REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministre de l'enseignement supérieur et de la recherche scientifique

UNIVERSITE LARBI TEBESSI – TEBESSA

FACULTE DES SCIENCES EXACTES ET SCIENCE DE

LA NATURE ET DE LA VIE

Département mathématique et informatique

MEMOIRE DE MASTER

DOMAINE : MATHEMATIQUE UE ET INFORMATIQUE.

FILIERE : INFORMATIQUE.

NIVEAUX : Deuxième Année Master Réseaux Et Sécurité Informatique.

Réalisé par :

Mr. CHERGUI Abdelmoumene zakaria

Thème

Protection de documents par tatouage numérique

Devant le jury :

Dr. MERZOUG Soltane	**MCA**	**Université de Tébessa**	**Président**
Dr. MENASSEL Rafik	**MCA**	**Université de Tébessa**	**Examinateur**
Dr. MEKHAZNIA Tahar	**MCA**	**Université de Tébessa**	**Encadreur**

Date de soutenance : 07 /06 /2023

Promotion : 2022-2023

REMERCIEMENTS

Je tiens à exprimer ma sincère reconnaissance et mes vifs remerciements à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

*Tout d'abord à Monsieur " **Dr. Tahar MEKHAZNIA** " l'encadreur de ce mémoire pour son aide et sa patience, qu'il trouve en ces lignes l'expression de ma gratitude.*

Ensuite aux membres du jury

*" **Dr. MERZOUG Soltane** " et " **Dr. MENASSEL Rafik** "qui ont accepté d'évaluer ce travail, je leurs adresse l'expression de ma reconnaissance.*

Sans oublier les enseignants du département d'informatique de l'université de Tébessa "LARBI TEBESSI", qui se sont succédés durant mon cursus, sans eux je n'aurais pas pu atteindre mon objectif.

A vous tous je dis <Merci>

Dédicace

A mon chère père Jillani qui n'a pas pu voir mon travail
Puisse Dieu, le tout puissant l'avoir en sa sainte miséricorde
A mon adorable mère
Merci tout simplement d'être. . . . ..ma mère

A mon frère Wassim et ma sœur Meriame

A mes amis et mes collègues

Résumé

De nos jours, la protection des textes et des images est devenue de plus en plus importante en raison de la prévalence des textes électroniques et de la nécessité de protéger les données contre l'accès non autorisé et la duplication. Les techniques de tatouage numérique apportent une solution à ce problème en incorporant des informations secrètes dans le contenu original, assurant ainsi sa protection et permettant l'accès uniquement aux utilisateurs autorisés. Cet article explore deux algorithmes bien connus dans le traitement et l'encodage d'images, à savoir la transformée discrète en ondelettes (DWT) et la transformée discrète en cosinus (DCT). Ces algorithmes sont utilisés pour combiner du texte avec des images et appliquer diverses opérations. L'étude menée adopte une approche scientifique appliquée pour étudier l'efficacité de la fusion de texte avec des images à l'aide des algorithmes susmentionnés, révélant que les images résultantes sont hautement protégées et difficiles à copier ou à partager sans autorisation. De plus, le niveau de sécurité peut être encore amélioré en ajustant les paramètres et en introduisant des interférences. Notamment, l'une des principales recommandations proposées est la possibilité d'inverser le processus pour extraire le texte intégré de l'image et restaurer l'image dans son état d'origine.

Mots-clés : tatouage numérique, la transformée discrète en cosinus (DCT) la transformée discrète en ondelettes (DWT),

Abstract

Nowadays, the protection of text and images has become increasingly important due to the prevalence of electronic texts and the need to safeguard data from unauthorized access and duplication. Digital watermarking techniques provide a solution to this problem by embedding secret information within the original content, ensuring its protection and enabling access only to authorized users. This article explores two well-known algorithms in image processing and encoding, namely the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). These algorithms are employed to combine text with images and apply various operations. The study conducted adopts an applied scientific approach to investigate the effectiveness of merging text with images using the aforementioned algorithms, revealing that the resulting images are highly protected and challenging to copy or share without authorization. Moreover, the security level can be further enhanced by adjusting settings and introducing interference. Notably, one of the key recommendations proposed is the possibility of reversing the process to extract the embedded text from the image and restore the image to its original state.

Keywords : Digital Watermarking, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT),

ملخص

في الوقت الحاضر، أصبحت حماية النصوص والصور ذات أهمية متزايدة بسبب انتشار النصوص الإلكترونية والحاجة إلى حماية البيانات من الوصول غير المصرح به والنسخ. توفر تقنيات العلامات المائية الرقمية حلاً لهذه المشكلة من خلال تضمين معلومات سرية في المحتوى الأصلي وضمان حمايتها وتمكين الوصول إلى المستخدمين المصرح لهم فقط. تستكشف هذه المقالة خوارزميتين مشهورتين في معالجة الصور وتشفيرها وهما التحويل الموجي المنفصل وتحويل جيب التمام المنفصل يتم استخدام هذه الخوارزميات لدمج النص مع الصور وتطبيق عمليات مختلفة. اعتمدت الدراسة التي أجريت على منهج علمي تطبيقي للتحقق من فاعلية دمج النص مع الصور باستخدام الخوارزميات المذكورة أعلاه، وكشفت أن الصور الناتجة محمية بدرجة عالية ويصعب نسخها أو مشاركتها دون إذن. علاوة على ذلك، يمكن تحسين مستوى الأمان بشكل أكبر عن طريق ضبط الإعدادات وإدخال التداخل. والجدير بالذكر أن إحدى التوصيات الرئيسية المقترحة هي إمكانية عكس العملية لاستخراج النص المضمن من الصورة واستعادة الصورة إلى حالتها الأصل.

الكلمات المفتاحية: العلامات المائية الرقمية، التحويل الموجي المنفصل، تحويل جيب التمام المنفصل.

Liste des tableaux

Liste des figures

Table des matières

Introduction générale

La dissimulation d'informations ou de données est un acte visant à protéger ces informations ou données contre tout changement involontaire. On peut également la définir comme le processus consistant à cacher les détails d'un objet. L'une des utilisations courantes de la dissimulation d'informations est de cacher les données de manière à ce que tout changement soit restreint à un petit sous-ensemble des données totales. Cela aide à empêcher les programmeurs de modifier intentionnellement ou involontairement des parties d'un programme [1]. Les techniques de dissimulation d'informations sont classées en trois catégories : la stéganographie, la cryptographie et le tatouage numérique.

Le but principal de la stéganographie est de dissimuler un message (M) dans des données d'audio, de vidéo, d'image ou de texte (couverture) (D), pour obtenir de nouvelles données (D'), pratiquement indiscernables de (D) par les gens, de telle manière qu'un espion ne puisse pas détecter la présence de (M) dans (D').

Il est souvent dit que le but de la stéganographie est de cacher un message dans des communications de type un à un et que le but du tatouage numérique est de cacher un message dans des communications de type un à plusieurs. En bref, on peut dire que la cryptographie vise à protéger le contenu des messages, que la stéganographie vise à dissimuler leurs existences même, et que le tatouage numérique vise à fournir une preuve d'authenticité et de propriété.

Les méthodes de stéganographie n'ont généralement pas besoin de fournir une sécurité solide contre le retrait ou la modification du message caché. Les méthodes de tatouage numérique doivent être très robustes pour résister aux tentatives de suppression ou de modification d'un message caché [10].

Le tatouage numérique est une technique totalement différente de la cryptographie. La cryptographie ne fournit une sécurité que par le chiffrement et le déchiffrement. Cependant, le chiffrement ne peut pas aider l'expéditeur à surveiller la manière dont un destinataire légitime gère le contenu après déchiffrement. Il n'y a donc aucune protection après déchiffrement. Contrairement à la cryptographie, les tatouages numériques peuvent protéger le contenu même après qu'ils ont été décodés.

Une autre différence est que la cryptographie implique une transformation du document de sorte que le contenu du document ne soit pas visible sans une clé de déchiffrement. Contrairement à la cryptographie, le tatouage numérique laisse le fichier original intact et reconnaissable [2]

CHAPITRE 1 : NOTIONS DE BASE EN TATOUAGE NUMÉRIQUE D'IMAGE

CHAPITRE 1 : NOTIONS DE BASE EN TATOUAGE NUMÉRIQUE D'IMAGE

1.1 Introduction

La dissimulation d'information, la stéganographie et le tatouage numérique sont des termes couramment utilisés dans le domaine de la sécurité de l'information. Ces techniques ont été développées pour protéger la confidentialité des données en les dissimulant dans des supports tels que des images, des vidéos ou des fichiers audio. L'histoire de ces techniques remonte à plusieurs siècles, mais leur importance a augmenté considérablement avec la prolifération des médias numériques. Les applications de ces techniques sont nombreuses et variées, allant de la surveillance de la diffusion à l'identification du propriétaire, en passant par la preuve de propriété et le suivi des transactions. Dans ce chapitre, nous allons explorer le lien de tatouage numérique avec d'autres technologies de sécurité ainsi l'histoire de tatouage numérique, les applications de tatouage numérique. Nous allons également discuter des différentes classifications des algorithmes de filigrane numérique finalement les métriques d'évaluation de la performance d'un système de tatouage numérique.

1.2 Techniques de protection numérique de documents

1.2.1 La stéganographie

La stéganographie est une discipline de la sécurité de l'information qui consiste à dissimuler des données secrètes au sein d'un support, tel qu'une image ou un fichier audio, de manière à ce que leur présence ne puisse être détectée. Elle vise à masquer l'existence même de ces données, permettant ainsi une communication confidentielle sans éveiller les soupçons d'un observateur externe. La stéganographie repose sur des techniques et des algorithmes spécifiques pour incorporer les données dissimulées de façon invisible et robuste. Son objectif est de fournir un moyen de dissimulation de données ou de communication secrète en utilisant des supports existants. [4]

1.2.2 Le filigrane

Le filigrane est une technique de marquage visuel ou numérique utilisée pour identifier, protéger ou authentifier un média, tel qu'une image, une vidéo ou un document. Il consiste en l'incorporation discrète d'informations, telles que des logos, des motifs ou des codes, dans le contenu principal du média. Le filigrane peut être visible ou invisible, et il peut être utilisé à des fins de propriété intellectuelle, de traçabilité ou de lutte contre la contrefaçon. Il offre une méthode de protection des médias en permettant de retracer leur origine et de dissuader la reproduction non autorisée. [1]

1.2.3 La cryptographie

La cryptographie est un domaine des mathématiques et de l'informatique qui étudie les méthodes de sécurisation de l'information en la transformant de manière à la rendre illisible pour des personnes non autorisées. Elle vise à assurer la confidentialité, l'intégrité et l'authenticité des données. La cryptographie utilise des algorithmes mathématiques avancés pour chiffrer les données en utilisant une clé secrète, rendant ainsi le contenu illisible sans cette clé. Elle permet également de vérifier l'origine et l'intégrité des données en utilisant des fonctions de hachage et des signatures numériques. La cryptographie joue un rôle crucial dans la protection des communications, des transactions en ligne, des informations sensibles et de la sécurité des systèmes informatiques. [4]

1.2.4 La signature numérique

La signature numérique est un mécanisme cryptographique utilisé pour vérifier l'authenticité, l'intégrité et la non-répudiation d'un message ou d'un document numérique. Elle est créée en utilisant un algorithme de cryptographie asymétrique, où une clé privée est utilisée pour générer la signature et une clé publique correspondante est utilisée pour vérifier la signature. La signature numérique est unique pour chaque message et est calculée à partir du contenu du message ainsi que de la clé privée de l'émetteur. Elle permet de garantir que le message n'a pas été altéré depuis sa signature et qu'il provient bien de l'émetteur légitime. Les signatures numériques sont largement utilisées dans les communications sécurisées, les transactions électroniques et les systèmes de certification pour garantir l'authenticité et l'intégrité des données numériques. [1]

1.2.5 Le tatouage numérique

a. Définition

Le tatouage numérique, également appelé marquage ou watermarking, est une technique de dissimulation d'informations dans des médias numériques tels que des images, des vidéos ou des fichiers audio. Il consiste à intégrer des données ou des signaux imperceptibles dans le contenu original, de manière à les rendre robustes aux transformations et aux altérations. Le tatouage numérique vise à fournir une identification, une authentification ou une traçabilité des médias numériques, ainsi qu'à protéger les droits de propriété intellectuelle. Les informations tatouées peuvent être utilisées pour suivre la provenance, détecter la contrefaçon ou protéger les droits d'auteur des médias numériques. Le tatouage numérique doit être réalisé de manière invisible et résistante aux attaques malveillantes afin de préserver l'intégrité et la fiabilité des données tatouées. [1]

b. Historique

Les premières applications du tatouage numérique étaient axées sur la protection des droits d'auteur et la lutte contre la contrefaçon. Les chercheurs ont exploré différentes méthodes pour insérer des marques d'authentification dans les médias numériques, permettant ainsi de retracer leur provenance et d'identifier les propriétaires légitimes.

Au fil des années, le tatouage numérique a évolué pour inclure d'autres utilisations, telles que la gestion des droits numériques, la traçabilité des contenus, la protection des données sensibles et la lutte contre la falsification. Les avancées technologiques, telles que l'amélioration des algorithmes de tatouage et des capacités de traitement informatique, ont permis d'améliorer la robustesse et l'efficacité de cette technique.

Aujourd'hui, le tatouage numérique est utilisé dans de nombreux domaines, tels que l'industrie du divertissement, la protection des marques, la sécurité des documents, la gestion des droits d'auteur et la lutte contre la contrefaçon. Il continue d'évoluer avec l'émergence de nouvelles technologies, telles que l'apprentissage automatique et la blockchain, pour renforcer encore davantage la sécurité et l'authenticité des contenus numériques. [1]

1.3 Applications de tatouage numérique

1.3.1 La surveillance de diffusion

Le tatouage numérique est utilisé dans la surveillance de diffusion pour garantir l'intégrité et la traçabilité des contenus diffusés. Il permet d'incorporer des informations invisibles dans les médias diffusés, comme des codes uniques ou des marques d'identification. Ces tatouages numériques servent à suivre la diffusion des contenus, à vérifier l'authenticité et à détecter toute manipulation ou violation de contrat. Ils offrent une méthode automatisée et fiable pour surveiller la diffusion des contenus, assurant ainsi la conformité des diffusions et la protection des droits des annonceurs et des détenteurs de contenu. [5]

1.3.2 Identification du propriétaire

Le tatouage numérique est utilisé dans l'identification du propriétaire pour marquer les médias numériques avec des informations uniques liées au propriétaire légitime. Il permet d'incorporer des signatures numériques invisibles dans les fichiers, tels que des codes de traçabilité ou des métadonnées spécifiques au propriétaire. Ces tatouages numériques servent à prouver l'authenticité et l'origine des médias, facilitant ainsi l'identification et la protection des droits de propriété intellectuelle. Ils offrent une méthode discrète et robuste pour identifier les propriétaires légitimes et dissuader la contrefaçon ou l'utilisation non autorisée de contenu numérique. [5]

1.3.3 Contrôle des dispositifs

Les filigranes numériques ont la capacité d'ajouter de la valeur plutôt que de restreindre leur utilisation. Un exemple récent de contrôle des dispositifs est l'identification unique imprimée aux côtés des publicités, des billets, de l'emballage, etc. Après avoir scanné l'image via la caméra du téléphone, le logiciel utilise l'identification unique pour diriger le navigateur web vers le site web correspondant. [5]

1.4 Algorithmes de tatouage numérique

Il existe différentes classifications des algorithmes de tatouage numérique. Tout d'abord, les techniques de tatouage peuvent être divisées en quatre groupes en fonction du type de données à être marqué. [4]

A. Tatouage numérique de texte
B. Tatouage numérique d'image
C. Tatouage numérique de vidéo
D. Tatouage numérique d'audio

1.5 Tatouage numérique visible et invisible

La visibilité est associée à la perception de l'œil humain, de sorte que si le tatouage numérique est intégré aux données de manière à être visible sans extraction, on parle de tatouage numérique visible. Des exemples de tatouages numériques visibles sont les logos utilisés dans les papiers et les vidéos. En revanche, un tatouage numérique invisible ne peut pas être vu par l'œil humain. Il est donc intégré aux données sans affecter le contenu et peut être extrait par le propriétaire ou la personne qui en a le droit. Par exemple, les images distribuées sur Internet peuvent être tatouées numériquement de manière invisible pour une protection contre la copie. [4]

Figure 1:Exemple d'un tatouage visible et invisible **[14]**

1.5.1 Tatouage numérique public

Dans le tatouage numérique public, il n'est pas nécessaire d'avoir l'image original pendant le processus de détection pour détecter le tatouage numérique. Seule la clé secrète est requise. Par exemple, dans le tatouage numérique public d'image, nous n'avons pas besoin de l'image d'origine. [4]

1.5.2 Tatouage numérique privé

Dans le tatouage numérique privé, l'image originale est nécessaire pour détecter le tatouage numérique. [4]

1.6 Domaines d'application de techniques de tatouage numérique

1.6.1 Domaine spatial

Une technique de tatouage numérique basée sur le domaine spatial, propage les données de tatouage numérique à être intégrées dans la valeur de pixel. Ces approches utilisent des changements mineurs dans l'intensité de la valeur de pixel. L'exemple le plus simple des techniques précédentes consiste à intégrer le tatouage numérique dans les bits de poids faible des pixels de l'image. En d'autres termes, des portions significatives de composants de basse fréquence de l'image doivent être modifiées afin d'insérer les données de tatouage numérique de manière fiable et robuste. Comme autre exemple, une image est divisée en blocs de même taille et des données de tatouage numérique sont ajoutées avec les sous-blocs. [6]

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

Pour avoir une imperceptibilité ainsi qu'une robustesse, l'ajout de watermark se fait dans le domaine fréquentiel. Dans cette méthode, les coefficients de transformation sont modifiés pour intégrer le tatouage.

Le domaine transformé est également appelé le domaine de fréquences car les valeurs de fréquences peuvent être modifiées par rapport à leur valeur d'origine.

Les techniques les plus importantes dans le domaine de transformation sont la transformée en cosinus discrète (DCT) et la transformée en ondelettes discrètes (DWT) et Transformation de Fourier rapide (FFT).[10]

	Domaine spatial	Domaine fréqeuntiel
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 1.1 : Comparaison entre le domaine spatial et le domaine fréquentiel *[5]*

1.7 Classification de techniques de tatouage

Différentes techniques de cette catégorie sont les suivantes.

1.7.1 Tatouage numérique robuste

L'une des propriétés du tatouage numérique est la robustesse. Nous appelons un algorithme de tatouage robuste s'il peut survivre après des opérations courantes de traitement du signal telles que le filtrage et la compression avec pertes.[7]

1.7.2 Tatouage numérique fragile

Un tatouage numérique fragile doit pouvoir être détecté après tout changement de signal et il doit également être possible d'identifier le signal avant modification. Ce type de watermark est utilisé principalement pour la vérification ou l'authenticité du contenu original. [7]

1.7.3 Tatouage numérique semi-fragile

Un tatouage numérique semi-fragile est sensible à un certain degré de changement apporté à une image avec filigrane.

Le processus d'incorporation de watermark fait référence à la technique d'ajout d'un watermark à une image ou une vidéo numérique. Le processus consiste à intégrer le watermark dans l'image ou la vidéo hôte de manière perceptiblement invisible mais détectable par des algorithmes de détection de watermark appropriés. [7]

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

1.8.1 SSIM (Structural SIMilarity index)

Est un indice de similarité d'image qui mesure la similarité structurelle entre deux images. Il prend en compte la luminance, le contraste et la structure de l'image. Plus l'indice SSIM est proche de 1, plus les images sont similaires. [7]

1.8.2 Un histogramme d'image

Est une représentation graphique de la distribution des intensités de pixels dans une image. Il trace le nombre de pixels pour chaque valeur d'intensité de couleur, qui se situe généralement entre 0 et 255 pour les images en niveaux de gris et entre 0 et 255 pour chacun des canaux de couleur rouge, vert et bleu des images en couleur.

Les histogrammes peuvent fournir des informations utiles sur le contraste, la luminosité et l'équilibre des couleurs d'une image. Par exemple, un histogramme avec la plupart de ses valeurs inclinées vers le côté gauche indique que l'image est principalement sombre, tandis qu'un histogramme avec des valeurs inclinées vers le côté droit indique que l'image est principalement lumineuse. Les histogrammes peuvent également être utilisés pour ajuster la luminosité et le contraste d'une image en manipulant la distribution des intensités de pixels. [7]

1.9 Conclusion

Ce chapitre fournit une présentation des fondamentaux d'un système de tatouage numérique, y compris son schéma général, ses principales propriétés, sa classification, son histoire, ainsi que la classification basée sur la fonctionnalité de robustesse. De plus, il aborde les métriques d'évaluation de la performance d'un système de tatouage numérique. Cette revue nous permet de comprendre les grandes lignes de la conception d'un système de tatouage numérique. Le prochain chapitre sera consacré à l'aspect juridique du tatouage numérique.

CHAPITRE 2 : LA PERSPECTIVE JURIDIQUE SUR LE TATOUAGE NUMERIQUE

CHAPITRE 2: LA PERSPECTIVE JURIDIQUE SUR LE TATOUAGE NUMERIQUE

2.1 Introduction

Le domaine des médias numériques a révolutionné la manière dont nous consommons et distribuons l'information, mais cette évolution entraîne le défi de protéger les droits de propriété intellectuelle. Cela a donné lieu à des techniques telles que la stéganographie, le tatouage numérique et la détection de manipulation d'images et de vidéos numériques. Dans ce contexte, il est essentiel de comprendre le cadre juridique entourant les droits de propriété intellectuelle et leur application. Ce document explore les concepts de dissimulation d'informations, de stéganographie et de tatouage numérique, ainsi que leurs implications juridiques. Nous discutons des diverses organisations nationales et internationales chargées de surveiller les droits de propriété intellectuelle et explorons le processus d'obtention et de mise en application de ces droits. Enfin, nous soulignons l'importance du tatouage numérique et de son rôle dans la protection de la propriété intellectuelle à l'ère numérique.

2.2 La perspective juridique sur le tatouage numérique

2.2.1 Les droits des propriétés intellectuelles

Les droits de propriété intellectuelle sont des droits qui protègent les créations de l'esprit humain, Les droits de propriété intellectuelle comprennent les droits d'auteur, les brevets, les marques commerciales, les secrets commerciaux et les dessins et modèles. Les droits de propriété intellectuelle protègent le travail des créateurs et des inventeurs, leur permettant de profiter des avantages financiers de leur travail. [8]

2.2.2 Les droits d’auteur

Le droit d'auteur est un type de droit de propriété intellectuelle qui protège les créations de l'esprit humain, notamment les œuvres littéraires, les œuvres musicales, les œuvres dramatiques, les œuvres audiovisuelles, les œuvres architecturales et les œuvres graphiques ou photographiques. Le droit d'auteur donne à l'auteur un droit exclusif de reproduire, de modifier, de publier et de communiquer sa création au public. [8]

2.2.3 Les indications géographiques

Les indications géographiques sont des mots, des expressions ou des signes qui sont associés à un lieu ou à une région et qui sont utilisés pour désigner les produits et services qui ont une origine géographique spécifique. Ces indications sont protégées par le droit

de la propriété intellectuelle et sont conçues pour protéger les consommateurs contre les produits similaires qui sont fabriqués dans un lieu différent. Par exemple, le fromage de papillon est une indication géographique qui est réservée aux produits qui sont fabriqués dans la région française du même nom. [8]

2.2.4 Les organismes qui détiennent les lois de propriété intellectuelle

Les lois de propriété intellectuelle sont détenues par diverses organisations et gouvernements à travers le monde. Les nations membres de l'Organisation Mondiale du Commerce sont tenues de respecter les conventions internationales sur le droit de la propriété intellectuelle, telles que l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC). De nombreux pays ont également leurs propres lois de propriété intellectuelle qui protègent les droits des inventeurs et des créateurs. Ces lois peuvent varier considérablement d'un pays à l'autre et sont appliquées par des organismes nationaux tels que les offices nationaux de la propriété intellectuelle. Les lois de propriété intellectuelle sont détenues par un certain nombre d'organisations différentes, y compris les gouvernements nationaux et leurs organes législatifs, l'Organisation Mondiale de la Propriété Intellectuelle (OMPI), l'Organisation Mondiale du Commerce (OMC), l'Union européenne et leurs agences respectives. Chacune de ces organisations à son propre ensemble de lois et de règles régissant la propriété intellectuelle, ce qui signifie que, pour connaître les lois applicables à un cas donné, il faut connaître les lois des différentes organisations, ainsi que la manière dont elles s'appliquent. [8]

A. À l'échelle nationale

L'Office national des droits d’auteur et des droits voisins, ONDA

L'ONDA est une organisation algérienne chargée de la gestion des droits d'auteur. Fondée en 1973, sa principale mission est de protéger les intérêts moraux et matériels des auteurs, ainsi que de leurs ayants droit et des titulaires de droits voisins. Son rôle est d'assurer la protection des droits de propriété intellectuelle et de faciliter la gestion collective des droits d'auteur en Algérie. L'ONDA joue un rôle essentiel dans la promotion et la préservation de la création artistique et littéraire en veillant à ce que les créateurs bénéficient d'une juste rémunération pour leur travail. [8]

L'INAPI -Institut National Algérien de la Propriété Industrielle

L'Institut National Algérien de la Propriété Industrielle (INAPI) est un établissement public à caractère industriel et commercial (EPIC) placé sous la tutelle du Ministère de

l'Industrie et des Mines. Doté de la personnalité civile et de l'autonomie financière, l'INAPI a pour mission principale la protection des droits de propriété industrielle en Algérie.

L'INAPI offre des services publics essentiels, notamment l'enregistrement des demandes de protection des brevets d'invention, des marques, des dessins, des modèles, des appellations d'origine et des circuits intégrés. Son rôle consiste à recevoir, examiner et délivrer les titres de propriété industrielle, garantissant ainsi la protection légale des innovations et des créations industrielles.

Créé par le décret exécutif 98-68 du 21 février 1998, l'INAPI a été établi suite à la restructuration de l'INAPI initiale qui englobait à la fois la propriété industrielle et la normalisation. Son statut lui confère l'autorité nécessaire pour promouvoir et mettre en œuvre les réglementations relatives à la propriété industrielle en Algérie, favorisant ainsi l'innovation, la créativité et le développement économique du pays.

B. À l'échelle internationale

L'Organisation mondiale de la propriété intellectuelle OMPI

Est une agence spécialisée des Nations Unies qui se concentre sur la protection et la promotion de la propriété intellectuelle à l'échelle internationale. Elle offre des services, des politiques, des informations et des initiatives de coopération pour aider les gouvernements et les organisations à exploiter la valeur de la propriété intellectuelle à des fins commerciales et sociales. L'OMPI a été fondée en 1967 et est basée à Genève, en Suisse. Elle est l'un des principaux organes politiques et judiciaires pour le traitement des questions relatives à la propriété intellectuelle à l'échelle internationale. L'OMPI s'efforce d'améliorer les systèmes nationaux de propriété intellectuelle et de promouvoir l'harmonisation des lois et des pratiques internationales. Elle offre également des services de recherche et de formation pour les états membres. [8]

Société des auteurs dans les arts graphiques et plastiques ADAGP

ADAGP (Société des auteurs dans les arts graphiques et plastiques) est une société de gestion collective des droits d'auteur en France. Elle représente les auteurs d'œuvres graphiques, plastiques et visuelles tels que les artistes, les illustrateurs, les designers, les photographes, etc.

L'ADAGP a pour mission de protéger, de promouvoir et de gérer les droits d'auteur de ses membres. Elle agit en leur nom pour percevoir et répartir les redevances liées à l'utilisation de leurs œuvres, que ce soit au niveau national ou international. L'ADAGP négocie également des accords de licences avec les utilisateurs d'œuvres artistiques, garantissant ainsi une juste rémunération aux créateurs. [8]

La China Written Works Copyright Society (CWWCS)

La China Written Works Copyright Society (CWWCS) est une société chinoise spécialisée dans la gestion collective des droits d'auteur pour les œuvres littéraires. Elle joue un rôle essentiel dans la protection des intérêts des auteurs en représentant leurs droits et en veillant à ce qu'ils reçoivent une rémunération équitable pour l'utilisation de leurs œuvres.

La CWWCS exerce différentes fonctions clés pour atteindre ses objectifs. Tout d'abord, elle négocie des contrats de licence avec les utilisateurs potentiels des œuvres littéraires, tels que les éditeurs, les médias ou les plateformes en ligne, afin de garantir que les droits des auteurs sont respectés et que leur travail est utilisé légalement. Elle perçoit également les redevances et les droits de reproduction au nom des auteurs, en veillant à ce qu'ils soient correctement rémunérés pour l'utilisation de leurs œuvres.

En plus de ses activités de gestion des droits, la CWWCS joue un rôle de surveillance en surveillant les utilisations illégales des œuvres littéraires et en prenant des mesures pour faire respecter les droits des auteurs. Cela peut inclure des actions en justice contre les contrevenants et la coopération avec les autorités compétentes pour lutter contre le piratage et d'autres formes d'infraction au droit d'auteur. [8]

2.2.5 Comment être titulaire du droit d'auteur

Pour être titulaire du droit d'auteur d'une œuvre, on doit être l'auteur de l'œuvre et avoir le contrôle exclusif de cette œuvre. Nous pourrait être l'auteur d'une œuvre en la créant nous-mêmes ou en travaillant avec d'autres personnes pour la créer. Nous pouvait également être titulaire du droit d'auteur d'une œuvre en achetant ou en héritant des droits d'auteur sur l'œuvre. Pour être titulaire des droits d'auteur, nous devons nous assurer que nous avons les droits exclusifs sur l'œuvre et que nous sommes en mesure de les défendre.

2.2.6 Comment on obtient les droit des propriétés intellectuelles

Les droits de propriété intellectuelle sont des droits accordés par le gouvernement afin de protéger les créations intellectuelles. Ces droits sont obtenus en déposant une demande auprès des autorités compétentes chargées de leur octroi. Les détenteurs de droits de propriété intellectuelle peuvent ensuite exercer leurs droits en utilisant leurs créations, que ce soit pour les commercialiser, les louer ou les céder à d'autres parties intéressées.

2.2.7 Copyright et droit d'auteur : quelles différences ?

Le droit d'auteur et le copyright sont très proches mais il existe des différences importantes. Le droit d'auteur est le droit exclusif conféré à l'auteur d'une œuvre littéraire, artistique ou scientifique de la divulguer et de l'exploiter. Ce droit est reconnu dans la plupart des pays et est généralement acquis par l'auteur dès qu'il crée l'œuvre. Le

copyright, par contre, est un système de droit d'auteur qui fonctionne à l'échelle internationale et qui est reconnu dans une multitude de pays. Le copyright offre une protection supplémentaire aux auteurs en leur donnant le droit de s'opposer à la copie et au partage non autorisé de leur œuvre.

2.3 Attaques sur les algorithmes de tatouage numérique

L'attaque est définie comme étant tout traitement susceptible d'altérer la marque ou provoquer une ambiguïté lors son exécution.

On distingue plusieurs types d'attaques. Parmi ces attaques nous retrouvons :

2.3.1 L'attaque de protocole

L'objectif de cette technique est de remettre en cause l'authenticité de la marque, plutôt que de la détruire. Elle est utilisée lorsque le propriétaire de l'image originale appose sa marque et la diffuse. L'attaquant crée ensuite un faux original en retirant la marque du propriétaire de l'image et en apposant sa propre marque sur le faux original. Cela lui permet de revendiquer les droits du propriétaire légitime de l'image en cas de litige entre le propriétaire légitime et l'usurpateur [5].

2.3.2 L'attaque de collusion

Est une méthode visant à créer un document à partir de plusieurs versions de documents tatoués par des clés différentes, dans le but de supprimer le signal de tatouage. Cette attaque se divise en deux grandes catégories [5] :

Plusieurs attaquants peuvent collecter différentes images contenant le même tatouage, afin d'estimer la marque et de la supprimer après chaque image.

Lorsque la même image est tatouée avec différentes marques, il suffit des moyennes pour obtenir une estimation de l'image originale.

2.3.3 L'attaque cryptographique

On utilise le principe de la cryptographie pour réaliser l'attaque cryptographique. Elle vise à découvrir la clé secrète utilisée pour insérer la marque en essayant toutes les clés possibles de manière exhaustive. Il est important de noter que l'algorithme est public selon le principe de sécurité Kerchoff. [5]

2.4 Conclusion

Le domaine des médias numériques a apporté de nombreuses avancées, mais a également posé d'importants défis pour la protection des droits de propriété intellectuelle. L'utilisation de techniques telles que la stéganographie, le tatouage numérique et la détection de falsification d'images et de vidéos peut aider à relever ces défis. Cependant, il est essentiel de comprendre le cadre juridique entourant les droits de propriété intellectuelle et leur application pour assurer leur protection efficace. Le prochain chapitre sera dédié aux techniques numériques de tatouage.

CHAPITRE 3 : SYSTEMES DE TATOUAGE

CHAPITRE 3 : SYSTEMES DE TATOUAGE

3.1 Introduction

Le tatouage numérique est un processus utilisé pour intégrer des marques invisibles dans des médias numériques. Le schéma général du système de tatouage numérique comprend trois étapes essentielles : la génération de la marque, l'insertion du filigrane numérique et l'extraction du filigrane numérique. Parmi les différents algorithmes de tatouage numérique, certains sont spécifiquement conçus pour le domaine spatial, tels que l'algorithme de modification du bit de poids faible (LSB), l'algorithme du modèle binaire local (LBP) et l'algorithme de modification d'histogramme.

D'autres algorithmes se basent sur le domaine fréquentiel ou les transformées, notamment la transformée en cosinus discrète (DCT) et la transformée en ondelettes discrètes (DWT). Ces algorithmes exploitent les caractéristiques de fréquence des médias numériques pour intégrer les marques de manière efficace et robuste.

L'utilisation de ces algorithmes de tatouage numérique permet d'assurer l'authenticité, l'intégrité et la traçabilité des médias numériques dans différents domaines d'insertion, tels que la protection des droits d'auteur, la sécurité des données et la gestion des contenus numériques

3.2 Le schéma général du système de tatouage numérique

Le modèle de base du schéma de tatouage numérique se compose de trois éléments le processus de génération de la marque, le processus d'insertion de la marque et le processus d'extraction de la marque. La génération de la marque est illustrée dans la figure 3.1, l'insertion de la marque est présentée dans la figure 3.2 tandis que l'extraction de la marque est présentée dans la figure 3.3

3.2.1 Le processus de génération de la marque

La génération de la marque n'est pas une fonction standard. La marque doit être adaptée aux applications souhaitées. Dans les applications simples, les données insérées peuvent être un texte ou une image. Dans les applications développées, la marque peut avoir des propriétés particulières en fonction des objectifs souhaités. [4]

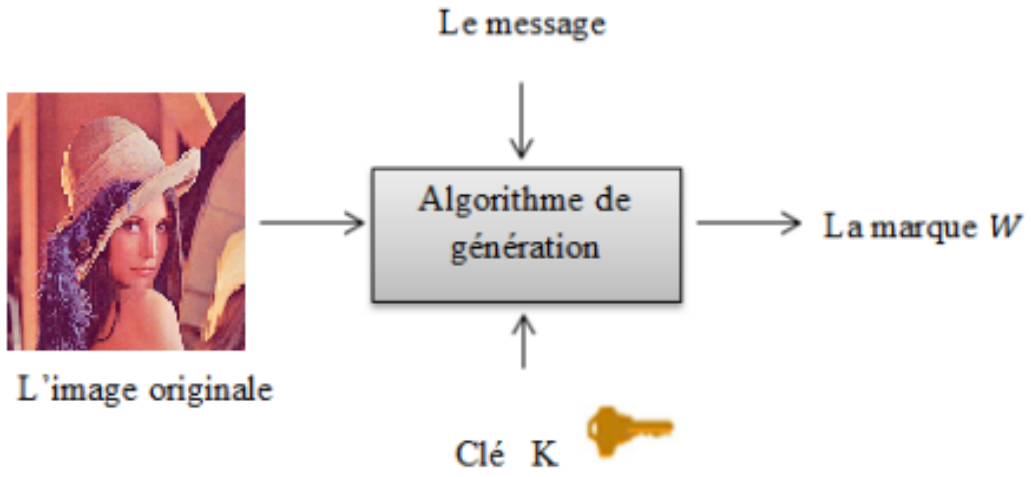


Figure 2:le processus de la génération de la marque.

3.2.2 Le processus d'insertion de filigrane numérique

Le processus d'insertion du filigrane se fait côté expéditeur. Dans cette étape, la marque est insérée aux données originales en appliquant un certain algorithme de tatouage et en utilisant une clé secrète k pour générer les données tatouées [4]

Cette étape consiste en plusieurs opérations :

a : Compression du message à insérer et chiffrement avec une clé cryptographique.

b : Sélection d'un support de couverture.

c : Utilisation de l'algorithme de dissimulation pour sélectionner les sous-parties du support favorables à la dissimulation.

d : Dissimulation aléatoire du message chiffré dans les parties favorables en utilisant la clé stéganographique/tatouage.

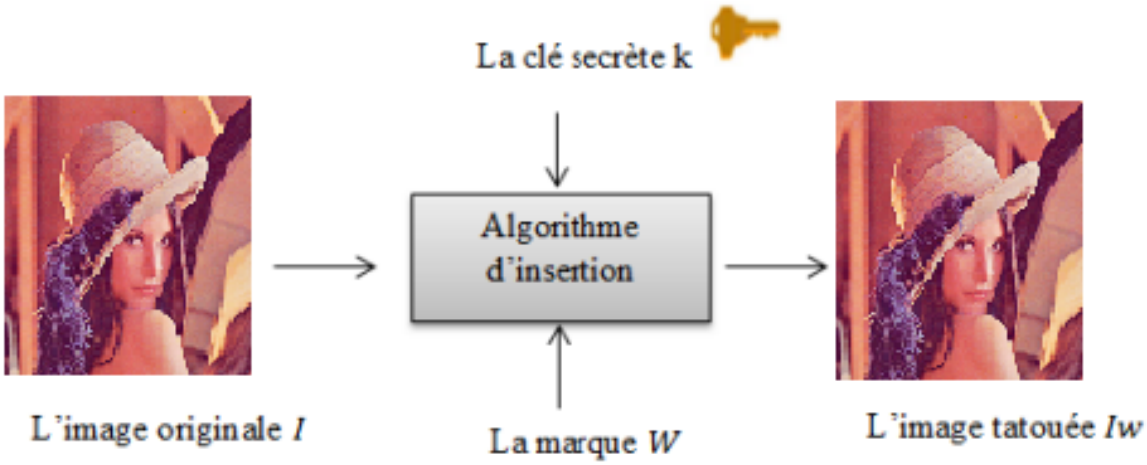


Figure 3:Algorithme d'insertion de tatouage numérique

3.2.3 Le processus d'extraction de filigrane numérique

Le processus d'extraction se fait en inversant l'algorithme d'insertion implémenté et en utilisant la clé secrète et les données originales pour extraire la marque intégrée. La Figure 1.3 montre le principe du processus d'extraction de la marque. [4]

Cette étape comprend les opérations suivantes :

a : La sélection des sous-parties du support favorable à la dissimulation à l'aide de l'algorithme de la dissimulation.

b : Retrouver les positions du message chiffré dans les parties favorables, à l'aide de la clé stéganographique/tatouage.

c : Déchiffré le message à l'aide de la clé cryptographique et le décompresser

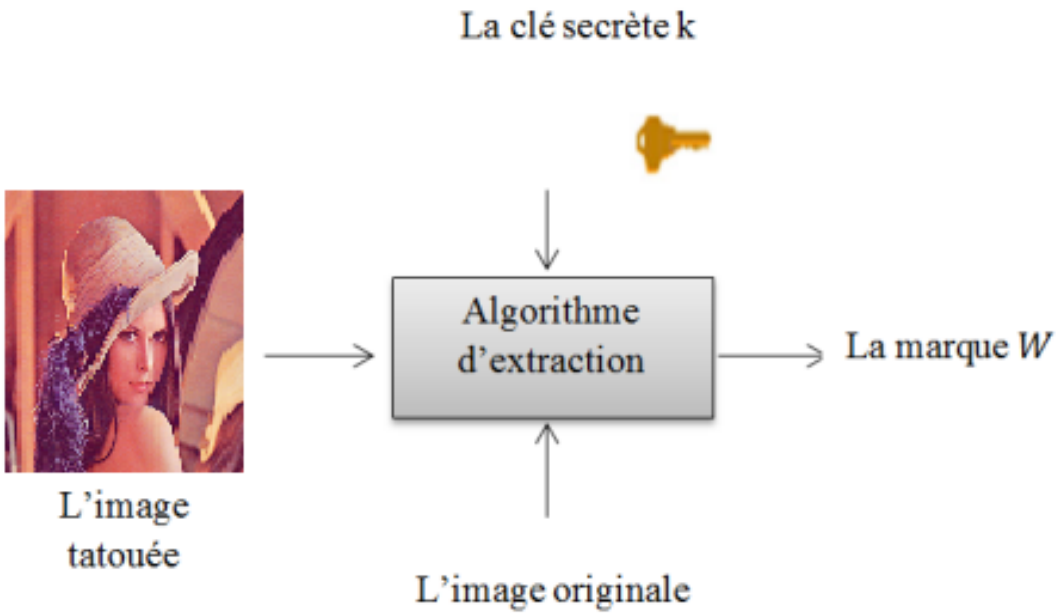


Figure 4:Algorithme d'extraction de tatouage numérique

3.3 Les algorithmes de tatouage numérique selon le domaine d'insertion

3.3.1 Algorithme de domaine spatial

a. Algorithme 1 : modifie le bit de poids faible (LSB)

La méthode du bit le moins significatif (Least Significant Bit (LSB)) représente l'une des techniques du domaine spatial les plus anciennes et les plus simples. Elle peut être appliquée à n'importe quelle forme de tatouage. Dans cette technique, le LSB de l'image originale est remplacé par la marque. Les bits de la marque sont codés dans une séquence qui sert de clé. Cette séquence doit être connue pour récupérer les bits insérés dans l'image originale. La valeur en pixels décimaux de l'image originale est d'abord convertie en binaire. Ensuite, les bits les plus à droite de chaque pixel sont remplacés par les bits de la marque. [6]

b. Exemple

L'invisibilité des données de filigrane est obtenue en supposant que les bits LSB sont visuellement insignifiants. Il existe deux façons de modifier un LSB. Il y a des méthodes pour changer les bits LSB. Le LSB de chaque pixel peut être remplacé par le message secret ou les pixels de l'image peuvent être choisis au hasard selon une clé secrète.

Voici un exemple de modification des LSB: supposons que nous avons trois composantes R, G et B dans une image. Leur valeur pour un pixel choisi est verte

(R, G, B) = (0, 255, 0).

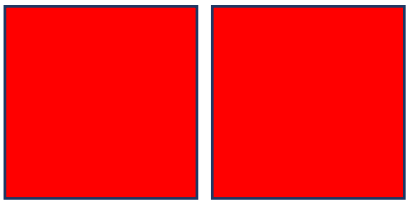
Si un algorithme de tatouage numérique veut cacher la valeur de bit 1 dans la composante R, alors la nouvelle valeur de pixel aura des composantes

(R, G, B) = (1, 255, 0)

Comme cette modification est très petite, la nouvelle image est indiscernable à l'œil humain par rapport à l'originale.

Bien que ces techniques de domaine spatial puissent être facilement utilisées sur presque toutes les images, elles ont les inconvénients suivants.

Ces techniques sont très sensibles aux opérations de traitement de signal et peuvent être facilement endommagées. Par exemple, la compression avec perte peut complètement détruire le filigrane. En d'autres termes, le filigranage dans le domaine spatial est facile à détruire en utilisant certaines attaques telles que le filtrage passe-bas. Par conséquent, les algorithmes de filigranage de domaine de transformation sont utilisés.



(A) (B)

Figure 5:255ème rouge (A), 254ème rouge (B)

c. Algorithme 2 Le modèle binaire local (LBP)

Le modèle binaire local (LBP) est une méthode initialement conçue pour l'analyse de la texture, la reconnaissance d'objet / motif. L'idée de base de LBP est de résumer la structure locale de l'image en comparant chaque pixel avec ses pixels de voisinage. Premièrement, l'image originale est partitionnée en blocs carrés non superposés. Deuxièmement, les différences de pixels locaux entre le pixel central et ses pixels adjacents dans chaque bloc sont calculées. Ensuite, ces pixels sont utilisés pour insérer les bits de la marque en utilisant le pixel central comme seuil. Le pixel de voisinage est étiqueté à 1 si son intensité est supérieure au seuil, sinon étiqueté à 0. À la fin de ce processus, LBP produit un code binaire de 8 bits de 0 à 255. [1]

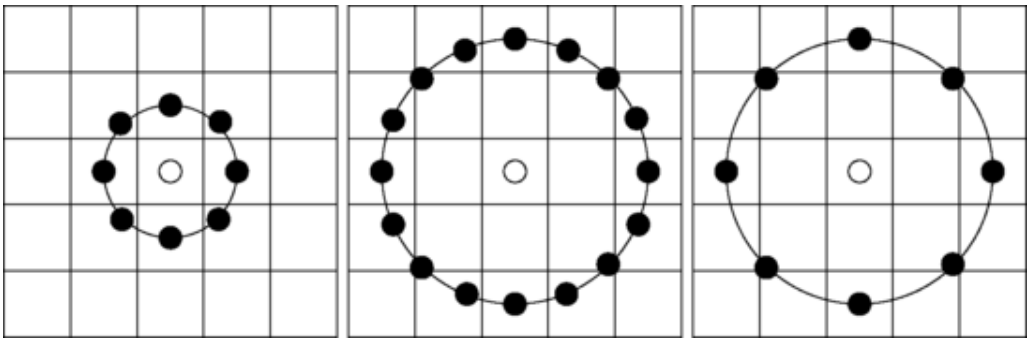
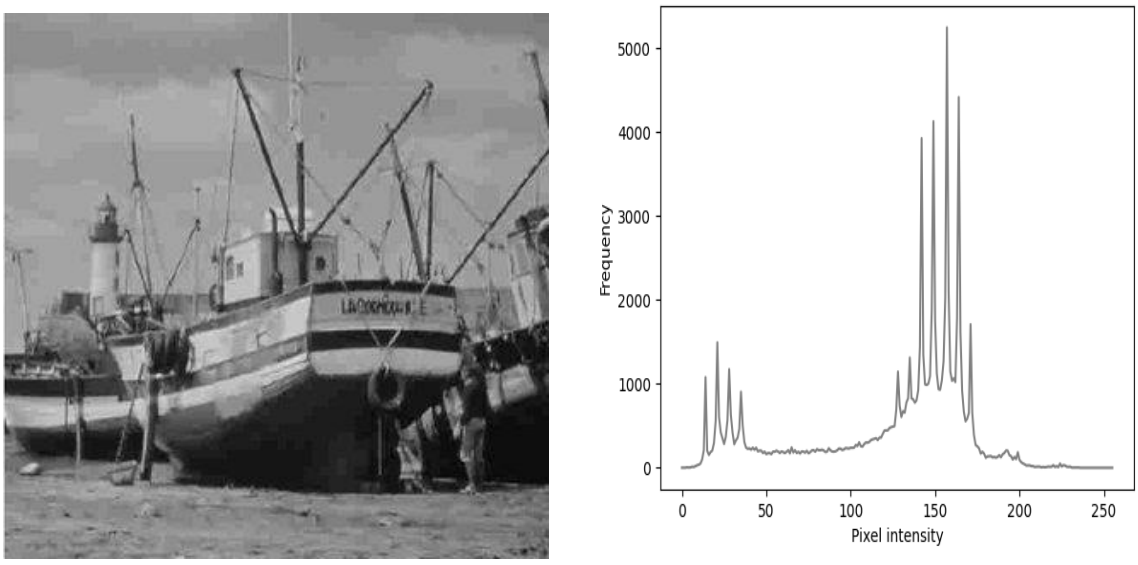


Figure 6:le pixel central et ses pixels adjacents dans chaque bloc

d. Algorithme 3 La modification d'histogramme

La technique de modification d'histogramme est une autre technique de tatouage dans la catégorie du domaine spatial, cet technique et basée sur les valeurs de pixels de l'image hôte pour construire l'histogramme de l'image après l'insertion de tatouage on utilise la redondance des informations statistiques de l'image hôte pour masquer les données secrètes. Cette technique insère la marque en décalant le maximum et le zéro (ou le minimum s'il n'y a pas de zéro) de l'histogramme. Cette méthode peut être exécutée facilement, mais la capacité d'insertion est limitée par le nombre de points maximum qui apparaissent.



A B

Figure 7:(A) l'image hôte (B) l'histogramme de l'image**[14]**

3.3.2 Les Algorithmes de domaine fréquentiel ou le domaine des transformées

Pour avoir une imperceptibilité ainsi qu'une robustesse, l'ajout de watermark se fait dans le domaine fréquentiel. Dans cette méthode, les coefficients de transformation sont modifiés pour intégrer le tatouage.

Le domaine transformé est également appelé le domaine de fréquence car les valeurs de fréquence peuvent être modifiées par rapport à leur valeur d'origine.

a. La transformée en cosinus discrète (DCT)

La DCT est une transformation mathématique qui convertit la fonction du domaine temporel en domaine fréquentiel. Elle donne lieu à de nombreux coefficients : un seul courant continu (CC) et un ensemble de courants alternatifs (CA). La matrice DCT montre les bandes de la matrice DCT dans un bloc de 8 * 8. Les basses fréquences sont situées dans le coin supérieur gauche de la matrice DCT. [10]

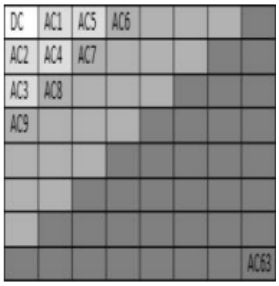


Figure 8:DCT matrice

Algorithme de la transformée en cosinus discrète (DCT)

Début d'algorithme
Variables
Image de couverture
Image de filigrane

Pour chaque bloc non chevauchant de l'image de couverture :
Segmenter le bloc en blocs de 8x8 pixels
Calculer la transformée en cosinus discrète (DCT) du bloc
Appliquer un critère de sélection de bloc pour déterminer les blocs à modifier
Appliquer un critère de sélection de coefficient pour déterminer les coefficients à modifier
Modifier les coefficients sélectionnés en intégrant le filigrane
Appliquer la transformée inverse de la DCT sur le bloc

Fin de l'algorithme
Retourner l'image avec le filigrane intégré.

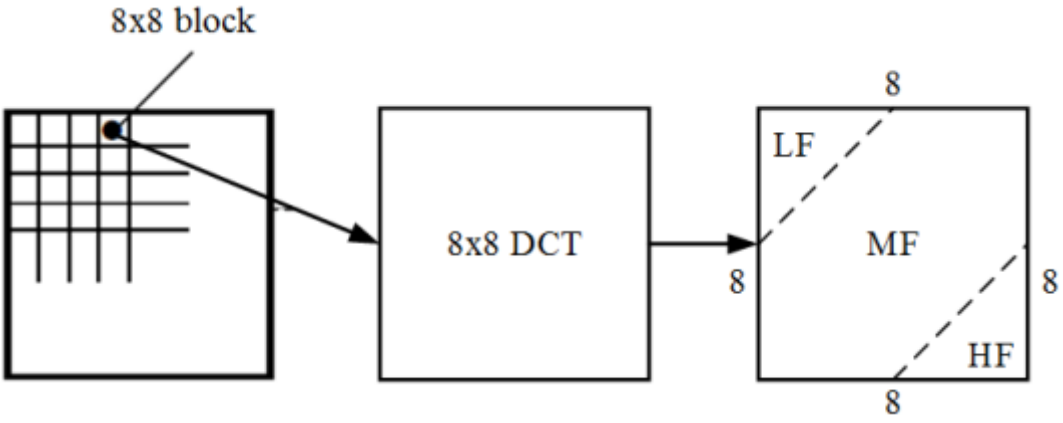


Figure 9:Application de la (DCT) sur une image.

b. La transformée en ondelettes discrètes (DWT)

DWT est une méthode analytique mathématique utilisée pour traiter les signaux dans de nombreuses applications. Elle capture à la fois des informations spatiales et fréquentielles de l'image. DWT est largement utilisée dans le tatouage numérique et la compression d'images car elle fournit une bonne qualité d'image visuelle.

DWT décompose l'image en une bande de sous-fréquence basse (LL) et trois bandes de sous-fréquences élevées (LH, HL et HH). LL contient la plupart des informations de l'image et cette bande est plus proche de l'image d'origine. LH représente les détails

horizontaux, HL représente les détails verticaux et HH représente les détails diagonaux de l'image. L'image est reconstruite à partir de ces sous-bandes à l'aide d'une DWT inverse. L'image peut également être décomposée plusieurs fois, LL décomposée en quatre sous-bandes, et ainsi de suite. [10]

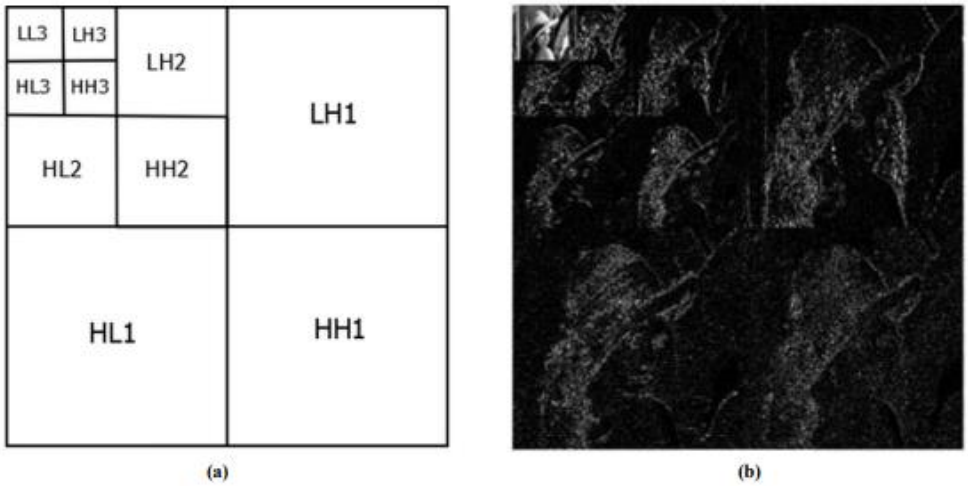


Figure 10:Décomposition d'image de 3 niveaux à l'aide de la transformée en ondelettes 2D

Algorithme de la transformée en ondelettes discrètes (DWT)
Début d'algorithme
Variables
Image de couverture
Image de filigrane
Préparation de l'image de couverture et du filigrane.
Décomposition de l'image de couverture en sous-bandes avec DWT.
Sélection des coefficients de la sous-bande appropriée.
Modification des coefficients sélectionnés pour intégrer le filigrane.
Reconstruction de l'image tatouée avec la transformation inverse de DWT.
Évaluation de la qualité et de l'imperceptibilité de l'image tatouée
Fin de l'algorithme
Retourner l'image avec le filigrane intégré.

3.4 Conclusion

En conclusion, le système de tatouage numérique offre un moyen efficace de générer, d'insérer et d'extraire des filigranes numériques. Les algorithmes de tatouage numérique, qu'ils soient basés sur le domaine spatial (comme LSB et LBP) ou sur le domaine fréquentiel (comme DCT et DWT), offrent des solutions adaptées à différents domaines d'insertion. Ces algorithmes permettent de garantir l'authenticité, l'intégrité et la traçabilité des médias numériques, renforçant ainsi la protection des droits d'auteur, la sécurité des données et la gestion des contenus numériques

CHAPITRE 4 : CONCEPTION ET REALISATION

CHAPITRE 4 : CONCEPTION ET REALISATION

4.1 Introduction

Ce chapitre est structuré de manière à fournir une compréhension approfondie de notre étude sur le tatouage numérique. Nous commençons par examiner les travaux connexes, afin de mettre en contexte notre recherche par rapport aux travaux existants dans le domaine.

Ensuite, nous présentons en détail la base de données d'images que nous avons utilisée comme référence dans nos expériences. Nous expliquons les critères de sélection des images et les caractéristiques de cette base de données, qui constituent la base de notre évaluation expérimentale.

Nous consacrons une section à la présentation et à la discussion des résultats expérimentaux de notre étude sur la robustesse du tatouage numérique en utilisant les algorithmes DCT et DWT. Nous détaillons les procédures expérimentales, les paramètres utilisés et les métriques de performance évaluées. Les résultats obtenus sont analysés et interprétés pour évaluer l'efficacité et la résistance des algorithmes de tatouage numérique.

Enfin, nous abordons deux critères importants pour évaluer la qualité des images originales et des images avec tatouage numérique, à savoir la similarité structurale (SSIM) et l'histogramme. Nous décrivons ces critères en détail et expliquons comment ils ont été utilisés dans notre évaluation.

À travers cette organisation claire et méthodique, nous résumons les principales découvertes de notre étude dans une conclusion générale. Nous soulignons également les perspectives futures et les pistes de recherche qui peuvent être explorées pour approfondir et améliorer les techniques de tatouage numérique.

4.2 Survol de la littérature

Dans [1], une nouvelle méthode de tatouage de texte est proposée pour les documents Word, présentant une bonne robustesse. Le schéma intègre les signaux secrets dans les propriétés spéciales de l'objet Word. Les informations de tatouage sont chiffrées, divisées en plusieurs groupes et emballées dans le message avant d'être intégrées de manière circulaire dans le document Word. Toutes ces opérations rendent la performance du schéma excellente en termes de robustesse en cas d'attaques, par rapport aux méthodes basées sur les caractéristiques de la police de caractères. Cette stratégie présente des perspectives prometteuses pour une utilisation étendue dans les domaines de la protection des droits d'auteur et du contrôle de la diffusion, et peut s'appliquer à la fois à la langue anglaise et chinoise.

Dans [2], l'objectif est de décrire les bases du tatouage numérique et de retracer l'historique du tatouage numérique, tout en abordant également les applications ainsi que les méthodes utilisées pour évaluer les systèmes de tatouage numérique. En outre, la

technique de tatouage numérique est discutée. Il existe deux types de techniques de tatouage numérique connues sous le nom de tatouage numérique visible et invisible. Il a été élaboré des algorithmes importants pour dissimuler des messages dans des signaux numériques. Ceux-ci peuvent être décrits par de nombreux modèles différents, tels que les modèles basés sur la communication et les modèles géométriques.

Dans [3], un algorithme de tatouage numérique sans marqueur est proposé pour la protection des droits d'auteur des documents textuels. L'algorithme intègre la fréquence d'occurrence des caractères articles et voyelles dans le texte pour le protéger. L'algorithme avec une approche de tatouage numérique sans marqueur fournit une solution robuste au problème de tatouage numérique pour les documents textuels. Pour vérifier la fréquence d'occurrence de chaque caractère voyelle dans chaque texte et générer une clé en utilisant les propriétés intrinsèques du texte. La clé qui est générée est enregistrée auprès de l'autorité de copyright (CA) et cette clé est utilisée lorsqu'il y a un conflit dans les revendications de droit d'auteur, puis ce tatouage numérique peut être extrait du contenu numérique pour identifier le propriétaire original. Les résultats expérimentaux illustrent l'efficacité de l'algorithme proposé sur des documents textuels confrontés à diverses attaques de falsification telles que l'insertion et la suppression et les résultats sont également comparés aux travaux récents sur le tatouage numérique pour les documents textuels.

Dans [4], une méthode de tatouage numérique novatrice pour les applications web de texte électronique en langue arabe a été proposée en utilisant l'extension de caractère arabe « Kashida ». Cette méthode peut également s'adapter à d'autres langues sémitiques similaires, telles que l'ourdou et le Persan. L'idée principale derrière la méthode proposée est d'utiliser tous les caractères extensibles dans un mot pour représenter certains bits de tatouage ou des bits trompeurs. Les bits trompeurs sont intégrés dans le texte de couverture en fonction d'une clé secrète avant que les bits de tatouage ne soient intégrés. Ces Kashidas trompeuses sont ajoutées pour rendre la tâche d'une attaque très difficile et offrir une sécurité au système. Cette étude a montré que ce schéma de tatouage rendait la tâche d'une attaque beaucoup plus difficile par rapport aux méthodes similaires et liées précédentes. Elle a également montré la possibilité de cacher plus de bits de données secrètes sans dégrader la sécurité, ce qui est considéré comme attractif pour les applications de données de texte électronique web telles que la préservation des propriétés intellectuelles ou des caractéristiques de copyright.

Dans [5], une vue d'ensemble des différentes caractéristiques du tatouage numérique, de ses diverses applications et de son utilisation dans différents domaines est présentée. Le texte est le moyen de communication le plus largement utilisé et nous avons proposé un algorithme qui assure l'intégrité du document. Une nouvelle technique est avancée qui crée un tatouage numérique basé sur le contenu du document et l'incruste sans changer le contenu du document. Comme le mot-clé utilisé pour l'algorithme est choisi au hasard dans une liste de mots, cela améliore la robustesse de cet algorithme. En outre, le décalage alternatif ajoute à la sécurité et à l'imperceptibilité sans ajouter de complexité. Pour authentifier et prouver l'intégrité du document, le tatouage numérique peut être

facilement extrait et vérifié contre toute altération. Le contenu du document reste inchangé, ce qui assure l'un des avantages de cet algorithme.

Auteur(s)	La fonctionnalité de tatouage numérique utilisée.	Texte-image	Avantages	Limitations
Huang et kot (2001) [11]	Modification de l'espace des mots	Anglais	Robuste contre les interférences	Faible capacité
Kim et al. (2003) [12]	Déplacement de mots	Anglais	Marquage aveugle, haute imperceptibilité	Faible capacité Haute complexité
Young et Kyung(2004)	Modification de l'espace des mots	Anglais	Watermarking Capacité plus élevée que le décalage de ligne et de mot	Pas robuste contre le bruit
Shirali-Shahreza (2006) [13]	Décalage de points.	Persian et arabe	Grande capacité	Pas robuste contre les attaques d'image
Davarzani et Yaghmaie (2009) [14]	Changer la pente	Arabe	Marquage aveugle	Pas robuste contre les attaques d'image
Kim et Oh (2004) [2]	Modifier l'histogramme de direction des bords.	Coréen, Chinois, Anglais	Appliqué dans différentes langues	consommation du temp
Tirandaz et Darvaziany. (2009)	Changer la pente	Coréen, Chinois, Anglais	Appliqué dans différentes langues	Pas robuste contre les attaques d'image

Tableau 4.1 :Comparaison des méthodes de tatouage d'image-texte dans le domaine spatial

4.3 La base d'images

Il est important d'évaluer un algorithme de tatouage numérique d'image sur des images différentes. Les images devraient couvrir une large gamme de contenus et de types. Nous avons utilisé 3 images fournies dans la base de données de Fabien Petitcolas [14] comme base standard d'évaluation des algorithmes de tatouage numérique d'image.

« Singe » « Bateau de pêche» « Lenna »

Figure 11:montre certaines des images d'échantillon utilisées dans les expériences**[14]**

Images logo

une image de logo noir et blanc (1 bit par pixel). Il s'agit de l'image de logo "TEST" qui mesure 64 × 64. Une image de logo en noir et blanc ont été choisies pour maintenir une longueur de filigrane gérable.

L'images de logo et montré dans la Figure 12.

Figure 12:Image logo « TEST »

4.4 Environnement et outils de développement

4.4.1 Outils matériels

Les outils matériels utilisés pour le développement de notre application sont les suivants :

PC : On a utilisé un PC pour la réalisation de l'application.

- Mémoire centrale : 8.00 GB
- Processeur : Intel(R) Core (TM) i5-4300HQ CPU @ 2.50GHz.
- Disque dur : 256 GB SSD
- Système d'exploitation : Windows 10 Professionnel - 64 bits

4.4.2 Outils logiciels

Nous allons utiliser le langage de programmation Python dans l'environnement de développement intégré (PyCharm) pour mettre en place note méthode proposer nous allons directement travailler sur les pixels d'image par l'utilisation des bibliothèques suivante :

a. La bibliothèque opencv

La très puissante bibliothèque opencv (https://opencv.org) permet d'effectuer des traitements particulièrement effficaces sur des images et des vidéos. En particulier, elle implémente des algorithmes préentraînés par exemple pour le traitement des pixels. Ce prétraitement interne permet d'avoir accès aux algorithmes les plus performants du moment dans une version optimisée (une CPU suffit alors que souvent un GPU est requis pour de gros calculs).

b. La bibliothèque numpay

La bibliothèque **numpy** (http://www.numpy.org/) permet d'effectuer des calculs numériques avec Python. Elle introduit une gestion facilitée des tableaux de nombres.

c. La bibliothèque pywavelets

En particulier, elle implémente des algorithmes de domaine fréquentiel ou le domaine des transformées come DCT DWT.

4.5 Evaluation des algorithmes de tatouage numérique d'image (DCT) (DWT)

4.5.1 Évaluation de l'imperceptibilité des images après l'insertion de filigrane numérique :

a. Basée sur SSIM

Cette partie présente une comparaison en termes d'imperceptibilité et de robustesse entre les performances du tatouage optimisé par l'algorithme (DCT) et l'algorithme (DWT)

Images	DWT	DCT
Singe	0.9939346494108038	0.9791995644133354
Bateau de pêche	0.9815328439970166	0.9448550854692739
Lenna	0.8469821123085007	0.9418588227255881

Tableau 4.3: SSIM entre les images Singe, Bateau de pêche, Lenna

Les chiffres indiquent les mesures de similarité (SSIM) entre les images originales et leurs versions transformées en utilisant les techniques de transformation en ondelettes discrètes (DWT) et de transformation en cosinus discrètes (DCT). La similarité est généralement mesurée par une valeur proche de 1 indique une forte similarité.

Pour l'image "Singe", la similarité entre l'image originale et sa version transformée est de 0.9939 avec DWT et de 0.9792 avec DCT.

Pour l'image "Bateau de pêche", la similarité entre l'image originale et sa version transformée est de 0.9815 avec DWT et de 0.9449 avec DCT.

Pour l'image "Lenna", la similarité entre l'image originale et sa version transformée est de 0.8470 avec DWT et de 0.9419 avec DCT.

Ces mesures indiquent à quel point les images transformées sont similaires aux images originales après l'application des transformations DWT et DCT. Une valeur élevée de similarité suggère que la transformation a préservé de manière efficace les caractéristiques visuelles de l'image originale.

b. Basée sur Histogramme : L'image « Lenna »

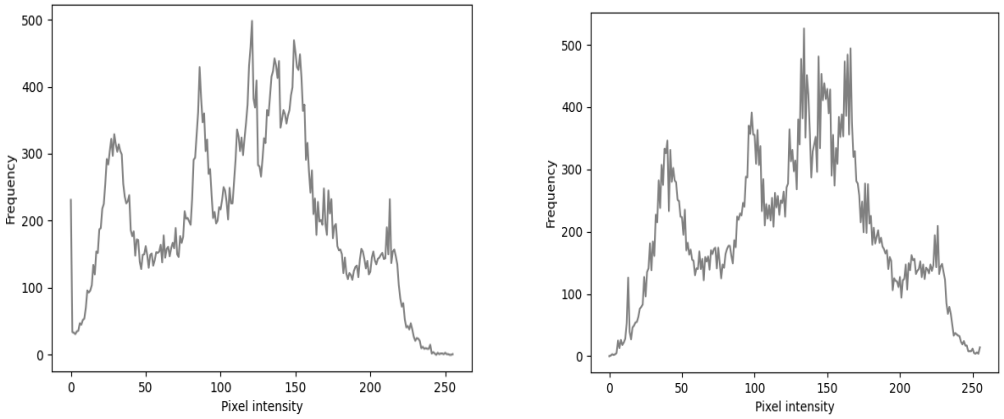


Figure 13:Histogramme de l'image « Lenna » avant et après l'insertion de filigrane avec l'utilisation de (DCT)

L'insertion d'un filigrane dans une image peut avoir un impact sur son histogramme, qui représente la distribution des niveaux de couleur ou de luminosité. Avant l'insertion du filigrane, l'histogramme de l'image est généralement uniforme, avec une répartition équilibrée des valeurs de pixels. Cela signifie que les différentes zones de l'image ont des intensités similaires.

Cependant, après l'insertion du filigrane, l'histogramme de l'image peut présenter des modifications significatives. Les valeurs de pixels correspondant au filigrane peuvent créer des pics ou des creux dans l'histogramme, en fonction de la manière dont il est intégré. Ces variations peuvent être perceptibles visuellement, car elles modifient la répartition des intensités dans l'image.

En comparant les deux histogrammes, on peut observer des différences au niveau de la répartition des intensités. Les zones contenant le filigrane peuvent afficher des valeurs de pixels distinctes, ce qui crée des variations dans l'histogramme. Cependant, il est important que ces variations soient suffisamment subtiles pour ne pas compromettre la qualité visuelle de l'image.

En résumé, l'histogramme de l'image avant l'insertion du filigrane est généralement uniforme, tandis que l'histogramme après l'insertion du filigrane peut présenter des variations dues à la présence du filigrane. L'analyse comparative de ces histogrammes peut aider à évaluer l'impact visuel de l'insertion du filigrane sur l'image.

c. L’image « singe »

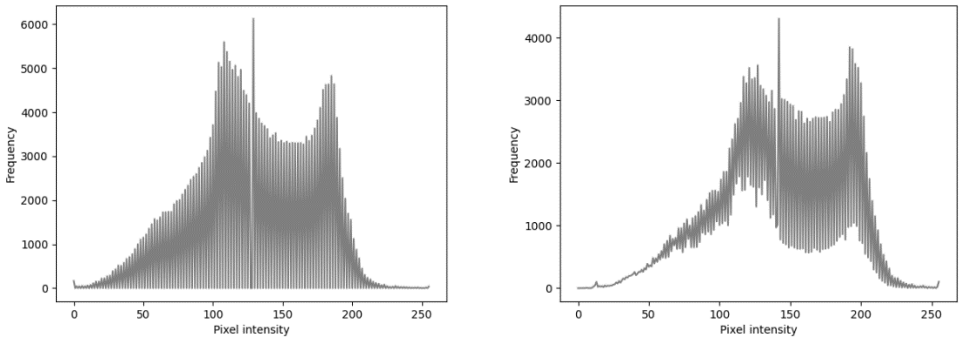


Figure 14:(A) histogramme de l’image original « singe »(B) histogramme de limage apprêt l’insertion de filigrane avec l’utilisation de (DWT)

4.6 L’approche proposée

4.6.1 Algorithme de tatouage numérique d'image basé sur la transformée en ondelettes discrètes et la transformée en cosinus discrète

a. La méthode d’insertion de tatouage numérique

C’est une algorithme de tatouage numérique d'image basé sur la transformée en ondelettes discrètes et la transformée en cosinus discrète.

L'algorithme proposé applique une transformée en ondelettes discrètes à un niveau sur l'image de couverture et divise les sous-bandes LH1 et HL1 résultantes en blocs de 4x4. Une décomposition en valeurs singulières est ensuite appliquée à chaque bloc, et le tatouage est intégré dans les valeurs singulières de chaque bloc. Les bits MSB et LSB du tatouage sont séparés en deux images, et une transformation en cosinus discrète est appliquée à chaque image. Les coefficients DCT résultants sont ensuite intégrés dans les valeurs singulières des sous-bandes LH1 et HL1.

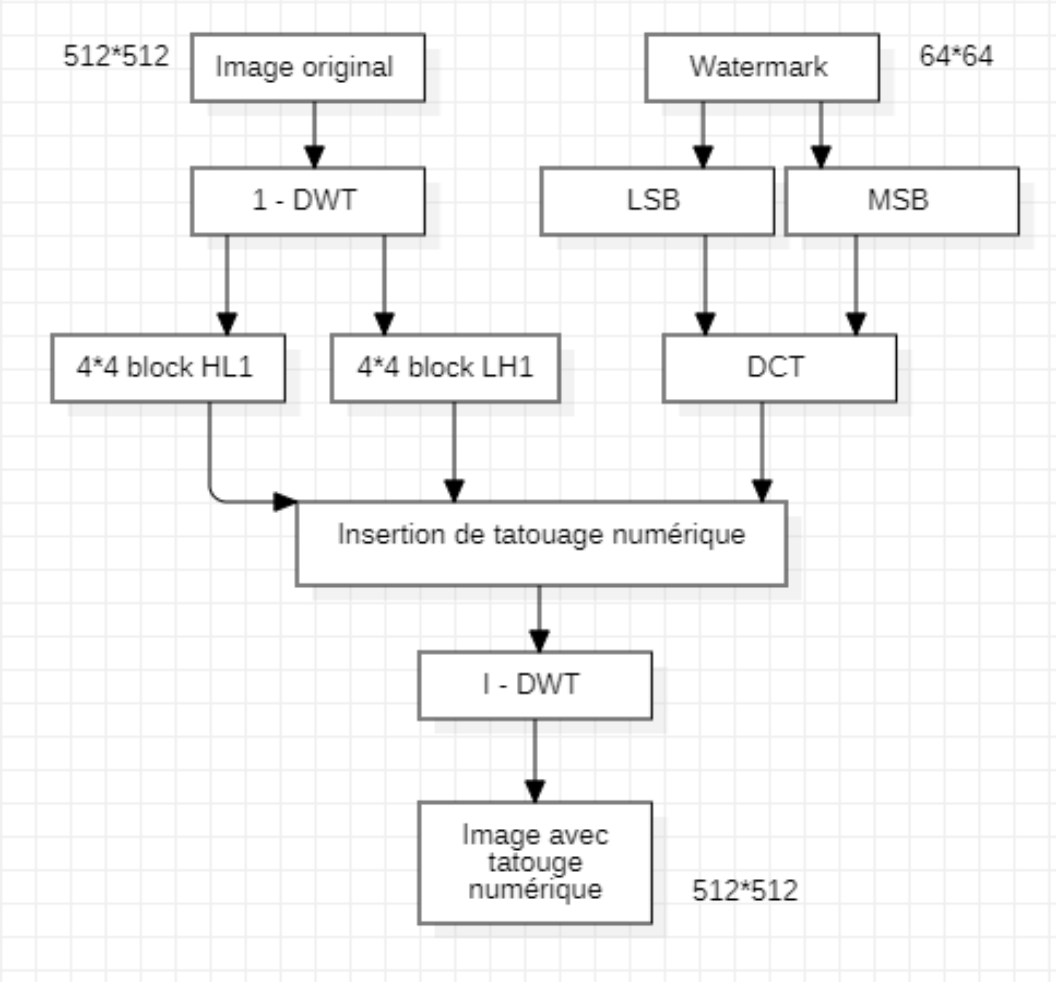


Figure 15:Notre méthode d'insertion de tatouage numérique

Algorithme de notre méthode d'insertion de tatouage numérique

Début d'algorithme

Variables

Image de couverture
Image de filigrane

Appliquer une transformée en ondelettes discrètes à un niveau sur l'image de couverture.
Diviser les sous-bandes LH1 et HL1 résultantes en blocs de 4x4.
Appliquer une décomposition en valeurs singulières à chaque bloc.
Intégrer le tatouage dans les valeurs singulières de chaque bloc.
Séparer les bits MSB (Most Significant Bit) et LSB (Least Significant Bit) du tatouage en deux images distinctes.
Appliquer une transformation en cosinus discrète à chaque image.
Intégrer les coefficients DCT résultants dans les valeurs singulières des sous-bandes LH1 et HL1.

Fin de l'algorithme

b. La méthode d'extraction de tatouage numérique

C'est un algorithme d'extraction de tatouage numérique d'image. Il utilise les bibliothèques PyWavelets et SciPy pour effectuer une transformée en ondelettes discrètes et une transformée en cosinus discrète. Le tatouage est intégré dans les valeurs singulières de blocs 4x4 obtenus à partir des sous-bandes LH1 et HL1 de l'image de couverture. La fonction "Watermark_Extraction" prend en entrée des blocs, key1 et key2 et extrait le filigrane en utilisant une décomposition en valeurs singulières. La fonction "Merge_W1_W2" fusionne le filigrane extrait de W1 et W2 et le renvoie sous forme de tableau. Enfin, le filigrane extrait est enregistré sous forme d'image avec le nom "Extracted_Watermark.png".

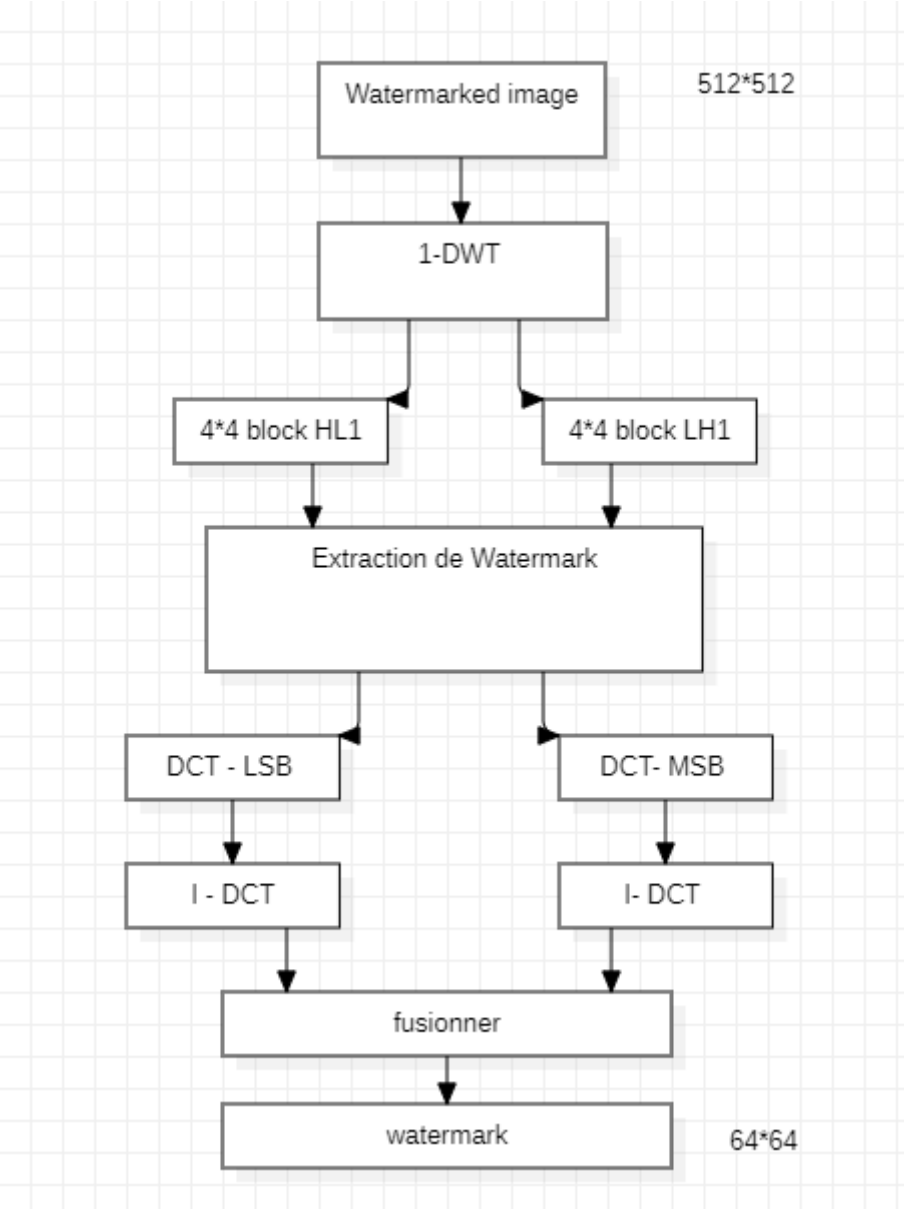


Figure 16:Notre méthode d'extraction de tatouage numérique

Algorithme de notre méthode d'extraction de tatouage numérique

Début d'algorithme
Variables
Image avec filigrane

Effectuer une transformée en ondelettes discrètes (DWT) sur l'image de couverture.
Diviser les sous-bandes LH1 et HL1 résultantes en blocs de taille 4x4.
Intégrer le tatouage dans les valeurs singulières de chaque bloc.
Utiliser la fonction "Watermark_Extraction" en fournissant les blocs, key1 et key2 en entrée.
Appliquer une décomposition en valeurs singulières pour extraire le filigrane.
Utiliser la fonction "Merge_W1_W2" pour fusionner le filigrane extrait de W1 et W2.
Enregistrer le filigrane extrait sous forme d'image avec le nom "Extracted_Watermark.png".

Fin de l'algorithme

c. La phase de générer un tatouage numérique

Notre méthode commence par implémenter un texte par les paramètres suivant :

La taille de texte, le type de texte, l'emplacement de texte, la direction du texte et la taille de l'image.

4.7 Résultats expérimentaux

Dans cette partie, les résultats expérimentaux sont menés pour valider les performances du notre schéma proposé. Une variété d'expériences ont été menées pour évaluer les performances du schéma proposé, et pour comparer ses performances à celles de schémas similaires. Les critères utilisés pour valider les performances de notre schéma proposé sont le SSIM (La similarité de structure) et l'histogramme.

4.7.1 Évaluation de l'imperceptibilité des images après l'insertion de filigrane numérique avec notre schéma proposer

A. Basée sure SSIM

Les images	Le schéma proposer
Singe	0.9818324199740478
Bateau de pêche	0.9815328439970166
Lenna	0.9469821123085007

Tableau 4.4 : SSIM entre les images (A) et (B)

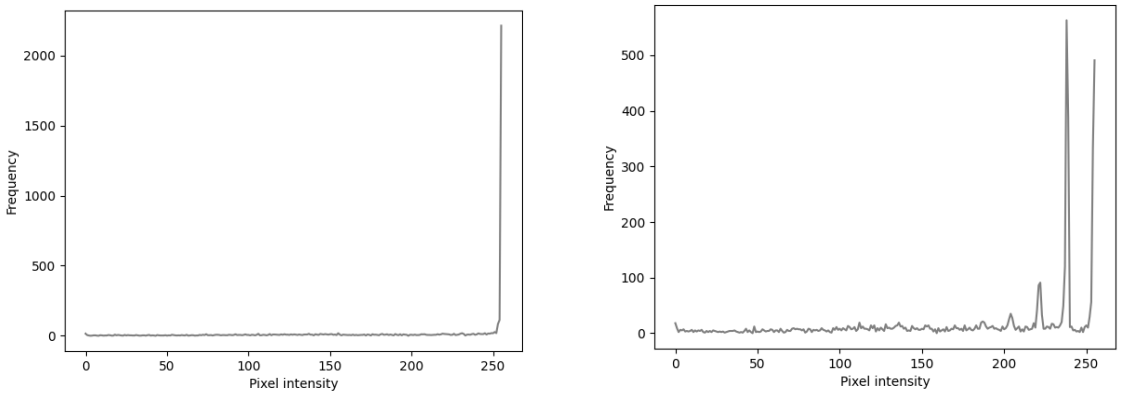
Les valeurs de la mesure SSIM dans le tableau 4.3 obtenues pour les différentes images utilisées indiquent la grande similitude entre les images tatouées et les images originales correspondantes.

4.7.2 Évaluation de la similitude de tatouage numérique avant et après l'extraction de tatouage numérique avec notre schéma proposer

a. Basée sur SSIM

On remarque que la mesure de SSIM est très élevée (SSIM=0.8735664628635798) ce qui montre que la qualité de filigrane est excellente, et ce, malgré le choix de la sous bande de basse fréquence, qui crée des distorsions à l'image lorsque le filigrane est inséré. Ceci indique que le choix de notre méthode, contribue fortement aux performances requises d'imperceptibilité du tatouage. Avec notre schéma proposer

b. Basée sure histogramme



(A) **(B)**

Figure 17:(A) histogramme de tatouage numérique original (B) histogramme de tatouage numérique apprêt l'extraction de tatouage numérique de limage

4.8 Conclusion

Le travail présenté dans ce mémoire s'inscrit dans le cadre de veille de sécurité des documents via le tatouage numérique et plus précisément la détection des informations cachées dans les images fixes. Dans le cadre de notre travail, nous avons proposé une méthode de tatouage numérique universelle dans le domaine fréquentiel basée DCT et DWT. Cette dernière consiste à insérer et extrait d'un message caché dans une image, seul cette présence est déterminée.

Pour valider notre méthode de stéganalyse, nous avons récupéré la même base d'images et nous avons utilisé deux critères le SSIM et l'histogramme pour évaluer notre travail.

Conclusion générale et perspectives

La dissimulation d'informations à travers la stéganographie, la cryptographie et le tatouage numérique joue un rôle essentiel dans la protection des données et de la propriété intellectuelle. Chaque technique offre des avantages spécifiques : la stéganographie permet de dissimuler l'existence même d'un message, la cryptographie assure la confidentialité des messages, et le tatouage numérique offre une preuve d'authenticité et de propriété. Il est crucial de développer des méthodes robustes

Dans ce travail, nous avons introduit le concept et les objectifs du tatouage numérique pour la protection des images et la vérification de l'intégrité des données. Le tatouage numérique est une alternative à la cryptographie, offrant une fonctionnalité de sécurité polyvalente, notamment la protection des droits d'auteur, l'intégrité des données et l'authentification. Il est essentiel que le tatouage numérique soit à la fois fragile et imperceptible. Dans ce mémoire, nous avons présenté les notions de base de l'image numérique et de son traitement, en fournissant des définitions clés. Ensuite, nous avons exploré les différentes techniques et méthodes de tatouage numérique existantes, ainsi que les algorithmes de marquage utilisés. Nous avons également étudié les différentes attaques possibles sur les images numériques.

Notre travail reste ouvert et extensible. Nous prévoyons plusieurs extensions à ce travail, dont les principales sont les suivantes :

A. Notre travail ne s'applique que dans le domaine fréquentiel (DCT)(DWT). Nous proposons de compléter le travail pour qu'il s'applique dans le domaine spatial.

B. Nous proposons de compléter le travail pour insérer la date et le jour de l'insertion de tatouage numérique.

Références

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

[2] Y.-W. Kim et I.-S. Oh, «Watermarking text document images using histograms,» *Elsevier,* p. 1243–1251, 2004.

[3] A. A.-A. Gutub, F. Al-Haidari, K. M. Al-Kahsah et J. Hamodi, «E-Text Watermarking: Utilizing 'Kashida' Extensions in Arabic Language Electronic Writing,» *JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE,* vol. 2, n° %11, p. 48.55, 2010.

[4] J. FRIDRICH, Steganography in Digital Media Principles, Algorithms, and Applications, New York,United States: Cambridge University Press, 2009.

[5] M. Tayachi, *Sécurité des images par tatouage numérique et,* Sfax: Université de Tunis El Manar, 2021.

[6] D. Chopra, P. Gupta, G. S. B.C et A. Gupta, «Lsb Based Digital Image Watermarking For Gray Scale Image,» *IOSR Journal of Computer Engineering (IOSRJCE),* vol. 6, n° %11, pp. 36-41, 2012.

[7] A. Naveed, Y. Saleem, N. Ahmed et A. Rafiq, «PERFORMANCE EVALUATION AND WATERMARK SECURITY ASSESSMENT OF DIGITAL WATERMARKING TECHNIQUES,» *Sci.Int.,* vol. 27, n° %12, pp. 1271-1276, 2015 .

[8] O. w. o. t. U. S. Government. [En ligne]. Available: https://www.state.gov/intellectual-property-enforcement/. [Accès le 20 mars 2023].

[9] H. Yang et A. C. Kot, «Text document authentication by integrating inter character and word spaces watermarking,» *IEEE,* vol. 2, n° %123, pp. 955-958, 2004.

[10] K. K. Jabbar et M. B. Tuieb, «Compare Between DCT and DWT for Digital Watermarking in Color Image,» *IISTE,* pp. 22-31, 2015.

[11] Y.-W. Kim, K.-A. Moon et I.-S. Oh, «A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics,» *IEEE,* vol. 1, n° %13, pp. 7695-1960, 2003.

[12] M. H. Shirali-Shahreza et M. Shirali-Shahreza, «A New Approach to Persian/Arabic Text Steganography,» *IEEE,* vol. 6, n° %17, pp. 7695-2613, 2006.

[13] R. D. e. K. Yaghmaie, «Farsi Text Watermarking Based on Character Coding,» chez *International Conference on Signal Processing Systems*, Singapore, 2009.

[14] H. Tirandaz, R. Davarzani, M. Monemizadeh et J. Haddadnia, «Invisible and High Capacity Data Hiding in Binary Text Images Based on Use of Edge Pixels,» chez *International Conference on Signal Processing Systems*, Singapore, 2009.

[15] «Practical Introduction to Frequency-Domain Analysis – MATLAB & Simulink Example – MathWorks United Kingdom,» [En ligne].

[16] D. Huang et H. Yan, «Interword Distance Changes Represented by Sine Waves for Watermarking Text Images,» *IEEE,* vol. 11, n° %112, pp. 1237-1245, 2001.

[17] S. Tyagi, H. V. Singh, R. Agarwal et S. K. Gangwar, «Digital Watermarking Techniques for,» chez *IEEE*, Sultanpur, India, 2016.

[18] «petitcolas.net,» [En ligne]. Available: https://www./steganography/index.html. [Accès le 17 mars 2023].