MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE FERHAT ABBAS –SETIF 1-
UFAS (ALGERIE)

MEMOIRE

Présenté à la faculté de Technologie

Département d'Electronique

Pour l'obtention du Diplôme de

MAGISTER

Option : Communication

Par

Mr. ATTALLAOUI Ahmed

THEME

Technique de protection de biens numériques par un filigrane texte ou image

Soutenu le : 24 / 12 / 2014 devant la commission d'examen :

Mr. A. FERHAT HAMIDA	Prof à l'université de Sétif -1-	Président
Mr. N.BOUKEZZOULA	MCA à l'université de Sétif -1-	Rapporteur
Mr. F.DJAHLI	Prof à l'université de Sétif -1-	Examinateur
Mr. A.BARTIL	MCA à l'université de Sétif -1-	Examinateur

Remerciements

Avant tout, je remercie "**Allah**"le tout puissant de m'avoir donné la force et le courage pour accomplir ce travail. Mes sincères remerciements vont à mon encadreur le ***Dr. BOUKEZZOULA Naceur-Eddine.***

Je remercie aussi tous les enseignants et les responsables du département d'électroniques de l'université de SETIF 1.

Je tiens à remercier également le le ***Pr. Ferhat Hamida Abdelhak*** d'avoir accepter de présider ce jury.

Mes remerciements sont également aux membres de jury le ***Pr. Farid Djahli*** et le ***Dr. Bertil Arrés*** .

Je remercie aussi .me familles, mes amis et collègues, et tous ceux qui de prés ou de loin qui ont contribué à la réalisation de mes travail.

Dédicaces

Je dédié ce modeste travail à :

- Mes parents.
- Mes frères et sœurs.
- Tous mes amis.
- Toute personne ayant contribuée de près ou de loin à l’accomplissement de ce travail.
- Tous mes proches.

SOMMAIRE

SOMMAIRE

CHAPITRE II : TATOUAGE NUMERIQUE, CONCEPTS DE BASE ET TERMINOLOGIES

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS

CMJN **C**yan, **M**agenta, **J**aune et **N**oir

DCT **D**iscrete **C**osine **T**ransform

DFT **D**iscrete **F**ourier **T**ransform

DPI **D**ots **P**er **I**nch

GIF **G**raphical **I**nterchange **F**ormat

JPEG **J**oint **P**hotographic **E**xperts **G**roup

KLT **T**ransformation de **K**arhunen-**L**oève

LSB **L**east **S**ignificant **B**it

LZW **C**odage **L**empel-**Z**iv-**W**elch

MSE **M**ean **S**quare **E**rror

NC **C**orrélation **N**ormale

PAO **P**ublication **A**ssistée par **O**rdinateur

PPP **P**ixels **P**ar **P**ouce

PSNR **P**eak **S**ignal **N**oise **R**atio

RVB **R**ouge, **V**ert et **B**leu

SVD La **D**écomposition en **V**aleurs **S**ingulières

SVH **S**ystème **V**isuel **H**umain

TIFF **T**agged **I**mage **F**ile

WHT **W**alsh-**H**adamard **T**ransform

Résumé

Ce travail présente un tatouage d'image avec détection aveugle basée sur la modulation d’amplitude. Fondamentalement, l’intégration de filigrane est réalisée en modifiant les valeurs des pixels dans le canal bleu d'une image, tandis que la récupération du filigrane est obtenue en utilisant une technique de prédiction basée sur une combinaison linéaire des valeurs des pixels voisins autour des pixels intégrés. Les résultats expérimentaux obtenus montrent clairement l’efficacité et la robustesse de la méthode proposée et présentent une légère amélioration par rapport à celles des méthodes de tatouage d’images par la modulation d’amplitude publiées.

Mot clés : filigrane, amplitude, modulation, prédiction.

Introduction générale

Introduction générale

L'ère numérique que nous traversons depuis quelques années a permis un accès à l'information bien plus aisé que par le passé. Les documents numériques étant immatériels, leur diffusion est extrêmement rapide et peu coûteuse. Les réseaux et les supports numériques de forte capacité facilitent les échanges de documents [01].

Avec l'apparition de ces nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité. Une image numérique, diffusée par exemple sur Internet, peut être aisément copiée puis rediffusée sur un réseau ou stockée sur CD-ROM sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le ***tatouage*** ou ***watermarking***. Le principe des techniques dites de tatouage d'images consiste en l'insertion d'une marque imperceptible dans l'image. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée "signature", correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelque soit les attaques (licites ou illicites) que l'image tatouée subit, la marque doit rester présente tant que l'image reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée). De nombreux algorithmes ont été présentés récemment et certains produits sont même commercialisés, cependant, aucun d'eux ne satisfait pleinement au cahier des charges idéal [02].

Le travail présenté dans ce mémoire a pour objectif de proposer une méthode de tatouage des images numériques fondée sur la modulation d'amplitude. Le principe consiste en l'insertion d'une signature dans l'image en exploitant le plan de bleu.

Le présent mémoire est organisé en quatre chapitres :

Le premier chapitre présente les images numériques d'une manière générale. Nous nous intéresseront au processus de numérisation, au codage des images numériques et enfin à quelques aspects du traitement d'image, tels que le filtrage, la compression et le tatouage.

Le deuxième chapitre présente assez largement la discipline du tatouage des images numériques. Nous revenons sur les origines du tatouage et nous exposons les principes des processus de tatouage et leurs spécificités. Après avoir étudié les méthodes développées les plus représentatives de l'état de l'art, nous présentons une revue des attaques visant à empêcher la détection de la marque.

Le troisième chapitre présente l'étude et l'implémentation d'une méthode de tatouage d'images basée sur la modulation d'amplitude.

Le dernier chapitre présente l'essentiel de notre travail et les différentes étapes nécessaires à la mise en œuvre de la technique de tatouage proposée, ainsi que les résultats obtenus et les performances de méthode de tatouage préposée. L'ajout d'une signature et la prédiction de tatouage s'appuie sur une étude psychovisuelle de l'image, afin d'optimiser le compromis robustesse/invisibilité.

Nous terminons par une conclusion générale et quelques perspectives.

CHAPITRE I:

Généralités sur les images.

I-1. Introduction

L'image est un support d'information très performant, et comme on dit : une image vaut plus que mille mots. Vu l'importance de l'image, et la grande quantité d'information qu'elle peut contenir, le monde s'intéresse de plus en plus à l'image et tends vers l'universalisation de son utilisation. En effet, l'image a touché plusieurs domaines de notre vie : la médecine, la météo, la télécommunication, la cartographie, la géologie, etc.

Avec le développement de l'outil informatique, plusieurs techniques de traitement des images ont vu le jour [03].

I-2. Les images numériques et le système visuel humain

L'étude de la perception visuelle est intéressante pour le traitement d'images pour deux raisons principales. La première est qu'elle peut nous mettre sur la voie de nouveaux algorithmes reflétant les mécanismes naturels. Et la seconde est quelle nous permet de connaître les limites de notre perceptions. Ainsi, il est par exemple inutile de représenter plus de couleurs que nous pouvons en percevoir lors d'une application de visualisation.

Dans un système d'analyse d'images, on distingue la lumière captée par un récepteur (camera), transmise par des transmetteurs (câbles ou autres) à l'analyseur (l'ordinateur). On peut effectuer la même décomposition avec la perception visuelle. La lumière est captée par l'œil, l'information visuelle est transmise via les nerfs optiques vers l'analyseur qui est le cerveau [04].

La perception visuelle est un mécanisme complexe qui met en jeu plusieurs structures : l'œil, la rétine et le cerveau. La compréhension de ce mécanisme repose sur la modélisation du SVH (Système Visuel Humain) en vue d'en simuler son fonctionnement.

Le SVH est un système sophistiqué qui détecté et agit sur des stimuli visuels. Intuitivement, la vision par ordinateur et la vision humaine semblent avoir la même fonction. Le but des deux systèmes est d'interpréter des données spatiales. Même si l'ordinateur et la vision de l'homme sont Fonctionnellement similaires, on ne peut pas s'attendre à un système de vision par ordinateur pour reproduire exactement la fonction de l'œil humain. Cela s'explique en partie parce que nous ne comprenons pas entièrement comment l'œil fonctionne. En fait, certaines des propriétés de l'œil humain sont utiles pour ´élaborer des

techniques de vision par ordinateur, alors que d'autres sont en fait pas souhaitables dans un système de vision par ordinateur. Mais il existe des techniques de vision par ordinateur qui peuvent être reproduites dans une certaine mesure et, dans certains cas, améliorés même sur le SVH. Pour mieux comprendre ce qu'est une image numérique, voyons d'abord ce qu'est une image et comment fonctionne le SVH.

Dans le SVH, l'élément sensible est l'œil à partir duquel les images sont transmises via le nerf optique au cerveau, pour un traitement ultérieur. Le nerf optique a une capacité insuffisante pour transporter toutes les informations perçues par l'œil. En conséquence, il doit y avoir de prétraitement avant que l'image ne soit transmise par le nerf optique.

Le SVH peut être modélisé en trois parties :

1. *L'œil* : il s'agit d'un modèle physique puisqu'une grande partie de sa fonction peut être déterminée par pathologie ;

2. *Le système nerveux* : il s'agit d'un modèle expérimental, puisque sa fonction peut être modélisée, mais ne peut pas être déterminée avec précision ;

3. *Le traitement par le cerveau* : c'est un modèle psychologique puisque nous ne pouvons pas modéliser le traitement directement, mais nous pouvons seulement déterminer le comportement par l'expérience et la déduction [05].

Tout d'abord, pour obtenir une image, il faut de la lumière. Cette dernière est émise d'une ou plusieurs sources telles que le soleil, des spots, des néons, etc. Cette lumière est représentée par des rayons qui partent de la source dans toutes les directions.

Généralement, lorsqu'un rayon de lumière rencontre un objet, ce dernier en absorbe une partie correspondant à sa couleur, et disperse le reste en une infinité de rayons qui peuvent éventuellement être captés par un œil annonçant la présence de l'objet ainsi que sa couleur. Pour recevoir ces rayons, l'œil est équipé d'un appareil optique complet illustré par la Figure (I.1).

– *L'iris* sert de diaphragme il s'ouvre et se ferme pour accepter plus ou moins de lumière.

– *Le Cristallin* fait la mise au point en fonction de la distance de l'objet [04].

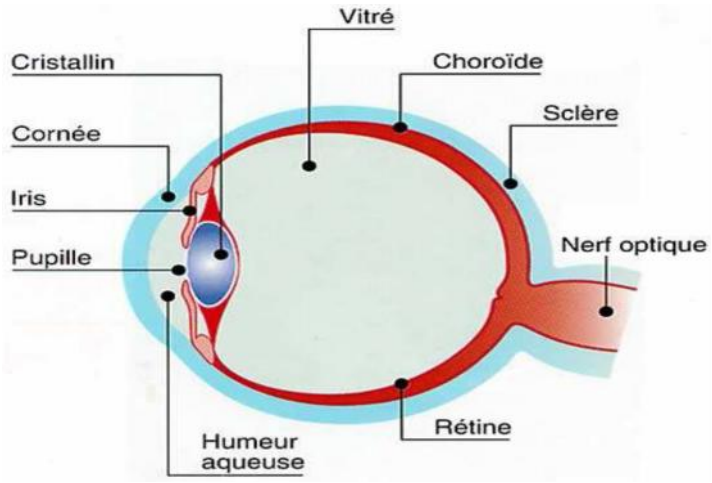


Figure I.1: L'œil, note capteur.

Finalement, cette lumière arrive sur des capteurs placés sur la rétine appelés cellules à cônes et cellules à bâtonnets du fait de leur forme. Les cellules à bâtonnets, plus sensibles, sont spécialisées dans la vision nocturne. Les cellules à cônes, plus précises, sont séparées en trois types, chacun étant plus sensible à une couleur qu'aux autres. C'est ce découpage de l'image en trois couleurs primaires que vient la vision des couleurs.

Ces informations sont ensuite transmises au cerveau par le nerf optique. C'est le cerveau qui réalise ensuite la partie la plus complexe de regroupement de toutes ces informations pour former une image mentale en couleur de notre environnement [06].

Du point de vue fonctionnel, l'œil peut être comparé à un appareil photo et la rétine à la pellicule photographique (Figure I.2). En effet, le rôle de l'appareil photo est de concentrer sur le film une image nette ni trop sombre ni trop lumineuse. On y parvient grâce à la bague de mise au point qui met l'objet au foyer et au diaphragme qui s'ouvre et se ferme pour laisser passer juste la bonne quantité de lumière pour la sensibilité du film [07].

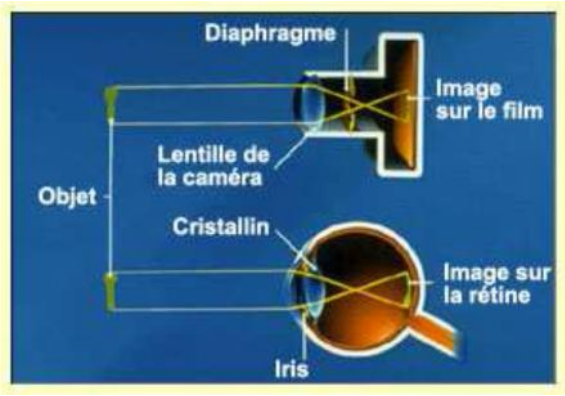


Figure I.2: Analogie entre l'œil et l'appareil photo.

L'animation des images est basée sur le phénomène suivant : Lorsqu'une cellule capte de la lumière, l'impression lumineuse persiste pendant environ 1/50s. En effet, quand l'image change rapidement, l'œil n'est pas assez rapide pour percevoir une succession d'images fixes et croit voir un mouvement continu [05].

I-3. Définition de l'image

L'image est une représentation d'une personne ou d'un objet par la peinture, la sculpture, le dessin, la photographie, le film,…etc. C'est aussi un ensemble structuré d'informations qui, après affichage sur l'écran, ont une signification pour l'œil humain.

Elle peut être décrite sous la forme d'une fonction I(x,y) de brillance analogique continue, définie dans un domaine borné, tel que x et y sont les coordonnées spatiales d'un point de l'image et I est une fonction d'intensité lumineuse et de couleur. Sous cet aspect, l'image est inexploitable par la machine, ce qui nécessite sa numérisation [08].

I-4. Image Numérique

Contrairement aux images obtenues à l'aide d'un appareil photo (analogique), ou dessinées sur du papier, les images manipulées par un ordinateur sont numériques (représentées par une série de bits). L'image numérique est l'image dont la surface est divisée en éléments de tailles fixes appelés cellules ou pixels, ayant chacun comme caractéristique un niveau de gris ou de couleurs prélevé à l'emplacement correspondant dans l'image réelle, ou calculé à partir d'une description interne de la scène à représenter [09].

La numérisation d'une image est la conversion de celle-ci de son état analogique (distribution continue d'intensités lumineuses dans un plan xOy) en une image numérique représentée par une matrice bidimensionnelle de valeurs numériques X(n,m) où : n, m sont les coordonnées cartésiennes d'un point de l'image et X(n,m) le niveau de gris ou de couleur en ce point .

I-5. Caractéristiques d'une image numérique

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants:

I-5-1. Pixel

Contraction de l'expression anglaise " Picture élément ": élément d'image, le pixel est le plus petit point de l'image, c'est une entité calculable qui peut recevoir une structure et une quantification. Si le bit est la plus petite unité d'information que peut traiter un ordinateur, le pixel est le plus petit élément que peuvent manipuler les matériels et logiciels d'affichage ou d'impression.

La quantité d'information que véhicule chaque pixel donne des nuances entre images monochromes et images couleurs. Dans le cas d'une image monochrome, chaque pixel est codé sur un octet, et la taille mémoire nécessaire pour afficher une telle image est directement liée à la taille de l'image.

Dans une image couleur (R.V.B.), un pixel est représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B).

I-5-2. La définition (dimension de l'image)

La définition de l'image est le nombre fixe de pixels qui est utilisé pour représenter l'image dans ses deux dimensions. Pour une image numérique donnée, plus la définition est grande, plus la précision des détails sera élevée. Ce nombre de pixels détermine directement la taille des informations nécessaire au stockage de l'image (du fichier numérique brut). La dimension, en pixels, détermine le format d'affichage à l'écran (la taille des pixels de l'écran étant fixe) .

Nombre de pixels constituant l'image = nombre de lignes x nombre de colonnes.

I-5-3. La résolution

La résolution est le nombre de pixels par unité de longueur, Plus la résolution est élevée (plus le pas de discrétisation est faible), mieux les détails seront représentés. A titre indicatif, le théorème de Shannon indique qu'il est nécessaire d'utiliser une fréquence d'échantillonnage deux fois plus élevée que celle du signal à représenter.

La résolution d'image se mesure en "pixels par pouce" (ppp) équivalent à "dots per inch" (dpi) .

I-6. Numérisation

C'est le moyen technique de transformer de l'information. Il permet le passage d'un phénomène appréhendé de manière analogique (par exemple le son, la couleur, la lumière appréhendés par l'homme de façon continue et globale), à un phénomène appréhendé de manière numérique à l'aide de nombres en mode binaire 0 et 1. Toute opération de numérisation comporte deux phases : une phase d'échantillonnage, suivie d'une phase de quantification.

La représentation informatique d'une image est nécessairement discrète, alors que l'image est de nature continue. Si on regarde de près, la transformation d'un signal analogique 2D nécessite à la fois une discrétisation de l'espace : c'est l'échantillonnage, et une discrétisation des couleurs : c'est la quantification. Le processus de numérisation d'une image suit les étapes suivantes .

I-6-1. Echantillonnage

l´échantillonnage est le procède de discrétisation spatiale d'une image consistant à associer à chaque pixel R(x,y) une valeur unique I(x,y) (Figure I.3). On parle de sous échantillonnage lorsque l'image est déjà discrétisée et qu'on diminue le nombre de pixels [10].

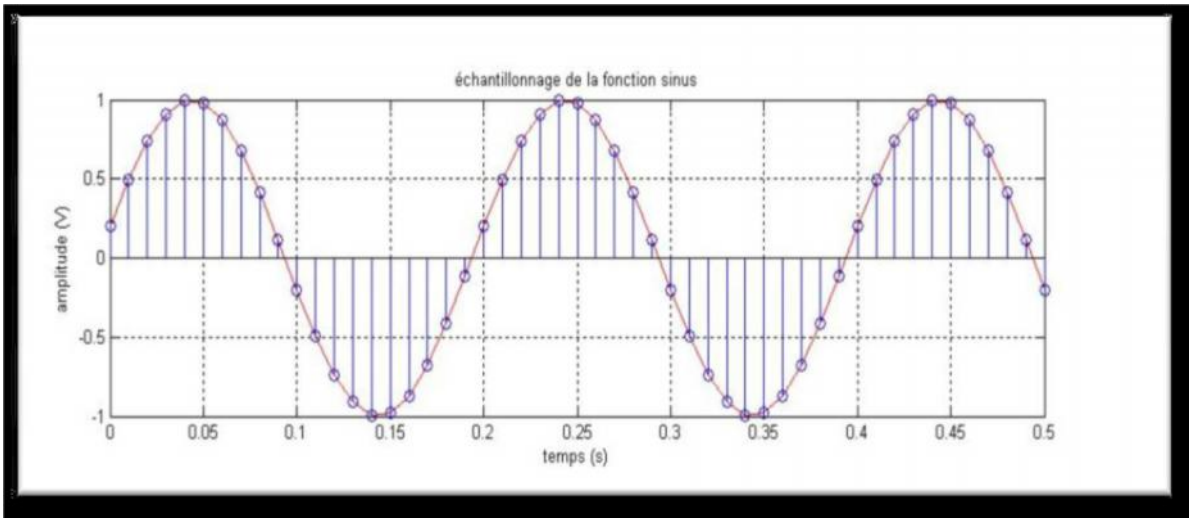


Figure 1.3: Echantillonnage de la fonction sinus

I-6-2.Quantification

La quantification désigne la discrétisation tonale correspondant à la limitation du nombre de valeurs différentes que peut prendre chaque pixel. Idéalement, le nombre de valeurs différentes devrait d´éprendre de l'amplitude des grandeurs observées (réflectance de la lumière visible, luminance infrarouge, ...) dans la scène. Mais en pratique, le nombre de valeurs utilisées pour coder une image lors de son acquisition dépend de la capacité effective du capteur à observer des signaux de grandeurs différentes, qui s'assimile à un rapport signal sur bruit [12], [13].

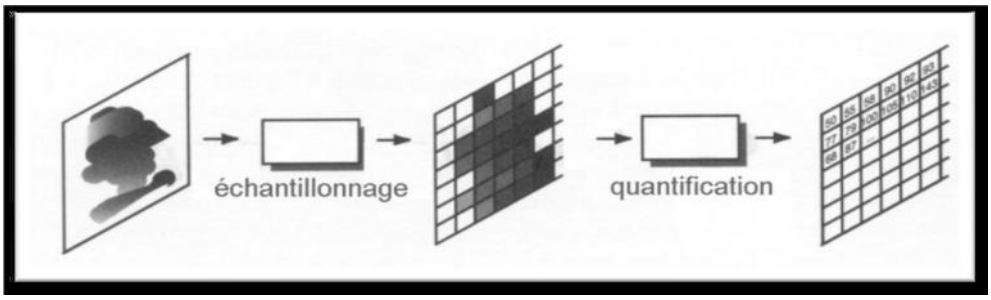


Figure 1.4: Echantillonnage et quantification.

I-6-3. Le codage

Les niveaux de quantification sont codés sous la forme d'un mot binaire sur k bits $\Rightarrow 2^k$ niveaux possibles [14].

I-6-3-1. Codage d'une image binaire

On code chaque pixel sur 1 bit (0 ou 1) permettant de définir deux couleurs : noir ou blanc. Le 0 pour le noir, et le 1 pour le blanc. L'image de 1000 pixels par exemple occupe donc 1000 bits en mémoire. Ce type de codage peut convenir pour un plan ou un texte mais on voit ses limites lorsqu'il s'agit d'une photographie [12].

I-6-3-2. Codage d'une image en niveaux de gris

Si on code chaque pixel sur 2 bits on aura 4 possibilités (noir, gris foncé, gris clair, blanc). L'image codée sera très peu nuancée.

En général on code chaque pixel sur 8 bits = 1 octet. On a alors 256 possibilités (on dit 256 niveaux de gris). L'image de 10 000 pixels codée occupe alors 10 000 octets en mémoire [10].

I-6-3-3. Codage d'une image en couleurs 24 bits

Il existe plusieurs modes de codage de la couleur. Le plus utilisé est le codage Rouge, Vert, Bleu (RVB). Chaque couleur est codée sur 1 octet = 8 bits. Chaque pixel sur 3 octets c'est à dire 24 bits : le rouge de 0 à 255, le vert de 0 à 255, le Bleu de 0 à 255.

Le principe repose sur la synthèse additive des couleurs : on peut obtenir une couleur quelconque par addition de ces 3 couleurs primaires en proportions convenables. On obtient ainsi 256 x 256 x 256 = 16777216 (plus de 16 millions de couleurs différentes) [15].

I-6-3-4. Codage d'une image en couleurs 8 bits

Dans ce cas on attache une palette de 256 couleurs à l'image. Ces 256 couleurs sont choisies parmi les 16 millions de couleurs de la palette RVB. Pour chaque image le programme recherche les 256 couleurs les plus pertinentes. Chaque code (de 0 à 255) désigne une couleur. L'image occupe 3 fois moins de place en mémoire qu'avec un codage 24 bits. L'image est moins nuancée : sa qualité est bonne mais moindre [15].

I-7. Représentation de la couleur

L'espace des couleurs primaires (RVB) est calqué sur notre perception visuelle. Il utilise trois couleurs de base : le rouge (λ = 700nm), le vert (λ = 546nm) et le blue (λ = 435, 8nm) ; où λ est la longueur de l'onde.

I-7-1. Synthèse additive de la lumière (mode RVB)

L'image est obtenue par superposition de trois rayonnements lumineux : le rouge (R), le vert (V) et le bleu (B). Dans le cas d'un écran cathodique, ces trois rayonnements sont obtenus en bombardant les luminophores photosensibles de l'écran.

Une image (RVB) est composée de la somme de trois rayonnements lumineux rouge, vert, et bleu dont les faisceaux sont superposés. A l'intensité maximale, ils produisent un rai de lumière blanche, et à l'extinction une zone aussi noire que l'éclairage ambiant le permet [04].

I-7-2. Synthèse soustractive de la lumière (mode CMJN)

La synthèse soustractive permet de restituer une couleur par soustraction, à partir d'une source de lumière blanche, avec des filtres correspondant aux couleurs complémentaires : Cyan (C), Magenta (M), Jaune (J). Ce procédé est utilisé en photographie et pour l'impression des couleurs. Si on soustrait la lumière Magenta de la lumière blanche (par exemple par un filtre), on obtient de la lumière verte. Si on soustrait la lumière Cyan, on obtient de la lumière rouge et si on soustrait la lumière jaune, on obtient de la lumière bleue. Si on soustrait à la fois la lumière magenta, Cyan et jaune (par exemple en superposant trois filtres), on n'obtient plus de lumière, donc du noir (que l'on note donc en toute logique :"N", comme Noir) [04], [15]. La gamme des couleurs reproductibles par le mode CMJN est plus restrictive que celle de la gamme RVB. Elle est, de surcroît, particulièrement sensible aux variations inévitables dues aux conditions mécaniques et physiques de l'impression en machine.

I-8. Stockage des images

Il existe de nombreux formats plus ou moins performants et ne permettant pas de faire les mêmes choses. Par ailleurs, certains éditeurs de logiciel créent leur format propriétaire, l'interopérabilité n'étant souvent pas assurée.

Techniquement, on peut distinguer les images matricielles (bitmap) et les images vectorielles. Les premières sont composées d'une matrice de points à plusieurs dimensions. En deux dimensions, cas le plus fréquent, les points sont nommés des pixels tout comme sur un moniteur d'ordinateur.

Les images vectorielles de leur côté utilisent des formules géométriques décrivant le contenu de l'image à afficher. Ainsi au lieu de mémoriser un ensemble de points comme c'est le cas pour l'image matricielle, seront mémorisées les opérations conduisant au résultat. Si cette méthode présente de nombreux avantages, il n'en faut pas moins passer par une conversion de l'image vectorielle en représentation matricielle pour l'afficher sur les moniteurs d'ordinateur actuels [15].

Les applications des images vectorielles sont multiples. Elles sont en effet très utilisées pour des applications de visualisation scientifique ainsi que pour la création Web (format flash), la PAO (Publication Assistée par Ordinateur) et surtout l'illustration. Ceci est en effet dû à plusieurs raisons.

La première vient de la taille des fichiers. Ceux-ci sont en effet très peu volumineux en comparaison des images bitmap. La seconde vient de la qualité et de la précision des images. Cela vient de la manière dont sont crées ces images. Comme son nom l'indique une image vectorielle est faite de vecteurs. Ainsi, pour créer une droite, il suffit de déterminer les coordonnées d'un des points de la droite ainsi que son orientation. Pour créer un segment, les coordonnées de début et de fin de segment suffisent. Un cercle sera défini par son centre et son rayon, etc. De même, les couleurs sont réparties en fonction d'équations mathématiques. Si l'on veut faire un dégradé, le principe est le même. Une autre chose très intéressante en dessin vectoriel, c'est que les objets ne s'écrasent pas entre eux. Chaque objet créé existe. Il faut alors définir pour chaque objet sur quelle couche il se situe, les zones dessinées des couches les plus´élevées masquant les zones des couches les plus basses. Ceci a comme énorme avantage que si l'on veut modifier des objets ou modifier la taille de l'image, la qualité restera la même. En effet, il suffit de recalculer les dimensions de chaque objet et les zones de couleur. Ainsi, il n'y a pas de perte d'information.

I-8-1. Formats d'image matricielle

I-8-1-1. JPEG

Ce format est l'un des plus complexes, son étude complète nécessite de solides bases mathématiques, cependant malgré une certaine dégradation il offre des taux de compressions plus qu'intéressants. JPEG est la norme internationale (ISO 10918-1) relative à la compression d'images fixes, notamment aux images photographiques. La méthode de compression est "avec pertes" et s'appuie sur l'algorithme de transformée en cosinus discrète DCT. Un mode "sans perte" a ensuite été développé mais n'a jamais été vraiment utilisé. Cette norme de compression a été développée par le comité JPEG (*Joint Photographic Experts Group*) et normalisée par l'ISO/JTC1 SC29. Ce type de compression est très utilisé pour les photographies, car il est inspiré des caractéristiques de perception visuelles de l'œil humain.

Le JPEG2000 est la norme internationale (ISO 15444-1). Elle apporte quelques améliorations au JPEG classique et notamment permet un réglage autorisant une compression sans perte ou encore la résistance aux erreurs de transmission. JPEG 2000 est relative à la compression d'images qui s'appuie sur un mécanisme de compression par ondelettes.

I-8-1-2.GIF

Le format GIF (*Graphical Interchange Format)* été créé en 1987 par Compuserve pour que les utilisateurs puissent s'échanger des images de façon efficace et moins onéreuse. Ce format permet une compression sans perte (algorithme LZW).

Il autorise une bonne compression et une décompression très rapide grâce à la méthode LZW. Cette compression est plus efficace pour les dessins et graphiques que pour les photographies numériques [13].

I-8-1-3. TIFF

Le format TIFF (*Tagged Image File) est* un ancien format graphique, permettant de stocker des images en noir et blanc, en couleurs réelles (True color, jusqu'à 32 bits par pixels) ainsi que des images indexées, faisant usage d'une palette de couleurs.

I-8-1-4. BMP

Le BMP est un des formats les plus simples développé conjointement par Microsoft et IBM, ce qui explique qu'il soit particulièrement répandu sur les plates formes Windows et OS/2. C'est un format ouvert et non compressé. Sa grande taille rend son utilisation en ligne difficile, mais sa grande compatibilité en fait un format de travail efficace. En BMP la couleur est codée en (RVB) (synthèse additive [13], [15].

I-8-1-5. PSD

Format natif de Photoshop, c'est un métafichier qui peut contenir du bitmap et du vectoriel. La couleur peut être codée sur 8, 16, 24 ou 32 bits, en Noir et Blanc, (RVB) et CMJN. Il gère la transparence, les couches alpha et peut prendre énormément de poids suivant le nombre de calques utilisés (chaque calque ajouté pèse !) [09].

I-8-2. Formats d'image vectorielle

I-8-2-1. PICT

PICT pour *Picture* de Apple est obsolète comparé aux autres formats disponibles. Le format PICT est le format standard d'images du monde Macintosh, toutes les applications de dessin sous cet environnement sont généralement capables d'exporter des images dans ce format. Les fichiers PICT peuvent provenir directement du Macintosh, ou encore être générés par des applications de dessin Windows comme Photoshop ou CorelDraw. L'utilisation du

format PICT à l'intérieur de la base de données permet de visualiser ces images à la fois sur Macintosh et sur PC. L'extension des fichiers PICT sous Windows peut être soit PIC, soit PCT, suivant le logiciel ayant généré l'image. Les fichiers PICT sont compressés ou non par QuickTime.

I-8-2-2. PS

PS pour *PostScript* utilisé avec la majorité des applications d'aujourd'hui, autant les logiciels de mise en pages, de traitement de textes et autres, il est possible d'exporter un document en format PS (PostScript) lequel pourra être acheminé vers un périphérique d'impression. Ce format est également une façon sûre de rendre disponible un document seulement pour impression sans droit de modification. Il s'agit toutefois d'un format très lourd à éviter lorsqu'il doit être transféré par Internet sur des liens à basse vitesse.

I-8-2-3. DXF

Le format DXF est un format créé par la compagnie AutoDesk pour son logiciel de CAO AUTOCAD. Bien qu'étant un format très répandu dans le monde de la conception et du dessin assisté par ordinateur, le format DXF est très peu répandu en d'autres domaines.

I-8-2-4. WPG

Le format WPG est un format utilisé par les logiciels de la gamme de WordPerfect (Word-Perfect, DrawPerfect, WP Presentations et autres) sous DOS, Windows ou Macintosh. Ce format donne un résultat acceptable lors de l'impression, mais qui doit surtout être utilisé en tant que format de travail. D'autant plus que ce n'est pas un format qui est reconnu par tous les logiciels [04], [19].

I-9. Aspects du traitement d'images

Dans cette section, nous présentons les trois aspects du traitement d'images qui nous intéressons : filtrage, compression et tatouage.

I-9-1. Filtrage

Pour améliorer la qualité visuelle de l'image, on doit éliminer les effets des bruits (parasites) en lui faisant subir un traitement appelé filtrage. Le filtrage consiste à appliquer une transformation (appelée filtre) à tout ou à une partie d'une image numérique en appliquant un opérateur.

Définition de Filtre

Un filtre est une transformation mathématique permettant, pour chaque pixel de la zone à laquelle il s'applique, de modifier sa valeur en fonction des valeurs des pixels avoisinants, affectées de coefficients [21].

Le filtre est représenté par un tableau (matrice), caractérisé par ses dimensions et ses coefficients, dont le centre correspond au pixel concerné. Les coefficients du tableau déterminent les propriétés du filtre.

Définition de Bruit

Le bruit caractérise les parasites ou interférences d'un signal, c'est-à-dire les parties du signal déformées localement. Ainsi le bruit d'une image désigne les pixels de l'image dont l'intensité est très différente de celles des pixels voisins [21].

Le bruit peut provenir de différentes causes :

- Environnement lors de l'acquisition.
- Qualité du capteur.
- Qualité de l'échantillonnage.

I-9-1-1. Filtre passe-bas (lissage)

Un filtre passe-bas accentue les éléments qui ont une basse fréquence spatiale tout en atténuant les éléments à haute fréquence spatiale (pixels foncés). Il en résulte une image qui apparaît plus homogène (un peu floue) particulièrement en présence d'arêtes. Ce type de filtrage est généralement utilisé pour atténuer le bruit de l'image, c'est la raison pour laquelle on parle habituellement de lissage.

Lors de l'application du filtre, une nouvelle valeur de pixel est générée en tenant compte du voisinage de chaque pixel de l'image originale. Une fenêtre de 3 pixels sur 3 ou plus, sert à prélever les pixels du voisinage dont on utilisera les statistiques. Plus la fenêtre est grande, plus le lissage sera important (ce qui produira une image très floue). En appliquant une pondération aux éléments de la fenêtre, il est possible d'accentuer certains ´éléments directionnels de l'image. Parce qu'un filtre passe-bas tend à rendre une image plus lisse, les plages de l'image apparaissent plus homogènes. Les filtres passe-bas sont donc très utiles pour réduire le bruit d'une image [22]. Parmi les filtres passe-bas, on cite : les filtres moyenneur, médian et gaussien .

I-9-1-2. Filtre moyenneur

Ce filtre très simple préserve la radiométrie mais tend à brouiller les parties texturées de l'image. Ce lissage de l'image est souhaitable lorsque l'on applique le filtre en tant que filtre spatial. Les fenêtres de grande dimension reflètent les fréquences spatiales les plus basses alors que les fenêtres plus petites reflètent les fréquences spatiales basses et intermédiaires [23].

I-9-1-3. Filtre médian

Le filtre médian préserve l'information texturale plus efficacement que le filtre moyenneur. Toutefois, le filtre modifie l'information radiométrique et ne préserve pas la signature des cibles ponctuelles. Lorsqu'on se sert de ce filtre comme filtre spatial, il préserve bien les arêtes tout en lissant des données [23].

I-9-1-4. Filtre gaussien

Un filtre o'u tous les éléments du filtre sont pondérés selon une distribution gaussienne (distribution normale). Selon la dimension du filtre, la convolution de ce filtre avec une image donne une image plus ou moins lissée (une petite dimension de filtre donne une image peu lissée) [23].

En pratique, il faut choisir un compromis entre l'atténuation du bruit et la conservation des détails et contours significatifs.

I-9-1-5. Filtre passe-haut (accentuation)

Les filtres passe-haut atténuent les composantes de basse fréquence de l'image et permettent notamment d'accentuer les détails et le contraste, c'est la raison pour laquelle le terme de "filtre d'accentuation" est parfois utilisé [21]. Ce filtre n'affecte pas les composantes de haute fréquence d'un signal, mais doit atténuer les composantes de basse fréquence.

Un filtre passe haut favorise les hautes fréquences spatiales, comme les détails, et de ce fait, il améliore le contraste. Toutefois, il produit des effets secondaires [22] .

– Augmentation du bruit : dans les images avec un rapport Signal/Bruit faible, le filtre augmente le bruit granuleux dans l'image.

– Effet de bord : il est possible que sur les bords de l'image apparaisse un cadre. Mais cet effet est souvent négligeable et peut s'éliminer en tronquant les bords de l'image [22].

I-9-1-6. Filtre passe-bande (différentiation)

Cette opération est une dérivée du filtre passe-bas. Elle consiste à éliminer la redondance d'information entre l'image originale et l'image obtenue par filtrage passe-bas. Seule la différence entre l'image source et l'image traitée est conservée. Les filtres différentiels permettent de mettre en évidence certaines variations spatiales de l'image. Ils sont utilisés comme traitements de base dans de nombreuses opérations comme le rehaussement de contraste ou la détection de contours [22].

I-9-1-7. Filtre directionnel

Dans certains cas, on cherche à faire apparaître des détails de l'image dans une direction bien déterminée. Pour cela, on utilise des filtres qui opèrent suivant des directions (horizontales, verticales et diagonales).

I-9-2. Compression

Certes, les capacités de disques durs de nos ordinateurs et le débit des réseaux ne cessent d'augmenter. Mais notre utilisation de l'image et les capacités d'acquisition des capteurs numériques s'accroissent tout autant.

De nombreux autres appareils numériques ont fais leurs apparitions. Il ne faut pas parler uniquement de mémoire pour un ordinateur mais également pour un assistant

personnel (PDA), pour un téléphone portable, un GPS, un appareil photo numérique, etc., et les applications actuelles n'envisagent plus de se passer de l'image. Une page web sans image, l'imaginez-vous encore ?

A quand la disparition du SMS pour le MMS ? Acceptez-vous d'attendre avant de commencer à visualiser un film acheté sur un service de vidéo à la demande sur Internet ?

Dans d'autres domaines professionnels tels que l'imagerie médicale, des masses gigantesques de données sont acquises chaque jour. On chiffre à environ dix téraoctets la masse de données produites annuellement dans un service radiologique d'un hôpital dans un pays industrialisé. La compression d'images est donc encore plus d'actualité aujourd'hui [04].

I-9-2-1. Objectif de la compression

En fonction de l'application recherchée, différentes qualités vont être demandées à un algorithme de compression. Parmi elles, on cite la rapidité de la compression et de la décompression.

En effet, il serait dommage, dans une application de transmission, que le temps gagné par une réduction de la taille des données à transmettre soit inférieur au temps passé à la compression ou décompression. Cette qualité sera cependant moins cruciale dans des applications visant à l'archivage de données.

Viennent ensuite deux qualités antagonistes : le taux de compression et la qualité de l'image après un cycle de compression/décompression. Il existe des algorithmes de compression sans pertes mais dont le taux de compression est limité. Les algorithmes avec perte d'informations peuvent obtenir de meilleurs taux de compression mais en jouant sur les dégradations. Selon l'application visée, on voudra obtenir une qualité suffisante pour distinguer certaines informations, ou bien une qualité visuelle parfaite du point de vue d'un humain, ou bien encore conserver la qualité la meilleure possible afin de pouvoir effectuer des traitements ultérieurs sur l'image et éviter des artefacts dûs à la compression [04].

I-9-2-2. Notions générales

Définition de Histogramme

Dans une image en niveaux de gris, l'histogramme comptabilise le nombre d'occurrences de chacune des valeurs. En couleur, l'histogramme peut être réalisé sur les indices de couleurs dans des systèmes de couleurs indexées ou bien nécessite plusieurs histogrammes sur chacune des composantes du système de représentation de couleur [04].

Un histogramme permet d'obtenir des informations sur la répartition des intensités comme la moyenne ou la variance . Par contre, un histogramme ne fournit aucune information de répartition spatiale. Ainsi, deux images peuvent posséder le même histogramme sans pour autant se ressembler.

De même, un histogramme est invariant aux transformations réarrangeant les pixels (par exemple les symétries).

Définition de Taux de compression

Le taux de compression est défini comme le rapport du nombre de bits utilisés par l'image originale et du nombre de bits utilisées par l'image compressée. Les méthodes réversibles ont un taux de compression entre 1 et 2.5, tandis que les méthodes irréversibles prouvent voir de bien meilleurs taux de compression mais avec une distorsion [04].

I-9-2-3. Quelques idées pour la compression

Les principales idées pour la compression sont basées sur :

- La quantification des niveaux de gris ou composantes couleurs ou bien des coefficients dans les images transformées.
- La mémorisation des occurrences (on remplace la chaîne 00000 par 50).
- Le codage des valeurs avec un code de longueur inversement propositionnelle aux occurrences [04].

On cite deux algorithmes de codage largement utilisés : codage d'Huffman et le codage LZW.

Codage d'Huffman

Le Codage de Huffman est basé sur le principe suivant : coder ce qui est fréquent sur moins de bits que ce qui n'est pas fréquent. Les pixels sont regroupés par blocs de L pixels puis, la probabilité des différents niveaux de gris du bloc est estimée.

A un niveau donnée m, on combine deux symboles de probabilités minimales. On obtient alors un ensemble de niveau m − 1 comportant un élément de moins.

Le code de chaque élément est identique, sauf pour les combinaisons. Les codes associés aux deux caractères combinés à un niveau m sont obtenus à partir de leur code au niveau inférieur (m − 1) auquel on joute 0 et 1 [04].

Codage LZW (Lempel-Ziv-Welch)

En 1977, Lempel et Ziv créèrent l'algorithme de compression LZ77, évoluant l'année d'après en LZ78. Welch, de la société Unisys, modifia l'implémentation de ce codage LZW. Autant les précédentes peuvent être utilisées librement, autant le LZW fait l'objet de plusieurs brevets dont certains pourraient le bientôt expirer.

Le principe de codage est similaire pour LZ77, LZ78 et LZW. Il s'agit d'une compression sans pertes qui fonctionne bien pour les images de grandes zones homogènes. Considérant les pixels comme un tableau mono dimensionnel, l'algorithme est basé sur le découpage de l'ensemble des pixels en mots les plus longs possibles. Chaque mot, quelque soit sa longueur, se voit attribuer un code de taille fixe. Le tableau étant mono dimensionnel, les redondances verticales ne sont pas prises en compte.

L'algorithme d'Huffman attribue des codes de longueurs variables en fonction de l'occurrence des éléments. L'algorithme de LZW, quant à lui, attribue des codes de longueur fixe à des chaînes d'éléments de taille variables [04].

I-9-3. Tatouage numérique

L'objectif du tatouage pour la protection du copyright est d'introduire dans une image originale une marque invisible, appelée « watermark », contenant un code de copyright. L'image ainsi marquée ou tatouée peut alors être distribuée. Elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces

transformations peuvent être licites (comme la compression) ou illicites, elles ont alors pour but de détruire la marque. Si elles ne dégradent pas trop la qualité de l'image, ces modifications ne doivent pas gêner la détection de la marque : le processus de tatouage est alors qualifié de robuste à ces attaques [24].

Dans la plupart des algorithmes 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.

Le marquage doit être imperceptible, c'est à dire qu'un utilisateur quelconque ne doit pas pouvoir différencier visuellement l'image marquée de l'image originale. Cette propriété est importante pour deux raisons. La première est évidente : le marquage ne doit pas empêcher la compréhension de l'œuvre, celle-ci doit garder toute sa qualité artistique ou commerciale. Une autre raison est que, ainsi cachée, la marque est plus difficilement détruite par piratage.

I-10. Conclusion

Nous avons essayé dans cette section de donner quelques notions de base concernant les images numériques (caractéristique, codage, numérisation, …) afin de comprendre l'ensemble des techniques qui permettent par un traitement de modifier une image. Parmi ces techniques on trouve le tatouage des images numérique qui est présenté d'une manière générale dans les chapitres suivant.

CHAPITRE II:

Tatouage numérique, concepts de base et terminologie.

II-1. Introduction

Le tatouage des données numériques est une discipline récente qui trouve son origine dans le manque de techniques fiables de protection de ce type de données. En effet, associé à d'autres techniques, cet axe de recherche a pour but de résoudre des problèmes aussi variés que la protection du copyright et des droits d'auteurs, la réglementation des copies, la prévention de la redistribution non autorisée, le suivi de documents et l'intégrité du contenu d'une donnée.

L'objectif du tatouage pour la protection du copyright est d'introduire dans une image originale une marque invisible, appelée ***signature*** ou ***marque***, contenant un code de copyright. L'image ainsi marquée ou tatouée peut alors être distribuée, elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces transformations peuvent être licites ou illicites, elles ont alors pour but de détruire le marquage. Si elles ne dégradent pas trop la qualité de l'image, ces modifications ne doivent pas gêner la détection de la marque : Le processus de tatouage est alors qualifié de robuste à ces attaques. Nous ne développerons dans la suite de ce mémoire que la partie du tatouage ayant trait à la protection du copyright et des droits d'auteurs des images numériques.

Après avoir présenté les premières définitions et propriétés du tatouage, nous décrivons les processus d'implémentation puis de détection de la marque et soulignons les contraintes auxquelles doit faire face un schéma de tatouage. Nous présentons ensuite les différentes techniques de tatouage que l'on peut rencontrer dans la littérature. Nous soulignons l'importance du choix du domaine d'insertion et nous définissons deux grandes classes de schémas de tatouage, les schémas additifs et substitutifs.

II-2. Aux origines du tatouage

La cryptographie, la stéganographie et le tatouage sont des techniques très proches les unes des autres puisqu'elles consistent à transmettre une information à caractère confidentielle. Elles répondent toutes les trois à des problèmes de sécurité. Cette section vise à établir les différences et les similitudes entre ces trois disciplines**.**

II-2-1. La cryptographie

Puisque le tatouage consiste à transmettre une information non accessible, la discipline est souvent rattachée aux questions de sécurité des données numériques, et donc naturellement à la discipline de la cryptographie.

La cryptographie est une discipline très vieille, des techniques ont été mises en place dés le Vème siècle avant JC. Elle consiste à transformer un message pour qu'il devienne illisible. Seule la connaissance d'une clef et du moyen de cryptage peut permettre de décoder le message afin de le rendre lisible. Alors que pour le tatouage, la donnée tatouée est disponible, diffusée et exploitable, la donnée cryptée est elle inexploitable sans la connaissance des clés de déverrouillage de l'algorithme de cryptage. En fait les deux disciplines sont considérées comme complémentaires puisque d'un coté la cryptographie tend à renforcer le contrôle d'accès aux données, leur authenticité et leur intégrité, d'un autre coté le tatouage tend à lier le contenu des données avec des informations auxiliaires [03].

II-2-2. La stéganographie

Le terme stéganographie vient du mot Grec *steganos* signifiant *caché* et de *graphia* signifiant *écriture*, littéralement on traduit par *écriture cachée* [05].

Elle consiste à dissimuler un message dans un autre. Ainsi, seule la personne connaissant le procédé de dissimulation peut lire le message caché. Contrairement à la cryptographie, la stéganographie est "invisible". La différence entre la stéganographie et le tatouage, est que dans la stéganographie, l'existence d'un message caché doit rester secrète alors que pour le tatouage seul le message doit rester caché mais son existence (tant qu'on ne peut le détecter) peut être connue.

II-3. Principe général du tatouage d'image

Afin d'étudier les différents aspects de tatouage, nous devons clarifier le modèle général du tatouage. Un schéma classique de tatouage des images peut se décomposer en deux étapes fondamentales : *la phase d'insertion et La phase de détection*.

II-3-1. Phase d'insertion

Cette phase consiste à insérer une marque dans une image afin d'identifier son propriétaire. Cette insertion nécessite la possession de l'image originale (I) et de la marque à insérer (M), un troisième paramètre facultatif peut être utilisé en cas de besoin, qui est la clé secrète k. Cette clé peut servir soit à la mise en forme de la signature, soit pour localiser l'emplacement de pixels sur l'image d'origine.

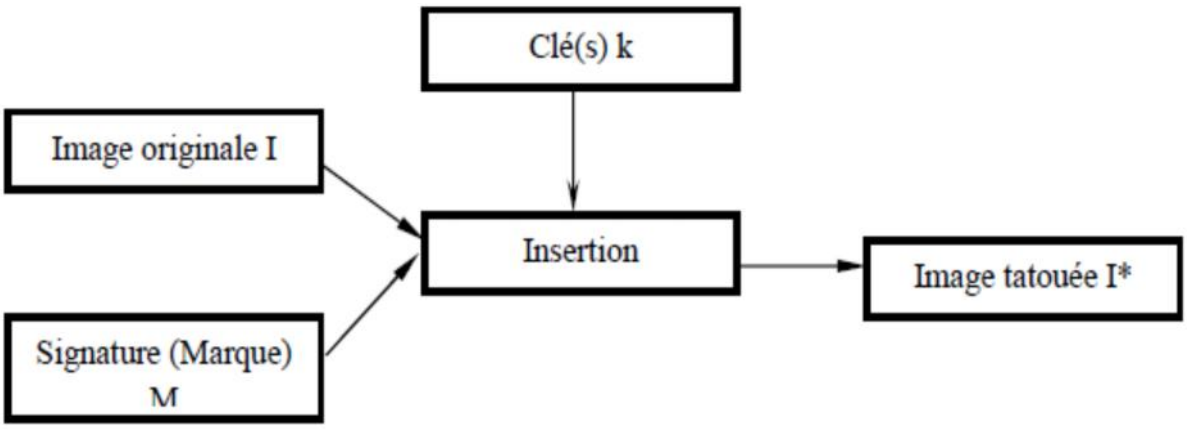


Figure II.1: Schéma d'insertion.

II-3-2. Phase de détection

Cette phase permet de prouver la présence de la marque, ceci peut être réalisé par extraction complète de la marque insérée ou par détection d'un pic supérieur à un certain seuil prédéfini obtenu par un simple inter corrélation entre la marque d'origine et celle extraite.

Premièrement, on a besoin d'une image tatouée (I*), des clés (k) et éventuellement de l'image d'origine(I). Et en suite, on se sert en plus de la marque d'origine. D'une manière générale, lors de l'utilisation de l'image d'origine, on qualifie la détection d'"Aveugle" et de "Non Aveugle" dans le cas contraire. Selon la visibilité de la marque, on distingue deux types***:*** ***tatouage visible*** et tatouage invisible de tatouage.

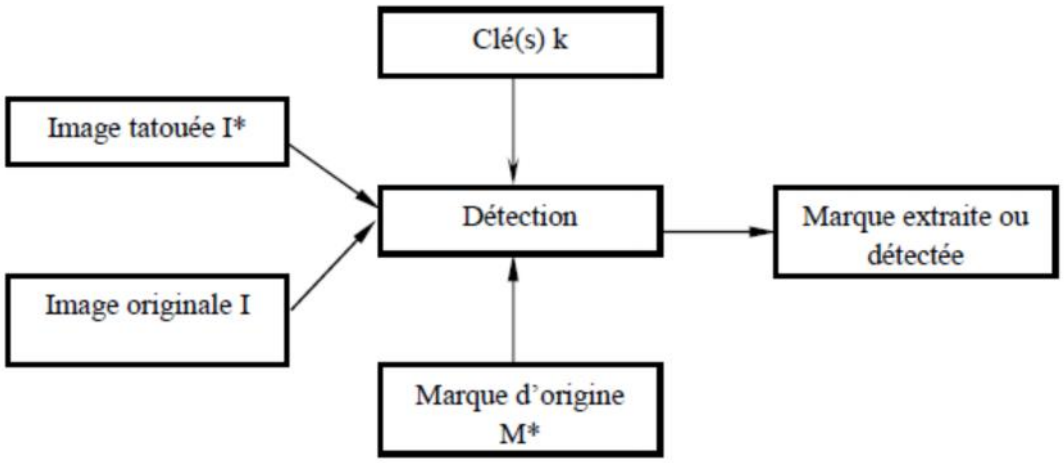


Figure 1I.2 : Schéma de détection.

II-4. Classifications du tatouage d'image

Les Techniques du tatouage ont différents types de classifications en fonction de la nature de son application. Chaque application du tatouage a ses propres exigences. Parmi ces techniques nous citons :

II-4-1. Tatouage visible et invisible

Le tatouage est classé en fonction de l'aspect visuel. Si la marque est visible à l'œil de l'observateur et indique un type d'information comme un sigle de fabrication ou toute autre information nécessaire, il est alors appelé un tatouage visible. En revanche, si la marque est intégrée d'une manière invisible et indétectable par l'observateur, ce tatouage est appelé invisible [17].

II-4-2. Tatouage aveugle et non-aveugle

Ce type de tatouage est basé sur le fait que l'image originale est requise pour le système de récupération ou non. Si l'image originale n'est pas nécessaire, alors la méthode est appelée tatouage aveugle (aussi appelé complet). Dans le cas contraire, si l'image originale s'impose, le tatouage est non-aveugle (aussi appelé incomplet). Dans certaines applications, telles que la protection du droit d'auteur et le suivi des données, les algorithmes d'extraction de marque peuvent utiliser les originaux non tatoués de données pour trouver la marque. En d'autres applications, par exemple, protection contre la copie, l'algorithme d'extraction de la marque n'a pas d'accès aux données originaux non tatoués. Cela rend l'extraction de marque plus difficile [17].

II-4-3. Tatouage Fragile et robuste

Dans le tatouage fragile, la marque est fortement sensible aux modifications de l'image tatouée. Cette approche sert à prouver l'authenticité et l'intégrité d'un fichier tatoué.

Le tatouage robuste dispose d'un large champ de théories et de résultats. Celui-ci cherche à préserver les données cachées face aux attaques. La marque doit donc être suffisamment résistant aux attaques afin de rester identifiable

II-5. Les Applications de tatouage d'image

Nous présenterons dans cette section quelques applications récurrentes du tatouage. En effet, le tatouage peut avoir pour but la protection des droits d'auteur mais aussi celle des documents. Il peut aussi faciliter l'indexation d'images. Ces diverses applications conditionnent la robustesse exigée pour la signature, comme nous allons le montrer ci-après.

II-5-1. Droit d'auteur et suivi de transaction

L'application la plus évidente du tatouage est la protection des droits d'auteur. Dans le cas d'utilisation du tatouage pour un copyright, la signature ne doit pas forcément contenir beaucoup d'informations car son existence même prouve que le document est protégé.

Le suivi de transaction consiste à insérer dans l'image des informations relatives au propriétaire du document mais aussi à son destinataire, ainsi que l'utilisation qui peut en être faite. Il s'agit de savoir qui a acquis le document si ce dernier venait à circuler librement. Cela permet de connaître la personne à l'origine de la dispersion du document [18].

II-5-2. Authentification de documents

Le tatouage permet de vérifier qu'une image n'a pas été modifiée. Dans ce cas, la signature ajoutée est dite fragile. Le tatouage peut être détecté tant que l'image n'a pas été modifiée. Le tatouage fragile est dit semi-fragile s'il résiste à des dégradations provoquées par la compression ou bien encore par le filtrage, sachant que la modification du contenu doit être signalée. Certains algorithmes permettent la détection des zones attaquées de l'image. Ce système peut être utilisé pour sécuriser des papiers d'identité ou des documents médicaux.

II-5-3. Tatouage et indexation intelligente

On peut envisager d'insérer un tatouage représentant un lien vers une autre source d'information (un lien vers un site Internet) afin d'obtenir des renseignements complémentaires sur l'image [19].

II-6. Critères d'évaluation des systèmes de tatouage

II-6-1. Transparence visuelle

Chaque système de tatouage à insertion invisible doit être capable d'insérer une marque invisiblement à l'œil humaine, avec préservation de la qualité visuelle de l'image originale. Pour cela on doit prendre en considération les propriétés du système visuel humain.

II-6-2. Robustesse

Chaque tatouage non fragile est dite robuste, si sa résistance face à toute sorte de manipulation, transformation et modification est suffisamment élevée. Ces modifications et transformations peuvent être introduites pendent les traitements nécessaires au transfert ou stockage de l'image, comme compression, filtrage, débruitage, conversion analogique-numérique, ou bien

numérique-analogique et aussi lors des opérations géométriques comme rotation, agrandissement, découpage et translation effectués pour l'utilisation de l'image dans différentes applications [20].

II-6-2. Capacité d'encastrement

La capacité d'insertion (d'encastrement) d'un algorithme de tatouage présente la quantité maximale d'informations qui peut être insérée dans l'image sans dégrader sa qualité originale. Cette capacité dépend de l'algorithme utilisé, la taille de l'image et ses caractéristiques statistiques. En général, l'augmentation de celle-ci diminue la transparence de la marque et augmente sa robustesse, mais ce n'est pas toujours le cas [20].

II-6-3. Complexité de calcul

Un système de tatouage doit être capable de tatouer une image rapidement et facilement avec le minimum de matériel, afin de réduire le coût de fonctionnement. La rapidité est nécessaire pour des opérations de tatouage en temps réel, où chaque retard provoque une perte d'informations et une réduction de rendement. Cette rapidité est liée directement à la complexité du calcul à effectuer durant le processus d'insertion et d'extraction.

II-6-4. Compromis à réaliser

Les trois caractéristiques citées ci-dessus sont souvent liées par des relations contradictoires qui sont appelées compromis. L'augmentation de la quantité d'information insérée réduit la robustesse de la marque et son invisibilité, ce qui est le contraire si on réduit la capacité d'insertion, car l'invisibilité s'améliore et la robustesse augmente.

Il est vraiment difficile de satisfaire tous ces critères par un même algorithme de tatouage. Cela explique le recours au développement spécialisé des algorithmes selon les recommandations et les exigences de chaque application.

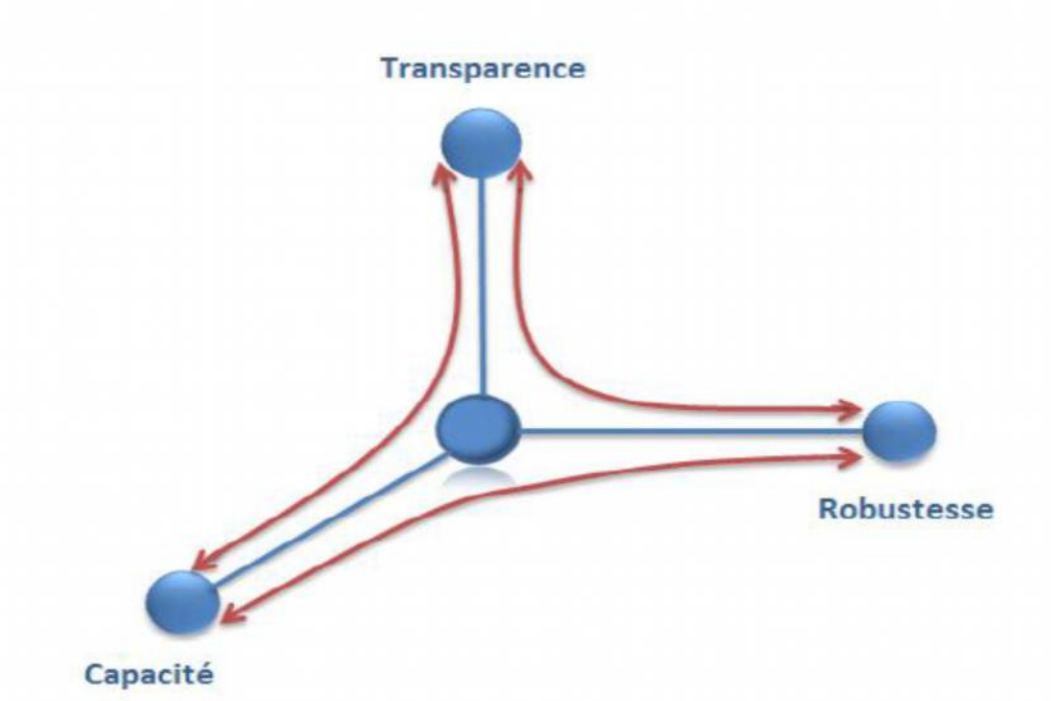


Figure II.3: Contraintes d'un algorithme de tatouage.

II-7. Etat de l'art des techniques de tatouage existantes

Les schémas de tatouage des images que l'on peut rencontrer dans la littérature scientifique sont très variés et peuvent sembler à première vue très différents les uns des autres. Cependant, les techniques de tatouage courantes peuvent être groupées selon [02].

La multiplicité des algorithmes de marquage rend leur présentation exhaustive assez difficile. Pour classifier ces algorithmes on se base sur deux critères.

- le mode d'insertion de la marque (schéma additif, schéma substitutif).
- le domaine utilisé (spatial, fréquentiel) [21].

II-7-1. Classification selon la manière d'insertion

La classification selon la manière d'insertion se présente sous les différents schémas :

II-7-1-1. Schéma additif

L'insertion peut s'effectuer soit directement sur l'image, dans le domaine spatial, soit dans un domaine transformé. De ce fait, adapter la marque à l'objet d'origine est une contrainte essentielle à respecter pour que le signal qu'elle représente ne soit ni trop faible (problème de robustesse) ni trop fort (dégradation du signal original) [21].

II-7-1-2. Schéma substitutif

Dans les modes substitutifs, l'information à insérer est substituée à des caractéristiques de l'image. Par exemple, P.Bas et J. M. Chassery proposent dans une méthode basée sur l'insertion de similarités. L'idée de base consiste donc à insérer une signature en modifiant le contenu structurel de l'image. Ainsi, l'étape d'insertion consiste d'une part à détecter les points d'intérêt et d'autre part à insérer des similarités autour de ces points. A la suite, la détection de marque s'effectue par recherche de ces similarités [22].

II-7-2. Classification selon le domaine d'insertion

Comme nous l'avons mentionné dans la section II-3, l'insertion de la marque est effectuée dans un domaine d'une transformation inversible. Le choix du domaine d'insertion est une étape délicate dans la conception du système de tatouage. Différents critères régissent le choix d'un domaine adapté [23]. Ce domaine peut :

- Permettre de décorréler le signal hôte (l'image) du signal de tatouage. Cette décorrélation tente de ramener le système de tatouage à avoir des performances optimales.

- Rendre la distorsion d'insertion moins faible. En effet, permettre une altération importante de certaines composantes de l'image sans modifier la perception de celui-ci peut faciliter la détection du tatouage.

- Etre invariant à certaines perturbations subies par l'image; ce critère est fréquemment utilisé lorsque les perturbations désynchronisantes sont considérées. Cette invariance facilite la conception de systèmes robustes aux perturbations.

La littérature propose les différents domaines respectant au moins l'un de ces critères (mais jamais les trois). Nous présentons dans les sous sections suivantes les domaines d'insertion les plus utilisés. Ainsi, nous présentons quelques exemples des méthodes de tatouage pour chaque domaine :

II-7-2-1. Le domaine spatial

L'insertion de la marque est effectuée en modifiant directement les valeurs des pixels de l'image. L'avantage principal de ce domaine est le faible coût, ce qui permet de l'utiliser dans les applications du tatouage en temps réel. Parmi les exemples des méthodes opérantes dans le domaine spatiales, nous citons : La technique de substitution de plan LSB [24] qui constitue l'une des premières méthodes proposées dans la littérature. En effet, les valeurs des pixels de l'image sont codées sur 8 bits. Ce qui permet de découper l'image en 8 plans comme illustré dans la Figure II.4. La méthode de tatouage du LSB consiste donc à forcer le poids faible de chaque pixel à 0 ou 1, suivant la valeur du bit de la séquence contenue dans le watermark. Cette méthode est très simple, l'image marquée n'est pas visiblement dégradée parce que les données contenues dans les bits LSB sont visuellement insignifiantes. Cette simplicité se paye par une très faible robustesse : n'importe quel traitement, même peu important, suffit à modifier les LSB et donc à rendre l'extraction impossible. D'où elle peut être utilisée pour véhiculer des informations ou pour concevoir un schéma de tatouage fragile (La section II.3).

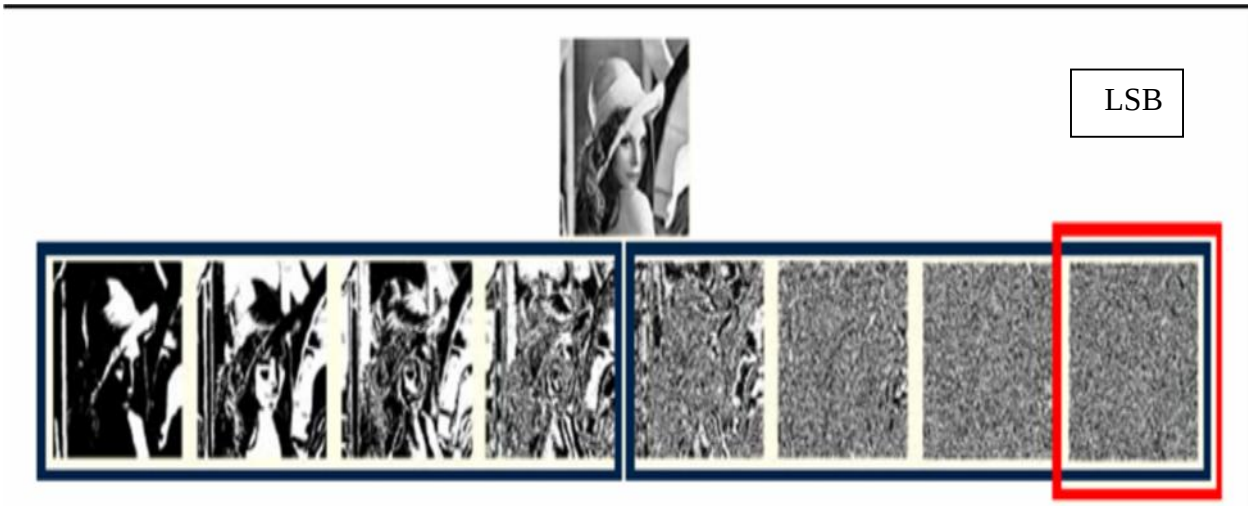


Figure II.4: Découpage de l'image Lena en 8 plans.

Afin de profiter les performances au niveau de la robustesse, [25] ont proposé une méthode renommée par modulation d'amplitude, basé sur changement de luminance et utilisé la permutation par XOR à l'insertion ,cette méthode est une amélioration des méthodes basé sur la modulation d'amplitude étudiés dans [26] et [27].

Récemment, des algorithmes robustes à quelques attaques géométriques sont proposés dans le domaine spatial. Nous citons par exemple celles publiés dans [28], [29].

Néanmoins, les marquages dans le domaine spatial résistent très mal à tout type d'attaque, géométrique ou fréquentiel. Cet inconvénient a dirigé les chercheurs vers l'utilisation d'autres domaines robustes à ce type d'attaques comme DFT, DCT et DWT.

II-7-2-2. Le domaine de Fourier

La théorie de Fourier permet de décomposer une image en une série de sinusoïdes à différentes fréquences. L'équation (II.1) donne la décomposition d'une image I_0 de taille en $N_1 \times N_2$ utilisant la transformée de Fourier :

$$F(p,q) = \sum_{m=0}^{N_1-1} \sum_{n=0}^{N_2-1} I_0(m,n) e^{-j\left(\frac{2\pi}{N_1}\right)pm} e^{-j\left(\frac{2\pi}{N_2}\right)qn} \qquad (II.1)$$

Avec j =$\sqrt{-1}$, p=1,22…,N_1 et q=1,2,…,N_2 .

La décomposition de la transformée de Fourier inverse est donnée par :

$$I_0(m,n) = \frac{1}{N_1 N_2} \sum_{m=0}^{N_1-1} \sum_{n=0}^{N_2-1} F(p,q) e^{j\left(\frac{2\pi}{N_1}\right)pm} e^{j\left(\frac{2\pi}{N_2}\right)qn} \qquad (II.2)$$

L'équation (II.3) peut être représentée aussi sous la forme :

$$F(p,q) = |F(p,q)| e^{-j.\emptyset(p,q)} \qquad (II.3)$$

Où la fonction $|F(p,q)|$ représente le spectre de la transformée de Fourier de I_0 tandis que $\emptyset$ est sa phase. $|F(p,q)|^2$ est le spectre de puissance de I_0. La Figure (II.5) représente l'image Lena et le spectre de sa transformée de Fourier.

Figure II.5: Image Lena et son spectre de Fourier.

Cette transformation permet de contrôler les fréquences du signal. Elle permet de choisir adquatement les zones adéquates à l'insertion de la marque, de telles sortes à obtenir un bon compromis robustesse-invisibilité. Aussi, le principal avantage de ce domaine est qu'il est invariant à la translation et au changement d'échelle.

Piva et al [30]. ont présenté une approche de tatouage d'images basée sur la transformée de Fourier discrète (DFT). Malgré sa faible robustesse, elle est intéressante pour la compréhension du tatouage d'image dans le domaine de Fourier. Cette méthode a été améliorée par Solachidis [31], puis par F. Ros et al [32]. La marque est générée d'une manière pseudo aléatoire à moyenne nulle. L'insertion se fait dans les bandes moyennes de fréquence. Comme illustré dans la Figure II.6., les auteurs proposent d'insérer le même message deux fois dans deux sous bandes des fréquences moyennes. Un masque psychovisuels est utilisé pour remédier au problème de la difficulté de maîtriser le résultat au niveau local sur l'image finale.

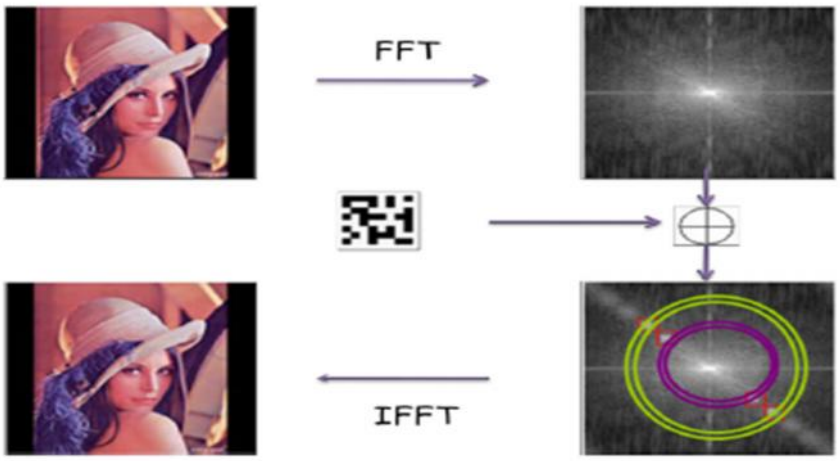


Figure II.6: Exemple d'insertion dans le domaine de Fourier.

Afin de pouvoir compenser une attaque basée sur des transformées géométriques, F. Ros et al [32], ont ajouté des pics de référence aux amplitudes de DFT de l'image. Grâce à cette technique, il est possible de synchroniser le signal en détectant les pics insérés, la marque peut alors être extraite et décodée. La phase de détection consiste à calculer de la corrélation entre la marque générée et les coefficients de Fourier de l'image tatouée. Une autre technique dans le domaine de Fourier est proposée par Perreira et al [33]. Cette méthode de tatouage est particulière dans le sens où elle fait intervenir deux techniques distinctes; l'une est destinée à réaliser le tatouage, l'autre utilise un gabarit particulier dont le

but est de permettre la recherche de la transformation affine que l'image tatouée a subit afin de réaliser un recalage des informations à extraire.

L'invariance par translation est obtenue par la transformation de Fourier de l'image en utilisant que le module [32]. Alors que les invariances par rotation et changement d'échelles peuvent être obtenues par la transformation de Fourier-Mellin du module [34], [35]. En effet, L'espace invariant est obtenu; d'une part grâce à la propriété de la transformée de Fourier qui répercute une translation de l'image exclusivement sur la phase et laisse invariant l'amplitude et d'autre part, par un changement de repère, de cartésien vers logarithmique-polaire. Ce changement de repère ramène les opérations de rotation et de changement d'échelle à une translation. Cependant, la difficulté de l'implémentation constitue un problème majeur de cette transformation [36].

II-7-2-3. Le domaine de la transformée en Cosinus Discrète (DCT)

La transformée en cosinus discrète DCT afin d'anticiper et de rendre le watermark plus robuste à une compression JPEG, puisqu'elles utilisent le même espace qui sert au codage de l'image. Elle permet entre autres de réduire la corrélation spatiale entre les pixels d'une image. Un autre avantage en faveur de l'utilisation de DCT est la possibilité de bénéficier des études psychovisuelles déjà menées en codage de source (par exemple, les travaux de Watson [37], et Lubin [38]). En effet, elles se proposent de prendre en compte les phénomènes connus comme la représentation de la couleur, la sensibilité au contraste et les effets de masquage.

La transformée en cosinus discrète d'une image I_0 de taille $N_1 \times N_2$, notée par F_{DCT} (I_0), est donnée par :

$$F(p,q) = \frac{2 \wedge (p) \wedge (q)}{\sqrt{N_1 N_2}} \sum_{m=0}^{N_1-1} \sum_{n=0}^{N_2-1} I_0(m,n).\cos\left[\frac{\pi(2m+1)p}{2N_1}\right].\cos\left[\frac{\pi(2n+1)q}{2N_2}\right] \quad (II.4)$$

Avec :

$$\wedge(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & si\ \xi = 0 \\ 1 & sinon \end{cases}$$

La transformée en cosinus discrète inverse, notée par F_{DCT}^{-1}, est donnée par :

$$I(m,n) = \frac{2 \wedge}{\sqrt{N_1 N_2}} \sum_{p=1}^{N_1} \sum_{q=1}^{N_2} F(p,q) \wedge (p) \wedge (q) . \cos\left[\frac{\pi(2m+1)p}{2N_1}\right] . \cos\left[\frac{\pi(2n+1)q}{2N_2}\right] (II.5)$$

De nombreuses méthodes ont été développées dans ce domaine. Dans [54], Cox et al présentent un schéma non aveugle de tatouage par l'étalement de spectre dans le domaine de DCT. La marque est insérée par une modification de 1000 coefficients DCT plus grandes amplitudes, de façon à ce que le watermark soit inséré dans les zones visuellement significatives

Le calcul la DCT sur toute l'image prendrait un temps très long. Pour éviter cela, on applique la DCT sur des blocs de longueur fixe. Généralement, la taille des blocs DCT utilisée est de 8 x 8 pixels : ce choix donne un meilleur compromis entre la qualité et le temps de calcul. La Figure II.7. présente une technique non-aveugle proche de la méthode de [39] est présentée par Suhail [40], mais ne travail pas sur l'image complète.

L'image est préalablement découpée en blocs. Le message, constitué d'une séquence aléatoire, est inséré dans les fréquences moyennes de chaque bloc. Les résultats présentés par les auteurs montrent une nette amélioration de l'ensemble des caractéristiques comparées aux résultats de [39].

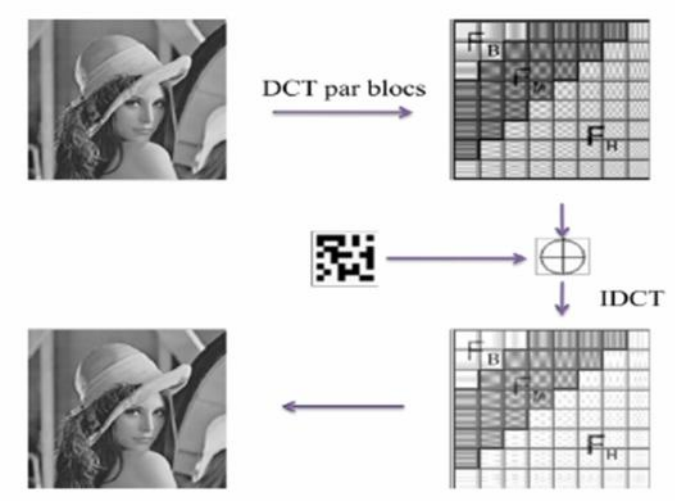


Figure II.7: Exemple d'insertion dans les fréquences moyennes de DCT.

Dans [41] une technique de tatouage d'image dans le domaine de DCT est proposée.

Le principe consiste à insérer la marque dans un bloc de taille 8×8. Pour chaque bloc, les auteurs calculent la transformé DCT puis ils sélectionnent deux ou trois coefficient des moyennes fréquences. Ces coefficients sont ensuite quantifiés à l'aide de la table de quantification correspondant à la compression JPEG [42]. La quantification des coefficients DCT par QIM est présentée dans [43], [44].

II-7-2-4. Domaine d'ondelettes

L'utilisation de la transformée en ondelette discrète DWT est intéressante pour le tatouage numérique grâce à son utilisation dans l'algorithme de la compression JPEG2000.

De plus, cette transformée peut être interprétée comme une décomposition de l'image en sous bandes fréquentielles ce qui permet de développer facilement des masques psycho-visuels En plus de la robustesse commune avec la DCT, le tatouage dans le domaine d'ondelettes est robuste à un changement d'échelle de facteur. De plus, les masques perceptuels sont plus fins et il y a moins d'effets de blocs.

Dans le chapitre suivant, nous détaillons le principe de cette transformation, ainsi que les différents algorithmes basant sur cette transformée comme domaine d'insertion.

II-7-2-5. Autres domaines

Outre les FFT, DCT et DWT précédemment cité, d'autres transformations inversibles classiques en traitement d'images ont été aussi envisagées, sans apporter en pratique une amélioration significative des performances ou des invariances géométriques. Nous citons par exemple, l'utilisation de la décomposition en valeurs singulières (SVD) [45], [46] et La transformation de Karhunen-Loève (KLT) [47].

II-7-2-6. La combinaison des domaines

Nous trouvons aussi dans la littérature des méthodes qui reposent sur l'utilisation de la combinaison entre les domaines d'insertion (algorithmes hybrides). Nous citons l'exemple de la méthode présentée dans [48]. Cette méthode de tatouage est particulière dans le sens où elle effectue un tatouage dans le domaine spatial et fréquentiel. Dans le domaine spatial, la marque est incrustée via l'algorithme du "2-D Cyclic Pattern". Dans le domaine fréquentiel, un gabarit est incrusté afin de permettre la détection des transformations géométriques de

type rotation et changement d'échelle. Enfin, un masque psychovisuel est utilisé afin de garantir l'invisibilité de la marque dans l'image.

Dans [49] et [50], un schéma hybride basé sur DWT et la décomposition en valeurs singulières (SVD) est présenté. Après la décomposition de l'image en quatre sous-bandes, Les auteurs appliquent la SVD à chaque bande, et insèrent les données de la marque en modifiant les valeurs singulières.

Le domaine DWT et celui de Fourier ont été combinés par Hu et al [51]. DFT est utilisée pour palier au problème de désynchronisation liée aux attaques géométriques par l'insertion d'un gabarit dans les moyennes fréquences. Alors que, DWT est utilisé pour insérer la marque.

II-8. Attaques sur les images tatouées

Dans le cas d'un tatouage robuste, la marque doit résistée à un grand nombre d'attaques volontaires (piratage) ou naturelles Les algorithmes de tatouage d'image sont généralement développés pour répondre à une ou plusieurs attaque(s) en particulier. Cela signifie qu'il est impossible de développer un algorithme général pour l'ensemble des attaques connues et inconnues. Dans cette section, nous allons présenter une liste non exhaustive des attaques les plus courantes que peut subir une image.

Dans la littérature, plusieurs classifications des attaques de tatouages ont été proposées. Par exemple, celles présentées par S. Voloshynovskiy et al. [52] et Cox et al [53].

La classification proposée par Cox et al est basée sur la nature des transformations appliquées sur l'image et sur l'intention de l'utilisateur. En effet, cette classification distingue deux types d'attaques : les attaques à la robustesse et celles sur la sécurité. En outre, celle proposé par Voloshynovskiy comporte quatre catégories d'attaques : les attaques d'effacement, les attaques géométriques, les attaques de cryptographie et les attaques de protocoles.

En se basant sur [52] et [53], nous proposons dans la Figure (II.8) une classification en trois catégories :

- Les attaques d'effacements.
- Les attaques géométriques.
- Les attaques de sécurités

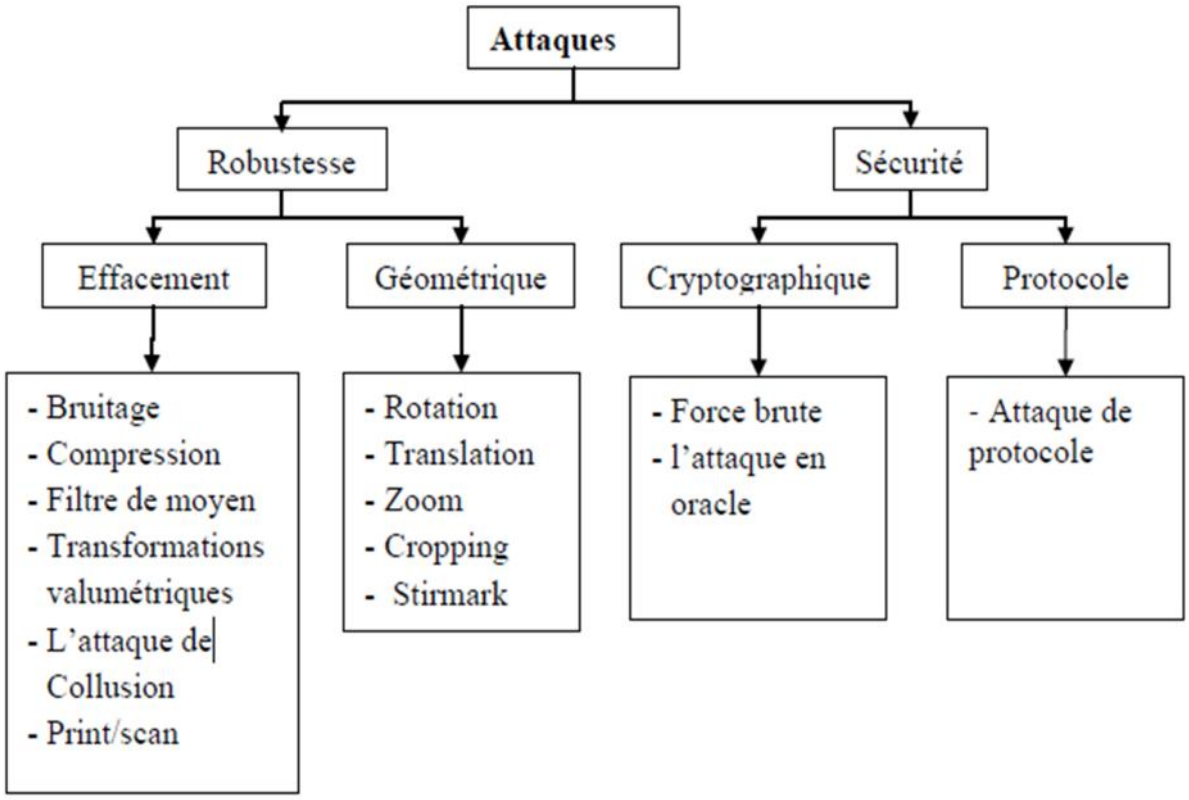


Figure II.8: La classification des attaques que peut subir un document tatoué.

II-8-1. Attaque d'effacement

Ce sont des attaques liées à l'image (ou au signal de watermark), dont le but est de faire disparaître le watermark masqué dans l'image. Cela se résume à des transformations plus ou moins violentes. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer néanmoins que ces attaques ne sont pas forcément volontaires. En effet, sans le savoir, l'image peut être dégradée suffisamment pour que le tatouage soit effacé. Un algorithme de marquage robuste est sensé résister de manière efficace à ce type de transformations, ou du moins tant que l'image reste utilisable. Nous citons par exemple :

II-8-1-1. Attaques par filtrage

Le filtrage correspond à l'augmentation (resp. la diminution) des composantes hautes fréquences. En effet, L'ajout d'un bruit blanc gaussien ou un filtre moyen permet de désynchroniser la phase de l'insertion et la détection. Un exemple simple, si le marquage est effectué en modifiant la luminance de certains pixels. Il suffit alors d'effectuer un filtre passe-bas sur l'image afin d'avoir alors la quasi certitude de détruire complètement le tatouage.

II-8-1-2. Attaque par mosaïques

Ce type d'attaque a comme principe de découper l'image en plusieurs morceaux, qui sont ensuite juxtaposés. On peut donc la regarder sans s'apercevoir de la manipulation, mais le tatouage est totalement désynchronisé si sa détection est automatisée. Cette attaque vise les moteurs de recherche automatique (crawlers) des marques dans les images sur Internet.

II-8-1-3. Transformations valumétriques

Le principe de ce type d'attaque est de changer la luminance de l'image par une fonction non-linéaire. Nous distinguons dans ce type d'attaques l'étalement d'histogramme, égalisation d'histogramme, transformation Gamma, etc.…

II-8-1-4. Compression

La compression avec perte cherche à simplifier le codage du document, en supprimant l'information peu significative ; comme le tatouage est imperceptible, il est naturellement considéré comme peu significatif. En fait, les algorithmes dans le domaine spatial souffrent des attaques par compression. Dans le but d'augmenter la robustesse face à la compression, l'une des techniques de tatouage consiste à mettre en évidence la simulation d'un processus de compression dans la mise au point d'un algorithme de tatouage [23], d'autres techniques consistent à concevoir des algorithmes de tatouage adaptés au contenue des images dans le domaine DCT ou DWT.

II-8-1-5. Conversions analogique-numérique

La conversion analogique-numérique entraîne en général une désynchronisation du signal de tatouage, ainsi que de petites distorsions. Par exemple, le processus d'impression suivie d'un scan (Print/scan) d'une image, l'enregistrement d'un film à l'aide d'un caméscope dans une salle de cinéma ou le réenregistrement de la musique.

II-8-2. Attaques géométriques

Ce genre de transformation a pour effet de désynchroniser le signal de tatouage, ce qui empêche la détection de la marque, c'est-à-dire la difficulté de localiser la marque en empêchant ou diminuant l'exactitude de celle-ci. Il existe plusieurs transformations géométriques. Certaines sont utilisées couramment dans le traitement d'images, nous citons les plus usuelles:

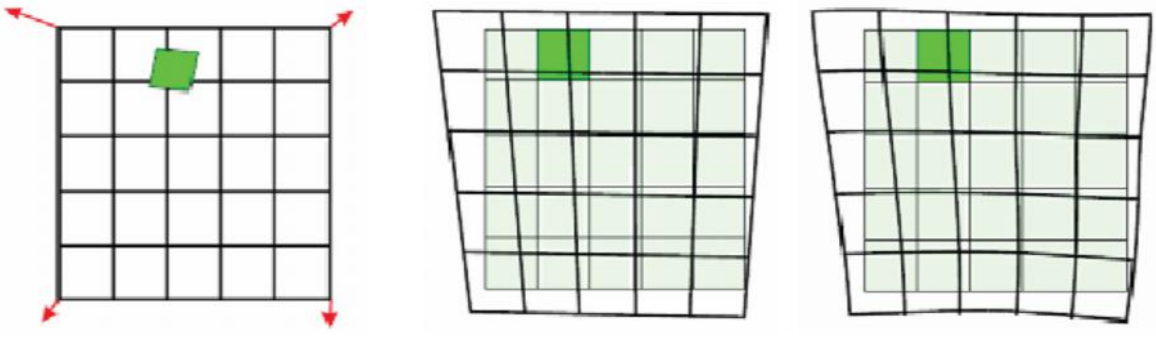
- Rotation : des petites angles de rotation, n'ont pas l'habitude de changer la valeur commerciale de l'image, mais peuvent rendre le watermark non détectable.

- Scaling (modification des dimensions) : ce type d'opération est appliqué quand une image imprimée est scannée ou quand une image numérique de haute résolution est utilisée pour des applications électroniques, telles que la publication Web.

- Cropping (rognage) : Supprimer ou couper une partie d'une image qui s'étend au-delà d'une certaine limite, le bord de la fenêtre, par exemple. Certains programmes graphiques autorisent aussi le rognage comme moyen de tout masquer, sauf un objet donné, afin que les outils de dessin s'appliquent à l'objet seul.

- Stirmark : consiste à appliquer une succession de distorsions géométriques aléatoires

  appliquées globalement et localement à plusieurs endroits dans l'image [54] (voir la Figure (II.9).



L'image originale

Figure II.9: la distorsion géométrique locale appliquée par Stirmark [54].

Bien que plusieurs méthodes de tatouage soient plus robustes à plusieurs attaques d'effacement, souvent elles ne sont pas robustes aux attaques géométriques. Une solution consiste à utiliser en parallèle des techniques de synchronisation spéciales pour résister à ces attaques. Ces techniques reposent souvent sur l'utilisation soit d'un domaine d'une transformation invariante (Fourier-Mellin), l'ajout d'un pattern de synchronisation (insertion d'un template) [55] ou des marques périodiques [56].

Cependant, en exploitant la connaissance préalable du système de synchronisation utilisé, l'attaquant peut concevoir des attaques dédiées pour introduire une désynchronisation entre la phase d'insertion et celle de la détection.

II-8-3. Attaques sur la sécurité

La plupart des algorithmes de tatouage sont public, alors si on suppose qu'un pirate connaît l'algorithme mais il n'a aucune information le secret (comme par exemple des porteuses ou des clefs secrètes). Il lui suffit d'avoir plusieurs documents tatoués puis d'observer la réponse des documents modifiés à la zone de détection et de choisir celui qu'est proche d'un document tatoué sans modification mais en hors de la zone de détection.

Parmi les attaques sur la sécurité nous citons:

L'attaque de cryptographie

Le principe consiste à rendre un système de tatouage inutilisable en exploitant des failles dans la gestion des clés (déchiffrer la clé) et ensuite de faire disparaître de la marque de tatouage, d'accéder aux informations confidentielles, ou de tatouer un document en s'appropriant illégalement une identité. On distingue généralement deux types : L'attaque par force brute qui consiste à tester toutes les clés possibles. L'autre est l'attaque en oracle imaginée par Linnartz et al [57]. Dans cette attaque le pirate insère des contenus en entrée au décodeur puis observe en sortie les messages décodés afin d'estimer la forme de la frontière entre les documents tatoués et les documents non tatoués [58].

L'attaque de protocoles

Cette attaque vise à trouver une faille dans le protocole de système de tatouage, puis d'accéder aux informations confidentielles, ou de tatouer un document avec une fausse marque.

L'attaque de collusion

Dans ce type d'attaque suppose que le pirate dispose de plusieurs versions d'un document tatoué par différentes clés ; l'attaque consiste à construire un document sans tatouage. Une modélisation par la théorie des jeux [59] consiste à formaliser la rivalité naturelle entre le tatoueur et l'attaquant et d'établir une stratégie optimale de tatouage.

II-9. Mesure des performances

Dans un système de tatouage, l'invisibilité de la marque et la qualité de l'image tatouée sont mesurées par les mêmes outils de mesure de performances ; comme le PSNR et EQM. Pour mesurer la capacité d'insertion, on doit utiliser un rapport entre la taille de l'image et la quantité d'informations qu'on peut insérée. Pour mesurer la robustesse du tatouage, on compare les deux marques, originale et extraite et on calcule la corrélation et le taux d'erreurs entre eux, les résultats nous permettent d'évaluer la résistance de la marque insérée aux différentes attaques.

II-10. Conclusion

Dans ce chapitre, nous avons présenté la technologie du tatouage numérique d'une manière générale. Nous nous sommes intéressés aux terminologies et notions liées aux techniques du tatouage invisible des images numériques. Ces terminologies sont nécessaires pour les chapitres suivants tels que les conditions requises, les attaques possibles et l'évaluation de la qualité perceptuelle.

Nous avons présenté aussi une taxonomie des techniques du tatouage selon différents critères : le type de l'algorithme, le champ d'application et le domaine d'insertion. Selon le dernier critère les techniques du tatouage peuvent être regroupées en deux catégories : ceux travaillant dans le domaine spatial et ceux travaillant dans le domaine fréquentiel.

CHAPITRE III:

Le tatouage d'images fixes basé sur la modulation d'amplitude.

III-1. Introduction

Cette méthode présente un tatouage d'image avec détection aveugle basée sur la modulation d'amplitude. Fondamentalement, l'intégration de filigrane est réalisée en modifiant les valeurs des pixels dans le canal bleu d'une image, tandis que la récupération du filigrane est obtenue en utilisant une prédiction technique basée sur une combinaison linéaire des valeurs des pixels voisins autour des pixels intégrés.

III-2.Principe général du tatouage d'image par la méthode de la modulation d'amplitude

III-2-1. Phase d'insertion

Fondamentalement, un flux de bits binaires unique est généré et considéré comme un filigrane $w(i,j) = \{1,-1\}$ pour être intégrés dans une image couleur, l'intégration de filigrane est réalisée par la modification de la composante bleue à une donnée de coordonnées (i,j),

L'image numérique (aux niveaux de gris) peut être représentée comme une matrice de N colonnes et M lignes où chaque élément correspond au niveau de gris du pixel (Picture Elément) de l'image. Une image de résolution 512×512 est donc une matrice de dimension 512×512 où le premier pixel est le premier élément de la matrice et chaque élément est compris entre 0 (correspondant au noir) et 255(correspondant au blanc).

On parle des images binaires si un seul bit décrit chaque pixel, 0 représentant un pixel noir et 1 un pixel blanc. En attribuant plusieurs bits aux pixels, un nombre plus élevé de niveaux de gris peut être distingué. La plupart du temps, les images monochromes sont codées sur 8 bits par pixel, puisque cela devient exactement un octet et les 256 (2^8 =256) différentes intensités ainsi représentables sont largement suffisantes pour la perception humaine.

Pour les images couleurs, chaque pixel est caractérisé par 3 intensités lumineuses, celles des canaux rouge (R), vert (V) et bleu (B), définissant des images 3×8=24 bits [60].

Dans la méthode fondée sur la modulation d'amplitude, la composante bleue est sélectionnée pour être un filigrane car, selon le modèle de couleur RVB, il est le moins sensible à œil humain [61]. Les modifications de la composante bleue dans chaque pixel

$B(i,j)$ sont soit additive ou soustractive, en fonction de $w(i,j)$, et proportionnelle à la luminance du pixel d'encastrement selon l'équation (III.1).

$$L(i,j) = 0.299R(i,j) + 0.587V(i,j) + 0114B(i,j) \qquad (III.1)$$

L'œil humain est moins sensible aux pixels de luminance élevée. La valeur de luminance est donc considérée et utilisée pour le réglage de la force du filigrane, de sorte que plus d'énergie de filigrane peut être ajouté pour parvenir à un niveau plus élevé de robustesse. Le pixel filigrane $B'(i,j)$ est exprimé par l'équation (III.2).

$$B'^{(i,j)} = B(i,j) + w(i,j)S.L(i,j) \qquad (III.2)$$

Où S est un facteur d'échelle utilisé pour régler la force de filigrane pour la trame de l'image entière. Pratiquement, S doit être soigneusement sélectionné pour obtenir le meilleur compromis entre imperceptibilité et robustesse.

Avant la mise au point de la force du filigrane, l'application d'une technique basée sur des clés pour la permutation filigrane a été suggéré afin d'améliorer la sécurité des ensembles du système, Le processus de l'intégration de filigrane est illustré sur la figure (III.1).

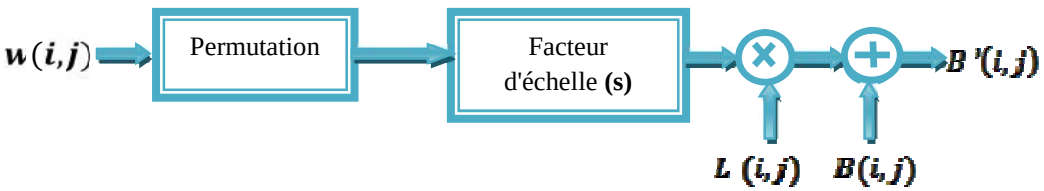


Figure III.1: Schéma générale d'insertion de filigrane.

III-2-2. Phase de détection

Sur le site du récepteur, le filigrane intégré peut être récupéré sur la base de deux hypothèses. Tout d'abord, une valeur de pixel dans une image est proche de ses proches voisins, de sorte qu'une valeur de pixel à une donnée de coordonnées (i,j) peut être estimée par la moyenne de ses valeurs de pixels à proximité. D'autre part, la somme de w autour de (i,j) est proche de zéro, de sorte que le bit intégré à la position de (i,j) peut être estimée par l'équation (III.3).

$$w'(i,j) = B'(i,j) - B''(i,j) \qquad (III.3)$$

Où $B''(i,j)$ est considéré comme une prédiction de $B(i,j)$ et déterminée à partir des valeurs de pixels à proximité de (i,j) comme l'équation (III.4).

$$B''_{(i,j)} = \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} B'_{(i+m,j+n)} - B'_{(i,j)}\right) \qquad (III.4)$$

Puisque la valeur de $w'(i,j)$ peut être soit 1 et -1, la valeur de $w'(i,j) = 0$ est définie comme un seuil, et son signe est utilisé pour estimer la valeur de $w(i,j)$.Si $w'(i,j)$ est positif (ou négatif), $w(i,j)$ est 1 (ou -1, respectivement).

Pour analyser les facteurs qui influent sur l'estimation de w, Eq. (III.3) est réécrite par :

$$w''_{(i,j)} = B_{(i,j)} + w_{(i,j)}S.L_{(i,j)} - \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} B_{(i+m,j+n)} - B_{(i,j)}\right)$$
$$-\frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} w_{(i+m,j+n)}S.L_{(i+m,j+n)} - w_{(i,j)}S.L_{(i,j)}\right) \qquad (III.5)$$

Le premier et deuxième terme du côté droit de l'équation. (III.5) représentent la valeur de pixel originale, et l'énergie du filigrane à (i,j), tandis que les troisième et quatrième termes représentent la prédiction de $B(i,j)$ et la sommation de l'énergie autour de filigrane (i,j), respectivement. Nous pouvons voir que l'énergie de filigrane à (i,j) peut être recouverte si le premier terme est égal au troisième terme, et le quatrième terme est égal à zéro.

Selon les hypothèses déjà faites, si la première hypothèse est la différence entre la première et la troisième condition doivent approcher de zéro, et si la deuxième hypothèse est, le quatrième terme devrait tendre vers zéro. L'estimation de $w(i,j)$ dépendra maintenant du second terme qui est proportionnel à S et $L(i,j)$.

En présence de bruit, l'amplitude du second terme doit être supérieure aux bruits (et / ou) aux attaques introduites, afin d'estimer $w(i,j)$ correctement.

Basé sur l'analyse ci-dessus, trois différentes méthodes sont développées et utilisées pour réduire les effets du premier, troisième et quatrième terme de l'équation (III.5).

III-3. Les méthodes appliquées [25]

III-3-1. Phase d'insertion

Les auteurs ont considéré uniquement les deuxième et quatrième termes de l'équation (III.5). En supposant que toutes les valeurs de luminance autour de (i,j) sont identiques. L'effet quatrième terme est éliminé lorsque le nombre de $w=1$ et $w=-1$ autour de (i, j) sont égaux et il reste que le second terme. Cette condition est rarement rencontrée dans un système pratique, surtout quand une image en noir et blanc textuel est utilisé comme filigrane. Le tableau (III.1) montre la sommation de w autour de (i,j).

Tableau III.1 : Sommation de w autour de (i,j) pour tous les possibles des w.

Ne de w=1 et w=-1 autour (i,j)	8 et 0	7 et 1	6 et 2	5 et 3	4 et 4	3 et 5	2 et 6	1 et 7	0 et 8
Sommation de w	1	0,75	0,5	0,25	0	-0,25	-0,5	-0,75	-1

Pour plus de simplicité, les résultats obtenus sont normalisés en le divisant par sa valeur maximum, selon l'équation (III.6).

$$w = \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} w_{(i+m,j+n)} - w_{(i,j)}\right) \qquad (III.6)$$

Où $L_{(i+m,j+n)} \simeq L_{(i,j)}$

Notez que le plus mauvais est lorsque tous les bits autours de $w\ (i,j)$ sont identiques et égaux à 1. Comme dans le ca d'un filigrane contenant des motifs reconnaissables, tel qu'un logo d'entreprise ou des textes en noir et blanc.

De toute évidence, le processus de permutation n'aide pas beaucoup, puisque le nombre de $w=1$ et $w=-1$ dans le filigrane d'intégration est toujours le même, pour améliorer l'équilibre de w, on utilise le XOR où lieu de la permutation à tous les w autour (i,j) avec un autre train de bits pseudo-aléatoire, généré à partir d'une clé secrète.

Cette approche est basée sur une hypothèse que le nombre de 1 et de -1 sont égaux et le quatrième terme est éliminé.

Dans la pratique, le nombre de 1 et -1 générés à partir d'un chiffrement de flux peut être légèrement différent [62], ce qui conduit à l'existence du quatrième terme. La sommation de nouveau w autour (i,j) devrait être proche de zéro et donne un petit effet au deuxième terme.

Au niveau de récepteur, le XOR est appliqué aux bits récupérés avec le même flux de bits pseudo-aléatoire pour obtenir le bon résultat.

Il est évident que l'utilisation d'un flux de bits pseudo-aléatoire dans le processus peut fournir un niveau de sécurité supplémentaire pour le filigrane intégré, par rapport aux techniques ordinaires de permutation.

Pour réduire l'effet d'une partie de luminance dans le second et quatrième terme, toutes les valeurs de luminance autour de (i,j) doivent être égalisées. Nous introduisons donc un nouveau paramètre $L'_{(i,j)}$, que nous utilisons en remplacement de $L\ (i,j)$.

En pratique, un procédé basé sur l'espace filtrage passe-bas peut être utilisé pour obtenir $L'_{(i,j)}$ comme décrit précédemment [63]. Cette approche a été la première introduite dans [27], où un filtre appelé masque de pondération Gaussien a été utilisé pour égaliser les valeurs de luminance autour de (i,j), et en même temps, pour donner plus de poids graduellement vers le centre de la zone de filtrage.

Les auteurs ont utilisé cette méthode pour obtenir $L'_{(i,j)}$, leur résultat obtenu est équivalent à un prétraitement de l'image avec un filtre passe-bas, et par conséquent, toutes les valeurs de luminance dans (i,j) seront modifiées pour atteindre sa valeur moyenne locale.

Fondamentalement, dans un filtre de masque Gaussien, les coefficients à l'intérieur de la zone de filtrage $g\ (x,y)$ peuvent être décrits par une distribution Gaussien et déterminé selon l'équation (III.7).

$$g_{(x,y)} = \frac{1}{2\pi\sigma^2} e^{-((x^2+y^2)/2\sigma^2)} \qquad (III.7)$$

Par exemple, le coefficient au centre de la zone de filtrage, $g\ (0,0)$, est obtenu par la substitution à la fois de x et y à zéro. Pour un masque Gaussien 3×3 pixels, les valeurs de x et y varient entre -1 et 1, et les coefficients obtenus sont donnés par l'équation (III.8).

$$\begin{bmatrix} \frac{0.5e^{-(1/\sigma^2)}}{\pi\sigma^2} & \frac{0.5e^{-(0.5/\sigma^2)}}{\pi\sigma^2} & \frac{0.5e^{-(1/\sigma^2)}}{\pi\sigma^2} \\ \frac{0.5e^{-(0.5/\sigma^2)}}{\pi\sigma^2} & \frac{0.5}{\pi\sigma^2} & \frac{0.5e^{-(0.5/\sigma^2)}}{\pi\sigma^2} \\ \frac{0.5e^{-(1/\sigma^2)}}{\pi\sigma^2} & \frac{0.5e^{-(0.5/\sigma^2)}}{\pi\sigma^2} & \frac{0.5e^{-(1/\sigma^2)}}{\pi\sigma^2} \end{bmatrix} \quad (III.8)$$

Généralement, $L'_{(i,j)}$ obtenu à partir du filtrage spatial linéaire d'une image avec le masque Gaussien ci-dessus est donnée par l'équation (III.9).

$$L'_{(i,j)} = \left(\sum_{m=-1}^{1} \sum_{n=-1}^{1} g_{(m,n)} L_{(i+m,j+n)} \right) \quad (III.9)$$

La Figure III.2 représente les valeurs des coefficients de la matrice gaussienne 3×3 pixels à des valeurs particulières de σ^2. Comme on peut le voir sur la figure (III.2).

$$\begin{bmatrix} 0.019 & 0.100 & 0.019 \\ 0.100 & 0.531 & 0.100 \\ 0.019 & 0.100 & 0.019 \end{bmatrix} \quad \begin{bmatrix} 0.050 & 0.115 & 0.050 \\ 0.115 & 0.265 & 0.115 \\ 0.050 & 0.115 & 0.050 \end{bmatrix} \quad \begin{bmatrix} 0.059 & 0.097 & 0.059 \\ 0.097 & 0.159 & 0.097 \\ 0.059 & 0.097 & 0.059 \end{bmatrix}$$

(a) (b) (c)

Figure III.2 : Les Valeurs des coefficients du masque Gaussien (a) $\sigma^2 = 0.3$ (b) $\sigma^2 = 0.6$ (c) $\sigma^2 = 1$.

L'algorithme d'insertion de la méthode appliquée [26] donnés par la figure (III.3).

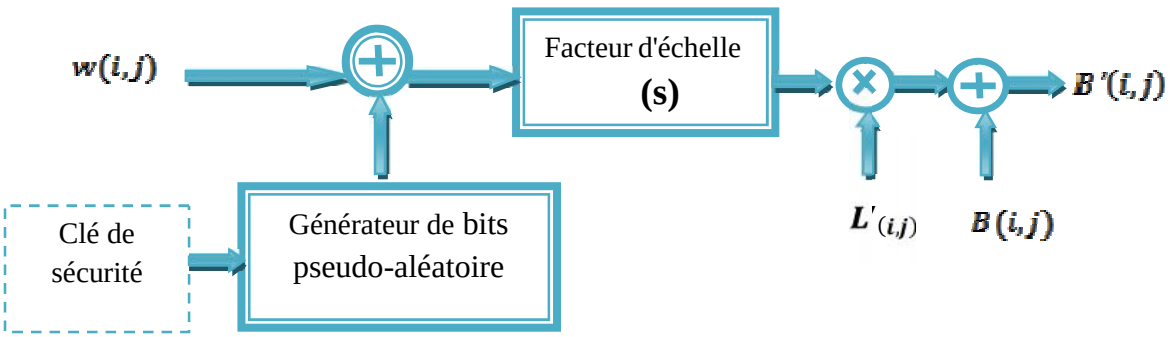


Figure III.3: Schéma d'insertion de filigrane [25].

Dans un système pratique, une valeur appropriée de σ^2 doit être soigneusement choisie, autrement une valeur de $L'_{(i,j)}$ très faible diminuera la robustesse du filigrane inséré.

III-3-2. Phase de détection

En considérant le premier et le troisième terme de l'équation. (III.5) seront retirés selon l'effet de la luminance $L'_{(i,j)}$ si la prédiction de $B(i,j)$correspond à la $B\ (i,j)$ originale.

En théorie, la valeur de $B'(i,j)$ devrait être plus proche de $B\ (i,j)$ par rapport à ses voisins.

au lieu de calculer $B''(i,j)$ de 8 valeurs de pixels voisins autour (i,j), les auteurs déterminé $B''(i,j)$ de 7 parmi 8 valeurs de pixels voisins autour (i,j) et la valeur de pixel elle-même tatouée. Les auteurs Notez qu'il donne à la fois des impacts sur le troisième et le quatrièmes terme, une nouvelle prédiction de $B\ (i,j)$ devrait approcher $B\ (i,j)$.

Les résultats obtenus dans [25] peuvent varier en fonction des caractéristiques de l'image tatouée. La procédure de remplacement de la valeur du pixel indiqué ci-dessous.

$diff\_max = 0$
$m\_max = 0$
$n\_max = 0$
DO $m = -1, 1$
DO $n = 1, 1$
IF ($|B'[m, n] - B'[i, j]| > diff\_max$)
$diff\_max = |B'[m, n] - B'[i, j]|$
$m\_max = m$
$n\_max = n$
E ND IF
$|B'[m\_max, n\_max] - B'[i, j]| = B'[i, j]$
END DO
END DO

On peut voir que, dans le cas extrême d'avoir où l'on a deux valeurs des pixels ou plus dans le voisinage, le premier détecté sera remplacé par calcul. Dans le schéma de tatouage présenté dans [25], toutes les méthodes proposées produisent une amélioration maximale.

Le Schéma Bloc de la procédure de modulation du filigrane est illustrée sur la Figure(III.3) et une nouvelle modulation du pixel et une nouvelle prédiction de $B(i,j)$, peut alors être exprimé selon les équations (III.10), (III.11).

$$B'(i,j) = B(i,j) + w(i,j)SL'(i,j) \qquad (III.10)$$

$$B''_{(i,j)} = \frac{1}{8}\left(\sum_{m=-1}^{1}\sum_{n=-1}^{1} B'_{(i+m,j+n)} - B'_{(\text{m\_max,n\_max})}\right) \qquad (III.11)$$

III-4. Outils d'évaluation

III-4-1. Le MSE: Mean Square Error

Le MSE représente l'erreur quadratique moyenne entre l'image tatouée et celle originale. Afin de permettre d'évaluer l'influence de la marque sur l'image cette mesure évalue l'influence de la marque sur l'image. Il est définit comme suit :

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{ij} - I_{ij}^{*})^2}{MN} \qquad (III.12)$$

I et I^{*} sont respectivement l'image originale et l'image tatouée de tailles $N \times M$ où I_{ij} et I_{ij}^{*} sont leurs composantes.

III-4-2. Le PSNR : Peak Signal Noise Ratio

Le PSNR permet de déterminer l'imperceptibilité de la signature. En d'autre terme, il permet d'évaluer la dégradation en dB de l'image originale provoquée par l'insertion de la marque, et éventuellement par d'autres attaques. Lorsque le PSNR est élevé, la distorsion devient moins importante. On considère généralement en tatouage d'images qu'un tatouage est imperceptible quand le PSNR est supérieur à 36 dB [64].

Le PSNR est définit comme suit :

$$PSNR = 10log_{10}\left(\frac{I_{max}^2}{MSE}\right) \qquad (III.13)$$

III-4-3. Le NC : Corrélation Normale

Une étude comparative entre ces mesures est présentée par Eskicioglu et Fisher [65]. La corrélation normale (NC), entre la marque extraite $\acute{\omega}$ et l'originale ω , est aussi utilisée pour évaluer la qualité de l'extraction de la marque cachée. Cette corrélation est calculée par la formule suivante :

$$NC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\omega(i,j) \times \acute{\omega}(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\omega(i,j))^2} \qquad (III.14)$$

Où N × M est la taille du message binaire.

III-5. Conclusion

Dans ce chapitre, nous avons présenté le tatouage d'images numériques basé sur la modulation d'amplitude d'une manière générale où nous mentionnons des notions théoriques. Nous nous sommes intéressés aux principes et aux notions pertinentes dans le domaine de modulation de filigrane telles que la permutation, l'insertion, et la détection de filigrane où nous mentionnons des notions théoriques.

CHAPITRE IV:

Résultats et discussion

IV-1. Introduction

La couleur est une donnée importante pour une image, elle modifie la perception que l'on a de l'image. Malgré leur intérêt capital, la plupart des méthodes de tatouage d'images sont pointées vers les images à niveaux de gris.

Dans ce chapitre on se concentrera essentiellement sur la comparaison entre notre méthode et des méthodes de tatouage numérique d'images couleurs qui vise à insérer une marque dans le plan de couler bleu (B) de matrice d'image (RVB).

On étudiera quelques attaques sur les images tatouées pour définir les caractéristiques relatives (robustesse et transparence) à ces algorithmes telles que la compression et la rotation.

IV-2. Méthode proposée

Notre méthode basée sur la technique présentée dans la section (III-2) avec une seule modification sur L'algorithme d'insertion et une autre technique de détection de la marque.

Une image couleur est décomposée en trois matrices (RVB), et notre marque $w(i,j)$ est insérée dans le plan de bleu(B)

IV-2-1. Algorithme d'insertion

1. Décomposition de l'image originale en trois matrices (rouge, vert, bleu).
2. Permutation de la marque $w(i,j)$ par les XOR avec un train de bits pseudo-aléatoires, générés à partir d'une clé choisie.
3. Insertion de la marque dans la matrice bleue (B) par la méthode utilisée dans le chapitre trois avec une autre permutation.
4. Reconstruction de l'image tatouée à partir des trois composantes R , V et B'.

Le principe de cet algorithme est présenté sur la figure (IV.1).

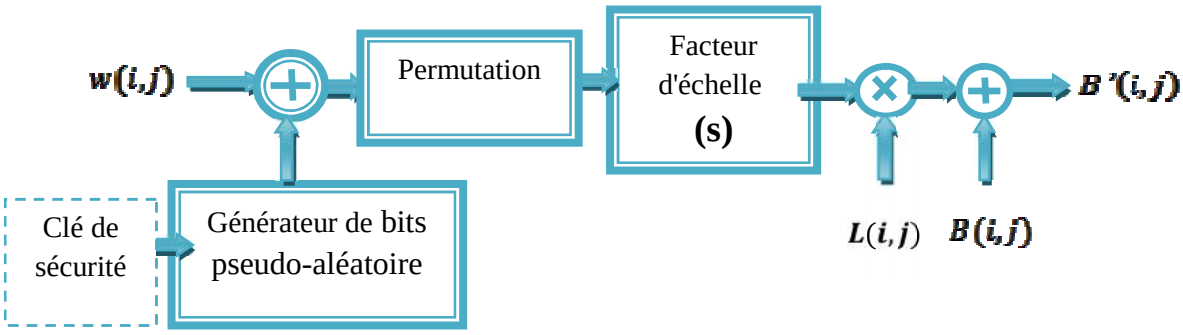


Figure IV.1: Schéma d'insertion de la marque.

IV-2-2. Algorithme d'extraction

1. Décomposition de l'image originale en trois matrices (rouge, vert, bleu).
2. Utilisation du plan de bleu (B) pour détecter la marque par les valeurs de pixels voisins autour de (i, j) comme la méthode utilisée dans le chapitre trois.
3. Détection de la marque $w(i, j)$ par les XOR avec un même train de bits pseudo-aléatoire, généré à partir d'une clé choisie.

Le principe de cet algorithme est présenté sur la figure (IV.2).

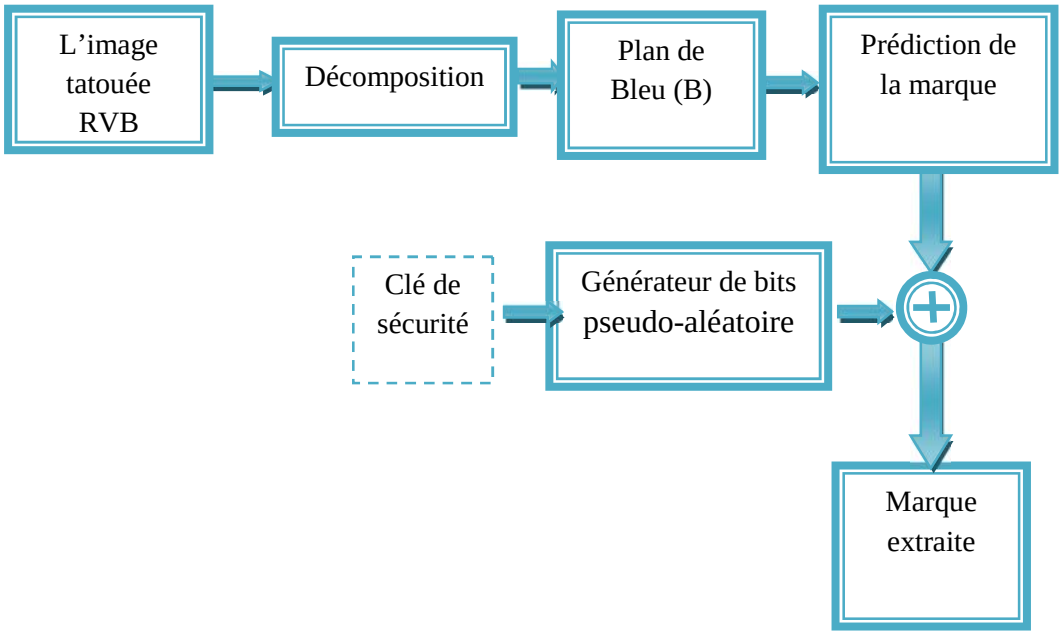
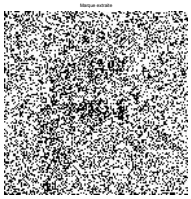


Figure IV.2: Schéma d'extraction de la marque.

IV-3. Application de l'algorithme proposé sur l'image test Lena

Nous appliquons l'algorithme décrit précédemment sur l'image hôte « Lena» de taille 512*512 qui est très utilisée en traitement d'images. L'image tatouée est représente sur le tableau (IV.1).

Tableau IV.1 : Les effets du facteur d'échelle **S** sur l'image tatouée.

L'Image originale et La Marque originale	**facteur d'échelle S**		
	S=0,01	S=0,1	S=0,5
			
			
Nc	Nc=0.8140	Nc=0,9893	Nc=0,9969

Le tableau (IV.1) montre les effets des diverses valeurs du facteur d'échelle **S** sur l'image tatouée. On peut voir que le choix d'un facteur d'échelle élevé provoque un changement significatif sur l'image tatouée, par contre la marque détectée bien visible.

Alors if faut choisir de facteur d'échelle optimal avec l'imperceptibilité et la robustesse optimal les résultats expérimentaux montrent que la valeur S=0.1 permet une bonne imperceptibilité de l'image tatouée et une bonne robustesse de la marque.

IV-4. Conditions pour les techniques de tatouage d'images numériques

Les méthodes de tatouage requièrent différentes propriétés selon leurs domaines d'application. La marque cachée dans une image doit remplir deux conditions essentielles.

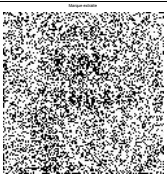
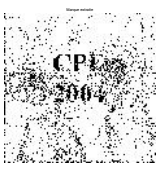
La première est consacrée au test de la propriété d'imperceptibilité alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques.

IV-4-1. Propriété d'imperceptibilité

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, les images originales et les images tatouées sont présentées respectivement dans le tableau (IV.2).

Les résultats ont été obtenus avec un facteur d'échelle S = 0,01 et une variance $\sigma^2 = 0{,}3$.

Tableau IV.2 : Exemples d'application de l'imperceptibilité avec plusieurs images.

	lena	**poivron**	Parrots
Image originale			
Image tatouée			
Marque extraite			
Nc	Nc= 0.8154	Nc= 0.9461	Nc= 0.9369

A partir de ce tableau, on peut voir qu'il est difficile de différencier entre les images originales et les images tatouées, alors la méthode est donc imperceptible.

Après l'extraction de la marque, le coefficient de corrélation est calculé en utilisant les marques originales et extraites. Ce coefficient permet de juger l'existence de la marque extraite**.**

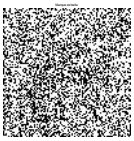
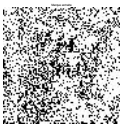
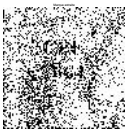
IV-4-2. Propriété de robustesse

Une propriété très importante que doit garantir un algorithme de tatouage est la robustesse contre les attaques. Afin d'évaluer la robustesse de notre technique de tatouage, plusieurs types d'attaques ont été implantées.

IV-4-2-1. La compression JPEG

La compression JPEG est le schéma de codage d'images le plus populaire et est généralement considéré comme une attaque dure contre les algorithmes de tatouage d'images. En effet, plusieurs méthodes ne sont pas robustes à ce type d'attaque. Les expériences sont appliquées sur l'image « lena » de taille 512*512.

Tableau IV.3 : Extraction de marque en appliquant plusieurs facteurs de Compression JPEG avec un facteur d'échelle constant S = 0,3.

	facteur de Compression (%)		
	88%	**95%**	**100%**
Image originale			
Image compressée			
Marque extraite			
Nc	Nc= 0.7835	Nc= 0. 8423	Nc= 0.8694

Les marques sont identifiables et les coefficients de corrélation sont proches de **0.9.** On peut alors conclure que la méthode est très robuste à la compression JPEG**,** mais la diminution du facteur de compression va affecter la qualité de la marque extrait.

IV-4-2-2. Le filtrage

Parfois pour améliorer la qualité visuelle de l'image, on doit éliminer les effets des bruits (Parasites) en lui faisant subir un traitement appelé filtrage. Le filtrage consiste à appliquer une transformation (appelée filtre) à tout ou à une partie d'une image numérique en appliquant un opérateur. Dans cette partie en applique deux types de filtrage : le filtre médian (Disque) et un filtre passe-bas (Gaussien).

Les images filtrées sont représentées sur les tableaux (IV.4) et (IV.5).

Tableau IV.4: Extraction de la marque après application du filtre passe-bas.

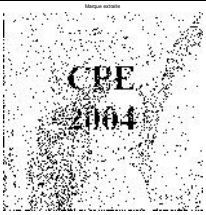
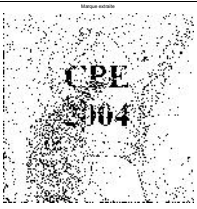
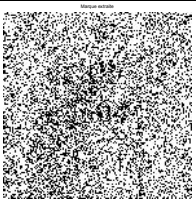
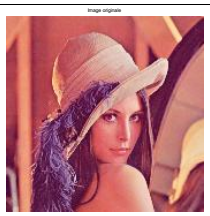
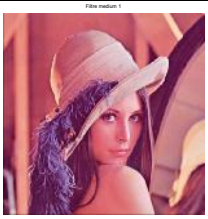
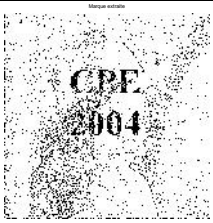
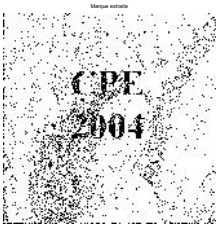
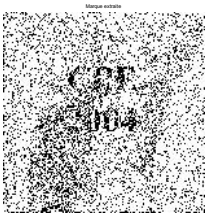
L'Image originale et La Marque originale	**L'Image filtrée et La Marque extraite**		
	sigma = 0,3	**sigma = 0,5**	**sigma = 1**
			
			
Nc	Nc=0. 9521	Nc=0, 9476	Nc= 0.8243

Tableau IV.5: Extraction de la marque après application de filtre médian (disque).

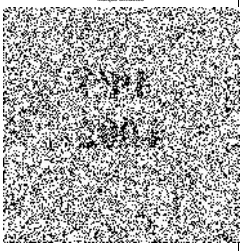
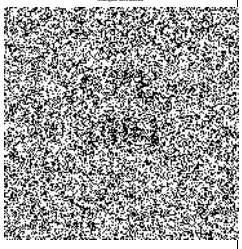
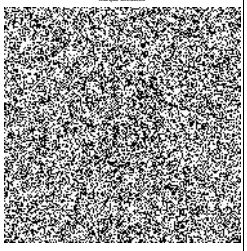
L'Image originale et La Marque originale	**L'Image filtrée et La Marque extraite**		
	rayon = 0,3	**rayon = 0,5**	**rayon =1**
			
			
Nc	Nc= 0. 9526	Nc = 0, 9520	Nc = 0. 8862

Les tableaux (IV.4) et (IV.5) montrent que les marques extraites en appliquant les divers types de filtre utilisés sont identifiables et les coefficients de corrélation sont proches de **1.** On peut alors conclure que la méthode est robuste contre ces types de filtres.

IV-4-2-3. Bruitage

Afin d'évaluer la robustesse de notre méthode contre le bruit, on applique quelques types de bruit sur l'image tatouée avec divers pourcentages de bruit. Le tableau suivant présente les marques extraites après ajout de bruit Gaussien.

Tableau IV.6: L'extraction de la marque après l'application d'un bruit de Gaussien.

L'Image originale et La Marque originale	**L'Image filtrée et La Marque extraite**		
	La force d'attaque = 3%	**La force d'attaque = 9%**	**La force d'attaque = 18%**
			
			
Nc	Nc=0. 8314	Nc=0, 7826	Nc= 0.7603

Le tableau montre les marques extraites après l'application du bruit Gaussien. Les marques sont identifiables et les coefficients de corrélation sont proches de **0.8**, mais l'augmentation du pourcentage de bruit va diminuer les coefficients de corrélation mais on peut identifier la marque facilement donc la méthode est robuste au bruit de Gaussien.

IV-5. Performance de la méthode proposée

Pour pouvoir étudier la performance de notre méthode il faut faire des comparaisons avec d'autres méthodes de tatouages d'images.

Les résultats obtenus avec notre méthode basée sur la modulation d'amplitude doivent être comparés avec des méthodes basées sur le même domaine comme les méthodes sont proposées dans [25], [26] et [27].

Nous présentons une comparaison de notre méthode et de celles dans les références [25], [26] et [27] dans le tableau (IV.7).

Tableau IV.7: comparaison des schémas utilisés dans [25], [26] et [27].

Schéma	***Preparation de filigrane***	***Modulation de filigrane***	***Detection de filigrane***
Kutter's [27]	Sans L'opération de XOR	Utilise les valeurs de luminance par modulation de pixel	Utilise les voisinage (4 pixels)
Puterpan's [26]	Sans L'opération de XOR	Utilise les valeurs de luminance par modulation de pixel, et leurs pixels voisins	Utilise les valeurs de pixels voisins autour de (i, j) (8 pixels)
Amornraksa [25]	Avec L'opération de XOR	Utilise les valeurs de luminance par modulation de pixel, et leurs pixels voisins	Utilise les valeurs de pixels voisins autour de (i, j) , Et le pixel central (8 pixels)
Méthode proposée	Avec L'opération de XOR	Utilise les valeurs de luminance par modulation de pixel, et leurs pixels voisins et permutation.	Utilise les valeurs de pixels voisins autour de (i, j)

Pour mieux tester les algorithmes, nous choisissons des images de tests de Lena, Bird , Tower et Fish de tailles 256×256, qui sont considérées comme des échantillon des images homogènes (douces).

Les valeurs du RMSE de quatre image (lena , bird, tower et fish) sont présentées dans la Tableau (IV.8) .

Tableau IV.8: Les RMSE des images tatouées.

L'image taouée	lena	bird	fish	moyenne
RMSE	10.27	4.83	5.56	6.92

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, il faut calculer la moyenne de PSNR de quatre images tatouées (lena ,bird, tower et fish) pour différents facteurs d'échelle S et des variances σ^2 sont présentées respectivement dans les tableau (IV.9) (IV.10) .

Tableau IV.9: PSNR Moyenne (dB) de différent facteur d'échelle S.

Facteur d'échelle (S)	0.02	0.06	0.1	0.2	0.3	0.4	0.5
PSNR moyenne (dB)	34.05	24.51	20.07	14 ,05	10,53	8 ,03	6.09

Tableau IV.10: PSNR Moyenne (dB) de différent valeurs de variance σ^2 .

σ^2	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
PSNR Moyenne (dB)	23,31	25,03	26,55	26.73	26.90	27.13	27.28	27.35	27.43	27.81

D'après les tableaux (IV.9) et (IV.10), On remarque une diminution du PSNR moyenne lorsque de facteur d'échelle S augment, mais Pour les différentes valeurs de variance σ^2 les PSNR moyennes sont presque constantes.

Pour pouvoir étudier la comparaisons de notre méthode avec les méthodes étudiées dans [25], [26] et [27] , il faut sélectionner le même PSNR moyenne que celle fixée dans les références [25], [26] et [27].

Apres l'extraction de la marque, le coefficient de corrélation est calcule en utilisant la marque originale et celui extrait. Ce coefficient permet de juger l'existence et l'exactitude de la marque extrait.

Dans notre travail nous calculons la moyenne de Nc de quatre images pour faire la comparaison.

IV-5-1. Comparaison de l'influence des parametres de modulation

Ces comparaisons sont basées sur des l'influence des parametres des methodes de modulation d'amplitude comme le facteur d'echelle S et la variance σ^2. Nous présentons les résultats de la Comparaison des Nc moyennes à différents S avec une variance σ^2 = 0,3 sur la Figure (IV.3) et la Comparaison des Nc moyennes à différents σ^2 avec un facteur d'échelle S = 0,1 sur la Figure (IV.4).

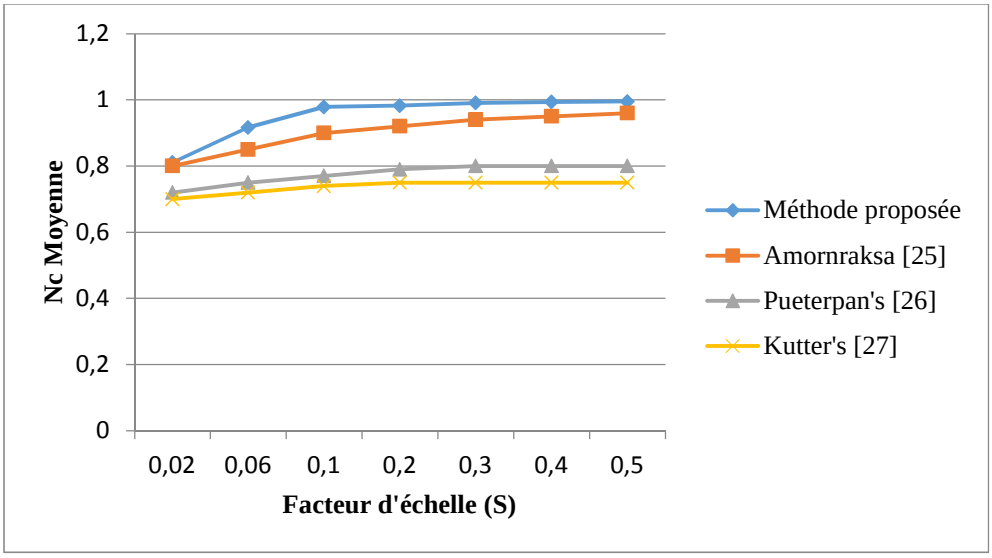


Figure IV.3: Comparaison des Nc moyennes à différents S.

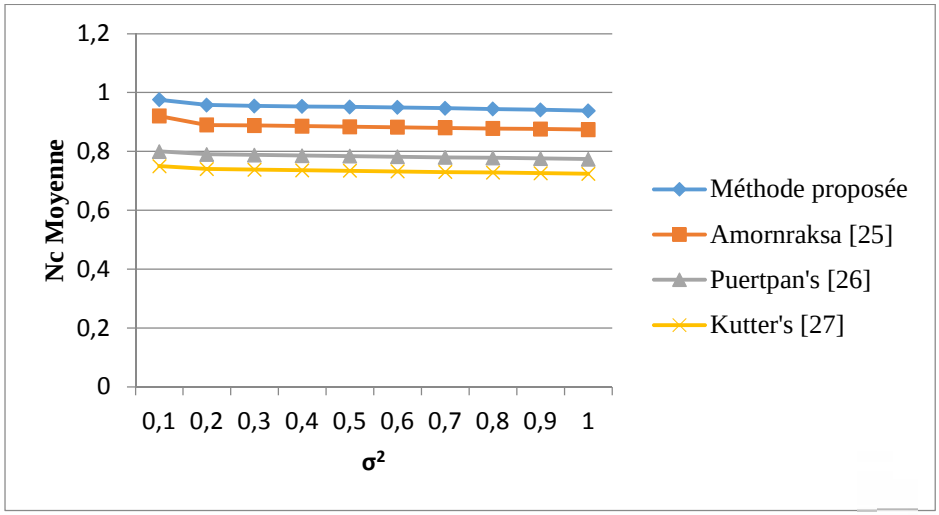


Figure IV.4: Comparaison des Nc moyennes à différents σ^2.

D'après les Figures (IV.3) et (IV.4), les Nc moyennes de notre tatouage sont plus grandes par rapport à celles obtenues par les autres algorithmes (légère amélioration).

On remarque aussi une augmentation de le Nc moyenne lorsque de facteur d'échelle S augment, mais Pour les différentes valeurs de variance σ^2 les Nc moyennes sont presque constantes.

IV-5-2. Robustesse contre les attaques

Une propriété très importante que doit garantir un algorithme de tatouage est la robustesse contre les attaques. Dans cette partie, les expériences sont conduites sur les images couleurs (RVB) Lena, Bird, Tower et Fish des tailles 256 × 256 avec facteur d'échelle s=0,2 et variance σ^2= 0,3004.

Les figures (IV.5), (IV.6) et (IV.7) présentent les comparaisons des Nc moyennes pour différentes attaques :

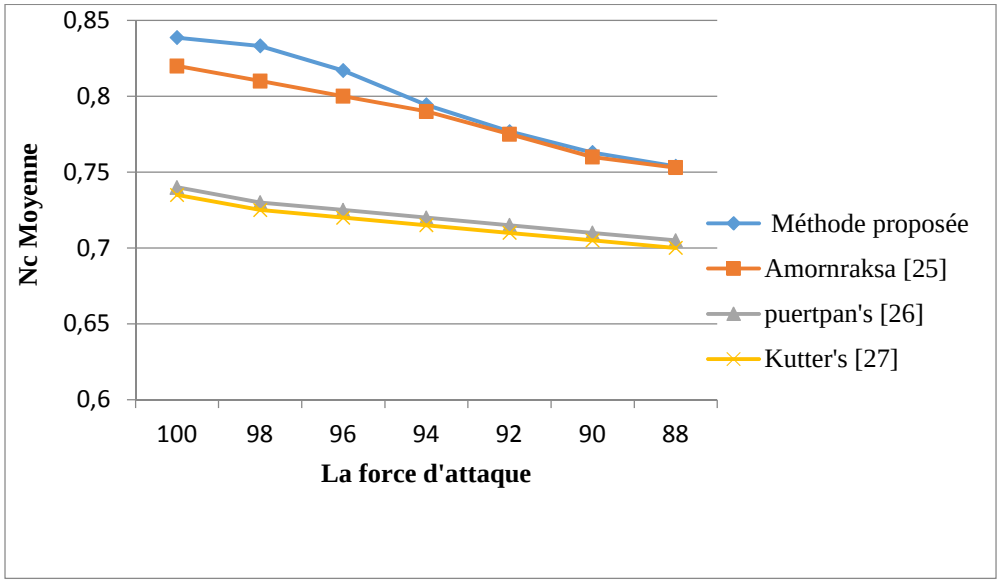


Figure IV.5: Comparaison des Nc moyennes après l'application d'une Compression JPEG.

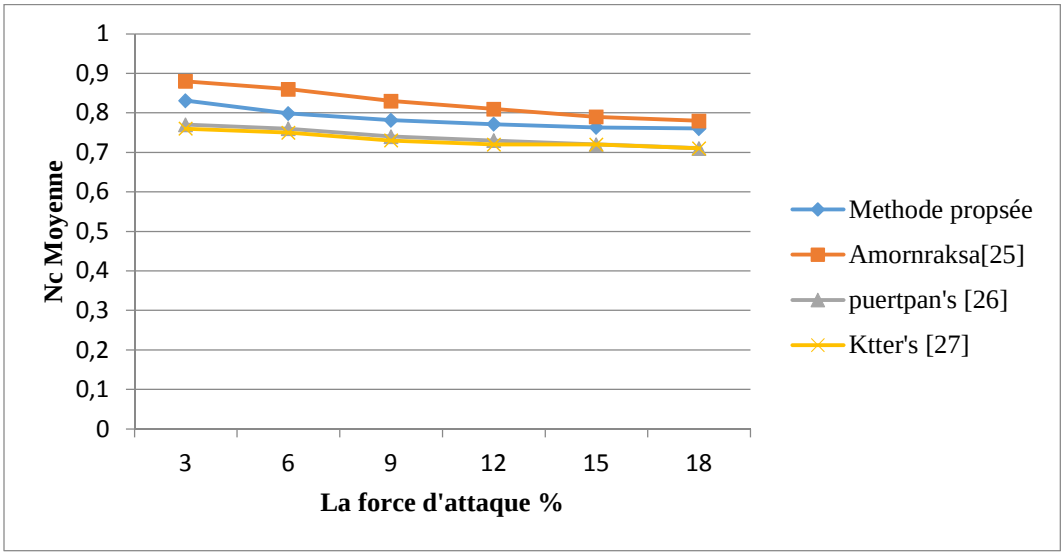


Figure IV.6: Comparaison des Nc moyennes après l'application d'un bruit de Gaussien.

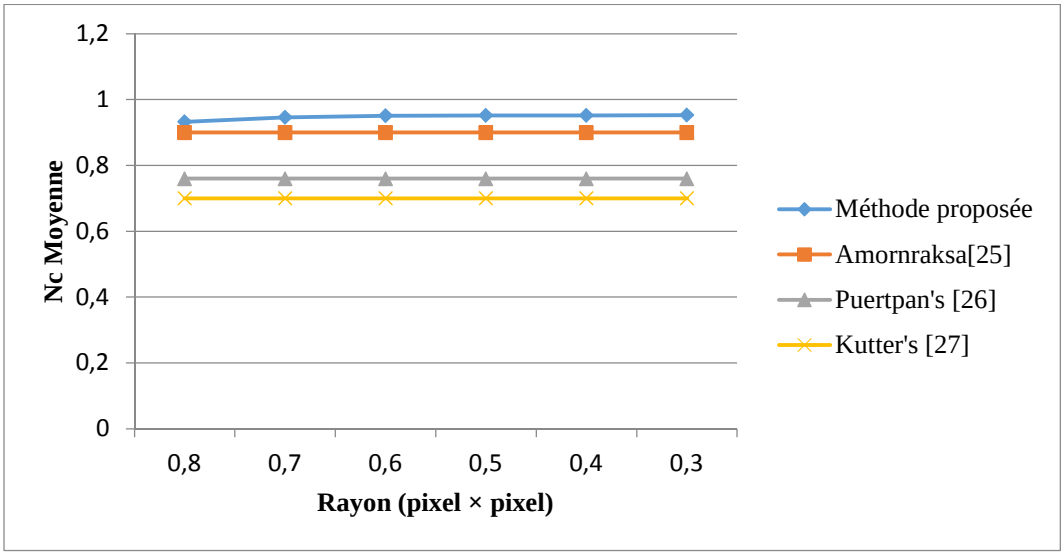
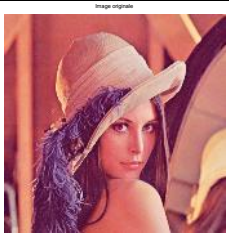
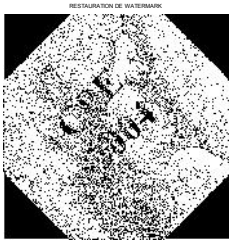
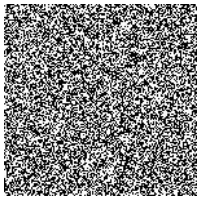
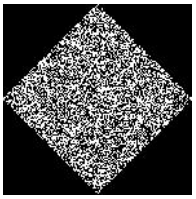
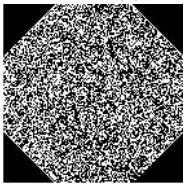


Figure IV.7: Comparaison des Nc moyennes après l'application d'un filtre médian (disque)

D'après les Figure (IV.5), (IV.6) et (IV.7) les Nc moyennes de notre tatouage sont plus grande par rapport à celles obtenues par les autres algorithmes sauf pour le bruit Gaussien, Les résultats obtenus nous permettent de déduire que la méthode du tatouage proposée est efficace du point de vue qualité et robustesse de l'image tatouée.

Le point faible de notre algorithme est la détection de la marque après l'attaque géométrique de rotation. Donc pour détecter la marque il faut appliquer une même rotation pour la matrice de Générateur pseudo-aléatoire de clé de secrète. La rotation de l'image est représentée sur le tableau (IV.11).

Tableau IV.11: Extraction de la marque après l'application d'une rotation de 45^0 et redimensionnement (fenêtrage) de 50%.

L'Image tatouée et La Matrice de clé secrète	**L'Image filtrée et La Marque extraite**		
	Rotation(45^0)	**fenêtrage (50%)**	**Détection**
			
			

IV-6. Conclusion

Dans ce chapitre, nous avons présenté une étude de performance de la méthode de tatouage des images fixes à base de la modulation d'amplitude. La technique a été testée sur un certain nombre d'images comme Lena et Parrots. La robustesse du marquage a été validée à l'aide des attaques de compression JPEG, filtrage passe – bas, bruitage et rotation. Les résultats obtenus montrent que le tatouage par la modulation de amplitude est insensible au filtrage, au bruitage et à la compression JPEG, mais très fragile devant les attaques géométriques (rotation et redimensionnement).

BIBLIOGRAPHIE

[01] B. Furht and D. Kirvsski : *"Multimedia Security Handbook "*, Chapter 4, *"Chaos-Based Encryption for Digtal Images and Videos"* Published by CRC Press LLC in December2004.

[02] A. Manoury : *"Tatouage d'images numériques par paquets d'ondelettes"*, Thése de doctorat, Université de Nantes, 2001.

[03] M. Nelson : "*La compression de données textes, Image, son* ", Edition Dunod, 1993.

[04] D. Lingrand: "*Introduction aux traitement d'images*", Vuibert, 2008.

[05] M . Nixon and A. Aguado: "*Feature Extraction and Image Processing*", British Library Cataloguing in Publication Data, 2002.

[06] A. Benoit: "Le *système visuel humain au secours de la vision par ordinateur*", PhD thèses, Ecole Doctorale EEATS : Electronique, Electrotechnique, Automatique et Traitement du signal, Grenoble - France, 2007.

[07] Phil Gates: " *Wild Technology* ". de, p. 54.

[08] M. André: "*Introduction aux Technique de traitement d'image* ", Eyrolles, 1987.

[09] R.C. Gonzales et P. Wintz: "*Digital Image* Processing" Addition Wessley, 1997.

[10] M. Bergounioux: "Quelques *méthodes mathématiques pour le traitement d'image* ", In Cours master, chapitre 1, 2009.

[11] M. Nixon, A. Aguado: "*Feature extraction and image processing*", British Library Cataloguing in Publication Data, 2002.

[12] D.Lingrand: "*Introduction aux traitement d'images* " Vuibert. 2008.

[13] M-T . Alaoui : "*introduction au traitement d'images* **"**, Simulation sous Matlab, Département Mathématique et Informatique, Oujda.

[14] Jean Luc Le Luron: " *Les images numérique, généralités*", 2003.

[15] M. Bergounioux. **:** " *Quelques méthodes mathématiques pour le traitement d'image*" , In Cours master, chapter 1, 2009.

[16] N.Golea: "*Tatouage numérique des images couleurs RGB* ", thèse présentée en vue de l'obtention magister en informatique de l'université ELHADJ LAKHDER – BATNA, 2010.

[17] Ahmed M. N. Al-Gindy : "*design and analysis of discrete cosinetransform-based watermarking algorithms for digitalimages*", School of Computing, Informatics and Media University of Bradford 2011.

[18] G. Chareyron: "*Tatouage d'images: une approche couleur* ", thèse présentée en vue de l'obtention du titre de docteur de l'université Jean Monnet Saint-Etienne, le 8 Décembre 2005.

[19] Khaled Loukhaoukha: "*Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective* ", mémoire de doctorat, université laval québec, 2010.

[20] Vu Duc Minh : "*Tatouage des images dans un domaine fréquentiel* ", Thèse de Doctorat en traitement d'images, Ha noi, Janvier 2006.

[21] Drira Fadoua: "*Tatouage d'image par techniques multidirectionnelles et multi résolution*", mémoire d'étude approfondies, université Claude Bernard Lyon, 09juillet 2003.

[22] F. Raynal: "*Etudes d'outils pour la dissimulation d'information: approches Fractales, protocoles d'évaluation et protocoles cryptographiques*", thèse de doctorat, Université Paris XI, mars 2002.

[23] Mohamed El Hajji "*la sécurité d'images par le tatouage numérique dans le domaine d'ondelettes*", Thèse de doctorat.28/01/2012.

[24] S. Pan, H.-C. Huang, et L. C. Jain: "*Intelligent Watermarking Techniques*", World Scientific Publishing Company, Singapore, ISBN: 981-238-757-9,2004.

[25] T. Amornraksa and K. Janthawongwilai, "*Enhanced Images Watermarking Based on Amplitude Modulation,*", Image and Vision Computing, vol. 24, no. 2, pp. 111-119, 2006.

[26] M. Kutter, F. Jordan, F. Bossen, *"Digital signature of colour images using amplitude modulation"* , Journal of Electronic Imaging 7. 326–332,1998.

[27] R. Puertpan, T. Amornraksa: *"Gaussian pixel weighting marks in amplitude modulation of colour image watermarking"*, in: Proceedings of the IEEE ISSPA, Kuala-Lampur, Malaysia, 2001.

[28] **Lei-Da Li, Bao-Long Guo**: *"Localized image watermarking in spatial domain resistant to geometric attacks"*, AEU - IJE, Vol. 63(2): pp. 123-131, 2009.

[29] X. Wu, Z-H. Guan, Z. Wu: *"A Chaos Based Robust Spatial Domain Watermarking"*, Vol. 4492: pp.113-119, 2007.

[30] A. Piva, M. Barni, F. Bartolini: *"Copyright Protection of Digital Images by Means of Frequency Domain Watermarking, in Mathematics of Data/Image Coding, Compression, and Encryption"*, Proceedings of SPIE, Vol. 3456, pp. 25-35, San Diego, California, 1998.

[31] V. Solachidis, I Pitas: *"Self-similar ring shaped watermark embedding in 2-D DFT domain"*, EUSIPCO 2000, 5-8 September 2000.

[32] F. Ros, J. Borla, F. Leclerc, R. Harba, N. Launay : *"Watermarking for Plastic Card Supports"*, 9ème Conference Maghrébine sur Les Technologies de L'Information, MCSEAI, Agadir 2006.

[33] S. Perreira, J. J. K. O Ruanaidh, F. Deguillaume, G. Csurka, T. Pun: *"Template Based Recovery of Fourier-Based Watermarks Using Log-polar and Log-log Maps"*, IEEE int. Conf on Multimedia Computing and Systems (ICSMS'99), Florence, Italy, June 1999.

[34] J. Ruanaidh, T. Pun: *"Rotation, scale and translation invariant digital image watermarking"*, Proceedings of the IEEE International Conference on Image Processing (ICIP), 1997.

[35] C.-Y. Lin, M.Wu, J. Bloom, M. Miller, I. Cox, and Y.- M. Lui: *"Rotation, scale, and translation resilient public watermarking for images"*, IEEE Transactions on Image Processing, vol. 10(5): pp. 767–782, 2001.

[36] X. Qi and J. Qi: *"Improved affine resistant watermarking by using robust templates"*, Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), vol. 3: pp. 405-408, 2004.

[37] A. B. Watson and J. Solomon: *"Model of visual constrast gain control and pattern masking"*, Journal of the Optical Society of America, vol. 14, pp. 2379–2391, Sept. 1997.

[38] J. Lubin: *"A visual discrimination model for imaging system design and evaluation, Dans Vision Models for Target Detection and Recognition"*, ed. E. Peli, 245–283, World Scientific Publishing, 1995.

[39] I.J. Cox, J. Killian, F.T. Leighton, T. Shamoon*: "Secure spread spectrum watermarking for multimedia"*, IEEE Trans. Im. Proc., Vol. 6(12: pp. 1673–1687, 1997.

[40] Mohamed A. Suhail: *"Digital Watermarking-Based DCT and JPEG Model"*, IEEE Transactions on Instrument and Measurements, vol. 52(5), pp. 1640-1647, October 2003.

[41] E. Koch, S. Burgett, and J. Zhao: *"Copyright labeling of digitized image data"*, IEEE Commun. Mag., pp. 94-100, Mar. 1998.

[42] W.B. Pennebakker, J.L. Mitchell: *"The JPEG Still Image Data Compression Standard"*, New York, Van Nostrand, 1993.

[43] Q Li, I J. Cox: *"Using Perceptual Models to Improve Fidelity and Provide Resistance to Valumetric Scaling for Quantization Index Modulation Watermarking"*, IEEE transactions on information forensics and security, vol. 2 (2), june 2007.

[44] C. Chen, X. Wu: *"An Angle QIM Watermarking Algorithm Based on Watson Perceptual Model"*, Fourth International Conference on Image and Graphics ICIG 2007, pp. 324-328, 2007.

[45] Y. Hu, Z. Wang, H. Liu, G. Guo: *"A Geometric Distortion Resilient Image Watermark Algorithm Based on DWT-DFT"*, Journal Of Software, Vol. 6(9): pp. 1805-1812. 2011.

[46] Liu Quan, AI Qingsong: *"A combination of DCT based and SVD based watermarking, ICSP proceedings of IEEE International conference on signal processing"*, pp. 873-876, 2004.

[47] T. Stathaki,P Dafas: *"Digital Image Watermarking Using Block-Based Karhunen-Loeve Transform"*, Proceedings of the 3rd International Symposium (ISPA), Rome, Italy, pp. 1072–1075, September 18-20, 2003.

[48] F. Lefèvre, D. Guéluy, D. Delannay, B. Macq: *"A Print and Scan Optimized Watermarking Scheme"*, IEEE Multimedia Signal processing, 2001.

[49] E. Yavuz, Z Telatar: "*Improved SVD-DWT based digital image watermarking against watermark ambiguity"*, In Proceedings of the 2007 ACM symposium on Applied computing (SAC '07), ACM, New York, NY, USA, pp. 1051-1055, 2007.

[50] Ke-feng he, et al: *"Watermarking for images using the HVS and SVD in the wavelet domain"*, Dans Proceedings of IEEE International Conference on Mechatronics and Automation, pp.2352- 2356,2006.

[51] Y. Hu, Z. Wang, H. Liu, G. Guo: *"A Geometric Distortion Resilient Image Watermark Algorithm Based on DWT-DFT"*, Journal Of Software, Vol. 6(9): pp. 1805-1812. 2011.

[52] S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun: Attack modelling: *"Towards a second generation watermarking benchmark"*, Proc. Signal Processing, vol.81: pp.1177–1214, 2001.

[53] I J. Cox and M L. Miller and J. Bloom and J. Fridrich and Ton Kalker: *"Digital watermarking and steganography (second edition) "*, Morgan Kaufmann, 2007.

[54] F.Petitcolas, R. anderson, M. Kuhn: *"Attacks on copyritht Marking Systems"*, Lecture Notes in computer Sciences (LNCS), Vol. 1525: pp. 219-239, 1998.

[55] S. Voloshynovskiy, F. Deguillaume, T. Pun: *"Multibit digital watermarking robust against local nonlinear geometrical distortions"*, Proceedings of the IEEE International Conference on Image Processing (ICIP), IEEE Computer Society Press, Los Alamitos, CA, pp. 999-1002, 2001.

[56] A. Keskinarkaus, A. Pramila, T. Seppanen: *"Image watermarking with a directed periodic pattern to embed multibit messages resilient to print-scan and compound attacks"*, Journal of Systems and Software, Vol. 83(10): pp. 1715-1725, 2010.

[57] J.P. Linnartz, M.V. Dijk: *"Analysis of the Sensitivity attack against Electronic Watermarks in Images"*, Proceedings of 2nd Workshop on Information Hiding, Portland, Springer Verlag – LNCS, avril 1998.

[58] P. Nguyen et S. Baudry: *"Le tatouage de données audiovisuelles"*, Les Cahiers du numérique, Vol. 4 : pp. 135-165, 2003.

[59] J P Boyer, P Duhamel, J Blanc-Talon: *"Tatouage Semi-Fragile et Théorie des Jeux : Etude d'un Système Basé sur le SCS"*, Compression et représentation des signaux Audiovisuels, coresa, Renne, 2005.

[60] A .Cziho: *"quantification vectorielle et compression d'image médicale"*, Thése Doctorat ,Université de Rennes 1 France 1999.

[61] J.F. Delaigle, C. Devleeschouwer, B. Macq, I. Langendijk, *"Human visual system features enabling watermarking"*, in: Proceedings of IEEE ICME, pp. 489–492.2002

[62] B. Schneier, *"Applied Cryptography"*, second ed., Wiley, New York, 1996.

[63] R.C. Gonzalez, R.E. Woods: *"Digital Image Processing"*, second ed., Prentice-Hall, New Jersy, 2002.

[64] I J. Cox and M L. Miller and J. Bloom and J. Fridrich and Ton Kalker: *"Digital watermarking and steganography (second edition) "*, Morgan Kaufmann, 2007.

[65] A. Eskicioglu and P. Fisher: *"Image Quality Measures and their Performance"*, *IEEE Transaction on communication*, Vol. 43(12): pp.2959–2965, 1995.

ملخص

قمنا في دراستنا بعملية وشم الصورة بواسطة طريقة تضمين السعة و التي تعتمد أساسا على إدراج الوشم بتغيير قيم الخلايا في المصفوفة الزرقاء للصورة الملونة , بينما تتم عملية استرجاع الوشم بالاعتماد على الخلايا المجاورة للخلية الموشومة , النتائج المتحصل عليها توضح قيمة وقوة طريقتنا مع تحسين طفيف مقارنة مع الطرق السابقة التي تعتمد على تضمين السعة.

كلمات مفتاحية :الوشم, السعة, تضمين, استرجاع.

Abstract

This work presents an image watermarking method with blind detection based on amplitude modulation. Basically, the watermark embedding is performed by modifying the pixel values in the blue channel of an image, while the watermark retrieval is achieved by using a prediction technique based on a linear combination of nearby pixel values around the embedded pixels. The experimental results obtained in this work clearly show the effectiveness and robustness of the proposed method and present a few improvements over the published methods of watermarking based on amplitude modulation.

Keywords: watermark, amplitude, modulation, prediction.

Résumé

Ce travail présente un tatouage d'image avec détection aveugle basée sur la modulation d'amplitude. Fondamentalement, l'intégration de filigrane est réalisée en modifiant les valeurs des pixels dans le canal bleu d'une image, tandis que la récupération du filigrane est obtenue en utilisant une technique de prédiction basée sur une combinaison linéaire des valeurs des pixels voisins autour des pixels intégrés. Les résultats expérimentaux obtenus montrent clairement l'efficacité et la robustesse de la méthode proposée et présentent une légère amélioration par rapport à celles des méthodes de tatouage d'images par la modulation d'amplitude publiées.

Mot clés : filigrane, amplitude, modulation, prédiction.