RÉPUBLIQUE DU CAMEROUN
****
PAIX - TRAVAIL - PATRIE
****
UNIVERSITÉ DE YAOUNDÉ I
****
FACULTÉ DES SCIENCES
****
DÉPARTEMENT D'INFORMATIQUE
****

REPUBLIC OF CAMEROON
****
PEACE - WORK - FATHERLAND
****
UNIVERSITY OF YAOUNDÉ I
****
FACULTY OF SCIENCE
****
DEPARTMENT OF COMPUTER SCIENCE
****

TATOUAGE NUMÉRIQUE COMBINÉ À UNE CRYPTOGRAPHIE ASYMÉTRIQUE APPLIQUÉ AUX IMAGES NUMÉRIQUES

Mémoire soutenu dans le but d'obtenir le Master Recherche en Informatique.

Rédigé par:

NOUNDUI Yvan Kessel

Matricule : 13C2324

Mémoire dirigé par :

Dr. AMINOU HALIDOU

Chargé de Cours, Université de Yaounde I, Faculté des Sciences

Année académique: 2023-2024

♣ Dédicaces ♣

A toute ma famille pour leur soutien indéfectible

♣ Remerciements ♣

Ce travail a été réalisé grâce à la conjugaison des efforts de plusieurs personnes, à qui je ne saurais manquer l'occasion d'exprimer ma profonde gratitude. Je pense notamment aux personnes ci-après :

- Au Chef de département **Dr AMINOU Halidou**, mon encadreur, pour son soutien, sa disponibilité, son ardeur au travail ;
- Au **Pr NDOUMDAM René**, Directeur du laboratoire LAMOCA, pour son accueil et son encadrement ;
- Au **Dr TAPAMO KENFACK Hippolyte Michel** qui a décidé d'examiner ce travail ;
- Aux enseignants du département informatique de l'Université de Yaoundé 1, pour les cours dispensés et les connaissances m'ayant permis d'effectuer ce travail ;
- A mes parents **MAJOUNDOUM Marie Thérèse** et **NOUKUIKO NOUNDUI FELIX** pour leur soutien incommensurable ;
- A **NOUNDUI Christian** et **MOUGOUE Steve** qui sont des modèles pour moi et dont les efforts m'ont permis d'aboutir à ce résultat ;
- Aux **Pr TIAM** et **Dr YOUSSOUFA Mohamadou** pour les différentes observations et recommandations dans la rédaction du mémoire ;
- Aux **Dr MESSI NGUELE Thomas**, **Dr NZEKON Armel**, **NKONDOCK MI BAHANAG Nicolas** pour les encouragements dans la rédaction de ce mémoire ;
- A **MBOULE Brice**, **EONE Vianney**, **MOSSEBO**, **TCHANA Gil Thibaut** pour les efforts consentis et les encouragements pour la réalisation de ce travail ;
- Au **Chef de Bataillon - Magistrat EYEBE ETOUNDI Ignace** dont j'ai beaucoup d'estime et dont les encouragements m'ont permis de terminer ce travail ;
- Au **Pr BELL BITJOKA** dont les encouragements m'ont permis de finir ce travail ;
- A Mon parent **MR DJOMO Jean** qui m'a toujours guidé dans les bons choix de vie ;
- A Mes camarades et ami(e)s pour les motivations dans la réalisation de ce travail ;

♣ Résumé ♣

Le tatouage numérique a connu ces dernières années un essor spectaculaire. Avec le développement sans cesse grandissant des logiciels de traitement d'image et aussi à cause de l'utilisation illicite des images numériques, les propriétaires de ces images ayant les droits initiaux ont été affectés. Pour cela, ils sont motivés plus que jamais à les protéger pour empêcher la modification de ces dernières. Bien que, le tatouage numérique est un nouvel axe de recherche, il a gagné beaucoup d'attention et a évolué très rapidement. Plusieurs méthodes efficaces de tatouage des images numériques dans le domaine fréquentiel ont été proposées. La plupart des méthodes proposées se sont focalisées sur les images à niveaux de gris, domaine dans lequel s'inscrit ce travail. Pour cette raison, une méthode de tatouage numérique d'images a été proposée à laquelle une cryptographie asymétrique a été associée afin d'augmenter la sécurité de la marque dans les images. Dans la méthode de tatouage robuste proposée, la marque est d'abord chiffrée avec la clé privée K_s avant d'être insérée dans le domaine fréquentiel en utilisant la Transformée en Cosinus Discrète (TCD) au niveau des blocs des moyennes fréquences de l'image hôte I assurant ainsi un compromis entre robustesse et imperceptibilité pour fournir une image tatouée $I_{W'}$. Le mode d'extraction aveugle a été mis en exergue car le caractère aveugle constitue un enjeu majeur dans les applications réelles. Les expérimentations menées sur 04 images à niveaux de gris démontrent une bonne qualité visuelle *(PSNR > 47.5 dB & 0.99 ≤ SSIM ≤ 1)*, une résistance significative face aux altérations ($NC \geq 0{,}79$) et également la simplicité d'implémentation (*temps d'exécution satisfaisant*). Cette solution hybride constitue ainsi une contribution efficace dans des environnements numériques sensibles.

Mots clés: tatouage numérique , tatouage robuste, cryptographie asymétrique, Transformé en Cosinus Discret, extraction aveugle, PSNR, SSIM, NC.

♣ Abstract ♣

Digital watermarking has experienced significant growth in recent years. The continuous advancement of image processing software and the increasing incidence of unauthorized use of digital images have adversely affected the original rights holders. Consequently, they are more motivated than ever to protect their images against unauthorized modifications. Although digital watermarking is a relatively new research area, it has garnered substantial attention and has evolved rapidly. Numerous effective frequency-domain image watermarking methods have been proposed, with most focusing on grayscale images, the context of this work. To enhance security, a digital image watermarking method incorporating asymmetric cryptography has been proposed. In the robust watermarking approach, the watermark is first encrypted using the private key K_s and then embedded into the mid-frequency blocks of the host image I using the Discrete Cosine Transform (DCT). This strategy ensures a balance between robustness and imperceptibility, resulting in a watermarked image $I_{W'}$. The blind extraction mode is emphasized, as blind watermarking is crucial for real-world applications. The experiments conducted on four grayscale images demonstrate high visual quality *(PSNR > 47.5 dB & 0.99 ≤ SSIM ≤ 1)*, significant robustness against alterations ($NC \geq 0.79$), and ease of implementation (*satisfactory execution time*). This hybrid solution thus represents an effective contribution in sensitive digital environments.

Keywords: digital watermarking, robust watermarking, asymmetric cryptography, Discrete Cosinus Transform, blind extraction, PSNR , SSIM, NC.

♣ Contents ♣

♣ Abréviations ♣

- **dB:** *decibel* - Décibel
- **DCT :** *Discrete Cosinus Transform* - Transformé en Cosinus Discrète
- **DE :** *Differential Evolution* - Evolution Différentielle
- **DFT :** *Discrete Fourrier Transform* - Transformé de Fourrier Discrète
- **DWT :** *Discrete Wavelet Transform* - Transformé en Ondelette Discrète
- **HVS :** *Human Visual System* - Système Visuel Humain
- **IDCT :** *Inverse Discret Cosinus Transform* - Inverse de la Transformé en Cosinus Discrète
- **JPEG :** *Joint Photographics Experts Group* - Groupe Mixte d'Experts en Photographie
- **JPEG2000 :** *Joint Photographics Experts Group* - Groupe Mixte d'Experts en Photographie 2000
- **KELM :** *Kernel Extreme Learning Machine* - Noyau de la Machine d'Apprentissage Extrême
- **LSB :** *Least Significant Byte* - Bit de Poids Faible
- **NC :** *Normalized Correlation* - Corrélation Normalisée
- **PN:** *Pseudo Noise* - Pseudo Bruit
- **PSNR :** *Peak Signal Noise to Ratio* - Rapport Signal sur Bruit de Crête
- **RSA :** Rivest, Shamir, et Adelman - Algorithme de Rivest-Shamir-Adelman
- **SSIM :** *Structural Similarity Index Measure* - Mesure de l'Indice de Similarité Structurelle

♣ List of Figures ♣

♣ List of Tables ♣

♣ INTRODUCTION ♣

0.1 Contexte

L'arrivée de l'ère numérique à la fin du 20ème siècle a permis un accès à l'information plus facile que par le passé. Les documents numériques sont devenus de plus en plus utilisés puisque leur diffusion est peu coûteuse et extrêmement rapide, même ceux de grand volume, grâce aux réseaux informatiques et aux supports numériques. Parmi les documents numériques, une grande importance est accordée aux images. Cette extraordinaire révolution technique de l'analogique vers le numérique ne s'est pas fait sans engendrer des inquiétudes puisque n'importe qui peut facilement copier, modifier et distribuer les images sans risque de les détériorer [2]. Il est très difficile de trouver un compromis entre le libre accès à l'information et le respect des droits d'auteurs. Des personnes peuvent s'approprier une image pour faire des profits aux dépens des personnes légitimes ayant les droits initiaux. Elles peuvent aussi changer facilement son contenu [3].

0.2 Problématique

Parmi les méthodes de protection du contenu numérique, le tatouage numérique s'est imposé comme une technique efficace s'inspirant principalement de la cryptographie et la stéganographie. Cependant, les travaux existants reposent en grande majorité sur des systèmes de cryptographie symétrique pour la protection des marques dans les images, ce qui présente une limite notable en terme de sécurité en cas de fuite de la clé : la nécessité de partager une clé unique entre l'émetteur et le récepteur ouvre des failles potentielles lors de la transmission ou du stockage. La résolution de ce problème amène à poser la question centrale : **Comment protéger les images numériques de manière sécurisée et robuste face aux risques de manipulations et aux attaques ?** De ce fait, ce qui reviendra à répondre à la question : **Comment combiner efficacement le tatouage numérique et la cryptographie asymétrique pour protéger les images numériques ?** C'est dans ce contexte que s'inscrit le présent travail, qui vise à combiner le tatouage numérique et la cryptographie asymétrique afin de renforcer la sécurité globale du processus tout en maintenant une bonne imperceptibilité et robustesse du tatouage face aux manipulations et attaques de natures variées. Il s'agit ici d'une problématique d'intérêt public, scientifique et social.

0.3 Définitions de base

- **tatouage numérique :** est une technique qui consiste à introduire généralement de manière invisible, une information dans une image, puis à tenter de la récupérer après que l'image ait éventuellement subi des manipulations de natures variées [4].
- **cryptographie :** ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données afin d'en préserver la confidentialité et l'authenticité [5].
- **stéganographie :** C'est une technique qui consiste à dissimuler un message, que l'on désire transmettre confidentiellement, dans un ensemble de données d'apparence anodine, de façon à ce que sa présence soit imperceptible [6].
- **image numérique :** est un signal fini bidimensionnel échantillonné à valeurs quantifiées dans un certains espace de couleurs et est constitué de points faibles (pixels) [7].
- **document numérique :** C'est une représentation électronique d'une information et qui existe sous forme de donnée numérique stockée sur ordinateur, smartphones, cloud et serveurs en ligne [8].

0.4 Objectifs

Il s'agit ici d'étudier et de concevoir un algorithme de tatouage numérique sécurisée et robuste à diverses attaques qui exploite la cryptographie asymétrique (clé publique/clé privée) dans le but d'assurer une protection des contenus numériques dans les images à niveau de gris. A cette fin, le procédé se fera de la manière suivante :

- Faire une étude des travaux existants ;
- Proposer un schéma de tatouage basé sur une cryptographie asymétrique intégrée au processus de marquage ;
- Évaluer le modèle proposé en utilisant un jeu de données et des métriques appropriées ;
- Comparer les résultats obtenus avec ceux des travaux existants ;
- Interpréter les résultats obtenus .

0.5 Méthodologie

La résolution de ce problème passera par l'intégration d'un système de cryptographie asymétrique au processus de tatouage numérique dans les images à niveau de gris. En effet, la solution pro-

posée exploitera le tatouage numérique dans le domaine fréquentiel plus précisément la Transformé en Cosinus Discret (TCD en français ou DCT en anglais). Cette approche a ceci de particulier qu'elle permet de cacher la marque (qui a préalablement été chiffrée grâce à une clé privée K_s) dans des blocs au niveau des fréquences moyennes de l'image. Ce qui rend la méthode robuste face à divers attaques et aussi les informations cachées sont quasi imperceptibles à l'œil humain preuve du critère d'imperceptibilité. L'utilisation du chiffrement a pour but d'augmenter la sécurité de la marque et de ce faite la solution proposée. L'intérêt s'est porté au mode d'extraction aveugle car le caractère aveugle constitue un enjeu majeur dans les applications réelles.

0.6 Résultats attendus

A la fin de ce travail :

- Le modèle proposera une bonne performance au niveau de l'insertion et de l'extraction de la marque dans l'image ce qui caractérise un bon critère d'imperceptibilité de tout algorithme de tatouage ;
- Le modèle proposera une bonne performance au niveau de la robustesse de l'algorithme face à diverses attaques ;
- Le modèle pourra être utilisé dans d'autres domaines d'applications à l'instar de la télémédecine, la vidéosurveillance ;

0.7 Plan

Pour l'atteinte des objectifs susmentionnés, le travail sera structuré ainsi qu'il suit :

- Le chapitre 1 présentera les techniques de dissimulation et donc l'accent sera mis sur le tatouage numérique et à la fin des travaux de tatouage liés au domaine fréquentiel seront présentés ;
- Le chapitre 2 proposera une méthode de tatouage numérique à travers les deux opérations de base que sont l'insertion et l'extraction de la marque dans l'image ;
- Le chapitre 3 sera consacré à l'expérimentation où l'accent sera mis sur l'environnement de développement et également les différents tests qui seront utilisés dans le but de valider la méthode de tatouage proposé ;
- Le chapitre 4 présentera les résultats et donc à la fin une interprétation sera faite.

CHAPTER 1

CONCEPTS DE LA SECURITE DES CONTENUS NUMERIQUES

Le tatouage numérique a connu un essor considérable dans le transfert des fichiers et la communication. Il trouve son origine dans le manque de techniques fiables de protection des contenus numériques qui sont devenues volatiles et facile à pirater. La compréhension de ce travail passe par la définition des concepts clés. Dans ce chapitre, les concepts y afférents seront présentés et pour terminer sur les travaux existants.

1.1 Techniques de sécurité de l'information

La cryptographie, la stéganographie et le watermarking sont des techniques de protection et de sécurisation de l'information mais leurs premiers objectifs sont différents. Bien que la cryptographie et la stéganographie faisant partie des sciences du secret, elles ont été utilisées avant le commencement de notre ère à des fins diverses.

1.1.1 La Cryptographie

La cryptographie est employée dans des domaines de la vie. Elle qui est étroitement liée aux systèmes de communication fut une première proposition pour sécuriser les documents numériques. Son objectif est de rendre illisible le message à toute personne ne possédant pas l'information secrète adéquate. Elle offre des outils permettant d'assurer la confidentialité, l'intégrité, l'authentification [9]. Avec l'avènement de l'ère numérique et notamment avec l'apparition de l'ordinateur, cette science de cryptologie a considérablement évolué. Elle est devenue une discipline de recherche publique de l'informatique théorique basée sur des outils mathématiques sophistiqués.

1.1.2 La stéganographie

La stéganographie est l'art de la dissimulation. Son objectif est de faire passer inaperçu un message secondaire dans un message primaire. Le message primaire reste lisible à tous, tandis que le message secondaire n'est lisible que par une ou plusieurs personnes propriétaires d'une information secrète [6]. De plus, alors que la cryptographie offre une sécurité plutôt à priori (par exemple, contrôle d'accès), la stéganographie offre une sécurité plutôt à posteriori,

dans la mesure où le message secondaire est supposé rester accessible après recopies et manipulations du message primaire [6]. Avec l'avènement de l'informatique et le développement des échanges électroniques, les possibilités de cacher un message se sont multipliées : on peut cacher un message dans un texte, une image, un site internet, un programme ou une musique. La stéganographie a aussi trouvé des applications commerciales avec l'émergence d'un nouvel axe de recherche qui est le tatouage numérique ou digital watermarking. La stéganographie repose sur 3 critères à savoir : l'imperceptibilité, la capacité et la robustesse.

1.1.3 Le tatouage numérique ou Digital Watermarking

Le tatouage cherche à répondre au problème de la protection des droits d'auteur. Il s'agit bien de dissimulation d'information puisque, pour y parvenir, on insère une marque (watermark) dans l'image spécifique au propriétaire. Comme celui-ci souhaite protéger son image et non une version trop déformée, l'insertion doit minimiser les modifications subies par le médium afin d'être imperceptible. Ici, la dissimulation ne signifie pas la même chose qu'en stéganographie : un attaquant sait qu'un tatouage est présent dans le document tatoué, mais cette connaissance ne doit cependant pas lui permettre de le retirer [10].

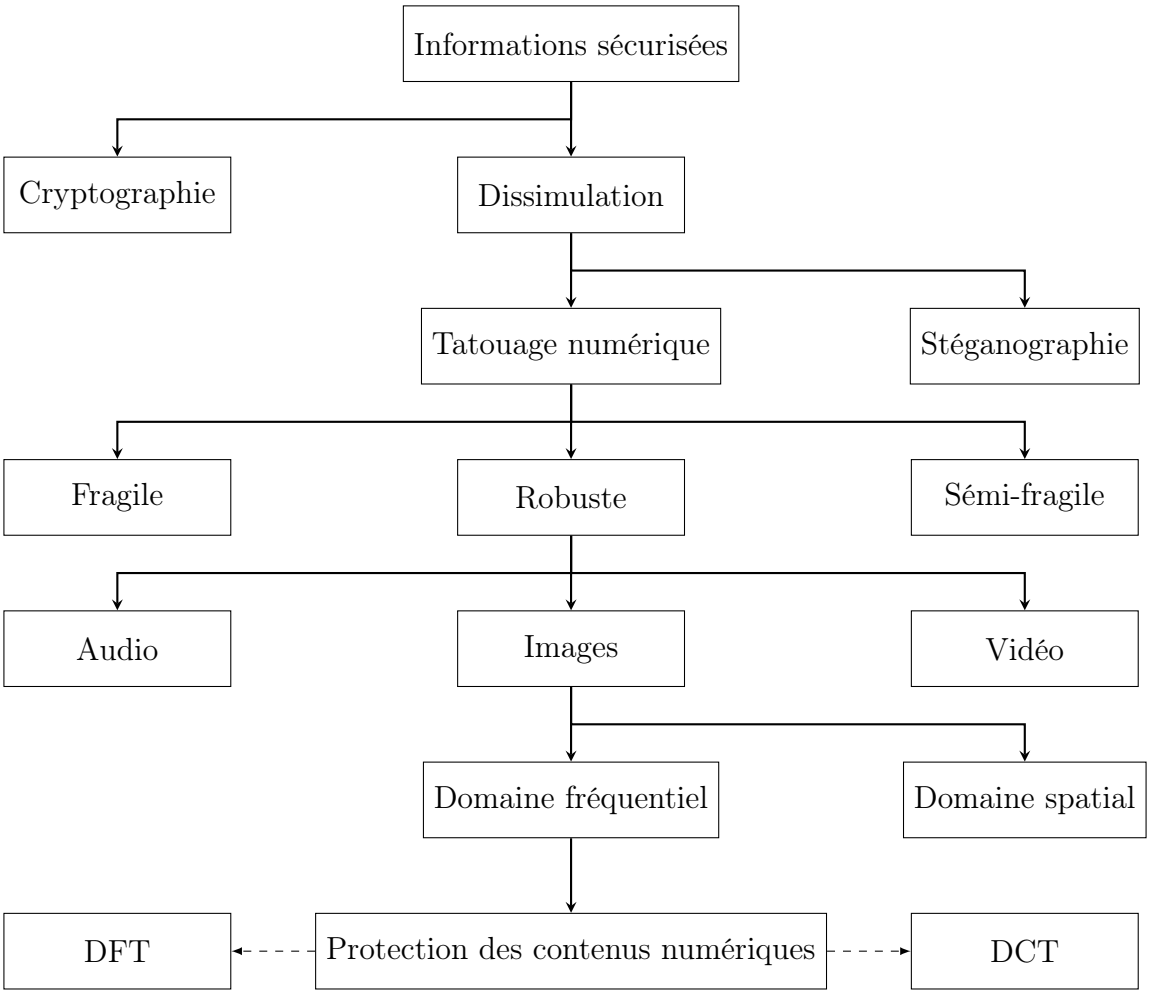


Figure 1.1: Technique de sécurisation des contenus numériques

1.2 Tatouage numérique, concepts de base et terminologies

La particularité du tatouage numérique par rapport à d'autres techniques, comme par exemple un stockage simple de l'information dans l'en-tête du fichier, est que le watermark est lié de manière intime et résistante aux données. De ce fait, le tatouage est théoriquement indépendant du format de fichier et il peut être détecté ou extrait même si le document a subi des modifications ou s'il est incomplet [4]. Le tatouage permet alors une vérification ou une extraction efficace et automatique de certaines informations liées à l'origine, au contenu ou même à la diffusion d'une image.

1.2.1 Structure générale du tatouage numérique

Un système de tatouage numérique comprend 2 phases à savoir :

- **l'insertion du tatouage** : Cette phase consiste à introduire une marque dans un document afin d'identifier son propriétaire. cette insertion nécessite la possession d'une image originale et de la marque à insérer et éventuellement d'une clé secrète [1].
- **l'extraction / détection du tatouage** : Cette phase permet de prouver la présence de la marque. Ceci peut être réalisé par extraction complète de la marque insérée ou par détection d'un pic, supérieur à un certain seuil prédéfini, obtenu par un simple inter corrélation entre la marque d'origine et celle extraite [1].

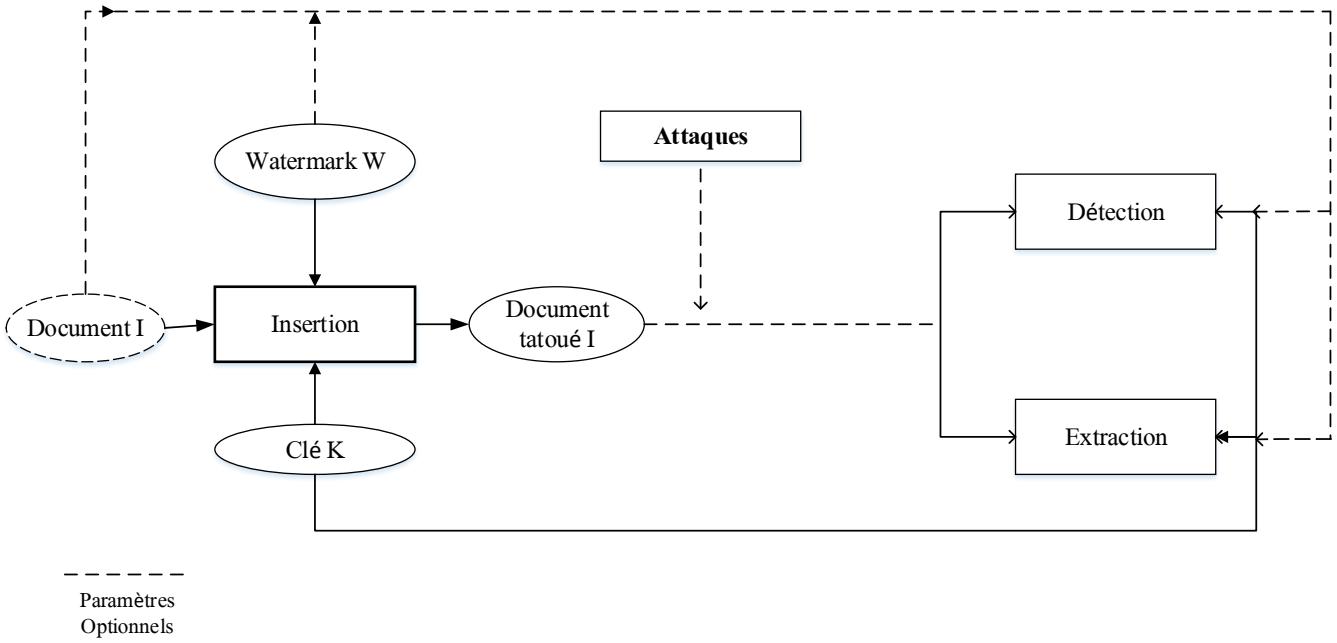


Figure 1.2: Modèle générique d'un système de tatouage numérique [1]

1.2.2 Propriétés du tatouage numérique

Toute marque insérée doit satisfaire essentiellement trois contraintes : la capacité, l'invisibilité et la robustesse.

- **la capacité** : C'est la quantité d'informations que l'on espère cacher par rapport à la quantité d'informations associée au document hôte [4]. Il est également judicieux de parler de la capacité d'une technique donnée, comme étant la quantité de bits d'information qu'elle est capable de transmettre d'une manière plus ou moins fiable. Donc il est très facile de comprendre que la capacité est une propriété fondamentale de tout algorithme de tatouage [9].

- **l'imperceptibilité** : la marque doit être invisible. En effet, une marque visible peut être aisément écrasée par une autre marque. De ce fait garantir l'invisibilité de la signature revient à respecter la qualité visuelle de l'image. Aucune dégradation ne doit être perçue sur l'objet d'origine. C'est pour cette raison que plusieurs algorithmes de marquage existants ont tendance à effectuer l'insertion dans les zones d'intérêts les moins sensibles à l'œil humain ou à utiliser un masque psycho visuel adaptant la marque à l'image à tatouer [4].

- **la robustesse**: Le document tatoué est destiné à être distribué à grande échelle, il est donc amené à subir des déformations ou des attaques. Celles-ci peuvent être involontaires (innocentes) ou volontaires (malveillantes : pirate voulant endommager le tatouage). La robustesse à de telles attaques est l'une des propriétés importantes d'une méthode de tatouage [9].

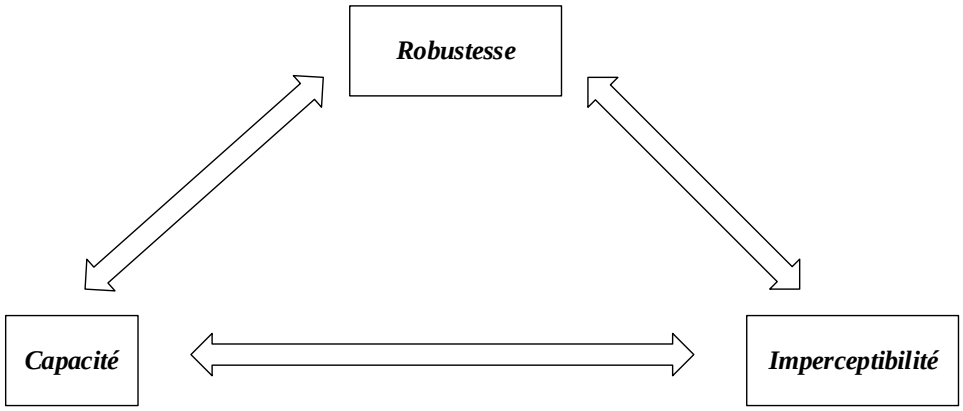


Figure 1.3: Propriété du tatouage numérique [1]

1.2.3 Quelques applications du tatouage numérique

Les applications du watermarking sont nombreuses. On peut citer entre autres :

- **Protection des droits d'auteurs** : Ça a été une des premières applications étudiée en tatouage d'images. Ce service reste cependant toujours d'actualité et concerne encore la majorité des publications. L'objectif est d'offrir, en cas de litige, la possibilité à l'auteur ou au propriétaire d'une image d'apporter la preuve qu'il est effectivement ce qu'il prétend être, et ce même si l'image concernée a subi des modifications par rapport à l'original [1,11] ;

- **Contrôle du nombre de copies** : les données numériques peuvent être dupliquées sans subir de détérioration de la qualité. Dans ce contexte, si une personne détient en main un document numérique, 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 [7] ;

- **Authentification** : L'objectif est de détecter la manipulation des données originales. Ceci peut être fait en utilisant un tatouage fragile. Si le document original est modifié avec malveillance, le watermark sera détruit. Si le watermark peut être récupéré par le destinataire, le travail est considéré authentique, autrement il devrait être considéré comme truqué. Un niveau bas de compression est habituellement autorisé mais pas le changement du contenu. Il y a plusieurs types du tatouages fragiles : certains nous permettent de détecter si l'image a été modifié et certains nous permettent de calculer une approximation de l'image originale dans les régions modifiées [1] ;

- **Indexation** : On peut enfin cacher des informations descriptives (méta-informations) dans une image. Par exemple, un médecin peut inclure dans une radiographie, de façon discrète afin de ne pas la dénaturer, le nom du patient traité, son diagnostic et ses observations. Ce cas est le plus simple, puisqu'une attaque visant à détruire le watermark ne présente aucun intérêt et n'est donc a priori pas à craindre [1] ;

- **Transmission secrète** On peut aussi tatouer une image, de façon aussi discrète que possible, dans le but d'échanger des messages secrets. Ceux-ci sont cachés dans l'image, et nécessitent une clé secrète pour être décodés. Cette application a été formulée par Simmons [12] avec le problème du prisonnier, dans laquelle on suppose deux détenus dans des cellules séparées tentent de passer les messages secrets. Leur problème est qu'ils ne peuvent pas passer directement ces messages, mais plutôt, ces derniers doivent passer à travers le gardien de prison. Le gardien est prêt à transporter des messages inoffensifs

entre eux, mais les punir s'il constate, par exemple, que leurs messages contiennent un plan pour s'enfuir. La solution consiste à déguiser le plan d'évacuation dans les messages inoffensifs [1, 13] ;

1.2.4 Classification des algorithmes de tatouage numérique

Au cours des deux dernières décennies, plusieurs schémas du tatouage numérique des images ont été développés pour diverses applications. À première vue ces schémas semblent très différents les uns des autres. Dans cette section, nous allons présenter une classification des algorithmes de tatouage numérique des images. Cette classification peut se faire selon 2 différents critères principaux à savoir : le type d'algorithme et le domaine d'insertion. La figure 1.4 suivante en est la parfaite illustration.

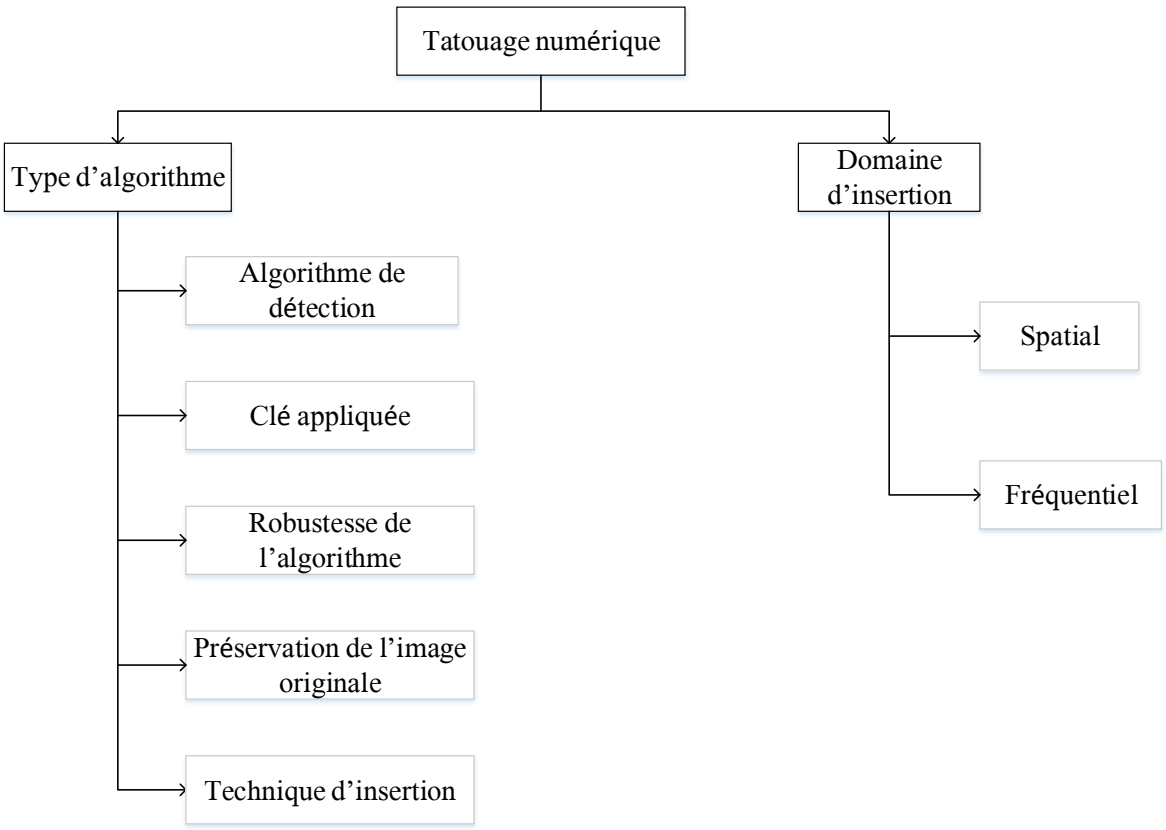


Figure 1.4: Organigramme de la classification des algorithmes de tatouage numérique [2]

1.2.4.1 Classification selon le type d'algorithme

Il est aussi possible de grouper les techniques du tatouage selon différents critères : conformément au type de clé appliquée, selon l'information nécessaire à l'extraction, conformément à la robustesse, selon la préservation de l'image originale et conformément à la technique d'insertion.

1) **La clé appliquée : Asymétrique et Symétrique**

Le tatouage asymétrique repose sur l'utilisation de deux clés : une clé K_s privée pour l'insertion et une clé K_p publique pour la détection/extraction. K_p est issue de K_s par une transformation non inversible. N'importe quel utilisateur peut détecter la marque en connaissant K_p, mais seul la connaissance de K_s permet d'enlever ou modifier la marque [14].

Dans **le tatouage symétrique**, les paramètres utilisés pour insérer la marque sont les mêmes que pour l'extraire. Le rôle de clé-privée et clé-publique n'existe pas, l'insertion et l'extraction sont faites à l'aide de la même clé et procédure [15].

2) **La robustesse de l'algorithme**

- **le tatouage fragile** : ici le tatouage est fortement sensible aux modifications de l'image tatouée. cette approche sert à prouver l'authenticité et l'intégrité d'un fichier tatoué [7].
- **le tatouage sémi-fragile** : Il combine les caractéristiques du tatouage robuste et fragile pour avoir une situation intermédiaire, dans laquelle la marque est robuste pour un ensemble défini de dégradations, et fragile à d'autres [16].
- **le tatouage robuste** : il dispose d'un vaste champ de théorie et de résultats. il cherche à préserver les données cachées face aux attaques. la marque doit donc suffisamment être résistante aux attaques afin de rester identifiable [3] .

3) **L'algorithme de détection : Aveugle, Sémi-aveugle et Non aveugle**

- **Le tatouage aveugle** est la plus ancienne forme du tatouage. Il n'oblige pas l'extracteur d'avoir connaissance de l'image originale, ni de la marque. Seule l'image tatouée et la clé secrète doivent être disponibles au moment de l'extraction. En se basant sur le modèle générique présenté à la figure 1.2 , la fonction d'extraction est modélisée comme suit :

$$W' = D\ (I_w^*, K)$$

- Dans le cadre d'un système **sémi-aveugle**, nous avons besoin d'informations supplémentaires pour aider la détection ou l'extraction. Cette demande est dûe à la perte de synchronisation à cause de canal bruité ou de la technique d'insertion. La phase d'extraction peut requérir la marque ou l'image tatouée (l'image originale juste après l'incrustation de la marque). En se basant sur le modèle générique présenté à la figure 1.2 , la fonction d'extraction est modélisée comme suit :

$$W' = D\ (I_w^*, K, W, I_w)$$

- Au contraire du tatouage aveugle, les algorithmes de **tatouage non-aveugle** nécessitent toujours l'image originale. En se basant sur le modèle générique présenté à la figure 1.2, la fonction d'extraction est modélisée comme suit :

$$W' = D\ (I_w^*, K, I)$$

Le nombre d'algorithmes non-aveugle n'est pas important par rapport aux nombreux algorithmes sémi-aveugles et aveugles. Ceci est dû au fait que la disponibilité des données originales au moment de l'extraction de la marque, ne peut pas toujours être garantie.

4) **La préservation de l'image originale : Inversible et Non-inversible**

Le tatouage inversible permet de récupérer toutes les propriétés originales de l'image hôte après l'extraction du watermark [15].
Dans **le tatouage non-inversible**, l'image originale est définitivement altérée par le mécanisme d'insertion du watermark. La matrice originale de pixels est irrécupérable. La plupart des méthodes citées jusqu'ici sont non-inversibles [15].

5) **La technique d'insertion : Additif et substitutif**

Le tatouage additif consiste principalement à ajouter une marque W qui représente le signal à des composantes de l'image I correspondant au bruit. Afin de respecter la contrainte d'imperceptibilité, l'énergie de W est très inférieure à celle de l'image I. Donc nous sommes en face d'un système de transmission très fortement bruité. Dans un tel contexte, la difficulté consiste à mettre en forme le signal de telle manière qu'il puisse être détecté malgré le bruit causé d'une part par l'image et d'autre part par les attaques [9].
Le tatouage substitutif modifie les bits de l'image hôte afin de les faire correspondre au watermark. Ce type de marquage est connu comme tatouage par contrainte, parce qu'il force l'image hôte à respecter certaines propriétés qui déterminent le watermark [1].

1.2.4.2 Classification selon le domaine d'insertion

Le choix de l'espace ou du domaine de travail nous conduit à définir la nature des éléments de l'image recevant l'information de la marque. Cette nature dépend essentiellement de l'espace de représentation de l'image à marquer. Chaque espace apporte diverses possibilités en termes de performance et de robustesse. On distingue principalement deux domaines : spatial et transformé.

1) **Domaine spatial**

Le watermark est inséré en modifiant directement les valeurs de pixels de l'image hôte. Ce sont des méthodes simples et peu coûteuses en temps de calcul. Elles sont consacrées

aux tatouages en temps réel demandés dans des environnements de faible puissance. La plupart des techniques spatiales sont basées sur l'addition d'une séquence pseudo bruit (PN) d'amplitude fixe . Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB de l'image hôte. Le watermark est généralement inséré en utilisant la connaissance de la séquence PN(et peut être la connaissance d'une clé secrète) [10].

2) **Domaine fréquentiel**

Les méthodes présentées précédemment permettent en général de retrouver le watermark en faisant la différence entre l'image originale et l'image tatouée. Cela leur confère un sérieux désavantage : une personne qui voudrait attaquer ces images et qui se serait procurée une image originale, ou bien plusieurs personnes mettant en commun leurs images tatouées peuvent détruire le watermark. Des algorithmes incluant le watermark non pas directement dans l'image, mais dans une transformée (DCT,DFT,DWT) de l'image seront à cet égard plus robustes, et permettent en plus de choisir les pixels qui seront plus résistants à certains types d'attaques [1].

1.2.5 Les attaques liées au tatouage

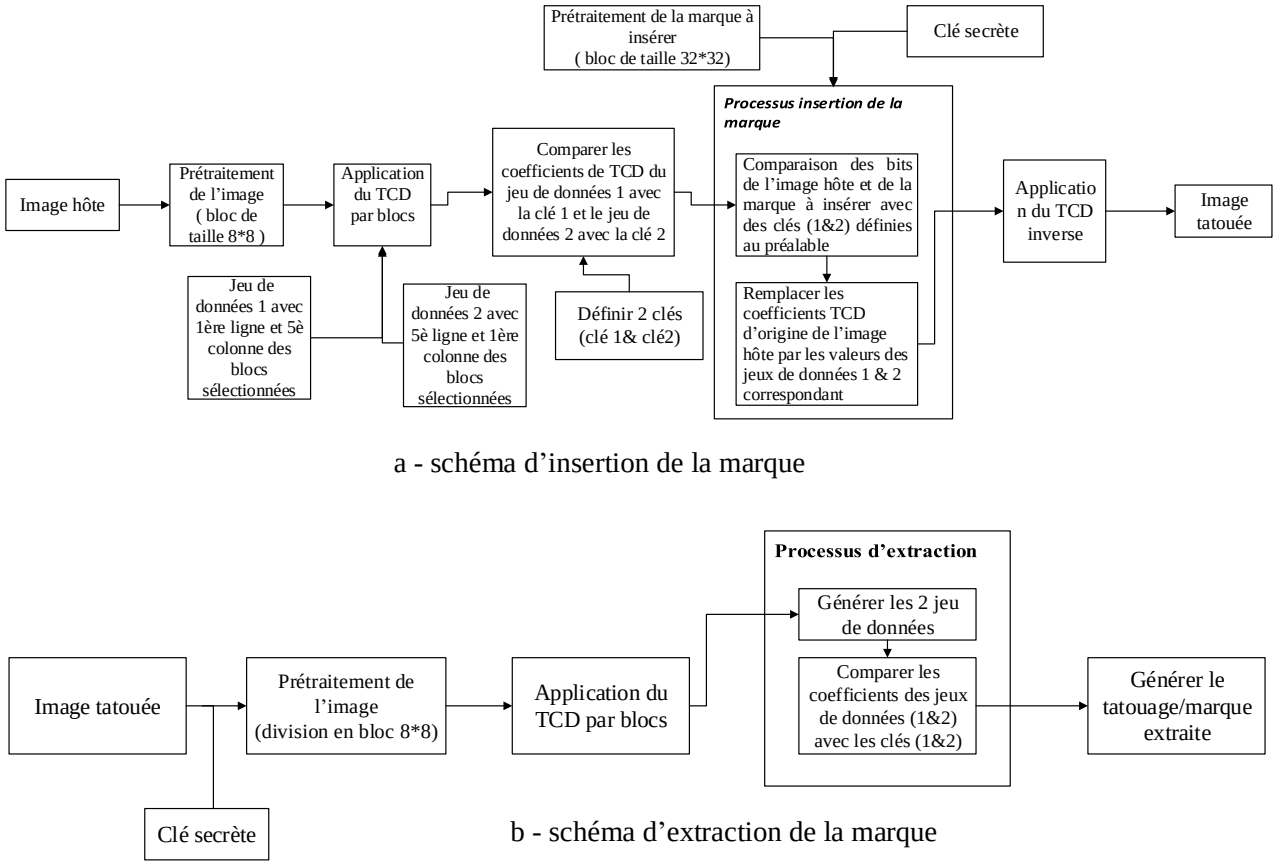
Un des critères fondamentaux à prendre en compte lors de la conception d'un algorithme de tatouage numérique est la robustesse de la marque. En effet, la marque doit pouvoir résister à certaines attaques qu'elles soient bienveillantes ou malveillantes, sauf pour le tatouage fragile [7].

- **attaques bienveillantes**: regroupe les manipulations effectuées par un utilisateur qui n'ont pas initialement pour objectif d'empêcher la détection de la marque. il peut s'agir des dégradations dues à une compression (JPEG, JPEG2000), à un filtrage avec pour but de réduire le bruit, à une conversion de format, à un changement de résolution, etc [7].
- **attaques malveillantes**: regroupe les opérations qui ont pour objectifs de supprimer ou d'empêcher l'extraction correcte de la marque [7].

1.3 Travaux existants

Sunesh et R.Rama Kishore (2022) [17] dans **A Novel and Efficient Blind Image Watermarking in Transform Domain** proposent une méthode de tatouage numérique aveugle d'images utilisant la Transformée en Cosinus Discrète (DCT). La méthode proposée offre une bonne imperceptibilité (PSNR $\approx$ 47 dB) et une très bonne complexité de calcul, mais manque de robustesse car elle ne teste que deux attaques, laissant la robustesse aux autres attaques courantes non vérifiée. Les applications concrètes nécessitent une résistance à un éventail d'attaques plus large. De plus, l'utilisation du chiffrement symétrique peut entraver la sécurité. Elle repose sur des valeurs de seuil préfixées ($key1$ et $key2$), qui peuvent ne pas être généralisées

à différentes images ou attaques. Des seuils adaptatifs pourraient améliorer la robustesse. La portée limitée des tests de robustesse et le recours à des seuils fixes constituent des inconvénients majeurs.

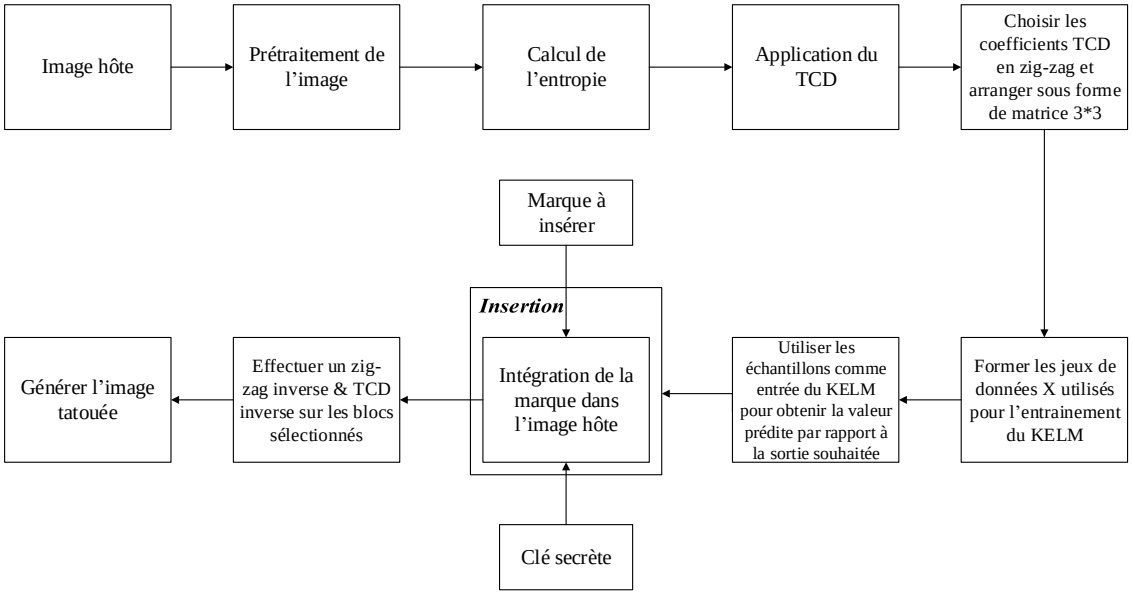


Source: A Novel and Efficient Blind Image Watermarking In Transform Domain [17]

Figure 1.5: Schéma de fonctionnement de la solution de Sunesh et R.Rama Kishore

Virendra P. Vishwakarma et Varsha Sisaudia (2020) [18] dans **Gray-scale image watermarking based on DE-KELM in DCT domain** proposent une technique de tatouage semi-aveugle pour les images en niveaux de gris, utilisant l'évolution différentielle (DE) et le Kernel Extreme Learning Machine (KELM) dans le domaine de la transformée en cosinus discrète (DCT). L'objectif est d'optimiser l'imperceptibilité et la robustesse. Elle nécessite des informations de sélection de blocs lors de l'extraction, ce qui la rend semi-aveugle. Une extraction totalement aveugle améliorerait sa praticabilité. L'optimisation DE, bien qu'efficace, ajoute une charge de calcul lors de l'intégration. Les applications temps réel peuvent nécessiter une optimisation supplémentaire. Les performances de KELM dépendent de la qualité des données d'entraînement. Des blocs mal sélectionnés ou des échantillons d'entraînement insuffisants peuvent réduire la précision des prédictions, affectant ainsi l'extraction du tatouage. La sélection de blocs basée sur l'entropie privilégie les régions lisses, mais les bords et les textures

peuvent encore souffrir de distorsions visibles sous des facteurs d'échelle agressifs. L'utilisation du chiffrement symétrique peut entraver la sécurité de la méthode.



a – Processus d'insertion de la marque

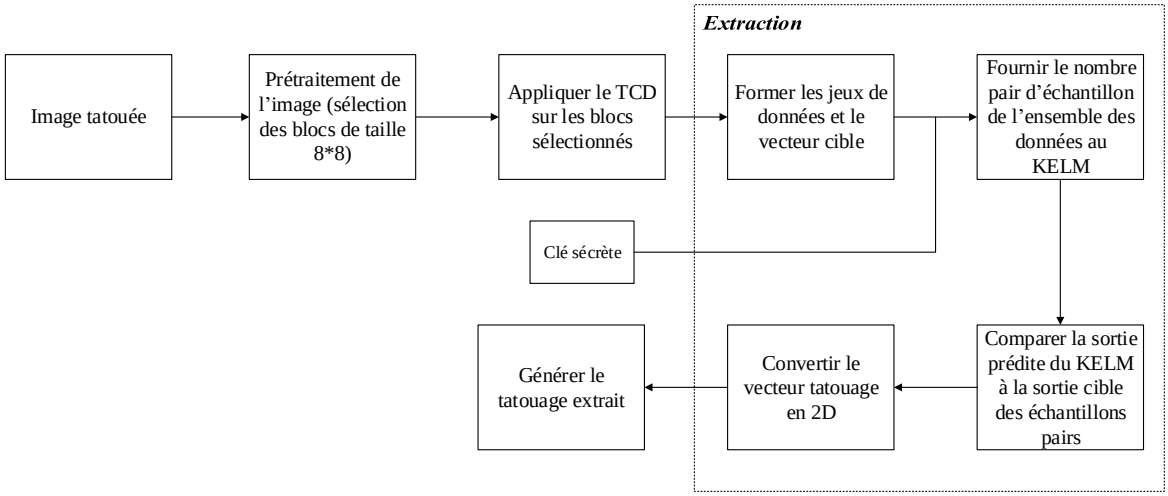


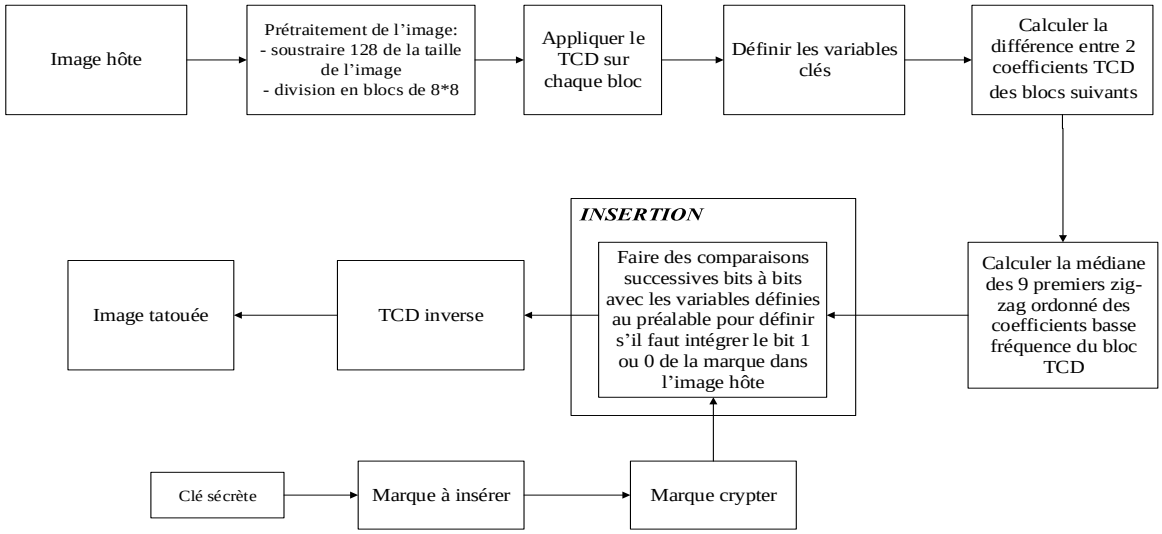
Figure b : Processus d'extraction de la marque

Source: Gray-scale image watermarking based on DE-KELM in DCT domain [18]

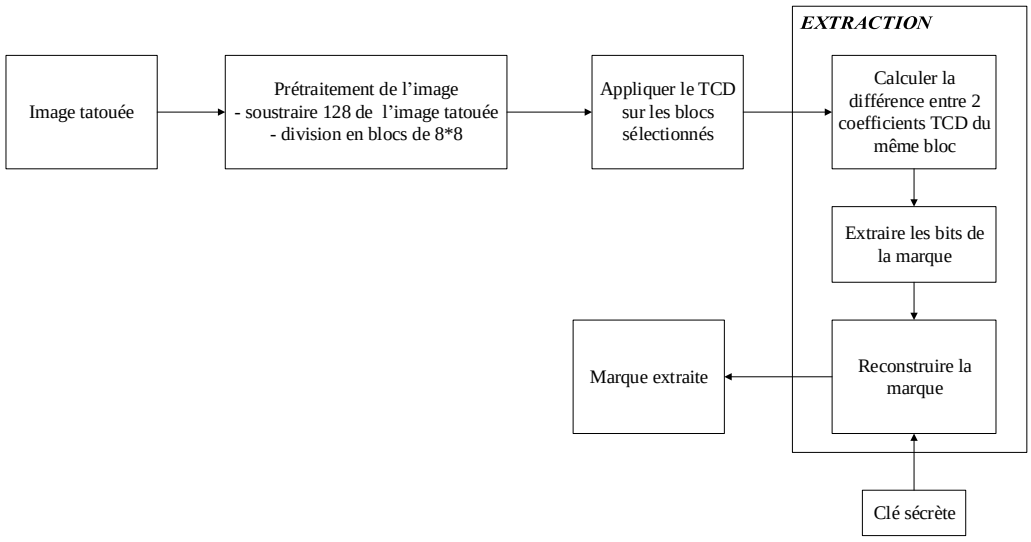
Figure 1.6: Schéma de fonctionnement de la solution de Virendra P. Vishwakarma et al

Shabir A. Parah et al. (2018) [19] dans **Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing** proposent une technique robuste de tatouage aveugle, basée sur la modification du coefficient DCT par bloc. Cette technique de tatouage basée sur le DCT offre une excellente capacité (4096 bits pour les images en niveaux de gris, 12 kbits pour les images couleurs). Bien que les valeurs PSNR soient satisfaisantes, des modifications agressives des coefficients DCT dans les régions texturées peuvent introduire des

artefacts visibles, en particulier pour les forces d'intégrations élevées (par exemple, les facteurs d'échelle importants). La méthode suppose un alignement fixe de blocs 8×8, qui peut ne pas être maintenu après des transformations géométriques (redimensionnement ou rotation), ce qui entraîne des erreurs d'extraction. La modification itérative des coefficients et la rerotation pour l'extraction augmentent la charge de calcul, limitant ainsi l'applicabilité en temps réel. L'utilisation du chiffrement symétrique peut entraver la sécurité de la méthode.



b : Processus d'extraction de la marque



a : Processus d'insertion de la marque

Source: Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing [19]

Figure 1.7: Schéma de fonctionnement de la solution de Shabir A. Parah et al

Dans la suite, un tableau de comparaison des différents travaux va être proposé .

Auteurs	*Approches*	*Résultats*	*Avantages*	*Limites*
Sunesh et R. Rama Kishore (2022) [17]	DCT à deux (02) positions différentes	PSNR ≈ 47 dB NC = 0.9984	- Haute imperceptibilité - Bonne capacité de stockage - Résistance à l' attaque (histogramme d'égalisation) - Excellent temps d'exécution des opérations	- Faible niveau de sécurité - Ne prend pas en compte plusieurs attaques singulières (salt & pepper, Filtre laplacien, Filtre wiener)
Virendra P. Vishwakarma et Varsha Sisaudia (2020) [18]	DCT combiné au DE/KELM	PSNR = 44.9 dB NC = 1	- Très bonne imperceptibilité - Marque acceptable après extraction - Bonne capacité de stockage - Robustesse face aux attaques singulières (Filtre wiener, histogramme d'égalisation)	- Faible niveau de sécurité -Impact négatif des paramètres du DE sur la robustesse et l'imperceptibilité - Ne prend pas en compte plusieurs attaques singulières (Salt & pepper, Filtre laplacien)
S.A Parah et al (2018) [19]	DCT combiné aux coefficients différentiels inter-block	PSNR ≈ 41.5 dB NC = 1	- Bonne imperceptibilité - Marque acceptable après extraction - Robustesse aux attaques singulières (salt & pepper, histogramme d'égalisation) et hybrides - Prend en compte les images couleurs et à niveau de gris - Excellente capacité de stockage	- Temps d'exécution long - Faible niveau de sécurité - Ne prend pas en compte d'autres attaques singulières (Filtre Laplacien, Filtre Wiener)

Table 1.1: Tableau comparatif des différentes approches

L'analyse des travaux antérieurs met en évidence une prédominance de l'utilisation des clés symétriques pour les opérations de protection des contenus numériques dans les images

numériques. Ce constat soulève une limite majeure à savoir le risque sécuritaire lié à la compromission des clés symétriques par des tiers. Cette préoccupation a motivé l'adoption d'une approche fondée sur la cryptographie asymétrique, combinant clé publique et clé privée pour renforcer la sécurité de la marque dans le processus d'insertion et d'extraction.

Ce chapitre a été axé sur la présentation du tatouage numérique dans sa généralité et les travaux existants y afférents dans le domaine fréquentiel. Ces éléments seront utiles dans la démarche de réalisation et à la proposition du modèle qui sera décrit dans la suite.

CHAPTER 2

TATOUAGE NUMERIQUE ASYMETRIQUE DANS LE DOMAINE DCT

La méthode proposée dans ce chapitre est un tatouage opérant dans un domaine fréquentiel obtenu par l'application de la *DCT*. Etant donné que le tatouage numérique se base sur deux (02) opérations fondamentales à savoir : l'insertion et l'extraction, un algorithme de chiffrement sera couplé aux différentes opérations afin d'augmenter le niveau de sécurité de la méthode proposée. En effet, l'extraction de la marque ne fait pas recours à l'image originale mais à l'image tatouée et éventuellement une clé, ce qui permet de qualifier le tatouage d'aveugle.

2.1 Approche proposée

Tout d'abord, l'algorithme de chiffrement qui sera utilisé sera présenté et ensuite pour terminer par la présentation du modèle avec ses différentes parties.

2.1.1 Choix de l'algorithme de Chiffrement

Au vu des différents travaux présentés à la section 1.3, un tableau de comparaison entre les 2 méthodes de chiffrement les plus connus sera proposé et le choix sur la méthode de chiffrement sera adopté pour réaliser les 2 opérations.

Caractéristiques	Chiffrement Symétrique	Chiffrement Asymétrique
Principe	Une seule clé .	une paire de clé : publique et privée.
Vitesse	Très rapide car les algorithmes sont moins complexes.	Plus lent en raison des calculs mathématiques complexes.
Sécurité	Moins sécurisé si la clé est compromise.	Plus sécurisé car la clé privée n'est jamais partagée.
Gestion des clés	Difficile car il faut partager la clé secrète entre les parties.	Plus simple car seule la clé publique est distribuée.
Complexité	Simple à mettre en œuvre.	Plus complexe à mettre en œuvre.

Table 2.1: Comparaison entre les méthodes de chiffrement

Au vu du tableau 2.1, le chiffrement asymétrique est plus avantageux en terme de sécurité que le chiffrement symétrique et donc le choix sera porté sur le chiffrement asymétrique RSA qui présente les caractéristiques suivantes :

- Il est utilisé pour la transmission sécurisée des données ;
- Il utilise le concept mathématique de factorisation du produit de deux grands nombres premiers ;
- Il est rapide en termes de chiffrement ;
- Il est mieux adapté à la vérification et au cryptage.

2.1.2 Génération des clés

Les clés utilisées seront générées par l'algorithme de chiffrement RSA.

Algorithm 1 Génération de paires de clés RSA

1: **Entrées** : p , q deux grands nombres premiers ;
2: **Sorties** : Clé publique K_p , Clé privée K_s
3: Calculer $n = p \times q$
4: Calculer $\phi(n) = (p-1)(q-1)$
5: Choisir K_p tel que $1 < K_p < \phi(n)$ et $\gcd(K_p, \phi(n)) = 1$
6: Calculer K_s tel que $K_s \times K_p \equiv 1 \mod \phi(n)$
7: Générer : Clé publique (K_p, n) et Clé privée (K_s, n)
8: **Fin** =0

2.1.3 Modèle proposé

En se basant sur le modèle générique présenté à la figure 1.2 plus haut, le modèle proposé est présenté par le schéma 2.1.

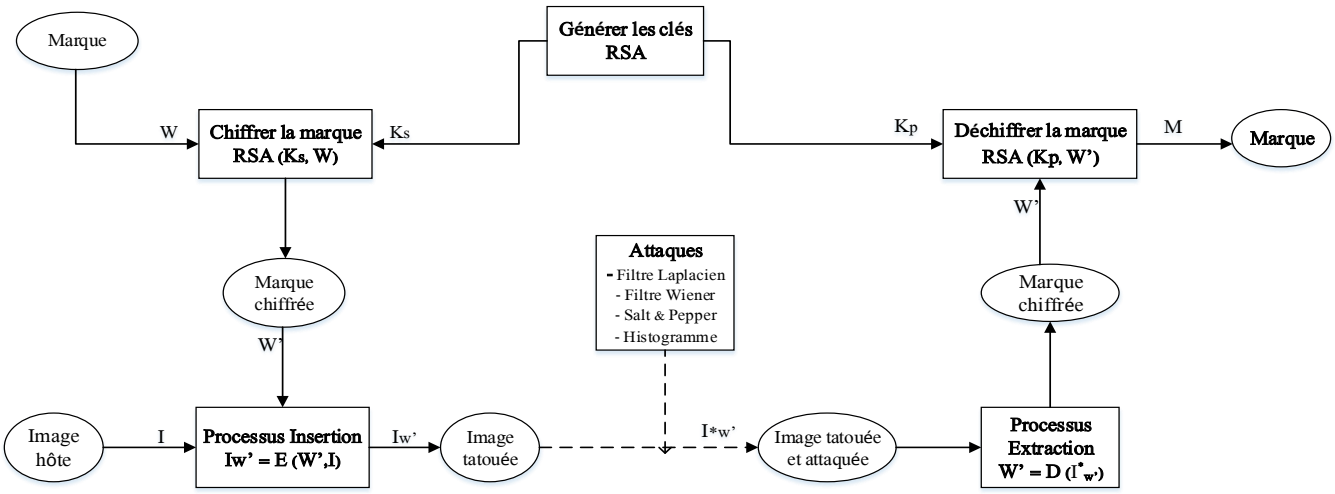


Figure 2.1: Modèle proposé

a) **Insertion**

Au tout début, la marque W est chiffrée en utilisant la clé privée K_s grâce à l'algorithme de chiffrement RSA. Ensuite, la marque chiffrée $W^{'}$ est insérée dans l'image hôte I au niveau des blocs des moyennes fréquences pour Générer en sortie une image tatouée $I_{W'}$. La phase d'insertion est modélisée par la fonction suivante :

$$\mathrm{I}_{W'} = \mathrm{E}\ (\mathrm{W}, K_s, \mathrm{I}) \tag{2.1}$$

b) **Extraction**

L'image tatouée pourrait ensuite être copiée et attaquée, l'image reçue est $I^*_{W'}$. Pendant la phase d'extraction, la marque chiffrée $W^{'}$ est extraite et ensuite on applique le déchiffrement grâce à l'algorithme RSA en utilisant la clé publique K_p correspondante à la clé privée K_s utilisée à l'insertion pour cette fois Générer la marque extraite M. La phase d'extraction consiste à calculer une estimation M de W obtenue après extraction de la marque M dans l'image reçue.

La phase d'extraction est modélisée par la fonction suivante :

$$M = \mathrm{D}\ (\mathrm{I}^*_{W'}, K_p) \tag{2.2}$$

2.1.4 Processus d'insertion

L'algorithme va Générer une image tatouée $\boldsymbol{I}_{W'}$ en se servant de l'image hôte I, de la marque W et aussi de la clé privée K_s issue de l'algorithme précédent. En plus de cela, la marque sera insérée dans les blocs des moyennes fréquences de l'image grâce à la DCT.

Le choix de la DCT est motivé par plusieurs considérations à la fois techniques, pratiques et liées à la sécurité. En effet, les coefficients de la DCT peuvent être modifiés légèrement sans altérer la qualité visuelle de l'image, ce qui permet d'intégrer des données (tatouage ou message chiffré) de manière invisible et robuste. La DCT est largement compatible avec les standards de compression d'image (comme JPEG), ce qui la rend plus résiliente face aux attaques courantes telles que la recompression, les filtres ou l'ajout de bruit.

En conclusion, la DCT offre un excellent compromis entre simplicité de mise en œuvre, efficacité de compression, robustesse du tatouage, et sécurité des données. Ces caractéristiques en font une méthode particulièrement pertinente dans le cadre de cette étude sur la protection des images numériques par tatouage et cryptographie.

1. **Formule du DCT**

Le calcul du DCT est donné par la formule suivante :

$$DCT(u,v) = \frac{1}{\sqrt{2 \cdot M \cdot N}} C(u)C(v) \sum_{x=1}^{M} \sum_{y=1}^{N} I(x,y) cos(\frac{(2 \cdot x + 1)\pi \cdot u}{2 \cdot M}) cos(\frac{(2 \cdot y + 1)\pi \cdot v}{2 \cdot N}) \tag{2.3}$$

avec :

- **[M,N]** : taille de l'image ;
- $I(x, y)$: intensité du pixel dans la ligne x et la colonne y de l'image ;
- **DCT(u,v)** : coefficient DCT à la ligne u et la colonne v ;

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{si } x = 0 \\ 0, & \text{sinon} \end{cases}$$

2. **Algorithme d'insertion de la marque** :
L'algorithme présenté ci-dessous permet d'insérer la marque W dans l'image I en utilisant un chiffrement RSA, suivi d'un tatouage dans le domaine fréquentiel (DCT). Cette méthode assure à la fois la sécurité de la marque (par chiffrement) et une robustesse face aux attaques (en insérant l'information dans les composantes moyennes des blocs de l'image).

2.1.4.1 Description de la méthode

L'insertion de la marque suit les étapes suivantes :

(a) **Chiffrement de la marque** : La marque W est d'abord chiffrée à l'aide de la clé privée K_s via l'algorithme RSA, générant ainsi la marque chiffrée W' ;

(b) **Calcul de la taille de la signature** : Cette taille, notée sig_size, détermine la quantité d'espace nécessaire pour l'insertion ;

(c) **Définition des zones d'insertion** : Selon la taille de l'image, différentes positions (x, y) sont sélectionnées pour insérer la marque. Cela permet une insertion redondante ou multi-localisée pour améliorer la robustesse ;

(d) **Tatouage dans le domaine fréquentiel** :

- L'image est parcourue par blocs de taille $size \times size$ à partir des positions d'insertion ;
- Dans chaque bloc, la marque est insérée dans la composante située à la position $(size - 1, size - 1)$, souvent associée à une fréquence moyenne dans la DCT ;
- La modification est pondérée par un facteur de qualité Q, qui ajuste l'intensité de l'insertion ;
- Une DCT inverse est appliquée pour revenir à l'espace image, avec une vérification pour rester dans les valeurs valides de pixels (0 à 255).

(e) **Génération de l'image tatouée** : Une fois tous les blocs modifiés, l'image tatouée $I_{W'}$ est générée.

2.1.4.2 Schéma illustratif de la méthode

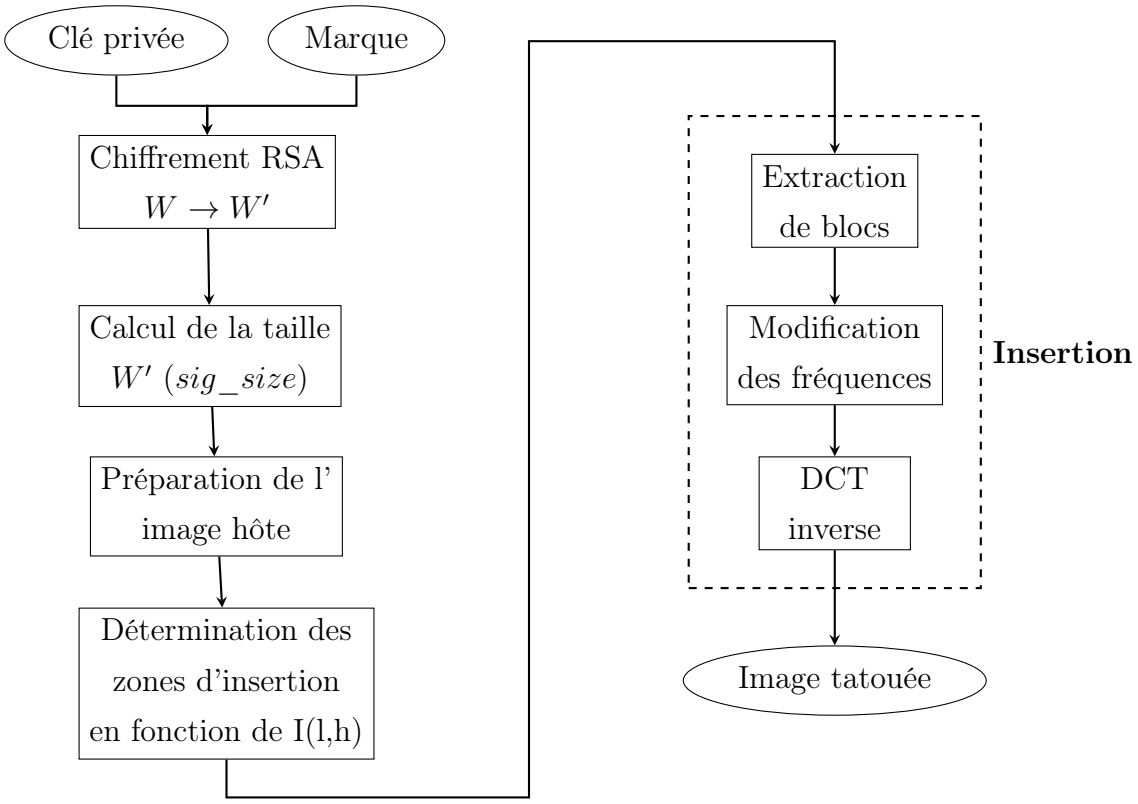


Figure 2.2: Schéma de fonctionnement

Algorithm 2 Insertion de la marque

1: **Entrées:** Image I , marque W, clé privée K_s
2: **Sortie:** Image tatouée $I_{W'}$
3: **Début:**
4: $W' \leftarrow RSA(W, K_s)$
5: Parcourir et récupérer un bloc de I
6: **for** Chaque bloc de I **do**
7: Appliquer la DCT à ce bloc
8: Insérer la marque dans ce bloc
9: Appliquer la DCT Inverse à ce bloc
10: **end for**
11: Répéter (5) jusqu'à ce que W' soit totalement inséré
12: Générer l'image tatouée $I_{W'}$
13: **Fin** =0

La figure 2.2 illustre parfaitement le fonctionnement de la méthode d'insertion de la marque dans l'image. Dans la suite, l'organigramme correspondant à l'algorithme d'insertion de la marque dans l'image sera présenté.

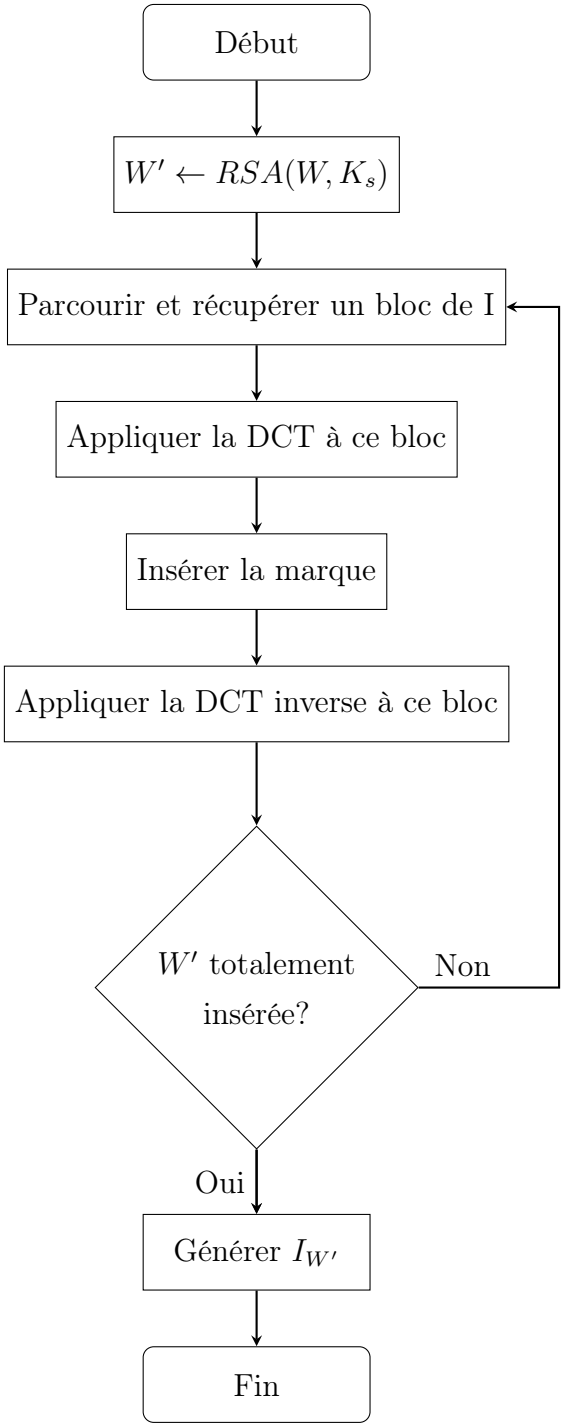


Figure 2.3: Organigramme de l'algorithme d'insertion

2.1.5 Processus d'extraction

L'algorithme d'extraction quant à lui nécessite en plus de l'image tatouée et éventuellement attaquée $I^*_{W'}$, de la clé publique K_p pour l'extraction de la marque.

2.1.5.1 Description de la méthode

L'algorithme repose sur les étapes suivantes :

1. **Initialisation** : On fixe les paramètres utilisés lors de l'insertion, notamment :
   - La taille de la marque sig_size (doit être connue ou convenue à l'avance) ;
   - La taille de bloc $size$ (utilisée dans la DCT) ;
   - Le facteur de qualité Q utilisé pour l'insertion.
2. **Parcours de l'image** : L'image tatouée est parcourue par blocs de taille $size \times size$;
3. **Analyse fréquentielle** :
   - Pour chaque bloc, la DCT est appliquée pour retrouver les coefficients fréquentiels ;
   - Le coefficient situé à la position $(size - 1, size - 1)$ est analysé ;
   - S'il dépasse un seuil $(Q/2)$, un bit 1 est extrait ; sinon un bit 0;
4. **Reconstruction de la marque** : Un tableau W' binaire est formé à partir des bits extraits ;
5. **Déchiffrement RSA** : La marque binaire est ensuite déchiffrée avec la clé publique K_p pour obtenir la marque originale M.

Cette méthode permet de récupérer une marque de manière robuste et sécurisée, même après modification de l'image.

2.1.5.2 Schéma illustratif de la méthode

Par la suite, le schéma de fonctionnement, l'algorithme et l'organigramme correspondant à l'extraction de la marque dans l'image seront présentés.

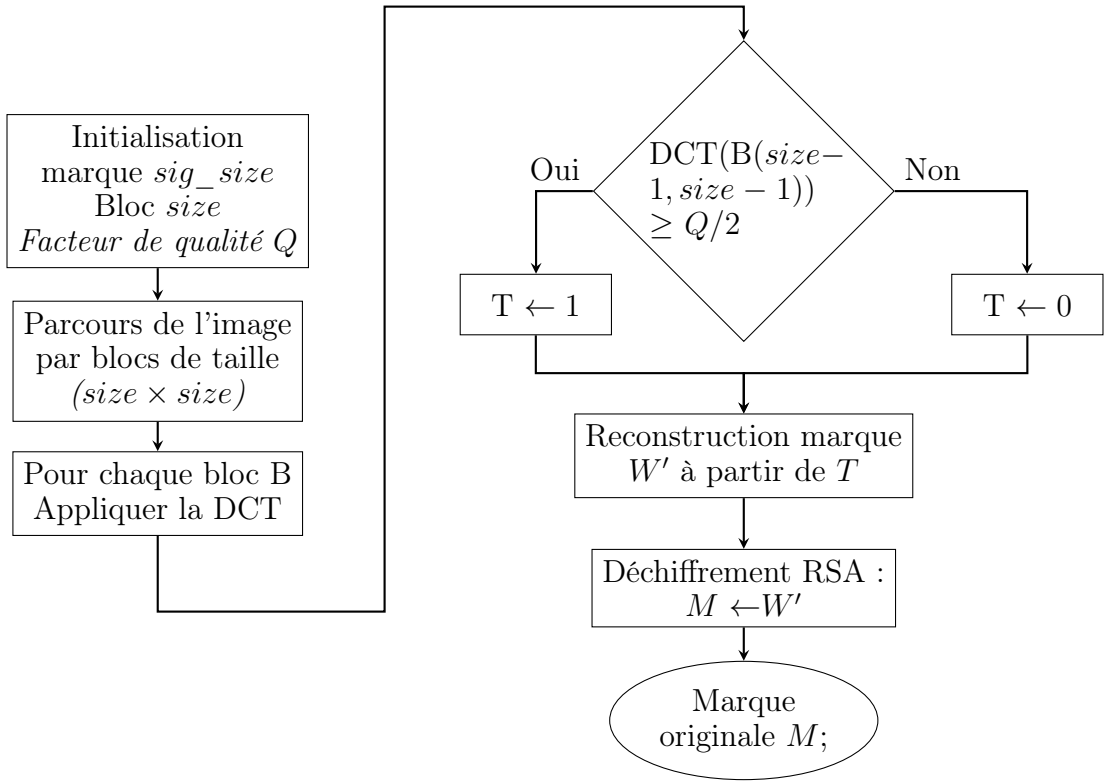


Figure 2.4: Schéma de fonctionnement

Algorithm 3 Extraction de la marque

Entrées: Image tatouée attaquée $I^*_{W'}$, clé publique K_p
Sortie: Marque extraite M
Début:
Initialiser un vecteur T, Définir un seuil
Parcourir et récupérer un bloc de $I^*_{W'}$
for Chaque bloc récupéré de $I^*_{W'}$ **do**
    Appliquer la DCT à ce bloc
    Vérifier la présence de la marque dans ce bloc {DCT(bloc)>seuil}
  if Marque trouvée **then**
        Marquer cela dans un tableau T
  end if
end for
Transformer T en matrice
Ajuster les valeurs de la matrice (0-255)
Générer la marque chiffrée W'
$M \leftarrow RSA(W', K_p)$
Générer la marque M
Fin =0

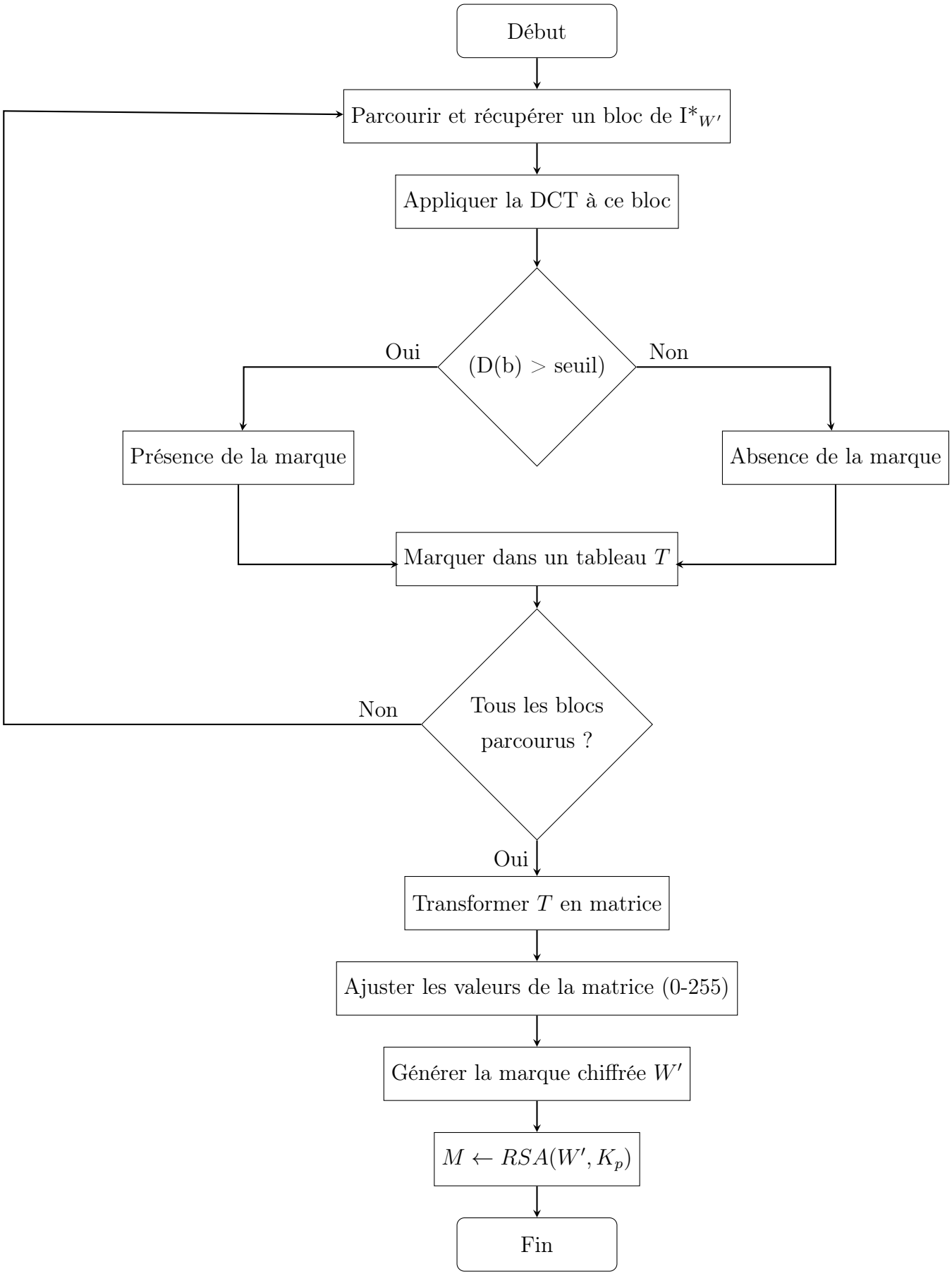


Figure 2.5: Organigramme de l'algorithme d'extraction

2.2 Modélisation Formelle

Les formules mathématiques essentielles seront présentées dans cette section.

2.2.1 Au niveau du processus d'insertion

L'élément à prendre en compte sera l'insertion de la marque qui a été chiffrée au préalable.

1. **Insertion de la marque** ;
   Plusieurs sous étapes sont effectuées à savoir :

   (a) **Application de la DCT** : Pour chaque bloc **b** de taille $m \times n$ la DCT est calculée selon la formule à la section 2.3:

   $$B_{(i,j)} = \text{DCT } [b_{(i,j)}]$$

   où b = I(i:i+m,j:j+n)

   (b) **Modification du coefficient DCT** : Le watermark est inséré en modifiant un coefficient spécifique B avec le bit correspondant $W_{(i,j)}$ du watermark. La modification est effectuée selon la relation suivante :

   $$B_{(i,j)}(\text{m-1,n-1}) = B_{(i,j)}(\text{m-1,n-1}) + \text{Q} \cdot W_{(i,j)}$$

   Cette relation montre que le coefficient DCT à l'indice $(m-1, n-1)$ est remplacé par le produit du bit du watermark $W_{(i,j)}$ et du facteur de qualité Q.

   (c) **Reconstruction du bloc** : Après modification du coefficient DCT, on applique l'inverse de la DCT (IDCT) pour revenir dans le domaine spatial et obtenir le bloc modifié $B'_{(i,j)}$:

   $$B'_{(i,j)} = DCT^{-1} \ [B_{(i,j)}]$$

   où $B^{'}$ est le bloc de pixels reconstruit contenant l'information du watermark.

2. **Remplacement dans l'image** : Le bloc $B'_{i,j}$ avec le watermark inséré, remplace le bloc original $B(i : i+m, j : j+n)$ dans l'image :

   $$B(i : i+m, j : j+n) = B^{'}$$

   Une fois que tous les blocs $B'_{i,j}$ ont été modifiés, l'image finale contenant le watermark est reconstruite en combinant tous les blocs $B'_{i,j}$.

La formule mathématique sous-jacente qui se dégage est la suivante :

$$I_{W'} = \sum_{i=1}^{M} \sum_{j=1}^{N} [\text{D}^{-1} \ (\text{D } (\text{B}_{(i,j)}) + Q \cdot \text{W}_{(i,j)})] \tag{2.4}$$

où la somme est effectuée sur tous les blocs sélectionnés pour l'insertion de la marque dans l'image I. Dans cette formule :

- $I_{W'}$ représente l'image tatouée ;
- Q représente le facteur de qualité pour contrôler la force d'insertion du watermark ;
- $W_{(i,j)}$ représente le bit du watermark correspondant au bloc $B_{(i,j)}$;
- $B_{(i,j)}$ représente le bloc de l'image originale ;
- D et D^{-1} représentent respectivement la DCT et son inverse (IDCT) ;

La formule 2.4 permet de constater que la solution proposé est un tatouage de type *additif* comme stipulé à la section 1.2.4.1.

2.2.2 Au niveau du processus d'extraction

L'élément important à prendre en compte est l'extraction de la marque malgré les différentes manipulations subies .

1. **Application de la DCT** : Pour chaque bloc $b'_{i,j}$, on applique la DCT pour obtenir la matrice des coefficients $B^*_{i,j}$:
$$B^*_{i,j} = \text{DCT } (b'_{i,j})$$
2. **Condition de détection du watermark** : Le bit du watermark $W'_{i,j}$ est déterminé en analysant la valeur du coefficient $B^*_{i,j}$ (m-1, n-1). Si ce coefficient est supérieur à un certain seuil, on considère que le bit est 1, sinon il est 0 :
$$W'_{i,j} = \begin{cases} 1 & \text{si DCT } (B^*_{(i,j)}) \text{ (m-1,n-1)} > \frac{Q}{2} \\ 0 & \text{sinon} \end{cases} \tag{2.5}$$
Cela compare la valeur du coefficient DCT modifié par le watermark avec un seuil. Ce seuil est choisi en fonction du facteur Q utilisé lors de l'insertion pour que la valeur soit distinguable ;
3. **Reconstruction du watermark** : Le watermark extrait est progressivement reconstruite en combinant tous les bits $W'_{i,j}$ extraits de chaque bloc de l'image. Le résultat final est une matrice représentant le watermark ;

La formule 2.5 permet de constater que l'algorithme de détection proposé est de type *aveugle* comme stipulé à la section 1.2.4.1.

Le modèle présenté dans ce chapitre a mis en exergue les 2 opérations clés de la solution de tatouage proposée à savoir l'insertion et l'extraction de la marque dans l'image. Le chapitre suivant présentera la mise en place des éléments nécessaire à la réalisation du modèle.

CHAPTER 3

EXPÉRIMENTATION

Ce chapitre est consacré à l'expérimentation de la solution de tatouage c'est-à-dire tous les éléments (matériels et outils) ayants servis à la réalisation de la solution proposée ainsi que les différentes métriques réparties selon deux critères qui seront utilisés pour évaluer l'algorithme de tatouage numérique proposé.

3.1 Environnement de développement

Les éléments nécessaires à la réalisation de ce travail seront présentés à savoir les outils utilisés, l'environnement matériel et également le jeu de données typiquement utilisés dans le traitement du signal.

3.1.1 Outils utilisés

- **Python** : Python est un langage de programmation de haut niveau interprété et orienté objet avec une sémantique dynamique. Il est très sollicité par une large communauté de développeurs et de programmeurs. Python est un langage simple, facile à apprendre et permet une bonne réduction du coût de la maintenance des codes [20] ; Ce langage a permis de rédiger les fonctions et classes à travers les modules qui ont permis à la réalisation de ce travail.

- **CV2** : Le module le plus important d'**OpenCV** est une bibliothèque open-source très populaire en Python utilisée pour le traitement d'images, la vision par ordinateur et la reconnaissance de formes. Elle a été développée par Intel et est maintenant maintenue par la communauté open-source. OpenCV fournit un large éventail de fonctionnalités et d'algorithmes pour travailler avec des images [20] ; C'est cette bibliothèque qui a particulièrement aidé sur les opérations liées aux images à travers :

  - **Manipulation des images** : OpenCV a permis d'ajuster la luminosité, le contraste et la saturation des images. De plus, il a permis d'effectuer des opérations arithmétiques sur les images ;
  - **Chargement et affichage des images** : OpenCV a permis de lire et de charger des images à partir de fichiers et d'afficher des images à l'écran ;

– **Traitement des images** : OpenCV a permis de réaliser les opérations telles que la suppression du bruit, le filtrage de couleur, etc.

3.1.2 Environnement matériel

La Configuration matériel inclut les caractéristiques suivants :

- **Modèle** : Toshiba Satellite Pro C650 ;
- **Processeur** : Intel R Core (TM) 2 Duo CPU T6570 @2.10 Ghs (2 CPUs) ;
- **RAM** : 4G ;
- **Ecran** : 15.6 pouces ;
- **Système** : Linux Mint x64 ;

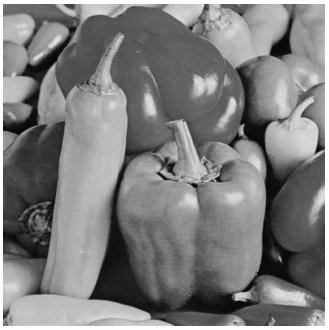
3.1.3 Jeu de données

Un jeu de données classique en traitement d'images sera utilisé comme images hôtes.

Lena
320 * 320

Barbara
512 * 512

Cameraman
256 * 256



Pepper
474 * 474

Table 3.1: Jeu de données

Par la suite, une image est utilisée comme marque/signature à insérer dans l'image hôte :

signature
100 * 100

3.2 Évaluation

L'évaluation de l'efficacité de l'algorithme proposé se fera en terme de degré de dégradation de l'image tatouée, de sa sensibilité et son aptitude à détecter toute transformation dans l'image. L'évaluation a été séparée en deux parties : la première est d'analyser la propriété d'imperceptibilité à travers les métriques $PSNR$ et $SSIM$ et la deuxième est l'évaluation de la propriété de fragilité par rapport aux attaques à travers la métrique NC.

3.2.1 Propriété d'imperceptibilité

Le ***PSNR*** (Peak Signal to Noise Ratio) est la mesure de la distorsion de pixel à pixel entre l'image tatouée et l'image originale. Elle est la mesure la plus utilisée en traitement d'image. On considère généralement en tatouage d'images qu'un tatouage est imperceptible (PSNR $>$ 36 dB), et plus il est élevé, moins la distorsion est importante. Sa formule est la suivante :

$$\text{PSNR} = 10 \log_{10} \frac{\max(I)^2}{MSE(I, I_w)} \tag{3.1}$$

où le MSE de 3.1 est donnée par :

$$\text{MSE} = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} (I_{(i,j)} - I_{W(i,j)})^2 \tag{3.2}$$

Avec : I est l'image originale, I_W est l'image marquée, $[M * N]$ est la taille de l'image, (i, j) qui représente le pixel de l'image.

Malgré l'utilisation courante du PSNR pour mesurer la qualité des images, celui-ci n'est pas bien adapté au SVH (Système Visuel Humain). Le SVH ne perçoit pas tous les signaux de la même façon comme la sensibilité au contraste par exemple. L'utilisation de PSNR seul ne peut donc pas être considérée comme une mesure objective de la qualité visuelle de l'image. Le **SSIM** (Structural Similarity Index Measure) a été développée pour mesurer la qualité visuelle d'une image compressée par rapport à l'image originale. L'idée du SSIM est de mesurer la similarité de structure entre les deux images plutôt qu'une différence pixel à pixel comme le fait par exemple le PSNR. L'hypothèse sous-jacente est que l'œil humain est plus sensible aux changements dans la structure de l'image. Elle évalue la distorsion entre l'image hôte I et l'image tatouée I_w. Elle est axée sur 3 éléments majeurs à savoir : la luminance $\boldsymbol{l}$, le contraste $\boldsymbol{c}$ et la structure $\boldsymbol{s}$. Elle est donnée par la formule suivante:

$$SSIM(I, I_w) = l(I, I_w) \cdot c(I, I_w) \cdot s(I, I_w) = \frac{(2\mu_I \mu_{Iw} + C_1) * (2\sigma_I \sigma_{Iw} + C_2)}{(\mu_I^2 + \mu_I^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} * \frac{(\sigma_{II_w} + C_3)}{(\sigma_I \sigma_{Iw} + C_3)} \tag{3.3}$$

Avec : σ_{II_w} représente la covariance de I et I_w ; σ_{Iw} et σ_I représentent respectivement la variance de I_w et I ; μ_I et μ_{I_w} représentent respectivement la moyenne de I et I_w.

3.2.2 Propriété de robustesse

La robustesse est la caractéristique en digital watermarking de préserver les informations même après les différents bruits et attaques malveillantes. La performance d'un algorithme de tatouage d'image en terme de robustesse peut-être évaluée par une métrique qui porte le nom de **NC** (Normalized Correlation). Le NC mesure la ressemblance des images plutôt que leur différence. Sa formule est la suivante :

$$NC(W, W') = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W_{i,j} * W'_{i,j}}{\sum_{i=1}^{M}\sum_{j=1}^{N} (W_{i,j})^2} \tag{3.4}$$

Avec : W et $W^{'}$ représentent respectivement la marque originale et la marque extraite ; $[M * N]$ représente la taille de la marque ; (i, j) représente le pixel dans la marque.

Au cours de ce chapitre, l'environnement de développement a été mis en exergue à travers les outils utilisés, l'environnement matériel ainsi que le jeu de données qui sera utilisée et enfin les critères sur lesquels l'évaluation de l'algorithme sera fait à travers les métriques. Dans le chapitre suivant, les résultats seront présentés selon les deux critères (imperceptibilité et fragilité) et enfin pour terminer sur une interprétation de ces résultats.

CHAPTER 4

RESULTATS

Les différents résultats seront présentés selon les deux critères (imperceptibilité et robustesse) et par la suite une interprétation liée à ces résultats sera donnée.

4.1 Analyse des résultats

Les résultats seront évalués sur 2 critères à savoir l'imperceptibilité et la robustesse.

4.1.1 Imperceptibilité

Les résultats suivant sur les images déterminent le niveau d'imperceptibilité de la marque dans l'image. Elle est présentée dans le tableau 4.1 par les images suivantes :

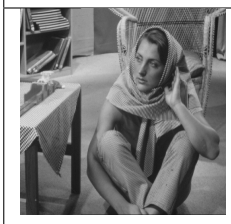
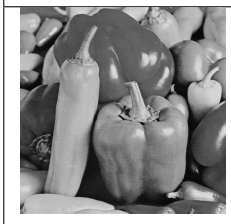
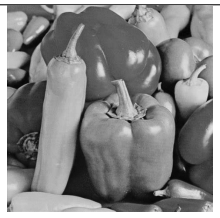
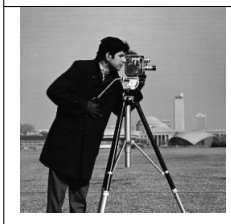
Image hôte	Image marquée	PSNR	SSIM	Tatouage extrait	Robustesse
		**50.31 dB**	**1**		NC : **1**
		**47.52 dB**	**0.99**		NC : **1**
		**47.71 dB**	**0.99**		NC : **1**
		**48.81 dB**	**1**		NC : **1**

Table 4.1: Analyse de l'imperceptibilité de la méthode proposée

4.1.2 Robustesse

La robustesse de la méthode est décrite avec les attaques répertoriées sur les images tatouées et la marque extraite M est évaluée grâce à la métrique **NC**. Les attaques testées sont :

- **Salt** & **pepper** : Modélise des erreurs de transmission ou du bruit capteur. Ces perturbations aléatoires évaluent la tolérance du système aux interférences [1] ;
- **Filtrage de Wiener** : Ce filtre adaptatif, souvent utilisé pour restaurer une image dégradée par du bruit, agit en fonction de la variance locale. Il peut atténuer le tatouage, notamment s'il est intégré dans des zones homogènes. Il est donc pertinent pour tester la robustesse du tatouage face à des restaurations adaptatives [1] ;
- **Filtrage Laplacien** : Ce filtre détecte les contours et accentue les détails fins. Son effet de renforcement des hautes fréquences peut déstabiliser un tatouage inséré dans les composantes fréquentielles moyennes ou faibles, et constitue donc une attaque pertinente pour tester la stabilité du marquage sous accentuation [1] ;
- **Égalisation d'histogramme** : Réajuste la répartition des niveaux de gris pour améliorer le contraste global. Ce traitement modifie la dynamique des pixels et peut affecter la structure statistique du tatouage, notamment s'il repose sur des relations d'intensité [1].

Ces attaques couvrent un large spectre de manipulations réelles. Leur application rigoureuse permet de valider la pertinence du schéma proposé dans des conditions réalistes.

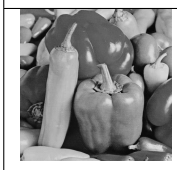
Images	Histogramme	Salt & Pepper	Filtre Laplacien	Filtre Weiner
	NC=0.94	NC=0.82	NC=0.81	NC=0.94
	NC=0.96	NC=0.89	NC=0.89	NC=0.95
	NC=0.94	NC=0.79	NC=0.79	NC=0.94
	NC=0.97	NC=0.91	NC=0.90	NC=0.96

Table 4.2: Analyse de la robustesse de la solution proposée

Le tableau 4.3 suivant propose un récapitulatif de la méthode proposée :

Images	*PSNR*	*SSIM*	*NC*	*Temps Insertion*	*Salt & Pepper*	*Égalisation histogramme*	*Filtre Laplacien*	*Filtre Weiner*	*Temps Extraction*
Lena	50.31	1	1	0.4844	0.82	0.94	0.81	0.94	0.1879
Pepper	47.71	0.99	1	0.4982	0.89	0.96	0.89	0.95	0.2052
Barbara	47.52	0.99	1	0.5168	0.91	0.97	0.90	0.96	0.2058
Cameraman	48.81	1	1	0.4851	0.79	0.94	0.79	0.94	0.1834

Table 4.3: Analyse expérimentale de la solution de tatouage d'image proposée

La solution de tatouage proposée est évaluée en comparant ses performances à celles des approches de Sunesh et al. [17], Virendra et al. [18] et Shabir A. Parah et al. [19] selon plusieurs critères : la qualité visuelle **(PSNR)**, la fidélité du tatouage **(NC)**, la résistance à l'égalisation d'histogramme, ainsi que l'efficacité en termes de temps d'exécution.

Le tableau 4.4 présente l'évaluation comparative du **PSNR** de la méthode proposée avec les autres solutions ([17–19]). La valeur du PSNR obtenue est très élevée indiquant une meilleure qualité visuelle des images tatouées par rapport à [18], [19] et proche des valeurs de [17].

Images	Sunesh et al [17]	Virendra et al [18]	Shabir A. P. et al [19]	Méthode proposée
Lena	47.7	44.9	41.27	**50.31**
Pepper	47.2	-	41.84	**47.71**
Barbara	46.9	-	-	**47.52**
Cameraman	47.5	-	-	**48.81**

Table 4.4: Evaluation de la qualité visuelle par PSNR

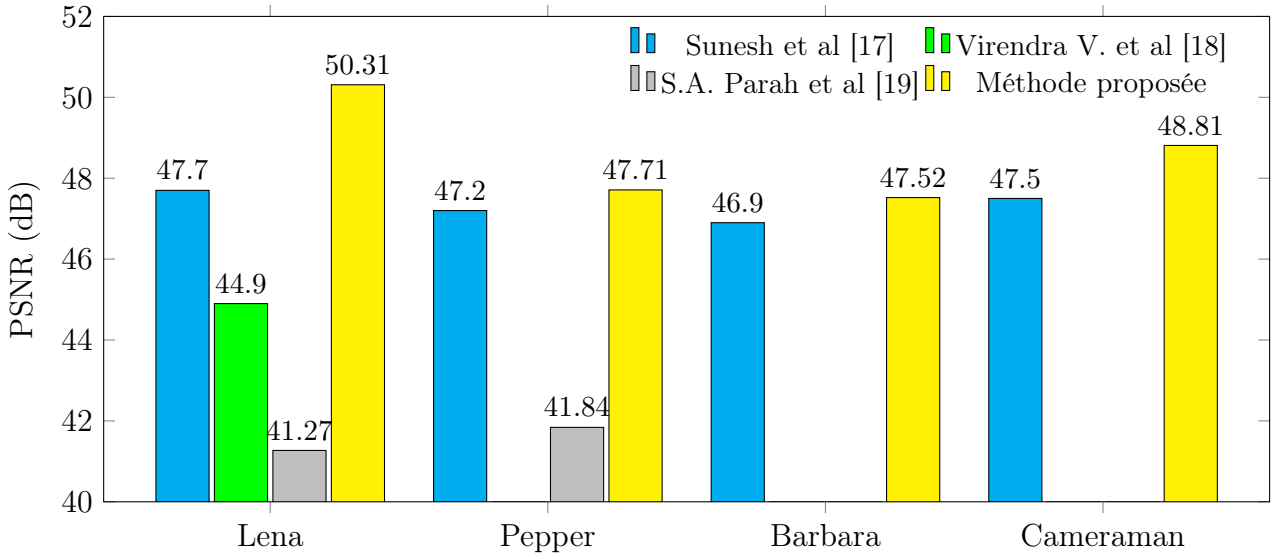


Figure 4.1: Evaluation de la qualité visuelle par PSNR

Le tableau 4.5 suivant illustre l'évaluation comparative du **NC** de la méthode proposée avec les autres méthodes (Sunesh et al [17], Virendra et al [18] et Shabir A. Parah et al [19]) à l'insertion.

Images	Sunesh et al [17]	Virendra et al [18]	Shabir A. P. et al [19]	Méthode proposée
Lena	1	1	1	**1**
Pepper	1	-	1	**1**
Barbara	0.9936	-	-	**1**
Cameraman	1	-	-	**1**

Table 4.5: Évaluation comparative du NC à l'insertion

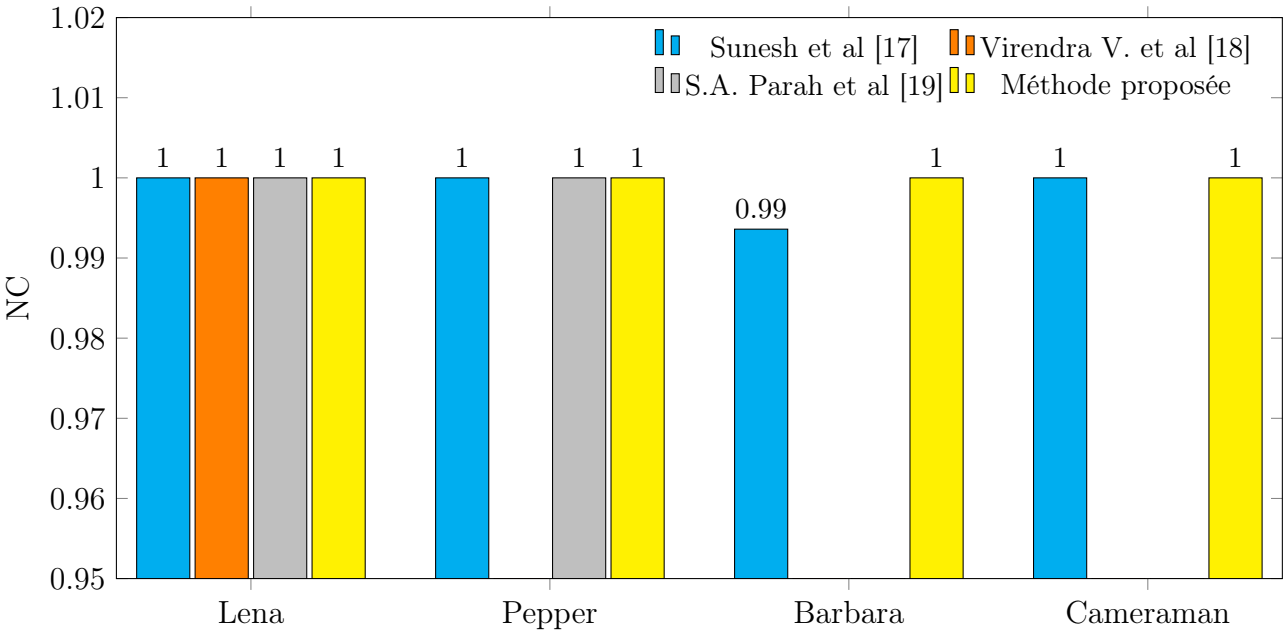


Figure 4.2: Évaluation comparative du NC à l'insertion

Le tableau 4.6 suivant illustre la comparaison des performances de la solution proposée sous l'attaque d'**égalisation d'histogramme** avec les autres solutions (Sunesh et al [17], Virendra et al [18] et Shabir A. Parah et al [19]).

Images	Sunesh et al [17]	Virendra Vishwakarma et al [18]	Shabir A. Parah et al [19]	Méthode proposée
Lena	1	1	0.90	**0.94**
Pepper	0.9078	-	-	**0.96**
Barbara	0.8473	-	-	**0.97**
Cameraman	0.9451	-	-	**0.94**

Table 4.6: Évaluation comparative des performances sous l'attaque égalisation d'histogramme

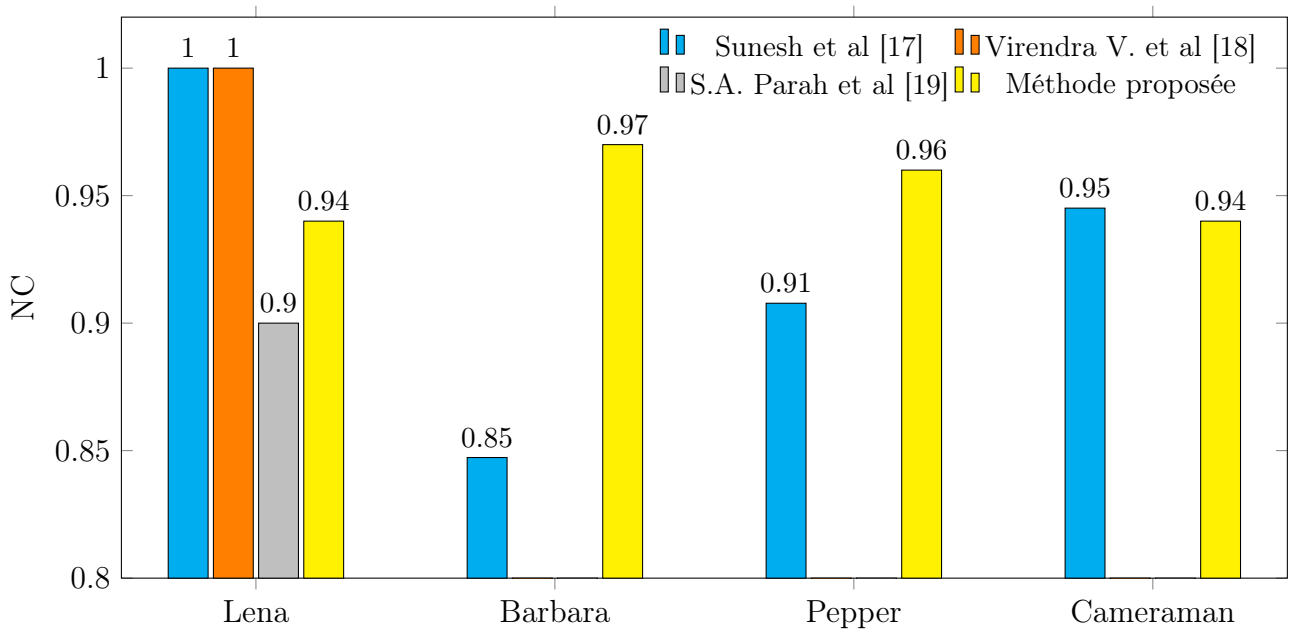


Figure 4.3: Évaluation comparative des performances sous l'attaque égalisation d'histogramme

Le tableau 4.7 illustre la comparaison du temps d'exécution des opérations et est évaluée en secondes.

Temps / Images	Sunesh et al [17]		Méthode proposée	
	Insertion	Extraction	Insertion	Extraction
Lena	1.691	2.32	**0.47844**	**0.1879**
Pepper	2.01	2.27	**0.4982**	**0.2052**
Barbara	1.64	2.33	**0.5168**	**0.2058**
Cameraman	1.76	2.31	**0.4851**	**0.1834**

Table 4.7: Évaluation comparative du temps d'exécution des 2 opérations

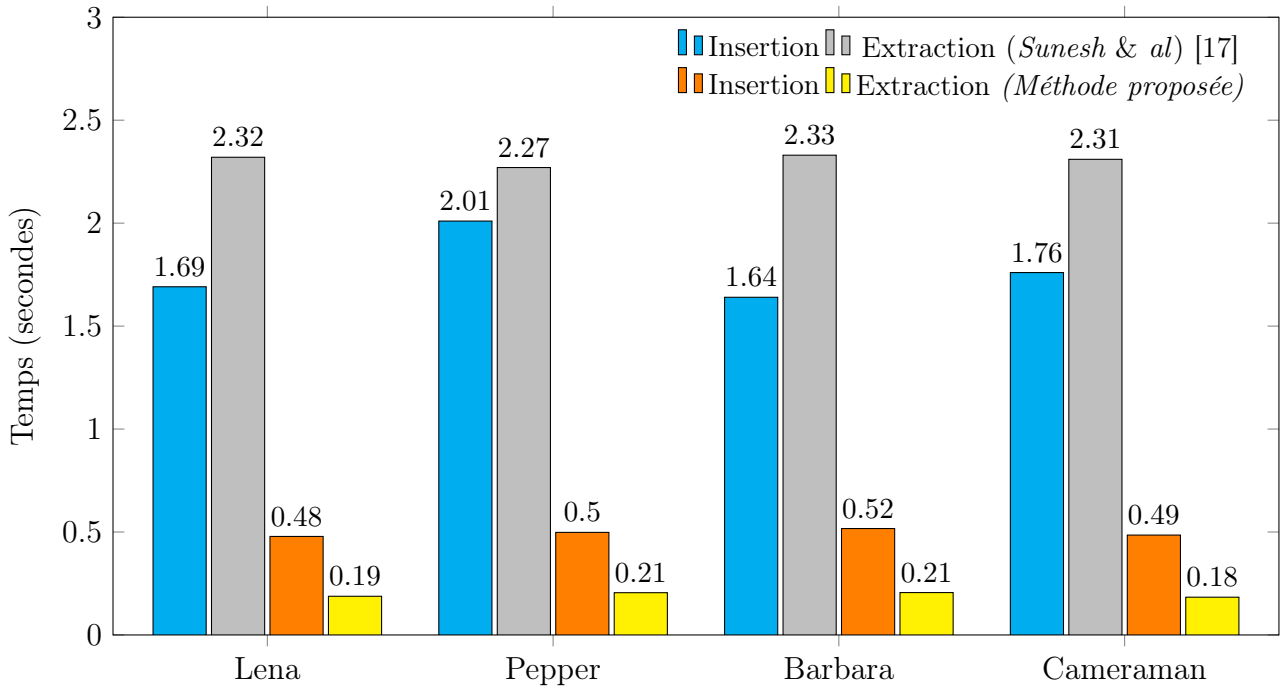


Figure 4.4: Évaluation comparative du temps d'exécution des 2 opérations

D'après le tableau 4.4 ci-dessus, la valeur du **PNSR** est très bonne (PSNR $>$ 47 dB) preuve que la solution proposée présente une haute imperceptibilité c'est-à-dire que la marque est imperceptible à l'oeil nu.

D'après le tableau 4.5 ci-dessus, la valeur du **NC** est de **1** au niveau du processus d'insertion de la marque dans l'image. Ce qui prouve une ressemblance entre l'image originale et l'image tatouée.

D'après le tableau 4.6 ci-dessus, la valeur du ***NC*** au niveau de l'attaque **l'histogramme d'égalisation** est satisfaisante ($NC \geq 0{,}94$), preuve que la marque extraire ne présente pas une dégradation trop importante. Ce qui correspond à un bon critère de robustesse.

D'après le tableau 4.3 ci-dessus, la solution proposée est également robuste face à d'autres attaques dites singulières (Filtre laplacien, Filtre wiener, Salt & pepper) au vue de la valeur du NC (NC $\geq 0{,}79$). Preuve que la solution proposée présente un critère de robustesse acceptable.

D'après le tableau 4.7 ci-dessus, la méthode proposée fournit **un temps d'exécution** meilleure que Sunesh [17] au niveau des deux opérations (insertion et extraction). Ce qui prouve que la solution proposée fournit un très bon temps d'exécution des deux (02) opérations.

De l'analyse ci-dessus, il ressort que l'algorithme de tatouage proposé est efficace en termes d'imperceptibilité, de robustesse, de sécurité, une bonne capacité et aussi présente une complexité acceptable au vu des résultats présentés au tableau 4.3 de l'analyse expérimentale. Ces résultats montrent que la méthode est adaptée aux applications nécessitant à la fois sécurité et fidélité visuelle, comme l'imagerie médicale, les archives numériques ou la protection des droits d'auteur.

♣ CONCLUSION ♣

Dans ce travail, il a été question de sécuriser la marque dans les images numériques à travers une approche combinée de tatouage numérique robuste et de cryptographie asymétrique. L'objectif visé était d'assurer la protection du contenu numérique (marque) dans les images numériques. L'approche proposée s'articule autour d'un double enjeu : d'une part préserver la qualité visuelle de l'image hôte après l'insertion de la marque, et d'autre part permettre une extraction fiable de cette dernière tout en évaluant sa dégradation éventuelle.

Après avoir posé les fondements théoriques relatifs au tatouage numérique et analysé des travaux existants, le modèle élaboré a été structuré en deux phases principales : l'insertion et l'extraction de la marque. Lors de l'insertion, la marque W a préalablement été chiffrée à l'aide de l'algorithme RSA avec une clé privée K_s, puis insérée dans les coefficients de fréquence moyenne de l'image via la Transformée en Cosinus Discrète (TCD), générant ainsi l'image tatouée $I_{W'}$. L'extraction quant à elle consiste à retrouver la marque M à partir de l'image potentiellement attaquée $I^*_{W'}$, avant de la déchiffrer à l'aide de la clé publique K_p. L'approche a été pensée pour maximiser à la fois l'imperceptibilité et la robustesse.

Les expérimentations menées sur un jeu d'images standard ont démontré des performances prometteuses. Les mesures d'imperceptibilité ont révélé des valeurs du **PSNR** très satisfaisantes (PSNR $>$ 47 dB) et des valeurs du **SSIM** excellentes ($0.99 \leq$ SSIM ≤ 1), traduisant une altération visuelle négligeable. Par ailleurs, les valeurs du **NC** obtenues après insertion et après attaques attestent à la fois de la fidélité de la reconstruction et de la robustesse du procédé. La simplicité d'implémentation et aussi la très bonne capacité de stockage en font des atouts majeurs dans le contexte de la protection des contenus visuels sensibles.

Bien qu'ayant obtenu des résultats satisfaisants, ce travail pourrait être amélioré en intégrant les mécanismes d'auto-synchronisation pour améliorer la robustesse aux transformations géométriques complexes. L'exploitation des techniques d'apprentissage profond pour optimiser dynamiquement la position et la puissance du marquage pourrait également constituer une piste prometteuse. Enfin, la prise en compte des images couleurs doit aussi être explorée car les images couleurs constituent un enjeu majeur dans les applications réelles.

♣ Bibliography ♣

[1] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 9, pp. 165–175, 2013.

[2] N. E.-H. Golea, "Tatouage numérique des images couleurs rgb." Ph.D. dissertation, Université de Batna 2, 2010.

[3] K. Loukhaoukha, "Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective," 2010.

[4] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," Information, vol. 11, no. 2, p. 110, 2020.

[5] B. Michel, Le Marquage et la Propriété Intellectuelle, 2003.

[6] F. Y. Shih, Digital watermarking and steganography: fundamentals and techniques. CRC press, 2017.

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

[8] https://www.proarchives-systemes.fr.

[9] A. Dahmani, "Contribution au developpement d'une technique de watermarking pour images," Ph.D. dissertation, Université de Batna 2, 2014.

[10] A. K. Singh, B. Kumar, M. Dave, S. P. Ghrera, and A. Mohan, "Digital image watermarking: techniques and emerging applications," Handbook of research on modern cryptographic solutions for computer and cyber security, pp. 246–272, 2016.

[11] P. Kadian, S. M. Arora, and N. Arora, "Robust digital watermarking techniques for copyright protection of digital data: A survey," Wireless Personal Communications, vol. 118, pp. 3225–3249, 2021.

[12] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Advances in Cryptology: Proceedings of Crypto 83. Springer, 1984, pp. 51–67.

[13] J. Nin and S. Ricciardi, "Digital watermarking techniques and security issues in the information and communication society," in 2013 27th International Conference on Advanced Information Networking and Applications Workshops. IEEE, 2013, pp. 1553–1558.

[14] A. H. Allaf and M. A. Kbir, "A review of digital watermarking applications for medical image exchange security," in The proceedings of the third international conference on smart city applications. Springer, 2018, pp. 472–480.

[15] A. Dixit and R. Dixit, "A review on digital image watermarking techniques," International Journal of Image, Graphics and Signal Processing, vol. 9, no. 4, p. 56, 2017.

[16] R. Riad, "Tatouage robuste d'images imprimées," Ph.D. dissertation, Université d'Orléans; Université Ibn Zohr (Agadir), 2015.

[17] R. R. Kishore et al., "A novel and efficient blind image watermarking in transform domain," Procedia Computer Science, vol. 167, pp. 1505–1514, 2022.

[18] V. P. Vishwakarma and V. Sisaudia, "Gray-scale image watermarking based on de-kelm in dct domain," Procedia computer science, vol. 132, pp. 1012–1020, 2020.

[19] S. A. Parah, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Robust and blind watermarking technique in dct domain using inter-block coefficient differencing," Digital Signal Processing, vol. 53, pp. 11–24, 2018.

[20] G. V. M. Alchin, J. Kaplan-Moss, "Pro django," Springer, vol. 2, 2013.

♣ ANNEXE ♣

4.2 Algorithme d'insertion

Nous allons présenter de manière plus détaillée l'algorithme d'insertion.

Algorithm 4 Insertion de la marque

Input: Image I , marque W, clé privée K_s , facteur de qualité Q, $size$
Output: Image tatouée $I_{W'}$
$W' \leftarrow RSA(W, K_s)$
Initialiser sig_size à la taille de la signature
Récupérer la largeur l et la hauteur h de I
Définir les positions d'insertion $embed\_pos$
if $l > 2 \times sig\_size \times size$ **then**
    Ajouter $(l - sig\_size \times size, 0)$ à $embed\_pos$
end if
if $h > 2 \times sig\_size \times size$ **then**
    Ajouter $(0, h - sig\_size \times size)$ à $embed\_pos$
end if
if taille de $embed\_pos = 3$ **then**
    Ajouter $(l - sig\_size \times size, h - sig\_size \times size)$ à $embed\_pos$
end if
for chaque (x, y) dans $embed\_pos$ **do**
  for $i = x$ à $x + sig\_size \times size$ avec un pas de $size$ **do**
    for $j = y$ à $y + sig\_size \times size$ avec un pas de $size$ **do**
      Récupérer un bloc $B = I[i : i + size, j : j + size]$
      Insérer la marque dans les fréquences moyennes avec $B[size - 1, size - 1] = Q \cdot W$
      Appliquer la DCT inverse à B
      Régler B pour s'assurer que les valeurs soient entre 0 et 255
      Mettre à jour le bloc $I[i : i + size, j : j + size]$ avec B
    end for
  end for
end for
Générer $I_{W'}$ =0

4.3 Algorithme d'extraction

Nous allons présenter de manière plus détaillée l'algorithme d'extraction.

Algorithm 5 Extraction de la marque

Input: Image tatouée attaquée $I^*_{W'}$, Clé publique K_p, Facteur de qualité Q
Output: Marque M
Initialiser $W^{'}$
$sig\_size \leftarrow 100$
$size \leftarrow$ taille du bloc DCT
$W' \leftarrow$ tableau de zéros de taille sig_size^2
for $i \leftarrow 0$ **to** $sig\_size \times size$ **step** $size$ **do**
  for $j \leftarrow 0$ **to** $sig\_size \times size$ **step** $size$ **do**
    $B \leftarrow DCT(I[i : i + size, j : j + size])$
    if $B[size - 1, size - 1] > \frac{Q}{2}$ **then**
      $W'[\left(\frac{i}{size}\right) \times sig\_size + \left(\frac{j}{size}\right)] \leftarrow 1$
    else
      $W' \leftarrow 0$
    end if
  end for
end for
Générer $W^{'}$
$M \leftarrow RSA(W', K_p)$
Générer M
return =0