République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Kasdi Merbah Ouargla

Faculté des Nouvelles Technologies de l'Information et la Communication

Département de l'informatique et Technologies de l'information

Mémoire présenté en vue de l'obtention du diplôme Master spécialité ASR

Titre :

Tatouage Numérique Des images JPEG

---

par :

MARIF Oussama Benzid

Devan le jury :

- Encadreur : Amine KHALDI
- Examinateur : Akram BOUKHEMLA
- Examinateur : Chahrazad TOUMI

Année Universitaire 2019/2020

Remerciment

Tout d'abord je tiens à remercier Dieu, le tout puissant et miséricordieux, qui m'a donné la force, l'intelligence et la patience d'accomplir ce modeste travail.

Je remercier sincèrement Monsieur KHALDI AMINE Encadreur de ce travail, pour m'avoir dirigé tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'il a bien voulu me consacrer, je dis merci.

Je tiens à remercier vivement les membres du jury pour l'honneur qu'ils me font en acceptant de juger et d'évaluer mon travail, ainsi qu'aux enseignants du département d'informatique.

Je remercie toute ma famille,pour leur soutien et encouragement au cours de mes études.

Résumé

La technologie de l'information et la de communication révolutionne de plus en plus,le problème majeur reste au niveau de l'échange des données, sur le réseau internet, tout en conservant leurs intégrités ainsi que leurs confidentialités contre différentes attaques. Dans ce contexte plusieurs solutions informatiques basées sur l'utilisation des techniques de contrôle d'accès existent mais elles restent insuffisantes, d'où l'apparition de tatouage numérique comme solution complémentaire dans le but de contribuer à la sécurité des images partagés sur le réseau. L'objectif de notre travail est la mise au point d'un algorithme de tatouage d'images numériques. les informations à insérer sont des données relatives aux image, l'insertion de la marque est effectuée dans le domaine fréquentiel. La marque insérée doit cependant respecter deux contraintes fondamentaux : l'imperceptibilité et l'indélébilité. L'apport du tatouage numérique est la sécurité des images, il convient notamment de s'assurer que la marque ne dégrade pas la quality visuel. Dans ce sens, nous souhaitons apporter une nouvelle approche optimale de codage qui vise à garantir le compromis de la performance entre la capacité d'insertion, l'imperceptibilité et la robustesse du tatouage des images. Afin qu'un tatouage numérique soit efficace il doit être robuste, imperceptible et statistiquement invisible.

mots clé: Tatouage numérique,Images numérique,Dct,Sécurité

Abstract

Information and communication technologie revolutionizes more and more, however the main probleme is data exchange over the internet network, retaining its integrity in addition to its confidentiality against differente attacks. in this context varius computer science solutions based on access controle techniques exists but they remain insufficient, the appearance of the digital watermarking as a complementary solution to contribute in the security of digital images shared over the network,where a relative information to the image is hidden inside of it . our work aims to provide a digital image watermarking algorithme. the insertion of the watermark is performed in the frequency domain where the it has to respect some fundamental constraints such as imperceptibility and robustness,The contribution of digital watermarking is Represented in image security, it also has to be suitable especialy regarding visual quality . In this direction we wish to bring a novel optimal coding approch to guarantee the compromise of the performence between insertion capacity , imperceptibility and robustness of the image watermark. an efficient digital watermark system has to be robust , imperceptible and statistically invisible.

Key words: Digital watermark,Digital images,Dct,Security

Table des matières

Table des figures

Liste des tableaux

Introduction Général

La révolution numérique et l'explosion des réseaux de communication entrainent une circulation importante des documents multimédia , cela pose des questions essentielles relative à la protection et au contrôle des données échangées. Les documents multimédia par leur nature numérique peuvent être dupliqués, modifiés, transformés et diffusés trés facilement, il devient donc nécessaire de mettre en oeuvre des systémes permettant de faire respecter les droits d'auteur, de contrôler les copies et de protéger l'intégrité des documents .

Pour répondre à ces besoins, un nouvel axe de recherche est apparu au début des années 90 et ne cesse de prendre de l'importance au sein de la communauté scientifique. Issu de la cryptographie et la stéganographie, le tatouage numérique appelé en anglais watermarking est une approche qui a émergée ces dernières années et se présente comme une solution alternative ou complémentaire pour renforcer la sécurité des documents numériques. Le principe de cette technique consiste à enfouir au sein même du document numérique (image, son, vidéo, etc.. . .) une signature (appelée marque ou aussi watermark) indélébile et imperceptible tout en lissant le document signé exploitable, cette signature permet de résoudre des problèmes de copyright, d'authentification, de traçabilité,... etc.

Le tatouage numérique est relative à la steganographie sauf que le but de la steganographie est de cacher des données non relative au document ,ce document est utilisé comme un mechanisme pour guarentir l'impercemptibilité de l'information .

Maintenir une bonne qualité exige une dégradation de capacité ce qui est acceptable

dans l'application du watermarking, contrairement à la steganographie la capacité est considèreé assez importante comme la quality et la robustesse.

Le but de ce mémoire est d'élaborer une méthode de tatouage d'image JPEG.Cette méthode est basée sur l'utilisation de domaine transformés obtenus par la transformée en cosinus discrète (DCT), Nous avons choisi d'utiliser un codage spécifique pour l'insertion de nos données dans l'image utilisée comme support .

Dans le premier chapitre, nous avons présentés un état de l'art du domaine du tatouage numérique des données multimédias d'une façon générale. En premier lieu nous avons présenté la définition du tatouage numérique, Puis, nous avons évoqué Les éléments d'un système de tatouage numérique Par la suite, nous avons parlé des contraintes des systèmes de tatouage et leurs types ainsi que des domaines d'application.

Dans le deuxième chapitre, notre étude est focalisée en particulier sur le tatouage des images numérique. nous avons présenté la notion "image numérique" et ces carectéréstiques Ensuite, nous avons abordé le shéma de tatouage des image numérique et les domaine du tatouage,aprés nous avons abordé la question des attaques de tatouage,et dans la fin de ce chapitre nous avons parlé d'évaluation des algorithmes de tatouage d'image.

Le troisième chapitre est consacré exclusivement pour présenter notre méthode du tatouage, nous avons d'abord effectué une démonstration des outils et méthodes utilisés, ensuite nous avons présenté notre application de tatouage ainsi les résultats obtenus.

Chapitre 1

Le tatouage numérique

1.1 Introduction

Ce chapitre présente un état de l'art sur les méthodes de tatouage numérique Nous commençons par introduire la technique de tatouage numérique ou (watermarking), ces contraintes, les différents concepts et techniques utilisées, ainsi que les différents domaines d'application.

1.2 Définition

La technique de tatouage numérique (watermarking) représente le processus permettant d'ajouter des informations supplémentaire à un document numérique appelé médium ou support sans dégradation importante de la quality de cet objet, afin de tester l'intégrité et l'authenticité. [1]

Le message inclus dans le médium, généralement appelé marque ou signature, cette marque peut être une séquence de bits,un message,un logo binaire.

Il exist généralement deux classes de tatouage : visibles et invisibles.

Le tatouage visible: ou la marque sera visiblement clair, par exemple l'ajout d'une image pour en marquer une autre.

Le tatouage invisible: peut être considéré comme une forme de stéganographie, puisque l'utilisateur final ignore la présence du tatouage et donc de l'information cachée [2].

1.3 Les éléments d'un système de tatouage numérique

Un système de tatouage est composé de deux phases principaux: la phase d'insertion, et la phase de détection.

Tout système de tatouage prend la forme donnée sur la figure suivante :

Figure 1.1: Les éléments d'un système de tatouage

1.3.1 La phase d'insertion

Cette phase est considéré comme l'étape fondamentale d'un système de tatouage dont la marque est combinée avec le document numérique. Ce dernier peut être un fichier audio, une image fixe, une séquence vidéo,... etc.

La marque est encodée en utilisant une clé secrète K , elle peut être utilisée en tant qu'entrée supplémentaire dont l'objectif est d'augmenter la securité et rendre la détection de la marque impossible pour les utilisateurs non autorisés qui n'ont pas accés a K , il exist deux manières pour insérer une marque dans un objet numérique , une manière substitutive et une manière additive.

1.3.1.1 Les méthodes substitutive

C'est un mécanisme d'insertion du tatouage consiste à modifier des bits du support original afin de les faire correspondre au tatouage à insérer.

1.3.1.2 Les méthodes additive

Les méthodes additives consistes principalement à ajouter la marque au support c'est le mécanisme le plus utilisé.peut se faire sur l'image dans le domaine spatial ou transformée .

$$I_t = I_0 + w \tag{1.1}$$

Où I_o represente le document original et w la marque à insérer, I_t le document tatouée.

1.3.2 La phase d'extraction

C'est la phase qui permet de vérifier que la marque extraite est bien celle d'origine,il existe deux schémas :

Extraction aveugle C'est La technique d'extraction de la marque qui nécessite juste l'objet à analyser et la clé .

Extraction non-aveugle C'est La technique d' extraction qui nécessite l'objet originale pour extraire la marque . Elle est plus robuste que l'extraction aveugle mais elle est moins utilisée car elle requiert l'objet originale.

1.4 Les contraintes des systèmes de tatouage

Un système de tatouage est caractèrisé par trois contraintes importantes: capacité, imperceptibilité, robustesse qui ne peuvent être maximisée à la fois, vu qu'elles sont inversement proportionnelles. [3]

Parmi lesquelles un système de tatouage doit vérifier l'imperceptibilité qui est un critére

quantatif .

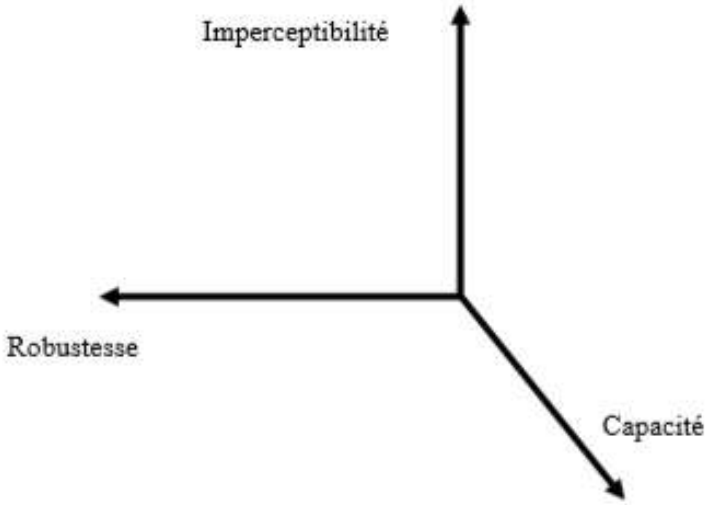

Figure 1.2: Les contraintes des systèmes de tatouage

1.4.1 La capacité

La capacité d'une méthode de tatouage est définie par la taille en bits d'une marque qui peut être intégré dans un document de taille donnée. De ce fait, on déduit que la capacité d'insertion relative est la relation entre la taille du message secret et la taille du médium utilisé [4].

1.4.2 L'imperceptibilité

Une marque est dite imperceptible si toute personne est incapable de faire la différence entre le support original et le support marqué. c'est a dire la différence ne doit pas être visible . L'objectif est qu'une tierce personne en dehors des personnes concernées par le message ne détecte pas l'existence de l'information cachée [5]. Des tests visuels sont pratiqués pour certifier ce caractère d'invisibilité. Lors de ces

tests, des supports marqués et non marqués sont présentés aléatoirement aux sujets qui doivent déterminer lequel a la meilleure qualité.

1.4.3 La robustesse

C'est la capacité que possède un algorithme de tatouage à résister aux attaques extérieures, volontaires ou non, par exemple la compression, le filtrage, bruits, coupures... ect. en utilisant des logiciels extrêmement répandus. Ces modifications entraînent alors un risque de détérioration du tatouage [6].

1.5 Les types de tatouage numérique

1.5.1 Tatouage robuste

Le tatouage robuste consiste à cacher un message dans un support en respectant les contraintes de perceptibilité. Dans ce cas, il faut pouvoir garantir que l'information insérée puisse résister à des transformations (licites et/ou illicites) l'information doit rester présente même si le document numérique a subit une dégradation [7].

1.5.2 Tatouage fragile

Le tatouage fragile est un tatouage invisible, qui est utilisé pour détecter toute modification du médium, par exemple pour vérifier que le contenu n'a pas été modifié par un tiers. Certains types de tatouages fragiles peuvent également être intégrés dans des images qui sont ensuite imprimées, permettant ainsi de détecter des contrefaçons de documents physiques, De tels tatouages ont été utilisés pour l'authentification et la vérification d'intégrité [7].

1.6 Les Domaines d'application du tatouage

Plusieurs applications sont connues pour le fait de tatouage numérique , en fait il peut être intégrer dans divers domaines, en considérant le contexte c'est à dire qu'il exist pas un seul algorithme adaptable à toutes les applications, il est nécessaire de prendre en compte les besoins de l'application visée lors de la conception d'un algorithme de tatouage numérique.
Dans la suite, nous citons quelques champs d'application du tatouage numérique.

1.6.1 La protection des droits d'auteurs

C'est la premiére application de tatouage numérique, dont la marque est utilisé comme une signature permettant de prouver qu'une œuvre donnée a bien été créée par un certain utilisateur. Notons que l'utilisation de la preuve de propriété implique un schéma de gestion privée des droits d'auteur, c'est-à-dire chaque créateur doit faire la preuve qu'il est propriétaire de son œuvre, par opposition à un schéma public où les droits sont gérés par une société d'auteurs qui a la confiance à la fois des utilisateurs et des tribunaux en cas de litige. Un autre cas d'utilisation est celui où une personne met à disposition gratuitement ses œuvres, sur internet par exemple, mais ne souhaite pas que celles-ci soient réutilisées ou revendues par un tiers : l'utilisateur ne veut alors pas payer les droits d'enregistrement puisque la diffusion n'est pas rentable, mais souhaite garder le contrôle de ses droits de propriété [8].

1.6.2 L'authentification

L'idée de base de cette application consiste à contrôler une modification éventuelle de support. Une manière d'y parvenir est d'insérer une marque fragile dans le support qui sert à alerter l'utilisateur de sa modification par une personne non autorisée. L'objectif de la fragilité de la marque est que cette dernière disparaît à la moindre modification. Si la marque fragile a disparu, le média n'est plus sûr et on évitera

de l'utiliser. Cette application est généralement utilisée dans le domaine juridique et médical

1.6.3 Le contrôle de diffusion

On peut insérer une marque dans une publicité , afin de s'assurer que certains annonces ont été effectivement diffusées

1.6.4 Surveillance de l'audience

C'est une nouvelle application ou l'information cachée est le nom de la chaine dans la bande son des chaines télé. Les panelistes ont un appareil placé sur la télé qui captent le son ambiant dans la pièce, décode le tatouage et envoie par Internet le nom de la chaine regardée par la famille. Ils peuvent mesurer l'audience et la part de marché en direct [11].

1.6.5 Traçage d'utilisateur

C'est l'une des nouvelles applications de tatouage numérique elle est utilisé dans les sites web vendant du contenu multimédia (films, chansons) envoient au client une copie personnalisée du contenu. L'ID du client est intégré de manière à ce que les personnes malhonnêtes qui partagent illégalement leurs versions soient identifiées et inscrites sur une liste noire (ou poursuivies en justice) [12].

1.6.6 Traçage de contenu

Dit aussi Le fingerprint constitue un autre outil de protection du droit d'auteur. Il consiste à insérer dans l'œuvre un identifiant caractéristique de distributeur, ce qui permet de déterminer l'auteur d'une diffusion illégale lorsque l'on retrouve un document piraté. Cet outil de traçage a pour but de dissuader le piratage ou la négligence, ce

qui peut s'avérer particulièrement utile dans les échanges de données sensibles (images militaires par exemple), ainsi que dans l'audiovisuel. Il est en effet très fréquent que, avant sa sortie, un film à gros budget soit disponible partiellement ou en intégralité sur internet, du fait de fuites émanant du circuit de production lui-même. Cela nuit évidemment à l'effet d'annonce escompté par les distributeurs, qui cherchent à tracer l'origine de la diffusion illicite.

1.6.7 Sécurité médicale

Insertion d'un ID confidentiel assurant la correspondance entre le patient et son document médicale (radio) afin d'éviter toutes confusion.

1.7 Conclusion

Dans ce chapitre, nous avons présenté les notions élémentaires liées au domaine du tatouage numérique . Nous avons exliqué les phases d'insertion et d'extraction ainsi les contraintes des systèmes de tatouage numérique, nous avons aussi détaillé les domaines d'application du tatouage.

Chapitre 2

Le Tatouage d'images numériques

2.1 Introduction

L'objectif de ce chapitre est d'introduire le domaine du tatouage des images numériques. Nous découvrons en premier lieu les notions de base des image numérique , ces différent types et caractéristiques, ensuit passant vers le principe du tatouage et le domaine d'insertion puis,les attaques utilisé pour détruire le tatouage et en dernier lieu les métrics d'evaluation des algorithme de tatouage.

2.2 Image numérique

Le terme image se définit par la représentation concrète ou abstraite d'un objet, d'un être vivant ou encore d'un concept.
Le terme "Image Numérique" désigne, toute image qui a été Acquise,sauvegardée et traitée sous une forme codée représentable par des valeurs numériques.C'est cette forme numérique qui permet une exploitation ultérieure par des outils logiciels sur ordinateur.
En Informatique elle signifie une structure de données sous la form d'une matrice bidimentionelle de pixels (Picture élément) [13] .

2.2.1 Les images matricielles

Une image matricielle est composée d'un ensemble de points dit pixels. Ce type d'image est adapté à l'affichage sur écran mais peu adapté pour l'impression car en cas d'agrandissement une perte de qualité peut se produire . [14]

2.2.2 Les images vectorielles

Une image vectorielle est représentée l'aide de formules mathématiques. Cela permet alors de la redimensionner sans aucune perte de qualité. [14]

2.2.3 Le Pixel

Le pixel est le plus petit point de l'image. Chaque pixel de l'image véhicule des informations, la quantité de ces informations donne des nuances entre images au niveau de gris (monochrome) et images de couleur.

2.2.3.1 Image au niveau de gris

Une image au niveaux de gris est représentée sur un seul canal dit aussi monochrome, chaque pixel est codé sur un octet de 256 valeurs possibles.

2.2.3.2 Image couleur

Dans une image couleur (R.G.B), un pixel peut être représenté sur trois octets, un pour chacune des trois couleurs (Rouge, Vert, Bleu) . Chacune de ces couleurs est codée sur un octet, appelé canal. Il existe 256 valeurs possibles par canal. On peut représenter 16777216(256^3) couleurs .

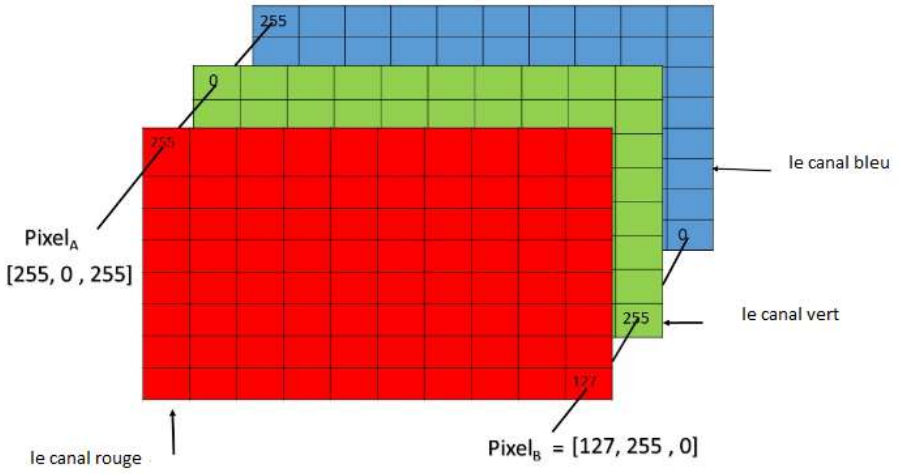

Figure 2.1: Présentation des pixels couleur

2.2.4 Formats d'image

Une image matricielle peut être représentée de différentes façons. Parmi les principaux formats matriciels : Windows bitmap (BMP), Portable Network Graphics (PNG) et Joint Photographic Experts Group (JPEG).

2.2.4.1 Format BMP (bitmap)

Le format BMP a été développé par Microsoft et IBM. Il s'agit d'un format universel, non compressé. Ce format est fidèle concernant la restitution des couleurs de l'image d'origine. Son inconvénient est que le fichier généré a un poids élevé . [15]

2.2.4.2 Format PNG (Portable Network Graphic)

Le format PNG est standardisé par le W3C (World Wide Web Consortium). Ce format propriétaire est aussi très utilisé dans le web. Il permet une optimisation maximum du poids du visuel, car il utilise un système de couleurs indexées. Par ailleurs, c'est possible de n'utiliser que des valeurs chromatiques spécifiques. De plus, il permet

d'enregistrer de 1 à 48 bits et aussi la gestion de la transparence . [15]

2.2.4.3 Format JPEG (Joint Photographic Expert Group)

Le format JPEG est très utilisé. Il a été établi par un comité d'experts qui édite des normes de compression pour les images fixes. Son inconvénient est que la qualité des images d'origine est fortement dégradée par ce format compressé. Cependant, il permet d'avoir une reproduction relativement fidèle des couleurs et permet aussi d'avoir un fichier très léger. [15]

2.2.5 Les différents espaces couleurs

Un espace de couleur ou espace colorimétrique est une représentation de couleurs dans un système de synthèse des couleurs . Une couleur est généralement représentée par trois composantes [16]. Un espace de couleurs est défini par ces composantes . Il existe de nombreux espaces de couleurs, parmi eux : RGB, YUV.

2.2.5.1 Le modèle RGB

L'espace RGB (Red, Green, Bleu) ou en français RVB (Rouge, Vert, Bleu) est défini à partir de ces trois couleurs primaires dont son nom est composé de leurs initiales. Il est considéré comme l'espace de couleurs le plus utilisé. La représentation des couleurs dans cet espace donne un cube appelé Cube de Maxwell. [17]

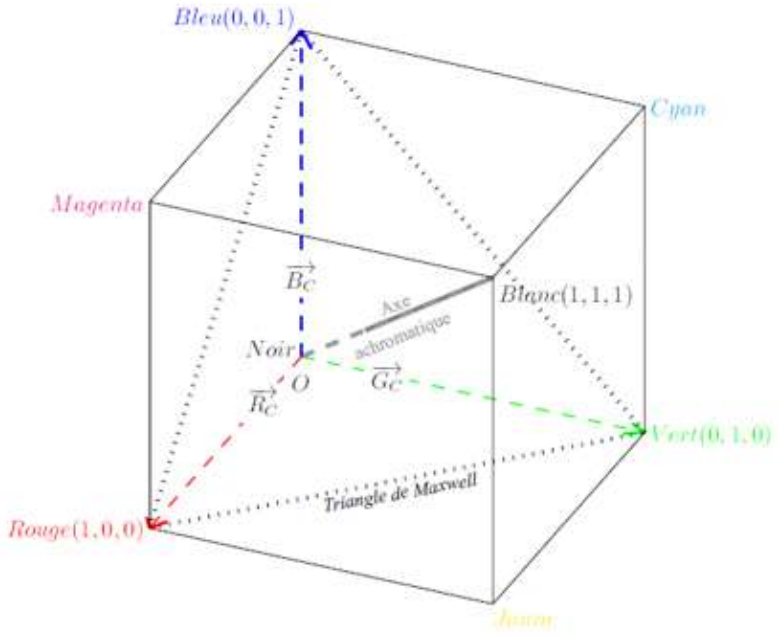

Figure 2.2: Cube de Maxwell

L'origine O correspond au noir ($R_C = G_C = B_C = 0$). Tandis que le point $(R_C, G_C, B_C) = (1, 1, 1)$ représente le blanc. L'axe achromatique représenté dans la figure 2.2 aussi appelé axe des gris, représente des nuances de gris, allant du noir au blanc. D'après le cube de Maxwell, le point $(R_C, G_C, B_C) = (1, 0, 0)$ représente la couleur rouge. Le point $(R_C, G_C, B_C) = (0, 1, 0)$ le vert et le point $(R_C, G_C, B_C) = (0, 0, 1)$ le bleu.
Dans le système RVB, on utilise la synthèse additive des trois couleurs. C'est-à-dire, l'addition des trois couleurs donne du blanc, le rouge et le vert donnent du jaune, le vert et le bleu du cyan et le bleu et le rouge du magenta.

2.2.5.2 Le modèle YUV

Le modèle YUV ou plus précisément Y'UV représente un espace de couleur en trois composantes . Y représente la luminance (C'est-à-dire l'information en noir et blanc), et U et V la chrominance (C'est-à-dire l'information sur la couleur). L'œil humain est plus sensible à la modification de la luminance contrairement à la modification de la

chrominance. Le YUV est un modèle de représentation de la couleur dédié à la vidéo analogique. Y'UV est créé depuis une source R'G'B', les symboles prime indiquent une correction gamma. Le gamma étant un facteur de contraste.

2.2.6 Fréquence dans une image

Une fréquence dans une image est le changement d'intensité. Il y a deux types de fréquences dans une image : Hautes et basses fréquences, les hautes fréquences correspondent à des changements d'intensité rapides et les basses fréquences correspondent à des changements d'intensité lents. La plus grande partie de l'énergie d'une image se situe dans les basses fréquences . [18]

2.2.7 La résolution

La résolution d'une image est le nombre de pixels par pouce(1 pouce = 2.54 centimètres).Plus il y a de pixels par pouce et plus il y aura d'information dans l'image. [18]

Figure 2.3: Les différentes résolutions d'une image.

2.2.8 La Dimension

La dimension d'une image présente le nombre de pixels de celle-ci , donné par le produit du nombre de lignes et le nombre de colonnes de la matrice associée à l'image. [18]

2.3 Le Principe général d'un schéma de tatouage d'images

Le principe général d'un schéma de tatouage d'une image numérique pour divers buts tel que la protection du copyright, consiste principalement à insérer une marque d'une maniére imperceptible et robuste.

C'est à dire que la déformation de l'image doit être visiblement faible pour que l'utilisateur ne puisse distinguer la différence entre l'image tatouée et l'image originale, et la marque insérée ne peut être perdue après diverses attaques.

Dans la plupart des systèmes de tatouage, le marquage est protégé par un code secret. Seules les personnes ou les organismes autorisés peuvent savoir si une image a été marquée et le cas échéant lire cette marque.Cette exigence se concrétise dans les algorithmes de tatouage par l'usage d'une clé privée cryptographique appartenant au propriétaire de l'image.

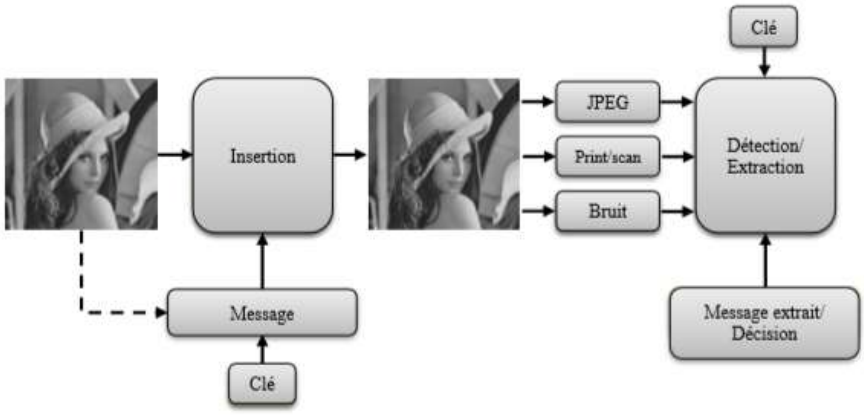

Figure 2.4: Schèma d'un système de tatouage d'image

2.4 Le Domaine d'insertion du tatouage

2.4.1 Domiane spatial

Consiste à modifier directement les valeurs des pixels de l'image Comme aucun traitement initial n'est requis. Les schémas de tatouage du domaine spatial sont simple et peu couteuse en temps de calcul .Ils aussi offre une régulation entre la robustesse, la capacité et l'imperceptibilité .
Leurs inconvinient qu'ils sont pas robuste face aux attaques de traitement d'image, donc le tatouage peut être détruit facilement. [15]

2.4.1.1 Bit le moins significatif (LSB)

Parmi les algorithme proposées, LSB qui modifient les bits de poids faible de l'image hote. L'invisibilité de la marque est obtenu par l'hypothése que les données contenus dans les bits LSB sont visuellement insignifiantes. La marque est généralement inséré en utilisant la connaissance d'une clé secrète, comme la location de la marque.

2.4.2 Domaine transformé

Le domaine transformé est un espace d'insertion de la marque après une transformation inversible, on distingue la Transformée de Fourier Discrèt(DFT), la Transformée en Cosinus Discrète (DCT) et la transformée en ondelettes discrète (DWT).
L'image transformé représente la relation spatial entre les pixels, et sert à obtenir une représentation plus adaptée au tatouage robuste.les méthodes de tatouage qui utilise le domaine transformé sont considéré plus robuste face aux attaques d'extraction ou de destruction du tatouage. [19]

2.4.2.1 La transformée de Fourier discrète (DFT)

La transformation de Fourier F est une opération qui transforme une fonction intégrable sur R en une autre fonction. Elle permet de traiter directement les fréquences des images (à la manière des signaux) ou encore de compresser des images. En général, pour représenter la transformée, on représente uniquement le module , l'utilisation de la phase de l'image complexe pour l'insertion de la marque est possible mais avec précaution.En fait, la phase dispose de beaucoup d'informations pertinentes de l'image, afin de trouver un compromis entre la visibilité et la robustesse seuls les coefficients de fréquence moyenne sont exploités [20].

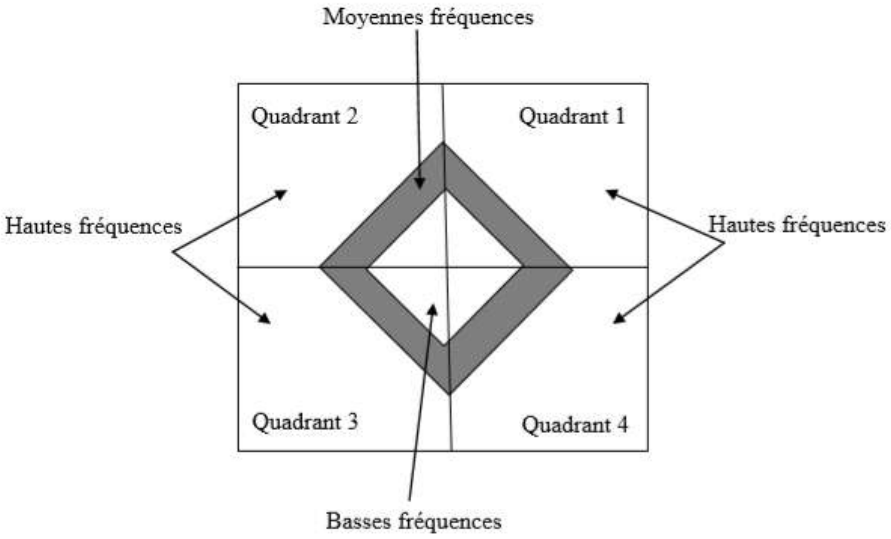

Figure 2.5: Répartition fréquentielle des coefficients de module d'une DFT

La DFT (transformée de Fourier discrète), d'une image I(x, y) de taille M x N avec $f(x, y)$ signifie image spatial et $f(u, v)$ image dans le domain frequentiel est données comme suite :

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \mathrm{e}^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \tag{2.1}$$

La transformation inverse est donnée par :

$$f(x,y) = \frac{1}{M \times N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) \mathrm{e}^{j2\pi(\frac{ux}{M}+\frac{vy}{N})} \tag{2.2}$$

2.4.2.2 La Transformée en Cosinus Discrète (DCT)

La DCT est une fonction linéaire inversible ou de manière équivalente une matrice carrée N × N inversible. La DCT, et en particulier la DCT-2 est très utilisée en traitement du signal et de l'image, et spécialement en compression. La DCT possède en effet une excellente propriété de regroupement de l'énergie : l'information est essentiellement portée par les coefficients basses fréquences. [21]

Les basses fréquences se trouvant en haut à gauche de la matrice,et les hautes fréquences en bas à droite Cette transformée souvent calculée sur des blocs de l'image de taille 8x8, soit 64 coefficients. Ces coefficients sont répartis sur trois zones : basses, moyennes et hautes fréquences [22].

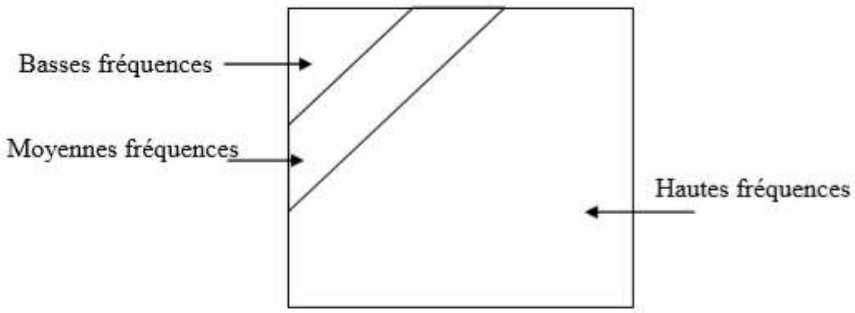

Figure 2.6: Répartition des fréquences dans un bloc DCT

La transformée DCT se calcule comme suit :

$$C(u,v) = c(u)c(v)\frac{2}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i,j) \cos\left(\frac{\pi}{N} u \left(i+\frac{1}{2}\right)\right) \cos\left(\frac{\pi}{N} v \left(j+\frac{1}{2}\right)\right) \tag{2.3}$$

$$C(x) = \begin{cases} 2^{\frac{-1}{2}} & \text{si } x = 0 \\ 1 & \text{si } x > 1 \end{cases}$$

La transformée DCT inverse se calcule comme suit :

$$I(i,j) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u)c(v)C(u,v) \cos\left(\frac{\pi}{N} u \left(i + \frac{1}{2}\right)\right) \cos\left(\frac{\pi}{N} v \left(j + \frac{1}{2}\right)\right) \quad (2.4)$$

2.4.2.3 La transformée en ondelettes discrète (DWT)

Une transformée en ondelettes discrète (DWT) est toute transformée en ondelettes pour laquelle les ondelettes sont échantillonnées discrètement.

La transformée en ondelettes utilise des filtres pour transformer l'image, un avantage clé qu'il a sur les transformées de Fourier est la résolution temporelle: il capture à la fois les informations de fréquence et de localisation (localisation dans le temps).

Cette formulation est basée sur l'utilisation de relations de récurrence pour générer des échantillonnages discrets de plus en plus fins d'une fonction implicite d'ondelettes mère, chaque résolution est le double de l'échelle précédente.

La transformée en ondelettes discrète a un grand nombre d'applications dans les sciences, l'ingénierie, les mathématiques et l'informatique. Plus particulièrement, il est utilisé pour le codage du signal , pour représenter un signal discret sous une forme plus redondante, souvent comme condition préalable à la compression des données .

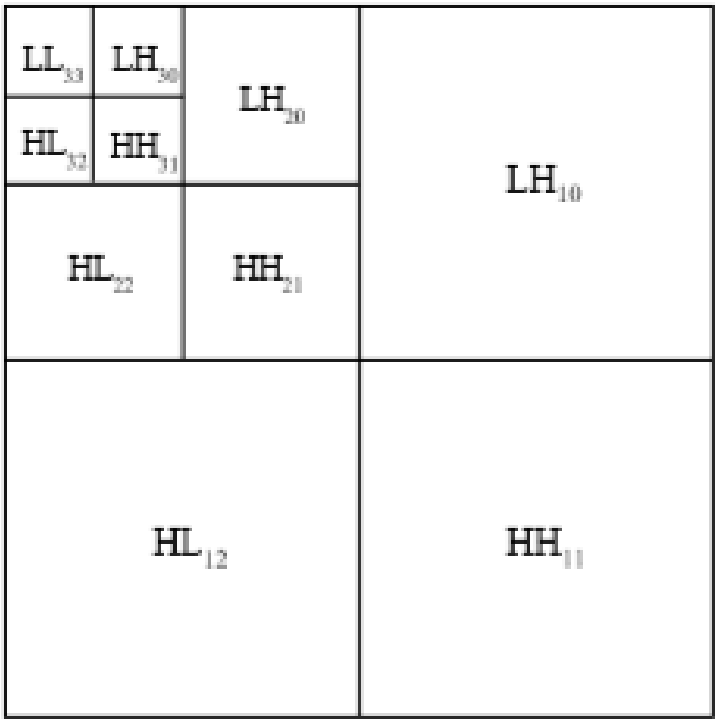

Figure 2.7: Décomposition d'une image en ondelettes

L'image d'approximation (LL) est une version réduite et lissée de l'image initiale tandis que les images de détails horizontale (LH), verticale (HL) et diagonale (HH) contiennent uniquement des informations relatives à la texture locale et aux contours des régions de l'image, à une résolution donnée et selon une direction donnée.

2.5 Les attaques et la robustesse

Une méthode de tatouage peut être fragile ou robuste, la robustesse comme on a expliqué précédemment est la capacité d'une méthode à résister face aux attaques d'alteration ou de destruction du tatouage .

On peut classifier les attaques en deux catégories, non intentionnelle et intentionnelle. Les attaques non intentionnel peut arriver à cause d'une action innocente par exemple

la reduction des dimension d'une image.
Les attaques intentionnel pour détruire le tatouage afin de falsification ou de vol des droits de propriété , dans cette section on va expliquer quelque attaques .

2.5.1 Le filtrage

Le filtrage indique un traitement d'image consiste à balayer l'image par une fenêtre d'analyse de taille finie.
Il est utilisés principalement pour améliorer son aspect. Par exemple pour rendre une image plus douce par une opération de lissage ou supprimer un bruit (la marque) présent dans l'image [23].

2.5.2 La compression

La taille importante d'une image numérique pose de grands problèmes de transmission ou de sauvegarde.
La compression est une technique qui supprime les informations redondantes des images dont le but de diminuer la taille du fichier image. Comme le tatouage est invisible, il peut donc être considéré comme non significatif et donc aussi être supprimé.

2.5.3 La rotation

La rotation est parmi les attaques géomètriques qui peuvent empecher la détection du tatouage. Si la marque est insérée dans le domaine spatial, elle subira les mêmes transformations que subit l'image.Des petites angles de rotation peuvent faire le tatouage non détectable.
En particulier lorsque l'on impose une extraction en mode aveugle.

2.5.4 Le Débruitage

L'objectif de cette attaque est d'approcher au mieux la forme d'onde du tatouage pour pouvoir l'enlever. Le tatouage peut étre estimé en utilisant des filtres spécifiques. L'idée générale consiste à estimer la marque a partir de l'image tatouée est l'image filtrée. [24]

2.5.5 Attaque par copiage

Appartient au type d'attaques de protocole visant à trouver une faille dans le protocole de gestion des droits d'auteurs. Le but est de Créer une ambiguïté de tatouage entre deux images différente,c'est à dire extraire la marque d'une image marquée à travers le Débruitage et la insérer dans une autre image . Le but est toujours de créer un conflit lors de l'authentification du propriétaire. [24]

2.6 Les métriques d'évaluation des algorithmes de tatouage

2.6.1 Erreur quadratique moyenne (MSE)

L'image dégradée I' est toujours comparée à l'originale I pour déterminer son rapport de ressemblance [25]. Ce critère est le plus utilisé. Il est basé sur la mesure de l'erreur quadratique moyenne (MSE) calculée entre les pixels originaux et traités:

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} \left(I(m,n) - I'(m,n)\right)^2 \tag{2.5}$$

Où (M × N) est la taille de l'image, et I_p et I'_p sont respectivement les amplitudes des pixels sur les images originale et dégradée. Il est vraisemblable que l'œil tienne beaucoup plus compte des erreurs à grandes amplitudes, ce qui favorise la mesure

quadratique.

2.6.2 Le rapport signal / bruit de crête (PSNR)

PSNR est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Elle permet de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale. [26]

$$PSNR = 10 \log_{10} \left(\frac{{I_{max}}^2}{MSE} \right) \tag{2.6}$$

Une valeur de PSNR infini correspond à une image non dégradée.

2.6.3 Indice de similarité structurelle (SSIM)

Est une mesure de similarité entre deux images numériques. Elle a été développée pour mesurer la qualité visuelle d'une image déformée, par rapport à l'image originale [26].La mesure entre deux fenêtres x et y est donnée par la formule suivante :

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\varphi_{xy} + c_2)}{({\mu_x}^2 + {\mu_y}^2 + c_1)({\varphi_x}^2 + {\varphi_y}^2 + c_2)} \tag{2.7}$$

μ et φ sont respectivement la moyenne et la variance de la fenêtre, c1, c2 deux variables destinées à stabiliser la division quand le dénominateur est très faible.

2.6.4 Le Taux de changement des pixel (NPCR)

Number pixel change rate(NPCR) signifie le taux de changement des pixel de l'image tatouée par apport à l'image original. NPCR $\in$ [0,1] [27].
$NPCR = 0$ signifie que aucun changement .

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{2.8}$$

W et H les dimension de l'image.

avec:

$$D(i,j) = \begin{cases} 0 & \text{si } (C_1(i,j) = C_2(i,j)) \\ 1 & \text{si } (C_1(i,j) \neq C_2(i,j) \end{cases}$$

2.6.5 La moyenne d'intensité modifié (UACI)

Unified averaged changed intensity (UACI) c'est a dire la moyenne d'intensité changée entre les deux images [27].
UACI∈[0,1].

$$UACI = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100 \tag{2.9}$$

C_1 et C_2 sont l'image original et l'image tatouée .

2.7 Conclusion

Dans ce chapitre, on a essayé de présenter un état de l'art sur le tatouage des images numériques .En donnant quelques définitions élémentaires sur les images numériques,et d'autre mécanismes relative au tatouage des images numériques qui seront des points essentiels dans la suite de notre travail.

Chapitre 3

Conception et Implémentation

3.1 Introduction

Dans ce chapitre nous présentons la conception et la réalisation de notre application de tatouage numérique. Nous présentons en détail les techniques et outils utilisées dans notre travail. En plus des fonctions effectuées par cette application Ensuite une étude expérimentale visant à évaluer la performance de notre algorithme du tatouage .

3.2 Outils utilisés

Afin de réaliser notre application de tatouage numérique nous avons utilisés le langage de programmation C++ ainsi la bibliothèque OPENCV et le langage QT pour l'interface graphique .

3.2.1 C++

Créé initialement dans les années 1980, C++ est un langage de programmation compilé permettant la programmation sous de multiples paradigmes (comme la programmation procédurale, orientée objet ou générique). Ses bonnes performances font

un des langages de programmation les plus utilisés dans les applications où la performance est critique. [28]

3.2.2 QT

QT est une boîte à outils de widget gratuite et open-source pour créer des interfaces utilisateur graphiques ainsi que des applications multiplateformes qui s'exécutent sur diverses plates-formes logicielles et matérielles telles que Linux , Windows , macOS , Android .Qt prend en charge divers compilateurs, y compris le compilateur GCC C ++ et la suite Visual Studio [29] .

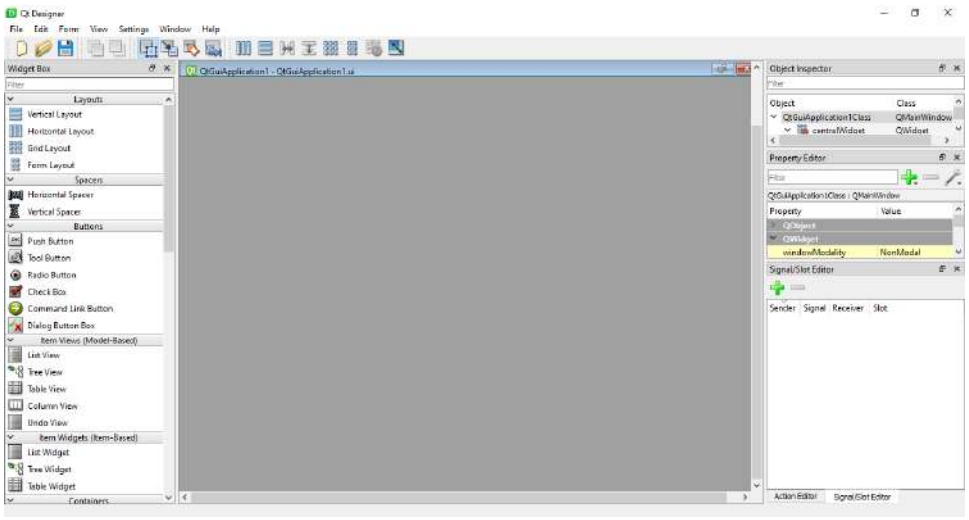

Figure 3.1: Environement QT

3.2.3 Opencv

OpenCV (pour Open Computer Vision) est une bibliothèque graphique libre, initialement développée par Intel, spécialisée dans le traitement d'images. OpenCV met à disposition de nombreuses fonctionnalités très diversifiées permettant de créer des programmes en partant des données brutes pour aller jusqu'à la création d'interfaces graphiques basiques.

3.2.4 Microsoft visual studio

Microsoft Visual Studio est un environnement de développement intégré (IDE) pour Windows , Linux et macOS . Il comprend toutes les caractéristiques d'un IDE moderne, il permet également de supporter plusieurs langages de programmation , tels que C++ , .NET,Java,Python , Ruby et PHP , ainsi que des environnements de développement Web, tels que ASP.NET MVC, Django, etc.

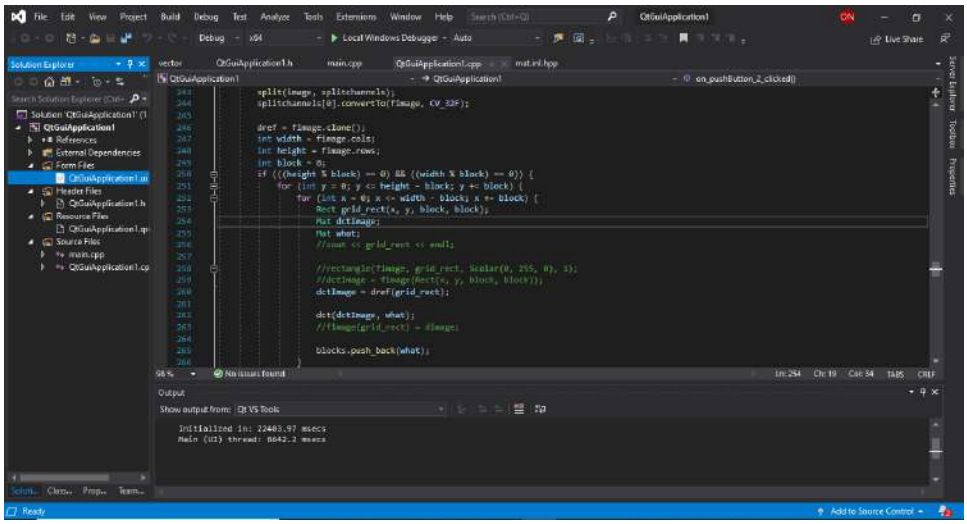

Figure 3.2: Environement de develeomppent visual stuio

3.3 Méthode utilisé

Nous avons utilisé une méthode de domain transformé sur les images JPEG ,la transformée de cosinus discret DCT est utilisé pour passer vers le domain frequentiel. L'algorithme d'insertion comprend en entrée une marque a inserer, une image hote. La phase d'insertion génère en sortie une image tatouée.L'extraction de la marque se fait d'une manière aveugle, c'est-à-dire sans faire recours à l'image originale, ce qui qualifié le tatouage d'être non informé .

Notre méthode est considiré semi-fragile , elle est robust face au certain manipulation (compression),tandis que fragile face au attaque malveillants .

3.3.1 Présentation de la méthode

L'idée de notre approche est de cacher le message on utilisons un codage spécifique,le message sera cacher dans les blocs d'un canal de couleur de l'image hote, ce codage sert a ameliorer la sécurite ainsi la robustesse de notre algorithme.

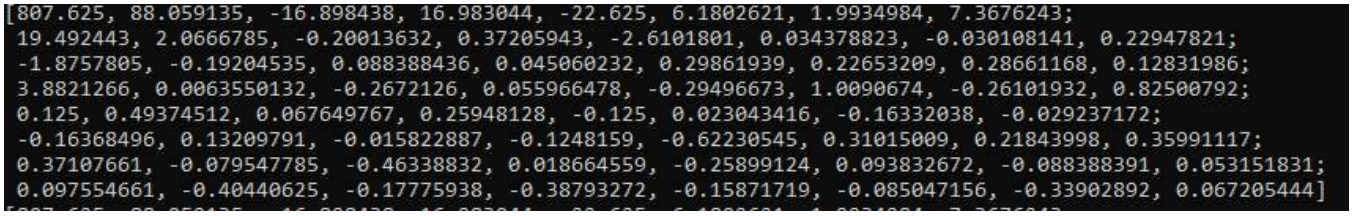

Figure 3.3: Une sous-matrice dans le domaine fréquentiel

Les valeurs de ce bloc seront changé pour cacher le bit equivalant dans le message.

3.3.2 Algorithm d'insertion

L'algorithme de la technique proposée se déroule comme suit:

1. Lire l'image hote et le message .
2. Separer les canaux de couleur c-a-d , le canal R ,B,V dans des matrices afin de pouvoir appliquer la dct.
3. Deviser les matrice de couleurs en sous-matrices de 8×8 .
4. Calcuer la dct a chacune des sous-matrices obtenu pour passer vers le domaine frequentiel.
5. Transformer le message en binnaire.
6. Pour cacher le message :
   (Si bit a inserer =0 et la valeur lsb du coefficient >5)
   alors(valeur de coefficient -5).

(Si bit a inserer =1 et la valeur lsb du coefficient <5)

alors(valeur de coefficient +5)

7. Calculer la dct-inverse pour tous les sous-matrices 8×8 .

8. Fusionner les 3 cannaux de couleur et reconstituer l'image.

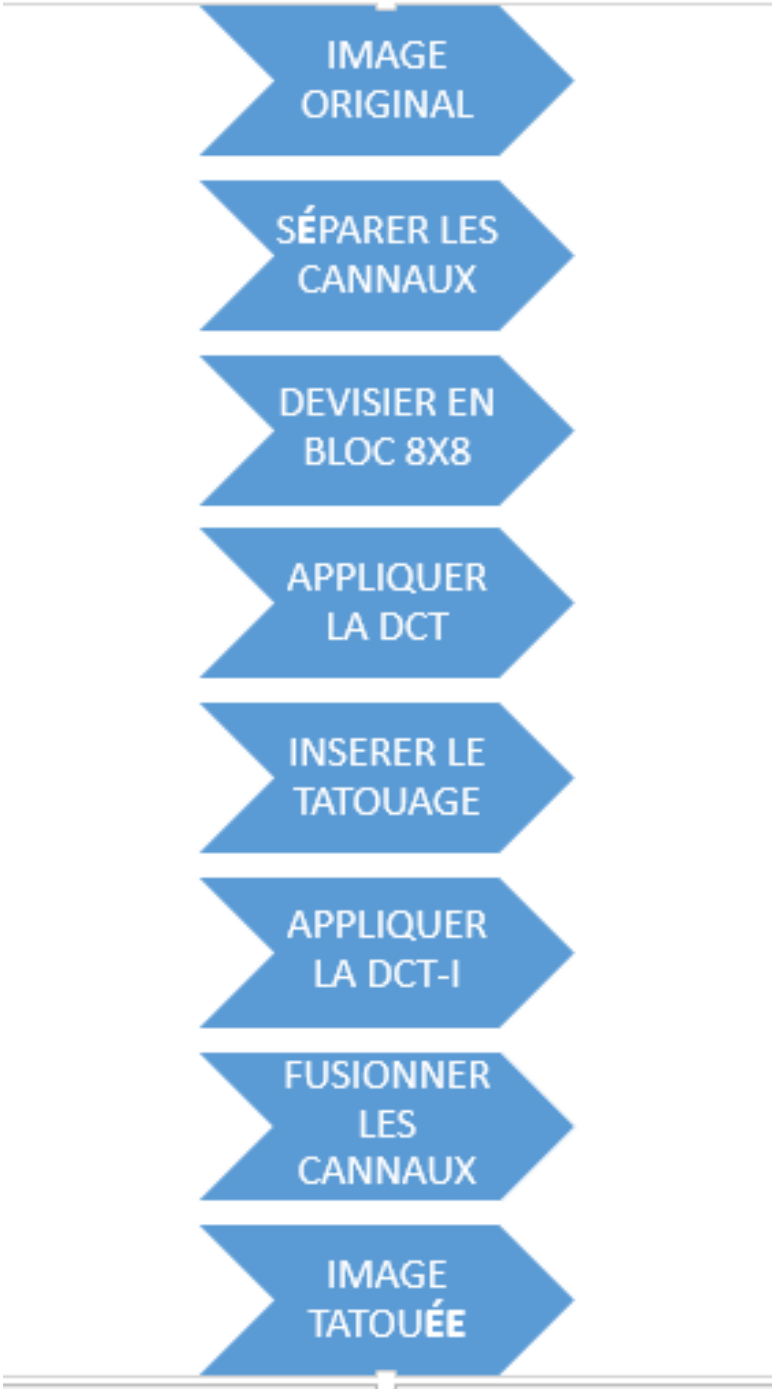

Figure 3.4: Organigrame d'insertion

3.3.3 Algorithm d'extraction

L'extraction de la marque se fait sans recours à l'image originale.

1. Lire l'image tatouée.
2. Separer les canaux de couleur c-a-d , le canal R ,B,V dans des matrices afin de pouvoir appliquer la dct.
3. Deviser les matrice de couleurs en sous-matrices de 8×8 .
4. Calcuer la dct a chacune des sous-matrices obtenu pour passer vers le domaine frequentiel.
5. Pour chaque bloc vérifier les valeur des coefficient
   si ((la valeur de coefficient mod 10) >5)
   alors(le bit cacher =1)
   si((valeur de coefficient mod 10) <5)
   alors(le bit cacher =0)
6. Récuperer tous les bits de message.
7. Transformé les bits en une suite de caractères lisible.

Figure 3.5: Organigrame d'extraction du tatouage

3.4 Présentation de l'application réalisée

3.4.1 Interface graphique

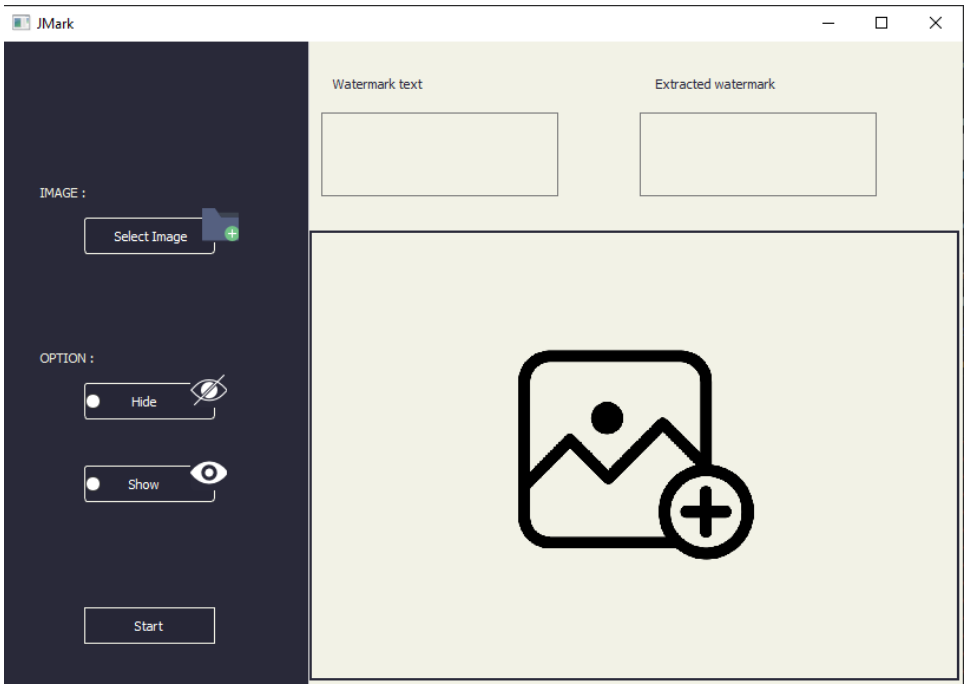

Figure 3.6: Interface graphique de l'application

L'interface de notre application contient deux boutons, le premier est "Select image" pour imorter une image qui sera afficher dans une zone d'affichage d'image,le deuxième est "start" sert à commencer le processus d'insertion ou d'extraction de tatouage, ainsi deux radio boutons "hide" et "show" pour choisir le processus à executer. Aussi deux zones de texte, une pour la lecture de la marque à inserer et l'autre pour l'affichage du résultat d'extraction .

3.4.2 Processus d'insertion du tatouage

La phase d'insertion commence avec la selection d'image ainsi l'écriture du message dans la zone du text , ensuite le choix de l'option "hide" et enfin début de l'opération.

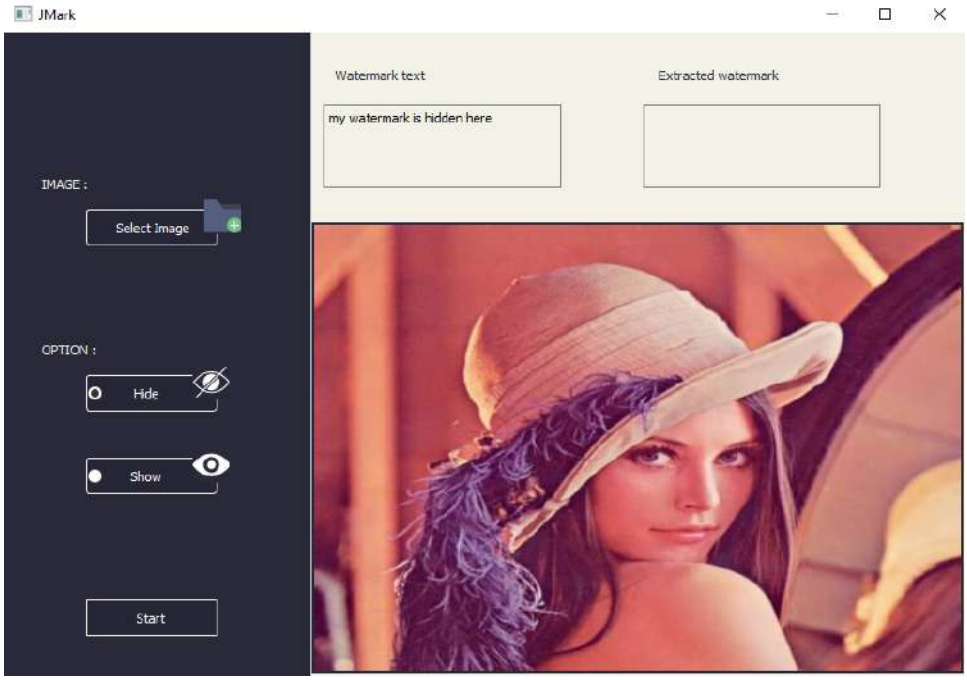

Figure 3.7: Interface graphique de l'application lors l'insertion du tatouage

3.4.3 Processus d'extraction du tatouage

L'extraction du tatouage s'effectue par le choix d'image tatouée et l'option "show",puis début de l'opération et le message est afficher dans la zone du text.

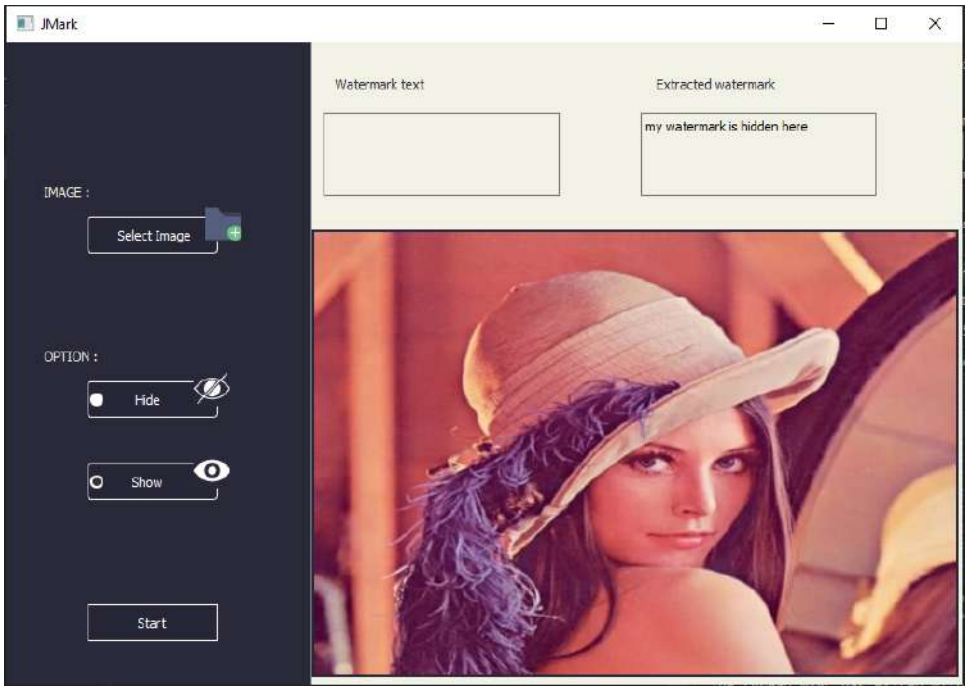

Figure 3.8: Interface graphique de l'application lors l'extraction du tatouage

3.5 Résultat obtenu

Dans cet section, nous évaluons les performances de notre méthode en termes d'imperceptibilité ,capacité et robustesse. Les résultats expérimentaux sont séparés en trois parties : la premiére est consacrée au teste de la propriété d'imperceptibilité alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques standards et plus intéressante,et la troisième partie on a montrer la capacité d'insertion de notre algorithme.

3.5.1 Propriété d'imperceptibilité

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, plusieurs images couleurs RGB de taille différents sont tatouées avec un text simlaire. Une image hote et l' image tatouée sont présentées Au-dessus:

(a) Figure X (Original) (b) Figure Y (Tatouée)

Figure 3.9: Comparaison entre Images

À partir des images on peut voir qu'il est difficile de différencier entre l' image originale et l'images tatouée.Pour évaluer concrètement la qualité de notre méthode, on utilise quelqes métrics d'evaluation parmi ceux qu'on a expliquer précédement (PSNR ,SSIM) .

image	taille	PSNR	SSIM
Monalisa	256*256	46.5321	0.9984
pepper	256*256	51.3954	0.9998
lena	512*512	47.5427	0.9996
mini	640*560	53.9392	0.9997
moon	800*640	56.3797	0.9978
tiger	1024*1024	57.7929	0.9995
nature	1024*1024	59.6869	0.9999

Tableau 3.1: Mesures de la qualité d'images tatouée

3.5.2 Propriété de robustesse

3.5.2.1 Filtre de gaussian

Figure 3.10: Monalisa gaussian filtre gaussian

Le résultat représente l'image tatouée aprés le filtrage. La tentative d'extraction du message a échoué, ce qui veut dire qu'en appliquant le filtre Blur Gaussian, le message a été détruit complètement. Nous concluons que notre méthode n'est pas robuste à ce filtre.

3.5.2.2 Compression

Figure 3.11: Lena compressée

Nous avons testé cela sur une image tatoué (lena)qui contient le message (my watermark is hidden here). Nous avons effectué l'extraction du message à partir de l'image tatoué compressée. cela veut dire que notre méthode est robuste face au compression .

3.5.2.3 Attaque Sharpene

Figure 3.12: Moon Sharpene Filtre

Nous avons testé cela sur une image tatoué (moon)qui contient le message (moon watermarked). Nous avons effectué l'extraction du message à partir de l'image tatoué filtrée. cela veut dire que notre méthode est robuste face au attaque sharpen .

3.5.2.4 La rotation

Figure 3.13: Image mini tournée °90

La tentative d'extraction du message a échoué donc notre méthode est fragile contre ce type d'attaque , car la rotation de l'image cause le déplacement des blocs tatoués.

3.5.3 Capacité

Concernant la capacité, l'application de la DCT sur les image RGB met à notre disposition un espace important car on peut cacher l'information dans trois canals de couleurs ,Prenons comme exemple une image de taille 512*512 .

$$((512 \times 512)/(8 \times 8) = 4096 \tag{3.1}$$

4096 bits par canal , pour une image de tel taille c'est une capacité énorme. Ceci c'est la capacité maximal mais comme nous avons exliqué précédement qu'on doit prend on consideration de faire une régulation entre la capacité et l'imperceptibilité .

3.6 Conclusion

Dans ce chapitre, nous avons présenté les outils et méthode utilisés pour dévlopper notre application ,ensuit nous avons expliquer la phase d'insertion et la phase d'extraction de notre alorithme, en dernier lieu, nous avons montré les résultat obtenu en terme de contraintes de tatouage numérique.

Conclusion Général

Le tatouage numérique a été réalisé comme une technique intéressante pour la sécurité des images et des données : L'intégrité, la confidentialité et l'authentification.Notre objectif est de vérifier les trois propriétés de sécurité ensemble, dans ce cas le tatouage doit trouver un meilleur compromis entre deux critères : l'imperceptibilité et la robustesse pour garantir l'authentification et la protection des images.

Au cours de ce mémoire nous avons étudié la problématique liée au tatouage numérique des images, ainsi la notion d'image numérique. Nous avons présenté une méthode de tatouage qui a permis d'assurer l'intégrité des images . Notre travail a porté sur le développement d'une technique de tatouage d'images couleurs RGB .Ce travail prend en compte la détection aveugle du tatouage et le bon compromis entre la qualité visuelle d'images tatouée et la robustesse contre des attaques connues. Le tatouage est inséré dans le domaine transformé, la transformation est effectuée en appliquant la DCT sur des blocs de taille 8×8 , précisément cette taille car elle offre un équilibre entre le temps de calcul et l'information traité.

La suite de notre travail visait d'abord à évaluer notre méthode en utilisant des métrics d'évaluation , ce qui a donnait des trés bon résultats montrent l'impercemptibilité et que notre approche permet d'obtenir une haute qualité d'images tatouées,ensuite l'analyse des performances de la méthode développée face à un ensemble d'attaques. Les résultats obtenus sont satisfaisants, puisqu'ils démontrent une semi-fragilité du schéma face à une variété d'attaques ce qui assure un compromis entre l'authentification et la protection d'images .

Les perspectives ouvertes par notre travail peuvent être résumés dans les points suivants :

1. s'orienter vers d'autres applications, en dehors du contexte du watermarking, telles que La steganographie.

2. développer notre algorithme pour l'utilsé sur le tatouage video.

3. améliorer notre travail concernant les critère robustesse / fragilité.

Bibliographie

[1] C. Rey, "Tatouage d'image: gain en robustesse et intégrité des images." Avignon, 2003.

[2] D. Kirovski, *Multimedia watermarking techniques and applications.* Auerbach Publications, 2006.

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

[4] K. Stefan and A. Fabien, "Information hiding techniques for steganography and digital watermarking," *Artech House, London, UK*, 2000.

[5] R. Riad, "Tatouage robuste d'images imprimées," Ph.D. dissertation, 2015.

[6] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, *Digital watermarking.* Springer, 2017.

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

[8] P. Bas, J.-M. Chassery, and B. M. Macq, "Robust watermarking based on the warping of predefined triangular patterns," in *Security and Watermarking of Multimedia Contents II*, vol. 3971. International Society for Optics and Photonics, 2000, pp. 99–109.

[9] T. Furon, "Application du tatouage numérique à la protection de copie," Ph.D. dissertation, Paris, ENST, 2002.

[10] J. Chou, S. S. Pradhan, L. El Ghaoui, and K. Ramchandran, "Watermarking based on duality with distributed source coding and robust optimization principles," in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, vol. 1. IEEE, 2000, pp. 585–588.

[11] S. Craver, N. Memon, B.-L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," *IEEE Journal on selected Areas in communications*, vol. 16, no. 4, pp. 573–586, 1998.

[12] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," in *Proceedings of International Conference on Image Processing*, vol. 1. IEEE, 1997, pp. 528–531.

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

[14] Wikipédia, "Image numérique — wikipédia, l'encyclopédie libre," 2020, [En ligne; Page disponible le 8-janvier-2020]. [Online]. Available: http://fr.wikipedia.org/w/index.php?title=Image_num%C3%A9rique&oldid=166159206

[15] D. Battikh, "Sécurité de l'information par stéganographie basée sur les séquences chaotiques," Ph.D. dissertation, Rennes, INSA, 2015.

[16] M. Tkalcic and J. F. Tasic, *Colour spaces: perceptual, historical and applicational background*. IEEE, 2003, vol. 1.

[17] N. Vandenbroucke, "Segmentation d'images couleur par classification de pixels dans les espaces d'attributs colorimétriques adaptés: application à l'analyse d'image," Ph.D. dissertation, ANRT [diff.], 2000.

[18] Y. NEDJAR and I. MOUSSI, "Application des méthodes numériques de traitement d'image sous android." Ph.D. dissertation.

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

[20] Wikipédia, "Transformation de fourier discrète — wikipédia, l'encyclopédie libre," 2019, [En ligne; Page disponible le 12-décembre-2019]. [Online]. Available: http://fr.wikipedia.org/w/index.php?title=Transformation_de_Fourier_discr%C3%A8te&oldid=165340100

[21] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transform," *IEEE transactions on Computers*, vol. 100, no. 1, pp. 90–93, 1974.

[22] D. Marshall, "Transformation de cosinus discrète," 2001.

[23] L. Diane, "Cours de traitement d'images," *Laboratoire I3S Informatique, Signaux et Systèmes, Université de Nice Sophia Antipolice, Rapport de recherche ISRN I3S/RR*, vol. 22, 2005.

[24] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures*. Springer Science & Business Media, 2001, vol. 1.

[25] L. K. Saini and V. Shrivastava, "A survey of digital watermarking techniques and its applications," *arXiv preprint arXiv:1407.4735*, 2014.

[26] Y. A. Al-Najjar, D. C. Soong *et al.*, "Comparison of image quality assessment: Psnr, hvs, ssim, uiqi," *Int. J. Sci. Eng. Res*, vol. 3, no. 8, pp. 1–5, 2012.

[27] Y. Wu, J. P. Noonan, S. Agaian *et al.*, "Npcr and uaci randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology,*

Journal of Selected Areas in Telecommunications (JSAT), vol. 1, no. 2, pp. 31–38, 2011.

[28] M. Sandilya and M. Chawla, "Spatial domain image steganography based on security and randomization," *Editorial Preface*, vol. 5, no. 1, 2014.

[29] Wikipédia, "Qt — wikipédia, l'encyclopédie libre," 2020, [En ligne; Page disponible le 16-mai-2020]. [Online]. Available: http://fr.wikipedia.org/w/index.php?title=Qt&oldid=170935077