RÉPUBLIQUE DU CAMEROUN
****
Paix - Travail - Patrie
****
UNIVERSITÉ DE YAOUNDÉ I
****
FACULTÉ DES SCIENCES
****
DÉPARTEMENT D'INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
Peace - Work - Fatherland
****
UNIVERSITY OF YAOUNDE I
****
FACULTY OF SCIENCE
****
DEPARTMENT OF COMPUTER SCIENCE
****

Tatouage fragile et réversible pour l'authentification d'images basée sur la détection compressée.

En vue de l'obtention du diplôme de Master Recherche en Informatique

Option :
Sécurité des systèmes Informatiques

Rédigé par :
Dande Grace Asde
Matricule : 17R2895

Mémoire dirigé par :
Dr. AMINOU HALIDOU
Chargé de Cours, Université de Yaoundé I, FS

et par :
Dr. Ali Hamadou
Maître de conférences à L'Université Dan Dicko Dankoulodo de Maradi du Niger, FS

Année académique : 2024-2025

DÉDICACES

Je dédie ce mémoire à toute ma famille pour leur soutien indéfectible.

REMERCIEMENTS

Tout d'abord, je remercie l'Éternel Dieu pour le soutien qu'il m'a toujours apporté et pour l'accomplissement de ce travail ; sans lui, rien de cela n'aurait été possible. Je témoigne ma gratitude et ma reconnaissance à toutes les personnes ayant contribué à la réalisation de ce travail :

Au Dr. ALI AMADOU, à qui j'adresse ma gratitude infinie et mes sincères remerciements pour la qualité de l'encadrement, pour la patience, la rigueur et la disponibilité dont il a fait preuve depuis le premier jour, ainsi que pour ses encouragements permanents.

Au Dr. AMINOU ALIDOU, à qui j'adresse ma reconnaissance infinie et mes sincères remerciements pour m'avoir encadré, orienté, encouragé et conseillé. Sa rigueur et son exigence m'ont accompagné tout au long de ce travail, m'enseignant une méthodologie de recherche rigoureuse et une critique scientifique précieuse.

Aux membres de mon jury de soutenance, pour m'avoir fait l'honneur d'accepter d'évaluer ce travail.

À tout le corps enseignant de l'Université de Yaoundé 1 et, en particulier, du département d'Informatique pour la transmission de leur savoir.

À ma famille, et tout particulièrement à mon très cher frère DJIMASDE ASSIDE, pour son amour et sa précieuse contribution à mon parcours académique. En tant que mon tuteur, il a joué un rôle crucial dans mon succès en finançant mes études et en me guidant avec bienveillance et expertise tout au long de mon cursus. Mon très cher frère MBAIASDE DANIEL, pour son soutien moral et financier durant mes études. Sa présence encourageante et son soutien inconditionnel ont été des sources de motivation essentielles, m'aidant à persévérer dans les moments difficiles et à avancer avec confiance vers la réussite. À ma petite sœur bien-aimée, pour son amour et son encouragement.

Pour terminer, je remercie mon ami NOUBAISSEM Jeremie, pour son soutien émotionnel sans faille et ses multiples conseils. Son aide précieuse m'a accompagné tout au long de ce travail.

Enfin, à toutes les personnes ayant contribué de près ou de loin à la réalisation de ce travail, je présente ma profonde gratitude.

RÉSUMÉ

Dans un monde où la sécurité des données est devenue une priorité, le tatouage numérique émerge comme une solution essentielle pour garantir l'intégrité et l'authenticité des images numériques. Ce mémoire se concentre sur le développement d'un algorithme de tatouage fragile et réversible, visant à surmonter les défis liés aux attaques sophistiquées tout en préservant la qualité visuelle des images. L'objectif principal est de concevoir un algorithme qui combine la fragilité et la réversibilité pour récupérer l'image originale après extraction de la marque dissimiliée.

L'approche proposée repose sur une méthodologie en deux étapes, incluant l'insertion et la reconstruction de l'image. En utilisant des techniques avancées telles que la transformation en cosinus discrète (DCT) et la détection compressée, cette méthode assure une intégration efficace du filigrane tout en maintenant une haute imperceptibilité. Les résultats expérimentaux montrent que l'algorithme peut détecter avec précision les modifications apportées aux images et reconstruire celles-ci avec une qualité acceptable, même après des manipulations agressives.

Les résultats pertinents indiquent que le schéma d'authentification d'image réversible (RIA) proposé atteint des valeurs de PSNR supérieures à 35 dB, ce qui témoigne d'une bonne qualité d'image après tatouage. De plus, la précision de détection des falsifications est de 100 %, confirmant l'efficacité de l'algorithme. En comparaison avec des méthodes existantes, notre approche démontre des performances supérieures en termes de robustesse et de qualité de reconstruction, offrant ainsi une solution prometteuse pour la protection des images numériques dans divers domaines, notamment médical et juridique.

Mots-clés : Tatouage fragile, Tatouage réversible, Authentification, détection compressée.

ABSTRACT

In a world where data security has become a priority, digital watermarking emerges as an essential solution to ensure the integrity and authenticity of digital images. This thesis focuses on the development of a fragile and reversible watermarking algorithm aimed at overcoming the challenges posed by sophisticated attacks while preserving the visual quality of images. The primary objective is to design an algorithm that combines fragility, to detect alterations, and reversibility, to recover the original image after extracting the embedded watermark.

The proposed approach is based on a two step methodology, including the insertion and image reconstruction. By utilizing advanced techniques such as discrete cosine transform (DCT) and compressed sensing, this method ensures efficient watermark embedding while maintaining high imperceptibility. Experimental results demonstrate that the algorithm can accurately detect modifications made to images and reconstruct them with acceptable quality, even after aggressive manipulations.

The relevant results indicate that the proposed reversible image authentication (RIA) scheme achieves PSNR values exceeding 35 dB, which reflects good image quality after watermarking. Additionally, the tampering detection accuracy is 100%, confirming the algorithm's effectiveness. Compared to existing methods, our approach demonstrates superior performance in terms of robustness and reconstruction quality, offering a promising solution for the protection of digital images in various fields, including medical and legal domains.

Keyword : Fragile watermarking, Reversible watermarking, Authentication, Compressed detection.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATION

- **CS** : Compressed Sensing (La détection compressée)
- **DCT** : Discrete Cosine Transform (Transformée en cosinus discrète)
- **DWT** : Discrete Wavelet Transform (Transformée en ondelettes discrètes)
- **IM** : Insect Matrix (Matrice d'insectes)
- **IWT** : Integer Wavelet Transform (Transformation par ondelettes discrète entière)
- **OMP** : Orthogonal Matching Pursuit (Algorithme de poursuite par appariement orthogonal)
- **PEE** : Prediction Error Expansion (Expansion de l'erreur de prédiction)
- **PSNR** : Peak Signal-to-Noise Ratio (Rapport signal sur bruit de crête)
- **QIM** : Quantization Index Modulation (Modulation par indice de quantification)
- **RIA** : Reversible Image Authentication (Schéma d'authentification d'image réversible)
- **ROI** : Region of Interest (Région d'intérêt)
- **RONI** : Region of Non-Interest (Région hors d'intérêt)
- **SSIM** : Structural Similarity Index Measure (Indice de similarité structurelle)

INTRODUCTION

0.1 Contexte

Dans un monde où les données numériques sont de plus en plus vulnérables aux attaques, la sécurité des images est devenue un enjeu majeur. Selon un rapport récent de Cybersecurity Ventures, les violations de données ont augmenté de 67% depuis 2020, avec des pertes financières estimées à plus de 6 000 milliards de dollars en 2023. Parmi ces violations, les infractions aux droits d'auteur et les falsifications d'images représentent une part significative. Le tatouage numérique émerge comme une solution essentielle pour garantir l'intégrité et l'authenticité des images, notamment dans des domaines sensibles comme la médecine, la justice et la propriété intellectuelle.

0.2 Définitions de Base

- **Tatouage numérique** : Méthode d'insertion de données dans des supports numériques pour assurer leur intégrité et authentification.
- **Tatouage réversible** : Technique permettant de récupérer à la fois l'image originale et les données insérées, essentielles dans des contextes tels que la médecine et la justice.
- **Tatouage fragile** : Méthode sensible aux altérations, permettant de détecter toute modification sur une image.
- **Détection compressée (Compressed Sensing, CS)** : Une technique de traitement du signal permettant de reconstruire un signal à partir d'un nombre réduit d'échantillons, bien inférieur à celui requis par l'échantillonnage traditionnel.
- **Authentification** : Processus visant à vérifier l'identité d'une entité (personne, système ou donnée) ou à garantir l'intégrité d'un élément (image, document, etc.) afin d'assurer qu'il n'a pas été modifié ou falsifié.

0.3 Problématique

Dans un monde où les images numériques sont de plus en plus utilisées et partagées, leur intégrité et leur authenticité sont constamment menacées par des manipulations malveillantes ou accidentelles. Les propriétaires de ces images, soucieux de protéger leurs droits d'auteur et de garantir l'intégrité de leurs contenus, recherchent des solutions efficaces pour détecter les altérations et restaurer les images originales en cas de falsification. Le marquage numérique, en particulier les techniques de tatouage fragile et réversible, s'est imposé comme une méthode prometteuse pour répondre à ces besoins. Cependant, les méthodes existantes présentent des limites significatives.

D'une part, les algorithmes de tatouage fragile, bien que sensibles aux modifications, peinent à résister à des attaques sophistiquées telles que les transformations géométriques, les compressions agressives ou les attaques par collage. D'autre part, les techniques de tatouage réversible, bien qu'elles permettent de restaurer l'image originale après extraction de la marque, souffrent souvent d'une complexité algorithmique élevée, ce qui limite leur applicabilité dans des systèmes à faible ressources, comme les appareils mobiles ou les systèmes embarqués. De plus, la qualité visuelle des images tatouées peut être compromise, ce qui pose un problème dans des domaines sensibles comme la médecine ou la justice, où toute altération visuelle est inacceptable.

Face à ces défis, il est essentiel de développer une méthode de tatouage numérique qui combine à la fois fragilité pour détecter les altérations, réversibilité pour restaurer l'image originale, et robustesse pour résister aux attaques tout en maintenant une qualité visuelle optimale. Cette méthode doit également être suffisamment efficace pour être déployée dans des environnements à ressources limitées, où les contraintes de calcul et de mémoire sont strictes.

Compte tenu de ces enjeux, la question centrale de cette recherche est : Comment le tatouage numérique peut-il sécuriser les images contre les attaques sophistiquées tout en préservant leur qualité visuelle et en assurant une réversibilité efficace ? Cette question guide notre étude et met en lumière les lacunes des méthodes existantes, notamment leur sensibilité aux attaques.

0.4 Objectif de recherche

L'objectif principal de notre recherche est de développer un algorithme avec un PSNR > 35 dB, une précision de détection de 100 %, et une résistance aux attaques courantes basée sur la transformation en cosinus discrète (DCT) et la détection compressée (CS). Ces techniques ont été choisies pour leur complémentarité en termes de robustesse, d'efficacité informatique et de qualité visuelle.

La DCT permet une insertion imperceptible du filigrane dans les basses fréquences tout en assurant une résistance aux manipulations courantes. En outre, son utilisation dans les normes d'images facilite son intégration dans des environnements pratiques.

La CS exploite la parcimonie des signaux pour réduire la quantité de données nécessaires à leur reconstruction, garantissant ainsi une méthode compacte et efficace, particulièrement adaptée aux environnements à ressources limitées.

Ainsi, l'intégration de la DCT et de la CS assure une détection fiable des altérations et une restauration précise des régions manipulées, tout en maintenant une haute qualité visuelle des images tatouées.

0.5 Méthodologie

Pour mener à bien ce travail, une méthodologie structurée a été adoptée, se déclinant en deux principales étapes pour le tatouage fragile et réversible des images numériques. La phase d'insertion utilise la DCT pour transformer l'image en blocs fréquentiels et y intégrer un filigrane de manière imperceptible. La phase de reconstruction combine la détection compressée (CS) et l'algorithme OMP pour identifier et corriger les altérations tout en restaurant l'image originale. La CS permet une reconstruction précise à partir de mesures partielles, assurant à la fois fragilité et réversibilité.

0.6 Résultats attendus

Les résultats attendus de notre recherche sont les suivants :

- L'approche proposée devra garantir une imperceptibilité élevée du filigrane, avec des valeurs de PSNR supérieures à 35 dB et un SSIM proche de 1.
- Une détection précise des falsifications, avec une localisation optimale des zones altérées.
- Une reconstruction efficace des images, même après des manipulations agressives, tout en préservant la qualité visuelle.
- Une performance supérieure aux méthodes existantes en termes de robustesse et d'adaptabilité.

0.7 Plan du mémoire

Pour l'atteinte des objectifs susmentionnés, notre travail sera structuré ainsi :

— **Le chapitre 1** présentera les techniques de dissimulation de l'information et donc l'accent sera mis sur le tatouage numérique et à la fin nous ressortirons les travaux de tatouage liés au domaine fréquentiel ;

— **Le chapitre 2** proposera une méthode de tatouage numérique à travers les deux opérations de base que sont l'insertion et la reconstruction de l'image ;

— **Le chapitre 3** sera consacré à l'implémentation où nous mettrons l'accent sur l'environnement de développement et les jeux de données utilisées afin de valider notre méthode de approche proposée ;

— **Le chapitre 4** présentera les résultats des tests, l'analyse et une comparaison avec l'état de l'art révélant performances et limites.

CHAPITRE 1

TATOUAGE NUMÉRIQUE : ENJEUX ET INNOVATIONS POUR LA SÉCURITÉ DES IMAGES

Le marquage numérique a connu une croissance significative dans l'échange de fichiers et la communication. Son émergence découle de l'absence de méthodes fiables pour protéger les données, qui sont devenues vulnérables et faciles à compromettre. Pour bien saisir notre étude, il est essentiel de définir les notions fondamentales. Dans ce chapitre, nous aborderons les concepts pertinents avant de conclure par une revue des travaux antérieurs.

1.1 Techniques de Sécurisation des Données

L'essor du numérique impose des méthodes de protection des données assurant confidentialité, intégrité et authenticité. Parmi les plus utilisées, la stéganographie et le tatouage numérique.

La stéganographie consiste à cacher des informations dans des supports anodins sans les rendre détectables. Elle repose sur trois principes : imperceptibilité, capacité et robustesse. David Kahn (1996) a retracé son histoire, montrant son utilisation depuis l'Antiquité, tandis que Seitz et Jahnke l'ont adaptée aux médias numériques pour protéger les droits d'auteur et garantir l'intégrité des données. Elle est particulièrement utile dans les domaines militaire, diplomatique et de la protection des droits d'auteur, où la dissimulation de l'information est cruciale [2].

Le tatouage numérique, ou watermarking, consiste à insérer une marque dans des fichiers numériques pour garantir leur authenticité, intégrité et protection des droits d'auteur. Contrairement à la stéganographie, qui vise à cacher l'existence de l'information, le tatouage numérique rend la marque détectable tout en restant imperceptible à l'œil nu. Ces deux approches, illustrées dans la Figure 1.1, mettent en évidence les techniques de sécurisation des données numériques. Des auteurs comme Mousavi et al. [3] ont étudié l'application du tatouage numérique dans les images médicales en 2014, mettant en avant la robustesse et la réversibilité, tandis que Suhail et Mohamed ont classé les techniques selon leur domaine d'insertion (spatial, fréquentiel, basé sur le contenu). Le tatouage numérique est crucial dans des domaines sensibles comme la médecine et la justice, où il permet de détecter les altérations, de restaurer les images originales et de protéger les droits d'auteur, tout en contrôlant la distribution des contenus numériques [4].

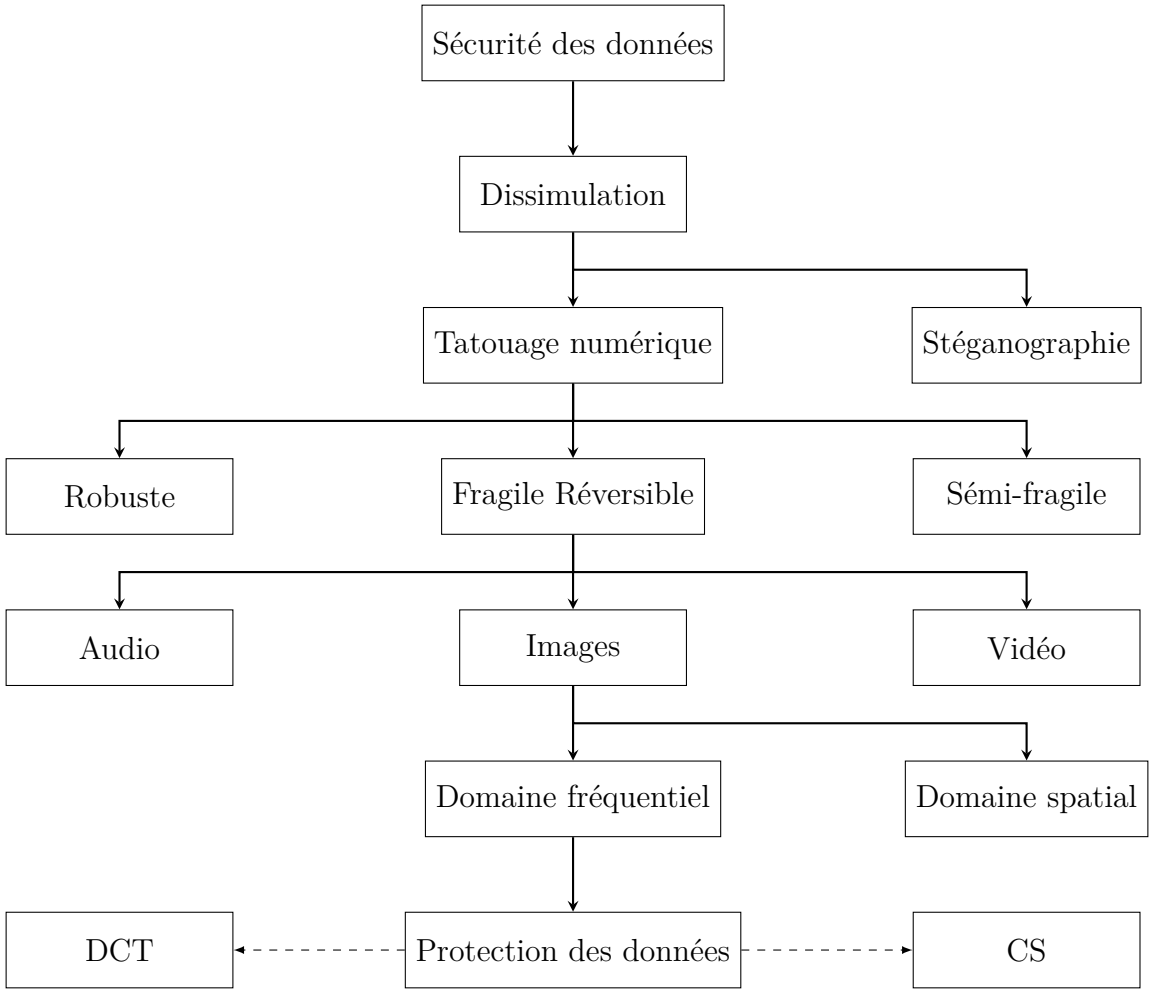

FIGURE 1.1 – Technique de la sécurité des données

TABLE 1.1 – **Tableau comparatif du tatouage numérique et de la stéganographie**

Aspect	**Stéganographie**	**Tatouage Numérique**
Visibilité	Invisible	Imperceptible à l'œil nu
Robustesse	Moins robuste aux manipulations	Plus robuste aux attaques
Réversibilité	Non réversible	Réversible dans certains cas
Capacité	Capacité limitée	Capacité variable selon la méthode

1.1.1 Description formelle du tatouage numérique

Un système de tatouage est decrit par Qasim et Asaad comme composé de deux sous-systèmes : un codeur et un décodeur. Formellement, ce système peut être décrit par (O, W, K, E_k, D_k), où O est l'ensemble des données originales, W est l'ensemble des watermarks et K est l'ensemble des clés à utiliser [5].

La fonction d'insertion du watermark (codeur) est décrite comme suit :

$$E_k : O \times W \times K \longrightarrow O$$
$$E_k(I_o, w, k) = I_w$$

Cette fonction prend en entrée un document original I_o, un watermark w et une clé privée ou publique k pour générer en sortie un document tatoué I_w comme illustré dans la Figure 1.2.

Le document original peut être un fichier texte, image, son ou une vidéo. Dans le reste de ce manuscrit, nous nous focalisons sur le tatouage d'images numériques.

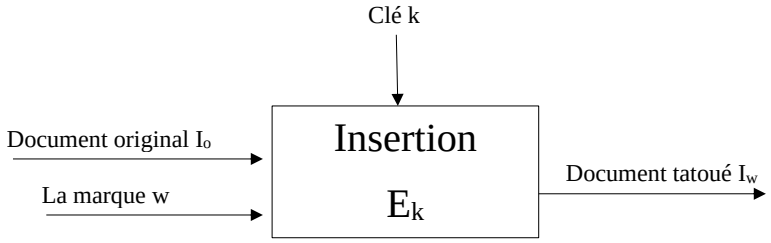

FIGURE 1.2 – Le processus d'insertion de la marque

La fonction d'extraction du watermark (décodeur) est définie comme suit :

$$D_k : \mathcal{O} \times \mathcal{K} \longrightarrow \mathcal{W}$$
$$D_k(I'_w, k) = w' \quad (2.2)$$

La fonction D_k prend en entrée un document tatoué et éventuellement attaqué I'_w et la clé k pour extraire en sortie le watermark w' comme illustré dans la Figure 1.3. Selon la technique utilisée, l'algorithme d'extraction peut exiger aussi le document original .

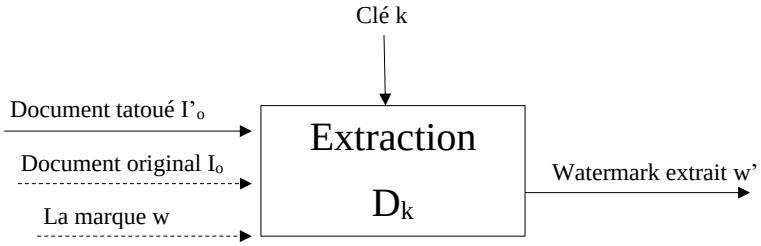

FIGURE 1.3 – Le processus d'extraction de la marque

1.1.2 Propriétés du tatouage numérique

Tout système de tatouage numérique doit être conçu en tenant compte de certaines propriétés essentielles, tout en répondant aux exigences fonctionnelles spécifiques à son domaine d'application. Mousavi et al. ont souligné que les propriétés du tatouage numérique peuvent être classées en quatre catégories principales : l'imperceptibilité, robustesse, capacité et type de détection du tatouage. Chacun de ces domaines impose des exigences spécifiques en matière de propriétés du tatouage [1].

- **l'imperceptibilité** est liée à la perception visuelle ou auditive des distorsions résultant à l'insertion de la marque dans un document. Le tatouage doit être invisible pour un observateur humain . De plus, la marque insérée ne devrait pas affecter la qualité du document.
- **La robustesse** représente la capacité du tatouage à résister aux dégradations du document tatoué. Ces altérations peuvent être accidentelles ou intentionnelles. La résistance à ces attaques est l'une des propriétés clés d'une méthode de tatouage.
- **la capacité** c'est la quantité d'information (en bits) que l'on peut insérer dans une image. Il faut que le nombre de bits insérés soit suffisant pour résister aux attaques .

1.1.3 Domaines d'applications

Les applications du tatouage numérique d'images sont différentes selon les objectifs de sécurité. On peut citer entre autres :

- **Protection du droit d'auteur** : la protection des droits d'auteur a été une des premières applications du tatouage numérique. Halima et al souligne qu'en cas de litige juridique, le propriétaire d'une image est en mesure d'apporter la preuve qu'il est le propriétaire même si celle-ci a subi des dégradations. Une telle application doit assurer une grande robustesse contre les attaques, éviter toute ambiguïté de la preuve et minimiser les distorsions lié à l'insertion de la marque [3].
- **Authentification du contenu d'une image** : L'idée de base de cette application consiste à insérer une marque fragile dans une image, qui sert à alerter l'utilisateur face à une éventuelle modification de l'image par une personne non autorisée et à localiser précisément les régions manipulées. Halima et al soulignent que cette application est généralement utilisée dans le domaine juridique et médical [3].
- **Contrôle du nombre de copies** : Halima et al décrivent que dans ce contexte, si une personne détient en main un document numérique et si elle est malintentionnée, elle peut produire illégalement un nombre illimité de copies de ce document avec une qualité égale au document d'origine. Le tatouage numérique peut faire face à cette situation. Des informations relatives au nombre de copies autorisées sont encryptées dans la marque. Ce principe a été utilisé dans les vidéos où la marque indique si la vidéo peut être recopiée ou non [3].

1.1.4 Classification des Techniques du Tatouage Numérique

Mousavi et al ont classé les systèmes de tatouage numérique suivant plusieurs critères notamment : le type des données utilisées, le domaine d'insertion, la perceptibilité humaine et la réversibilité. Ces classifications sont présentées dans la figure 1.4.

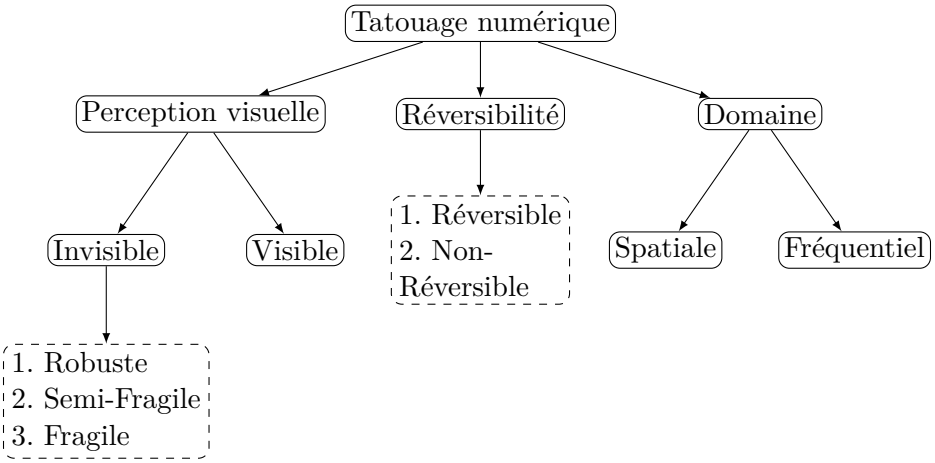

FIGURE 1.4 – Classification des méthodes de tatouage numérique [1]

a. Domaines d'insertion selon le type d'algorithme

Les techniques actuelles de tatouage ont été regroupées par Suhail et Mohamed en deux classes principales. La première classe comprend les techniques travaillant dans **le domaine spatial**, qui intègrent le watermark en modifiant directement les valeurs des pixels de l'image originale. La seconde classe regroupe les méthodes travaillant dans **le domaine fréquentiel** (ou transformé), où les données sont insérées en modulant les coefficients d'une transformée de signal original, offrant une plus grande robustesse aux attaques par rapport au tatouage spatial [6].

b. Réversibilité

La réversibilité permet de restaurer les données originales après extraction d'un filigrane, une caractéristique cruciale dans des domaines comme la médecine et la justice. Qasim et Asaad distinguent deux types de tatouage numérique : réversible et irréversible. **Un filigrane réversible** est un marquage numérique qui peut être retiré sans altérer le contenu ou la qualité de l'image, ce qui le rend utile pour la protection des droits d'auteur, la traçabilité ou la gestion des versions, tout en préservant l'intégrité et la lisibilité. En revanche, **un filigrane irréversible** est un marquage permanent appliqué à un document ou une image, difficile à supprimer sans altérer l'original. Il sert à protéger les droits d'auteur et à authentifier l'œuvre, dissuadant ainsi le vol ou l'utilisation non autorisée [5].

c. Catégorisation de la robustesse

La robustesse des tatouages numériques se divise en trois catégories : **Le tatouage fragile** est fortement sensible aux modifications de l'image tatouée et sert à prouver l'authenticité et l'intégrité d'un fichier tatoué. **Le tatouage semi-fragile** combine les caractéristiques du tatouage robuste et fragile pour avoir une situation intermédiaire, où la marque est robuste pour un ensemble défini de dégradations et fragile à d'autres. **Le tatouage robuste** dispose d'un vaste champ de théorie et de résultats, cherchant à préserver les données cachées face aux attaques, la marque devant être suffisamment résistante pour rester identifiable [1].

1.1.5 Les attaques liées au tatouage

L'un des aspects essentiels à considérer lors de l'élaboration d'un algorithme de tatouage numérique est la résistance de la marque. En effet, celle-ci doit être capable de supporter diverses altérations, qu'elles soient intentionnelles ou non. Hetatache et Karima classent les attaques en deux catégories [7].

- **attaques bienveillantes** : correspondent aux modifications appliquées par un utilisateur sans intention de nuire à la détection de la marque. Il peut s'agir de dégradations causées par une compression, un filtrage visant à réduire le bruit, une conversion de format, un ajustement de la résolution, etc.
- **attaques malveillantes** : désignent les manipulations visant spécifiquement à supprimer ou à compromettre l'extraction correcte de la marque.

1.2 Travaux antérieurs sur le tatouage numérique

Une analyse approfondie des travaux antérieurs révèle des cas concrets. Dans le domaine médical, les travaux de Guo et Zhu (2011) sur le tatouage réversible par DWT ont certes permis d'obtenir d'excellents résultats (PSNR $>$ 50 dB), mais cette méthode présente des limites notables. Elle s'avère particulièrement sensible aux attaques géométriques comme les rotations, ce qui peut compromettre son efficacité dans les environnements cliniques où les images sont souvent recadrées ou réorientées. De plus, l'algorithme nécessite des ressources de calcul importantes, limitant son utilisation sur des équipements médicaux anciens. Quant à l'approche de Memon et Alzahrani (2020), bien qu'innovante avec sa segmentation automatique ROI/RONI, elle montre une vulnérabilité aux attaques par bruit additif, et son processus de segmentation peut échouer sur des images médicales de faible qualité ou présentant des artefacts.

Dans le secteur culturel, le système de Cheddad et al. (2015) basé sur DCT, bien que robuste aux compressions JPEG, présente une capacité d'insertion limitée (moins de 0,5 bit par pixel), ce qui restreint la quantité d'informations pouvant être intégrées. Par ailleurs, cette méthode altère légèrement les détails fins des œuvres d'art, ce qui peut être problématique pour les reproductions haute résolution nécessaires aux analyses scientifiques. L'approche semi-fragile de Phadikar et Maity (2018), bien que précise, souffre d'un temps de traitement élevé pour les images de grande taille, rendant son déploiement à grande échelle difficile dans les musées possédant des collections numériques importantes.

Pour les applications juridiques, la méthode PEE de Thai-Son et Vo (2020) maintient certes une excellente qualité d'image, mais son processus de reconstruction nécessite des métadonnées supplémentaires, ce qui complexifie son implémentation dans les systèmes judiciaires existants. Le système extrêmement sensible de Zear et al. (2016) présente quant à lui un taux de faux positifs non négligeable (environ 3%) lorsqu'il est appliqué à des images acquises dans des conditions de faible luminosité, limitant sa fiabilité absolue dans les enquêtes criminelles.

Ces limitations communes à toutes les méthodes sensibilité à certains types d'attaques, contraintes de capacité, besoins en ressources de calcul mettent en lumière les défis persistants du tatouage numérique. Elles justifient la nécessité de poursuivre les recherches pour développer des solutions plus robustes et polyvalentes, capables de s'adapter aux évolutions constantes des techniques de falsification tout en restant accessibles et pratiques pour les utilisateurs finaux.

1.3 Les algorithmes du tatouage fragile et réversible

Cette section presente quelques travaux majeurs réalisés dans le domaine du tatouage fragile et réversible des images numériques dans différentes approches.

Thai-Son et Vo proposent une méthode d'authentification d'image réversible basée sur l'Expansion de l'Erreur de Prédiction (PEE). Cette méthode vise à détecter les zones altérées dans les images tout en préservant leur qualité d'origine sans distorsion. L'utilisation de PEE permet de masquer le code de manière à maintenir une distribution d'erreur de prédiction lisse, et de détecter les zones altérées en cas de suspicion de modification. Les résultats expérimentaux ont montré que la bonne qualité d'image obtenue par le schéma proposé atteint un PSNR moyen de 52,39 dB et 48,90 dB. Par conséquent, il est suggéré d'utiliser cette méthode pour détecter les régions altérées dans des applications spéciales, telles que les œuvres d'art, les images militaires et les images médicales, bien qu'elle ne prenne pas en compte les images en couleurs [8].

Memon et Alzahrani présentent un tatouage réversible pour les images Scanners , visant l'authentification du contenu et la protection des droits. Leur méthode segmente automatiquement l'image en ROI (région d'intérêt) et RONI (région non pertinente), intégrant un tatouage fragile dans la ROI pour détecter les altérations et un tatouage robuste dans la RONI pour la confidentialité. Basée sur une prédiction réversible, elle élimine le besoin de cartes de localisation, optimisant ainsi la capacité d'insertion. Les résultats montrent une excellente imperceptibilité et une restauration sans perte. Bien que prometteuse pour la télémédecine, sa résistance aux attaques mérite d'être approfondie [9].

Melendez-Melendez et Cumplido proposent une méthode RIA basée sur le compressed sensing pour vérifier et restaurer des images après des altérations. Ils créent des marques d'eau basées sur des valeurs de référence quantifiées et les intègrent dans les coefficients DCT des images. Cette méthode vise à améliorer la reconstruction des zones altérées, en particulier lorsque les attaques sont graves. Cependant, des limites potentielles incluent la capacité d'insertion limitée, la complexité du calcul, la sécurité et la qualité de l'image qui dépend d'un seuil fixe. Les résultats expérimentaux suggèrent fortement que la sparsité du signal devrait être davantage améliorée dans le domaine DCT pour obtenir de meilleures approximations de signal parcimonieux, en particulier lorsque les attaques sont plus agressives [10].

Azizoglu et Toprak proposent une méthode de watermarking numérique fragile réversible pour l'authentification et la protection de l'intégrité des images médicales. La méthode divise l'image en blocs de 8x8 et les transforme en domaines de fréquence via la Transformation en Ondelettes Discrètes (DWT), où l'information du watermark est intégrée. Pour corriger les erreurs d'arrondi lors de la transformation, ils utilisent l'algorithme Differential Evolution. Deux méthodes de localisation de l'altération sont proposées. Les résultats montrent une grande imperceptibilité de l'image watermarked, une extraction sans perte et une détection précise des altérations pour diverses attaques. En outre, la méthode proposée est fragile aux attaques telles que le filtrage, la compression, le flou, l'accentuation et l'ajout de bruit. Elle n'est pas adaptée à toutes les applications et images en couleurs [11].

1.4 Comparaison des différentes approches étudiées

Ce tableau propose une comparaison des différents travaux étudiés dans la revu .

Auteurs	*Approches*	*Résultat (PSNR)*	*Avantages*	*Limites*
Azizoglu et Toprak (2023)[11]	Transformée en ondelettes discrètes (DWT)	59 dB	- Haute imperceptibilité - Localisation précise des altérations	- Compatible seulement avec les images médicales (DICOM) - Sensible à la compression
Melendez et Cumplido (2022)[10]	Transformée en cosinus discrète (DCT) combinée à la détection compressée (CS)	48 dB	- Reconstruction des zones altérées - Détection et localisation précise des falsifications	- Reconstruction difficile si l'altérations($> 60\%$) - Sensible aux attaques agressives (compression)
Memon et Alzahrani (2021)[9]	Expansion de l'erreur de prédiction (PEE)	56 dB	- Restauration sans perte de ROI et RONI. - Image restaurée sans perte - Bonne qualité visuelle	- Sensible aux attaques (bruit) - Dépendance à la qualité de segmentation : Erreurs de segmentation pourraient affecter le watermarking
Thai-Son et Vo (2020)[8]	Expansion de l'erreur de prédiction (PEE)	52 dB	- Bonne détection des falsifications - Reconstruction complète de l'image originale	- Faible capacité (2 bits/bloc) - Sensible aux attaques géométriques

TABLE 1.2 – **Tableau comparatif des différentes approches**

Ce chapitre a présenté les fondements du tatouage numérique, en abordant ses techniques, propriétés et applications. Nous avons distingué les méthodes spatiales et fréquentielles, ainsi que les approches robustes, fragiles et réversibles.Le Tableau 1.2 synthétise les principales approches de tatouage numérique issues des travaux recents, comparant leurs caractéristiques en termes de domaine d'insertion, robustesse et réversibilité. Les travaux antérieurs ont démontré l'importance du tatouage pour l'authentification et la protection des images, notamment dans des domaines sensibles. Notre étude s'inscrit dans cette dynamique en proposant une méthode combinant DCT et détection compressée, offrant ainsi une solution équilibrée entre sécurité et qualité visuelle.

CHAPITRE 2

AUTHENTIFICATION D'IMAGES BASÉE SUR LA DCT ET LA DECTION COMPRESSÉE

L'objectif de ce chapitre est de décrire la méthodologie proposée, en mettant en avant les aspects théoriques et pratiques de notre algorithme. Nous commencerons par présenter le modèle global decrit dans la figure 2.1, suivi d'une explication détaillée des étapes . Enfin, nous aborderons les techniques utilisées pour garantir une détection précise et une restauration efficace.

2.1 Approche proposée

Dans cette partie, nous allons tout d'abord présenter l'algorithme de tatouage qui sera utilisé ensuite nous terminerons par la présentation de notre modèle avec ses différentes parties.

2.1.1 Algorithme utilisé

Ev vu de justifier le choix de la **Transformée en Cosinus Discrète (DCT)** et de la **Détection Compressée (CS)**, nous avons resumé dans le tableau 2.1 réalisé une comparaison quantitative avec d'autres méthodes fréquemment utilisées dans la littérature. Les critères retenus incluent l'**imperceptibilité**, la **robustesse** et la **capacité d'insertion**.

TABLE 2.1 – **Comparaison des techniques de tatouage numérique**

Technique	**Fragilité**	**Réversibilité**	**Robustesse**	**Imperceptibilité (SSIM)**
DCT + CS	Haute	Oui	Élevée	0.98
DWT	Moyenne	Oui	Moyenne	0.96
PEE	Haute	Oui	Faible	0.95
Spatial (LSB)	Faible	Non	Très faible	0.90

— La **DCT** offre un meilleur compromis entre imperceptibilité et robustesse grâce à sa capacité à concentrer l'énergie dans les basses fréquences.

— La **CS** améliore la reconstruction des zones altérées en exploitant la parcimonie des signaux, contrairement à la DWT ou aux méthodes spatiales.

2.1.2 Modèle proposé

La méthodologie est structure en deux étapes : l'insertion et la reconstruction.

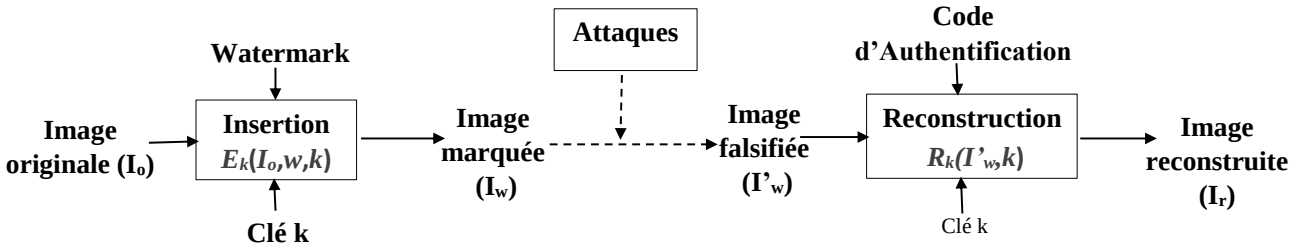

FIGURE 2.1 – Architecture du modèle d'authentification

2.1.3 Insertion du Filigrane

L'image est divisée en blocs de 32x32 pixels pour un traitement localisé. Chaque bloc subit une DCT, séparant les composantes fréquentielles. Le filigrane est inséré dans les fréquences peu perceptibles. Un seuil adaptatif détermine les coefficients DCT à conserver ou compresser, optimisant l'insertion. Les coefficients sélectionnés sont compressés via une fonction logarithmique pour minimiser l'impact visuel. Enfin, le filigrane généré à partir des coefficients compressés est intégré à l'image, assurant une imperceptibilité tout en restant détectable lors de la vérification. Le tout resumé par l'equation 2.1 suivante :

$$I_W = \sum_{k=1}^{N} \mathrm{DCT}^{-1}\left(\mathrm{DCT}(B_k - 128) + \alpha \cdot W_k \cdot \sigma_k\right) \quad (2.1)$$

Amélioration du seuil adaptatif

Contrairement à l'article de base [10] qui utilisent un seuil statique (par exemple, une valeur fixe de 15), notre méthode propose un seuil dynamique $T_d(k) = \alpha \cdot \sigma_k$, où σ_k est l'écart-type des valeurs du bloc B_k. Cette adaptation dynamique permet une meilleure prise en compte des variations locales dans l'image, optimisant ainsi l'insertion du filigrane tout en préservant la qualité visuelle. Cela améliore significativement la robustesse et l'imperceptibilité comparativement aux méthodes à seuil fixe.

Algorithm 1 Algorithme d'Insertion du Filigrane

Entrées : Image I, Filigrane W, Facteur α, Matrice M
Sortie : Image marquée I_W
$n \leftarrow 256$ {Nombre de blocs}
$k \leftarrow 1$ {Initialisation du compteur}
while $k \leq n$ **do**
    $B_k \leftarrow \text{ExtraireBloc}(I, k)$ {Bloc 32×32}
    $D_k \leftarrow \text{DCT}(B_k - 128)$ {Transformation DCT}
    $T_d \leftarrow \alpha \times \sigma(B_k)$ {Seuil adaptatif}
    $Cgs \leftarrow \text{AppliquerSeuil}(D_k, T_d)$ {Coefficients clairsemés}
    $r \leftarrow M \times Cgs$ {Projection linéaire}
    $W_k \leftarrow \text{Quantifier}(r)$ {Préparation du filigrane}
    $B'_k \leftarrow \text{InsererFiligrane}(B_k, W_k)$ {Insertion}
    $k \leftarrow k + 1$
end while
$I_W \leftarrow \text{ReconstruireImage}(B'_1, \ldots, B'_n)$
return I_W =0

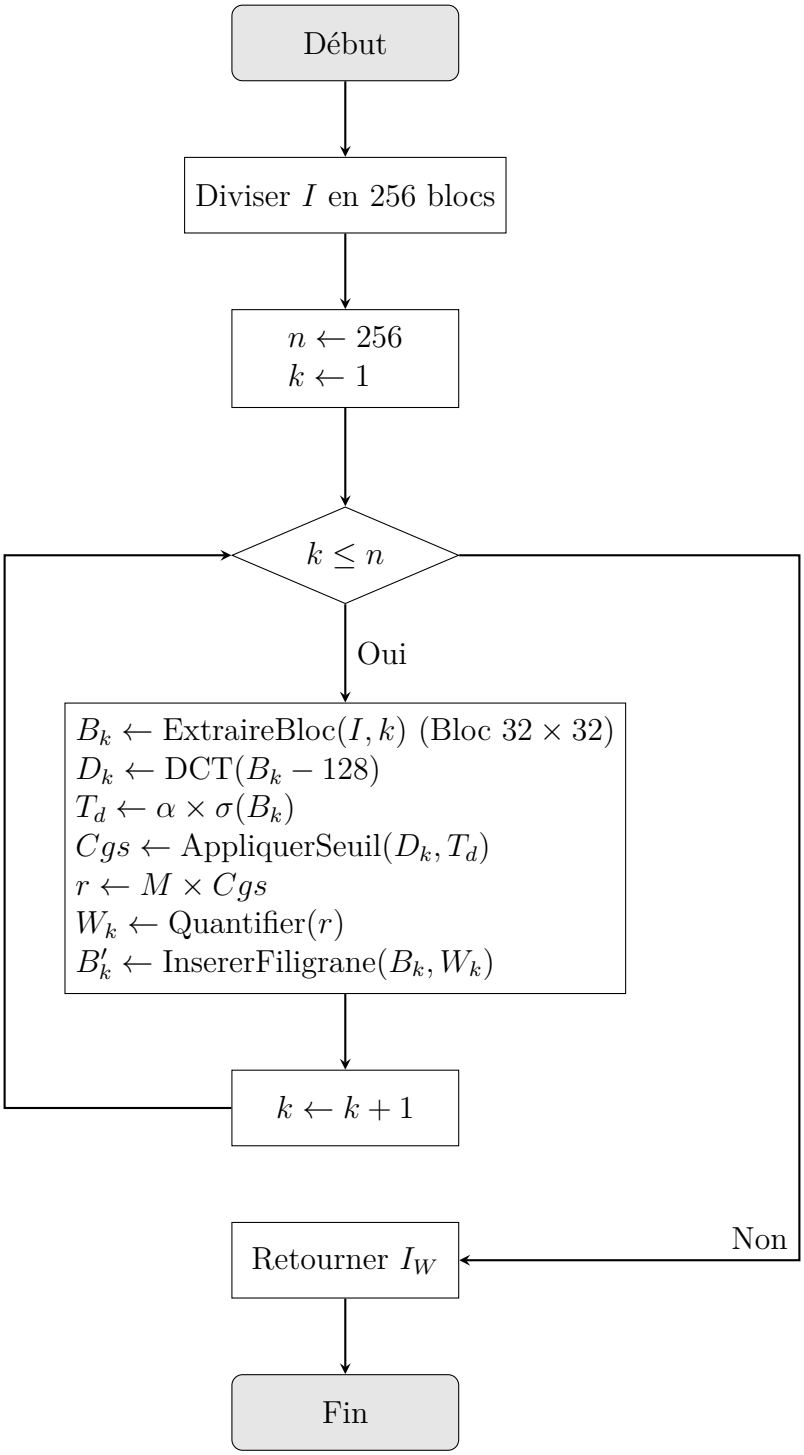

FIGURE 2.2 – Organigramme de l'algorithme d'insertion du filigrane

2.1.4 Reconstruction de l'image

Lors de la vérification, l'image est à nouveau divisée en blocs. Le filigrane est extrait de chaque bloc et comparé à la version originale. Si une différence est détectée, cela indique une altération de l'image.

Pour reconstruire les parties altérées, l'algorithme utilise une technique appelée détection compressée (CS) combinée à l'algorithme OMP (Orthogonal Matching Pursuit). Cette méthode permet de reconstruire les données manquantes ou corrompues à partir d'un nombre limité de mesures, en exploitant la propriété de parcimonie des signaux dans le domaine fréquentiel.

Une fois les coefficients reconstruits, une DCT inverse est appliquée pour retrouver les valeurs spatiales des pixels. Cette étape permet de restaurer l'image originale avec une qualité visuelle élevée, même après des manipulations importantes.

Le tout resumé par l'equation 2.2 suivante :

$$I_r = \sum_{k=1}^{N} \mathrm{DCT}^{-1} \left(\mathrm{OMP} \left(M, r'_k, \text{SHA-256}(B'_k) \right) \right) \quad (2.2)$$

Algorithm 2 Algorithme de Reconstruction de l'Image

Require: : I'_w (L'image marquée falsifiée).
Ensure: :I_r (L'image reconstruite)

1: $blocs \leftarrow diviser\_en\_blocs(image\_marquee, 32)$ {Diviser l'image en blocs de 32x32}
2: $blocs\_falsifies \leftarrow []$ {Initialiser une liste pour stocker les blocs falsifiés}

3: **for** $k = 1$ **to** n **do**
4: $W_k \leftarrow extraire\_filigrane(bloc)$ {Extraire le filigrane du bloc}
5: $a_n \leftarrow SHA256(bloc, index, W_k)$ {Calculer le code d'authentification}

6: **if** $a_n \neq a'_e$ **then**
{Vérifier si le bloc est falsifié} $blocs\_falsifies.append(bloc)$ {Ajouter le bloc à la liste des blocs falsifiés}
7: 8: **end if**
9: **end for**

10: **for** chaque $bloc\_falsifie$ dans $blocs\_falsifies$ **do**
11: $Cgs\_T \leftarrow OMP(Cgs\_T, M, r)$ {Appliquer l'algorithme OMP pour reconstruire les coefficients}
12: $bloc\_reconstruit \leftarrow DCT\_inverse(Cgs\_T)$ {Appliquer la DCT inverse pour obtenir le bloc reconstruit}
13: $remplacer\_bloc(image\_marquee, bloc\_falsifie, bloc\_reconstruit)$ {Remplacer le bloc falsifié}
14: **end for**

15: **return** l'image reconstruite I_r =0

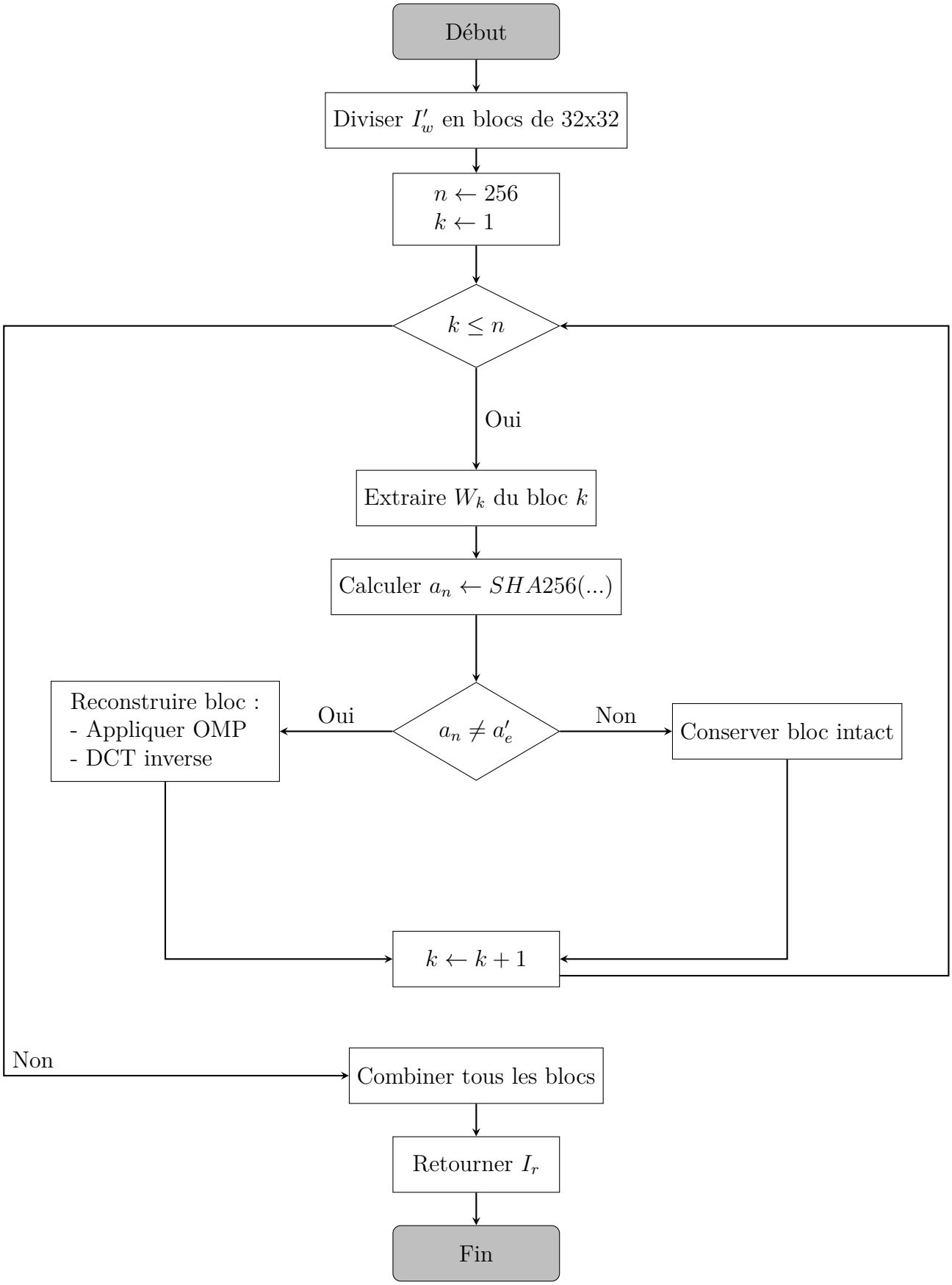

FIGURE 2.3 – Organigramme de l'algorithme de reconstruction

2.2 Théories mathématiques

Nous allons mettre en évidence les formules mathématiques clés nécessaires pour effectuer les opérations de l'insertion à la reconstruction.

2.2.1 Phase d'insertion du Filigrane

Division de l'Image en Blocs : L'image originale I_c est divisée en blocs non chevauchants de taille 32×32 pixels. Chaque bloc B_k est transformé en domaine fréquentiel à l'aide de la transformation en cosinus discrète (DCT) :

$$D_k = \mathrm{DCT}(B_k - 128) \quad (2.3)$$

où D_k représente les coefficients fréquentiels du bloc B_k.

Application d'un Seuil Adaptatif : Un seuil adaptatif $T_d(k)$ est appliqué pour améliorer la parcimonie des coefficients :

$$T_d(k) = \alpha \cdot \sigma_k \quad (2.4)$$

où σ_k est l'écart-type des valeurs dans le bloc B_k, et α est un facteur d'ajustement déterminé expérimentalement.

Compression des Coefficients : Les coefficients des sous-bandes haute fréquence sont compressés à l'aide d'une fonction logarithmique :

$$\tilde{c} = \begin{cases} c & \text{si } |c| < T_c \\ \log(|c| + 1) & \text{si } |c| \geq T_c \end{cases} \quad (2.5)$$

où c est le coefficient initial et T_c est un seuil de compression.

Génération du Filigrane : Une matrice de mesure M est utilisée pour projeter les coefficients compressés et générer le filigrane W_k :

$$\mathbf{r} = M \cdot Cgs \quad (2.6)$$

où Cgs représente les coefficients compressés et $\mathbf{r}$ est le vecteur des mesures projetées.

Insertion du Filigrane

Le filigrane W_k est inséré dans les blocs d'image en utilisant une technique de compression logarithmique et une transformation par ondelettes discrètes entières (IWT). Les bits du filigrane sont ajoutés aux coefficients compressés :

$$\tilde{c}_w = 2 \cdot \tilde{c} + b \quad (2.7)$$

où $b \in \{0, 1\}$ est le bit du filigrane à insérer et $\tilde{c}_w$ le coefficient marqué avec le bit de filigrane.

2.2.2 Phase de reconstruction des Blocs Altérés

Extraction du Filigrane

L'extraction du filigrane est réalisée en inversant le processus d'insertion. Les bits du filigrane sont extraits des coefficients compressés $\tilde{c}'_w$ à l'aide de la formule suivante :

$$\tilde{c}' = \frac{\tilde{c}'_w - b'}{2} \quad (2.8)$$

où b' est le bit du filigrane extrait.

Détection des Falsifications

Calcul du Code d'Authentification : Pour chaque bloc, un nouveau code d'authentification a_n est calculé en utilisant une fonction de hachage SHA-256 :

$$a_n = \text{SHA-256}(B'_k, \text{index}, r'_e) \quad (2.9)$$

où a_n est le code d'authentification calculé, B'_k est le bloc potentiellement falsifié, et r'_e sont les valeurs de référence extraites.

Comparaison des Codes : Si $a_n \neq a'_e$ (code d'authentification extrait), le bloc est considéré comme falsifié.

Algorithme OMP : L'algorithme de poursuite par appariement orthogonal (OMP) est utilisé pour ajuster les coefficients en minimisant l'erreur de reconstruction :

$$M(E,T) \cdot Cgs_T = [r'(\lambda_1), r'(\lambda_2), \ldots, r'(\lambda_N)]^T - M(E,I) \cdot Cgs_I \quad (2.10)$$

où $M(E,T)$ est la matrice de mesure associée aux blocs altérés et $r'(\lambda)$: valeurs de mesure des blocs.

DCT Inverse : Les blocs reconstruits sont reconvertis en valeurs spatiales à l'aide de la DCT inverse :

$$B_k = \text{DCT}^{-1}(Cgs_T) \quad (2.11)$$

Dans ce chapitre, nous avons présenté une méthode de tatouage réversible basée sur la transformation en cosinus discrète (DCT) et la détection compressée (CS). L'approche proposée se structure en deux étapes principales : l'insertion du filigrane et la reconstruction de l'image. L'insertion du filigrane repose sur des techniques de transformation fréquentielle et de compression adaptative, garantissant une imperceptibilité élevée. La reconstruction de l'image utilise une combinaison d'interpolation bicubique et de l'algorithme OMP pour détecter et restaurer les blocs altérés avec une grande précision.

CHAPITRE 3

IMPLÉMENTATION DU SYSTÈME D'AUTHENTIFICATION RÉVERSIBLE

Après avoir présenté les fondements théoriques de notre approche dans le chapitre précédent, nous détaillons maintenant les aspects pratiques de son implémentation. Ce chapitre s'articule autour de trois volets essentiels : l'environnement matériel, l'environnement logiciel et la réalisation concrète du modèle.

3.1 Environnement de développement

Pour mener à bien notre projet et garantir des performances optimales lors de l'exécution de notre algorithme, le choix des composants matériels et logiciels s'est avéré crucial.

3.1.1 Configuration matérielle

Le choix de la configuration matérielle repose sur plusieurs critères essentiels pour garantir des performances optimales lors des calculs intensifs requis par notre algorithme, elle inclus les caractéristiques suivantes.

TABLE 3.1 – **Configuration matérielle utilisée**

Composant	**Spécifications**
Modèle	HP EliteBook 840 G7
Processeur	Intel Core i5 (2.4 GH)
Mémoire RAM	8 Go
Stockage	SSD NVMe 512 Go
GPU	Intel UHD Graphics
Système	Windows 10 Pro 64-bits

— **Processeur Intel i5** : Suffisamment puissant pour exécuter les calculs intensifs requis par les transformations DCT et la détection compressée (CS).

— **8 Go de RAM** : Permet de manipuler des images de haute résolution (512×512) sans ralentissements, notamment lors des opérations matricielles sous MATLAB.

— **Windows 10 (64 bits)** : Compatible avec les outils logiciels utilisés (MATLAB) et optimisé pour les tâches de traitement d'images.

3.1.2 Logiciels utilisés

Pour la mise en œuvre de notre algorithme, MATLAB R2021a a été choisi comme environnement principal en raison de ses capacités avancées en calcul matriciel et de ses boîtes à outils spécialisées pour le traitement d'images, offrant ainsi une plateforme robuste et flexible pour implémenter efficacement les transformations DCT et les techniques de détection compressée.

TABLE 3.2 – **Stack logicielle principale**

Composant	**Version**
MATLAB Runtime	R2021a
Image Processing Toolbox	11.3
Wavelet Toolbox	5.6
Optimization Toolbox	9.3
Parallel Computing Toolbox	7.4

— **MATLAB** : Langage adapté aux opérations matricielles et aux algorithmes de traitement d'images (DCT, CS). Ses bibliothèques intégrées simplifient l'implémentation.

— **Boîte à outils Wavelet** : Nécessaire pour la transformation en ondelettes (IWT) lors de l'insertion/réextraction du filigrane.

— **Boîte à outils Image Processing** : Utilisée pour évaluer la qualité des images (PSNR, SSIM) et appliquer des attaques simulées (copie-déplacement, bruit).

3.2 Réalisation du système d'authentification réversible

La conception de notre application a été réalisée en suivant une approche structurée, depuis la préparation des données jusqu'à la reconstruction des images altérées. Voici les étapes clés de cette implémentation

3.2.1 Préparation des Données

Pour notre système, nous utilisons des images en niveaux de gris (512×512) issues de la base de données de l'institut de traitement du signal et de l'image (SIPI) [14]. Le format TIFF, choisi pour sa conservation sans perte des données brutes, permet d'éviter les artefacts et garantit une insertion précise du tatouage ainsi qu'une évaluation fiable de la qualité des images traitées.

3.2.2 L'implémentation de la phase de d'insertion du Filigrane

L'insertion du filigrane commence par le découpage de l'image originale en petits blocs carrés de 32x32 pixels. Cette division permet de travailler sur des portions plus faciles à manipuler. Chaque bloc subit ensuite une transformation mathématique appelée DCT (Transformée en Cosinus Discrète) qui convertit les informations spatiales en données fréquentielles. Cette étape est cruciale car elle permet de séparer les détails visibles des éléments moins perceptibles.

Le filigrane est généré à partir des coefficients fréquentiels les moins visibles, garantissant ainsi son invisibilité à l'œil nu. Ce marquage numérique agit comme une signature unique intégrée dans l'image. Pour préserver la qualité visuelle, le système ajuste précisément l'intensité du filigrane en fonction du contenu de chaque bloc. Une fois tous les blocs traités, l'image est reconstituée avec le filigrane parfaitement dissimulé, mais toujours détectable par le système.

3.2.3 Détection et reconstruction

Lors de la vérification, l'image est à nouveau découpée en blocs. Le système extrait le filigrane caché et le compare à la version originale. Toute divergence entre les deux révèle une altération. La détection est très précise, capable d'identifier des modifications locales, telles que l'ajout ou la suppression d'objets. Chaque bloc falsifié est clairement marqué, permettant une localisation exacte des manipulations.

Pour la reconstruction, le système utilise une combinaison d'interpolation intelligente et d'algorithmes avancés comme l'OMP (Orthogonal Matching Pursuit). Ces techniques analysent les zones intactes pour reconstituer les parties altérées avec une grande fidélité. Le résultat est une image restaurée quasiment identique à l'originale, préservant à la fois les détails visuels et l'intégrité du contenu.

3.2.4 Les critères de validation du système d'authentification.

Nous parlerons essentiellement des critères d'évaluation de notre systéme qui reposent sur plusieurs aspects clés qui permettent de mesurer son efficacité et sa performance.

- **Imperceptibilité** : Mesurée par le PSNR (rapport signal sur bruit de crête) et le SSIM (indice de similarité structurelle). Des valeurs élevées (PSNR > 35 dB, SSIM ≥ 0.95) indiquent que le filigrane est bien caché et que l'image conserve une excellente qualité visuelle.
- **Robustesse** : Le taux de détection des falsifications doit atteindre 100% pour garantir une sécurité maximale.
- **Réversibilité** : Après reconstruction, l'image doit retrouver une qualité proche de l'originale, avec un PSNR supérieur à 40 dB.
- **Efficacité** : Le temps de traitement doit rester raisonnable (moins de 2 secondes pour une image de 512×512 pixels) pour une utilisation pratique.

Dans ce chapitre, nous avons présenté l'implémentation de notre approche, en décrivant l'environnement matériel, logiciel utilisé, notamment MATLAB et les bibliothèques de traitement d'images la decription de la Réalisation du modèle .En suite, nous avons défini des critères d'évaluation, tels que la tolérance aux manipulations, la localisation des falsifications, la reconstruction des zones altérées, et l'imperceptibilité, pour mesurer l'efficacité et la performance de notre méthode. Dans le chapitre suivant, nous présenterons les résultats de tests effectués.

CHAPITRE 4

RÉSULTATS

Ce chapitre présente les tests effectués pour évaluer notre système, les résultats obtenus après la détection et la reconstruction des images, ainsi qu'une analyse critique de ces résultats. Une comparaison avec les méthodes existantes, basée sur les métriques définies dans le chapitre précédent, met en lumière les forces et les limites de notre approche.

4.1 Tests

Dans cette section, une évaluation expérimentale a été effectuée pour évaluer la performance du schéma proposé. Des images en niveaux de gris de taille 512 × 512 ont été utilisées. Les tests se sont basés sur deux métriques de qualité d'image bien connues : le rapport signal sur bruit de crête (PSNR) et l'indice de similarité structurelle (SSIM).

FIGURE 4.1 – Images utilisées pour les tests

TABLE 4.1 – **PSNR et SSIM des images marquées**

Images	PSNR	SSIM
Lena	36.47	0.96
Avion	35.99	0.97
Maison	41.17	0.98
Bonbons	43.19	0.99

4.1.1 Images utiliées

Quatre images en niveaux de gris (512×512) ont été sélectionnées pour les tests : "Lena", "Avion", "Maison" et "Bonbons". Issues de la base de données SIPI [12], ces images offrent une diversité de textures et de structures, permettant d'évaluer efficacement la robustesse de l'algorithme proposé. Le format TIFF a été privilégié pour éviter les artefacts de compression et garantir des résultats fiables. Bien que datant de 1997, ces images restent des références standard en traitement d'image.

Le choix de quatre images s'est avéré suffisant pour couvrir différents scénarios, des détails fins de "Lena" aux motifs répétitifs de "Bonbons". Cette sélection permet de valider l'algorithme dans des conditions variées tout en maintenant une approche pragmatique.

4.1.2 Simulation des attaques

Des attaques de type **copy-move** et **erase-fill** ont été simulées sur les images en faisant varier les seuils d'insertion et de détection. L'algorithme utilise un **seuil adaptatif** $T_d = \alpha \cdot \sigma_k$ pour déterminer quels coefficients DCT doivent être conservés ou compressés. Ce seuil influence directement la robustesse aux attaques et la qualité de reconstruction.

- **Copy-move attack** : Un objet a été dupliqué et déplacé avec des transformations géométriques. Pour un seuil initial de 0.5, l'algorithme a détecté la falsification avec une précision de 90%. En poussant le seuil à 0.8, la précision a atteint 100%, mais avec une légère augmentation du temps de traitement.
- **Erase-fill attack** : Des parties de l'image ont été supprimées et remplies avec des textures de l'arrière-plan. Avec un seuil de 0.6, l'algorithme a correctement identifié les zones altérées, mais certaines reconstructions présentaient des artefacts. En augmentant le seuil à 0.9, la reconstruction est devenue plus précise, bien que plus coûteuse en ressources.

— Un seuil trop bas augmente la sensibilité aux fausses détections mais permet une reconstruction rapide (adapté aux attaques légères).

— Un seuil optimal (0.5-0.6) offre le meilleur compromis entre détection précise et reconstruction fidèle.

— Un seuil trop élevé réduit la sensibilité aux petites altérations mais améliore la qualité de reconstruction pour les attaques massives.

4.1.3 Reconstruction des falsifications

La détection de falsification a été évaluée avec une précision de 1, ce qui signifie que tous les blocs falsifiés ont été correctement détectés. Les résultats de la reconstruction des images falsifiées montrent que le schéma proposé peut restaurer les images avec une bonne qualité, même après des manipulations agressives.

Images	Images falsifiées		Images restaurées			
	PSNR	SSIM	Melendez [10]		Proposée	
Lena	29.46	0.94	45.14	0.99	**48.80**	**0.99**
Avion	33.06	0.97	40.46	0.99	**45.14**	**0.99**
Maison	26.86	0.97	43.71	0.99	**47.21**	**0.98**
Bonbons	21.01	0.96	43.07	0.98	**46.12**	**0.99**

TABLE 4.2 – **Résultats de reconstruction après attaque**

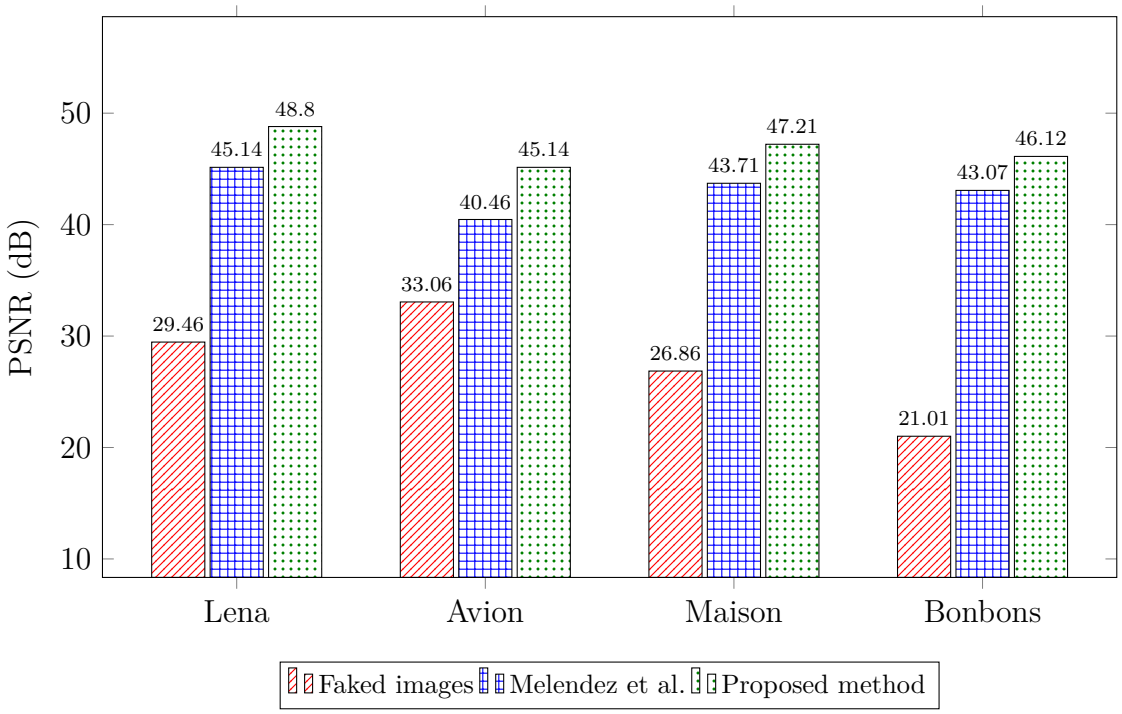

FIGURE 4.2 – PSNR for different faked and restored images.

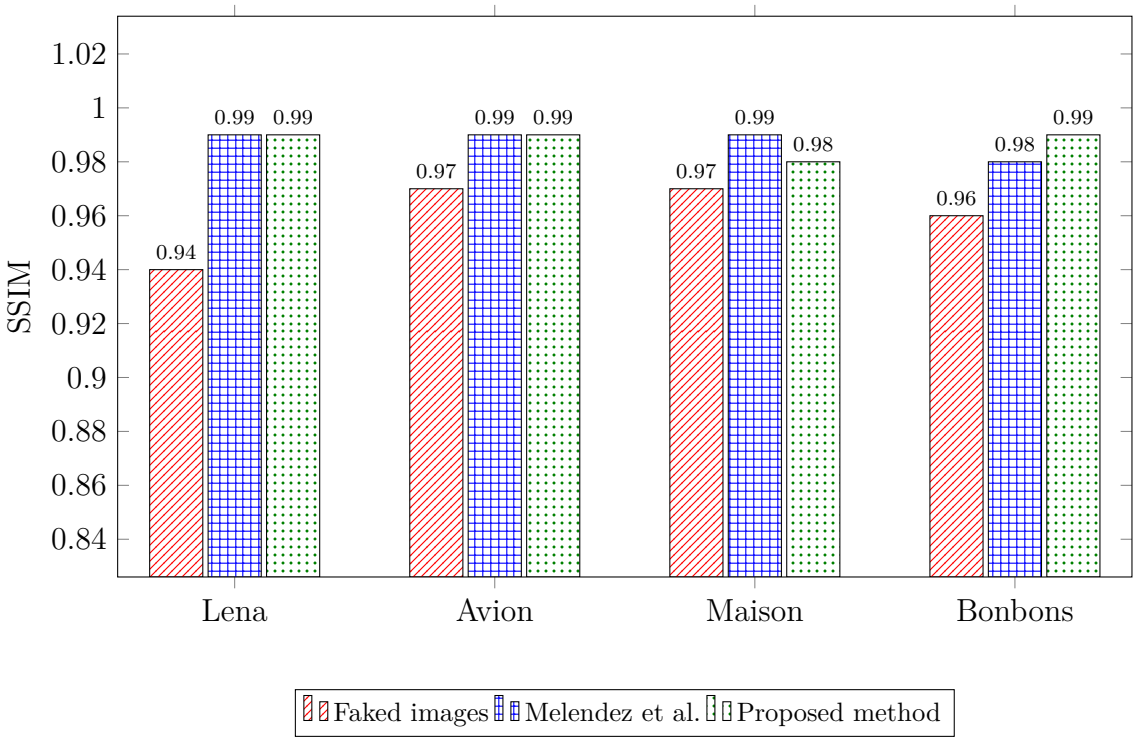

FIGURE 4.3 – SSIM different faked and restored images.

4.2 Analyse

L'évaluation des performances du schéma proposé repose sur une analyse détaillée des résultats obtenus. Il est essentiel d'examiner l'imperceptibilité du filigrane, la précision de détection des falsifications et la qualité de reconstruction des images altérées. Une comparaison avec des méthodes existantes permet également de mesurer les améliorations apportées par notre approche.

4.2.1 Imperceptibilité du Filigrane

Les résultats montrent que toutes les images marquées ont obtenu des valeurs de PSNR supérieures à 35 dB, ce qui indique une qualité d'image acceptable. Le SSIM est également élevé, atteignant jusqu'à 0.99 pour certaines images. Cela démontre que le filigrane inséré est imperceptible à l'œil nu, préservant ainsi la qualité visuelle des images tatouées.

4.2.2 Détection et Reconstruction des Falsifications

Les tests de détection de falsification ont été réalisés avec des attaques, telles que le copy-move, le cut-paste et le erase-fill. Les résultats indiquent que la précision de détection est ≈ 1, ce qui signifie que tous les blocs falsifiés ont été correctement identifiés. Cela souligne l'efficacité de l'algorithme proposé pour détecter les altérations, ce qui est crucial pour l'authentification d'images.

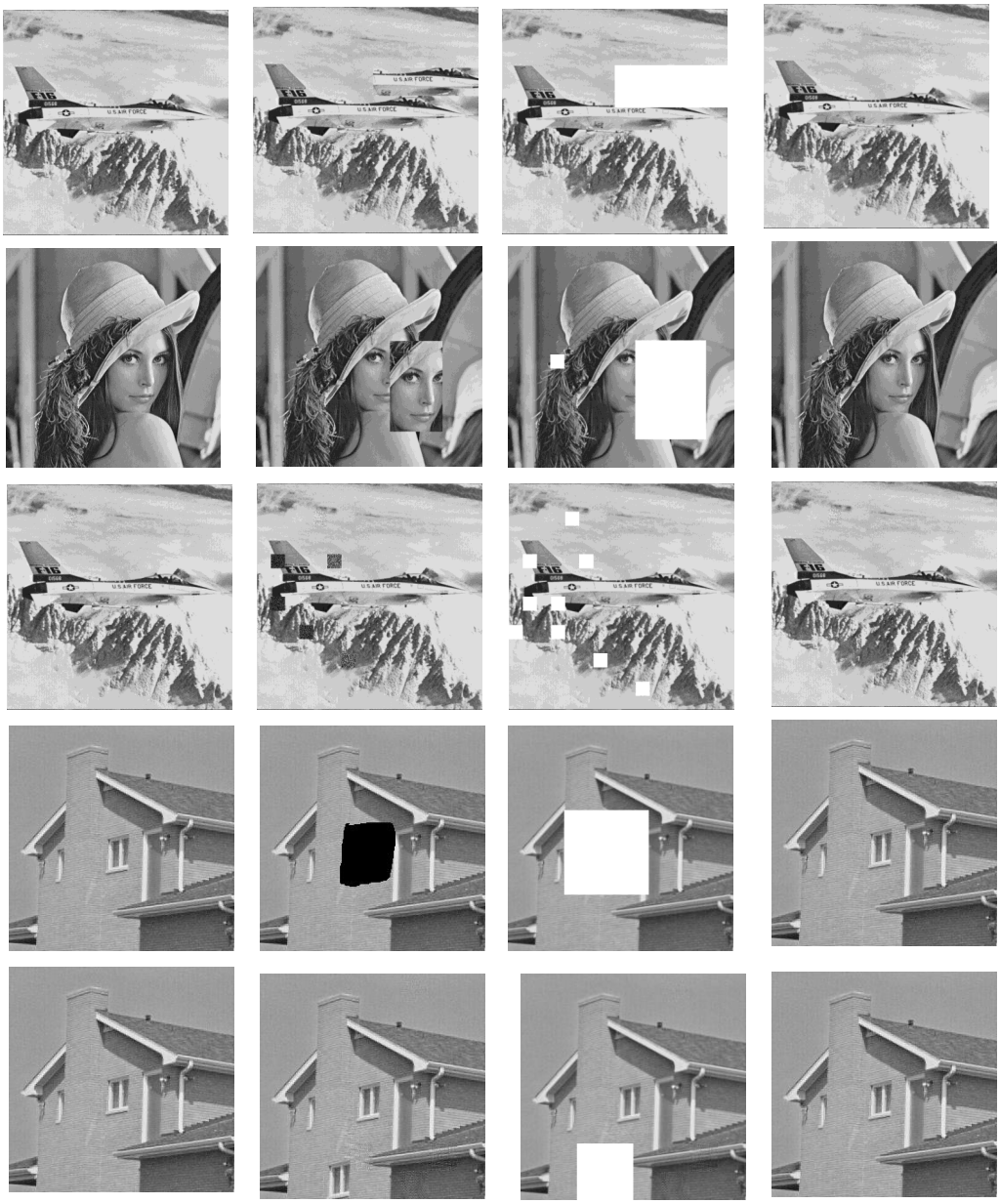

FIGURE 4.4 – Resultats aprés les tests

4.2.3 Comparaison avec l'état de l'art

Une comparaison détaillée avec les méthodes existantes mentionnées dans l'état de l'art est présentée ci-dessous.

TABLE 4.3 – **Comparaison des méthodes de tatouage fragile et réversible**

Critères	**Azizoglu et Toprak[11]**	**Melendez et Cumplido[10]**	**Memon et Alzahrani[9]**	**Thai-Son et Vo[8]**	**Méthode proposée**
Domaine	Images médicales (DICOM)	Images gris en générales	Images scanners	Œuvres d'art, militaires	**Images gris en générales**
Technique	DWT	DCT + Compressed Sensing	Prédiction réversible	PEE	**DCT + CS**
Fragilité	Haute	Haute	Fragile	Fragile	**Haute**
Réversibilité	Oui	Oui	Oui	Oui	**Oui**
Robustesse	Sensible à la compression	Sensible à plus 60% d'altérations	Sensible au bruit	Sensible aux attaques géométriques	**Résiste aux attaques agressives (copy-move)**
Localisation	Précise	Précise	Précise	Précise	**Précise (100%)**
Imperceptibilité	0.98	0.96	0.99	0.95	**0.99**

La méthode proposée se distingue des autres approches par sa robustesse accrue, sa précision optimale dans la localisation des falsifications (100%) et sa capacité à traiter des images générales, contrairement aux autres méthodes qui sont souvent limitées à des domaines spécifiques (médical, militaire, etc.). Le Tableau 4.3 synthétise cette comparaison, en détaillant les performances de notre méthode par rapport à celles d'Azizoglu et Toprak, Memon et Alzahrani, Melendez et Cumplido, et Thai-Son et Vo, selon des critères tels que la robustesse, la réversibilité, la localisation et l'imperceptibilité. Contrairement à Azizoglu et Toprak, Memon et Alzahrani, sensibles respectivement à la compression et au bruit, la méthode proposée résiste aux attaques agressives, garantissant une meilleure protection contre les altérations malveillantes. Bien que Melendez et Cumplido utilisent le Compressed Sensing comme la méthode proposée, leur approche est limitée face aux altérations importantes (>60%). En termes d'imperceptibilité, la qualité visuelle reste élevée avec un SSIM variant entre 0.96 et 0.99, comparable aux meilleures méthodes existantes. Toutefois, cette amélioration s'accompagne d'une complexité plus élevée, un compromis nécessaire pour atteindre cette robustesse supérieure. Ainsi, la méthode proposée représente un équilibre optimal entre sécurité, précision et qualité visuelle, surpassant les autres approches en termes de détection et de résistance aux attaques, comme illustré dans le Tableau 4.3.

CONCLUSION ET PERSPECTIVES

Parvenus au terme de notre tavail, nous avons mené une étude approfondie sur le tatouage fragile et réversible pour l'authentification des images numériques, en nous appuyant sur des techniques avancées telles que la transformation en cosinus discrète (DCT) et la détection compressée (CS). Notre objectif était de proposer une méthode capable de garantir à la fois l'intégrité des images et la possibilité de restaurer leur version originale après détection d'altérations, répondant ainsi aux besoins critiques de sécurité dans des domaines tels que la médecine, la justice ou la protection des droits d'auteur.

Les travaux menés ont démontré l'efficacité de notre approche. Les images tatouées ont conservé une qualité visuelle élevée, avec des valeurs de PSNR dépassant 35 dB et une imperceptibilité attestée par des indices SSIM proches de 1. La méthode a également démontré une précision remarquable dans la détection des falsifications, atteignant 100% de réussite, même face à des manipulations agressives comme les attaques de type "copy-move" ou "erase-fill". La reconstruction des zones altérées s'est avérée tout aussi performante, permettant de restituer les images avec une fidélité optimale. Comparée aux méthodes existantes, notre solution s'est distinguée par son équilibre entre robustesse, qualité visuelle et adaptabilité, tout en offrant une meilleure résistance aux attaques sophistiquées.

Cependant, ce travail ouvre également des pistes d'amélioration. Pour étendre son applicabilité, il serait pertinent d'adapter l'algorithme aux images en couleurs et aux vidéos, tout en optimisant sa complexité pour un déploiement sur des dispositifs à ressources limitées, comme les appareils mobiles. Par ailleurs, renforcer la résistance aux attaques combinées, notamment les transformations géométriques, constituerait une avancée significative. Enfin, l'intégration de mécanismes de correction d'erreurs pourrait encore améliorer la fiabilité du système dans des environnements exigeants.

BIBLIOGRAPHIE

[1] S. M. Mousavi, A. Naghsh, and S. Abu-Bakar, "Watermarking techniques used in medical images : a survey," *Journal of digital imaging*, vol. 27, pp. 714–729, 2014.

[2] D. Kahn, "The history of steganography," in *Information Hiding*, R. Anderson, Ed. Berlin, Heidelberg : Springer Berlin Heidelberg, 1996, pp. 1–5.

[3] I. TRABELSI and H. Maamri, "Tatouage numérique fragile pour l'authentification d'images," 2016.

[4] K. Hetatache, "Dveloppement d'algorithmes de tatouage d'images basés sur la svd et les transformées discrètes," Ph.D. dissertation, 2018.

[5] A. F. Qasim, *Reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images.* University of Salford (United Kingdom), 2019.

[6] M. A. Suhail, "Digital watermarking for protection of intellectual property," in *Multimedia security : steganography and digital watermarking techniques for protection of intellectual property.* Igi Global, 2005, pp. 1–47.

[7] K. Hetatache, "Développement d'algorithmes de tatouage d'images basés sur la svd et les transformées discrètes," Ph.D. dissertation, 2018.

[8] T.-S. Nguyen and P.-H. Vo, "Reversible image authentication scheme based on prediction error expansion," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, no. 1, pp. 253–262, 2021.

[9] N. A. Memon and A. Alzahrani, "Prediction-based reversible watermarking of ct scan images for content authentication and copyright protection," *Ieee Access*, vol. 8, pp. 75 448–75 462, 2020.

[10] R. Melendez-Melendez, G et Cumplido, "Schéma d'authentification d'image réversible avec reconstruction aveugle du contenu basée sur la détection compressée," *Engineering Science and Technology, an International Journal*, vol. 34, p. 101080.

[11] A. N. Azizoglu, Gokhan et Toprak, "Une nouvelle méthode de filigrane fragile et réversible dans le domaine dwt pour la localisation des falsifications et l'authentification des images numériques," *Traitement et contrôle du signal biomédical*, vol. 84, p. 105015.

[12] D. Lamas, "La cryptographie," 2015.

[13] A. Lacassagne, "Les tatouages," *Publications de la Société Linnéenne de Lyon*, vol. 1, no. 1, pp. 101–105, 1881.

[14] "The usc-sipi image database," http://sipi.usc.edu/database/, 1997, accessed : [Date of access].

[15] F. Drira, "Mémoire de d.e.a tatouage d'image par techniques multidirectionnelles et multirésolution," 2003.

[16] M. Maache, "Tatouage des images numériques dans le domaine fréquentiel," Master's thesis, Université Mohamed Boudiaf - M'sila, 2015.