الجمهورية الجزائرية الديمقراطية الشعبية
Republique Algerienne Democratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جـــــــامعـــــــــة الشهيـــــــد الشيـــــــــخ العربـــــــــي التبســـــــــي -تـــــبســـــــــــة
Université Echahid Cheikh Larbi Tébessi – Tébessa
Faculté des Sciences et de la Technologie
Département d'Électronique et Télécommunications

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

Filière : Electronique

Spécialité : Instrumentation

Par : ABDELLI Imene
SAHRAOUI Ghadir

THEME

Protection des données multimédia par le Tatouage (Watermarking)

Présenté et évalué, le 12 / 06 / 2024, par le jury composé de :

Nom et prénom		Grade	Qualité
M.	BOUABIDA Seddik	MAB	Président
Mme.	CHERIET Leyla	MCB	Rapporteur
Mme.	GOUDER Soraya	MCA	Examinateur

Promotion : 2023/2024

بِسْمِ اللَّهِ الرَحمَنِ الرَحِيمْ

"وَقُلِ اعْمَلُواْ فَسَيَرَى اللّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَى عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ" [التوبة: 105]

ويقول العماد الأصفهاني

(إني رأيت أنه لا يكتب أحد كتابا في يومه إلا قال فيه عنه : لو غير هذا لكان أحسن ، ولو زيد لكان يستحسن ، ولو قدم هذا لكان أفضل ، ولو ترك هذا لكان أجمل ، وهذا من أعظم العبر ، وهو دليل على استيلاء النقص على جملة البشر).

REMERCIEMENTS

Nous remercions avant tout **ALLAH** le tout puissant de nous avoir donné la force et le courage pour réaliser ce labeur.

Notre plus profonde gratitude va à la directrice de mémoire : le docteur **CHERIET Leyla** d'avoir accepté de diriger ce travail, merci pour votre perfectionnisme, soutien, disponibilité et gentillesse, merci pour votre sympathie et vos encouragements et pour avoir partagé vos compétences avec nous tout au long de ces mois ainsi pour l'inspiration, l'aide et le temps que vous avez bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour, que vous trouvez ici l'expression de notre plus profond respect et nos sincères gratitudes.

Je souhaiterais également remercier le professeur **BOUABIDA Seddik** et le docteur **GOUDER Soraya** pour leur contribution en tant que membres de jury. Leurs commentaires et leurs suggestions ont grandement amélioré la qualité de ce mémoire.

Je remercie mes collègues, tous les enseignants au département de l'électronique et télécommunication à l'université de Tébéssa pour m'avoir encouragée à aller jusqu'au bout du périple.

Enfin, je tiens à remercier tous les gens qui ont contribué à ma réussite tout au long de mon parcours d'études.

DÉDICACE

Je tiens à exprimer toute ma gratitude envers mes parents, mes frères et sœurs, pour leur présence constante et leur encouragement inestimable tout au long de cette aventure académique

A mes amis, pour leur amitié sincère.

Et enfin, à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce mémoire, je vous adresse ma plus profonde gratitude.

Abdelli & Imene

DÉDICACE

Je dédie ce modeste travail à :

Celui qui m'a appris que la vie est un combat et que son arme est le savoir et la connaissance, à mon modèle dans la vie. À celui qui a relevé ma tête avec fierté, mon cher père.

Mon cher ange, absente à mes yeux mais présente dans mon cœur, à celle par qui j'ai triomphé, à ma mère que Dieu ait son âme et lui accorde les plus hauts paradis. Et même si elle est partie de cette vie, ton rêve doit vivre.

La joie de ma vie, ma force et mon refuge après Dieu, ma chère tante et ma sœur et mes précieux frères.

Sahraoui & Ghadir

RESUMÉ

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes liés à la sécurité des documents ou des images échangés. Ce qui nécessite de trouver une solution pour protéger les données contre l'interférence et la duplication. Ce problème est résolu par les techniques de tatouage numérique qui intègrent des informations confidentielles dans le contenu original, garantissant ainsi sa sécurité et permettant l'accès uniquement aux utilisateurs autorisés. Il existe plusieurs méthodes pour réaliser un tatouage numérique, chacune avec ses propres avantages et inconvénients. Cependant, notre travail est basé sur une étude des différents algorithmes de tatouage des images avec l'exploitation de la décomposition en valeurs singulières (SVD) et la décomposition en ondelettes discrètes (DWT). Enfin, les résultats expérimentaux obtenus par les métriques de qualité objective et subjective sont très encourageants et confirment clairement l'efficacité des techniques appliquées.

Mots clés : Tatouage numérique, SVD, Transformée en ondelettes (DWT).

ABSTRACT

The rapid development of communications networks has caused new problems related to the security of documents or images exchanged. Which requires finding a solution to protect data against interference and duplication. This problem is solved by watermarking techniques that embed confidential information into the original content, thereby ensuring its security and allowing access only to authorized users. There are several methods for creating a digital watermark, each with its own advantages and disadvantages. However, our work is based on a study of different image watermarking algorithms using singular value decomposition (SVD) and discrete wavelet decomposition (DWT). Finally, the experimental results obtained by the objective and subjective quality metrics are very encouraging and clearly confirm the effectiveness of the applied techniques.

keywords : Watermarking, SVD, Wavelet transform (DWT).

ملخص

أدى التطور السريع لشبكات الاتصالات إلى حدوث مشكلات جديدة تتعلق بأمن المستندات أو الصور المتبادلة. الأمر الذي يتطلب إيجاد حل لحماية البيانات من التداخل والازدواجية. تم حل هذه المشكلة عن طريق تقنيات وضع العلامات المائية التي تدمج المعلومات السرية في المحتوى الأصلي، وبالتالي ضمان أمنها والسماح بالوصول إليها فقط للمستخدمين المصرح لهم. هناك عدة طرق لإنشاء وشم رقمي، ولكل منها مزايا وعيوب ولذلك يعتمد عملنا على دراسة خوارزميات العلامات المائية للصور المختلفة باستخدام تحليل القيمة المفردة (SVD) وتحلل الموجيات المنفصلة .(DWT) وأخيرا، فإن النتائج التجريبية التي تم الحصول عليها من خلال مقاييس الجودة الموضوعية والذاتية مشجعة للغاية وتؤكد بوضوح فعالية التقنيات المطبقة.

الكلمات المفتاحية :العلامة المائية، ،SVD التحويل الموجي،

TABLE DES MATIÈRES

Contents *Page*

TABLE DES FIGURES

LISTE DES TABLEAUX

ABRÉVIATIONS

Abréviations	Anglais	Français
AMR	Multi-resolution analyzes	Analyse multi-résolution
dB	Decibel	Décibel
db	Daubechies Wavelet	Ondelette de Daubechies
JPEG	Joint Photographic Experts Group	Groupe dexperts en photographie conjointe
MSE	Mean Square Error	Erreur quadratique moyenne
PSNR	Peak Signal to Noise Ratio	Rapport signal sur bruit
SVD	Singular Values Decomposition	Décomposition des valeurs singulières
TO	Wavelet transform	Transformé en ondelettes
TOC	Continuous Wavelet Transform	Transformée en ondelettes continue(CWT)
TOD	Discret Wavelet Transform (DWT)	Transformée en ondelettes discrète
TF	Fourier Transform	Transformé de Fourier

INTRODUCTION GÉNÉRALE

La révolution numérique, principalement liée au développement rapide des réseaux de communication, constitue en soi un grand défi et un mécanisme important pour assurer la sécurité de l'échange d'informations, un meilleur traitement des différents types d'informations et la rapidité de transmission. En effet, divers outils multimédias sont utilisés comme des outils importants dans plusieurs domaines d'application, tels que l'imagerie médicale, les images satellite, et bien d'autres applications qui nécessitent une très forte sécurité du contenu (données) et des droits d'auteur. Pour protéger ces documents numériques de telles manipulations, les chercheurs ont développé plusieurs techniques telles que le tatouage numérique.

Le tatouage numérique est un moyen de masquer des informations privées appelées marques ou signatures dans un document numérique sans dégrader la qualité. Ces informations, qui peuvent prendre de nombreuses formes (image, vidéo, texte, etc.), doivent être non identifiables et résistantes à toute manipulation légale ou illégale visant à détruire ou retirer la marque du document. L'algorithme de tatouage se compose de deux étapes : l'insertion et l'extraction. Ce dernier doit extraire la marque quel que soit l'attaque exercée sur le document contenant.

Dans le cadre de notre mémoire, nous nous intéressons d'investiguer le potentiel des ondelettes discrètes et les valeurs singulières de réaliser un tatouage robuste.

Ce mémoire est organisé en trois chapitres :

- **Chapitre 1 Généralité sur le tatouage numérique :** Nous allons présenter dans ce chapitre introductif, quelques concepts attachés au domaine du tatouage numérique, tout en donnant un aperçu sur : La définition et l'objectif du tatouage des images ainsi que le principe des schémas et les types du tatouage, les applications du tatouage numérique d'images et aussi la classification des algorithmes d'insertion et d'extraction.
- **Chapitre 2 Transformée en ondelettes :** Dans le deuxième chapitre, nous dressons une présentation rapide des transformées en ondelettes classiques. Nous voyons l'évolution de la transformée de Fourier à la transformée en ondelettes. Ainsi, nous traitons l'analyse multi résolutions qui est un outil essentiel de traitement du signal et permet de décomposer une image à plusieurs échelles (résolutions) et de le reconstruire à partir des éléments de cette décomposition.
- **Chapitre 3 Résultats des simulations :** Dans ce chapitre nous présentons les résultats de nos simulations obtenus suite à l'implémentation des algorithmes de tatouage numérique basés sur la SVD et la DWT. Nous allons utilisé le PSNR comme critère d'évaluation de notre méthode.

Enfin, une conclusion générale récapitule l'essentiel de notre travail et expose les perspectives de cette étude.

Chapitre 1

GÉNÉRALITÉS SUR LE TATOUAGE D'IMAGE

1.1 Introduction

Les entreprises ou les personnes souhaitant partager ou vendre leurs produits multimédias ont pu le faire grâce à l'explosion récente des systèmes de communication et de l'internet en tant que supports de collaboration. Cependant, les avantages de ces supports ouverts peuvent entraîner de graves problèmes pour les propriétaires de médias numériques qui ne souhaitent pas que leurs produits soient distribués sans leur consentement. La reproduction, la manipulation et la distribution illégales de fichiers numériques échangés via des réseaux de communication ou sur des appareils multimédias sont très faciles. Le tatouage numérique résout ces problèmes et d'autres problèmes de sécurité des données.

Il permet d'intégrer un message ou une signature (un tatouage) qui démontre la propriété d'un signal audio, vidéo ou image sans altérer sa valeur perceptuelle. Malgré les nombreuses applications du tatouage numérique, nous nous concentrons sur la protection des droits d'auteur en raison de sa domination. Le tatouage numérique a été créé pour répondre aux problèmes de protection des droits d'auteur. Cependant, de nombreuses autres applications peuvent facilement l'utiliser (BELILITA Sarra, 2019).

Ce chapitre présente une explication du tatouage numérique en raison de l'intérêt grandissant de ce domaine. Nous montrons comment il diffère de la cryptographie et de la stéganographie. Nous détaillons les principes des schémas de tatouage, ses limites, ses types et les menaces pour les tatouages numériques. La dernière partie de ce chapitre est consacrée aux applications de ce dernier.

1.2 Nécessité de la protection des droits d'auteurs

Une des premières applications du marquage est la protection des droits d'auteurs. Ce type d'application nécessite l'ajout d'une marque de l'auteur ou du propriétaire légal du document image. Par conséquent, la détection de la marque peut être utilisée pour démontrer la propriété en cas de conflit. Dans ce cas, la robustesse de la marque est nécessaire pour la protéger contre toutes tentatives visant à l'effacer (attaque destructive), à faire échouer sa détection (attaque géométrique) ou à créer une ambiguïté dans la décision (SELLAMI, 2017).

Les œuvres originales, telles que les œuvres littéraires, artistiques, musicales, cinématographiques, etc..., sont protégées par le droit d'auteur. Il accorde aux auteurs et créateurs un droit exclusif de reproduire, distribuer, afficher et exécuter leurs créations. Le droit d'auteur ne protège pas les idées ou les concepts seulement les créations réalisées. Peu importe sa forme d'expression, son genre, son mérite ou sa destination, l'œuvre est protégée dès le jour de sa création car elle s'acquiert sans formalité.

1.3 Tatouage numérique

Le tatouage numérique, également appelé watermarking, est une technique consistant à insérer une marque visible ou invisible dans un support numérique afin d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, une vidéo, une image ou un autre document numérique (A. Tirkel, 1993).

Le message qui est inclus dans le signal hôte est un ensemble de bits appelés marque ou message, dont le contenu dépend de l'application. La marque peut être une forme de signature décrivant le signal hôte ou le nom ou un identifiant du créateur, du propriétaire ou de l'acheteur. Cette méthode a été nommée en raison du marquage des documents papier et des billets (JEAN Luc, 2003).

1.3.1 Objectif du tatouage

L'objectif du tatouage pour la protection du copyright est d'introduire une marque invisible contenant un code de copyright dans une image originale. Il est possible de diffuser l'image marquée ou tatouée de cette manière, mais elle conservera toujours la marque de son propriétaire. Il est probable que cette image subisse plusieurs modifications. Ces changements peuvent être légaux (comme la compression) ou illégaux, ayant pour but de détruire le marquage (BENJAMIN, 2011).

1.4 Lien de tatouage numérique avec d'autres technologies de sécurité

1.4.1 Stéganographie

La stéganographie est une méthode pour cacher un message ou des données dans un autre fichier (texte, image, son, vidéo...). Il diffère de la cryptologie, qui ne cache pas le message mais le rend inintelligible sans un code de décryptage (BOUGUERNE, 2017).

Le terme « stéganographie » provient du mot grec « stéganos » qui signifie « dissimulé » et du mot grec « graphien » qui signifie « écriture », ce qui signifie littéralement « écriture dissimulée ». Elle consiste à cacher ou dissimuler un message dans un autre, ainsi que le message caché n'est détectable que par la personne qui sait comment le faire (G. SIMMONS, 1998). La figure 1.1 présente un exemple de stéganographie basé sur le principe de l'encre invisible.

FIG. 1.1 : Exemple de stéganographie basé sur le principe de l'encre invisible.

1.4.2 Filigrane

Le filigrane est une technique de marquage visuel ou numérique utilisée pour identifier, protéger ou authentifier un média, tel qu'une image, une vidéo ou un document. Il consiste en l'incorporation discrète d'informations, telles que des logos, des motifs ou des codes, dans le contenu principal du média. Le filigrane peut être visible ou invisible, et il peut être utilisé à des fins de propriété intellectuelle, de traçabilité ou de lutte contre la contrefaçon. Il offre une méthode de protection des médias en permettant de retracer leur origine et de dissuader la reproduction non autorisée (Cox, 2003).

1.4.3 Cryptographie

L'origine du mot cryptographie remonte aux Grecs : "kruptos" signifie caché et "graphein" signifie écriture. C'est l'ensemble des principes, méthodes et techniques utilisés par l'application pour chiffrer et déchiffrer les données afin de préserver leur confidentialité et leur authenticité (KUNDUR, 1989).

Il peut alors être défini comme une science mathématique qui vise à protéger les données sensibles. En d'autres termes, la cryptographie est l'art de coder et de chiffrer des messages.

L'objectif de la cryptographie n'est pas de dissimuler des informations dans d'autres, mais plutôt de rendre l'information que l'on souhaite transmettre complètement illisible pour toute personne ne disposant pas des informations nécessaires à son décodage. De plus, si le message primaire est modifié en cryptographie, il devrait être impossible de le recouvrer (JULIEN PUGLIESI, 2004). La figure 1.2 présente le schéma de cryptage et décryptage de texte.

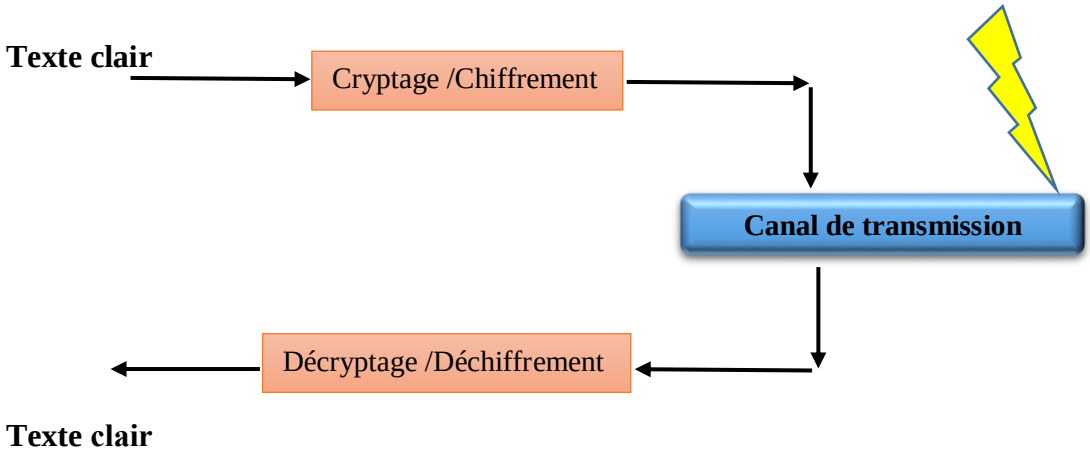


FIG. 1.2 : Schéma de cryptage et décryptage de texte.

1.5 Principe des schémas de tatouage

Considéré comme une tâche de communication, le processus de tatouage peut être divisé en trois étapes principales : l'incorporation du tatouage, la transmission par le canal du signal tatoué (soumis à des attaques éventuelles) et la récupération de tatouage (figure 1.3).

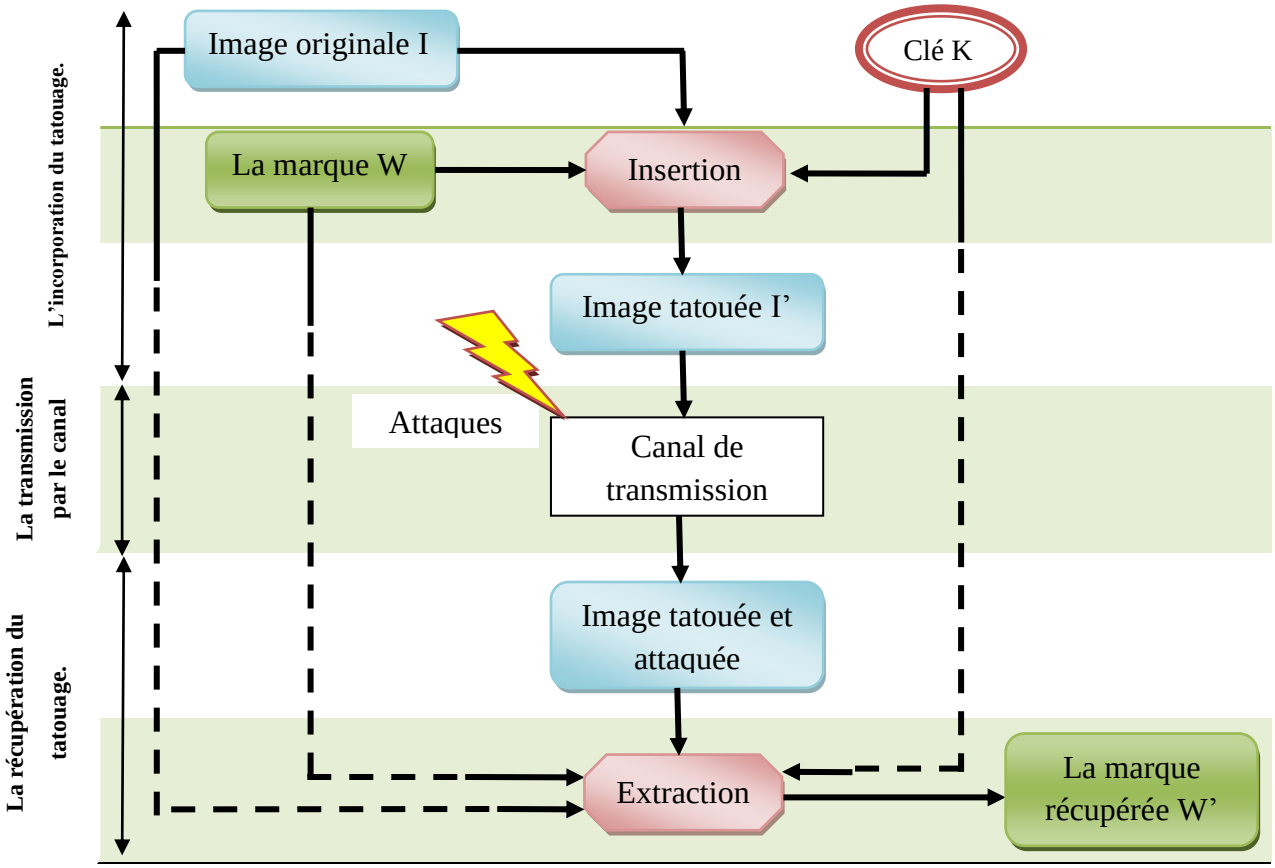


FIG. 1.3 : Principe du système du tatouage.

1.5.1 Phase d'insertion (Incorporation du tatouage)

La première étape dans la conception d'un système de tatouage est la définition de la procédure d'incorporation ou d'intégration de la marque. Cette tâche est cruciale, car les propriétés du tatouage dépendent fortement de la manière dont il est inséré dans les données. La phase d'insertion nécessite comme entrées le document hôte (image dans notre cas) qu'on note I et la marque à insérer (généralement sous format binaire) qu'on note (Watermark). Souvent, le schéma utilise en plus une clé d'insertion (BELILITA Sarra, 2019).

L'insertion de la marque consiste à insérer dans l'image originale I, une marque M et ainsi créer une nouvelle image appelée image tatouée $I^{'}$. Les images tatouées et les images originales sont presque identiques. La différence entre $I^{'}$ et I est appelée distorsion de l'insertion (Figure 1.4). Un troisième paramètre facultatif peut être ajouté : la clé secrète de marquage K qui permet d'assurer un certain ni-

veau de sécurité au processus de tatouage. La marque est encodée en utilisant cette clé secrète K. Pour faire en sorte que les distorsions de l'insertion soient suffisamment faibles et imperceptibles, la marque est ensuite modulée (BOUHOUS, 2018)

.

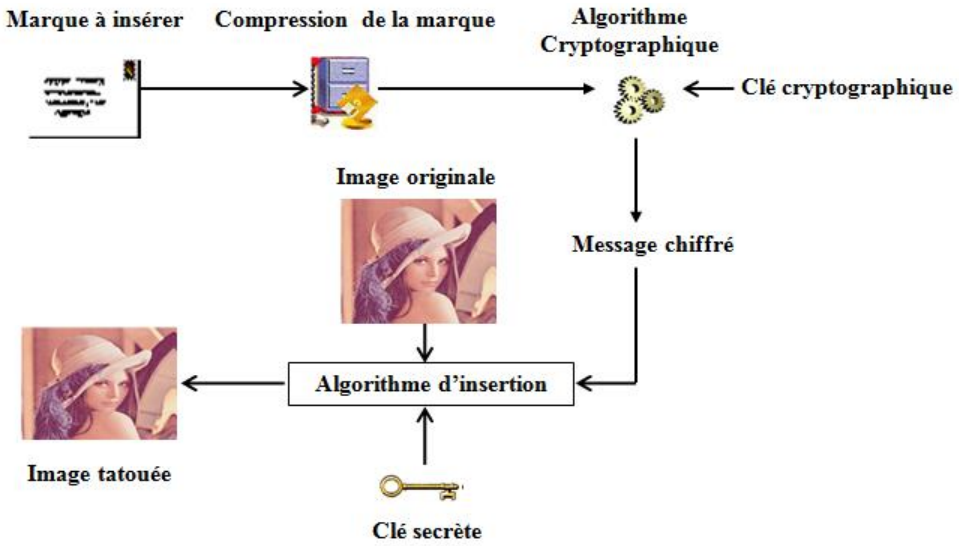


FIG. 1.4 : Phase dinsertion.

1.5.2 Phase d'extraction : Récupération du tatouage

L'objectif d'un système de tatouage consiste essentiellement à introduire des informations sur un support, puis à les extraire de manière aussi fiable que possible. Si nous considérons l'intégrateur de tatouage comme un émetteur dans une chaîne de communication, un extracteur de tatouage sera le récepteur. La détection peut avoir deux objectifs différents : décider si l'image testée contient un tatouage et extraire un message que le tatouage peut véhiculer (Figure 1.5). A la fin de cette phase, on aura soit une marque W' soit une décision indiquant si l'extraction a été faite avec succès ou non (BELILITA Sarra, 2019).

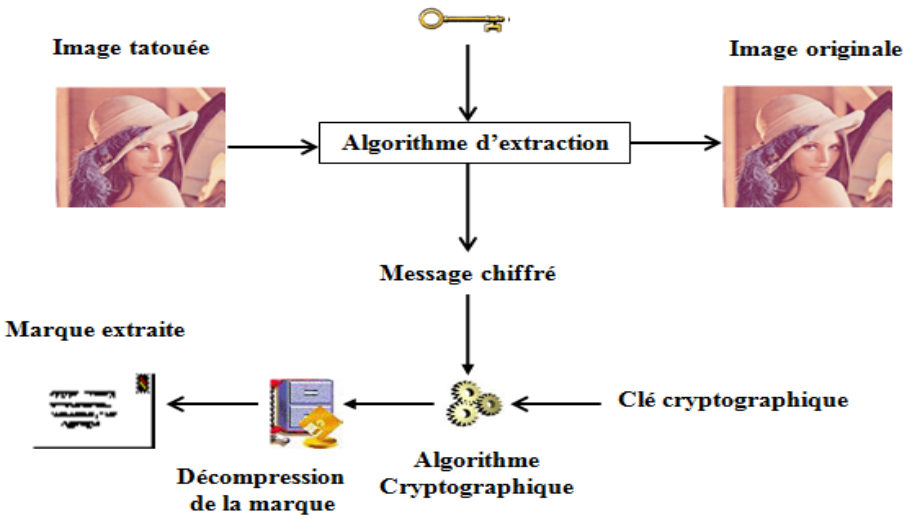


FIG. 1.5 : Phase d'extraction.

1.6 Contraintes du tatouage numérique

Depuis l'apparition du tatouage numérique, les chercheurs n'ont pas cessé de rénover les méthodes de marquage. Ces perfectionnements visent surtout à améliorer les principales propriétés du tatouage qui sont principalement : la robustesse ou fragilité, l'invisibilité, la capacité d'insertion et la sécurité de l'information secrète. Il doit y avoir un compromis entre les exigences et les propriétés du tatouage en fonction de ses applications (Figure 1.6).

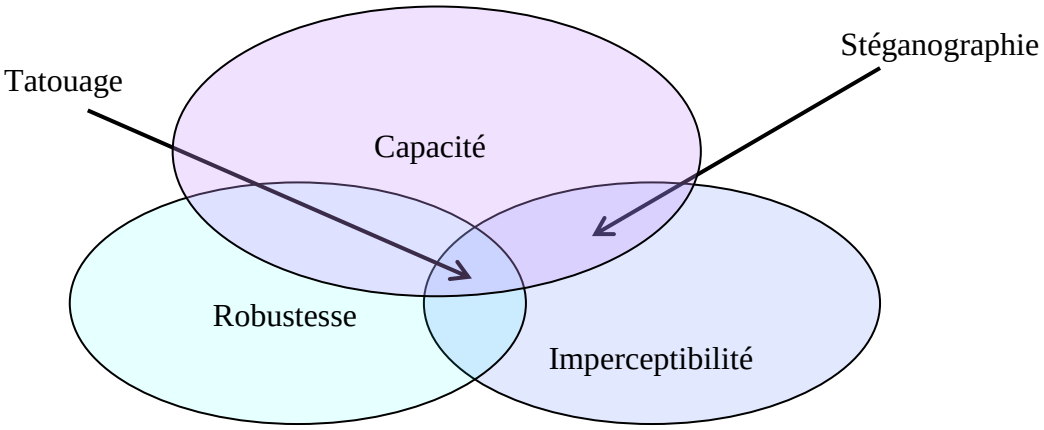


FIG. 1.6 : Compromis entre l'imperceptibilité, la capacité et la robustesse.

1.6.1 Capacité

La taille en bits d'une marque qui peut être intégrée dans un document de taille donnée détermine la capacité d'une méthode de stéganographie. Par conséquent, la capacité d'insertion relative est la relation entre la taille du message confidentiel et la taille du média utilisé (K. Stefan, 2000).

1.6.2 Imperceptibilité

Si un personne ne peut pas distinguer le support original du support marqué, la marque est dite imperceptible. En d'autres termes, la différence ne doit pas être perceptible. L'objectif est qu'aucune autre personne que les personnes concernées par le message ne détecte pas l'existence de l'information cachée des tests visuels est utilisée pour garantir cette invisibilité. Les sujets de ces tests reçoivent des supports marqués et non marqués aléatoirement afin de déterminer la meilleure qualité (BOUGEUERNE, 2017).

1.6.3 Robustesse

La robustesse représente la capacité du tatouage à résister aux dégradations du document tatoué. La marque doit être difficile à supprimer. Si un utilisateur malveillant tente de supprimer la marque (en termes de dégradations visibles inacceptables et/ou d'utilisation commerciale rendue impossible) ou bien si l'image subit des dégradations non intentionnelles (on trouve dans cette catégorie la compression JPEG, les conversions de format en général et les changements de résolution entre autres) ceci doit causer une forte dégradation au niveau de la qualité de l'image (Meina, 2008).

1.7 Types de tatouage numérique

Plusieurs formes et degrés de tatouages existent. Ils sont généralement répertoriés par leurs degrés de priorités : robuste ou fragile et visibles ou non visibles (LAIMECHE, 2009).

1.7.1 Tatouage robuste

Dans un tatouage robuste, la détection de la marque est effectuée même si le document tatoué a été altéré ou attaqué. Un système de tatouage robuste doit résister aux opérations licites effectuées sur le document numérique telles que la compression, la conversion analogique-numérique, le filtrage, etc. Et celles illicites, comme les attaques malveillantes des pirates. Ce type de tatouage est utilisé surtout dans les applications de protection de copyright et le contrôle de copies (BOUHOUS, 2018).

1.7.2 Tatouage fragile

C'est un tatouage qui permet de détecter si l'image a été modifiée. La moindre modification du document se répercute fortement sur la marque extraite et on peut en déduire que le document n'est pas authentique (Meina, 2008) (figure 1.7).

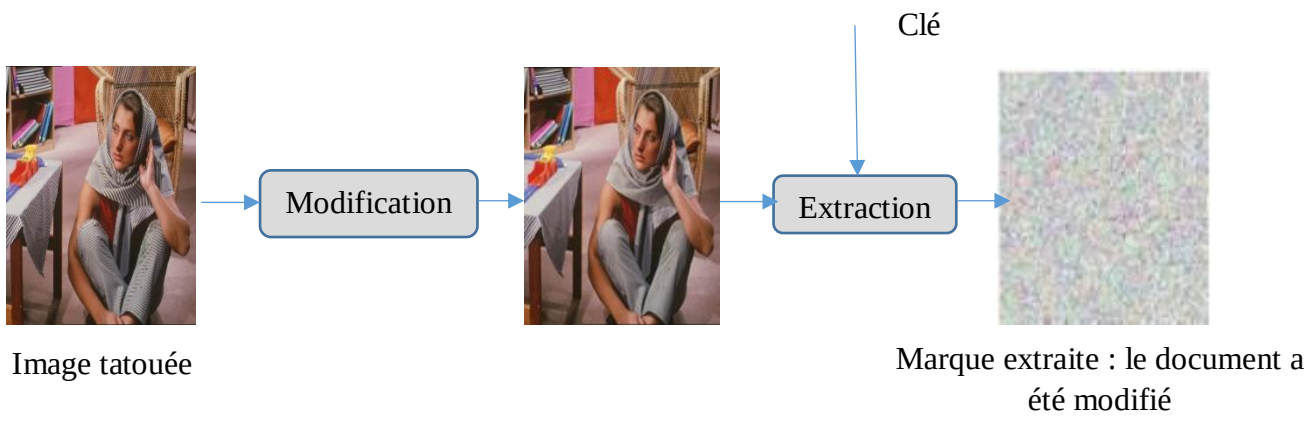


FIG. 1.7 : Tatouage fragile.

1.7.3 Tatouage visible et invisible

Du point de savoir si la marque insérée peut être vu par l'œil humain ou non toutes les techniques de tatouage d'images peuvent être classées comme des techniques de tatouage visibles ou invisibles. Le principe fondamental du tatouage visible consiste à dissimuler partiellement une image. Pour ce faire il faudra utiliser un nombre indéterminé de marques visibles, qui ne pourront être efficace-

ment effacées que si l'on possède une "clef secrète" adéquate. Ce type de tatouage est étudié actuellement pour gérer tout ce qui concerne les contrôles d'accès d'un unique document, correspondant en quelque sorte a une distribution de permission. On entend par contrôles d'accès la possibilité de restreindre la divulgation d'un document en fonction de l'appartenance d'un utilisateur ou non la classe des "ayants droit" à la lecture de ce document. En pratique, l'intérêt d'un watermark efficace réside dans son invisibilité.(JULIEN PUGLIESI, 2004).

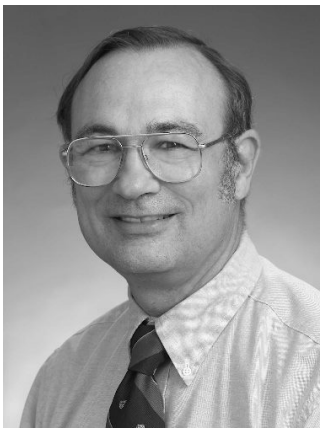
Par exemple, la figure **??** montre une image qui contient un logo visible dans son coin supérieur gauche et la figure 1.8d montre la même image tatouée par le même logo mais d'une manière invisible (KHALED, 2010).

Dans les techniques de tatouage visible, il existe au moins deux inconvénients :

✓La marque insérée est facilement enlevée par un simple cropping.

✓La visibilité de la marque insérée dégrade la qualité visuelle de l'image l'hôte.

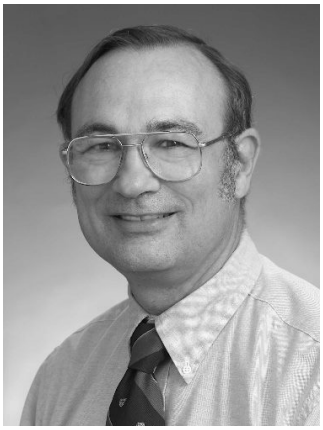
Dans la technique de tatouage invisible, il n'est pas facile de faire la distinction entre l'image originale et l'image tatouée. Ainsi, il est difficile d'enlever ou détruire la marque insérée sans avoir une dégradation de la qualité visuelle de l'image tatouée de manière significative (FARES, 2023).



(a) Image original.

(b) Watermark.

(c) Tatouage visible.



(d) Tatouage invisible.

FIG. 1.8 : Tatouage visible et invisible.

1.8 Classification des techniques de tatouage

Les techniques de tatouage courantes décrites dans la littérature peuvent être regroupées selon leurs domaines d'insertion en deux classes, techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

1.8.1 Domaine spatial

Dans le domaine spatial, la marque est insérée en modifiant les LSB (bits de poids faible). Les images sont en général manipulées en modifiant un ou plusieurs bits de l'octet constituant les pixels de l'image. Pour une image codée sur 8 bits, une modification du LSB entraîne une variation du niveau de gris de 1 sur une échelle de 256. Cette modification est en pratique invisible.

Cette méthode d'insertion consiste alors à supprimer tous les bits de poids faible de l'image à marquer, puis à y insérer les données voulues. Un bit de donnée est ainsi inséré par pixel de l'image.

En règle générale, le tatouage dans le domaine spatial est facile à mettre en œuvre, mais trop fragile pour résister aux nombreuses attaques, par exemple l'ajout de bruit ou bien la compression avec perte peut facilement dégrader la qualité de l'image ou de supprimer la marque (R. Schyndel, 1994).

1.8.2 Domaine fréquentiel

Le principal inconvénient des méthodes de tatouage spatial est la faible robustesse face aux attaques et notamment face aux attaques géométriques.Les techniques de tatouage spatial telles que celles que nous venons de découvrir peuvent tout aussi bien être adaptées aux domaines fréquentiels (Pereira, 1999).

Les techniques de tatouage qui travaillent dans le domaine fréquentiel sont plus robustes. Les domaines transformées les plus fréquemment exploités pour les applications de tatouage numérique des images sont : le domaine de transformée de Fourier discrète (DFT), le domaine de transformée en Cosinus discrète (DCT), le domaine de transformée en Ondelette discrète (DWT) (Low, 2008).

1.9 Évaluation des images de tatouage

Il est difficile d'évaluer un algorithme de tatouage vu les multiples applications envisagées et les critères qui rentrent en jeu. Il est néanmoins possible

d'identifier un des éléments qui influencent l'évaluation de tatouage telle que la qualité de l'image.

1.9.1 Mesure de la qualité de l'image

Cette mesure est basée sur la comparaison de pixels entre l'image originale et l'image Tatouée. Parmi ces mesures nous retrouvons : l'erreur quadratique moyenne, l'erreur moyenne absolue et le rapport signal sur bruit.

— L'erreur quadratique moyenne (MSE) : L'erreur quadratique moyenne est donnée par :

$$MSE = \frac{1}{MN}\sum_{i}\sum_{j}\left(I(i,j) - I_w(i,j)\right)^2 \tag{1.1}$$

Où I (i, j) est la valeur de la luminance du pixel (i, j) de référence et $I_w(i, j)$ celle de l'image à tester, les deux images étant de taille $M \times N$. Cette mesure nous donne une indication sur la dégradation introduite au niveau du pixel. Plus le MSE est grand, plus le niveau de dégradation est élevé.

— L'erreur moyenne absolue (MAE) : L'erreur moyenne absolue est donnée par :

$$MAE = \frac{1}{MN}\sum_{i}\sum_{j}\left|I(i,j) - I_w(i,j)\right| \tag{1.2}$$

Cette mesure quantifie les moyennes des différences absolues dans I et I_w.

— Le rapport signal sur bruit (PSNR) : La mesure de distorsion le plus utilisée afin de quantifier la distorsion entre deux images est : le rapport signal sur bruit (Peack Signal to Noise Ratio). Le PSNR est défini par :

$$PSNR = 10\log_{10}\left(\frac{x_{\max}^2}{MSE}\right) \tag{1.3}$$

Ou x_{max} désigne la luminance maximale et MSE définit l'erreur quadratique moyenne calculée entre les pixels des deux images à comparer. Une valeur de PSNR égale à l'infini correspond à deux images parfaitement identiques.

Elle décroît en fonction de la distorsion et relie donc l'erreur quadratique moyenne à l'énergie maximale de l'image (Vidyasagar, 2009) .

1.10 Attaques de tatouage numérique

Nous avons vu les différentes possibilités de protection de données, à travers la cryptographie, la stéganalyse et en particulier le tatouage. Une science s'oppose à ces techniques : la stéganalyse. Elle concerne l'étude des attaques. Dans ce paragraphe, nous allons expliquer les différents types d'attaques que nous connaissons et quelques techniques d'applications de celles-ci.

1.10.1 Compressions JPEG

Il est très classique de compresser une image pour pouvoir faciliter son transfert. Toutefois, la compression JPEG provoque une perte de détails et une apparition de la géométrie des blocs pour des taux de compression élevés (Figure 1.9).

Ce type d'attaque est non linéaire et ne peut pas se modéliser très facilement. Cependant, la perte de petits détails (composantes haute-fréquences de l'image) résultant de la compression et la conservation des informations prépondérantes nous permettent d'assimiler la compression à un filtrage passe-bas. Donc, pour contrer l'attaque compression, la marque doit posséder, en général, une composante basse-fréquence qui pourra être conservé après le processus de compression (AHMED, 2007).

FIG. 1.9 : Exemple de perte de qualité lors de compression jpeg.

L'avantage de cette méthode réside dans les taux de compression important que l'on peut obtenir, mais son désavantage se situe lui dans le fait qu'il s'agit d'une compression destructive. En effet plus l'on compresse l'image plus des défauts apparaissent. Voyons en détail les différentes étapes de cette compression :

1. On découpe d'abord l'image en blocs carrés de 8 pixels sur 8 pixels.

2. On effectue ensuite une Transformée de Fourier (en pratique, une transformée DCT) en 2 dimensions du bloc.

3. Et pour finir, on applique un filtre passe bas et c'est la que l'on choisit le taux de compression. Plus celui ci va être élevé, plus l'on va supprimer une gamme de fréquences importantes et plus l'image va être dégradée. Ce type d'attaque s'applique aussi à tout ce qui est conversion de format, par exemple du jpeg vers du gif (JULIEN PUGLIESI, 2004).

1.10.2 Ajouts de bruit

Nous allons présenter ici les principes de deux méthodes classiques en tatouage d'images dont le principe général est d'ajouter un bruit sur l'image. La première méthode, plus ancienne, a été fondée sur l'idée d'ajouter des patchs à

certains endroits secrets de l'image. La détection est basée sur la connaissance de ce secret. Dans la seconde méthode, un bruit large bande est ajouté à l'image, cette méthode est dérivée de techniques utilisées en théorie de la télécommunication. Après une présentation de ces deux méthodes, nous montrerons qu'on peut les considérer comme une unique méthode (Anne Manoury, 2001).

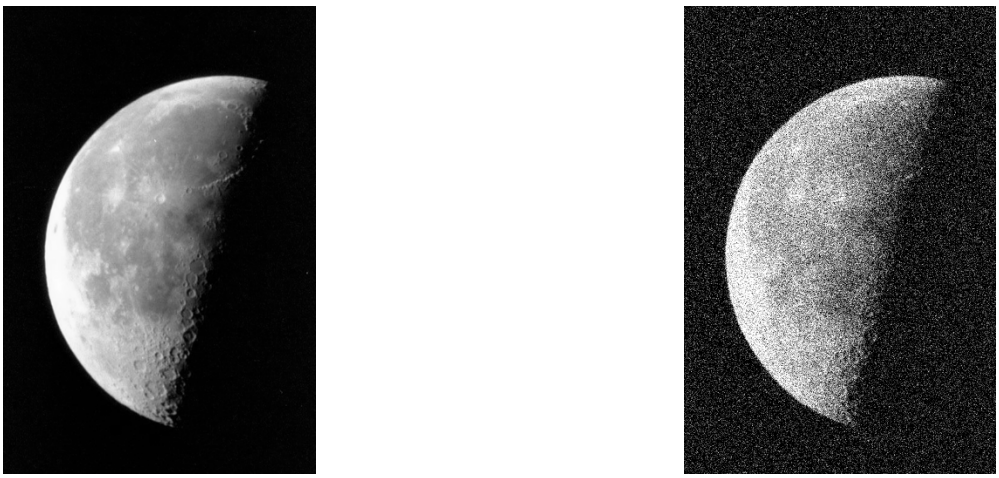


FIG. 1.10 : Exemple de perte de qualité lors de l'ajouts de bruit.

1.10.3 Filtrage

L'application de filtres dans le cadre du traitement d'images sert en général à améliorer l'aspect de l'image. Par exemple, l'augmentation des composantes hautes fréquences de l'image (le rehaussement) augmente le contraste car les détails sont mis en valeur. Un autre exemple est celui du lissage. Cette fois-ci, les composantes hautes fréquences sont atténuées. L'image apparaît alors plus floue mais cela permet d'atténuer le bruit contenu dans l'image. Dans tous les cas, ces opérations sont linéaires et l'influence sur le tatouage est facilement prévisible. Des traitements plus complexes, comme le filtrage médian ou certains algorithmes de dé bruitage, vont utiliser des opérations non linéaires et vont donc être plus difficilement caractérisables par rapport à leur influence sur le tatouage. Tou-

tefois, comme pour la compression, en analysant leur effet, nous pouvons essayer d'approximer l'influence de l'attaque par une opération linéaire (AHMED, 2007).

FIG. 1.11 : Exemple de perte de qualité lors de l'application de filtrage.

1.11 Application de tatouage

Les applications du tatouage sont diverses. Initialement dédié à la protection de la propriété intellectuelle des documents numériques, le tatouage est utilisé aujourd'hui pour le contrôle d'intégrité, de l'authentification ou encore de la production de documents enrichis.

1.11.1 Protection des droits d'auteur

Le tatouage numérique est couramment utilisé dans le but de protéger les droits d'auteur, en insérant une signature unique qui permet d'identifier de manière fiable le propriétaire de l'œuvre. Il s'agit de l'application la plus évidente du tatouage numérique dans le domaine de la protection des droits d'auteur. Les deux caractéristiques primordiales à respecter sont l'invisibilité et la robustesse de la marque. En effet, la marque doit être invisible pour préserver l'intégrité de l'œuvre originale, tout en étant suffisamment résistante pour contrer les tentatives de piratage et de violation des droits d'auteur (K. Amine, 2022).

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

L'idée de base consiste à utiliser les techniques de tatouage d'image afin de cacher dans certaines zones de l'image des informations sur d'autres zones. Ces informations servent à alerter l'utilisateur face à une éventuelle modification ou découpe de l'image par une personne non autorisée et à localiser précisément les régions manipulées, voire éventuellement à les restaurer. Ce service remet partiellement en cause les paramétrages usuellement établis dans le cadre d'un service classique de droits d'auteur, notamment en termes de quantité et nature des informations à cacher, de robustesse, etc. Mais on peut déjà se demander s'il est préférable d'utiliser un tatouage fragile (ou semi-fragile), un tatouage robuste, ou opter au contraire pour une technique faisant appel à une signature externe (CHRISTIAN, 2003).

1.11.3 Contrôle d'accès

Le but dans ce cas est d'ôter tout intérêt commercial à l'image en insérant une marque visible (nom de la société, logo…). La figure 1.12 nous illustre cette application, seules les personnes ayant les droits d'accès sont en mesure d'inverser le processus de marquage de manière à reconstituer l'image originale (C. REY, 2003).

FIG. 1.12 : Controle d'accés par masquage visible d'une image.

1.11.4 Indexation

L'indexation des images consiste à classer de manière automatique des images selon leur contenu, en facilitant ainsi la recherche dans une base de données. La marque insérée décrit brièvement l'image, comme elle peut être un pointeur vers lequel il y a une description plus détaillée, cette technique commence à être appliquée dans les services hospitaliers, où les clichés sont classés dans des bases de données suivant l'âge, le nom ou la pathologie du patient.

Dans cette application, la marque n'a pas besoin d'être robuste aux attaques, puisqu'il ne s'agit plus de protection mais juste d'identification. Un nouveau concept d'image intelligente (smart image) a été introduit par la société «Digimarc11». A des fins publicitaires, le tatouage est utilisé pour insérer un pointeur vers un lien internet qui pourra donner toute la description du produit, en le présentant juste à un dispositif d'acquisition, en le décodant , tous les détails concernant le produit seront affichés sur un navigateur Web comme l'illustre la figure 1.13.(P. BAS, 2000)

FIG. 1.13 : Application du tatouage pour l'indexation d'image (smart image).

1.12 Conclusion

Dans ce chapitre, nous avons présenté brièvement, dans une première étape, les outils de la sécurité d'information afin de de montrer la position de tatouage numérique qui fait l'objet de notre projet. Ensuite, nous avons présenté le concept

général du tatouage des images ainsi le schéma général de tatouage, ses différents critères, les différentes attaques, ses applications et les domaines d'insertion.

Chapitre 2

TRANSFORMÉE EN ONDELETTES

2.1 introduction

Les ondelettes sont, avant tout, un puissant outil de représentation creuse des signaux. L'idée est de représenter la majeure partie des informations du signal à partir d'un nombre de coefficients le plus restreint possible (BENYAHIA, 2014). La transformation en ondelettes a connu un succès remarquable dans divers domaines d'application, tels que le débruitage, l'analyse des images médicales, la compression et la transmission de données, le tatouage numérique, ainsi que les solutions numériques des équations différentielles. Les ondelettes, telles que la décomposition de Fourier, jouent un rôle essentiel dans l'analyse du signal. Cette discipline tente d'analyser et de saisir les signaux en utilisant les mathématiques (BERNARD, 2002).

Dans ce chapitre, nous allons commencer par rappeler la théorie de la transformée de Fourier et de la transformée de Fourier Fenêtré (STFT), la transformée en ondelette continue et discret , les espaces d'approximations et détails, la citation des différents familles d'ondelettes et enfin choisir la meilleur d'entre elles.

2.2 De la transformée de Fourier à la transformée en ondelettes

2.2.1 Transformée de Fourier (TF)

En 1807, le mathématicien français J. Fourier, a prouvé que toute fonction périodique peut être exprimée comme une somme infinie de fonctions exponentielles complexes et périodiques, des années plus tard, ses idées ont été généralisées aux fonctions continues non périodiques, puis aux fonctions discrètes qui sont périodiques ou non périodique dans le temps. La transformée de Fourier décompose un signal en fonctions de base trigonométriques orthogonales. La TF est donnée par la formule (2.1), le signale transformé par cette transformation donne la distribution de fréquence globale du signal temporel (Kok, 2002). La transformée de Fourier nous donne la possibilité de reconstruire le signal original (la transformée de Fourier inverse) par la formule (2.2) :

$$X(f) = \int_{-\infty}^{+\infty} x(t).e^{-2j\pi ft}dt \tag{2.1}$$

$$x(t) = \int_{-\infty}^{+\infty} X(f).e^{2j\pi ft}dt \tag{2.2}$$

La figure 2.1 présente un exemple de la transformée de Fourier d'un signal monodimensionnel. Cependant, l'analyse de Fourier, de par sa nature, montre assez vite ses limitations : son calcul nécessite la connaissance de toute l'histoire temporelle du signal. De plus, dans une transformée de Fourier, l'information sur le temps est présente (la transformée inverse est donc possible), mais elle est cachée dans les phases : elle est en pratique impossible à extraire. On en est donc réduit à étudier un signal soit en fonction du temps, soit en fonction des fréquences qu'il contient, sans possibilité de conjuguer les deux analyses.

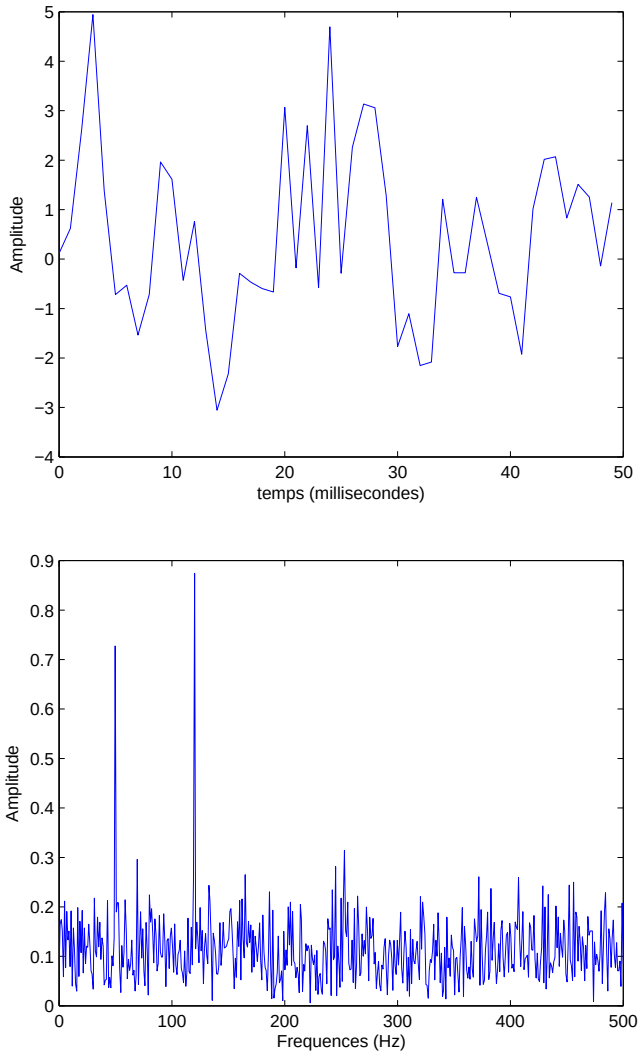


FIG. 2.1 : Exemple d'une transformée de Fourier d'un signal monodimensionnel.

2.2.2 Transformée de Fourier Fenêtré (STFT)

Afin de remédier au problème de la location temporelle de la transformée de Fourier, Gabor a proposé en 1946 d'utiliser une transformée de Fourier à fenêtre. Cette transformation peut être adaptée au signal non-stationnaire et très proche de l'analyse spectrale. Elle consiste à calculer la transformée de Fourier sur une partie du signal sélectionnée à l'aide d'une fenêtre bien localisée en temps. Des translations successives de cette fenêtre permettent d'analyser localement le comportement temps-fréquence du signal. La transformée de Gabor (TG) revient à

projeter un signal sur des fonctions analysantes de la forme (JAIDEVA, 1999) :

$$g_{a,b}(t) = e^{iat}(t-b) \tag{2.3}$$

On constate que le membre « $g(tb)$ » de l'équation (2.3) est indépendant de « a », ce qui signifie que l'enveloppe de la fenêtre glissante sera constante : on aura donc une résolution fixe sur toute la durée du signal. Où « a » représente le facteur d'échelle, et « b » le facteur de translation. L'étude d'un signal avec la transformée de Gabor permet d'obtenir à la fois une information sur le temps et sur la fréquence, mais la résolution d'analyse est fixée par le choix de la taille de l'enveloppe (JAIDEVA, 1999) : si la fenêtre est trop petite, les basses fréquences n'y seront pas contenues, et si la fenêtre est trop grande, l'information sur les hautes fréquences est noyée dans l'information concernant la totalité de l'intervalle contenu dans la fenêtre.

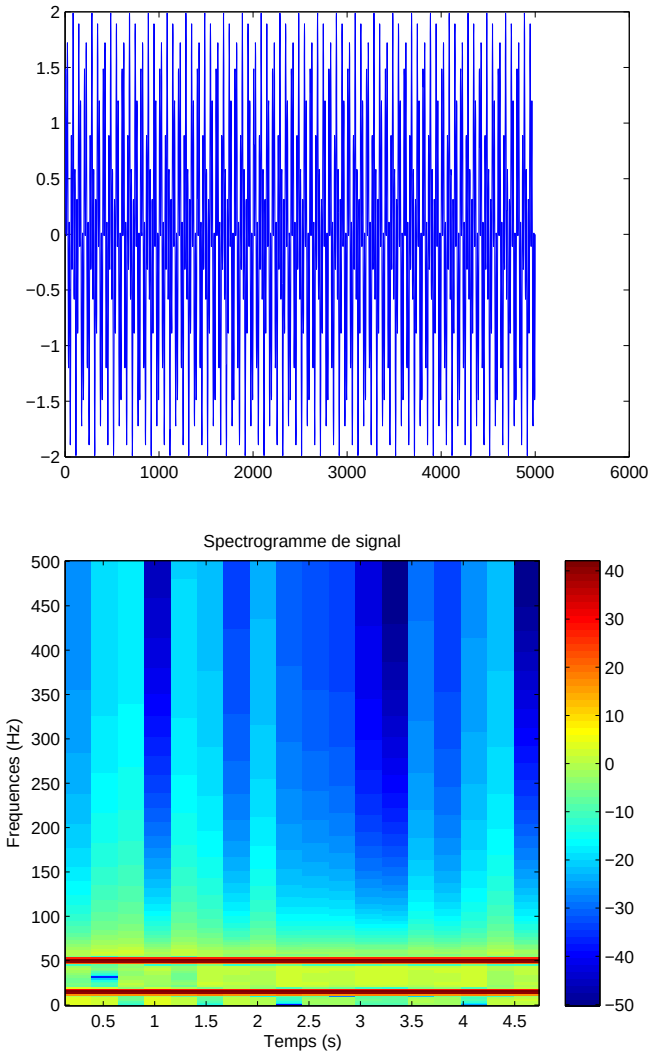


FIG. 2.2 : Exemple d'une transformée de Fourier fenêtrée STFT d'un signal monodimensionnel.

2.2.3 Transformée en ondelettes (TO)

La transformée en ondelette (T.O) est un outil mathématique qui décompose un signal en fréquences en conservant une localisation temporelle . Le signal de départ est projeté sur un ensemble de fonctions de base qui varient en fréquence et en temps. Ces fonctions de base s'adaptent aux fréquences du signal à analyser. La fenêtre est de surface constante mais sa taille varie en fonction de la fréquence à analyser (KHELIFA, 2013).

2.2.4 Transformée en ondelettes continue

De façon analogue à l'analyse de Fourier, les analyses en ondelettes réalisent la transformation intégrale d'un signal donné par projection sur un ensemble (continu ou dénombrable) de fonctions. Dans le cas des analyses en ondelettes, ces dernières fonctions sont toutes déduites par dilatation et translation d'une unique fonction de référence localisée en temps et en fréquence. De telles analyses fournissent une caractérisation d'un signal donné dans le plan temps-fréquence. Soit une ondelette Ψ, on définit la transformée en ondelettes continue d'un signal par l'application linéaire X_Ψ donnée par la formule suivante :

$$X_\Psi(a,b) = \frac{1}{\sqrt{C_\Psi}} \int_{-\infty}^{+\infty} x(t).\Psi_{a,b^*}(t)dt \tag{2.4}$$

Cette transformation intégrale peut s'interpréter comme le produit scalaire d'un signal $x(t)$ de avec l'ensemble des atomes temps-fréquence $\Psi_{a,b}$ obtenus par dilatation et translation d'une ondelette admissible Ψ pour des coefficients de résolution a et de translation b. Cette transformée est dite continue car c'est une fonction continue de paramètres de dilatation et de translation et on verra que ces paramètres peuvent être discrétisés, on obtient alors la transformée en ondelettes discrète.

La transformée en ondelettes continue renseigne sur le comportement du signal autour du point b dans un voisinage (intervalle) de taille qui est de l'ordre de a. Toutefois, le mécanisme d'analyse de l'information transitoire contenue dans le signal $x(t)$ par les atomes temps-fréquence s'explicite en remarquant que l'ondelette Ψ est un filtre passe-bande et que la voie de coefficients ondelettes $X_\Psi(a,.)$ s'exprime comme une convolution du signal $x(t)$ et du motif Ψ dilaté à la résolution a. Le coefficient $X_\Psi(a,b)$ est alors appelé coefficient ondelettes ou coefficient de détails de résolution a et de translation. L'astérie $(*)$ indique que le conjugué complexe de la fonction d'ondelette qui est utilisé. Les paramètres a et b permettent la dilatation (échelle) et la translation (retard) sur l'axe des temps de

l'ondelette. La transformés d'ondelette est appelée communément 'microscope mathématique' qui peut `zoomer' sur les composantes du signal par le biais du paramètre de l'échelle a et le déplacement le long de l'axe du temps par le biais du paramètre (BOUFENAR, 2016).

2.2.5 Transformée en ondelettes discrète

La transformée en ondelettes discrète (TOD) est produite pour surmonter le problème de redondance de la TOC, Cette redondance mobilise une grande quantité de ressource de calcul. La TOD, au contraire, fournit suffisamment d'information, tant pour l'analyse que pour la reconstruction du signal original. Ceci en un temps de calcul notablement réduit.

La TOD est considérablement plus simple à implémenter que la TOC. La TOD translate et dilate l'ondelette selon des valeurs discrètes. Ces coefficients τ et s seront discrétisés de la manière suivante : $s = s_0^j$ et $\tau = k\tau_0 s_0^j$ avec $s_0 > 1$ et $\tau_0 > 0$ fixés et appartenant à Z (JAIDEVA, 1999).
Les ondelettes sont alors définies de la manière suivante :

$$\Psi(\tau, s) = \frac{1}{\sqrt{s_0^j}} \Psi\left(\frac{t - k\tau_0 s_0^j}{s_0^j}\right) \tag{2.5}$$

La TOD est donnée par la formule ci-dessous :

$$TOD(\tau_0, s_0) = \frac{1}{\sqrt{s_0^j}} x(t) \Psi\left(\frac{t - k\tau_0 s_0^j}{s_0^j}\right) dt \tag{2.6}$$

◇ s_0^j Facteur d'échelle.

◇ τ_0 Facteur de translation.

◇ k et j sont des entiers.

2.3 Familles d'ondelettes

Avant de détailler quelques familles d'ondelettes usuelles, nous dressons dans le tableau suivant. la liste de quelques-unes de ces familles, avec les abréviations associées (BEYLKIN, 1991).

Nom des familles d'ondelettes	**Abréviations**
ondelettes de haar	Haar
ondelettes de Daubechies	Db
ondelettes symlets	Sym
ondelettes coiflets	Coif
ondelettes biorthogonales	Bior
ondelettes de meyer	Meyr
ondelettes gaussiennes	Gaus
ondelettes gaussiennes complexes	Ggau
ondelettes mexician	Mexh
ondelettes de morlet	Morl
ondelettes de morlet complexe	Cmor
ondelettes de shannon complexes	Shan

TAB. 2.1 : Abréviation de quelques familles d'ondelettes.

Les ondelettes à filtre sont associées à des analyses multi-résolutions orthogonale sou bio orthogonales, la transformée discrète et les calculs rapides en utilisant l'algorithme de mallât sont alors possibles. Les ondelettes sans filtres, en revanche, sont utiles pour la transformée en ondelettes continues. En général les

ondelettes à supports compacts n'ont pas de forme analytique (c'est à dire : on sait comment calculer la fonction, mais on ne peut pas l'exprimer avec une formule mathématique).

2.3.1 Exemples de familles d'ondelettes

◇ **Ondelette de Haar**

L'ondelette de Haar est une ondelette créée par Alfréd Haar en 1909. On considère que c'est la première ondelette connue. Il s'agit d'une fonction constante par morceaux, ce qui en fait l'ondelette la plus simple à comprendre et à implémenter. L'ondelette de Haar peut être généralisée par ce qu'on appelle le système de Haar comme illustré dans la figure 2.3 (BEYLKIN, 1991).

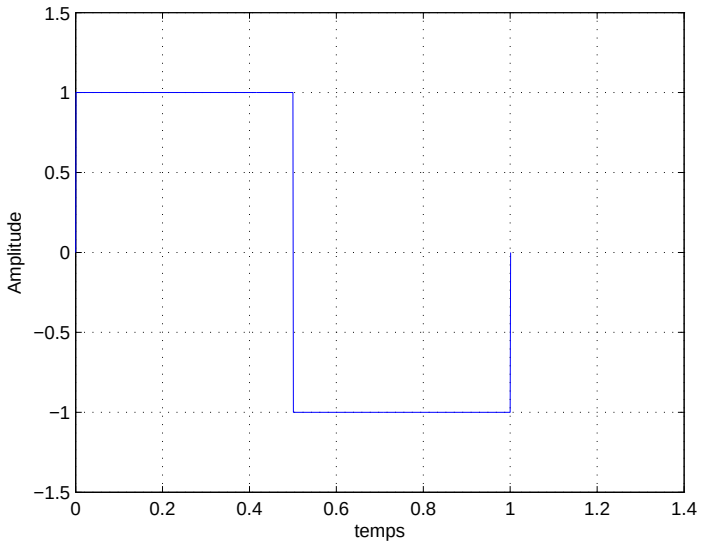


FIG. 2.3 : Ondelette de Haar.

La fonction-mère des ondelettes de Haar est une fonction constante par morceaux, elle est donnée comme suit :

$$\psi(t) = \begin{cases} 1 & \text{pour } 0 \leq t < \frac{1}{2} \\ -1 & \text{pour } \frac{1}{2} \leq t < 1 \\ 0 & \text{sinon} \end{cases} \tag{2.7}$$

La fonction d'échelle associée est alors une fonction porte :

$$f(t) = \begin{cases} 1 & \text{pour } 0 \leq t < 1 \\ 0 & \text{sinon} \end{cases} \tag{2.8}$$

◇ **Ondelettes à support compact (Daubechies)**

Cette famille d'ondelettes orthonormale est caractérisée par la compacité des supports. Cependant, elle n'est pas à phase linéaire. La compacité des fonctions de base et des filtres associés permet une réduction du coût de calcul, ce qui facilite d'envisager des applications en temps réel (KACHA, 2022). L'ondelette de Daubechies possède $q(\geq 2)$ moments nuls, soit donc :

$$\int_{-\infty}^{+\infty} t^n \psi(t) dt = 0, \quad n = 0, 1, \cdots, q-1 \tag{2.9}$$

ce qui permet d'écrire $G_0(f)$ sous la forme :

$$G_0(f) = \left(\frac{1 + e^{j2\pi f}}{2} \right)^q P(f) \tag{2.10}$$

où $P(f)$ est un polynôme trigonométrique. Le développement de la condition d'orthogonalité de $\psi(t)$ permet d'aboutir à une équation dont la solution fournit les coefficients du filtre associé à l'ondelette. La figure 2.4 représente graphiquement la fonction d'ondelette de Daubechies d'ordre 4 (KACHA, 2022) .

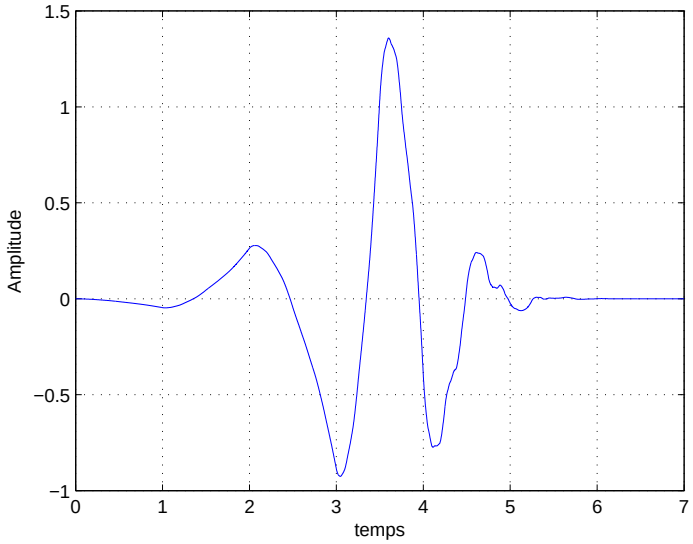


FIG. 2.4 : Ondelette de db4.

◇ Ondelette de Morlet

L'ondelette de Morlet est l'ondelette complexe la plus fréquemment utilisée. Elle est obtenue en modulant une exponentielle complexe par une enveloppe gaussienne. Elle permet de minimiser le produit des étalements temporel et fréquentiel de l'ondelette, et donc de maximiser la précision de la localisation de l'énergie dans le plan temps-fréquence. Cette ondelette est étroitement liée à la perception humaine, à la fois auditive et visuelle (G.Mallat). Elle est définie par :

$$\psi_\sigma(\mathrm{w}) = c_\sigma \pi^{-1/4} \left(e^{-1/2(\sigma - w)^2} - k_\sigma e^{-1/2w^2} \right) \tag{2.11}$$

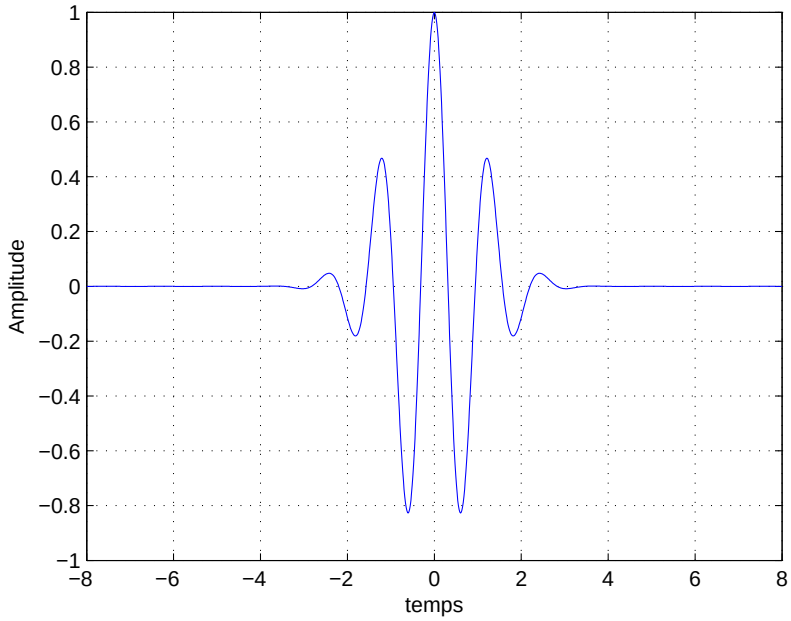


FIG. 2.5 : Ondelette de Morlet.

◇ Ondelette de Mexican Hat

L'ondelette de Mexican Hat est le négatif normalisé de la dérivée seconde d'une fonction gaussienne (Figure 2.6). Elle est généralement dénommée "chapeau mexicain" aux États-Unis, car la forme de sa courbe rappelle un chapeau typique du Mexique, le "sombrero". Elle est définie par :

$$\psi(x) = \frac{2}{\sqrt{3}}\pi^{-1/4}\left(1-x^2\right)e^{-x^2/2} \tag{2.12}$$

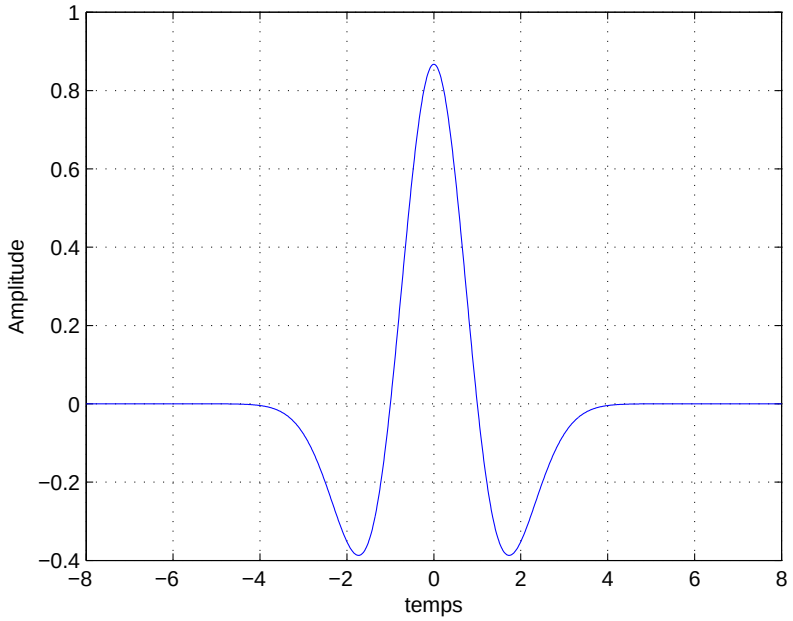


FIG. 2.6 : Ondelette de Mexican Hat.

La généralisation à plusieurs dimensions de cette ondelette est appelée fonction la placienne de Gauss. Dans la pratique, cette ondelette est parfois approchée par une différence de gaussiennes, car elle est séparable et permet donc de gagner un temps de calcul très important (BRINKS, 2008).

Les familles d'ondelettes peuvent être caractérisées par quatre propriétés principales : l'existence de filtres associés, l'orthogonalité ou bi-orthogonalité, le support compact ou non, l'ondelette réelle ou complexe.

Les ondelettes à filtre sont associées à des analyses multi-résolutions orthogonale sou bio-orthogonales, la transformée discrète et les calculs rapides en utilisant l'algorithme de mallât sont alors possibles. Les ondelettes sans filtres, en revanche, sont utiles pour la transformée en ondelettes continues (BEYLKIN, 1991).

2.3.2 Choix de la meilleure ondelette

Dans la littérature, il existe plusieurs types d'ondelettes. Le critère de choix de la meilleure ondelette reste un problème à déterminer. Malheureusement, il n'y a pas de d'ondelette qui soit meilleure que les autres, tout dépend de l'application. Dans certains cas, l'ondelette la plus simple (Haar) sera optimale. Pour d'autres

applications ce sera le pire des choix possibles (ABID, 2008).
Les fonctions gaussiennes sont souvent utilisées comme ondelettes pour la transformée continue en raison de leur bonne résolution cependant elles sont difficiles à implémenter.
En pratique le choix de la meilleure ondelette se base sur :

- La forme de l'ondelette analysante : plus la fonction ressemble à l'événement à traiter, plus l'analyse sera efficace .
- Les propriétés mathématiques (moments nuls, régularité,...).
- Une ondelette qui permet un traitement de signal efficace et acceptable, même si elle n'est pas la meilleure possible.

En théorie, plus la fonction ressemble à l'événement à traiter, plus l'analyse sera efficace. De toute façon, une ondelette optimale pour les signaux mesurés lors d'une certaine expérimentation dans un domaine donné ne le serait pas nécessairement lors d'une autre prise démesures pour un autre domaine.

2.4 Analyse multi-résolution (AMR)

Une analyse multi-résolution consiste à obtenir une approximation d'un signal f par projection de celui-ci sur l'espace d'approximation V_j, grâce à un opérateur A_j (MALLAT, 1989) et sur l'espace de détail W_j par le biais d'un opérateur D_j, cependant la reconstruction du signal f nécessite l'association des deux opérateurs tel que :

$$A_{j+1}f = A_j f + D_j f \tag{2.13}$$

L'analyse multi-résolution permet de rapprocher l'analyse en variable d'espace avec l'analyse en variable de fréquence. Elle formalise l'idée intuitive selon laquelle tout signal peut être construit par raffinements successifs, c'est-à-dire par l'ajout de détails lorsque l'on passe d'une résolution à la suivante.

D'une manière plus précise, une analyse multi-résolution de $L^2(\Re)$ est définie comme une suite de sous-espaces fermés V_j de $L^2(\Re)$, $j \in Z$, ayant les propriétés suivantes (MALLAT, 1989) :

✓$V_{j+1} \subset V_j$: l'approximation à la résolution a_j contient toutes les informations nécessaires pour calculer le même signal à la résolution inférieure a_{j+1}.
✓$f(x) \in V_j \Leftrightarrow f\left(\frac{x}{2}\right) \in V_{j+1}$: si $f(x)$ appartient à V_j, la même fonction dilatée d'un facteur 2 appartient à V_{j+1}.
✓$f(x) \in V_j \Leftrightarrow f\left(x - 2^j k\right) \in V_j$: si $f(x)$ appartient à V_j , la même fonction translatée d'un facteur quelconque appartient aussi à V_j .

2.5 Espaces d'approximations et détails

2.5.1 Fonction d'échelle et espaces d'approximation

La dernière propriété de l'analyse multi-résolution introduit une nouvelle fonction dite fonction d'échelle qui par dilatation et translation engendre une base orthonormée, Cette fonction sera notée $\varphi \in V_l \subset V_0$, elle est définie par l'expression suivante :

$$\varphi(x) = \sqrt{2}\sum_k h_k \varphi(2x-k) \tag{2.14}$$

La séquence h_k est la séquence génératrice de la fonction d'échelle : elle définit la multi résolution et permet d'engendrer la famille des fonctions aux différentes échelles. Cette séquence joue un rôle fondamental dans l'AMR. En revanche, Les fonctions d'échelle $\phi\, j,k$ $\varphi_{j,k}$ pour $k \in [-\infty, +\infty]$ engendrent l'espace des approximations V_j.

2.5.2 Fonction d'ondelette et espaces de détail

L'espace W_j complémentaire de V_j est l'espace des détails à l'échelle j. Ceci revient à dire chaque élément de V_{j-1} peut être écrit de manière unique comme la

somme d'un élément de W_j et d'un élément de V_j :

$$V_{j-1} = V_j \oplus W_j b \tag{2.15}$$

L'espace W_j contient l'information de détail nécessaire pour passer d'une résolution j à une résolution $j-1$. En revanche, à partir de la fonction d'échelle, il est possible de construire une fonction appelée ondelette qui par dilatations et translations engendre une base orthonormée des W_j. Cette fonction est notée :

$$\psi(x) \in L^2(\mathbb{R}) \tag{2.16}$$

L'ondelette $\psi(x)$ est dans le sous-espace W_1 qui est contenu dans V_o. Les fonctions d'échelle translatées $\varphi(2x-k)$ constituent une base de V_o. Il s'ensuit que l'ondelette $\psi(x)$ est une combinaison linéaire des fonctions d'échelle translatées :

$$\psi(x) = \sqrt{2}\sum_k g_k \varphi(2x-k) \tag{2.17}$$

Comme les fonctions d'échelle, les ondelettes sont engendrées par une séquence génératrice, g_k, qui définit l'AMR (LANANI, 2020).
La décomposition d'un signal 2D tel qu'une image selon l'AMR ce présente comme suit :

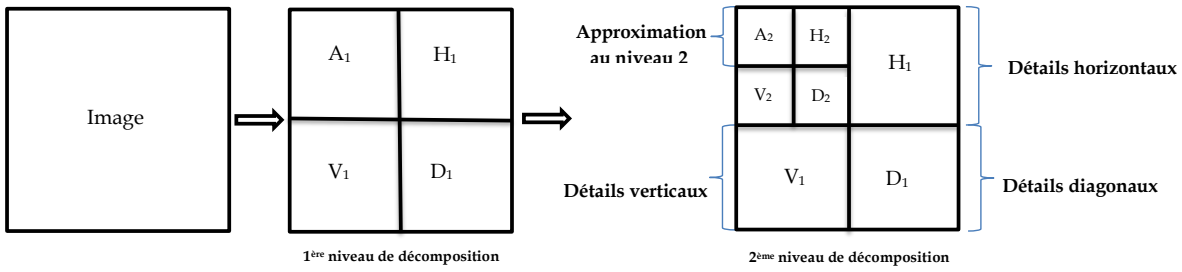


FIG. 2.7 : Décomposition d'ondelettes à différents niveaux.

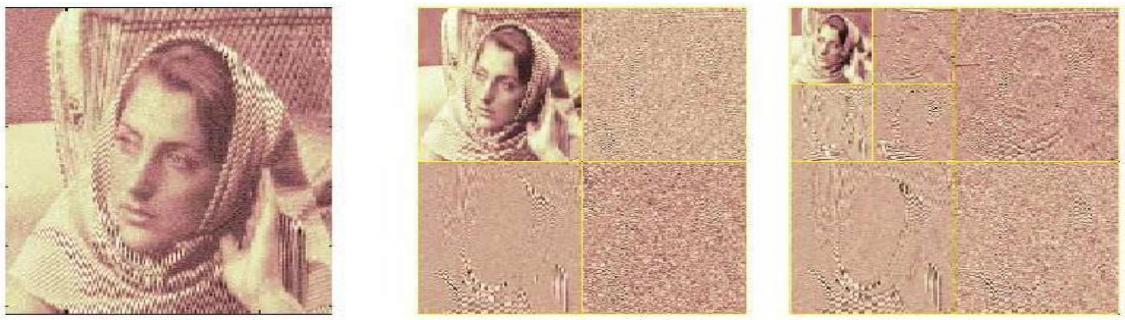


FIG. 2.8 : Exemple des 2 premiers niveaux d'une décomposition pyramidale en ondelettes.

2.6 Conclusion

Les ondelettes ont joué un rôle essentiel dans de nombreuses applications, en raison de leurs avantages et de leurs caractéristiques qui sont basées sur l'analyse du signal, qui joue un rôle crucial dans le traitement du signal numérique. Dans ce chapitre, notre objectif était de comprendre les ondelettes classiques, comment elles peuvent être utilisées dans le tatouage numérique.

Chapitre 3

RESULTATS DE SIMULATION

3.1 Introduction

Un tatouage numérique est une forme de marquage ou d'empreinte virtuelle qui est souvent appliquée à des médias numériques tels que des images numérique, des vidéos ou des documents. Il peut être utilisé pour identifier l'origine ou la propriété des médias, suivre leur utilisation ou fournir des informations supplémentaires.

Les méthodes de tatouage numérique varient en fonction des besoins spécifiques et des exigences de sécurité. Certaines méthodes de tatouage numérique sont visibles, telles que l'ajout d'un logo ou d'un texte directement sur l'image, tandis que d'autres sont invisibles, telles que l'incorporation de données imperceptibles dans le contenu lui-même. Les méthodes de tatouage numérique peuvent également être conçues pour être robustes contre diverses transformations ou altérations de l'image, telles que la compression, le recadrage ou le filtrage, afin d'assurer leur efficacité dans des environnements numériques dynamiques et variés.

Dans ce chapitre nous allons présenter les résultats de simulation de deux méthodes d'insertion et d'extraction de tatouage qui sont basées sur les valeurs singuliers SVD et la décomposition en ondelettes DWT.

3.2 Méthodes du tatouage numérique

Dans cette partie, nous expliquerons les méthodes utilisées pour insérer la marque numérique invisible dans l'image à protéger, qui sont les suivantes :

— Méthode 1 : nous utiliserons la décomposition SVD seulement pour faire le tatouage.

— Méthode 2 : Il s'agit d'un système hybride, dans lequel nous combinerons les deux techniques DWT et SVD, où l'on applique le SVD dans la bonde LL de la décomposition DWT du niveau 2.

3.3 Méthode du tatouage numérique basés sur le SVD

On présente l'algorithme spatial de tatouage numérique basé sur la SVD. Dans cet algorithme on utilise deux procédures d'insertion et d'extraction.

3.3.1 Transformée SVD

Toute image, indiquée par une matrice, peut être factorisée en un produit d'une matrice orthogonale par une matrice diagonale par une autre matrice orthogonale. On appelle cette transformation la décomposition en valeur singulières (SVD) d'une matrice. L'objectif de décomposition SVD est de crée une approximation de l'image en utilisant uniquement quelque termes de la matrice diagonale de la décomposition. Cette approximation est utilisée dans plusieurs domaines de traitement d'image tel que la compression d'image, le débruitage d'image, le tatouage, ...etc. La décomposition d'une image en SVD peut donc s'écrire :

$$I = U \times S \times V^T = \sum_{i=1}^{n} \sigma_i \times u_i \times v_i^T \tag{3.1}$$

Où S est une matrice dont les termes diagonaux sont positifs, et ordonnée d'une manière décroissante, tous les autres termes étant nuls. Les termes non nuls sont appelés valeurs singulières de l'image. Les valeurs singulières représentent

l'énergie de l'image (D. Chandra, 2002). Les colonnes de U et V sont appelées vecteurs singuliers gauche et droit de I respectivement, et représentent principalement les détails de la géométrie de l'image originale. U représente les détails horizontaux et V les détails verticaux de l'image originale. Ils y a deux caractéristiques importantes de la SVD pour qu'on l'utilise dans les schémas de tatouage numérique :

— une petite variation dans les valeurs singulières qui n'affecte pas la qualité de l'image.

— Les valeurs singulières d'une image en une grande stabilité et donc changent très peu après l'application des différentes attaques.

3.3.2 Algorithme d'insertion

La procédure d'insertion est représentée par la figure 3.1

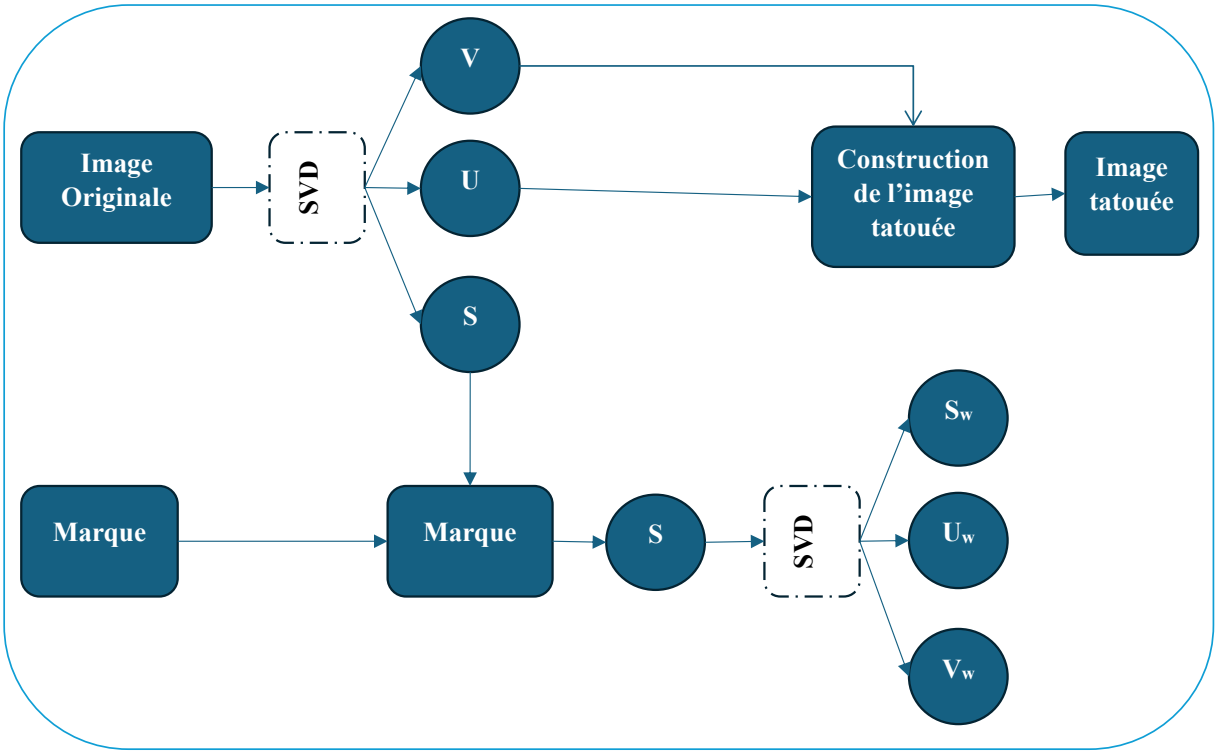


FIG. 3.1 : Procédure d'insertion de la marque de l'algorithme de tatouage numérique basé sur la SVD .

— **Étape 1** : On lit l'image sur laquelle on veut tatouer (image de couverture).

— **Étape 2** : Appliquer la décomposition en valeurs singulières SVD sur l'image de couverture, tel que :

$$svd(double(I)) = [U_y, S_y, V_y] \tag{3.2}$$

— **Étape 3** : On lit l'image de tatouage.

— **Étape 4** : Appliquer la décomposition en valeurs singulières SVD sur l'image de tatouage, tel que :

$$[U_w, S_w, V_w] = svd(double(I_{1_w})) \tag{3.3}$$

— **Étape 5** : Incorporer les valeurs singulières S_w dans la matrice S_y de l'image de couverture, comme suit :

$$S_{\text{mark}} = S_{\text{y}} + \alpha * S_{\text{w}} \tag{3.4}$$

Avec α : facteur de pondération, il contrôle la force d'insertion du tatouage.

— **Étape 6** : Appliquer la SVD inverse pour obtenir l'image tatouée, cela se fait en utilisant les composantes SVD de l'image de couverture et celles de la matrice S_mark.

$$\text{LL}_2 = U\text{y} \times S\,\text{mark} \mid \times V\text{y}_{\text{m}}^{\text{T}} \tag{3.5}$$

3.3.3 Algorithme d'extraction

La procédure d'extraction est représentée par la figure 3.2

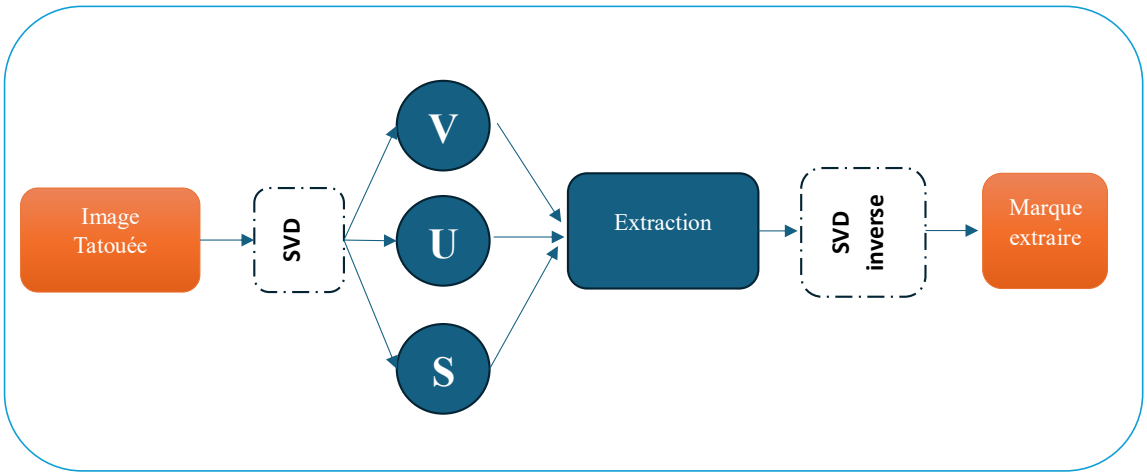


FIG. 3.2 : Procédure d'extraction de la marque de l'algorithme de tatouage numérique basé sur la SVD .

— **Étape 1** : Appliquer la décomposition en valeurs singulières sur l'image tatouée :

$$[Uy_wmv, Sy_wmv, Vy_wmv] = svd(I_1) \tag{3.6}$$

— **Étape 2** : Extraire les valeurs singulières du tatouage inséré en utilisant la matrice S_y de l'image de couverture ainsi que le facteur de pondération :

$$Swrec = (Sy_wmv - Sy)/\alpha \tag{3.7}$$

— **Étape 3** : Appliquer la SVD inverse pour la reconstruction de l'image du tatouage à base des composantes $[U_w, V_w]$ ainsi que la composante S_{wrec} extraite :

$$\mathrm{WMy} = U_{\mathrm{w}} \times S_{\mathrm{wrec}} \times V_{\mathrm{w}^{\mathrm{T}}} \tag{3.8}$$

3.4 Méthode de tatouage numérique basé sur la SVD et la DWT

Dans cette section on présente l'algorithme de tatouage numérique basé sur la SVD et la DWT. Cette algorithme contient deux procédures fondamentales, procédure d'insertion, et procédure d'extraction.

3.4.1 Algorithme d'insertion

La procédure d'insertion représentée par la figure 3.3, est décrite comme suit :

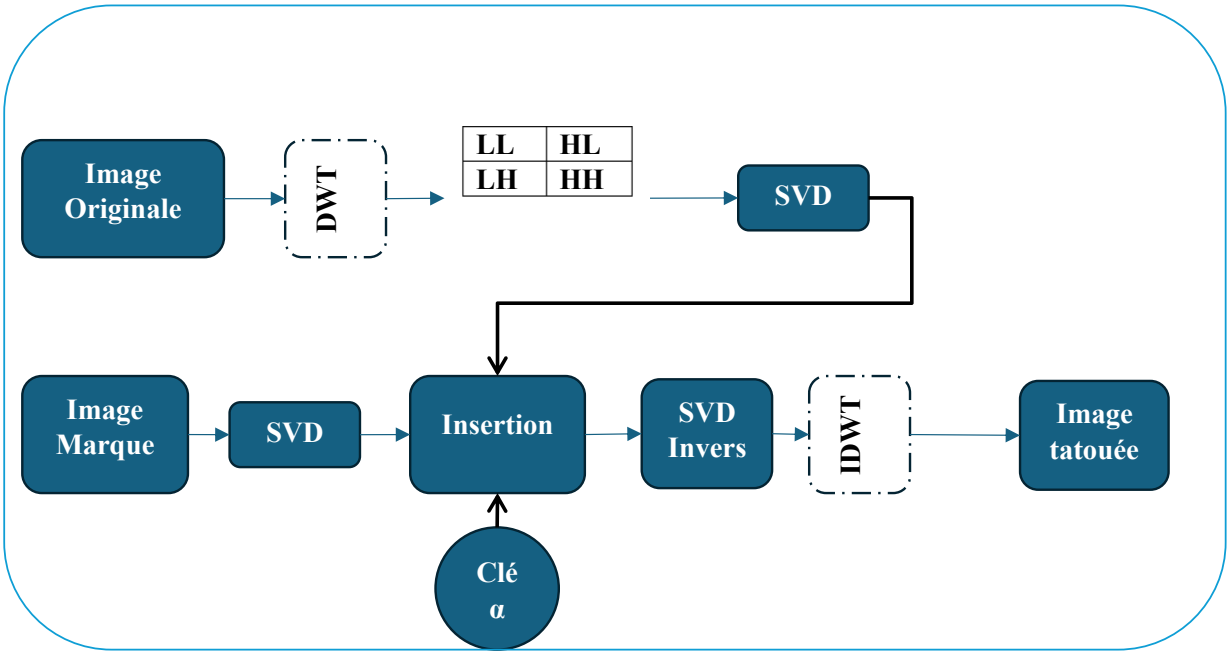


FIG. 3.3 : procédure d'insertion de l'algorithme de tatouage numérique basé sur la SVD et DWT.

— **Etape 1** : On lit l'image sur laquelle on veut tatouer 'image de couverture'.

— **Etape 2** : Effectuer la DWT niveau-2 à l'image originale.

— **Etape 3** : Appliquer la décomposition en valeurs singulières SVD sur la matrice d'approximation d'image de couverture, tel que :

$$SVD(LL2) = [Uy, Sy, Vy] \tag{3.9}$$

— **Etape 4** : On lit l'image de tatouage.

— **Etape 5** : Appliquer la décomposition en valeurs singulières SVD sur l'image de tatouage, tel que :

$$[Uw, Sw, Vw] = svd(double(I1_w)) \tag{3.10}$$

— **Etape 6** : Incorporer les valeurs singulières S_w dans la matrice S_y de l'image de couverture, comme suit :

$$S\,\text{mark} = S\text{y} + \alpha * S\text{w} \tag{3.11}$$

Avec α : facteur de pondération, il contrôle la force d'insertion du tatouage.

— **Etape 7** : Appliquer la SVD inverse pour obtenir l'image tatouée, cela se fait en utilisant les composantes SVD de l'image de couverture et celles de la matrice S_mark.

$$\text{LL2} = U\text{y} \times S\,\text{mark} \mid \times V\text{y}_\text{m}^\text{T} \tag{3.12}$$

— **Etape 8** : rassembler les blocs et appliquer la transformée en ondelettes inverse IDWT pour obtenir l'image tatouée.

3.4.2 Algorithme d'extraction

La procédure d'extraction de la marque est représentée par la figure 3.4.

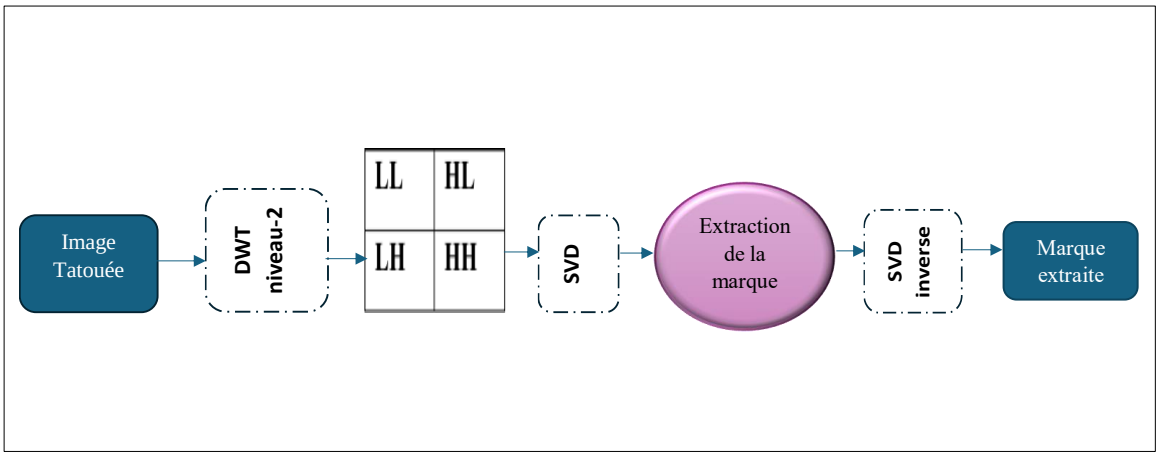


FIG. 3.4 : Procédure d'extraction de la marque de l'algorithme de tatouage numérique basé sur la SVD et la DWT.

— **Etape 1** : Effectuer la DWT niveau-2 à l'image tatouée.

— **Etape 2** : Appliquer la décomposition en valeurs singulières la matrice d'approximation d'image tatouée :

$$[Uy_w mv, Sy_w mv, Vy_w mv] = svd(LL2_w mv) \tag{3.13}$$

— **Etape 3** : Extraire les valeurs singulières du tatouage inséré en utilisant la matrice S_y de l'image de couverture ainsi que le facteur de pondération :

$$Swrec = (Sy_w mv - Sy)/\alpha \tag{3.14}$$

— **Etape 4** : Appliquer la SVD inverse pour la reconstruction de l'image du tatouage à base des composantes $[U_w, V_w]$ ainsi que la composante $S_w rec$ extraite :

$$\mathrm{WMy} = U\mathrm{w} \times S\ \mathrm{wrec}\ \times V\mathrm{w}^{\mathrm{T}} \tag{3.15}$$

3.5 Discussion des résultats obtenus

Nous avons appliqué deux techniques de tatouage toutes basées sur SVD et DWT afin de les comparer pour savoir lequel est le meilleur. Les résultats de simulation sont exposés sous forme des tableaux comparatifs afin de mieux distinguer les cas étudiés.

Cependant, pour étudier le critère d'imperceptibilité ainsi que la robustesse de ces méthodes, nous avons appliqué un ensemble d'attaques différents (bruit, compression, filtrage).

✓**Images de tests**

Les images de tests utilisées dans ce travail sont :

- L'image de couverture, , Cameraman, de taille (256 × 256).
- L'image du tatouage numérique, signe de l'université Tébessa , de taille (256 × 256).

Les deux images sont présentées respectivement dans la figure 3.5 ci-dessous :

(a) Image de couverture.

(b) Image de tatouage

FIG. 3.5 : Base d'images utilisées pour les tests de performances de tatouage.

✓**Mesures de qualité du tatouage**

La pertinence des méthodes de tatouage dépend de deux critères, subjectif et objectif permettant d'estimer l'efficacité de ces méthodes. Le critère subjectif représente l'aspect visuel. Ces critères recherchés ont pour objectifs de mesurer

le degré d'amélioration de l'image qui peut être selon l'application : la qualité visuelle de l'image, l'élimination ou la réduction du bruit, la préservation des détails et la préservation ou l'amélioration de la qualité du contraste. Les critères retenus sont les suivants :

A) Critère subjectif (aspect visuel)

L'œil humain est un outil essentiel pour apprécier la qualité d'une image. Il va permettre à l'utilisateur d'identifier le contenu des images, la netteté de celles-ci, la présence d'artefacts et la qualité des contours. Il est donc capital que les méthodes de tatouage en compte le système optique humain. Cependant, cette évaluation ne peut être que subjective puisqu'il n'existe aucune mesure correcte pouvant traduire fidèlement la perception de l'œil humain.

B) Critères objectifs

La performance d'une méthode de restauration peut être calculée à l'aide d'un des indicateurs suivants :

✓**Erreur quadratique moyenne (Mean Square Error MSE)**

L'image restaurée u est toujours comparée à l'originale u pour déterminer le rapport de différence. Ce critère est le plus utilisé. Il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et tatouées :

$$MSE(u,u') = \frac{1}{(N*M)} \sum\sum (u(i,j) - u'(i,j))^2 \tag{3.16}$$

avec u l'image originale, u l'image débruitée, M le nombre de lignes de l'image, N le nombre de colonnes de l'image et (i,j) le positionnement des pixels. La différence $u(i,j)$ –$u(i,j)$ est considérée comme un bruit (J.L.Olivès, 1998). La valeur la plus faible est à retenir, pas d'échelle de valeur. Pour corriger cet inconvénient (pour pouvoir effectuer des comparaisons), on emploie plutôt une version corrigée du rapport signal sur bruit, notée PSNR.

✓**Rapport signal sur bruit (Peak Signal to Noise Ratio PSNR)** Le PSNR est l'une des métriques les plus connues et les plus utilisées, c'est une mesure de

distorsion utilisée en image numérique. Elle est basée sur l'erreur quadratique moyenne et est donnée par :

$$PSNR(u,u') = 10log\frac{L_d^2}{MSE} \tag{3.17}$$

où L_d est la dynamique du signal (la valeur maximum possible pour un pixel), dans le cas standard d'une image codée sur 8-bits,$L_d = 255$. Sa valeur étant indéfinie lorsque les deux images comparées sont identiques et une valeur de PSNR infini correspond à une image non dégradée et cette valeur décroît en fonction de la dégradation (J. CoxI, 1997).

3.5.1 Simulation de la méthode du tatouage numérique basé sur la SVD

A) Résultats sans attaques

α	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image orginale			
Watermark			
Image tatouée			
Watermark extré			

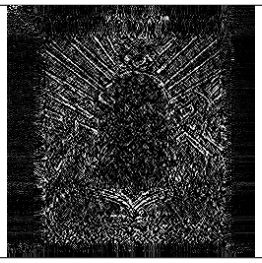
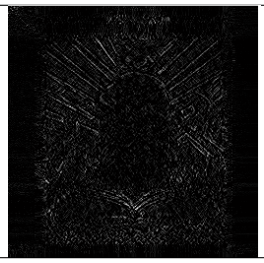
TAB. 3.1 : Images tatouées sans attaques par la méthode de SVD.

D'après les figures résultantes, nous pouvons bien remarquer que dans le cas où il n'y a aucune attaque les résultats d'extractions de tatouage sont bien restaurés pour tous les valeurs de α, cependant pour $\alpha = 0{,}75$ l'image tatouée est potentiellement dégradée.

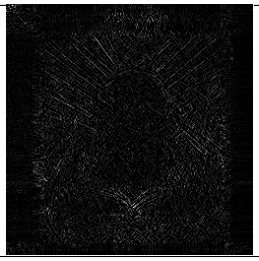
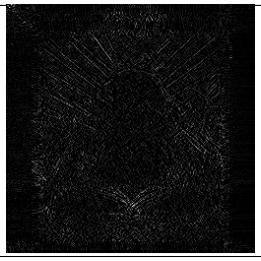
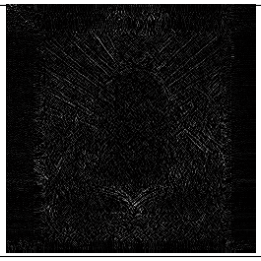
B) Résultats avec attaques :

✓**Attaque par l'ajout du bruit Gaussien et 'salt & pepper'**

Les images tatouées attaquées par ajout d'un bruit gaussien et 'salt & pepper' sont illustrées par les tableaux suivants :

Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaquée par bruit 'salt & pepper'			
Watermark extré			
PSNR	2,35 db	1,82 db	1,75 db

TAB. 3.2 : Images obtenues par la méthode **SVD** sous l'effet d'ajout d'un **bruit 'salt** & **pepper'**.

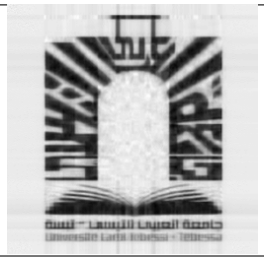
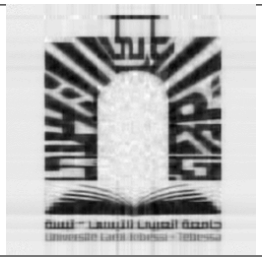
Facteur de pondération	$\alpha = 0{,}15$	$\alpha = ,60$	$\alpha = 0{,}75$
Image tatouée et attaquée par bruit 'Gaussien'			
Watermark extré			
PSNR	1,55 db	1,57 db	1,84 db

TAB. 3.3 : Images obtenues par la méthode **SVD** sous l'effet d'ajout d'un **bruit Gaussien**.

Les résultats obtenus lors d'attaques par l'ajout des bruits gaussien et sel & poivre indiquent que la qualité visuelle des tatouages extraits devient détériorée avec d'erreurs de détections en augmentant le facteur α. Dans ce cas, les valeurs du PSNR sont très faibles, ce qui confirme l'inefficacité de cette technique face à l'attaque du bruit.

✓**Attaque par l'ajout de la compression**

Les images tatouées attaquées par l'opération de compression sont présentées dans le tableau suivant :

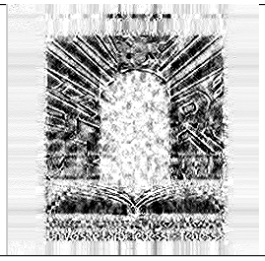
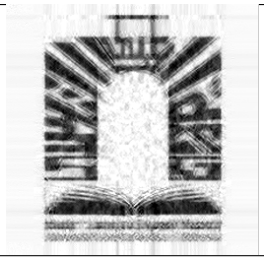
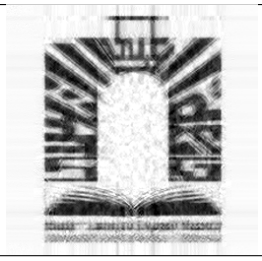
Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaqué par une compression			
Watermark extré			
PSNR	3,90 db	4,63 db	20,40 db

TAB. 3.4 : Images obtenues par la méthode **SVD** sous l'effet d'attaque de **compression**.

La plus grande valeur de $PSNR = 20{,}59$ db pour $\alpha = 0{,}2$, lorsque cette valeur augmente, la valeur de PSNR diminue et l'image sera déformée. Cette technique est inefficace pour l'attaque de compression.

✓**Attaque par filtrage**

Les images tatouées attaquées par l'action du filtrage sont illustrées dans le tableau suivant :

Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaqué par un filtrage			
Watermark extré			
PSNR	10,36 db	17,89 db	19,02 db

TAB. 3.5 : Images obtenues par la méthode **SVD** sous l'effet d'attaque de **filtrage**.

Dans ce cas, nous avons filtré les images tatouées pour différentes valeurs alpha afin de connaître leur effet sur la qualité des images extraites. Nous avons remarqué que la plus grande valeur de $PSNR = 19{,}33$ db lorsque la valeur $\alpha = 0{,}8$. La relation entre le facteur de pondération et le PSNR est une relation directe. Nous avons également remarqué que la qualité d'image est mauvaise si α est inférieur à $0,8$.

3.5.2 Simulation de la méthode du tatouage numérique basé sur la SVD et DWT

A) Résultats sans attaques

Nous avons appliqué l'algorithme hybride qui combine les techniques SVD et DWT pour insérer et extraire les tatouages des images. Nous avons également effectué une comparaison entre les watermarks réels et extraits, comme le montre le tableau suivant.

α	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image orginale			
Watermark			
Image tatouée			
Watermark extré			

TAB. 3.6 : Images tatouées sans attaques par la méthode de SVD et DWT

D'après les figures résultantes, nous pouvons bien remarquer que dans le cas où il n'y a aucune attaque les résultats d'extractions de tatouages sont bien restaurés pour tous les valeurs de α.

B) Résultats avec attaques :

Les images tatouées et les tatouages extraits en utilisant la technique de tatouage hybride DWT et SVD sont présentées sous forme de tableaux comparatifs afin de mieux distinguer les cas étudiés.

✓**Attaque par l'ajout du bruit Gaussien et 'salt** & **pepper'**

Les images tatouées attaquées par ajout d'un bruit gaussien et 'salt & pepper' sont illustrées par les tableaux suivants :

Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaquée par bruit 'salt & pepper'			
Watermark extré			
PSNR	16,75 db	25,35 db	28,93 db

TAB. 3.7 : Images obtenues par la méthode **SVD** & **DWT** sous l'effet d'ajout d'un **bruit 'salt** & **pepper'**.

Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaquée par bruit 'Gaussien'			
Watermark extré			
PSNR	19,90 db	31,41 db	31,25 db

TAB. 3.8 : Images obtenues par la méthode **SVD** & **DWT** sous l'effet d'ajout d'un **bruit Gaussien**.

Les résultats obtenus lors d'attaques par l'ajout des bruits gaussien et sel & poivre indiquent que la qualité visuelle des tatouages extraits devient moyenne, avec un valeur de PSNR variable entre 16 et 28 db Dans ce cas, les valeurs du PSNR sont moyennes, ce qui confirme l'efficacité de cette technique face à l'attaque du bruit.

✓ **Attaque par compression**

Les images tatouées attaquées par l'opération de compression sont présentées dans le tableau suivant :

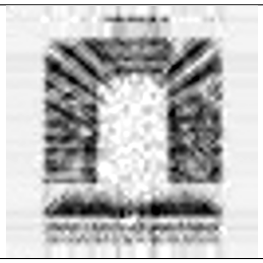
Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaqué par une compression			
Watermark extré			
PSNR	09,94db	21,97db	36,68db

TAB. 3.9 : Images obtenues par la méthode **SVD** & **DWT** sous l'effet d'attaque de **compression**.

La plus grande valeur de PSNR $= 36{,}68$ pour $\alpha = 0{,}75$, lorsque cette valeur augmente, la valeur de PSNR diminue et l'image sera déformée. L'efficacité de cette technique dépend de la valeur α . La qualité de l'image est déformée lorsque la valeur de α est supérieure à 0,75.

✓**Attaque par filtrage** :

Les images tatouées attaquées par l'action du filtrage sont illustrées dans le tableau suivant :

Facteur de pondération	$\alpha = 0{,}15$	$\alpha = 0{,}60$	$\alpha = 0{,}75$
Image tatouée et attaqué par un filtrage			
Watermark extré			
PSNR	8,11 db	16,63 db	18,05 db

TAB. 3.10 : Images obtenues par la méthode **SVD** & **DWT** sous l'effet d'attaque de **filtrage**.

Nous avons filtré les images tatouées pour différentes valeurs α afin de connaître leur effet sur la qualité des images extraites. Nous avons remarqué que la plus grande valeur de PSNR =18,05 db lorsque la valeur $\alpha = 0{,}75$. Cette technique est efficace si la valeur de PSNR est comprise entre $0,6$ et $0{,}75$.

3.6 Interprétation des résultats obtenus

Après avoir réalisé et simulé les résultats de l'algorithme, nous allons faire une étude comparative entre les deux méthodes qui se basent sur la SVD et DWT.

L'objectif c'est de faire le bon choix entre les méthodes présentées pour avoir un système de tatouage numérique efficace et robuste. D'après les résultats obtenus et les tableaux comparatifs et les figures 3.6 et 3.7 , nous remarquons que la combinaison entre les deux compositions SVD et DWT donne un résultat élevé et efficace (la méthode hybride).

D'autre part, cette combinaison entre les deux techniques rend le tatouage résiste contre les divers attaques (bruit, compression, filtrage) par rapport à l'algorithme qui repose sur une seule technique de SVD. Une différence largement remarquable entre les résultats des deux techniques, que ce soit dans les valeurs du PSNR ou dans la qualité visuelle d'image, en tenant compte de la valeur α qui doit être proportionnelle à l'algorithme.

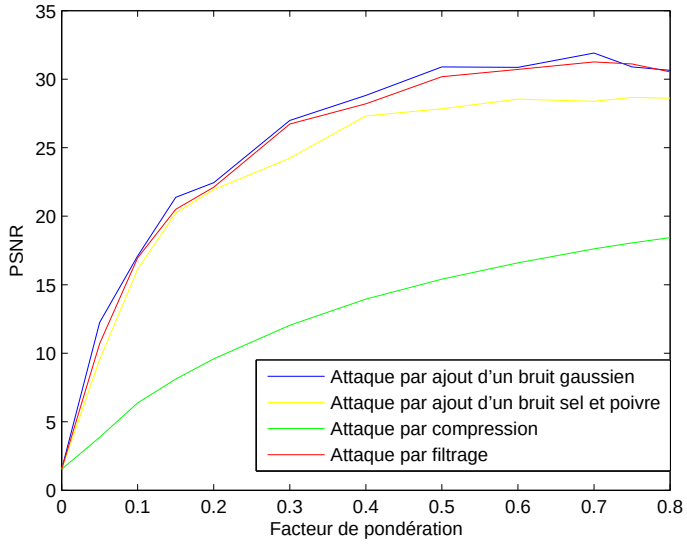


FIG. 3.6 : Comparaison entre les PSNR pour les attaques de la méthode DWT et SVD.

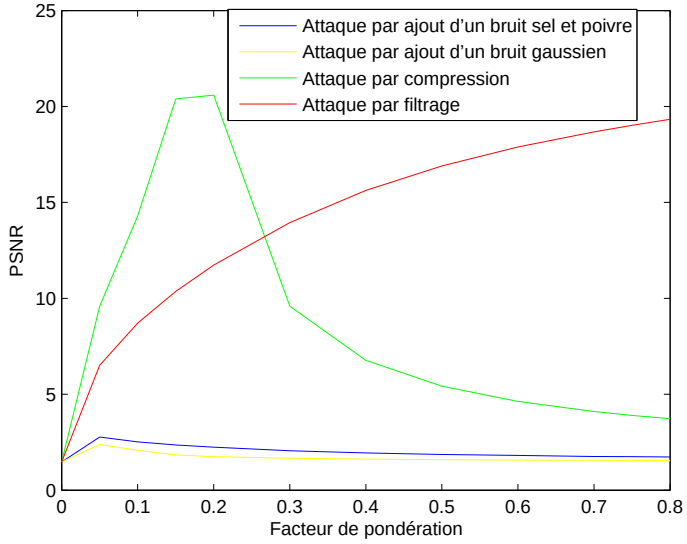


FIG. 3.7 : Comparaison entre les PSNR pour les attaques de la méthode SVD.

3.7 Conclusion

Dans ce travail nous avons exposé deux algorithmes de tatouage d'images basées sur les valeurs singuliers et la décomposition en ondelettes, dans l'objectif de vérifier l'authentification et protéger l'intégrité des images numériques. Nous concluons que la technique hybride de SVD et DWT est adaptée en termes d'imperceptibilité et de robustesse. Elle est aussi très efficace malgré les attaques que nous lui avons fait subir, car elle peut extraire facilement le watermark en utilisant uniquement l'image tatouée sans nécessité de l'image originale. Les résultats expérimentaux montrent la faisabilité de cette méthode, qui permet de maintenir une haute qualité d'images tatouées, et en même temps d'être moins sensible contre plusieurs types d'attaques comme la compression, l'ajout du bruit et le filtrage.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Le développement rapide des réseaux de communication a provoqué de nouveaux problèmes liés à la sécurité des documents ou des images échangés. La sécurisation des images stockées ou transmises, est habituellement réalisée par des algorithmes de tatouage.

Dans le cadre de ce mémoire nous avons présenté deux techniques de tatouage numérique pour résoudre le problème. Ces méthodes sont basées sur la DWT et la SVD.

Les résultats expérimentaux ont démontré que les techniques proposées sont efficaces et tout dépond des objectifs visés dans le processus de l'insertion et d'extraction du tatouage. De plus, l'efficacité de chaque méthode varie en fonction d'un choix de certains paramètres d'insertion du tatouage et les techniques de décomposition de l'image.

Afin de garantir l'efficacité de la méthode proposée, nous avons appliqué un ensemble d'attaques (bruit, compression, filtrage) sur les images tatouées pour voir l'étendue de leur impact et de leur force sur les méthodes que nous avons appliquée.

Pour la mesure de qualité nous avons utilisé le PSNR comme un critère d'évaluation, une étude comparative sous forme des tableaux représente les résultats des méthodes étudiées. D'où l'on peut conclure que la meilleure méthode est la méthode hybride qui est combinés de deux décompositions SVD et DWT, grâce à ses bons résultats face aux attaques auxquelles elle est exposée.

Perspectives

✓Une première perspective serait d'utiliser les ondelettes géométriques dans notre méthode afin d'améliorer la qualité de tatouage.

✓Une deuxième perspective serait d'appliquer l'outil de réseaux de neurones artificiels et accélère le processus de tatouage.

BIBLIOGRAPHIE

[ABID, 2008] ABID Tarek, 'Analyse du signal ECG par les ondelettes', mémoire Magister, Université Badji Mokhtar Université Annaba, 2008.

[A. Tirkel, 1993] A. A. Tirkel, G. Rankin, R. Schyndel, W. Ho, N. Mee, and C. Osborne : 'Electronic Watermark' . In DICTA 1993, pages 666–672, 1993.

[AHMED, 2007] AHMED Ben Atitallah, 'Etude et Implantation d'Algorithmes de Compression d'Images dans un Environnement Mixte Matériel et Logiciel', UNIVERSITE BORDEAUX I, 2007.

[Anne Manoury, 2001] Anne Manoury. 'Tatouage d'images numériques par paquets d'ondelettes', Ecole Centrale de Nantes (ECN), Université de Nantes, 2001.

[BELILITA Sarra, 2019] BELILITA Sarra, 'Développement et Implémentation d'algorithmes de tatouage robustes des images fixes et vidéo', thèse doctorat, Université Ferhat Abbas - SETIF1,2019 .

[BENYAHIA, 2014] BENYAHIA Ahmed, 'Application des ondelettes à la détermination de l'espacement moyen entre diffuseurs' , thèse doctorat, Université des sciences et de la technologie d'Oran Mohamed Boudiaf, 2014.

[BENJAMIN, 2011] BENJAMIN Mathon, 'Développement de méthodes de tatouage sûres pour le traçage de contenus multimédia', Université de Grenoble, 2011.

[BEYLKIN, 1991] BEYLKIN.G Coifman. R and Rokhlin. V (1991), "Fast wavelet transforms and numerical algorithms", Comm. Pure Appl. Math., 44, pp. 141–183.

[BOUGUERNE, 2017] BOUGUERNE IMEN. 'La Sélection des Caractéristiques Parallèle pour la Stéganalyse', thèse doctorat, UNIVERSITÉ BADJI MOKHTAR-ANNABA, 2017.

[BOUHOUS, 2018] BOUHOUS Adil, 'Sécurisation de l'information via un canal optique', pour l'obtention du Diplôme de Doctorat en Sciences en Electronique, Université Mohamed Seddik Ben Yahia,2018.

[BOUGEUERNE, 2017] BOUGUERNE , ' la sélection des caractéristiques parallèle pour la stéganalyse', Thèse de Doctorat, Université d'Annaba. Soutenue en 2017.

[BOUFENAR, 2016] BOUFENAR Mohamed, ' Approche comparative des techniques de detection et d'analyse en presence des defauts conjugues dans les machines tournantes', Ecole Nationale Polytechnique - ENP, 2016.

[BRINKS, 2008] BRINKS R, 'On the convergence of derivatives of B-splines to derivatives of the Gaussian functio', Comp. Appl. Math., 27, 1, 2008.

[BERNARD, 2002] Montaine Bernard, 'Méthodologie d'analyse des synchronisations neuronales dans les signaux EEG à l'aide de graphs d'information temps-fréquence', thèse doctorat, Université de Poitiers, Avril 2002.

[CHRISTIAN, 2003] CHRISTIAN REY , 'Tatouage d'image Gain en robustesse et intégrité des images',Thèse Doctorat de l'Université d'Avignon et des Pays de Vaucluse, 2003.

[C. REY, 2003] C. REY, Tatouage d'image : Gain en robustesse et intégrité des images, thèse de doctorat, université d'Avignon et des Pays de Vaucluse, Février 2003.

[Cox, 2003] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich et T. Kalker, Digital Watermarking, NEW YORK, Elsevier, 2008.

[KUNDUR, 1989] D. Kundur and D. Hatzinakos. 'Digital Watermarking Using Multi resolution Wavelet Decomposition', In IEEE International Conference on Acoustics, Speech and Signal Processing, Seattle, Washington, volume 5, pages 2969–2972, 1998.

[D. Chandra, 2002] D. Chandra, 'Digital Image Watermarking using Singular Value Decomposition', IEEE Midwest Symposium on Circuit and Systems, 2002.

[FARES, 2023] FARES Kahlessenane, 'Une approche aveugle et irréversible pour le tatouage d'images numériques dans le domaine spatiale', thèse doctorat, Université Kasdi Merbah de Ouargla, 2023.

[G. SIMMONS, 1998] G. SIMMONS , 'The History of Subliminal Channels', IEEE Journal on Selected Areas in Communications, Vol 16, No. 4: pp.452-462. May 1998.

[G.Mallat] Stéphane G.Mallat, "Time-Frequency Dictionaries".

[JEAN Luc, 2003] JEAN Luc Le Luron, 'Les images numériques, généralités' , 2003.

[JULIEN PUGLIESI, 2004] JULIEN PUGLIESI - Cedric PIOVANO, 'LE TATOUAGE D'IMAGES OÙ "WATERMARKING»'. Licence d'Informatique Travail d'études. Université de Nice - Sophia Antipolis, 2004.

[JAIDEVA, 1999] JAIDEVA C. Goswamiet Andrew K. Chan , 'Fundamentals of Wavelets : Theory, Algorithms, and Applications, Wiley Series in Microwave and Optical Engineering. Wiley Interscience, 1999.

[J.L.Olivès, 1998] J. L. Olivès, 'Opimisation globale d'un Système imageur à l'aide de critères de qualité visuelle', Thése de Doctorat,l'Ecole Nationale Supérieure de l'Aéronautique et de l'Espace, 1998.

[J. CoxI, 1997] J. CoxI, J. Killian, F. Leighton, T. Shamoon, 'Secure spread spectrum watermarking for multimedia', IEEE Transactions on Instrument and Measurements, 1997.

[KACHA, 2022] KACHA Abdellah, ' ANALYSE DES SIGNAUX DANS LE DOMAINE TEMPS-FREQUENCE', Thèse doctorat. UNIVERSITE FERHAT ABBAS – SETIF, 2022.

[K. Stefan, 2000] K. Stefan and A. Fabien, 'Information hiding techniques for steganography and digital watermarking', Artech House, London, UK, 2000.

[KHALED, 2010] KHALED LOUKHAOUKHA, 'Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective', Thèse doctorat, Faculté des Sciences et de Génie université LAVAL QUÉBEC, 2010.

[K. Amine, 2022] K. Amine, K. Redouane, and M. Bilel,'A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine application' , Multimed Tools Appl, Aug. 2022, doi : 10.1007/s11042-022-13649-7.H , 2022.

[Kok, 2002] J.J. Kok and M.J.G. van de Molengraft, 'Signal analysi', Technical report, Eindhoven University of Technology, Department of Mechanical Engineering, 2002.

[KHELIFA, 2013] KHELIFA Sofiane, 'Stabilité des signaux des séries temporelles de coordonnées de stations de géodésie spatiale issues des techniques radioélectriques (GPS, DORIS) et Laser (SLR)', thèse doctorat, Université des Sciences et de la Technologie d'Oran, 2013.

[LAIMECHE, 2009] LAIMECHE L., Merouani F.H., 'Détection des informations cachées dans les images numérique', Thèse de magistère, Université Badji Mokhtar, Annaba, 2009.

[Low, 2008] Low C.Y., Andrew B.J., Tee C, 'Fusion of LSB and DWT Biometric Watermarking for Offline Handwritten Signature', Congress on Image and Signal Processing, 2008.

[LANANI, 2020] LANANI Abderrahim, 'Construction d'une ondelette fractionnaire Adaptative Appliquée au Traitement de Signal et au Traitement d'image', thèse doctorat, Université Batna 2 – Mostefa Ben Boulaïd ,2020.

[SELLAMI, 2017] SELLAMI Chaima, 'Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète', dans université mohamed boudiaf - Msila, 2017. [2]

[Meina, 2008] Meina Amar, 'Masque psychovisuel à base d'ondelettes pour le Watermarking', hal.science, 2008.

[MALLAT, 1989] S. MALLAT, 'A theory for multi-resolution signal decomposition : the wavelet representation', IEEE, PAMI, vol. 11, N°7, pp. 674-693, 1989.

[P. BAS, 2000] P. BAS, 'Méthode de Tatouage d'image fondé sur le contenu', thèse de doctorat, Institut National Polytechnique de Grenoble, 2000.

[Pereira, 1999] S. Pereira, J. J. K. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of fourier-based watermarks using log-polar and log-log maps," IEEE International Conference on Multimedia Computing and Systems, pp 870–874, June 1999.

[R. Schyndel, 1994] R. Schyndel, A. Tirkel, and C. Osborne, "A Digital Watermark," In IEEE International Conference on Image Processing. ICIP, Vol. 2, pp. 86–90, 1994.

[Vidyasagar, 2009] Vidyasagar M. P., Song H., Elizabeth C. "A Survey of Digital Image watermarking Techniques". School of Information Systems, Curtin University of technology, Perth, Western Australie. 2009.