Tatouage robuste d'images imprimées

Rabia Riad

Université d'Orléans

École doctorale Mathématiques, Informatique, Physique Théorique et Ingénierie des Systèmes (MIPTIS)
Laboratoire PRISME
Pôle IRAuS, Axe Image et Vision

Université Ibn Zohr

Faculté des Sciences d'Agadir
Centre des Etudes Doctorales IBN ZOHR

Laboratoire IRF-SIC

THÈSE EN COTUTELLE INTERNATIONALE présentée par

RIAD Rabia

Soutenue le **19 décembre 2015**

Pour obtenir le grade de
Docteur de l'Université d'Orléans
et de l'Université Ibn Zohr

Discipline / Spécialité : **Automatique et Traitement du Signal**

Tatouage robuste d'images imprimées

THÈSE dirigée par :

DOUZI Hassan	Professeur, Université Ibn Zohr (Maroc)
HARBA Rachid	Professeur, Université d'Orléans (France)

RAPPORTEURS :

EL OUAHIDI Bouabid	Professeur, Université Mohammed-V Rabat (Maroc)
JACQUET Gérard	Professeur, Université de St Etienne (France)

JYRY :

MAMMASS Driss	Professeur, École Supérieure de Technologie d'Agadir (Maroc)
El HAJJI Mohamed	Professeur assistant, CRMEF (Maroc)

Remerciement

Je tiens tout d'abord à exprimer ma profonde gratitude à mes directeurs de thèse, Monsieur Hassan Douzi professeur d'enseignement supérieur à l'université Ibn Zohr Agadir, et Monsieur Rachid Harba professeur des universités à l'université d'Orléans, pour m'avoir proposé ce sujet riche d'informations. J'aimerais bien les remercier pour leur disponibilité envers moi ainsi que pour leurs conseils judicieux qui m'ont permis de surmonter les difficultés et de mener à bien ce travail.

Je tiens à exprimer mes profonds remerciements au professeur Driss Mammass directeur de l'école supérieur de technologie d'Agadir, qui m'a fait l'honneur de présider le jury. Je tiens à remercier profondément Monsieur Bouabid El Ouahidi professeur d'enseignement supérieur à l'université Mohammed-V de Rabat, pour l'attention qu'il a manifestée à l'égard de cette recherche en s'engageant à être rapporteur. Je souhaiterais aussi adresser mes remerciements au Monsieur Gérard Jacquet professeur des universités à l'université Jean Monnet de Saint-Étienne, pour avoir rapporté ma thèse ainsi que pour le temps qu'il a consacré pour la lecture de ce manuscrit.

Je voudrais remercier également Monsieur Mohamed El Hajji professeur assistant au centre régional des métiers de l'éducation et de la formation, d'avoir et être présent parmi les membres du jury, et pour l'aide qu'il m'a apportée.

Je tiens à remercier sincèrement Monsieur Frédéric Ros HDR, chercheur associé à l'université d'Orléans, qui m'a apporté une aide précieuse ainsi que le temps qu'il m'a accordé pour m'écouter et discuter avec moi.

Ces remerciements seraient incomplets si je n'en adressais pas à tous les collègues du laboratoire IRF-SIC et l'ensemble des membres des équipes « Image et Vision » et « Signal » du laboratoire PRISME pour leur soutien moral ainsi que le cadre agréable dans lequel ils m'ont permis de préparer ce travail dans une ambiance chaleureuse et conviviale.

J'adresse aussi mes remerciements à tous ceux qui m'ont aidé de près ou de loin à réaliser ce travail. Enfin j'exprime ici ma reconnaissance à ma famille et mes proches pour leurs encouragements.

Résumé

Le tatouage invisible d'images d'identité imprimées sur un support en plastique est un problème difficile qui intéresse le monde industriel. Dans cette étude, nous avons développé un algorithme de tatouage robuste aux diverses attaques présentes dans ce cas. Ces attaques sont liées aux processus d'impression/numérisation sur le support plastique ainsi qu'aux dégradations qu'une carte plastique peut rencontrer le long de sa durée de vie. La méthode de tatouage opère dans le domaine de Fourier car cette transformée présente des propriétés d'invariances aux attaques géométriques globales. Une méthode préventive consiste en un prétraitement de l'image originale avant le processus d'insertion qui réduit la variance du vecteur support de la marque. Une méthode corrective comporte deux contre-attaques corrigeant le flou et les variations colorimétriques. Pour une probabilité de fausse alarme de 10^{-4}, nous avons obtenu une amélioration moyenne de 22% par rapport à la méthode de référence lorsque seule la méthode préventive est utilisée. La combinaison de la méthode préventive avec la méthode corrective correspond à un taux de détection supérieur à 99%. L'algorithme de détection prends moins de 1 seconde pour à une image de 512×512 pixels avec un ordinateur classique ce qui est compatible avec l'application industrielle visée.

Résumé en anglais

Invisible watermarking for ID images printed on plastic card support is a challenging problem that interests the industrial world. In this study, we developed a watermarking algorithm robust to various attacks present in this case. These attacks are mainly related to the print/scan process on the plastic support and the degradations that an ID card can encounter along its lifetime. The watermarking scheme operates in the Fourier domain as this transform has invariance properties against global geometrical transformations. A preventive method consists of pre-processing the host image before the embedding process that reduces the variance of the embeddable vector. A curative method comprises two counterattacks dealing with blurring and color variations. For a false alarm probability of 10^{-4}, we obtained an average improvement of 22% over the reference method when only preventative method is used. The combination of the preventive and curative methods leads to a detection rate greater than 99%. The detection algorithm takes less than 1 second for a 512×512 image with a conventional computer, which is compatible with the industrial application in question.

Table des matières

Table des figures

Liste des tableaux

Glossaire

A/N : Analogique/Numérique

AWGN: Additive white Gaussian noise (bruit blanc gaussien additif)

CCD : Charge-Coupled Device (dispositif à couplage de charge)

CD : Compact Disc (Disque compact)

CMJ : Cyan Magenta Jaune

DCT : Discrete cosine transform (Transformée en cosinus discrète)

DFT : Discrete Fourier transform (Transformation de Fourier discrète)

Dpi : Dots per Inch (points par pouce ou ppp)

DWT : Discrete wavelet transforms (Transformée en ondelettes discrète)

EQM : Erreur quadratique moyenne

FFT : Fast Fourier Transform (Transformation de Fourier rapide)

FMT : Fourier Mellin transform (Transformation de Fourier-Mellin)

GGD : Generalized Gaussian Distribution **(**Distribution Gaussienne Généralisée)

HVS : Human visual System (Systéme visuel humain)

JPEG : Joint Photographic Experts Group

JND : Just Noticeable Distortion

LPM : Log polar mapping

LUT : Look up table (Table de correspondance entre des valeurs d'entrée et de sortie)

MP3 : MPEG-1/2 Audio Layer 3

MPEG : Moving Picture Experts Group

N/A : Numérique/Analogique

PDF : Probability Density Function (Densité de Probabilité)

PSNR : Peak Signal to Noise Ratio (Mesure objective de la qualité visuelle basée sur l'erreur quadratique moyenne normalisée)

QIM : Quantization index modulation

RVB : Rouge Vert Bleu

SSIM : Structural Similarity (une mesure de similarité entre deux images numériques)

USB : Unviersal Serial Bus (Bus unviersel en série)

UV : Ultraviolet

Introduction générale

Avec le développement des technologies de l'information et de la communication (TIC), l'utilisation des documents numériques est en augmentation constante. Malgré cette croissance, un grand nombre de documents officiels utilisent encore une version imprimée. Ces documents, tels que par exemple les cartes d'accès, les cartes d'identité, les passeports et les permis de conduire, contiennent des informations textuelles, une photo du propriétaire légitime, et quelquefois des caractéristiques biométriques du propriétaire. Ces données sont imprimées sur le support du document pour former une interface pratique pour la lecture humaine. La décroissance des prix des technologies d'imagerie numérique (logiciels, imprimantes et appareils photo), rend la menace de la contrefaçon numérique et la falsification des documents de plus en plus facile. Avec une connaissance limitée de la technologie, un contrefacteur peut remplacer une photo ou modifier les informations sur un document d'identité dans la mesure où il est très difficile de la différencier du document légal.

Les documents d'identités peuvent être sécurisés avec un certain nombre de techniques [Picard *et al.* 2004, Schimke *et al.* 2005, Ambadiyil *et al.* 2015]. Certaines techniques impliquent l'ajout d'un dispositif de sécurité physique sur le corps du document. Par exemple, l'ajout d'un hologramme, ou l'utilisation de l'impression à l'aide d'encre à variabilité optique, d'encre fluorescente invisible ou sous rayonnement UV nécessitent un traitement supplémentaire après l'impression sur le document d'identité. Ces techniques exigent des équipements spéciaux et souvent coûteux et ne peuvent être utilisés que pour des applications à grande échelle ou dans un environnement de haute sécurité qui justifierait les coûts. Parmi toutes les solutions innovantes disponibles pour augmenter la sécurité, celle consistant à insérer des données cachées dans la photographie d'identité imprimée, appelée tatouage d'image, semble être l'une des solutions les plus intéressantes en raison de son invisibilité, de sa simplicité et de sa robustesse.

Le tatouage est considéré comme une discipline relativement jeune, au même titre que la stéganographie. La stéganographie consiste à dissimuler un message à transmettre de façon confidentielle au sein d'un ensemble de données. Le tatouage diffère de la stéganographie principalement dans son but mais s'appuie sur des techniques similaires. Plutôt que d'échanger des messages avec des correspondants pour la sténographie, le tatouage sert à sécuriser un media comme un son, une image ou une vidéo.

Au cours des 20 dernières années, le tatouage numérique a changé si bien qu'aujourd'hui c'est une discipline majeure dans la communauté scientifique des TIC. Les techniques de tatouage numériques ont évolué depuis les méthodes basiques (dites de première génération dans les années 1990-2000) jusqu'à des méthodes très sophistiquées visant à relever les verrous scientifiques et technologiques

identifiés dans les applications des premières. De nombreux industriels ont vu dans cette nouvelle branche une solution innovante pour sécuriser les documents numériques.

Les techniques de tatouage numérique d'images permet d'incorporer une signature (appelée aussi marque) imperceptible à l'œil nu. Ces informations pourront être vérifiées par la suite à tout moment en utilisant la marque. Dans le cas d'un document d'identité, les informations à insérer dans la photographie peuvent concerner la validité du document, les autorisations attachées au document, une indication de l'identité du propriétaire du document, ou plus simplement attester de l'authenticité du document. Le challenge est de pouvoir maîtriser les deux contraintes d'imperceptibilité et de robustesse dans un contexte applicatif spécifique.

Approche suivie dans cette thèse

Un système d'authentification de documents d'identité basé sur le tatouage numérique a été présenté par Ros *et al.* pour une application dans le domaine des cartes à puce [Ros *et al.* 2006]. La détection de la marque est dite aveugle, c'est-à-dire que l'on dispose seulement de l'image scannée et de la marque, mais pas de l'image originale. Il est ainsi possible de s'assurer que la photo imprimée sur le support est valide, et donc que le document est authentique. Ces travaux ont été réalisés au sein de la société Gemalto en collaboration avec l'Université d'Orléans.

Cette thèse s'inscrit dans la continuité de ces travaux.

Dans ce contexte applicatif, le tatouage doit satisfaire à un ensemble de contraintes spécifiques :

Imperceptibilité : La première contrainte imposée au système de tatouage pour les cartes est l'imperceptibilité de la marque insérée dans l'image. Le tatouage doit être invisible lorsque les images d'identité sont imprimées sur les supports des cartes. La mesure de la qualité visuelle des images tatouées est basée soit sur des critères subjectifs tel que le MOS (Mean Opinion Score) [Moorthy *et al.* 2010] ou des critères objectifs pour mesurer la différence entre l'image originale et l'image tatouée tel que par exemple le PSNR (Peak Signal to Noise Ratio). Dans cette application nous utilisons des métriques objectives (le PSNR) pour mesurer la qualité visuelle des images tatouées car les mesures subjectives sont difficiles à mettre en place en pratique.

Robustesse : Les contraintes de robustesse pour ce genre de support sont nombreuses et la marque doit donc résister à un grand nombre d'attaques volontaires (piratage) ou involontaire (usure de la carte). Les attaques à prendre en compte pour l'application visée sont :

- L'attaque de type impression / numérisation (ou Print/Scan) : Il s'agit de l'attaque principale à laquelle la méthode doit résister. Pas ou peu adaptée aux techniques de première génération, cette attaque a amené la communauté scientifique à travailler sur les techniques de deuxième génération dans les années 2000. Elle continue à être étudiée aujourd'hui. L'image est imprimée sur un support physique puis scannée avec un scanner (ou une

caméra). Il y a donc une forte attaque de l'image du fait de la conversion numérique / analogique suivie d'une conversion analogique / numérique, des transformations affines (rotation, changement d'échelle, translation,…) et du bruit additif.

- L'attaque de vieillissement : Cette attaque est une attaque de vieillissement naturel qui apparaît avec le temps et l'utilisation du document d'identité.

Il est donc nécessaire de réaliser un système de tatouage robuste, à l'ensemble de ces attaques, voire de leurs combinaisons et simple à l'utilisation. Le coût de calcul est un paramètre important qui sera aussi évalué.

Choix de la méthode de tatouage

La littérature du tatouage d'image est abondante car liée à la demande pressante d'outils sécuritaires. Les techniques de tatouage d'images numériques dans la littérature sont généralement développées pour faire face à une ou plusieurs attaques en particulier. Résister à une combinaison d'attaques reste un problème difficile. Il est impossible de développer un algorithme généraliste pour l'ensemble des attaques possibles.

La stratégie est de comprendre l'effet des attaques combinées afin de les contre attaquer tout en préservant l'imperceptibilité et la robustesse.

Le critère fondamental qui a été retenu pour la sélection de l'algorithme de tatouage est la robustesse face à l'attaque de type impression / numérisation. En effet, les images seront imprimées avec leur marque sur un support en plastique de type badge. La vérification de l'authenticité de la carte se fera à l'aide d'un appareil de numérisation (scanner).

L'algorithme final devra par conséquent être robuste aux attaques impression / numérisation (la marque devra être détectée malgré ces fortes attaques), et fonctionner en aveugle (l'image source n'est pas disponible lors de la détection de la marque, seule l'image scannée et la marque sont disponibles). Dans ce cadre-là, le tatouage dans le domaine de Fourier est le plus adapté. Il consiste à insérer la marque le long d'un cercle de rayon prédéfini. Ainsi, cette méthode est insensible aux attaques de rotation et de translation grâce à l'invariance du module de la transformée de Fourier pour la translation et du fait qu'une rotation spatiale induit une même rotation fréquentielle du module.

Contributions de la thèse

Cette thèse aborde le problème du tatouage robuste d'image imprimées sur des documents type carte plastique, puis scannées en utilisant un scanner. L'insertion de la marque dans les images imprimées avec une détection automatique constitue un problème difficile en raison des distorsions introduites

pendant l'impression suivie d'une numérisation du document, ainsi qu'à l'utilisation du document pendant de nombreuses années.

L'objectif de cette thèse est la mise en œuvre d'une stratégie de tatouage de Fourier robuste aux attaques d'impression / numérisation et aux attaques liées au vieillissement dans un contexte d'application industrielle.

La stratégie proposée se décompose en deux étapes :

- Une étape préventive consiste à prétraiter l'image originale avant la phase d'insertion de la marque. La variance du vecteur support de la marque est artificiellement réduite soit par un filtre passe bas, soit par sélection des coefficients. L'idée inhérente dans cette étape est d'accroitre la robustesse sans altérer l'imperceptibilité.
- Une étape corrective consiste à corriger les distorsions liées aux attaques d'impression / numérisation. Cette phase est composée de deux corrections. La première est une correction du flou en utilisant un filtre de Wiener adapté à la chaine d'impression / numérisation. La deuxième est une correction colorimétrique.

Cette nouvelle méthode sera testée sur des images d'identité imprimées sur un support plastique puis ensuite scannées. Elle sera comparée à la méthode de base qui fait référence. Finalement une série d'attaques de durabilité des cartes d'identité a été développée. Ces attaques ont pour objectif de tester la robustesse des méthodes de tatouage contre les distorsions produites lors l'utilisation de documents officiels.

Organisation de la thèse

Cette thèse est organisée en quatre chapitres.

Dans le premier chapitre nous présenterons un état de l'art des méthodes du tatouage pour des images numériques. En premier lieu, nous présenterons le tatouage numérique et ses différentes propriétés. Puis nous évoquerons le schéma général du tatouage numérique, en décrivant notamment les différentes étapes d'insertion et de détection de la marque. Finalement, nous proposerons une classification des méthodes de tatouage selon le domaine d'insertion en se concentrant sur les méthodes basées Fourier.

Le deuxième chapitre décrit le processus d'impression / numérisation qui concerne les documents d'identité. Pour une meilleure compréhension des phénomènes physiques qui se produisent dans ce processus complexe, nous caractériserons les dispositifs d'impression et de numérisation. Puis nous identifierons les effets de l'impression et de la numérisation sur une image. Finalement, nous présenterons les modèles d'impression / numérisation et les contre-attaques proposées dans la littérature.

Le troisième chapitre est consacré en premier lieu à la description d'une méthode de tatouage dans le domaine de Fourier avec une détection aveugle pour des images d'identité imprimées sur des supports en plastique. Dans un deuxième temps, nous proposerons une amélioration de l'algorithme de tatouage décrit précédemment. Cette nouvelle amélioration est basée sur un prétraitement de l'image avant l'insertion de la marque. Ce prétraitement consiste à diminuer la variance du vecteur qui supporte la marque. La réduction de la variance peut être réalisée soit par une modification directe ou par une sélection des coefficients dans lesquels la marque sera insérée. Nous présenterons les résultats face aux différentes attaques.

Toujours dans le but d'améliorer les performances de notre algorithme, nous décrirons dans le quatrième chapitre une technique corrective qui permet de replacer l'image imprimée puis scannée dans un état favorable à la détection de la marque. Cette technique corrective consiste en une correction de flou suivie d'une correction colorimétrique. Ainsi, nous présenterons la performance de la méthode contre des attaques de vieillissement des documents d'identité.

En conclusion, nous récapitulerons les principales contributions de ce travail de thèse avant d'exposer les perspectives envisagées.

Cette thèse s'est effectuée dans le cadre d'une cotutelle entre l'université d'Orléans et l'université d'Agadir. Elle a bénéficié d'un support Egide (projet Toubkal MA/12/279) ainsi que du support de la société Gemalto, leader mondial de la sécurité numérique, (Contrat SUREO 13090).

Chapitre I :

1 Etat de l'art sur le tatouage numérique

1.1 Introduction

Au cours de ces dernières années, le tatouage numérique est devenu une discipline majeure dans la communauté du traitement de l'information. Les techniques de tatouage numériques ont évolué jusqu'à proposer des méthodes très sophistiquées. De nombreux secteurs industriels ont vu dans cette nouvelle branche une solution innovante pour sécuriser les documents numériques.

Ce chapitre présente un état de l'art sur les méthodes de tatouage numérique. Nous commençons par introduire l'aspect général du tatouage numérique puis nous donnons ses différentes propriétés. Ensuite nous présentons le schéma général du tatouage numérique, en décrivant notamment les différentes étapes d'insertion et de détection de la marque. Après ces généralités, une classification des méthodes de tatouage selon les domaines de l'insertion sera proposée. Nous présentons ensuite un bref descriptif sur les méthodes de tatouage robuste aux transformations géométriques. Nous exposerons ensuite les raisons qui ont motivé notre choix des méthodes de tatouage basées sur la transformée de Fourier ainsi que quelques méthodes basées sur cette transformation seront finalement présentées.

1.2 Aspect général du tatouage

1.2.1 Contraintes générales

Le tatouage numérique consiste à insérer une marque imperceptible à l'œil dans un document. Cette marque est une séquence aléatoire de bits, un logo binaire, ou un message, en fonction de l'application visée. La détection de la marque doit être robuste, même si le document tatoué est attaqué. Pour qu'une méthode de tatouage soit facilement intégrée dans des applications industrielles, l'insertion/détection de la marque doit être réalisée dans un temps de calcul raisonnable. Dans la suite nous présentons les propriétés principales du tatouage numérique.

1.2.1.1 Imperceptibilité

La notion d'imperceptibilité est liée à la perception visuelle ou auditive des distorsions résultant à l'insertion de la marque dans un document. Le tatouage doit être invisible dans le cas des images pour un observateur humain. De plus, la marque insérée ne devrait pas affecter la qualité du

document. L'évaluation de la qualité visuelle ou auditive des documents après le tatouage devient un critère important pour la validation des algorithmes de tatouage. En ce qui concerne les images, une telle évaluation nécessite une analyse du système visuel humain (HVS). Plusieurs mesures objectives ont été proposées dans la littérature pour mesurer la qualité visuelle d'un document tatoué. Une description détaillée des mesures objectives peut être trouvée dans [Nguyen 2011].

1.2.1.2 La capacité

La capacité d'une méthode du tatouage représente la quantité maximale d'information que l'on peut insérer dans un document sans dégrader sa qualité visuelle au auditive. Cette quantité d'information dépend essentiellement du type de l'application visée. L'information est quantifiée généralement en bits. Dans les applications dites tatouage zéro bit (zero-bit watermarking) la marque insérée dans un document ne contient aucun message caché [Gao *et al.* 2011]. Le détecteur vérifie seulement la présence de la marque dans les documents reçus.

1.2.1.3 La robustesse

La robustesse représente la capacité du tatouage à résister aux dégradations du document tatoué. Ces modifications définissent l'ensemble des attaques qu'elles soient intentionnelles ou non intentionnelles. Le premier type d'attaques vise à supprimer la marque insérée dans un document, tandis que le deuxième type d'attaque n'a pas pour objectif de supprimer la marque mais plutôt l'altérer. Selon le critère de robustesse on distingue trois types du tatouage numérique :

- **Tatouage robuste :** Un système de tatouage est dit robuste, si la détection de la marque est effective même si le document tatoué a été altéré ou attaqué. Un système de tatouage robuste doit résister aux opérations licites effectuées sur le document numérique (compression, conversion analogique-numérique, filtrage, etc.) et celles illicites (attaques malveillantes des pirates).
- **Tatouage fragile :** Dans le tatouage fragile, la marque est très sensible aux modifications du document tatoué. Cette technique sert à prouver l'authenticité et l'intégrité d'un document tatoué. Une technique de tatouage fragile devrait détecter (avec une forte probabilité) toute altération du document tatoué. Une comparaison de la marque extraite et de la marque originale est effectuée afin d'identifier si le document est manipulé ou pas.
- **Tatouage semi-fragile :** Il combine les caractéristiques du tatouage robuste et fragile pour avoir une situation intermédiaire, dans laquelle la marque est robuste pour un ensemble défini de dégradations, et fragile à d'autres.

Ces trois contraintes (imperceptibilité, capacité et robustesse) sont contradictoires (voir la figure 1-1). Si l'on augmente par exemple la force du marquage dans le but de rendre le tatouage plus robuste,

cela aura en contrepartie pour effet de rendre le tatouage plus visible. De la même manière, si l'on augmente la quantité d'information à insérer, on aura en contrepartie un tatouage visible et moins robuste. Donc il faut respecter un compromis entre ces trois critères pour construire une méthode de tatouage.

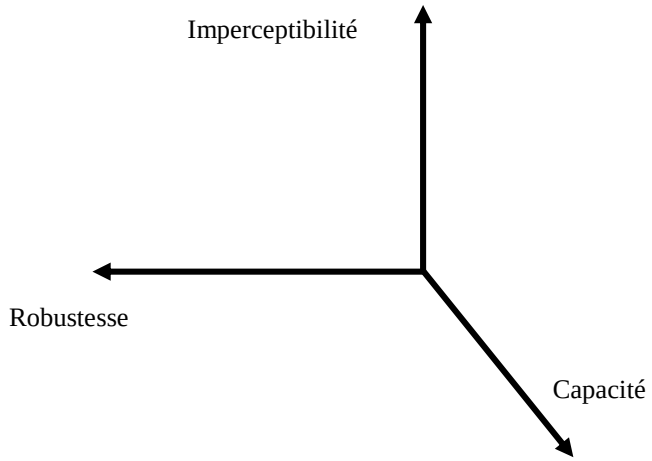


Figure 1-1- Contraintes du tatouage numérique.

Il existe dans la littérature d'autres propriétés liées aux algorithmes du tatouage qu'il faut prend en compte comme par exemple la complexité.

1.2.1.4 La complexité

Le coût de calcul est un élément très important pour les applications du tatouage dans le domaine industriel. En général, le temps calcul doit être inférieur à une certaine valeur. Par exemple dans le contrôle d'accès la complexité de l'insertion est moins importante que la complexité de la détection. Le temps de calcul de la détection doit être de l'ordre d'une à deux secondes.

1.2.2 Domaines d'applications

Le tatouage numérique est utilisé dans une variété d'applications où il est nécessaire d'associer certaines informations à un document numérique. Le tatouage inséré dans un document est essentiellement caractérisé par l'invisibilité, l'inséparabilité du document, et enfin il subit les mêmes transformations que le document. Ces trois aspects sont les principales raisons qui permettent l'intégration du tatouage dans diverses applications. D'autre part, les objectifs contradictoires rendent impossible la création d'un algorithme universel adaptable à toutes les applications. Jusqu'à ce jour il n'existe pas une méthode de tatouage qui soit à la fois imperceptible, robuste et qui puisse insérer une grande quantité d'information. Il est nécessaire de prendre en compte les besoins de

l'application visée lors de la conception d'un algorithme de tatouage numérique. Dans la suite, nous citons quelques champs d'application du tatouage numérique.

1.2.2.1 La protection des droits d'auteurs

La protection des droits d'auteurs est la première application du tatouage numérique. Ce dernier, offre une alternative intéressante à la cryptographie car il fournit une protection du document même lorsqu'il est diffusé. Dans ce cas, une marque contenant des informations du copyright est insérée dans un document de sorte qu'elle identifie le propriétaire du document [Khan *et al.* 2014]. Par exemple, une marque visible sous la forme « © Auteur Date » peut être utilisée dans ce but. Cette technique a montré quelques limites. Dans le cas des images, cette marque visible est souvent insérée sur l'un des coins de l'image, ce qui peut cacher une partie de l'image. Cette marque visible peut facilement être retirée. D'où l'utilité du tatouage numérique qui permet l'insertion d'une marque invisible à l'œil humain mais détectable avec un logiciel dédié [Surekha *et al.* 2013]. Dans ce cas, la marque insérée dans le document à protéger doit être robuste car elle permet d'attester de la propriété d'un document [Patrick Bas 2000].

1.2.2.2 La protection contre la copie

C'est une application très importante dont le but est de contrôler ou d'empêcher la copie illégale d'un document protégé [Shukla *et al.* 2012]. Cette application est particulièrement intéressante dans la protection des DVD. En fait, il est très facile de faire plusieurs copies d'un contenu multimédia (image, films,...), et de les distribuer sur Internet. Pour éviter cela, une marque contenant des informations concernant la restriction de la copie est incorporée dans la vidéo originale [Ingemar J. Cox *et al.* 2001]. Dans ce cas, la marque indiquera si la vidéo peut être lue et/ou recopiée. Cependant, ce procédé n'est bien entendu fiable que si tous les lecteurs DVD sont également équipés par un détecteur de la marque.

1.2.2.3 Le contrôle de diffusion

Les annonceurs paient un prix élevé pour présenter leurs produits lors d'une parenthèse publicitaire pendant des manifestations sportives importantes ou des films. Par conséquent, ils veulent s'assurer que leurs annonces ont été effectivement diffusées. Le tatouage numérique sert à prouver que le contenu a été totalement présenté à un moment précis [Liu *et al.* 2013, Gupta *et al.* 2014].

1.2.2.4 L'authentification

La marque est insérée dans le document original, et elle est utilisée par la suite pour vérifier si le document a été modifié ou non. Si on prend comme exemple une image, il serait facile de supprimer une partie de l'image. Ceci peut changer la sémantique de l'image originale. Ainsi, pour éviter ce

traitement illicite, une marque est insérée dans le document de telle sorte que si on élimine une partie de l'image, une partie de la marque sera aussi éliminée et cela va empêcher sa détection correcte. Si la marque n'est pas détectée d'une manière correcte, on pourra conclure que le document a été modifié [Iliyasu *et al.* 2012].

1.2.2.5 L'ajout d'informations publicitaires

Une image peut contenir une information complémentaire à diffuser vers un utilisateur. Cette information représente, par exemple, la référence d'un produit mis en vente sur internet. Un exemple typique de cette application est le concept d'images intelligentes (Smart Image) développé par la société Digimarc, une société spécialisée dans le domaine du tatouage d'image numérique. Selon Alattar [Alattar 2000], le concept de base des images intelligentes consiste à insérer une marque dans une image ou une vidéo, afin de jouer le rôle d'un pointeur vers un site web par exemple. Cette marque permet de relier l'utilisateur à une information annexe.

1.3 Schéma général du tatouage numérique

Le tatouage numérique, consiste à insérer une marque généralement imperceptible dans un document numérique (image, son, vidéo…). La modification s'effectue dans les composantes perceptibles (dans les pixels d'une image par exemple). Un schéma général du tatouage numérique pour une image est présenté dans la figure 1-2.

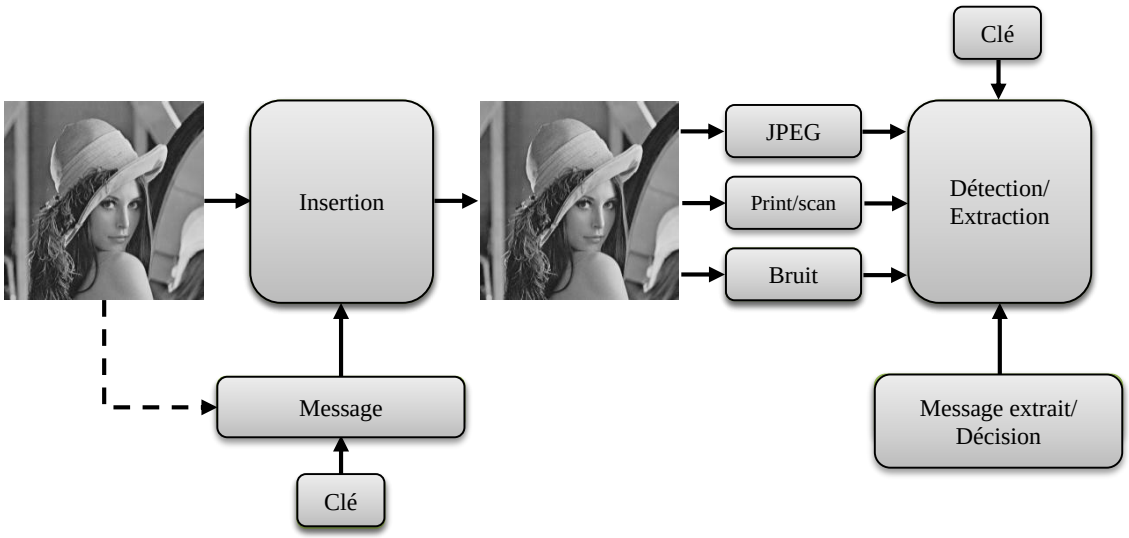


Figure 1-2- Schéma général du tatouage numérique.

Le tatouage numérique est composé de trois phases principales. La phase d'insertion, la transmission (ou l'attaque) et la phase de détection (ou l'extraction). Au cours de la phase d'insertion, la marque est insérée dans un document numérique. Le document numérique original est légèrement modifié après cette phase, le document modifié est appelé document tatoué. Dans la phase d'extraction, la marque est extraite à partir du document tatoué. La marque extraite est comparée par la suite avec la marque originale : si les deux marques sont identiques alors le document est authentifié, si non le document est falsifié. Au cours de la transmission du document tatoué sur un réseau public par exemple, un pirate peut altérer le document. Si cette altération est suffisamment importante, elle conduit à de mauvaises décisions.

1.3.1 Phase d'insertion

Dans cette phase l'image originale I_0 est combinée avec le message qui est une collection de bits représentant les données à ajouter. Cette opération a pour objectif de créer une image tatouée I_w. Les images tatouées sont perceptuellement identiques aux images originales. La différence entre I_w et I_0 est appelée distorsion de l'insertion [I. J. Cox *et al.* 1997].

Le message m est encodé en utilisant une clé secrète K. Pour faire en sorte que les distorsions de l'insertion soient suffisamment faibles et imperceptibles, la marque est ensuite modulée et/ou mise à l'échelle. Il existe deux manières pour insérer une marque W dans une image I_0, une manière substitutive et une manière additive.

1.3.1.1 Méthodes substitutives

Dans les méthodes substitutives, la marque à insérer est substituée à des composantes de l'image originale, ce qui correspond principalement à deux comportements : le premier est un tatouage quantitatif appelé aussi tatouage substitutif avec dictionnaire, le second est un tatouage substitutif avec contraintes. Il consiste à imposer un ensemble de contraintes aux données marquées [El-Hajji 2012]. Plusieurs techniques substitutives ont été proposées dans la littérature. La première méthode consiste à remplacer les bits les moins significatifs ou les bits de poids faibles des pixels d'une image par les bits de la marque. Cette méthode a été améliorée dans [Dharwadkar *et al.* 2009] pour les images couleurs. Une technique très utilisée dans le tatouage des images est appelée la quantification par la modulation d'index (QIM) proposée dans [Chen *et al.* 2001, Furon *et al.* 2013]. Le principe de cette technique consiste à quantifier l'image en utilisant un ensemble de quantificateurs indexés par la marque à insérer. Ainsi, chaque élément de la marque est attaché à un quantificateur différent, et le tatouage s'effectue par quantification de l'image avec le quantificateur correspondant à la marque.

1.3.1.2 Méthodes additives

Le principe des méthodes dites additives consiste à ajouter la marque aux composantes du document en utilisant l'une des équations suivantes [I. J. Cox *et al.* 1997] :

$$\begin{cases} I_w = I_0 + W \\ I_w = I_0 \times (1+W) \\ I_w = I_0 \times e^W \end{cases} \tag{1-1}$$

En pratique, la marque W est ajoutée aux certains composantes caractéristiques de l'image I_0. Cette opération peut se faire à partir de l'image elle-même ou à partir d'une transformation fréquentielle (DCT, DFT, DWT,…) [Mairgiotis *et al.* 2013, Zarmehi *et al.* 2013]. La figure 1-3 montre le principe du tatouage additif.

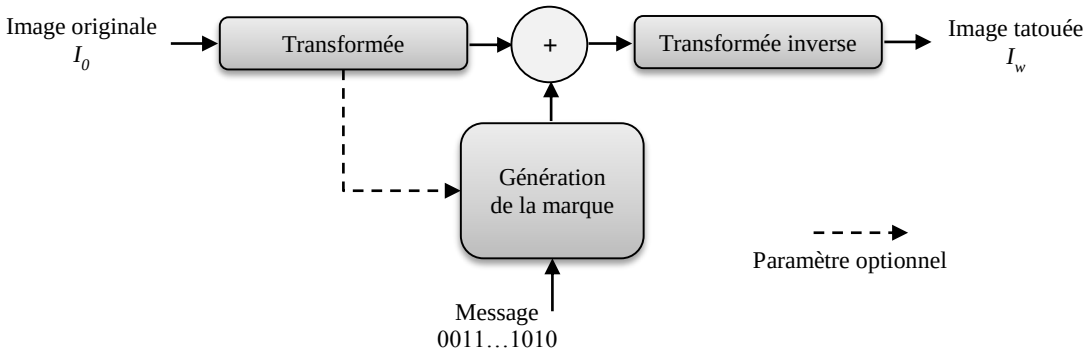


Figure 1-3- L'insertion de la marque par la méthode additive.

1.3.2 Phase de détection

L'image tatouée I_w peut être soumise à différentes attaques donnant une image tatouée corrompue I^*_w. Cette corruption peut être causée par différentes distorsions dues par exemple à des opérations usuelles (compression, conversion N/A et A/N,…) ou bien des distorsions introduites par différentes attaques malveillantes ou non malveillantes.

Dans la phase de la détection, le décodage de la marque doit être effectué à partir de l'image tatouée corrompue I^*_w. Il existe deux modes de décodage de la marque, selon les différentes techniques du tatouage, l'image originale peut être nécessaire ou pas lors la détection de la marque. Le choix du mode dépendra de l'application envisagée et des protocoles utilisés. On distingue :

- **Tatouage aveugle :** Une technique de tatouage est dite aveugle, si l'extraction ou la détection de la marque s'effectue avec l'image à analyser et la marque. Le tatouage aveugle est le plus populaire et largement utilisé. L'information cachée doit être détectée directement à partir de l'image à analyser sans avoir recours à l'image originale.
- **Tatouage non-aveugle :** La technique du tatouage qui nécessite l'image originale pour extraire la marque est dite tatouage non-aveugle. Elle est plus robuste que le tatouage aveugle mais elle est moins utilisée car elle requiert l'image originale.

La figure 1-4 montre le principe du décodage de la marque pour un tatouage additif. Les composantes caractéristiques marquées sont extraites à partir de l'image tatouée et attaquée. La clé K est utilisée pour générer la marque de référence. Puis le décodage de la marque est effectué soit par estimation soit par corrélation des composantes afin de produire une mesure indiquant la probabilité de présence de la marque dans I^*_w.

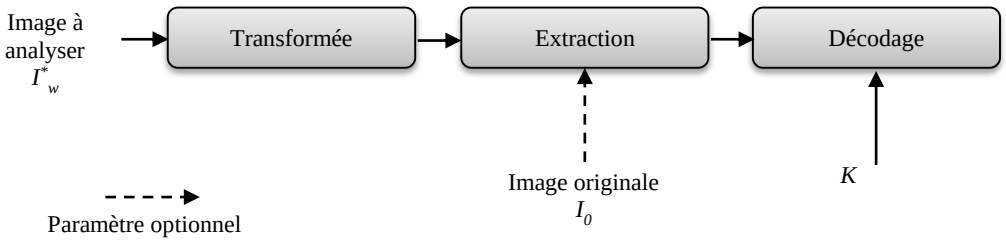


Figure 1-4- Décodage de la marque pour un tatouage additif.

1.3.3 La phase de transmission ou d'attaques

Les attaques dans le tatouage numérique sont définies comme l'ensemble des opérations qui peuvent rendre la marque indétectable/indécodable. Il existe deux grandes catégories d'attaques :

1.3.3.1 Attaques bienveillantes

Tous les traitements ou les manipulations effectuées par un utilisateur non malveillant sont classés comme étant des attaques bienveillantes. L'objectif de ces traitements est de modifier ou masquer certaines caractéristiques de l'image mais pas de supprimer la marque. Il est impossible de faire une étude exhaustive de ces traitements car ils sont trop nombreux, mais nous nous contenterons de présenter les plus couramment rencontrés.

- **La compression :** Les algorithmes de compression sont particulièrement dangereux pour les techniques de tatouage. Toute technique de tatouage robuste doit pouvoir résister jusqu'à un

certain niveau de compression. La compression a pour objectif de réduire autant que possible la quantité de données d'un document. Ce processus consiste à éliminer les composantes perceptuellement moins significatives en préservant les composantes importantes du document. JPEG et JPEG2000 sont considérés comme les algorithmes de compression d'image les plus utilisés actuellement. Pour pallier ce problème de compression, le tatouage est effectué dans des zones significatives de l'image [Qiao *et al.* 2007]. Ces zones sont généralement choisies dans les domaines de transformations utilisées par les algorithmes de compression, la DCT dans le JPEG standard ou la DWT dans la norme JPEG2000.

- **Le filtrage :** Le filtrage est un outil de base de traitement d'image, il est utilisé généralement pour la suppression du bruit. Ce type de filtrage a généralement pour effet d'atténuer les composantes hautes fréquences de l'image et par conséquent dégrader les composantes de la marque insérées dans ces fréquences.
- **Les transformations valumétriques :** Ces transformations fréquentes en traitement d'images incluent par exemple l'étalement et l'égalisation d'histogramme, transformation Gamma, etc... Le principe de ces transformations consiste à changer la valeur de la luminance de chaque pixel de l'image par une fonction linéaire ou non-linéaire, afin d'améliorer l'aspect visuel de l'image.
- **Le bruit :** L'ajout involontaire d'un bruit avec des proportions importantes peut avoir un effet de masquage de la marque et par conséquent gêner son extraction/détection. Le bruit peut s'introduire dans un canal de transmission bruité, par exemple une impression suivie d'une numérisation.
- **Transformations géométriques :** Ce genre de transformations n'a pas pour effet d'éliminer la marque mais plutôt rend la marque indétectable même si elle reste encore dans l'image. Ces transformations provoquent une désynchronisation entre la marque insérée dans l'image et le décodeur. Dans la majorité des algorithmes du tatouage, le décodeur a besoin de connaître la position exacte de la marque contenue dans l'image. Il existe plusieurs transformations géométriques, on peut citer par exemple les transformations géométriques affines (translation, rotation et changement d'échelle), le recadrage ou 'cropping' en anglais, qui consiste à supprimer une partie de l'image et par conséquent une partie de la marque. Il existe aussi des transformations géométriques locales comme l'attaque StirMark (voir la figure 1-5). Cette attaque consiste à une succession de distorsions géométriques aléatoires appliquées localement à plusieurs endroits dans l'image [Kutter *et al.* 1999].

Figure 1-5- Illustration des déformations géométriques aléatoires engendrées par StirMark.

- **Conversions numérique-analogique-numérique :** la conversion numérique-analogique-numérique représente une attaque particulièrement sévère face à laquelle beaucoup de méthode de tatouage numérique se révèlent inefficaces. Par exemple une impression suivie d'une numérisation d'une image, l'enregistrement d'un film dans une salle de cinéma à l'aide d'une caméra ou l'enregistrement de la musique à partir d'un lecteur CD ou un radio.

1.3.3.2 Attaques malveillantes

Il s'agit de manipulations particulières dont le but est de détruire intentionnellement la marque ou d'empêcher son extraction/détection. Toutes les attaques présentées précédemment peuvent être utilisées dans ce but. Nous citons aussi l'attaque par sur-marquage ou le tatouage multiple. Cette attaque consiste à tatouer une image déjà tatouée, ce type d'attaques rentre dans la catégorie d'attaques d'ambiguïtés ou attaques de confusion [Loukhaoukha 2011].

1.3.4 Outils d'évaluation des méthodes de tatouage

Le tatouage numérique se caractérise essentiellement par trois contraintes contradictoires ; l'imperceptibilité, la capacité et la robustesse contre les différentes attaques ou manipulations. L'évaluation des algorithmes du tatouage numérique d'images n'est pas une tâche facile. En effet, aucun cahier des charges ne donne réellement des valeurs fixées pour la capacité, la qualité visuelle de l'image tatouée ou les différentes attaques auxquelles l'algorithme du tatouage doit être robuste.

1.3.4.1 Evaluation de la qualité visuelle d'une image tatouée

Comme déjà mentionné la qualité d'une image tatouée est l'une des contraintes principales pour valider un algorithme du tatouage numérique. Plusieurs mesures de cette qualité ont été proposées

dans la littérature. Une description détaillée des mesures objectives peut être trouvée dans [Nguyen 2011]. Dans la suite, nous citons les métriques les plus utilisées dans le domaine du tatouage numérique.

A. Le PSNR

Le PSNR (Peak Signal to Noise Ratio) est la métrique la plus fréquemment utilisée dans la communauté du tatouage. Même si elle est critiquable, on la considère comme un bon indicateur pour fournir des scores quantitatifs dans l'ensemble de l'image tatouée. La valeur du PSNR est souvent donnée en décibels (dB), elle est calculée comme suit :

$$PSNR = 10 \times \log_{10}\left(\frac{d^2}{EQM}\right), \tag{1-2}$$

où d est la dynamique de l'image (la valeur maximum possible pour un pixel). Dans le cas standard d'une image dont les pixels sont codées sur 8 bits, d = 255. EQM représente l'erreur quadratique moyenne, il est défini pour deux images par l'équation suivante :

$$EQM = \frac{1}{M \cdot N}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\left\| I_0(m,n) - I_w(m,n)\right\|^2, \tag{1-3}$$

où I_0 et I_w sont respectivement l'image originale et l'image tatouée de dimension $M \times N$.

Une valeur supérieure à 40 dB du PSNR indique une faible dégradation invisible à l'œil, tandis qu'une valeur inférieure à 30 dB indique une forte dégradation [Cheddad *et al.* 2010]. Donc, si le PSNR est supérieur ou égal à 40 dB, nous considérons que le tatouage est invisible.

B. Le MSSIM

Contrairement au PSNR qui est une mesure basée sur la différence pixel à pixel entre deux images, la mesure SSIM évalue la similarité structurelle existante entre deux images. Cette mesure consiste à combiner trois paramètres ; la luminosité, le contraste et la comparaison de structure [Wang *et al.* 2004]. Le SSIM est calculé sur plusieurs fenêtres d'une image. La mesure entre deux fenêtres x et y est donnée par la formule suivante :

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \tag{1-4}$$

μ et σ^2 sont respectivement la moyenne et la variance de la fenêtre, c_1, c_2 deux variables destinées à stabiliser la division quand le dénominateur est très faible.

Pour l'évaluation de la qualité d'une image, la formule précédente est appliquée à la luminance sur *m* fenêtres de taille 8×8 des deux images. Finalement, la similarité entre l'image de référence et l'image tatouée est mesurée par la moyenne des SSIM calculé pour chaque fenêtre.

$$MSSIM(I_0, I_w) = \frac{1}{m}\sum_{i=1}^{m} SSIM(x_i, y_i)\,. \tag{1-5}$$

Derraz *et al.* [Derraz *et al.* 2004] considèrent que la compression des images médicales avec un *MSSIM* supérieur à 0.8 donne des images de qualité correcte pour l'aide au diagnostic.

1.3.4.2 Evaluation de la robustesse du tatouage ou « Benchmarking »

L'évaluation efficace de différentes méthodes de tatouages est une tâche difficile. Cette difficulté réside dans la nécessité d'une normalisation des attaques contre lesquelles les algorithmes doivent être testés. Plusieurs outils ont été proposés dans la littérature. Ces outils ou logiciels permettent de mettre en œuvre des manipulations spécifiques dont le but est de détruire la marque contenue dans une image ou d'empêcher sa détection. Il existe certains utilitaires opérant de nombreuses attaques, tels que StirMark benchmark développé par Kutter et Peticolas [Kutter *et al.* 1999], CheckMark benchmark proposé par Voloshynovskiy *et al.* [S. Voloshynovskiy *et al.* 2001], OptiMark benchmark réalisé par Nikolaidis *et al.* [N Nikolaidis *et al.* 2002]. StirMark est le plus utilisé et le plus éprouvé de tous.

1.4 Domaine d'insertion du tatouage

Selon le domaine d'insertion, les techniques du tatouage proposées dans la littérature peuvent être groupées en deux classes : celles qui opèrent dans le domaine spatial ou dans le domaine transformé. Cependant, il existe des techniques qui utilisent la combinaison de plusieurs domaines, appelées techniques hybrides [Agarwal *et al.* 2013]. Ces algorithmes sont peu rencontrés dans la littérature. Le choix du domaine influe directement sur la fiabilité de la technique en termes de robustesse et de capacité. C'est aussi un élément de contre-attaque. Ce choix dépend de l'application visée, vu que chaque domaine possède ses propres caractéristiques.

1.4.1 Domaine spatial

Dans les techniques basées sur domaine spatial comme domaine d'insertion, la marque est insérée par une modification directe des pixels. Ces pixels sont généralement sélectionnés par une clé secrète ou en se basant sur un modèle psycho-visuel [Sviatoslav Voloshynovskiy *et al.* 2000]. Les premières approches de tatouage numérique ont été conçues pour travailler dans ce domaine à cause de sa simplicité [N. Nikolaidis *et al.* 1998].

La première méthode de tatouage spatiale est proposée par Tanaka *et al.* [Tanaka *et al.* 1990]. Elle consiste à insérer chaque élément de la marque dans le bit le moins significatif de chaque pixel. Une autre méthode appelée algorithme « Patchwork » a été proposé par In-Kwon et Hyoung Joong [In-Kwon *et al.* 2003]. Cet algorithme opère aussi directement dans le domaine spatial, c'est-à-dire au niveau de la luminance des pixels. L'avantage principal de ce domaine est son faible coût de calcul, ce qui favorise son utilisation dans les applications du tatouage en temps réel [Emami *et al.* 2014]. Leur inconvénient est la sensibilité aux attaques géométriques, la compression avec perte et le filtrage. C'est la raison pour laquelle beaucoup de méthodes de tatouage utilisent l'insertion dans d'autres domaines basés sur des transformations.

1.4.2 Domaine transformé

Les méthodes du tatouage basées sur les transformations consiste à transformer le signal du domaine spatial/temporel vers un autre domaine (par exemple DCT, Fourier, ondelettes,…) [I. J. Cox *et al.* 1997], [Ros *et al.* 2006], [El Hajji *et al.* 2012]. Ensuite la marque est insérée dans certains coefficients dans ce domaine. Finalement la transformation inverse est effectuée pour revenir au domaine spatial/temporel. Les algorithmes de tatouage numérique conçus pour travailler dans un domaine transformé sont plus robustes et plus complexes mais largement utilisés. Différentes transformations sont utilisées dans le tatouage numérique, et plus particulièrement les transformations orthogonales qui offrent des propriétés très intéressantes pour le tatouage. En ce qui concerne les transformations fréquentielles (DFT, DCT,…) l'énergie du signal est concentrée dans les composantes basses fréquences. L'insertion d'une marque dans ces fréquences fournit une bonne robustesse, mais elle introduit des distorsions apparentes dans le domaine spatial/temporel. Par contre l'insertion dans les composantes hautes fréquences ne dégrade pas la qualité du signal, mais rend la marque fragile aux attaques telles que le filtrage passe-bas et la compression. Par conséquent, la bande des moyennes fréquences est généralement la plus appropriée pour le tatouage, car elle répond à l'exigence du compromis entre la robustesse et l'invisibilité.

1.4.2.2 La transformée en ondelettes discrète (DWT)

La transformée en ondelettes est née de la convergence des travaux théoriques très anciens, notamment les travaux de Haar (1910), de Littlewood et Paley (1930), de Zygmund (1930), de Gabor (1940), puis vers 1960 de Calderon, et des idées récentes pour le traitement numérique de certains signaux par Morlet (le premier à avoir proposé le nom d'ondelettes, 1982), ou pour le développement d'outils mathématiques utilisés en physique théorique par Grossmann (1983).

La transformée en ondelettes discrète est réalisée à l'aide des bancs des filtres par convolution ou avec des algorithmes rapides basés sur le schéma du « lifting scheme » [Sweldens 1998]. Cette transformation décompose une image en une sous-bande basses fréquences LL et trois sous-bandes

hautes fréquences: LH, HH et HL, correspondant, respectivement aux orientations spatiales verticales, diagonales et horizontales, comme illustré la figure 1-6.

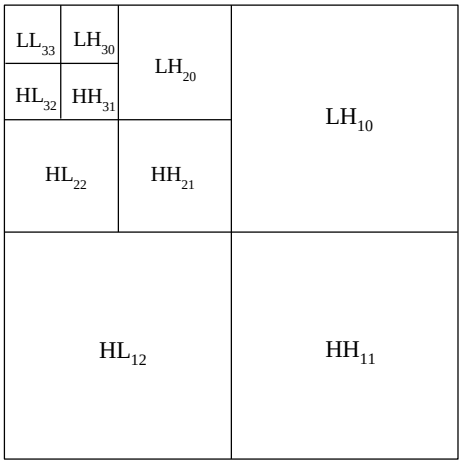


Figure 1-6- Exemple de décomposition d'une image en ondelettes à 3 niveaux.

Comme déjà mentionné, la transformée en ondelettes permet de décomposer l'image en sous bandes fréquentielles. Cette décomposition est souvent proche d'une décomposition en canaux perceptifs ce qui facilite l'utilisation d'un modèle psycho-visuel [Mallat 1987]. D'où l'intérêt de l'utilisation de cette transformation dans le tatouage des images. El Hajji *et al.* [El Hajji *et al.* 2012] ont présenté une méthode de tatouage basée sur la transformée d'ondelette dans la représentions à échelles mixée (voir la figure 1-7). La représentation à échelles mixées des coefficients DWT d'une image permet de distinguer des régions très particulières ; les contours de l'image et les zones texturées [Douzi *et al.* 2001]. Ces régions correspondent aux zones où on a une grande densité de coefficients d'ondelettes. La marque est insérée dans les blocks à grande densité de taille 8×8. Cet algorithme montre des bons résultats au niveau de l'invisibilité de la marque ainsi qu'une bonne robustesse contre la compression et le filtrage.

Figure 1-7- La représentation à échelles mixées de l'image Lena.

Le principal inconvenant de la transformée en ondelette est la sensibilité aux transformations géométriques (attaques de désynchronisation) [Xueyi *et al.* 2014].

1.4.2.2 La transformée en cosinus discrète (DCT)

Depuis quelques années, la transformée en cosinus discrète (DCT) est la représentation de choix pour la compression (MP3, JPEG et MPEG), grâce à son compromis intéressant entre son pouvoir de décorrélation proche de l'optimal, et une complexité algorithmique faible. Elle est utilisée dans les algorithmes de compression JPEG et MPEG par blocs de taille 8×8. Cette technique est très souvent reprise dans les techniques de tatouage utilisant la DCT.

La DCT d'une image $I(i, j)$ de taille $N \times N$ est donnée par l'équation suivante :

$$C(u,v) = c(u)c(v)\frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(j+\frac{1}{2}\right)\right). \tag{1-6}$$

Avec :

$$\begin{cases} c(x) = 2^{-1/2} \text{ si } x = 0 \\ c(x) = 1 \text{ si } x > 0 \end{cases}$$

La transformée DCT inverse se calcule comme suit :

$$I(i,j) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)C(u,v)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(j+\frac{1}{2}\right)\right). \tag{1-7}$$

Cette transformée souvent calculée sur des blocs de l'image de taille 8×8, soit 64 coefficients. Ces coefficients sont répartis sur trois zones : basses, moyennes et hautes fréquence, comme indiqué sur la figure 1-8.

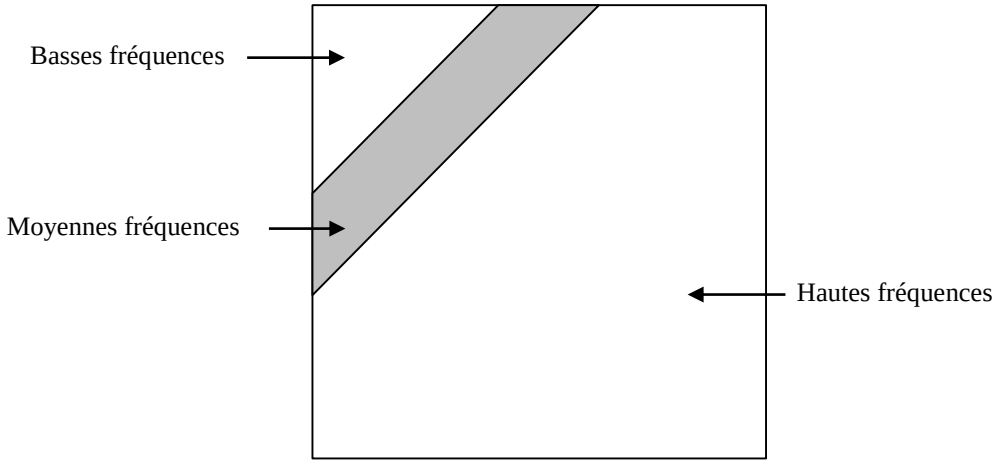


Figure 1-8- Répartition des fréquences dans un bloc DCT.

La DCT est utilisée principalement dans le tatouage numérique pour faire face aux attaques de compression JPEG. Dans ce cadre Suhail et Obaidat [Suhail *et al.* 2003] ont présenté un algorithme de tatouage basé sur la DCT. Dans cet algorithme, l'image originale est divisée en blocs de taille 8×8 pixels puis la DCT est appliquée à chaque bloc. Le message, constitué d'une séquence aléatoire, est inséré dans les fréquences moyennes de la DCT de chaque bloc, l'image tatouée est obtenue par une transformation inverse de la DCT. Un autre avantage en faveur de l'utilisation de la DCT est la possibilité de bénéficier des études psycho-visuelles déjà menées en codage de source, par exemple, les travaux de Watson et Solomon [Watson *et al.* 1997] et Lubin [Lubin 1997]. En effet, elles se proposent de prendre en compte des phénomènes comme la représentation de la couleur, la sensibilité au contraste et les effets de masquage [Qiao *et al.* 2007]. Malgré ces avantages le domaine de la DCT est très sensible aux transformations géométriques (attaques de désynchronisation). Ces transformations peuvent altérer fortement la valeur des coefficients de la DCT. D'où l'intérêt de l'utilisation d'un domaine qui possède des propriétés d'invariance contre les transformations géométriques telles que la rotation et la translation. Nous verrons dans la suite les différentes approches existent dans la littérature pour faire face aux attaques de désynchronisation.

1.5 Tatouage robuste aux attaques de désynchronisation

L'objectif de cette section est de présenter quelques méthodes de tatouage robuste aux distorsions provoquées par la désynchronisation. Ces distorsions sont connues comme un sérieux problème dans

le tatouage numérique. Plusieurs contre-mesures ont été proposées dans la littérature pour faire face à ce type d'attaques. Les attaques de désynchronisation ne retirent pas la marque insérée, mais ont pour effet d'introduire une perte de synchronisation entre la marque insérée et le décodeur. D'une autre manière ces attaques altèrent la position de la marque dans l'image tatouée, alors que la marque existe toujours dans l'image. En conséquence, le décodeur est incapable de détecter la marque après ce type d'attaques. En effet, dans la majorité des méthodes de tatouage, l'opération de l'extraction a besoin de connaitre la position exacte de la marque dans l'image. En général, les attaques de désynchronisation sont classées en deux grandes catégories ci-dessous :

- **Distorsion géométrique globale :** C'est une transformation paramétrique appliquée sur l'ensemble de l'image qui affecte tous les pixels de la même façon. Les transformations géométriques globales comprennent les transformations affines comme la rotation, mise à l'échelle, la translation, et les transformations projectives. La transformation globale est déterminée de façon unique par un ensemble de paramètres. Dans le tatouage d'images il n'y a pas une solution parfaite pour faire face aux transformations géométriques globales affines. On peut citer la recherche exhaustive des paramètres de la transformation pour corriger l'image [M. Barni 2005], les méthodes basées sur un modèle de resynchronisation [Pereira *et al.* 2000], une marque circulaire et symétrique dans le module de la transformée des Fourier [Licks *et al.* 2000] ou l'insertion dans des domaines invariants [Ruanaidh *et al.* 1998].
- **Distorsion géométrique locale :** Elle comporte un ensemble de transformations géométriques différentes (avec différents paramètres) appliquées à différentes parties de l'image de sorte que les pixels soient déformés d'une manière différente. Ce type d'attaques comprend principalement les distorsions aléatoires (RBA ou l'attaque StirMark [Kutter *et al.* 1999], distorsions introduites lors de l'impression et la numérisation,…). Les paramètres nécessaires pour décrire les transformations géométriques locales sont en général beaucoup plus nombreux que ceux nécessaires pour les transformations géométriques globales. Ainsi, la resynchronisation des distorsions géométriques locales est plus difficile que celle des distorsions géométriques globales. Par conséquent, la résistance aux distorsions aléatoires locales comme RBA reste un problème ouvert pour la plupart des techniques de tatouage en raison de la grande complexité de l'espace des paramètres d'attaques.

Dans la suite, nous donnerons un aperçu sur les techniques utilisées dans le tatouage numérique pour résister aux attaques géométriques.

1.5.1 Transformation invariante

La solution la plus évidente au problème de la désynchronisation, consiste à utiliser un domaine invariant aux transformations affines. Si la marque est insérée dans ce domaine, l'attaque sera tout simplement ignorée lors de la détection. Il existe des techniques qui profitent de l'invariance du module de la transformée de Fourier aux translations. En conséquence, la marque est robuste aux translations. La rotation qui se traduit par un décalage circulaire est compensée par l'insertion circulaire de la marque d'une manière redondante [Solachidis *et al.* 2001] ou par le calcul de la corrélation croisée [Licks *et al.* 2000], [Ante Poljicak *et al.* 2011].

La transformation de Fourier-Mellin (FMT) [Ruanaidh *et al.* 1998, Zhao 2015] est une autre alternative offrant des propriétés intéressantes ; invariance par translation, rotation et mise à l'échelle. Cette transformation est obtenue par une transformée de Fourier suivie par une transformation en coordonnées logarithmique-polaires puis une deuxième transformée de Fourier. Pour que la transformation soit inversible, les phases calculées après chaque transformée de Fourier sont conservées et réutilisées lors du retour au domaine spatial. Le module de la transformée de Fourier est invariant par translation. Sa conversion en coordonnées log-polaires permet de convertir le changement d'échelle et la rotation en translation horizontale et verticale. La deuxième transformation de Fourier permet d'obtenir un domaine invariant à la translation, rotation et le changement d'échelle. La figure 1-9 montre les différentes étapes de transformations nécessaires à la construction d'un espace d'insertion de la marque invariant aux transformations géométriques (translation, rotation et changement d'échelle).

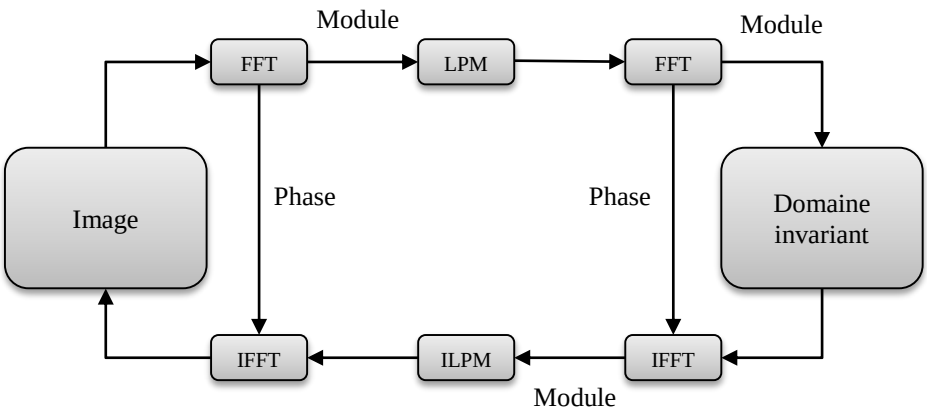


Figure 1-9- Prototype proposé dans [Ruanaidh *et al.* 1998], pour transformer une image du domaine spatial jusqu'au le domaine invariant aux RST. FFT et IFFT sont la transformée de Fourier et son inverse, LPM "Log Polar Maping" et ILPM est le changement de base en log-polaire et son inverse.

Cependant, cette transformation présente des difficultés de l'implémentation. Le passage des coordonnées euclidiennes aux coordonnées log-polaires implique des approximations numériques, liées au problème d'échantillonnage. Ces approximations provoquent une perte de la qualité de l'image et caractérise en soi une attaque. En raison de ces difficultés, des versions modifiées ont été proposées dans la littérature. Lin *et al.* [C. Y. Lin *et al.* 2001] ont proposé une méthode qui consiste à effectuer l'insertion de la marque sur la projection 1D de l'axe log-radial de l'image transformée par la FMT. De cette manière, l'invariance de la translation et du changement d'échelle est obtenue. Ainsi la rotation (qui se traduit par un décalage circulaire) est alors compensée par une recherche exhaustive sur l'axe radial.

Une autre approche basée sur la normalisation de l'image par le calcul des moments afin d'obtenir un espace invariant aux transformations affines. La normalisation a été largement utilisée dans la reconnaissance des formes et le recalage d'images. En tatouage d'image, l'insertion et la détection de la marque est effectuée dans une image ayant subi la normalisation [Dong *et al.* 2005, Nasir *et al.* 2012]. Dans ce cas, il s'agit donc d'un domaine spatial invariant aux transformations géométriques.

Bien que les techniques basées sur les domaines invariantes soient robustes aux transformations affines globales, elles ne résistent pas au recadrage car elles ont besoin de toute l'information pour effectuer la transformation vers l'espace invariant. En plus, ces techniques sont fragiles aux distorsions géométriques locales.

1.5.2 Insertion d'un motif de resynchronisation

Cette technique consiste à insérer, en plus de la marque, un motif appelé 'Template' ou pilote de resynchronisation dont on maîtrise les caractéristiques. Les pilotes peuvent être insérées dans le domaine spatial ou dans le domaine fréquentiel afin d'identifier les transformations affines que l'image a subies. Dans [Pereira *et al.* 2000], il s'agit de pics insérés dans les moyennes fréquences du module de la transformé de Fourier. Les pics subissent les mêmes transformations que l'image tatouée. En connaissant les positions des pics avant et après la transformation affine, il est possible d'appliquer les transformations inverses pour retomber sur l'image non déformée. Cette technique a été considérablement améliorée dans [Ming-Sui *et al.* 2010], où les pilotes de resynchronisation insérés tiennent compte de la connaissance de l'image originale dans la phase d'insertion. Cette technique n'est pas robuste à l'élimination des pilotes (par exemple par un filtrage coupe bandes permet de modifier les pics).

1.5.3 Tatouage basé sur le contenu

Les méthodes basées sur le contenu consistent à construire des références qui dépendent des caractéristiques robustes de l'image propres à son contenu. Kutter et Peticolas [Kutter *et al.* 1999]

introduisent une initiation au tatouage basé sur le contenu que l'on appelle aussi tatouage de deuxième génération. L'insertion et la détection de la marque sont effectuées on se basant sur des références dépendant de l'image. Le repère de l'insertion et la détection n'est plus alors un repère fixe, mais un repère dépend du contenu de l'image.

Une méthode proposée par Bas *et al.* [P. Bas *et al.* 2002], consiste à appliquer une détection de points caractéristiques sur l'image. Puis un partitionnement triangulaire de Delaunay est appliqué à partir de l'ensemble de points caractéristiques. Finalement, la marque sous la forme d'un triangle rempli par une séquence pseudo aléatoire est insérée dans chacun des triangles. L'insertion peut être effectuée également dans le domaine fréquentiel. Les premières étapes de l'algorithme de détection sont identiques à celles de l'algorithme de l'insertion de la marque; la détection des points est appliquée à nouveau, suivi d'un partitionnement triangulaire pour obtenir l'ensemble de triangles tatoués. Finalement, la marque est détectée dans chacun des triangles par corrélation entre le triangle extrait et le triangle de base.

L'inconvénient principal de ces méthodes est la nécessité d'une extraction robuste des points caractéristiques lors des différentes attaques.

1.5.4 Autres méthodes

On peut aussi penser d'utiliser l'image originale afin de détecter la transformation qu'a pu subir l'image tatouée. Une fois les attaques géométriques estimées, il est possible de tenter de les corriger. Dong *et al.* [Dong *et al.* 2005] ont présenté un schéma de tatouage non aveugle robuste aux transformations géométrique locales. Ce schéma est basé sur un maillage déformable qui permet de caractériser des transformations géométriques aléatoires locales puis les corrigées. Il existe aussi d'autres méthodes, telles que la recherche exhaustive [Lichtenauer *et al.* 2003]. Ces méthodes consistent à appliquer le détecteur à l'ensemble des versions déformées de l'image. Les versions déformées de l'image sont obtenues par l'application des transformations affines dont les paramètres varient dans un intervalle donné. Les inconvénients majeurs d'une telle approche sont le temps et la complexité du calcul qui augmentent de façon exponentielle avec la taille de l'espace de recherche.

Notons qu'il est plus facile de résister à des distorsions géométriques globales, que contre des distorsions géométriques locales. En ce qui concerne les distorsions géométriques locales, seules les approches utilisant l'image originale sont envisageables. D'autre part, chaque technique peut présenter des inconvénients spécifiques (implémentation, coût de calcul,...). Notons que la majorité des méthodes robuste aux transformations géométriques sont basées sur la transformée de Fourier. Dans la suite nous présentons un bref descriptif sur la transformée de Fourier et ses propriétés utiles pour le tatouage d'images ainsi quelques méthodes de tatouage d'image basées sur cette transformation.

1.6 Tatouage basé sur la transformé de Fourier discrète

1.6.1 La transformée de Fourier discrète

La transformée de Fourier consiste à décomposer un signal ou une image en une somme de signaux élémentaires, qui ont la propriété d'êtres faciles à mettre en œuvre et à observer. Ces signaux élémentaires sont périodiques et complexes, afin de permettre une étude en amplitude et en phase des systèmes.

La transformée de Fourier discrète d'une image *f(m, n)* de taille $M \times N$ est définie par :

$$F(u,v) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n) e^{-j2\pi(\frac{u.m}{M}+\frac{v.n}{N})} , \tag{1-8}$$

où *u* et *v* désignent les fréquences spatiales pour une position *m* et *n*. À partir de la transformée de Fourier, il est possible de reconstituer exactement l'image originale en prenant la transformée inverse,

$$f(m,n) = \frac{1}{M.N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi(\frac{u.m}{M}+\frac{v.n}{N})} . \tag{1-9}$$

Les images que l'on obtient après la transformée de Fourier discrète sont complexes. En général, pour représenter cette forme complexe on calcule le module *M* et la phase *P* données par les équations suivantes :

$$M(u,v) = \left|F(u,v)\right| = \sqrt{(\mathrm{Re}(u,v)^2 + \mathrm{Im}(u,v))} , \tag{1-10}$$

$$P(u,v) = \arg\left(F(u,v)\right) = \tan^{-1}\left(\frac{\mathrm{Im}(u,v)}{\mathrm{Re}(u,v)}\right), \tag{1-11}$$

où *Im* et *Re* représentent respectivement la partie imaginaire et la partie réelle de la transformée de Fourier de l'image *f*. En général, on représente uniquement le module dont la répartition fréquentielle est illustrée sur la figure 1-10.

Figure 1-10- Image et son module de Fourier.

En raison des propriétés de symétrie hermitienne de la DFT, les modules dans le premier et le deuxième quadrants sont égaux respectivement à ceux des coefficients du quatrième et troisième quadrants respectivement. La figure 1-11 montre la répartition des fréquences dans le module de la transformée de Fourier.

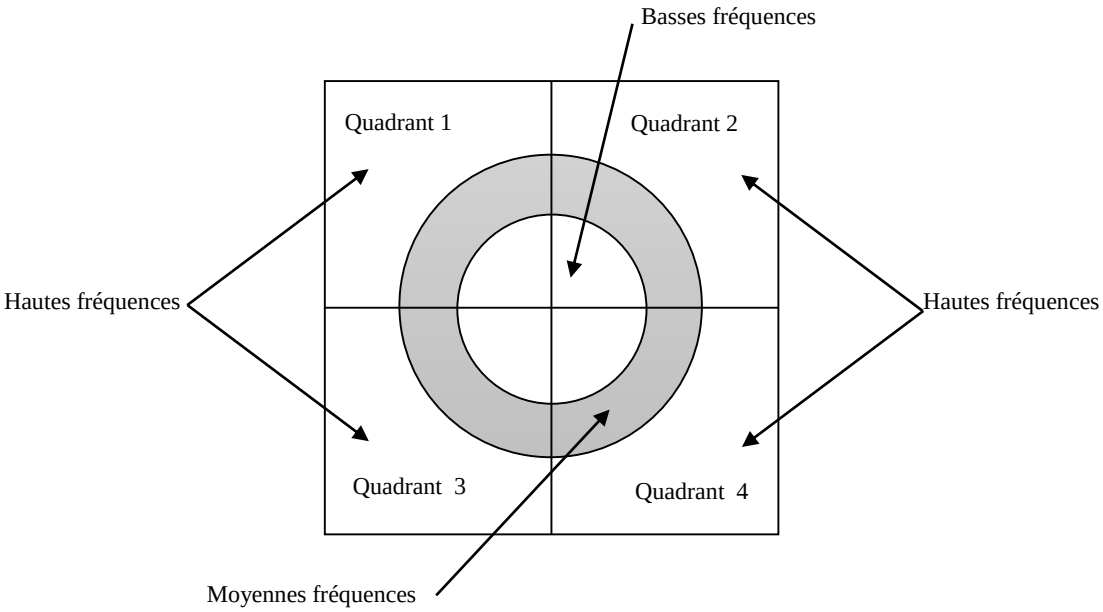


Figure 1-11- Répartition fréquentielle des coefficients de l'amplitude d'une DFT.

1.6.2 Propriétés de la transformée de Fourier

1.6.2.1 Produit de convolution

Une propriété essentielle de la transformation de Fourier, qui est en fait la principale raison de son utilisation, est qu'elle transforme un produit de convolution en un produit simple. En effet soit deux images $f(m,n)$ et $h(m,n)$ dont les transformées de Fourier sont respectivement $F(u,v)$ et $H(u,v)$. Leur produit de convolution $y(m,n)$ est défini par :

$$y(m,n) = f(m,n) * h(m,n) \,. \tag{1-12}$$

La transformée de Fourier de ce produit s'écrit :

$$Y(u,v) = F(u,v) \cdot H(u,v) \,. \tag{1-13}$$

Réciproquement, la transformée de Fourier d'un produit simple est un produit de convolution.

1.6.2.1 Translation

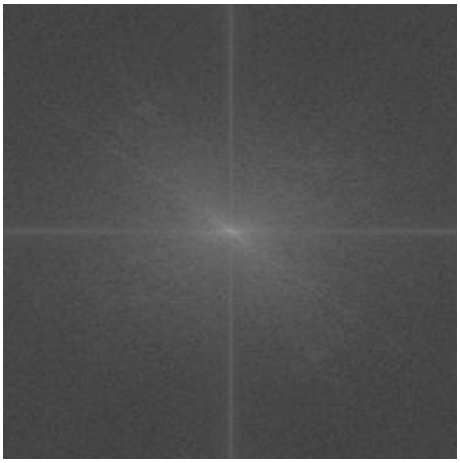
Dans le domaine de la transformée de Fourier, une translation de l'image *f* se répercute exclusivement sur la phase et laisse invariante l'amplitude (voir figure 1-12). La translation de *f* correspond un déphasage de *F*, la transformée de Fourier de l'image *f* translatée s'obtient en multipliant *F* par le facteur de phase comme il est indiqué par l'équation suivante :

$$f(m-a, n-b) \rightarrow F(u,v).e^{j(a.u+b.u)} \,, \tag{1-14}$$

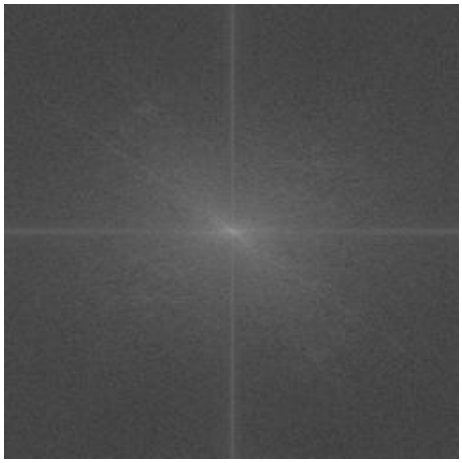
avec *a* et *b* représentent deux facteurs de translation.

Image originale

Image translatée



Amplitude de l'image originale



Amplitude de l'image translatée

Figure 1-12- Exemple d'une image translatée et son spectre d'amplitude.

1.6.2.1 Changement d'échelle

Un changement d'échelle avec un facteur a dans le domaine spatial d'une image f conduit à un changement d'échelle inverse dans le domaine de la transformée de Fourier comme décrit dans l'équation suivante :

$$f(a \cdot m, a \cdot n) \rightarrow \frac{1}{|a|} F(\frac{u}{a}, \frac{v}{a}) . \tag{1-15}$$

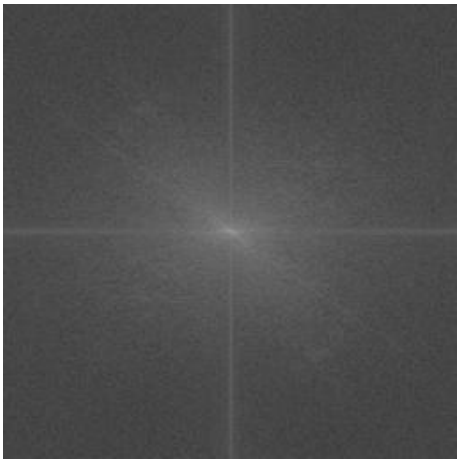
1.6.2.1 Rotation

La rotation de l'image d'un angle θ dans le domaine spatial se traduit par une rotation du même angle du spectre d'amplitude de la transformé de Fourier (voir figure 1-13).

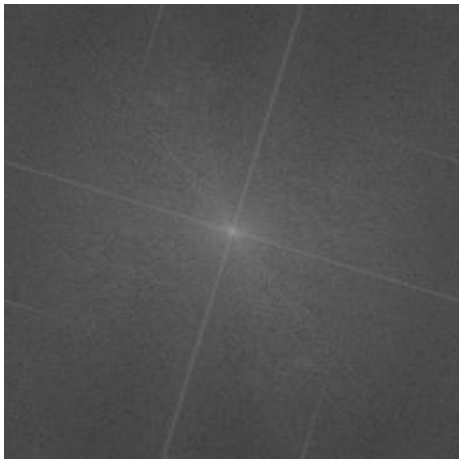
$$f(m.\cos\theta - n.\sin\theta, m.\sin\theta + n.\cos\theta) \rightarrow F(u.\cos\theta - v.\sin\theta, u.\sin\theta + v.\cos\theta)\ . \qquad (1\text{-}16)$$

Image originale

Image pivotée d'un angle de 30°



Amplitude de l'image originale



Amplitude de l'image pivotée

Figure 1-13- Exemple d'une image pivotée d'un angle 30° et son amplitude.

1.6.3 Méthode de tatouage basé sur la DFT

Il existe différentes domaines pour insérer une marque dans une image. Parmi ces domaines on trouve le domaine de la transformée de Fourier. Ce domaine se caractérise essentiellement par deux avantages par rapport au domaine spatial. Premièrement, il possède la propriété de distribuer l'énergie du tatouage à l'image entière dans le domaine spatial [Ante Poljicak *et al.* 2011]. Et d'autre part, le module de la transformée de Fourier est invariant aux translations. Donc, en travaillant sur le module, le tatouage est robuste à la translation dans le domaine spatial. Pour faire face aux problèmes

de rotation, des méthodes ont été proposées dans la littérature consistant à insérer la marque de manière circulaire.

Une méthode de tatouage présentée dans [Solachidis *et al.* 2001] est basée sur l'utilisation d'anneaux particuliers. Cette technique rend la méthode insensible aux transformations de type translation, rotation et changement d'échelle. L'algorithme d'insertion consiste à appliquer la transformée de Fourier à une image en niveaux de gris de dimensions $N \times N$. Puis la marque est insérée dans le module de la DFT. Le tatouage se réalise dans les moyennes fréquences de l'espace de Fourier (la représentation fréquentielle de la DFT est celle pour laquelle la composante continue est située au centre de l'image).

La marque W est définie comme étant une séquence pseudo-aléatoire ayant comme valeurs +1 ou -1 et possède une forme d'anneaux. L'expression polaire de l'anneau fréquentiel est définie par :

$$W(r,\theta) = \begin{cases} 0 & , si\ r < R_1\ ou\ r > R_2 \\ \pm 1 & , si\ \ R_1 < r < R_2 \end{cases} \text{, avec } r = \sqrt{u^2 + v^2} \text{ et } \theta = \arctan\left(\frac{v}{u}\right), \qquad (1\text{-}17)$$

où u et v sont les cordonnées cartésiennes des éléments de la marque. L'anneau est constitué de sous éléments dont la particularité repose sur le fait que chaque élément, en allant de l'extérieur vers l'intérieur de l'anneau, est la version deux fois plus petite de l'anneau immédiatement supérieur. De plus, les anneaux ainsi créés sont découpés en S secteurs identiques comme indiqué la figure 1-14.

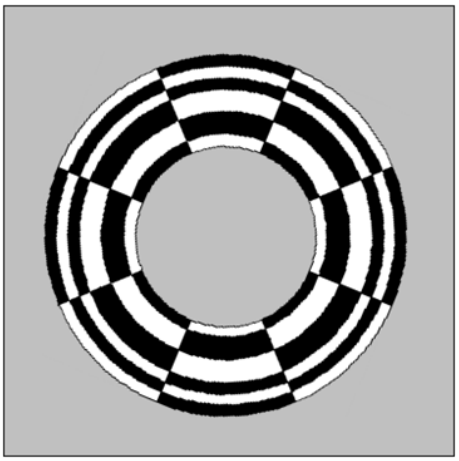


Figure 1-14- Présentation des anneaux dans le domaine fréquentiel. Le centre de l'image correspond à la fréquence DC de l'image.

Le module de la DFT noté M est après insertion de la marque noté M_W. L'insertion de la marque dans le domaine fréquentiel se réalise de la manière suivante :

$$M_w(u,v) = M(u,v) + \alpha \cdot W(u,v)\ , \tag{1-18}$$

où α représente la force avec laquelle la marque sera introduite sur les coefficients du module de la DFT. L'image tatouée est ensuite obtenue en réalisant la transformée inverse IDFT.

La détection de la présence ou non de la marque dans l'image est réalisée au moyen d'une corrélation entre la marque originale et le module de la transformée de Fourier de l'image :

$$c = \sum_{u=1}^{N}\sum_{v=1}^{N} W(u,v) \cdot M_W(u,v)\ , \tag{1-19}$$

avec :

- W les coefficients de la marque originale,
- M_W les coefficients du module de la transformée de Fourier de l'image.

Cette corrélation peut être réécrite de la manière suivante :

- si la marque est présente : $c = \sum_{u=1}^{N}\sum_{v=1}^{N}\left(W(u,v) \cdot M(u,v) + a \cdot W(u,v)^2\right)$,
- si la marque est absente : $c = \sum_{u=1}^{N}\sum_{v=1}^{N} W(u,v) \cdot M(u,v)$.

Comme W et M sont indépendants, et que W est de moyenne nulle et de variance unité, alors deux cas de valeur moyenne de c résultent :

$$\mu_c = \begin{cases} \pi \cdot \left(R_2{}^2 - R_1{}^2\right) \cdot \alpha & \text{si la marque est présente} \\ 0 & \text{si la marque est absente} \end{cases} \tag{1-20}$$

La corrélation est ensuite normalisée par rapport à la valeur non nulle de μ_c produisant un résultat compris entre 0 et 1 ($c' = c/\mu_c$). Ce résultat est ensuite comparé à un seuil de détection t :

- si $c' \geq t$, alors la marque est considérée comme présente,
- si $c' < t$, alors la marque est considérée comme absente.

Ce seuil t peut être déterminé par rapport à la prise en compte des fausses alarmes et des non détections. Durant leurs tests, les auteurs utilisent trois seuils, 0.1, 0.15, 0.2.

Licks et Jordan [Licks *et al.* 2000] ont proposé une autre méthode qui consiste à insérer une marque circulaire dans le module de la transformée de Fourier. La figure 1-15 montre la méthode de l'insertion. Si l'image a subi une rotation, le spectre et la marque subit la même rotation. En conséquence, la marque aura subi un décalage cyclique. Lors la phase de la détection la corrélation croisée est calculée entre la marque originale et les coefficients tatoués décalés.

Cette technique a été récemment améliorée par Poljicak *et al.* [Ante Poljicak *et al.* 2011]. La marque est insérée dans un rayon dit optimal pour minimiser les dégradations dues à l'insertion de la marque. Le PSNR est utilisé comme métrique de l'évaluation de la qualité visuelle de l'image tatouée. La détection de la marque consiste à calculer le maximum de la corrélation croisée entre les éléments de la marque de référence et le coefficient le long du rayon dans le module de la transformée de Fourier discrète. Si la valeur maximale de la cross-corrélation est supérieure à un certain seuil la marque et présente dans l'image sinon l'image ne contient pas la marque.

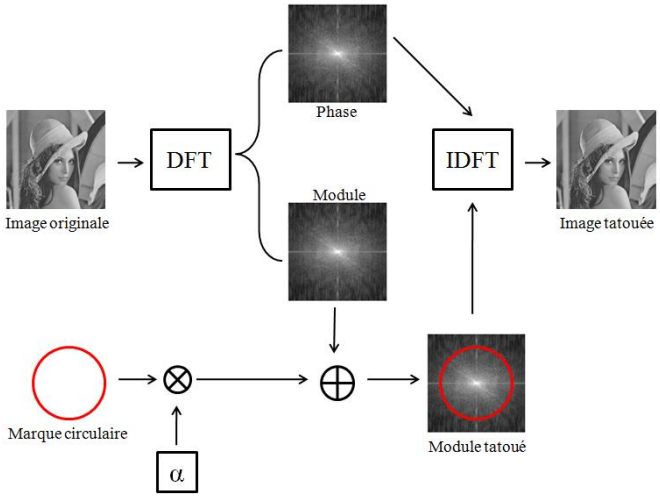


Figure 1-15- Tatouage basé sur la transformée de Fourier proposé dans [Licks *et al.* 2000].

1.7 Conclusion

Ce chapitre a présenté un état de l'art sur le tatouage des images numériques. Nous nous sommes intéressés aux notions liées aux techniques du tatouage numérique. Nous avons aussi abordé les différentes phases de la conception d'une méthode de tatouage. Un schéma de tatouage permet d'insérer une marque d'identification dans une image. Ce schéma se compose de deux phases : la phase d'insertion qui consiste à insérer (ou à cacher) une marque d'identification et la phase de détection qui consiste à détecter ou à décoder la marque insérée. Nous avons présenté un bref descriptif sur les méthodes de tatouage robuste aux transformations géométriques. Puis les raisons qui ont motivé notre choix des méthodes de tatouage dans le domaine de Fourier. Ce domaine d'insertion se caractérise par sa résistance contre les attaques géométriques globales. Dans le chapitre suivant nous présentons une étude détaillée sur l'attaque impression/numérisation ainsi que les modèles proposés dans la littérature afin de construire une méthode robuste à ce genre d'attaque.

Chapitre II :

2 La chaine impression / numérisation

2.1 Introduction

Pour récupérer la marque insérée dans une image analogique (imprimée sur un support physique), une numérisation de l'image est indispensable. Ceci est réalisé par un scanner ou une caméra numérique. La conversions numérique-analogique suivie d'une conversion analogique-numérique représentent une attaque très forte et la majorité des méthodes de tatouage sont sensibles à ce genre d'attaque. Le but de ce chapitre est de mettre en évidence les différentes distorsions produites dans la phase de l'impression/numérisation et de décrire les modèles proposés ainsi les solutions développés pour les éliminer ou les réduire.

2.2 Le processus impression/numérisation

Pendant l'opération de l'impression/numérisation, l'image subit plusieurs modifications. Même si l'image numérisée peut ressembler à celle d'origine, des distorsions, visibles ou invisibles à l'œil nu, sont présentes. Ces distorsions apparaissent à la fois dans la phase d'impression et dans la phase de numérisation [Smoaca 2011]. Les deux phases seront décrites dans les deux sections suivantes.

2.2.1 Système d'impression

L'impression est un processus de reproduction du texte et des images, généralement avec de l'encre sur du papier. Les technologies d'impression les plus utilisées par les particuliers et les professionnels sont les suivantes : l'impression jet d'encre, l'impression laser et l'impression par sublimation thermique [Imprimante-info 2012]. Nous allons dans la suite expliquer le fonctionnement de chacune de ces technologies.

2.2.1.1 L'impression jet d'encre

L'impression jet d'encre est réalisée par la projection de minuscules gouttelettes d'encre liquide, de l'ordre de quelques picolitres (10^{-12} litre), sur le support d'impression formant ainsi des points. Cette projection est réalisée en faisant varier la pression dans des canaux remplis d'encre qui se trouvent sur la tête d'impression. La variation de la pression est effectuée en utilisant deux technologies : il s'agit de la technique thermique basée sur le réchauffement de l'encre, et la technique piézo-

électrique qui utilise une tension pour changer la forme d'un élément en céramique qui change la pression.

2.2.1.2 L'impression laser

Une imprimante laser met en œuvre des technologies complexes pour produire une impression : électronique, mécanique, électrostatique, optique, thermique... Les imprimantes laser utilisent la même technologie utilisée par les photocopieurs. Mais contrairement aux photocopieurs qui utilisent une lampe, les imprimantes laser utilisent un rayon laser pour tracer une copie de l'image à imprimer sur un tambour photoconducteur. Le toner est une encre sèche sous forme de poudre constituée de particules en plastique très fines. Ces particules sont chargées négativement grâce à une source électrostatique. Les particules chargées sont transférées par la suite sur les parties du tambour qui ont été préalablement chargées positivement en fonction de l'image à imprimer, à l'aide du rayon laser. Le tambour dépose à son tour les particules de l'encre sur le support d'impression, un papier par exemple. Ces particules sont alors chauffées jusqu'à atteindre la température de fusion. En quelques millièmes de seconde, les particules de l'encre sont fusionnées puis pressées sur le support. Finalement le tambour est nettoyé pour qu'il soit prêt à la prochaine impression.

2.2.1.3 L'impression par sublimation thermique

La technologie utilisée pour l'impression des photos sur les cartes en plastique est l'impression par sublimation thermique. Dans nos expériences, nous avons utilisé une imprimante par sublimation thermique. Dans la suite, nous allons décrire brièvement le principe de fonctionnement de ce type d'imprimantes.

La technologie d'une imprimante à sublimation thermique est basée sur le passage d'un film plastifié qui comporte des couches de cire colorée devant une tête d'impression chauffante (voir figure 2-1). Cette tête d'impression possède plusieurs centaines d'éléments pouvant être portés à une température très élevée (entre 220 et 370°C) [Leppla *et al.* 2001]. Tout d'abord l'image au format RVB stockée dans l'ordinateur est envoyée à l'imprimante (par une liaison USB par exemple). Un processeur spécialisé la convertit en espace des couleurs CMJ (cyan, magenta, jaune, les trois couleurs utilisées pour l'impression) en la décomposant en trois image distinctes, une pour chaque couleur de base. Les informations correspondant à ces trois couches sont ensuite envoyées, les unes après les autres, à la tête d'impression. La tête d'impression chauffée est directement au contact avec le support et le film transparent sur lequel des couches de cire colorées ont été appliquées (cyan, magenta, jaune).

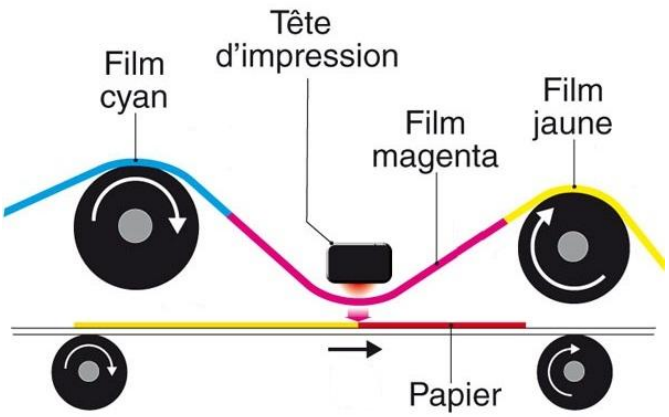


Figure 2-1- Fonctionnement d'une imprimante à sublimation thermique.

La cire colorée est sublimée (elle passe d'un état solide à un état gazeux). Puis elle est envoyée sur le support en trois passage ; un pour chaque couleur de base, plus un pour la couche protectrice. Le gaz de cire colorée se solidifie instantanément au contact avec le support au cours de l'impression. Les micro-résistances réparties sur la tête d'impression reçoivent des signaux électriques d'intensité variable proportionnels à la quantité de la couleur. Plus la température des résistances est élevée, plus la quantité du couleur est importante. Avec 256 niveaux de température par couleur, on atteint 16.7 million teintes différentes, par superposition des couches jaune, magenta et cyan. Le noir est obtenu par saturation de ces trois couleurs. La résolution de ce type d'imprimantes est limitée à 300 dpi.

2.2.2 Système de numérisation

Un système de numérisation est un dispositif permettant de numériser un document, c'est-à-dire d'affecter une valeur numérique à chacun des points de ce document. Ce dispositif permet donc de transformer un document sous forme papier (dessin, imprimé, photographie, etc.) en une image numérique pouvant être stockée dans la mémoire d'un ordinateur ou sur un support numérique. Plusieurs systèmes de numérisation se distinguent en fonction de leur conception technologique : les scanners à plat, les scanners à tambour, les scanners de poche et les scanners à défilement.

Un scanner inclut une source lumineuse, un support plat (vitre) pour placer le document, et un système permet de capturer et d'analyser la lumière émise par la source. La figure 2-2, illustre le principe de fonctionnement d'un scanner classique. La source lumineuse éclaire le document à numériser. Le faisceau lumineux traverse ensuite un système de miroirs et de lentilles convergentes qui l'envoie sur une barrette de capteurs CCD, associée à un jeu de filtres RVB. Les capteurs reçoivent le signal lumineux et convertissent cette énergie reçue en une tension électrique

proportionnelle à celle-ci. Enfin, un convertisseur analogique-numérique transforme cette dernière en une donnée numérique exploitable par un ordinateur.

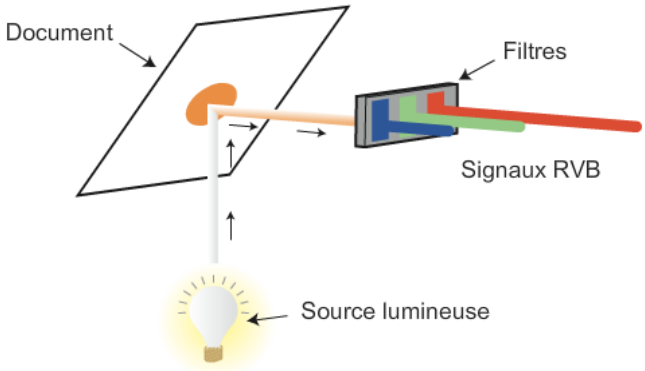


Figure 2-2- Fonctionnement d'un scanner classique.

2.3 Impact de l'impression/numérisation sur les images

L'opération impression/numérisation (Print-Scan) consiste à imprimer une image sur un support physique (carte en matière de plastique pour l'application visée), puis à scanner l'image préalablement imprimée à l'aide d'un scanner. Cette opération conduit à une combinaison complexe de différentes attaques, qui produisent des distorsions diverses sur l'image résultante (c.à.d. l'image imprimée/scannée). Après cette opération, le tatouage des images numériques est délicat. Pour élaborer un algorithme de tatouage robuste aux distorsions qui sont produites par l'attaque impression/numérisation, il est nécessaire d'effectuer une étude approfondie de l'influence de cette attaque sur les images.

Lin et Chang [Ching-Yung Lin *et al.* 1999] ont décomposé le processus d'impression/numérisation en deux types de distorsions : les distorsions géométriques et les distorsions de la valeur des pixels. Le premier type de distorsions groupe tous les distorsions liées à la rotation, le changement d'échelle et la translation. Ces distorsions peuvent être plus ou moins importantes, comme les distorsions géométriques locales qui mettent en défaut la majorité des algorithmes du tatouage numérique existants dans la littérature. Le deuxième type correspond aux distorsions de la valeur des pixels, il regroupe le flou dû à la réponse impulsionnelle du système, l'ajout de bruit et la variation des couleurs.

D'autre part, Solanki *et al.* [Solanki *et al.* 2006] ont présenté les différentes déformations interviennent durant le processus de l'impression/numérisation (voir figure 2-4). La chaine utilisée

par les auteurs est composée d'une imprimante laser et un scanner à plat. Les déformations d'image dues à l'impression/numérisation sont au nombre de sept, une brève description de ces distorsions est donnée ci-dessous :

- **Correction gamma de l'imprimante :** La correction gamma est une transformation non-linéaire qui permet à une image imprimée à correspondre l'image affichée sur un écran. Si x la luminance d'un pixel avant l'impression, la correction gamma consiste à imprimer un pixel de luminance x^{γ}.
- **Génération d'images en demi-teintes :** La plupart des dispositifs d'impression sont capables d'imprimer qu'en mode tout ou rien [Kundu *et al.* 2006]. Avant l'impression, l'image numérique en teintes continus est transformée en une image binaire imprimable grâce à des algorithmes de conversion (voir figure 2-3). Ce processus de conversion est appelé tramage ou « halftoning ». Cette conversion conduit essentiellement à un bruit coloré haut fréquence [Solanki *et al.* 2006].

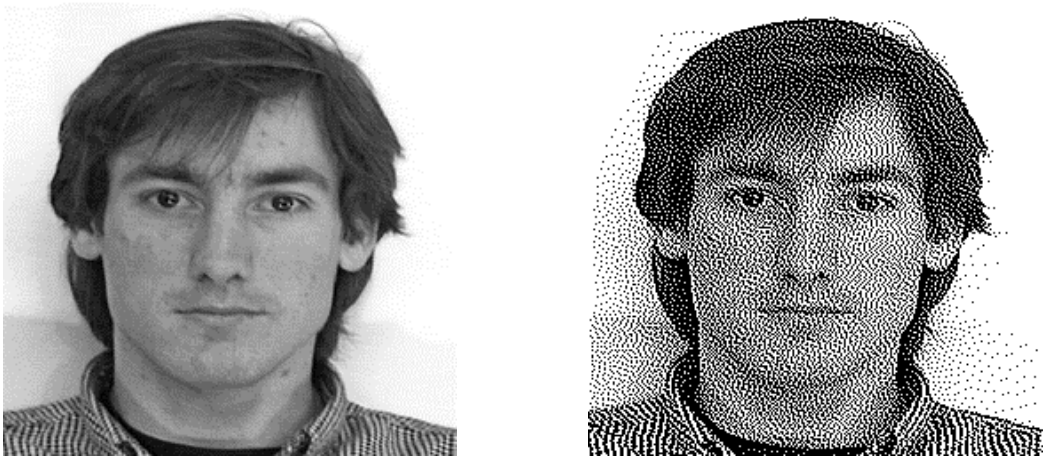


Figure 2-3- Photo d'identité en niveau de gris reproduit en demi-teintes.

- **Élargissement du point de trame :** L'élargissement du point de trame (couramment appelé dot gain) est un défaut d'impression lié à la façon dont l'encre s'étale sur le papier (principalement fonction de la qualité du papier). Sa conséquence est l'augmentation (ou l'étalement) de la taille des points de trame. Ces points occupent généralement plus d'espace que prévu et peuvent parfois se superposer [Boust *et al.* 2005]. En conséquent, l'image subit une perte de luminosité c.à.d. que l'image imprimée peut paraître plus sombre que l'image originale à cause de ce phénomène. L'élargissement du point est une transformation non-linéaire, mais peut être approchée par une approximation affine

par morceaux. Cette approximation est souvent prise en compte dans les algorithmes de la génération des images en demi-teintes.

- **Instabilité de l'impression :** Les incertitudes produites au cours de l'impression peuvent conduire à un bruit coloré sur l'image. Un exemple de l'instabilité de l'impression est le « banding », qui signifie l'apparition des bandes horizontales dans les documents imprimés. Ces distorsions sont considérées comme des variations mineures dans la sortie d'une imprimante.
- **Compensation de la correction gamma du scanner :** À l'inverse de la phase de l'impression, lorsqu'une image est numérisée, une compensation de la correction gamma doit être effectuée. Afin de garantir un bon affichage sur un moniteur, la luminance des pixels est élevée à la puissance de $1/\gamma$, où γ est la valeur gamma de l'écran sur lequel l'image numérisée doit être affichée.
- **Numérisation :** L'image sous forme analogique doit être numérisée avant le stockage, ce processus conduit aux erreurs de quantification. Les erreurs de quantification introduisent un bruit haut fréquences, ce bruit peut s'amplifier par la compensation de la correction gamma du scanner.

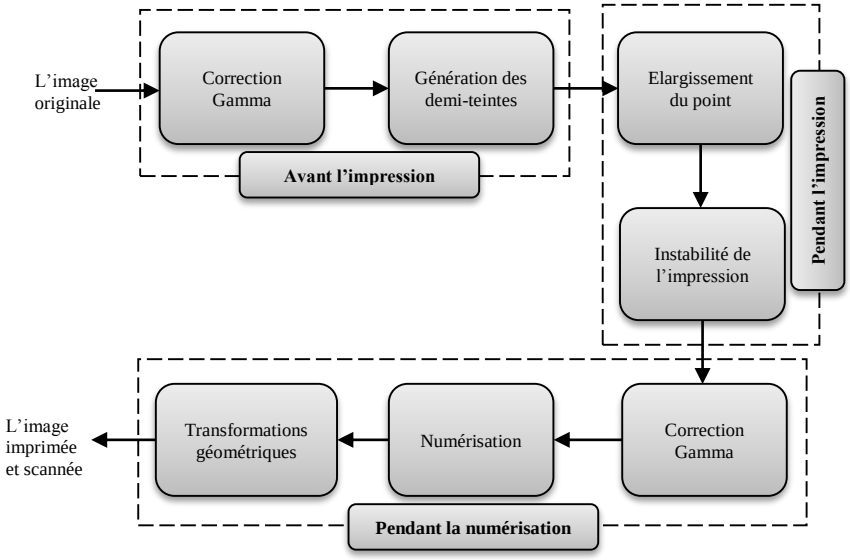


Figure 2-4- Différentes déformations produites par la chaîne d'impression/numérisation sur une image [Solanki *et al.* 2006].

- **Transformations géométriques :** Au moment de la numérisation, l'image subit un certain nombre de transformations géométriques, telles que la rotation, la translation, le recadrage, et la mise à l'échelle. Elles sont principalement dépendantes du positionnement de l'image.

2.4 État de l'art sur les modèles de la chaine impression / numérisation

Après avoir identifié les différents processus qui déforment une image quand elle est imprimée puis scannée, nous présentons les différents modèles de la chaîne d'impression/numérisation afin de réaliser une contre-attaque de ces distorsions. Pour ce faire, il faut considérer deux principales distorsions [C. Y. Lin *et al.* 2001, Nan *et al.* 2012] :

- **Les distorsions géométriques :** l'image subit alors une série de transformations comme la rotation, le changement d'échelle, la translation et le recadrage.
- **Les distorsions de la valeur des pixels :** elles comprennent principalement les changements de la luminosité, du contraste et de la couleur, et l'apparition d'un bruit. Le deuxième aspect couvre des erreurs aléatoires et la conversion numérique-analogique.

Dans la suite nous nous concentrerons sur les distorsions de la valeur des pixels. Les distorsions géométriques sont corrigées naturellement par la méthode de tatouage choisie (Fourier qui est robuste aux translations et rotations comme expliqué au chapitre 1).

2.4.1 Modèles basés sur l'approche Black-Box (Boite noire)

Cette approche considère la chaine d'impression/numérisation comme une boite noire, donc l'analyse est réduite à une comparaison empirique entre l'image originale et l'image après le processus impression/numérisation [Kasprzak *et al.* 2013]. Quelques travaux basés sur cette approche ont mis l'accent sur la recherche empirique des domaines invariants à un certain type de distorsions produites par la chaine. Dans ce cadre, Shi *et al. [Shi et al. 2008]* ont étudié les effets de l'opération impression/numérisation sur les pixels d'une image en utilisant l'image de test présentée dans la figure 2-5. Les histogrammes de l'image test avant et après impression/numérisation sont présentés dans la figure 2-6. Il est clair que les valeurs des pixels subissent un changement notable après le processus d'impression/numérisation. D'après les histogrammes présentés dans la figure 2-6, la dynamique de niveau de gris est réduite et les valeurs des pixels sont concentrées vers les niveaux de gris faibles. Les résultats de ce test montrent la difficulté de trouver une relation linéaire des changements des valeurs des pixels pendant le processus d'impression/numérisation.

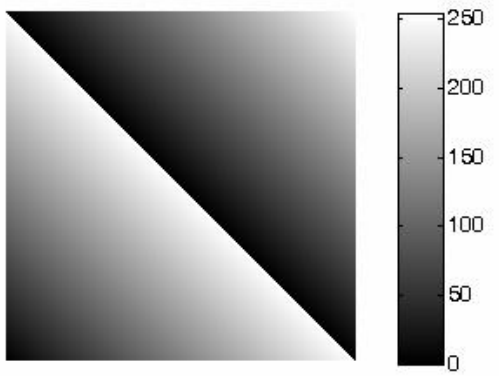


Figure 2-5- Image test utilisée par Shi *et al*. [Shi *et al.* 2008].

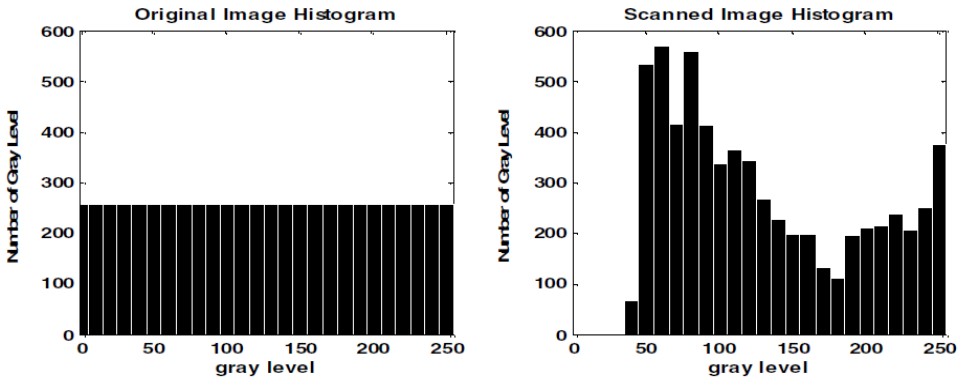


Figure 2-6- Histogrammes de l'image test avant et après impression/numérisation [Shi *et al.* 2008].

D'autres études ont été réalisées sur les effets de l'opération impression/numérisation dans le domaine fréquentiel. Par exemple, Cheng et Huang [Cheng *et al.* 2001] ont analysé les propriétés des coefficients de la DCT d'une image avant et après l'opération impression/numérisation. Ils ont constaté que la moyenne de certains coefficients de la DCT (MDC) est presque inchangée durant l'impression/numérisation. Les auteurs ont proposé une méthode de tatouage basée sur ce constat.

Solanki *et al. [Solanki et al. 2005]* ont étudié les propriétés de l'opération impression/numérisation sur l'amplitude des coefficients de la DFT, et sont arrivés aux constats suivants :

- Les coefficients basses et moyennes fréquence sont préservés beaucoup mieux que ceux des hautes fréquences. En général, plus la fréquence est basse, plus la chance de survie du processus impression/numérisation est grande.
- Dans les bandes basses et moyennes fréquences, les coefficients à faible amplitude peuvent avoir un bruit plus élevé que ceux de grande amplitude dans la même bande de fréquence.

Les auteurs ont proposé une méthode de tatouage qui consiste à insérer la marque dans les coefficients basses fréquences afin qu'elle soit robuste aux distorsions dues à l'impression numérisation. L'inconvénient de la méthode réside dans le fait que l'insertion dans les basses fréquences rend la marque visible.

2.4.2 Modèles statistiques de la chaine impression/numérisation

Plusieurs tentatives ont été faites pour développer des modèles statistiques de la chaine d'impression/numérisation. En fait, les principales références à ce sujet sont [Degara-Quintela *et al.* 2003, Kundu *et al.* 2006, Malvido *et al.* 2006, Villan *et al.* 2006, Amiri *et al.* 2014].

2.4.2.1 Modèle de Lin et Chang

Lin et Chang [Ching-Yung Lin *et al.* 1999] ont étudié les propriétés du processus d'impression/numérisation, ils ont déduit que les distorsions des valeurs de pixels sont produites par les fluctuations de luminance, les modifications de contraste, la correction gamma, les variations de chrominance, et le flou. L'ensemble de ces distorsions sont généralement perceptibles à l'œil humain. Le modèle proposé est basé principalement sur la luminance de l'image.

Pendant l'opération d'impression, l'image numérique discrète est convertie en image analogique continue. Il s'agit d'une image continue à support fini, construit à partir de l'image originale. Puis, l'image sous forme physique est convertie vers le monde numérique avec un bruit supplémentaire après la numérisation.

Le modèle de l'image imprimée puis scannée est donné par la relation ci-dessous :

$$I(i,j) = K[I_0(i,j) * \tau_1(i,j) + (I_0(i,j) * \tau_2(i,j)) \cdot N_1] \cdot s(i,j) \ , \tag{2-1}$$

avec $I(i,j)$ la luminance de l'image imprimée puis scanné et $I_0(i,j)$ la luminance de l'image originale, K est la fonction du transfert du système défini par l'équation suivante :

$$K(x) = \alpha \cdot (x - \beta_x)^{\gamma} + \beta_K + N_2(x) \ , \tag{2-2}$$

où N_2 représente le bruit thermique et le bruit lié au courant d'obscurité, les autres termes sont des ajustements de quantification et de correction gamma dans l'imprimante et dans le scanner [Rivoire 2012].

Le terme $\tau_1(i,j)$ désigne la réponse impulsionnelle de la chaine, il s'agit d'un produit de convolution de la réponse impulsionnelle de l'imprimante $\tau_p(i,j)$ et la fonction d'étalement du point (Point Spread Function ou PSF en anglais) du scanner $\tau_s(i,j)$:

$$\tau_1(i,j) = \tau_p(i,j) * \tau_s(i,j), \tag{2-3}$$

Le terme $\tau_2(i,j)$ représente un filtre passe haut mettant en évidence un variance du bruit plus élevée vers les bords, N_1 est un bruit blanc gaussien, et finalement $s(i,j)$ est la fonction de l'échantillonnage.

2.4.2.2 Modèle de Degara–Quintela

Degara-Quintela et Perez-Gonzalez *[Degara-Quintela et al. 2003]* ont proposé un modèle d'impression/numérisation dans le contexte des codes-barres 2D. La figure 2-7 montre le modèle proposé.

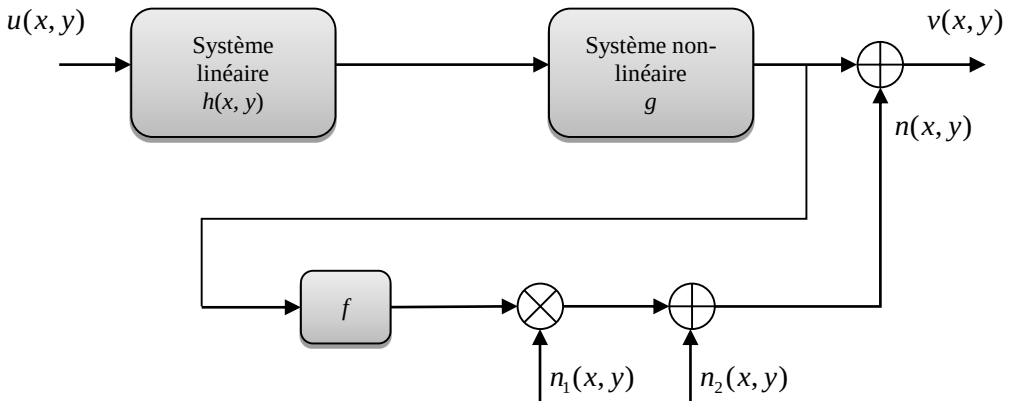


Figure 2-7- Modèle proposé par Degara-Quintela [Degara-Quintela *et al.* 2003]**.**

Les distorsions de la valeur des pixels sont modélisées par les équations suivantes :

$$v(x,y) = g\left[u(x,y) * h(x,y)\right] + n(x,y), \tag{2-4}$$

$$n(x,y) = f\left[g(u(x,y) * h(x,y))\right] n_1(x,y) + n_2(x,y), \tag{2-5}$$

où $u(x, y)$ est la valeur du niveau de gris du pixel de l'image considérée et $v(x, y)$ est la valeur du pixel modélisée après l'impression/numérisation. Le système linéaire $h(x, y)$ modélise le flou causé par la réponse impulsionnelle du système avec :

$$h(x,y) = \tau_p(x,y) * \tau_s(x,y), \tag{2-6}$$

avec τ_p est la réponse impulsionnelle de l'imprimante et τ_s la fonction d'étalement de point du scanner, tous les deux ont une caractéristique d'un filtre passe-bas.

Les fonctions *f* et *g* sont généralement non-linéaires. *g* est la réponse du capteur généralement s'écrit comme :

$$g(x) = \alpha x^{\beta}, \tag{2-7}$$

où α et β sont des paramètres dépendants du dispositif.

Le terme *n* dans l'équation (2-4) est un bruit additif composé de deux composantes aléatoires respectivement dépendantes et indépendantes de l'image ; n_1 est le bruit du capteur CCD (bruit de Poisson) et n_2 est un bruit thermique (bruit blanc gaussien).

Ce modèle prend en compte un nombre très important de paramètres, dans le même cadre des codes-barres Villàn *et al. [Villan et al. 2006]* ont présenté un modèle simplifié avec un nombre de paramètres réduit.

2.4.2.3 Modèle de Villàn

Villàn *et al. [Villan et al. 2006]* ont proposé un modèle simplifié de la chaine d'impression / numérisation sous la forme suivante :

$$Y = f(X) + Z(X), \tag{2-8}$$

où *X* est le niveau de gris du pixel original, *Y* est le niveau de gris de ce pixel après impression/numérisation, *f* est une fonction non-linéaire et *Z* représente un bruit modélisé par une distribution gaussienne généralisée aux paramètres dépendants de *X*. La fonction *f* est assimilée à la moyenne conditionnelle $\mu_{X|Y}$, et la dispersion du bruit par l'écart type conditionnel $\sigma_{X|Y}$. En pratique, $\mu_{X|Y}$ et $\sigma_{X|Y}$ ont été mesurés expérimentalement en utilisant une image test contient différentes bandes de niveau de gris connues varient de 0 à 255, un exemple est présenté dans la figure 2-8.

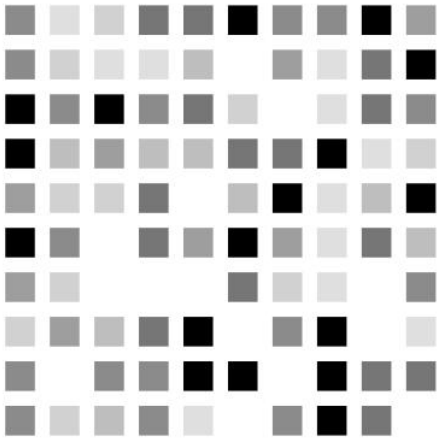
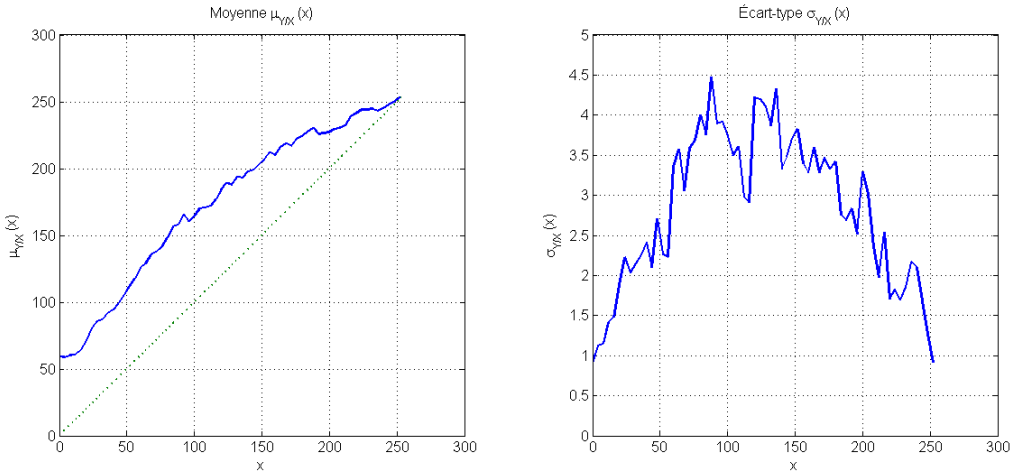


Figure 2-8- Image test utilisée par Villàn [Villan *et al.* 2006] pour la modélisation de la chaîne d'impression/numérisation.

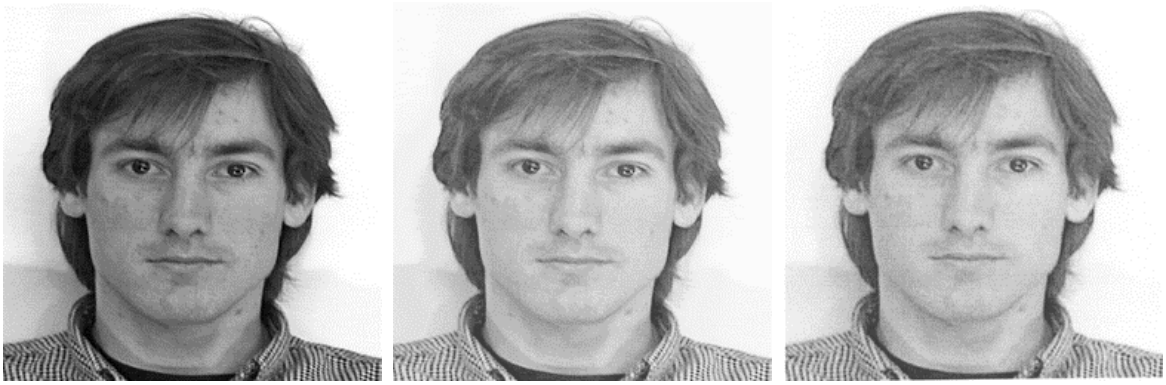
L'image test est imprimée sur du papier puis scannée, pour générer le document final qui correspond aux niveaux de gris originaux. Les estimations de $\mu_{X|Y}$ et $\sigma_{X|Y}$ obtenues en utilisant un couple imprimante/scanner composée de l'imprimante laser HP LaserJet 1300 et du scanner HP Scanjet 5550c. Les résultats sont présentés dans la figure 2-9. Avec l'estimation de $\mu_{X|Y}$ et $\sigma_{X|Y}$, on peut obtenir une caractérisation statistique simple d'un couple imprimante/scanner. Cette estimation empirique est différente pour chaque combinaison imprimante/scanner [Smoaca 2011].



(a) (b)

Figure 2-9- Mesures de la moyenne (a) et de l'écart-type (b) en fonction du niveau de gris initial *X* avec une chaine impression/numérisation composée de l'imprimante laser HP LaserJet 1300 et du scanner HP Scanjet 5550c.

En appliquant le modèle du Villàn sur une image de tests, nous obtenons le résultat dans la figure 2-10. Le résultat obtenu par la simulation de la chaine d'impression/numérisation semble visuellement assez réaliste.



(a) L'image originale (b) Image d'après le modèle de Villàn (c) L'image imprimée et scannée

Figure 2-10- Exemple de simulation du modèle de Villàn d'un couple composée de l'imprimante laser HP LaserJet 1300 et du scanner HP Scanjet 5550c.

2.4.2.4 Modèle d'Amiri et Jamzad

Dans l'article [Amiri *et al.* 2014], le modèle proposé repose sur l'estimation expérimentale du bruit comme un bruit dépendant de l'image et un bruit indépendant de l'image. Les effets de l'impression/numérisation sur les différents niveaux de gris et pour différents valeur de gamma sont étudiés. Le bruit dépendant de l'image est modélisé par une distribution gaussienne avec des paramètres dépendants des valeurs des niveaux de gris des pixels. La moyenne et la variance du bruit sont déterminées par des approximations polynomiales.

Ce qui concerne le bruit indépendant de l'image, Amiri et Jamzad impriment et scannent plusieurs fois différentes images de niveau de gris uniforme, le bruit est définit comme la différence entre la version originale et la version imprimée et scannée d'une image de même niveau de gris. Ils modélisent le bruit indépendant de l'image par une distribution logistique.

Finalement, pour prendre en compte l'influence des pixels voisins pour une valeur d'un pixel donné, une classification est conçue afin de distinguer des classes d'images en fonction de leur complexité. Pour chaque classe d'images, un réseau de neurones a été construit afin d'obtenir l'image après influence des voisins. Le réseau de neurones prend en entrée les valeurs des pixels voisins pour donner en sortie la valeur d'un pixel donné.

2.5 Contre-attaques de l'impression/numérisation

Dans le cadre du tatouage numérique, quelques méthodes dans la littérature ont été proposées afin de corriger les distorsions produites lors l'impression/numérisation [Yu *et al.* 2005, Kundu *et al.* 2006, A. Poljicak *et al.* 2012]. Les auteurs ne donnent pas des expressions statistiques des distorsions de la valeur des pixels, mais ils essaient de trouver des contre-attaques à ces distorsions. Ces contre-attaques sont appliquées après l'opération l'impression/numérisation et avant l'extraction ou la détection du tatouage.

2.5.1 Algorithme de Yu

Yu *et al.* [Yu *et al.* 2005] ont analysé la structure d'une imprimante laser et d'un dispositif de numérisation puis ils ont proposé une contre-attaque aux distorsions produite lors l'opération impression/numérisation. D'abord, ils ont décrit brièvement les différentes sources de distorsion dans le processus d'impression/numérisation, comme illustré dans la figure 2-11.

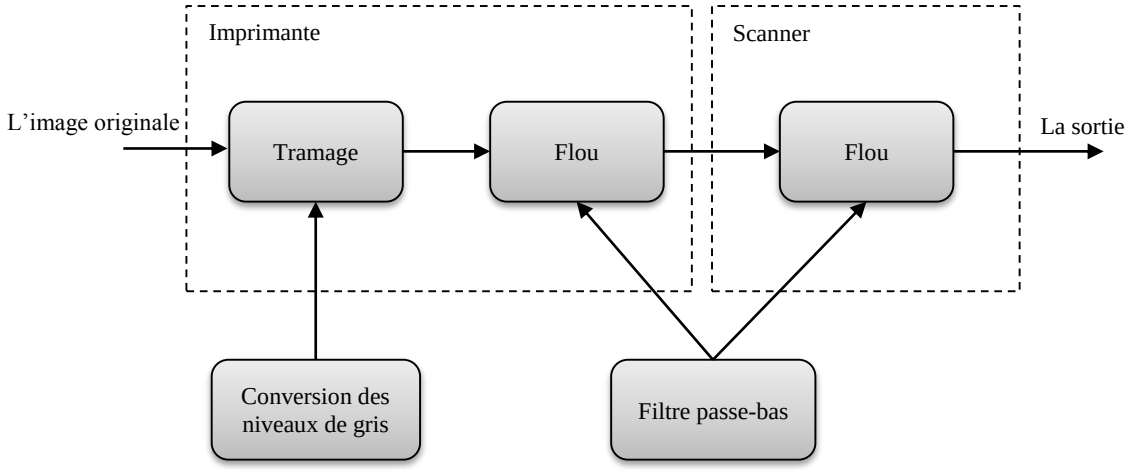


Figure 2-11- Distorsions produites pendent l'impression/numérisation selon Yu *et al.* [Yu *et al.* 2005].

Dans la phase de l'impression, une source de distorsions a été introduite par le système optique pendant la conversion du niveau de l'impulsion électrique vers une impulsion optique. Une autre distorsion appelé l'étalement de point de la trame où "dot gain", cette distorsion étale la poudre de toner de manière non uniforme sur le papier. La distorsion la plus puissante repose sur la génération d'images en demi-teintes, cette distorsion s'est produite avant l'impression. D'après les auteurs, une correction de cette dernière distorsion est obligatoire.

Dans la phase de la numérisation, le système optique introduit un flou Gaussien, il est considéré comme une attaque par filtrage passe-bas. Le bruit thermique et le bruit du courant d'obscurité ont été introduits par les capteurs CCD. D'après les auteurs, les différents types de bruit apparaissent dans le processus de numérisation sont difficiles à corriger, mais peuvent être minimisés en utilisant des scanners à haute résolution.

Yu *et al.* considèrent deux cas pour la contre-attaque de la conversion des niveaux de gris :

- **Sans flou :** cas idéal qui modélise la conversion en niveaux de gris. Dans ce cas l'image en demi-teintes scannée est subdivisée en blocks de taille $M \times N$, selon la dimension de la matrice de conversion utilisée. Chaque bloc est associé à un des ($M \times N + 1$) cellules des demi-teintes. La relation entre le pixel original x et numéros de la cellule de demi-teintes correspondant y est donnée par :

$$x = 256 - (y - 1) \times [256 / (M \times N)] \,. \tag{2-9}$$

- **Avec flou :** Comme dans le cas précédent l'image en demi-teintes est subdivisée en blocs de taille $M \times N$. Chaque bloc est comparée à ($M \times N + 1$) cellules des demi-teintes. Pour associer un bloc à une cellule en demi-teintes correspondante, un critère de minimisation de distance est employé. Chaque pixel original x est alors calculé par l'équation (2-9).

Cette correction réside dans la connaissance de l'algorithme de la génération des images en demi-teintes utilisé lors de l'impression. Finalement, un filtre rehausseur est appliqué à l'image résultante pour corriger le flou.

2.5.2 Algorithme de Kundu

Kundu et Maiti [Kundu *et al.* 2006] ont proposé une contre-attaque basée sur le modèle de Villàn [Villan *et al.* 2006] sans considérer les effets du bruit. Le processus d'impression/numérisation est modélisé par une équation :

$$Y_i = T(X_i), \quad i = 0,\ 1, \cdots 255 \,, \tag{2-9}$$

où X_i, Y_i est respectivement le niveau de gris de pixel avant l'impression et le niveau gris de pixel après la numérisation. T est la transformation produite durant l'opération impression/numérisation, c'est le résultat du passage de tramage (où la génération de l'image en demi-teintes) à l'impression et l'impression à la numérisation.

Les auteurs calculent la forme possible de la fonction de transformation expérimentalement. Finalement, la transformation T résultantes d'un couple particulier d'imprimante/scanner est estimée par la technique d'interpolation polynomiale représentée par l'équation suivante :

$$Y_i = \sum_{j=0}^{r} a_j X_i^j, \quad i = 0, 1, \cdots 255 \quad , \tag{2-10}$$

où a_j sont les coefficients du polynôme. La fonction de transformation inverse de T appelée P est calculée, la figure 2-12 montre le principe de la méthode développée par les auteurs.

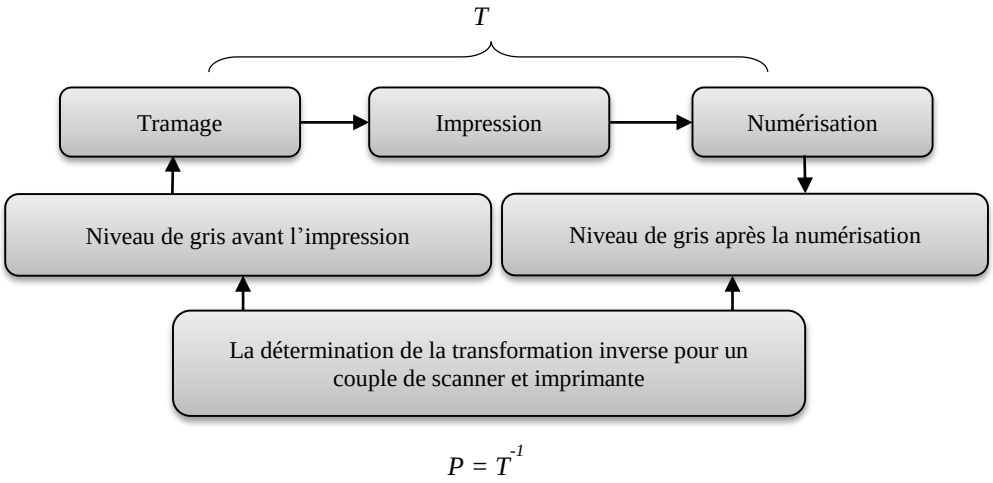


Figure 2-12- Schéma du principe d'impression/numérisation transformation proposé par Kundu [Kundu *et al.* 2006].

Dans la phase du décodage de la marque, la transformation inverse P appliquée à l'image imprimée et scannée juste avant l'extraction du tatouage.

2.5.3 Autres algorithmes

Poljicak *et al.* [A. Poljicak *et al.* 2012] ont proposé un modèle simplifié du processus impression/numérisation. Le modèle peut être considéré comme un filtrage passe-bas, dans lequel les composantes haute fréquence d'une image sont atténuées. Afin de corriger cet effet, les auteurs ont appliqué trois types de filtrage ; le filtre rehausseur « unsharp », le filtre Laplacian et la déconvolution aveugle. Ce modèle sera utilisé par la suite et donc détaillé ultérieurement.

2.6 Conclusion

Nous avons présenté dans ce chapitre les différentes distorsions produites dans la phase d'impression/numérisation, ainsi que les modèles proposés et les solutions développées pour les éliminer ou les réduire. Ces distorsions sont divisées principalement en deux catégories ; les transformations géométriques affectant la position des pixels ainsi les distorsions qui affectent la valeur des pixels. En ce qui concerne les distorsions de la valeur des pixels plusieurs modèles ont été

proposés mais peut de contre-attaque ont été développées. La plupart des travaux dans ce domaine ont porté sur la recherche de différents espaces qui sont robustes à l'impression/numérisation. Les outils d'impression et de numérisation ont été décrits et divisés en catégories principales. Les imprimantes à sublimation thermique sont les plus utilisées dans le domaine industriel pour les supports de carte en plastique. Les modèles de la littérature sont conçues pour travailler avec des imprimantes laser ou des imprimantes à jet d'encre. Cela nécessite une conversion de l'image de niveaux de gris en image binaire avant l'impression. Cette conversion est une attaque très importante dans le processus de l'impression/numérisation, Yu *et al*. ont proposé une contre-attaque pour surmonter ce problème. Dans notre étude, une imprimante à sublimation est utilisée pour imprimer des images d'identité sur des cartes à support en plastique. Ce type d'imprimantes n'utilise pas les algorithmes de conversion en demi-teintes, mais il produit des distorsions supplémentaires que nous verrons dans les prochains chapitres.

Chapitre III :

3 Algorithme de tatouage d'images dans le domaine de la transformée de Fourier

3.1 Introduction

Dans ce chapitre nous allons décrire dans un premier temps une méthode de tatouage dans le domaine de la transformée de Fourier, robuste, imperceptible et avec une détection aveugle. En effet, l'objectif est de présenter la conception d'un système de tatouage des images d'identité robuste aux transformations géométriques, les attaques principales dans l'opération impression/numérisation. Le système présenté est conçu sous forme d'un système de communication composé de deux parties qui sont :

- L'émetteur, ou le fabricant des cartes d'identité dans notre cas, qui a pour rôle d'insérer la marque W dans l'image d'identité. L'image tatouée est imprimée sur le support plastique de la carte d'identité.
- Le récepteur, ou l'autorité correspondante, qui dispose de la marque W, et qui a pour objectif de détecter si un document d'identité est un document non contrefait à partir de l'image d'identité scannée sur ce document.

Le domaine de Fourier a été choisi pour effectuer le tatouage car il présente des avantages très intéressants pour notre application. La rotation de l'image dans le domaine spatial produit une rotation dans le spectre de l'image avec le même angle de rotation. En tatouant l'image de manière circulaire, on peut donc s'affranchir d'une possible rotation.

Dans un deuxième temps, nous essaierons de répondre à la question suivante : pourquoi certaines images sont plus adaptées à l'opération du tatouage que d'autres ? En traitant cette question nous développerons une nouvelle méthode de tatouage basée sur le prétraitement de l'image avant l'insertion de la marque. Ce prétraitement consiste à diminuer la variance du vecteur qui supporte la marque. La réduction de la variance peut être réalisée soit par une modification directe des coefficients dans lesquels la marque sera insérée ou par la sélection judicieuse des coefficients dans lesquels la marque sera insérée.

3.2 Tatouage basé sur la transformée de Fourier

Plusieurs méthodes de tatouage basées sur la transformée de Fourier ont été développées ces dernières années [Solachidis *et al.* 2001], [Ros *et al.* 2006], [Ante Poljicak *et al.* 2011]. Généralement la marque est insérée dans le module des coefficients de la transformée de Fourier de l'image. La figure 3-1 présente un schéma général du tatouage dans le domaine de la transformée de Fourier. Dans un premier temps, la transformée de Fourier est appliquée à l'image originale. Dans le cas des images couleurs seule la luminance est concernée. Puis, la marque est insérée dans certains coefficients du module de la transformée de Fourier de l'image, la phase n'étant pas modifiée. Finalement, l'image tatouée est reconstruite à partir du module tatoué et de la phase en appliquant la transformée de Fourier inverse. La méthode la plus astucieuse pour résister aux rotations est d'insérer une marque circulaire dans le module de la transformée de Fourier. La détection de la marque est effectuée par le calcul de la corrélation croisée entre les coefficients de la marque et le module de la transformée de Fourier de l'image. Dans ce cas, l'image originale n'est pas nécessaire dans la phase de détection. Licks et Jordan [Licks *et al.* 2000] sont les premiers qui ont développé la méthode de l'insertion d'une marque circulaire dans la transformée de Fourier. Poljicak et al. [Ante Poljicak *et al.* 2011] ont proposé l'insertion dans un cercle de rayon optimal qui maximise le PSNR. C'est cette technique que nous allons décrire ci-dessous.

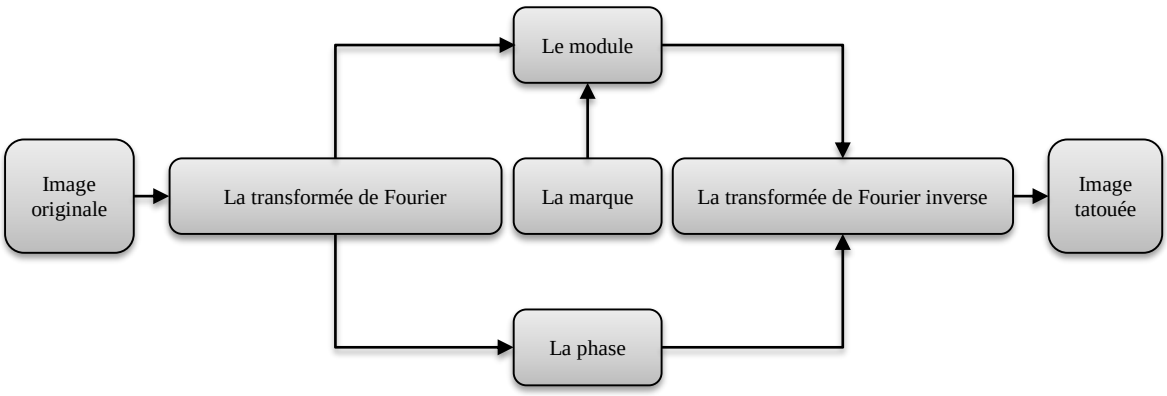


Figure 3-1- Schéma général du tatouage dans le domaine de la transformée de Fourier.

3.2.1 Codage et insertion de la marque

Lors de l'insertion de marque, la luminance de l'image originale est transformée vers le domaine de Fourier. Dans le cas des images couleurs, la luminance est obtenue par une transformation de l'espace des couleurs RVB vers l'espace YCbCr. Une séquence pseudo-aléatoire *v* est générée à l'aide d'une clé secrète *k* qui représente la graine (ou seed en anglais) du générateur pseudo aléatoire de +1 et -1.

Nous obtenons alors un vecteur v de l éléments de moyenne nulle et de variance unité. Connaissant le rayon du cercle où la marque doit être insérée, nous pouvons ainsi créer la marque W en utilisant l'équation suivante :

$$W(x_i, y_i) = v(j)\left[\frac{1}{9}\sum_{s=-1}^{1}\sum_{t=-1}^{1} M(x_i + s, y_i + t)\right], \tag{3-1}$$

avec $W(x_i, y_i)$ qui sont les coefficients de la marque, $v(j)$ représente le $j^{\text{éme}}$ élément de la séquence v, et $M(x_i,y_i)$ sont les coefficients du module de la transformée de Fourier de l'image originale. Pour plus de stabilité, on introduit un lissage du coefficient M avec ses huit voisins comme le montre l'équation 3-1.

Les coordonnées (x_i, y_i) sont définies par:

$$x_i = \left(\frac{m}{2} + 1\right) + round\left(r\cos\left(\frac{j \cdot \pi}{l}\right)\right), \tag{3-2}$$

$$y_i = \left(\frac{n}{2} + 1\right) + round\left(r\sin\left(\frac{j \cdot \pi}{l}\right)\right), \tag{3-3}$$

où m et n représentent la taille de l'image, généralement 512×512, r est le rayon du cercle où la marque sera insérée, l représente la taille du vecteur v, et *round* () désigne la fonction de l'arrondie.

Pour respecter la symétrie hermitienne, la marque est insérée dans le premier demi plan des coefficients du module de la transformée de Fourier de l'image originale, puis une copie de la marque est insérée dans le deuxième demi plan afin de former une marque circulaire et symétrique. La figure 3-2 montre la position de la marque dans le module de la transformée de Fourier. La marque W est insérée en utilisant l'équation suivante :

$$X_W = X_0 + \alpha \times W\,, \tag{3-4}$$

avec X_0 qui désigne les coefficients du cercle de rayon r dans module de la DFT de l'image originale, W représente la marque, α est la force de l'insertion, et X_W représente les coefficients tatoués. Le scalaire α est déterminée afin que le PSNR ait une valeur désirée.

Finalement, l'image est reconstruite en utilisant le module tatoué et la phase intacte par l'application de la transformée de Fourier inverse, afin d'obtenir la luminance de l'image tatouée. Dans le cas des images couleurs, les images sont reconstruites en utilisant la luminance tatouée et les composantes de chrominance non modifiées. La figure 3-3 résume le principe de l'insertion d'une marque dans une image en utilisant la transformée de Fourier.

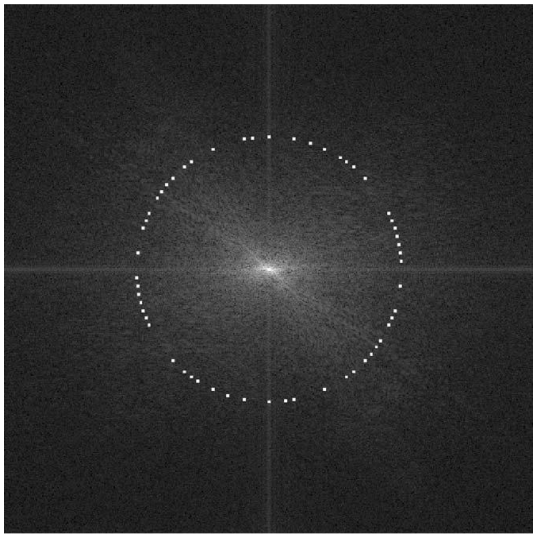


Figure 3-2- Positions des éléments de la marque dans le module de la transformée de Fourier, extrait de [Ante Poljicak *et al.* 2011].

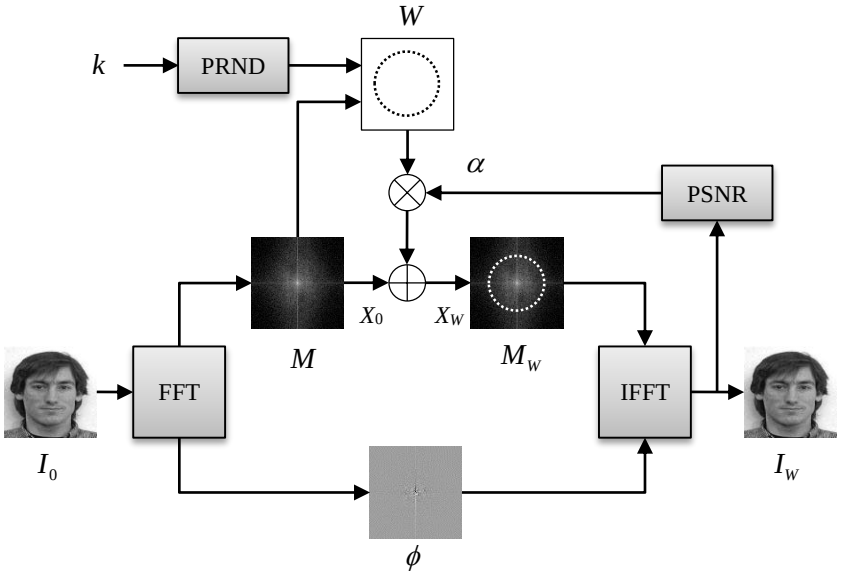


Figure 3-3- Principe de l'insertion d'une marque circulaire dans le domaine de Fourier.

3.2.2 Décodage et détection de la marque

Le décodeur effectue une détection aveugle de la marque. En conséquence, l'image originale n'est pas nécessaire dans la phase de détection. La seule exigence est la clé *k* utilisée dans la phase de l'insertion pour générer vecteur *v* et l'image à tester.

La transformée de Fourier est appliquée à la luminance de l'image, la figure 3-4 présente le schéma de la détection de la marque. Les coefficients de Fourier sont extraits du module de la transformation de Fourier de l'image le long du cercle du rayon *r*. Ensuite, la corrélation croisée normalisée est calculée entre les coefficients extraites X et le vecteur *v*. La corrélation croisée est une méthode standard pour l'estimation du degré dans lequel deux séries sont corrélées. La formule de la corrélation croisée normalisée est la suivante :

$$C_{X_w v}(j) = \frac{\sum_{i=1}^{l-j}(X_{i+j} - \overline{X})(v_i - \bar{v})}{\sqrt{\sum_{i=1}^{l}(X_i - \overline{X})^2 \sum_{t=1}^{n}(v_i - \bar{v})^2}}, \tag{3-5}$$

où $\overline{X}$ et $\bar{v}$ sont les moyens des séries correspondantes, dans notre cas les coefficients extraits et le vecteur *v*, et *l* représente la taille de la marque.

La détection de la marque est positif si la valeur maximale de la corrélation croisée normalisée dépasse un seuil prédéfini *t*, si non la marque est non détectée.

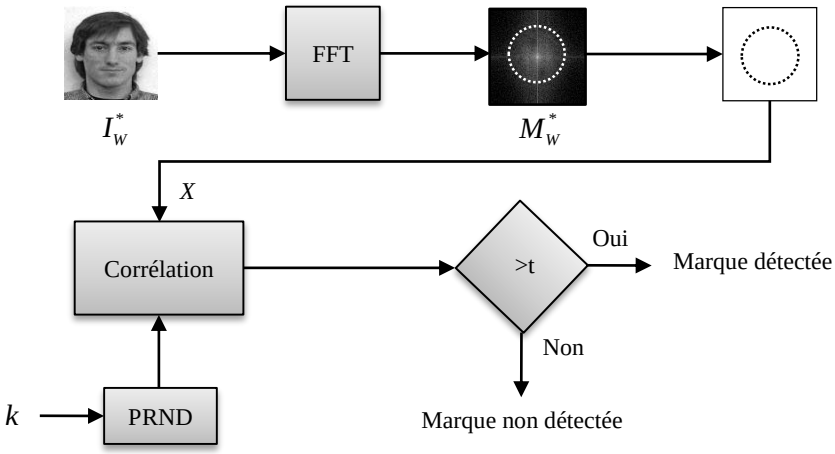


Figure 3-4- Principe de la détection de la marque dans le domaine de Fourier.

3.2.3 Influence des paramètres du tatouage sur la qualité visuelle de l'image tatouée

Dans cette section nous présentons une évaluation de l'influence des paramètres du tatouage sur la qualité visuelle des images tatouées. L'influence du tatouage sur la qualité de l'image dépend essentiellement de la taille du vecteur de la marque, la gamme des fréquences où la marque est insérée, et la force de l'insertion. Nous nous inspirons donc de la méthode proposée par Poljicak *et*

al. [Ante Poljicak *et al.* 2011] pour caractériser les modifications apportées aux images de la base utilisée dans ce travail après le tatouage.

Pour déterminer la façon dont chaque paramètre affecte la qualité visuelle de l'image tatouée, Poljicak *et al.* ont conçu une expérience où l'un des paramétrés varie tandis que les autres ont été fixés. Trois paramètres ont été contrôlés pendant l'expérience: la force de l'insertion α, le rayon r du cercle où la marque est insérée, et l la taille du vecteur de la marque. Les images ont été tatouées en utilisant la méthode présentée précédemment. La qualité des images tatouées a été évaluée avec deux métriques très utilisées dans le domaine de la vision, le PSNR et le MSSIM. Les deux métriques ont été calculées pour les différentes valeurs de chaque paramètre, tandis que les deux autres ont été maintenus constants.

La première partie de l'expérience consiste à évaluer l'influence de la force de l'insertion α sur la qualité de l'image après le tatouage. Dans cette expérience, la force de l'insertion α varie de 0 à 30, tandis que le rayon r a été fixé à 128 et la taille du vecteur de la marque l à 50. Dans la deuxième partie de l'expérience, la taille de la marque l varie entre 1 et 400, alors que la force α est fixée à 3 et le rayon r à 128. Pour la troisième partie, le rayon r varie dans un intervalle de 25 à 250, la force de l'insertion α est fixée à 3 et la taille de la marque l à 50. La figure 3-5 montre l'influence des paramètres du tatouage sur la qualité visuelle d'une image sélectionnée aléatoirement de la base des images d'identité. Les résultats sur d'autres images sont similaires.

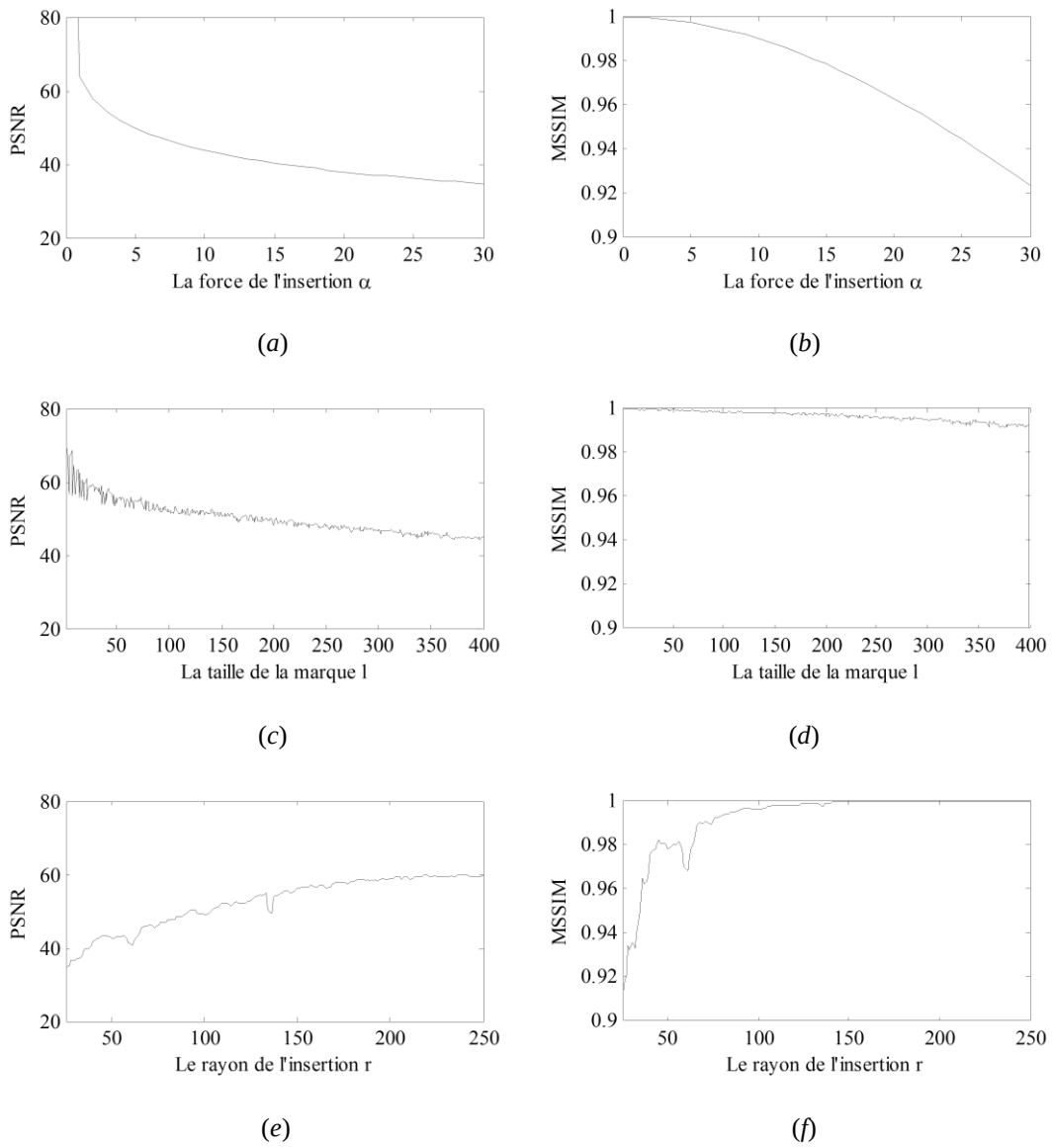


Figure 3-5- Influence des paramètres du tatouage sur la qualité visuelle d'une image de la base des images d'identité.

D'après les figures 3-5-a et 3-5-b, on remarque qu'avec l'augmentation de la force α, le PSNR et MSSIM diminuent de façon monotone. Cependant, la force α est inversement proportionnelle à la qualité visuelle de l'image. Pour les petites valeurs de la force de l'insertion, le PSNR diminue d'abord rapidement, puis cette diminution ralentit. Généralement, pour des grandes valeurs de la force de l'insertion, une image tatouée est plus robuste aux attaques, mais il est plus facile de percevoir la marque insérée dans l'image.

Les figures 3-5-c et 3-5-d montrent que la taille de la marque a aussi une influence sur la qualité de l'image tatouée. Pour les images issues de la base utilisée dans ce travail, la taille de la marque affecte

la qualité des images tatouées. Les valeurs du PSNR et du MSSIM diminuent à mesure que la taille est augmentée. Cependant, pour des petites valeurs de la taille de la marque, il y a des fluctuations de la valeur du PSNR. Lorsque la taille de la marque augmente, les fluctuations sont de moins en moins notables. Par contre les valeurs du MSSIM sont plus ou moins stables et diminuent avec l'augmentation de la taille de la marque. En général, la taille de la marque insérée dans l'image, n'a pas un effet significatif sur la qualité visuelle de l'image tatouée.

Le rayon de l'insertion est un paramètre très important dans le tatouage basé sur la transformée de Fourier. Les résultats présentés dans les figures 3-5-e et 3-5-f montrent qu'avec l'augmentation de la valeur du rayon, les valeurs du PSNR et du MSSIM augmentent. Cependant, il existe des rayons pour lesquelles les valeurs du PSNR et du MSSIM sont imprévisibles ; pour certains rayons la dégradation est faible, tandis que pour d'autres rayons la dégradation est plus forte que prévue. Même pour des valeurs de rayon proches nous pouvons distinguer des qualités visuelles différentes. Alors on peut constater qu'il existe des rayons qui sont plus appropriés pour l'insertion. Poljicak *et al.* [Ante Poljicak *et al.* 2011] ont utilisé ce constat pour développer une méthode basée sur la recherche du rayon de l'insertion, dit optimal qui minimise la dégradation produites lors de l'insertion de la marque.

3.3 Prétraitement avant l'insertion

Dans la plupart des méthodes de tatouage nous pouvons remarquer que certaines images sont naturellement plus appropriées pour recevoir le tatouage que d'autres images même si les images ont été tatouées par la même méthode en utilisant les mêmes paramètres. Dans certains cas, la différence de niveau peut être relativement élevée, même si les images sont issues d'une même base. Autrement dit les performances d'une méthode de tatouage sont fortement dépendantes des documents auxquels elle est appliquée [Ingemar J. Cox *et al.* 2004]. Cela conduit naturellement à la question d'appliquer un prétraitement intelligent aux images avant le processus du tatouage afin d'obtenir des résultats comparables. Par ailleurs, il existe des méthodes de tatouage qui utilisent un prétraitement basé sur la normalisation d'image [Dong *et al.* 2005], [Nasir *et al.* 2012]. Dans ces approches l'insertion et la détection de la marque ont été effectuées en utilisant une image normalisée ayant une taille et orientation standard. L'image normalisée est obtenue à partir d'un procédé de transformations géométriques qui est invariant à des distorsions géométriques globales. Cette approche n'a pas l'objectif d'améliorer le taux de détection, par contre elle permet de faciliter le processus du tatouage dans le cas des distorsions géométriques globales.

Dans ce travail, nous proposons une stratégie préventive pour le système de tatouage présenté dans la section précédente. Cette méthode est basée principalement sur une phase de prétraitement appliquée avant la phase de l'insertion de la marque. Dans un premier temps, nous présentons les

justifications théoriques et expérimentales de l'approche proposée. Puis, nous testons les performances de cette approche sous différentes attaques.

3.3.1 Justification théorique et expérimentale

Dans cette section nous montrons que la mesure de détection est fortement liée aux certaines caractéristiques de l'image porteuse de la marque. Dans notre cas, la marque est insérée dans le module de la transformée de Fourier, et plus précisément le long d'un cercle de rayon optimal. Dans la phase de détection de la marque un vecteur X extrait du module de la DFT est comparée au vecteur de la marque W, pour obtenir une mesure de détection C. Cette mesure de détection est comparée à un seuil t, et le résultat de cette comparaison détermine si la marque est présente dans l'image ou non. Il est clair que si la mesure de détection est plus grande, alors la probabilité que la marque est présente dans l'image est plus importante.

Selon Miller et Bloom [Miller *et al.* 2000], trois types des mesures de détection ont été utilisés dans la phase de détection de la marque : la corrélation linéaire, la corrélation normalisée et le coefficient de corrélation. Le coefficient de corrélation est considéré dans ce travail comme référence de la mesure de détection. Il fournit une bonne robustesse contre les variations de la composante moyenne de l'image [Ingemar Cox *et al.* 2007]. Le coefficient de corrélation C peut s'exprimer en termes des moments non centré comme suit :

$$C = \frac{\mathrm{cov}(X,W)}{\sqrt{\sigma_X^2 \sigma_W^2}} = \frac{\mathrm{E}[(X-\mu_X)(W-\mu_W)]}{\sqrt{\mathrm{E}[(X-\mu_X)^2]\mathrm{E}[(W-\mu_W)^2]}}, \tag{3-6}$$

où la fonction cov() représente la covariance, σ_X et σ_W sont l'écart type respectivement de X et W, μ_X et μ_W représentent les moyenne respectivement de X et W, et E[] désigne l'espérance mathématique.

3.3.1.1. Contexte théorique

Le récepteur est face à trois situation lors la phase du décodage ; image non tatouée (cas 1), image tatouée par une marque W (cas 2), ou une image tatouée par une marque W^* différent de la marque W utilisée par le décodeur (cas 3). Dans la suite nous analysons le coefficient de corrélation dans chaque cas.

Cas 1 : *L'image est non tatouée*.

Si le récepteur reçoit une image non tatouée, le décodeur calcule le coefficient de corrélation entre le vecteur de la marque W et le vecteur X extrait de l'image non tatouée. Dans ce cas, le vecteur X ne contient pas la marque, en conséquence, X et W sont statistiquement indépendants donc leur

covariance est nulle et la quantité dans le numérateur de l'équation (3-6) est égale à zéro. Alors, la mesure de détection *C* est nulle.

Cas 2 : *L'image est tatouée avec W.*

Dans ce cas le vecteur *X* extrait de l'image tatouée contient la marque *W*. il s'écrit sous la forme suivant ; $X = X_0 + \alpha W$, où X_0 désigne le vecteur des coefficients le long du cercle dans le module de DFT de l'image avant l'insertion et α représente la force de l'insertion. Nous pouvons démontrer dans le cas où l'image contient la marque *W* que le coefficient de corrélation est inversement proportionnel à la variance du vecteur X_0.

Preuve 1 :

A partir de l'équation (3-6), il se trouve que le coefficient de corrélation peut s'écrire dans le cas d'une image tatouée avec la marque *W* comme suite :

$$C = \frac{\mathrm{E}[(X_0 + \alpha W - \mu_{X_0} - \alpha\mu_W)(W - \mu_W)]}{\sqrt{\mathrm{E}[(X_0 + \alpha W - \mu_{X_0} - \alpha\mu_W)^2]\mathrm{E}[(W - \mu_W)^2]}}. \tag{3-7}$$

Après un simple calcule d'arithmétique, en tenant compte les propriétés de l'espérance mathématique, nous obtenons l'équation suivante :

$$C = \frac{\mathrm{E}[(X_0 - \mu_{X_0})(W - \mu_W)] + \alpha\mathrm{E}[(W - \mu_W)^2}{\sqrt{(\mathrm{E}[(X_0 - \mu_{X_0})^2] + 2\alpha\mathrm{E}[(X_0 - \mu_{X_0})(W - \mu_W)] + \alpha^2\mathrm{E}[(W - \mu_W)^2])\mathrm{E}[(W - \mu_W)^2]}}. \tag{3-8}$$

Le vecteur extrait de l'image originale X_0 et le vecteur des éléments de la marque *W* sont statistiquement indépendants, cela conduit à : $\mathrm{E}[(X_0 - \mu_{X_0})(W - \mu_W)] = 0$, alors le coefficient de corrélation s'écrit :

$$C = \frac{\alpha \times \mathrm{E}[(W - \mu_W)^2}{\sqrt{(\mathrm{E}[(X_0 - \mu_{X_0})^2] + \alpha \times \mathrm{E}[(W - \mu_W)^2])\mathrm{E}[(W - \mu_W)^2]}}. \tag{3-9}$$

Notons que : $\sigma_A^2 = \mathrm{E}[(A - \mu_A)^2]$, alors l'expression de coefficient de corrélation s'écrit sous la forme :

$$C = \frac{\alpha\sigma_W^2}{\sqrt{(\sigma_{X_0}^2 + \alpha^2\sigma_W^2)\sigma_W^2}} = \frac{1}{\sqrt{\frac{\sigma_{X_0}^2}{\alpha^2 \times \sigma_W^2} + 1}}, \quad (3\text{-}10)$$

où $\sigma_{X_0}^2$ et σ_W^2 représentent la variance respectivement de X_0 et W.

L'équation (3-10) montre que le coefficient de corrélation est inversement proportionnel à la variance du vecteur X_0. Si la variance du vecteur X_0 tend vers zéro, alors le coefficient de corrélation C est tends vers 1. Plus la variance du vecteur X_0 est petite, plus le coefficient de corrélation est grand.

<u>Cas 3</u> : *L'image est tatouée avec W**.

Ce cas peut être considéré comme une attaque malveillante, où le récepteur reçoit une image tatouée par une marque W^* générée avec une mauvaise clé. Donc le vecteur extrait de l'image tatouée prend la forme suivante ; $X = X_0 + \alpha W^*$. Si le décodage est effectué avec la marque W, le coefficient de corrélation s'écrit sous la forme suivante :

$$C^* = \frac{\mathrm{E}[(X_0 + \alpha W^* - \mu_{X_0} - \alpha\mu_{W^*})(W - \mu_W)]}{\sqrt{\mathrm{E}[(X_0 + \alpha W^* - \mu_{X_0} - \alpha\mu_{W^*})^2]\mathrm{E}[(W - \mu_W)^2]}}. \quad (3\text{-}11)$$

Nous pouvons démontrer que le coefficient de corrélation C^* dans ce cas, tend vers zéro indépendamment de la variance du vecteur X_0.

Preuve 2 :

Après quelque calcules arithmétiques nous obtenons l'équation suivante :

$$C^* = \frac{\mathrm{E}[(X_0 - \mu_{X_0})(W^* - \mu_{W^*})] + \alpha\mathrm{E}[(W^* - \mu_{W^*})(W - \mu_W)]}{\sqrt{(\mathrm{E}[(X_0 - \mu_{X_0})^2] + 2\alpha\mathrm{E}[(X_0 - \mu_{X_0})(W^* - \mu_{W^*})] + \alpha^2\mathrm{E}[(W^* - \mu_{W^*})^2])\mathrm{E}[(W - \mu_W)^2]}}. \quad (3\text{-}12)$$

Les vecteurs des deux marques W et W^* sont statistiquement indépendantes alors leur covariance est nulle, la marque W^* et le vecteur X_0 sont aussi indépendantes alors :

$$\mathrm{E}[(X_0 - \mu_{X_0})(W^* - \mu_{W^*})] = 0.$$

Par conséquent, le coefficient de corrélation est nul quel que soit la valeur de la variance du vecteur X_0.

3.3.1.2 Illustration expérimentale

Pour illustrer le concept présenté dans l'équation (3-10), nous considérons le schéma de tatouage basée sur la transformée de Fourier décrit dans les sections précédentes. Un ensemble d'images sélectionnées aléatoirement dans notre banque de 1000 images d'identité. Les images sont redimensionnées à 512 × 512 pixels puis tatouées en utilisant une force d'insertion constante $\alpha = 3$. La taille de la marque est $l = 180$ éléments. Ensuite, le coefficient de corrélation est calculé à partir des images tatouées. La figure 3-6 illustre la relation entre le coefficient de corrélation C et les variances des vecteurs extraites à partir de l'ensemble des images avant le tatouage. Les résultats expérimentaux ont été comparés avec les valeurs théoriques du coefficient de corrélation obtenues par l'équation (3-10). La figure 3-6 montre que les valeurs de coefficient de corrélation obtenues expérimentalement correspondent bien aux ceux obtenues théoriquement.

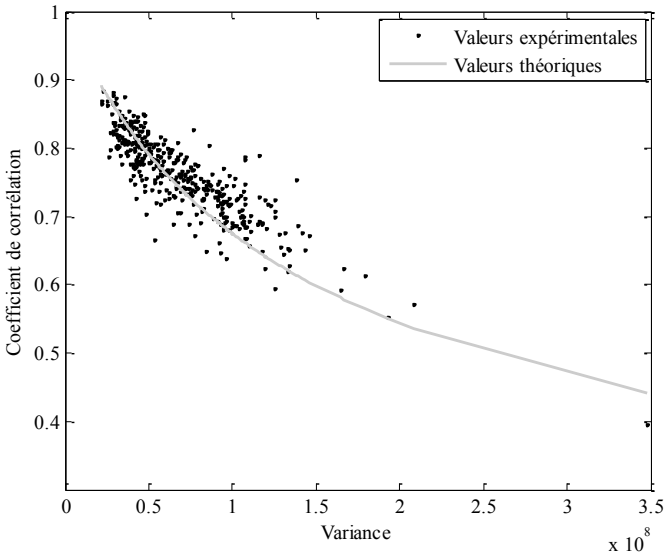


Figure 3-6- La relation entre le coefficient de corrélation et la variance du vecteur X_0

D'après les résultats présentées dans la figure 3-6, nous pouvons remarquer que la mesure de détection est meilleure si la variance de du vecteur X_0 est faible. Pour les images utilisées dans ce test, le coefficient de corrélation C prend la valeur 0.88 lorsque la valeur de la variance est de 2.28×10^7 par contre C prend la valeur 0.39 si la variance prend la valeur 3.47×10^8. Lorsqu'il n'y a pas de marques dans les images, C tend vers zéro quelles que soient les valeurs de la variance du vecteur X_0.

3.3.2 Méthodes proposées

Pour une image tatouée, le coefficient de corrélation prend des valeurs proches à la valeur 1 si la variance de X_0 tend vers zéro. Donc, il est évident que l'insertion de la marque dans un vecteur avec une faible variance conduit à une mesure de détection C élevée ce qui est favorable pour réduire les erreurs. Dans la suite nous présentons deux méthodes pour réduire la variance du vecteur X_0. La première méthode proposée dans ce travail consiste à modifier directement les coefficients du cercle de rayon optimal r_0 en appliquant un filtre passe-bas avant l'insertion de la marque. La seconde consiste à sélectionner les éléments un vecteur pour l'insertion de la marque, de sorte que sa variance soit la plus faible possible.

3.3.2.2 Filtrage des coefficients de l'insertion

A. Présentation de la méthode

Afin d'améliorer le taux de détection, il est suggéré que l'image originale soit prétraitée avant la phase de l'insertion de la marque. Ce prétraitement consiste à diminuer la variance des coefficients sélectionnés pour l'insertion. La marque est insérée dans des coefficients du module de la DFT le long d'un cercle de rayon optimal r_0. Alors les coefficients le long du cercle de rayon r_0 sont filtrés en utilisant un filtre passe bas avant l'insertion de la marque. Notons que la longueur de la marque est limitée à 180 éléments.

B. Algorithme de la méthode

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

1. La FFT de la luminance de l'image est calculée.
2. Les basses fréquences sont déplacées vers le centre du module de la transformée de Fourier.
3. Le rayon optimale r_0 qui maximise le PSNR est déterminé dans un intervalle $[r_{\min}, r_{\max}]$.
4. Un filtre gaussien d'un écart-type σ est appliqué aux coefficients X_0 de l'amplitude de la transformée de Fourier le long du cercle de rayon r_0 pour obtenir les coefficients filtrées X_f.
5. La force de l'insertion α est adaptée à chaque image d'une manière à obtenir un niveau fixe de qualité visuelle.
6. La marque circulaire W est insérée dans les coefficients filtrés X_f du module de la FFT de la luminance d'une image selon l'équation suivante :

$$X_W = X_f + \alpha \times W \,. \tag{3-13}$$

7. L'image tatouée finale est reconstruite par l'application de la FFT inverse pour obtenir la luminance pour les images couleur, puis une conversion vers l'espace couleur RBG est appliquée.

Le PSNR est calculé entre l'image originale avant le prétraitement et l'image finale après le tatouage. La figure 3-7 présente le block diagramme de la phase d'insertion.

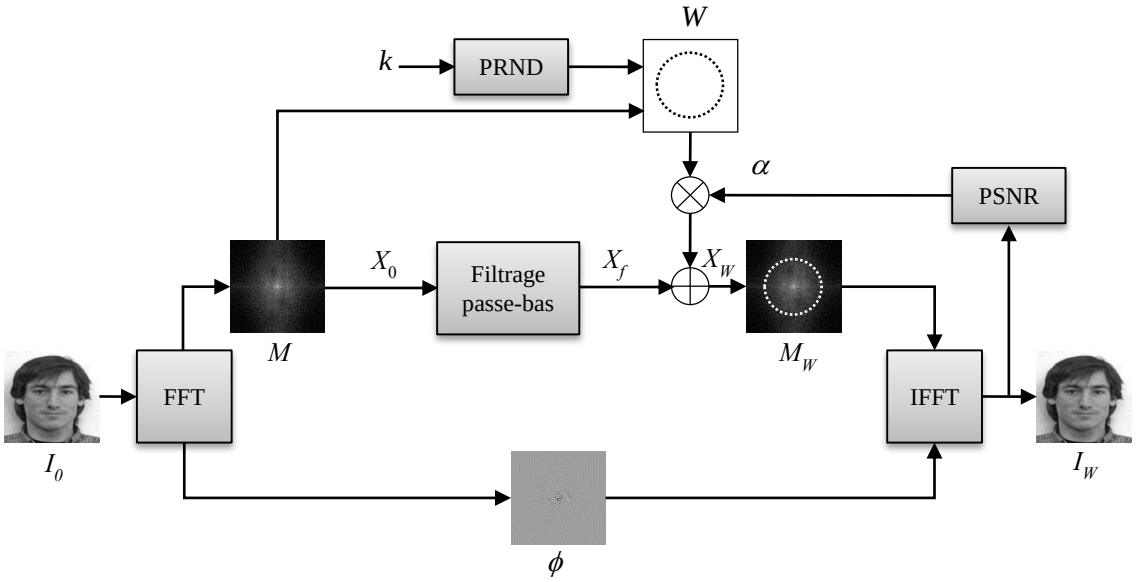


Figure 3-7- Schéma modifié de l'insertion de la marque dans les coefficients filtrés

C. Paramètres de l'insertion

Pendant la phase de l'insertion, il est nécessaire de déterminer les différents paramètres (l, α, r_0, σ) pour atteindre la valeur désirée du PSNR. La taille de la marque a été fixée à 180 éléments. La force de l'insertion a été choisie d'une maniéré itérative afin d'obtenir une valeur du PSNR = 40dB, le rayon de l'insertion a été cherché dans un intervalle dans la gamme des moyennes fréquences avec r_{min} = 60 et r_{max} = 120. La force de l'insertion et le rayon optimale ont été déterminés pour chaque image, par contre l'écart-type σ du filtre a été choisi pour l'ensemble des images de la base utilisé dans ce travail de sorte qu'il respecte les contraintes suivantes :

- Il doit avoir une valeur petite pour que les dégradations soient faibles,
- Il donne un meilleur taux de détection (une mesure de détection forte).

Une phase préliminaire est obligatoire afin de chercher la valeur désirée de σ du filtre pour un ensemble d'images de la base. L'expérience consiste à tatouer un ensemble d'images prétraitées par des filtres Gaussiens avec différentes valeurs de σ. Les résultats de la détection ont été présentés dans

la figure 3-8, ils représentent la moyenne de la mesure de détection en fonction de la valeur de l'écart-type du filtre utilisée. D'après ces résultats, la mesure de détection augmente rapidement avec la valeur l'écart-type et se stabilise à pour atteindre une valeur constante comme présenté sur la figure 3-8. Le filtre choisi est celui avec un écart-type $\sigma = 2$.

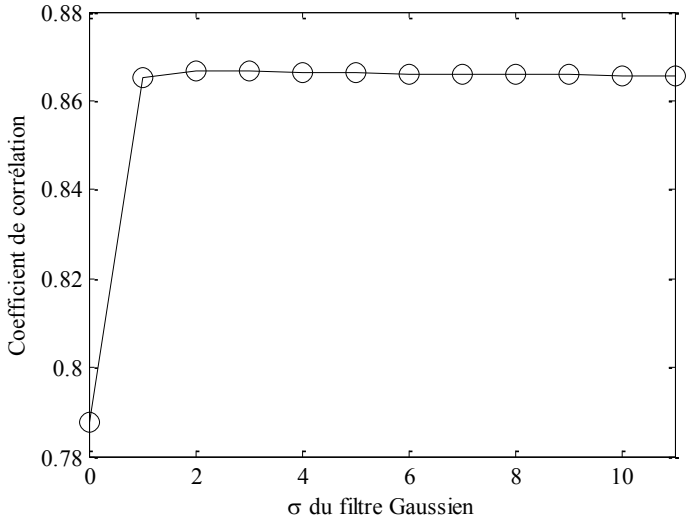


Figure 3-8- Coefficient de corrélation en fonction de l'écart-type du filtre Gaussien

D. Impacte du prétraitement sur la qualité visuelle

La modification des coefficients dans le module de la transformée de Fourier produit une modification de l'image dans le domaine spatial. Le prétraitement proposé consiste à appliquer un filtre Gaussien d'un écart-type égale à 2 aux coefficients le long du cercle d'un rayon optimal r_0 dans le module de la DFT avant l'insertion. Deux points peuvent être considérés :

- Les coefficients à modifier se situent dans la région des moyennes fréquences,
- La quantité des coefficients modifiés n'altèrent pas la qualité visuelle de l'image.

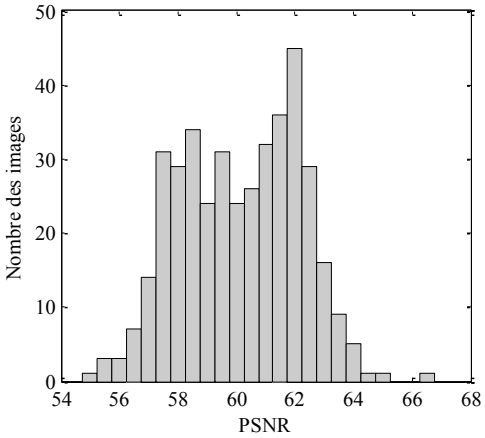
La figure 3-9 montre l'effet du respect des deux points ci-dessus. En effet, la qualité de l'image est préservée et aucune différence n'est perceptible entre l'image originale et l'image après le prétraitement.

Image originale

Image après prétraitement

Figure 3-9- Image originale et image après prétraitement (modification de 180 coefficients).

Pour évaluer la distorsion engendrée à cause du prétraitement applique à l'image originale nous avons utilisé deux paramètres populaires en traitement d'image. Il s'agit du PSNR (Peak Signal to Noise Ratio) et la mesure de similarité MSSIM. Un ensemble d'images de la base ont été utilisés pour ce test, la figure 3-10 présente l'histogramme des valeurs de PSNR et de MSSIM calculées entre les images originales et les images après le prétraitement. Les resultats montrent que le prétraitement n'affecte pas beaucoup la qualité visuelle de l'image, la moyenne des valeurs du PSNR est de 60.14 dB et celle du MSSIM est 0.9986.



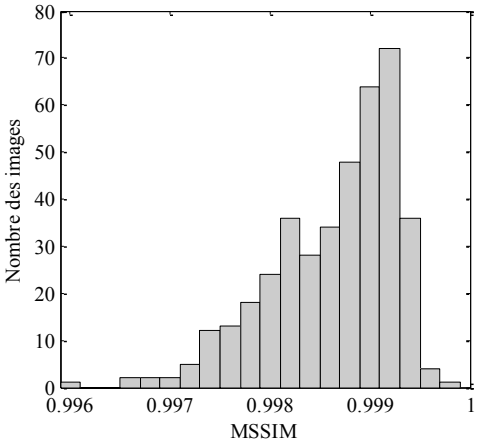


Figure 3-10- Histogrammes des valeurs de PSNR et de MSSIM des images après le prétraitement.

Notons que dans la phase d'insertion de la marque, la force de l'insertion est choisie de manière à avoir une valeur du PSNR égal à 40 dB. Cette valeur est calculée à partir de l'image originale avant le prétraitement et l'image finale après tatouage.

3.4.2.3. Sélection des coefficients de l'insertion

A. Présentation de la méthode

Dans le même but de diminuer la variance des coefficients d'insertion de la marque, nous avons proposé une autre alternative. Cette approche consiste à sélectionner des coefficients à partir du module de la transformée de Fourier de telle sorte que leur variance soit la plus faible possible. Ces coefficients se situent dans une bande entre deux cercles de rayons $r_{\min}$ et $r_{\max}$ dans le module de la DFT (voir figure 3-11). Cette bande appartient aux moyennes fréquences pour avoir un bon compromis entre l'invisibilité et la robustesse de la marque. Puis l'insertion de la marque est effectuée dans les coefficients sélectionnés.

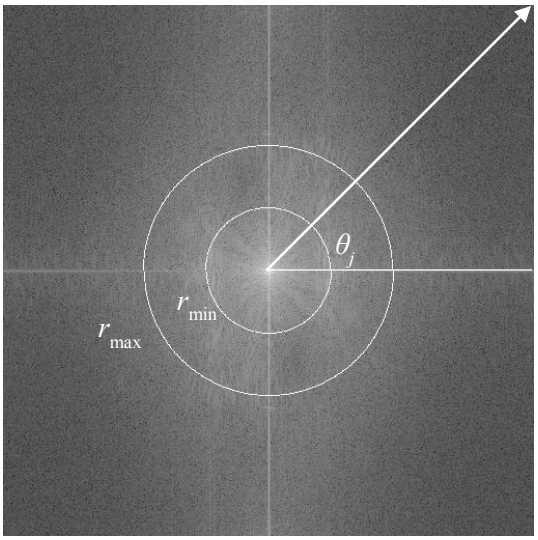


Figure 3-11- Région de la recherche des coefficients de l'insertion de la marque

B. Algorithme de la méthode

L'algorithme proposé se déroule comme suit :

1. La FFT de luminance de l'image est calculée.
2. Les basses fréquences sont déplacées vers le centre du module de la transformée de Fourier.
3. La moyenne des coefficients situés entre les deux cercles de rayons $r_{\min}$ et $r_{\max}$ est calculée.
4. Pour chaque direction θ_j radiale, le coefficient sélectionné est celui dont la valeur la plus proche de la valeur moyenne calculée précédemment. La figure 3-12 montre les positions des coefficients sélectionnés dans le module de la DFT.
5. La force de l'insertion α est déterminée pour obtenir une valeur du PSNR souhaitée.

6. La marque circulaire W est insérée dans les coefficients sélectionnés X_s du module de la DFT la luminance d'une image selon l'équation suivante :

$$X_W = X_s + \alpha \times W \ . \tag{3-14}$$

7. L'image tatouée finale est reconstruite par l'application de la transformée de Fourier inverse pour obtenir la luminance pour les images couleur, puis une conversion vers l'espace couleur RBG est appliquée.

La figure 3-13 présent le block diagramme de l'insertion de la marque dans les coefficients.

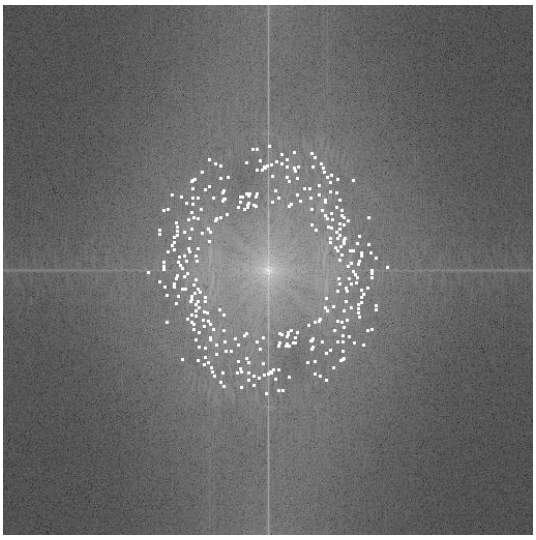


Figure 3-12- Coefficients sélectionnés pour l'insertion de la marque dans le module de la DFT.

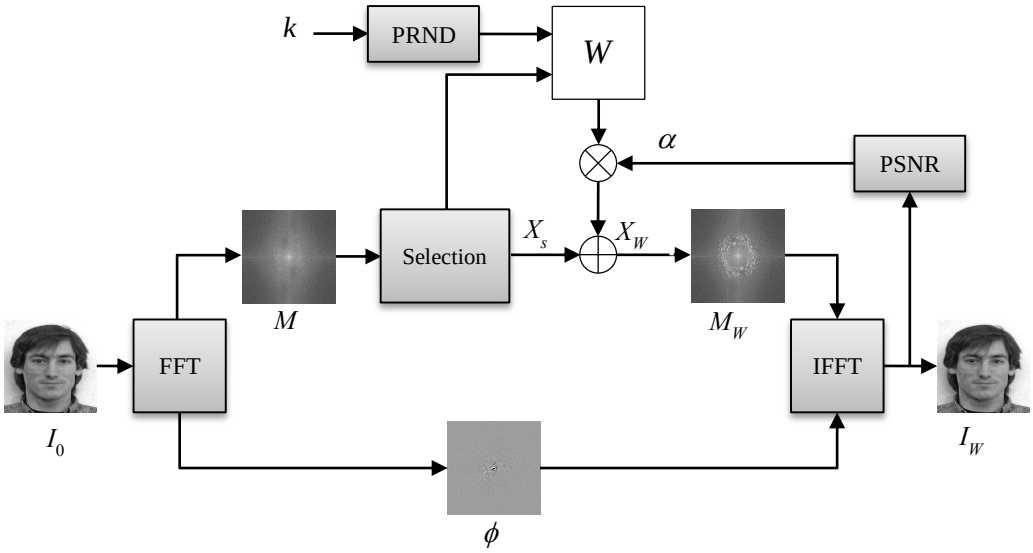


Figure 3-13- Block diagramme de l'insertion de la marque dans les coefficients sélectionnés.

3.3.3 Détection de la marque

En théorie de la détection, le problème de détection de la marque est souvent formulé sous forme du problème de test d'hypothèse classique :

- H_0 (l'hypothèse nulle): l'image ne contient pas de marque ;
- H_1 (l'hypothèse alternative): l'image contient la marque ;

La décision doit être prise sur la base des observations d'un ensemble d'images tatouées et non tatouées. Une solution classique consiste à minimiser le risque bayésien [Nguyen 2011]. Cette minimisation conduit à une décision basée sur le rapport de vraisemblance (ou le rapport de vraisemblance logarithmique) $L(C)$ définie comme ci-dessous :

$$L(C) = \frac{p(C \mid H_1)}{p(C \mid H_0)}, \tag{3-15}$$

où $p(C \mid H_i)$ est la densité de probabilité du C sous l'hypothèse H_1. Un exemple des densités de probabilité sous H_0 et H_1 est présenté dans la figure 3-14.

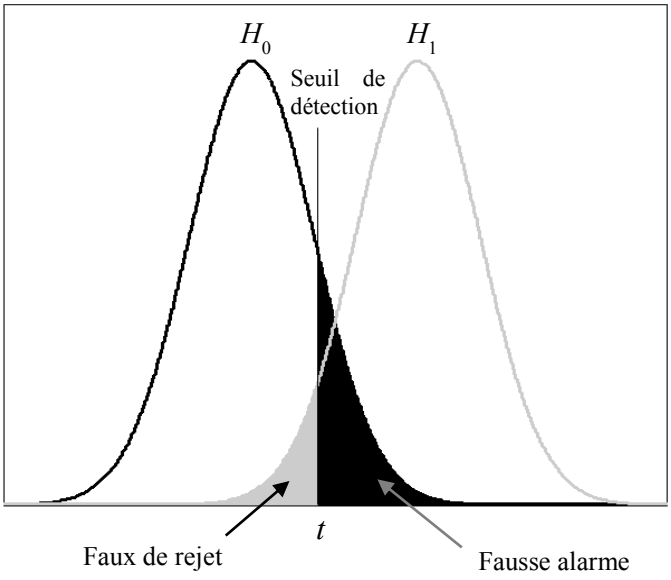


Figure 3-14- Illustration des fonctions de densité de probabilité (PDF) de la sortie du détecteur sous des hypothèses H_0 et H_1.

A partir de cette formulation, la décision est prise en comparant le rapport de vraisemblance à un seuil de détection t. En général, le calcul de L nécessite une caractérisation complète de la distribution statistique du C (le coefficient de corrélation dans notre cas), les coefficients de marque, la méthode de l'insertion ainsi que le comportement des attaques ce qui impossible dans la pratique.

Les détecteurs optimaux, proposés dans la littérature ont été obtenues sous des hypothèses simplistes tels que dans les canaux à bruit blanc gaussien additif AWGN où à la fois les coefficients d'accueil de la marque et les attaques sont modélisés comme des processus blancs gaussiens [Mauro Barni *et al.* 2004]. Cette hypothèse a été prouvée irréalisable dans un certain nombre de travaux [Mitrea *et al.* 2004], [Briassouli *et al.* 2004], [Cheng *et al.* 2001] où les coefficients de la DCT sont modélisés par une distribution gaussienne généralisée (GGD) et les coefficients de la DFT suivent une distribution de Weibull. Cependant, ces conditions sont aussi impraticables et permettent seulement l'évaluation de l'efficacité plutôt que l'évaluation robustesse du système de tatouage.

Dans notre cas, l'insertion est effectuée dans le module de la transformée de Fourier et la détection est effectuée par le calcul du coefficient de corrélation. Pour tester la présence de la marque dans une image, le coefficient de corrélation est calculé pour chaque angle θ_j dans un intervalle $[\theta_{\min}, \theta_{\max}]$. Soit X_j les coefficients tatoués (éventuellement attaqués) et W les éléments de la marque, le coefficient de corrélation entre eux est défini comme suit :

$$C(j) = \frac{\mathrm{cov}(X_j, W)}{\sqrt{\sigma_{X_j}^2 \sigma_W^2}}. \tag{3-16}$$

La valeur finale est alors définie comme la valeur maximale des coefficients de corrélation calculés pour chaque angle θ_j dans l'intervalle $[\theta_{\min}, \theta_{\max}]$:

$$C_{\max} = \max_j \{C(j)\}. \tag{3-17}$$

Si l'image ne contient pas de marque le coefficient de corrélation prend des valeurs proches de zéro, car X et W sont supposées statistiquement indépendants. Par contre si l'image contient la bonne marque le coefficient prend une valeur différente de zéro. En conséquence, la sortie de détection sous H_0 et H_1 sont différentes. La décision entre ces deux hypothèses peut être effectuée par une comparaison de la valeur du coefficient de corrélation avec à un seuil prédéfini.

Le choix du seuil est effectué en fonction de certains critères liés à l'application envisagée, soit par minimisation du faux de rejet (se produit lorsque le détecteur indique l'absence de la marque dans l'image tatouée) et de la fausse alarme (se produit lorsque le détecteur indique la présence de la marque dans l'image non tatouée) ou de trouver un compromis entre eux. Cependant, l'analyse du faux rejet est souvent difficile puisque il nécessite une modélisation de l'attaque ainsi que la méthode d'insertion. Il est donc préférable de travailler avec la fausse alarme. Le seuil est finalement défini en fixant la probabilité de fausse alarme (appelé aussi critère de Neyman-Pearson). La probabilité de fausse alarme est définie par l'équation suivante :

$$P_{fa} = P(C_{\max} > t \mid H_0) = \int_t^{+\infty} pdf(H_0), \tag{3-18}$$

où $C_{\max}$ est la valeur de détection obtenue par le détecteur appliqué sur une image non tatouée sélectionné de façon aléatoire et t représente le seuil de détection. L'indice *max* spécifie la valeur maximale de détection calculée sur tous les angles θ_j dans l'intervalle $[\theta_{\min}, \theta_{\max}]$.

Dans le cas où la valeur de détection est le maximum des J valeurs de coefficient de corrélation différentes, la probabilité de la fausse alarme s'écrit selon Lin *et al.* [C. Y. Lin *et al.* 2001] sous la forme :

$$\begin{aligned} P_{fa} &= P(C_{\max} > t \mid H_0) \\ &= P(C_1 > t \mid H_0) \text{ ou } P(C_2 > t \mid H_0) \text{ ou } \cdots P(C_J > t \mid H_0), \end{aligned} \tag{3-19}$$

Où $C_1 \ldots C_J$ sont les J coefficients de corrélation calculés pour chaque angles θ_j.

Le calcul de la probabilité de fausse alarme nécessite l'utilisation d'un modèle théorique du comportement du système de tatouage. Le modèle le plus utilisé dans le cas du tatouage basé sur la DFT tel que dans [C. Y. Lin *et al.* 2001] et [Ante Poljicak *et al.* 2011] est le modèle proposé par Miller et Bloom [Miller *et al.* 2000]. Ce modèle montre que, si le coefficient de corrélation C entre

une marque de dimension L et un vecteur extrait d'une image non tatouée, la probabilité de détection de fausse alarme peut être modélisée comme :

$$P(C > t \mid H_0) = \frac{\int_0^{\cos^{-1}(t)} \sin^{L-2}(u)du}{2\int_0^{\pi/2} \sin^{L-2}(u)du} \tag{3-20}$$

A partir de l'équation (3-19), Lin *et al.* [C. Y. Lin *et al.* 2001] ont obtenu une estimation de la borne supérieur de la probabilité de fausse alarme sous la forme suivant :

$$P(C_{\max} > t \mid H_0) \leq \min\left(1, \sum_{j=1}^{J} P(C_i > t \mid H_0)\right) \tag{3-21}$$

3.4 Résultats numériques

Dans cette section, nous examinons les résultats des deux méthodes proposées (par filtrage et par sélection). D'abord nous présentons la base d'image d'identité utilisée. En outre, les performances des deux méthodes ont été également comparées à la technique de tatouage présenté dans [Ante Poljicak *et al.* 2011] afin de démontrer les avantages de l'exploitation du prétraitement proposé dans ce travail.

3.4.1 Base expérimentale d'image

La base d'image utilisée dans ce travail est la base d'image écossaise PICS (Psychological Image Collection at Stirling)-Aberdeen[1]. Elle contient des photographies des visages couleurs de 90 personnes, avec des variations d'éclairage et de différentes positions. La résolution des images varie entre 336×480 et 624×544. Les images ont toutes été redimensionnées à 512×512. Cela permet l'utilisation de l'algorithme FFT. Un exemple d'images de la base est présenté dans la figure 3-15.

[1] http://pics.stir.ac.uk/.

Figure 3-15- Exemples d'images de la base expérimentale redimensionnées à 512× 512

3.4.2 L'imperceptibilité de la marque

Le degré d'imperceptibilité de la marque insérée est important pour s'assurer qu'il n'y a pas de dégradations visuelles remarquables produites à cause du processus d'insertion. Le PSNR est adopté pour mesurer les distorsions perceptuelles des méthodes proposées. Les images ont été tatouées par les trois méthodes testées en utilisant une valeur de PSNR fixée à 40dB. La taille de la marque est 180 éléments. Pour une illustration de l'imperceptibilité fournie par les trois méthodes de tatouage, l'image originale et les images tatouées ont été présentées dans la figure 3-16. Nous pouvons remarquer qu'elles sont presque identiques perceptuellement. Pour évaluer la similarité entre l'image originale et les images tatouées, nous avons utilisé le MSSIM. Cette mesure objective prend en compte la sensibilité de l'œil humain aux changements de structures dans les images. Le tableau 3-1 présente les résultats de la mesure de similarité obtenue par les trois méthodes testées. Idéalement, le MSSIM entre deux image identiques prend la valeur un. Alors, les résultats de MSSIM présentées dans le tableau 3-1 pour les trois méthodes montrent une similarité élevée entre l'image originale et les images tatouées.

Figure 3-16- Image originale (*a*) et les images tatouées par (*b*) la méthode de Poljicak *et al.* [Ante Poljicak *et al.* 2011], (*c*) le schéma proposé par filtrage et (*d*) schéma proposé par sélection.

Tableau 3-1- Valeurs du MSSIM pour 1000 images tatouée avec un PSNR = 40dB.

	Poljicak *et al.* [Ante Poljicak *et al.* 2011]	**Schéma proposé par filtrage**	**Schéma proposé par sélection**
Maximum	0.9791	0.9794	0.9796
Minimum	0.9646	0.9637	0.9643
Moyenne	0.9729	0.9728	0.9730

3.4.3 Probabilité de fausse alarme

Afin de valider le modèle choisi pour calculer la probabilité de fausse alarme, nous avons effectué une estimation empirique en appliquant la détection sur 1000 images non tatouées. Dix clés différentes ont été utilisées lors la détection. Nous obtenons au total 10,000 valeurs de détection. L'objectif ici est de comparer probabilité de fausse alarme obtenue dans le cas réel et celle obtenue théoriquement par l'équation (3-21). Les valeurs empiriques de la probabilité de fausse alarme ont été présentées en traits pleins avec les valeurs obtenues théoriquement en traits pointillés dans la figure 3-17. Cette comparaison montre que le modèle choisi il correspond bien à nos résultats expérimentaux. Ce modèle est utilisé par la suite pour estimer la probabilité de fausse alarme ainsi que pour calculer le seuil désiré.

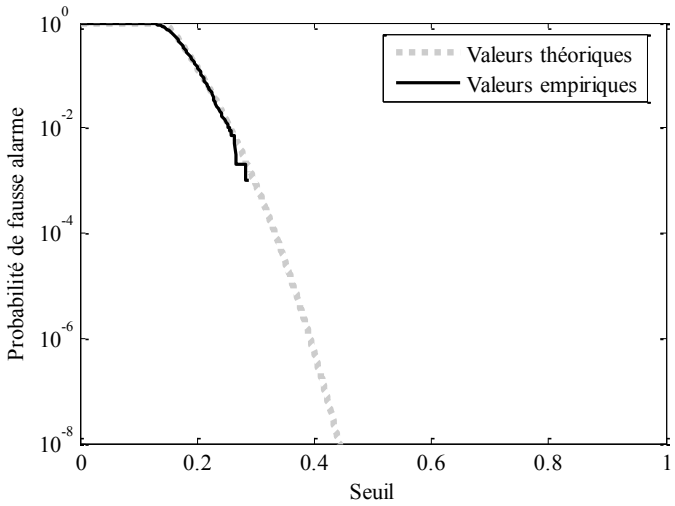


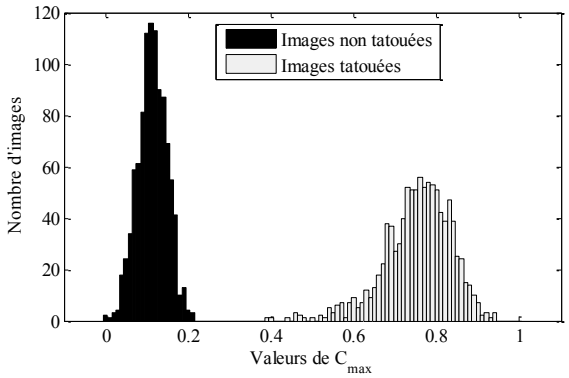
Figure 3-17- Probabilité de fausse alarme mesurée expérimentalement tracée avec celle obtenue théoriquement.

3.4.4 Efficacité des méthodes

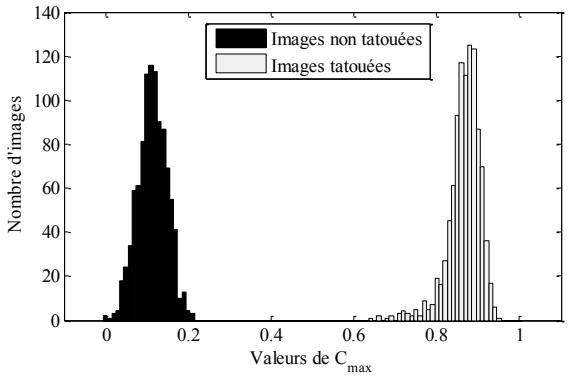
Nous présentons dans la figure 3-18 les densités de probabilité de C_{max} calculées à partir de 1000 images non tatouées (histogramme noir) et 1000 images tatouées (histogramme gris) en utilisant les trois méthodes testées : la méthode de Poljicak *et al.* [Ante Poljicak *et al.* 2011], les deux schémas que nous proposons par filtrage et par sélection.

Les résultats montrent que la densité de probabilité de C_{max} obtenue à partir les images non tatouées est identique pour les trois méthodes. Ceci vient du fait que la variance du vecteur n'est pas modifiée puisque les images ne sont pas tatouées.

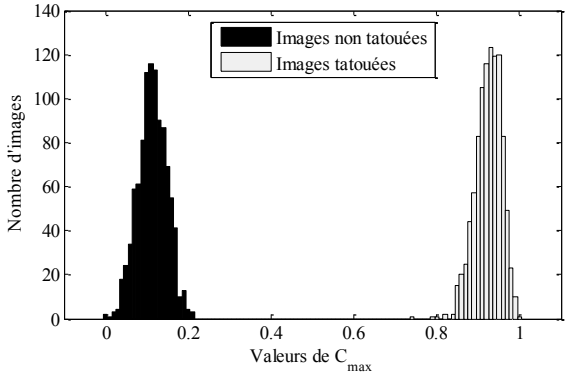
Par contre, pour les images tatouées, la densité de probabilité de C_{max} est soumise à une translation vers la droite (c.à.d. vers les valeurs proches de 1) si la variance du vecteur de l'insertion de la marque est réduite. Cela signifie que les erreurs seront faibles lorsque la variance du vecteur l'insertion de la marque est réduite. Par conséquent, les deux méthodes proposées donneront des résultats meilleurs que la méthode proposée par Poljicak *et al.* [Ante Poljicak *et al.* 2011].



(*a*)



(*b*)



(*c*)

Figure 3-18- La densité de probabilité de la C_{max} utilisant trois méthodes: (*a*) La méthode de Poljicak *et al.* [Ante Poljicak *et al.* 2011], (*b*) le schéma par filtrage, (*c*) schéma par sélection.

Pour valider ces résultats, nous avons effectué une comparaison des valeurs expérimentales en termes de la probabilité de vrai positif en fonction de la valeur de seuil. Les courbes ont été présentées dans la figure 3-19. Lorsque les valeurs de seuil sont faibles, les trois méthodes donnent des résultats similaires. Pour des valeurs de seuil plus élevées, les schémas par filtrage et par sélection proposées dans ce travail surpassent la méthode dans [Ante Poljicak *et al.* 2011]. Les meilleurs résultats sont obtenus par le schéma par sélection.

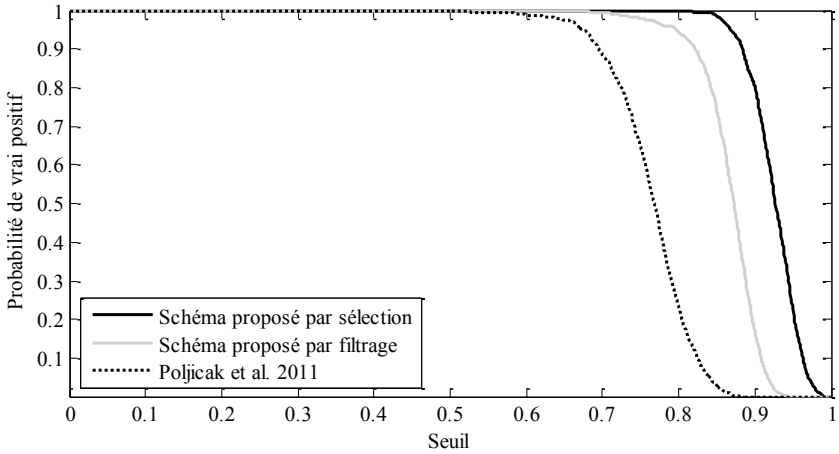


Figure 3-19- La probabilité de vrai positif en fonction de différentes valeurs de seuil.

3.4.5 Robustesse contre les attaques numériques

Afin d'évaluer la robustesse des schémas de tatouage proposés, le programme StirMark 4.0 [Petitcolas 2000] a été utilisé. Ce programme permet de tester une méthode de tatouage contre différentes attaques. Dans nos expériences, les attaques numériques ont été appliquées aux images tatouées. Ces attaques incluent la compression JPEG avec perte, filtrage médian et l'ajout d'un bruit blanc gaussien. La robustesse des méthodes est mesurée puis tracée sous forme des courbes ROC dans les figures 3-21, 3-22 et 3-23.

D'abord, les images tatouées ont été compressées en utilisant la compression JPEG avec perte, le facteur de qualité est de 20% (taux de compression élevé). A titre d'exemple, le résultat de compression JPEG avec un taux de compression de 20% d'une image issue de la base d'images d'identité est présenté dans la figure 3-20.

Figure 3-20- Image issue de la base d'image compressée avec un taux de compression JPEG 20% avec le programme StirMark 4.0.

Les résultats de la détection sous l'attaque de compression ont été tracés dans la figure 3-21. D'après ces résultats nous remarquons que le tatouage basé sur la transformé de Fourier est robuste lorsque les images tatouées sont compressées avec un facteur de compression élevé (20%). La robustesse des schémas proposés contre la compression JPEG est expliquée par le fait d'insérer la marque dans les fréquences moyenne de la transformée de Fourier qui sont moins affectées par la compression.

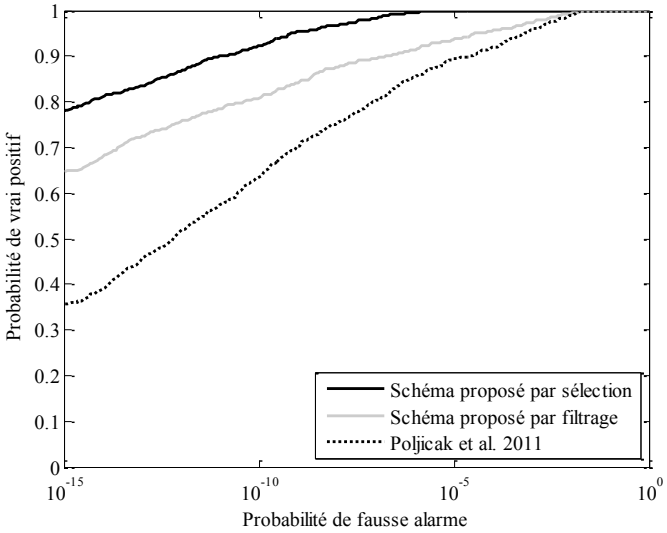


Figure 3-21- Courbe ROC des images tatouées sous l'attaque de la compression JPEG.

Les résultats obtenus sous les autres attaques (filtre médian 7×7 et ajout de 10% de bruit blanc gaussien) sont présentés dans les figures 3-22 et 3-23. Le bruit et le filtrage affectent généralement les hautes fréquences ce qui justifie la robustesse de la méthode basée sur la transformée de Fourier contre ce genre d'attaques.

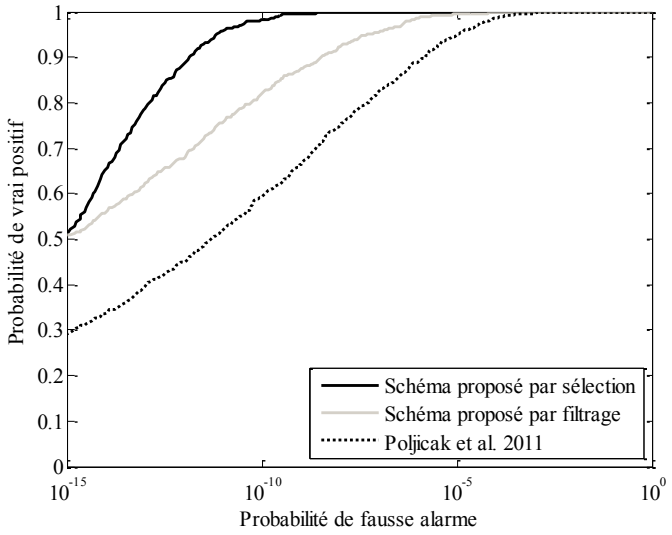


Figure 3-22- Courbe ROC des images tatouées sous l'attaque du filtrage médian.

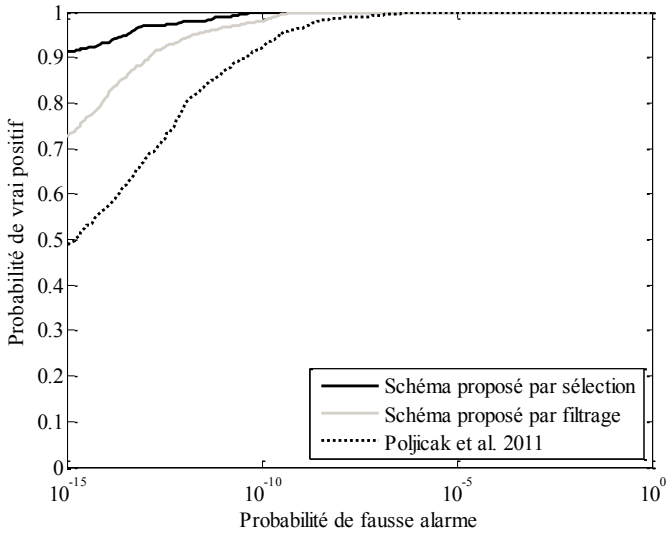


Figure 3-23- Courbe ROC des images tatouées sous l'attaque de l'ajout de bruit.

D'après les résultats présentés ci-dessus, les deux schémas proposés donnent des meilleurs résultats que la méthode proposé par Poljicak *et al.* [Ante Poljicak *et al.* 2011].

3.4.6 Robustesse contre les attaques géométriques

Lors d'une opération d'impression/numérisation, l'image est soumise principalement à des transformations géométriques. Nous devons nous assurer que les deux méthodes proposées sont suffisamment robuste vis-à-vis de ces transformations géométriques. La robustesse des schémas proposés contre les attaques géométriques a été évaluée en appliquant une attaque de rotation.

Le test est exécuté sur les images tatouées avec des rotations de 3°, 5°, 30° et 45°. Le fond des images a été rempli par des valeurs de niveau de gris égal à zéro, comme le montre la figure 3-24.

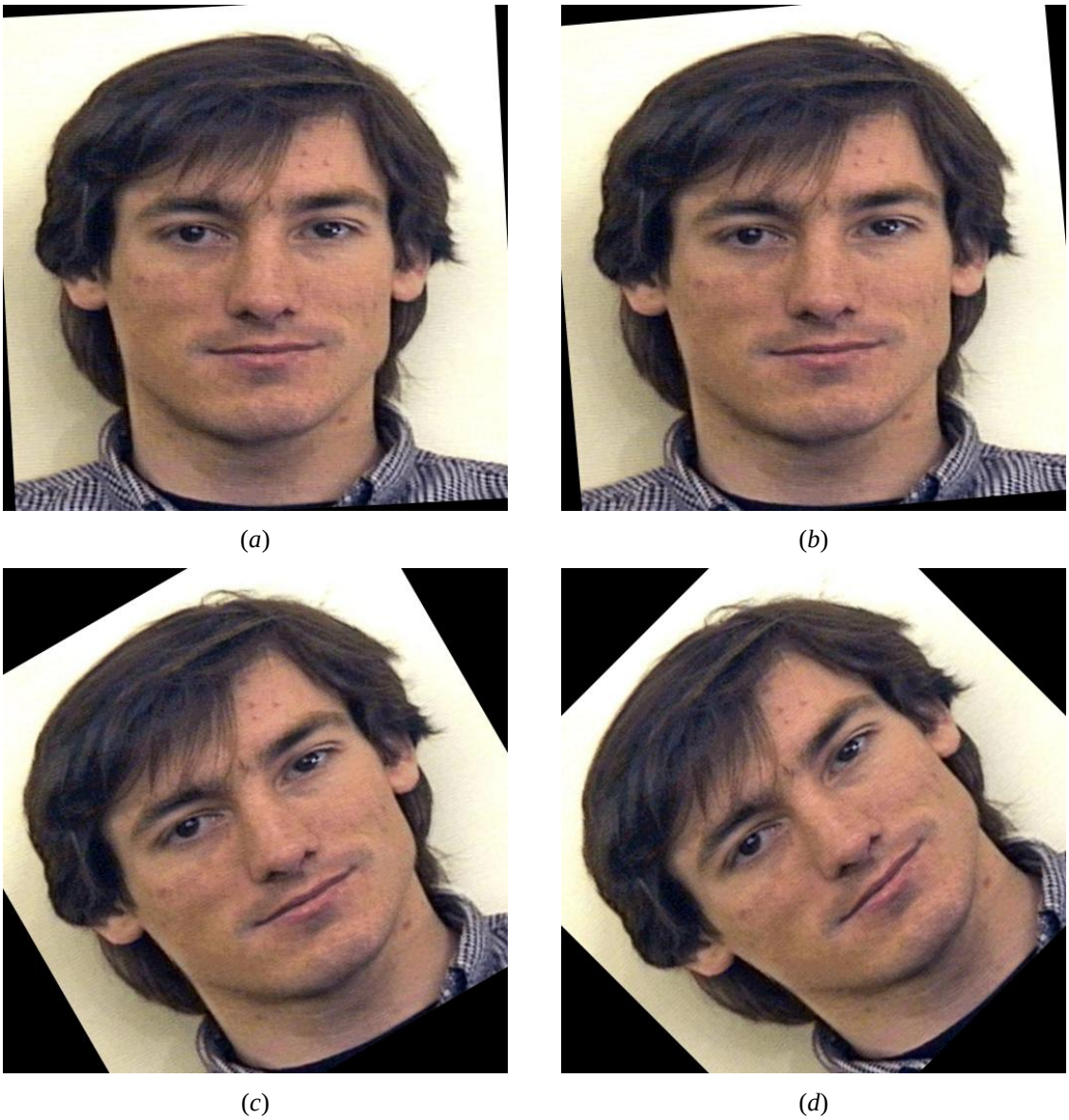


Figure 3-24- Attaques de rotation avec recadrage, (*a*) Rotation de 3°, (*b*) Rotation de 5°, (*c*) Rotation de 30°, (*d*) Rotation de 45°.

Les résultats de détection pour les trois méthodes ont été présentés sous forme des courbes ROC dans les figures 3-25 à 3-28. Les résultats montrent que la robustesse des méthodes de tatouage diminue sous ces transformations lorsque la rotation est importante. Dans ce test, des parties de l'image ont été remplacées par des zéros (figure 3-24), ces zones ne contienne aucune information de la marque ce qui explique la diminution de la robustesse des méthodes si la rotation est importante.

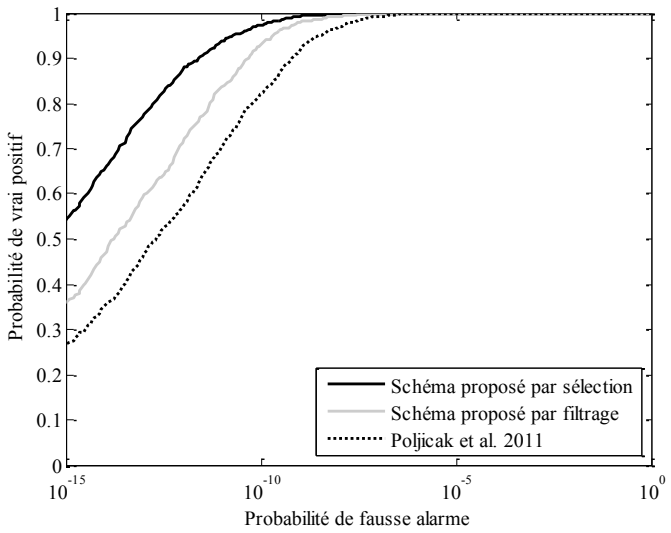


Figure 3-25- Courbe ROC des images tatouées sous l'attaque de rotation par 3°.

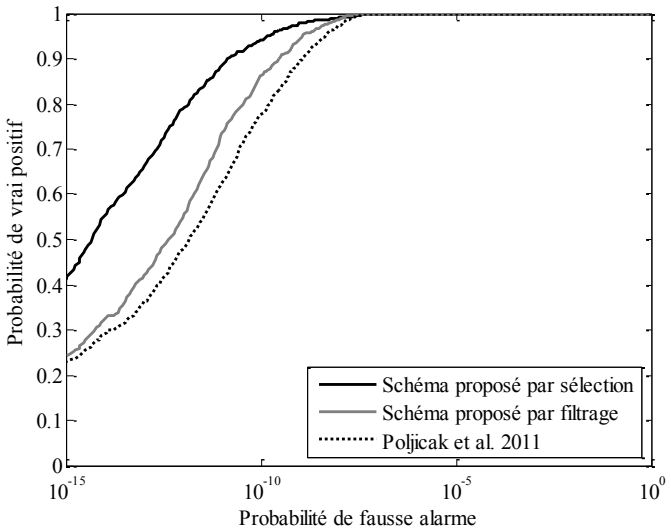


Figure 3-26- Courbe ROC des images tatouées sous l'attaque de rotation par 5°.

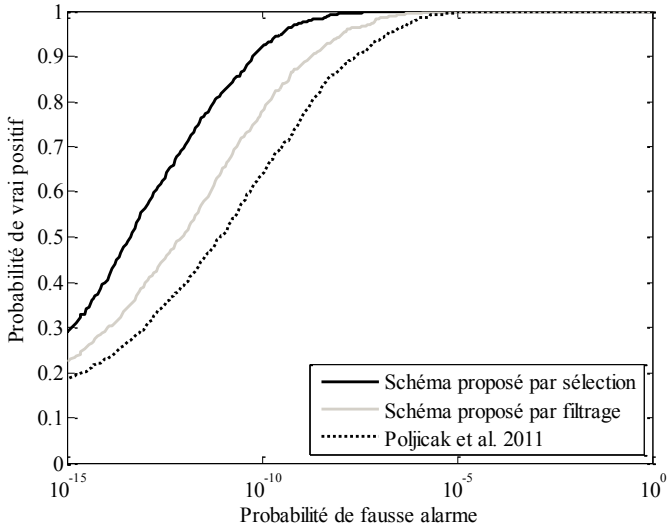


Figure 3-27- Courbe ROC des images tatouées sous l'attaque de rotation par 30°.

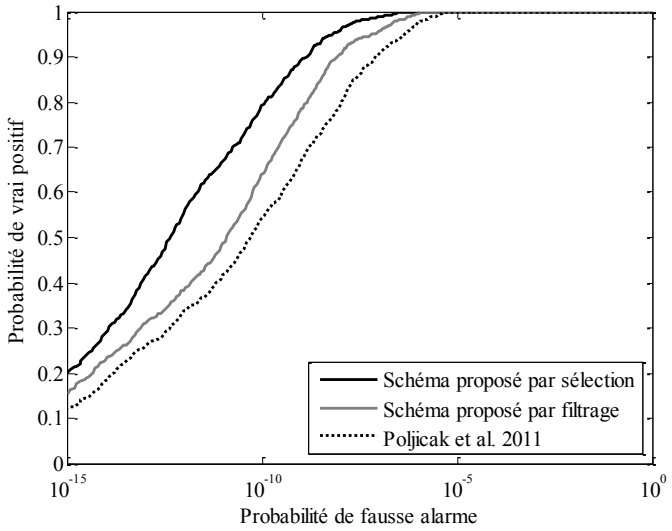


Figure 3-28- Courbe ROC des images tatouées sous l'attaque de rotation par 45°.

Ces résultats montrent que les deux méthodes proposées surpassent la méthode proposée par Poljicak *et al.* [Ante Poljicak *et al.* 2011].

3.5 Conclusion

Dans ce chapitre nous avons présenté notre première contribution dans le domaine du tatouage d'images. L'approche développée appartient aux schémas additifs avec une détection aveugle. Nous avons développé une nouvelle méthode de tatouage par transformée de Fourier basées sur le prétraitement de l'image avant l'insertion de la marque. Ce prétraitement consiste à diminuer la

variance du vecteur qui supporte la marque. La réduction de la variance a été réalisée soit par une modification directe des coefficients dans lesquels la marque est insérée ou par sélection des coefficients.

Les résultats sont de bonne qualité en termes d'invisibilité et de robustesse vis-à-vis des attaques numériques telles que la compression, l'ajout de bruit et le filtrage, ainsi que contre les attaques géométriques tel que la rotation.

Une comparaison avec une technique de tatouage de littérature [Ante Poljicak *et al.* 2011] a démontré que les méthodes proposées permettent d'améliorer la robustesse du système de tatouage. En outre, on remarque que le schéma basé sur la sélection est plus performant que celui basé sur le filtrage des coefficients.

Cependant, lors de l'impression/numérisation, d'autres attaques interviennent et se combinent entre elles :

- Flou,
- Variations de couleurs.

Une analyse de ces problèmes nous a conduit à développer une approche corrective qui fera l'objet du chapitre suivant.

Chapitre IV :

4 Contre-attaque de l'impression / numérisation

4.1 Introduction

Dans le cadre de l'application envisagée, les images d'identité sont imprimées sur des cartes en plastique puis scannées. L'objectif de ce chapitre est le développement une méthode corrective basée sur des contre-attaques (filtre de Wiener et correction colorimétrique). Cette technique permet de replacer l'image imprimée puis scannée dans un état favorable à la détection de la marque. Ainsi, nous présentons la performance de la méthode contre des attaques de vieillissement des documents d'identité

Dans une première partie de ce chapitre, la chaîne expérimentale est présentée dans la section 4.2. Ensuite, le modèle de la chaîne ainsi que les dégradations dues à l'impression / numérisation et au vieillissement du document sont décrits dans la section 4.3. Les étapes préalables à la détection de la marque sont présentées dans la section 4.4. Dans la première étape, une phase de correction de flou des images imprimées et scannées a été intégrée suivie d'une seconde étape de correction colorimétrique spécifique aux images d'identité. Puis les résultats sous différentes attaques (impression/numérisation et de vieillissement du document) sont présentés dans la section 4.5. Finalement, la conclusion de ce chapitre est présentée dans la section 4.6.

4.2 Description de la chaîne d'impression/numérisation

La chaîne d'impression/numérisation utilisé pour les expériences est présentée dans la figure 4-1.

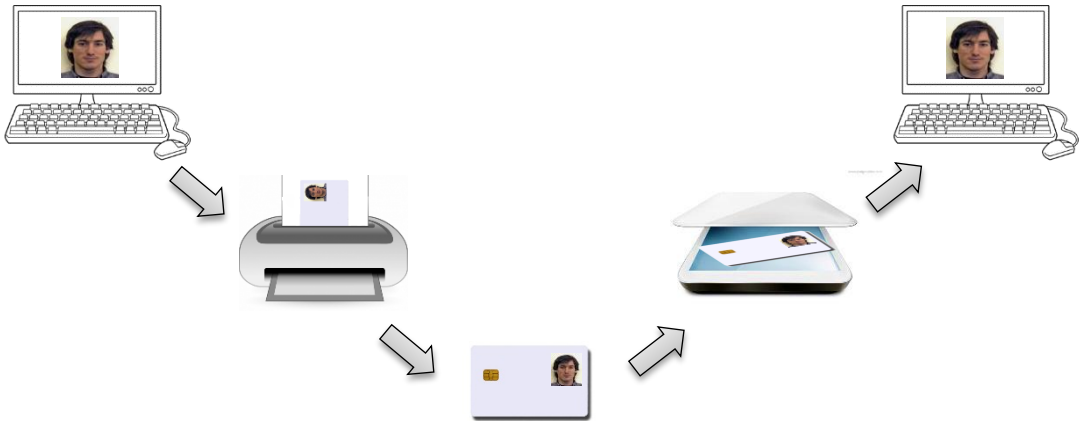


Figure 4-1- La chaîne d'impression/numérisation.

La transformation physique de l'image numérique à l'image imprimée est réalisée avec une imprimante de carte de type Fargo Persona C25. Une fois que l'image tatouée est imprimée sur le document, le propriétaire légitime peut utiliser le document pour prouver son identité ou pour accéder à des zones sécurisées. En cas de perte ou de vol du document, des pirates peuvent modifier le contenu de l'image ou faire des copies non autorisées du document. Les copies frauduleuses peuvent être ensuite scannées et imprimées à nouveau sur un nouveau document.

À un certain moment, l'image originale, la copie non autorisée de l'image ou l'image modifiée, est scannée lors du passage du document à travers un système de vérification, en utilisant un dispositif de numérisation spécifique. Dans ce travail c'est un scanner HP ScanJet 5550c. Ainsi, l'image peut être récupérée pour vérifier si l'image est tatouée ou non. En conséquence, on peut décider si le document est authentique ou si c'est une copie illicite.

Afin de faciliter la tâche de la vérification, il serait utile de prévoir précisément les effets du processus de l'impression / numérisation ainsi les distorsions produites lors l'utilisation du document. Dans la suite, nous présentons un modèle de la chaîne d'impression / numérisation, ainsi les dégradations produites pendant l'utilisation du document d'identité ou attaque de vieillissement.

4.3 Modèle proposé de la chaîne

4.3.1 Modèle d'impression/numérisation

Les images d'identité seront imprimées avec leur marque sur un support de carte en plastique, directement après la phase d'insertion. La détection se fera ultérieurement et à distance du lieu de fabrication, après une numérisation de la carte à l'aide d'un appareil de numérisation. Cette opération

d'impression/numérisation empêche la bonne détection de la marque. D'après le chapitre 2, il a été décrit de nombreux facteurs qui contribuent à la distorsion de l'image dans le processus d'impression/numérisation. Cette distorsion, propre à la chaîne de traitement, est à la fois, globale et locale. On trouve notamment : la translation, la rotation, le changement d'échelle, un flou dû à la réponse impulsionnelle du système d'impression/numérisation, un bruit liée à l'acquisition et les distorsions des couleurs.

Notre objectif est d'élaborer un modèle simple de la chaîne d'impression/numérisation afin de développer une contre-attaque des distorsions produites par la chaîne. Dans cette section, nous se concentrons principalement sur l'effet du flou dû à la réponse impulsionnelle de la chaîne ainsi que les variations et les changements de couleurs. Les distorsions géométriques (rotation et translations) sont compensées par la méthode de tatouage sélectionnée.

Poljicak *et al.* [A. Poljicak *et al.* 2012] modélisent les dégradations produites pendant l'opération d'impression/numérisation comme un filtrage passe-bas plus un bruit. Le modèle adopté dans cette étude est de la forme suivante :

$$I^{*}(i,j) = I(i,j) * h(i,j) + n(i,j), \tag{4-1}$$

avec I^{*} désigne l'image imprimée puis scannée, I est l'image originale, h est la réponse impulsionnelle de la chaîne et n est un bruit blanc Gaussien de moyenne nulle et de variance inconnue indépendant de l'image.

Dans [Kundu *et al.* 2006] et [Villan *et al.* 2006], les auteurs ont modélisé les variations des niveaux de gris pendant l'impression/numérisation par une fonction non linéaire. Le contexte de notre application impose de travailler avec des images couleurs, pour cette raison nous avons modélisé les distorsions des couleurs par des fonctions non linéaires pour chaque composante couleur.

4.3.2 Vieillissement des documents d'identité

L'image tatouée subit des dégradations naturelles au cours de l'utilisation du document d'identité. Ces dernières sont nombreuses et variées. Nous citons à titre d'exemple : vieillissement du support (atténuation des couleurs), rayures, et taches, … Toutes ces attaques apparaissent au cours de l'utilisation du document et peuvent gêner la détection de la marque lors d'une vérification de l'intégrité ou de l'authenticité du document.

Une série d'attaques a été réalisée afin de tester la robustesse de la méthode de tatouage. L'objectif de ces attaques est de quantifier les capacités des algorithmes du tatouage face à des attaques réalistes simulant le vieillissement du document d'identité. La simulation de ces attaques est effectuée d'une manière numérique sur des images tatouées, imprimées puis scannées.

Dans la section résultats, une étude a été menée pour analyser le comportement des algorithmes de tatouage face à la fois aux distorsions de l'impression/numérisation et aux attaques de vieillissement. Ces dernières peuvent être divisées en deux catégories : attaques mécaniques et attaques photométriques.

4.3.2.1 Attaques mécaniques

Les attaques mécaniques regroupent toutes les dégradations du document d'identité suivantes :

- **Rayures :** Le passage du document d'identité à travers un système de vérification consiste à insérer le document dans le lecteur puis le retirer. Si le nombre de répétition de cette opération est important, elle produit des rayures. D'autres rayures peuvent apparaitre sur l'image à cause de l'utilisation non protégée du document. Nous avons décidé de tracer des traits horizontaux ou verticaux dans l'image pour simuler ces types de détérioration car il n'est pas possible de simuler toutes les dimensions, tailles et orientations des rayures sur l'image.
- **Découpe de l'image :** Cette attaque se nomme cropping en anglais. Cette modification de l'image se traduit par la disparition d'une partie de l'image due à des frottements ou à des chocs. On observe donc un trou dans l'image. Les tests réalisés sont basés sur la découpe, dans l'image, d'un carré de dimensions $N \times N$ pixels en différents endroits de l'image.
- **Flexion :** Le document d'identité peut se plier dans un portefeuille ou une poche, cette opération peut se traduire par une flexion du document ou bending en anglais. Cette distorsion conduit à une déformation de la forme de barillet, où les bords de l'image sont des arcs de cercle. Le modèle de distorsion en barillet [Bailey 2002] s'exprimé par l'équation suivante :

$$a_d = a_u(1 + k \times a_u^2), \tag{4-2}$$

avec a_d et a_u représentent les distances radiales respectivement dans l'image déformée et dans l'image non-déformée, et la constance k et le paramètre de distorsion. La figure 4-2 montre l'effet barillet sur une grille carrée.

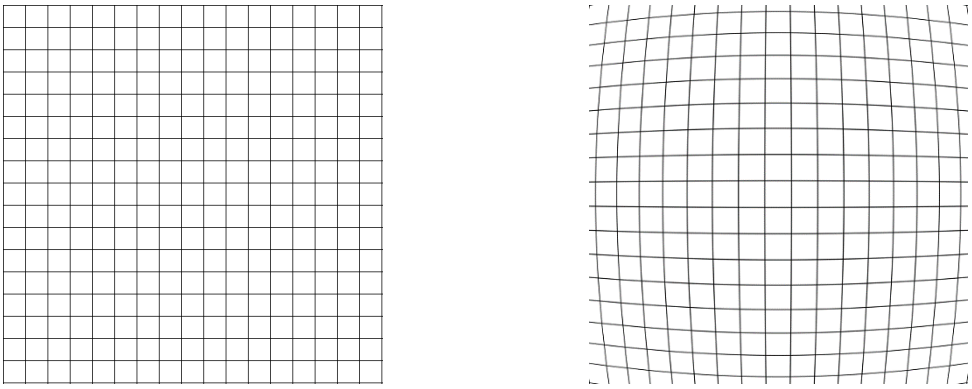


Figure 4-2- Exemple de l'effet barillet sur une grille carrée.

- **Poussière:** La carte d'identité et l'image peuvent également souffrir de la poussière à cause de l'utilisation non-protégée du document. Ce genre d'attaque est simulé par l'ajout d'un bruit impulsionnel.

4.3.2.2 Attaques photométriques

Naturellement, les couleurs changent au cours du temps. Cette dégradation peut être retardée par différents moyens (ex. film de protection anti-UV sur l'image), mais il y aura toujours une modification des couleurs.

- **Décoloration :** la décoloration de la couleur ou (color fading) se produite lorsque le document d'identité est exposé aux rayonnements du soleil pendant une longue période. Cette dégradation consiste à une perte de densité de couleur, elle se traduit par une diminution de la saturation des images imprimées sur le document.
- **Taches :** que ce soit au niveau de l'impression ou au niveau de l'utilisation, une image peut subir une attaque de type tache. Les résultats de cette attaque sont variés : atténuation locale de la luminance, apparition locale de taches rouge, vert, bleu ou composées,…

4.4 Contre-attaques d'impression/numérisation

La meilleure défense aux attaques produites pendant l'impression/numérisation est de corriger leurs effets avant la phase de détection de la marque. Cette défense vue comme une contre-attaque va permettre de replacer l'image dans un contexte favorable pour la détection de la marque. La dégradation d'impression/numérisation est souvent agressive. Elle est toujours présente. Par contre les attaques de vieillissement ne sont pas toujours présentes. En conséquence, elles sont difficiles à corriger de manière préventive. Dans ce travail, des contre-attaques de l'impression/numérisation ont été proposées, elles consistent à réduire les effets de flou et de corriger les variations de couleur.

On part du principe que la chaîne d'impression/numérisation est connue. Nous pouvons mesurer les différentes caractéristiques de la chaîne. Il faut noter que les contre-attaques développées dans ce travail sont spécifiques à un couple d'imprimante/scanner. En conséquence, une phase de calibration est nécessaire à chaque utilisation d'un nouveaux matériels (imprimante / scanner).

4.4.1 Correction du flou

L'équation (4-1) modélise le flou subit les images imprimées puis scannées, nous pouvons schématiser ce processus par la figure 4-3.

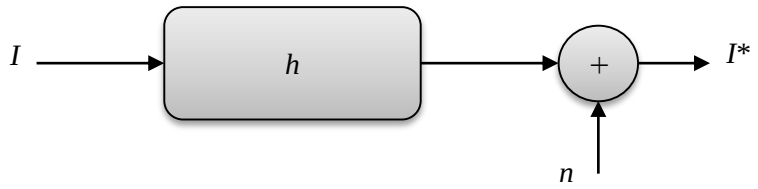


Figure 4-3- Modélisation du flou avec prise en compte du bruit.

Le filtre inverse est sans doute l'une des premières approches à être utilisée afin de corriger la dégradation d'impression/numérisation. Cette technique est très rapide en temps de calcul et permet une restauration parfaite de l'image à condition que la transformée de Fourier de la réponse impulsionnelle de la chaîne n'ai aucune fréquence nulle ou proche de zéro, ainsi que le bruit ne soit pas présent dans l'image. Dans le cas réel les images sont bruitées. C'est la raison pour laquelle cette technique ne peut pas être utilisée en présence de bruit.

Il existe d'autres alternatives qui tiennent compte de la présence de bruit dans une image, la technique la plus communément utilisée est le filtre de Wiener. Le filtre de Wiener considère que l'image et le bruit sont des réalisations d'un processus aléatoire stationnaire. Il cherche alors à restaurer l'image dégradée par minimisation de l'erreur quadratique moyenne entre l'image restaurée $\hat{I}$ et l'image originale I. La solution de cette minimisation est définie dans le domaine fréquentiel [Gonzalez *et al.* 2007] par :

$$\hat{I}(u,v) = I^*(u,v)\frac{\bar{H}(u,v)}{\bar{H}(u,v)H(u,v) + \dfrac{S_n(u,v)}{S_I(u,v)}}, \tag{4-4}$$

H et $\bar{H}$ sont respectivement la transformée de Fourier de la réponse impulsionnelle et son conjugué complexe, S_I et S_n sont respectivement les puissances spectrales de l'image originale et du bruit. Généralement, la fraction S_n/S_I est remplacée par une constante. Elle peut être caractérisée approximativement par l'inverse du rapport signal sur bruit ou 1/SNR.

L'utilisation du filtre de Wiener nécessite une connaissance correcte ou une bonne estimation de la réponse impulsionnelle de la chaîne ainsi une estimation de la puissance spectrale du bruit. Dans la suite nous présentons l'estimation de la réponse impulsionnelle et du bruit à partir de la chaîne expérimentale.

4.4.1.1 La réponse impulsionnelle de la chaîne

A. Rappel sur l'estimation de la réponse impulsionnelle

Dans notre contexte industriel le matériel d'impression/numérisation est connu. Il est donc possible d'obtenir une estimation de la réponse impulsionnelle d'une manière expérimentale. Plusieurs méthodes ont été développées dans la littérature pour estimer la réponse impulsionnelle d'un système qu'il soit électronique, mécanique ou optique. La méthode classique pour mesure la réponse impulsionnelle consiste à appliquer une impulsion à l'entrée d'un système et mesurée sa réponse [Gonzalez *et al.* 2007, Sharif *et al.* 2007]. Cette technique a montré quelques limites en présence de bruit. Une autre méthode consiste à estimer la fonction de transfert (la réponse fréquentielle) dans le domaine spectral et de la transformer dans le domaine spatial pour obtenir la réponse impulsionnelle du système [Brauers *et al.* 2010].

Pour explique le principe de l'estimation de la réponse impulsionnelle en utilisant la corrélation, nous nous plaçons dans le cas de signaux temporels. Nous supposons que l'on dispose d'une observation sans bruit de la forme suivant: $y(t) = h(t)*x(t)$ où $x(t)$ est le signale d'entrée, $h(t)$ la réponse impulsionnelle et $y(t)$ est le signal de la sortie du système. Puisque la relation d'entrée-sortie est une convolution, la relation entre le signal $y(t)$ et $x(t)$ en termes de la fonction de corrélation croisée est donnée comme suit :

$$R_{yx}(\tau) = h(\tau) * R_{xx}(\tau), \tag{4-5}$$

où $R_{xx}(\tau)$ représente la fonction d'autocorrélation du signal $x(t)$.

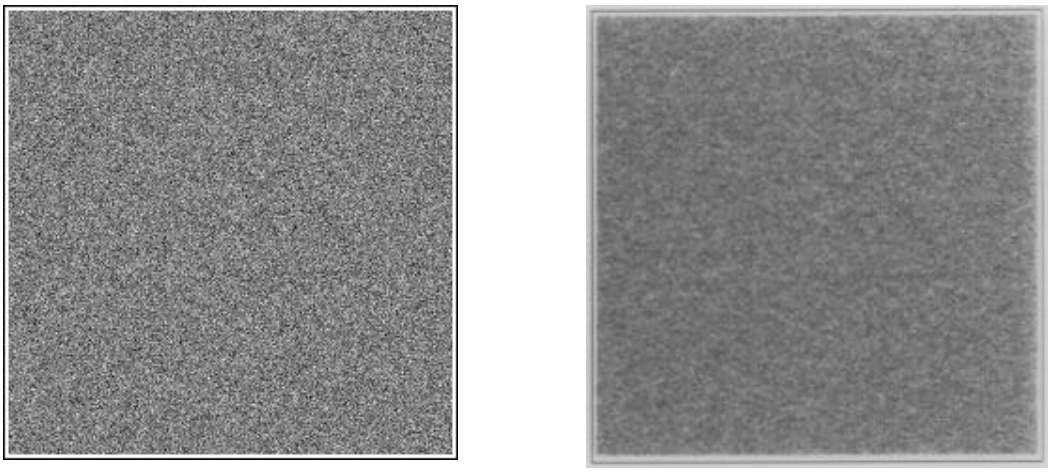
Si le signal d'entrée $x(t)$ est un bruit blanc centré, alors sa fonction d'autocorrélation est une impulsion de Dirac à l'origine, d'ou la fonction de corrélation croisée s'écrit comme suit :

$$R_{yx}(\tau) = h(\tau) * \delta(\tau) = h(\tau). \tag{4-6}$$

A partir de ces résultats nous pouvons constater que la réponse impulsionnelle d'un système est égale la fonction de corrélation croisée normalisée de la sortie $y(t)$ et l'entrée $x(t)$ lorsque $x(t)$ est un bruit blanc.

B. Estimation de la réponse impulsionnelle

La réponse impulsionnelle a été estimée par la méthode de corrélation d'un bruit blanc et sa réponse à la chaîne d'impression/numérisation. Nous utilisons le modèle représenté sur la figure 4-4, ce modèle est composé d'une de bruit blanc avec un cadre rectangulaire pour la mise en correspondance entre l'image scannée et l'image originale. L'image a été imprimée sur des cartes en plastique à plusieurs reprises en utilisant une résolution d'impression de 300 dpi. Ensuite, les images imprimées ont été scannées avec la même résolution afin d'éviter le problème de la mise à l'échelle. Les coins du cadre rectangulaire dans chaque image ont été détectés et leurs positions ont été utilisées pour calculer la transformation géométrique entre l'image acquise et l'image numérique. Cette transformation géométrique permet de positionner les pixels imprimés et numérisés dans leurs positions originales correspondantes.



(a) (b)

Figure 4-4- Modèle utilisé pour estimer la réponse impulsionnelle ; (a) Modèle numérique, (b) Modèle imprimé et scanné.

D'après l'équation (4-6), la réponse impulsionnelle égale à la corrélation croisée normalisé du bruit d'entrée avec celui de sortie, supposons que N_{in} représente l'image de taille $M \times M$ du bruit originale et N_{out} limage obtenue après l'impression/numérisation et le recalage. L'estimation préliminaire de la réponse impulsionnelle de la chaîne d'impression/numérisation est égale à la corrélation croisée entre N_{in} et N_{out} :

$$\hat{h}(i,j) = \frac{1}{(M-i)(M-j)} \sum_{m=0}^{M-i-1} \sum_{n=0}^{M-j-1} N_{in}(m,n) N_{out}(m+i, n+j), \tag{4-7}$$

avec $0 \le i < 2M-1$ et $0 \le j < 2M-1$.

Cette opération est répétée plusieurs fois, puis l'estimation de la réponse impulsionnelle est obtenue par la moyenne de dix tests. Après recadrage pour avoir une matrice de taille $M \times M$, le résultat final de la réponse impulsionnelle est représenté sur la figure 4-5.

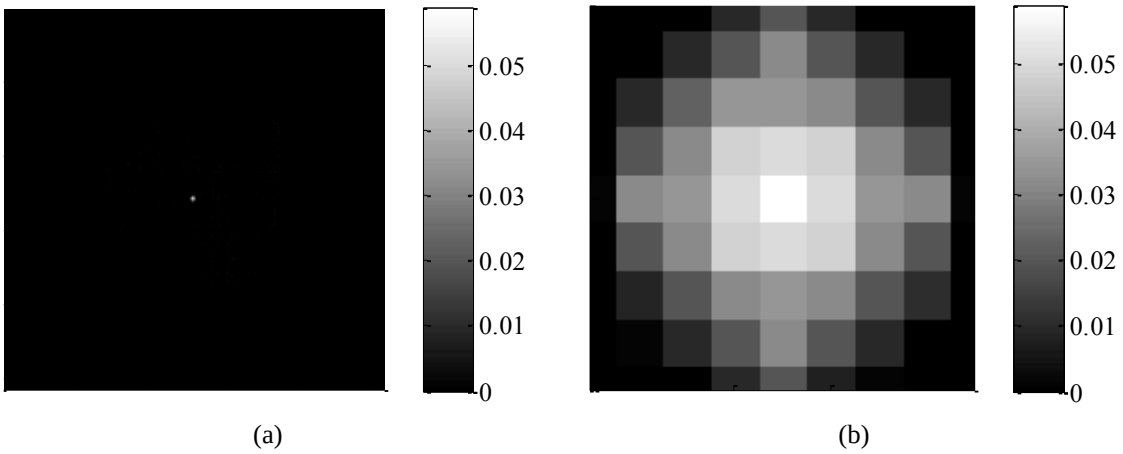


Figure 4-5- La réponse impulsionnelle estimée (a), zoom de la réponse impulsionnelle.

4.4.1.2 Estimation du bruit

Dans la phase de la numérisation où l'image imprimée est convertie en une version numérique de cette image, plusieurs facteurs ont de l'influence sur le processus d'acquisition. Le facteur non déterministe qui se produit lors de la numérisation est le bruit. Dans le cas de notre application, il est très utile de connaitre les statistiques de bruit afin d'appliquer le filtre de Wiener d'une manière correcte.

Les principales sources de bruit dans la phase de l'acquisition sont les capteurs CCD. D'après Luisier *et al.* [Luisier *et al.* 2011] deux types de bruit sont généralement considérés dans l'acquisition. Le premier type correspond à la nature stochastique du procédé de comptage de photons dans le détecteur. Ils se traduisent le plus souvent par des pixels de haute intensité de niveaux de gris sur l'image. Le second type correspond aux fluctuations thermiques et électroniques intrinsèques du dispositif d'acquisition, ce type de bruit est indépendant de l'intensité de signal.

Pour déterminer le bruit dans la chaîne d'impression/numérisation, nous avons effectué les mesures suivantes. Nous avons imprimé des images ayant des niveaux de gris uniforme de 0 à 255 (256 images), les images imprimées ont été scannées par la suite. La figure 4-6 présente l'histogramme du niveau 128. Les histogrammes des images numérisées présentent des distributions sensiblement gaussiennes.

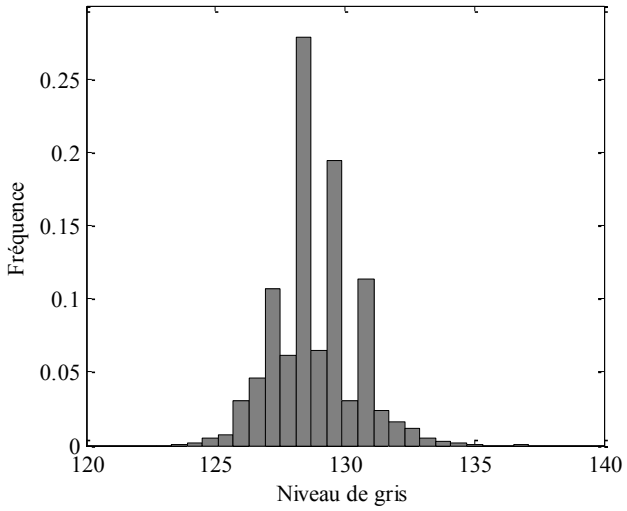


Figure 4-6- Histogramme d'une image avec des niveaux de gris uniformes imprimée et scannée pour un niveau de gris égal à 128.

A partir de ces résultats, nous considérons que le bruit dans la chaîne d'impression/numérisation est un bruit additif blanc gaussien de moyenne nulle et sa variance est la moyenne des variances de 256 images imprimées/scannées. Dans le cas de notre expérience, la variance du bruit est de 2.13.

4.4.2 Correction colorimétrique

Que ce soit au niveau de l'impression ou au niveau de la numérisation, des dégradations de couleurs sont présentes dans les images tatouées. Par exemple lors de la numérisation les capteurs engendrent une modification des couleurs de l'image. Cet effet provient de leurs caractéristiques propres, différentes d'un capteur à un autre, à capter les longueurs d'ondes du rouge, vert et bleu (de même pour les niveaux de gris). Dans ce travail nous proposons une phase de correction colorimétrique comme une deuxième étape des contre-attaques proposées. Cette correction consiste tout d'abord à estimer la fonction de dégradation des couleurs, puis à appliquer la fonction inverse aux images imprimées/scannées. L'estimation de la fonction de la dégradation des couleurs adoptée est décomposée en étapes décrites dans la figure 4-7.

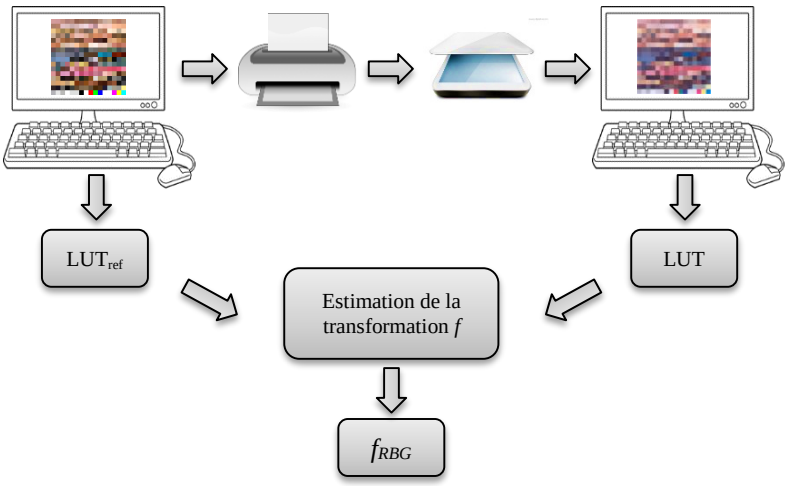


Figure 4-7- Organigramme de l'estimation de fonction de dégradation des couleurs.

Les images utilisées dans le contexte de notre application sont des images d'identité dont le visage occupe de 70 à 80% de l'image, le fond de l'image est de couleur claire et unie. Les visages ne présentent qu'un sous-ensemble assez réduit de teintes, dont les nuances proposées dans la mire (figure 4-8) utilisée pour estimer la fonction de dégradation des couleurs.

(*a*) (*b*)

Figure 4-8- Mire utilisée pour estimer la fonction de correction des couleurs ; (*a*) Originale, (*b*) Imprimée et scannée.

Premièrement, la mire des couleurs spécifique aux visages est imprimée sur une carte en plastique puis scannée en utilisant notre chaîne expérimentale. L'extraction des 256 valeurs RGB est effectuée par moyennage sur les carreaux de la mire acquise. La correction de l'image s'effectue ensuite dans

chaque canal de l'espace RGB, d'où l'estimation de la fonction de dégradation est effectuée dans les trois canaux en utilisant une régression polynomiale d'ordre 4 [Nakamura 1993] comme suit :

$$\begin{cases} \hat{R} = a_1R^4 + a_2R^3 + a_3R^2 + a_4R + a_5 \\ \hat{G} = b_1G^4 + b_2G^3 + b_3G^2 + b_4G + b_5 \\ \hat{B} = c_1B^4 + c_2B^3 + c_3B^2 + c_4B + c_5 \end{cases} \tag{4-8}$$

Avec $a_1 \ldots a_5$, $b_1 \ldots b_5$ et $ci \ldots c_5$ sont les coefficients des polynômes pour chaque canal dans l'espace RGB. Dans notre expérience les valeurs de ces coefficients sont présentées dans le tableau 4-1. Les valeurs R, G et B correspondent respectivement aux valeurs moyennes dans les canaux rouge, vert et bleu, et $\hat{R}$, $\hat{G}$ et $\hat{B}$ sont ceux estimés. Finalement, les fonctions inverse sont calculées (voir figure 4-9). Ces fonctions ont été stockées par la suite dans des tables de conversion LUTs.

Tableau 4-1- Coefficients des polynômes de la régression polynomiale pour chaque canal RGB.

Indice	**1**	**2**	**3**	**4**	**5**
R	-1.6108×10^{-7}	7.2143×10^{-5}	-8.3833×10^{-3}	0.8640	46.6845
G	-7.3029×10^{-8}	2.2437×10^{-5}	7.4734×10^{-4}	0.2450	49.9323
B	3.3609×10^{-8}	-1.8068×10^{-5}	3.8517×10^{-3}	0.3278	70.5916

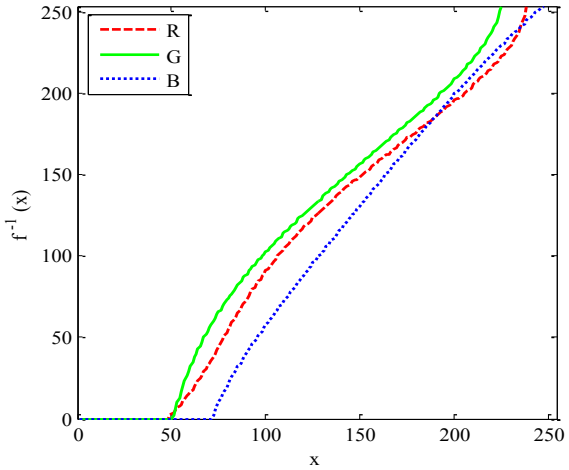


Figure 4-9- L'inverse des fonctions de dégradation pour chaque canal dans l'espace RGB.

4.5 Résultats

Les expériences ont été effectuées sur 400 images couleurs d'identité extraites de la base expérimentale : les 400 images sont tatouées et ces mêmes 400 sont non tatouées, soit 800 images au total. Les images numériques ont été imprimées avec une résolution de 300 dpi sur des cartes en plastique. Les carte ont une surface de 86×54 mm^2 et une épaisseur de 0.76 mm. La taille de l'image imprimée sur la carte est de 20×20 mm^2. Les 800 images imprimées ont été numérisées par la suite avec une résolution de 300 dpi. Avant la phase de détection, les images numérisées ont été redimensionnées à 512×512 pixels en utilisant l'interpolation bilinéaire. La figure 4-10 montre un exemple de distorsions résultantes de l'opération impression/numérisation.

(*a*) (*b*)

Figure 4-10- Exemple de distorsions résultantes d'une opération impression/numérisation. (*a*) Image numérique issue de la base d'image expérimentale, (*b*) la même image imprimée à 300 dpi et scannée à 300 dpi.

L'algorithme de tatouage développé dans le chapitre 3 a été optimisé pour qu'il soit adapté à l'application industrielle. Tout d'abord une marque de 180 bits est insérée dans les images avec une force adapté à chaque image afin d'avoir un PSNR égal à 40dB. Dans la phase de numérisation, chaque carte à numériser est placée sur le plateau du scanner. L'angle de rotation est généralement inférieure à 10 degrés en pratique, car le coin de l'image à numériser est aligné avec le coin du plateau du scanner ce qui limite les rotations. Pour cette raison dans de la détection, la recherche de la meilleure corrélation a été effectué pour des angles de rotation de -/+ 10°.

4.5.1 Impression / numérisation

La dégradation due à l'impression/numérisation est clairement visible dans l'image imprimée puis scannée présenté dans la figure 4-10-b. Dans la suite nous appliquons l'algorithme de détection de la marque aux images imprimée/scannée, afin d'étudier le comportement de la méthode de tatouage développée dans le chapitre 3 lors de l'attaque d'impression/numération. Les contre-attaques développées dans ce chapitre sont étudiées par la suite.

Premièrement, nous présentons l'effet de l'opération impression/numérisation sur la densité de probabilité de la mesure de détection C_{max}. La figure 4-11 présent les densités de probabilité de C_{max} calculée à partir de 400 images non tatouées (histogramme noir) et 400 images tatouées (histogramme gris).

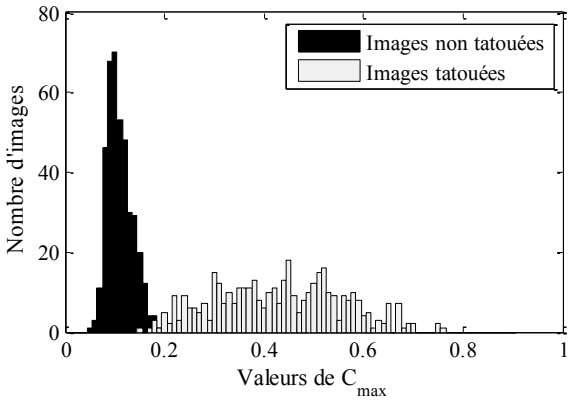


Figure 4-11- La densité de probabilité de C_{max} sous l'attaque impression/numérisation.

A titre indicatif, nous représentons dans la figure 4-12, un rappel de la figure 3-18-a du chapitre précédent pour comparaison. Cette figure représente cette même ddp pour 1000 images numériques tatouées et non tatouées sans attaque impression/numérisation.

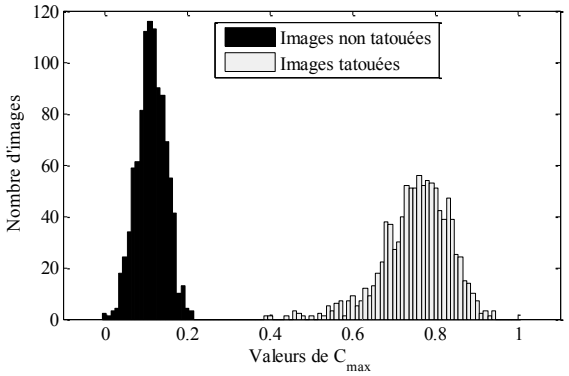
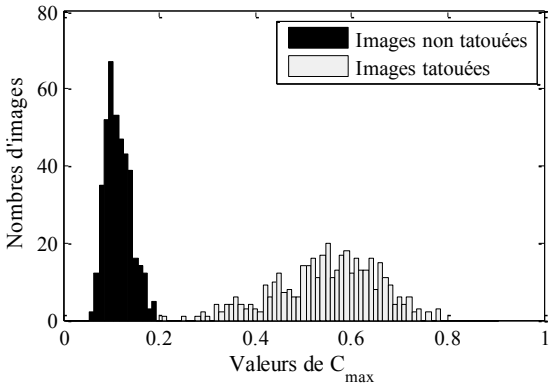


Figure 4-12- Rappel de la figure 3-18-a du chapitre 3 (sans attaque impression/numérisation).

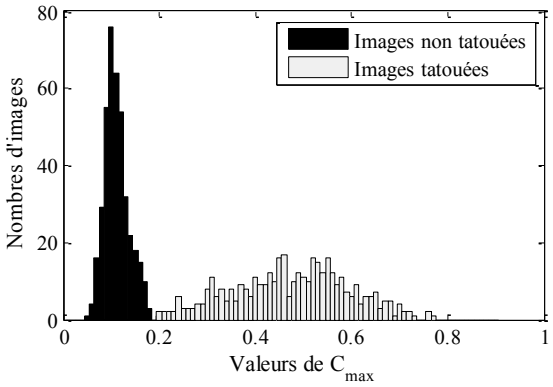
D'après les figures 4-11 et 4-12, l'impression/numérisation n'a que peu d'effet sur la densité de probabilité de $C_{\max}$ calculée à partir des images non tatouées. Par contre son effet sur celle obtenue par les images tatouées est significatif. L'histogramme se déplace très sensiblement vers la gauche lors de l'attaque impression/numérisation. Les deux distributions montrées dans la figure 4-11 ne sont pas bien séparées. Un chevauchement est observé dans la zone entre 0.15 et 0.20. Ce chevauchement engendre des erreurs lors de la détection. Il est espéré que les contre-attaques proposées améliorent les performances de la méthode.

4.5.1.1 Evaluation de la correction de flou

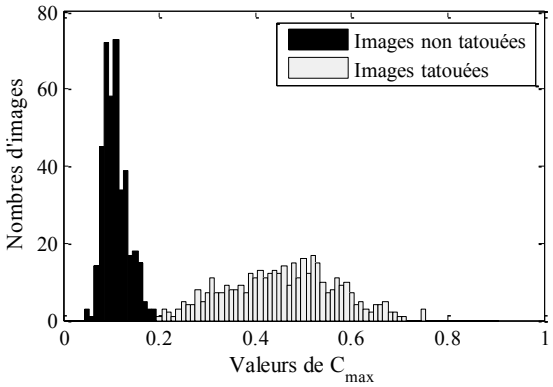
La première contre-attaque proposée dans ce travail est la correction du flou. Elle consiste à appliquer le filtre de Wiener en utilisant la réponse impulsionnelle et la variance du bruit estimées à partir de la chaîne d'impression/numérisation. Les résultats obtenus ont été comparés avec des méthodes de contre-attaques de la littérature, la déconvolution aveugle utilisée dans [A. Poljicak *et al.* 2012] et le filtre rehausseur dans [Yu *et al.* 2005]. Le filtre de Wiener, la déconvolution aveugle et le filtre rehausseur ont été appliqués aux images imprimées et scannées avant la détection de la marque. Les résultats obtenus par les trois méthodes de correction de flou sont présentés dans la figure 4-13 sous la forme des densités de probabilité de $C_{\max}$ des images non tatouées (histogramme noir) et des images tatouées (histogramme gris).



(*a*)



(*b*)



(*c*)

Figure 4-13- Densités de probabilité de C_{max} sous l'impression/numérisation après la correction du flou ; (*a*) avec le filtre de Wiener, (*b*) le filtre rehausseur, (*c*) la déconvolution aveugle.

La comparaison de la figure 4-11 et la figure 4-13 montre clairement que les trois méthodes de correction de flou améliorent la détection de la marque, le chevauchement entre les deux densités probabilité est réduit. Pour mieux analyser les résultats, les courbes ROC sont présentées dans la figure 4-14.

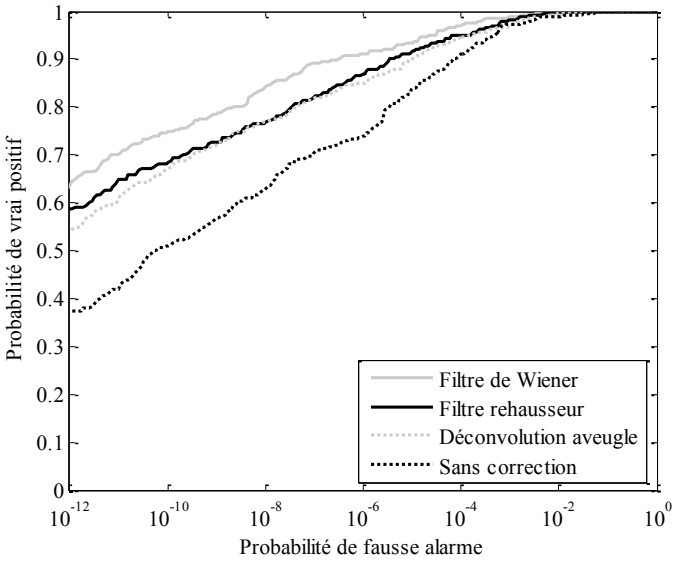


Figure 4-14- Courbe ROC des images tatouées sous l'attaque impression/numérisation avant et après la correction de flou.

Les courbes ROC montrent que la correction de flou par le filtre de Wiener est plus efficace que la correction par filtre rehausseur [Yu *et al.* 2005] par la déconvolution aveugle [A. Poljicak *et al.* 2012].

4.5.1.2 Evaluation de la correction colorimétrique

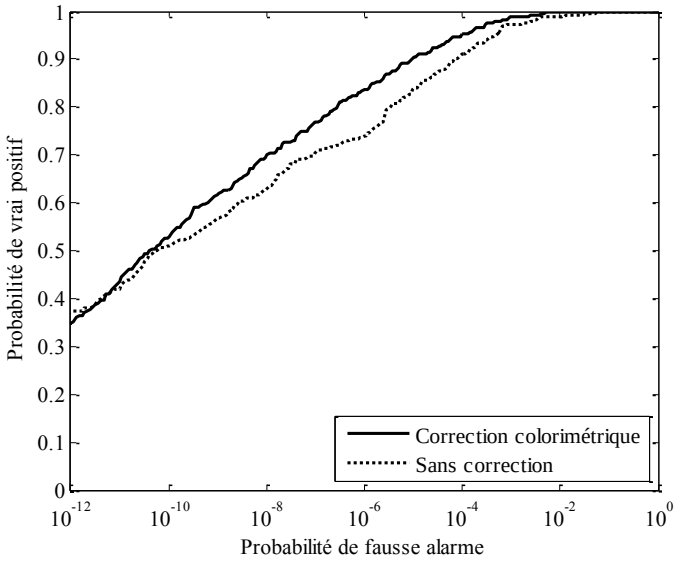
La deuxième contre-attaque proposée dans ce travail consiste en une correction colorimétrique des images dégradées. L'inverse des fonctions de dégradation des couleurs présentées dans la figure 4-9 ont été appliquées aux images imprimées et scannées. Un exemple de la correction colorimétrique d'une image est présenté dans la figure 4-15. Les résultats sont de bonne qualité en particulier dans les régions des cheveux et de la peau du visage. Après cette correction l'algorithme de détection est appliqué aux images imprimés et scannées. La figure 4-16 présente les courbes ROC sans et avec la correction colorimétrique.

(*a*) (*b*)

(*c*)

Figure 4-15- Résultats de la correction colorimétrique ; (*a*) l'image originale, (*b*) l'image imprimée/scannée, (*c*) l'image après la correction.

D'après la figure 4-16, la correction colorimétrique améliore légèrement les performances de méthode de tatouage lors de l'attaque impression/numérisation. La correction colorimétrique est combinée avec la correction de flou par le filtre de Wiener. Cette combinaison donne des bons résultats au niveau de la détection lors des dégradations de l'impression/numérisation. La figure 4-17 présente les courbes ROC obtenues sans contre-attaque, avec correction de flou par le filtre de Wiener seul et la combinaison du filtre de Wiener avec la correction colorimétrique.



0

Figure 4-16- Courbe ROC des images tatouées sous l'attaque impression/numérisation avant et après la correction colorimétrique.

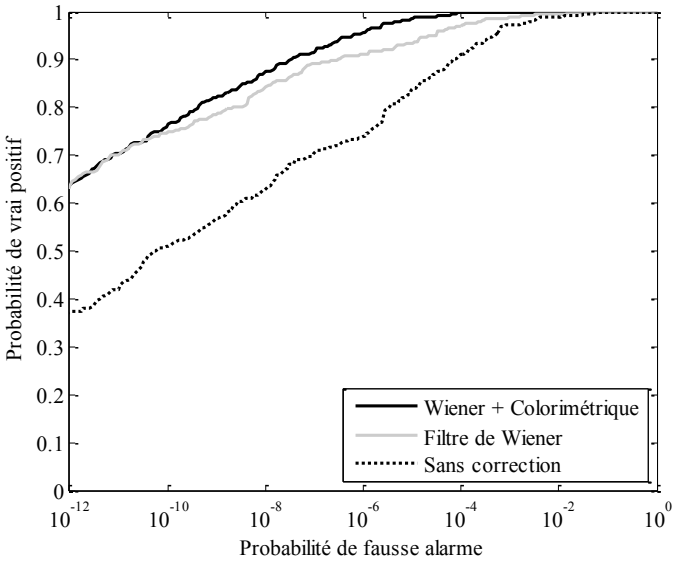


Figure 4-17- Courbe ROC des images tatouées sous l'attaque impression/numérisation avant et après la correction de flou et la correction colorimétrique.

4.5.1.3 Schéma complet et comparaison

Avant de passer à la comparaison de la méthode proposée avec une méthode dans la littérature, nous présentons notre schéma complet. Ce schéma est composé d'une méthode préventive qui consiste à filtrer l'image passe bas avant l'insertion de la marque et une méthode corrective basée sur des contre-attaques. Ces contre-attaques sont composées d'une correction du flou par le filtre de Wiener

et une correction colorimétrique après avoir estimé les différentes caractéristiques de la chaîne d'impression/numérisation. Comme l'indique la figure 4-18, la méthode préventive est appliquée avant l'insertion de la marque et la méthode corrective est appliquée après l'opération d'impression/numérisation et avant la détection de la marque.

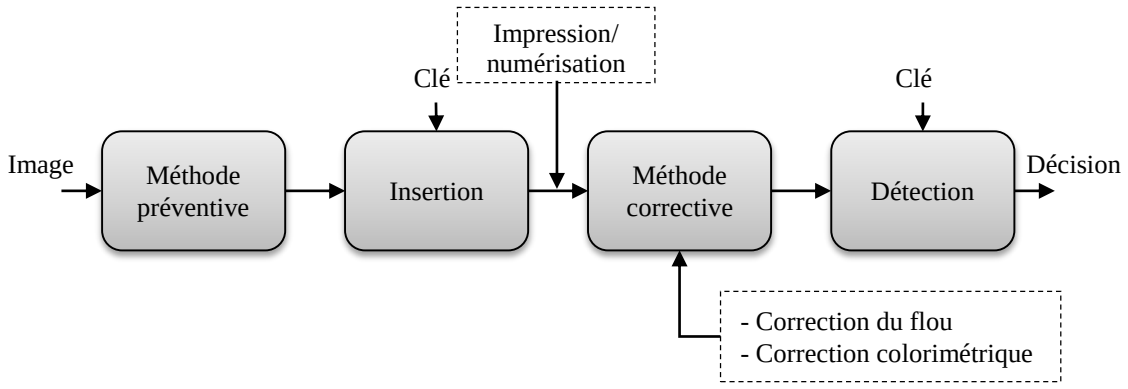


Figure 4-18- Schéma complet proposé dans ce travail.

La méthode proposée est comparée avec la méthode de tatouage présenté dans [Ante Poljicak *et al.* 2011]. Dans les deux méthodes de tatouage, nous avons fixé la valeur du PSNR des images tatouées à 40dB afin d'obtenir une comparaison équitable. Les images tatouées ont été imprimées sur des cartes en plastique puis scannées. Dans cette expérience, la méthode corrective (la combinaison de la correction de flou avec la correction colorimétrique) est appliquée seulement à la méthode de tatouage proposée dans ce travail. Les résultats sont présentés sous forme des courbes ROC dans la figure 4-19.

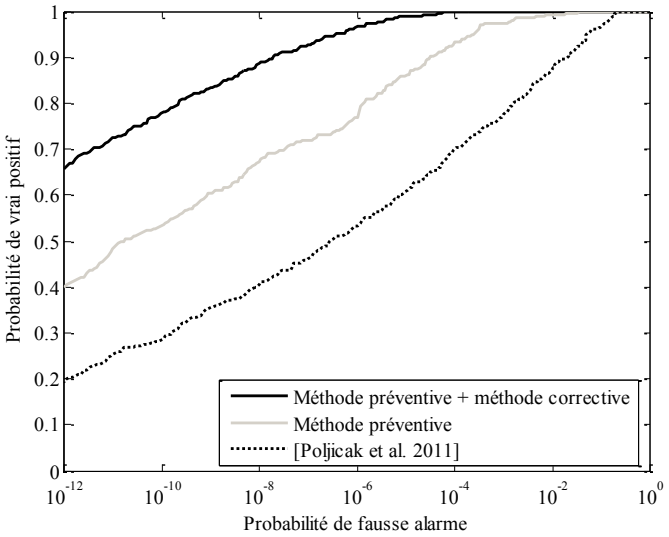


Figure 4-19- Courbe ROC des images tatouées sous l'attaque impression/numérisation avant et après la correction.

Les résultats finaux sont résumés dans le tableau 4-2. Pour chaque valeur fixe de la probabilité de fausse alarme, le seuil *t* est calculé. Les résultats correspondent au taux de détection (pourcentage des images tatouées déclarées comme image tatouées) pour la méthode présentée dans [Ante Poljicak *et al.* 2011], la méthode de tatouage proposée dans ce travail (méthode préventive avec réduction de la variance du vecteur support par filtrage) et finalement la méthode proposée plus la méthode corrective (filtrage de Wiener + correction colorimétrique). Les résultats obtenus montrent que la méthode de tatouage proposée présente de meilleures performances sous l'attaque impression/numérisation comparée à la méthode proposée dans [Ante Poljicak *et al.* 2011]. En plus la combinaison de la méthode corrective avec la méthode préventive améliore considérablement le taux de détection.

Tableau 4-2- Les résultats de la robustesse de la méthode proposée sous l'opération d'impression/numérisation.

Probabilité de fausse alarme (seuil)	**[Ante Poljicak *et al.* 2011]**	**Méthode preventive Seule**	**Méthode préventive et méthode corrective**
$P_{fa} = 10^{-3}$ **(*t* = 0.298)**	77.75%	97.75%	100%
$P_{fa} = 10^{-4}$ **(*t* = 0.334)**	70%	92.75%	99.75%
$P_{fa} = 10^{-5}$ **(*t* = 0.365)**	61%	85.75%	98.25%
$P_{fa} = 10^{-6}$ **(*t* = 0.393)**	53.5%	77.25%	96.75%

Il faut noter que les dégradations ne sont pas limitées à l'impression / numérisation dans la situation réelle de l'application industrielle. La carte d'identité et l'image imprimée sur celle-ci sont régulièrement exposées à une variété d'éléments potentiellement destructeurs tout au long de sa durée

de vie. Dans la section suivante nous présentons une étude de la robustesse du tatouage sous les attaques de vieillissement.

4.5.2 Les attaques de vieillissement

Les résultats présentés dans cette section sont ceux obtenus pour une attaque donnée appliquée aux 400 images tatouées après l'impression / numérisation. Il faut noter que les attaques présentées dans les tests sont plus agressives que les attaques naturelles, notre but est d'atteindre la limite de la méthode proposée.

4.5.2.1 Rayures

Dans ce teste des lignes verticales ou horizontales ont été ajoutées aux images imprimées et scannées, la figure 4-20 présente un exemple de l'ajout des lignes verticale a une image imprimée et scannée.

(*a*) (*b*)

Figure 4-20- Attaque par ajout de lignes verticales aléatoirement. (*a*) L'image sans distorsion, (*b*) ajout de 8 lignes.

4.5.2.2 Découpe de l'image

Cette attaque consiste à simuler l'apparition d'une tache noire dans l'image d'identité qui se produit soit lors de l'impression ou lors de l'utilisation du document d'identité. Des portions de différentes tailles et positions ont été supprimées de l'image imprimée et scannée. La figure 4-21 illustre la suppression de 5% des pixels de l'image soit un carré de 115×115 pixels.

(*a*) (*b*)

Figure 4-21- Suppression de 5% des pixels de l'image.

4.5.2.3 Flexion

L'attaque de flexion ou binding, a été simulée par la transformation en barillet, le facteur de distorsion prend les valeurs 0.01, 0.03 et 0.05 et les résultats de ce test sur une image imprimée puis scannée sont présentés dans la figure 4-22.

(*a*) (*b*)

Figure 4-22- Attaque par distorsion en barillet. (*a*) l'image sans distorsion, (*b*) distorsion avec un facteur k = 0.05.

4.5.2.3 Poussière

Il s'agit de tester le comportement des algorithmes face à des poussières qui se déposent sur la carte. Cette dernière est simulée par l'ajout d'un bruit impulsionnel (exemple sel et poivre) sur l'image. La figure 4-23 présente le résultat de cette simulation sur une image.

(*a*) (*b*)

Figure 4-23- Attaque par ajout de bruit impulsionnel, (*a*) l'image originale, (*b*) image bruitée avec une densité de bruit de 1%.

4.5.2.4 Attaques photométriques

La décoloration des images d'identité consiste à modifier la composante de saturation en pourcentage dans l'espace Teinte, Saturation, Luminosité (LST). La saturation varie de 0 à 255, elle représente l'intensité de la coloration d'une couleur, en d'autres termes, la saturation dénote la proximité par rapport au gris. Si la composante de saturation d'une image est égale à 0 alors l'image est en niveau de gris. Dans ce test, les images imprimées et scannées ont été transformées vers l'espace LST, puis nous avons diminué la composante de saturation avec différentes pourcentages. Le résultat de ce test est présenté dans la figure 4-24.

(*a*) (*b*)

Figure 4-24- Simulation de la décoloration ; (*a*) image originale, (*b*) l'image après modification de 50% de la composante de saturation.

4.5.2.4 Résultats et discussion

Sur la base expérimentale de 400 images imprimées et scannées puis attaquées avec les attaques de vieillissement simulées, nous avons mesuré le taux de détection pour chaque attaque. Les résultats sont présentés dans le tableau 4-3. Le seuil de détection est fixé à 0.334 pour une probabilité de fausse alarme $P_{fa} = 10^{-4}$.

Les tests présentés montrent que la méthode préventive proposée dans ce travail est plus performante que la méthode présentée dans [Ante Poljicak *et al.* 2011] en terme de la robustesse. Les résultats montrent que la combinaison de la méthode préventive et corrective conduit à des meilleurs résultats. Malgré les bons résultats obtenus, la méthode corrective est très sensible au bruit. Ceci est expliqué par le fait que la déconvolution d'image augmente les hautes fréquences dans l'image qui correspondant au bruit. L'effet du bruit impulsionnel peut être réduit par l'utilisation d'un filtre médian. Nous avons appliqué un filtre médian 3×3. Les résultats sont présentés entre parenthèses dans le tableau 4-3. Nous constatons que l'application du filtre médian améliore le taux de détection dans ce cas.

Tableau 4-3- Taux de détection sous l'attaque de vieillissement pour une $P_{fa} = 10^{-4}$.

Rayures	**Nombre de lignes**			
	2	**4**	**8**	**16**
Poljicak *et al.* [Ante Poljicak *et al.* 2011]	66.75%	66.25%	63.5%	61.25%
Méthode préventive	88.25%	87.75%	84.25%	81.25%
Méthode préventive et méthode corrective	98.5%	96.75%	89.75%	87.5%
Découpe de l'image	**Pourcentage de suppression**			
	1%	**3%**		**5%**
Poljicak *et al.* [Ante Poljicak *et al.* 2011]	66%	65.5%		62.25%
Méthode préventive	87.5%	86.75%		82.5%
Méthode préventive et méthode corrective	98.75%	98.25%		97.5%
Flexion	**Facteur de distorsion *k***			
	0.01	**0.03**		**0.05**
Poljicak *et al.* [Ante Poljicak *et al.* 2011]	65.75%	64.75%		61.25%
Méthode préventive	87.25%	86%		81.5%
Méthode préventive et méthode corrective	98.25%	96.75%		91.75%
Poussière	**Densité de bruit**			
	1%		**2%**	
Poljicak *et al.* [Ante Poljicak *et al.* 2011]	59.75% (61%)		57.75% (60.75%)	
Méthode proposée	79.25% (80.75%)		76.75% (80.5%)	
Méthode préventive et méthode corrective	74.75% (97.75%)		72.25% (96.25%)	
Décoloration	**Pourcentage de diminution**			
	20%	**50%**	**80%**	**100%**
Poljicak *et al.* [Ante Poljicak *et al.* 2011]	66.75%	66%	64.25%	62.75%
Méthode préventive	88.5%	87.25%	85.25%	83%
Méthode préventive et méthode corrective	99.15%	98.75%	95.25%	90.25%

4.6 Conclusion

Dans ce chapitre nous avons montré que le tatouage d'image permet de vérifier son authenticité grâce à une méthode préventive et une méthode corrective. La méthode préventive consiste à prétraiter l'image avant l'insertion de la marque en réduisant la variance du vecteur tatoué par filtrage passe bas ; la méthode corrective basée sur les contre-attaques (filtre de Wiener et correction colorimétrique), elle permet de replacer l'image dans le contexte favorable à la détection de la marque. Les attaques de vieillissement inhérentes à la vie des cartes rajoutent de la complexité car elles se combinent à l'attaque impression/numérisation déjà difficile à contre attaquer. Les tests que nous avons réalisés montrent que la méthode corrective proposée présente quelques limites en présence du bruit impulsionnel. L'application d'un filtre médian est efficace pour nettoyer l'image et par conséquence nous pouvons obtenir des bons taux de détection. Par contre si l'image n'est pas bruitée, le filtre médian modifiera la marque insérée. L'utilisation d'un filtre médian adaptatif pallierait certainement ce problème.

Conclusion générale

Dans cette thèse, nous nous sommes intéressés au problème du tatouage invisible d'image dans le cadre d'une application industrielle. Nos travaux ont essentiellement porté sur le tatouage d'images d'identité imprimées sur des documents type carte plastique. L'opération d'impression suivie d'une numérisation produit des attaques puissantes qui détériorent la marque insérée dans l'image d'identité. Les principales caractéristiques attendues de l'algorithme du tatouage sont l'invisibilité et la robustesse contre les attaques d'impression/numérisation et les attaques de vieillissement.

Nous avons débuté ce rapport de thèse par un chapitre de l'état de l'art du tatouage numérique. Dans ce chapitre, nous avons abordé les différentes phases de la conception d'une méthode de tatouage. Nous avons présenté un bref descriptif sur les méthodes de tatouage robuste aux transformations géométriques puis les raisons qui ont motivé notre choix des méthodes de tatouage dans le domaine de Fourier. Ce domaine d'insertion se caractérise par sa résistance contre les attaques géométriques globales.

Après avoir décrit les différentes méthodes de tatouage des images numériques, nous avons présenté dans le deuxième chapitre une étude détaillée des distorsions produites dans la phase d'impression/numérisation, ainsi que les modèles proposés et les solutions développées pour les éliminer ou les réduire. Ces distorsions sont divisées principalement en deux catégories ; les transformations géométriques affectant la position des pixels ainsi les distorsions qui affectent la valeur des pixels. En ce qui concerne les distorsions de la valeur des pixels plusieurs modèles ont été proposés mais finalement peu de contre-attaques ont été développées.

Notre première contribution dans le domaine du tatouage d'images est exposée dans le troisième chapitre. L'approche développée appartient aux schémas additifs avec une détection aveugle dans le domaine de la transformé de Fourier. Il s'agit d'une méthode préventive qui consiste à prétraiter l'image originale avant l'insertion de la marque. Nous avons montré que le coefficient de corrélation entre la marque et les coefficients tatoués est inversement proportionnel à la variance du vecteur support de la marque. Nous avons ensuite développé deux techniques pour réduire la variance de ce vecteur. La première consiste à une modification directe aux coefficients de l'insertion par l'application d'un filtre passe bas. La deuxième vise à diminuer la variance par sélection des coefficients de l'insertion selon leurs valeurs. Cette approche permet d'améliorer le taux de détection et d'accroitre la robustesse de l'algorithme. L'étude de l'imperceptibilité a montré que les deux techniques produisent des images tatouées avec une bonne qualité visuelle où le PSNR est fixé à 40dB et le MSSIM et supérieure à 0.96. L'approche mis au point possède des bonnes performances en termes de robustesse vis-à-vis des attaques numériques telles que la compression, l'ajout de bruit

et le filtrage, ainsi que contre les attaques géométriques telles que la rotation et le recadrage. Une comparaison avec la méthode de base qui fait référence présentée dans [Ante Poljicak *et al.* 2011] a démontré que les méthodes proposées permettent d'améliorer la robustesse du système de tatouage. En outre, on remarque que le schéma basé sur la sélection est plus performant que celui basé sur le filtrage des coefficients.

Lors de l'impression / numérisation, d'autres attaques interviennent et se combinent entre elles. Les plus importantes sont le flou et les variations des couleurs. Une analyse de ces problèmes nous a conduit à proposer une approche corrective dans le chapitre 4. Elle consiste à traiter les distorsions liées aux attaques d'impression / numérisation en deux phases. La première est une correction de flou en utilisant un filtre de Wiener adapté à la chaine d'impression / numérisation. La deuxième est une correction colorimétrique en utilisant une table de transcodage. Cette méthode a été testée sur des images d'identité imprimées sur des supports plastiques puis ensuite scannées. L'étude comparative présenté dans la section 4.5 montre que la méthode corrective proposée dans ce travail est plus performante que les méthodes de la littérature [Yu *et al.* 2005], [A. Poljicak *et al.* 2012].

Il existe des dégradations additionnelles à celles de l'impression/numérisation : il s'agit des attaques de vieillissement. L'image tatouée imprimée subit des dégradations naturelles au cours de l'utilisation du document d'identité. Dans ce travail, nous avons développé une série d'attaques simulant le vieillissement du document d'identité. Ces attaques ont pour objectif de tester la robustesse des méthodes de tatouage contre les distorsions produites lors de l'utilisation de documents officiels. Les résultats obtenus en termes de taux de détection montrent que la méthode de tatouage proposée présente de meilleures performances comparée à la méthode de référence proposée dans [Ante Poljicak *et al.* 2011]. Nous notons que la combinaison des méthodes corrective et préventive améliore considérablement le taux de détection. Le plus intéressant est que les deux méthodes ont un rôle complémentaire. A titre d'exemple, pour une probabilité de fausse alarme $P_{fa} = 10^{-4}$, nous avons obtenu une amélioration moyenne de 22% par rapport la méthode originale proposée dans [Ante Poljicak *et al.* 2011] avec la méthode préventive seule. La combinaison de la méthode préventive avec la méthode corrective donne un taux de détection supérieur à 99%. L'algorithme de détection peut détecter la présence de la marque en moins de 1 seconde pour à une image de 512×512 pixels avec un ordinateur classique ce qui est compatible avec l'application industrielle visée.

Bien que la stratégie présentée possède des performances considérables au niveau de l'invisibilité et la robustesse de la marque, les tests que nous avons réalisés montrent que la méthode corrective présente quelques limites en présence du bruit impulsionnel. L'application d'un filtre médian est efficace pour nettoyer l'image et par conséquence nous pouvons obtenir des bons taux de détection.

Par contre si l'image n'est pas bruitée, le filtre médian modifiera la marque insérée. L'utilisation d'un filtre médian adaptatif pallierait certainement ce problème.

Perspectives :

La méthode de tatouage proposée dans ce travail ne prend pas en compte l'aspect psycho-visuel lors l'insertion de la marque. De nombreux travaux exploitant les masques psycho-visuels (sensibilité au contraste, l'adaptation de luminance…) existent et ont démontré leur efficacité [Tang *et al.* 2015]. Dans nos travaux futurs, notre approche consistera à construire un modèle psycho-visuel qui prend en compte les propriétés les plus courantes du système visuel humain afin de déterminer le seuil de la détection visuelle généralement appelé le JND (Just Noticeable Distortion). L'objectif étant d'améliorer l'efficience de notre approche tout en maintenant sa simplicité.

Comme autre perspective, nous visons à développer une technique robuste aux attaques Print/Cam où la numérisation de l'image est effectuée à l'aide d'un smartphone équipé d'un appareil photographique numérique (ou APN). Dans ce cas, les distorsions produites sont plus compliquées que celles produites lorsque l'image est numérisée par un scanner. Dans le processus d'impression/numérisation avec un scanner, l'extraction de la marque est traitée comme un problème en deux dimensions mais dans le cas d'une caméra le processus devient un problème tridimensionnel. En conséquence, les transformations géométriques dans ce cas sont des transformations projectives. En plus des attaques géométriques, d'autres attaques interviennent avec l'utilisation d'une caméra, il s'agit des transformations radiométriques où la luminosité du milieu varie fortement. Cette luminosité est variable selon la présence d'une ou plusieurs sources de lumière de différentes couleurs et directions. Les travaux existant sont encore émergeants, mais les applications industrielles des méthodes de tatouage robustes aux attaques Print/Cam sont réelles.

Bibliographie

Agarwal, C., A. Mishra and A. Sharma. 2013. Gray-scale image watermarking using GA-BPN hybrid network. *Journal of Visual Communication and Image Representation* 24(7): 1135-1146.

Alattar, A. M. 2000. Smart images using Digimarc's watermarking technology. *Electronic Imaging*, International Society for Optics and Photonics.

Ambadiyil, S., K. S. Soorej and V. P. M. Pillai. 2015. Biometric Based Unique ID Generation and One to One Verification for Security Documents. *Procedia Computer Science* 46: 507-516.

Amiri, S. H. and M. Jamzad. 2014. Robust watermarking against print and scan attack through efficient modeling algorithm. *Signal Processing: Image Communication* 29(10): 1181-1196.

Bailey, D. G. 2002. A new approach to lens distortion correction. *Image and Vision Computing* New Zealand

Barni, M. 2005. Effectiveness of exhaustive search and template matching against watermark desynchronization. *IEEE Signal Processing Letters* 12(2): 158-161.

Barni, M. and F. Bartolini. 2004. Watermarking systems engineering: enabling digital assets security and other applications, CRC Press.

Bas, P. 2000. Méthodes de tatouage d'images basées sur le contenu, Institut national polytechnique de Grenoble, Grenoble, FRANCE.

Bas, P., J. M. Chassery and B. Macq. 2002. Image watermarking: an evolution to content based approaches. *Pattern Recognition* 35(3): 545-561.

Boust, C. and H. Chaine. 2005. La qualité des images imprimées. *Ecole d'Hiver sur l'Image Numérique Couleur, Laboratoire d'Automatique, Génie Informatique et Signal, Lille*

Brauers, J., C. Seiler and T. Aach. 2010. Direct PSF estimation using a random noise target. *IS&T/SPIE Electronic Imaging*, International Society for Optics and Photonics.

Briassouli, A. and M. G. Strintzis. 2004. Locally optimum nonlinearities for DCT watermark detection. *IEEE Trans Image Process* 13(12): 1604-1617.

Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt. 2010. Digital image steganography: Survey and analysis of current methods. *Signal Processing* 90(3): 727-752.

Chen, B. and G. W. Wornell. 2001. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory* 47(4): 1423-1443.

Cheng, Q. and T. S. Huang. 2001. An additive approach to transform-domain information hiding and optimum detection structure. *IEEE Transactions on Multimedia* 3(3): 273-284.

Cox, I., M. Miller, J. Bloom, J. Fridrich and T. Kalker. 2007. Digital watermarking and steganography, Morgan Kaufmann.

Cox, I. J. and M. L. Miller. 2001. Electronic watermarking: the first 50 years. *IEEE Fourth Workshop on Multimedia Signal Processing*.

Cox, I. J. and M. L. Miller. 2004. Facilitating Watermark Insertion by Preprocessing Media. *EURASIP Journal on Advances in Signal Processing* 2004(14): 2081-2092.

Cox, I. J., J. Kilian, F. T. Leighton and T. Shamoon. 1997. Secure spread spectrum watermarking for multimedia. *IEEE Trans Image Process* 6(12): 1673-1687.

Degara-Quintela, N. and F. Perez-Gonzalez. 2003. Visible encryption: using paper as a secure channel.

Derraz, F., M. Beladgham and M. h. Khelif. 2004. Mesure Objective de la Qualité d'Image Médicale Dérivée de l'Index de Similarité Structurelle, Tlemcen - ALGERIE.

Dharwadkar, N. V. and B. Amberker. 2009. Secure Watermarking Scheme for Color Image Using Intensity of Pixel and LSB Substitution. *Journal of Computing* 1(1): 1-6.

Dong, P., J. G. Brankov, N. P. Galatsanos, Y. Yang and F. Davoine. 2005. Digital watermarking robust to geometric distortions. *IEEE Trans Image Process* 14(12): 2140-2150.

Douzi, H., D. Mammass and F. Nouboud. 2001. Faber-Schauder Wavelet Transform, Application to Edge Detection and Image Characterization. *Journal of Mathematical Imaging and Vision* 14(2): 91-101.

El-Hajji, M. 2012. La sécurité d'images par le tatouage numérique dans le domaine d'ondelettes, Université Ibnou Zohr, Faculté des Sciences, Agadir.

El Hajji, M., H. Douzi, D. Mammass, R. Harba and F. Ros. 2012. New image watermarking algorithm based on mixed scales wavelets. *Journal of Electronic Imaging* 21(1): 013003-013001-013003-013007.

Emami, M. S., K. Omar, S. Sahran and S. N. H. S. Abdullah. 2014. Spatial Domain Approaches for Real-Time Ownership Identification.

Furon, T. and P. Bas. 2013. A New Measure of Watermarking Security Applied on QIM. Information Hiding. M. Kirchner etD. Ghosal, Springer Berlin Heidelberg. 7692**:** 207-223.

Gao, G.-y. and G.-p. Jiang. 2011. Zero-bit watermarking resisting geometric attacks based on composite-chaos optimized SVR model. *The Journal of China Universities of Posts and Telecommunications* 18(2): 94-101.

Gonzalez, R. C. and R. E. Woods. 2007. Digital image processing, Prentice Hall.

Gupta, V. and A. Barve. 2014. A review on image watermarking and its techniques. *International Journal of Advanced Research in Computer Science and Software Engineering* 4(1): 92-97.

Iliyasu, A. M., P. Q. Le, F. Dong and K. Hirota. 2012. Watermarking and authentication of quantum images based on restricted geometric transformations. *Information Sciences* 186(1): 126-149.

Imprimante-info. 2012. "Actualité et resources pour imprimantes." Retrieved 23/12/2014, from http://www.imprimante-info.com/.

In-Kwon, Y. and K. Hyoung Joong. 2003. Modified patchwork algorithm: a novel audio watermarking scheme. *IEEE Transactions on Speech and Audio Processing* 11(4): 381-386.

Kasprzak, W., M. Stefańczyk and J. Popiołkiewicz. 2013. The Print-Scan Problem in Printed Steganography of Face Images. *Proceedings of the 8th International Conference on Computer Recognition Systems CORES 2013*, Springer.

Khan, M. and T. Shah. 2014. A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics. *Neural Computing and Applications* 26(4): 845-855.

Kundu, M. K. and A. K. Maiti. 2006. An Inexpensive Digital Watermarking Scheme for Printed Document. *IET International Conference on Visual Information Engineering.*

Kutter, M. and F. A. P. Petitcolas. 1999. Fair benchmark for image watermarking systems. *Security and Watermarking of Multimedia Contents*.

Leppla, M. and N. Richart. 2001, 2003. "KleoColor Training by QUBYX." Retrieved 15 Juin, 2015, from http://www.kleocolor.com/.

Lichtenauer, J. F., I. Setyawan, T. Kalker and R. L. Lagendijk. 2003. Exhaustive geometrical search and the false positive watermark detection probability.

Licks, V. and R. Jordan. 2000. On digital image watermarking robust to geometric transformations. *International Conference on Image Processing*, IEEE.

Lin, C.-Y. and S.-F. Chang. 1999. Distortion modeling and invariant extraction for digital image print-and-scan process. *Proceedings of International Symposium on Multimedia Information Processing*.

Lin, C. Y., M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller and Y. M. Lui. 2001. Rotation, scale, and translation resilient watermarking for images. *IEEE Trans Image Process* 10(5): 767-782.

Liu, L., T. Guan and Z. Zhang. 2013. Broadcast monitoring protocol based on secure watermark embedding. *Computers & Electrical Engineering* 39(7): 2299-2305.

Loukhaoukha, K. 2011. Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective, Université Laval.

Lubin, J. 1997. A human vision system model for objective picture quality measurements. *International Broadcasting Convention, 1997.*

Luisier, F., T. Blu and M. Unser. 2011. Image denoising in mixed Poisson-Gaussian noise. *IEEE Trans Image Process* 20(3): 696-708.

Mairgiotis, A., L. Kondi and Y. Yongyi. 2013. Locally optimum detection for additive watermarking in the DCT and DWT domains through non-Gaussian distributions. *Digital Signal Processing (DSP), 2013 18th International Conference on*.

Mallat, S. G. 1987. A theory for multiresolution signal decomposition: the wavelet representation.

Malvido, A., F. Pérez-González and A. Cousiño. 2006. A novel model for the print-and-capture channel in 2D bar codes. Multimedia Content Representation, Classification and Security, Springer**:** 627-634.

Miller, M. and J. Bloom. 2000. Computing the Probability of False Watermark Detection. Information Hiding. A. Pfitzmann, Springer Berlin Heidelberg. 1768**:** 146-158.

Ming-Sui, L. and C. Yu-Hsiang. 2010. Image recovery of geometric distortion with multi-bit data embedding. *IEEE International Conference on Multimedia and Expo (ICME)*.

Mitrea, M., F. Prêteux, A. Vlad and C. Fetita. 2004. The 2D-DCT coefficient statistical behaviour: a comparative analysis on different types of image sequences. *Journal of Optoelectronics and Advanced Materials* 6(1): 95-102.

Moorthy, A. K. and A. C. Bovik. 2010. A Two-Step Framework for Constructing Blind Image Quality Indices. *IEEE Signal Processing Letters* 17(5): 513-516.

Nakamura, S. 1993. Applied numerical methods in C, Prentice-Hall, Inc.

Nan, L., W. Quan and Z. Kefeng. 2012. A Print-Scan Modeling Scheme Based on BP Neural Network. *International Conference on Computational Intelligence and Security (CIS)*.

Nasir, I., F. Khelifi, J. Jiang and S. Ipson. 2012. Robust image watermarking via geometrically invariant feature points and image normalisation. *IET Image Processing* 6(4): 354-363.

Nguyen, P. B. 2011. On The Use of Human Visual System Modelling in Watermarking, Université de Paris 13.

Nikolaidis, N. and I. Pitas. 1998. Robust image watermarking in the spatial domain. *Signal Processing* 66(3): 385-403.

Nikolaidis, N., V. Solachidis, A. Tefas, V. Arguriou and I. Pitas. 2002. Benchmarking of still image watermarking methods: Principles and state of the art. *Proc. of Electronic Imaging and the Visual Arts (EVA2002)*.

Pereira, S. and T. Pun. 2000. Robust template matching for affine resistant image watermarks. *IEEE Trans Image Process* 9(6): 1123-1129.

Petitcolas, F. A. P. 2000. Watermarking schemes evaluation. *IEEE Signal Processing Magazine* 17(5): 58-64.

Picard, J., C. Vielhauer and N. Thorwirth. 2004. Towards fraud-proof id documents using multiple data hiding technologies and biometrics. *Electronic Imaging*, International Society for Optics and Photonics.

Poljicak, A., L. Mandic and D. Agic. 2011. Discrete Fourier transform–based watermarking method with an optimal implementation radius. *Journal of Electronic Imaging* 20(3): 033008-033008-033008.

Poljicak, A., L. Mandic and M. Strgar Kurecic. 2012. Improvement of the watermark detector performance using image enhancement filters. *19th International Conference on Systems, Signals and Image Processing (IWSSIP)*.

Qiao, L. and I. J. Cox. 2007. Improved Spread Transform Dither Modulation using a Perceptual Model: Robustness to Amplitude Scaling and JPEG Compression. *IEEE International Conference on Acoustics, Speech and Signal Processing. ICASSP*.

Rivoire, A. 2012. Contributions au guillochage et à l'authentification de photographies, Université Jean Monnet-Saint-Etienne.

Ros, F., J. Borla, F. Leclerc, R. Harba and N. Launay. 2006. An industrial watermarking process for plastic card supports. *IEEE International Conference on Industrial Technology, 2006. ICIT 2006.*, IEEE.

Ruanaidh, J. J. K. Ò. and T. Pun. 1998. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing* 66(3): 303-317.

Schimke, S., S. Kiltz, C. Vielhauer and T. Kalker. 2005. Security analysis for biometric data in ID documents. *Security, Steganography, and Watermarking of Multimedia Contents VII*.

Sharif, Z. and A. Z. Sha'ameri. 2007. The Application of Cross Correlation Technique for Estimating Impulse Response and Frequency Response of Wireless Communication Channel. *Student Conference on Research and Development (SCOReD)*, IEEE.

Shi, D., Q. Wang and C. Liang. 2008. Digital Watermarking Algorithm for Print-and-Scan Process Used for Printed Matter Anti-counterfeit. *Congress on Image and Signal Processing, 2008. CISP '08.* .

Shukla, D. and M. Sharma. 2012. A Comparative Analysis of Watermarking Techniques for Copy Protection of Digital Images. Advances in Computer Science and Information Technology. Computer Science and Engineering. N. Meghanathan, N. Chaki etD. Nagamalai, Springer Berlin Heidelberg. 85**:** 313-318.

Smoaca, A. 2011. ID Photograph hashing: a global approach, Université Jean Monnet-Saint-Etienne; Université Politehnica (Bucarest, Roumanie).

Solachidis, V. and L. Pitas. 2001. Circularly symmetric watermark embedding in 2-D DFT domain. *IEEE Trans Image Process* 10(11): 1741-1753.

Solanki, K., U. Madhow, B. S. Manjunath and S. Chandrasekaran. 2005. Modeling the print-scan process for resilient data hiding.

Solanki, K., U. Madhow, B. S. Manjunath, S. Chandrasekaran and I. El-Khalil. 2006. `Print and Scan' Resilient Data Hiding in Images. *IEEE Transactions on Information Forensics and Security* 1(4): 464-478.

Suhail, M. A. and M. S. Obaidat. 2003. Digital watermarking-based DCT and JPEG model. *IEEE Transactions on Instrumentation and Measurement* 52(5): 1640-1647.

Surekha, B. and G. Swamy. 2013. Sensitive Digital Image Watermarking for Copyright Protection. *IJ Network Security* 15(2): 113-121.

Sweldens, W. 1998. The lifting scheme: A construction of second generation wavelets. *SIAM Journal on Mathematical Analysis* 29(2): 511-546.

Tanaka, K., Y. Nakamura and K. Matsui. 1990. Embedding secret information into a dithered multi-level image. *Conference Record, A New Era. IEEE Military Communications Conference, 1990. MILCOM '90,* .

Tang, W., W. Wan, J. Liu and J. Sun. 2015. Improved Spread Transform Dither Modulation Using Luminance-Based JND Model. Image and Graphics. Y.-J. Zhang, Springer International Publishing. 9218**:** 430-437.

Villan, R., S. Voloshynovskiy, O. Koval and T. Pun. 2006. Multilevel 2-D Bar Codes: Toward High-Capacity Storage Modules for Multimedia Security and Management. *IEEE Transactions on Information Forensics and Security* 1(4): 405-420.

Voloshynovskiy, S., A. Herrigel, N. Baumgaertner and T. Pun. 2000. A Stochastic Approach to Content Adaptive Digital Image Watermarking. Information Hiding. A. Pfitzmann, Springer Berlin Heidelberg. 1768**:** 211-236.

Voloshynovskiy, S., S. Pereira, V. Iquise and T. Pun. 2001. Attack modelling: towards a second generation watermarking benchmark. *Signal Processing* 81(6): 1177-1214.

Wang, Z., A. C. Bovik, H. R. Sheikh and E. P. Simoncelli. 2004. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing* 13(4): 600-612.

Watson, A. B. and J. A. Solomon. 1997. Model of visual contrast gain control and pattern masking. *J Opt Soc Am A Opt Image Sci Vis* 14(9): 2379-2391.

Xueyi, Y., C. Xueting, D. Meng and W. Yunlu. 2014. A SIFT-based DWT-SVD blind watermark method against geometrical attacks. *Image and Signal Processing (CISP), 2014 7th International Congress on*.

Yu, L., X. Niu and S. Sun. 2005. Print-and-scan model and the watermarking countermeasure. *Image and Vision Computing* 23(9): 807-814.

Zarmehi, N., M. Banagar and M. A. Akhaee. 2013. Optimum decoder for an additive video watermarking with Laplacian noise in H.264. *Information Security and Cryptology (ISCISC), 2013 10th International ISC Conference on*.

Zhao, J. 2015. Robust Image Watermarking Algorithm Based on Radon and Analytic Fourier-Mellin Transforms. *Open Automation and Control Systems Journal* 7: 1071-1074.

Bibliographie de l'auteur

Revues:

R. Riad, H. Douzi, M. El-hajji, R. Harba, F. Ros, "A Print-Scan Resilient Watermarking based on Fourier Transform and Image Restoration". *International Journal of Computer Applications*, Published by Foundation of Computer Science (FCS), NY, USA. Vol. 128(15), pp.13-17, October 2015.

Chapitre de livre

R. Riad, M. El-hajji, H. Douzi, R. Harba, F. Ros, "Evaluation of a Fourier Watermarking Method Robustness to Cards Durability Attacks," *Lecture Notes in Computer Science, edited by Springer*. Vol. 8509, pp. 280-288, 2014.

Communications Internationales

R. Riad, F. Ros, R. Harba, H. Douzi, M. El-hajji, "Pre-Processing the Cover Image before Embedding Improves the Watermark Detection Rate," *The 2nd World Conference on Complex Systems*, edited by IEEE, pp. 705-709, 10-12 November 2014, Agadir, Morocco.

R. Riad, R. Harba, H. Douzi, M. El-hajji, F. Ros, "Print-and-Scan Counterattacks for Plastic Card Supports Fourier Watermarking," *IEEE International Symposium on Industrial Electronics* (ISIE), pp. 1036-1041, 01-04 June 2014. Istanbul, Turkey.

M. El-hajji, R. Riad, H. Douzi, "Improved Watermarking Algorithm Based on DWT-Mixed Scales Using SVD," *International Symposium on Operational Research and Applications*, pp. 164-168, May 8-10, 2013. Marrakesh, Morocco.

R. Riad, A. Ibhi, H. Douzi, M. Elhajji, O. Rozenbaum, R. Harba and R. Jennane, "Investigation of the Meteorites Porosity by X-ray Tomography and 3D Image Processing," *The 2nd World Conference on Complex Systems*, edited by IEEE, pp. 710 - 714, 10-12 November 2014, Agadir, Morocco.

Revues en cours d'évaluation

R. Riad, R. Harba, H. Douzi, F. Ros, "M. El-hajji, Robust Fourier watermarking for ID images on plastic card supports," (Soumis).

R. Riad, R. Harba, F. Ros, H. Douzi, M. El-hajji, "A Preventive and Curative watermarking scheme for ID smart card support," (Soumis).

Rabia RIAD

Tatouage robuste d'images imprimées

Résumé :

Le tatouage invisible d'images d'identité imprimées sur un support en plastique est un problème difficile qui intéresse le monde industriel. Dans cette étude, nous avons développé un algorithme de tatouage robuste aux diverses attaques présentes dans ce cas. Ces attaques sont liées aux processus d'impression/numérisation sur le support plastique ainsi qu'aux dégradations qu'une carte plastique peut rencontrer le long de sa durée de vie. La méthode de tatouage opère dans le domaine de Fourier car cette transformée présente des propriétés d'invariances aux attaques géométriques globales. Une méthode préventive consiste en un prétraitement de l'image originale avant le processus d'insertion qui réduit la variance du vecteur support de la marque. Une méthode corrective comporte deux contre-attaques corrigeant le flou et les variations colorimétriques. Pour une probabilité de fausse alarme de 10^{-4}, nous avons obtenu une amélioration moyenne de 22% par rapport à la méthode de référence lorsque seule la méthode préventive est utilisée. La combinaison de la méthode préventive avec la méthode corrective correspond à un taux de détection supérieur à 99%. L'algorithme de détection prends moins de 1 seconde pour à une image de 512×512 pixels avec un ordinateur classique ce qui est compatible avec l'application industrielle visée.

Mots-clés : tatouage d'image, documents d'identité, impression/numérisation, transformée de Fourier, prétraitement, filtre de Wiener, correction colorimétrique.

Robust Watermarking for printed images

Abstract :

Invisible watermarking for ID images printed on plastic card support is a challenging problem that interests the industrial world. In this study, we developed a watermarking algorithm robust to various attacks present in this case. These attacks are mainly related to the print/scan process on the plastic support and the degradations that an ID card can encounter along its lifetime. The watermarking scheme operates in the Fourier domain as this transform has invariance properties against global geometrical transformations. A preventive method consists of pre-processing the host image before the embedding process that reduces the variance of the embeddable vector. A curative method comprises two counterattacks dealing with blurring and color variations. For a false alarm probability of 10^{-4}, we obtained an average improvement of 22% over the reference method when only preventative method is used. The combination of the preventive and curative methods leads to a detection rate greater than 99%. The detection algorithm takes less than 1 second for a 512×512 image with a conventional computer, which is compatible with the industrial application in question.

Keywords: Image watermarking, ID documents, Print/scan, Fourier transform, Preprocessing, Wiener filter, Color correction.

Laboratoire PRISME – Pôle IRAuS, Axe Image et Vision
Polytech'Orléans, 12 Rue de Blois, BP 6744 45067
Orléans Cedex 2 France.

Laboratoire IRF-SIC, Faculté des Sciences d'Agadir
Université Ibn Zohr BP 8106 - Cité Dakhla, 80000 Agadir,
Maroc.