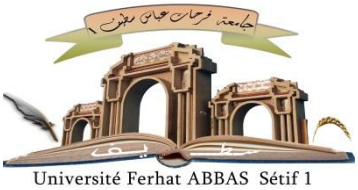
الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique



UNIVERSITÉ FERHAT ABBAS - SETIF1

FACULTÉ DE TECHNOLOGIE

THÈSE

Présentée au Département d'Électronique

Pour l'obtention du diplôme de

DOCTORAT LMD 3eme Cycle

Domaine : Sciences et Technologie

Filière: Électronique **Option: Systèmes Embarqués et Technologie**

Par

SOUADEK Razika

THÈME

Techniques sécurisantes par watermarking

Soutenue le 28/09/2021 devant le Jury:

HASSAM Abdelwahab	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Président**
BOUKEZZOULA Naceur-Eddine	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Directeur de thèse**
FERHAT Hamida Abdelhak	**Professeur**	**Univ. Ferhat Abbas Sétif 1**	**Examinateur**
ROUABAH Khaled	**Professeur**	**Univ. Bordj Bou Arreridj**	**Examinateur**

Laboratoire d'instrumentation Scientifique LIS

RÉSUMÉ

De nos jours le problème des droits d'auteur, la vie privée et l'authenticité des produits multimédia, devient un défi inquiétant. Une technique appelée tatouage numérique exploite des algorithmes mathématiques parvient à répondre à cette exigence dont le compromis : robustesse, invisibilité et capacité doit atteindre par la technique. Cette thèse propose tout abord de nouvelles approches qui visent à améliorer les performances des algorithmes publiés récemment. Dans la première approche, l'algorithme de tatouage est basé sur la compression JPEG 2000 et la technique SVD pour l'insertion de la marque, pour augmenter la sécurité et améliorer la robustesse de l'algorithme nous avons utilisé la technique DE afin de calculer la clé. Pour la deuxième approche, l'algorithme de tatouage est basé sur la transformée DWT-SVD avec l'utilisation de masquage de texture dans le système visuel humain, pour perfectionner la robustesse et la sécurité envers les attaques malveillantes nous avons implanté deux marques sur deux sous-bandes DWT. À la fin, nous avons présenté un nouvel algorithme fiable basé sur la combinaison de la transformée DWT avec une fonction de transfert permettant le changement de l'intensité lumineuse des pixels, après une nouvelle fonction appelée PMF, que nous avons développé, est appliquée pour changer l'emplacement des pixels où nous avons inséré la marque. Les résultats expérimentaux montrent clairement la robustesse et l'efficacité de la méthode développée.

DÉDICACES

Toutes les lettres ne sauraient trouver les mots qu'il faut…

Tous les mots ne sauraient exprimer la gratitude,

L'amour, le respect, la reconnaissance…

Aussi, c'est tout simplement que

Je dédie cette thèse,

À MES CHERS PARENTS

Aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours. Que ce modeste travail soit l'exaucement de vos vœux tant formulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez. Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

REMERCIEMENTS

J'ai le plaisir de formuler mes plus humbles remerciements à :

En premier lieu, au Professeur ***Boukezzoula Naceur-Eddine****, mon directeur de thèse mon conseiller. Je le remercie pour sa compréhension, sa disponibilité, son aide et surtout pour sa patience.*

En second lieu, à tous les enseignants, sans exception, qui m'ont honoré lors de mon cursus en me prodiguant le savoir avec dévouement.

À Messieurs les membres du jury, qui m'ont honoré en acceptant d'examiner, et d'évaluer mon travail.

A toute personne ayant contribué de près ou de loin à l'élaboration de ce travail, je dis, MERCI.

SOUADEK Razika

SOMMAIRE

LISTE DES FIGURES

CHAPITRE 1

CHAPITRE 2

CHAPITRE 3

CHAPITRE 4

CHAPITRE 5

Liste des tableaux

CHAPITRE 1

CHAPITRE 5

INTRODUCTION GÉNÉRALE

Le progrès énorme de la technologie de communication et la prolifération d'internet haut débit, ainsi les grands développements des équipements multimédia tel que les téléphones smart et les appareils photo ont permis de communiquer et d'échanger des multimédia, des audio ou des vidéo en temps réel. Tous ces développements font apparaître d'autre problèmes notamment liées à la protection des droits d'auteur. La protection de propriété intellectuelle nécessite en effet la conception et la mise en œuvre de techniques dans l'intention d'empêcher la réplication illégale.

Une nouvelle technique de dissimulation de l'information appelée tatouage numérique ou *Digital Watermarking* a été largement adoptée par la communauté de la recherche et l'industrie pour la préservation des droits d'auteur sur les produits multimédias. Cette technique sous base sur le fait d'insérer une marque numérique "indétectable" et non-effaçable sur une propriété intellectuelle, où la marque porte des informations telles que des codes d'authentification ou d'autorisations propres aux auteurs [1,2].

Le tatouage de l'image est l'un des moyens technologiques utilisés pour fournir la sécurité et l'authenticité aux images transmis sur des systèmes de communication. Le tatouage d'image, c'est l'ajout d'un nombre de pixels d'une marque à une image originale afin d'obtenir une image tatouée. À l'aide d'un algorithme d'extraction, cette marque peut être détectée aisément à partir de l'image originale et de l'image tatouée [3,4]. En effet, un algorithme de tatouage efficace doit répondre aux exigences telles que la robustesse, l'imperceptibilité, et la capacité d'insertion.

Le domaine de tatouage est déterminé par la méthode d'insertion, pour un algorithme de tatouage. Il existe deux domaines d'insertion, le domaine spatial et le domaine fréquentiel en fonction de l'application à laquelle le tatouage est dédié. Le domaine spatial basé sur l'insertion de la marque dans LSB (*Least Significant Bit*) de l'image, cette technique présente l'avantage de la bonne qualité visuelle. Cependant, elle n'est pas solide contre les attaques géométriques, bruitage et filtrage [5]. Le domaine fréquentiel fondé sur les transformés réversible comme la DCT (*Discret Cosin Transform*) [6], DWT (*Discret Wavelet Transform*) [7], et DFT (*Discret Fourier Transform*) [8] dont la marque est insérée dans les coefficients de la transformée, après la transformée inverse permet de concevoir à nouveau une image, dite tatouée. La combinaison entre deux transformées dans un seul algorithme de tatouage façome un système hybride comme DCT-DWT [9], DWT-SVD [10] et DCT-SVD [11],

l'avantage des systèmes hybrides est d'augmenter le facteur de sécurité, la robustesse et l'invisibilité de la marque.

Le sujet de tatouage numérique d'image est un sujet crucial, car il est lié à la demande pressante des outils sécurisants souples et faciles à implanter dans un software et à intégrer dans des applications industrielles avec un temps d'insertion et de détection raisonnable. Plusieurs techniques de tatouage numérique d'image sont proposées dans la littérature dont le but est de faire face à une ou plusieurs attaques en particulier. Dans ce paragraphe, nous allons présenter en bref quelques techniques de tatouage récentes.

W. Zengh et al. ont présenté, en 2018 [12], un nouvel algorithme robuste basé sur les réseaux de neurones à convolution (CNN) [13], ils ont utilisé dans la phase d'insertion, la transformée en ondelettes discrètes (DWT) dont la technique de décomposition en valeur singulière (SVD) est employée pour insérer la marque. Le réseau de neurones est établi dans le domaine spatial sur la base des relations des pixels avec la marque, l'image originale et l'image tatouée. Après cela, les pixels de l'image tatouée sont légèrement modifiés par le réseau de neurones. Cinq images de test de taille 512*512 en niveaux de gris ont été utilisées pour vérifier cet algorithme, cet algorithme présente un PSNR supérieur à 35 dB.

En 2019, J. Liu et al. [14] ont proposé une nouvelle méthode de tatouage de l'image basée sur la transformée d'ondelettes discrètes (DWT), la décomposition de Hessenberg (HD) et la décomposition en valeur singulière (SVD). L'image originale est décomposée, par le biais de la DWT en sous-bandes, et dont les coefficients résultants sont ensuite utilisés comme entrée pour la HD. En parallèle, la technique SVD est exploitée pour décomposer la marque. Finalement, la marque est insérée dans l'image originale via un facteur d'échelle. Ce facteur est obtenu par l'algorithme d'optimisation de la mouche du fruit. Cette méthode présente un bon compromis entre la robustesse et l'invisibilité de la marque. Cette méthode donne un rapport signal sur le bruit (PSNR) supérieur à 38 dB et un facteur d'auto-corrélation normalisé NC égale à 1, la mesure de similarité SSIM est environ 0.99 pour toutes les tailles de la marque.

A. M. Cheema et al. en 2020, ont introduit un nouveau schéma pour le tatouage d'une image en couleur [15]. Le nouveau schéma de tatouage d'image est fondé sur une méthode hybride dont plusieurs transformées mathématiques sont employées, telles que la transformée en Ridgelet finie (FRT), la transformation en ondelettes discrètes (DWT), la décomposition en valeur singulière (SVD), l'optimisation de l'essaim de particules (PSO) et la transformation d'Arnold et sont assemblées pour concevoir un algorithme de tatouage robuste. Tout d'abord,

l'image en couleur est convertie de l'espace colorimétrique RVB à l'espace YCbCr, la composante de luminance (Y) est prise en compte pour insérer les données de la marque. La composante principale de la marque est directement insérée dans la valeur singulière correspondante de l'image de couverture par un facteur de mise à l'échelle afin d'éviter le problème des faux positifs (FPP). Pour améliorer de plus la sécurité, la transformation d'Arnold est appliquée pour traiter le canal Y de l'image avant l'insertion de la marque dans la couverture de l'image. Cet algorithme est appliqué pour tatouer des images en couleurs, le facteur d'auto corrélation égale à 1 avec un rapport signal sur le bruit supérieur à 45 dB.

En 2021 R. Hu et al. ont publié un article [16] sur une nouvelle méthode de tatouage de l'image. Cette méthode exploite les moments de Zernick d'ordre inférieur pour intégrer efficacement et sans pertes la marque. Cette méthode permet de masquer les distorsions dues au tatouage de l'image. Pour garantir la fidélité de l'algorithme, le processus d'insertion de la marque est suivi d'une phase d'insertion des informations de compensation, il s'agit de l'erreur quantifiée, erreur de tatouage et erreur arrondie pour représenter la différence entre l'image originale et l'image tatouée. Résultat, un système de tatouage d'image avec de bonnes performances, robuste contre les déformations géométriques et sans perte de couverture. Les auteurs ont utilisé plusieurs images de tests afin de valider la méthode proposée et confirment que le PSNR est supérieur à 36 dB.

Un algorithme de tatouage d'image en couleur utilisant les moments d'ordre fractionnaire est présenté par K. M. Hosny et al. en 2021 [17]. Dans cet article, de nouveaux moments d'ordre fractionnaire (MFrEM) et leurs invariances aux transformations géométriques sont dérivés pour la première fois. L'idée de cet algorithme est basée sur l'utilisation de ces moments, connus par leur précision, pour construire un nouvel algorithme de tatouage robuste pour les images couleurs. Cet algorithme est constitué de trois phases ; premièrement, les bits de la marque binaire sont brouillés par une carte chaotique sinusoïdale 1 D. Deuxièmement, les ordres fractionnaires de l'image en couleur (l'image à tatouée) sont calculés. Finalement, un processus de quantification est effectué, où les bits brouillés de la marque binaire sont insérés dans l'image en couleur. Dix (10) images en couleurs sont utilisées pour tester l'efficacité de cet algorithme, la simulation numérique garantit l'invisibilité et la robustesse de la marque insérait contre différents types d'attaques.

Dans cette thèse, nous concentrons sur les techniques de tatouage d'image sécurisées. Le choix de la transformée DWT pour implanter notre algorithme a été déterminé par le fait que le DWT est efficace en terme d'invisibilité, de robustesse et de capacité. Notre manuscrit a été organisé en cinq chapitres comme suit:

- Des généralités sur l'image, des notions sur le traitement de l'image et les schémas de compression d'image sans perte et avec perte ont été présenté dans le premier chapitre.
- Dans le second chapitre, nous avons présenté en bref le schéma de tatouage d'image les méthodes de tatouage telles que les domaines de tatouage des images, le tatouage additif, le tatouage substitutif, les différents types de tatouages. les applications du tatouage numérique des images, les métriques d'évaluations pour un bon jugement sur la technique de tatouage appliquée et la présentation des attaques menaçants le tatouage de l'image.
- Le troisième chapitre est consacré à la présentation de quelque transformées discrètes usuelles utilisés dans le tatouage d'image, où on a défini la décomposition en valeurs singulières (SVD), transformation d'Arnauld, évolution différentielle (DE) et masquage texture (TM) avec l'exploitation du système visuel humain (HVS). Cette dernière aide énormément pour sélectionner les composants les plus appropriés pour insérer la marque. Nous avons aussi présenté des nouveaux outils que nous avons développés. Les outils mathématiques employés dans ce domaine donnent une valeur ajoutée aux exigences de robustesse et d'imperceptibilité.
- Le quatrième chapitre décrit les algorithmes de tatouage hybride améliorés basés sur la transformée DWT et la technique SVD. Dans la première approche, l'algorithme de compression standard JPEG 2000 est développé pour qu'il soit un algorithme de tatouage de l'image, en effet la marque sécurisée par une clé est insérée dans la sous-bande de la DWT, cette méthode permet d'améliorer considérément la robustesse. Les caractéristiques du système visuel humain (HVS) sont exploitées dans une deuxième approche où on applique la fonction de masquage de texture pour extraire la clé appropriée à l'algorithme de tatouage, cette approche présente une bonne imperceptibilité. Une nouvelle technique prometteuse que nous avons développée dans ce travail a été aussi présentée, elle base sur la transformée DWT et une nouvelle fonction de mouvement des pixels qu'on appelle PMF (*Pixels Mouvement Function*).
- Les algorithmes de tatouage proposé dans le chapitre précédent seront implémentés et testés dans le dernier chapitre, nous avons utilisé le Matlab comme moyen de simulation. Les résultats expérimentaux très satisfaisants, spécialement l'analyse des attaques malicieuses, qui montre clairement l'efficacité des méthodes hybride. Nous avons aussi testé notre approche développée. Les résultats expérimentaux montrent qu'elle correspond aux exigences et aux métriques appliquées sur les algorithmes de tatouage récents; la robustesse, l'imperceptibilité et l'efficacité que nous avons obtenues sont comparables avec des travaux récents. L'algorithme proposé présente

aussi un avantage de complexité réduite par rapport à celles des méthodes de tatouage d'images existantes.

Enfin, nous terminerons ce travail par une conclusion générale récapitulant les approches développées et donnant quelques perspectives.

CHAPITRE 1 : GÉNÉRALITÉS SUR LE TRAITEMENT D'IMAGE

1.1. Introduction

Le traitement d'image s'est considérablement développé au cours des dernières années en raison de la diversité et de la sophistication de la technologie. En effet, le traitement d'image est un ensemble de processus et de méthodes appliqués à l'image elle-même, ce qui permet d'améliorer la qualité des images, le rehaussement de contraste. La compression d'image aussi employée un rôle très important dans le traitement d'image, la réduction des pixels redondantes permettre de transmis des informations rapidement et réduire l'espace de stockage.

Dans ce chapitre, nous présenterons les définitions et les techniques qui caractérisent le traitement d'image. Une étude approfondie sur la compression d'image et leurs étages.

1.2. Traitement d'image

1.2.1. Définition de l'image

Une image réelle est la projection sur un espace de trois dimensions, elle est considérée comme une fonction de deux variables $f\ (x, y)$, où x et y sont la position du point dans l'espace et f (x, y) représente son intensité lumineuse ou sa brillance [18].

Une image numérique est composée d'unités élémentaires nommées pixels qui représentent chacun une portion de l'image dans une forme de matrice. La valeur de ce pixel représente une intensité discrète de la lumière ainsi c'est le plus petit élément constitutif d'une image numérique. Une image est définie par le nombre de pixels qui la compose en largeur et en hauteur [18, 19,20]. Selon la couleur du pixel, nous définissons le type d'images ; les images en couleurs sont des images numériques dans l'espace de couleur Rouge, Vert et Bleu (R, V, B). Cet espace est basé sur la synthèse additive des couleurs, c'est à dire que le mélange des trois composantes (R, V, B) donne une autre couleur [19]. Pour les images binaires, un pixel peut prendre uniquement les valeurs noir ou blanc. Les images en niveaux de gris contiennent 256 teintes de gris. Par convention la valeur zéro représente le noir c'est à dire l'intensité lumineuse nulle et la valeur 255 représente le blanc au l'intensité lumineuse est maximale (Figure 1.1) [21].

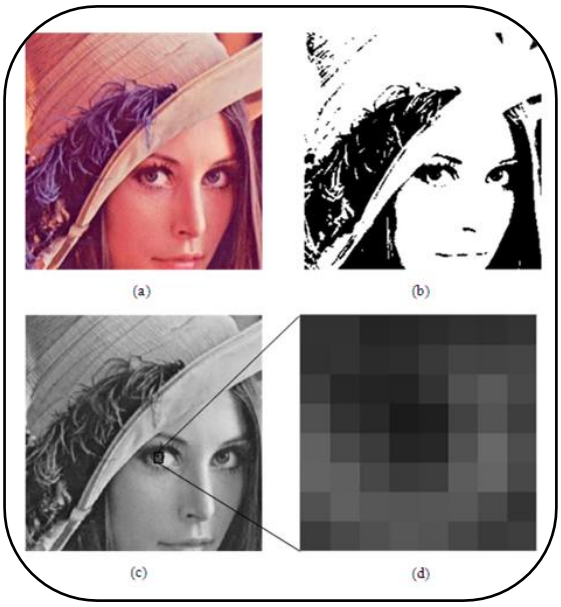


Figure 1. 1: Image de test Lena : (a) Image en couleur, (b) Image binaire, (c) Image en niveaux de gris (d) Teintes de gris.

1.2.2. Acquisition d'une image

L'articulateur entre l'image réelle et l'image numérique en traitement d'image est la procédure d'acquisition d'image, c'est une mesure spatiale d'une interaction entre une onde et de la matière. L'onde est émise par une source et reçue par un capteur ou une camera. L'opération de calibration de caméra est de trouver la relation entre les coordonnées spatiales d'un point de l'espace avec le point associé dans le capteur.

Les principes de l'acquisition d'image sont des sources lumineuses éclairant une scène composée d'objets. Chaque objet absorbe et renvoie cette énergie lumineuse, et le capteur d'images transforme l'énergie lumineuse renvoyée dans sa direction en un signal électrique [22, 23, 24].

1.2.3. Caractéristiques d'une image numérique

- **Dimension**

La dimension peut être mesurée à partir de la matrice d'une image numérique, où le nombre de colonnes (j) représente la longueur et le nombre de lignes (i) représente la largeur, et le point d'intersection de la ligne avec la colonne nous donne un pixel (l'intensité lumineuse), où les coordonnées (i, j) représentent l'emplacement du pixel. La multiplication de la longueur par la largeur donne le nombre de pixels dans l'image numérique.

- **Résolution**

La résolution est le nombre de points par unité de surface (en pouce ou en centimètre). Elle est exprimée en points par pouce (PPP) et (en anglais DPI pour *Dots Per Inch*). Elle est

définie par le rapport entre la définition en pixels d'une image et la dimension réelle de sa représentation sur un support physique (affichage écran, impression papier...) (Figure 1.2) [20,25].

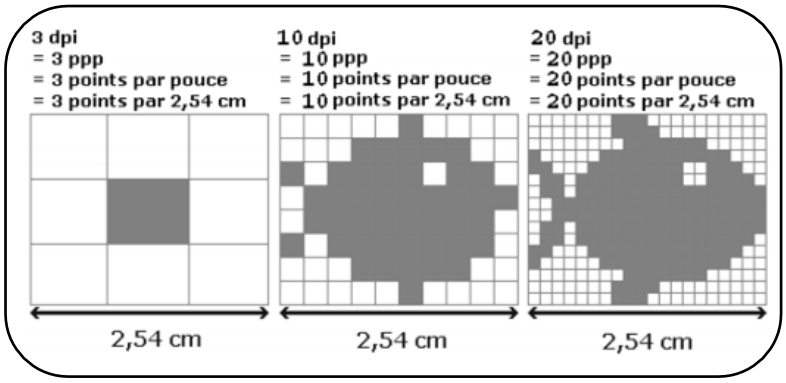


Figure 1. 2: la résolution d'une image.

- **Bruit**

Le bruit est la présence d'une information parasite dans le signal d'image qui provient des appareils électroniques, il crée des distorsions et par conséquent baisse la qualité d'image [26, 27].

- **Histogramme**

L'histogramme représente la distribution des intensités (ou des couleurs) de l'image. Pour une image monochrome, l'histogramme est défini comme une fonction discrète qui associe à chaque valeur d'intensité le nombre de pixels prenant cette valeur. La détermination de l'histogramme est donc réalisée en comptant le nombre de pixel pour chaque intensité de l'image. Il peut être utilisé pour améliorer la qualité d'une image (Rehaussement d'image) en introduisant quelques modifications [28, 29].

- **Luminance**

C'est le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, Elle est définie aussi comme le degré de luminosité des pixels de l'image. La luminance est la quantité de lumière de la couleur, ce mot est substitué au mot brillance, qui correspond à l'éclat d'un objet. Une bonne luminance se caractérise par [28, 30]:

- Des images lumineuses (brillantes).
- Un bon contraste : il faut éviter les images où la gamme de contraste tend vers le blanc ou le noir; ces images entraînent des pertes de détails dans les zones sombres ou lumineuses.
- L'absence de parasites.

- **Contraste**

C'est une propriété intrinsèque d'une image qui quantifie la différence de luminosité entre les parties claires et sombres d'une image. Le contraste est défini en fonction des luminances de deux zones d'images. Le contraste global d'une image est donné par l'équation 1.1, elle est souvent utilisée avec des mires de test pour déterminer la fonction de transfert de modulation d'un système optique, elle est définie par la formule de Michelson [28, 31].

$$C_m = \frac{L_{max} - L_{min}}{L_{max} + L_{min}} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \qquad (1.1)$$

Où **L** désigne la luminance et **I** l'intensité lumineuse

- **Image en niveaux de gris**

Le niveau de gris est la valeur de l'intensité lumineuse en un point. En effet, la couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires, donc pour représenter les images en niveaux de gris, on peut donner à chaque pixel de l'image une valeur correspondante à la quantité de lumière renvoyée. Cette valeur peut être comprise par exemple entre 0 et 255. Chaque pixel est représenté par un octet [28].

- **Image en niveaux couleurs**

Une image couleur est la composition de trois composantes. On définit donc trois plans; un rouge, un vert et un bleu (espace de couleur RVB). La couleur finale est obtenue par synthèse additive de ces trois plans (Figure 1.3) [1].

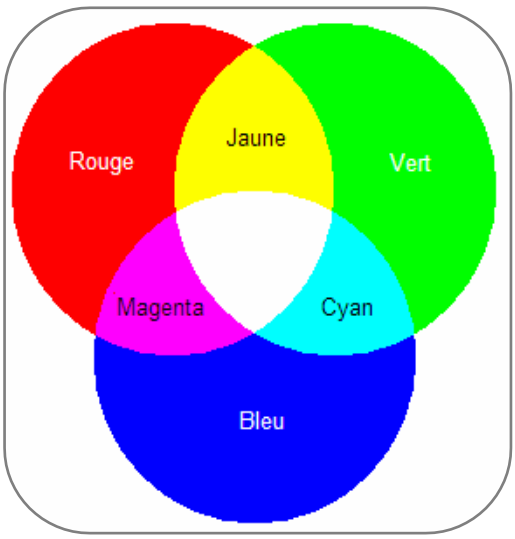


Figure 1. 3: La synthèse additive des couleurs.

1.3. Compression d'image

On distingue deux types de compression d'image: le premier type est la compression sans pertes c.-à-d. qui conserve la suite de bits strictement identiques à l'image originale sans aucune perte dans l'information, l'information est réécrite d'une manière plus concise avec certaines données qui restent inchangées. Le deuxième type est la compression avec pertes où les pixels obtenus après la compression sont différents de ceux de l'image originale, mais l'information reste sensiblement la même. Des fois, cette modification ne peut être remarquée par un humain. La perte d'information est irréversible, il est impossible de retrouver les données d'origine après une telle compression [32].

1.3.1. Technique de compression le standard JPEG 2000

La compression JPEG2000 suit la même structure générique pour la dé-corrélation des pixels dans la trame par une transformée, suivie par la quantification et le codage entropique. La Figure (1.4) illustre le diagramme du bloc de compression JPEG2000 [33].

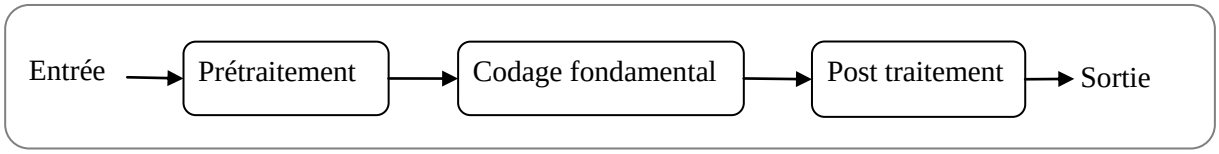


Figure 1. **4:** Le diagramme du bloc général de la compression JPEG 2000.

- **Prétraitement**

Les pixels de l'image sont traités à priori afin de rendre la réalisation des objectifs de conception du JPEG2000 plus facile. Il existe trois éléments dans l'étape de prétraitement :

- ***Tuilage***

Le tuilage est l'opération de division de l'image en des blocs séparés. Toutes les opérations de codage sont appliquées aux tuiles. L'avantage du tuilage est de réduire l'utilisation de la mémoire et de ce fait, il est également possible de traiter et d'accéder à n'importe quelle partie de l'image, de manière indépendante.

- ***Décalage de niveau DC (la composante continue de l'image)***

Pour chaque tuile, une valeur qui correspond à 2^{B-1} est soustraite des valeurs des composants RGB où B est le nombre de bits par composant de couleur. Une telle compensation rend certains types de traitement plus faciles, comme le débordement numérique ou le codage arithmétique. Cette valeur est rajoutée aux composants de couleur au niveau du décodeur.

- ***Transformation de couleur***

La compression JPEG-2000 définit un troisième type de RCT (*Reversible Color Transform*) à utiliser dans le mode sans pertes. Les valeurs des pixels RGB doivent être des entiers (eq. 1.2) :

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.25 & 0.5 & 0.25 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \quad (1.2)$$

Dans le standard JPEG2000, les composants de couleurs de la transformée sont référés comme Y, U et V avec la propriété de rétablir les valeurs exactes RGB des pixels originaux.

- **Codage fondamental**

Dans cette étape, chaque composant de couleur YUV est codé par le codeur. Les étapes du codage par JPEG2000 sont : la transformation, la quantification et le codage entropique.

- ***Transformée d'ondelette discrète***

La DWT est utilisée pour la transformation des pixels. Elle est choisie pour remplir certains besoins de performances prises a priori par le comité « JPEG ». La représentation multi-résolution de l'image est une propriété intrinsèque de la transformée en ondelettes, cela fournit également une scalabilité spatiale, sans avoir à sacrifier l'efficacité de la compression. Le standard définit deux types d'ondelette à utiliser pour la compression avec perte et sans perte. Pour le mode sans perte, le standard choisit l'ondelette 5/3 de Le Galle et Tabatai [34] où il y a cinq coefficients entiers pour le filtre passe-bas et trois coefficients pour le filtre passe-haut. Pour le mode avec perte, l'ondelette 9/7 de Daubechies à coefficients réels [35, 36] est utilisée. Le Tableau (1.1) met en évidence les coefficients des filtres d'analyse passe-bas et passe-haut pour les filtres 9/7 et 5/3 respectivement.

Coefficients	Compression avec perte $(9/7)$		Compression sans perte $(5/3)$	
	Passe bas	Passe haut	Passe bas	Passe haut
0	$+0{,}602949$	$+1{,}115087$	¾	1
± 1	$+0{,}266864$	$-0{,}591272$	¼	$-1/2$
± 2	$-0{,}078223$	$-0{,}057544$	$-1/8$	
± 3	$-0{,}016864$	$+0{,}091272$		
± 4	$+0{,}026729$			

Tableau 1. 1: Les filtres d'analyse passe bas et passe haut utilisés dans JPEG2000.

- ***Quantification***

Après la transformation en ondelette discrète, les coefficients obtenus sont quantifiés linéairement par un quantificateur à zone morte. Le choix du pas de quantification est conduit par l'importance perceptuelle de la bande en question pour le système visuel humain.

- ***Codage entropique***

Les indices des coefficients quantifiés dans chaque sous-bande sont codés en entropie afin de créer un flux binaire compressé. Pour JPEG2000, le comité de JPEG propose le codage *« embedded bloc coding with optimized truncation »* ou EBCOT [33, 37].

- **Post-traitement**

Une fois l'image compressée, le flux binaire produit par les blocs de code individuels est retraité pour faciliter certaines fonctionnalités du standard JPEG2000 :

- La région d'intérêt : la capacité de compresser certaines parties d'une image avec un faible taux de compression.
- L'évolutivité : la capacité de décoder une image avec plusieurs niveaux de qualités ou de résolutions depuis le flux binaire.

1.3.2. Technique de compression le standard JPEG

La technique de la compression JPEG s'applique sur des données perceptuelles (audio, image, vidéo). Le système visuel ne perçoit pas tous les détails d'une image mais plutôt seul un sous-ensemble très faible qui a un caractère exploitable et informatif. L'œil est basé sur la recherche de corrélations entre pixels voisins pour trouver des zones contiguës de couleurs voisines qui lui donneront un résultat très proches de l'original [32, 38].

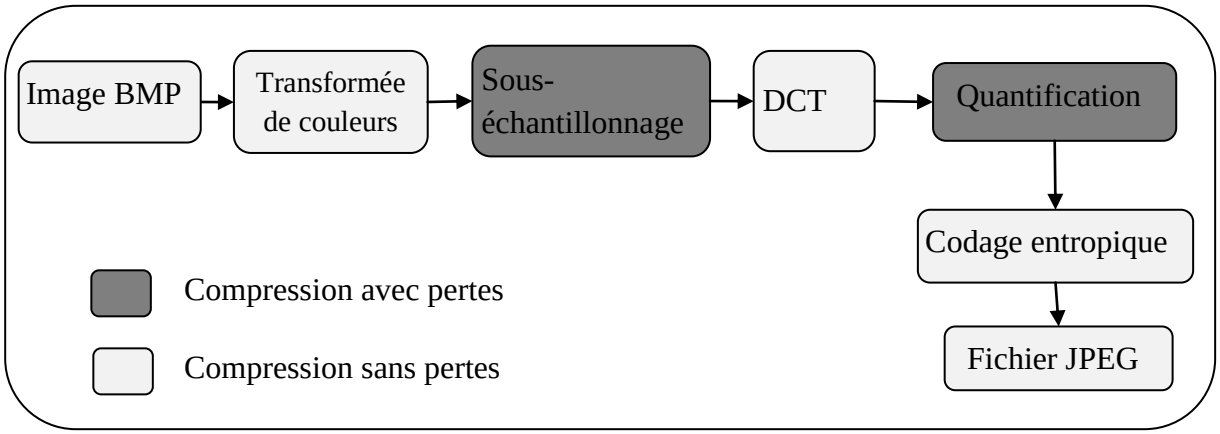


Figure 1. 5: Processus de la compression JPEG.

La compression JPEG (Figure 1.5) peut se décomposer en quatre grandes étapes:

- Transformation de l'espace colorimétrique ;
- Transformation en cosinus discrète ;
- Quantification ;

- Codage run-length et codage entropique.

➢ **Prétraitement**

- ***Transformée des couleurs***

Transformation de l'espace colorimétrique consiste à transformer de manière linéaire l'image de l'espace RVB (Rouge Vert Bleu) dans un espace YC_bC_r Chaque pixel peut s'exprimer (Luminance (Y), chrominance bleue (C_b), chrominance rouge (C_r)). Ces composantes sont souvent sous-échantillonnées afin de diminuer la quantité d'informations à transmettre. La conversion de l'espace RVB à YC_bC_r est réalisable grâce aux équations (eq. 1.3) [38].

$$\begin{cases} Y = 0.299\,R + 0.587\,V + 0.114\,B \\ C_b = -0.1687\,R - 0.3313\,V + 0.5\,B + 128 \\ C_r = -0.5\,R - 0.4187\,V - 0.0813\,B + 128 \end{cases} \qquad (1.3)$$

- ***Division en blocs***

Le choix de bloc de 8 fois 8 est très essentiel parce qu'un groupe formé de 64 pixels constitue une zone spatiale aux propriétés relativement similaires sur toute sa surface. Ce traitement des données de manière séquentielle (par bloc de 64 coefficients) permet de minimiser la mémoire requise lors de l'exécution du programme de compression JPEG d'autant plus de multiples optimisations du code, notamment dans le domaine de l'embarqué.

➢ **Codage fondamental**

- ***Transformée en cosinus discrète DCT***

La DCT est une transformation linéaire (eq. 1.4) qui associe un vecteur de N dimensions à un ensemble de coefficients. La combinaison linéaire de N vecteurs de base connus pondérés par ces coefficients donnera le vecteur original. Les vecteurs de base sont des vecteurs sinusoïdaux. Dans JPEG, on utilise une transformation à deux dimensions.

$$DCT(i,j) = \frac{2}{N} C(i) C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel(x,y) cos\left[\frac{(2x+1)i\pi}{2N}\right] cos\left[\frac{(2y+1)j\pi}{2N}\right] \qquad (1.4)$$

Avant d'appliquer la transformée en cosinus discrète, on divise l'image en blocs de taille 8 fois 8 pixels après on applique la DCT pour obtenir les coefficients. L'information contenue dans le bloc est réorganisée en fonction de la fréquence spatiale. Les hautes fréquences correspondent aux détails et les basses fréquences représentent les variations lentes au sein du bloc (Figure 1.6). Cette réorganisation va permettre de diminuer le poids de l'image tout en maintenant une qualité acceptable (phase de quantification) [39]. Dans l'équation précédente, $C_{i,j} = \sqrt{\frac{1}{N}}$ *si i et j égal* 0 , $C_{i,j} = \sqrt{\frac{2}{N}}$ *si i et j diffèrent de* 0, et N vaut 8.

On distingue deux types de coefficients DCT :

– le coefficient DC correspond à la valeur moyenne de la sinusoïde (premier coefficient du bloc).

– les coefficients AC regroupent les variations dues aux détails. Plus on avance dans la liste des coefficients AC, plus on considère des valeurs qui ont une faible influence dans le codage de l'image [39].

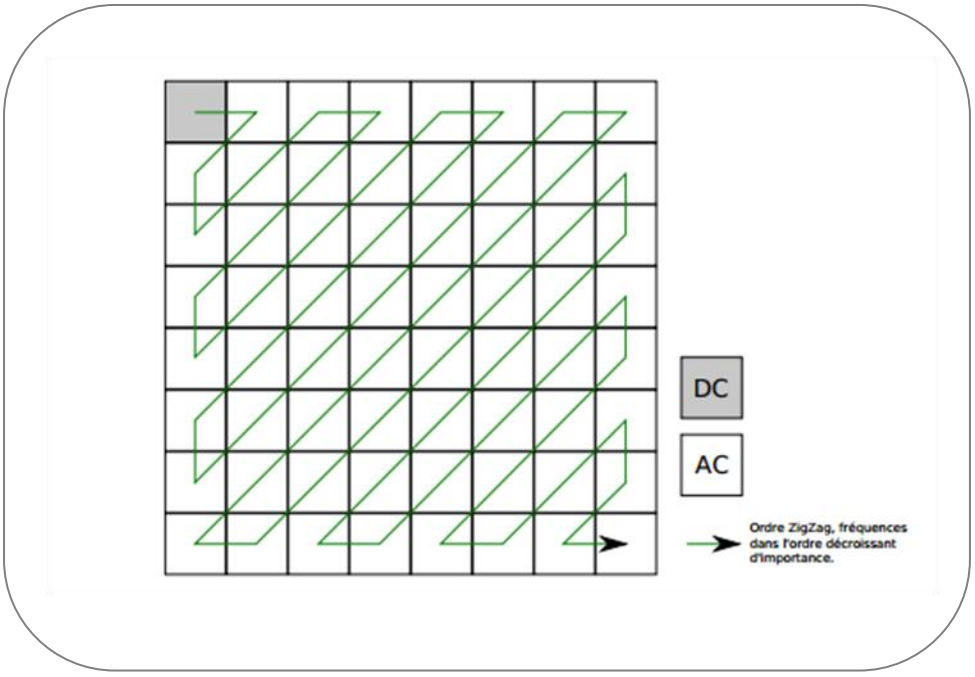


Figure 1. 6: Coefficients dans un bloc DCT et importance des fréquences.

- ***La quantification***

La quantification est l'opération qui permet d'éliminer les informations redondantes et similaires au sein de la chaine de compression. Cela signifie d'appliquer à un bloc DCT donné une matrice de quantification qui va réduire la précision de la représentation de chaque coefficient DCT [38]. L'équation (eq. 1.5) montre le calcul les coefficients DCT quantifiés C_{QT} :

$$C_{QT}(i,j) = \lfloor DCT(i,j)/QT(i,j) \rfloor \qquad (1.5)$$

DCT: matrice des coefficients DCT et QT: matrice de quantification.

- ***Codage Run-length***

Après l'opération de quantification on remarque plusieurs coefficients réduits à zéro ce qui permet de compressé l'image. Chaque coefficient est un octet qui se compose par un bit de poids faible nommé LSB *(Least Significant Bit)* et d'autres bits de poids fort appelés MSB *(Most Significant Bit)*. Le choix de LSB s'effectue sous certaines contraintes liées à un compromis Codage run-length; Une fois les données quantifiées, elles sont compressées sans

pertes à l'aide d'un codeur entropique. Le codage passe par deux étapes le codage run-length et le codage de Huffman [40].

- **Post-traitement**

La compression d'un fichier permet de réduire l'occupation de la bande passante. Il est donc possible d'enregistrer une image sous format JPEG surtout pour les appareils photos numériques et téléphones portables. Cependant, les pertes se produisent lors de la compression dite ''classique'' ce qui fait qu'elle est moins utilisée dans certains domaines comme l'imagerie médicale où la restitution fidèle de l'image initiale est un facteur primordial [40].

1.4. Conclusion

Le traitement de l'image est une partie très importante de traitement du signal qui sert soit à améliorer la qualité de l'image en filtrant les effets parasites, ou à protéger l'image contre la reproduction non-autorisée. Dans ce chapitre, nous avons abordé les notions de base sur l'image où nous avons donné les définitions de chaque caractéristique. Les deux types de compression ont été présentés dans ce chapitre, compression JPEG et compression JPEG 2000. Chaque étage de ces deux algorithmes de compression a été détaillé point par point pour évaluer la qualité de l'image compressée. Dans le chapitre suivant nous présentons les notions de base sur le tatouage des images numériques.

CHAPITRE 2 : GÉNÉRALITÉS SUR LE TATOUAGE D'IMAGE

2.1. Introduction

Le ''Watermarking'' ou tatouage d'image a connu, et connaît encore ces dernières années, un essor spectaculaire. Initialement développé pour renforcer la protection des droits d'auteur sur des documents multimédia, il tend de plus en plus à être utilisé pour remplir d'autres fonctions de sécurité, notamment des fonctions d'intégrité, ou des services d'information. Les techniques de tatouage numériques ont évolué jusqu'à proposer des méthodes très sophistiquées. De nombreux secteurs industriels ont vu dans cette nouvelle branche une solution innovante pour sécuriser les documents numériques.

Nous consacrons ce chapitre pour une étude bibliographique sur le tatouage d'image et les techniques et leurs domaines seront regroupés dans cette partie.

2.2. Le tatouage d'image

Le tatouage d'image est un domaine très actif depuis la fin des années 90. C'est le processus qui consiste à modifier une image en incrustant une information relative appelée la marque qui doit être extraite plus tard. Le tatouage aveugle consiste à extraire la marque du média tatoué sans utiliser l'original. On trouve un exemple de comparaison entre tatouage informé et tatouage aveugle dans [41]. Les deux types de tatouages contiennent un traitement différent de la source. Dans le premier cas, le tatouage informé, le média représente un bruit. On lui ajoute la marque qui sera par la suite retirée par soustraction du bruit. En revanche, dans le cas du tatouage aveugle, on ne peut considérer l'image comme bruit puisque qu'on ne possède pas l'original comme référence. Nous devons utiliser un maximum d'informations concernant cette source afin de charger la marque de la manière la plus fiable possible.

Eggers et Girod ont présenté dans [42] un tatouage aveugle d'authentification utilisant un schéma de tatouage appelé Scalar Costa Scheme. Ce schéma permet de récupérer l'information d'authentification sans l'image originale. C'est un concept qu'il nous faudra reprendre pour la validation d'une image en tant que preuve. En effet, l'image doit nous fournir à elle seule l'information qui nous est nécessaire pour l'authentifier. On peut remarquer que dans ces deux cas, informés et aveugle, la marque peut-être ou non connue à l'avance. D'autres types de tatouage existent, mais sont plus marginaux.

2.2.1. Principe de tatouage d'image

➢ **La phase d'insertion:** Pour insérer une marque dans une image originale on passe par plusieurs étapes par rapport au model d'insertion. Dans le domaine spatial on peut insérer le pixel de la marque sous forme binaire dans le LSB (least significant bit) du pixel de l'image [5]. Par contre dans le domaine fréquentiel, la marque est insérée dans les coefficients de la transformée qui confirme la robustesse de l'algorithme [43, 44, 4]. Dans le troisième cas, la marque est une séquence binaire pseudo aléatoire insérée directement dans les pixels de l'image originale (Figure 2.1) [2].

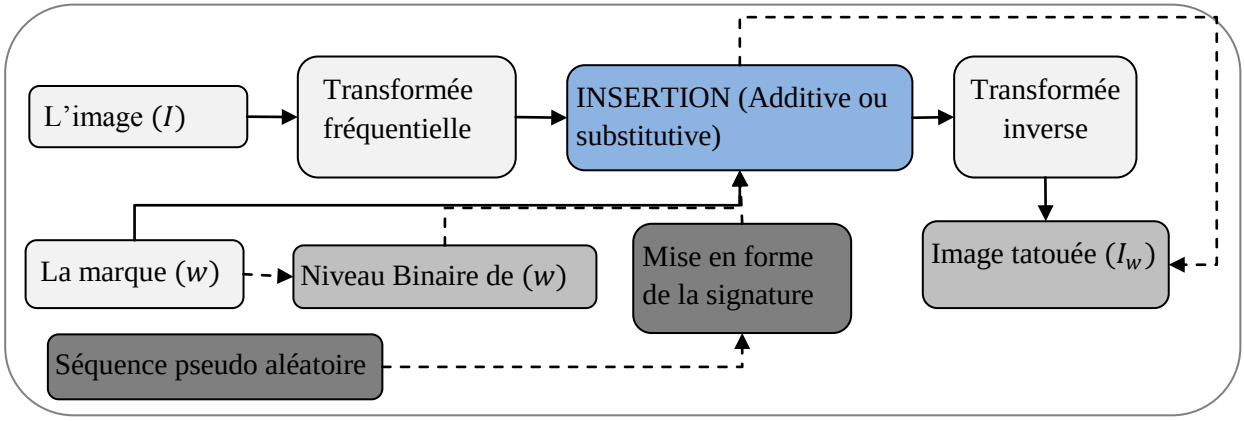


Figure 2. 1 : Schéma du processus d'insertion de la marque.

➢ **Phase de détection:** pour détecter la marque suit l'algorithme d'extraction par rapport au domaine d'insertion, où l'extraction est l'opération inverse de l'insertion. Dans ce cas, on a besoin de l'image tatouée, de l'image originale et de l'algorithme inverse pour obtenir la marque extraite (Figure 2.2) [4].

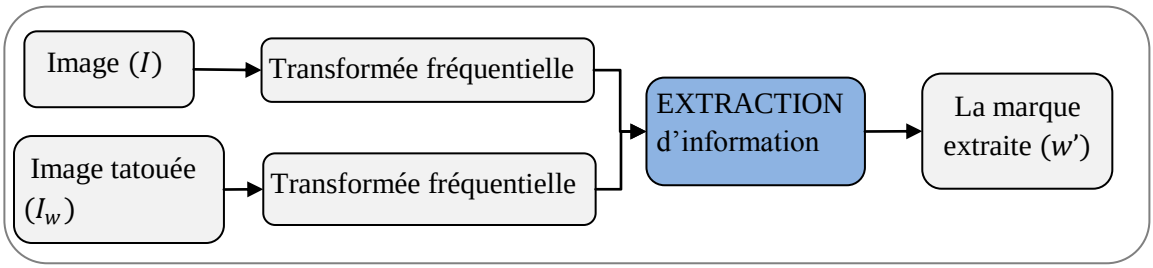


Figure 2. 2 : Schéma du processus de détection de la marque.

La marque extraite w' est comparée à la marque originale w par la mesure de corrélation (eq. 2.1). La mesure de similitude la plus utilisée entre w et w' est la corrélation normalisée pour les séquences pseudo-aléatoires,

$$NC = \frac{\sum_i \sum_j w(i,j) * w'(i,j)}{\sqrt{\sum_i \sum_j w(i,j)^2} \sqrt{\sum_i \sum_j w'(i,j)^2}} \qquad (2.1)$$

Cette mesure est finalement comparée avec un seuil approprié de valeur un ''1'', si le coefficient NC est proche de 1 la marque détectée est similaire sinon elles sont dissimilaires.

2.2.2. Catégories de tatouage d'image

Le Tatouage d'image se divise selon le type d'extraction de la marque en quatre catégories comme suit:

- **Les schémas non-aveugles:** l'image originale, l'image tatouée et la clé secrète sont nécessaires pour détecter la marque.
- **Les schémas semi-aveugles:** dans ce cas on n'utilise pas l'image originale, mais on se base sur quelques caractéristiques dérivées de cette dernière.
- **Les schémas aveugles:** c'est le cas où l'image originale n'est pas une référence pour le processus d'extraction, on utilise uniquement l'image tatouée et la clé.
- **Les schémas asymétriques:** la détection par algorithmes asymétriques peut être schématisée comme une détection aveugle, ces algorithmes utilisent des clés différentes pour insérer et détecter la marque.

D'une manière générale, la robustesse d'un schéma non-aveugle est plus importante que celle d'un schéma aveugle. L'image originale fournit une référence qui sert à améliorer l'estimation de la signature ou encore à identifier les divers traitements subis par l'image tatouée [5].

2.2.3. Les contraintes d'un schéma de tatouage efficace

Un système de tatouage d'image doit vérifier les conditions suivantes:

- **Robustesse :** c'est l'aptitude d'un algorithme de tatouage à résister aux attaques extérieures, qu'elles soient bienveillantes ou malveillantes. La marque doit être difficile à enlever ou à détruire. Elle est définit aussi comme la mesure d'immunité de la marque contre les modifications ajoutées à l'image tatouée comme la compression, le filtrage et le bruitage [45].

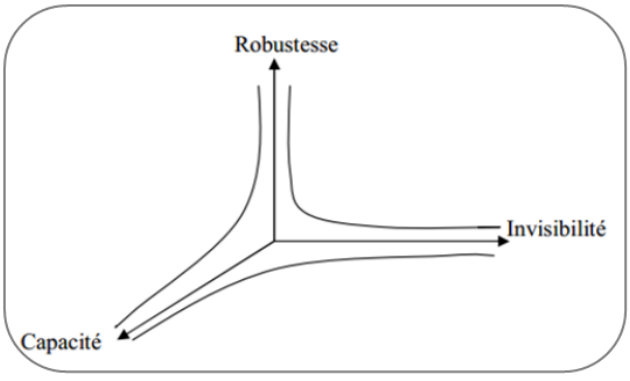


Figure 2. 3 : Problématique des contraintes d'un schéma de tatouage.

- **Capacité :** c'est la quantité d'information (bits de tatouage) que l'on peut cacher au sein d'une image. Il paraît évident que plus on augmente la capacité, plus la marque sera perceptible, et plus la robustesse diminuera [46].

- **Invisibilité :** c'est l'aptitude de l'image tatouée à conserver la meilleure qualité en terme de visibilité de la marque, qui doit être invisible. Concevoir un algorithme de tatouage revient à trouver le meilleur compromis entre ces trois principes : robustesse, capacité et invisibilité (Figure 2.3) [45].

2.3. Domaines de tatouage des images

L'algorithme de tatouage varie par rapport au domaine d'insertion, en effet, chaque domaine de tatouage se caractérise par certains avantages qui permettent son évaluation, c'est pour ça qu'on cite les différents domaines de tatouage.

2.3.1. Domaine spatial

L'algorithme de tatouage dans le domaine spatial modifie directement la luminance des pixels de l'image ce qui permet d'optimiser le temps de calcul lors de l'incrustation, la détection de la marque et le travail en temps réel. Ce type d'algorithme est simple à implanter. La technique additive «patchwork» proposée par Bender et al. [46] est basée sur la décomposition de l'image originale en deux ensembles de même taille. Les pixels de chaque ensemble seront modifiés différemment. Pour détecter la marque on doit faire la différence entre les moyennes des pixels. Cet algorithme est faible relativement à la compression JPEG, un faible taux de compression permet de supprimer complètement la marque.

L'une des méthodes de tatouage d'image utilisées dans le domaine spatial est celle proposée par Kutter et al. [47]. L'algorithme est basé sur l'insertion d'une marque binaire dans la composante bleue de l'image originale. Ces modifications sont proportionnelles à la luminance et additives ou soustractives, selon la valeur du bit. La détection de la marque est réalisée par l'estimation des valeurs de la composante bleue avant et après tatouage.

Généralement, le tatouage dans le domaine spatial n'offre pas de bonne performance en terme de robustesse contre la compression et les attaques de filtrage et géométriques, une légère modification de l'image tatouée est suffisante pour supprimer la marque, d'où l'idée des algorithmes agissant dans le domaine fréquentiel. Le tatouage des images contenant du texte est basé sur la modification de l'espacement vertical et horizontale entre phrases et mots [49]. Dans l'algorithme cité dans la référence [5], la marque est insérée dans le LSB (*Least Significant Bit*) de l'image originale avec une altération des valeurs de pixels qui est une méthode simple à implanter.

2.3.2. Domaine fréquentiel

L'utilisation de la transformée fréquentielle réversible est venue comme une alternative du domaine spatial pour améliorer la robustesse de l'algorithme de tatouage. Parmi les

transformées qui ont prouvé leur efficacité dans ce domaine, on cite la transformée de Fourier discrète (DFT) et la transformée en cosinus discrète (DCT). Chacune de ces conversions a ses propres caractéristiques, par exemple l'utilisation de l'algorithme d'insertion de la marque basé sur la DCT dans la technique de compression JPEG résiste plus à l'attaque de compression. Barni et al [49] ont proposé un algorithme basé sur l'algorithme de compression JPEG. En fait, après la sélection des coefficients DCT à tatouer, une séquence pseudo-aléatoire est adaptée à l'image, en profitant des caractéristiques de masquage du système visuel humain, afin d'assurer la contrainte d'invisibilité de la marque. Le test de cet algorithme contre les différentes attaques donne des résultats médiocres contre les attaques géométriques. Pour améliorer la robustesse, Barni et al. proposèrent d'utiliser la DFT qui est une technique qui possède des propriétés d'invariance permettant d'être robuste face aux attaques géométriques. Cependant, le développement de nouveaux standards comme JPEG2000 a dirigé les regards vers la recherche d'autres domaines d'insertion; soit le domaine multi-résolution.

2.3.3. Domaine multi-résolution

La création de la norme JPEG2000 qui utilise la transformée d'ondelettes discrètes DWT met la lumière sur l'exploitation des avantages de cette technique dans le tatouage d'image. L'analyse multi-résolution est la décomposition de l'image en sous-bandes par les sous-échantillonnages successifs de l'image par la DWT, qui permet un isolement affiné des composantes basses fréquences [50] afin de former un espace d'insertion moins sensible. Xia et al. dans [51] proposèrent un algorithme basé sur l'ajout d'un code pseudo-aléatoire sur les coefficients des bandes à hautes fréquences de la DWT. La détection de la marque est réalisée par une inter-corrélation entre les bandes de l'image initiale et celles de l'image tatouée.

2.4. Les schémas de tatouage additifs

Les méthodes de tatouage les plus sollicitées sont les méthodes additives. Le principe de base de ces méthodes est d'ajouter la marque à des coefficients ou des pixels de l'image originale.

2.4.1. Phase d'insertion

L'incrustation de la marque pour les schémas additifs (Figure 2.4) peut se décomposer en plusieurs étapes :

- la marque W_0 est générée par la modulation d'un bruit blanc par un message M et la clé K.
- la pondération de W_0 par la force de tatouage α, issue du calcul d'un masque psycho-visuel de l'image.

- l'incrustation de la marque amplifiée par α dans l'image, soit dans le domaine spatial ou via un domaine transformé.

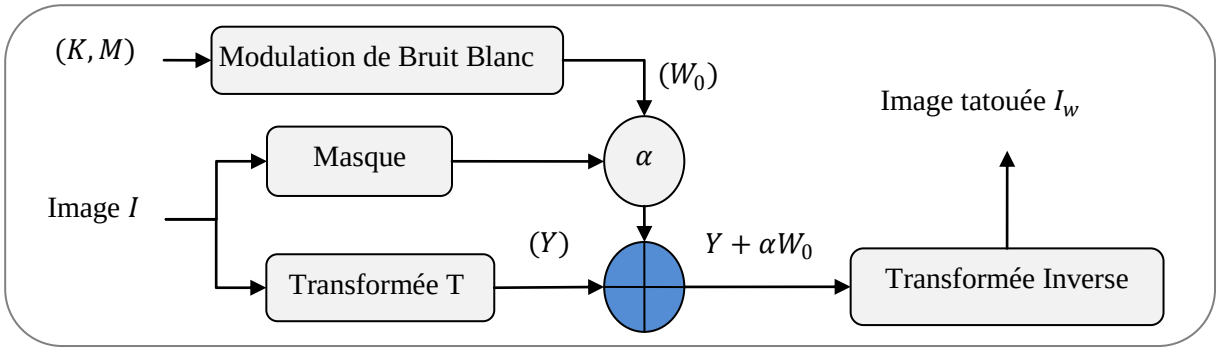


Figure 2. 4: Schéma général d'une méthode de tatouage additive.

Les méthodes basées sur l'incrustation additive sont celles fondées sur des patchs dans le domaine spatial, et sur l'étalement du spectre dans le domaine fréquentiel. Dans les deux méthodes le principe de base est d'ajouter un bruit à l'image originale.

2.4.2. Phase d'extraction

➢ **Détection par corrélation:** Cette technique est largement utilisée dans le tatouage aveugle et semi-aveugle, elle détermine généralement l'existence de la marque. La corrélation entre l'image tatouée I_w et la marque W est effectuée par un vecteur d'observation r, cette corrélation peut s'exprimer sous la forme (eq. 2.2) :

$$r = \sum_{i,j} W(i,j) I_w(i,j)$$

$$r = W * I + W * W \qquad (2.2)$$

La détection de la marque doit passer par les étapes suivantes:

- Extraire les composantes tatouées,
- Générer la marque de base à partir de la clé secrète.
- Effectuer une corrélation entre la marque de base et les composantes tatouées. La marque peut enfin être décodée (Figure 2.5).

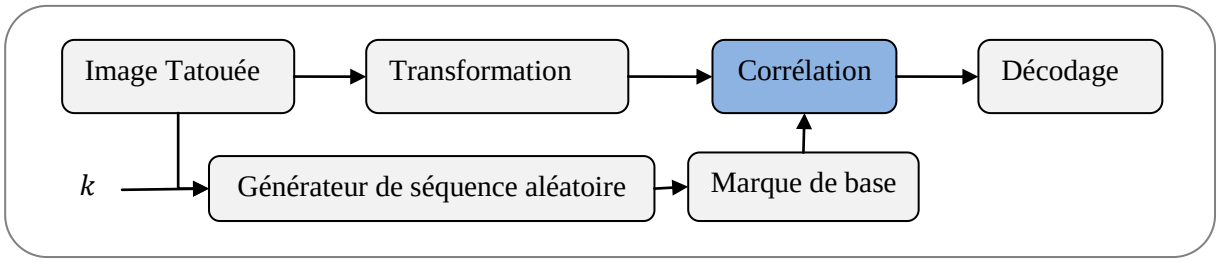


Figure 2. 5 : Détection de la marque par corrélation.

2.4.3. Tatouage additif dans les différents domaines

➢ **Domaine spatial:** Dans cette section, nous présentons un éventail de différentes méthodes de tatouages additifs dans le domaine spatial. L'algorithme « Patchwork » proposé par Bender et al. [46] consiste à sélectionner N paires de pixels de l'image originale (a_i, b_i) à

partir de deux ensembles disjoints A et B de pixels qui dépendent d'une clé secrète K. Ensuite ces pixels, sont modifiés différemment selon l'ensemble A et B auxquels ils appartiennent, selon les formules suivantes (eq. 2.3 et 2.4):

$$a_{iw} = a_i + 1 \quad (2.3)$$

$$b_{iw} = bi - 1 \quad (2.4)$$

À la détection, une différence S_w de la luminance des couples de pixels sélectionnés est calculée (eq. 2.5):

$$S_w = \sum_{i=1}^{N}(a_{iw} - b_{iw}) \quad (2.5)$$

Cependant, une personne ne dispose pas de la clé K ne peut que générer deux ensembles différents de A, B et obtiendra $S_w = 0$ (l'espérance de la somme est alors nulle). Seule la personne disposant de la clé sera en mesure d'obtenir la bonne valeur de S_w. Alors, si l'on choisit pseudo-aléatoirement deux ensembles de pixels de même cardinal que A et B, l'espérance mathématique E de la somme de leur différence est nulle (eq. 2.6):

$$E(S) = \sum_{i=1}[E(a_i) - E(b_i)] = 0 \quad (2.6)$$

Cette méthode peut se résumer par l'addition de l'image et une matrice W pseudo-aléatoire obtenue à partir de la clé K, qui ne contient que des 1, -1 et 0 et de même taille que l'image à tatouer. La valeur 1 représente les pixels de l'ensemble$A$, la valeur -1 pour les pixels de l'ensemble B et le 0 sinon. Si I est l'image originale, I_w l'image tatouée (eq : 2.7):

$$I_w = I + W \quad (2.7)$$

- **Utilisation de l'étalement de spectre:** Le principe de cette méthode est d'étaler le spectre du signal de tatouage (la marque à incruster) sur un canal de transmission bruité (l'image hôte) en utilisant une large bande passante. La marque doit être robuste aux attaques. Tirkel et al. [1, 2] ont été les premiers auteurs à utiliser la technique de l'étalement de spectre pour insérer un signal dans une image. Cette technique se base sur le marquage des bits de poids faible de l'image d'une façon redondante en utilisant la même marque et la détection s'effectue par l'inter-corrélation entre les séquences ajoutées. Cette technique a été améliorée par Hartung et al. [52] par l'utilisation d'un masque de l'image comme espace d'insertion.

La marque étalée a alors la même taille que l'image, avec des 1 et -1 dans les mêmes coordonnées que les pixels du masque présélectionné, 0 sinon. Avant la pondération de la marque par le masque sélectionné, cette marque doit être modulée par une séquence aléatoire. La séquence obtenue est ensuite ajoutée à l'image. La détection s'effectue par corrélation entre la séquence aléatoire et l'image marquée sur le masque d'étalement. Le signe de la corrélation

donne la valeur du bit inséré. Les auteurs précisent que les performances de la corrélation peuvent être améliorées en estimant la marque à l'aide d'un filtre passe-haut (Figure 2.6).

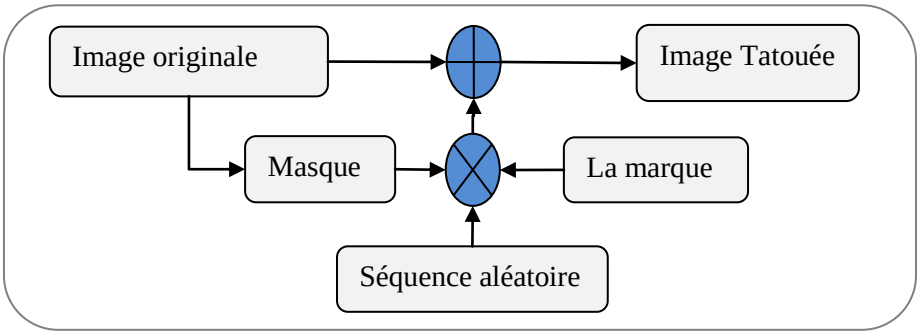


Figure 2. 6: Principe d'incrustation du schéma de Hartung et al.

➢ **Domaine fréquentiel:** Cox et al. [53] proposèrent l'insertion de la marque dans les basses fréquences de la DCT de l'image originale. Dans cette méthode un seuil est utilisé afin de ne modifier que les coefficients de plus grande amplitude (supérieur au seuil sélectionné) suivant l'une des formules suivantes (eq. (2.8),(2.9) et (2.10)):

$$y_i = x_i + \alpha w_i \quad (2.8)$$

$$y_i = x_i(1 + \alpha w_i) \quad (2.9)$$

$$y_i = x_i e^{\alpha w_i} \quad (2.10)$$

y_i : Coefficient DCT de l'image tatouée.

x_i : Coefficient DCT de l'image à tatouer.

α: force du tatouage.

w_i : Coefficient de la marque.

➢ **Domaine multi-résolution:** Barni et al. [54] ont proposé un schéma basé sur l'insertion dans les composants obtenus par la transformée d'ondelettes (DWT). Ils ont utilisé les trois sous-bandes (LH1, HL1, HH1) afin d'obtenir un meilleur compromis entre la robustesse d'algorithme et l'invisibilité de la marque avec l'utilisation d'une pondération d'une séquence pseudo-aléatoire W (Figure 2.7).

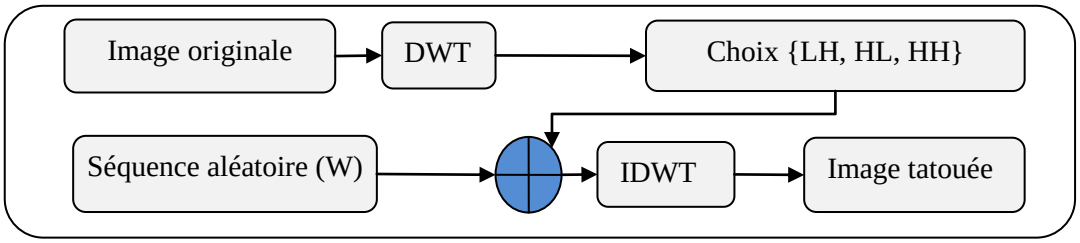


Figure 2. 7: Incrustation de la marque après une décomposition multi-résolution selon le schéma de Barni et al.

2.5. Les schémas de tatouage substitutifs

Le schéma substitutif de tatouage basé sur l'insertion des pixels d'information (la marque). Nous détaillons dans cette section les différentes particularités de cette classe.

2.5.1. Phase d'insertion

Les schémas substitutifs se résument en quatre étapes (Figure 2.8).

- la marque est insérée dans l'espace $C_k(I)$, à partir de la sélection de la clé secrète k.
- la contrainte F sur $C_k(I)$ en fonction de la marque modulée par la clé K donne La marque, Cette contrainte réalise une relation d'ordre, un critère de corrélation, ou une propriété géométrique de l'image.
- l'étape de substitution est appliquée comme suit:

$$C_k(I_w) = F(C_k(I), W) \qquad (2.11)$$

- La dernière étape est la reconstruction de l'image tatouée à partir des composantes propres à la marque.

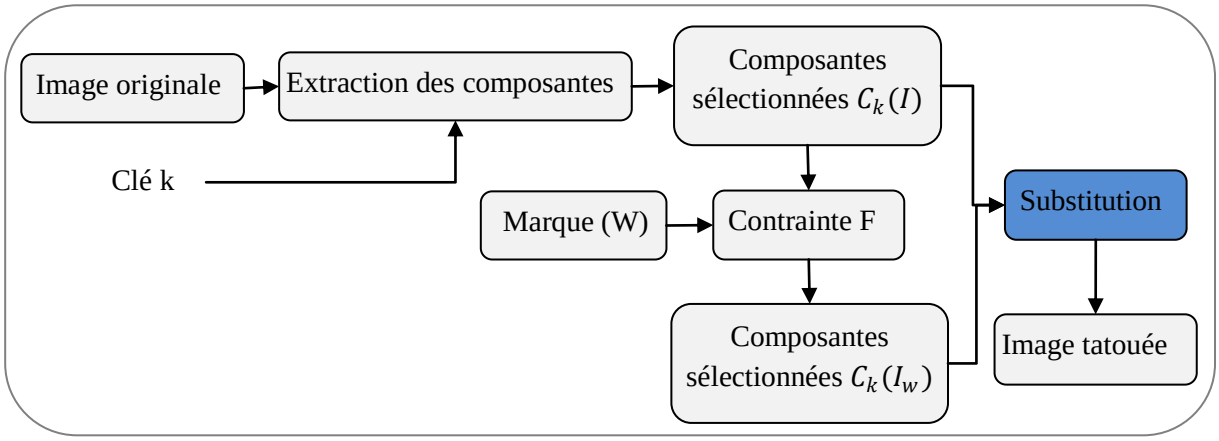


Figure 2. 8: Principe de l'insertion par substitution.

2.5.2. Phase d'extraction

Les étapes de détection de la marque passent par quatre étapes (Figure 2.9):

- l'extraction des composantes de l'image tatouée I_w , $(C_k(I_w))$ en utilisant la clé secrète k.
- l'extraction de W par l'utilisation de la contrainte F utilisée lors de la phase d'incrustation.
- On compare le degré de similitude entre la séquence retrouvée et la séquence utilisée lors de l'incrustation pour détecter la marque.
- La marque peut ensuite être extraite.

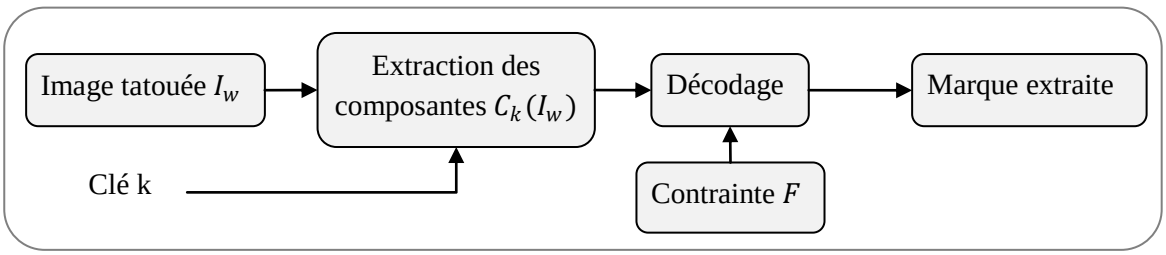


Figure 2. 9: Détection de la marque par substitution.

2.5.3. Tatouage substitutif dans les différents domaines

Nous montrons dans cette section plusieurs schémas de tatouage par substitution.

- **Domaine spatial:** Plusieurs méthodes sont développées, dont l'objectif est d'améliorer la robustesse des schémas de tatouage. Parmi ces techniques nous pouvons citer :

- ***Quantification Vectorielle Spatiale***

Le principe de base de la quantification vectorielle est de remplacer l'espace d'insertion par des blocs appartenant à un dictionnaire formé à partir de la marque à insérer. Une distance minimale entre les blocs du dictionnaire et les blocs de l'image est exigée afin d'assurer une robustesse maximale de l'algorithme. Ce principe a été utilisé par Chen et al. [56] pour insérer la marque dans l'image originale. L'inconvénient de la quantification vectorielle par rapport aux autres techniques est la dégradation de l'effet d'étalement de spectre après les différentes attaques.

- ***Substitution d'histogramme***

Cette méthode de tatouage est basée sur le changement effectué dans l'histogramme de l'image originale par l'utilisation de ses caractéristiques. Coltuc et al. [56] proposèrent un algorithme qui permet d'insérer la marque dans l'histogramme de l'image afin d'assurer une bonne invisibilité de la marque. Les auteurs insèrent la marque dans les pixels de même valeur, ces pixels peuvent être différenciés selon la moyenne des valeurs associées aux différents voisinages. L'histogramme de l'image originale est substitué par un histogramme modifié. Mais on remarque que l'algorithme est à faible résistance contre les attaques.

- ***Tatouage par incrustation de similarités***

Dans les schémas de tatouage basés sur les similarités, remplaçant des blocs de l'image par des blocs similaires, la détection de la marque s'effectue par la recherche de ces blocs. Certains auteurs ont proposé d'incruster la marque par les techniques de substitution via un domaine spatial en utilisant des techniques de similarité. Maes et al. [57] proposèrent d'utiliser la substitution des caractéristiques géométriques de l'image originale.

- **Domaine fréquentiel**

- ***Modification des coefficients TCD***

La modification des coefficients TCD est utilisée dans les normes de compression JPEG et MPEG par blocs de taille 8x8. Cette caractéristique est reprise dans les techniques de tatouage utilisant la DCT. Zhao et al. [58] ont choisi de découper l'image en blocs de 8x8 afin d'être d'avantage robuste à la compression JPEG puis calculer la transformée DCT de chacun des

blocs. L'incrustation de la marque est effectuée à partir des 8 coefficients choisis parmi les fréquences moyennes de chaque bloc.

Seulement trois de ces coefficients sont choisis pour insérer la marque. L'extraction de la marque s'effectue depuis les blocs tatoués sélectionnés. L'algorithme proposé est à faible robustesse contre les attaques géométriques.

- **Domaine multi-résolution:** La transformée en Ondelettes discrète (DWT) est l'aspect multi-échelle permettant une répartition plus robuste du tatouage. Kundur et al [59] insérèrent plusieurs bits dans l'image sur les triplets de coefficients de la DWT dans les sous-bandes de décomposition HL, LH et HH appliqué sur l'image originale. Une séquence aléatoire permet de sélectionner les différents triplets dans lesquels la marque sera incrustée. Ces triplets sont ordonnés en fonction de la valeur du bit à insérer. La détection de la marque s'effectue en localisant les coefficients tatoués grâce à la séquence aléatoire utilisée lors de l'insertion.

2.6. Types de tatouage d'images

2.6.1. Tatouage fragile

Le principe de tatouage fragile est d'incruster une marque binaire dans l'image hôte de telle sorte que le tatouage disparaît au moindre traitement subit sur l'image tatouée (Figure 2.10) La détection de la marque s'effectue en vérifiant la parité des vecteurs appartenant à la base optimale [60].

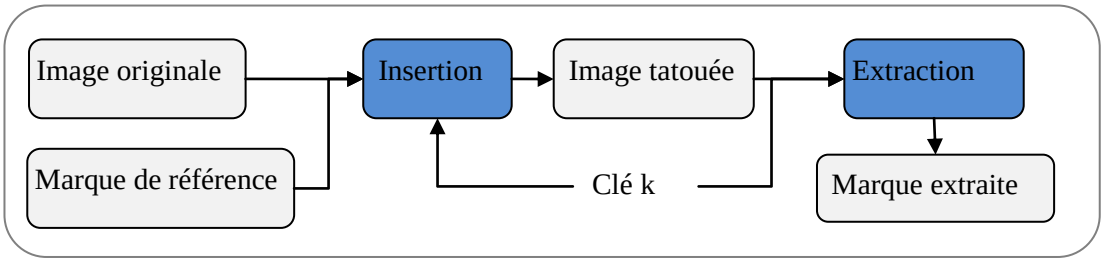


Figure 2. 10: Schéma général d'un système de tatouage fragile.

- **Utilisation des LSB:** Walton [60] était parmi les précurseurs des schémas de tatouage fragiles par les LSB. L'auteur a choisi d'insérer des valeurs de contrôles « checksums » dans les LSB des pixels afin d'assurer une bonne invisibilité. L'algorithme consiste à sélectionner par une clé des blocs de pixels, selon l'algorithme suivant :

- Diviser l'image en blocs de taille 8×8 pixels, pour chaque bloc B_i.
- Définir un ordre de parcours pseudo-aléatoire (selon par exemple une clé secrète et l'indice du bloc Bi) des 64 pixels $(p_1, p_2, \dots, p_{64})$;
- Générer une séquence pseudo-aléatoire de 64 entiers $(a_1, a_2, \dots, a_{64})$ de même ordre de grandeur que N ;
- La valeur de checksum S est alors calculée de la manière suivante (eq. 2.12) :

$$S = \sum_{j=1}^{64} \left(a_j . g(p_j)\right) mod\ N \qquad (2.12)$$

Avec $g(p_j)$ le niveau de gris du pixel p_j en ne tenant compte que des 7 MSB (Most Significant Bits).

- Coder S en binaire ;
- Insérer la séquence binaire obtenue au niveau des LSB des pixels du bloc.

L'algorithme proposé, présente plusieurs avantages en termes d'invisibilité de la marque et de qualité de tatouage vis-à-vis de la quantité d'information incrustée. En plus, il est sensible à la moindre modification de l'image.

➢ **Utilisation de la méthode Self-embedding:** Fridrich et al. [61] ont montré la reconstruction partielle des régions détériorées après attaques par l'insertion d'une grande quantité d'information à l'aide des LSB selon les étapes suivantes :

- Appliquer la transformée DCT sur des blocs de 8x8 pixels de l'image.
- Quantifier les coefficients DCT de chaque bloc, à l'aide de la table de quantification correspondant à une compression JPEG d'une qualité de l'ordre de 50%.
- Les coefficients résultants, sont encodés sur 64 bits.
- Incruster les coefficients dans les LSB des pixels d'un bloc suffisamment éloigné du bloc quantifié afin d'assurer que les distorsions locales que peut subir l'image ne détériorent pas à la fois l'image et les informations de reconstruction.

Ces auteurs ont essayé d'agrandir la matrice de quantification par l'utilisation des deux bits de faible poids. Cette modification a donné de bons résultats pour la reconstruction avec une qualité moyenne en termes d'imperceptibilité.

L'inconvénient majeur de cette méthode est sa fragilité au filtrage passe-bas ainsi la reconstruction correcte des blocs est très difficile. Ce problème a dirigé les regards vers la recherche sur d'autres types de tatouage; soit le tatouage semi-fragile.

2.6.2. Tatouage semi-fragile

Le tatouage semi fragile résiste à certains types de distorsions légères de l'image, tant que le contenu sémantique de l'image n'est pas manipulé. Lin et al. [62] proposèrent un algorithme de tatouage robuste à la compression avec pertes ainsi qu'aux ajustements de la luminance des pixels, afin d'assurer une bonne reconstruction des zones altérées, même après un taux de compression important. Le schéma proposé repose sur deux propriétés invariantes des coefficients de la DCT avant et après compression JPEG.

La première propriété est de modifier les coefficients DCT originaux à un pas de quantification multiple avec un taux de compression JPEG acceptable. La deuxième propriété

définit une règle d'invariance de la relation d'ordre entre les coefficients homologues de deux blocs DCT vis-à-vis de la compression JPEG.

2.6.3. Tatouage robuste

Les schémas de tatouage robuste et non aveugle effectuent une grande robustesse de la marque aux différentes attaques volontaires ou non volontaires. La marque utilisée n'est pas fixe, mais dépend de l'image elle-même Zhao et al. [58] appliquèrent la DCT à des blocs de 8x8 pixels de l'image originale, afin de rendre le schéma proposé plus robuste à la compression JPEG. Un autre schéma robuste, a été proposé par Rey [63], dans le but de vérifier l'intégrité d'une image. L'auteur a proposé d'utiliser une marque qui dépend de l'image elle-même, construite à partir de certaines caractéristiques de l'image originale. Le principe de base de cette méthode est de comparer simplement la marque incrustée avec les caractéristiques préalablement utilisées. Si les caractéristiques sont identiques, cela signifiera que l'image n'a pas été manipulée, sinon les différences indiqueront les régions qui ont été altérées.

2.7. Les applications du tatouage d'image

- **Protection de Copyright:** cette méthode permet d'insérer une information ou marque dans l'image avec le bais d'une clé secrète avec un niveau de robustesse très élevé, pour prévenir toute revendication frauduleuse de propriété. Cette marque est connue par la personne ou par l'organisme de tatouage.
- **Les Empreintes :** cette application est utilisée pour tracer les copies illégales des medias. Ce type d'application engendre un marquage unique pour chaque copie distribuée (typiquement un numéro de série) [64].
- **Protection contre la copie :** un souhait des distributeurs de multimédia est l'existence d'un moyen de protection contre la copie, afin d'interdire une circulation de medias illégaux. Cependant, il est possible d'utiliser des marques spécifiant le statut de la copie de la donnée. Un exemple est le système DVD. Un problème survient dans DVD crypté pour le lecteur non-conforme lorsqu'il est attaqué, et qu'il devient possible de se procurer une copie décryptée de ce DVD. L'utilisation du tatouage permet de combler cette faille, en insérant des informations au sein du flux MPEG4. Les lecteurs non-conformes sont capables de lire seulement les DVDs illégaux, et les lecteurs conformes, les DVDs légaux [64].
- **Contrôle de diffusion** On peut insérer une marque dans une publicité, afin d'en contrôler la diffusion. Cela peut également servir à réaliser une audiométrie.
- **Authentification de données :** L'objectif est de détecter toutes modifications éventuelles des données, afin de pouvoir certifier si celles-ci ont été modifiées ou non.

- **Sécurité médicale :** Insertion d'un identifiant confidentiel assurant la correspondance entre le patient et la radio, afin d'éviter toutes confusions [64].

2.8. Les outils d'évaluation des performances

L'insertion d'une marque dans une image effectue la condition de l'invisibilité, les algorithmes de tatouage utilisent les caractéristiques du système visuel humain (HVS) en cachant la marque dans les régions les moins sensibles de l'image (e.g. les contours et les zones de textures). Une bonne métrique de qualité d'image se doit également de prendre en compte les caractéristiques HVS. le paramètre PSNR (Peak Signal to Noise Ratio) est la mesure de qualité de l'image tatouée par rapport à l'image originale [65, 66, 67].
La métrique classique du PSNR est donnée par la formule suivante (eq. 2.13) :

$$PSNR = 10log_{10}\frac{\max(x)^2}{\|x' - x\|^2} \qquad (2.13)$$

Où x', x représentent l'image tatouée et l'image originale respectivement.

2.9. Attaques menaçant le tatouage d'image

L'image tatouée subit des changements sur le canal de transmission de façon intentionnelle ou de façon accidentelle. Ces déformations introduisent des dégradations de performances sur la détection des marques. Nous présentons quelques types d'attaques connues.

- **Bruit Additif :** La conversion numérique/analogique ou la transmission introduit des bruits, détectés dans la marque extraite. Le système peut introduire un bruit imperceptible pour rendre méconnaissable la marque.
- **Filtrage :** Le filtrage génère des dégradations qui apparaissent dans les images tatouées, et la marque extraite peut être invisible, aussi il peut considérablement affecter la performance de la détection des marques.
- **Découpage :** Dans le cas où la personne est intéressée par une petite partie de l'image tatouée, la marque extraite est déformé parce que la marque insérée est répartie sur toute l'image.
- **Compression :** C'est généralement une attaque involontaire qui apparaît très souvent dans des applications de multimédia. Pratiquement les images tatouées actuellement distribuées par l'intermédiaire de l'Internet ont été compressées. La réduction des bits dans l'image compressée cause des pertes de l'information incrustée. C'est pour cette raison que le fichier multimédia doit avoir une robustesse face à la compression [68,69].

2.10. Classification des attaques du tatouage

Les attaques de suppression visent à enlever et supprimer la marque comme le bruit avec ses statistiques. Les algorithmes de tatouages tentent d'enlever ce bruit. L'objectif des attaques

géométriques est la distorsion de la marque, ou la désynchronisation, avec comme résultat le fait que le lecteur n'est plus capable de relire la marque, même si celle-ci est toujours là. On pourra prendre comme exemple les rotations d'images. L'objectif des attaques de cryptographie est de découvrir des informations sur les paramètres secrets comme les clés. Finalement, on trouve les attaques de protocole qui n'essayent ni de supprimer ni d'altérer la marque, mais cherchent à la manipuler par exemple en inversant la marque, en la copiant, ou en accédant au codeur (Figure 2.11) [70].

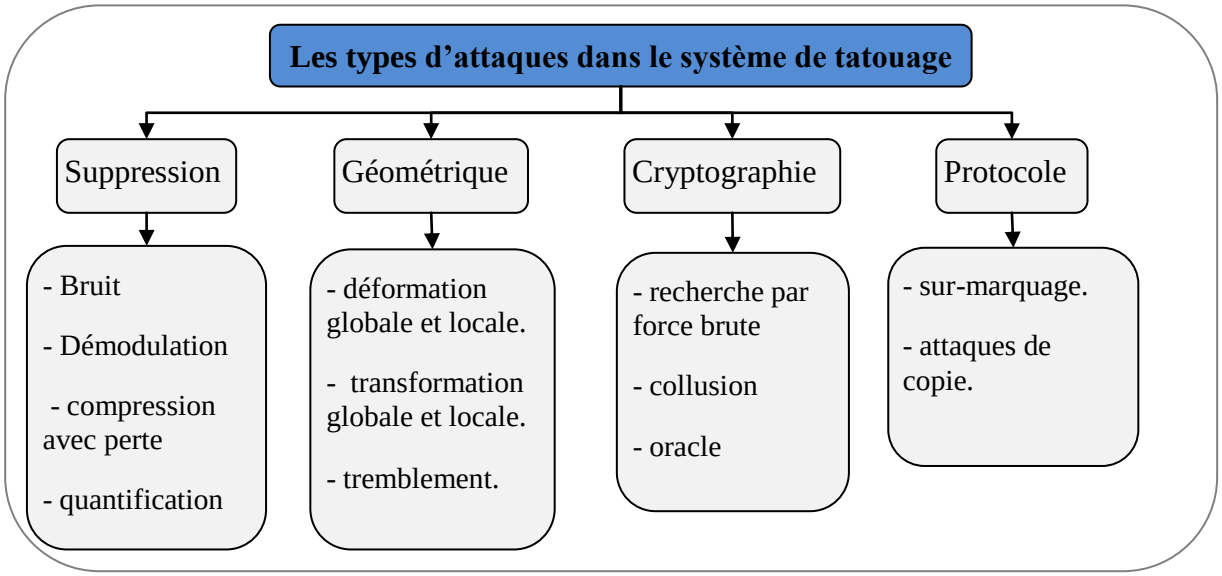


Figure 2. 11: Les types d'attaques dans le système de tatouage.

2.11. Conclusion

Le tatouage d'image est l'ensemble des techniques permettant d'incruster une marque imperceptible à l'œil dans une image originale afin de garder aux propriétaires légitimes leurs droits d'auteur où il est présenté dans ce chapitre. Différents algorithmes de tatouage de l'image ont été développés par les chercheurs, dont la différence entre eux est définie par la méthode d'insertion, l'emplacement de l'insertion et la méthode d'extraction de la marque. Pour évaluer la puissance de protection de l'algorithme, trois critères doivent être vérifiés ; la robustesse, l'imperceptibilité et la capacité. Les algorithmes présentés dans ce chapitre montrent des avantages et des inconvénients en termes des exigences de la protection. Pour mieux maitriser le sujet des algorithmes de tatouage de l'image, les outils mathématiques et les transformées seront présentés dans le chapitre suivant.

CHAPITRE 3: LES TRANSFORMÉES FRÉQUENTIELLES ET LES OUTILS MATHÉMATIQUES

3.1. Introduction

Dans ce chapitre, nous présenterons les différenttes transformées les plus employées dans le domaine de traitemant d'image comme la transformée d'ondelettes, la transformée de Fourier, la transformée de cosinus et la transformée de Hartley, l'idée de base des transformées consiste à insérer la marque dans les coefficients de l'image après reconstruire l'image dans le but est de formé une image tatouée, où la marque est invisible. Ensuite nous expliquerons l'ensemble des outils mathématiques utilisés dans le domaine de tatouage d'image, en effet, la phase d'insertion de la marque nécessite des outils mathémathique adéquats qui servent à mixer les paramatters de la marque avec celle de l'image. L'image résultante, dite image tatouée me montre aucune différence par rapport à l'image originale (hôte).

3.2. Transformées fréquentielles

3.2.1. Transformée DCT

La DCT (*discrete cosine transform*) est une dérivée des transformées de Fourier. En effet, la DCT transforme une matrice N*N en une autre matrice N*N, dont les amplitudes sont rangées selon leurs fréquences : les basses fréquences sont situées en haut à gauche et les hautes fréquences en bas à droite. Les basses fréquences sont les plus importantes pour le tatouage de l'image, tandis que les hautes fréquences sont moins importantes. La valeur de coordonnées (0,0) correspond à la valeur moyenne des éléments de la matrice.

La DCT fait correspondre à chaque valeur de $Y(x,y)$ une valeur de $F(u,v)$ donnée par la formule (eq. 3.1) [71]:

$$F(u,v) = \frac{2}{N} c(u)c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Y(x,y) \cos\left(\frac{\pi}{N} u\left(x+\frac{1}{2}\right)\right). \cos\left(\frac{\pi}{N} v\left(y+\frac{1}{2}\right)\right) \qquad (3.1)$$

Avec : $u, v, x, y \; variant \; de \; 0 \ldots N-1$ (N ensemble de nombre naturelle correspond à la taille de l'image).

$$c(j) = \frac{1}{\sqrt{2}} \; si \; j = 0$$

$$c(j) = 1 \; si \; j > 0$$

Pour revenir à l'image, on utilise la formule suivante (eq. 3.2) :

$$Y(x,y) = \frac{2}{N} \sum_{v=0}^{N-1} \sum_{u=0}^{N-1} c(u)c(v)F(u,v) \cos\left(\frac{\pi}{N} u\left(x+\frac{1}{2}\right)\right). \cos\left(\frac{\pi}{N} v\left(y+\frac{1}{2}\right)\right) \qquad (3.2)$$

3.2.2. Transformée DWT

La transformée en ondelettes continue est très redondante. Afin d'appliquer efficacement la transformée en ondelettes aux signaux discrets, il convient de discrétiser les coefficients de translation a et de dilatation b.

On impose donc une grille de valeurs discrètes pour a et b. On pose $b = b_0^m$ et $a = na_0b_0^m$ avec $a_0 \in Z \; et \; b_0 \in Z$.

La transformée en ondelettes discrète (DWT) est donnée par (eq. 3.3) [11, 72]:

$$f(m,n) = b_0^{\frac{-m}{2}} \int_{-\infty}^{+\infty} f(t)\psi(b_0^{-m}t - na_0)dt \qquad (3.3)$$

Si on choisit $b_0 = 2$ et $a_0 = 1$, on se place dans le cas dyadique. On a alors (eq. 3.4) :

$$f(m,n) = 2^{\frac{-m}{2}} \int_{-\infty}^{+\infty} f(t)\psi(2^{-m}t - n)dt \qquad (3.4)$$

- ***Les familles d'ondelettes***

Il existe une infinité de fonctions d'ondelettes parce que toute fonction oscillante localisée est une ondelette mère possible. Cependant, elles ne possèdent pas toutes des propriétés intéressantes. En fait, de nombreux spécialistes des ondelettes ont construit des familles d'ondelettes possédant certaines propriétés remarquables.

Parmi les familles d'ondelettes, il y a la famille des ondelettes splines dont la réponse fréquentielle est bien localisée. Les différentes familles d'ondelettes sont utilisées selon leurs propriétés en fonction du problème à résoudre.

- ***Ondelette de Haar***

C'est la plus simple des ondelettes : définie sur l'intervalle $[0, 1]$ (ou parfois sur $[-1/2,1/2]$ c'est la fonction H constante par morceaux qui vaut (eq. 3.5) et illustrée (Figure 3.1) :

$$H(x) = \begin{cases} -1 \; si \; x \in \left[0, \frac{1}{2}\right[\\ 1 \; si \; x \in \left]\frac{1}{2}, 1\right] \end{cases} \qquad (3.5)$$

Cette ondelette est très simple et donc facile à mettre en œuvre algorithmiquement. De plus, son support est compact : elle est bien localisée en espace. En contrepartie, elle n'a qu'un seul moment nul.

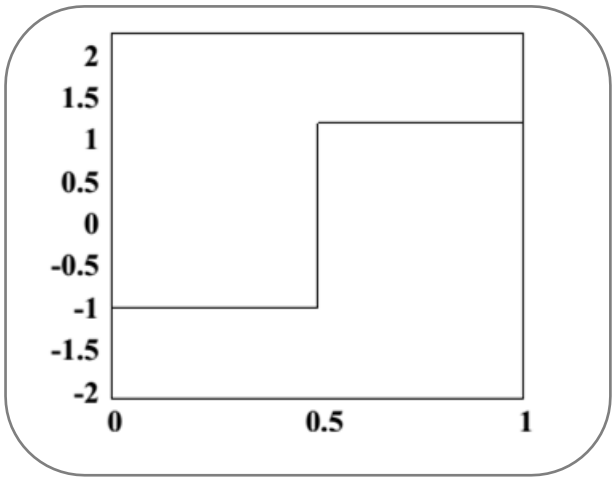


Figure 3. 1 : Ondelettes de Haar.

3.2.3. Transformée DFT paramétrique

La transformée de Fourier est la transformée la plus populaire et la plus utilisée. Elle a des applications dans plusieurs domaines de la science et de la technologie en raison de l'existence de la transformée de Fourier rapide (*Fast Fourier Transform : FFT*) [73-75]. La transformée de Fourier fractionnaire (*Fractional Fourier Transform : FrFT*) et la transformée de Fourier discrète (DFT) paramétrique sont intéressantes pour certaines applications [76-79]. La DFT paramétrique est obtenue en remplaçant convenablement quelques éléments spécifiques dans le vecteur du noyau de la DFT classique par des paramètres indépendants qui peuvent être choisis arbitrairement dans le plan complexe.
La DFT paramétrique de trois paramètres (*three-parameter DFT*) d'une séquence Complexe $x(k)$ de taille $N = 2^r$, où $r > 3$, est définie par [78]:

$$X^{a,b,c}(n) = \sum_{k=0}^{N-1} x(k) v_{F^{a,b,c}}(nk \bmod N), \quad avec \ 0 \le n \le N-1 \tag{3.6}$$

Où $v_{F^{a,b,c}}$, dénote les éléments de vecteur $V_{F^{a,b,c}}$ donnés par

$$V_{F^{a,b,c}} = [1 \quad V \quad c \quad -jV \quad -1 \quad -V \quad -c \quad jV] \tag{3.7}$$

Avec

$$V = \begin{matrix}[W_N^1 & \dots & W_N^{(N/16)-1} & a & W_N^{(N/16)+1} & \dots & W_N^{(N/8)-1} & b & W_N^{(N/8)+1} \\ \dots & W_N^{(3N/16)-1} & -ja^* & W_N^{(3N/16)+1} & \dots & W_N^{(N/4)-1}]\end{matrix} \tag{3.8}$$

Où $W_N = exp(-j(2\pi/N))$ et $a, b \ et \ c$ sont trois paramètres indépendants qui peuvent être choisis arbitrairement du plan complexe. La transformée inverse est donnée par :

$$x(t) = \frac{1}{N} \sum_{K=0}^{N-1} X^{a,b,c}(n) \frac{1}{v_{F^{a,b,c}}(nk \ mod \ N)}, \quad avec \ 0 \le k \le N-1 \tag{3.9}$$

Les deux équations (3.6) et (3.9) peuvent être écrites sous forme matricielle comme suit :

$$X^{a,b,c} = F_N^{a,b,c}.x \quad (3.10)$$

$$x = (F_N^{a,b,c})^{-1}.X^{a,b,c} \quad (3.11)$$

0ù les éléments de la matrice $F_N^{a,b,c}$ sont :

$$F_N^{a,b,c}(n,k) = v_{F^{a,b,c}}\,(nk\ mod\ N),$$
$$avec\ 0 \le n\ et\ k \le N-1$$

3.2.4. Transformée DHT

La DHT est une transformation mathématique qui transforme une fonction temporelle ou spatiale à valeurs réelles en une fonction fréquentielle. Elle est obtenue par la soustraction de la partie imaginaire de la partie réelle de la matrice DFT. Comme la matrice F_N^{α} d'un seul paramètre présentée dans la section précédente est une matrice unitaire de valeurs complexes, une matrice réelle d'un seul paramètre est obtenue en soustrayant la partie imaginaire de la partie réelle de la matrice F_N^{α}. La matrice résultante H_N^{α} représente la matrice DHT paramétrique d'un seul paramètre (DHT^{α}) définie par (eq. 3.12) [78]

$$H_N^{\alpha} = Re(F_N^{\alpha}) - Im(F_N^{\alpha}) \quad (3.12)$$

3.3. Outils mathématiques

3.3.1. Technique SVD

La théorie de la décomposition en valeurs singulières SVD a été établie pour les matrices réelles carrées puis les matrices complexes. Récemment, la décomposition en valeurs singulières a été utilisée dans différentes applications du traitement d'image telles que la compression, la dissimulation de l'information et la réduction du bruit [82].

- ***Principe***

Soit A une matrice quelconque de taille $m * n$ et de rang r (le rang de la matrice A est le nombre de valeurs singulières non nulles). Alors il existe une matrice orthogonale U d'ordre $m * m$, Une matrice orthogonale V d'ordre $(n * n)$ et une matrice S *"pseudo diagonale"* (tous les éléments hors de la diagonale principale sont nuls, mais la matrice n'est pas carrée) de dimension $(m * n)$, telles que:

$$A = U * S * V^T \quad (3.13)$$

$$\begin{cases} U * U^T = I(m) \\ V * V^T = I(n) \\ S(m,n) = \begin{bmatrix} S_1 & 0 & \dots & 0 \\ 0 & S_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & S_n \end{bmatrix} \end{cases} \quad (3.14)$$

$S_1, S_2, \dots, S_n$ représentent les valeurs singulières de A, lesquels sont des nombres réels non négatifs, et qui respectent la condition: $S_1 > S_2 > \cdots > S_n$.

Le principal intérêt de la méthode SVD pour le traitement d'images vient du fait que:

- Les valeurs singulières représentent l'énergie de l'image, c'est-à-dire que la SVD range le maximum d'énergie de l'image dans un minimum de valeurs singulières.
- Les valeurs singulières d'une image ont une très bonne stabilité, c'est-à-dire que quand une petite perturbation (par exemple une marque) est ajoutée à une image, les valeurs singulières ne changent pas significativement.
- En plus, la factorisation en SVD est unique.

3.3.2. Transformation d'Arnold

Pour renforcer la sécurité du schéma de tatouage, la marque doit être randomisé avant d'être insérer dans l'image. Il y a plusieurs façons de brouiller, mais nous allons discuter ici uniquement la transformation d'Arnold [83] qui est un processus itératif permettant de changer la position du pixel. Généralement, la transformée d'Arnold à deux dimensions (2D) est définie comme suit (eq. 2.20):

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_{k-1} \\ y_{k-1} \end{bmatrix} mod\ (n) \quad (3.15)$$

où x_k et y_k sont des coordonnées transformées correspondant aux coordonnées x_{k-1} et y_{k-1} après k itérations; n est la hauteur ou la largeur de l'image carrée traitée, a et b sont des entiers positifs.

Il s'agit d'un processus itératif, si l'emplacement (x, y) est transformé plusieurs fois, il revient à sa position initiale après T itérations. Ce T s'appelle la période de la transformation et dépend des paramètres a, b et k. Ces paramètres peuvent être utilisés comme clés secrètes.

Pour récupérer l'image d'origine, une périodicité est requise. Supposons que l'embrouillage soit effectué après k itérations, de sorte que l'on puisse récupérer l'image d'origine en effectuant des itérations $(T - k)$ [84].

3.3.3. Évolution Différentielle

Un algorithme évolutif simple, rapide et robuste appelé DE a été introduit par Storn et Price [85] en 1995. Il commence par une population initiale NP d'individus $X_{i,G}$, $i = 1, \dots, NP$, de

dimension D, où l'indice i représente la résolution de la population à la génération G. Il existe trois opérations principales de DE qui sont brièvement décrites ci-dessous [84, 86, 87].

- **Mutation**

L'individu cible $X_{i,G}$ peut produire l'individu perturbé $V_{i,G}$. Le processus de mutation commence par la sélection aléatoire de trois individus distincts (X_{r1}, X_{r2}, X_{r3}) parmi la population actuelle qui doit également être différente de l'individu cible $X_{i,G}$ (c'est-à-dire, $r1 \neq r2 \neq r3 \neq i$). Il applique la différence vectorielle entre les individus de la population existante pour déterminer à la fois le degré et la direction de la perturbation. La différence entre deux individus après la mise à l'échelle par un facteur de mise à l'échelle $F \in [0,1]$, ajoutée au troisième individu [84, 86, 87] (eq. 3.16) :

$$V_{i,G} = X_{r1,G} + F \times (X_{r2,G} - X_{r3,G}) \qquad (3.16)$$

où, i varie avec le nombre d'individus.

- **Cross over**

Une opération de Cross Over est effectuée entre un individu perturbé $V_{i,G}$ et un individu cible de population $X_{i,G}$ afin de générer l'individu d'essai $T_{i,G}$. Cette opération dépend d'une probabilité de croisement $C_r \in [0,1]$ qui détermine les composants de l'individu soumis à l'essai. Il dépend de $k \in \{1, \ldots, D\}$ [84, 86, 87]. L'équation mathématique de la génération individuelle d'essai est la suivante (eq. 3.17):

$$t_{j,i,G} = \begin{cases} v_{j,i,G} \; si \; rand_j \leq C_r \; \vee j = k \\ x_{j,i,G} \qquad\qquad ailleurs \end{cases} \qquad (3.17)$$

où, j s'étend sur la dimension du problème.

- **Sélection**

Après la reproduction de l'individu à l'essai, l'aptitude physique est évaluée et comparée à l'individu ciblé correspondant. Cette opération est effectuée par l'opération de sélection qui sélectionne le meilleur individu parmi les individus cibles et à l'essai. Mathématiquement, il est défini par l'équation suivante (eq. 3.18) :

$$X_{i,G+1} = \begin{cases} T_{i,G} \; si \; f(T_{i,G}) \leq f(X_{i,G}) \\ X_{i,G} \qquad\qquad ailleurs \end{cases} \qquad (3.18)$$

Si l'individu à l'essai est meilleur que l'individu ciblé, il remplace l'individu ciblé dans la génération suivante, sinon l'individu ciblé continue. Ainsi, chaque individu de la population temporaire (à l'essai) est comparé à son homologue de la population actuelle [84, 86, 87].

La fonction d'évaluation qui évalue tous les individus selon leur forme utilise la fonction de corrélation normalisée, mathématiquement, est donnée comme suit (eq. 3.19) :

$$Maxf = \frac{\sum_{i=1}^{N} NC(W,W_i^*)}{N} + NC(I,I_w) \quad (3.19)$$

Où I, I_w représentent l'image originale et l'image tatouée respectivement.

Où W, W_i^* représentent la marque originale et la marque extrait après l'attaque respectivement.

N : représente le nombre de types d'attaque.

3.3.4. Masquage de texture

Pour une image I, le masque de texture $T_M(i,j)$ est calculé en utilisant la procédure décrite dans [88] comme suit (eq. 3.20):

$$T_M(i,j) = |I(i,j) - \bar{I}(i,j)| \quad (3.20)$$

$$\bar{I}(i,j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^{L} \sum_{l=-L}^{L} I(i+k, j+l) \quad (3.21)$$

k, l : Des nombres entiers.

Une fenêtre glissante de taille $3 * 3$ est utilisée, $I(i,j)$ est la valeur du pixel, $\bar{I}(i,j)$ c'est la valeur moyenne de bloc à l'emplacement (i,j). $(2L + 1)^2$ Représente le nombre de pixels dans un seul bloc.

Remarque: L'œil humain est moins sensible aux modifications de la surface texturée que de la surface lisse d'une image [89, 90]. Ainsi, une marque avec un facteur de résistance élevé, moyen et faible peut être intégrée respectivement dans les zones à texture élevée, moyenne et petite d'une image.

3.3.5. Système d'inférence floue

Le système d'inférence floue [91] est utilisé pour trouver le facteur de mise à l'échelle adaptatif pour les bandes (LH et HL) en utilisant le masquage de texture (selon l'équation 2.28). Les fonctions utilisées pour le masquage de texture sont illustrées à la Figure (3.2).

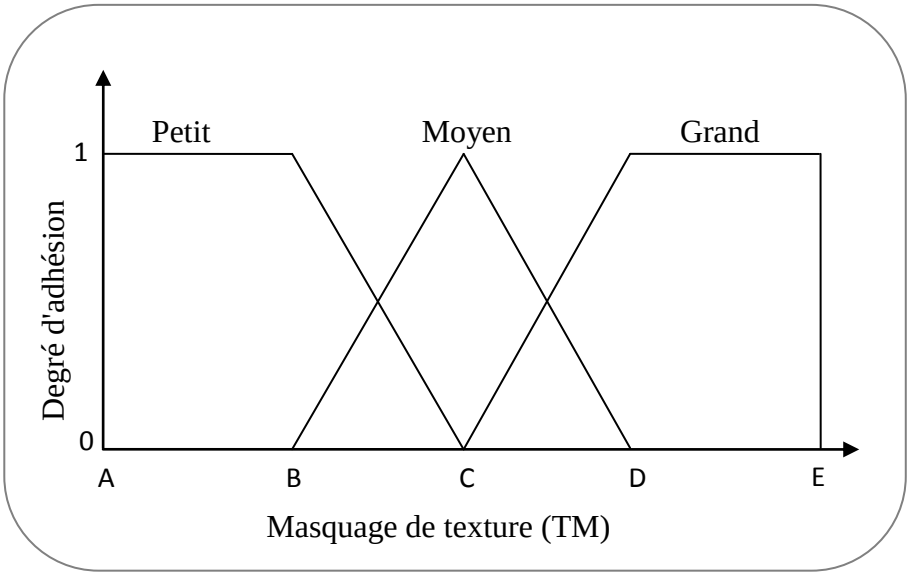


Figure 3. 2 : Fonction d'adhésion pour le masquage de texture.

Les valeurs A; B; C; D et E sont calculées comme suit:

$$A = min_{i=1}^{M} min_{j=1}^{N} T_M(i,j) \quad (3.22)$$

$$C = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} T_M(i,j) \quad (3.23)$$

$$E = max_{i=1}^{M} max_{j=1}^{N} T_M(i,j) \quad (3.24)$$

Les valeurs de B et D sont calculées de manière à ce que la condition suivante soit remplie:

$$C - B = D - C \quad (3.25)$$

Remarque: on Note dans certains cas, la fonction texture de type triangulaire et trapézoïdale est utilisée, mais tout type de fonction d'appartenance peut être utilisé en fonction des besoins. La fonction d'appartenance pour le facteur de résistance adaptative est illustrée à la Figure 3.3.

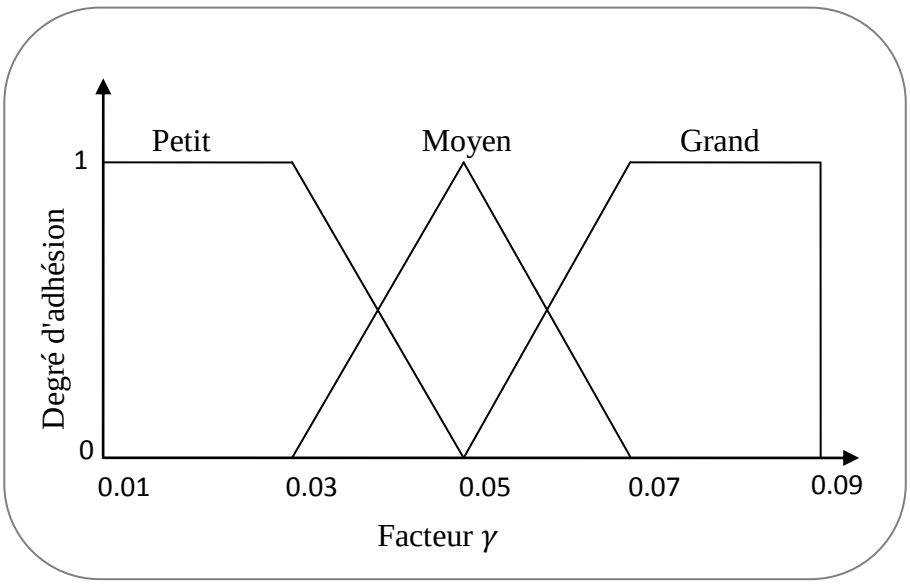


Figure 3. 3 : Courbe de degré d'adhésion en fonction du facteur $\boldsymbol{\gamma}$

Les règles de calcul sont les suivantes: [92].

Règle1: Si T_M est grand; ALORS γ est grand

Règle 2: Si T_M est moyen; ALORS γ est moyen

Règle 3: SI T_M est petit; ALORS est γ petit.

3.4. Outils mathématiques développé

3.4.1. Fonction de mouvement de pixel PMF

La fonction de mouvement de pixels PMF (*Pixel Movement Function*) est implémentée en déplaçant un pixel dans les deux cas; colonnes impaires et lignes impaires de la matrice pour chaque N itération [93].

Le décalage vertical des colonnes impaires (Figure 3.4) est déterminé par l'équation 3.26.

$$y_{i+1}(i,j) = \bar{y}_i(i-1,j) \qquad (3.26)$$

Où $= 1,2,\cdots n$, et j sont les nombres impaires de 1 à n.

Le décalage à gauche des lignes impaires (Figure 3.5) est déterminé par l'équation 3.27.

$$x_{i+1}(i,j) = \bar{x}_i(i,j-1) \qquad (3.27)$$

Où $j = 1,2,\cdots n$, et i sont les nombres impaires de 1 à n.

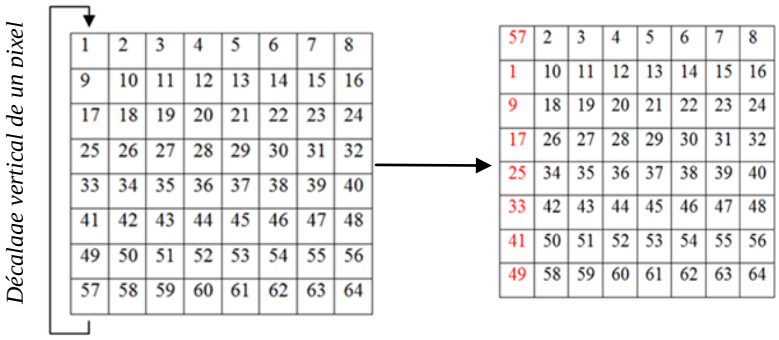


Figure 3. 4 : Le décalage vertical de un pixel pour j=1.

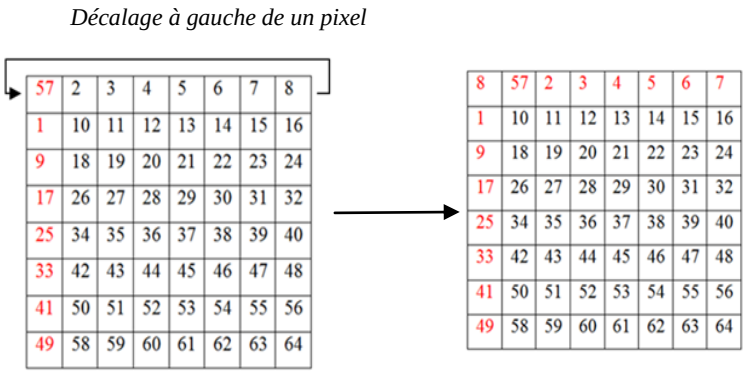


Figure 3. 5 : Le décalage à gauche de un pixel pour i=1.

3.4.2. Fonction de mouvement de pixel inverse IPMF

Cette étape définit l'opération pour revenir à l'état initial en utilisant le décalage opposé sur les lignes et les colonnes impaires, comme indiqué dans les équations (3.28) et (3.29) [93]

$$\bar{x}_{i+1}(i,j) = x_{i+1}(i,j+1) \tag{3.28}$$

Où $i = 1,2,\cdots n$ et j sont les nombres impairs de 1 à n.

$$\bar{y}_{i+1}(i,j) = y_{i+1}(i+1,j) \tag{3.29}$$

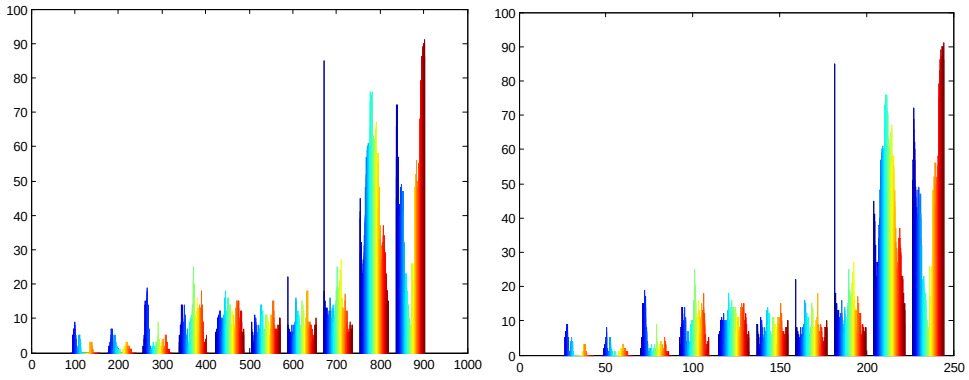
Où $j = 1,2,\cdots n$ et i sont les nombres impairs de 1 à n.

3.4.3. Fonction de transfert TF

La fonction de transfert (TF) est dérivée de la fonction de sensibilité au contraste du système visuel humain (HVS) [94]. La fonction de transfert applique la sous-bande LL1 telle qu'elle est donnée dans l'équation 3.30, le facteur l'exponentielle diminue les valeurs des pixels dans les composants LL1. Pour cette raison, la marque extraite n'est pas vraiment affectée par différentes attaques, ce qui permet d'obtenir de meilleurs résultats pour le tatouage.

$$H = TF(LL1) = a(b + c \times LL1)e^{-(c)^{fe}} \tag{3.30}$$

Où a, b, c sont des nombres réels sélectionnés de manière aléatoire.
Où f_e est un nombre réel positif choisi aléatoirement.



(a) (b)

Figure 3. 6 : (a) L'histogramme de LL1 de l'image Airplane, (b) L'histogramme de LL1 après l'application de TF sur l'image Airplane.

Les histogrammes de la figure 3.6 montrent qu'avant et après l'application du TF, les valeurs en pixels ont été réduites de trois quarts. Dans la partie (a), avant d'appliquer la fonction de transfert, les valeurs de pixels sont définies sur une valeur égale à 900 et avec la fonction de transfert, les valeurs de pixels sont ramenées à 250, comme indiqué en (b). Ceci est pour protéger les informations et renforcer la robustesse contre les attaques.

3.5. Conclusion

Les outils mathématiques nécessaires pour le traitement de l'image ont été présentés dans ce chapitre. Les transformées fréquentielles comme la DCT, DWT, DFT et la DHT offrent la possibilité pour l'incorporation de la marque en effectuant une modification des coefficients de la transformée de l'image en fonction des coefficients de la marque. Ces techniques permettent de consolider et améliorer la robustesse et l'imperceptibilité de l'image. Nous avons implanté une nouvelle fonction du mouvement des pixels basé sur le déplacement des lignes et des colonnes impaires de l'image.

Dans le chapitre suivant, nous allons exploiter ces outils mathématiques pour améliorer les performances des algorithmes de tatouage existant.

CHAPITRE 4: IMPLANTATION DES ALGORITHMES DE TATOUAGE DÉVELOPPÉS

4.1. Introduction

Dans ce chapitre, Nous présenterons de nouveaux algorithmes de tatouage d'image. Nous allons exploiter les avantages de la DWT pour développer de nouvelles approches. En effet, la DWT permet de séparer les caractéristiques de l'image en termes de luminance, les quatre sous-bandes contiennent des informations globales sur les couleurs de l'image et les détails de l'image. Ces avantages nous ont permis de développer nos algorithmes de tatouage de l'image où nous avons introduit des techniques mathématiques pour augmenter la sécurité et l'efficacité de l'algorithme.

4.2. Première approche ; tatouage basé sur la SVD et la compression JPEG2000

Dans cette partie nous allons présenter une nouvelle approche d'un algorithme de tatouage de l'image basé sur la technique de compression JPEG2000 [95] qui a l'avantage de réduire la redondance des pixels en gardant la bonne qualité de l'image. L'idée de l'algorithme de la nouvelle approche consiste à modifier le schéma de JPEG2000 standard où la marque est insérée dans les sous-bandes LL3, HL3 du bloc de la DWT, plus exactement dans les valeurs singulières des matrices résultantes de l'application de la SVD sur les dites sous-bandes. Pour augmenter l'impact de la sécurité, l'algorithme de sécurisation de l'évolution différentiel DE est appliqué. L'approche présentée dans le cadre des schémas non aveugles dont l'image hôte est nécessaire pour l'extraction de la marque et dont l'algorithme d'extraction applique la technique SVD sur les sous-bandes des deux images, ensuite une fonction de sommation qui permet l'extraction de la marque.

Pour confirmer l'efficacité de l'algorithme, nous avons appliqué les métriques d'évaluation de performance telles que le NC (*Normalized Correlation*) et le PSNR (*Peak signal to noise ratio*). Les résultats obtenus montrent que cet algorithme correspond aux exigences demandées pour un système de tatouage efficace. Par la suite nous allons détailler l'approche proposée.

4.2.1. Principe d'insertion

1- Lire l'image originale et la marque à insérer.
2- Appliquer la phase de sous-échantillonnage sur l'image originale.
3- Appliquer la DWT sur l'image originale et obtenir les sous-bandes suivantes{ $LL3$, $HL3, LH3, HH3, HL2, LH2, HH2, HL1, LH1, HH1$}.
4- Sélectionner les deux sous-bandes { $LL3, HL3$}.
5- Appliquer la SVD sur les sous-bandes sélectionnées de la transformée DWT, pour décomposer chaque sous-bande en trois matrices U, S et V.
6- Appliquer la SVD sur la marque pour obtenir les trois composantes U_w, S_w et V_w.
7- Calculer les valeurs de la matrice de la clé par l'algorithme DE.
8- Insérer la composante S_w dans les deux composantes S_1 et S_2 des deux sous-bandes {$LL3, HL3$}.
9- Appliquer la SVD inverse sur les deux sous-bandes précédentes.
10- Appliquer la DWT inverse (IDWT) pour obtenir l'image tatouée.
11- Appliquer les étages de quantification et le codage entropique sur l'image tatouée pour obtenir l'image tatouée compressée.

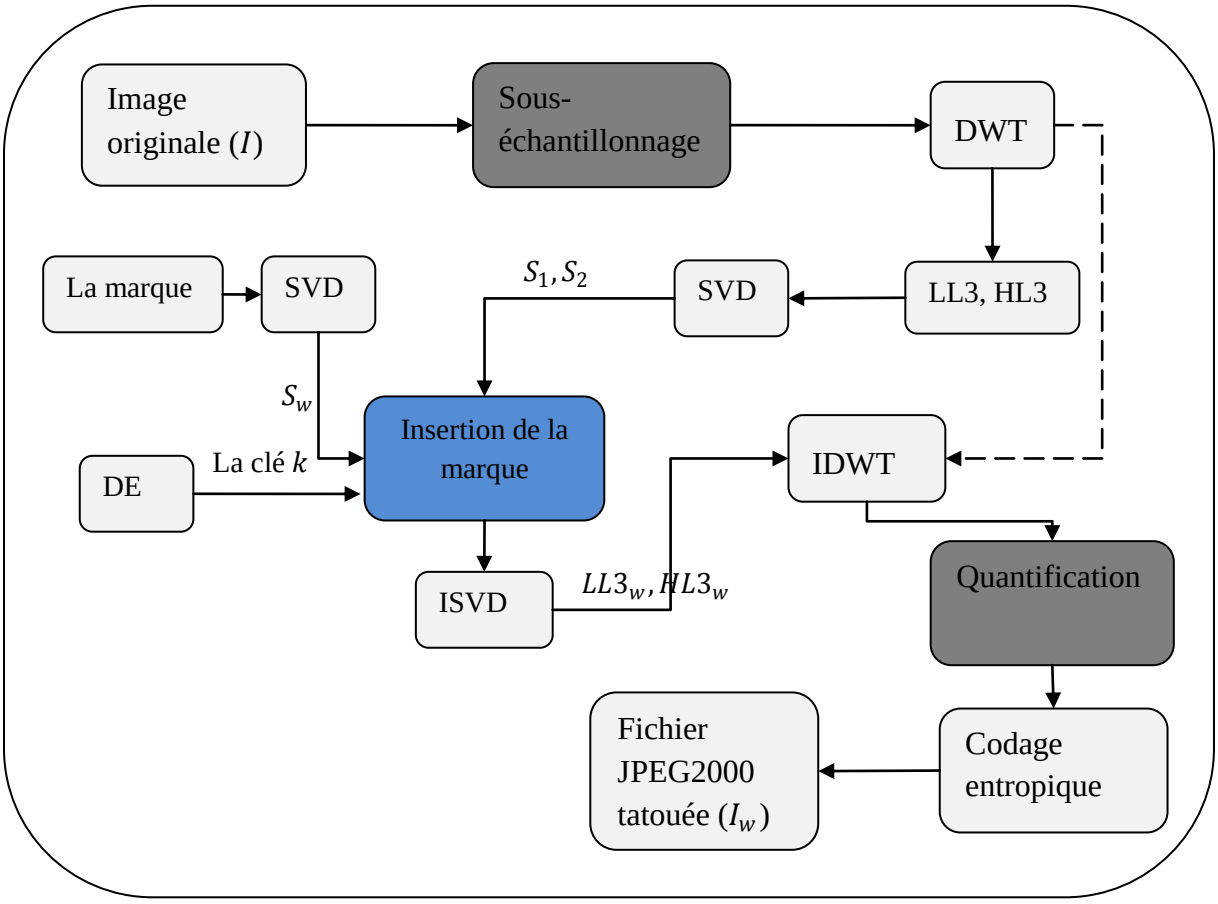


Figure 4. 1: Algorithme d'insertion de la marque.

4.2.2. Principe d'extraction

1- Lire l'image originale et l'image tatouée.
2- Appliquer la phase de sous-échantillonnage sur les deux images.
3- Appliquer la DWT sur les deux images.
4- Sélectionner les sous-bandes $\{ LL3, HL3, LL3_w, HL3_w \}$.
5- Appliquer la SVD sur les sous-bandes sélectionnées de la transformée DWT, pour décomposer chaque sous-bande en trois matrices U, S et V.
6- Calculer les valeurs de la matrice de la clé par l'algorithme DE.
7- Extraire la marque depuis ses sous-bandes par le biais de la clé k et les composantes $\{U_w, V_w\}$.

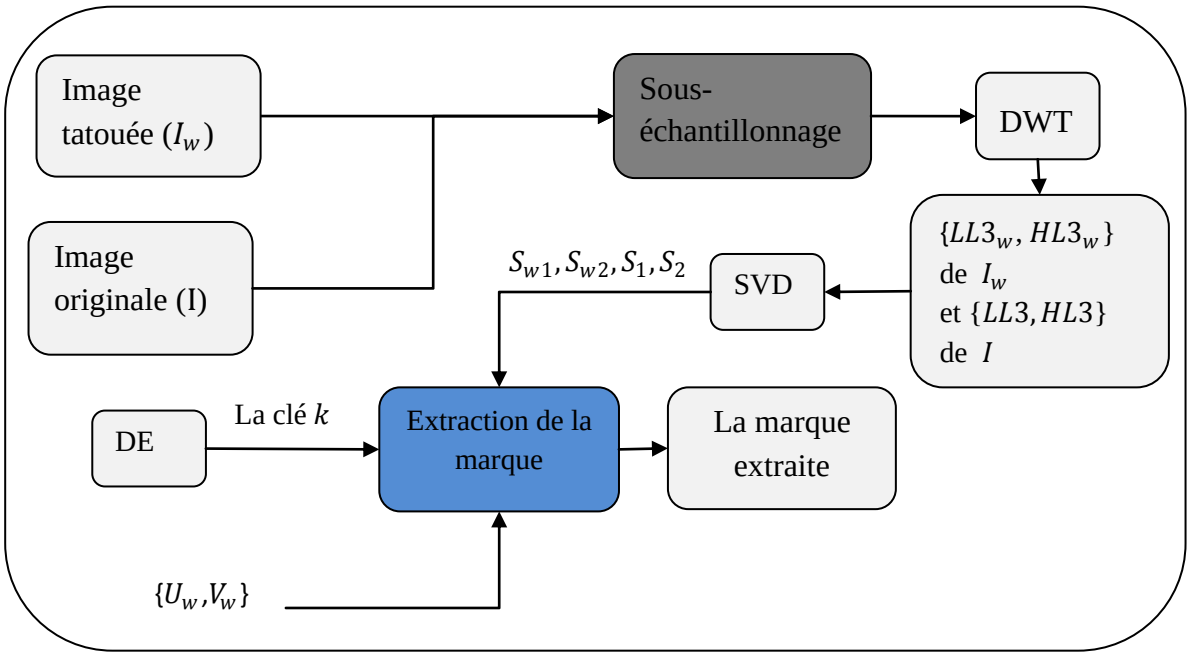


Figure 4. 2: Algorithme d'extraction de la marque

4.3. Deuxième approche : tatouage basé sur la DWT et la SVD

Dans une deuxième approche nous avons développé un nouvel algorithme hybride basé sur la DWT et la SVD [96]. La transformée DWT permet d'extraire les sous-bandes de l'image hôte, alors que la SVD décompose les sous-bandes LL3 et HL3 afin d'insérer la marque dans les composantes singulières. Cette approche est testée avec plusieurs images contre plusieurs attaques, les résultats trouvés surtout en termes de robustesse et d'imperceptibilité démontrent la fidélité de cette méthode.

4.3.1. Principe d'insertion

1- Lire l'image originale et la marque à insérer.
2- Appliquer la DWT sur l'image originale et obtenir les sous-bandes suivantes{ $LL3$, $HL3, LH3, HH3, HL2, LH2, HH2, HL1, LH1, HH1$}.
3- Sélectionner les deux sous-bandes { $HL3, HH3$}.
4- Appliquer la SVD sur les sous-bandes sélectionnés de la transformée DWT, pour décomposer chaque sous-bande en trois matrices U, S et V.
5- Appliquer la SVD sur la marque pour obtenir les trois composantes U_w, S_w et V_w.
6- Calculer la valeur de clé γ à partir de l'algorithme de HVS.
7- Insérer la composante S_w dans les deux composantes S_1 *et* S_2 des deux sous-bandes $\{HL3, HH3\}$ à l'aide de deux clés ; la clé γ et la clé α (où α est un nombre réel positif).
8- Appliquer la SVD inverse sur les deux sous-bandes $\{HL3_w, HH3_w\}$.
9- Appliquer la DWT inverse (IDWT) pour obtenir l'image tatouée.

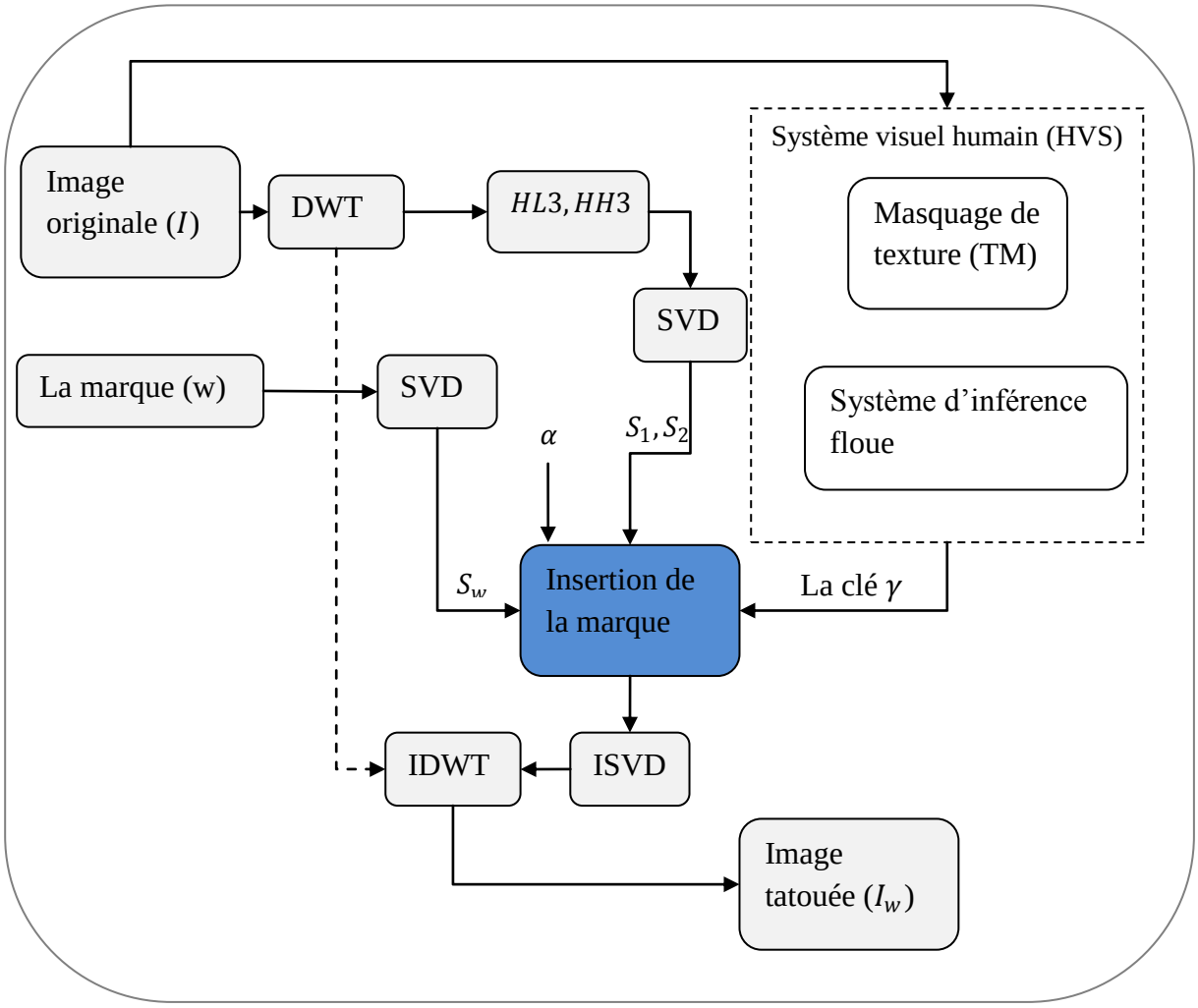


Figure 4. 3: Algorithme d'insertion de la marque

4.3.2. Principe d'extraction

1- Lire l'image originale et l'image tatouée.
2- Appliquer la DWT sur les deux images.
3- Sélectionner les sous-bandes { $HL3, HH3, HL3_w, HH3_w$ }.
4- Appliquer la SVD sur les sous-bandes sélectionnées de la transformée DWT, pour décomposer chaque sous-bande en trois matrices U, S et V.
5- calculer la valeur de la clé γ par l'algorithme de HVS.
6- Extraire la marque depuis les sous-bandes { $HL3, HH3, HL3_w, HH3_w$ } par le biais de la clé γ.

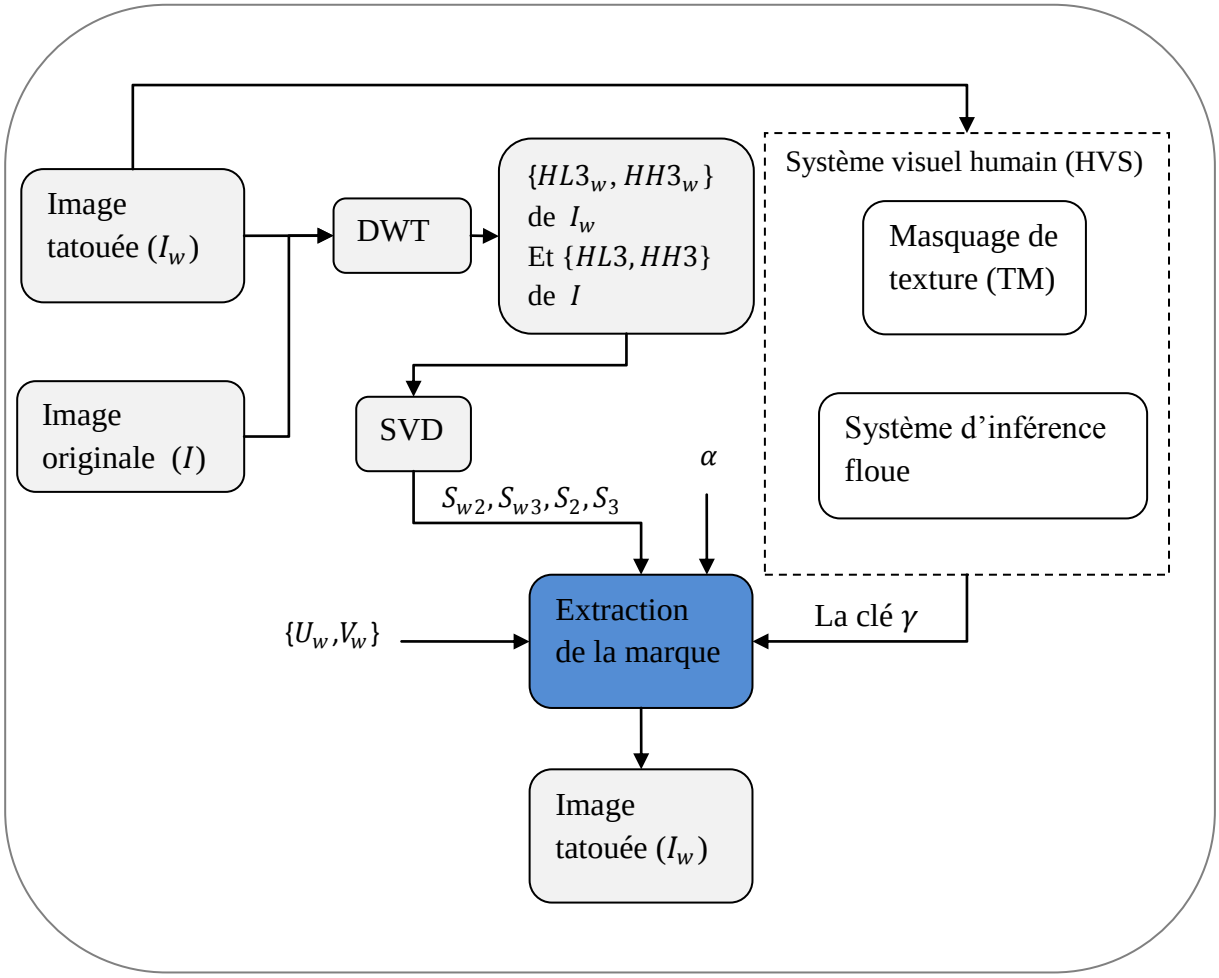


Figure 4. 4: Algorithme d'extraction de la marque.

4.4. Troisième Approche : tatouage basé sur la DWT

Dans une troisième approche [93], nous proposons un nouveau schéma de tatouage d'image basé sur la transformation en ondelettes discrètes (DWT) comprenant une fonction de déplacement des pixels. L'algorithme proposé utilise une DWT à deux niveaux afin de compacter un niveau d'énergie plus élevé dans la composante LL1. Le principe de cette

méthode est de changer le site des pixels dans les blocs de l'image originale pour assurer la sécurité, afin que les personnes non autorisées ne puissent pas extraire la marque. D'autant plus, l'ajout de la fonction de transfert et de la fonction de sensibilité au contraste (CSF) permet d'évaluer la dégradation de l'image après l'insertion de la marque, et donc adopter le meilleur moyen pour renforcer l'algorithme contre diverses attaques. Une nouvelle fonction de mouvement de pixels (PMF) développée est appliquée. La fonction de mouvement de pixels (PMF) permet de changer l'emplacement de pixels. Cette fonction nécessite une clé modifiable k calculée pour chaque position de bloc. Des expériences ont été effectuées pour démontrer que la méthode proposée apporte une amélioration sur la qualité du tatouage en termes d'imperceptibilité de la marque, de capacité d'insertion et de robustesse contre les différentes attaques telles que la compression JPEG, l'addition de bruit et les attaques géométriques.

4.4.1. Principe d'insertion

1- Lire l'image originale et la marque à insérer.
2- Appliquer la DWT sur l'image originale.
3- Sélectionner la sous-bande $\{ LL1\}$.
4- Appliquer la fonction de transfert TF sur la sous-bande $\{LL1\}$.
5- Diviser la sous-bande résultante en blocs de (8×8).
6- Diviser la marque en blocs de 20 pixels.
7- Calculer et organiser les moyennes de chaque bloc de la marque dans un vecteur M.
8- Convertir les éléments décimaux du vecteur M en nombres binaires.
9- Compter le nombre de bits égaux à 1 dans chaque nombre binaire et sélectionner l'emplacement du bit 1 avant le bit MSB. Cet emplacement correspond au nombre d'itérations N.
10- Appliquer la PMF sur les blocs de la sous-bande $LL1$ pour N itérations (chaque bloc a un nombre d'itérations N différent des autres).
11- Insérer la marque dans la position principale de chaque bloc de la composante $LL1$ par une clé k, cette clé est calculée à partir de la racine de N et de la position de chaque bloc.
12- Appliquer le $IPMF$ sur les blocs de la sous-bande résultante pour N itérations.
13- Appliquer la fonction de transfert inverse ITF sur la sous-bande précédente.
14- Appliquer la DWT inverse (IDWT) pour obtenir l'image tatouée.

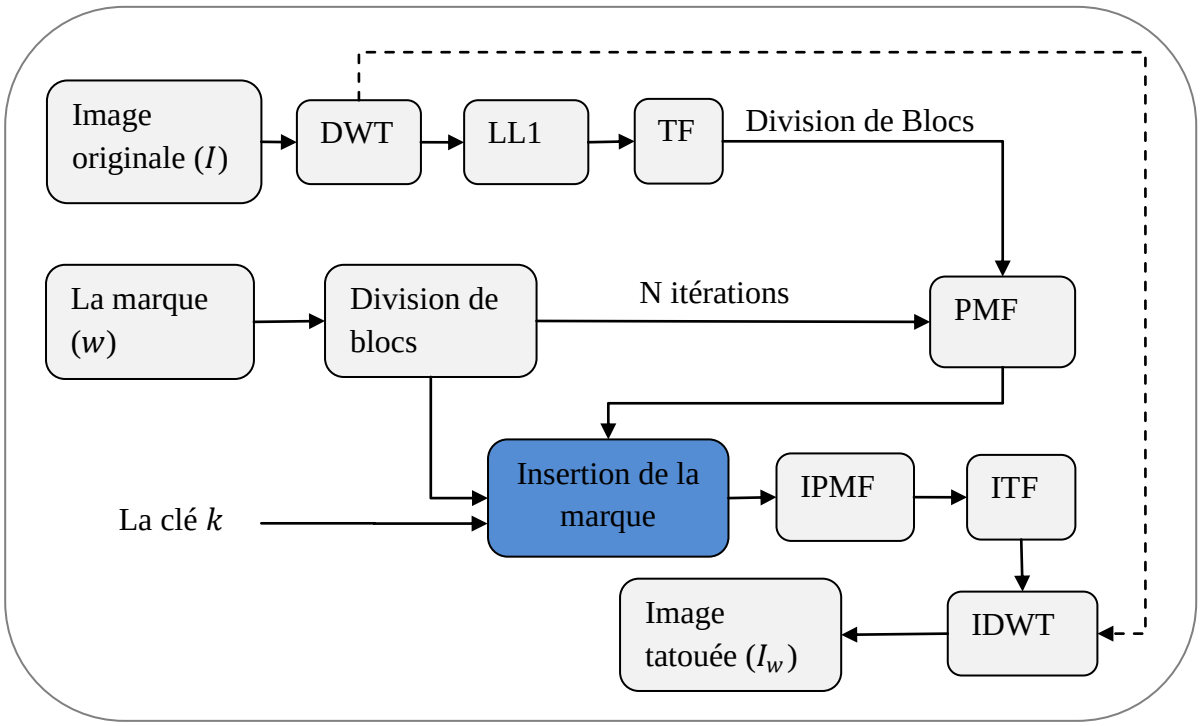


Figure 4. 5: Algorithme d'insertion de la marque

4.4.2. Principe d'extraction

1- Lire l'image originale et l'image tatouée.
2- Appliquer la DWT sur les deux images.
3- Sélectionner les sous-bandes $\{ LL1, LL1_w \}$.
4- Appliquer la fonction de transfert TF sur les sous-bandes $\{LL1, LL1_w\}$.
5- Diviser les deux sous-bandes résultantes sur des blocs de (8× 8).
6- Appliquer le PMF sur les blocs des sous-bandes $\{LL1, LL1_w\}$ pour N itérations.
7- Extraire la marque par le biais d'une clé k.

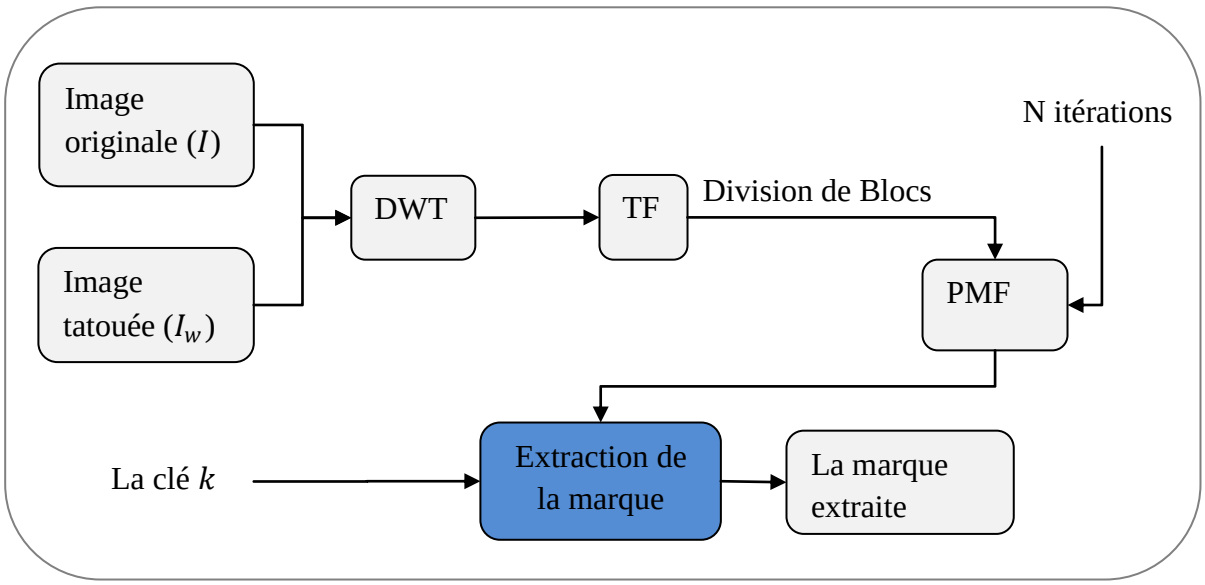


Figure 4. 6: Algorithme d'extraction de la marque.

4.5. Conclusion

Ce chapitre a été dédié à la présentation de trois nouveaux algorithmes de tatouage de l'image. L'idée de ces algorithmes consiste à ajouter des améliorations aux algorithmes existants. Dans la première approche, l'algorithme standard de JPEG2000 à été adapté pour qu'il soit un algorithme de tatouage, où la SVD est utilisée pour insérer la marque. La deuxième et la troisième approche sont basées sur la transformée DWT, où la technique SVD est utilisée pour insérer la marque dans la deuxième approche. Pour la troisième approche, une fonction de mouvement des pixels dite PMF est employée pour augmenter la sécurité de l'algorithme. Pour vérifier la fidélité des approches présentées, les algorithmes seront testés avec plusieurs images. Le chapitre suivant, récapitule les résultats de simulation.

CHAPITRE 5 : RÉSULTATS DE SIMULATION ET DISCUSSION

5.1. Introduction

Les algorithmes de tatouage récents sont basées sur des méthodes hybrides où les transformées classiques sont combinées avec des techniques mathématiques dont le but est d'améliorer considérablement l'efficacité de l'algorithme. Ce chapitre sera consacré à l'implantation pratique de trois nouveaux algorithmes que nous avons développés durant cette étude. Ces nouveaux algorithmes sont basés sur des améliorations attribuées aux algorithmes de tatouage classiques telles que la DWT et la technique de compression JPEG2000. Ces nouveaux algorithmes seront testés face à des attaques malveillantes et non-malveillantes, afin de vérifier la fidélité et la robustesse de ceux-ci. En effet, il s'agit de l'attaque de bruit additif, filtrage, compression et attaque géométrique pour évaluer l'efficacité mathématique de l'algorithme. Des métriques d'auto-corrélation normalisées (NC) et de rapport signal sur bruit (PSNR) seront calculées après chaque opération d'extraction de la marque, ces métriques de performance mesurent la ressemblance entre la marque extraite et celle insérée. Des mesures élevées du facteur d'auto-corrélation démontrent que l'algorithme de tatouage est efficace.

5.2. Première approche ; tatouage basé sur la SVD et la compression JPEG2000

L'algorithme de tatouage de l'image basé sur la technique de compression JPEG2000 est testé dans ce paragraphe. Le détail de cet algorithme est déjà présenté dans le paragraphe 4.2 du chapitre précédent. Pour tester la fidélité de la méthode présentée nous allons utiliser quatre images de taille 512×512 pixels comme celle de Lena, Airplane, Aepper et Sailboat, la marque est de taille 64×64 pixels.

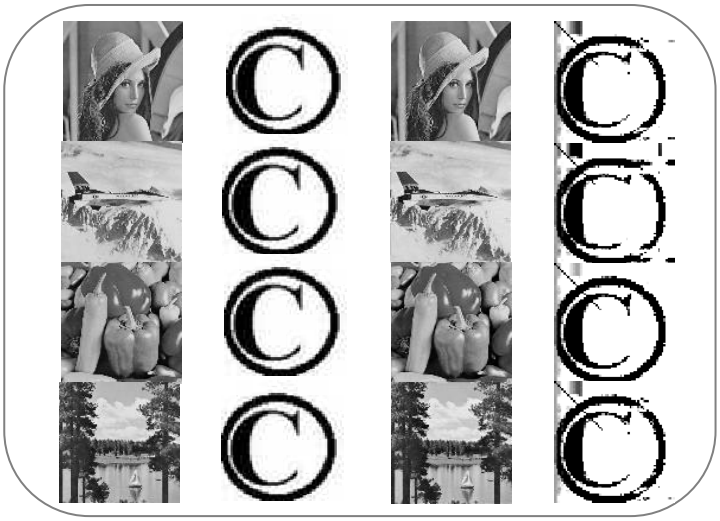


Figure 5. 1: Simulation de l'algorithme de tatouage proposé par les images de tests suivants: Lena (37.2951dB, 0.9431) airplane (38.0320 dB, 0.9418); Pepper (37.4100 dB, 0.9396); et Sailboat (36.8558 dB, 0.9409).

La figure 5.1 montre les résultats de simulation pour les quatre images de test. Nous pouvons examiner la similarité entre la marque insérée et la marque extraite. Le facteur d'auto-corrélation est supérieur à 0.9 pour toutes les images. La mesure de l'invisibilité de la marque dans l'image tatouée par le calcul de PSNR donne une bonne qualité de l'image tatouée pour les quatre images avec une valeur supérieure à 36 décibels.

5.2.1. Addition de bruit

- ***bruit de sel et poivre***

Nous allons attaquer l'image par un bruit non-intentionnelle appelé sel et poivre, avec une variance de 0,1%. Les résultats de simulation obtenus sont illustrés sur la figure 5.2. Nous remarquons que la marque extraite est toujours semblable à la marque insérée. Le facteur d'auto-corrélation normalisé est supérieur à 0.93 avec un PSNR supérieur à 36 dB. On peut conclure que l'algorithme est solide face à cette attaque.

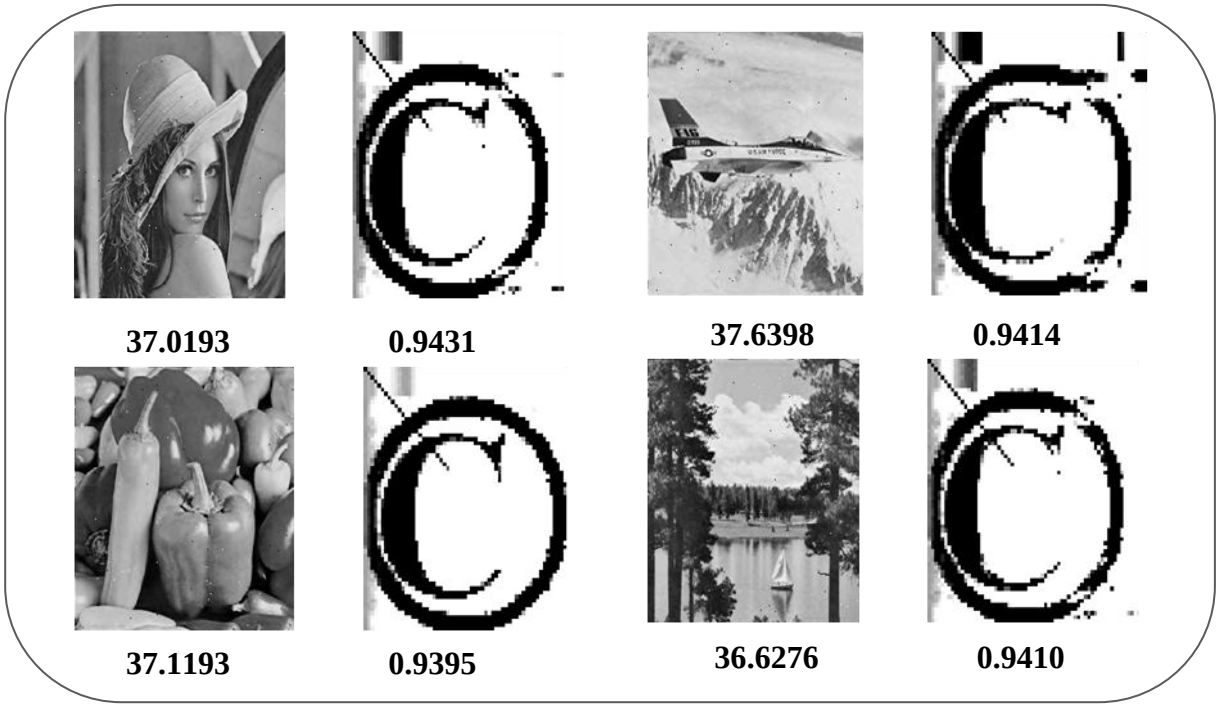


Figure 5. 2 : Résultats de simulation d'algorithme de tatouage proposé contre l'attaque de bruit sel et poivre de variance 0.1%.

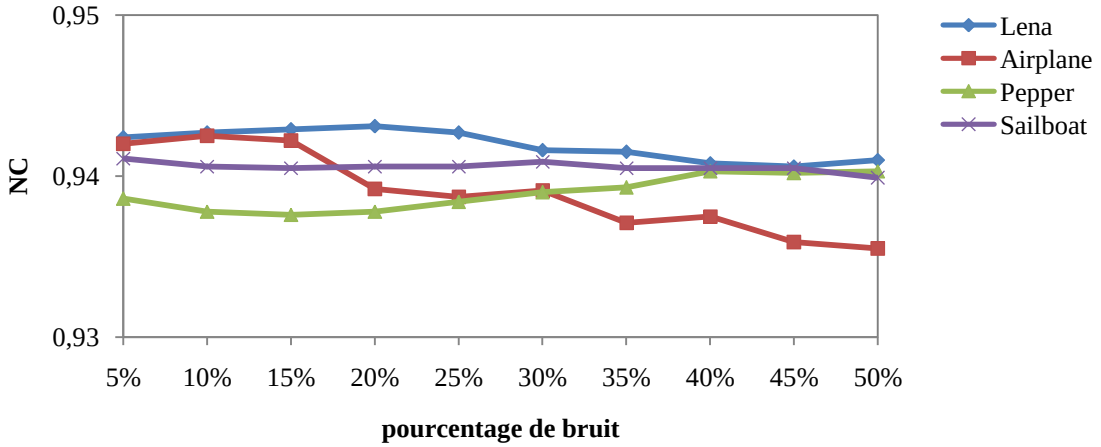


Figure 5. 3 : Robustesse de l'algorithme de tatouage contre le bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat.

Les résultats de NC après l'application de bruit sel et poivre jusqu'à la valeur de 50% exprime la robustesse de l'algorithme contre ce type d'attaque avec un NC toujours supérieur à 0.93 (Figure 5.3), pour la figure 5.4 les valeurs de PSNR diminuent a cause de l'augmentation du bruit.

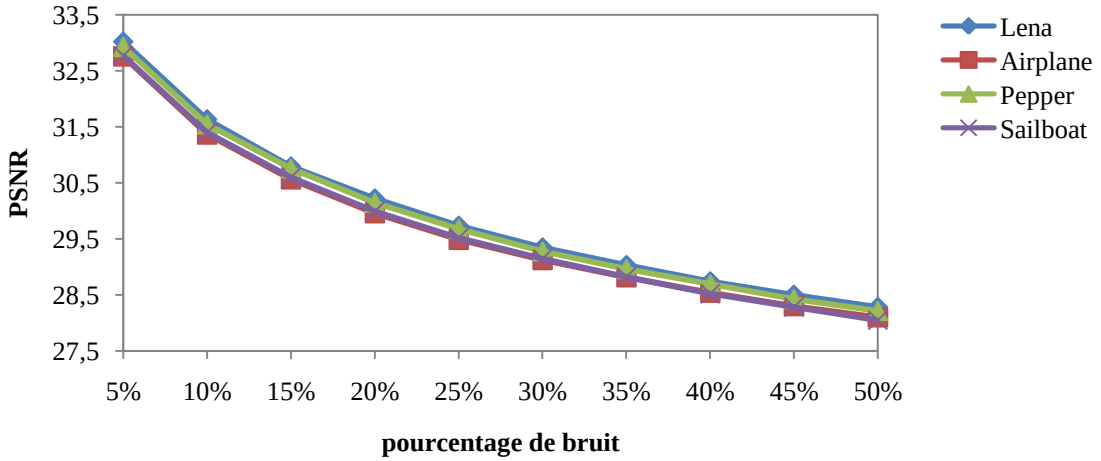


Figure 5. 4 : Variation de PSNR pour différentes valeurs de l'attaque de bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat.

- ***Bruit Gaussien***

Le Bruit gaussien est une perturbation dont la densité de probabilité du variable qui décrit le bruit suit une loi gaussienne (ou loi normale) il est ajouté à l'image tatouée pour affecté la résolution de la marque extraite. Le bruit Gaussien est une attaque avec une influence remarquable sur la marque extraite, nous avons appliqué un bruit Gaussien avec une variance de 0.1% et on trouve le NC supérieur à 0.93, ainsi l'image extraite garde une bonne qualité (Figure 5.5).

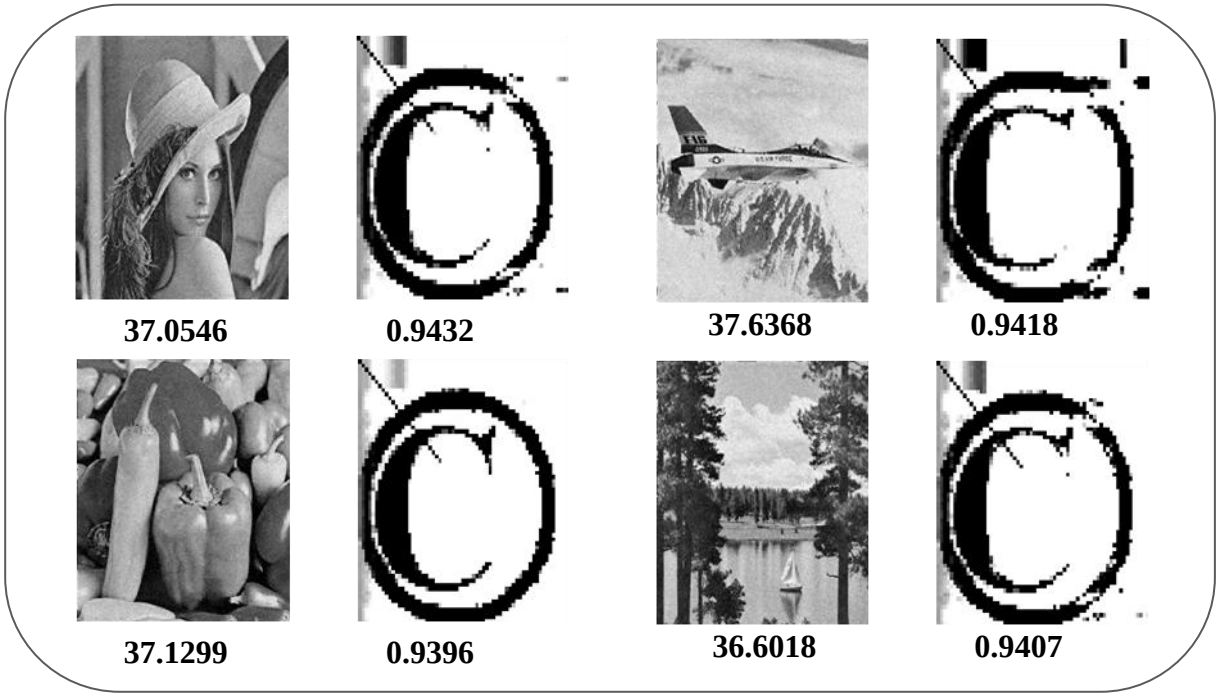


Figure 5. 5 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de bruit Gaussien de variance 0.1%.

Le tableau 5.1 présente les valeurs de NC et PSNR en fonction de la densité de bruit Gaussien, on remarque que le système est robuste avec un NC supérieur à 0.93 et un rapport de PSNR qui diminue si on augmente la variance du bruit.

Bruit Gaussien (%)	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
5%	0.9416	30.9258	0.9415	31.3066	0.9375	30.9897	0.9402	31.1880
10%	0.9411	29.8217	0.9400	30.1487	0.9367	29.8783	0.9408	30.0551
15%	0.9411	29.2688	0.9396	29.5373	0.9373	29.3036	0.9410	29.4544
20%	0.9411	28.9137	0.9365	29.1436	0.9391	28.9458	0.9412	29.0565
25%	0.9408	28.6815	0.9382	28.8735	0.9393	28.6965	0.9405	28.7869
30%	0.9411	28.4931	0.9370	28.6672	0.9403	28.5116	0.9411	28.5744
35%	0.9411	28.3578	0.9361	28.5098	0.9399	28.3606	0.9400	28.4051
40%	0.9407	28.2419	0.9359	28.3842	0.9402	28.2428	0.9411	28.2705
45%	0.9400	28.1568	0.9359	28.2857	0.9402	28.1537	0.9405	28.1669
50%	0.9404	28.0761	0.9360	28.1902	0.9409	28.0643	0.9400	28.0720

Tableau 5. 1 : Les Valeurs de NC et de PSNR après l'attaque de bruit gaussien.

5.2.2. Attaque de filtrage

- ***Filtre médian***

Le filtre médian parmi les attaques non malveillantes qui permet de supprimer la marque.

Il s'agit d'une matrice 3 × 3 pixels, ce filtre glisse sur tous les pixels de l'image. La figure 5.6 illustre la marque extraite d'une image tatouée et attaquée par un filtre médian. L'image extraite présente une très bonne qualité visuelle. Le facteur NC est supérieur à 0.93 ce qui montre la robustesse de l'algorithme.

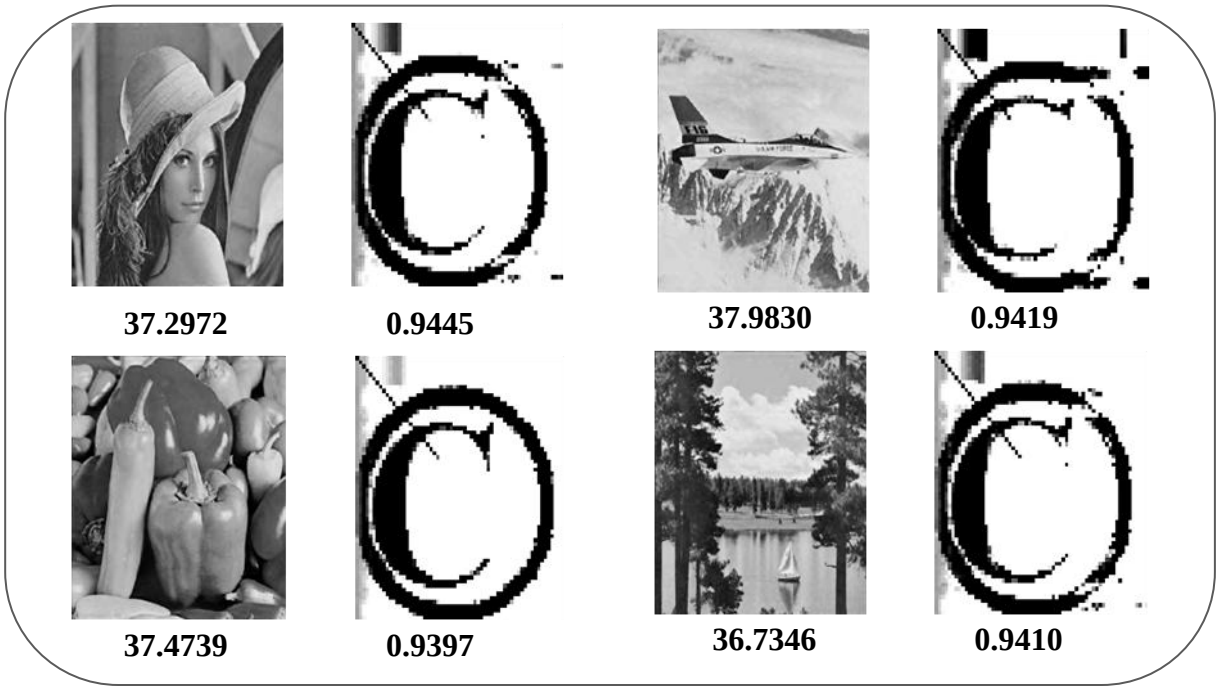


Figure 5. 6 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de Filtre Médian de taille **3 × 3** pixels.

Le tableau 5.2 montre la robustesse de l'algorithme contre l'attaque de Filtre médian avec un NC supérieur à 0.94 jusqu'à la taille 13 × 13 pixels de filtre médian, et la diminution du PSNR jusqu'à 34 décibels, cela pour quatre images de test.

Filtre Médian	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
3 × 3	0.9445	37.2972	0.9419	37.9830	0.9397	37.4739	0.9410	36.7346
5 × 5	0.9449	37.1108	0.9419	37.4765	0.9404	37.4046	0.9424	36.2130
7 × 7	0.9467	36.8123	0.9424	36.8324	0.9407	37.2207	0.9449	35.6093
9 × 9	0.9477	36.5330	0.9427	36.2478	0.9419	36.9688	0.9465	35.1134
11 × 11	0.9479	36.2794	0.9406	35.7274	0.9433	36.6614	0.9474	34.7042
13 × 13	0.9493	36.0254	0.9403	35.3036	0.9438	36.3203	0.9498	34.3644

Tableau 5. 2 : Les Valeurs de NC et de PSNR après l'attaque du filtre médian.

- ***Filtre moyenneur***

Le filtre moyenneur est un filtre passe-bas où pour chaque pixel de l'image il permet de calculer la valeur moyenne des pixels en fonction des pixels de l'environnement. Une matrice 3 × 3 est glissée sur tous les pixels de l'image dont le résultat est une image filtrée. Ce filtre a un impact sur l'image tatouée en supprimant la marque. La figure 5.7 montre les résultats de

simulation d'une image tatouée par l'algorithme proposé et attaqué par un filtre moyenneur. L'auto-corrélation normalisée NC est supérieur à 0.94, le PSNR enregistre une valeur supérieure à 36 dB pour toutes les images de test.

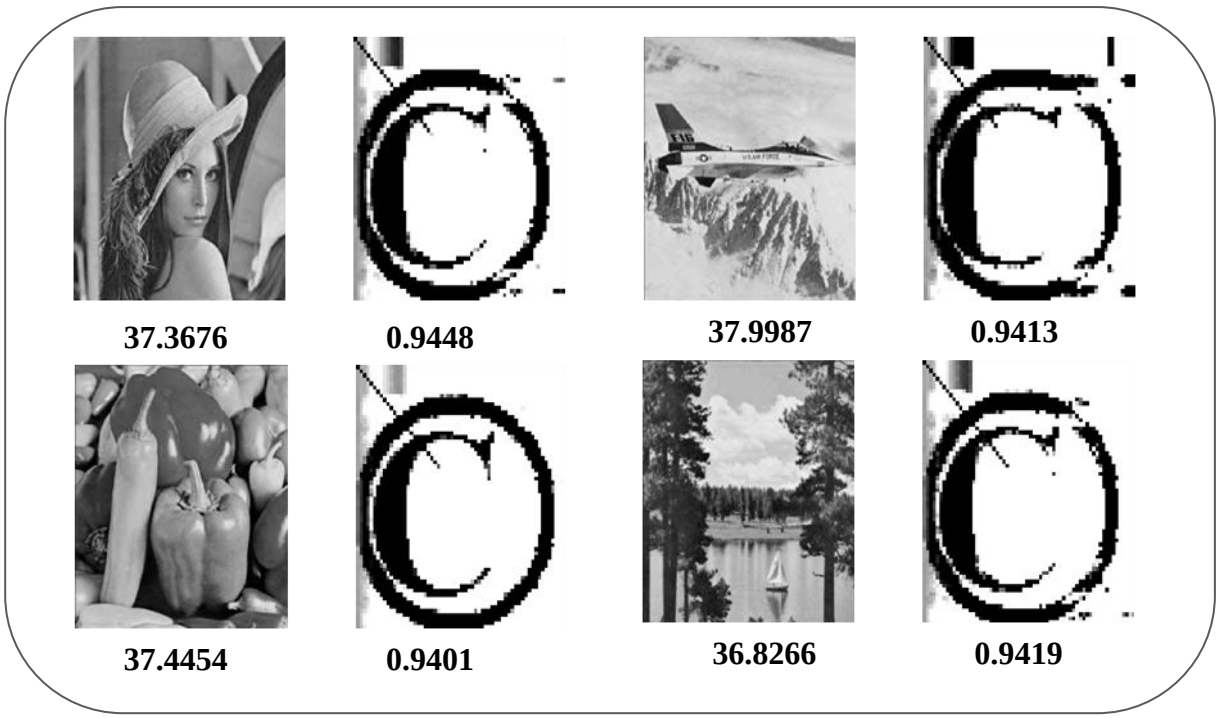


Figure 5. 7 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre moyenneur de taille **3 × 3** pixels.

Le Tableau 5.3 récapitule les résultats des paramètres NC et PSNR en fonction de la taille du filtre moyen jusqu'à la taille 13*13 pixels, les valeurs de NC obtenues sont supérieures à 0.93 ce qui confirme la robustesse de l'algorithme, avec une modeste décroissance du PSNR.

Taille de filtre moyen	**Lena**		**Airplane**		**Pepper**		**Sailboat**	
	NC	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**	**NC**	**PSNR**
3 × 3	0.9448	37.3676	0.9413	37.9987	0.9401	37.4454	0.9419	36.8266
5 × 5	0.9465	37.0756	0.9411	37.2344	0.9410	37.1705	0.9446	36.2280
7 × 7	0.9478	36.7112	0.9433	36.7922	0.9433	36.7922	0.9467	35.6107
9 × 9	0.9491	36.3898	0.9393	35.8609	0.9449	36.4136	0.9499	35.1273
11 × 11	0.9514	36.1037	0.9384	35.4003	0.9471	36.0515	0.9511	34.7426
13 × 13	0.9531	35.8439	0.9369	35.0415	0.9477	35.7214	0.9527	34.4268

Tableau 5. 3 : Les valeurs de NC et de PSNR après l'attaque de filtre moyen.

- ***Filtre Gaussien***

Le filtre de Gauss est un filtre où la procédure de filtration s'effectue par une convolution entre une fonction Gaussienne et le signal entrant. Nous avons examiné l'algorithme contre l'attaque de filtre gaussien de taille 3 × 3 pixels; Nous avons remarqué pour les quatre

images de test que la valeur de NC était supérieure à 0.94 avec une bonne qualité de la marque extraite (Figures 5.8).

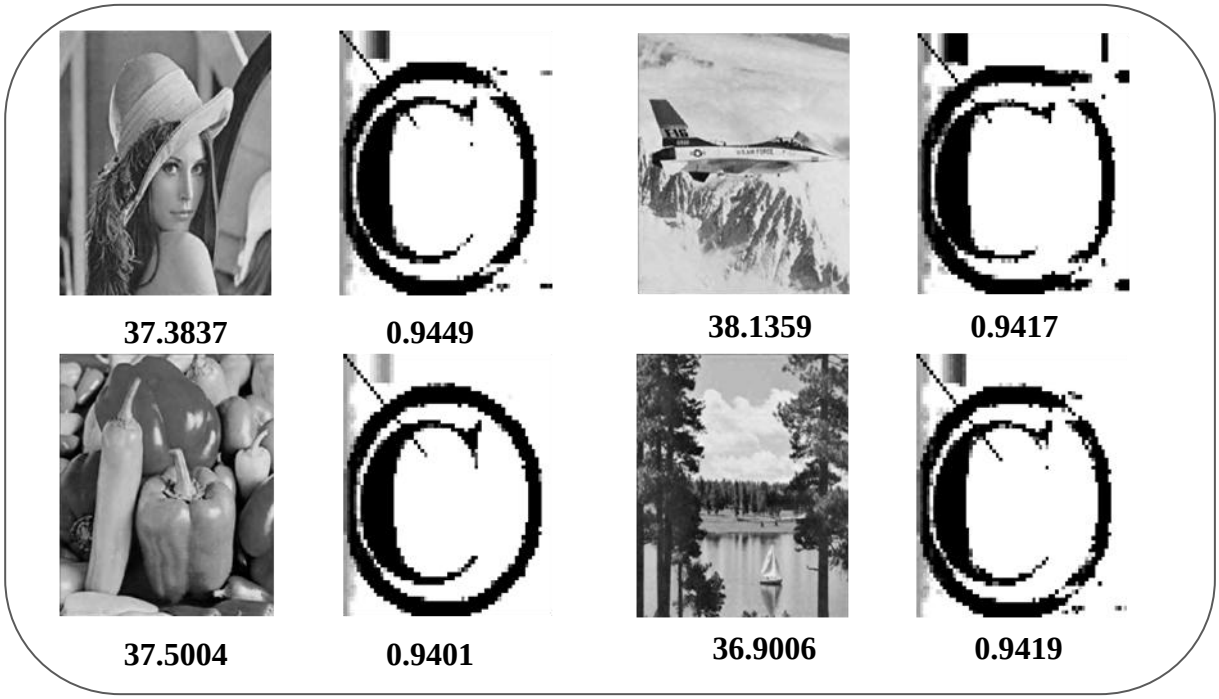


Figure 5. 8 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Gaussien de taille **3 × 3** pixels.

Pour vérifier la robustesse de l'algorithme présenté, nous l'avons testé contre un filtrage Gaussien dont la taille du filtre s'agrandit jusqu'à 13×13 pixels. Les résultats de NC et du PSNR sont regroupés dans le tableau 5.4. Le facteur d'auto-corrélation est supérieur à 0.94 avec un PSNR supérieur à 36 dB. Les résultats obtenus montrent l'efficacité de l'algorithme contre le filtre Gaussien.

Taille de filtre Gaussien	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
3×3	0.9449	37.3837	0.9417	38.1359	0.9401	37.5004	0.9419	36.9006
5×5	0.9447	37.3517	0.9408	38.0114	0.9404	37.4762	0.9424	36.7988
7×7	0.9448	37.3488	0.9410	37.9991	0.9405	37.4751	0.9426	36.7881
9×9	0.9449	37.3488	0.9410	37.9990	0.9405	37.4752	0.9426	36.7880
11×11	0.9449	37.3488	0.9410	37.9990	0.9405	37.4752	0.9426	36.7880
13×13	0.9449	37.3488	0.9410	37.9990	0.9405	37.4752	0.9426	36.7880

Tableau 5. 4 : Les valeurs de NC et de PSNR après l'attaque de filtre gaussien.

- ***Filtre Sharpen***

La technique de filtre Sharpen utilise une image négative floue pour créer un masque de l'image originale. Ce masque flou est ensuite combiné avec l'image originale en créant une image moins floue que l'originale. Ce filtre permet d'amplifier les composantes hautes

fréquences d'un signal. La figure 5.9 représente les résultats de simulation dont les images tatouées par l'algorithme proposé ayant subit un filtrage de Sharpen de valeur 0.8. L'auto-corrélation NC est supérieure à 0.93 pour tout les images de test, la marque extraite est lisible mais avec une distorsion.

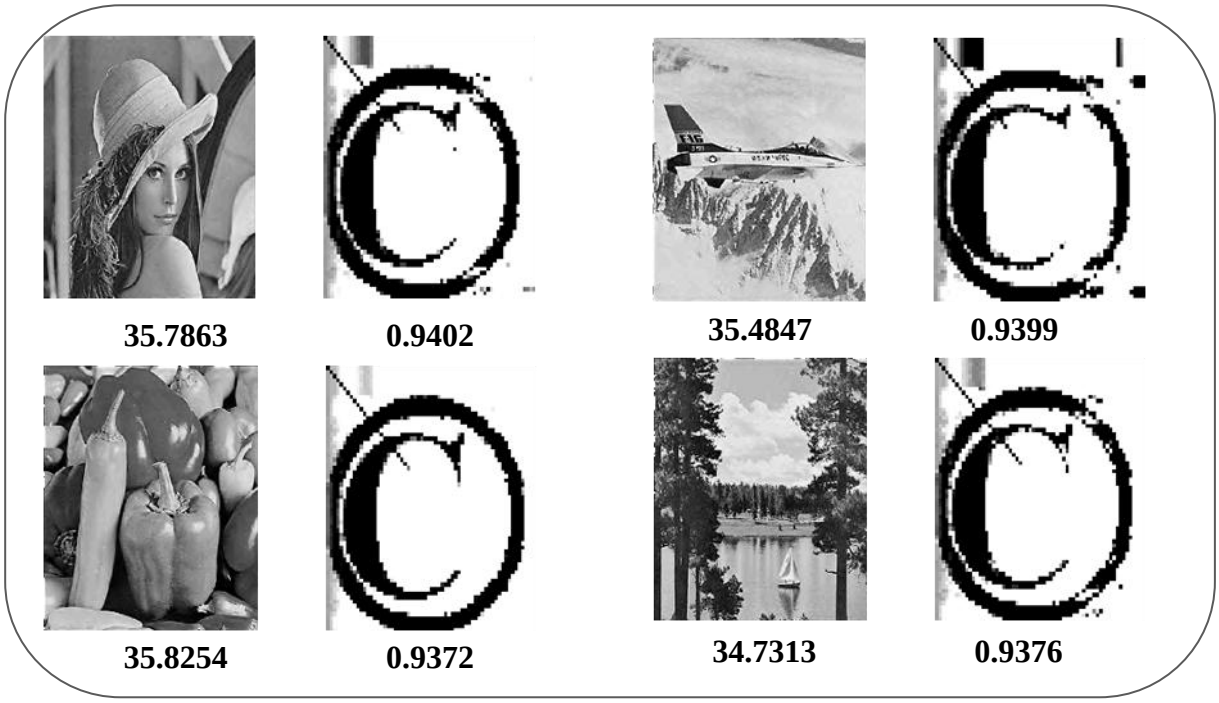


Figure 5. 9 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Sharpen de valeur 0.8.

5.2.3. Attaques géométriques

Les attaques géométriques sont l'ensemble des attaques qui affectent la géométrie de l'image. Ce paragraphe va traiter la résistance de l'algorithme proposé contre les attaques géométriques.

- ***Rotation***

La rotation est une attaque géométrique dont l'image se fait tourner autour de son axe central. On expérimente l'algorithme contre cette attaque avec une rotation de 60° (Figure 5.10). Nous remarquons que la rotation ne fait pas une distorsion de la marque, elle garde une bonne qualité avec un NC supérieur à 0.93.

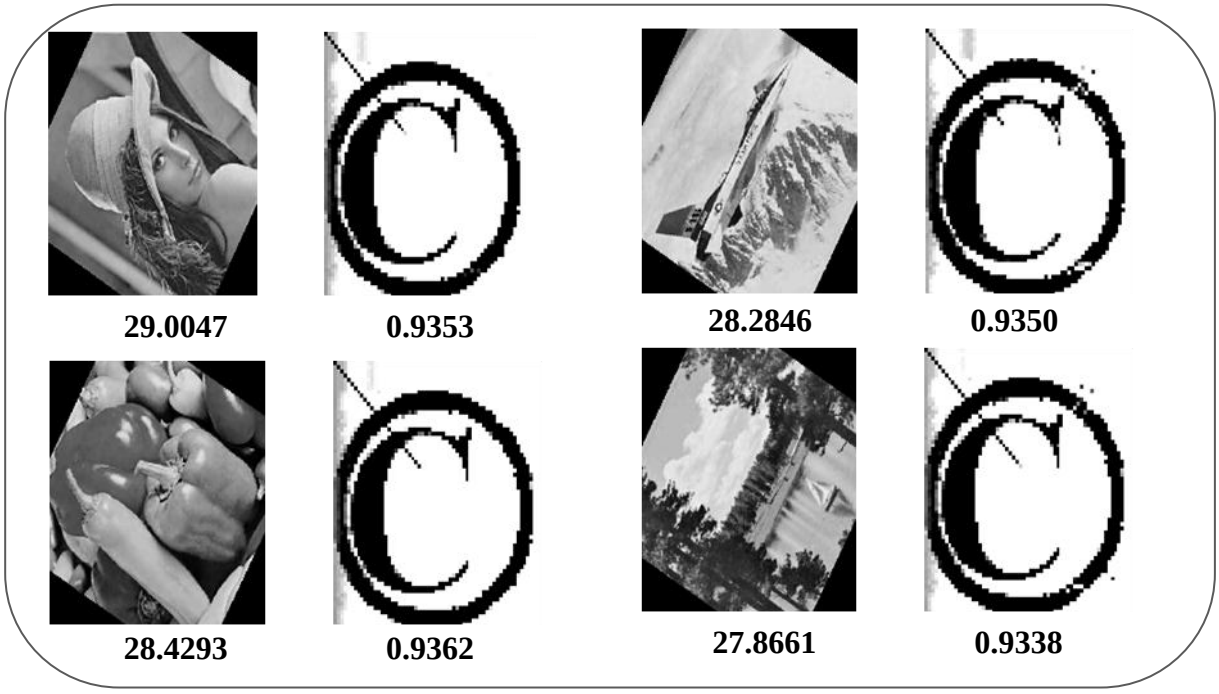


Figure 5. 10 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de rotation 60°.

- ***Égalisation d'histogramme***

L'égalisation d'histogramme est une méthode d'ajustement du contraste d'une image numérique. Elle consiste à appliquer une transformation sur chaque pixel à partir de l'histogramme cumulé de l'image de départ. Des images de test sont tatouées par l'algorithme proposé après elles subissent l'attaque d'égaliseur d'histogramme. Les résultats obtenus sont illustrés sur la figure 5.11. L'auto-corrélation est supérieure à 0.93 et la marque est toujours visible.

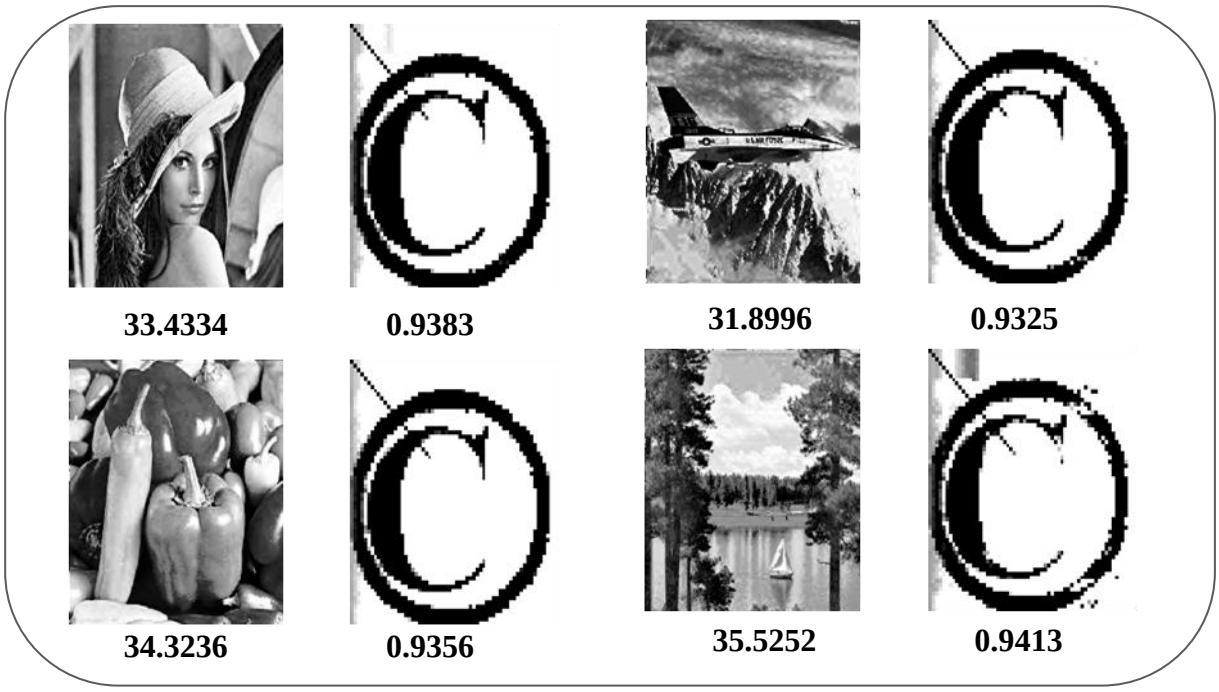


Figure 5. 11 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de l'égalisation d'histogramme.

- ***correction gamma***

La correction gamma est une opération non linéaire utilisée pour coder et décoder la luminance. La robustesse de l'algorithme contre ce type d'attaque est acceptable avec un NC proche de 0.93 et la marque extraite contient quelques distorsions cependant, elle est toujours visible (Figure 5.12).

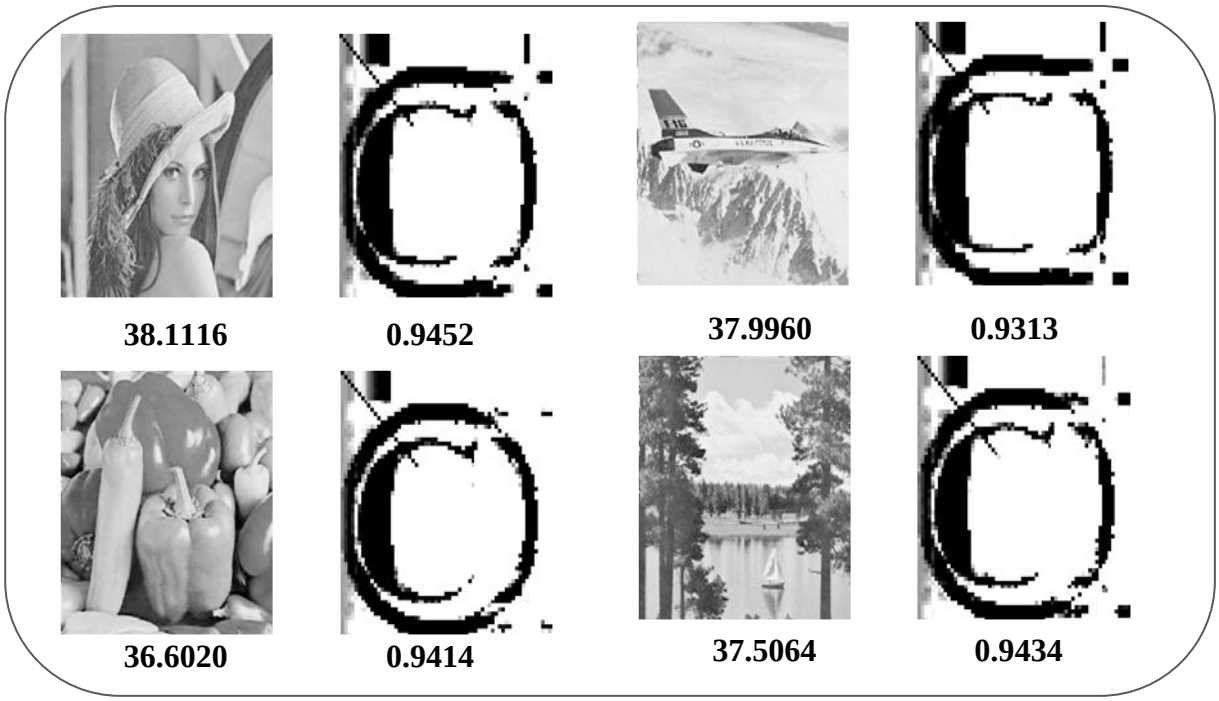


Figure 5. 12 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de correction gamma de valeur 0.6.

- ***Translation:***

La translation est une attaque non malvaillante dont les pixels de l'image se sont décalés en créant des aspaces noir dans l'image, la taille de l'image est toujours la même. Dans la figure suivante on remarque que le NC est proche de 0.94 avec une marque extraite acceptable pour une attaque de 50×50 pixels de translation (Figure 5.13).

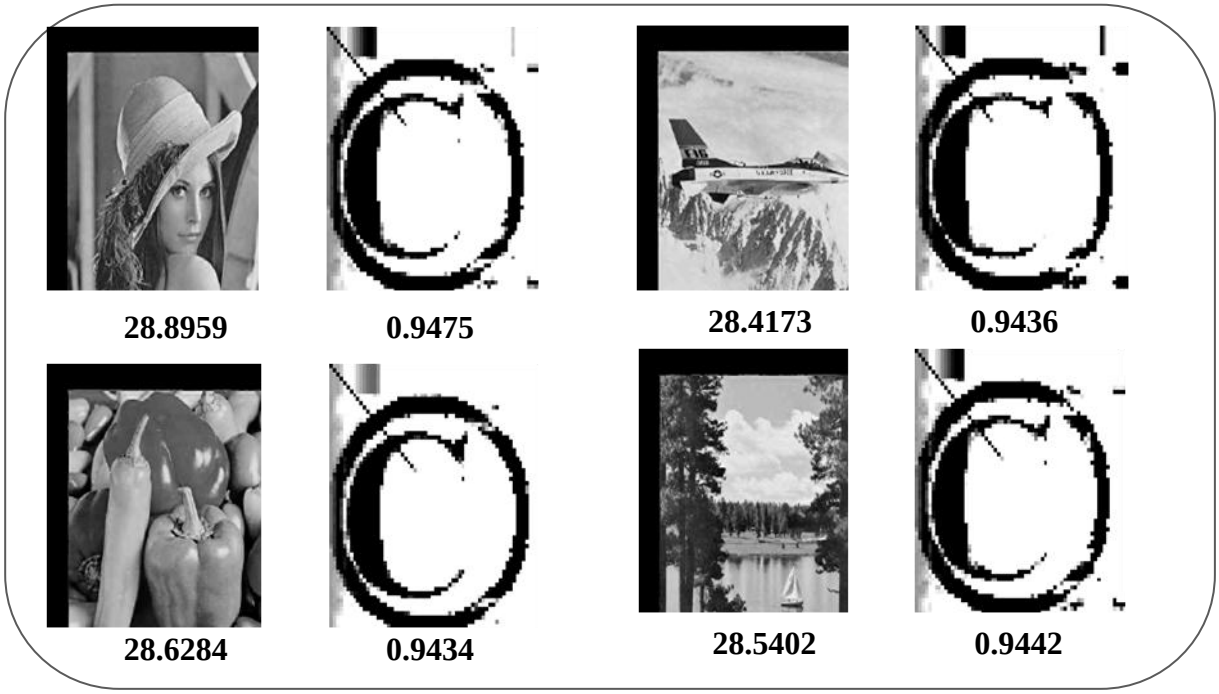


Figure 5. 13 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de translation de taille $\mathbf{50 \times 50}$ pixels.

- ***Coupure :***

L'attaque de coupure consiste à couper une partie de l'image et faire agrandir cette partie en produisant une image de même taille que l'image hôte. L'attaque de coupure est connue par les changements amenés à la marque extraite. L'algorithme proposé est testé face à cette attaque. La marque extraite présente une bonne qualité visuelle avec un facteur d'auto-corrélation supérieur à 0.93.

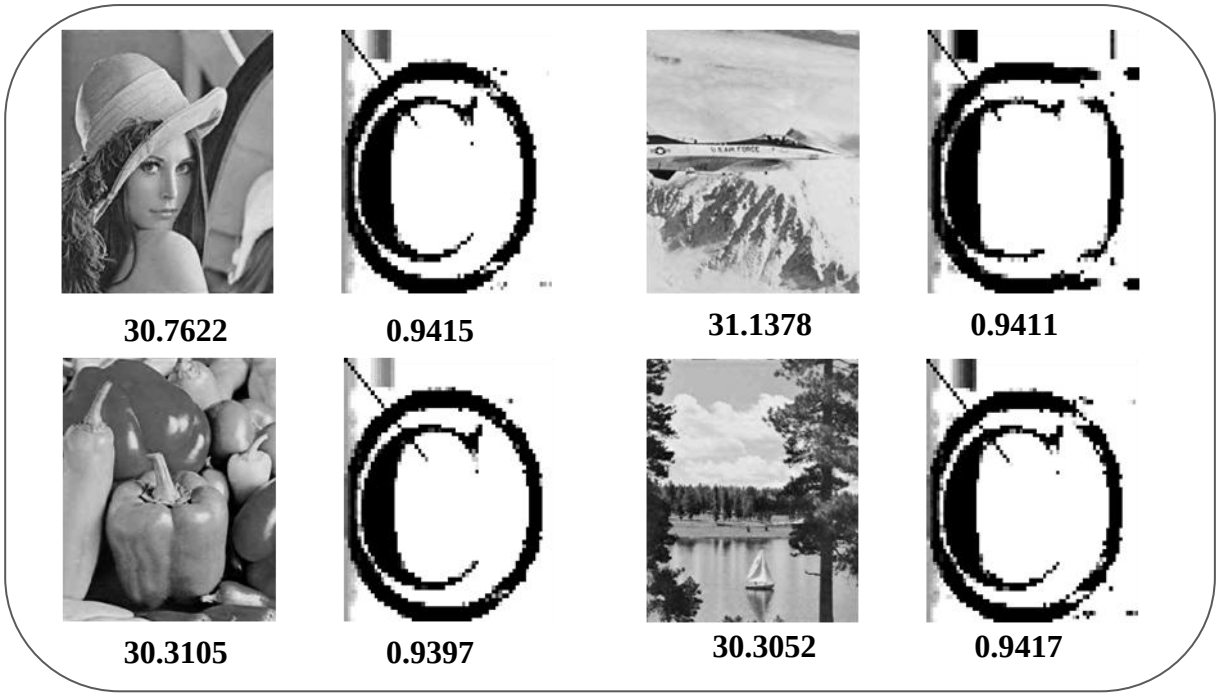


Figure 5. 14 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de coupure.

- ***Redimensionnement***

Le redimensionnement est une attaque géométrique qui consiste à changer la taille de l'image. Cette attaque affecte la marque vu que les pixels de l'image tatouée sont compactés. L'algorithme est testé contre l'attaque géométrique de redimensionnement avec l'échelle 256×256 (Figures 5.15); on remarque que la marque comporte une bonne qualité avec un facteur NC proche de 0.94; et la marque extraite est toujours visible.

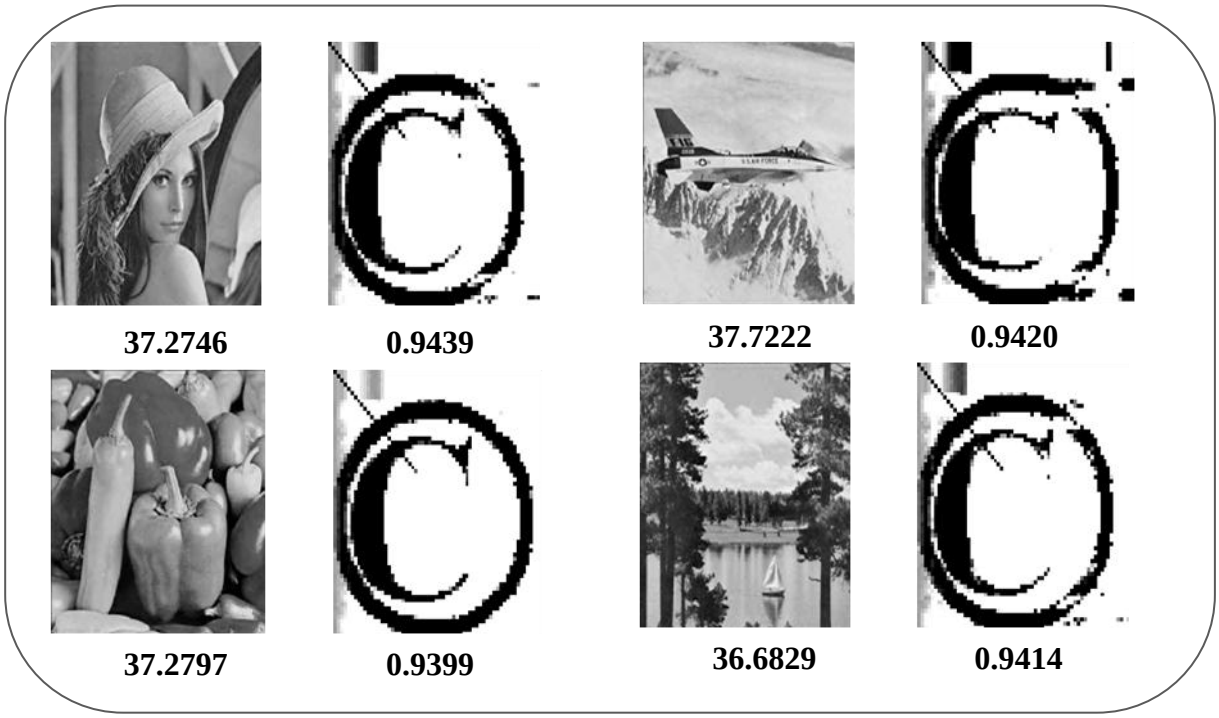


Figure 5. 15 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de redimensionnement à $\mathbf{256 \times 256}$ pixels.

5.2.4. Compression JPEG

La compression JPEG est une sorte d'attaque intentionnelle, elle a la capacité d'effacer la marque d'une image tatouée. Une image tatouée est compressée avec un rapport de 60%. Le facteur d'auto-corrélation est de l'ordre de 0.93 avec un PSNR supérieur à 36 dB. On peut conclure que l'algorithme proposé est solide face à cette attaque.

Le tableau 5.5 récapitule les résultats des paramètres NC et PSNR après l'attaque de compression JPEG à différentes valeurs du rapport de compression. On remarque que le NC varie entre 0.93 et 0.95 et le PSNR entre 36 dB et 39 dB. Les résultats obtenus démontrent la robustesse et l'efficacité de l'algorithme proposé.

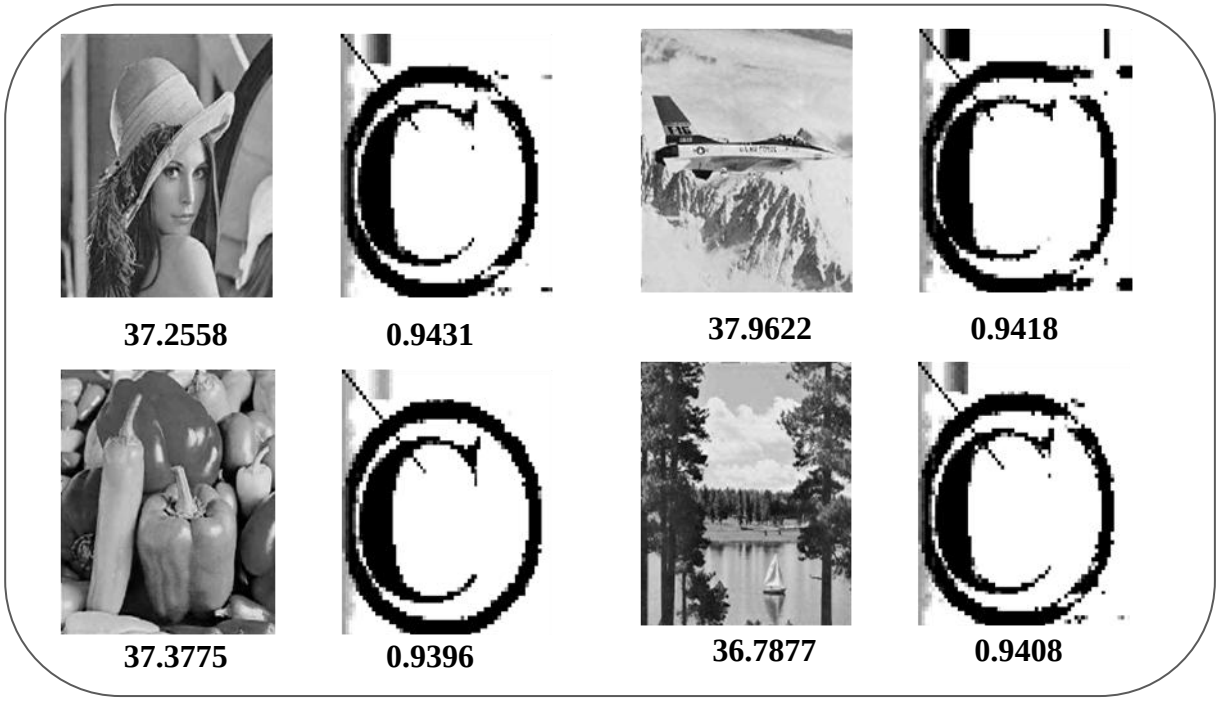


Figure 5. 16 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de compression JPEG de rapport 60%.

compression JPEG (%)	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
10%	0.9424	36.8229	0.9415	37.2355	0.9398	36.9892	0.9407	36.2353
20%	0.9429	37.0738	0.9418	37.6750	0.9394	37.2266	0.9408	36.5739
30%	0.9430	37.1621	0.9414	37.8236	0.9396	37.2994	0.9407	36.6805
40%	0.9429	37.2111	0.9418	37.9033	0.9396	37.3517	0.9409	36.7400
50%	0.9431	37.2318	0.9415	37.9164	0.9395	37.3636	0.9408	36.7691
60%	0.9431	37.2558	0.9418	37.9622	0.9396	37.3775	0.9408	36.7877
70%	0.9434	37.2667	0.9418	37.9941	0.9395	37.3985	0.9409	36.8128
80%	0.9433	37.2837	0.9418	38.0151	0.9395	37.4013	0.9409	36.8323
90%	0.9431	37.2846	0.9418	38.0235	0.9395	37.4074	0.9409	36.8410

Tableau 5. 5 : Les Valeurs de NC et de PSNR après l'attaque de compression JPEG.

5.3. Deuxième approche : tatouage basé sur la DWT et la SVD

Dans cette section nous allons tester la deuxième approche. Cette approche est basée sur la transformée DWT où la marque est insérée dans la composante singulière de la marque SVD. Cette technique est détaillée dans le paragraphe (3.3) du chapitre précédent. Pour le test, on utilise un ensemble d'images de tests de taille 512×512 pixels, Lena Airplane, Pepper et Sailboat. La marque à insérer est de taille 64×64 pixels. Dans la figure suivante, nous examinons la similarité entre la marque insérée et la marque extraite par le calcul du facteur de corrélation normalisé. Et on trouve un facteur de similitude supérieur à 0.98 entre la marque insérée et la marque extraite.

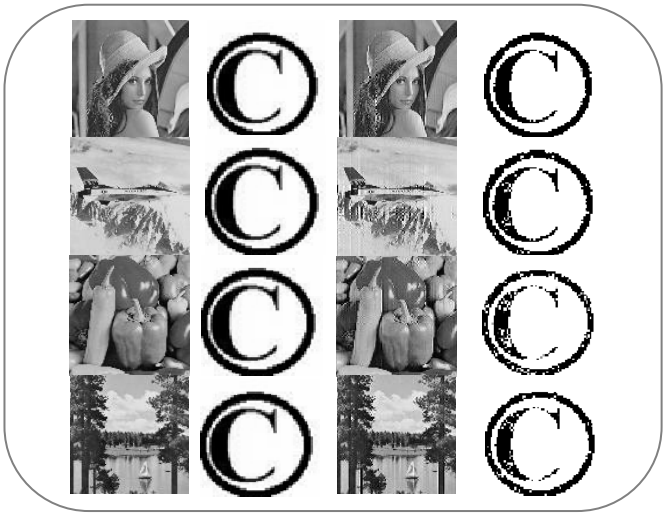


Figure 5. 17 : Résultats de Simulation de l'algorithme de tatouage proposé par les images de tests suivantes: Lena (37.0956 dB ; 0.9891) Airplane (35.3540 dB ; 0.9837); Pepper (36.9455 dB; 0.9968); et Sailboat (37.1149 dB; 0.9954).

La mesure de l'invisibilité de la marque dans l'image tatouée par le calcul de rapport signal sur bruit PSNR donne une bonne qualité de l'image tatouée pour les quatre images de test avec une valeur supérieure à 36 décibels (Figure 5.17).

5.3.1. Addition du bruit

- ***bruit de sel et poivre***

Nous avons utilisé la variance 0.1% de l'attaque de bruit de sel et poivre. Les résultats de la simulation sont illustrés dans la figure 5.18; nous avons remarqué que la marque extraite était toujours visible et n'a pas une grande influence sur l'image tatouée, le rapport NC est supérieur à 0.98.

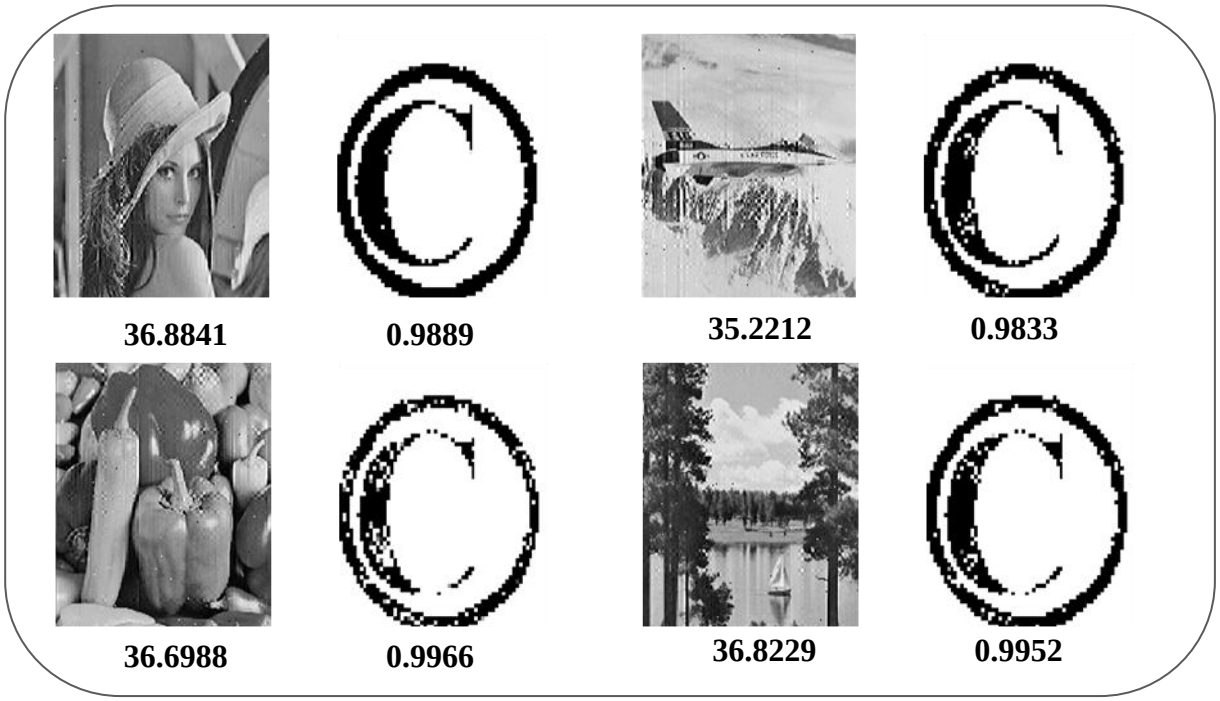


Figure 5. 18 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de bruit sel et poivre de variance 0.1%.

Le bruit sel et poivre possède la capacité de supprimer la marque d'une image tatouée. Alors l'approche présentée résiste efficacement à cette attaque avec un facteur d'auto-corrélation supérieur à 0.9 pour une variance de 1% à 20 %. Le PSNR présente des valeurs supérieures à 29 dB, il est inversement proportionnel à la variance.

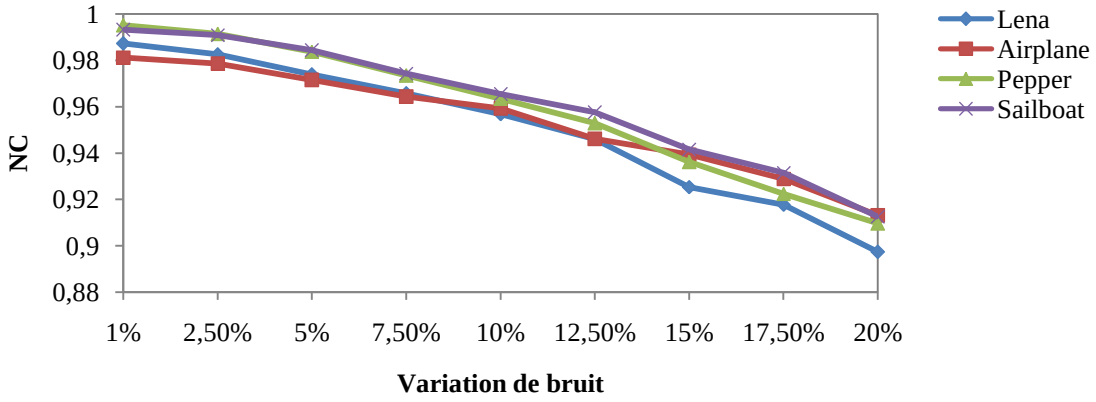


Figure 5. 19: Robustesse de l'algorithme de tatouage contre le bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat.

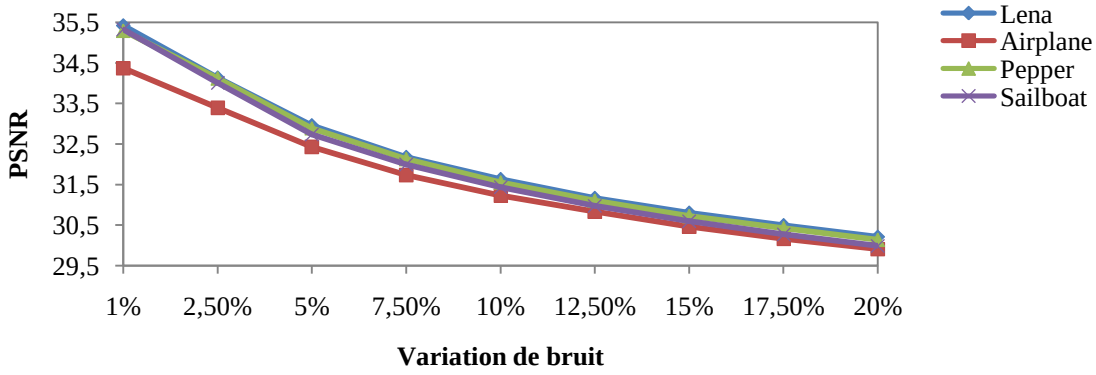


Figure 5. 20 : Valeurs de PSNR pour différentes variations de l'attaque de bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat

- ***Bruit Gaussien***

Une image tatouée par l'approche présentée est attaquée par un bruit Gaussien de variance égal à 0,1%. Dans la figure 5.21 nous illustrons la marque extraite et l'image tatouée, on peut remarquer que la marque et l'image tatouée sont de bonnes qualités où le facteur d'auto-corrélation NC est supérieur à 0.98, et le PSNR supérieur à 35 dB.

Les Figures 5.22 et 5.23 présentent les valeurs de NC et PSNR après l'attaque de bruit Gaussien. Pour la première figure on remarque que le système de tatouage garde le NC supérieur à 0.9 jusqu'à la valeur de bruit 7.5%, au-delà de cette valeur le système est fragile contre cette attaque.

Le PSNR montre une courbe décroissante contre une variance croissante, pour des variances supérieures à 7.5% le PSNR est inferieur à 30 dB.

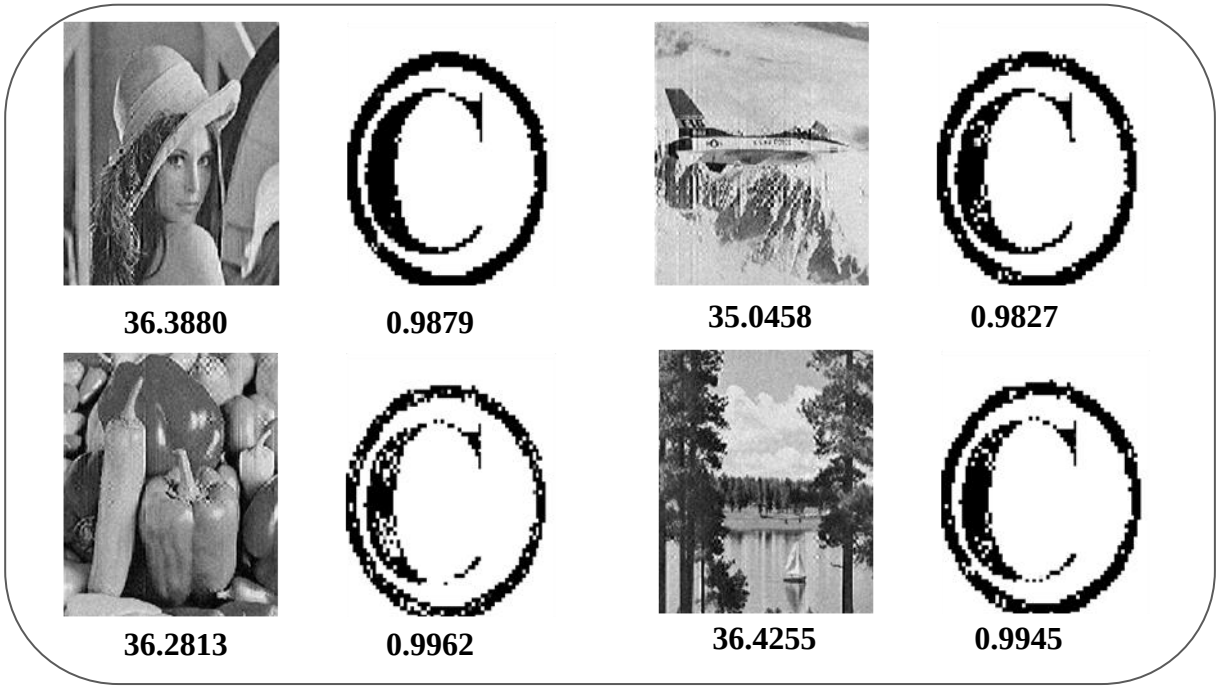


Figure 5. 21 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de bruit gaussien de variance 0.1%.

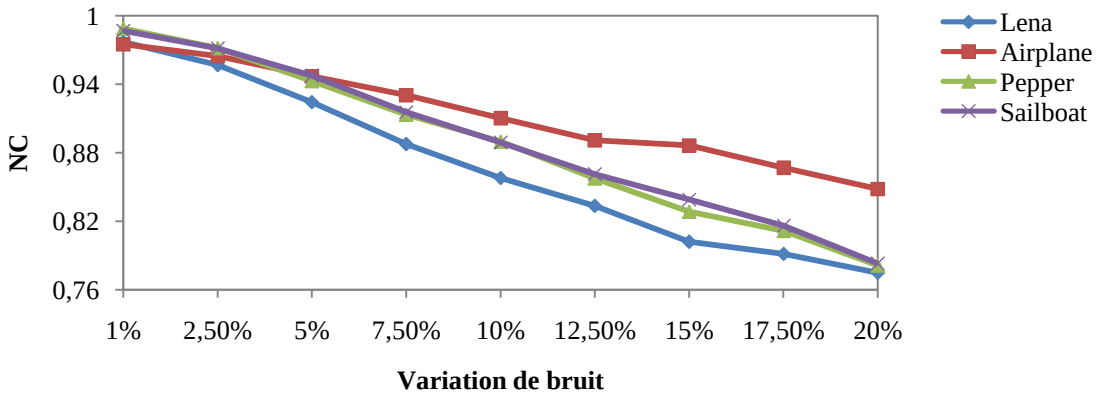


Figure 5. 22 : Robustesse de l'algorithme de tatouage contre le bruit gaussien pour les images Lena, Airplane, Pepper et Sailboat.

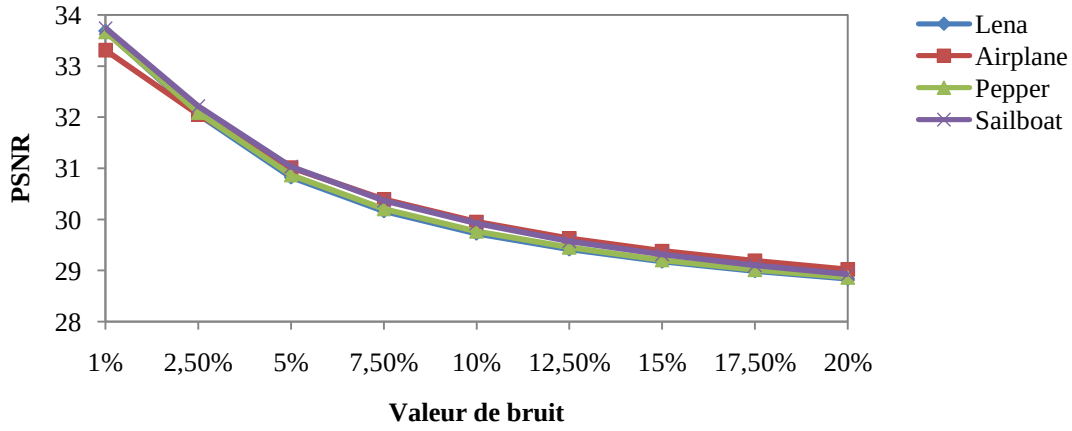


Figure 5. 23 : Valeurs de PSNR pour différentes variations de l'attaque de bruit Gaussien pour les images Lena, Airplane, Pepper et Sailboat.

5.3.2. Attaque de filtrage

- ***Filtre médian***

On utilise un filtre médian de taille 3×3 comme attaque contre une image tatouée par l'algorithme proposé. On peut remarquer sur la figure 5.24 que la marque extraite garde une bonne qualité visuelle avec un NC supérieur à 0.98, le rapport signal sur bruit PSNR est supérieur à 35 dB.

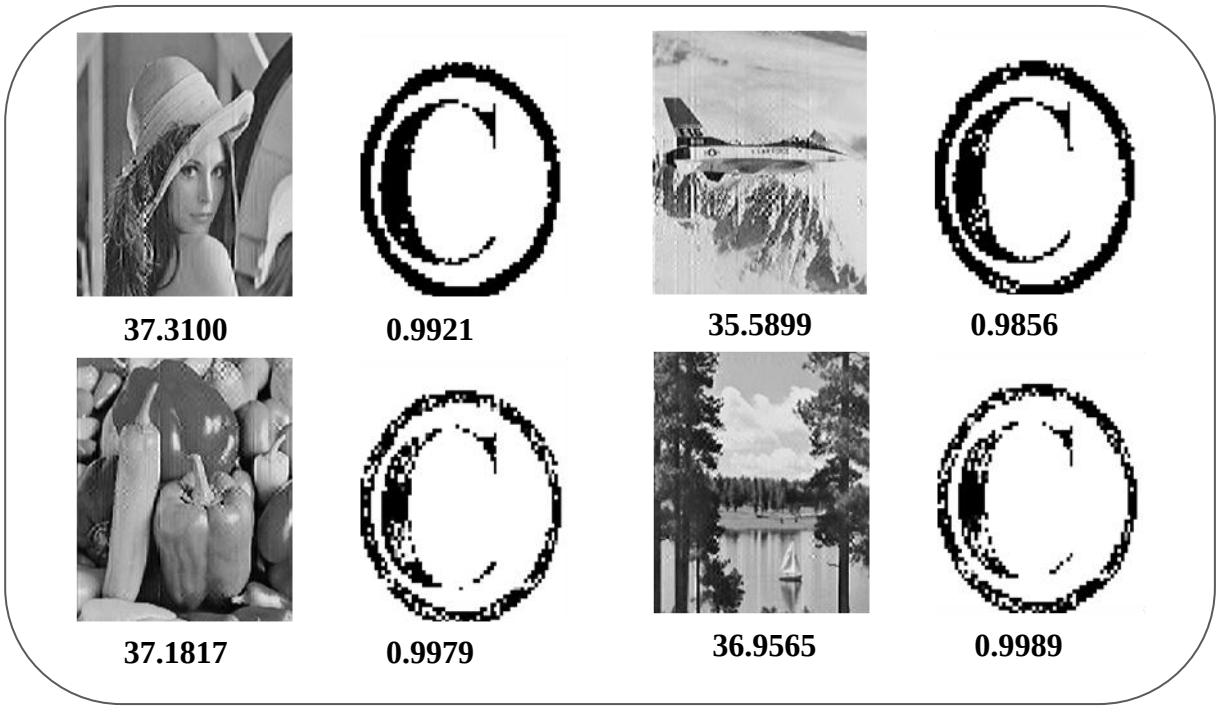


Figure 5. 24 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre médian de taille **3 × 3** pixels.

Pour confirmer la robustesse de cette algorithme une image tatouée est attaquée par plusieurs filtres médians dont la taille s'étale de 3×3 à 11×11. Nous avons constaté que le facteur d'auto-corrélation est supérieur à 0.9, au delà de la taille 11×11. L'algorithme n'est plus solide et le PSNR enregistre des valeurs entre 34,5 et 38 dB.

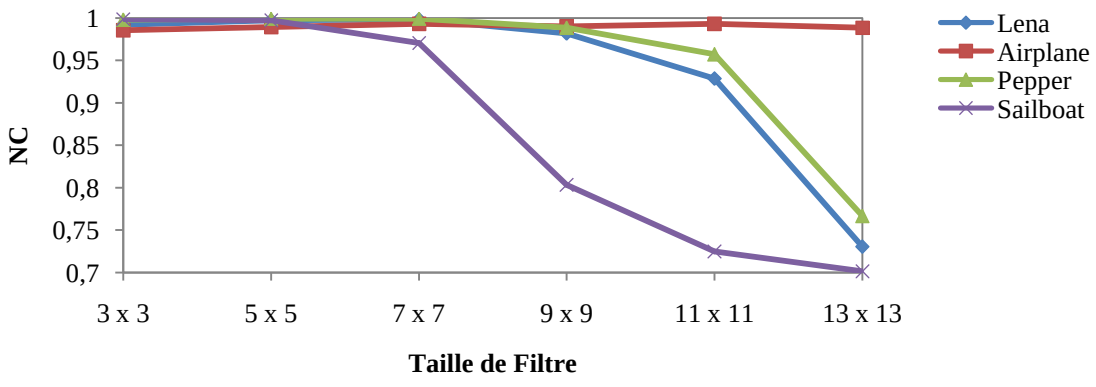


Figure 5. 25 : Robustesse de l'algorithme de tatouage contre l'attaque de filtre Médian pour les images Lena, Airplane, Pepper et Sailboat.

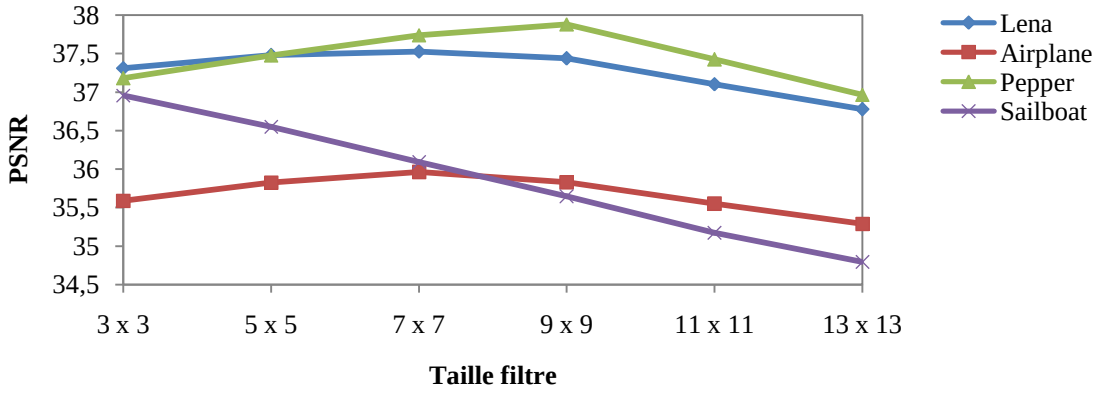


Figure 5. 26 : Valeurs de PSNR pour les différentes tailles de l'attaque de filtre Médian pour les images Lena, Airplane, Pepper et Sailboat.

- ***Filtre moyen***

L'attaque par filtre moyen pour la taille 3 × 3 pixels donne des NC proches de 0.98 (Figure 5.27).

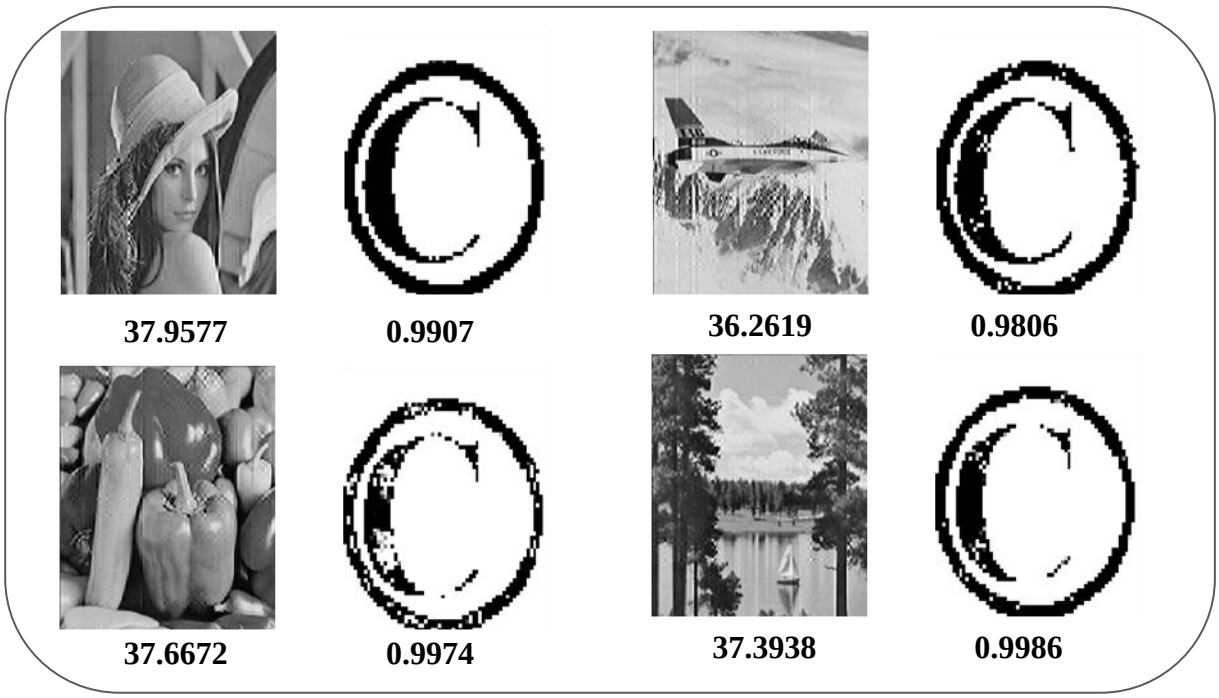


Figure 5. 27 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre moyen de taille **3 × 3** pixels.

- ***Filtre Gaussien***

Le filtre Gaussien est l'un des attaques nocives pour le tatouage d'image. Nous allons examiner l'algorithme proposé contre l'attaque de filtre Gaussien de la taille 3 × 3 pixels, nous remarquons que le facteur d'auto-corrélation NC est proche de 0.98 avec une bonne qualité de la marque extraite (Figure 5.28).

Le tableau 5.6 présente les facteurs d'auto-corrélation et du PSNR pour les filtres Gaussiens de taille 3×3 à 13×13. On peut remarquer que le NC est supérieur à 0.98 et le PSNR supérieur à 36 dB. Ces critères montrent que l'algorithme est robuste.

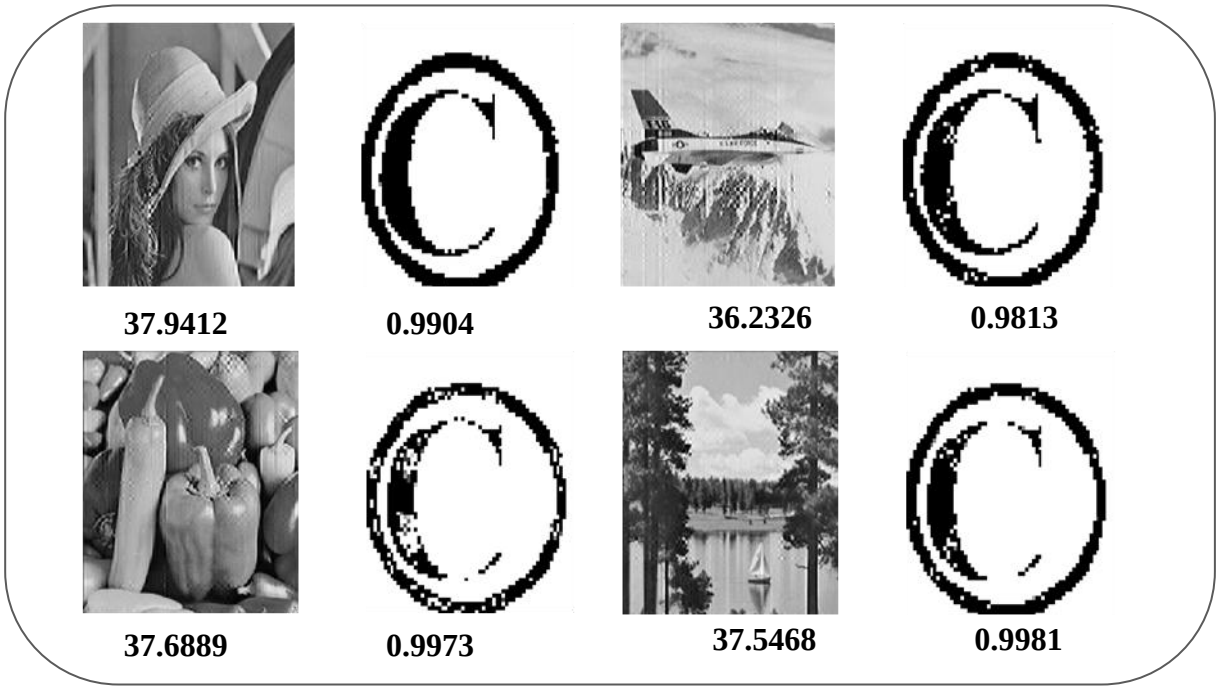


Figure 5. 28 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Gaussien de taille **3 × 3** pixels.

Taille de filtre Gaussien	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
3 × 3	0.9904	37.9412	0.9813	36.2326	0.9973	37.6889	0.9981	37.5468
5 × 5	0.9925	38.1488	0.9824	36.4721	0.9982	37.8978	0.9993	37.5534
7 × 7	0.9928	38.1817	0.9826	36.5089	0.9984	37.9320	0.9993	37.5632
9 × 9	0.9929	38.1833	0.9826	36.5106	0.9984	37.9336	0.9993	37.5638
11 × 11	0.9929	38.1833	0.9826	36.5106	0.9984	37.9336	0.9993	37.5638
13 × 13	0.9929	38.1833	0.9826	36.5106	0.9984	37.9336	0.9993	37.5638

Tableau 5. 6 : Les Valeurs de NC et de PSNR après l'attaque de filtre gaussien.

- ***Filtre Sharpen***

Les résultats obtenus après l'attaque du filtre Sharpen avec la variance de 0.8 sont illustrés sur la figure 5.29. La marque extraite est visible avec un facteur d'auto-corrélation de 0.97.

Le tableau 5.7 récapitule les résultats de NC et de PSNR pour le filtre Sharpen, nous faisons varier la variance de 0.1 à 0.9. On peut remarquer que le NC est supérieur à 0.97 et le PSNR marque des valeurs supérieures à 32 dB.

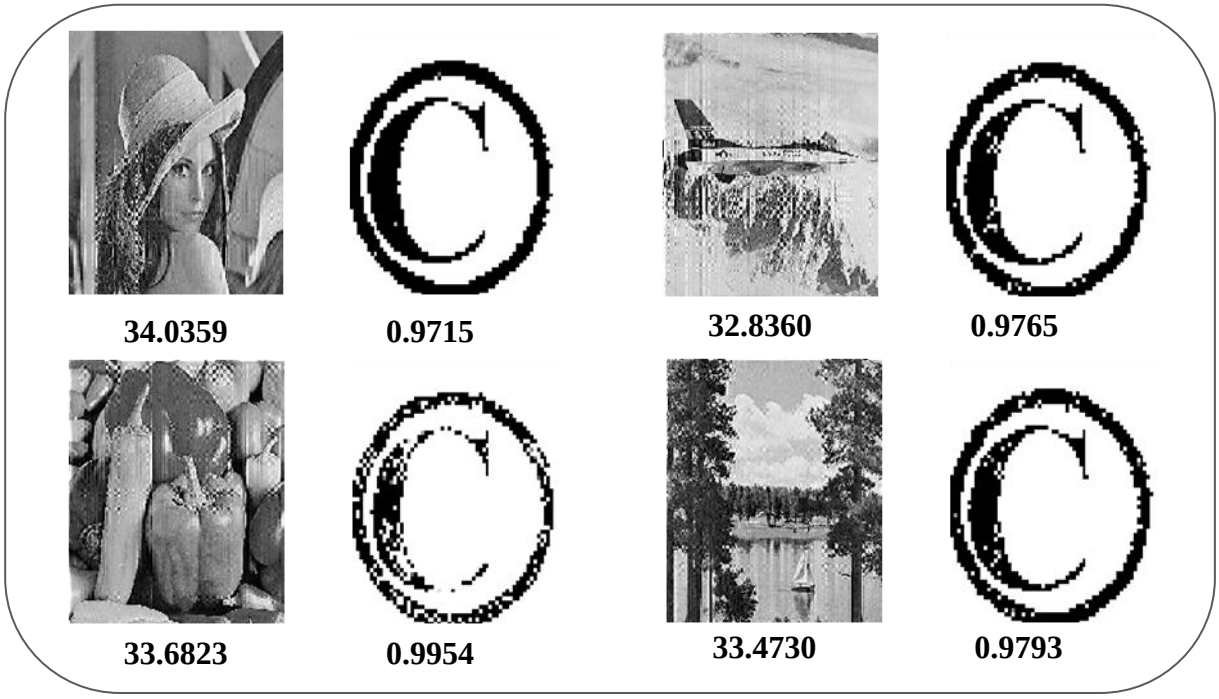


Figure 5. 29 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Sharpen de valeur 0.8.

Filtre Sharpen	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
0.1	0.9712	33.7984	0.9767	32.6777	0.9957	33.4600	0.9797	33.1635
0.2	0.9713	33.8533	0.9767	32.7134	0.9956	33.5103	0.9796	33.2340
0.3	0.9713	33.8979	0.9766	32.7426	0.9956	33.5517	0.9795	33.2923
0.4	0.9714	33.9358	0.9766	32.7680	0.9955	33.5873	0.9795	33.3416
0.5	0.9714	33.9670	0.9766	32.7890	0.9955	33.6168	0.9794	33.3826
0.6	0.9714	33.9935	0.9766	32.8071	0.9955	33.6421	0.9794	33.4175
0.7	0.9715	35.0161	0.9766	32.8225	0.9954	33.6636	0.9793	33.4472
0.8	0.9715	34.0359	0.9765	32.8360	0.9954	33.6823	0.9793	33.4730
0.9	0.9715	34.0524	0.9765	32.8476	0.9954	33.6985	0.9793	33.4947

Tableau 5. 7 : Les Valeurs de NC et de PSNR après l'attaque de filtre Sharpen.

5.3.3. Attaques géométriques

- ***Rotation***

L'attaque de rotation est une attaque très forte car elle permet de supprimer la marque, alors on teste l'algorithme contre cette attaque avec une rotation de 5° (Figure 5.30). La rotation ne crée pas de distorsion et la marque extraite présente une très bonne qualité visuelle avec une valeur de NC proche de 0.80.

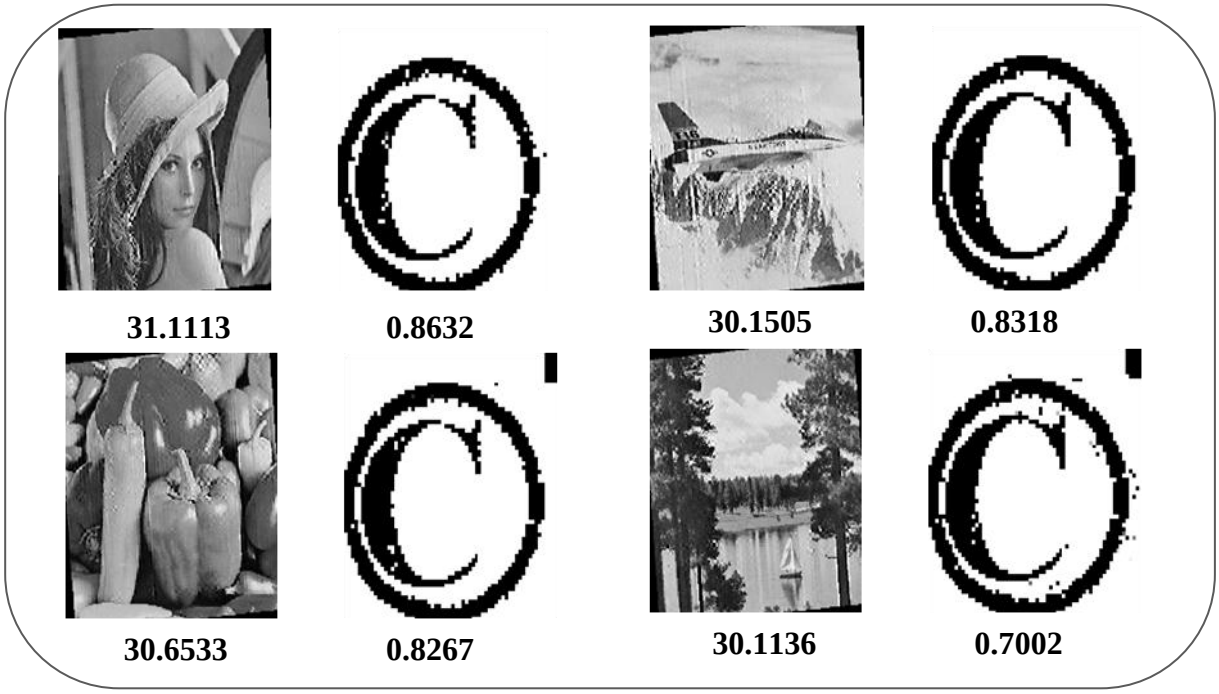


Figure 5. 30 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de rotation de 5 degrés.

- ***Égalisation d'histogramme***

L'attaque d'égalisation de l'histogramme donne une marque extraite avec des distorsions où la valeur de NC est supérieure à 0.95; mais la marque reste visible (Figure 5.31).

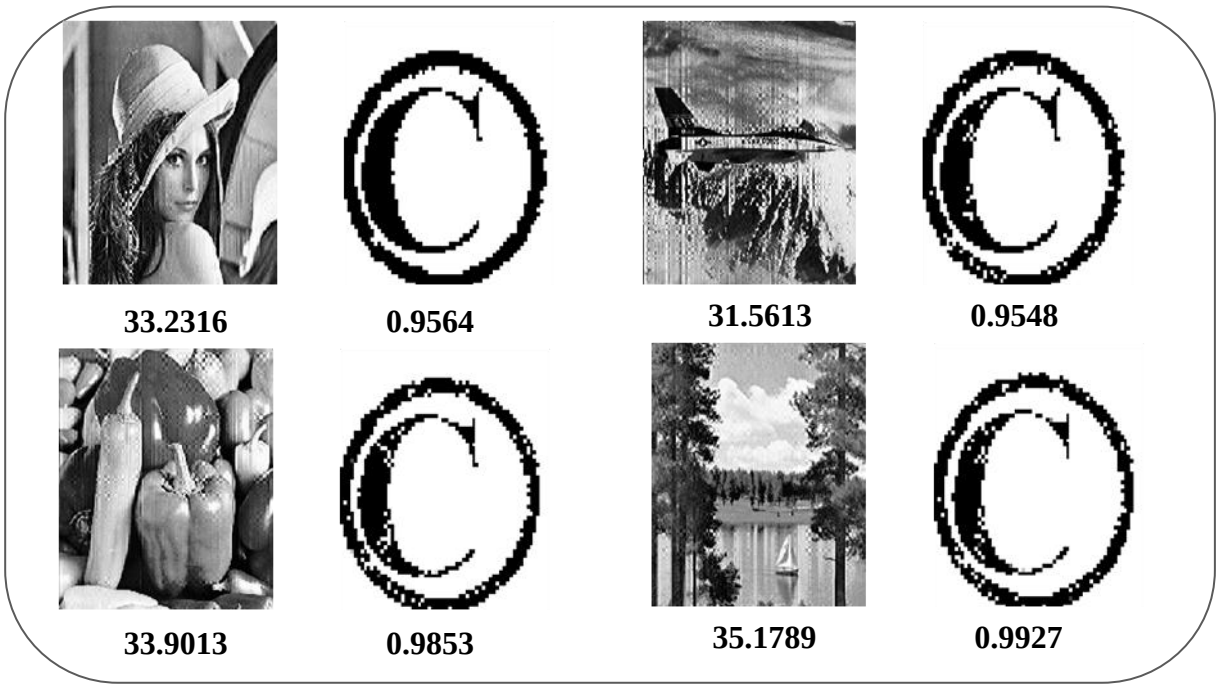


Figure 5. 31 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de l'égalisation d'histogramme.

- ***correction gamma***

Les images tatouées sont testées contre l'attaque de la correction gamma. Les résultats obtenus sont illustrés sur la figure 5.32. Le facteur d'auto-corrélation NC est supérieur à 0.98 et le PSNR est supérieur à 35 dB.

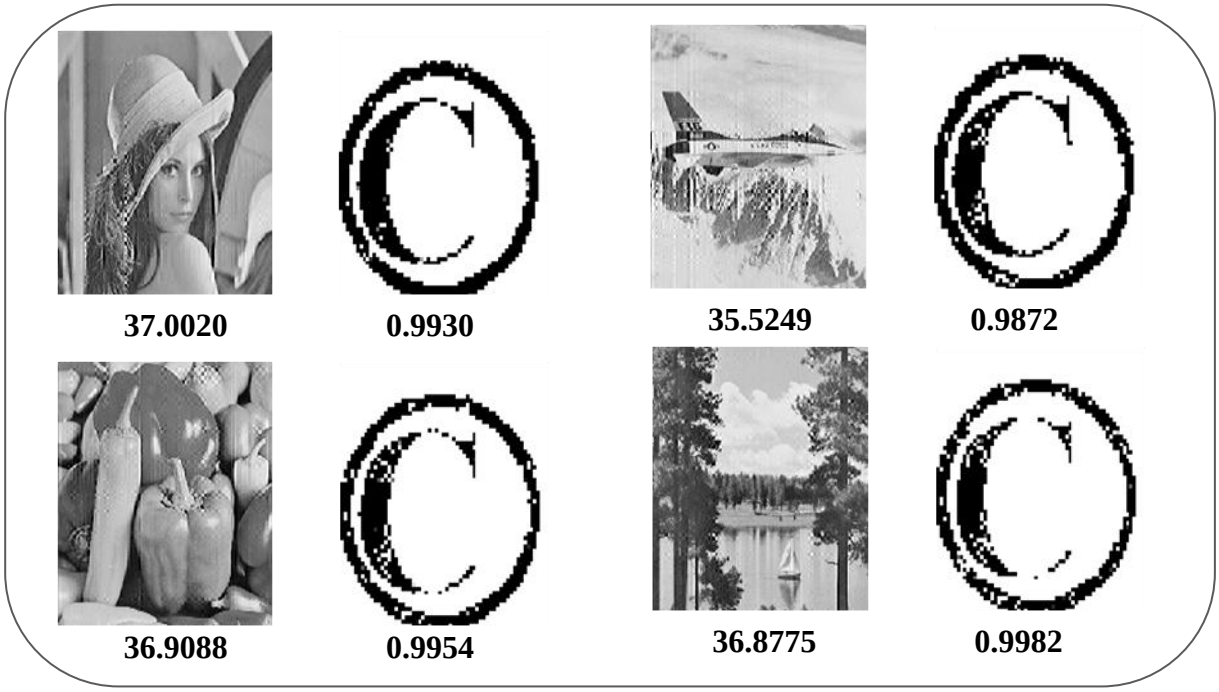


Figure 5. 32 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de correction gamma de valeur 0.8.

- ***Redimensionnement***

L'attaque de redimensionnement est très répandue en traitement d'image, pour cette raison nous allons tester notre algorithme contre cette attaque. En effet, une image tatouée de taille 512×512 subit une attaque de redimensionnement de l'échelle 256×256. La marque extraite est toujours visible à l'œil nue ainsi le facteur d'auto-corrélation est supérieur à 0.97 avec un PSNR supérieur à 35 dB pour toute les images de tests.

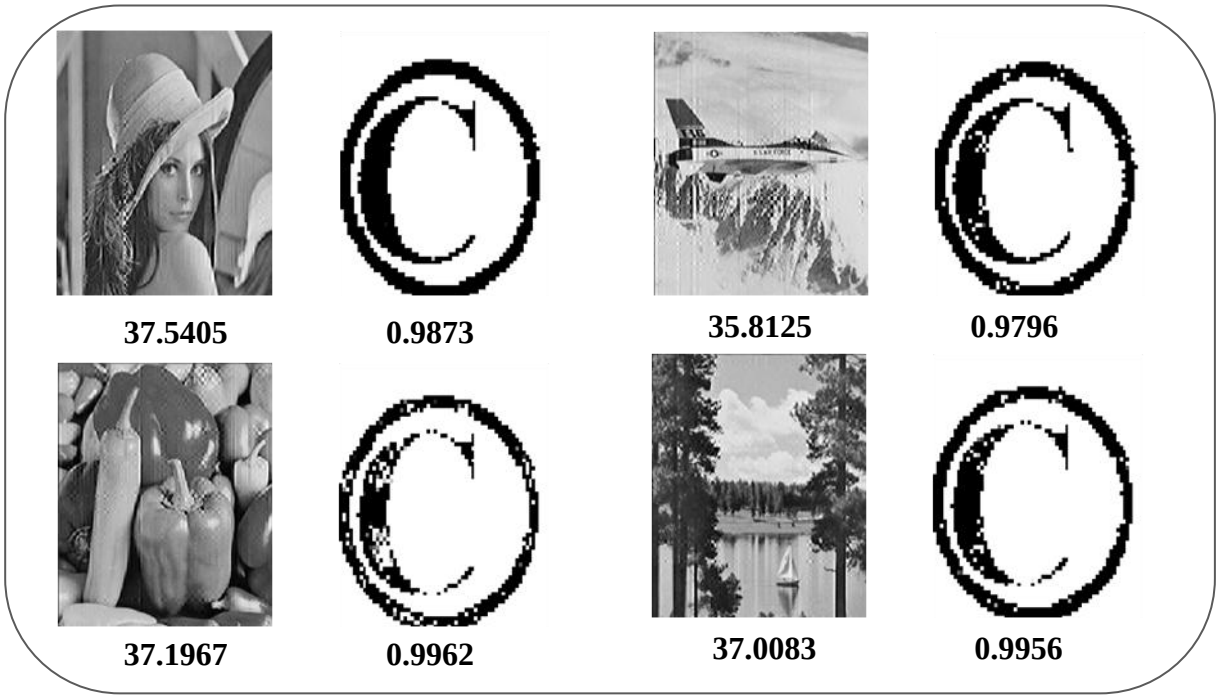


Figure 5. 33 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de redimensionnement de $\mathbf{512 \times 512}$ pixels à $\mathbf{256 \times 256}$ pixels.

5.3.4. Compression JPEG

L'attaque de compression JPEG est capable d'effacer définitivement la marque. Notre algorithme est utilisé pour tatouer des images de tests. Une compression JPEG avec un facteur de 60% est appliquée. Nous remarquons que le facteur d'auto-corrélation est supérieur à 0.98 et le PSNR supérieur à 35 dB. On peut déduire que notre algorithme est toujours solide contre cette attaque (Figure 5.35).

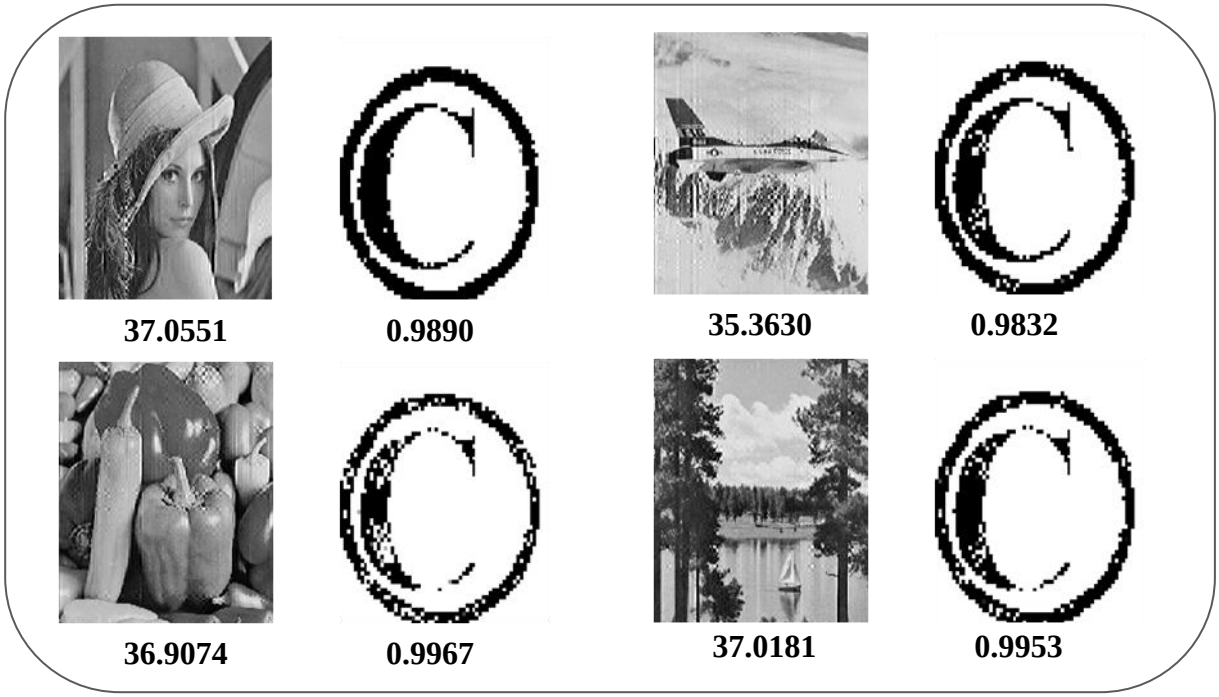


Figure 5. 34 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de compression JPEG de rapport 60%.

L'algorithme est robuste contre l'attaque de compression JPEG comme montré dans le tableau 5.8, où le NC est supérieur à 0.97 et le PSNR varie entre 35 et 37 décibels.

Rapport de compression JPEG	Lena		Airplane		Pepper		Sailboat	
	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR
10%	0.9856	36.6573	0.9793	35.2424	0.9935	36.5792	0.9919	36.2823
20%	0.9890	36.8640	0.9824	35.3103	0.9957	36.7563	0.9940	36.6283
30%	0.9891	36.9464	0.9830	35.3262	0.9965	36.8014	0.9949	36.7598
40%	0.9890	36.9680	0.9830	35.3300	0.9964	36.8140	0.9951	36.8003
50%	0.9886	36.9787	0.9832	35.3295	0.9965	36.8242	0.9950	36.8334
60%	0.9890	37.0551	0.9832	35.3630	0.9967	36.9074	0.9953	37.0181
70%	0.9891	37.1044	0.9836	35.3772	0.9969	36.9418	0.9955	37.1120
80%	0.9892	37.0895	0.9836	35.3679	0.9968	36.9363	0.9955	37.1027
90%	0.9890	37.0930	0.9837	35.3596	0.9968	36.9335	0.9954	37.1059

Tableau 5. 8 : Les Valeurs de NC et de PSNR après l'attaque de compression JPEG.

5.4. Troisième Approche : tatouage basé sur la DWT

Dans cette section nous allons mettre en œuvre un nouvel algorithme de tatouage de l'image. Il est présenté en détail dans la section (3.4). Nous rappelons que ce nouveau algorithme est basé sur la transformée DWT combinée avec une nouvelle fonction du mouvement des pixels que nous avons nommé PMF (Pixel Mouvement Function). Pour valider notre algorithme de tatouage il est intuitif de le tester face aux attaques connues dans le domaine de traitement de l'image. Tout d'abord nous commençons par appliquer cet algorithme afin de tatouer quatre images de test de taille 512×512 pixels ; Lena, Airplane, Pepper et Sailboat. La marque est de taille 72×70 pixels. Les résultats de simulation trouvés sont montrés sur la figure 5.35. Nous pouvons remarquer la grande similarité entre la marque insérée et la marque extraite. Le facteur d'auto-corrélation et le rapport signal sur bruit sont marqués successivement de valeurs supérieures à 0.99 et 42.77 dB.

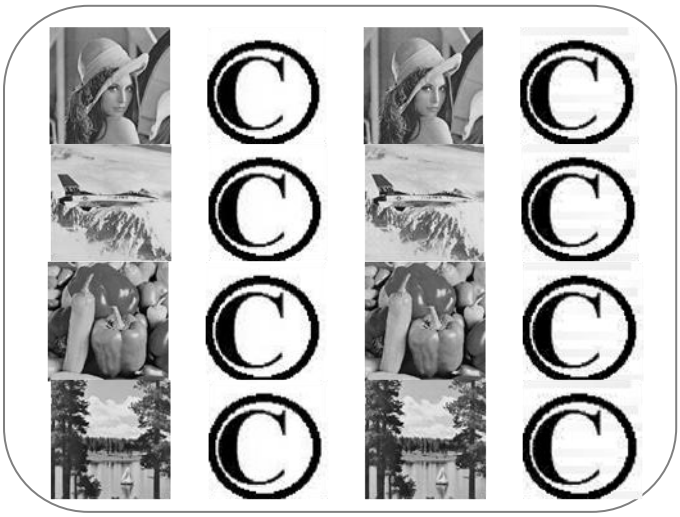


Figure 5. 35 : Résultats de simulation de l'algorithme de tatouage proposé par les images de tests suivants: Lena (42.7700 dB; 0.9995) Airplane (42.7700 dB; 0.9995); Pepper (42.7700 dB; 0.9995); et Sailboat (42.7700 dB; 0.9995).

5.4.1. Addition de bruit

- ***bruit de sel et poivre***

Les résultats de simulation d'une image tatouée attaquée par le bruit sel et poivre sont illustrés sur la figure 5.36. En effet, une image de taille 512×512 est tatouée en utilisant l'algorithme proposé avec une marque de taille 72×70, ensuite l'image résultante est attaquée par le bruit sel et poivre de variance 0.1%. On peut remarquer que le facteur d'auto-corrélation est toujours supérieur à 0.99, presque idéal et le PSNR est de l'ordre de 40 dB. Cet algorithme répond à l'exigence de la résistance contre ce bruit.

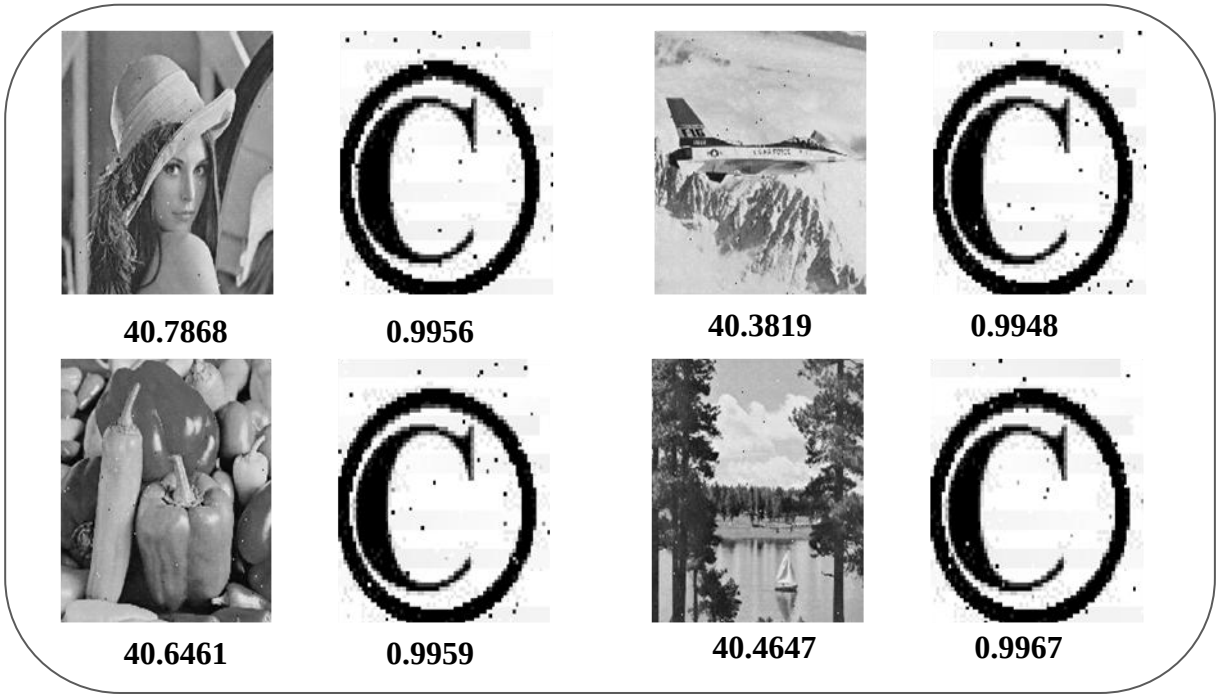


Figure 5. 36 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de bruit sel et poivre de variance 0.1%.

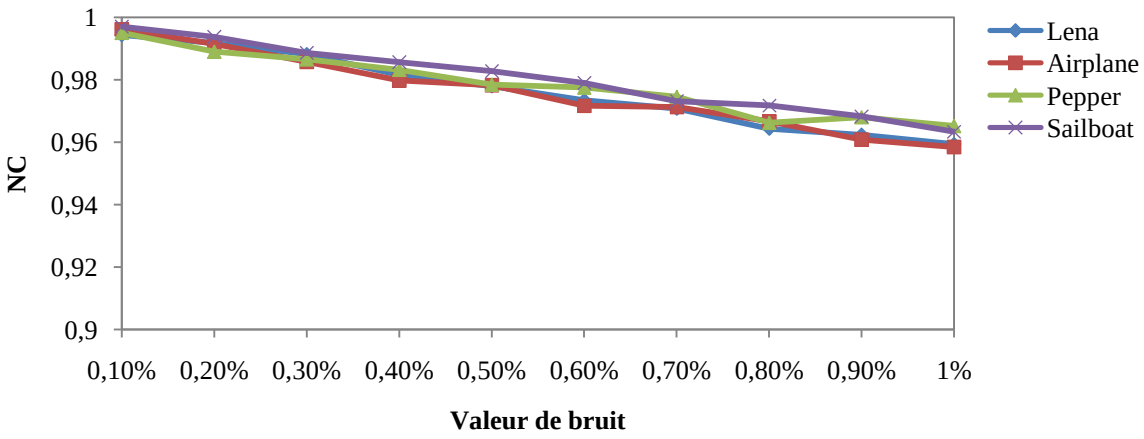


Figure 5. 37 : Robustesse de l'algorithme de tatouage contre bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat.

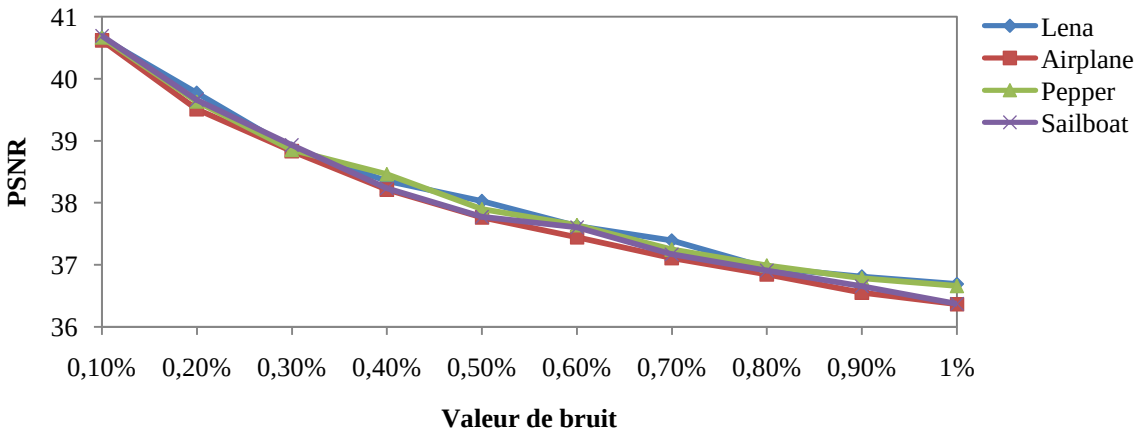


Figure 5. 38 : Valeurs de PSNR après les différentes valeurs de l'attaque de bruit sel et poivre pour les images Lena, Airplane, Pepper et Sailboat.

Un autre test consiste à faire changer la variance du bruit sel et poivre de 0.1% à 1%, puis un ensemble d'images de tests tatouées est attaqué par ces bruits. Les figures 5.37 et 5.38 présentent successivement le facteur d'auto-corrélation NC et le PSNR décroissant avec la l'augmentation de la variance, ils sont supérieurs à 0.8 et 36 dB successivement. Les résultats obtenus confirment la robustesse et l'efficacité de cet algorithme contre cette attaque.

- ***Bruit Gaussien***

Nous avons testé notre algorithme contre le bruit Gaussien avec une variance de 0.1% dans la Figure 5.39 on remarque que la marque extraite est de bonne qualité avec un rapport de similitude proche de 0.97 et un rapport signal sur bruit de 38 dB.

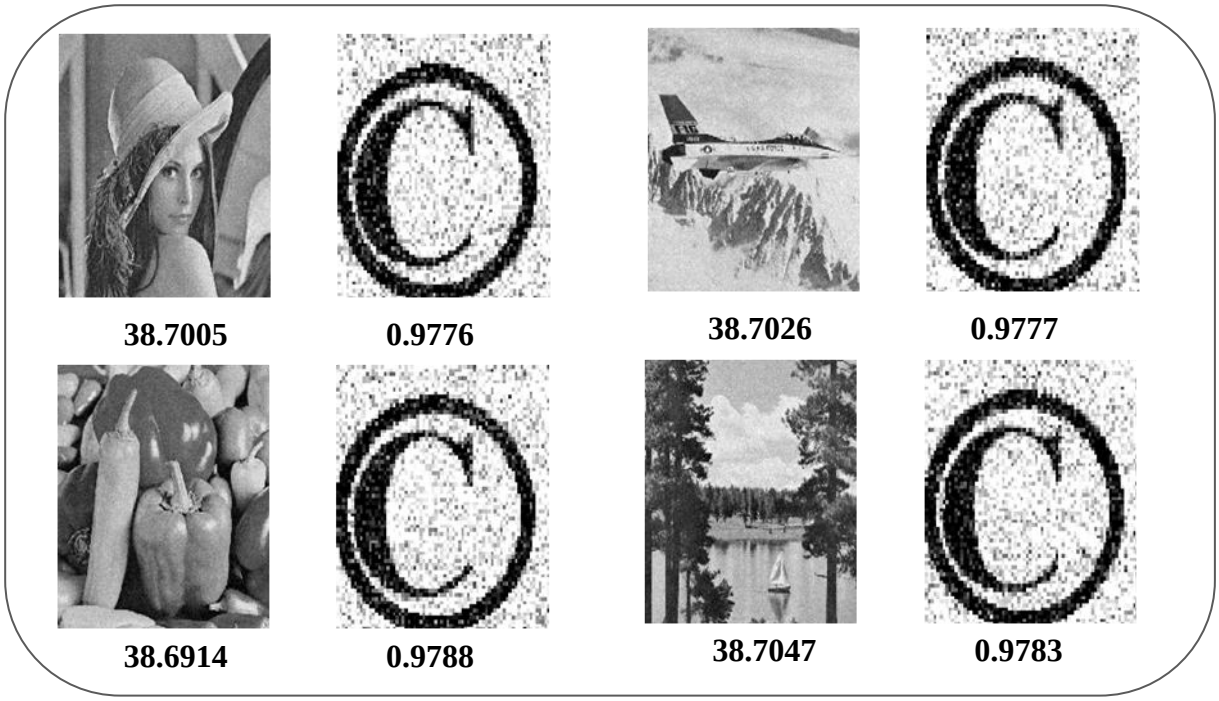


Figure 5. 39 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de bruit Gaussien de variance 0.1%.

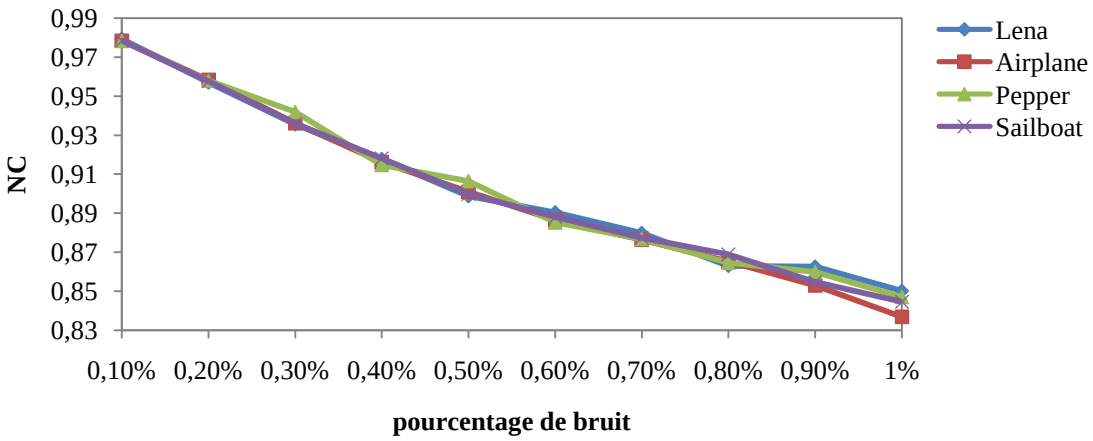


Figure 5. 40 : Robustesse de l'algorithme de tatouage contre l'attaque de bruit Gaussien pour les images Lena, Airplane, Pepper et Sailboat.

Les Figures 5.40 et 5.41 illustrent les valeurs de NC et de PSNR en fonction du bruit Gaussien. Dans la figure 5.40 on remarque que l'algorithme est robuste contre cette attaque jusqu'à la valeur de variance du bruit est égal à 0.4% avec un NC supérieur à 0.91 mais après 0.4% le NC diminue et les courbes de PSNR décroissent entre 39 et 33 décibels.

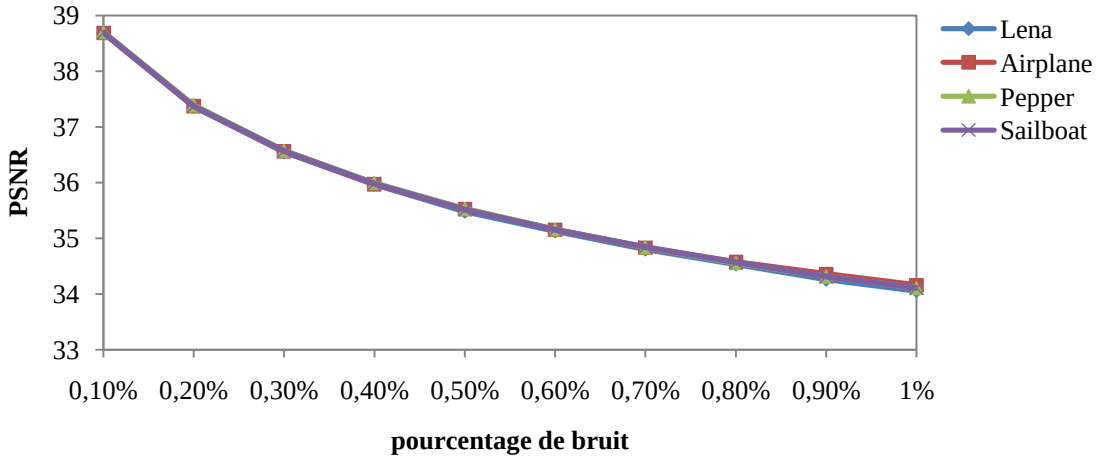


Figure 5. 41 : Valeurs de PSNR pour différentes variations de l'attaque de bruit Gaussien pour les images Lena, Airplane, Pepper et Sailboat.

5.4.2. Attaque de filtrage

- ***Filtre médian***

Sur la figure 5.42 nous présentons le résultat de l'attaque du filtre médian de taille 3×3 pixels contre une image tatouée par l'algorithme proposé.

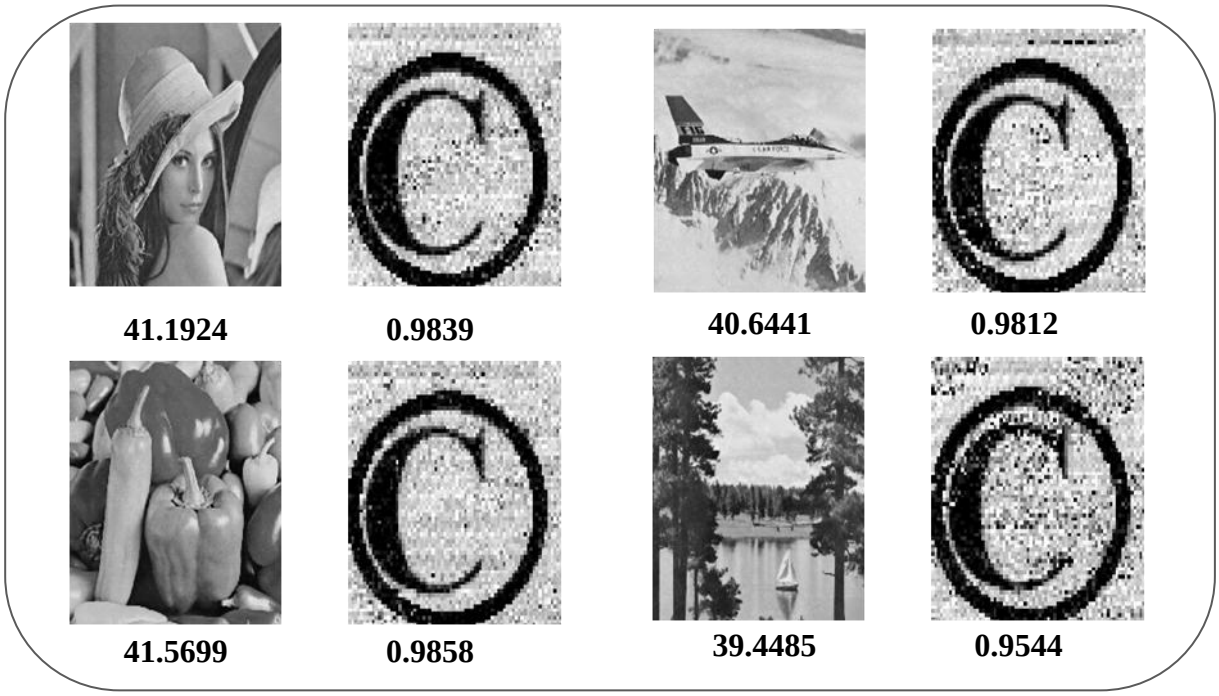


Figure 5. 42 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre médian de taille **3 × 3** pixels.

Nous avons un coefficient d'auto-corrélation supérieur à 0.95 ce qui signifie une ressemblance entre la marque extraite et la marque insérée. Le PSNR aussi enregistre un seuil de 39 dB, donc cet algorithme est encore solide contre cette attaque (Figure 5.42).

- ***Filtre moyen***

Une attaque d'un filtre moyen de taille 3 × 3 est appliquée contre une image tatouée. Les résultats de simulation sont représentés sur la figure 5.43. On peut constater que le facteur d'auto-corrélation et le PSNR sont respectivement de l'ordre de 0.94 et 38 dB.

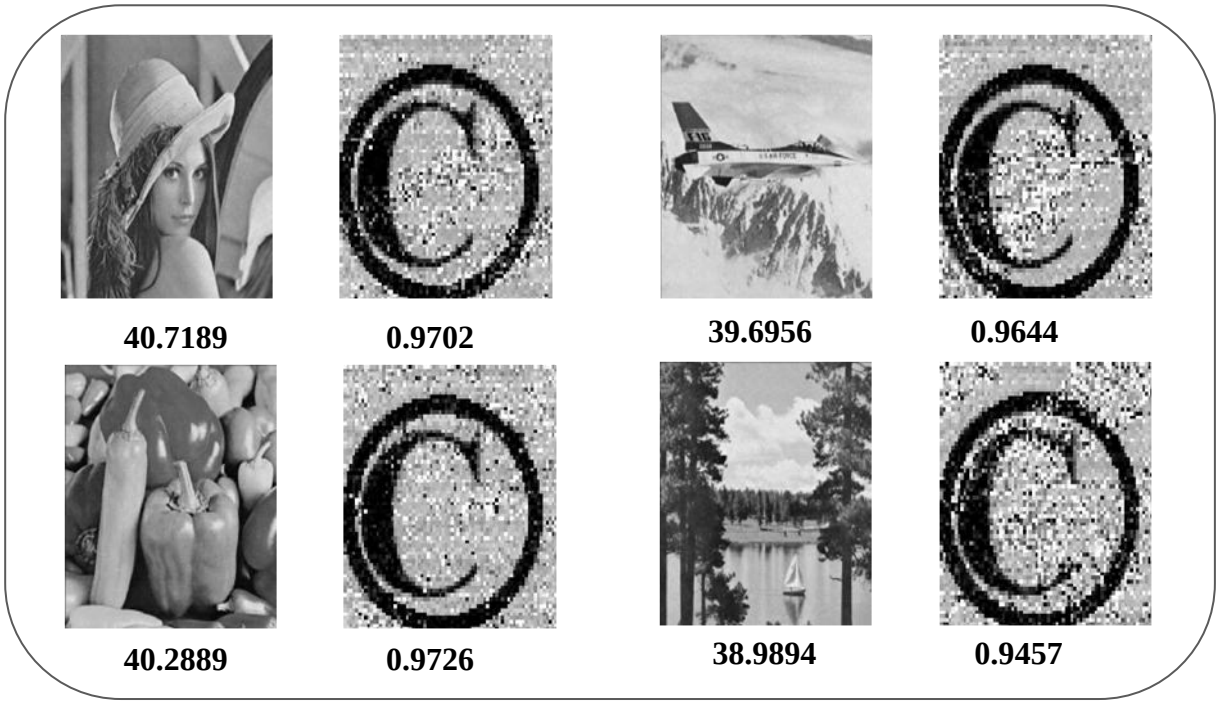


Figure 5. 43 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre moyen de taille **3 × 3** pixels.

- ***Filtre Gaussien***

Nous avons examiné l'algorithme contre l'attaque de filtre Gaussien avec la taille 3 × 3 pixels; et on remarque que la valeur de NC est supérieure à 0.96 avec une bonne qualité de la marque extraite (Figure 5.44). Plusieurs filtres Gaussiens de taille 3 × 3 à 13 × 13 sont employés pour attaquer une image tatouée. Nous avons constaté que le facteur d'auto-corrélation diminue avec l'augmentation de la taille du filtre, à partir de la taille 7 × 7 il se stabilise, voir la figure 5.45. Le PSNR aussi se comporte de la même manière (Figure 5.46). Les résultats obtenus montrent que l'algorithme est robuste contre le filtre Gaussien.

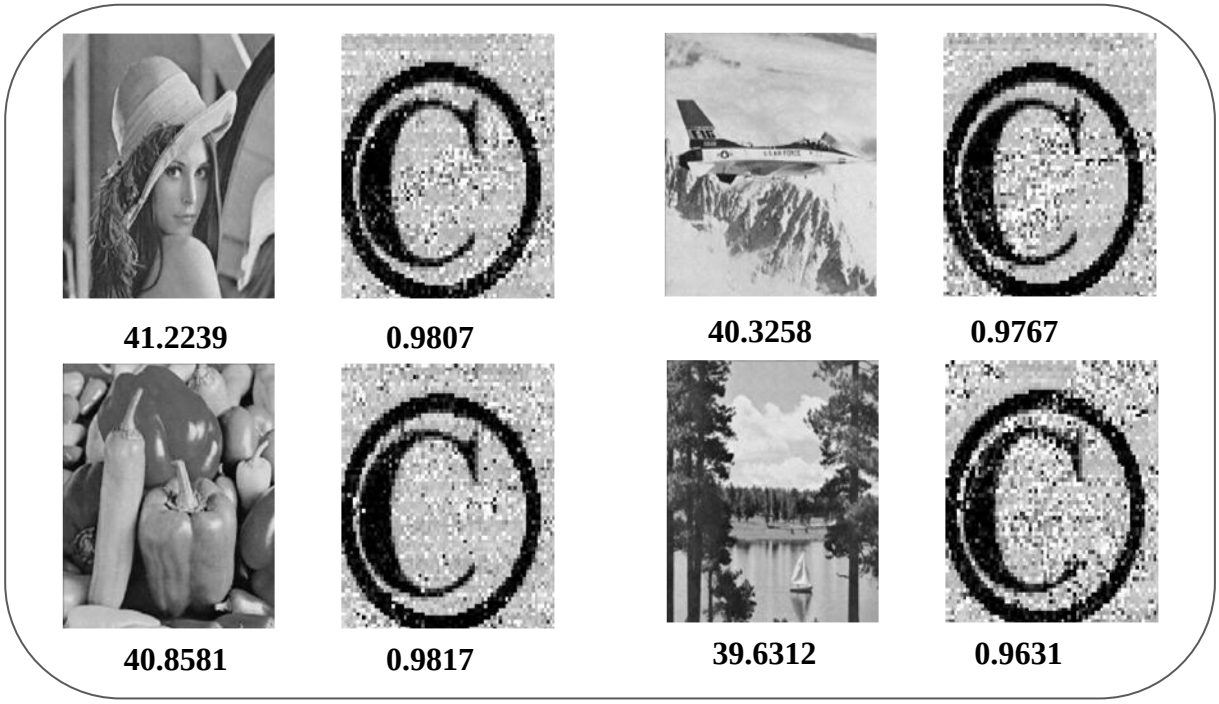


Figure 5. 44 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Gaussien de taille **3 × 3** pixels.

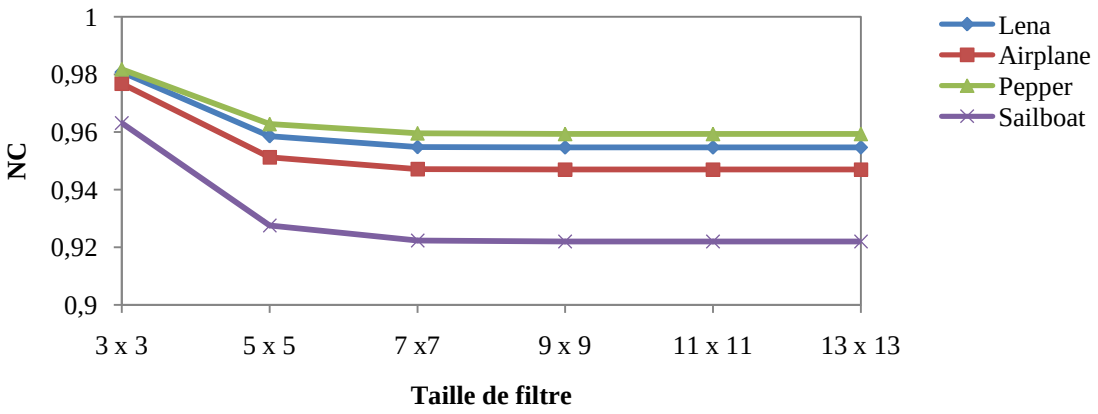


Figure 5. 45 : Robustesse de l'algorithme de tatouage contre l'attaque de filtre Gaussien pour les images Lena, Airplane, Pepper et Sailboat.

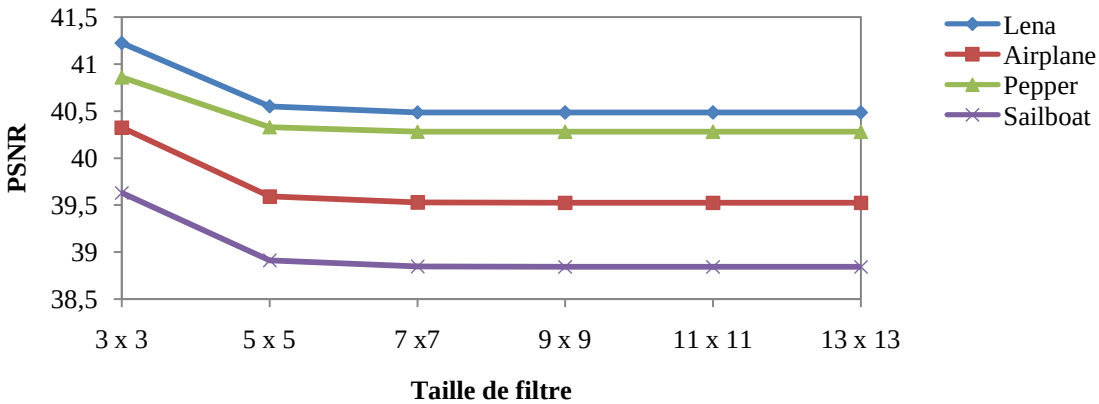


Figure 5. 46 : Valeurs de PSNR pour différentes valeurs de l'attaque de filtre Gaussien pour les images Lena, Airplane, Pepper et Sailboat.

- ***Filtre Sharpen***

Les résultats obtenus après le filtrage de Sharpen de variance 0.8 sont illustrés sur la figure 5.47. La marque bruitée présente un facteur de qualité NC proche de 0.95.

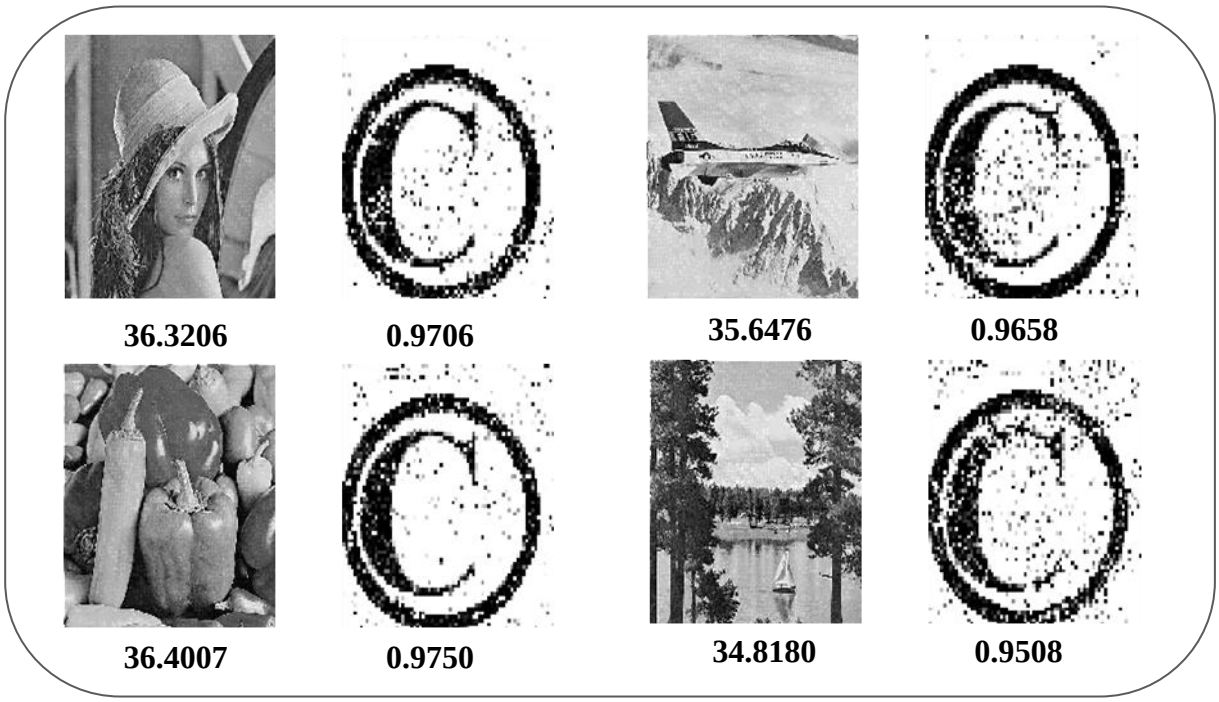


Figure 5. 47 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de filtre Sharpen de valeur 0.8.

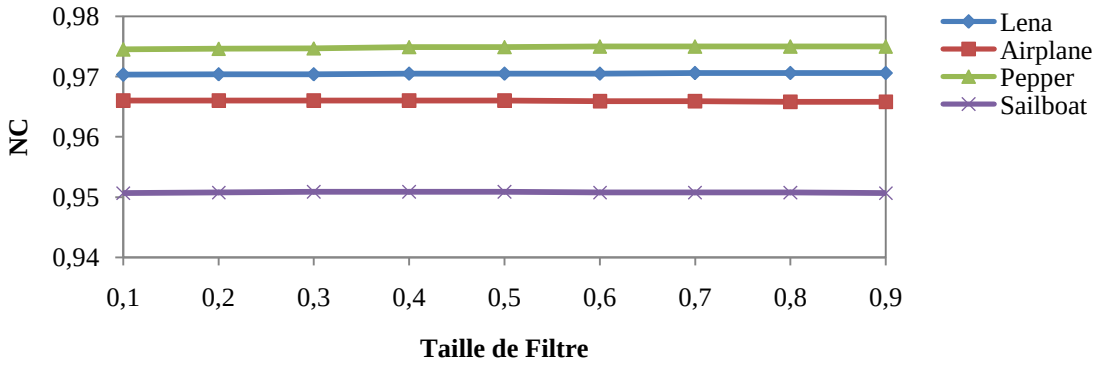


Figure 5. 48 : Robustesse de l'algorithme de tatouage contre l'attaque de filtre Sharpen pour les images Lena, Airplane, Pepper et Sailboat.

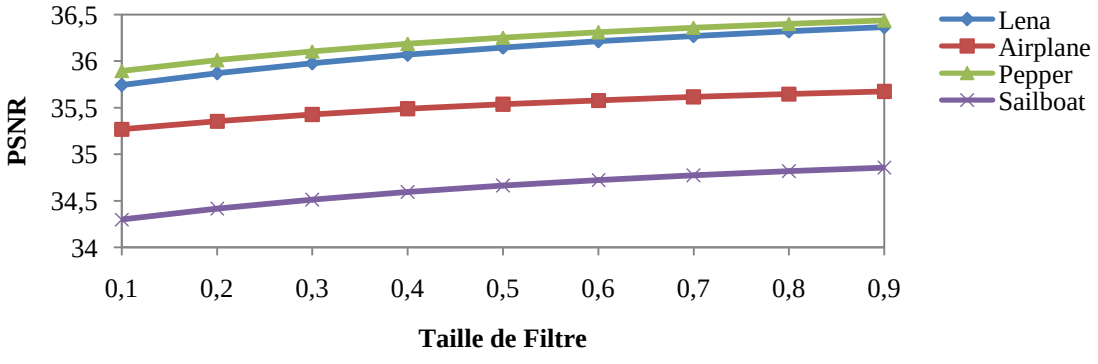


Figure 5. 49 : Valeurs de PSNR pour les différentes tailles de l'attaque de filtre Sharpen pour les images Lena, Airplane, Pepper et Sailboat

Les valeurs de NC dans la figure 5.48 sont constantes quelque soit la valeur de filtre Sharpen, et cela signifie que l'algorithme est robuste contre cet attaque, mais les valeurs de PSNR dans la figure 5.49 croissent entre 34 et 37 décibels.

5.4.3. Attaques géométriques

- ***Rotation***

Une attaque géométrique de rotation de 0.1 degré est appliquée. La marque extraite présente une très bonne qualité visuelle avec un facteur d'auto-corrélation supérieur à 0.99 et un PSNR supérieur à 42 dB. L'algorithme résiste parfaitement à cette attaque.

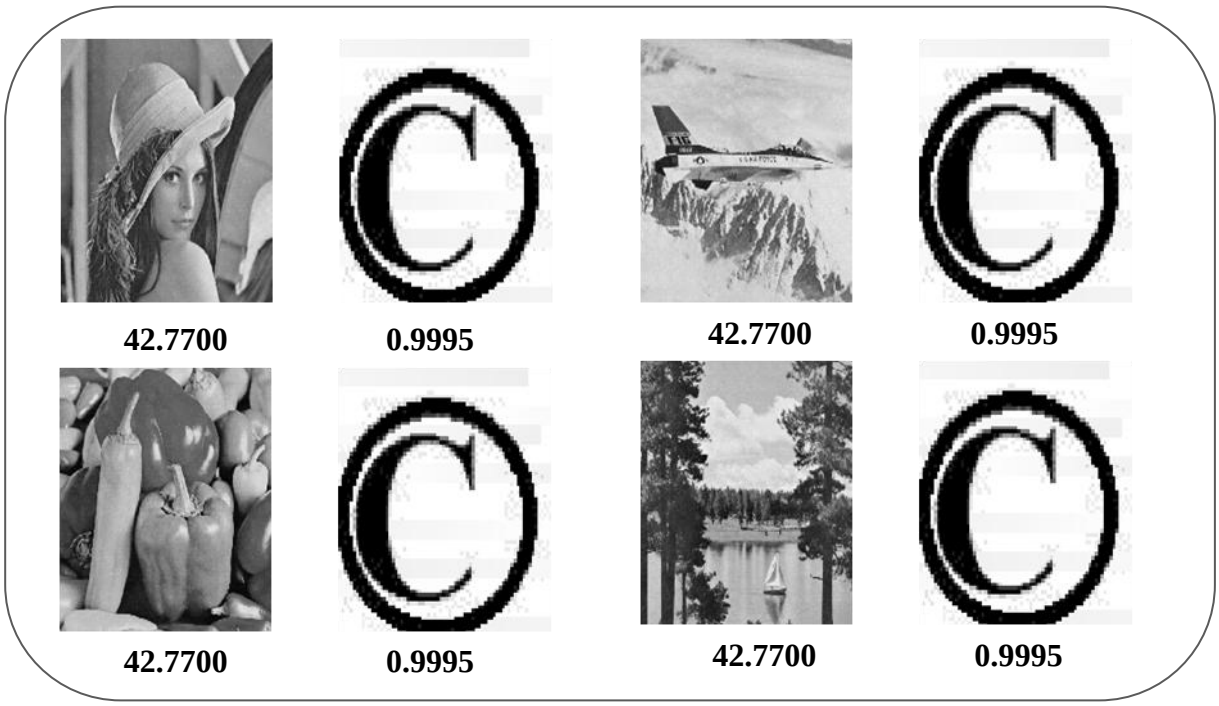


Figure 5. 50 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de rotation de 0.1°.

- ***Redimensionnement***

L'attaque de redimensionnement (zoom) est une attaque géométrique qui consiste à changer la taille de l'image, On teste l'algorithme contre cette attaque avec l'échelle 256×256 pixels, la marque extraite est de très bonne qualité avec un facteur de NC proche de 0.98 (Figure 5.51).

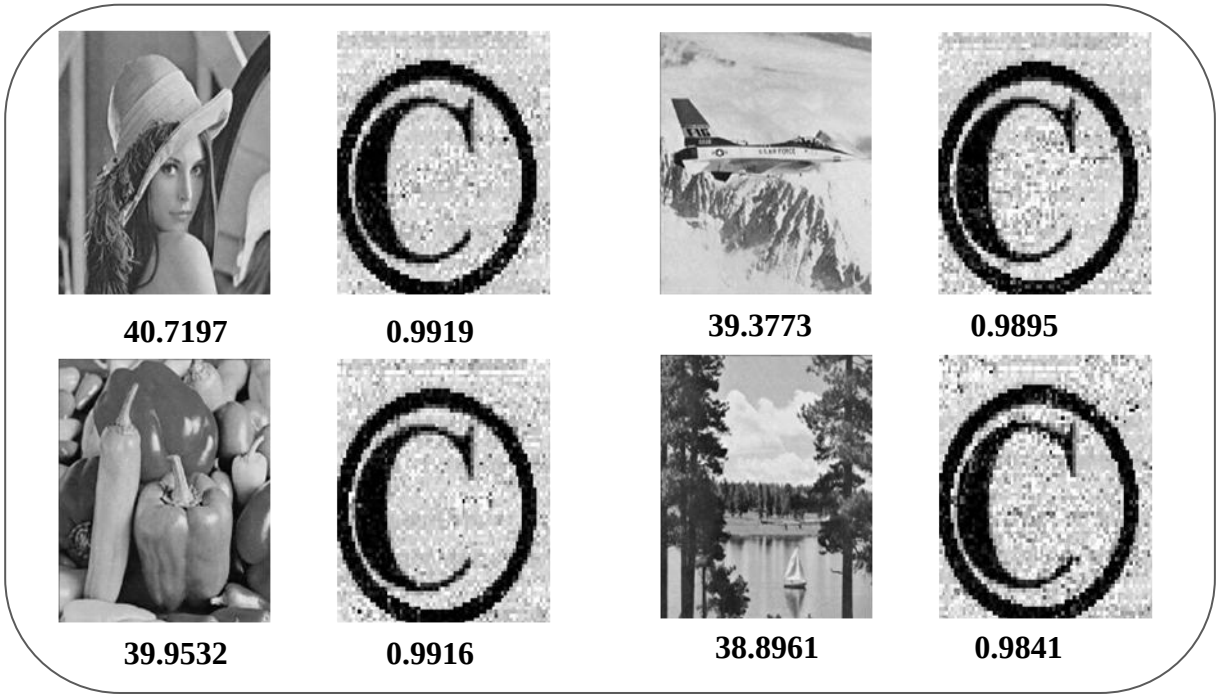


Figure 5. 51 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de zoom de $\mathbf{512 \times 512}$ pixels à $\mathbf{256 \times 256}$ pixels.

5.4.4. Compression JPEG

La compression JPEG est l'une des attaques qui permettent d'effacer la marque, mais dans cet algorithme on remarque que le NC est supérieur à 0.99 pour un facteur de compression de 60% et la marque extraite est de très bonne qualité, (Figure 5.52).

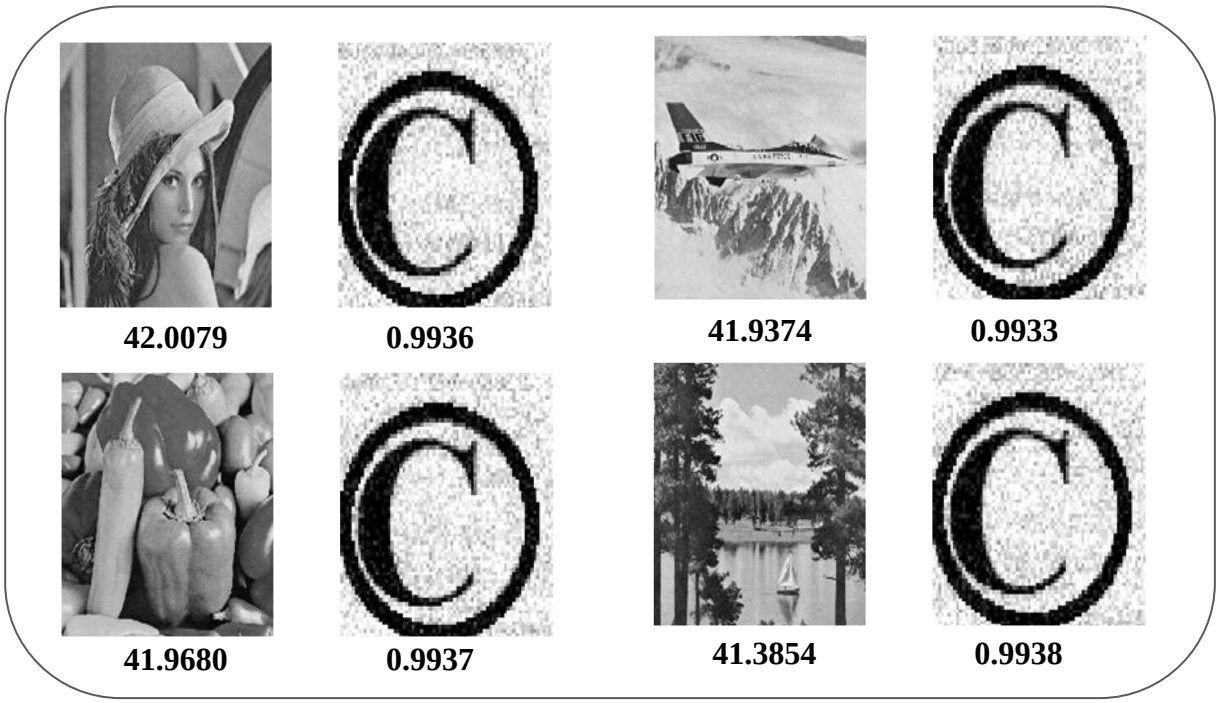


Figure 5. 52 : Résultats de simulation de l'algorithme de tatouage proposé contre l'attaque de compression JPEG de rapport 60%.

Les Figures 5.53 et 5.54 montrent les valeurs de NC et de PSNR en fonction du facteur de compression JPEG. L'algorithme est robuste contre cette attaque et le NC croit jusqu'à 1 si on augmente le facteur de compression, et le PSNR varie entre 37 et 43 décibels.

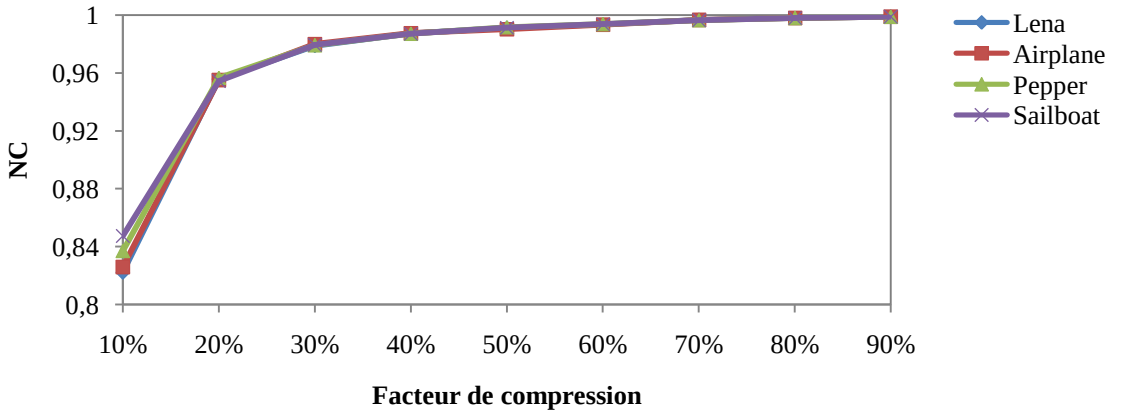


Figure 5. 53 : Robustesse de l'algorithme de tatouage contre la compression JPEG pour les images Lena, Airplane, Pepper et Sailboat.

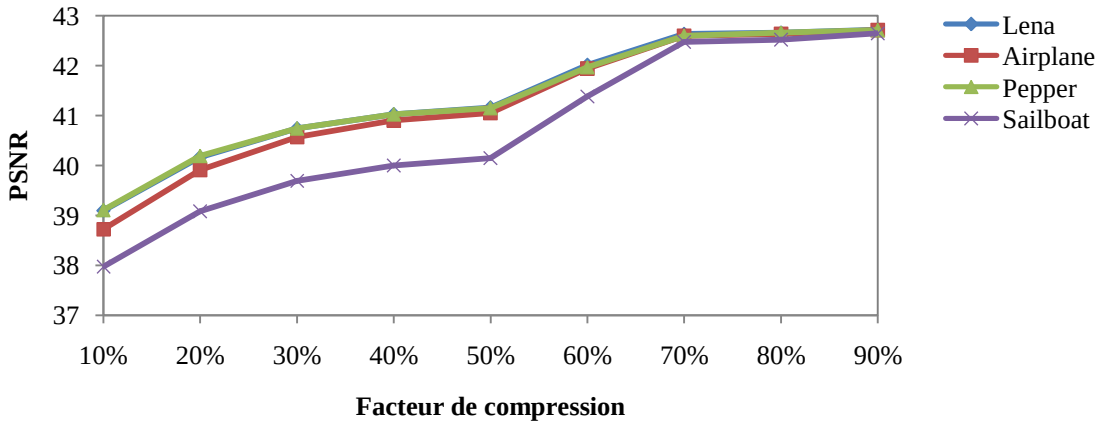


Figure 5. 54 : Valeurs de PSNR pour différents facteurs de l'attaque de compression JPEG pour les images Lena, Airplane, Pepper et Sailboat

5.5. Comparaison des approches

Les approches développées dans cette thèse donnent des très bons résultats de robustesse contre les attaques, cela nous a poussés à faire une comparaison avec des travaux scientifiques existants.

Dans le premier cas, les auteurs ont utilisé dans leur approche la transformée DWT-SVD et DE [87]. Ce qui favorise vraiment une comparaison entre les résultats des travaux. Les résultats obtenus dans le Tableau 5.9 confirment bien l'efficacité de l'utilisation de l'étage de quantification de la compression JPEG 2000 dans la première approche, arrivent à détecter la marque complète similaire à la marque originale insérée.

Dans le deuxième cas, les auteurs ont utilisé dans leur approche la transformée DWT-SVD et le système visuel humaine HVS [92], ce qui nous a permet de comparer entre les résultats des travaux. Les résultats obtenus dans le Tableau 5.10 confirment la robustesse de notre algorithme où nous choisissions les deux composants HL3 et HH3 de la transformée DWT

pour insérer la marque, la marque extraite et la marque originale sont similaire pour chaque attaque.

Dans le troisième cas, les auteurs ont utilisé dans leur approche la transformée DWT-SVD et le système visuel humaine HVS [92], les résultats obtenus dans la Figure 5.55 confirment la robustesse et l'efficacité de notre algorithme où nous choisissions la composant LL de la transformée DWT pour insérer la marque avec l'utilisation de TF et PMF [93], la marque extraite et la marque originale sont similaire pour chaque attaque.

attaque	Algorithme proposée dans [87]				Approche N°1 [95]			
	Lena	Aireplane	Pepper	Sailboat	Lena	Aireplane	Pepper	Sailboat
SP 1%	0.8322	0.8212	0.8366	0.8244	0.9425	0.9410	0.9390	0.9405
BG 1%	0.6391	0.6420	0.6381	0.6389	0.9427	0.9414	0.9385	0.9404
FM 7*7	0.7619	0.6767	0.8225	0.6019	0.9467	0.9424	0.9407	0.9449
FM 7*7	0.6694	0.5783	0.6945	0.5446	0.9478	0.9433	0.9433	0.9467
FG 9*9	0.9221	0.8970	0.9343	0.8663	0.9449	0.9410	0.9405	0.9426
SH 0.8	0.8085	0.7638	0.8270	0.7008	0.9402	0.9399	0.9372	0.9376
RO 1°	0.8252	0.8020	0.8291	0.8465	0.9431	0.9413	0.9391	0.9408
RE 256*256	0.9740	0.9658	0.9767	0.9516	0.9439	0.9420	0.9399	0.9414
C-JPEG 60%	0.9892	0.9889	0.9888	0.9852	0.9431	0.9418	0.9496	0.9408

Tableau 5. 9 : La Comparaisons des valeurs de NC après les différentes attaques.

Attaque	Algorithme proposée dans [92]				Approche N°2 [96]			
	Lena	Aireplane	Pepper	Sailboat	Lena	Aireplane	Pepper	Sailboat
SP 1%	0.8474	0.8038	0.7350	0.7943	0.9901	0.0.9806	0.9956	0.9950
BG 1%	0.6273	0.6291	0.6793	0.6651	0.9713	0.9710	0.9807	0.9803
FM 7*7	0.8729	0.9888	0.9145	0.8723	0.9976	0.9986	0.9978	0.9755
FM 3*3	0.8506	0.8362	0.8228	0.8661	0.9907	0.9806	0.9974	0.9986
FG 3*3	0.9015	0.9236	0.9045	0.9067	0.9904	0.9813	0.9973	0.9981
SH 0.8	0.9595	0.8145	0.8684	0.8085	0.9715	0.9765	0.9954	0.9793
RO 1°	0.9079	0.8826	0.8993	0.8778	0.8831	0.9333	0.9438	0.9103
C-JPEG 60%	0.9785	0.9237	0.9438	0.9436	0.9890	0.9832	0.9967	0.9953

Tableau 5. 10 : La Comparaisons des valeurs de NC après les différentes attaques.

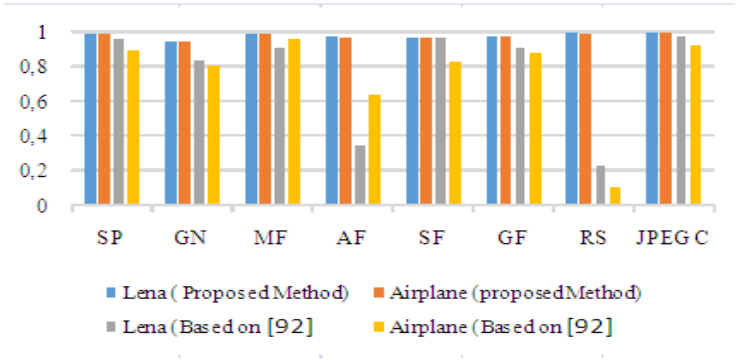


Figure 5. 55 : La Comparaisons des valeurs de NC après les différentes attaques.

5.6. Conclusion

Dans ce chapitre nous avons examiné l'efficacité de trois nouveaux algorithmes de tatouage de l'image. La méthode de test est basée sur une phase d'insertion de la marque en utilisant l'algorithme proposé, une attaque sur l'image tatouée après une phase d'extraction de la marque. Les résultats obtenus en termes de facteur d'auto-corrélation (NC) et du rapport signal sur bruit (PSNR) démontrent que les algorithmes proposés sont robustes et efficaces contre les attaques conventionnelles en traitement de l'image. Ce chapitre représente le fruit de notre étude dont un algorithme a fait l'objet d'une publication internationale.

CONCLUSION GÉNÉRALE

Dans cette thèse, nous avons abordé la problématique de copyright des droits d'auteurs dans le domaine numérique, problème qui a pris de plus en plus d'importance depuis l'échange de multimédia à travers l'Internet. Le tatouage d'image numérique est une technique permettant d'assurer la sécurité à travers l'insertion d'une information à l'image originale pour répondre à la propriété intellectuelle des œuvres numériques.

Nous avons abordé ce travail par un état de l'art sur les algorithmes récents de tatouage d'image. Ces schémas de tatouage actuels sont divisés sur deux domaines ; le domaine spatial et le domaine fréquentiel qui tentent tous à assurer un tatouage robuste et imperceptible. Cependant, les algorithmes de tatouages ne répondent pas aux exigences dédiées au tatouage, alors les chercheurs et les concepteurs ont développé des algorithmes hybrides qui sont à base d'une combinaison de transformées afin d'avoir plus de robustesse et donc augmenter le taux d'imperceptibilité.

Dans la première partie nous avons approfondi dans les outils mathématiques et les transformées fréquentielles qui sont utilisé dans cette thèse, l'optimisation DE utilisé permet d'améliorer les résultats surtout en matière d'imperceptibilité et de robustesse. Le masquage de texture et le HVS ont été montré; la marque est incrustée dans des pixels prédéfinis de l'image où les caractéristiques du système visuel humain ont été exploitées afin de trouver une bonne imperceptibilité.

Dans la deuxième partie nous avons dévoilé deux approches, ces approches sont basées sur l'amélioration des schémas de tatouage DWT-SVD-DE dans l'algorithme de compression JPEG 2000 et DWT-HVS. Pour la première approche nous avons combiné DWT-SVD avec DE dont l'algorithme DWT est utilisé dans l'étape de compression ainsi nous avons inséré la marque par le biais de l'algorithme SVD où l'algorithme DE nous a permis d'insérer la marque. Dans la deuxième approche la DWT est employée comme transformé pour extraire les sous-bandes, la SVD est appliquée par la suite sur deux bandes afin d'insérer la marque, enfin la HVS est exploitée pour calculer la clé. Ces approches ont été testées contre plusieurs attaques, les résultats obtenus montrent l'efficacité et la robustesse de celles-ci. Les valeurs de PSNR et NC sont les témoins de la puissance des approches présentées surtout en termes de l'imperceptibilité.

Le fruit de ce travail est symbolisé par une nouvelle approche qui traite le tatouage d'image. Elle est basée sur la transformée DWT et PMF; la transformé DWT permet de diviser l'image en quatre sous-bandes dont nous avons choisi la première sous-bande LL1 pour appliquer une fonction de transfert (TF) afin de changer l'intensité des pixels. Par la suite l'emplacement des pixels à été changé à l'aide de la fonction de mouvement de pixel (PMF) qu'on a développé lors de cette étude. La marque est insérée à la fin dans la sous-bande LL1 résultante. Pour confirmer notre nouvelle méthode de tatouage d'image, plusieurs images de tests ont été attaquées par le bruitage, filtrage, compression et attaques géométriques. Les résultats acquis confirment la robustesse de notre nouvelle méthode, en effet, la valeur de NC est proche de 1 pour toute les images de tests ce qui illustre la robustesse de la méthode proposée, ainsi le PSNR est supérieur à 42 dB ce qui montre l'imperceptibilité de l'algorithme proposé.

Comme perspective, une implémentation par processeur de signal numérique (DSP) de notre méthode de tatouage est nécessaire pour prouver la précision et la rapidité du système en temps réel.

RÉFÉRENCES

[1] A.Z.Tirkel, G.A.Rankin, R.M. van Schyndel, W.J.Ho, N. R . A . Mee, C. F. Osborne, "Electronic Water mark", In DICTA, pp. 666-672, 1993.

[2] R. Schyndel, A. Tirkel, C. Osborne, "A Digital Watermark". Conference: Image Processing, Proceedings. ICIP-94., IEEE International Conference, Vol. 2, pp. 86-90. November 1994.

[3] J. Hussein, "Spatial Domain Watermarking Scheme for Colored Images Based on LogAverage Luminance". Journal of Computing, January, vol. 2, no. 1, pp. 100-103, 2010.

[4] J. Hernández, F. Pérez-González, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images". IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, pp. 510-524, 1998.

[5] P. Reddy, M. Prasad, D. Rao, "Robust Digital Watermarking of Images using Wavelets". International Journal of Computer and Electrical Engineering, vol. 1, no. 2, pp. 111-116, 2009.

[6] S. Lin, S. Shie, J. Guo, "Improving the Robustness of DCT-based Image Watermarking Against JPEG Compression". Computer Standards and Interfaces, vol. 32, no. 1-2, pp. 54-60, 2010.

[7] Z. Dawei, C. Guanrong, L. Wenbo, "A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm". Chaos, Solitons and Fractals, vol. 22, no. 1, pp. 47-54, 2004.

[8] X. Qi, J. Qi, "A Robust Content-Based Digital Image Watermarking Scheme". Signal Processing, vol. 87, no. 6, pp. 1264-1280, 2007.

[9] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking". Journal of Computer Science, vol. 3, no. 9, pp. 740-746, 2007.

[10] C. Yin, L. Li, A. Lv, Q. Li, "Color Image Watermarking Algorithm Based on DWT-SVD". IEEE International Conference on Automation and Logistics, pp. 2607-2611, 2007.

[11] E. Ganic, A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding Data in All Frequencies". Proceedings of the Multimedia and Security Workshop on Multimedia and Security - MM&Sec '04, pp. 166-174, 2004.

[12] W. Zheng, S. Mo, X. Jin, Y. Qu, F. Deng, J. Shuai, S. Long, "Robust and high capacity watermarking for image based on DWT-SVD and CNN". 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 1233-1237, 2018.

[13] G. E. Hinton, “To recognize shapes, first learn to generate images”. Progress in Brain Research, Vol. 165, no. 6, pp. 535-547, 2007

[14] J. Liu, J. Huang, Y. Luo, L. Cao, S. Yang, D. Wei, R. Zhou, “An optimized image watermarking method based on HD and SVD in DWT domain”. IEEE Access, Vol. 7, pp. 80849-80860, 2019.

[15] A. M. Cheema, S. M. Adnan, Z. Mehmood, “A Novel Optimized Semi-Blind Scheme for Color Image Watermarking”. IEEE Access, Vol. 8, pp. 169525-169547, 2020.

[16] R. Hu and S. Xiang. “Cover-Lossless Robust Image Watermarking Against Geometric Deformations”. IEEE Transactions On Image Processing, Vol. 30, pp. 318-331. 2021.

[17] K. M. Hosny, M. M. Darwish AND M. M. Fouda. “Robust Color Images Watermarking Using New Fractional-Order Exponent Moments”. IEEE ACCESS, Vol.9, pp. 47425-47435, 2021.

[18] Séverine Dubuisson, “Introduction au traitement d’images”. Fondements du Traitement d’Images, novembre, pp. 1-64, 2006.

[19] Maïtine Bergounioux, “Quelques méthodes mathématiques pour le traitement d’image”. Cours M2 - Université d’Orléans, pp.1-110, 2008.

[20] cour de Raphaël Isdant, “ Traitement numérique de l'image ”, pp. 1-18, 2009.

[21] http://www.imageprocessingplace.com/root_files_V3/image_databases.htm

[22] Traitement d'images, **https://fr.wikipedia.org/wiki/Traitement_d%27images**

[23] Calibration de caméra,

https://fr.wikipedia.org/wiki/Calibration_de_cam%C3%A9ra.

[24] Hervé Mathieu, “ La chaîne de l’acquisition d’images ”. pp. 1-82, Janvier 2009.

[25] G. Dauphin, “ Notes de cours Traitement d’images numériques ”, 2015.

[26] Bendaoud Mohammed Habib, “Développement de méthodes d’extraction de contours sur des images à niveaux de gris”. Thèse Doctorat, pp.1-108, 2017.

[27] Bruit numérique, http://fr.m.wikipedia.org/wiki/bruit_numérique

[28] Sarah Ghandour, “Segmentation d'images couleurs par morphologie mathématique: application aux images microscopiques”, Thèse doctorat, pp.1-128, 2010.

[29] Histogramme (imagerie numérique),

https://fr.wikipedia.org/wiki/Histogramme_(imagerie_num%C3%A9rique)

[30] Elise Arnaud, Edmond Boyer, “ Analyse d’images – introduction”. Université Joseph Fourier / INRIA Rhône-Alpes. pp. 1-30.

[31] Contraste, https://fr.wikipedia.org/wiki/Contraste, Système intégres de protection et de surveillance,

[32] https://www.sysmilan.com/wp-content/uploads/2018/06/la_compression.pdf

[33] M. W. Marcellin, M. J. Gormish, A. Bilgin, M. P. Boliek, "An overview of JPEG-2000", Data Compression Conference Proceedings, pp. 523-541, March 2000.

[34] D. L. Gall, A. Tabatabai, "Sub-band coding of images using symmetric short kernel filters and arithmetic coding techniques", in International conference on Acoustic, speech and signal processing, pp. 761-764, 1988.

[35] I. Daubechies, "Ten Lectures on Wavelets", SIAM, 1992.

[36] I. Daubechies, "The wavelet transform, time frequency localization and signal analysis" IEEE Transactions on information theory, vol. 36, no. 5, pp.442-487, 1990.

[37] M. Ghanbari, "Standard Codecs: Image Compression to Advanced Video Coding". Book, IET Telecommunication Series, 2003.

[38] ISO et IEC. "Information technology - Digital compression and coding of continuous-tone still images requirements and guidelines". ISO 10918-1, International Organization for Standardization / International Electrotechnical Commission, Geneva, Switzerland, 2004.

[39] N. Ahmed, T. Natarajan, K.R. Rao, "Discrete Cosine Transform". IEEE Transactions on Computers, vol. C-23, no. 1, pp. 90-93, Jan 1974.

[40] JPEG: https://fr.wikipedia.org/wiki/JPEG.

[41] M.L. Miller, I.J. Cox et J.A. Bloom. "Informed embedding: exploiting image and detector information during watermark insertion". In IEEE International Conference on Image Processing, Citeseer, volume 3, pp. 1-4, 2000.

[42] J.J. Eggers, B. Girod. "Blind watermarking applied to image authentication". In IEEE International Conference on Acoustics Speech and Signal Processing, Citeseer, volume 3. pp.1977-1980, 2001.

[43] J. Ye, G. Tan, "An Improved Digital Watermarking Algorithm for Meaningful Image". International Conference on Computer Science and Software Engineering, vol. 2, pp. 822-825, 2008.

[44] S. Radharan, M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication". International Journal of Computer Applications, vol. 4, pp. 24-32, June 2010.

[45] L. G. Baisa, R.R. Manthalkar, "an overview of transform domain robust digital image watermarking algorithm". Journal of emerging trends in computing and information science, Vol. 2, no 1. pp. 37-42, 2011.

[46] W. Bender, D. Gruhl, N. Morimoto, A. LU. “Techniques for data hiding”. IBM systems journal, Vol. 35, No 3-4, pp. 313-336, 1996.

[47] M. Kutter, F. Jordan, F. Bossen, “Digital Watermarking of Color Images using Amplitude Modulation”. Journal of Electronic Imaging, Vol. 7, No 2. pp. 326-332, 1998.

[48] J. Brassil, S. Low, N. Maxemchuk, L.O' Gorman, “Electronic marking and identification techniques to discourage document copying”. IEEE Journal on Selected Areas in Communications, pp. 1278-1287, 1994.

[49] M. Barni, F. Barolini, V. Cappellini, A. Piva, “A DCT- domain system for robust image watermarking”. Signal processing, Publisher Elsevier North-Holland, Vol. 66, No 3, pp. 375-372, 1998.

[50] J.P. DUBUS, “Analyse Multirésolution Et Psychovisuelle”. technique de l’ingénieur Mesures et contrôle, Vol RE1, pp. 1-21, 1998.

[51] X. Xia, C. Boncelet, G. Arce. “A Multiresolution Watermark for Digital Images”. In Processing IEEE International Conference on Image Processing, Vol. 3. pp. 548-551, 1997.

[52] F. Hartung, B. Girod. “Watermarking of uncompressed and compressed video”. Signal Processing, Vol. 66, No 3, pp. 283-333, 1998.

[53] L. Cox, J. Killian, T. Leighton, T. Shamoon. “Secure spread spectrum watermarking for multimedia”. IEEE Transactions on Image Proceessing, Vol. 6, No 12, pp.1673-1687, 1997.

[54] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva. “A dwt-based technique for spatiofrequency masking of digital signatures”. Security and Watermarking of Multimedia Contents (Electronic Imaging'99), Vol. 3657 of Proceedings of SPIE. pp. 31-39, 1999.

[55] B. Chen, G. Wornell. “An information theoretic approach to the design of robust digital watermarking systems”. In International Conference on Acoustic, Speech and Signal Processing (ICASSP), pp. 2061-2064, 1999.

[56] D. Coltuc, P. Bolon. «Watermarking by histogram specification». Security and Watermarking of Multimedia Contents (Electronic Imaging '99), Vol. 3657 of Proceedings of SPIE, San Jose, California USA, pp. 252-263, Jan 1999.

[57] M.J.J. Maes, C.W.A.M. Overveld. “Digital watermarking by geometric warping”. ln IEEE- ICIP'98, Vol. 2, Chicago (IL, US), pp. 424-429, Oct 1998.

[58] E. Koch, J. Zhao. “Embedding robust labels into images for copyright protection”. Know Right '95: Proceedings of the conference on Intellectual property rights and new technologies, pp. 242-251, January 1995.

[59] D. Kundur, D. Hatzinakos. “Digital watermarking using multiresolution wavelet decomposition”. In IEEE ICASSP'98, Vol. 5, Seattle (USA). pp. 2659-2662, May 1998.

[60] S. Walton. “Information Authentication for a Slippery New Age”. Dr. Dobbs Journal, Vol. 20, No 4, pp. 18-26, Apr 1995.

[61] J. Fridrich, M. Goljan. “Protection of Digital Images using Self Embedding”. The Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, pp.1-6, 1999.

[62] C.Y. Lin, S.F. Chang. “Semi-Fragile Watermarking for Authenticating JPEG Visual Content”. SPIE International Conference on Security and Watermarking of Multimedia Contents II, Vol. 3971, No 13, San Jose, USA, pp.140-151, Jan 2000.

[63] C. Rey. “Tatouage d’image : Gain en robustesse et intégrité des images”. Thèse Doctorat de l’Université d’Avignon et des Pays de Vaucluse, 2003.

[64] Bouderbala Ahmed, “Implémentation d’un algorithme de tatouage Vidéo robuste dans Le domaine compressé”. Mémoire de Magistere. pp. 1-68, 2008.

[65] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun. “Attack modeling: towards a second generation watermarking benchmark”. IEEE Transactions on Signal Processing, no 81, pp. 1177-1214, 2001.

[66] C.J. Van d. B. Lambrecht, J.E. Farrell. “Perceptual quality metric for digitally coded color images”. Proceedings of EUSIPCO, Trieste, Italy, pp. 1175-1178, Sep. 1996.

[67] A.B. Watson. “DCT quantization matrices visually optimized for individual images. Human Vision”, Visual Processing and Digital Display IV, Bernice E. Rogowitz, Editor, pp.13-14, 1993.

[68] Rabia Riad. “Tatouage robuste d’images imprimées”. Thèse doctorat, Université d'Orléans 2015.

[69] 28.02.2011 helene.boye.roche.free.fr/epita/FG/exposes/28-2.pdf

[70] M. Kutter, S. Voloshynovskiy, A. Herrigel. “Watermark copy attack”. Proceedings of SPIE, Security and Watermarking of Multimedia Contents II, vol. 3971, pp. 371-380, 9 May 2000.

[71] H. B. Razafindradina, P. A. Randriamitantsoa, “Tatouage robuste et aveugle dans le domaine des valeurs singulières”, Revue arXiv preprint arXiv:1001.3928, pp. 1-15, Jan 2010.

[72] S. Mallat, “A theory for multiresolution signal decomposition: The wavelet representation”. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 11, No 7, pp. 674-693. Jul 1989.

[73] J.W. Cooley and J.W. Tukey, "An algorithm for machine computation of complex Fourier series". Mathimatics of Computation, Vol. 9, pp. 297-301, 1965.

[74] P. Duhamel and H. Hollmann, "Split radix FFT algorithm". Electronics. Letters, Vol. 20, No. 1, pp. 14-16. January 1984.

[75] S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, "A general class of split-radix FFT algorithms for the computation of the DFT of length-2^m". IEEE Transaction Signal Processing, Vol. 55, No. 8. pp. 4127-4138. August 2007.

[76] S.-C. Pei, W.-L. Hsue, "The multiple-parameter discrete fractional Fourier transform". IEEE Signal Processing Letters, Vol. 13, No. 6. pp. 329-332. June 2006.

[77] J. M. Vilardy, J. E. Calderon, C. O. Torres, and L. Mattos, "Digital images phase encryption using fractional Fourier transform". Proceedings IEEE Conference. Electronics, Robotics and Automotive Mechanics, Vol. 1, pp.15-18, September 2006.

[78] S. Bouguezel, M.O. Ahmad, M.N.S. Swamy, "New Parametric Discrete Fourier and Hartley Transforms, and Algorithms for Fast Computation". IEEE Transactions Circuits and Syst. I, Regular Papers, Vol. 58, No.03, pp. 562-575. March 2011.

[79] J. Guo, Z. Liu, and S. Liu, "Watermarking based on discrete fractional random transform". Optics Communications, Vol. 272, No. 2, pp. 344-348, April 2007.

[80] S. Bouguezel, M. O. Ahmad, M. N. S. Swamy, "An efficient split-radix FHT algorithm". International Symposium on Circuits and Systems (ISCA S), Vol. 3, pp. 565-568, May 2004.

[81] J. Cheng, F. Zhang, K. Yu, and J. Ma, "The Dynamic and Double Encryption System Based on Two-Dimensional Image". International Conference on Computational Intelligence and Security, pp. 458-462, 2009.

[82] F. Liu, K. Han, & C. Z. Wang. "A novel blind watermark algorithm based On SVD and DCT". IEEE International Conference on Intelligent Computing and Intelligent Systems, 2009.

[83] L. Wu, W. Deng, J. Zhang, D. He, "Arnold transformation algorithm and anti Arnold transformation algorithm". Proc. of 1st International Conference on Information Science and Engineering (ICISE2009). pp. 1164-1167, 2009.

[84] M. Ali, C. W. Ahn, M. Pant. "A robust image watermarking technique using SVD and differential evolution in DCT domain". Optik vol. 125, pp. 428- 434, 2014.

[85] R. Storn, K. Price, "Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces". J. Global Optimiz. 11(4), pp. 341-359, 1997.

[86] M. Ali, C.W. Ahn, M. Pant. "An Optimized watermarking Technique Based on DE in DWT-SVD Domain, Optimized Watermarking Technique". IEEE Symposium on Differential Evolution (SDE), pp.99-104, 2013.

[87] M. Ali, C. W. Ahn. "An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain". Signal Processing, vol. 94 pp. 545-556, 2014.

[88] H. Qi, D. Zheng, J. Zhao, "Human visual system based adaptive digital image watermarking". Int. Journal of Signal Processing, Vol. 88, Issue. 1, pp. 174-188, January 2008.

[89] K. Mahmoud, S.t Datta, J. Flint, "Frequency domain watermarking: An Overview". Int. Arab Journal of Information Technology, vol. 2, no. 1, pp. 33-47, January 2005.

[90] F. Drira, F. Denis, A. Baskurt, "Image watermarking technique based on the steerable pyramid transform". Proc. of wavelet application in industrial processing II, vol. 5607, pp. 165-176, November 2004.

[91] L. Z. Wing, "Fuzzy rule base and fuzzy inference engine". In A course in fuzzy systems and Control, 1st ed: Prentice Hall, pp. 90-104, 1997.

[92] M. Imran, A. Ghafoor, M. M. Riaz, "Adaptive watermarking technique based on human visual system and fuzzy inference system". IEEE International Symposium on Circuits and Systems (ISCAS2013), pp.2816-2819, 2013.

[93] R. Souadek, N.E. Boukezzoula; "New Image Watermarking Algorithm Based on DWT and Pixel Movement Function PMF".The International Arab Journal of Information Technology, Vol. 17, No. 1. pp. 1-7, January 2020.

[94] J. Mannos, D. Sakrison, "The Effects of A Visual Fidelity Criterion on The Encoding of Images". IEEE Transactions on Information Theory, vol. 20, no. 4, pp. 525-536, 1974.

[95] R. Souadek, N.E. Boukezzoula, "A robust watermarking scheme using a SVD technique and Differential Evolution in the algorithm of compression JPEG 2000". 3rdThe International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI'16), Annaba, Algeria, 2016.

[96] R. Souadek , N.E. Boukezzoula, N. Guellil, "Watermarking image based on DWT and SVD domain in Human Visual System". International Conference on Technological Advances in Electrical Engineering (ICTAEE'16), Sakikda, Algeria, 2016.

الملخص :

في الوقت الحاضر، أصبحت قضية حقوق النشر والخصوصية تحديًا مقلقًا. استخد ام تقنية معروفة باسم الوشم الرقمي للصور التي تستخدم الخوارزميات الرياضية لتلبية هذا المطلب، والذي يجب أن يتحقق بتقدير الشروط الثلاثة: القوة، الإخفاء والقدرة. يقترح هذا العمل بداية الطريقة الجديدة التي تهدف إلى تحسين أداء الخوارزميات المنشورة مؤخرًا . في الطريقة الأولى، تعتمد خوارزمية الوشم الرقمي على ضغط JPEG 2000 وتقنية SVD لإدخال الوشم ، لزيادة الأمان وتحسين متانة الخوارزمية التي استخدمناها بتقنية DE من أجل حساب المفتاح. بالنسبة للطريقة الثانية، تعتمد خوارزمية الوشم الرقمي على تحويل DWT-SVD باستخدام إخفاء النسيج في النظام البصري البشري، لتحسين المتانة والأمان ضد الهجمات الخبيثة، قمنا بتضمين وشمين في نطاقين من تحويل DWT . في هذه الأطروحة ، قدمنا خوارزمية جديدة موثقة تعتمد على الجمع بين تحويل DWT مع وظيفة التحويل (TF) التي تسمح بتغيير شدة البكسل ، بعد تطبيق وظيفة جديدة تسمى PMF ، والتي قمنا بتطويرها ، لتغيير موقع البكسل حيث أدخلنا الوشم. تظهر النتائج التجريبية بوضوح متانة وكفاءة الطريقة التي تم تطويرها.

الكلمات المفتاحية: الوشم الرقمي للصور، النظام البصري البشري، تحويلDWT.

Résumé :

De nos jours le problème des droits d'auteur, la vie privée et l'authenticité des produits multimédia, devient un défi inquiétant. Une technique appelée tatouage numérique exploite des algorithmes mathématiques parvient à répondre à cette exigence dont le compromis : robustesse, invisibilité et capacité doit atteindre par la technique. Ce travail propose tout abord de nouvelles approches qui visent à améliorer les performances des algorithmes publiés récemment. Dans la première approche, l'algorithme de tatouage est basé sur la compression JPEG 2000 et la technique SVD pour l'insertion de la marque, pour augmenter la sécurité et améliorer la robustesse de l'algorithme nous avons utilisé la technique DE afin de calculer la clé. Pour la deuxième approche, l'algorithme de tatouage est basé sur la transformée DWT-SVD avec l'utilisation de masquage de texture dans le système visuel humain, pour perfectionner la robustesse et la sécurité envers les attaques malveillantes nous avons implanté deux marques sur deux sous-bandes DWT. Dans cette thèse, nous avons présenté un nouvel algorithme fiable basé sur la combinaison de la transformée DWT avec une fonction de transfert permettant le changement de l'intensité lumineuse des pixels, après une nouvelle fonction appelée PMF, que nous avons développé, est appliquée pour changer l'emplacement des pixels où nous avons inséré la marque. Les résultats expérimentaux montrent clairement la robustesse et l'efficacité de la méthode développée.

Mots clés : tatouage d'image, Transformée DWT, SHV, PMF.

Abstract :

Nowadays the issue of copyright, privacy and authenticity of multimedia products is becoming a worrying challenge. A technique commonly known as digital watermarking uses mathematical algorithms has coming to meet this requirement, the compromise of which: robustness, invisibility and capacity must be achieved by the technique. This work first proposes new approaches which aim to improve the performance of algorithms published recently. In the first approach, the watermarking algorithm is based on the JPEG 2000 compression and the SVD technique for the insertion of the watermark, to increase the security and improve the robustness of the algorithm we used the DE technique in order to calculate the key. For the second approach, the watermarking algorithm is based on the DWT-SVD transform with the use of texture masking in the human visual system, to improve robustness and security against malicious attacks we have embedded two watermarks into two DWT sub-bands. In this thesis, we have presented a new reliable algorithm based on the combination of the DWT transform with a transfer function allowing the change of the intensity of the pixels, after a new function called PMF, which we have developed, is applied to change the location of the pixels where we inserted the watermark. The experimental results clearly show the robustness and efficiency of the method developed.

Key words: watermarking image, DWT Transform, HVS, PMF.