République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE KASDI MERBAH OUARGLA
Faculté des Nouvelles Technologies de l'Information et de la Communication
Département de l'informatique et Technologies de l'information

Mémoire de Fin d'Études Pour l'Obtention du Diplôme de Master en Informatique

Spécialité : Administration et sécurité des réseaux

Une méthode de tatouage d'image numérique dans le domaine spatial

Présenté par :
Bekhdidja Ikram Et Beddouda Rawane

Soutenue publiquement le 24/06/2024 devant jury composé de :

DR. Benbezziane Mohamed	Président	UKM Ouargla
DR. Eushi Salah	Examinateur	UKM Ouargla
DR. Kahlessenane Fares	Rapporteur	UKM Ouargla

Année universitaire : 2023/2024

REMERCIEMENT

Tout d'abord, nous tenons à exprimer notre profonde gratitude envers **Allah** *pour les innombrables bénédictions et faveurs qui ont éclairé notre chemin tout au long de ce voyage académique.*

Ensuite, nous souhaitons adresser nos plus sincères remerciements à **notre famille**, *qui a été notre rocher solide et notre plus grande source de soutien. Nous sommes particulièrement reconnaissants envers.*

Nous exprimons notre profonde reconnaissance envers notre encadrant , **Mr F.Kahlessenane**, *dont la guidance experte, les conseils précieux et le soutien indéfectible ont été cruciaux pour la réussite de ce travail de recherche.*

Nous tenons également à remercier chaleureusement **les membres du jury** *pour leur temps, leur expertise et leur précieuse contribution à l'évaluation de ce travail. Nos plus sincères remerciements vont également à tous nos enseignants dont la passion pour l'enseignement et le savoir a enrichi notre parcours universitaire et élargi nos horizons académiques.*

Enfin, nous sommes reconnaissants envers tous ceux qui, de près ou de loin, ont contribué à notre formation et à la réalisation de ce projet. Leurs efforts et leur soutien ont été essentiels à chaque étape de notre parcours, et nous leur sommes profondément reconnaissants pour leur précieuse contribution à notre réussite.

Résumé

Ces dernières années, le domaine du tatouage numérique a connu un développement important, tant pour protéger les images que les textes. Cette évolution répond au besoin urgent de renforcer le droit d'auteur sur les documents multimédias, notamment les images, l'audio et la vidéo. Avec l'utilisation croissante des applications numériques, il est devenu nécessaire de mettre en œuvre des solutions avancées pour lutter contre la contrefaçon et la falsification. Dans ce contexte, nos travaux visent à développer une application permettant d'insérer des tatouages numériques dans des images couleur au format RGB. Ces tatouages peuvent être soit des textes, soit des images. L'application est basée sur la méthode LSB du domaine spatial pour l'insertion et l'extraction de tatouages numériques.

Mots clés : Tatouages d'image numériques, Domaine spatial,LSB, L'imperceptibilité.

Abstract

In recent years, there has been significant development in the field of digital tattooing, both to protect images and texts. This development came in response to the urgent need to strengthen copyright in multimedia materials, including images, audio and video. With the increasing use of digital applications, it has become necessary to implement advanced solutions to combat counterfeiting and tampering. In this context, our work aims to develop an application that allows digital tattoos to be inserted into color images in RGB format. These tattoos can be either texts or images. The application is based on the spatial domain LSB method for digital tattoo insertion and extraction.

Keywords : Digital image watermarking, Spatial domain, LSB, Imperceptibility.

ملخص

في السنوات الأخيرة، حدث تطور كبير في مجال الوشم الرقمي، سواء لحماية الصور أو النصوص. وجاء هذا التطور استجابة للحاجة الملحة لتعزيز حق المؤلف في المواد المتعددة الوسائط، بما في ذلك الصور والصوت والفيديو. ومع تزايد استخدام التطبيقات الرقمية، أصبح من الضروري تنفيذ حلول متقدمة لمكافحة التزييف والتلاعب. وفي هذا السياق، يهدف عملنا إلى تطوير تطبيق يسمح بإدراج الوشم الرقمي في الصور الملونة بتنسيق .RGB يمكن أن تكون هذه الأوشام إما نصوصًا أو صورًا. يعتمد التطبيق على طريقة LSB في المجال المكاني لإدراج واستخراج الوشم الرقمي

الكلمات المفتاحية: الوشم الرقمي، المجال المكاني، ،LSB عدم القدرة على الإدراك.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

Dans notre ère dominée par la technologie numérique, les images digitales exercent une influence considérable sur notre quotidien, allant de la photographie personnelle aux données cartographiques satellites, en passant par la surveillance environnementale et les avancées scientifiques. Elles jouent un rôle essentiel en tant que véhicules d'information, touchant de nombreux secteurs d'activité.

Cependant, avec la multiplication et le partage des images sur les réseaux, des préoccupations émergent quant à la sécurité de ces données visuelles, qui peuvent contenir des informations sensibles ou confidentielles. Le risque de manipulation ou de falsification des images est une source croissante d'inquiétude. Pour relever ces défis, le concept de tatouage numérique se profile comme une solution prometteuse. Il s'agit d'incorporer des marques invisibles ou difficiles à détecter directement dans les images, offrant ainsi une protection robuste contre la falsification et la manipulation non autorisée.

Le tatouage numérique présente une flexibilité et une efficacité remar-

quables pour sécuriser les images digitales dans divers domaines tels que la photographie, l'édition, la médecine et l'industrie.

Ce mémoire vise à développer une application de tatouage numérique délicate spécialement conçue pour les images BMP et PNG. Cette application se fonde sur la méthode du dernier bit significatif (LSB) afin de garantir l'authentification et l'intégrité des images.

Ce travail est structuré en trois chapitre :

- ➢ Le chapitre 1 : aborde les fondements des images numériques, en explorant leurs caractéristiques, leurs types et leurs formats. Nous introduisons également des concepts clés dans le domaine du traitement d'images numériques.
- ➢ Le chapitre 2 : traite du tatouage numérique, abordant son principe général, ses contraintes, ses techniques et les attaques courantes, ainsi que ses divers domaines d'application. Nous clôturons ce chapitre en examinant les méthodes d'évaluation de la qualité des images numériques.
- ➢ Le chapitre 3 : Ce chapitre est consacré à la présentation de la conception et de la réalisation de notre application de tatouage numérique. Nous détaillons les techniques et les outils utilisés dans ce travail. Nous utilisons notamment l'algorithme LSB pour appliquer le tatouage fragile sur les images codées en 24 bits. De plus, nous présentons les résultats expérimentaux obtenus grâce à cette application.

CHAPITRE 1

L'IMAGE NUMÉRIQUE

1.1. Introduction

La transition vers l'ère numérique marque un point d'inflexion dans l'histoire humaine, caractérisé par une transformation profonde de notre approche de l'information visuelle. L'avènement rapide et généralisé des technologies numériques a engendré une prolifération sans précédent de l'image numérique dans notre quotidien, la rendant omniprésente dans notre société grâce à la diffusion généralisée des dispositifs numériques tels que les smartphones, les ordinateurs, les tablettes et les téléviseurs intelligents. Cette révolution technologique ne se limite pas à la simple représentation de pixels sur un écran ; elle repose sur des avancées majeures dans le domaine de la numérisation, de la compression de données et de la visualisation graphique.

L'image numérique, dans sa forme la plus élémentaire, est une représentation visuelle codée sous forme de données binaires. Cette représentation numérique permet une manipulation aisée et une transmission rapide de l'information visuelle à travers divers supports et réseaux.

Dans ce chapitre, notre objectif est de clarifier et d'expliquer des termes et concepts fondamentaux relatifs aux images numériques. Nous visons également à acquérir une compréhension approfondie de la manière dont les images sont représentées sur les ordinateurs, ainsi que des différentes caractéristiques qui les différencient. De plus, nous explorerons les nombreuses manipulations et traitements qui peuvent être appliqués à ces images.

1.2. Généra1ités et Notions de Base sur l'image

1.2.1. Définition de l'image numérique

Une image numérique est une représentation binaire d'informations visuelles, telles que des dessins, des images, des graphiques, des logos ou des images vidéo individuelles. Ces images sont composées de pixels connus aussi sous le nom de Picture Elements,les éléments fondamentaux

de l'image, organisés en une structure en grille. Chaque pixel contient des données sur sa couleur, sa luminosité et parfois sa transparence. Les images numériques peuvent être capturées à l'aide d'appareils photo numériques, de scanners ou générées par des logiciels informatiques. Elles jouent un rôle crucial dans divers domaines, notamment la photographie, le graphisme, la production vidéo et l'imagerie médicale.

D'un point de vue technique, une image numérique se présente comme une matrice de $X \times Y$ pixels, chaque pixel de l'image est habituellement lié à une tonalité de gris s'il s'agit d'une image monochrome, ou à des valeurs représentant les éléments fondamentaux de la couleur pour une image en couleur.En fonction du modèle colorimétrique utilisé, tel que l'espace RGB (rouge, vert, bleu), ces valeurs définissent la couleur et les caractéristiques visuelles du pixel. En outre, chaque pixel est précisément situé dans l'image grâce à ses coordonnées spatiales x et y, ce qui permet de définir sa position exacte dans la grille de pixels qui forme l'image. La figure 3.8 présente un exemple concret d'une image numérique de dimensions $X \times Y$ pixels.

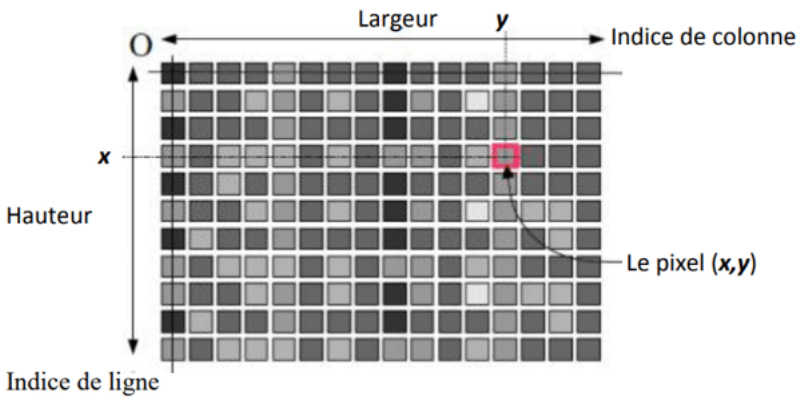


Figure 1.1 – Une image numérique.

1.2.2. Caractéristiques d'une image numérique

On peut décrire une image numérique comme une collection de données organisées caractérisées par les critères suivants :

1.2.2.1. pixels :

Ils sont les plus petits éléments contrôlables d'une image numérique. Ce sont les éléments de base des images numériques, disposés en une formation en grille pour former l'image complète. Chaque pixel contient des informations sur sa couleur, sa luminosité et parfois sa transparence.C'est aussi l'unité utilisée pour spécifier les définitions d'affichage (largeur × hauteur)[2].

1.2.2.2. Dimension

La dimension d'une image numérique fait référence à sa taille en pixels, mesurée en largeur et en hauteur. Par exemple, une image peut avoir une dimension de 1920 pixels de large sur 1080 pixels de haut, ce qui est souvent exprimé comme "1920x1080". Ces chiffres représentent respectivement le nombre de pixels horizontaux et verticaux présents dans l'image.

1.2.2.3. Résolution

La résolution d'une image numérique fait référence à sa capacité à reproduire des détails avec netteté et clarté, que ce soit lors de sa visualisation sur un écran ou lors de son impression. Elle est exprimée en nombre de pixels par unité de longueur, généralement en pixels par pouce (ppp) ou dots per inch (dpi). Une résolution plus élevée signifie qu'il y a plus de pixels par unité de mesure, ce qui permet de capturer plus d'informations visuelles et de produire une image plus détaillée.

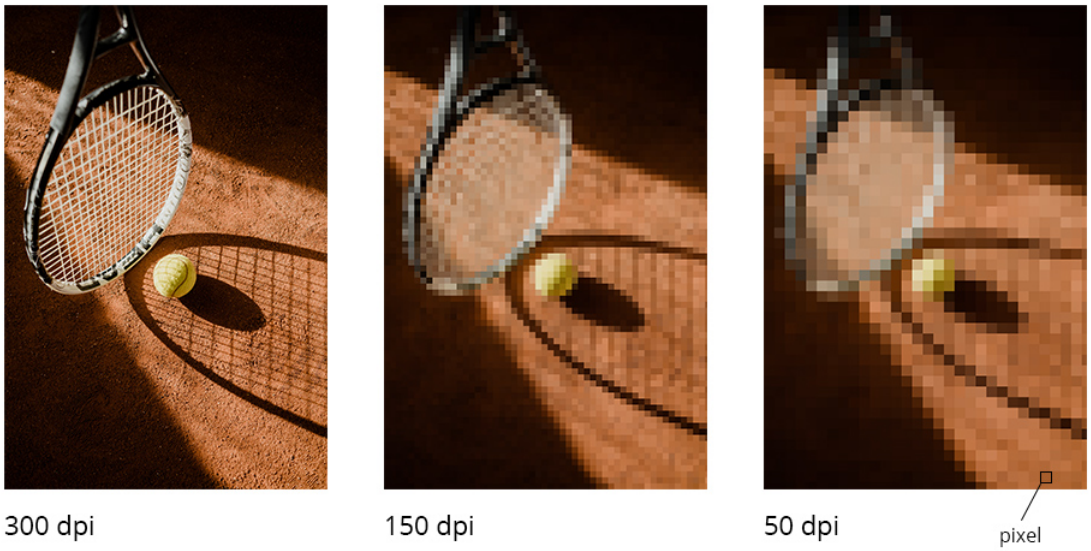


Figure 1.2 – Résolution d'une image.

1.2.2.4. Histogramme :

Un histogramme d'une image numérique est une représentation graphique qui montre la distribution des intensités de luminosité ou des couleurs dans l'image. Pour une image en niveaux de gris, l'histogramme affiche le nombre de pixels pour chaque niveau de luminosité, allant généralement de 0 (noir) à 255 (blanc) dans une échelle de gris de 8 bits. Pour une image couleur, il y a généralement trois histogrammes distincts, un pour chaque composante de couleur (rouge, vert et bleu dans le cas de l'espace colorimétrique RVB).

1.2.2.5. Luminosité :

La luminosité d'une image numérique se réfère au niveau de clarté des différents points qui la composent. Elle peut également être décrite comme la mesure de la quantité de lumière émise ou réfléchie par la surface des objets dans l'image, en rapport avec leur taille apparente. Pour certains contextes, le terme "luminance" est utilisé pour décrire cet aspect, remplaçant ainsi le terme "brillance" qui fait référence à la brillance ou à l'éclat d'un objet spécifique dans l'image. Une bonne luminance se caractérise par [3] :

— Des images lumineuses (brillantes).

— Un bon contraste : il faut éviter les images où la gamme de contraste tend vers le blanc ou le noir, ces images entraînent des pertes de détails dans les zones sombres ou lumineuses.

— L'absence de parasites.

1.2.2.6. Contraste :

Le contraste dans une image numérique se réfère à la différence entre deux parties distinctes de l'image, notamment entre les zones sombres et les zones claires. Ce contraste est déterminé en comparant les niveaux de luminance de ces deux zones de l'image. Si $L1$ et $L2$ sont les degrés de luminosité respectivement de deux zones voisines $A1$ et $A2$ d'une image, le contraste C est défini par le rapport [3] :

$$C = \frac{L1 - L2}{A1 - A2} \tag{1.1}$$

1.2.2.7. Contours et textures :

Les contours délimitent les objets présents dans l'image, marquant la séparation entre deux régions où les niveaux de gris des pixels présentent une variation notable. Quant aux textures, elles détaillent la structure et la composition de ces régions. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différente[3].

1.3. Les différents types d'images numériques

Dans le domaine des images numériques, le mode de représentation est une distinction essentielle qui divise les images en deux principales catégories : les bitmaps et les images vectorielles. Les bitmaps, qui comprennent les images binaires, en niveaux de gris et en couleurs, sont composées de pixels organisés dans une grille, tandis que les images vectorielles utilisent des formes géométriques définies mathématiquement.

1.3.1. les bitmaps

Les images au format raster sont compilées en utilisant un nombre spécifique de pixels - de minuscules points colorés individuellement qui se réunissent pour former l'image complète. Ainsi, une image raster est essentiellement une matrice bidimensionnelle de pixels [4].

1.3.1.1. Les images binaires :

Les images binaires ne contiennent que des éléments composés de deux valeurs de pixel, 0 et 1. Dans ce contexte, 0 représente le noir complet tandis que 1 représente le blanc total [4].

Figure 1.3 – Image codée en noir et blanc.

1.3.1.2. Image en niveaux de gris :

Également appelée image d'intensité, en niveaux de gris ou de niveaux de gris. Un tableau de classe uint8, uint16, int16, single ou double dont les valeurs de pixel spécifient les valeurs d'intensité.
Pour les tableaux single ou double, les valeurs varient de [0, 1]. Pour uint8, les valeurs varient de [0,255]. Pour uint16, les valeurs varient de [0, 65535]. Pour int16, les valeurs varient de [-32768, 32767][5].

Figure 1.4 – Image codée en niveaux de gris.

1.3.1.3. Image couleur (ou RGB)

Également appelée image RVB. Une image en couleur vraie est une image dans laquelle chaque pixel est spécifié par trois valeurs, une pour chacune des composantes rouge, bleue et verte du scalaire du pixel.
Tableau de dimensions M par n par 3 de classe uint8, uint16, single ou double dont les valeurs de pixel spécifient les valeurs d'intensité. Pour les tableaux single ou double, les valeurs varient de [0, 1]. Pour uint8, les valeurs varient de [0, 255]. Pour uint16, les valeurs varient de [0, 65535][5].

Figure 1.5 – Image codée en couleurs

1.3.2. les images vectorielles

Les images vectorielles sont constituées d'objets géométriques (lignes, courbes, cercles et polygones) exprimés à l'aide de formules mathématiques appelées trajectoires. Ces trajectoires relient un point à un autre pour former des formes complètes. Elles sont définies mathématiquement plutôt que par des pixels individuels [4].

Quelques caractéristiques des images vectorielles :

1. La possibilité de modifier la taille sans perte de qualité : Les images vectorielles conservent leur netteté lorsqu'elles sont agrandies ou réduites, car elles sont basées sur des équations mathématiques plutôt que sur une grille fixe de pixels.
2. Taille de fichier réduite : Les images vectorielles ont une taille de fichier plus petite que les images raster car elles utilisent des courbes et des zones colorées, ce qui les rend idéales pour le stockage et le transfert en ligne.
3. Impression de haute qualité : Les images vectorielles sont idéales pour l'impression haute résolution, car elles peuvent être redimensionnées à volonté sans perte de qualité, garantissant des résultats nets et professionnels.
4. Polyvalence pour diverses applications : Les images vectorielles trouvent leur utilité dans de nombreux domaines tels que la conception graphique, la création de logos, d'illustrations, d'animations, de graphiques, de typographie, et bien d'autres encore, où la précision et la flexibilité sont primordiales.

1.4. Les formats d'images numériques

1.4.1. Format BMP (bitmap)

Le format BMP, abréviation de "Bitmap Image File", est l'un des formats d'images les plus simples et les plus anciens utilisés sur les ordina-

teurs. Il a été développé par Microsoft pour stocker des images sous forme de données bitmap, où chaque pixel de l'image est représenté par une valeur de couleur définie, et la couleur est codée en RGB (synthèse additive), le format lui-même supportant la palette 256 couleurs que le « True Color »[6]. Elles sont caractérisées par leur structure simple : les données de l'image sont stockées pixel par pixel, ligne par ligne, sans compression, ce qui les rend faciles à manipuler mais souvent plus volumineuses que d'autres formats d'image plus récents.

1.4.2. Graphiques Inter change Format (GIF)

Le format GIF, acronyme de "Graphics Interchange Format", est un format d'image largement utilisé sur Internet, notamment pour les animations et les images à faible résolution. Développé par CompuServe dans les années 1980, le format GIF a été conçu pour permettre l'échange facile d'images sur les réseaux informatiques. le format GIF permet également la création d'animations et de détourages, ce qui en fait un choix polyvalent pour de nombreux types de contenus en ligne [7].

1.4.3. Portable Network Graphique (PNG)

Le format PNG, abréviation de "Portable Network Graphics", est un format d'image largement utilisé sur Internet et dans de nombreuses applications logicielles. Les images PNG sont caractérisées par leur capacité à prendre en charge une large gamme de couleurs, allant des images en niveaux de gris aux images en couleurs vraies. Cette variété permet l'utilisation de 13 profondeurs de couleurs différentes, allant de 1 à 48 bits [8]. Cela permet une reproduction précise des couleurs et convient parfaitement aux applications graphiques exigeantes, telles que la photographie et le graphisme. De plus, le format PNG offre une compression sans perte, ce qui signifie qu'il préserve la qualité de l'image tout en réduisant la taille du fichier. Cela en fait un choix populaire pour les images destinées au web, car il permet des temps de chargement plus rapides sans compromettre la qualité visuelle. En outre, le PNG prend en charge la transparence al-

pha, permettant ainsi des superpositions complexes et des effets visuels avancés, ce qui en fait un choix polyvalent pour une variété d'applications graphiques.

1.4.4. Joint Photographique Expert Group (JPEG)

Le format JPEG, acronyme de "Joint Photographic Experts Group", est l'un des formats d'image les plus répandus et les plus populaires sur Internet et dans le domaine de la photographie numérique. Ce format a été développé dans le but de créer un format d'image capable de compresser efficacement les fichiers tout en préservant une qualité visuelle acceptable. JPEG repose sur un algorithme qui lui permet de réduire significativement le volume des données numériques et il repose sur un processus de compression et de décompression comprenant six étapes allant de la transformation des couleurs au décodage, en passant par le découpage/non construction de blocs de pixels [9]. Les images JPEG sont caractérisées par leur capacité à offrir une compression avec perte, ce qui signifie que certaines informations de l'image sont sacrifiées pour réduire la taille du fichier. Cette compression est réalisée en éliminant les détails moins perceptibles pour l'œil humain, ce qui permet de réduire considérablement la taille des fichiers sans compromettre de manière significative la qualité visuelle de l'image.

1.5. Traitement d'image numérique

Le domaine du traitement d'images numériques représente un secteur fascinant et dynamique de l'informatique et de la technologie. Il couvre une vaste gamme de techniques et d'applications visant à améliorer, analyser et interpréter les images[10].

1.5.1. définition

Le traitement d'images consiste à améliorer les images initiales capturées par des caméras/senseurs embarqués sur des satellites, des sondes spatiales et des avions, ou encore des photographies prises au quotidien,

afin de les rendre utilisables pour diverses applications.

1.5.2. Techniques de traitement d'image

1.5.2.1. Améliorer les photos

Dans le domaine du traitement d'images, les données capturées par les capteurs des satellites sont rectifiées pour corriger les erreurs géométriques et de luminosité des pixels. Cette correction se fait à l'aide de modèles mathématiques appropriés, qu'ils soient déterministes ou statistiques. L'amélioration d'image, quant à elle, vise à améliorer l'apparence visuelle en ajustant les valeurs de luminosité des pixels.
Elle englobe diverses techniques telles que l'amélioration du contraste, la pseudo-coloration et le filtrage du bruit, qui sont utilisées pour mettre en évidence les caractéristiques importantes de l'image.
Bien que le processus d'amélioration n'augmente pas le contenu informationnel des données, il permet de mieux visualiser certaines caractéristiques. Ces techniques d'amélioration, telles que l'étirement de contraste, le filtrage du bruit et la modification de l'histogramme, sont essentielles pour l'extraction de caractéristiques, l'analyse d'images et l'affichage des images[10].

1.5.2.2. segmentation des images

La segmentation d'image est une étape initiale ou préliminaire du traitement de compression d'image. L'efficacité du processus de segmentation réside dans sa rapidité, sa capacité à faire correspondre les formes avec précision et à assurer une meilleure connectivité des formes avec le résultat de la segmentation.
La segmentation fait référence au processus d'identification et d'isolement des surfaces et des régions de l'image numérique correspondant aux unités structurales. La segmentation peut également dépendre de diverses caractéristiques présentes dans l'image, telles que la couleur ou la texture[11].

1.5.2.3. extraction de caractéristiques

Les techniques d'extraction de caractéristiques sont développées pour extraire des caractéristiques dans les images radar à synthèse d'ouverture. Cette technique extrait des caractéristiques de haut niveau nécessaires à la classification des cibles. Les caractéristiques sont des éléments qui décrivent de manière unique une cible, tels que la taille, la forme, la composition, la localisation, etc[10].

1.5.3. Applications de traitement d'images numériques

Les techniques de traitement et d'analyse d'images numériques sont largement utilisées aujourd'hui pour résoudre divers problèmes. De nombreuses outils d'analyse d'images sont disponibles, adaptées à des applications spécifiques et fonctionnent de manière robuste dans des environnements réels. Voici quelques domaines d'application principaux [12] :

— Automatisation de bureau : Reconnaissance optique de caractères (OCR) ; Traitement de fichiers ; Reconnaissance de texte manuscrit ; Reconnaissance de logo et symbole ; Détection de zone d'adresse sur les enveloppes ; etc.

— La biotechnologie médicale : Analyse des électrocardiogrammes (ECG), des électroencéphalogrammes (EEG), des électromyogrammes (EMG) ; Applications cellulaires, tissulaires et tridimensionnelles ; Imagerie médicale et pathologie, analyse des radiographies.

— Télédétection : Utilisée pour le relevé et la gestion des ressources naturelles ; l'estimation liée à l'agriculture, l'hydrologie, les forêts et la minéralogie ; la planification urbaine ; la préservation de l'environnement et la lutte contre la pollution ; et la cartographie.

— Technologie de l'information : Transmission d'images par télécopie, vidéofax ; Conférences vidéo et téléphones vidéo ; etc.

— La sécurité biométrique : Identification des caractéristiques humaines et vérification de l'identité présumée en utilisant des images du visage, de l'iris, de la paume de la main, de l'oreille et des empreintes digitales.

— Météorologie : Prévision météorologique à court terme, détection des changements climatiques à long terme à l'aide de données satellitaires et d'autres données de télédétection ; Analyse des modèles nuageux ; etc.

1.6. Conclusion

Dans ce chapitre, nous avons introduit quelques concepts de base liés au domaine des images numériques, en mentionnant les différentes caractéristiques de l'image et en donnant quelques définitions préliminaires des images numériques, car elles constitueront certainement des points fondamentaux dans la suite de notre travail. Nous avons également parlé du traitement d'image et de certains aspects connexes.

CHAPITRE 2

LE TATOUAGE NUMÉRIQUE

2.1. Introduction

Avec l'avancement rapide de la technologie et la prolifération d'Internet, nous sommes témoins d'une explosion de la quantité d'images numériques stockées et partagées. Cependant, cette facilité de transmission a engendré un besoin crucial de protéger ces images contre la falsification et l'utilisation non autorisée. Pour répondre à ce défi, le domaine du tatouage numérique des images a émergé comme une solution prometteuse. Les médias numériques, qu'il s'agisse d'images, de vidéos ou d'audio, sont désormais des outils essentiels dans divers domaines tels que la médecine et la surveillance satellitaire. Malheureusement, leur facilité de duplication et de manipulation a ouvert la porte à des problèmes de droits d'auteur et d'intégrité des données. Afin de protéger ces médias, il est impératif de mettre en place des systèmes adaptés aux technologies actuelles. Le tatouage numérique est l'une des techniques les plus prometteuses pour répondre à ces défis. Cette technique consiste à incorporer des informations, appelées marques, de manière invisible dans les médias numériques, notamment les images. Ces marques peuvent être utilisées pour diverses fins, allant de la protection des droits d'auteur à la vérification de l'authenticité des données.
Dans ce chapitre, nous explorerons d'abord le concept global du tatouage d'images. Nous aborderons ensuite ses domaines d'application, les différentes techniques employées pour tatouer les images, ainsi que les types d'attaques auxquelles ces techniques peuvent être confrontées.

2.2. Historique du tatouage numérique

L'histoire du tatouage numérique trouve ses racines dans les premiers tatouages sur papier, qui remontent à près de 700 ans. Ces tatouages étaient utilisés dans l'industrie papetière pour marquer la provenance, le format et la qualité du papier, ainsi que pour authentifier les documents. L'importance des tatouages sur papier était cruciale dans un marché où la concurrence entre les fabricants de papier était intense et où la

traçabilité des produits était essentielle. L'analogie entre les tatouages sur papier et le tatouage numérique est évidente. Les premières utilisations du terme "marque d'eau" dans le contexte des données numériques ont été influencées par les tatouages sur papier, tels que ceux trouvés sur les billets de banque et les timbres. Cette connexion entre les deux domaines a jeté les bases conceptuelles du tatouage numérique. Les premières recherches sérieuses sur le tatouage d'images numériques ont émergé dans les années 1990. En 1990, Tanaka et ses collègues ont publié des travaux pionniers dans ce domaine [13], suivis en 1993 par les recherches de Tirkel et al[14]. sur le même sujet. Ces premières études ont jeté les bases théoriques du tatouage numérique, explorant les techniques pour intégrer des informations invisibles dans les médias numériques tout en minimisant la dégradation perceptuelle. À partir de 1995, le tatouage numérique a commencé à attirer une attention croissante de la part de la communauté scientifique et industrielle. Les activités de recherche ont augmenté et de nombreux progrès ont été réalisés dans le développement de méthodes et de systèmes pratiques de tatouage numérique. Depuis lors, le domaine du tatouage numérique n'a cessé de croître, avec de nouvelles avancées technologiques et une diversification des applications, tout en restant un domaine de recherche active avec de nombreux défis à relever.

2.3. Définitions

Le tatouage numérique, également connu sous le nom de filigrane numérique, est une méthode utilisée pour intégrer des informations, également appelées marques, dans un support numérique tel qu'une image, une vidéo, un document audio, ou toute autre donnée numérique. Ces informations peuvent inclure des données de copyright, telles que le nom du propriétaire du fichier et la date de création, un message de vérification sous forme d'un code unique permettant de vérifier l'authenticité du fichier, ainsi que d'autres informations comme des données de géolocalisation ou des informations sur les licences.

L'objectif du tatouage numérique est d'insérer ces marques de manière

à ce qu'elles soient perceptibles ou imperceptibles, sans altérer la qualité visuelle de l'image dans son ensemble[15]. Cette technique est souvent utilisée pour protéger les données multimédias contre la violation du droit d'auteur dans des environnements non sécurisés où la cryptographie ne peut pas être efficacement appliquée [13].Le tatouage numérique s'inscrit dans un ensemble de solutions techniques visant à contrer les défis de sécurité liés aux données numériques. Parmi ces défis, on retrouve la protection des droits d'auteur, la lutte contre la redistribution illégale et la préservation de l'intégrité des données.

2.4. Schéma général du tatouage numérique des images

La technique simple de tatouage numérique se compose de deux modules : le module d'incorporation du tatouage et le module de détection et d'extraction du tatouage. L'incorporation du tatouage intègre le tatouage dans l'image d'origine en utilisant une clé [16].

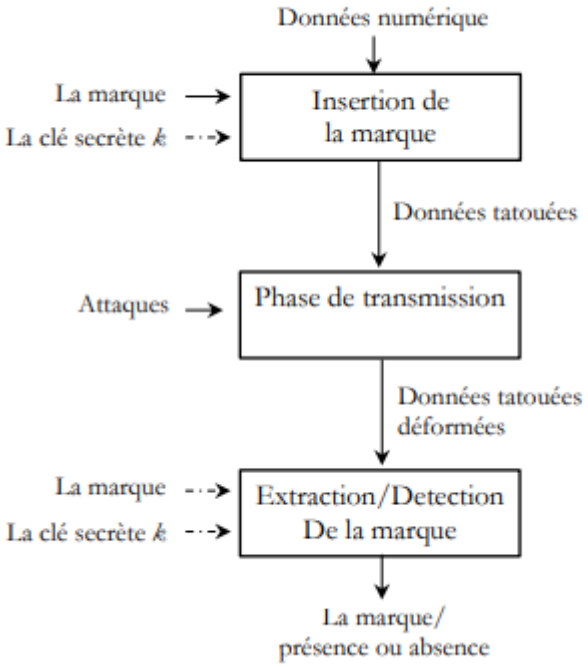


Figure 2.1 – Schéma général d'insertion et d'extraction de tatouage.

2.4.1. Phase d'insertion

L'insertion de tatouages comprend des éléments d'entrée tels que la marque, les données originales, et la clé de sécurité. La marque peut prendre la forme d'une séquence de nombres, d'une séquence binaire de bits, ou même d'une image. La clé est un élément essentiel pour renforcer la sécurité du système de tatouage.

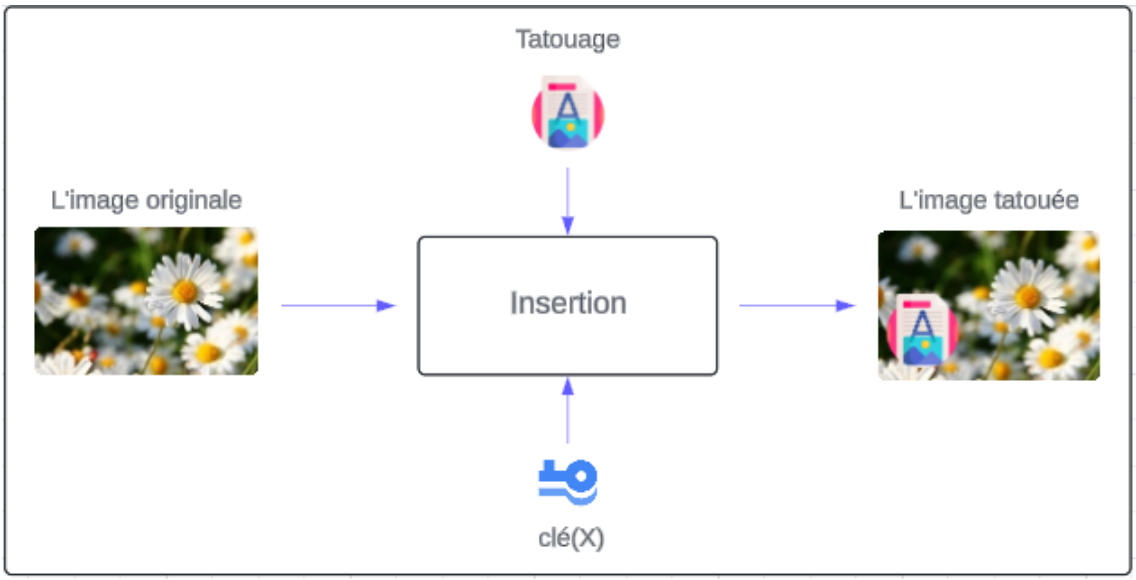


Figure 2.2 – Le schéma général d'insertion d'un tatouage.

☞ Il existe deux types d'insertion : l'insertion additive et l'insertion par substitution.

2.4.1.1. Insertion additive :

Dans cette méthode, la marque est ajouté aux données de l'image d'une manière qui modifie légèrement les valeurs des pixels. Par exemple, la marque peut être additionné aux valeurs de luminance ou de couleur des pixels de l'image. Cette méthode est souvent utilisée lorsque la marque doit être facilement identifiable et extrait de l'image, mais reste robuste contre les altérations.C'est le mécanisme le plus utilisé qui puisse être réalisé sur l'image dans le domaine spatial ou fréquentiel [17].

2.4.1.2. Insertion par substitution :

Cette méthode implique le remplacement d'une partie des données originales par la marque. Cela peut se faire en remplaçant des bits spécifiques dans une séquence binaire ou en remplaçant des pixels dans une image. L'insertion par substitution offre généralement une meilleure capacité d'insertion que l'insertion additive, mais peut être plus visible si elle n'est pas effectuée soigneusement. Cette approche est souvent utilisée lorsque la protection du watermark est une priorité et que la marque doit être difficile à supprimer sans endommager considérablement l'image.

2.4.2. Phase d'extraction

La détection ou l'extraction du tatouage numérique (ou du message M) incrusté dans le document hôte est chargée de vérifier la présence de la signature dans l'image. Si le tatouage est présent, le message pertinent peut être extrait. L'image et la clé privée d'origine peuvent être nécessaires ou non lors de la détection ou de l'extraction.
Il existe plusieurs modes pour l'extraction du tatouage qui spécifient l'information a priori dont le module d'extraction pour la vérification du tatouage. L'utilisation de tel ou tel mode dépendra de l'application visée et des protocoles utilisés.

2.4.2.1. Les schémas aveugles

C'est le seul mode dans lequel on peut véritablement parler d'extraction du tatouage, car ni la connaissance du tatouage ni la connaissance de l'image originale n'est requise. C'est le type d'extraction le plus intéressant, mais aussi le plus difficile à mettre en œuvre [18] [19].

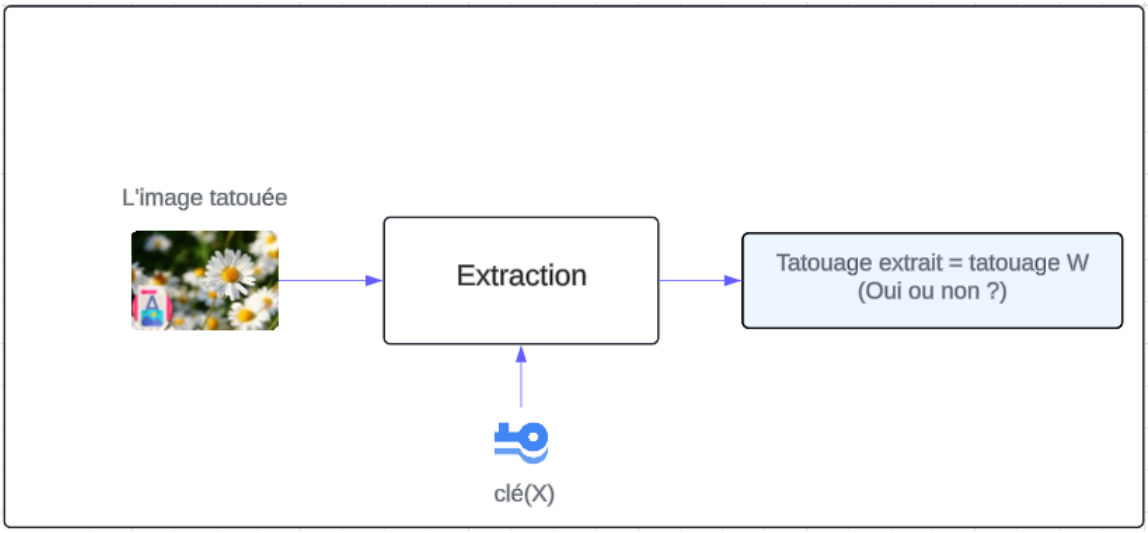


Figure 2.3 – Schéma général d'extraction aveugle d'une tatouage.

2.4.2.2. Les schémas non-aveugles

Les schémas non-aveugles de détection d'un tatouage numérique nécessitent l'image originale ainsi que la clé secrète (privée) [18] [19].

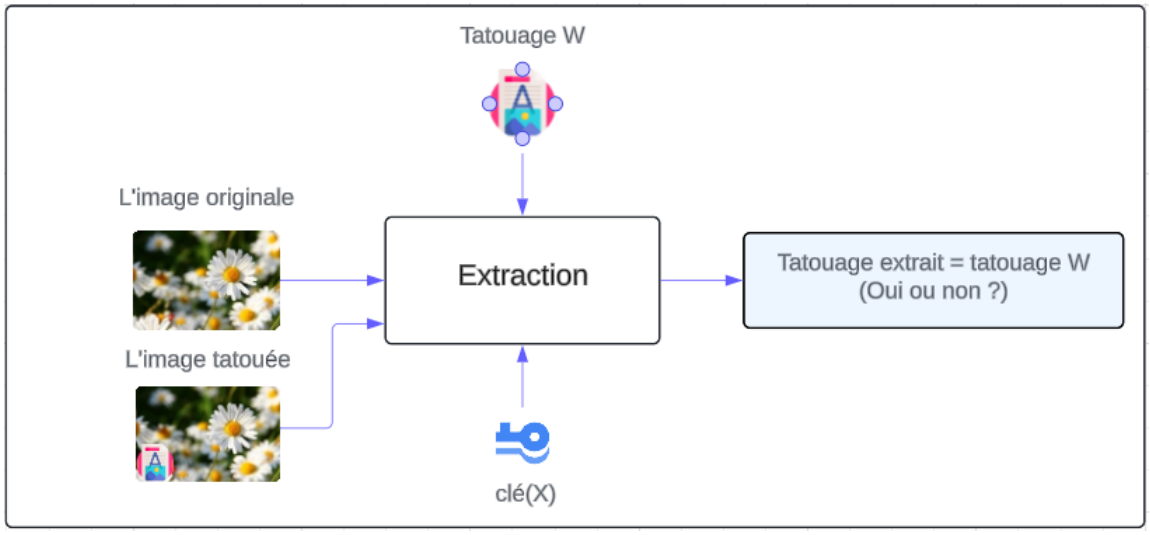


Figure 2.4 – Schéma général d'extraction non-aveugle d'une tatouage.

2.4.2.3. Les schémas semi-aveugles

Quant à l'extraction « semi-aveugle », elle n'utilise pas l'image originale, mais s'appuie plutôt sur quelques informations complémentaires [18] [19].

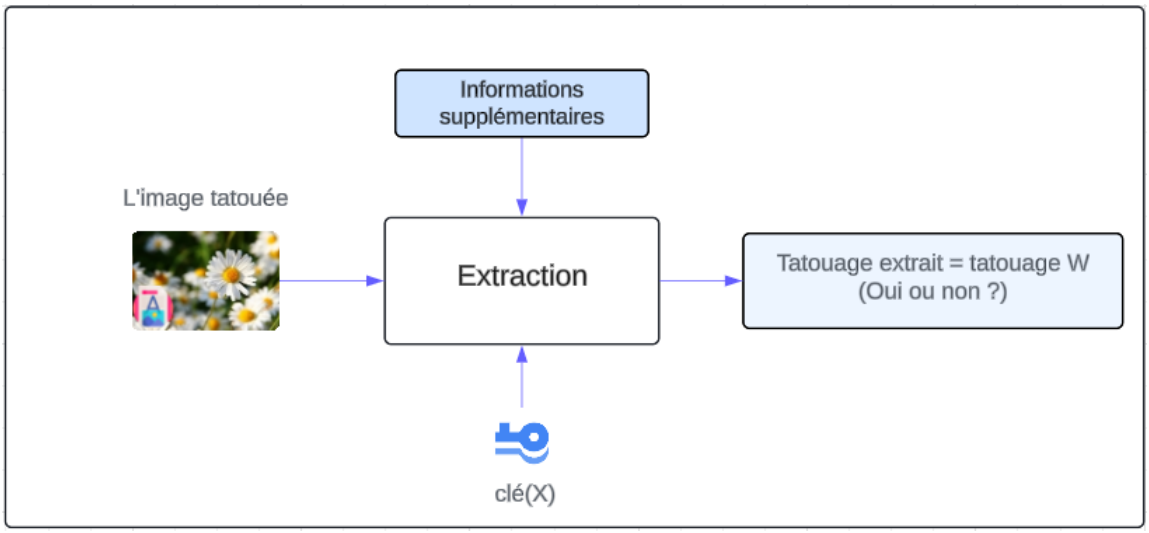


Figure 2.5 – Le schéma général de l'extraction de tatouage semi-aveugle..

2.5. Contraintes du tatouage d'image :

Pour évaluer l'efficacité d'une technique de tatouage ou concevoir un algorithme de tatouage performant, il est crucial de prendre en compte plusieurs facteurs fondamentaux.Ces facteurs sont l'imperceptibilité, robustesse, capacité et la sécurité[20, 21]. L'auteur [22] illustre le compromis entre l'imperceptibilité, la robustesse et la capacité à l'aide d'un triangle, comme le montre la figure

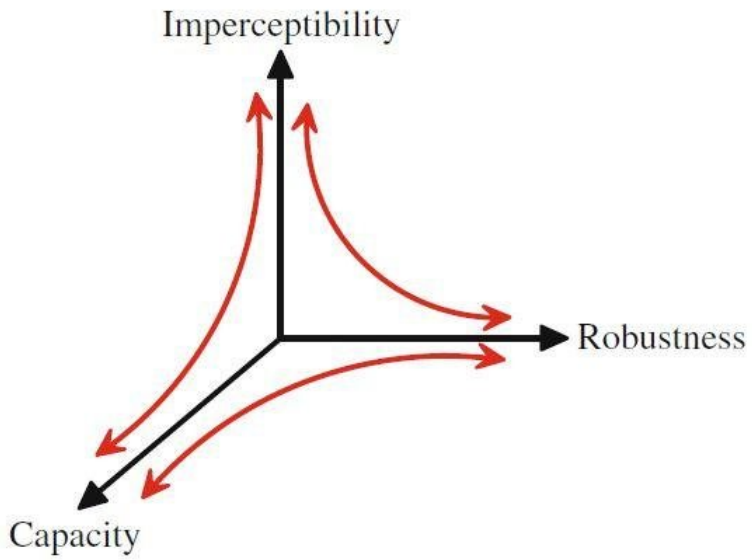


Figure 2.6 – Les Contraintes de tatouage d'image.

2.5.1. Capacité :

La capacité d'un algorithme de tatouage numérique se réfère à la quantité d'informations qu'il peut intégrer. Il est essentiel que cet algorithme dispose d'une capacité d'insertion adéquate pour incorporer la quantité souhaitée de données dans le support numérique. Cette capacité dépend de plusieurs facteurs, notamment la nature du support (image, vidéo, audio), sa taille et sa sensibilité aux altérations perceptibles. Il est crucial de prendre en compte ces contraintes pratiques afin d'assurer une intégration efficace des données sans compromettre l'imperceptibilité du tatouage. Par exemple, dans le cas d'une image hôte de petite taille, il est nécessaire d'être prudent quant à la quantité d'informations insérées, car une surcharge pourrait entraîner une dégradation de la qualité visuelle. De plus, la contrainte d'invisibilité exige que la marque soit de petite taille, facilitant ainsi sa dissimulation. Par conséquent, la taille de la marque joue un rôle crucial dans sa capacité à rester discrète dans l'image hôte.

2.5.2. L'imperceptibilité :

L'imperceptibilité dans le contexte du tatouage numérique implique de dissimuler le message dans des zones de l'image qui ne perturbent ni le confort visuel ni la compréhension du contenu sémantique. Elle repose sur une similitude perceptuelle entre la version originale et la version filigranée de la couverture. Cette propriété vise à préserver la valeur artistique et commerciale du document marqué tout en renforçant sa résistance aux attaques. Elle soulève ainsi la question de la représentation la plus efficace de l'information, c'est-à-dire s'il est préférable de tatouer dans le domaine original de l'image ou dans un domaine transformé.Il est également crucial que le filigrane numérique n'affecte pas la qualité de l'image originale après son application [23].

2.5.3. La robustesse :

La robustesse désigne la capacité d'un algorithme de tatouage à résister aux attaques externes, telles que la compression, le filtrage, le bruit, le recadrage, etc.

2.5.4. La sécurité :

La sécurité est un aspect primordial, en particulier si le tatouage numérique est utilisé pour des applications sensibles comme la protection des droits d'auteur ou l'authentification de documents. L'algorithme doit être conçu pour protéger la marque insérée contre l'extraction non autorisée et garantir l'intégrité du support numérique.. Ainsi, une technique de tatouage est vraiment sûre si la connaissance exacte des algorithmes pour l'insertion et l'extraction de la marque n'aide pas une personne non autorisée d'éliminer ou de détecter la présence de la marque [24].

2.6. Types de tatouage d'image

2.6.1. Selon caractéristiques/robustesse

2.6.1.1. Robuste

Le tatouage robuste est principalement utilisé pour signer les informations de droits d'auteur des œuvres numériques. Le tatouage intégré peut résister aux traitements d'édition courants, au traitement d'image et à la compression avec perte, et le tatouage n'est pas détruit après une attaque et peut toujours être détecté pour fournir une certification. Il résiste à diverses attaques, géométriques ou non géométriques, sans affecter le tatouage intégré[16].

2.6.1.2. Fragile

Le tatouage fragile est principalement utilisé pour la protection de l'intégrité, et doit être très sensible aux changements du signal. Nous pouvons déterminer si les données ont été altérées en fonction de l'état du

tatouage fragile[16].

2.6.1.3. Semi-fragile

Le tatouage semi-fragile est capable de tolérer un certain degré de changement dans une image tatouée, tel que l'ajout de bruit de quantification lors de la compression avec perte[16].

2.6.2. Selon le type de document

2.6.2.1. Le tatouage d'image

Il est utilisé pour dissimuler des informations spéciales dans une image et pour détecter et extraire ultérieurement ces informations spéciales pour l'appartenance de l'auteur[16].

2.6.2.2. Le tatouage vidéo

Il ajoute un tatouage dans le flux vidéo pour contrôler les applications vidéo[16].

2.6.2.3. Le tatouage audio

Ce domaine d'application est l'un des plus populaires et des plus brûlants en raison de la musique sur Internet, des fichiers MP3[16].

2.6.2.4. Le tatouage de texte

Il ajoute un tatouage aux fichiers PDF, DOC et autres fichiers texte pour empêcher les modifications apportées au texte.

Le tatouage est inséré dans la forme de police et l'espace entre les caractères et les espaces entre les lignes[16].

2.6.2.5. Le tatouage graphique

Il intègre le tatouage dans des graphiques générés par ordinateur en 2D ou 3D pour indiquer le droit d'auteur[16].

2.6.3. Selon la perception humaine

2.6.3.1. Tatouage visible

Le tatouage qui est visible dans les données numériques, comme estampiller un tatouage sur du papier, par exemple les chaînes de télévision comme HBO, dont le logo est visiblement superposé dans un coin de l'image télévisée [16].

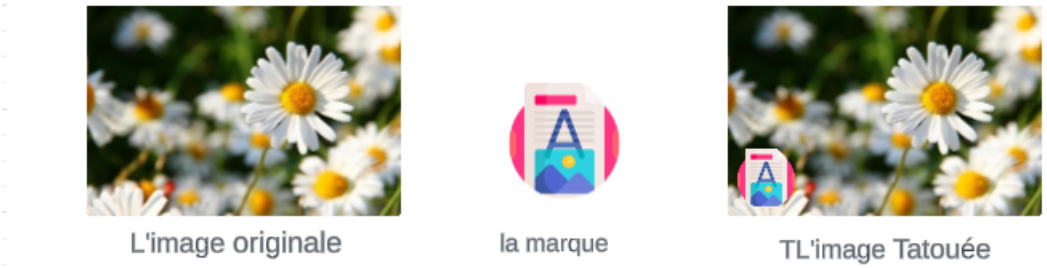


Figure 2.7 – Exemple d'un tatouage visible.

2.6.3.2. Tatouage invisible

Il existe une technologie disponible qui peut insérer des informations dans une image qui ne peuvent pas être vues, mais qui peuvent être interrogées avec le bon logiciel. Vous ne pouvez pas empêcher le vol de vos images de cette manière, mais vous pouvez prouver que l'image qui a été volée était la vôtre, ce qui est presque aussi bon [16].

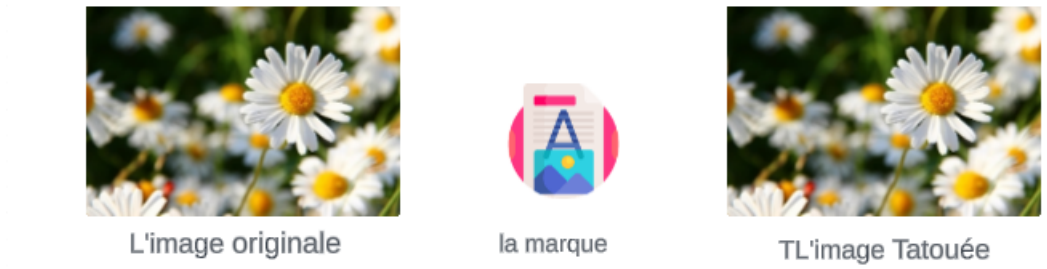


Figure 2.8 – Exemple d'un tatouage invisible.

2.7. Le Domaine d'insertion du tatouage

Les techniques de tatouages sont classées en fonction du domaine selon les catégories suivantes : les tatouages dans le domaine spatial et les

tatouages dans le domaine de fréquence (transformée)[25].

2.7.1. Domaine spatial

Les tatouages dans le domaine spatial consiste à modifier directement les valeurs des pixels de l'image sans traitement préalable. Les schémas de tatouage spatial sont simples et peu coûteux en temps de calcul. Ils offrent également un équilibre entre la robustesse, la capacité et l'imperceptibilité. Cependant, ils sont vulnérables aux attaques de traitement d'image, ce qui rend le tatouage facile à détruire.Une variété de méthodes sont mises en œuvre pour incorporer des tatouages numériques dans les images. Ces techniques, caractérisées par leur manipulation directe des valeurs des pixels, comprennent notamment :

2.7.1.1. Bit le moins significatif (LSB)

La méthode Least Significant Bit (LSB) est l'une des techniques les plus couramment utilisées en tatouage spatial. Elle consiste à remplacer les bits de poids faible (moins significatifs) des pixels de l'image hôte par les bits du tatouage. Puisque les changements introduits sont minimes et affectent principalement les parties moins perceptibles de l'image, le tatouage est généralement imperceptible à l'œil humain.

2.7.1.2. Différence de Valeurs de Pixels (DVP)

La méthode Pixel Value Differencing (DVP) est une approche de tatouage spatial qui se distingue par son utilisation des différences de valeurs entre pixels adjacents pour encoder le tatouage. Contrairement à la méthode LSB, qui modifie directement les valeurs des pixels, la méthode PVD évalue les différences de niveaux de gris ou de couleurs entre les pixels pour déterminer où insérer le tatouage. L'idée principale derrière la méthode PVD est d'exploiter les variations locales dans l'image hôte. Pour chaque paire de pixels voisins, la différence de valeur est calculée et comparée à un seuil prédéfini. Si la différence est inférieure au seuil, aucune modification n'est apportée. En revanche, si elle dépasse le seuil, des

ajustements sont effectués pour incorporer discrètement le tatouage. Cette approche présente certains avantages par rapport à la méthode LSB. Elle peut offrir une meilleure robustesse contre certaines attaques, car elle se concentre sur les relations locales entre les pixels plutôt que sur leurs valeurs absolues. Cependant, la complexité de mise en œuvre peut être plus élevée et il peut y avoir des compromis en termes de capacité de tatouage et d'imperceptibilité.

2.7.1.3. Incorporation de Pixels Aléatoires(IPA)

La méthode Random Pixel Embedding (RPE) est une technique de tatouage numérique qui vise à intégrer un tatouage dans une image en utilisant un processus aléatoire pour déterminer les emplacements des pixels modifiés. Contrairement à des méthodes comme LSB ou PVD qui suivent des schémas prédéfinis pour modifier les pixels, RPE sélectionne aléatoirement les pixels à tatouer.

2.7.2. Domaine Fréquentiel

L'algorithme du domaine de transformation est une méthode de dissimulation de données similaire à la technologie de communication à spectre étalé. Tout d'abord, il effectue une sorte de transformation orthogonale pour l'image, puis intègre les informations de filigrane dans le domaine de transformation de l'image. Enfin, il utilise la transformation inverse pour récupérer l'image dans le domaine spatial, la détection et l'extraction du filigrane sont également réalisées dans le domaine de transformation.
Il existe plusieurs méthodes couramment utilisées dans le domaine de transformation, telles que la transformée de Fourier discrète (DFT), les transformées en cosinus discrètes (DCT) et les transformées en ondelettes discrètes (DWT), etc [25].

2.8. Les Domaines d'application du tatouage

Le tatouage numérique est utilisé dans plusieurs applications, voici les plus importantes :

2.8.1. Protection des droits d'auteur

Le tatouage numérique peut être utilisé pour identifier et protéger la propriété des droits d'auteur. Le contenu numérique peut être intégré avec des tatouages numériques dépeignant des métadonnées identifiant les propriétaires des droits d'auteur[16].

2.8.2. Protection contre la copie

Le contenu numérique peut être marqué d'un tatouage numérique pour indiquer qu'il ne peut pas être reproduit illégalement. Les appareils capables de reproduction peuvent ensuite détecter ces tatouages numériques et empêcher la reproduction non autorisée du contenu [16].

2.8.3. Protection contre les altérations

Les tatouages numériques, de nature fragile, peuvent être utilisés pour garantir l'intégrité des contenus. Le contenu numérique peut être intégré avec des tatouages numériques fragiles qui se détruisent dès qu'une quelconque modification est apportée au contenu. Ces tatouages peuvent être utilisés pour authentifier le contenu [16].

2.8.4. Application médicale

Les noms des patients peuvent être imprimés sur les rapports de radiographie et les scanners IRM en utilisant des techniques de tatouage numérique visible. Les rapports médicaux jouent un rôle très important dans le traitement offert au patient. En cas de confusion entre les rapports de deux patients, cela pourrait entraîner un désastre [16].

2.8.5. Gestion des droits numériques

La gestion des droits numériques (DRM) peut être définie comme "la description, l'identification, le commerce, la protection, la surveillance et le suivi de toutes les formes d'utilisation des actifs tangibles et intangibles".

Elle concerne la gestion des droits numériques et l'application des droits de manière numérique [16].

2.9. Les attaques des images tatouées

Une image filigranée est susceptible d'être soumise à certaines manipulations, certaines involontaires telles que du bruit de compression et de transmission, d'autres intentionnelles telles que le recadrage, le filtrage, etc [1].

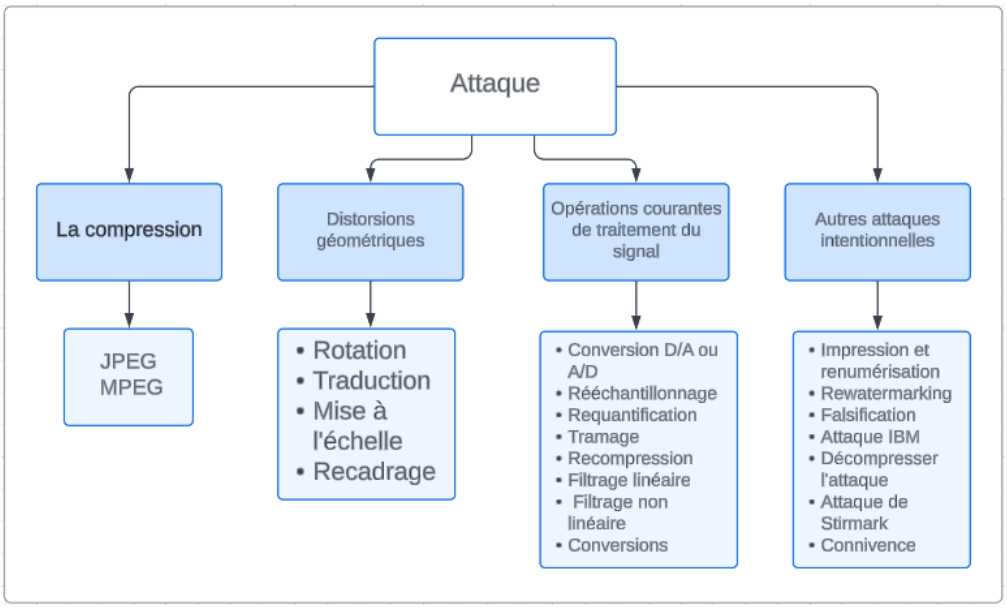


Figure 2.9 – Classification des attaques.

2.9.1. La compression

De nombreux schémas de compression tels que JPEG et MPEG peuvent potentiellement dégrader la qualité des données en raison d'une perte irréversible de données [1].

2.9.2. Distorsions géométriques

Les distorsions géométriques sont spécifiques aux images et vidéos et comprennent des opérations telles que la rotation, la translation, le redimensionnement et le recadrage [1].

2.9.3. Opérations courantes de traitement du signal

Opérations courantes de traitement de signal : Elles comprennent ce qui suit [1] :

— Conversion analogique-numérique (A/N)

— Conversion numérique-analogique (N/A)

— Reéchantillonnage

— Requantification

— Distorsion de bruit de fond (dithering)

— Recompression

— Filtrage linéaire tel que le filtrage passe-haut et passe-bas

— Filtrage non linéaire tel que le filtrage médian

— Réduction des couleurs

— Ajout d'un décalage constant aux valeurs des pixels

— Ajout de bruit gaussien et non gaussien

— Échange local de pixels

2.9.4. Autres attaques intentionnelles[1] :

— Impression et numérisation ultérieure Tatouage de l'image tatouée (retatouage) Collusion : Un certain nombre de destinataires autorisés de l'image ne devraient pas être en mesure de se réunir (colluder) et de fusionner les copies avec des tatouages différents pour générer une copie non tatouée de l'image (en moyennant toutes les images tatouées).

— Contrefaçon : Un certain nombre de destinataires autorisés de l'image ne devraient pas pouvoir conspirer pour former une copie de l'image tatouée avec le tatouage intégré valide d'une personne qui ne fait pas partie du groupe, dans l'intention d'incriminer un tiers.

— Attaque IBM : Il ne devrait pas être possible de produire une fausse image originale qui fonctionne aussi bien que l'originale et qui permet

également l'extraction du tatouage numérique, comme le prétend le détenteur de la fausse image originale. Unzign et Stirmark ont montré un succès remarquable dans la suppression des données intégrées par des programmes disponibles commercialement.

2.10. Métriques d'évaluation pour les algorithmes de tatouage numérique :

Afin de garantir le maintien de l'imperceptibilité tout en évaluant précisément la distorsion induite par les techniques de tatouage, il est essentiel d'intégrer un critère perceptuel reposant sur une modélisation de la perception des signaux multimédia. Généralement, pour évaluer cette imperceptibilité, on recourt à des métriques basées sur les pixels, qui calculent la différence entre l'image originale et l'image tatouée (qu'elle ait subi une attaque ou non). Le PSNR (Peak Signal-to-Noise Ratio) est couramment employé à cet effet, basé sur l'erreur quadratique moyenne (MSE). Cette mesure permet de déterminer la qualité du signal tatoué par rapport à l'original, avec un PSNR supérieur à 36 dB généralement considéré comme garant d'une imperceptibilité satisfaisante. Outre le PSNR, les métriques de corrélation telles que la corrélation normalisée (NC) sont également utilisées pour évaluer la similitude entre les images. Contrairement aux mesures de distorsion, ces métriques évaluent la ressemblance plutôt que la différence entre les images [26]. Le MAE (Mean Absolute Error) est également employé dans ce contexte, quantifiant la différence entre une marque originale et sa contrepartie extraite. Une valeur de MAE faible signifier une ressemblance proche des deux marques [27]. En complément, le SSIM (Structural Similarity Index) est une autre métrique largement utilisée dans le domaine du tatouage numérique. Cette mesure évalue la qualité visuelle d'une image ou d'une vidéo altérée en comparant sa structure à celle de l'original. Elle prend en compte des aspects perceptifs importants tels que la luminance et le contraste, les fusionnant en un indice unique. Cette révision intègre le SSIM de manière plus naturelle et

complète le contexte en fournissant une explication cohérente de son utilisation dans l'évaluation de la qualité visuelle des images tatouées. L'indice SSIM est exprimé sous forme d'une valeur décimale comprise entre 0 et 1, où 0 représente la pire qualité visuelle possible, indiquant que le dessin de tatouage est très différent de l'original, et 1 représente une correspondance parfaite entre le design original et le dessin de tatouage dégradé.[28] Bien que ces métriques fournissent une indication de la dégradation des images, elles ne capturent pas pleinement les caractéristiques de la perception visuelle humaine. Les formules mathématiques correspondantes pour ces métriques sont :

— la formule du PSNR (Peak Signal-to-Noise Ratio) est donnée par :

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{\max^2}{\text{MSE}} \right) \tag{2.1}$$

La MSE (Mean Squared Error) est calculée comme suit :

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

Où :

— max est la valeur maximale possible pour les pixels de l'image,

— MSE est l'erreur quadratique moyenne entre les pixels de l'image d'origine et ceux de l'image reconstruite.

— $I(i,j)$ est la valeur du pixel à la position (i,j) dans l'image originale.

— $K(i,j)$ est la valeur du pixel à la position (i,j) dans l'image compressée.

— m et n sont les dimensions de l'image.

— La formule de la corrélation croisée normalisée (NC) est donnée par :

$$NC = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2 \cdot \sum (y - \bar{y})^2}} \tag{2.2}$$

Où :

— x et y sont des variables aléatoires ou des séries de données,

— $\bar{x}$ et $\bar{y}$ sont les moyennes de x et y respectivement.

— La formule de l'erreur absolue moyenne (MAE) est donnée par :

$$MAE = \frac{\sum |x - y|}{n} \tag{2.3}$$

Où :

— x et y sont les valeurs réelles et prédites respectivement,

— n est le nombre total d'échantillons.

— La formule du SSIM (Structural Similarity Index) est donnée par :

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{2.4}$$

où :

— x et y sont les deux images à comparer,

— μ_x et μ_y sont les moyennes des pixels des images x et y,

— σ_x^2 et σ_y^2 sont les variances des pixels des images x et y,

— σ_{xy} est la covariance des pixels des images x et y,

— $C_1 = (K_1 L)^2$ et $C_2 = (K_2 L)^2$ sont deux constantes pour stabiliser la division.

Les valeurs typiques des constantes sont $K_1 = 0.01$ et $K_2 = 0.03$, et L est la valeur dynamique de la plage de pixels (par exemple, 255 pour des images sur 8 bits).

2.11. Conclusion

En conclusion, nous avons présenté les tatouages numériques sous toutes leurs facettes, explorant leur définition, leurs divers types, leurs méthodes d'inclusion, ainsi que leurs applications et les risques qui y sont associés. Ces gardiens numériques offrent une protection essentielle dans notre monde interconnecté, garantissant l'intégrité et l'authenticité des données.

CHAPITRE 3

CONCEPTION ET IMPLÉMENTATION

3.1. Introduction :

Le tatouage numérique fragile se profile comme une solution innovante pour aborder les enjeux de sécurisation des documents numériques. Son utilisation principale se concentre sur l'authentification des données. En cas de détérioration ou de modification du tatouage numérique, ces altérations sont interprétées comme des indications d'une possible altération des données sous-jacentes. D'autre part, l'extraction réussie du tatouage numérique peut servir de garantie quant à l'intégrité du document, offrant ainsi un mécanisme de validation robuste.

Ce chapitre se concentre sur la conception et la mise en œuvre d'une application utilisant le tatouage numérique fragile, ainsi que sur les algorithmes associés. L'objectif est d'insérer un tatouage dans les bits de poids faible (méthode LSB) d'une image couleur RGB afin d'assurer l'authenticité des images numériques. De plus, une analyse comparative de la qualité entre différents formats d'images est menée pour évaluer les performances de l'algorithme de tatouage fragile proposé.

3.2. les outils de développement

3.2.1. Python

Python est un langage de programmation polyvalent et interprété, réputé pour sa syntaxe claire et concise. Il favorise la lisibilité du code et offre une vaste bibliothèque standard ainsi que des modules tiers abondants pour diverses applications, de la science des données au développement web.
Sa simplicité en fait un choix populaire pour les débutants, mais il est également utilisé par de grandes entreprises pour des projets complexes [29].

3.2.2. QT Desigener

Qt Designer est un outil de conception graphique pour créer des interfaces utilisateur avec le framework Qt. Il permet de créer des interfaces graphiques en glissant-déposant des éléments visuels et en les configurant via une interface utilisateur intuitive.
Les fichiers de conception créés peuvent être ensuite convertis en code exécutable dans différents langages de programmation, tels que C++ ou Python, en utilisant les bibliothèques Qt[30].

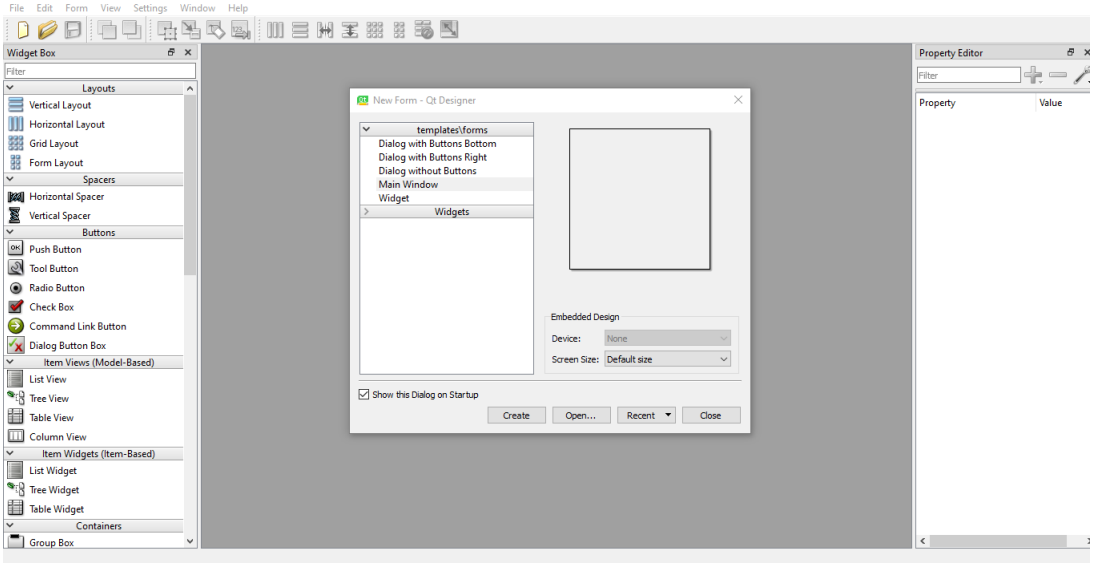


Figure 3.1 – QT Designer(Environnement QT).

3.2.3. QT

Qt est un framework de développement d'interfaces graphiques multiplateformes, offrant des outils robustes pour la création d'applications conviviales. PySide est une bibliothèque Python qui permet d'accéder aux fonctionnalités de Qt, offrant une alternative à PyQt. Ensemble, Qt et PySide permettent aux développeurs Python de créer des interfaces utilisateur riches et interactives pour une variété de plates-formes [31] .

3.2.4. visual studio code

Visual Studio Code (VS Code) est un éditeur de code source léger, extensible et multiplateforme développé par Microsoft. Il offre une expérience

de développement intuitive avec des fonctionnalités telles que la coloration syntaxique, l'autocomplétion intelligente, le débogage intégré et une vaste gamme d'extensions pour personnaliser et étendre ses fonctionnalités.
Avec son écosystème dynamique, VS Code est devenu l'un des outils préférés des développeurs pour divers langages de programmation et types de projets [32] .

3.2.5. OpenCV

OpenCV, ou Open Source Computer Vision Library, est une bibliothèque logicielle open-source largement utilisée pour le traitement d'images, la vision par ordinateur et l'apprentissage automatique. Développée initialement par Intel, elle est aujourd'hui maintenue par une communauté active sous l'égide de l'OpenCV Foundation [33].

3.2.6. PIL

PIL, ou Python Imaging Library est une bibliothèque open-source destinée au traitement d'images en Python. Créée par Fredrik Lundh en 1995, PIL a été la bibliothèque de référence pour le traitement d'images en Python pendant de nombreuses années [34].
En 2011, PIL a été abandonnée et remplacée par Pillow, un fork de la bibliothèque qui continue d'être activement développée et maintenue [35]. Pillow est compatible avec la plupart du code PIL existant et offre des fonctionnalités supplémentaires, telles que la prise en charge de nouveaux formats d'images et des performances améliorées [35].

3.2.7. Numpy

numpy, ou Numerical Python est une bibliothèque Python essentielle pour le calcul scientifique. Elle fournit des structures de données multidimensionnelles performantes, appelées tableaux, et une large gamme de fonctions mathématiques, statistiques et algorithmes linéaires algèbre [36]. NumPy est la base de nombreuses bibliothèques scientifiques Python populaires, telles que SciPy, Matplotlib et pandas.

3.3. Méthode utilisé

Nous avons opté pour l'utilisation de la méthode LSB, ou "Least Significant Bit", dans le tatouage numérique afin de dissimuler des informations au sein d'une image. Cette méthode exploite le fait que la modification du bit de poids faible (le bit de poids le moins significatif) dans les données est généralement imperceptible à l'œil humain, surtout lorsque les altérations sont subtiles.

Le processus de tatouage numérique LSB implique la substitution sélective des bits de poids faible de la donnée de couverture, par exemple une image, par les bits de l'information à dissimuler, constituant ainsi notre tatouage numérique. Cette substitution est effectuée de manière à minimiser tout impact visuel sur les données de couverture. En d'autres termes, nous avons encodé les bits de notre tatouage numérique dans les parties de la donnée de couverture où les modifications sont les moins susceptibles d'être perçues.

En adoptant cette approche, nous avons pu altérer un bit à la fois dans l'image de couverture, veillant à ce que les changements demeurent discrets et imperceptibles pour l'observateur. Cette technique nous a permis de dissimuler efficacement mes informations tout en préservant l'apparence globale de l'image.

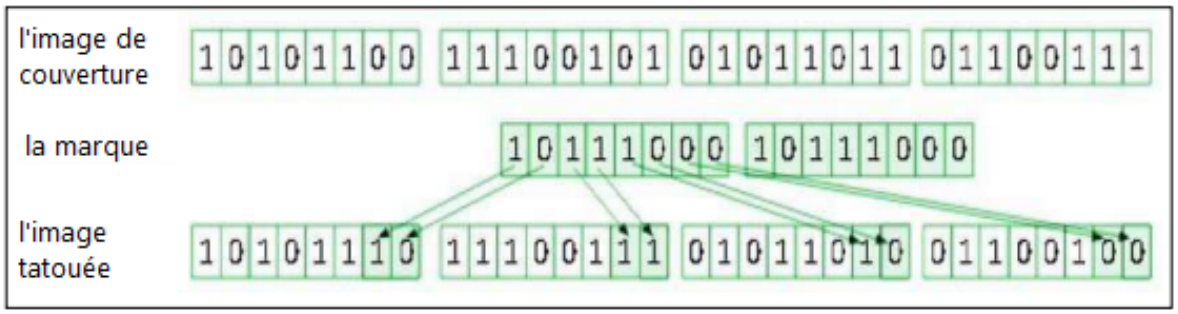


Figure 3.2 – La methode LSB.

3.4. L'organigramme de l'algorithme

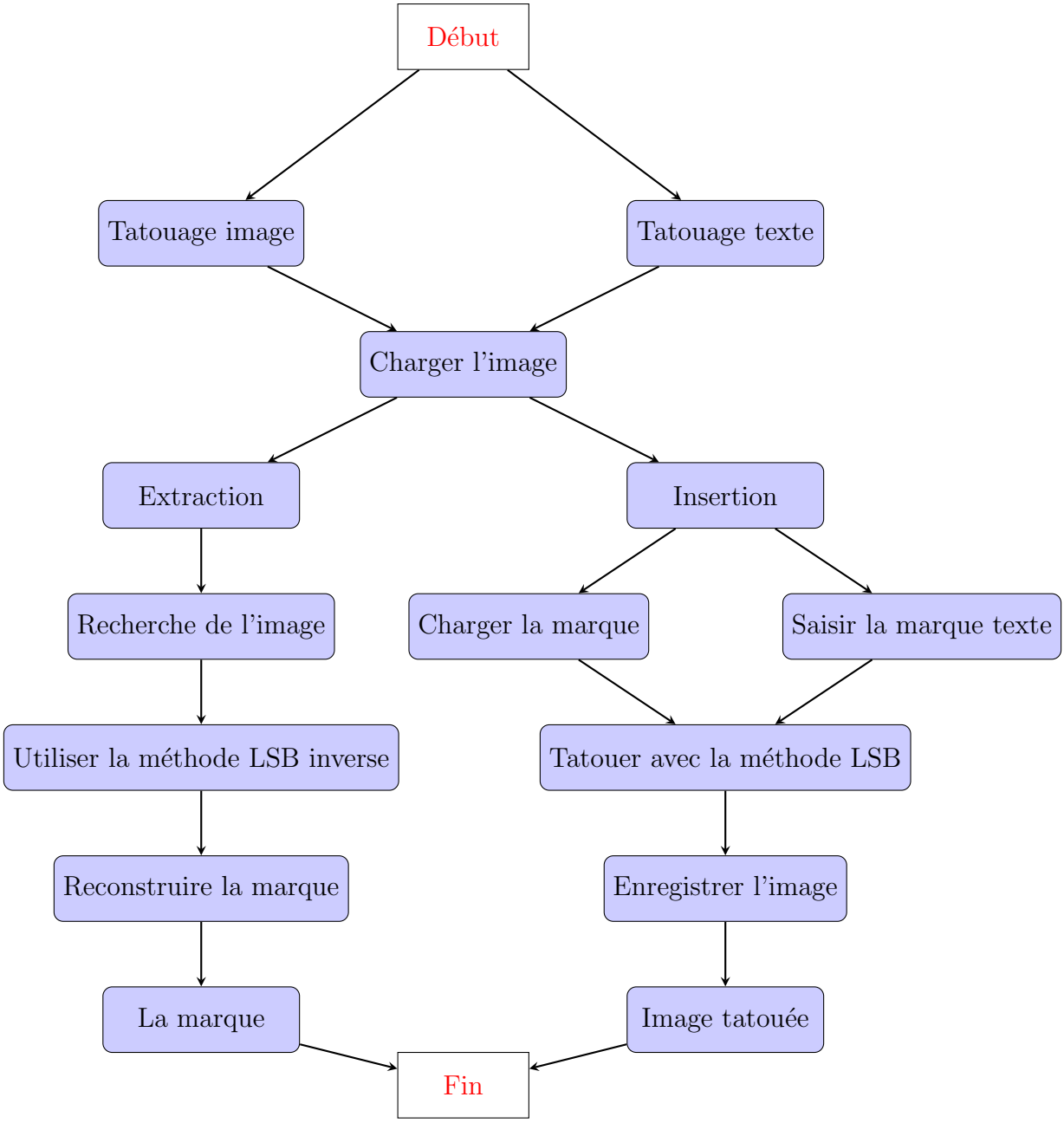


Figure 3.3 – Fonctionnement générale de l'algorithme

3.5. Algorithme d'insertion

L'algorithme détermine le nom de la fonction « insérer un tatouage numérique », qui contient une image et un fichier. Cela fonctionne si le filament supprime la capacité maximale de codage d'image en octets ; Le meilleur des cas est qu'il contient une exception ValueError. Le fichier est également converti en binaire et ajouté au sélecteur. Le pixel de l'image est parcoreux et les bits des objets qui activent les valeurs RVB sont modifiés

avec les bits qui correspondent au fichier. Ce processus dépend de l'encodage complet du fichier. Lorsque la photo sera publiée, elle apparaîtra avec le filament inclus et la recevra. Essentiellement, ce code implémentait la technique de tatouage numérique LSB (Least Significant Bit) pour intégrer le tatouage numérique dans les parties accessibles de l'image.

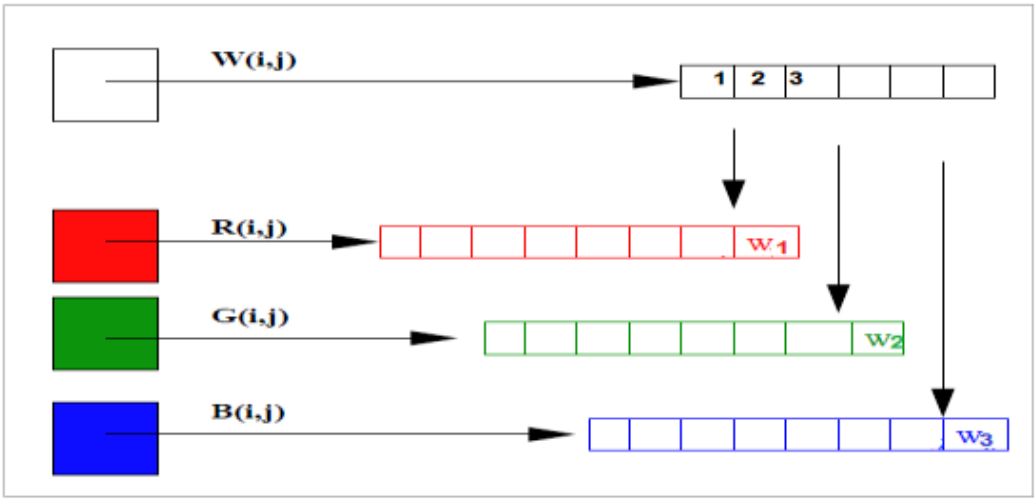


Figure 3.4 – Algorithme d'insertion.

Algorithm 1 Algorithme pour insérer un tatouage dans une image

```
1: function INSÉRER_WATERMARK(image, watermark)
2:     Lire l'image à partir du fichier (image)
3:     Calculer le nombre maximum d'octets à encoder dans l'image comme n_octets
4:     if la longueur du tatouage est supérieure à n_octets then
5:         Lever une ValueError
6:     end if
7:     Initialiser l'index_watermark à 0
8:     Convertir le tatouage en représentation binaire comme watermark_binaire
9:     Obtenir la longueur de watermark_binaire comme watermark_tatouage
10:    for all ligne dans l'image do
11:        for all pixel dans la ligne do
12:            Convertir le pixel en représentation binaire comme (r, g, b)
13:            if index_watermark est inférieur à longueur_watermark then
14:                Modifier le LSB de r avec le bit correspondant de watermark_binaire
15:                Incrémenter index_watermark
16:            end if
17:            if index_watermark est inférieur à longueur_watermark then
18:                Modifier le LSB de g avec le bit correspondant de watermark_binaire
19:                Incrémenter index_watermark
20:            end if
21:            if index_watermark est inférieur à longueur_watermark then
22:                Modifier le LSB de b avec le bit correspondant de watermark_binaire
23:                Incrémenter index_watermark
24:            end if
25:            if index_watermark est supérieur ou égal à longueur_watermark then
26:                Sortir de la boucle
27:            end if
28:        end for
29:    end for
30:    Retourner l'image modifiée et longueur_watermark
31: end function
```

3.6. algorithm d'extraction

L'algorithme définit une fonction nommée 'extract' pour décoder un filigrane intégré dans les bits de poids faible (LSB) des pixels d'une image. Il initialise initialement une chaîne vide pour stocker la représentation binaire du filigrane extrait. En parcourant chaque pixel de l'image, il extrait le LSB des valeurs RVB et les ajoute à la chaîne binaire. Si le filigrane est un texte, cette chaîne est ensuite divisée en segments de 8 bits (octets) et convertie en caractères. Si le filigrane est une image, la deuxième fonction, 'bit string to image', convertit la chaîne de bits en une image. Elle parcourt

cette chaîne pour extraire les valeurs de chaque canal de couleur (R, G, B) et les reconstitue en une image avec les dimensions spécifiées.

Algorithm 2 Algorithme pour extraire un tatouage d'une image

```
1: function EXTRAIRE_WATERMARK(image, longueur_watermark)
2:     image = lire l'image à partir du fichier (image) en utilisant cv2
3:     if image est None then
4:         Afficher "Erreur de lecture de l'image"
5:         return None
6:     end if
7:     Initialiser une chaîne de caractères vide watermark
8:     for all ligne dans l'image do
9:         for all pixel dans la ligne do
10:            b_lsb = obtenir le LSB du canal bleu du pixel
11:            g_lsb = obtenir le LSB du canal vert du pixel
12:            r_lsb = obtenir le LSB du canal rouge du pixel
13:            Concaténer b_lsb, g_lsb et r_lsb à watemark
14:            if la longueur de watermark est égale à longueur_watermark then
15:                return watermark
16:            end if
17:        end for
18:    end for
19: end function
```

3.7. Présentation de l'application réalisée

3.7.1. Interface graphique

Notre interface d'application est simple et facile à utiliser et se compose de deux sections principales. La première section est dédiée aux textes numériques (Tatouage Text), tandis que la deuxième section est dédiée aux images (Tatouage Image).

Dans chacune de ces rubriques, l'application permet à l'utilisateur de choisir les images sur lesquelles il souhaite ajouter un tatouage numérique ou un logo, en appuyant sur le bouton « Ouvrir l'image », puis en appuyant sur le bouton « Insérer » pour insérer le tatouage numérique. . De plus, l'utilisateur peut extraire des tatouages numériques, qu'il s'agisse de texte ou d'image, de l'image en appuyant sur le bouton « Extraire ».

Après ce processus, l'utilisateur obtient un tatouage numérique qu'il peut utiliser librement sans avoir à le conserver sur l'image finale.

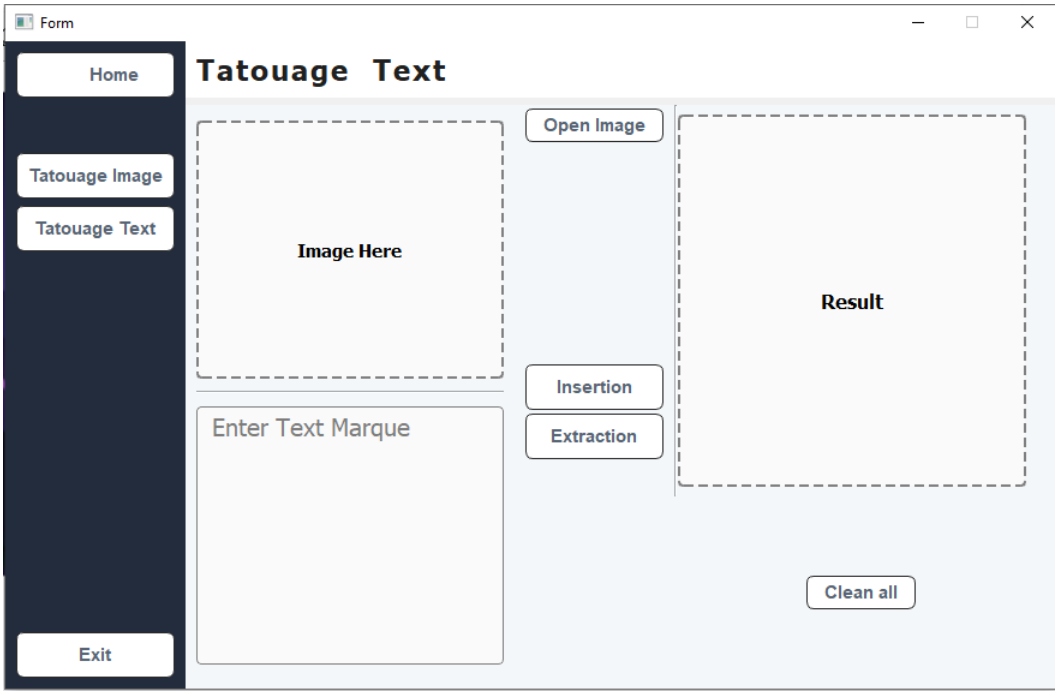


Figure 3.5 – Interface graphique de l'application..

3.7.2. Processus d'insertion du tatouage

Pour ajouter un tatouage de type texte à une image, procédez comme suit : Ouvrez l'image sur laquelle vous souhaitez ajouter le tatouage numérique à l'aide du bouton Ouvrir l'image. Ensuite, entrez le texte souhaité sous forme de tatouage numérique dans la zone de texte. Une fois terminé, appuyez sur le bouton « Insérer » pour confirmer l'ajout du tatouage numérique. Une fenêtre apparaîtra pour sélectionner l'emplacement où enregistrer l'image contenant le tatouage numérique. Choisissez l'emplacement approprié pour enregistrer l'image avec le tatouage numérique, puis l'image en surbrillance apparaîtra à l'emplacement sélectionné.

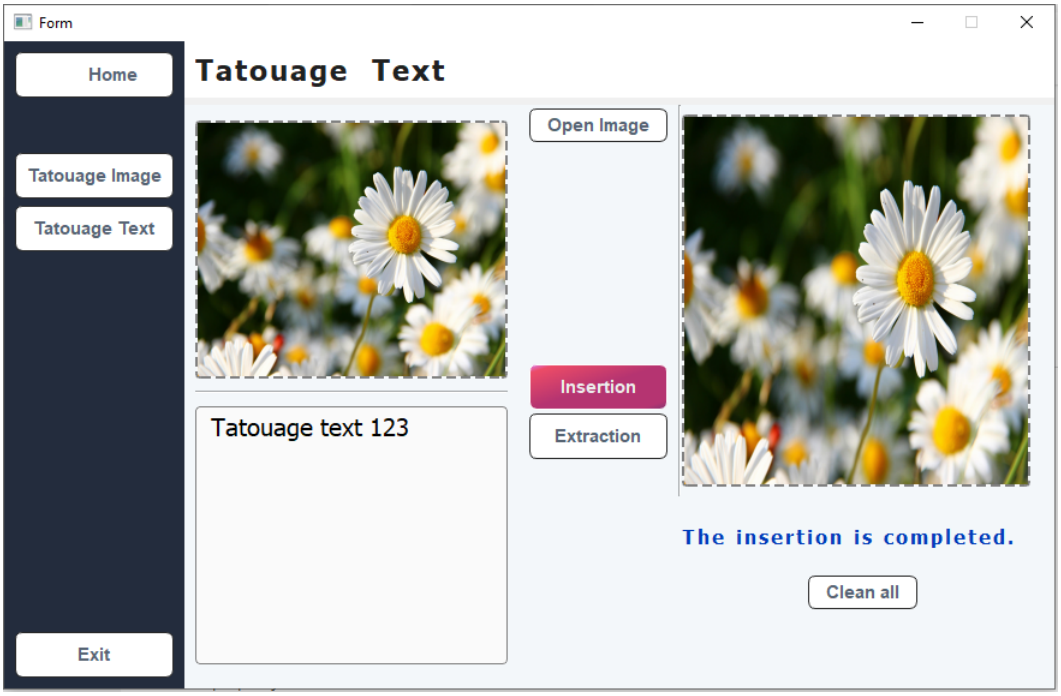


Figure 3.6 – Interface graphique de l'application lors l'insertion du tatouage (text dans une image).

Dans la section "Tatouage image", sélectionnez l'image d'origine et l'image secrète, puis suivez les mêmes étapes précédentes.

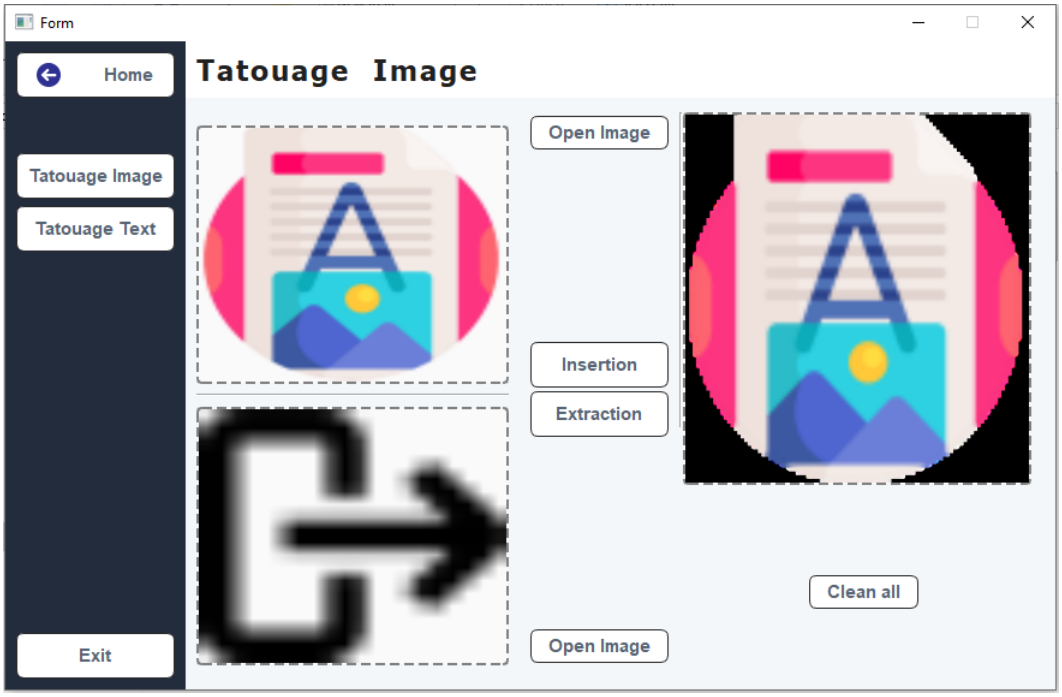


Figure 3.7 – Interface graphique de l'application lors l'insertion du tatouage(image dans une image).

3.7.3. Processus d'extraction du tatouage

Pour extraire le tatouage numérique, vous devez d'abord télécharger l'image tatouée en cliquant sur le bouton "Open image". Ensuite, veuillez sélectionner l'image souhaitée à partir de votre ordinateur ou de votre appareil mobile. Une fois l'image téléchargée, cliquez sur le bouton "Extraction" et attendez quelques instants. Le tatouage numérique extrait apparaîtra une fois le processus d'extraction terminé.

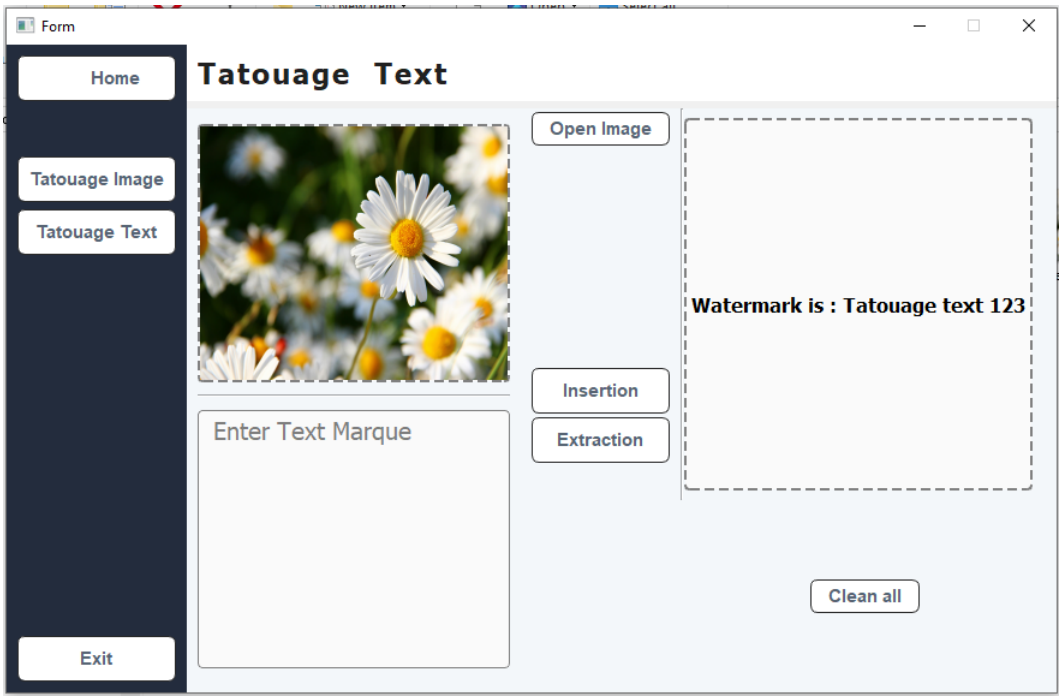


Figure 3.8 – Interface graphique de l'application lors l'extraction du tatouage(text dans une image).

3.8. Evaluation de l'algorithme

Pour évaluer les performances de l'algorithme proposé dans ce mémoire, nous avons étudié sa réaction aux modifications en analysant sa capacité à maintenir son imperceptibilité.

3.8.1. L'imperceptibilité

Nous appliquons l'algorithme décrit ci-dessus à deux images hôtes, présentées dans les figures 3.10(a) (format BMP) et 3.11(a) (format PNG).

Tatouages numériques dont le logo est copyright © NIS 3.9 qui sera utilisée pour tatouer les deux images.

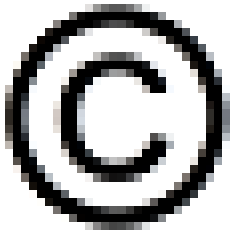


Figure 3.9 – Logo droit d'auteurs

1) Image de format BMP

(a) Image original (b) Image tatoué

Figure 3.10 – Comparaison entre les images de format BMP.

2) Image de format PNG

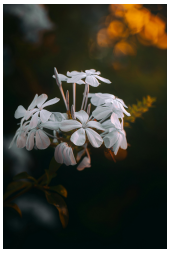
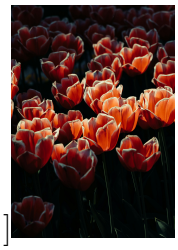
(a) Image original (b) Image tatoué

Figure 3.11 – Comparaison entre Images de format PNG.

En se référant aux images 3.10 et 3.11,Il est très difficile de faire la distinction entre la photo originale et la photo avec le tatouage. De plus, le tatouage reste invisible, préservant ainsi l'identité visuelle de l'image initiale grâce à sa similarité, sans que l'œil humain ne puisse déceler de

différence.

Pour évaluer de manière concrète l'efficacité de notre méthode, nous utilisons la métrique PSNR et SSIM afin d'estimer la distorsion des images tatouées présentes dans la collection d'images 3.12.

[(a)]  [(b)]  [(c)]  [(d)]  [(e)] 

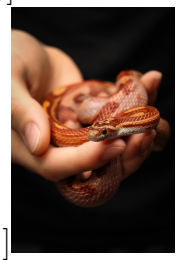
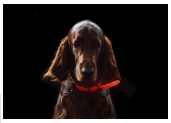
[(f)]  [(g)]  [(h)]  [(cat)] 

Figure 3.12 – Résultats de tatouage pour les images

Image	Taille	PSNR		SSIM	
		Image	Text	Image	Text
Lena	480 × 480	51.41	93.37	0.99	0.99
cat	480 × 480	51.42	88.89	0.99	0.99
Image a	3648 × 5472	70.69	98.80	0.99	0.99
Image b	4000 × 6000	70.69	99.45	0.99	0.99
Image C	3145 × 4480	69.16	97.09	0.99	0.99
Image d	4000 × 6000	71.58	99.12	0.99	0.99
Image e	2122 × 1593	62.20	90.94	0.99	0.99
Image f	4000 × 6000	72.13	99.42	0.99	0.99
Image g	5950 × 3967	72.64	99.27	0.99	0.99
Image h	3200 × 2223	64.93	94.14	0.99	0.99

Table 3.1 – Qualité des images tatouées.

Le tableau de qualité des images tatouées 3.1 montre clairement que

les valeurs sont excellentes, ce qui indique que notre méthode de tatouage fragile assure une haute qualité des images tatouées.

3.8.2. Discussion

Les résultats obtenus révèlent que les données d'authentification sont extrêmement sensibles à toute modification, même minime. Cette sensibilité accrue souligne l'importance de la précision et de la sécurité dans le traitement et la manipulation de ces données.

En termes de qualité de l'image tatouée, les valeurs de PSNR (Peak Signal-to-Noise Ratio) obtenues varient entre 51 et 98, indiquant une excellente qualité d'image, puisque des valeurs supérieures à 40 dB sont généralement considérées comme très bonnes. Cela signifie que l'altération visuelle due au tatouage est pratiquement imperceptible. Le SSIM (Structural Similarity Index Measure), quant à lui, est proche de 1, ce qui indique une forte similitude structurelle entre l'image originale et l'image tatouée. Ces résultats confirment que la modification des bits de poids faible (LSB) a un impact minimal sur la qualité visuelle de l'image.

De plus, la perte de la marque insérée dans l'image est considérée comme une preuve indiscutable de falsification des données. Toute tentative de modification non autorisée de l'image entraînera la disparition de cette marque, fournissant ainsi une méthode fiable pour détecter les manipulations. Cette caractéristique est particulièrement utile dans des contextes où l'intégrité des données visuelles est primordiale, tels que les documents officiels, les œuvres d'art numériques et autres contenus sensibles.

3.9. conclusion

Tout au long de ce chapitre, nous avons discuté des outils et méthodes utilisés pour développer notre application. Nous avons également présenté notre interface d'application et expliqué en détail le processus d'intégration et d'extraction des tatouages numériques. Enfin, nous présentons et analysons les résultats obtenus, en appliquant les propriétés d'imperceptibilité.

CONCLUSION GÉNÉRALE

Conclusion générale

Le tatouage numérique émerge comme une réponse aux préoccupations liées à la sécurité des documents numériques, offrant une alternative à la cryptographie. Il vise à sécuriser les images et à préserver l'intégrité des données. Initialement conçu pour protéger les droits d'auteur des contenus multimédias, son utilisation s'étend désormais à d'autres aspects de la sécurité numérique, comme l'authentification des données. La caractéristique essentielle du tatouage numérique est sa capacité à être à la fois délicat et imperceptible.

Dans notre travail, nous avons exploré les bases de l'imagerie numérique et de son traitement, en clarifiant les concepts clés de ce domaine. Nous avons examiné en profondeur le concept de tatouage numérique, en mettant en lumière ses contraintes, ses caractéristiques et les processus d'insertion et d'extraction. Nous avons également examiné les diverses vulnérabilités auxquelles sont confrontées les images numériques.

Notre recherche s'est concentrée sur l'application d'algorithmes de tatouage fragile aux différentes composantes chromatiques des images, en utilisant la méthode LSB (Least Significant Bit), dans le but de garantir l'authenticité et l'intégrité des données visuelles.

Les résultats de nos expérimentations ont confirmé la viabilité de notre approche. En utilisant la méthode LSB, nous avons réussi à produire des images tatouées de haute qualité.

Pour le futur, notre travail pourrait s'étendre à d'autres types d'images, tels que les formats JPEG (jpg), qui sont largement utilisés mais présentent des défis en raison de leur compression avec perte. De plus, l'ajout de techniques de cryptage d'images pourrait renforcer davantage la sécurité et rendre nos méthodes encore plus efficaces.

BIBLIOGRAPHIE

[1] Saraju P. Mohanty. Digital watermarking : A tutorial review. Dept of Comp Sc and Eng., University of South Florida, Tampa, FL 33620, smohanty@csee.usf.edu.

[2] Yaovi Gagou. Cours de traitement d'image. *Université de Picardie Jules Verne*, 2008.

[3] KADDOUR Chakib. Généralités sur les traitements d'images.

[4] The 2 types of digital images : Tools to prepare stunning images for publication, February 15, 2023.

[5] Tarun Kumar and Karun Verma. A theory based on conversion of rgb image to gray image. *International Journal of Computer Applications*, 7(2), September 2010.

[6] Université Mohamed Boudiaf-M'Sila. Tatouage fragile des images numériques, 2017.

[7] Khaldi Amine, Kafi Redouane, and Maghni Bilel. A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. *Multimedia Tools and Applications*, 82(5) :7901–7915, 2023.

[8] Moad Med Sayah, Kafi Med Redouane, and Khaldi Amine. Secure transmission and integrity verification for color medical images in telemedicine applications. *Multimedia Tools and Applications*, 81(30) :43613–43638, 2022.

[9] Marko Tkalcic and Jurij F Tasic. *Colour spaces : perceptual, historical and applicational background*, volume 1. IEEE, 2003.

[10] Chitradevi and Srimathi. An overview on image processing techniques. *International Journal of Innovative Research in Computer and Communication Engineering*, 2, November 2014. An ISO 3297 : 2007 Certified Organization.

[11] Dr. S. Kannan, Vairaprakash Gurusamy, and G. Nalini. Review on image segmentation techniques. Department Of Computer Applications Madurai Kamaraj University, March 2015.

[12] b. chanda and d. dutta majumder. *Digital image prosessing and analysis*. PHI Learning Private Limited, New Delhi-110001, 2nd edition, June 2011.

[13] Kiyoshi Tanaka, Yasuhiro Nakamura, and Kineo Matsui. Embedding secret information into a dithered multi-level image. In *IEEE Military Communications Conference*, volume 1, pages 216–220, 1990.

[14] Anatol Z Tirkel, GA Rankin, RM Van Schyndel, WJ Ho, NRA Mee, and Charles F Osborne. Electronic watermark. *Digital Image Computing, Technology and Applications (DICTA'93)*, pages 666–673, 1993.

[15] Mayssa Tayachi. *Sécurité des images par tatouage numérique et cryptographie dans les applications médicales*. PhD thesis, Brest, 2021.

[16] Prabhishek Singh and R. S. Chadha. A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9), March 2013.

[17] MARIF Oussama Benzid. digital image watermarking jpeg. 2019.

[18] OUMAKHLOUF Yasmine and RAHMOUNI Chahinez. Augmentation de la robustesse des techniques de tatouage par crypto-système. Master's thesis, Université Abderrahmane Mira Béjaia, 2022.

[19] Melouah Messaouda and Driche Imane. Tatouage numérique des données biomédicales dans le domaine des transformée. Master's thesis, UNIVERSITE KASDI MARBAH OUARGLA, 2023.

[20] Smitha Rao, AN Jyothsna, and Pinaka Pani. R,"digital watermarking : applications, techniques and attacks". *International Journal of Computer Applications*, 44(7) :29–34, 2012.

[21] Iwan Setyawan. Watermarking digital image and video data. *IEEE Signal Process. Mag*, 17(5) :20–46, 2000.

[22] Jiri Fridrich. Applications of data hiding in digital images. In *ISSPA'99. Proceedings of the Fifth International Symposium on Signal Processing and its Applications (IEEE Cat. No. 99EX359)*, volume 1, pages 9–vol. IEEE, 1999.

[23] Ensaf Hussein and Mohamed A Belal. Digital watermarking techniques, applications and attacks applied to digital media : a survey. *threshold*, 5(6), 2012.

[24] Teddy Furon and Pierre Duhamel. An asymmetric watermarking method. *IEEE Transactions on Signal Processing*, 51(4) :981–995, 2003.

[25] Hebah H.O. Nasereddin. Digital watermarking a technology overview. January 2011.

[26] Khaled Loukhaoukha. *Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective*. PhD thesis, Université Laval, 2010.

[27] Tianfeng Chai and Roland R Draxler. Root mean square error (rmse) or mean absolute error (mae) ?–arguments against avoiding rmse in the literature. *Geoscientific model development*, 7(3) :1247–1250, 2014.

[28] Mustafa Othman. *Objective video quality metric aware Adaptation mechanisms for video streaming based on DASH*. PhD thesis, Université Paris-Nord-Paris XIII, 2021.

[29] python. `https://www.python.org/`.

[30] QT Deigner. `https://doc.qt.io/qt-6/qtdesigner-manual.html`.

[31] QT. `https://www.qt.io/`.

[32] visual studio code. `https://code.visualstudio.com/`.

[33] OpenCV Foundation. Opencv : Open source computer vision library. `https://opencv.org/`, n.d.

[34] Pillow website. `https://readthedocs.org/projects/pillow/`.

[35] Pillow documentation. `https://readthedocs.org/projects/pillow/`.

[36] Numpy website. `https://numpy.org/`.