



Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université Oran 1, Ahmed Ben Bella

Institut des Sciences et Techniques Appliquées

**Mémoire du projet fin d'étude pour l'obtention du diplôme de master en
instrumentation et métrologie**

Spécialité : Instrumentation et Métrologie

**Tatouage intelligent d'images pour la protection des droits
d'auteurs**

Réalise par : Bouchouk Warda

Encadré par : Trache Najia

Jury composé par :

Présidente : Dr. Iles Nadia

Examineur : Dr. Dahan Amine

Année scolaire 2025 - 2026

Remerciement

*Je remercie Dieu Tout-Puissant pour la santé et la force accordées
afin de réaliser ce travail.*

*J'exprime ma profonde gratitude à ma famille pour son soutien, ses
encouragements et sa présence constante tout au long de mon
parcours.*

*Je remercie sincèrement mon encadrante, Dr Trache Najia, pour son
encadrement, ses conseils et son accompagnement précieux.*

*J'adresse également mes remerciements à tous mes enseignants pour
leur contribution, ainsi qu'à toutes les personnes qui m'ont soutenu
moralement ou aidé de près ou de loin durant mon parcours
académique.*

Dédicace

Je dédie ce modeste travail à mes très chers parents, en reconnaissance de leur amour, de leur soutien, de leur patience et de leurs sacrifices. Que Dieu les protège et les bénisse.

À mes chers frères et sœurs, pour leur affection et leurs encouragements.

À tous mes amis, pour leur soutien et leur présence.

À toutes les personnes qui m'ont aidé, de près ou de loin.

Enfin, à tous ceux que j'aime.

Table des matières

Les figure.....	Erreur ! Signet non défini.
Les tableaux.....	7
Résumé	8
Introduction générale.....	9
Introduction	12

Chapitre 1 : Etat de l'art sur le tatouage numérique

1 Les méthodes de protection des copyrights	12
1.1 Cryptographie.....	12
1.2 Stéganographie	13
1.3 Tatouage numérique	14
2 Historique.....	14
3 Concept général du tatouage d'images :	15
3.1 Le processus d'insertion de la marque.	15
3.2 Le processus d'extraction de la marque	16
4 Principaux défis dans un système de tatouage	16
4.1 L'imperceptibilité	17
4.2 Robustesse	17
4.3 La capacité.....	17
4.4 Sécurité de l'information secrète.....	18
4.5 La complexité	18
5 Classifications des systèmes de tatouage numérique.....	19
5.1 Types de données	19
5.2 Classification basée sur la perception visuelle	20
5.2.1 Le tatouage visible.....	20
5.2.2 Le tatouage invisible.....	20
5.3 Classification des marquages :	21
5.3.1 Le marquage faible (ou fragile)	21
5.3.2 Le marquage fort (ou robuste).....	21
5.3.3 Le marquage semi-fragile.....	21
5.4 Classification selon la méthode d'extraction.....	21
5.4.1 Algorithmes informés ou non aveugles :	22
5.4.2 Algorithmes semi-aveugle :	22
5.4.3 Algorithmes non informés ou aveugles :	22
5.5 Classification selon le domaine d'insertion.....	23

5.5.1	Le tatouage dans le domaine spatial	24
5.5.2	Le tatouage dans le domaine fréquentiel ou le domaine des transformées.....	25
5.6	Classification selon la réversibilité.....	28
5.6.1	Tatouage réversible	28
5.6.2	Le tatouage non réversible.....	28
5.7	Classification selon la technique d'insertion de l'image	28
5.7.1	Tatouage additif.....	28
5.7.2	Tatouage substitutif	29
6	Les attaque en tatouage numérique	30
7	Les métriques d'évaluation de la performance d'un système de tatouage numérique.....	32
7.1	L'erreur quadratique moyenne (MSE)	32
7.2	Le rapport signal-bruit (Peak Signal to Noise Ratio) PSNR	32
7.3	Le coefficient de normalisation (Normalization Coefficient NCC)	32
7.4	La mesure de l'indice de similarité structurelle (Structural Similarity Index Measurement (SSIM)).....	32
	Conclusion.....	33

Chapitre 2 techniques d'optimisation heuristiques et métaheuristiques pour tatouage numérique .

Introduction	35
1 Définition de l'optimisation	35
2 Techniques d'optimisation.....	35
2.1 Méthode Heuristique	35
2.1.1 Principes de fonctionnement	36
2.1.2 Avantages et inconvénients des méthodes Heuristiques :	36
2.2 Les méthodes Métaheuristiques	37
2.2.1 Principes de fonctionnement	37
2.2.2 Avantages et inconvénients des Métaheuristiques	38
3 La différence entre une heuristique et une Métaheuristique	38
4 Classification des métaheuristique et leurs algorithmes	39
4.1 Bases trajectoire :	39
4.1.1 Algorithme de recuit simulé (SA) :	39
4.1.2 Algorithme de Tabou (TS)	39
4.2 Bases population.....	40
4.2.1 Algorithme génétique (GA).....	40
4.2.2 Algorithme de colonies de fourmis (ACO)	40

4.2.3	Algorithme de Essaim Particulaire (PSO).....	41
5	Comparaison entre PSO, ACO et GA.....	43
	Conclusion.....	43

Chapitre 3: Conception et Mise en œuvre du système de tatouage d'Images

	Introduction	46
1	Outils, méthodes et critères d'évaluation.....	46
1.1	Outils logiciels.....	46
1.2	Les méthodes utiliser pour l'insertion de marque	46
1.2.1	la Transformée en Ondelettes Discrètes (DWT)	46
1.2.2	la transformation d'Arnold	47
1.2.3	L'algorithme d'optimisation (PSO).....	47
1.3	Métriques d'évaluation des performances du Tatouage numérique.	47
2	Etapas de Conception de notre projet :	48
3	Résultats et interprétations :.....	49
3.1	Evaluation des résultats :	52
	Conclusion.....	53
	Conclusion générale	54
	Références	55

Les Figure

Figure 1: Les différentes types de protection	12
Figure 2: exemple de transforme d'Arnold.....	13
Figure 3:exemple de stéganographie.....	13
Figure 4:le processus général de tatouage numérique.....	15
Figure 5:le processus d'insertion la marque	16
Figure 6:processus d'extraction	16
Figure 7:La compromis entre trois contraint.....	18
Figure 8:classification de tatouage numérique	19
Figure 9: tatouage visible	20
Figure 10: tatouage numérique invisible	21
Figure 11: Algorithme d'extraction non aveugle.....	22
Figure 12:Algorithme d'extraction semi- aveugle.....	22
Figure 13:Algorithme d'extraction aveugle.....	23
Figure 14: Classification du domaine d'insertion.....	23
Figure 15:La technique de tatouage LSB	25
Figure 16:Le principe de DWT	27
Figure 17: Principe de l'insertion de la marque par addition.	29
Figure 18: Principe de l'insertion par substitution	29
Figure 19: Classification des attaques	30
Figure 20:Technique d'optimisation.....	35
Figure 21 : Schéma générale des algorithmes heuristiques.....	36
Figure 22:schéma de principe de fonctionnement de métaheuristique	37
Figure 23:classification des métaheuristique et leurs algorithmes	39
Figure 24:principe de fonctionnement de PSO	42
Figure 25:Schéma général de projet.....	48
Figure 26: les types des images.....	49

Les Tableaux

Tableau 1:comparaison entre domaine spatial et fréquentiel	28
Tableau 2:Présent une comparaison entre les avantages et les inconvénients des méthodes heuristique	36
Tableau 3:Présent une comparaison entre les avantages et les inconvénients des méthodes Métaheuristique	38
Tableau 4:présente une Comparaison entre heuristique et métaheuristique	39
Tableau 5:Présentes les avantages et les inconvénients d'algorithme génétique GA	40
Tableau 6:Présente les avantages et les inconvénients d'algorithme de colonies de fourmis (ACO).....	41
Tableau 7:Présente les avantages et les inconvénients d'algorithme de Essaim Particulaire (PSO).....	43
Tableau 8:comparaison entre GA, ACO, PSO	43
Tableau 9 : les images tatouées et la marque extraite non attaquée et les valeurs de PSNR, SSIM et NCC	49
Tableau 10 : les images et la marque extraite après l'attaque de rotation 10° et les résultats des valeurs de NCC	50
Tableau 11 : les images et la marque extraite après l'attaque par filtre médian et les résultats des valeurs de NCC	51
Tableau 12: les images et la marque extraite après l'attaque par zoom et des valeurs de NCC	51
Tableau 13: les images et la marque extraite après l'attaque par compression et les résultats des valeurs de NCC	52

Résumé

Ce travail propose un système de tatouage numérique d'images visant la protection des droits d'auteur et de la propriété intellectuelle. La méthode repose sur la transformée en ondelettes discrète (DWT), le chiffrement par la transformation d'Arnold et l'optimisation du coefficient d'insertion α à l'aide de l'algorithme PSO, afin d'assurer un compromis optimal entre imperceptibilité et robustesse. L'approche est implémentée sous MATLAB et évaluée à l'aide de métriques objectives (PSNR, SSIM, NCC) ainsi que de tests de robustesse face à diverses attaques. Les résultats obtenus confirment l'efficacité et la fiabilité du système proposé.

Introduction générale

Le développement rapide des technologies de l'information et de la communication, ainsi que la généralisation d'Internet, ont profondément transformé notre société. Aujourd'hui, les données numériques, notamment les images, peuvent être facilement stockées, copiées et transmises à travers le monde en quelques secondes. Cette évolution a considérablement facilité le partage de l'information, mais elle a également engendré de nouveaux problèmes liés à la sécurité des données et à la protection de la propriété intellectuelle.

Face à ces défis, plusieurs techniques ont été développées afin d'assurer la confidentialité, l'authenticité et la protection des contenus numériques. Parmi ces techniques, le tatouage numérique constitue une solution efficace permettant d'intégrer des informations invisibles dans une image afin d'en attester la propriété et de lutter contre les utilisations non autorisées. Toutefois, un système de tatouage performant doit garantir à la fois une bonne qualité visuelle de l'image tatouée et une forte résistance aux différentes attaques et manipulations.

Dans ce mémoire, nous proposons une méthode de tatouage numérique d'images basée sur la transformée en ondelettes discrète (DWT), associée à la transformation d'Arnold pour le chiffrement de la marque et à l'algorithme d'optimisation par essaim particulaire (PSO) pour la détermination du coefficient d'insertion optimal. Cette approche vise à améliorer simultanément l'imperceptibilité et la robustesse du tatouage.

Ce mémoire est organisé en trois chapitres :

- **Le premier chapitre** présente un état de l'art sur le tatouage numérique. Il expose les concepts fondamentaux de cette technologie, ses principaux défis, ainsi que les principales classifications et les attaques susceptibles d'affecter les systèmes de tatouage numérique.
- **Le deuxième chapitre** est consacré aux techniques d'optimisation heuristiques et métaheuristiques appliquées au tatouage numérique. Une étude comparative des principaux algorithmes d'optimisation est réalisée, avec un intérêt particulier porté à l'algorithme d'optimisation par essaim de particules (PSO).

- **Le troisième chapitre** présente la conception et la mise en œuvre du système de tatouage numérique proposé. Les différentes étapes de l'algorithme sont décrites, puis les résultats expérimentaux sont présentés et analysés à l'aide des métriques d'évaluation, notamment le PSNR, le SSIM et le NCC. Enfin, les performances du système sont évaluées à travers plusieurs tests de robustesse face à différentes attaques afin de valider son efficacité.

Chapitre 01

Etat de l'art sur le tatouage numérique

Introduction

Le développement rapide des technologies numériques et d'internet a facilité l'échange des contenus multimédias, mais a également augmenté les risques de copie illégale, à la falsification et à la violation des droits d'auteur. Afin de protéger la propriété intellectuelle et d'assurer la sécurité des données numériques, plusieurs techniques ont été développées. Parmi les méthodes les plus efficaces figure le tatouage numérique (Watermarking), qui consiste à insérer des informations invisibles dans les contenus numériques afin de garantir leur authenticité, leur protection et le suivi de leur utilisation.

Le tatouage numérique occupe aujourd'hui une place importante dans le domaine de la sécurité multimédia grâce à ses nombreuses applications, notamment la protection des droits d'auteur, l'authentification des données et la lutte contre le piratage numérique.

Dans ce chapitre, nous présenterons les concepts fondamentaux du tatouage numérique, ses principales classifications, les différentes techniques utilisées, ainsi que les principaux défis et les attaques associés aux systèmes de tatouage numérique.

1 Les méthodes de protection des copyrights

Il existe plusieurs méthodes permettant de protéger la propriété intellectuelle d'un média. (fig.1)

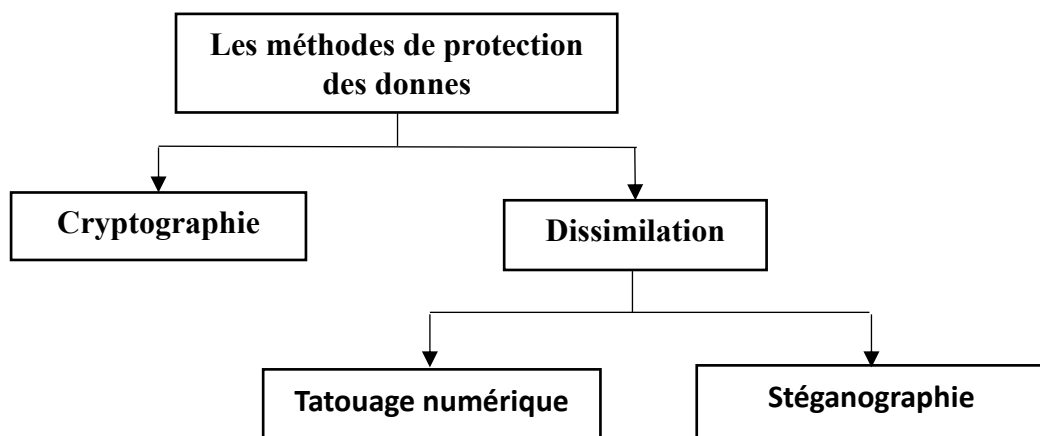


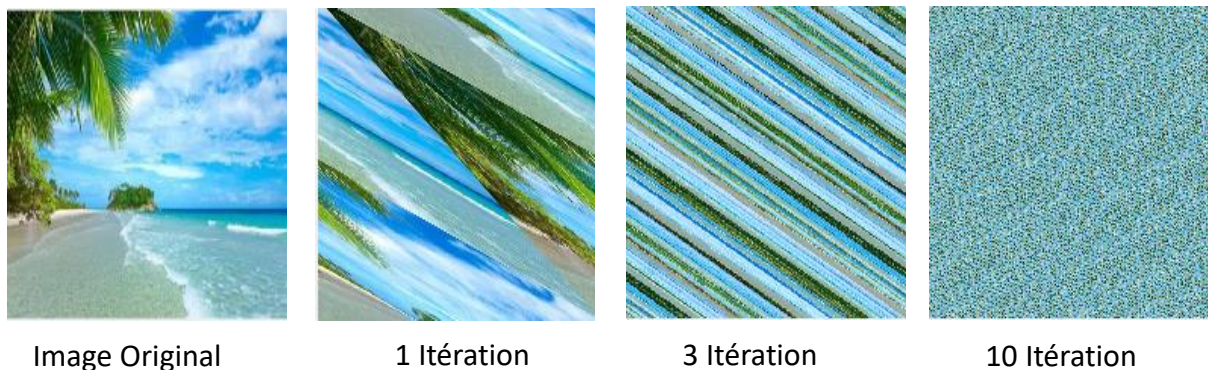
Figure 1: Les différents types de protection

1.1 Cryptographie

La cryptographie consiste à transformer les données en un format illisible à l'aide d'un algorithme et d'une clé.

Dans le domaine du traitement d'images numériques, plusieurs méthodes de chiffrement peuvent être utilisées pour renforcer la protection des informations. Parmi elles, la transformation d'Arnold est une technique particulièrement adaptée aux applications de tatouage numérique.

Le cryptage d'Arnold est une technique de permutation des pixels qui permet de brouiller une image de manière réversible afin de renforcer sa sécurité. Son principe repose sur l'application répétée d'une transformation mathématique qui réorganise les positions des pixels sans modifier leur valeur [1]



Plus le nombre K d'itération augment plus l'image devient brouillée

Figure 2: exemple de transforme d'Arnold

1.2 Stéganographie

La stéganographie vise à dissimuler des informations secrètes dans un support de communication, comme une image, une vidéo ou un fichier audio. [2]

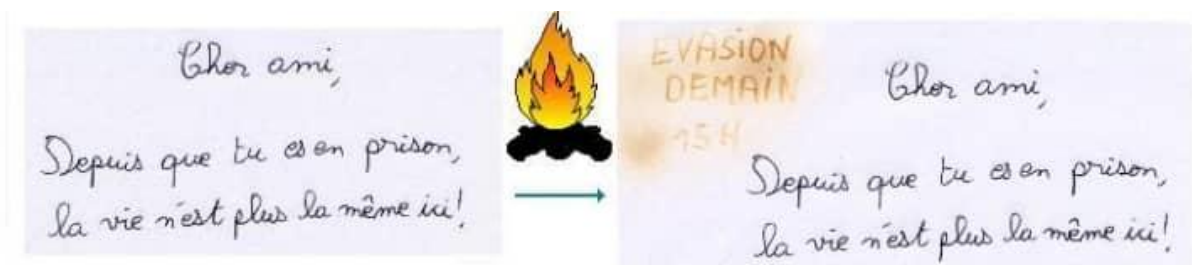


Figure 3: exemple de stéganographie

1.3 Tatouage numérique

Le tatouage numérique est une technique consistant à insérer une information appelée marque ou signature numérique dans un support numérique tel qu'une image, une vidéo, un audio ou tout autre média. Cette insertion peut être réalisée de manière visible ou invisible sans altérer significativement la qualité du contenu original. La marque intégrée doit être suffisamment résistante aux différentes attaques et traitements appliqués au média afin de pouvoir être détectée ou extraite ultérieurement pour confirmer l'authenticité et la propriété des données. Cette technologie joue un rôle important dans la protection des droits d'auteur et de la propriété intellectuelle, tout en assurant plusieurs services de sécurité tels que l'authentification, l'intégrité, le copyright et la non-répudiation [3]

- **Différence entre Stéganographie et Tatouage numérique**

Le tatouage numérique et la stéganographie sont toutes deux des techniques de dissimulation de données, mais elles diffèrent dans leur approche. La stéganographie consiste à cacher des données à l'intérieur d'autres données, le tatouage numérique, en revanche, consiste à ajouter des informations supplémentaires à un objet sans nécessairement les dissimuler. [4]

2 Historique

Le Tatouage numérique des images a émergé dans les années 1990 avec le développement des technologies numériques et de l'internet, de façon à répondre aux besoins de protection de la propriété intellectuelle (copyright) et de lutte contre la contrefaçon des contenus multimédias.

Les premières techniques de tatouage numérique visibles, consistant à insérer un logo ou une marque apparente dans l'image, ont rapidement été remplacées par des techniques de tatouage invisible, où la marque insérée est imperceptible à l'œil nu.

Dans le domaine de l'électronique, le tatouage numérique invisible a trouvé de nombreuses applications, notamment :

- La protection des circuits intégrés et puces électroniques contre la contrefaçon, en insérant des marques d'authentification dans les masques de fabrication.
- La traçabilité et l'authentification des appareils électroniques, téléphones portables, etc. en y incrustant des tatouages numériques au niveau matériel.

- La protection des contenus multimédias (images, vidéos) stockés ou transmis par des appareils électroniques contre la copie illégale.
- L'utilisation de tatouages fragiles pour détecter toute modification d'une image numérique dans des applications de stéganographie ou de cryptographie.

Au fil des années, de nombreux algorithmes de tatouage robustes ou fragiles ont été développés, exploitant différents domaines de représentation des images (Spatial, fréquentiel) et techniques d'insertion. Aujourd'hui, le tatouage numérique est devenu un outil essentiel pour assurer la traçabilité, l'authentification et la protection des contenus et produits électroniques contre les atteintes aux droits de propriété intellectuelle. [3]

3 Concept général du tatouage d'images :

Le modèle de base du schéma de tatouage numérique se compose de deux éléments processus d'insertion de la marque et processus d'extraction de la marque. [5]

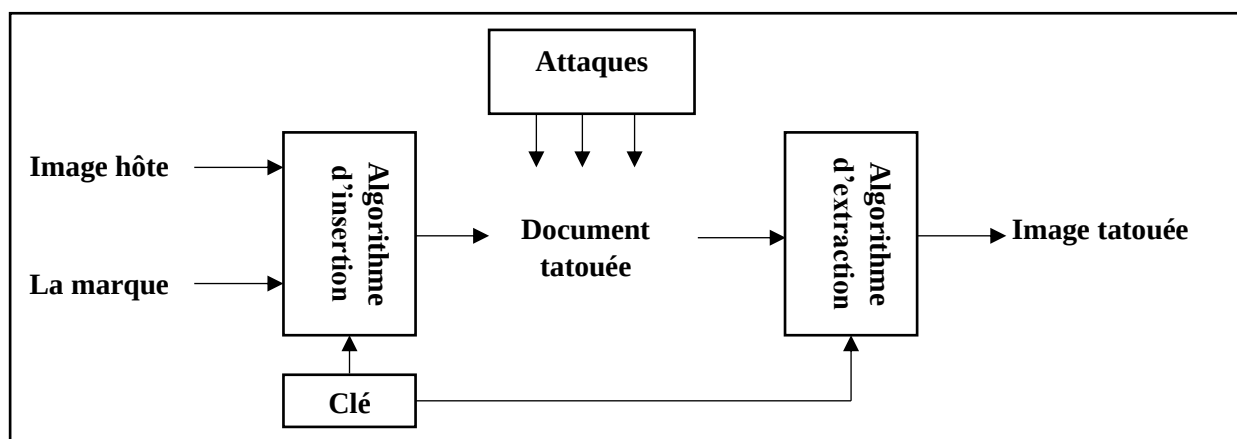


Figure 4:le processus général de tatouage numérique

3.1 Le processus d'insertion de la marque.

Dans la phase d'insertion, l'image originale (hôte) est tatouée en intégrant une marque connue uniquement par le propriétaire. Cette marque est transformée en une suite de bits puis insérée dans l'image sous forme de bruit contrôlé, dont l'effet dépend de son intensité. L'insertion peut se faire dans le domaine spatial ou fréquentiel, et peut être sécurisée par une clé secrète afin d'assurer la protection du tatouage numérique. [5]

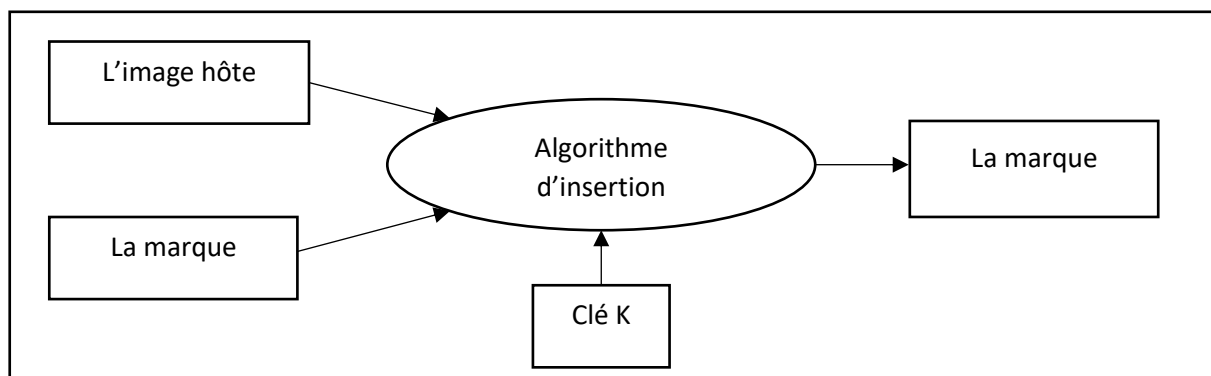


Figure 5:le processus d'insertion la marque

Une fois tatoués, les documents diffusés peuvent être soumis à des déformations quelconques. Ces déformations, qu'elles soient bienveillantes ou malveillantes, constituent des attaques sur le processus de tatouage. Dans la phase d'extraction, selon la conception de l'algorithme utilisé, les documents reçus doivent passer par deux étapes :

- L'étape de détection qui consiste à détecter la présence du marquage. Cette étape est faite à l'aide de la clé K utilisée précédemment dans la phase d'insertion. La détection peut être aveugle, semi-aveugle ou non aveugle selon qu'on utilise l'image originale ou la marque originale insérée pour la détection de la marque,
 - L'étape de décodage : dès que la présence de la marque est confirmée, cette étape prendra place. Une estimation du message caché auparavant doit être calculé et décodé correctement.
- [3]

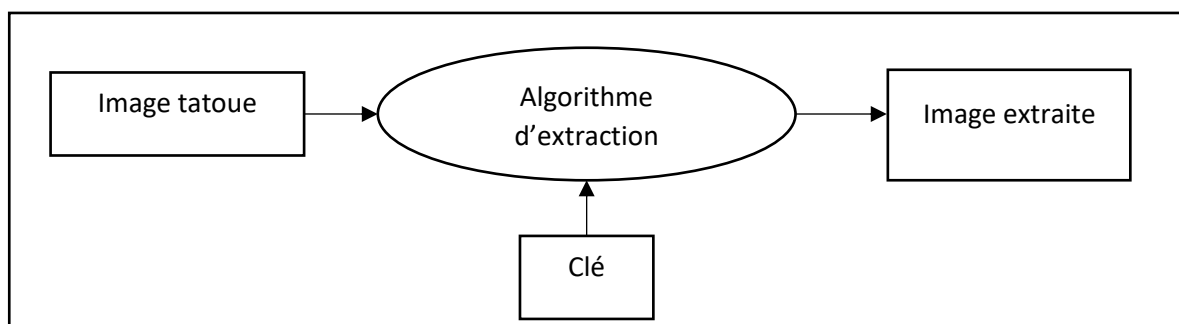


Figure 6:processus d'extraction

4 Principaux défis dans un système de tatouage

Depuis l'émergence du tatouage numérique, de nombreuses recherches ont été menées afin d'améliorer et d'optimiser les méthodes de marquage. Ces travaux portent principalement sur le renforcement des propriétés essentielles du tatouage numérique, notamment la robustesse ou la fragilité, l'invisibilité, la capacité d'insertion ainsi que la sécurité des informations secrètes.

Toutefois, l'optimisation de ces propriétés nécessite généralement un compromis, celui-ci dépendant des exigences et des domaines d'application du système de tatouage. Dans ce qui suit, ces différentes propriétés seront présentées et analysées. [6]

4.1 L'imperceptibilité

Le tatouage numérique ne doit en aucun cas altérer la qualité de l'image originale après l'insertion de la marque. Le filigrane intégré doit demeurer totalement imperceptible pour le système visuel humain (SVH). Ainsi, le processus d'insertion ne doit provoquer aucune dégradation visuelle perceptible de l'image hôte ; l'image tatouée doit conserver une apparence visuellement équivalente à celle de l'image originale. En outre, la présence d'un watermark visible risquerait non seulement de dénaturer l'image, mais également de faciliter sa détection et son élimination. [6]

4.2 Robustesse

La robustesse constitue un critère essentiel dans un système de tatouage numérique. Elle désigne la capacité de la marque insérée à résister aux différentes modifications ou attaques susceptibles d'affecter le document hôte. Ainsi, plus un schéma de tatouage est robuste, plus la probabilité d'extraire correctement la signature après des altérations est élevée. La robustesse peut donc être définie comme l'aptitude du système à détecter et récupérer le tatouage malgré les opérations de traitement ou de dégradation appliquées au contenu numérique. Par ailleurs, l'augmentation de la quantité d'informations insérées dans l'image peut améliorer la robustesse du tatouage, mais elle risque également de rendre la signature plus perceptible visuellement. [6]

4.3 La capacité

La capacité d'insertion correspond à la quantité d'informations ou de données pouvant être intégrée dans l'image hôte. Elle est généralement exprimée par le taux d'intégration de la marque numérique. Cette capacité dépend principalement du nombre de pixels ou de coefficients susceptibles d'être modifiés lors du processus d'insertion. En pratique, il est établi qu'une augmentation de la taille de la marque entraîne généralement une dégradation plus importante de la qualité de l'image, rendant ainsi le tatouage plus perceptible visuellement. [6]

4.4 Sécurité de l'information secrète

L'objectif principal du tatouage numérique est d'assurer la protection et la confidentialité des données insérées dans le document hôte. Cette sécurité dépend essentiellement du choix et de la gestion de la clé d'insertion utilisée lors du processus de tatouage. Ainsi, une technique de tatouage est considérée comme sécurisée lorsque la marque insérée ne peut être ni détectée ni extraite par une personne non autorisée, même si celle-ci possède des connaissances sur les algorithmes d'insertion et d'extraction employés. [6]

4.5 La complexité

Le coût computationnel constitue un critère essentiel dans les applications industrielles du tatouage numérique. De manière générale, le temps de calcul doit rester inférieur à un seuil acceptable afin de garantir l'efficacité du système. Par exemple, dans les applications de contrôle d'accès, la complexité de l'opération de détection revêt une importance plus importante que celle de l'insertion. Ainsi, le temps nécessaire à la détection du tatouage doit idéalement être limité à une durée comprise entre une et deux secondes. [5]

- **Compromis entre robustesse, imperceptibilité et capacité**

La robustesse, l'invisibilité et la capacité d'insertion sont des propriétés étroitement liées dans un système de tatouage numérique. L'amélioration de l'une de ces caractéristiques peut affecter les deux autres. En effet, l'augmentation de la taille de la marque peut dégrader la qualité visuelle de l'image ou réduire la fiabilité de l'extraction. Il est donc nécessaire de trouver un compromis entre ces trois propriétés afin d'assurer de bonnes performances du système de tatouage numérique. [6] [3]

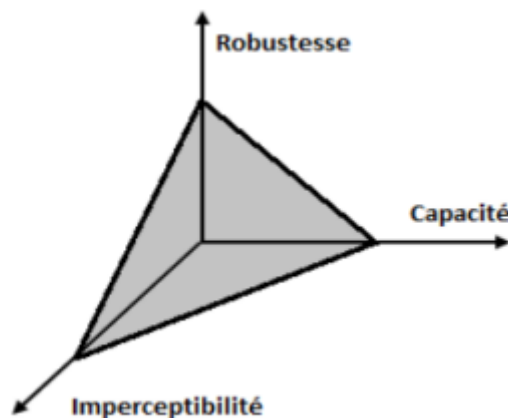


Figure 7: La compromis entre trois contrain

5 Classifications des systèmes de tatouage numérique

Les systèmes de tatouage numérique peuvent être classifiés selon plusieurs critères, comme l'illustre la figure suivante.

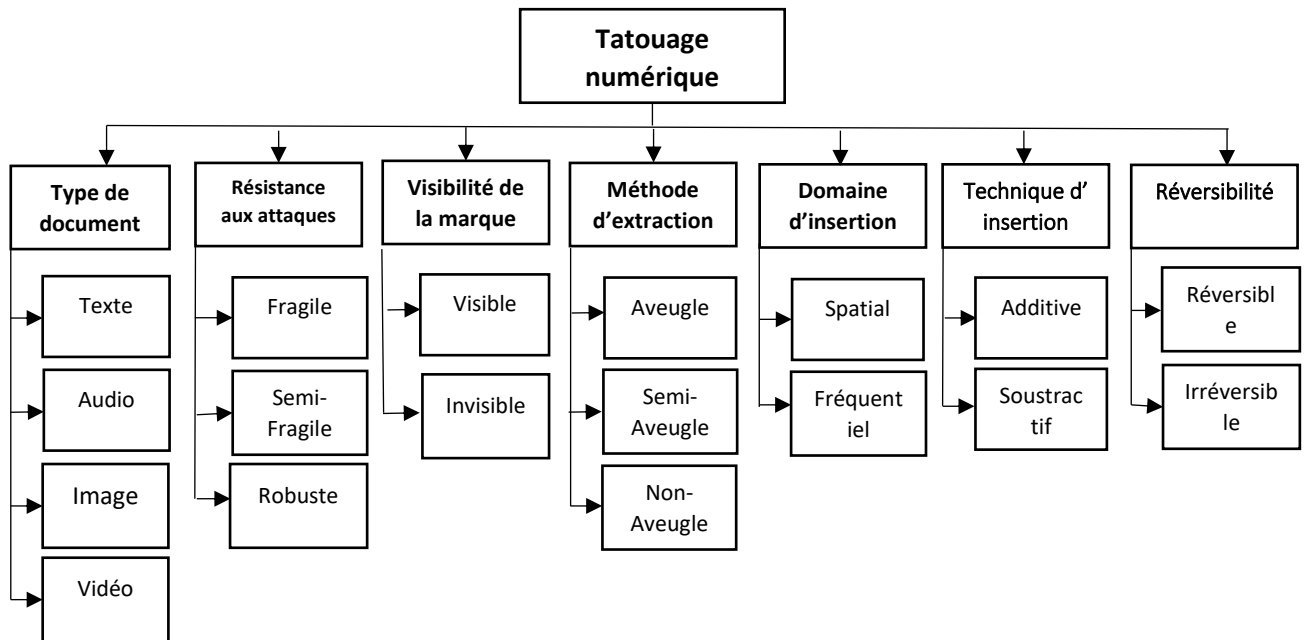


Figure 8:classification de tatouage numérique

Le tatouage numérique peut être appliqué à différents types de médias tels que l'image, l'audio et la vidéo et texte. Les techniques de tatouage sont généralement développées soit dans le domaine spatial, basé sur la modification directe des pixels, soit dans le domaine fréquentiel, utilisant différentes transformées mathématiques. Selon la perception humaine, le tatouage numérique se divise en approches visibles, invisibles. Selon la méthode d'extraction, le tatouage numérique peut être classé en tatouage aveugle, semi-aveugle et non aveugle. et leur niveau de robustesse en approches fragiles, semi-fragiles, robustes. Les principales classifications des approches de tatouage numérique seront présentées dans les sous-sections suivantes [6] :

5.1 Types de données

Les données numériques peuvent être de type texte, image, audio ou vidéo, Le tatouage numérique consiste à insérer une marque dans ces différents media afin d'assurer la protection du contenu contre la copie non autorisée, la transmission illégale ou toute forme de manipulation des données. [6] [7]

5.2 Classification basée sur la perception visuelle

En se basant sur la propriété de perception visuelle humaine, les approches de tatouage numérique sont classées en deux catégories : les approches visibles, invisibles

5.2.1 Le tatouage visible

Le tatouage visible consiste à insérer une marque perceptible à l'œil humain dans le support numérique original, tel qu'une image et les vidéo Cette technique est principalement utilisée pour indiquer la propriété, protéger les droits d'auteur et assurer l'authentification des données multimédias. Généralement, la marque insérée prend la forme d'un logo, d'un symbole ou d'une signature visible directement sur le contenu. [6] [7]

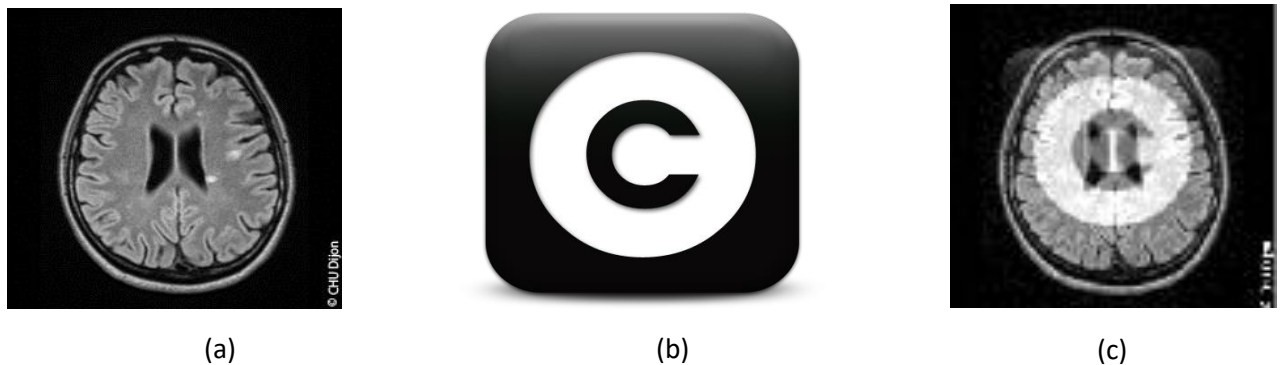
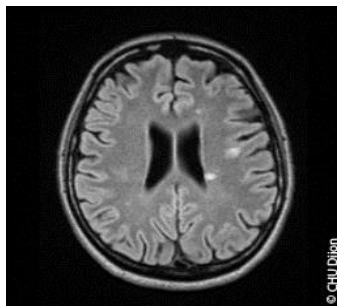


Figure 9: tatouage visible
(a) Image hôte, (b) Marque, (c) Image marquée

5.2.2 Le tatouage invisible

Le tatouage invisible consiste à insérer une marque numérique dans les données originales de manière imperceptible à l'œil humain, sans dégrader la qualité du support. [6] [7]



(a)



(b)



(c)

Figure 10: tatouage numérique invisible

(a) Image hôte , (b) Marque, (c) Image marquée

5.3 Classification des marquages :

5.3.1 Le marquage faible (ou fragile)

Dans ce cas particulier, le tatouage est destiné à avoir une très grande imperceptibilité et une faible robustesse. Ainsi, la marque ne supportera quasiment aucun traitement. Ce type de marquage servira à certifier ou non l'intégrité de l'image. [8]

5.3.2 Le marquage fort (ou robuste)

Il s'agit de la forme la plus commune de tatouage numérique. Elle est, en général, imperceptible et surtout très robuste. Le cas limite de ce type de marquage est un marquage visible, comme un logo, mais avec une robustesse à toute épreuve (le Vatican a utilisé ce type de marquage pour ses documents [8])

5.3.3 Le marquage semi-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. Les tatouages semi-fragiles doivent résister à une compression JPEG avec un haut niveau de qualité et à quelques attaques. Leurs applications sont surtout réservées à l'authentification d'images. [8]

5.4 Classification selon la méthode d'extraction

Les schémas de tatouages peuvent être classés en trois catégories Selon les éléments nécessaires pour l'extraction de la marque

5.4.1 Algorithmes informés ou non aveugles :

Dans ce type on utilise l'image originale lors de l'extraction de la marque. [8]

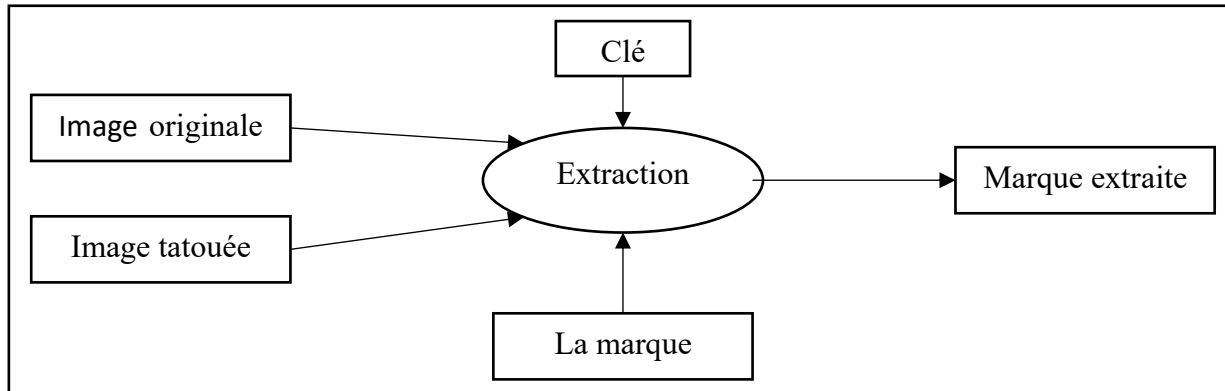


Figure 11: Algorithme d'extraction non aveugle

5.4.2 Algorithmes semi-aveugle :

Dans ce type on n'utilise pas l'image originale, mais on se sert uniquement de la marque et dans le cas échéant d'une clé qui a été utilisée lors de la phase d'insertion [8]

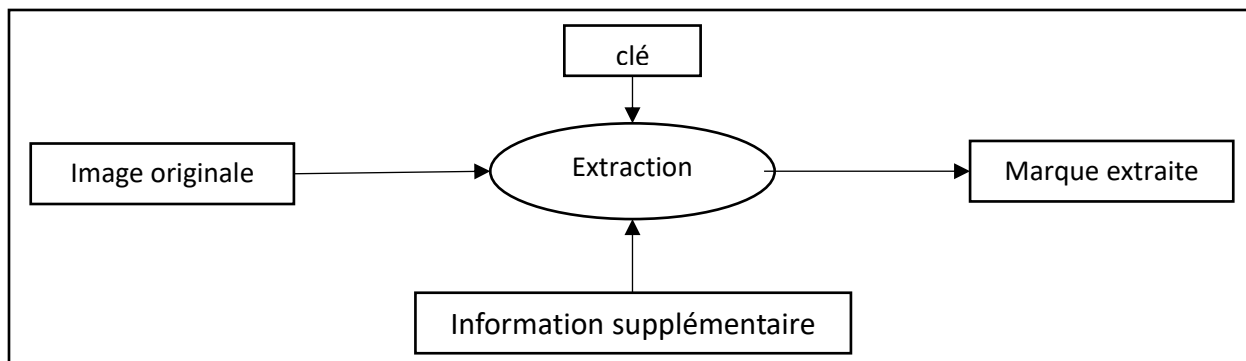


Figure 12: Algorithme d'extraction semi- aveugle

5.4.3 Algorithmes non informés ou aveugles :

Les algorithmes qui n'utilisent pas l'image originale. [8]

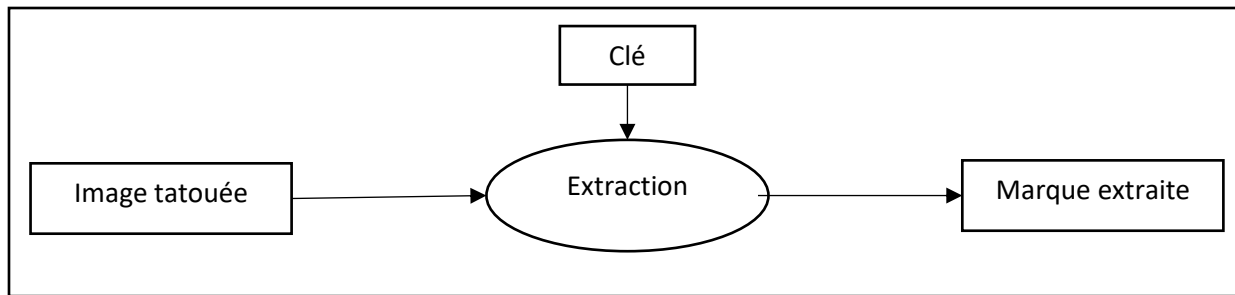


Figure 13: Algorithme d'extraction aveugle

5.5 Classification selon le domaine d'insertion

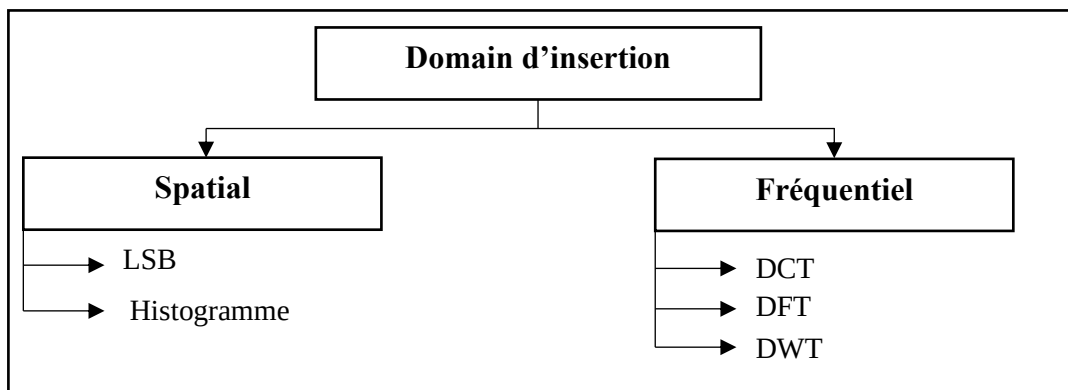


Figure 14: Classification du domaine d'insertion

Le domaine d'insertion est défini comme étant la représentation numérique de l'image. Il existe deux types de représentations : le domaine spatial et le domaine fréquentiel.

Dans une première approche, l'image numérique a été représentée comme une fonction $I(x, y)$ définie sur une matrice de pixels $M(x, y)$, $x = 1, \dots, n$; $y = 1, \dots, m$ et prenant des valeurs dans un ensemble de type $\{0, 2^1, 2^2, \dots, 2^n\}$ de niveaux de gris pour l'image noir et blanc ou dans un ensemble de type $M(x, y) \times \{1 \text{ 0 espace RGB}\}$ pour l'image en couleur. Cette représentation est appelée domaine spatial. Le domaine fréquentiel correspond à une représentation transformée de l'image obtenue à partir de la fonction $(I(x, y))$ grâce à différentes transformations mathématiques. Parmi les plus utilisées figurent la transformée en cosinus discrète (DCT), la transformée de Fourier rapide (DFT) ainsi la transformée discrète en ondelettes (DWT).

Selon le domaine d'insertion utilisé, les techniques de tatouage numérique sont généralement classées en deux grandes catégories : les techniques de tatouage dans le domaine spatial et celles dans le domaine fréquentiel. [3] [6] [7]

5.5.1 Le tatouage dans le domaine spatial

Dans le domaine spatial, une image est représentée par une fonction ($I(x,y)$) définie sur une matrice de pixels ($M(x,y)$), où chaque pixel correspond à un niveau de gris ou à une valeur de couleur. Les techniques de tatouage spatial consistent à insérer la marque directement dans l'image originale en modifiant les valeurs des pixels.

Ces méthodes se distinguent par leur simplicité de mise en œuvre, leur rapidité d'exécution ainsi que leur faible coût de calcul. Elles permettent également d'insérer une même marque plusieurs fois afin de renforcer sa présence dans l'image. [3] [6] [7]

5.5.1.1 La méthode du bit le moins significatif (LSB)

Le bit de poids faible, appelé Least Significant Bit (LSB), correspond au bit ayant la plus petite valeur dans une représentation binaire, généralement situé à droite. La technique de substitution LSB consiste à modifier les bits les moins significatifs des pixels de l'image porteuse afin d'y insérer un message secret. Cette méthode représente une approche simple et largement utilisée dans le tatouage et la stéganographie d'images.

L'utilisation du bit LSB permet de réduire les changements visuels dans l'image, car la modification d'un bit de faible poids entraîne seulement une légère variation de la valeur de couleur. Par exemple, l'insertion d'informations dans le bit le moins significatif modifie la valeur du pixel d'une unité seulement, tandis qu'une insertion dans le deuxième bit peut provoquer une variation de deux unités.

La méthode LSB dépend également du type d'image utilisé. Dans une image codée sur 8 bits, le 8^e bit de chaque octet est remplacé par les bits du message secret. Pour les images couleur de 24 bits, l'insertion s'effectue dans les composantes RVB (Rouge, Vert et Bleu), en modifiant les bits les moins significatifs de chaque composante. [8]

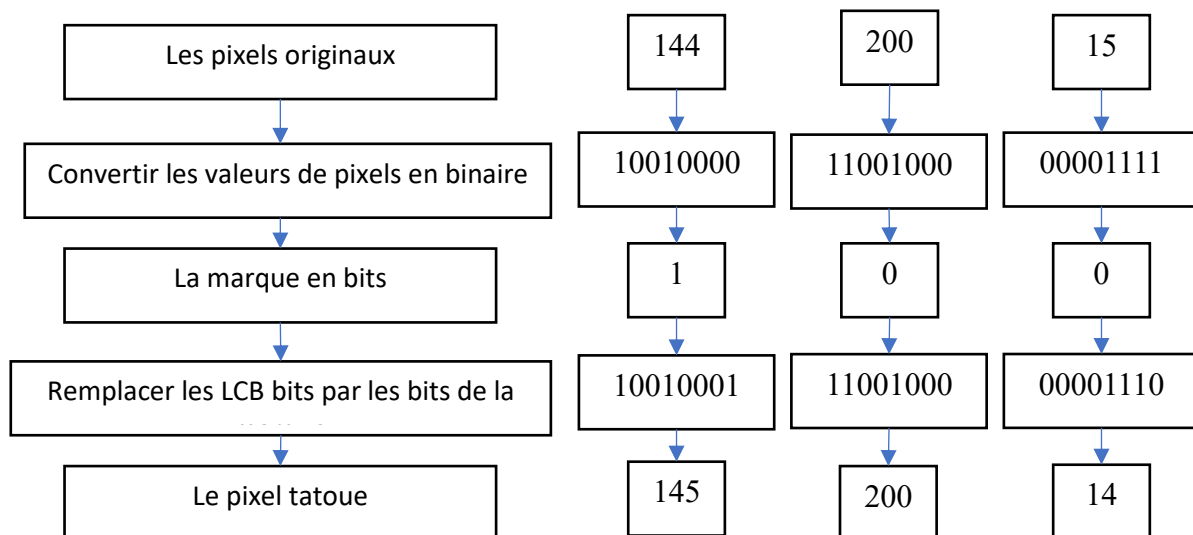


Figure 15: La technique de tatouage LSB

5.5.1.2 La technique de modification d'histogramme

Une autre méthode de tatouage appartenant au domaine spatial est la technique de modification d'histogramme. Cette approche repose sur les valeurs des pixels de l'image hôte afin de construire son histogramme, puis exploite la redondance des informations statistiques de l'image pour dissimuler les données secrètes.

Le principe consiste à insérer la marque en déplaçant le pic maximal de l'histogramme ainsi que les valeurs nulles, ou les valeurs minimales lorsqu'aucun zéro n'est présent. Cette technique est relativement simple à mettre en œuvre et nécessite peu de calculs. Toutefois, sa capacité d'insertion reste limitée par le nombre de points correspondant au maximum de l'histogramme. [8]

5.5.2 Le tatouage dans le domaine fréquentiel ou le domaine des transformées

Les techniques de tatouage numérique dans le domaine fréquentiel reposent sur l'utilisation d'algorithmes qui insèrent la marque dans les coefficients transformés de l'image, plutôt que directement dans les pixels de l'image ($I(x,y)$). Dans cette approche, l'image est d'abord décomposée à l'aide de différentes transformées mathématiques telles que la transformée en cosinus discrète (DCT), la transformée discrète en ondelettes (DWT), la transformée de Fourier discrète (DFT).

Le tatouage est ensuite intégré dans certains coefficients issus de ces transformées, ce qui permet d'améliorer la robustesse du watermark. Les méthodes fréquentielles offrent généralement une meilleure résistance à la compression, au bruit et aux différentes attaques géométriques par rapport aux méthodes spatiales. [3] [6] [7]

5.5.2.1 La transformée en cosinus discrète (DCT)

La DCT est une transformée fort semblable à la FFT, travaillant sur un signal discret. Elle prend un ensemble de points d'un domaine spatial et les transforme en une représentation équivalente dans le domaine fréquentiel. La propriété de la DCT est de regrouper l'énergie de l'image dans un petit nombre de coefficients de basse fréquence. Cela se traduit par une concentration de la plupart des informations importantes dans les premiers coefficients situés en haut à gauche de la matrice DCT alors que les coefficients de haute fréquence, contenant principalement du bruit ou des détails fins sont situés en bas à droite. [3] [6] [7]

5.5.2.2 Transformée de Fourier discrète DFT (Discret Fourier Transform)

Les chercheurs ont proposé une approche de tatouage numérique basée sur la phase de la DFT. Dans cette méthode, les auteurs privilégient la phase du spectre, car l'insertion de la marque dans les composantes les plus significatives de l'image permet d'améliorer la robustesse du système. En effet, toute attaque affectant la phase spectrale entraîne généralement une dégradation importante de la qualité visuelle de l'image.

Par ailleurs, selon les principes de la théorie des communications, la modulation de phase offre une meilleure résistance au bruit comparativement à la modulation d'amplitude. Néanmoins, plusieurs méthodes de tatouage numérique reposent encore sur la modulation d'amplitude dans le domaine de la DFT. De plus, l'invariance du spectre de Fourier face aux translations et aux décalages a conduit certains chercheurs à intégrer le tatouage au niveau de l'amplitude spectrale [3] [6] [7]

5.5.2.3 La transformée en ondelette discrète (DWT)

La DWT (Transformée en ondelettes discrète) est une description multi-résolution qui consiste à décomposer le signal en plusieurs bandes de fréquences (basse-fréquence et haute-

fréquence). Cette décomposition est réalisée en appliquant des filtres passe bas et passe haut sur les lignes et les colonnes de l'image.

- **LL** : obtenue par filtrage passe-bas sur les lignes et les colonnes, représentant l'image d'approximation.
- **HL** : obtenue par filtrage passe-bas sur les lignes et passe-haut sur les colonnes, représentant les détails verticaux.
- **LH** : obtenue par filtrage passe-haut sur les lignes et passe-bas sur les colonnes, représentant les détails horizontaux.
- **HH** : obtenue par filtrage passe-haut sur les lignes et les colonnes, représentant les détails diagonaux.

Le premier niveau de décomposition donne quatre sous bandes. La décomposition à un niveau supérieur se fait en répétant la même opération sur l'image d'approximation. Pour reconstruire le signal, il suffit de rassembler ces diverses sous-bandes. [3] [6] [7]

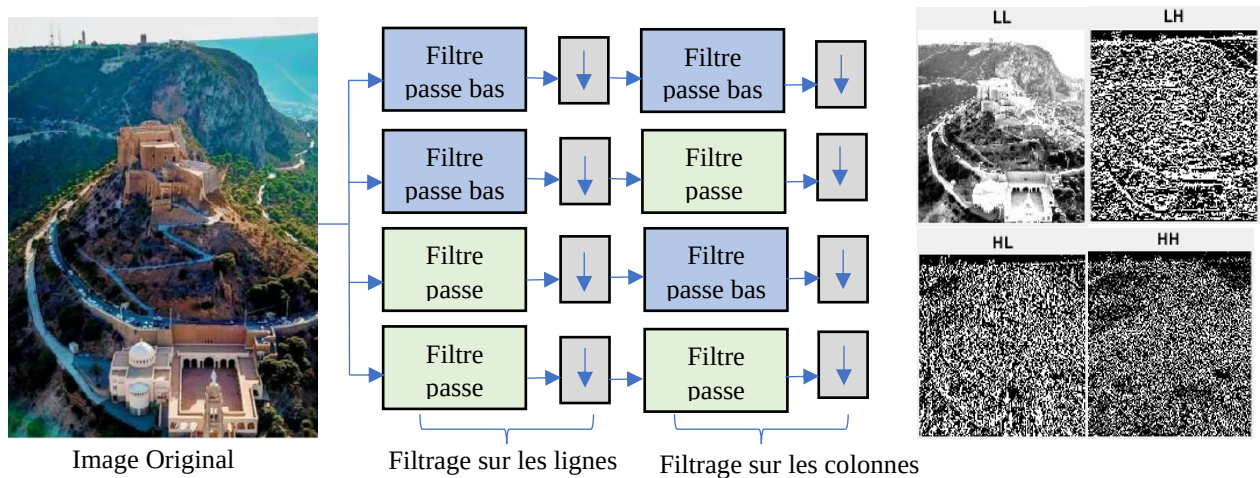


Figure 16:Le principe de DWT

• Comparaison entre le domaine spatial et le domaine fréquentiel

Les techniques de tatouage dans le domaine spatial insèrent la marque directement dans les pixels de l'image, ce qui les rend simples, rapides et faciles à contrôler en termes d'imperceptibilité. Cependant, elles sont moins robustes face aux attaques et aux traitements de l'image.

En revanche, les techniques du domaine fréquentiel insèrent la marque dans les coefficients transformés de l'image (DCT, DWT, FFT), offrant ainsi une meilleure robustesse et une plus grande capacité d'insertion. Toutefois, elles sont plus complexes et nécessitent un temps d'exécution plus élevé. [6]

	Domaine spatial	Domaine fréquentiel
Technique d'insertion	Directement dans les pixels de l'image	Dans les coefficients des transformées
Robustesse	Faible	Elevée
Imperceptibilité	Elevée et contrôlable	Faible et contrôlable
Capacité	Faible	Elevée
Complexité	Faible	Elevée
Temps d'exécution	Faible	Elevée

Tableau 1: comparaison entre domaine spatial et fréquentiel

Étant donné que le domaine fréquentiel offre de très bonnes performances, nous avons choisi d'utiliser, dans notre projet, la transformée en ondelettes discrètes DWT (Discrete Wavelet Transform).

5.6 Classification selon la réversibilité

5.6.1 Tatouage réversible

Dans ce type de tatouage, la marque peut être complètement supprimée de l'image tatouée, et donc la possibilité d'une reconstruction parfaite de l'image originale. Cependant, le prix d'une telle réversibilité implique une perte de robustesse, de sécurité et l'imperceptibilité du système. [6]

5.6.2 Le tatouage non réversible

Il introduit généralement une dégradation légère mais qui est une dégradation définitive de la qualité du signal d'origine [6]

5.7 Classification selon la technique d'insertion de l'image

5.7.1 Tatouage additif

Le schéma additif consiste à ajouter la marque ou la signature W à l'image hôte I selon l'équation (1). Le paramètre α représente le coefficient d'insertion (ou force d'insertion) de la marque. Le choix de ce coefficient est le but de notre étude. [6]

$$Im = I + kW \quad (1)$$

La marque est générée à l'aide d'une clé k de façon pseudo aléatoire et est directement insérée dans l'image originale. (fig 15)

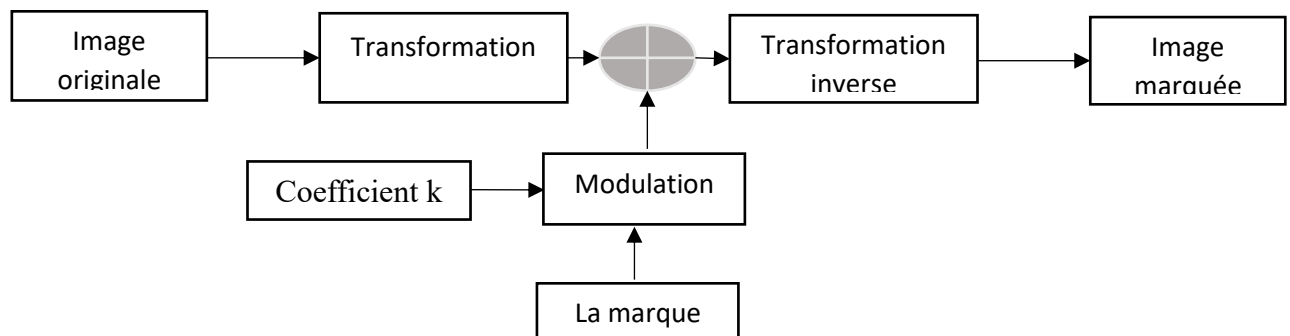


Figure 17: Principe de l'insertion de la marque par addition.

5.7.2 Tatouage substitutif

La marque n'est pas ajoutée mais substituée à des composants de l'image (pixel, coefficient de transformés) sélectionnés à l'aide d'une clé secrète.

La signature est insérée selon des contraintes appliquées sur les composants de l'image. Dans la phase d'extraction, on calcule le degré de similitude entre la marque retrouvée à partir des composants de l'image tatouée et la marque originale. Le processus d'insertion et de l'extraction du schéma substitutif sont présentés sur les figures suivantes [6] :

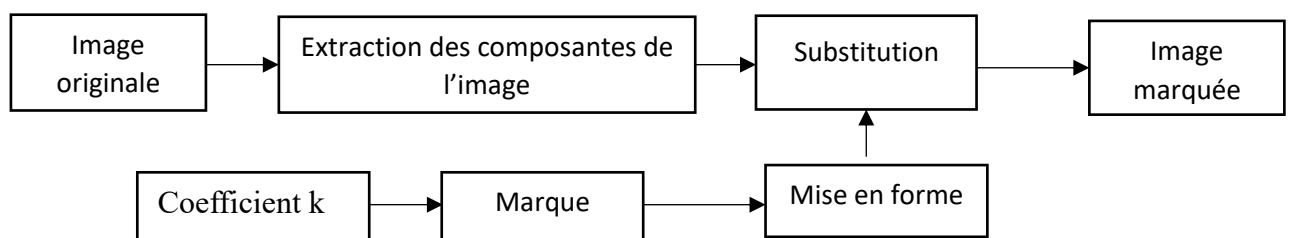


Figure 18: Principe de l'insertion par substitution

6 Les attaque en tatouage numérique

Une attaque, en informatique et en cyber-sécurité, se réfère à toute action intentionnelle menée par un individu ou un groupe pour compromettre la confidentialité, l'intégrité, ou la disponibilité d'un système d'information ou de ses données. [3] [8] [6]

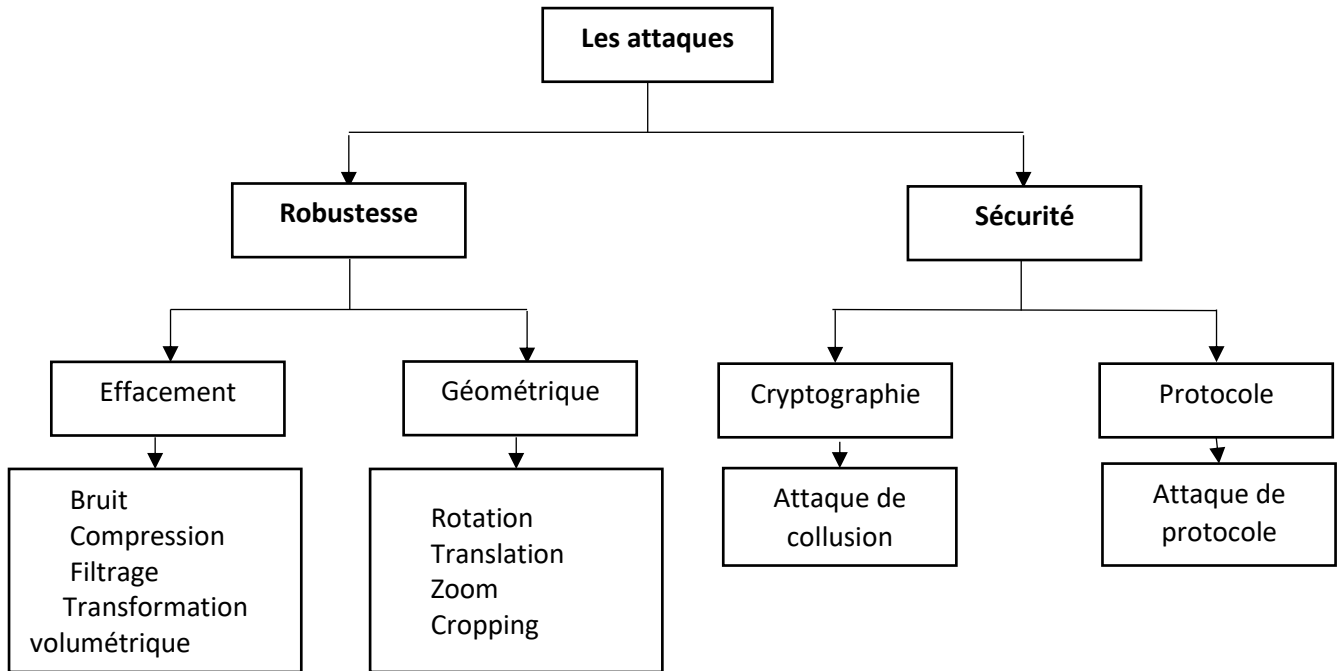


Figure 19: Classification des attaques

La figure (19) présente les principales catégories d'attaques pouvant affecter un système de tatouage numérique. Ces attaques ont pour objectif de dégrader, modifier ou supprimer la marque insérée dans le contenu numérique afin d'empêcher son extraction ou son identification. Les différentes catégories d'attaques ainsi que leurs caractéristiques seront présentées et expliquées dans les points suivants.

6.1 Les attaques de robustesse

Les attaques de robustesse ont pour objectif de dégrader ou supprimer la marque numérique tout en conservant une qualité acceptable du contenu multimédia. Elles cherchent principalement à empêcher la détection ou l'extraction correcte du tatouage numérique. [8]

6.1.1 Les attaques d'effacement

Ces attaques modifient directement les caractéristiques du signal afin d'affaiblir ou supprimer la marque insérée. Parmi les principales attaques d'effacement, on trouve [8]:

- **Le bruit** : ajout de perturbations aléatoires dans l'image afin de dégrader la marque numérique.
- **La compression** : réduction de la taille du fichier, comme la compression JPEG, pouvant entraîner la perte d'une partie des informations du tatouage.
- **Le filtrage** : application de filtres pour modifier les détails de l'image et réduire l'effet de la marque numérique.
- **Les transformations volumétriques** : modifications globales de l'intensité ou des caractéristiques du contenu multimédia.

6.1.2 Les attaques géométriques

Les attaques géométriques modifient la structure spatiale de l'image afin de perturber la localisation et la détection du tatouage numérique. Elles comprennent [5] [6]:

- **La rotation** : changement de l'orientation de l'image.
- **La translation** : déplacement de l'image horizontalement ou verticalement.
- **Le zoom** : agrandissement ou réduction de la taille de l'image.
- **Le coping** : Il consiste à supprimer ou couper une partie de l'image.

6.2 Les attaques de sécurité

Les attaques de sécurité ciblent directement le mécanisme de protection utilisé dans le système de tatouage numérique [8] [6].

6.2.1 Les attaques de cryptographie

Ces attaques exploitent les faiblesses des méthodes de sécurité utilisées pour protéger la marque numérique. Parmi elles [8] [6]:

- **L'attaque de collusion** : combinaison de plusieurs versions tatouées d'un même contenu afin d'estimer ou supprimer la marque numérique.

6.2.2 Les attaques de protocole

Ces attaques cherchent à contourner le fonctionnement du système de tatouage numérique en exploitant des failles dans le protocole utilisé [8] [6].

- **Attaque de protocole** : tentative de falsification ou de désactivation du mécanisme de vérification et d'authentification du tatouage numérique.

7 Les métriques d'évaluation de la performance d'un système de tatouage numérique

7.1 L'erreur quadratique moyenne (MSE)

Le MSE mesure l'erreur quadratique moyenne entre l'image x et l'image y . C'est une mesure directe de la différence de pixel entre deux images. La formule pour le MSE est :

$$MSE = \frac{1}{n} \sum_{n=1}^n (x_{ij} - y_{ij})^2 \quad 1$$

Où x_{ij} , y_{ij} sont les pixels (coefficients) à la position i, j respectivement des images x et y .

n représente le nombre de coefficients de l'image

7.2 Le rapport signal-bruit (Peak Signal to Noise Ratio) PSNR

Le PSNR est une mesure couramment utilisée pour évaluer la qualité d'une image compressée ou autrement altérée par rapport à l'originale. Il est défini par la formule :

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad 1$$

Où $\max(x)$ représente la valeur maximale d'un pixel ou coefficient de l'image

7.3 Le coefficient de normalisation (Normalization Coefficient NCC)

Le NCC est utilisé pour mesurer la similarité entre deux images. La valeur du NCC varie entre -1 et 1. Il est défini par la formule :

$$NCC = \frac{\sum_{i,j}^{MN} (x_{ij} * y_{ij})}{\sqrt{\sum_{i,j}^{MN} (x_{ij})^2 \sum_{i,j}^{MN} (y_{ij})^2}} \quad 2$$

Où x_{ij} est le coefficient de l'image x à la position i, j

7.4 La mesure de l'indice de similarité structurelle (Structural Similarity Index Measurement (SSIM))

Le SSIM est une métrique utilisée pour évaluer la similarité entre deux images en se basant sur la perception visuelle humaine. Il mesure la qualité de l'image en analysant les informations structurelles, la luminance et le contraste. Le SSIM considère que les dégradations sont moins visibles dans les zones lumineuses ou fortement texturées de l'image. Une valeur de SSIM proche de 1 indique une forte similitude entre les deux images.

$$SSIM(I, Im) = \frac{(2\mu_I \mu_{Im} + C_1)(2\delta_{I,Im} + C_2)}{(\mu_I^2 + \mu_{Im}^2 + C_1)(\delta_I + \delta_{Im} + C_2)} \quad 3$$

Où μ_I est la moyenne de l'image original et μ_{Im} est la moyenne d'image marquée $\delta_{I,Im}$ est la covariance de I et Im et δ_I est la covariance de I δ_{Im} est la covariance de Im.

$C_1 = K_1 L$ et $C_2 = K_2 L$ sont deux variables pour stabiliser la division avec un dénominateur faible

Avec : $K_1=0.01$ et $K_2=0.03$ par défaut, $M \times N$ est la taille de l'image.

L la plage dynamique des valeurs des pixels (est généralement de $2^{\text{bits per pixel} - 1}$)

Conclusion

Dans ce chapitre, nous avons présenté les notions de base du tatouage numérique, ainsi que les principaux défis associés à cette technique. En effet, la conception d'un système de tatouage efficace nécessite de trouver un compromis entre plusieurs critères essentiels, notamment l'invisibilité de la marque et la robustesse face aux différentes attaques. Afin d'assurer ces performances, il est nécessaire d'optimiser certains paramètres du système, en particulier le coefficient d'insertion α dont le choix influence directement la qualité du tatouage.

Chapitre 2

Les techniques d'optimisation heuristiques et métaheuristiques appliquées au tatouage numérique

Introduction

Dans de nombreux problèmes scientifiques et techniques, il est souvent difficile de choisir les paramètres appropriés permettant d'obtenir les meilleurs résultats. En effet, la sélection de ces paramètres de manière aléatoire peut conduire à des performances faibles ou à des solutions non optimales. Cette difficulté devient plus importante dans les domaines complexes où plusieurs variables influencent le résultat final. Pour résoudre ce problème, les algorithmes d'optimisation ont été développés afin de rechercher automatiquement les meilleures valeurs possibles des paramètres. Ces algorithmes permettent d'améliorer la qualité des résultats tout en réduisant le temps de recherche. Leur utilisation est particulièrement importante dans le domaine du tatouage numérique (digital watermarking), où il est nécessaire de trouver un bon compromis entre la qualité de l'image et la robustesse du tatouage. Ainsi, les algorithmes d'optimisation jouent un rôle essentiel pour déterminer les paramètres optimaux et améliorer les performances des systèmes de tatouage numérique.

1 Définition de l'optimisation

L'optimisation vise à résoudre des problèmes où l'on cherche à déterminer parmi un grand nombre de solutions candidates celle qui donne le meilleur rendement. Plus précisément, on cherche à trouver une solution satisfaisant un ensemble de contraintes qui minimise ou maximise une fonction donnée. L'application de l'optimisation est en expansion croissante et se retrouve dans plusieurs domaines. [9]

2 Techniques d'optimisation

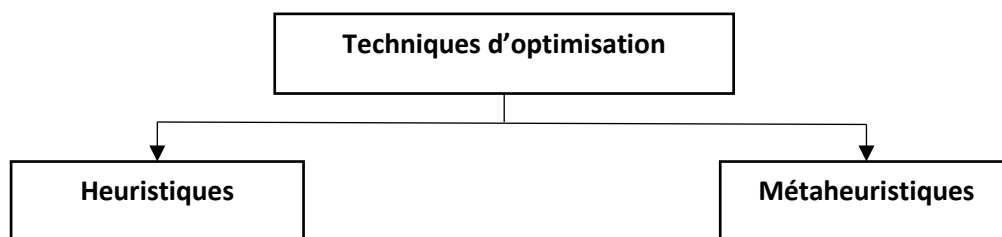


Figure 20: Technique d'optimisation

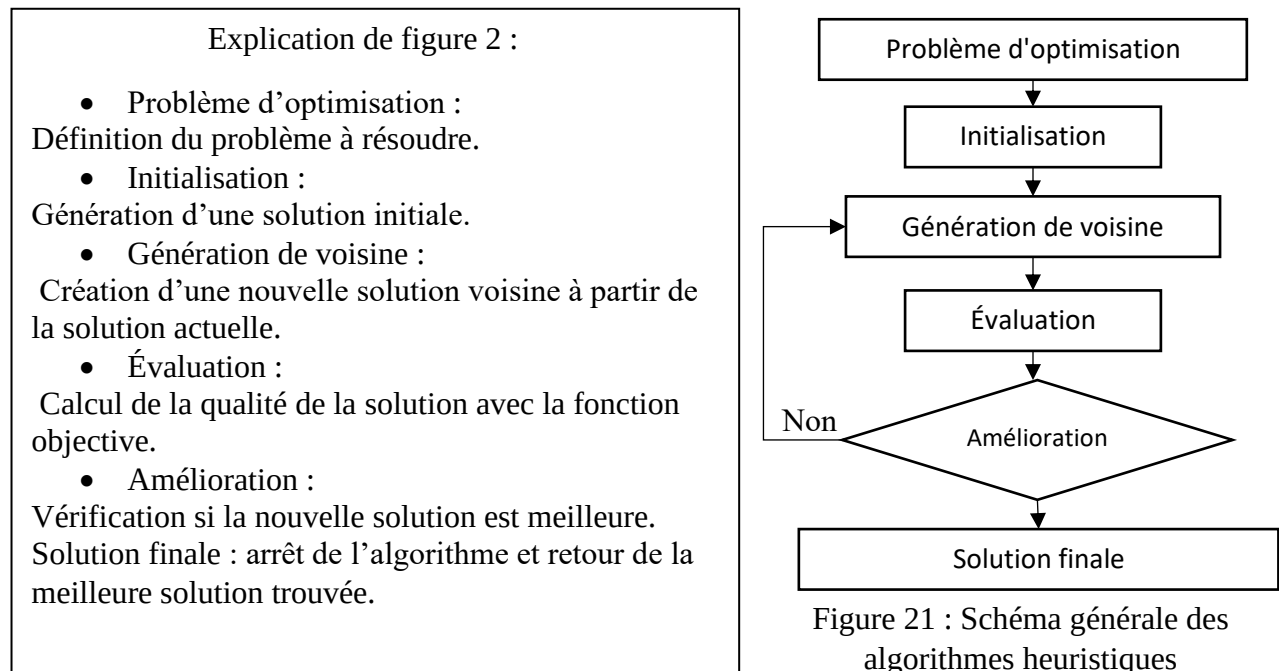
2.1 Méthode Heuristique

L'heuristique est une méthode de résolution de problèmes qui utilise des règles simples, des astuces et des approximations pour trouver des solutions. Les heuristiques sont souvent

employées pour résoudre des problèmes complexes dans des situations où la solution exacte n'est pas connue ou n'est pas réalisable. Ces méthodes peuvent être basées sur des connaissances expertes, des expériences passées ou des règles empiriques. [10] [9]

2.1.1 Principes de fonctionnement

Les heuristiques partagent généralement une structure de fonctionnement similaire



2.1.2 Avantages et inconvénients des méthodes Heuristiques :

Avantages	Inconvénients
Temps de calcul réduit.	Ne garantissent pas la solution optimale.
Simplicité de conception et d'implémentation.	Sensibles au choix de la stratégie heuristique.
Réduction de la complexité de recherche.	Risque de convergence vers un optimum local.
Adaptables à différents problèmes d'optimisation.	Peuvent produire des solutions approximatives uniquement.

Tableau 2:Présent une comparaison entre les avantages et les inconvénients des méthodes heuristique

2.2 Les méthodes Métaheuristiques

Une métaheuristique est une procédure de haut niveau conçue pour générer ou sélectionner une heuristique susceptible de fournir une solution suffisamment bonne à un problème d'optimisation, en particulier lorsque les méthodes classiques sont inefficaces. Ces algorithmes sont particulièrement utiles pour résoudre des problèmes complexes où les techniques d'optimisation traditionnelles peuvent ne pas parvenir à trouver une solution optimale dans un délai raisonnable. Les métaheuristiques sont souvent utilisées dans divers domaines, notamment la recherche opérationnelle, l'intelligence artificielle et la science des données, en raison de leur flexibilité et de leur adaptabilité. [10] [9])

2.2.1 Principes de fonctionnement

Les heuristiques partagent généralement une structure de fonctionnement similaire (Fig20)

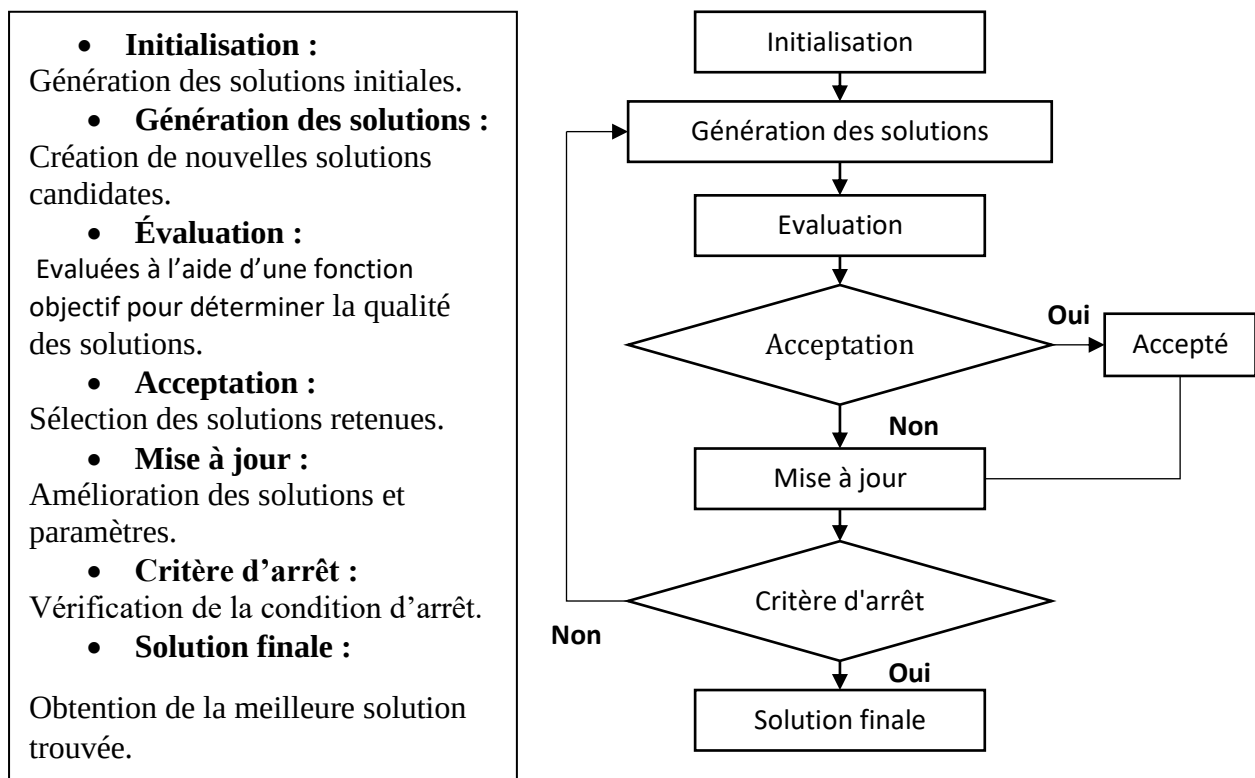


Figure 22:schéma de principe de fonctionnement de métaheuristique

2.2.2 Avantages et inconvénients des Métaheuristiques

Avantages	Inconvénients
Efficaces lorsque les méthodes exactes deviennent impraticables.	Forte dépendance au réglage des paramètres.
Permettent de résoudre des problèmes difficiles à modéliser mathématiquement.	Nécessitent souvent une adaptation spécifique au problème traité.
Plus performantes que la recherche exhaustive ou aléatoire dans plusieurs cas.	Sensibles au choix du critère d'arrêt.
Flexibles et adaptables à différents domaines d'application.	Risque de convergence vers des solutions sous-optimales.

Tableau 3:Présent une comparaison entre les avantages et les inconvénients des méthodes Métaheuristique

3 La différence entre une heuristique et une Métaheuristique

La différence entre une heuristique et une métaheuristique réside principalement dans leurs mécanismes de fonctionnement et leur domaine d'application. Les heuristiques sont des méthodes simples, rapides et généralement conçues pour résoudre un problème spécifique avec un nombre limité de paramètres. Elles permettent d'obtenir une solution acceptable en un temps réduit, mais sans garantir l'optimalité.

En revanche, les métaheuristiques sont des méthodes plus générales et flexibles, capables de traiter des problèmes complexes d'optimisation. Elles reposent sur des mécanismes avancés d'exploration et d'exploitation de l'espace de recherche, tout en utilisant plusieurs paramètres de contrôle afin d'améliorer la qualité des solutions et d'éviter les minima locaux. [11]

- **Comparaison entre heuristique et métaheuristique**

	Heuristique	Métaheuristique
Complexité	Généralement faible	Plus élevée
Temps d'exécution	Rapide	Plus lent que les heuristiques
Qualité de solution	Solution acceptable mais souvent locale	Solutions de meilleure qualité, proches de l'optimum global
Recherche de l'optimum global	Limitée	Meilleure capacité

Robustesse	Faible à moyenne	Élevée face aux problèmes complexes
Paramètres de réglage	Peu de paramètres	Plusieurs paramètres à ajuster
Exploration de l'espace de recherche	Limitée	Large exploration

Tableau 4:présente une Comparaison entre heuristique et métaheuristique

4 Classification des métaheuristique et leurs algorithmes

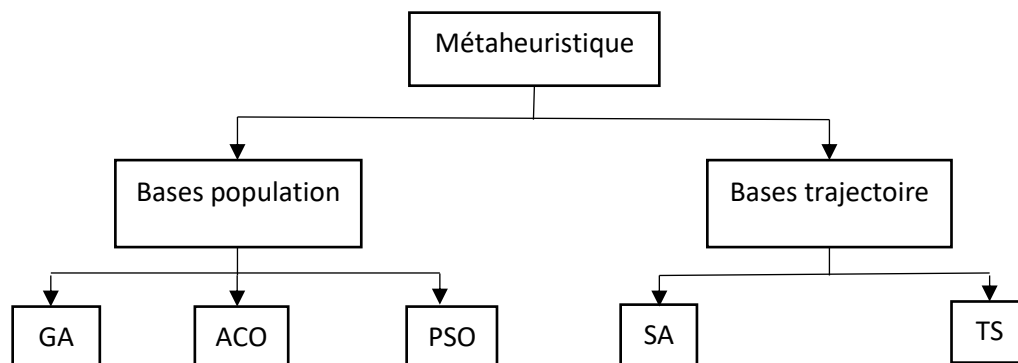


Figure 23:classification des métaheuristique et leurs algorithmes

4.1 Bases trajectoire :

Ces algorithmes d'optimisation partent d'une solution initiale (obtenue de façon exacte, ou par tirage aléatoire) et s'en éloignent progressivement, pour réaliser une trajectoire, un parcours progressif dans l'espace des solutions. Dans cette catégorie, se rangent :

4.1.1 Algorithme de recuit simulé (SA) :

Le recuit simulé (Simulated Annealing, SA) est une métaheuristique d'optimisation inspirée du procédé physique de recuit des métaux. Son principe consiste à rechercher une solution optimale en explorant progressivement l'espace des solutions tout en évitant les minima locaux grâce à l'acceptation probabiliste de certaines solutions moins bonnes. Basé sur l'algorithme de Métropolis, il contrôle cette exploration à l'aide d'un paramètre appelé température, qui diminue graduellement jusqu'à la convergence vers une solution proche de l'optimum global. [9]

4.1.2 Algorithme de Tabou (TS)

La recherche taboue (Tabu Search) est une métaheuristique d'optimisation proposée par Fred Glover dans les années 1980. Elle repose sur une exploration intelligente de l'espace des

solutions en utilisant une mémoire appelée liste taboue, qui interdit temporairement le retour vers les solutions récemment visitées. Cette stratégie permet d'éviter les cycles et de dépasser les minima locaux afin de guider la recherche vers des solutions de meilleure qualité. [9]

4.2 Bases population

Elles consistent à travailler avec un ensemble de solutions simultanément, que l'on fait évoluer graduellement. L'utilisation de plusieurs solutions simultanément permet naturellement d'améliorer l'exploration de l'espace des configurations. Elles sont largement utilisées en tatouage numérique pour l'optimisation des paramètres d'insertion. Dans cette catégorie, on retrouve plusieurs algorithmes utilisés en tatouage numérique, notamment :

4.2.1 Algorithme génétique (GA)

L'algorithme génétique est une méthode d'optimisation inspirée de la sélection naturelle de Darwin. Il manipule une population de solutions (individus) qui évolue à travers plusieurs générations jusqu'à un critère d'arrêt.

Elle est généralement utilisée dans le tatouage numérique robuste basé sur l'optimisation, notamment dans les domaines transformés (DWT/DCT), afin d'améliorer le compromis entre imperceptibilité et robustesse en optimisant les paramètres d'insertion du watermark. [3]

4.2.1.1 Les avantages et les inconvénients d'algorithme génétique GA

Avantages	Inconvénients
Très flexible (problèmes continus et discrets).	Coût computationnel élevé.
Bonne exploration de l'espace de recherche	Convergence parfois lente
Évite souvent les optimums locaux grâce à la mutation.	Dépend fortement du choix des paramètres (mutation, croisement, taille population).

Tableau 5:Présentes les avantages et les inconvénients d'algorithme génétique GA

4.2.2 Algorithme de colonies de fourmis (ACO)

L'algorithme Ant Colony Optimization (ACO) est une méthode à base de population inspirée du comportement des fourmis. Dans le tatouage numérique, il est utilisé pour optimiser les paramètres d'insertion du watermark, notamment le choix des coefficients dans les domaines transformés (DWT/DCT). Il permet d'améliorer le compromis entre imperceptibilité et robustesse en recherchant les meilleures solutions dans l'espace des configurations. [3]

4.2.3 Avantages et les inconvénients d'algorithme de colonies de fourmis (ACO)

Avantages	Inconvénients
Bon pour les problèmes combinatoires	Convergence parfois lente.
Exploration efficace grâce aux phéromones	Sensible au réglage des paramètres (α , β , ρ).
Robuste et capable d'éviter certains minima locaux	Peut devenir coûteux en calcul pour de grands graphes

Tableau 6:Présente les avantages et les inconvénients d'algorithme de colonies de fourmis (ACO)

4.2.4 Algorithme de Essaim Particulaire (PSO)

L'optimisation par Essaim Particulaire (Particle Swarm Optimization) : est une métaheuristique inspirée du comportement collectif des oiseaux et des bancs de poissons. Elle repose sur une population de particules représentant des solutions candidates qui se déplacent dans l'espace de recherche selon leur vitesse, leur meilleure position personnelle (pbest) et la meilleure position trouvée par l'essaim (gbest). À chaque itération, les particules mettent à jour leur vitesse et leur position afin de rechercher progressivement la solution optimale. PSO combine ainsi l'expérience individuelle et collective pour assurer un équilibre entre l'exploration globale et l'exploitation locale de l'espace de recherche. Initialement conçue pour les problèmes continus, cette méthode a également été adaptée aux problèmes discrets grâce à des représentations binaires et probabilistes.

Cet algorithme a été adopté dans le cas de notre étude. Le choix a été fait en fonction des résultats de la comparaison de cet algorithme avec ceux cités précédemment (Voir tableau de comparaison [12])

4.2.4.1 Principe de fonctionnement :

Le PSO est une méthode d'optimisation basée sur un essaim de particules qui explorent l'espace de recherche. Chaque particule ajuste sa position selon sa meilleure expérience (Pbest)

et celle de l'essaim (Gbest), jusqu'à convergence vers une solution optimale ou proche de l'optimum. [12]

Initialisation : initialise pour chaque particule :

x_{ij}^0 = position initiale, v_{ij}^0 = vitesse initiale, Pbest = meilleure position personnelle position i

Évaluation : calcul du fitness de chaque particule

Mise à jour v : ajustement de la vitesse de chaque particule selon la formule :

$$v_i = wv_i(t-1) + p_1C_1(p_i - x_i(t-1)) + p_2C_2(p_g - x_i(t-1))$$

Avec : v_i nouvelle vitesse de la particule.

w : Poids d'inertie.

$v_i(t-1)$: Ancienne vitesse.

p_i : Meilleure position personnelle.

p_g : Meilleure position globale.

C_1 : Facteur cognitif (expérience personnelle).

C_2 : Facteur social (influence du groupe).

$p_1 p_2$: Nombres aléatoires entre 0 et 1.

Mise à jour x : détermine le déplacement des particules vers de nouvelles positions selon la formule :

$$x_i = x_i(t-1) + v_i(t)$$

Évaluation : recalculer du fitness de chaque particule

Mise à jour Pbest : remplacement par la nouvelle solution si elle est meilleure.

Mise à jour Gbest : meilleure position globale de tout l'essaim

Solution finale : la meilleure solution globale [Gbest](#) représente la solution optimale

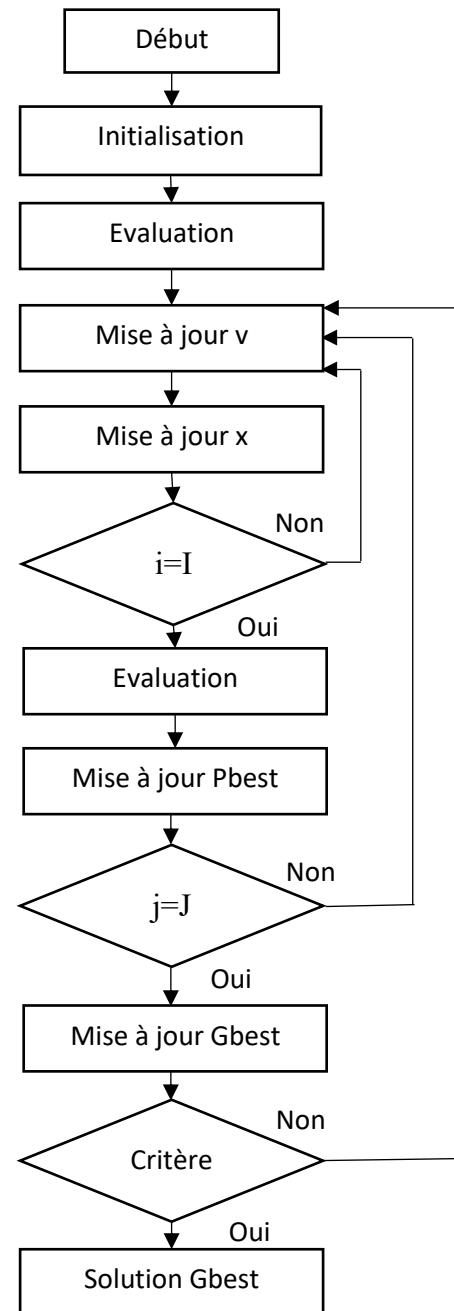


Figure 24: principe de fonctionnement de PSO

4.2.5 Les avantages et les inconvénients d'algorithme de Essaim Particulaire (PSO)

Avantages	Inconvénients
Simple à implémenter.	Risque de convergence prématurée.

Convergence rapide dans beaucoup de cas.	Moins efficace pour problèmes discrets complexes.
Peu de paramètres à régler.	Peut rester bloqué dans des optimums locaux.

Tableau 7:Présente les avantages et les inconvénients d'algorithme de Essaim Particulaire (PSO)

5 Comparaison entre PSO, ACO et GA

	PSO	ACO	GA
Vitesse de convergence	Rapide	Moyenne	Moyenne à lente
Complexité	Faible à moyenne	Élevée	Moyenne
Qualité des solutions	Très bonne pour optimisation continue	Bonne pour problèmes combinatoires	Bonne diversité des solutions
Nombre de paramètres	Peu	Moyen	Plusieurs
Adapté aux variables continues	Oui	Moins adapté	Oui

Tableau 8:comparaison entre GA, ACO, PSO

Pour les problèmes caractérisés par un espace de recherche réduit et une variable d'optimisation unique, l'algorithme de Essaim Particulaire (PSO) apparaît comme l'une des approches les plus appropriées parmi les métaheuristiques étudiées. Grâce à sa simplicité de mise en œuvre, au faible nombre de paramètres à ajuster et à sa rapidité de convergence, le PSO offre de bonnes performances pour les problèmes de faible dimension, notamment en tatouage numérique pour l'optimisation des paramètres d'insertion du watermark. En revanche, des algorithmes tels que le Genetic Algorithm (GA) et Algorithme de colonies de fourmis (ACO) sont généralement mieux adaptés aux problèmes d'optimisation complexes, multidimensionnels et combinatoires.

Conclusion

Dans ce chapitre, nous avons présenté les principales techniques d'optimisation, notamment les méthodes heuristiques et métaheuristiques. Nous avons également décrit quelques métaheuristiques utilisées dans le domaine du tatouage d'images tels que l'algorithme génétique, (GA), l'algorithme de colonie de fourmis (ACO) et l'algorithme d'essaim particulaire (PSO). Chacune de ces méthodes a ses avantages et limites. En se basant sur les résultats de cette comparaison, le choix d'utilisation de l'algorithme a été porté sur le PSO qui présente plusieurs avantages dans la résolution des problèmes complexes et son efficacité pour l'optimisation des paramètres dans les systèmes de tatouage numérique.

CHAPITRE 3

Conception et Mise en œuvre du système de tatouage d'Images

Introduction

Ce chapitre est consacré à la conception et à la mise en œuvre de l'algorithme choisi dans le cadre de notre étude. L'environnement de développement ainsi que les différentes étapes de mise en œuvre du système proposé sont décrits. Ensuite, les résultats expérimentaux obtenus lors des phases d'insertion et d'extraction du tatouage sont présentés. Enfin, une évaluation des performances du système est réalisée à travers différents critères de qualité.

1 Outils, méthodes et critères d'évaluation

1.1 Outils logiciels

Dans le cadre de notre projet, nous avons opté pour le langage Matlab car il est dédié au traitement d'images et offre plusieurs avantages significatifs :

Matlab dispose de bibliothèques et d'outils spécialisés pour le traitement d'images, tels que l'Image Processing Toolbox qui facilite l'implémentation et l'expérimentation de diverses techniques de watermarking et fournit des fonctions prédéfinies pour calculer des métriques telles que le PSNR, SSIM et le NCC, MSE, etc. ce qui simplifie grandement le processus d'évaluation des algorithmes du watermarking.

- Il permet de créer rapidement des prototypes grâce à son interface interactive et ses outils de visualisation. Cela nous aide à tester et améliorer nos algorithmes de manière progressive.
- Il offre des fonctions prédéfinies telles que la transformée en ondelettes discrète (DWT), la transformée en cosinus discrète (DCT), qui sont couramment utilisées dans les techniques de watermarking.
- Il est optimisé pour les calculs matriciels et les opérations de traitement d'images, ce qui garantit des performances élevées pour les algorithmes de watermarking.

1.2 Les méthodes utiliser pour l'insertion de marque

1.2.1 la Transformée en Ondelettes Discrètes (DWT)

Dans ce travail, la Transformée en Ondelettes Discrètes (DWT) a été utilisée pour l'insertion de la marque dans l'image hôte. Comparée aux transformées DFT et DCT, la DWT offre une meilleure localisation spatiale et fréquentielle ainsi qu'une représentation multi-résolution de l'image. Ces propriétés permettent d'obtenir un bon compromis entre l'imperceptibilité du tatouage et sa robustesse face aux différentes attaques. Parmi les

différentes familles d'ondelettes, l'ondelette de Haar a été retenue en raison de sa simplicité d'implémentation et de sa rapidité d'exécution.

1.2.2 la transformation d'Arnold

Afin de renforcer la sécurité du système de tatouage, l'image de la marque est préalablement chiffrée à l'aide de la transformation d'Arnold avant son insertion dans l'image hôte. Cette transformation repose sur une permutation réversible des pixels qui brouille l'apparence de la marque tout en conservant son contenu. Ainsi, même en cas d'extraction non autorisée, la marque reste difficile à interpréter sans connaître les paramètres de déchiffrement. L'association de la DWT pour l'insertion et de la transformation d'Arnold pour le chiffrement permet donc d'améliorer à la fois la robustesse et la sécurité du système de tatouage numérique.

1.2.3 L'algorithme d'optimisation (PSO)

D'après l'étude présentée dans le chapitre 2 ainsi que l'analyse des caractéristiques des algorithmes métaheuristiques étudiés, l'algorithme d'optimisation par essaim particulaire (PSO) a été retenu comme la méthode la plus adaptée à notre système de tatouage numérique d'images basé sur la transformation DWT.

Ce choix se justifie principalement par la simplicité d'implémentation du PSO, sa rapidité de convergence et sa faible complexité de calcul par rapport aux autres algorithmes étudiés tels que les algorithmes génétiques (GA) et les colonies de fourmis (ACO). De plus, le PSO offre un bon compromis entre l'invisibilité et la robustesse du tatouage grâce à sa capacité à rechercher efficacement la valeur optimale du coefficient d'insertion.

Par ailleurs, l'algorithme PSO nécessite un nombre réduit de paramètres de réglage, ce qui facilite son intégration sous MATLAB et améliore la stabilité des résultats expérimentaux. Ainsi, cet algorithme représente une solution efficace pour optimiser les performances du système de tatouage numérique proposé.

1.3 Métriques d'évaluation des performances du Tatouage numérique.

Afin d'évaluer les performances du système de tatouage numérique proposé, notamment en termes d'invisibilité et de robustesse, plusieurs métriques d'évaluation ont été utilisées, à savoir le PSNR, le NCC ainsi que le SSIM, présentés dans le chapitre I. Ces métriques permettent d'analyser efficacement la qualité du tatouage en mesurant

Ces critères constituent des indicateurs pertinents pour valider les choix méthodologiques adoptés dans cette étude.

2 Etapes de Conception de notre projet :

Voici le schéma général pour la conception de notre travail

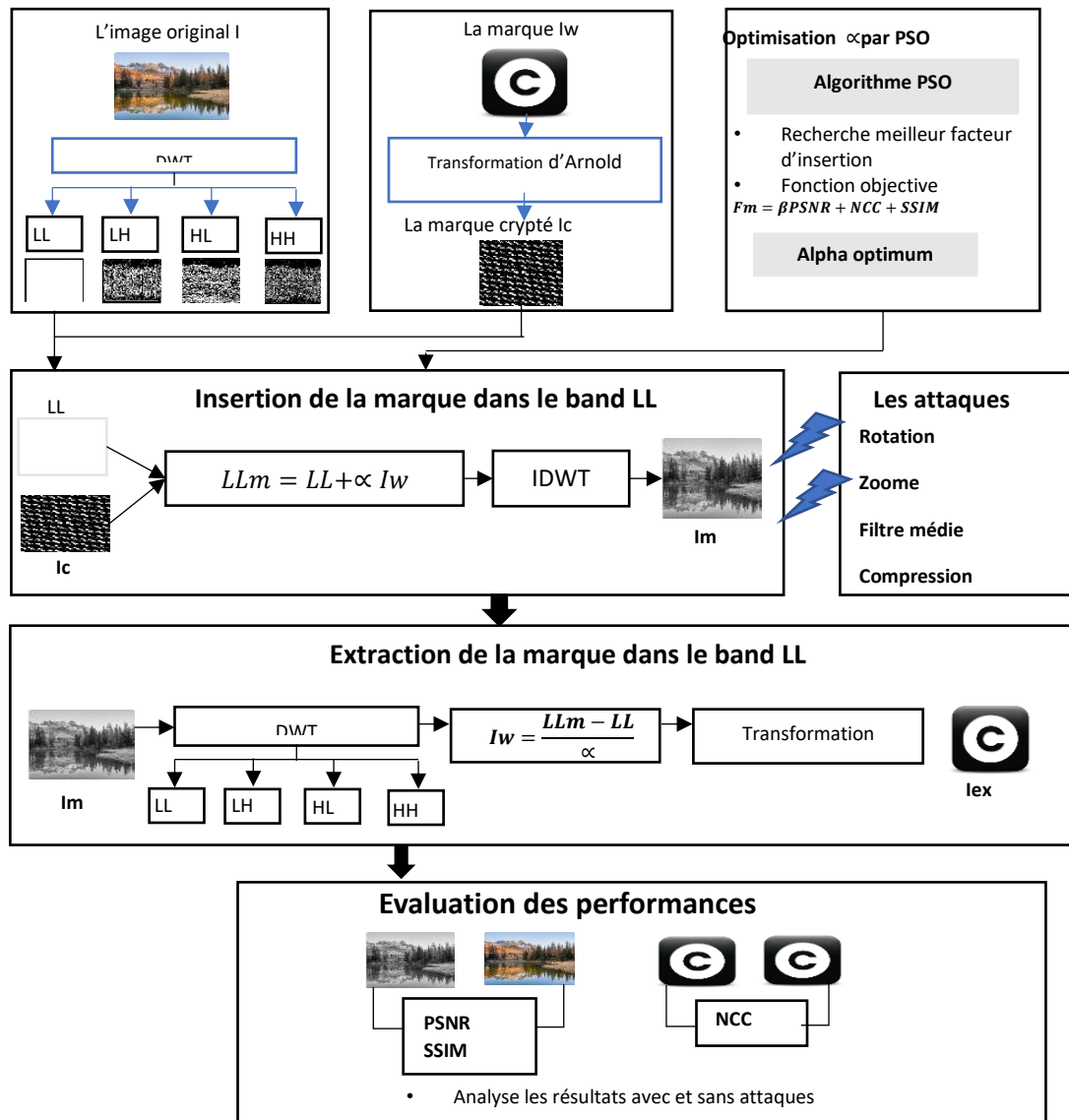


Figure 25:Schéma général de projet

3 Résultats et interprétations :

Nous appliquons l'algorithme du tatouage numérique tel décrit précédemment, sur quatre types d'images, en couleur et en niveau de gris et de tailles différentes.

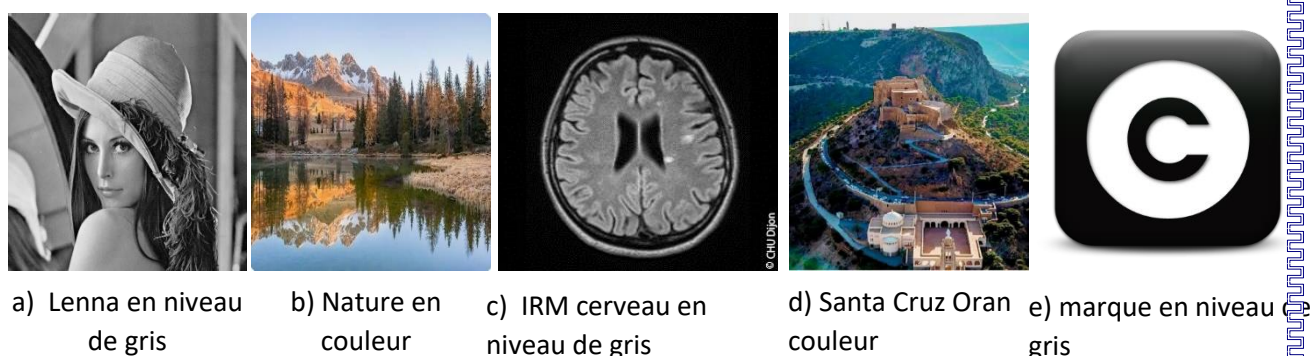


Figure 26: les types des images

Le tableau 1 représente les images tatouées et la marque extraite non attaquée et les valeurs de PSNR, SSIM et NCC :

Les images				
PSNR	33.1854	35.3075	44.3277	32.07264
SSIM	0.8942	0.9422	0.9709	0.9328
La marque				
NCC	0.9891	0.9879	0.9696	0.9891

Tableau 9 : les images tatouées et la marque extraite non attaquée et les valeurs de PSNR, SSIM et NCC

Les résultats obtenus en l'absence d'attaques montrent que la méthode proposée préserve efficacement la qualité visuelle des images hôtes tout en assurant une extraction fiable de la marque insérée. Les valeurs de PSNR, comprises entre 33.18 dB et 44.33 dB, indiquent que les distorsions introduites par le processus de tatouage demeurent faibles et pratiquement imperceptibles à l'œil humain. Par ailleurs, les valeurs élevées de SSIM (0.8942 à 0.9709) confirment une forte similarité structurelle entre les images originales et les images tatouées. En outre, les coefficients NCC, très proches de l'unité (≈ 0.99), témoignent d'une récupération précise et fidèle de la marque en l'absence de toute dégradation. Ces résultats mettent en

évidence l'excellente imperceptibilité du tatouage ainsi que la fiabilité et l'efficacité de la méthode proposée.

Le tableau 2 permet de visionner les images et la marque extraite après l'attaque de rotation 10° et les résultats des valeurs de NCC

Les images				
La marque				
NCC	0.0319	0.0274	0.0821	0.0374

Tableau 10 : les images et la marque extraite après l'attaque de rotation 10° et les résultats des valeurs de NCC

L'attaque par rotation entraîne généralement une dégradation notable des performances des systèmes de tatouage numérique. Les résultats obtenus montrent une forte diminution de la corrélation entre la marque originale et la marque extraite, ce qui indique une perte importante de l'information tatouée. Les marques récupérées deviennent souvent déformées et difficilement reconnaissables, traduisant une altération significative du signal.

Cette sensibilité s'explique principalement par la nature géométrique de la rotation, qui modifie la position spatiale des pixels et perturbe l'organisation des coefficients dans le domaine de la transformée en ondelettes discrète (DWT). Comme l'insertion et l'extraction du tatouage reposent sur ces coefficients, tout désalignement spatial entraîne une incohérence lors de la phase de récupération.

Ainsi, l'opération d'extraction ne parvient plus à reconstruire correctement l'information initialement insérée, ce qui se traduit par une baisse importante de la similarité entre les marques. De manière générale, ces résultats mettent en évidence la faiblesse des méthodes de tatouage basées uniquement sur la DWT face aux attaques géométriques, notamment la rotation.

Le tableau 3 permet de visionner les images et la marque extraite après l'attaque par filtre médian et les résultats des valeurs de NCC

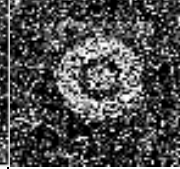
Les images				
La marque				
NCC	0.5520	0.4795	0.4025	0.4455

Tableau 11 : les images et la marque extraite après l'attaque par filtre médian et les résultats des valeurs de NCC

L'application du filtre médian entraîne une diminution modérée des performances avec des valeurs de NCC comprises entre 0.4025 et 0.5520. Malgré cette baisse, la marque reste encore visible et identifiable dans les images extraites. Cette dégradation est due au mécanisme du filtre médian qui remplace les valeurs des pixels par des valeurs voisines afin de supprimer le bruit, ce qui affecte également les coefficients contenant le tatouage. Les résultats indiquent donc une robustesse moyenne de la méthode face aux opérations de filtrage.

Le tableau 4 représente les résultats des images et la marque extraite après l'attaque par zoom et des valeurs de NCC

Les images				
La marque				
NCC	0.9704	0.9712	0.9279	0.9570

Tableau 12: les images et la marque extraite après l'attaque par zoom et des valeurs de NCC

Les résultats obtenus après l'attaque de zoom sont très satisfaisants. Les valeurs de NCC sont comprises entre 0.9279 et 0.9704, ce qui indique une forte corrélation entre la marque originale et la marque extraite. Visuellement, les marques récupérées conservent une très bonne

qualité. Cela montre que la méthode proposée résiste efficacement aux changements d'échelle et que l'information du tatouage demeure présente malgré la modification de la taille de l'image.

Le tableau 5 permet de visionner les images et la marque extraite après l'attaque par compression et les résultats des valeurs de NCC

Les images				
La marque				
NCC	0.9837	0.9820	0.9520	0.9851

Tableau 13: les images et la marque extraite après l'attaque par compression et les résultats des valeurs de NCC

Les meilleures performances sont observées sous l'effet de la compression, avec des valeurs de NCC comprises entre 0.9520 et 0.9851. Malgré la suppression d'une partie des informations de l'image lors de la compression, la marque reste parfaitement identifiable après extraction. Ces résultats montrent que les coefficients sélectionnés pour l'insertion du tatouage conservent efficacement l'information de la marque même après compression. La méthode proposée possède donc une très forte robustesse face à cette attaque couramment rencontrée lors du stockage et de la transmission des images numériques.

3.1 Evaluation des résultats :

L'analyse expérimentale confirme que la méthode de tatouage numérique basée sur la DWT, la transformation d'Arnold et l'optimisation par PSO offre un excellent compromis entre imperceptibilité et robustesse. En l'absence d'attaque, les valeurs élevées de PSNR (33–44 dB), de SSIM (0.89–0.97) et de NCC (≈ 0.99) démontrent que l'insertion de la marque n'altère pratiquement pas la qualité visuelle des images et permet une extraction très fidèle du tatouage.

Concernant la robustesse, les meilleures performances sont obtenues face aux attaques de compression et de zoom, avec des valeurs de NCC supérieures à 0.92, indiquant une excellente conservation de la marque. Le filtre médian provoque une dégradation modérée, mais la marque

reste détectable avec des valeurs de NCC comprises entre 0.40 et 0.55. En revanche, l'attaque de rotation constitue la principale faiblesse de la méthode, les valeurs de NCC devenant inférieures à 0.1 en raison de la désynchronisation spatiale introduite par la transformation géométrique.

La méthode proposée est particulièrement adaptée aux attaques de traitement du signal telles que la compression et le redimensionnement, tout en conservant une bonne imperceptibilité.

Conclusion

Dans ce chapitre, nous avons présenté le travail réalisé pour l'implémentation du système de tatouage numérique proposé. L'approche développée repose sur une combinaison de méthodes permettant d'assurer à la fois la protection de la marque et la préservation de la qualité de l'image hôte. Les résultats expérimentaux obtenus montrent que le système garantit une bonne qualité visuelle de l'image après insertion, ainsi qu'une récupération satisfaisante de la marque en conditions normales. De manière générale, le système présente un comportement stable et des performances globalement satisfaisantes face à différentes perturbations.

Cependant, les résultats mettent également en évidence certaines limitations face à des transformations plus complexes.

Conclusion générale

Le tatouage numérique d'images, qui consiste à introduire une marque dans l'image hôte, constitue une approche essentielle dans le domaine de la protection des contenus multimédias et de la propriété intellectuelle. Il permet d'assurer l'authenticité, la traçabilité et la sécurité des données numériques face aux risques de copie et de diffusion non autorisée des images.

Dans ce travail, une méthode de tatouage d'images a été proposée dans le cadre de la protection intellectuelle (ou le copyright) et implémentée en s'appuyant sur la transformée en ondelettes discrète (DWT), permettant une insertion efficace et imperceptible de l'information dans le domaine transformé et sur le cryptage de la marque qui permet une meilleure protection. L'approche adoptée pour une sécurité optimale a été l'utilisation d'une métaheuristique qui vise à garantir un compromis optimal entre invisibilité et robustesse du tatouage face aux différentes altérations susceptibles d'affecter l'image.

Les résultats obtenus montrent que le système développé présente de bonnes performances en termes de qualité d'image et de résistance aux attaques courantes, confirmant ainsi l'efficacité de la méthode proposée à travers les mesures objectives utilisées.

En perspective, plusieurs pistes d'amélioration peuvent être envisagées afin de renforcer davantage la robustesse et la sécurité du système. L'intégration de techniques de traitement avancées, telles que la combinaison de la transformations multi-résolution avec la décomposition en valeurs singulières (SVD), ainsi que l'utilisation de méthodes d'optimisation multi-objectives, intelligentes, pourraient contribuer à améliorer les performances globales du système de tatouage numérique et à répondre aux exigences croissantes en matière de sécurité de l'information.

Références

- [1] «<https://www.ssldragon.com/fr/blog/quest-ce-que-cryptage/#What-Is-Encryption>,» [En ligne].
- [2] «<https://en.wikipedia.org/wiki/Steganography>,» [En ligne].
- [3] K. LOUKHAOUKHA, «Tatouage numérique des images dans le domaine,» 2010.
- [4] «<https://interstices.info/cryptographie-steganographie-et-tatouage-des-secrets-partages/>,» [En ligne].
- [5] I. T. H. MAAMRI, «Tatouage numérique fragile pour,» 2016.
- [6] B. Sarra, «Développement et Implémentation d’algorithmes de,» 2019.
- [7] M. Tayachi, «Sécurité des images par tatouage numérique et cryptographie,» 2022.
- [8] B. Hafouda.A, «Tatouage numérique aveugle par LSB remplacement,» 2019.
- [9] S. m. S. Halima, «cours des méthode de rosolution exacte heuristique et metaheuristique».
- [10] «<https://developpement-informatique.com/cours/607/algorithmes-heuristiques-et-metaheuristiques>,» [En ligne].
- [11] «<https://commentouvrir.com/tech/heuristique-vs-metaheuristique-quelle-est-la-difference/>,» [En ligne].
- [12] E.-G. Talbi, «Metaheuristics: From Design to Implementation,» 2019.
- [13] «<https://www.ssldragon.com/fr/blog/quest-ce-que-cryptage/#What-Is-Encryption>,» [En ligne].
- [14] «http://archive.univ-biskra.dz/moodle2019/pluginfile.php/24003/mod_resource/content/1/chapitre%207.pdf,» [En ligne].