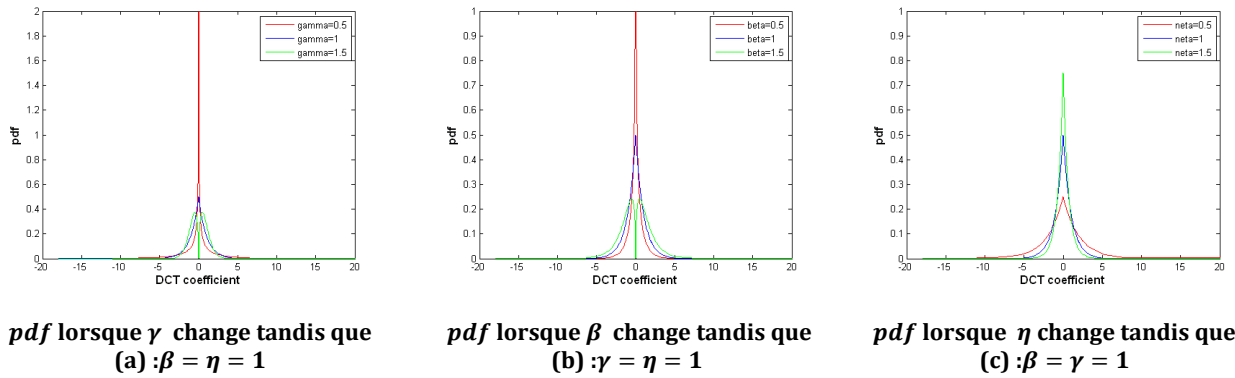


Figure VI. 3 : Sensibilité de GFD à ses paramètres pour l'image watch

3.2.2. Pdf des coefficients de DCT

La distribution GFD rapproche une grande classe des distributions statistiques comme la distribution de : Laplace ($\gamma = 1$ et $\eta = 1$), Gauss ($\gamma=2$ et $\eta=0.5$) et Gamma ($\gamma=1$ et $\eta=0.5$).

Sur la figure (VI.4), la distribution GFD et les distributions reliées à cette distribution sont données, comme la distribution Gaussienne, Laplacienne, et la distribution Gamma.

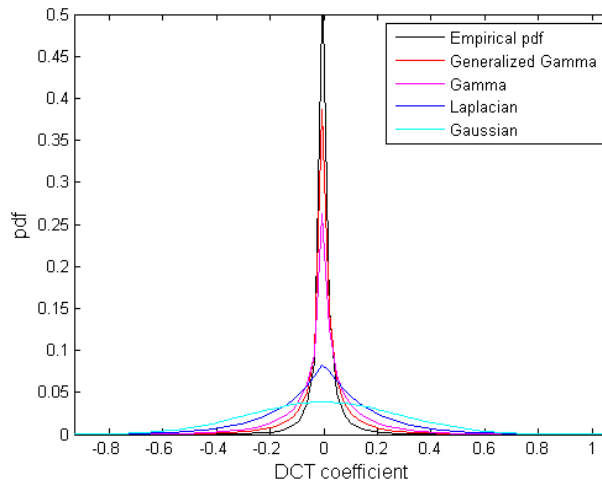


Figure VI. 4 : Le Pdf empirique et ses modèles statistiques

Nous remarquons que, la distribution $G\Gamma D$ s'adapte très bien les données empiriques plutôt que les autres distributions.

4. Modélisation des coefficients DCT : Application au tatouage d'image

Dans ce travail, les coefficients bas du bloc d'image de DCT en excluant le coefficient DC sont modélisés par $G\Gamma D$, où la méthode des moments est utilisée pour estimer ses paramètres. Ces coefficients sont choisis pour l'insertion de la marque d'une manière multiplicative. La carte logistique est utilisée pour la génération de filigrane. La détection du filigrane est effectuée sans utiliser l'image originale, et le détecteur dérivé est basé sur le maximum de la vraisemblance (MLE) des coefficients modélisés.

4.1. Evaluation des paramètres de la distribution $G\Gamma D$

Il y a un certain nombre de méthodes bien connues qui peuvent être utilisées pour estimer les paramètres de la distribution qui sont basés sur des échantillons de données disponibles.

Dans cette section, on applique la méthode des moments pour dériver un nouvel estimateur pour les trois paramètres de la distribution $G\Gamma D$. Le détail de la démonstration est donné dans l'annexe B :

On peut obtenir les valeurs η et γ après la solution du système d'équations suivant :

$$\begin{cases} \ln(E(|x|^2)) = 2 \ln(E(|x|)) + \ln(\Gamma(\eta)) - 2 \ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right) + \ln\left(\Gamma\left(\frac{\eta\gamma+2}{\gamma}\right)\right) \\ \ln(E(x^2|x|)) = 3 \ln(E(|x|)) + 2\ln(\Gamma(\eta)) - 3 \ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right) + \ln\left(\Gamma\left(\frac{\eta\gamma+3}{\gamma}\right)\right) \end{cases} \quad (\text{VI.7})$$

alors on estime la valeur de β à partir de l'équation (VI.8) en prenant son exponentiel.

$$\ln(\beta) = -\ln(E(|x|))\gamma - \ln(\Gamma(\eta))\gamma + \ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right)\gamma \quad (\text{VI.8})$$

4.2. Stratégie de tatouage d'image

L'algorithme d'insertion du filigrane peut être décrit comme suit :

Etape 1 : D'abord, nous produisons d'une séquence de longueur égale au nombre de bloc multiplié par 9, selon la carte logistique définie par sa forme récursive suivante [7] ;

$$X_{n+1} = \lambda X_n(1 - X_n), \text{ où } 0 \leq X_n \leq 1 \text{ et } 0 \leq \lambda \leq 4 \quad (\text{VI.9})$$

λ représente le paramètre de bifurcation. Selon la valeur de λ , la dynamique de ce système peut changer dramatiquement, dans l'intervalle $3.57 \leq \lambda \leq 4$, la séquence est non périodique, non convergente, et très sensible à la valeur initiale.

Etape 2 : Dans la deuxième étape, l'image est divisée en des blocs de taille 8×8 pixels, et chaque bloc est indépendamment transformé au domaine fréquentiel 2D-DCT.

Etape 3 : En se basant sur la position des neuf premiers coefficients d'image des DCT qui sont organisés dans un balayage en zigzag, de sorte que les coefficients soient en règle de la fréquence croissante. L'insertion du filigrane est faite d'une manière multiplicative suivante en utilisant l'équation (VI.10) :

$$y(u, v, b) = x(u, v, b)(1 + \alpha w_i) \quad (\text{VI.10})$$

où α est une constante définie par l'utilisateur, ses valeurs sont entre 0 et 1 ;

w_i : Est l'élément de filigrane ;

$x(u, v, b)$: Représente le coefficient de DCT dans les coordonnées (u, v) pour le bloc b ;

$y(u, v, b)$: Désigne le coefficient modifié de DCT de l'image à tatouer dans les coordonnées (u, v) pour le bloc b ;

Etape 4 : Enfin, l'inverse de la DCT est appliquée à chaque bloc, pour obtenir l'image tatouée.

4.3. Détecteur de filigrane

Dans la section suivante, nous dérivons l'expression de la fonction de densité de probabilité pour l'image tatouée, et la fonction de vrai semblance sous l'hypothèse que l'image originale est modélisée par *GFD*.

Le *pdf* dérivé de l'image tatouée basé sur la distribution *GFD* peut être exprimé comme suit :

$$P_y(y) = \prod_{i=1}^N \frac{\beta^\eta}{2\Gamma(\eta)} \left| \frac{y_i}{1+\alpha\omega_i} \right|^{\eta\gamma-1} \frac{1}{1+\alpha\omega_i} \exp - \beta \left| \frac{y_i}{1+\alpha\omega_i} \right|^\gamma \quad (\text{VI.11})$$

où N est le nombre de coefficients à être tatoués.

Le rapport vrai semblance est défini par l'équation (VI.12) :

$$l(y) = \frac{p(y|H_1)}{p(y|H_0)} \quad (\text{VI.12})$$

On prend le modèle de coefficients de DCT qui a été présenté dans la section précédente, y_i suit la même distribution comme x_i c'est à dire $G\Gamma D$ mais avec différents paramètres.

La fonction vrai semblance utilisée dans le détecteur de filigrane peut être exprimée en fonction d'un vecteur. Dans ce cas, les probabilités conditionnelles $p(Y|H_1)$ et $p(Y|H_0)$ peuvent s'exprimer comme suit :

$$p(Y|H_1) = \prod_{i=1}^N \frac{\gamma\beta^\eta}{2\Gamma(\eta)} \left| \frac{y_i}{1+\alpha\omega_i} \right|^{\eta\gamma-1} \frac{1}{1+\alpha\omega_i} \exp^{-\beta \left| \frac{y_i}{1+\alpha\omega_i} \right|^\gamma} \quad (\text{VI.13})$$

$$p(Y|H_0) = \prod_{i=1}^N \frac{\gamma\beta^\eta}{2\Gamma(\eta)} |y_i|^{\eta\gamma-1} \exp^{-\beta|y_i|^\gamma} \quad (\text{VI.14})$$

alors la vrai semblance est donnée par l'équation (VI.15) :

$$l(y) = \prod_{i=1}^N \frac{1}{|1+\alpha\omega_i|^{\eta\gamma}} \exp \left(-\beta \left| \frac{y_i}{1+\alpha\omega_i} \right|^\gamma + \beta|y_i|^\gamma \right) \quad (\text{VI.15})$$

Le maximum de vrai semblance $\mathcal{L}(y)$ est utilisée au lieu de $l(y)$:

$$\mathcal{L}(y) = \ln(l(y)) = \sum_{i=1}^N \left(\ln \frac{1}{|1+\alpha\omega_i|^{\eta\gamma}} + \beta|y_i|^\gamma - \beta \left| \frac{y_i}{1+\alpha\omega_i} \right|^\gamma \right) \quad (\text{VI.16})$$

En raison de l'imperceptibilité, la valeur de α est toujours choisie très petite ($\alpha \ll 1$), on utilise la décomposition en série de Taylor d'ordre 1 environ $\alpha = 0$, le rapport $\mathcal{L}(y)$ de MLE peut s'écrire comme suit :

$$\mathcal{L}(y) = \sum_{i=1}^N -\eta\gamma\alpha\omega_i + \beta\gamma|y_i|^\gamma\alpha\omega_i \quad (\text{VI.17})$$

Etant donné les trois paramètres de $G\Gamma D$, notre détecteur peut être exprimé comme suit :

$$T(y) = \frac{\partial \mathcal{L}(y)}{\partial \alpha} = \sum_{i=1}^N -\eta\gamma\omega_i + \beta\gamma|y_i|^\gamma\omega_i \leq \rho \quad (\text{VI.18})$$

Finalement la décision est basée sur la comparaison entre $T(y)$ et un seuil ρ : si le résultat est plus grand que le seuil, le détecteur décide la présence du filigrane autrement il décide de son absence. Le seuil ρ est défini par [26], [27] comme suit:

$$\rho = \sigma_T Q^{-1}(Pf) + \mu_T \quad (\text{VI.19})$$

$$\text{où } Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} e^{-t^2/2} dt$$

En se basant sur le détecteur que nous développé, la moyenne et la variance μ_T, σ_T sont dérivées et données par le système d'équation (VI.20). La démonstration mathématique de ces deux paramètres est faite dans l'annexe B.

$$\begin{cases} \mu_T = 0 \\ \sigma_T^2 = \sum_{i=1}^N \gamma^2 \eta w_i^2 \end{cases} \quad (\text{VI.20})$$

4.4. Résultats de simulation

Pour montrer l'efficacité de ce travail, les résultats de simulation par l'utilisation du MATLAB sont donnés dans cette section. Dans la simulation, quatre images de la taille 512×512 , appelées peppers, f16, boat et baboon sont utilisées. Le filigrane est produit avec une valeur initiale 0.01 et la valeur de λ est fixée à 3.98. Une séquence de filigrane de longueur de 36864 est utilisée. Pour la méthode de gradient ascendant, leurs paramètres sont fixés comme dans [12], et le nombre de classe de l'image de test est fixé à 256.

4.4.1. Qualité d'ajustement

Le test χ^2 a été utilisé pour vérifier laquelle des méthodes (les coefficients ac de la transformée DCT du bloc, ou seulement les coefficients basse de la DCT du bloc) qui donne le meilleur ajustement des valeurs empiriques. La valeur de la statistique χ^2 est évidemment petite pour les données qui sont bien approximées aux résultats théoriques. Les résultats du test sont récapitulés dans le tableau ci-dessous.

D'après les valeurs montrées dans le tableau (VI.1), on note que les coefficients bas du ac d'un bloc transformé en DCT sont mieux approximés par la distribution GFD, par rapport aux coefficients ac d'un bloc comme il a été montré par Chang et al. [12].

Images \ Coefficients	watch	f16	boat	Peppers
Coefficients ac [12]	4.4512×10^5	2.0131×10^8	1.9912×10^7	2.0135×10^{11}
Coefficients bas du ac	622.8236	2.6912×10^3	2.0539×10^3	1.1668×10^4

Tableau VI. 1: Test d'ajustement pour différentes images

Les neuf coefficients bas du ac suivants : C_{10} , C_{11} , C_{01} , C_{20} , C_{02} , C_{12} , C_{21} , C_{03} et C_{30} ont été choisis pour les utiliser dans les expériences parce qu'ils ont une grande influence sur la qualité d'image [10], [12]. Le paramètre γ estimé pour différentes images de test sont donné dans le tableau (VI.2).

	Méthode de Chang [12]				Notre méthode			
	peppers	f16	boat	baboon	peppers	f16	boat	baboon
C10	0.9342	0.9266	0.9649	0.9971	0.7348	0.9669	1.0283	1.0997
C11	0.9090	0.9253	0.9570	0.9989	0.7996	1.3504	1.0597	1.2353
C01	0.9113	0.8995	0.9409	0.9975	0.7546	1.7313	1.0270	0.8891
C20	0.8926	0.9113	0.9684	0.9920	0.6206	0.7445	1.2361	1.1624

C02	0.8979	0.9029	0.9277	0.9923	0.7031	1.4580	0.7636	0.7439
C12	0.8955	0.9148	0.9431	0.9925	0.5622	1.1286	0.7809	1.0306
C21	0.8926	0.9391	0.9655	0.9905	0.5640	0.8724	0.8799	0.9201
C03	0.9199	0.9082	0.9215	0.9924	0.6069	1.2204	0.6787	0.7602
C30	0.8949	0.9288	0.9729	0.9863	0.4834	0.8701	0.7778	1.0889

Tableau VI. 2: Paramètre γ estimé pour différentes images de test

On constate que, les valeurs obtenues de γ pour les deux méthodes ne sont pas vraiment éloignées pour la même image. Une fois qu'un modèle est spécifié avec ses paramètres, et les données sont collectées, on peut évaluer sa qualité d'ajustement.

Les résultats de la comparaison entre notre méthode basée sur la méthode des moments et celle proposée par Chang et al [12] en terme du test χ^2 sont fournis dans le tableau (VI.3). En se basant sur l'approche de χ^2 sa représentation avec des barres est fournie dans la figure (VI.5).

	Méthode de Chang [12]				Notre méthode			
	peppers	f16	boat	baboon	peppers	f16	boat	baboon
C10	2829.3	1171.5	598.0044	312.3664	814.1363	880.1532	573.3917	337.1917
C11	3344	1061.6	637.7806	263.8607	1043	1484.5	657.6492	311.8651
C01	3356.6	1173.6	912.6334	408.2799	946.9018	1698.8	801.2322	338.8811
C20	45347	4955.4	514.1500	373.3667	1210.4	1064.7	619.0267	439.6927
C02	9886.2	1400.9	4087	555.0271	1168.6	2080.5	783.7867	318.6287
C12	125620	1335.1	1500.7	297.4026	1108.3	1222.3	654.4057	280.8313
C21	3186600	1486.3	1463.8	449.2100	1046.9	835.8579	526.5127	342.5471
C03	32351	1418.5	16775	1717.2	803.7285	1627	702.8218	447.4049
C30	1328200	2076.8	2774.8	470.8735	98.5727	795.9682	608.7624	470.4208

Tableau VI. 3: Comparaison de la qualité de l'ajustement

D'après les valeurs données par le tableau (VI.3), on remarque que ; pour l'image peppers tous les coefficients sont bien modélisés par notre méthode, alors que pour l'image f16 quatre des coefficients étaient bien modélisés par [12] par rapport à cinq coefficients par la méthode des moments. Huit et six coefficients pour les deux images boat et baboon respectivement sont bien modélisés par la méthode des moments, et le reste des coefficients à neuf sont bien modélisés par [12].

Nous pouvons dire, la majorité des coefficients des images de test sont mieux modélisés par la méthode des moments que l'approche de gradient ascendant. En effet, il n'est pas possible de confirmer laquelle des méthodes qui peut mieux ajuster les données que l'autre, tous dépend des propriétés de l'image. Les résultats de simulation montrent que la méthode des moments constitue une alternative à la méthode de gradient ascendant, avec un compromis entre l'exactitude et la simplicité. Pour le tatouage d'image les deux méthodes d'évaluation des paramètres sont utilisées.

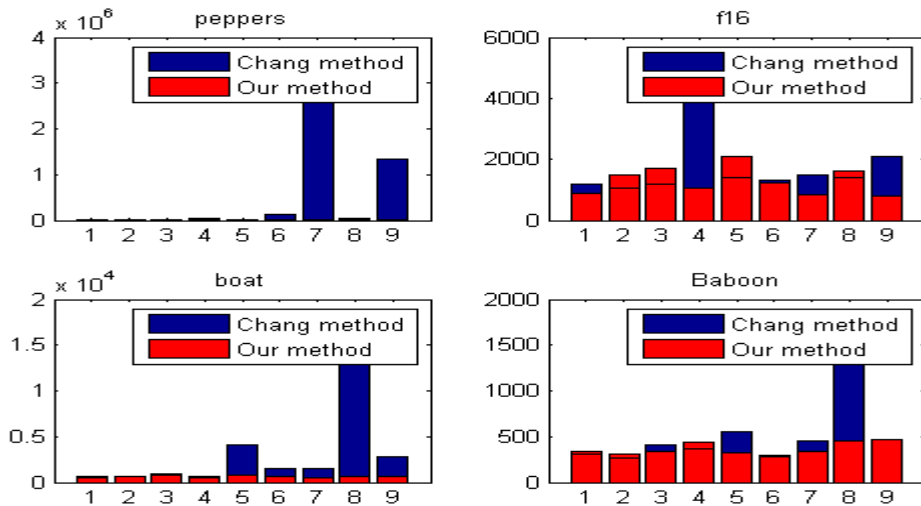


Figure VI. 5 : Comparaison de la qualité de l'ajustement

4.4.2. Mesure de qualité

Nous évaluons la qualité perceptuelle des images tatouées ; dans la figure (VI.6) on compare l'invisibilité des images tatouées ; quatre images de test en utilisant les coefficients bas du ac pour un facteur d'insertion égal à 0.1.

On peut dire que les images originales et tatouées avec notre algorithme sont perceptiblement indistinguables, ceci valide la condition d'invisibilité pour un système efficace de tatouage.

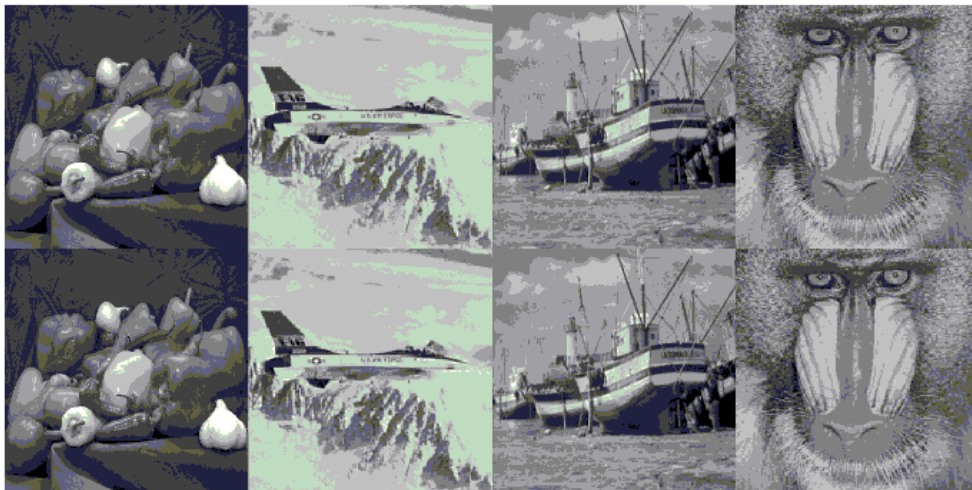


Figure VI. 6 : Comparaison visuelle de la qualité des images tatouées : le haut sont les images originales, et le bas sont les images tatouées

Variation de PSNR

Pour déterminer la dégradation dans l'image tatouée par rapport à l'image hôte, le PSNR est appliqué pour mesurer la distorsion produite après le processus d'insertion. En général, si la valeur de PSNR est plus grand de 30dB la qualité perceptuelle est acceptable, c'est à dire, le filigrane est presque invisible à l'œil humain [28].

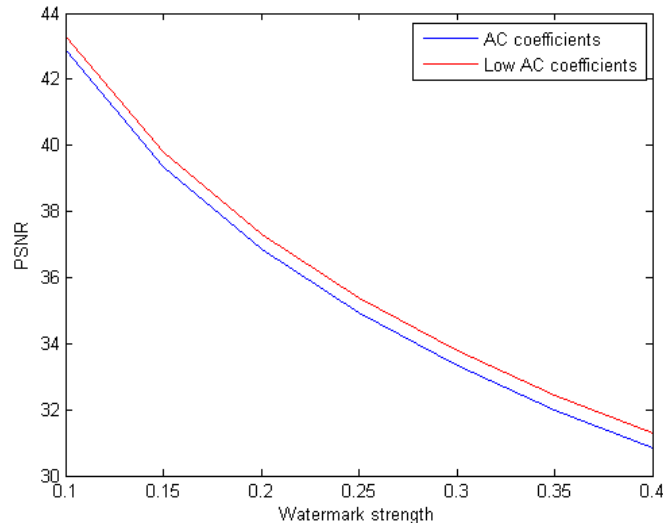


Figure VI. 7 : Comparaison de PSNR entre les ac et les coefficients bas du ac

Sur la figure (VI.7), on observe la variation du PSNR lorsque les coefficients bas du ac et les coefficients ac sont choisis pour l'insertion du filigrane.

La bande entre les valeurs de PSNR suggère les performances supérieures de la modélisation des coefficients bas du ac que les coefficients ac, et cette amélioration en terme de PSNR a été observée d'après des expériences multiples. Nous pouvons dire que la valeur la plus grande de la force α peut être utilisée, sans détruire la qualité d'image, lorsque la technique proposée est utilisée.

4.4.3. Test de robustesse

Un schéma pratique de tatouage doit être robuste aux attaques et au traitement d'image. La compression d'image est utilisée pour évaluer la robustesse du système proposé de tatouage. Dans la figure (VI.8) et la figure (VI.9) la ligne continue est consacrée au détecteur, et pour le seuil correspondant au détecteur les lignes sont présentées avec une ligne pointillée. Par le détecteur (GA) on indique l'approche du gradient pour l'évaluation des paramètres, et le détecteur (MM) pour celui qui estime ses paramètres par la méthode des moments.

Unicité de filigrane

Dans la figure (VI.8) on donne la réponse du détecteur à un ensemble de 2000 filigranes aléatoirement produits comprenant le filigrane inséré, pour lequel seulement un seul filigrane qui existe dans les images tatouées.

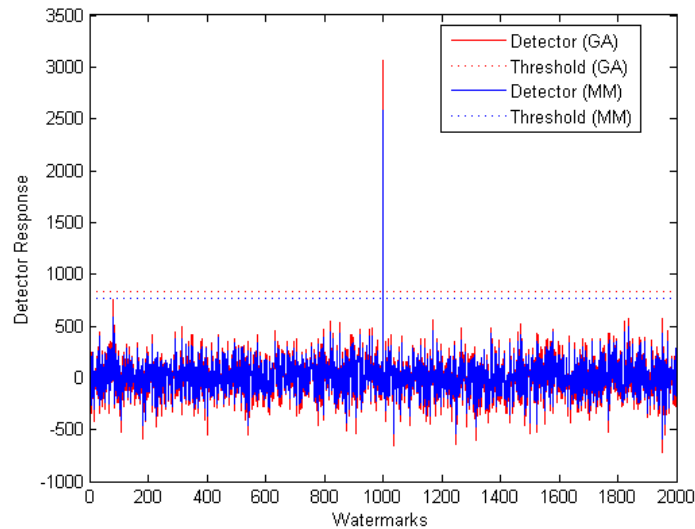


Figure VI. 8 : Réponse du détecteur pour l'image tatouée

Pour les deux détecteurs, le système de détection a détecté le filigrane inséré correct parmi 2000 filigranes différents.

La réponse du détecteur au filigrane inséré correct (1000) est plus grande que les réponses aux autres filigranes pour les deux méthodes. Cependant le détecteur proposé (MM) indique une grande valeur par rapport au détecteur (GA) pour la marque numéro 1000.

Robustesse contre la compression JPEG

Les résultats de la compression JPEG pour différent valeur de taux de compression CR sont montrés sur la figure (VI.9), il apparait que la robustesse se diminue lors des images tatouées qui sont compressée avec une grande valeur de CR.

Pour les images tatouées attaquées on peut atteindre une valeur de CR = 49, lorsque les valeurs du détecteur basés sur la méthode des moments soit en dessous du seuil, le filigrane est toujours détecté. On peut dire que le détecteur développé est robuste à la compression JPEG lorsque les trois paramètres de la distribution sont estimés par la méthode des moments par rapport à l'approche où le gradient ascendant est utilisé.

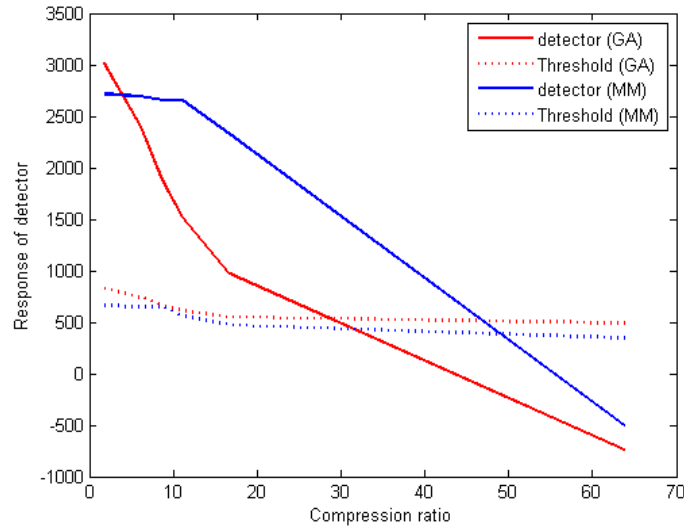


Figure VI. 9 : Réponse du détecteur face à la compression JPEG pour l'image baboon

Le pourcentage d'amélioration en terme de CR pour $\alpha = 0.1$ est donné dans la tableau ci-dessous.

Images	peppers	f16	boat	baboon
CR%	40.3509	51.3158	57.5758	41.8367

Tableau VI. 4: Amélioration du CR

D'après les valeurs données par le tableau (VI.4), nous pouvons dire que la robustesse de l'image attaquée par la compression JPEG en terme du CR est améliorée de plus de 40% lorsque les coefficients bas du ac sont modélisées par $G\mathcal{D}$ et leur paramètres sont estimés par notre méthode.

Conclusion

Dans ce travail, nous avons prouvé par l'intermédiaire de la simulation que $G\mathcal{D}$ a pu bien modélisés les coefficients bas du ac de la transformée DCT de chaque bloc de taille 8×8 pixels plutôt que les coefficients ac. La méthode des moments est comparée avec l'algorithme du gradient ascendant pour l'évaluation des paramètres de la distribution $G\mathcal{D}$. Nous avons testé avec succès notre algorithme sur plusieurs images standard de test en terme de la qualité de l'ajustement χ^2 . Le filigrane a été caché dans les coefficients de fréquence bas du ac du bloc d'image de DCT d'une manière multiplicative. Les résultats de simulation soutiennent notre méthode d'évaluation des paramètres, et la stratégie du choix des coefficients bas du ac et de leur modélisation par $G\mathcal{D}$. Notre système de tatouage a montré l'efficacité de l'approche proposée concernant la qualité

des images tatouées et la robustesse face à l'attaque JPEG, et le filigrane est toujours détecté dans l'image attaquée, avec une valeur d'amélioration en CR de plus de 40 %.

Bibliographie

- [1] R.B. Wolfgang, C.I. Podilchuk, Perceptual watermarks for digital images and video, *Proceedings of the IEEE*, 87, 1108-1126, 1999.
- [2] R. Kwitt, P. Meerwald, A. Uhl, Lightweight detection of additive watermarking in the DWT-domain, *IEEE Transactions On Image Processing*, 20(2), 474-484, 2010.
- [3] X. Yin, S. Peng, X. Zhu, Detection for multiplicative watermarking in DCT domain by Cauchy model, in: S. Qing et al. (Eds.), Springer-Verlag Berlin Heidelberg, 173-183, 2011.
- [4] A. Louchene, A. Dahmani, Watermarking method resilient to RST and compression based on DWT, LPM and phase correlation, *International Journal of Computers and Applications*, Acta Press- 35(1), 36-43, 2013.
- [5] A. Nikolaidis, I. Pitas, Comparison of different chaotic maps with application to image watermarking, *IEEE International Symposium on Circuits and Systems*, 509-512, Geneva, Switzerland, 2000.
- [6] Z. Dawei, C. Guanrong, L. Wenbo, A chaos-based robust wavelet-domain watermarking algorithm, *Chaos, Solitons and Fractals*, 22, 47-54, 2004.
- [7] A. Mooney, A. Keating, J. Pitas, A comparative study of chaotic and white noise signals in digital Watermarking, *Chaos, Solitons and Fractals*, 35, 913-921, 2008.
- [8] K. Veeraswamy, Adaptive AC-coefficient prediction for image compression and blind watermarking, *Journal of Multimedia*, 3(1), 16-22, 2008.
- [9] D.Y. Gang, C. Ying, W.L. Feng, Y. Zheng, Distributions of the DCT coefficient for watermark detection, *International Conference on Computer Application and System Modeling ICCASM*, 13, 96-97, 2010.
- [10] F. Muller, Distribution shape of two-dimensional DCT coefficients of natural images, *Electronics Letters*, 28(22), 1935-1936, 1993.
- [11] R. J. Joshi, T. R. Fischer, Comparison of generalized Gaussian and Laplacian modeling in DCT image coding, *IEEE Transactions on Signal Processing Letters*, 2(9), 81-82, 1995.
- [12] J.H. Chang, J. W. Shin, N.S. Kim, S.K. Mitra, Image probability distribution based on generalized gamma function, *IEEE Signal Processing Letters*, 12(4), 325-328, 2005.
- [13] E.W. Stacy, A generalization of the Gamma distribution, *Annals of Mathematical Statistics*, 33(3), 1187-1192, 1962.

- [14] J.W. Shin, J.H. Chang, N.S. Kim, Statistical modeling of speech signals based on generalized gamma distribution, *IEEE Signal Processing Letters*, 12(3), 258-262, 2005.
- [15] T.M. Ng and H. K. Garg, Maximum likelihood detection in image watermarking using generalized Gamma model, in *Proc. 39th Asilomar Conf. Signals, Systems, Computers*, Pacific Grove, CA, 1680–1684, 2005.
- [16] H.C. Li, W. Hong, Y.R. Wu, P.Z. Fan, On the Empirical-statistical modeling of SAR images with generalized gamma distribution, *IEEE Journal Of Selected Topics In Signal Processing*, 5(3), 386-397, 2011.
- [17] G. Almpandis and C. Kotropoulos, Phoneme segment boundary detection based on the generalized gamma distribution, *IEEE International Symposium on Industrial Electronics*, 1, 691 – 695, 2006.
- [18] A. Noufaily, M.C. Jones, On maximization of the likelihood for the generalized gamma distribution, *Comput Stat*, 28, 505–517, 2013.
- [19] E.Y. Lam, J.W. Goodman, A mathematical analysis of the DCT coefficient distributions for images, *IEEE Transactions on Image Processing*, 9(10), 1661 – 1666, October 2000.
- [20] F. Khelifi, F. Kurugollu, A. Bouridane, Statistical watermark detection in the transform domain for digital images, *Book Chapter*, 120 – 138, 2009.
- [21] K. Kokkinakis and A.K. Nandi, Speech modelling based on generalized Gaussian, *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1, 381 – 384, 2005.
- [22] M.K. Varanasi, B. Aazhang, Parametric generalized Gaussian density estimation, *Journal of the Acoustical Society of America*, 86(4), 1404-1415, October 1989.
- [23] H.L. Harter, Maximum-likelihood estimation of the parameters of a four-parameter generalized gamma population from complete and censored samples, *Technometrics*, 9, 159-165, 1967.
- [24] M.A.R. de Pascoa , E.M.M. Ortega , G.M. Cordeiro, The Kumaraswamy generalized gamma distribution with application in survival analysis, *Statistical Methodology*, 8, 411–433, 2011.
- [25] G.M. Cordeiro, F. Castellares, L.C. Montenegro & M.D. Castro, The beta generalized gamma distribution, *Statistics: A Journal of Theoretical and applied Statistics*, 1 – 13, 2012,
- [26] J. Wang, B.G. Liub, Y. Daib, J. Sunb, Z. Wangb, S. Lian, Locally optimum detection for Barni's multiplicative watermarking in DWT domain, *Signal Processing*, 88, 117–130, 2008.
- [27] R. Kwitt, P. Meerwald, A. Uhl, Efficient detection of additive watermarking in the dwt-domain, *European Signal Processing Conference EUSIPCO*, 17, 2072–2076, 2009.

[28] N.V. Rao, V.M. Kumari, Watermarking in medical imaging for security and authentication, *information security journal: a global perspective*, 20, 148–155, 2011.

Conclusion générale

Le tatouage des documents est encore un domaine de recherche ouvert et les solutions qu'il offre en matière de sécurité sont confrontées au problème de compromis entre la qualité et la robustesse des schémas qui sont utilisés. Les méthodes de tatouage sont diverses, elles sont souvent spécialisées pour un type de support (audio, image, vidéo, ...etc.). C'est pour cela que les recherches continuent dans cette branche, et de plus les algorithmes se spécialisent de plus en plus permettant de répondre au mieux à des applications données.

Nous avons présenté dans cette thèse les différentes méthodes de tatouage d'images numériques. Après avoir souligné les différents principes qui définissent le tatouage d'image, nous avons présenté une classification des différents schémas que l'on peut rencontrer dans la littérature.

Dans cette thèse on a expliqué brièvement les algorithmes de quelques unes de ces méthodes, en les classant selon la manière dont le filigrane est insérée : directement dans l'image (domaine spatial), ou bien dans une transformée de l'image (domaine fréquentiel).

Ce travail de recherche est divisé en deux parties, la première partie est réservée à la présentation de l'état de l'art sur le tatouage chaotique des images numériques, et la deuxième partie est consacrée à la présentation de nos travaux. Ces travaux sont divisés aussi en deux volets : le premier volet représente les algorithmes développés qui sont classés selon leurs domaines d'insertion (spatial, DCT et DWT). Le deuxième volet concerne la modélisation des coefficients bas du ac de la transformée DCT.

Quelques masques visuels sont proposés, en se basant sur la détermination des zones texturées et la modélisation mathématique de l'effet de la luminance sur le système HVS pour le tatouage d'image dans le domaine spatial.

- L'un de nos premiers travaux dans le domaine spatial, était le développement d'un masque visuel pour la pondération du filigrane avant leur insertion dans le domaine spatial, et au même temps de l'utiliser comme un filtre. L'évaluation de

la performance de l'algorithme en terme de visibilité prouve son efficacité ; cependant l'étude de sa robustesse na pas été traité.

- Dans le deuxième algorithme proposé, le masque conçu est basé sur la modélisation de l'effet de la luminance sur le système visuel. La courbe de la modélisation mathématique de la luminance possède une forme exponentielle qui donne des valeurs dans l'intervalle entre 0 et 1.7. Le filigrane est généré à base de la carte logistique. La méthode de la détection c'est une méthode semi aveugle qui nécessite la présence du filigrane seulement, et la procédure est basée sur la méthode de corrélation. L'évaluation de la qualité visuelle des images tatouées se fait par l'utilisation du métrique PSNR. La robustesse de l'algorithme face à la compression JPEG est étudiée.
- Dans un troisième travail, le masque utilisé est basé sur les deux masques qui ont été précédemment conçu ; la texture et la luminance avec une normalisation des valeurs du masque de luminance dans l'intervalle [0,1]. Le filigrane est généré par l'utilisation de la carte logistique ; cependant, le balayage de Peano est utilisé pour augmenter la sécurité du système. Dans l'étape de détection la présence de l'image originale est nécessaire pour faire la différence entre ces deux derniers. Puis le résultat est corrélé avec le filigrane mélangé. La détection de filigrane est basée sur la corrélation entre l'image de différence et la filigrane mélangée. L'évaluation de la qualité des images tatouées est basée sur la mesure de PSNR. Nous avons étudié la robustesse de l'algorithme proposé face à la compression JPEG, le filtrage médian, l'ajout du bruit et le découpage.

Pour le tatouage de l'image dans le domaine transformé, tel que la DCT ; trois travaux ont été présentés :

- Dans le premier algorithme de tatouage d'image la comparaison entre les coefficients de la DCT est analysée dans un système de tatouage complet.
- Vu les avantages présentés par les coefficients DC, ils ont été choisis pour l'insertion du filigrane avec l'utilisation du masque visuel qui contient la texture et la luminance, le filigrane est alors conçu par l'utilisation de la carte skew tent.
- Dans le troisième travail, une modélisation mathématique d'une manière linéaire de la luminance est proposée pour l'obtention d'un masque final qui est basé sur

la multiplication élément par élément entre la texture et la luminance. Ce masque est utilisé pour la pondération du filigrane. L'efficacité de cet algorithme est prouvée par la mesure du PSNR et de l'étude de la robustesse face à quelques attaques.

Quatre algorithmes de tatouage d'image à base du chaos sont proposés dans le domaine d'ondelettes :

- Le premier algorithme est basé sur l'utilisation du masque proposé précédemment (méthode de multiplication), et l'insertion du filigrane est faite dans la bande de basse fréquence. L'étape de la détection consiste à calculer la valeur de la corrélation entre l'image soustraite et le filigrane inséré. L'évaluation de performance de l'algorithme proposé est étudiée face à la compression JPEG et le filtrage médian.
- Un nouveau masque est conçu dont le but de l'amélioration des performances du système de tatouage est donné. Ce masque est basé sur le choix de la valeur minimale entre la luminance et la texture. Une comparaison entre les deux systèmes de tatouage utilisant ces deux derniers masques est faite en terme de visibilité et de robustesse.
- Dans le troisième schéma du tatouage, nous avons utilisé la notion de l'image auto-référence pour l'insertion du filigrane dans le domaine des ondelettes. Une comparaison est faite pour l'évaluation de performance de ce nouveau masque sur un schéma de tatouage complet.
- Le masque basé sur la multiplication entre la texture et la luminance est utilisé, et l'insertion est faite dans la bande basse, mais la détection se fait sans présence de l'image originale. Il s'agit d'une détection semi aveugle basée sur une détection de corrélation linéaire. Les performances de l'algorithme sont évaluées face à la compression JPEG.

Enfin, la modélisation des coefficients bas du ac de la transformée DCT pour le tatouage d'image est traité :

- Avant l'étape d'insertion du filigrane, la DCT est appliquée à l'image hôte, comme dans le chapitre (IV), mais l'insertion du filigrane est faite d'une manière multiplicative, au contraire de la méthode utilisée dans les chapitres (III, IV et V) qui a est sous la forme additive. Une étude statistique du problème de détection nous a conduit à l'élaboration d'un nouveaux détecteur basé sur la distribution GFD et la théorie du maximum de vrai semblance. Les trois paramètres de la distribution GFD sont estimés par l'utilisation de l'algorithme de gradient et de la méthode proposée, proprement dite méthode des moments. Puis l'évaluation des paramètres est mise en application numériquement, et le test d'ajustement est utilisé pour valider le résultat trouvé.

Au cours de ce travail de recherche, nous avons vu l'importance primordiale joué par les transformées DCT et DWT dans les systèmes de tatouage des images numériques. Nous avons amélioré les performances du système de tatouage soit dans le domaine spatial, comme dans le domaine transformé (DCT et DWT). Cette amélioration est faite grâce à la prise en compte des caractéristiques HVS et l'exploitation des propriétés des masques visuelles, que nous avons développés. Les techniques de tatouage dans le domaine transformé sont meilleures par rapport aux techniques spatiales, pour les deux contraintes de la robustesse et de l'imperceptibilité.

Des extensions de ce travail peuvent être envisagées afin de l'améliorer et d'aboutir à de meilleurs résultats. On cite quelques perspectives :

Le masque perceptuel à base de la fonction NVF ne fait pas la différence entre les zones texturées et les bords. Afin d'atteindre une meilleure qualité d'image tatouée une séparation entre les zones texturées et les bords est souhaité.

Une comparaison des performances des algorithmes du tatouage en termes de visibilité et de robustesse dans les deux domaines DCT et DWT sera possible.

D'une part, une combinaison entre les algorithmes développés dans le domaine de la transformée DCT et la DWT est a proposé. D'autre part, une comparaison des performances perceptuelles des masques proposés est a évalué à l'aide des mesures de qualité objectives et subjectives.

Une comparaison entre quelques algorithmes développés dans le domaine spatial et le domaine transformé (DCT ou DWT) sont faite. Il sera sans doute utile aussi de faire une comparaison des performances des algorithmes développés dans un même domaine.

Annexe A: Les techniques de balayage

Les techniques de balayage sont utilisées pour déterminer les régions où le processus d'insertion du filigrane doit se faire ; quelques procédés de balayage (zigzag, raster, Kutter et Peano) sont discutés dans les sections suivantes.

1. Le balayage Zig-Zag

Le balayage en zig-zag a été au départ effectué dans le domaine de DCT et utilisé pour grouper les coefficients de basse fréquence avant les coefficients de haute fréquence dans un vecteur. Le schéma de balayage Zig-Zag a été proposé par Barni [1].

Les 64 coefficients de DCT d'un bloc 8x8 sont réorganisés dans une rangée 1D par l'utilisation du balayage Zig-Zag sont représentés sur la figure (A.1).

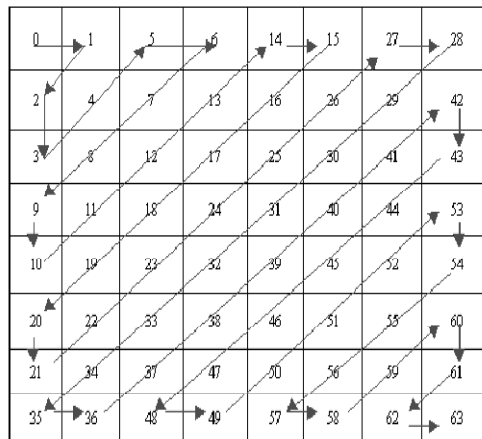


Figure A. 1: Le balayage Zig-Zag

2. Le balayage raster

Le balayage raster est un processus prévisible et peut être facilement mis en application [2].

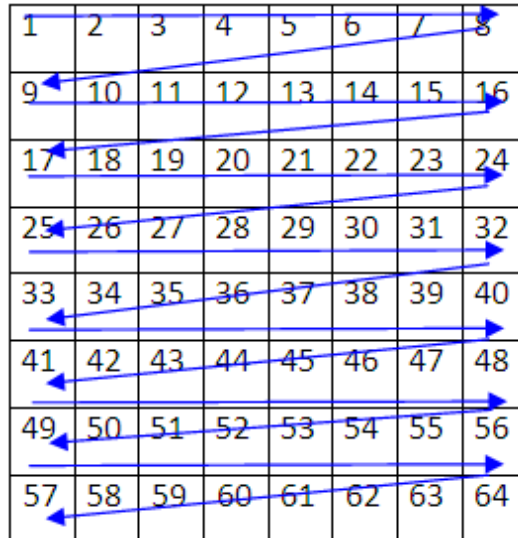


Figure A. 2: Le balayage raster

Tous les éléments d'une image sont balayés ligne par ligne.

3. Le balayage de Kutter

Kutter et al. [3] ont proposé un autre schéma de balayage qu'est donné sur la figure (A.3).

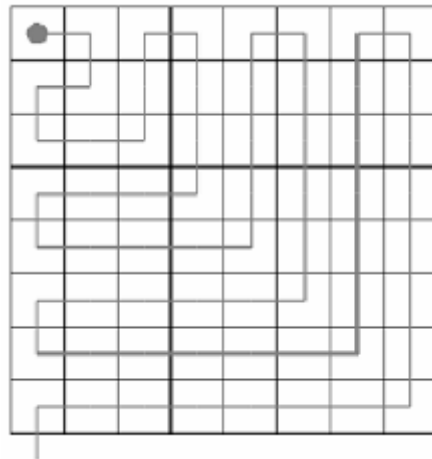


Figure A. 3: Le balayage de Kutter

4. Le balayage de Peano

Le balayage de Peano est une application de la courbe de Peano au balayage d'une image. Il est utilisé pour analyser ou compresser les images [4].

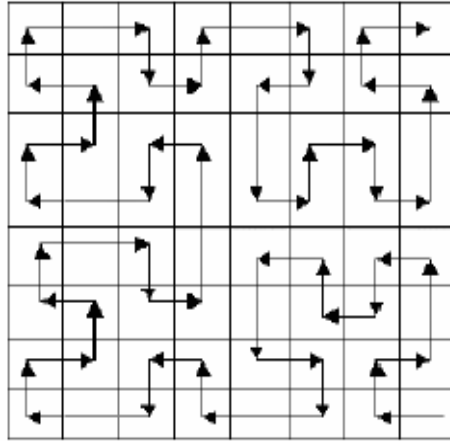


Figure A.4: Le balayage de Peano

Le balayage de Peano est une technique beaucoup très sécurisée si on souhaite de l'utiliser pour l'insertion dans une image. Cependant, le taux de calcul sera plus grand que le balayage raster.

Bibliographies

- [1] M. Barni, F. Bartolini, V. Cappellini, and A. Piva. A DCT-domain system for robust image watermarking. *Signal Processing, Special Issue on Copyright Protection and Control*, 66, 357–372, 1998.
- [2] A. Mooney, *The Generation and Detection of Chaos-Based Watermarks*, Thèse de Doctorat, University of NUI Maynooth, 2005.
- [3] M. Kutter, F. Jordan, and F. Bossen, Digital signature of color images using amplitude modulation, *SPIE Storage and Retrieval for Image and Video Databases*, 3022, 518–526, 1997.
- [4] A.C. Ansari, I. Gertner, and Y.Y. Zeevi, Combined wavelets DCT image compression. *SPIE Proc. Signal Processing, Sensor Fusion and Target Recognition*, 1699, 308-17, 1992.

Annexe B : Démonstration mathématique

Annexe B.0 : Calcul du moment k^{th}

Le moment k^{th} de la variable x qui suit la distribution GFD est donné par l'équation suivante :

$$E(|x|^k) = \int_{-\infty}^{+\infty} \frac{\gamma\beta^\eta}{2\Gamma(\eta)} |x|^{\eta\gamma-1} \exp(-\beta|x|^\gamma) |x|^k dx \quad (B.0-1)$$

Puisque le terme qui se trouve à l'intérieur de l'intégrale est pair, l'équation (B.0-1) devient comme suit :

$$E(|x|^k) = 2 \int_0^{+\infty} \frac{\gamma\beta^\eta}{2\Gamma(\eta)} |x|^{\eta\gamma-1+k} \exp(-\beta|x|^\gamma) dx \quad (B.0-2)$$

Avec le changement de variable :

$$\omega = \beta x^\gamma \Rightarrow x = \left(\frac{\omega}{\beta}\right)^{\frac{1}{\gamma}} \text{ puis } dx = \frac{1}{\beta} \left(\frac{\omega}{\beta}\right)^{\frac{1}{\gamma}-1} d\omega \quad (B.0-3)$$

On obtient :

$$E(|x|^k) = \frac{\gamma\beta^\eta}{\Gamma(\eta)} \int_0^{+\infty} \left(\frac{\omega}{\beta}\right)^{\left(\frac{\eta\gamma-1+k}{\gamma}\right)} \frac{\exp(-\omega)}{\beta\gamma} d\omega \quad (B.0-4)$$

L'équation (4) peut s'exprimer comme suit :

$$E(|x|^k) = \frac{\beta^\eta}{\Gamma(\eta)} \int_0^{+\infty} \left(\frac{\omega}{\beta}\right)^{\frac{1}{\gamma}(\eta\gamma-1+k)+\frac{1}{\gamma}-1} \frac{\exp(-\omega)}{\beta} d\omega \quad (B.0-5)$$

Après certaines étapes de calcul, on obtient :

$$E(|x|^k) = \frac{\beta^{-\frac{k}{\gamma}}}{\Gamma(\eta)} \int_0^{+\infty} \omega^{\eta+\frac{k}{\gamma}-1} \exp(-\omega) d\omega \quad (B.0-6)$$

Le terme qui se trouve à l'intérieur de l'intégrale est défini comme la fonction Gamma et le moment d'ordre k^{th} est donné par l'équation (B.0-7) :

$$E(|x|^k) = \frac{1}{\beta^{\frac{k}{\gamma}}\Gamma(\eta)} \Gamma\left(\eta + \frac{k}{\gamma}\right) \quad (B.0-7)$$

Annexe B.1 : Détermination des paramètres de $G\Gamma D$

Le système d'équations à résoudre, c'est le moment d'ordre un, deux et trois.

$$\begin{cases} E(|x|) = \frac{1}{\beta^{\frac{1}{\gamma}} \Gamma(\eta)} \Gamma\left(\eta + \frac{1}{\gamma}\right) \\ E(|x|^2) = \frac{1}{\beta^{\frac{2}{\gamma}} \Gamma(\eta)} \Gamma\left(\eta + \frac{2}{\gamma}\right) \\ E(|x|^3) = \frac{1}{\beta^{\frac{3}{\gamma}} \Gamma(\eta)} \Gamma\left(\eta + \frac{3}{\gamma}\right) \end{cases} \quad (\text{B.1-1})$$

En prenant le logarithme du système d'équations (B.1-1), et après simplification, on obtient les équations (B.1-2), (B.1-3) et (B.1-4):

$$\ln(E(|x|)) = \frac{-\ln(\beta) - \ln(\Gamma(\eta))\gamma + \ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right)\gamma}{\gamma} \quad (\text{B.1-2})$$

$$\ln(E(x^2)) = \frac{-2\ln(\beta) - \ln(\Gamma(\eta))\gamma + \ln\left(\Gamma\left(\frac{\eta\gamma+2}{\gamma}\right)\right)\gamma}{\gamma} \quad (\text{B.1-3})$$

$$\ln(E(x^2|x|)) = \frac{-3\ln(\beta) - \ln(\Gamma(\eta))\gamma + \ln\left(\Gamma\left(\frac{\eta\gamma+3}{\gamma}\right)\right)\gamma}{\gamma} \quad (\text{B.1-4})$$

A partir de l'équation (B.1-2), on peut obtenir l'équation (B.1-5) :

$$\ln(\beta) = -\ln(E(|x|))\gamma - \ln(\Gamma(\eta))\gamma + \ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right)\gamma \quad (\text{B.1-5})$$

Enfin, le système d'équation à résoudre est obtenu après la substitution de l'équation (B.1-5) dans les équations (B.1-3) et (B.1-4), respectivement.

$$\begin{cases} \ln(E(|x|^2)) = 2\ln(E(|x|)) + \ln(\Gamma(\eta)) - 2\ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right) + \ln\left(\Gamma\left(\frac{\eta\gamma+2}{\gamma}\right)\right) \\ \ln(E(x^2|x|)) = 3\ln(E(|x|)) + 2\ln(\Gamma(\eta)) - 3\ln\left(\Gamma\left(\frac{\eta\gamma+1}{\gamma}\right)\right) + \ln\left(\Gamma\left(\frac{\eta\gamma+3}{\gamma}\right)\right) \end{cases} \quad (\text{B.1-6})$$

Annexe B.2 : Calcul de la moyenne et de la variance

On va calculer la moyenne et la variance du détecteur $T(y)$ comme suit :

$$E(T(y)) = \sum_{i=1}^N -\eta\gamma\omega_i + \gamma\beta\omega_i E(|x_i|^\gamma) \quad (\text{B.2-1})$$

$$\text{Var}(T(y)) = \sum_{i=1}^N (\gamma\beta\omega_i)^2 \text{Var}(|x_i|^\gamma) \quad (\text{B.2-2})$$

En basant sur l'équation (B.0-7) de l'annexe B.0, le moment et la variance d'ordre γ peuvent s'exprimer comme suit :

$$E(|x|^\gamma) = \frac{\Gamma(\eta+1)}{\beta\Gamma(\eta)} = \frac{\eta\Gamma(\eta)}{\beta\Gamma(\eta)} = \frac{\eta}{\beta} \quad (\text{B.2-3})$$

$$\text{Var}(|x|^\gamma) = \frac{\eta}{\beta^2} \quad (\text{B.2-4})$$

La substitution des équations (B.2-3) et (B.2-4) dans les équations (B.2-1) et (B.2-2) respectivement et après certains calculs on obtient la moyenne et la variance comme suit :

$$\begin{cases} E(T(y)) = 0 \\ \text{Var}(T(y)) = \sum_{i=1}^N \gamma^2 \eta \omega_i^2 \end{cases} \quad (\text{B.2-5})$$