REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE.

UNIVERSITE MENTOURI CONSTANTINE
FACULTE DES SCIENCE DE L'INGENIEUR.
DEPARTEMENT D'ELECTRONIQUE.

MEMOIRE

Présenté pour obtenir
le Diplôme de Magister En Electronique.

Option : Traitement du signal.

par

Mr : **BOUAB MOHAMMED**.

TATOUAGE D'IMAGES BASE SUR DES PROPRIETES PSYCHOVISUELLES

Devant le jury :

PRESIDENT :	**BENNIA ABDELHAK**	**Prof**
RAPPORTEUR:	**MOHAMMED KHAMADJA**	**Prof**
EXAMINATEURS :	**CHAREF ABDELFATAH**	**Prof**
	BAATOUCHE MOHAMMED CHAWKI	**Prof**

Table des matières

Sommaire

Chapitre 2 : METHODE DE TATOUAGE DEVELOPPEE

Chapitre 3 : RESULTATS

INTRODUCTION

L'ère numérique que nous traversons depuis quelques années a permis un accès à l'information bien plus aisé que par le passé. Les documents numériques étant immatériels, leur diffusion est extrêmement rapide et peu coûteuse. Les réseaux et les supports numériques de forte capacité facilitent les échanges de documents [32].

Avec l'apparition de ces nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité. Une image numérique, diffusée par exemple sur Internet, peut être aisément copiée puis rediffusée sur un réseau ou stockée sur CD-ROM sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le ***tatouage*** ou ***watermarking***. Le principe des techniques dites de tatouage d'images consiste en l'insertion d'une marque imperceptible dans l'image. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée "signature", correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les attaques (licites ou illicites) que l'image tatouée subit, la marque doit rester présente tant que l'image reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée). De nombreux algorithmes ont été présentés récemment et certains produits sont même commercialisés, cependant, aucun d'eux ne satisfait pleinement au cahier des charges idéal [1].

Le travail présenté dans ce mémoire a pour objectif de proposer une méthode de tatouage des images numériques fondée sur la décomposition en d'ondelettes. Le principe consiste en l'insertion d'une signature chaotique dans l'image en exploitant l'analogie entre la transformée en ondelettes et le modèle du système visuel humain et l'estimation de la sensibilité de l'oeil humain au bruit pour moduler et adapter la signature selon les caractéristiques locales de l'image. Une technique d'estimation de mouvement différentielle est utilisée pour compenser les éventuelles déformations géométriques subies par l'image tatouée.

Le présent mémoire est organisé en trois chapitres :

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

Le deuxième chapitre de ce rapport présente l'essentiel de notre travail et les différentes étapes nécessaires à la mise en œuvre de la technique de tatouage proposée. L'ajout d'une signature chaotique aux coefficients résultants de la transformée en ondelettes s'appuie sur une étude psychovisuelle de l'image, afin d'optimiser le compromis robustesse/invisibilité. L'utilisation de la mise en correspondance des images nous permet de combattre les déformations géométriques subies par une image tatouée.

Le dernier chapitre conclut notre travail en présentant les résultants obtenus et les performances de la méthode de tatouage proposée.

1. INTRODUCTION

Le tatouage des données numériques est une discipline récente qui trouve son origine dans le manque de techniques fiables de protection de ce type de données. En effet, associé à d'autres techniques, cet axe de recherche a pour but de résoudre des problèmes aussi variés que la protection du copyright et des droits d'auteurs, la réglementation des copies, la prévention de la redistribution non autorisée, le suivi de documents et l'intégrité du contenu d'une donnée [1] [2].

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

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

Enfin, nous ajoutons à ces méthodes d'autres techniques qui rendent l'algorithme plus performant, nous distinguons les méthodes basées sur les modèles perceptifs du système visuel humain (SVH) et la catégorie des schémas qui permet une synchronisation de la signature lors de la détection, nous présentons notamment diverses attaques susceptibles d'empêcher la détection de la signature.

2. AUX ORIGINES DU TATOUAGE

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

2.1. La cryptographie

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

La cryptographie est une discipline très vieille, des techniques ont été mises en place dés le V^{ème} siècle avant JC. Elle consiste à transformer un message pour qu'il devienne illisible. Seule la connaissance d'une clef et du moyen de cryptage peut permettre de décoder le message afin de le rendre lisible. Alors que pour le tatouage, la donnée tatouée est disponible, diffusée et exploitable, la donnée cryptée est elle inexploitable sans la connaissance des clés de déverrouillage de l'algorithme de cryptage. En fait les deux disciplines sont considérées comme complémentaires puisque d'un coté la cryptographie tend à renforcer le contrôle d'accès aux données, leur authenticité et leur intégrité, d'un autre coté le tatouage tend à lier le contenu des données avec des informations auxiliaires[5].

2.2. La stéganographie

Le terme stéganographie vient du mot Grec *steganos* signifiant *caché* et de *graphia* signifiant *écriture*, littéralement on traduit par *écriture cachée* [2]. Elle consiste à dissimuler un message dans un autre. Ainsi, seule la personne connaissant le procédé de dissimulation peut lire le message caché. Contrairement à la cryptographie, la stéganographie est "invisible". La différence entre la stéganographie et le tatouage, est que dans la stéganographie, l'existence d'un message caché doit rester secrète alors que pour le tatouage seul le message doit rester caché mais son existence (tant qu'on ne peut le détecter) peut être connue.

3. PRINCIPES GENERAUX D'UNE METHODE DE TATOUAGE

Afin d' étudier les différents aspects du problème de tatouage, selon les applications particulières et ses exigences, nous devons clarifier le modèle général du tatouage.

Un schéma classique de tatouage des images peut se décomposer en deux étapes fondamentales :

- La phase d'insertion.
- La phase de détection.

3.1. La phase d'insertion

La figure 1.1 présente le schéma général d'implémentation de la marque [3]. L'insertion de la marque dans une image hôte I permet d'obtenir une image tatouée notée I_W. L'espace d'insertion $T(I)$ peut être le domaine spatial on bien le résultat d'une transformation réversible qui facilite l'insertion comme la Transformée en Cosinus Discrète (TCD), la Transformée de Fourier Discrète (TFD) ou encore une Transformation par Ondelettes (TOD). La marque insérée W, également désignée sous le terme de *signature* ou de *tatouage*, dépend d'une clé secrète K mais aussi du message $\{b_0, b_1, ..., b_{n-1}\}$ que l'on désire insérer. Cette signature peut être une séquence pseudo aléatoire possédant certaines propriétés (distribution gaussienne ou uniforme), une donnée binaire {-1, +1} ou bien une petite image (logo).

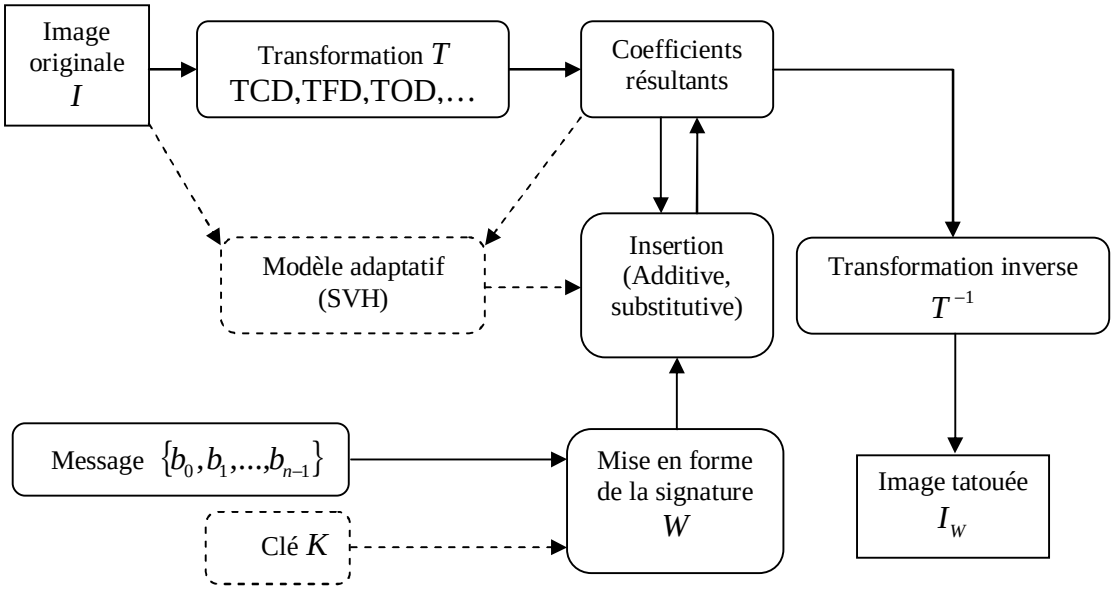


Figure 1.1 Schéma général du processus d'insertion d'une signature.

L'utilisation d'un modèle *psychovisuel* adaptatif permet de contrôler et d'augmenter la force de la signature. Notons que par le choix d'un domaine fréquentiel approprié tout en choisissant seulement certains coefficients, beaucoup de systèmes visuels humains (SVH) [4] peuvent être effectués implicitement. Plus la transformation de l'image approche les propriétés du SVH, plus il est facile de mettre plus d'énergie dans l'image hôte sans produire une déformation perceptible**.**

3.2. Phase de détection

La détection de la signature *W* et l'extraction du message *m* incorporé ont pour rôle d'attester si la signature est ou non présente dans l'image. Si la signature est présente, le message qui lui est associé peut ensuite être décodé.

Selon les différents algorithmes, l'image originale et la clé secrète peuvent être ou non nécessaires lors de la détection. Nous allons ici énumérer et caractériser ces différents processus :

- **Les schémas non-aveugles** : La détection est dite "non-aveugle" si l'image originale et la clé secrète (privée) sont nécessaires.
- **Les schémas semi-aveugles**: Une détection "semi-aveugle" n'utilise pas l'image originale, mais elle se base sur quelques caractéristiques dérivées de cette dernière.
- **Les schémas aveugles** : c'est le cas où l'image originale n'est pas disponible pendant le processus d'extraction, si la clé privée est aussi absente la détection est dite à *clé publique*.
- **Les schémas asymétriques** : la détection par algorithmes asymétriques peut être schématisée comme une détection aveugle, ces algorithmes utilisent des clés différentes pour insérer et détecter la marque.

D'une manière générale, la robustesse d'un schéma "non-aveugle" est plus importante que celle d'un schéma "aveugle". L'image originale fournit une référence pouvant servir à améliorer l'estimation de la signature ou encore à identifier les divers traitements subis par l'image tatouée.

La figure 1.2 présente le processus de détection global [3]. La marque extraite W' est comparée à la marque originale W par mesure de corrélation. La mesure de similitude la plus utilisée entre W et W' est la corrélation normalisée pour les séquences pseudo-aléatoires,

$$\delta = \frac{W'.W}{\|W'\|.\|W\|} \tag{1.1}$$

Cette mesure est finalement comparée avec un seuil approprié t pour obtenir la valeur de décision : si $d \geq t$ la marque est détectée sinon elle n'est pas détectée.

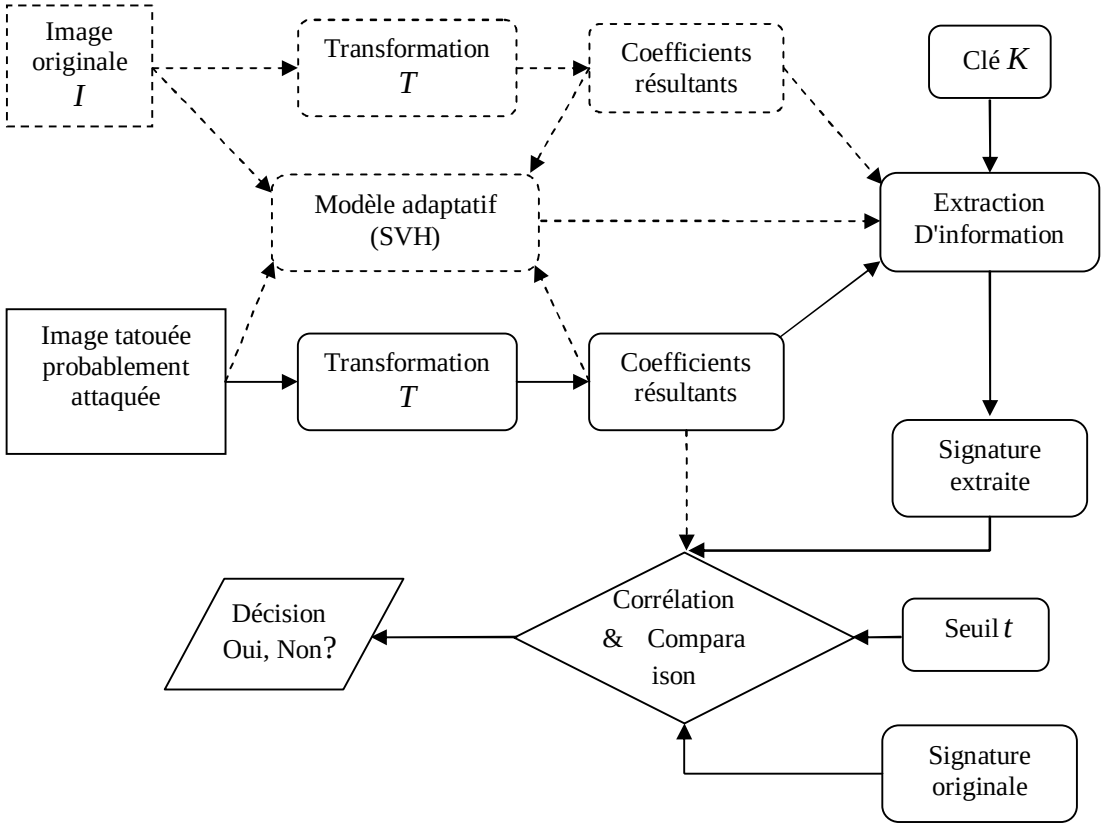


Figure 1.2 Schéma général du processus de détection d'une signature.

4. LES CONTRAINTES D'UN SCHEMA DE TATOUAGE EFFICACE

Pour être performant et efficace, le tatouage doit vérifier les trois critères suivants [23] :

4.1. L'invisibilité

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

Dans la plupart des algorithmes proposés, l'imperceptibilité du tatouage s'obtient en utilisant diverses propriétés du Système Visuel Humain (SVH). Ces propriétés, souvent trouvées à partir d'heuristiques, proposent des modélisations du comportement psychovisuel humain. L'utilisation de ces propriétés tend de plus en plus à se généraliser pour insérer une quantité d'information importante tout en gardant la marque invisible.

4.2. La sécurité

Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est assurée uniquement par la confidentialité de la clef *K*. Si *K* est inconnue, aucun utilisateur ne doit pouvoir retrouver l'image originale. Cette contrainte est souvent remplacée par la suivante, plus réaliste : Ne connaissant pas la clef secrète, un pirate ne doit pas pouvoir retrouver l'image originale sans pour cela mettre en oeuvre des moyens plus coûteux que ceux correspondant à l'achat des droits de copyright.

4.3. La robustesse

C'est l'un des critères les plus difficiles à vérifier. En effet beaucoup d'attaques permettent aujourd'hui de modifier l'image de telle sorte qu'on ne puisse plus y déceler la signature du propriétaire. Ces techniques utilisées pour le piratage combinent notamment les transformations géométriques, la compression, les filtrages divers et attaques de type cryptographique.

5. ETAT DE L'ART DES TECHNIQUES DE TATOUAGE EXISTANTES

Cette section a pour objet de présenter les algorithmes de tatouage d'image existants. Etant donnée de nouveaux procédés depuis quelques années, nous allons présenter uniquement les méthodes fondamentales.

Les schémas de tatouage des images que l'on peut rencontrer dans la littérature scientifique sont très variés et peuvent sembler à première vue très différents les uns des autres. Cependant, les techniques de tatouage courantes peuvent être groupées [2] [5] selon :

- Le domaine sur lequel ils agissent en trois classes principales :
  - Les techniques spatiales.
  - Les techniques fréquentielles et multi-résolutions.
  - Les techniques fondées sur le contenu.
- La façon dont la marque est insérée, on distingue deux grands ensembles
  - Les techniques additives et d'étalement du spectre.
  - Les techniques substitutives et de quantification non linéaire.

5.1. Rôles des différents domaines d'insertion

La diversité des différents schémas de tatouage est liée principalement au choix du domaine d'insertion de la signature [5]. Chaque espace de représentation de l'image apporte diverses possibilités en terme de performance et de robustesse.

5.1.1. Le domaine spatial

Les techniques de tatouage modifiant directement la valeur des pixels de l'image sont naturellement des schémas qui viennent à l'esprit en premier lieu et qui sont faciles à mettre en œuvre. Les opérations d'insertion et de détection sont alors peu coûteuses en temps de calcul ; elles peuvent être alors utilisées afin d'effectuer un tatouage en temps réel.

5.1.2. Le domaine fréquentiel

Les schémas qui utilisent le domaine fréquentiel comme domaine d'insertion peuvent être davantage robustes face aux opérations de compression puisqu'ils utilisent le même espace que celui qui sert au codage de l'image. D'autre part, grâce aux algorithmes de transformations rapides, le calcul de la transformée d'une image est devenu peu coûteux.

Par contre, l'utilisation de la TCD comme espace d'insertion rend le schéma très sensible aux transformations géométriques (translation, rotation,…etc.). En effet, celles-ci ont pour effet de modifier considérablement la valeur des différents coefficients TCD d'une manière qui n'est pas facilement modélisable. Par contre l'espace obtenu après la TFD possède des propriétés d'invariance qui peuvent être exploitées pour détecter la signature après une transformation géométrique.

5.1.3. Le domaine multirésolution

Le domaine multirésolution (Ondelettes) est un espace de tatouage intéressant car il est utilisé dans de récents standards de compression comme JPEG2000 ou encore MPEG4. La décomposition d'une image en sous-bandes permet d'en isoler les composantes basse fréquence. Celles-ci constituent un espace d'insertion qui est moins sensible que l'image elle-même. D'autre part, la décomposition de l'image en sous-bandes est souvent proche d'une décomposition en canaux perceptifs et facilite l'utilisation d'un modèle psychovisuel.

Enfin, le contenu spatial de l'image est aussi conservé après une transformation multirésolution, ce contenu peut alors servir à localiser la signature après une transformation géométrique.

5.2. Les méthodes additives

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un bruit à l'image [5]. La figure 1.3 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque W_0 qui est composée d'un bruit blanc *bb* de générateur K modulant parfois un message M. La seconde étape est la pondération de cette marque par un facteur a issu du calcul d'un masque psychovisuel *Ma*. La troisième étape est l'addition de la marque à l'image. Cette incrustation peut se faire

directement sur l'image I (dans le domaine spatial) ou sur une transformée Tr de celle-ci (TFD, TCD, TOD,…etc.) pour obtenir l'image tatouée I^*.

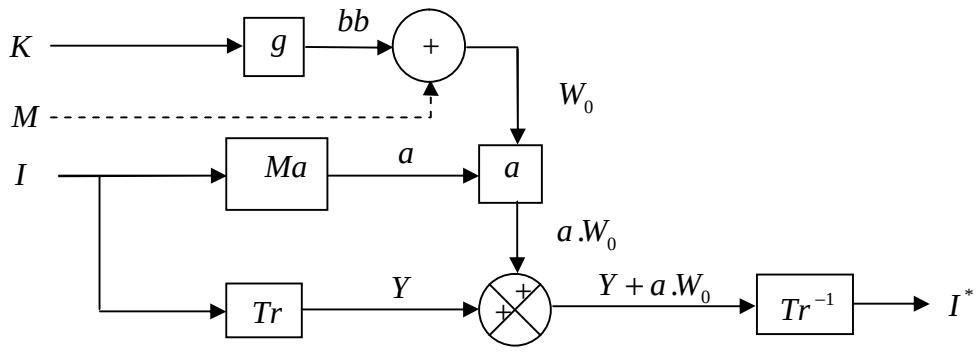


Figure 1.3 Schéma de tatouage d'une méthode additive.

5.2.1. Tatouage additif dans le domaine spatial

a) Insertion par l'étalement de spectre

Tirkel et Cox [21] [11] ont été les premiers à utiliser la technique de l'étalement de spectre pour le tatouage. Cette méthode est maintenant utilisée dans la grande majorité des schémas de tatouage additifs.

On peut voir le problème de tatouage comme un problème de communication. Le tatouage consiste à transmettre un message m dans un environnement bruité. Dans cette modélisation, on considère l'image hôte I comme un canal de transmission, la marque comme un message à transmettre et les attaques comme du bruit. Les outils utilisés en télécommunication s'imposent donc d'eux même.

L'étalement du spectre du message m est classiquement effectué en modulant ce dernier avec une séquence pseudo-aléatoire bb de fréquence bien supérieure pour obtenir la signature W_0. L'image résultante I^* est donnée par l'équation :

$$I^* = I + a \,.\, W_0 \tag{1.2}$$

Si on a accès à l'image originale, la détection extrait W_0 puis *m*, *bb* étant connu. Si le détecteur est semi-privé, la détection s'effectue par corrélation,

$$C = \frac{< I^*, bb >}{\| bb \|^2} \tag{1.3}$$

b) Division de l'image en "patchwork"

Bender [6] propose la technique Patchwork qui est similaire à la précédente. Celui-ci a ensuite été améliorée par d'autres auteurs [7]. A l'aide d'une clé secrète, les auteurs choisissent de façon aléatoire *N* couple de pixels A_i et B_i dans le domaine spatial. Si on appelle a_i et b_i les valeurs de luminance, le tatouage consiste à modifier ces valeurs suivant la formule :

$$\left.\begin{aligned} a'_i &= a_i + 1 \\ b'_i &= b_i - 1 \end{aligned}\right\} \tag{1.4}$$

Pour la détection, on déterminera les *N* couples de pixels à partir de la clé secrète et on calculera :

$$S = \sum_{i=0}^{N-1} (a'_i - b'_i) = \sum_{i=0}^{N-1} (a_i - b_i) + 2.N \tag{1.5}$$

Puisque les couples sont choisis aléatoirement et, si on considère *N* assez grand, la somme des différences $(a_i - b_i)$ est nulle en moyenne et négligeable devant *N*. Donc, si à la détection, *S* est proche de la valeur 2*N*, on pourra affirmer que la marque est présente, dans le cas contraire on conclura que l'image n'est pas tatouée.

5.2.2. Tatouage additif dans la TCD

Cox et *al* [11] appliquent la TCD à toute l'image pour insérer la signature parmi les basses fréquences de celle-ci. Ils modifient les *N* coefficients perceptuellement significatifs de la transformée de l'image (exceptée de la composante continue) suivant l'une des formules :

$$\begin{aligned} y_i' &= x_i + a.w_i \\ y_i' &= x_i.(1 + a.w_i) \\ y_i' &= x_i.e^{a.w_i} \end{aligned} \tag{1.6}$$

Avec :

y_i' : Coefficient TCD de l'image tatouée.

x_i : Coefficient TCD de l'image originale.

a : Coefficient d'invisibilité.

w_i : Coefficient réel issu d'une distribution gaussienne centrée normée.

Les basses fréquences constituent les composantes les plus significatives de l'image. Le fait de vouloir les modifier sans précaution altère alors fortement l'image, la rendant inexploitable. Ces composantes sont très peu détériorées après compression de l'image. L'extraction s'effectue en utilisant l'image originale pour retrouver par différence la signature insérée. La suite w'_i extraite est comparée à la suite w_i par un calcul de similitude :

$$S = \frac{W'W}{\sqrt{W'.W}} \tag{1.7}$$

L'utilisation de l'image initiale permet de s'affranchir de la distorsion provoquée par l'insertion de la signature. Dans [25] les auteurs utilisent le même principe d'insertion que [11]. L'image hôte est premièrement segmentée en utilisant le diagramme de Voronoi et l'extraction des points d'intérêts, une séquence pseudo-aléatoire est ensuite ajoutée aux coefficients de la TCD de chaque segment.

5.2.3. Tatouage additif dans la transformée FOURIER-MELLIN

Le problème de synchronisation de restitution de la marque après une transformation géométrique peut être résolu en choisissant un domaine transformé de l'image invariant par translation, rotation et changement d'échelles, comme le proposent [8].

L'invariance par translation est obtenue par la transformation de Fourier de l'image dont on ne prend que le module. Les invariances par rotation et changement d'échelles sont obtenues par transformation de Fourier-Mellin du module. En effet, cette transformation

peut être vue comme la composée d'un changement de repère en log-polaire et d'une transformée de Fourier. Le changement de repère a la propriété de transformer les rotations et changement d'échelles en translation, la transformée de Fourier, dont on ne prend que le module, rendant le tout invariant. L'insertion et la détection de la marque se font de façon classique dans le domaine transformé de l'image. La figure 1.4 présente le schéma de tatouage contenant les étapes de transformations de l'image du domaine spatial jusqu'au domaine invariant.

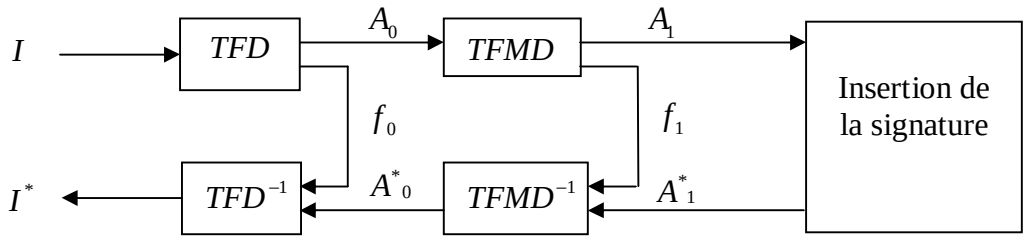


Figure 1.4 Schéma du tatouage dans le domaine d'invariance Fourier-Mellin.

5.2.4. Tatouage additif dans le domaine multirésolution (Ondelettes)

Dans [13] les auteurs proposent un schéma d'insertion additif dans l'espace obtenu à partir de la décomposition de l'image en trois niveaux de résolution. La signature est une séquence de nombres pseudo-aléatoires gaussiens. La longueur de la séquence dans la sous-bande d'approximations *LL* est fixée à 500. Dans les sous-bandes de détails restantes, 4500 coefficients sont modifiés. La signature est ajoutée aux coefficients de grandes valeurs dans chaque sous-bande, excepté les trois sous-bandes de détails de la décomposition (LH_1, HL_1, HH_1). Pour offrir le meilleur compromis entre robustesse/invisibilité, le nombre des éléments de la séquence dans chaque sous-bande de détail est proportionnel à l'énergie de cette bande ; l'énergie d'une sous-bande, E_s, est définie par :

$$E_s = \frac{1}{M.N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} I(i, j)^2 \qquad (1.8)$$

Où *M, N* indiquent la taille de la sous-bande. Avant l'insertion, les coefficients sont ordonnés suivant leur amplitude. Puis la signature w_i est additionnée aux coefficients de la transformée en ondelettes :

$$\tilde{I}(i,j) = I(i,j) + a \,.\, w_s \,.\, I(i,j) \,.\, w_i \tag{1.9}$$

La pondération visuelle w_s est calculée par sous- bande et incorporée dans (1.9) afin de garantir l'invisibilité de la marque. L'extraction s'effectue en inversant la relation précédente.

Loo et Kingsbury [18], choisissent eux aussi d'appliquer les méthodes à étalement de spectre dans un domaine invariant par translation. Pour cela, ils utilisent une décomposition en ondelettes complexes (DT-CWT: dual-tree complex-wavelet transform). Une signature *W* bipolaire $\{\pm 1\}$ est ajoutée aux coefficients de la transformée suivant :

$$C'(m,n) = C(m,n) + w_i \,.\, \sqrt{a\,.x\,(m,n)^2 + b^2} \tag{1.10}$$

Où a et b sont deux paramètres dépendants du niveau de la décomposition. $x(m,n)$ est l'amplitude moyenne dans un voisinage 3x3 autour du coefficient $C(m,n)$. Pour des raisons de meilleure reconstruction, le calcul de l'arbre de décomposition à valeur complexe se fait par l'intermédiaire de deux arbres, l'un représentant la partie imaginaire, l'autre la partie réelle des coefficients en ondelettes.

5.3. Les méthodes substitutives

La classe des schémas substitutifs peut être représentée par des schémas où la signature n'est pas ajoutée mais substituée des composantes de l'image [5]. Une clé secrète *K* associée à un générateur aléatoire permet de sélectionner les différentes composantes $C_K(I)$ de l'image. Ces composantes peuvent désigner les pixels d'une image, ou une transformée de celle-ci (TCD, TFD,…etc.). La signature à insérer est obtenue en appliquant une contrainte (par exemple : un critère de similarité ou une relation d'ordre) sur $C_K(I)$ en fonction du message à insérer. On procède ensuite à l'étape de substitution.

L'image *tatouée I** est reconstruite à partir des composantes propres à la signature (figure 1.5).

La détection de la signature s'effectue en comparant le degré de similitude entre le message retrouvé à partir des composantes extraites de l'image tatouée $C_K(I^*)$ et le préambule utilisé lors de l'insertion.

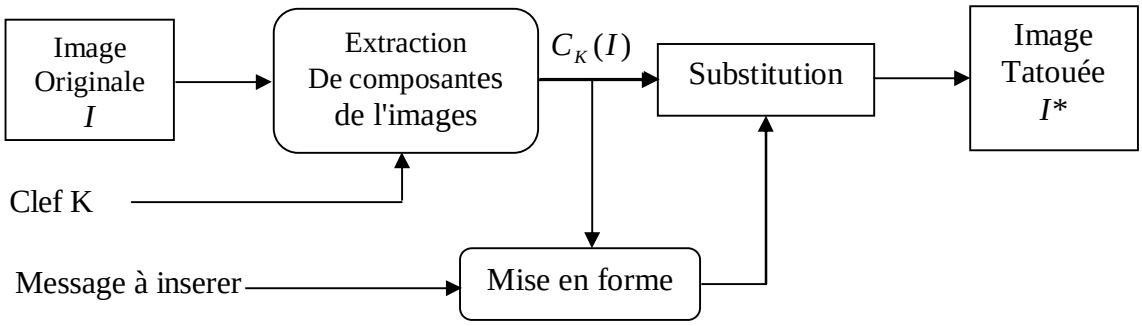


Figure 1.5 Principe de l'insertion par Substitution

5.3.1. Modification des coefficients TCD

Zhao et Koch [9] sont parmi les précurseurs des schémas de tatouage par substitution. Le principe de leur méthode consiste à calquer la méthode de compression JPEG, qui utilise la transformée cosinus discrète. La méthode sera alors robuste à cette transformée très répandue.

L'image est décomposée en blocs de pixels 8×8, dont certains sont choisis par la clef *K* pour porter le message. Les blocs sont ensuite transformés par DCT, puis les modifications se font sur un triplet (déterminé lui aussi par la clef) de coefficients basses fréquences (*C1; C2; C3*). Par souci d'invisibilité, on ne modifiera jamais les trois coefficients des plus basses fréquences. Le triplet modifié doit respecter des contraintes d'ordre différentes selon que la marque à implanter *W* porte le bit 0 ou 1 :

$$\begin{aligned} C1 > C3 + Cte \quad &\text{et} \quad C2 > C3 + Cte \quad \text{si} \quad w_i = 1 \\ C1 + Cte < C3 \quad &\text{et} \quad C2 + Cte < C3 \quad \text{si} \quad w_i = 0 \end{aligned} \tag{1.11}$$

Pour améliorer la robustesse, la modification se fait sur les valeurs quantifiées du triplet. La détection consiste à la lecture de l'ordre des coefficients.

5.3.2. Quantification des coefficients ondelettes

Kundur [10] applique une méthode substitutive où la transformée en ondelettes de l'image est calculée jusqu'à un niveau *l*. A chaque résolution *j* (niveau de la décomposition en ondelettes), on choisit aléatoirement (avec la clef *K*) trois coefficients de détails appartenant à trois orientations fréquentielles distinctes (horizontales, verticales et diagonales). Ces coefficients sont d'abord classés selon leur valeur : $c^1 \leq c^2 \leq c^3$, puis le coefficient "médian" c^2 est modifié. Les modifications se font par quantification. On divise le segment $[c^1; c^3]$ en 2Q-1 segments de longueur Δ (Q est la force du tatouage) :

-Si $w_i = 1$, $c^{*2} = c^3 - p_3\Delta : c^2$ est quantifié sur une grille passant par c^3.

-Si $w_i = 0$, $c^{*2} = c^1 + p_1\Delta : c^2$ est quantifié sur une grille passant par c^1.

Les coefficients entiers *p1* et *p3* minimisent les distorsions.

La détection s'effectue en regardant la position de la valeur moyenne du triplet par rapport aux deux autres. Cette technique a pour avantage de permettre de transmettre une marque de grande taille ($(N^2-1)/3$ pour une image de taille N^2), sa robustesse peut donc être fortement augmentée par redondance ou emploi de code correcteurs d'erreurs.

5.4. Techniques de deuxième génération

Les techniques de tatouage de première génération (1GW : First Generation Watermarking) ont été principalement focalisées sur l'application du tatouage sur l'image entière. Cependant, cette approche n'est pas compatible avec les nouvelles normes de compression d'image vidéo JPEG2000 et MPEG4/7, parce que ces dernières sont basées sur les régions ou des objets de l'image/vidéo. En outre, les algorithmes de la première génération proposés jusqu'ici ne répondent pas aux contraintes de tatouage.

Le tatouage de la deuxième génération (2GW : Second Generation Watermarking) a été développé afin d'augmenter la robustesse et l'invisibilité. Les méthodes de deuxième génération 2GW tiennent compte des caractéristiques de l'image (points, régions, contours et objets) et présentent des avantages additionnels en termes de détection et de recouvrement à partir des attaques géométriques par comparaison aux méthodes de première génération. Ceci est réalisé par l'exploitation des caractéristiques de l'image. En 2000, *ICIP* (International Conférence on Image Processing) a organisé une session spéciale sur les algorithmes de tatouage de deuxième génération pour fournir aux chercheurs l'opportunité de présenter les derniers résultats de la recherche sur le tatouage de deuxième génération [26].

Bas [5] propose une approche de tatouage basée sur le contenu des images ; le schéma présenté entre dans la catégorie des schémas de deuxième génération. La synchronisation de la signature s'effectue par l'utilisation du contenu de l'image pour apporter des repères liés à celle-ci (figure 1.6). Pour orienter l'insertion de la signature et permettre de la retrouver après une transformation géométrique, des ensembles de trois points, représentés par des triangles sont utilisés. Pour obtenir des points liés à l'image, le détecteur de points d'intérêts de Harris [5] est utilisé. L'insertion de la signature s'effectue ensuite sur chacun des triangles dans le domaine spatial ou fréquentiel.

Les performances du schéma reposent en grande partie sur la robustesse du détecteur de points d'intérêts utilisé.

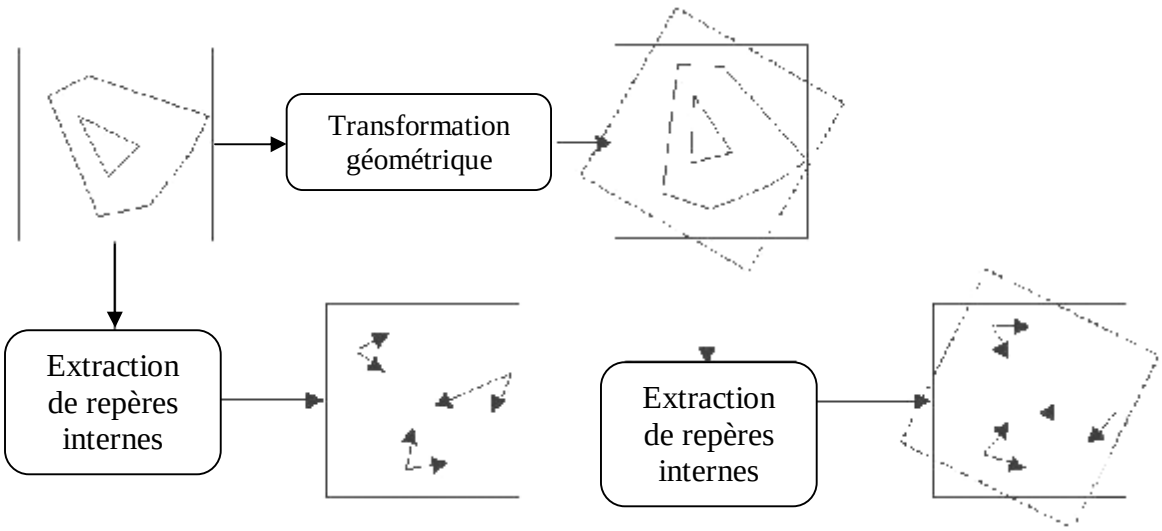


Figure 1.6 Utilisation du contenu de l'image pour fournir des repères nécessaires à la synchronisation de la signature.

5.5. Méthodes Psychovisuelles

L'utilisation de modèles psychovisuels permet d'augmenter la force de la signature sans que les dégradations soient visuellement perceptibles. L'objectif de ces techniques est de prendre en défaut le système visuel humain (SVH) et d'exploiter les différentes propriétés de masquage. Le masquage a lieu lorsqu'un signal (la signature) est rendu imperceptible par la présence d'un autre signal dit masquant (l'image). Plusieurs modèles de masque ont été utilisés en tatouage d'image, certains modèles sont dans le domaine spatial [28], d'autres dans le domaine fréquentiel. F. Autrusseau et A. Saadane [29], ont proposé un masque permettant d'allier des caractéristiques fréquentielles du SVH et des caractéristiques spatiales de l'image traitée.

5.6. Les schémas auto-synchronisants

Lorsqu'une transformation géométrique est appliquée à une image tatouée, ceci rend la détection de la signature beaucoup plus complexe. En effet les schémas classiques de détection utilisent le repère physique de l'image comme référence, c'est-à-dire un repère orthogonal dont l'origine est l'un des quatre coins de l'image. Si l'image a subi une transformation géométrique, le repère ne pourra pas endurer la même transformation mais restera inchangé.

Lorsque le schéma de tatouage appartient à la même classe des schémas additifs, une transformation géométrique va désynchroniser la corrélation entre la signature à détecter et la signature présente dans l'image. Le résultat de la corrélation sera alors erroné.

Si le schéma de tatouage est substitutif, une transformation géométrique va fausser la localisation des sites où la signature a été insérée, car dans la plupart des cas les sites d'insertion sont localisés à partir du repère physique de l'image. Dans chacun des cas, il faut retrouver le repère qui a servi à l'insertion de la signature.

Cette opération peut s'avérer extrêmement coûteuse en temps de calcul. Par exemple si on limite uniquement les transformations géométriques aux translations ou fenêtrage d'une image, le nombre de repères potentiels égale le nombre de pixels présents dans l'image. Le temps de calcul permettant de retrouver la signature devient alors considérable.

Nous présentons dans cette section les schémas de tatouage qui ont été conçus afin de permettre une synchronisation plus aisée de la signature lors de sa détection.

5.6.1. Insertion de mires (templates)

L'insertion de repères modèles dans l'image tatouée peut permettre d'identifier la transformation subie par l'image. Pereira et Pun [27] proposent d'insérer des *mires* ("templates" en anglais), c'est-à-dire des éléments remarquables permettant d'identifier la transformation géométrique qui a été appliquée à l'image.

Dans leur étude, la transformation géométrique recherchée se limite à la classe des transformations affines. Les points portant les mires sont localisés dans le spectre de l'image à l'intérieur d'un anneau correspondant aux moyennes fréquences de l'images. L'insertion de la mire s'effectue en augmentant la valeur des points sélectionnés afin de créer un pic local.

L'identification de la transformation géométrique est réalisée après la détection des pics locaux à l'intérieur du spectre de l'image, et en calculant la transformation géométrique à partir des ensembles de pics initiaux et de pics détectés après transformation (figure1.7). Leur algorithme permet de pouvoir détecter la signature après diverses transformations géométriques affines mais demeure inefficace contre l'attaque Stirmark.

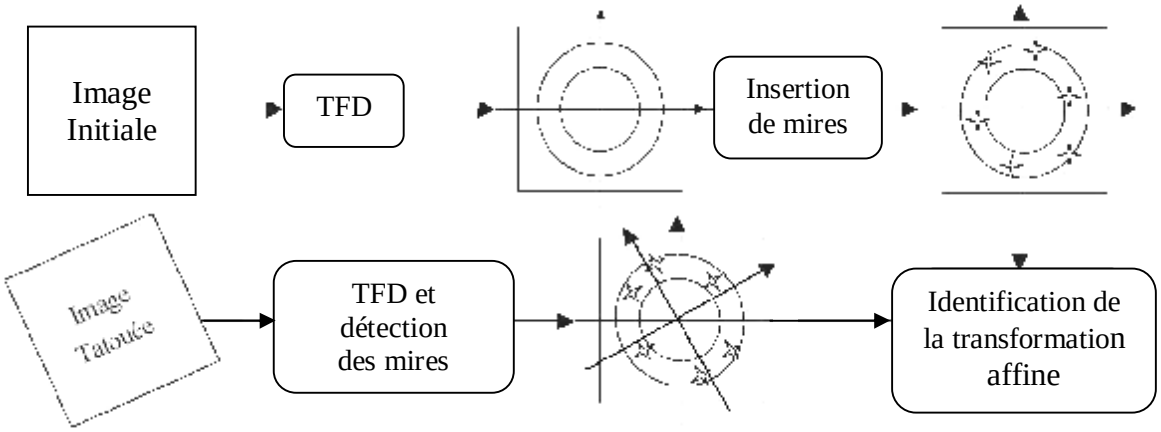


Figure 1.7 Principe de l'insertion de mires dans l'image tatouée.

5.6.2. Insertion périodique de la signature

Une stratégie pour réduire la complexité de la détection est d'insérer une signature périodique. L'espace de recherche est alors réduit à la taille du motif de base.

Kutter [30] propose d'insérer une signature périodique dans l'image et d'utiliser la fonction d'auto-corrélation de l'image pour identifier la transformation géométrique (figure1.8). La fonction d'auto-corrélation de la signature présente de pics de corrélation qui permettent de positionner la signature et de révéler la transformation géométrique. La détection s'effectue en calculant la corrélation entre la séquence aléatoire et l'image après la transformation géométrique inverse.

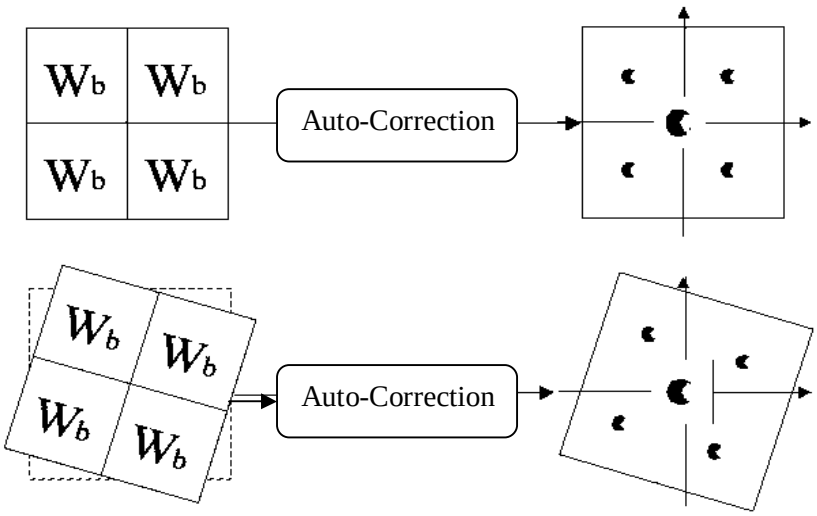


Figure 1.8 Synchronisation par insertion périodique de la signature.

6. ETAT DE L'ART DES ATTAQUES SUR LES SCHEMAS DE TATOUAGE D'IMAGES

Les attaques tiennent une place très importante dans le cahier des charges d'un processus de tatouage puisqu'elles définissent sa robustesse. Les principales classifications dans la littérature scientifiques ont été présentées par Voloshinovskiy [31].

Classiquement, on peut séparer les attaques de la manière suivante :

- **Les attaques non-intentionnelles** : ce sont les traitements usuels de l'image comme la compression, le filtrage, la conversion A/N…etc. ces attaques ne visent pas forcément à supprimer la signature, l'identifier ou l'isoler.

- **Les attaques intentionnelles** : ces attaques visent à supprimer ou à dégrader la signature insérée comme l'attaque jitter qui consiste à enlever des lignes et des colonnes de l''image tatouée et à en dupliquer d'autres.

6.1. Attaques non intentionnelles

Nous parcourons un éventail des différentes techniques utilisées en traitement d'images qui sont susceptibles d'altérer la détection de la signature.

a) Les techniques de compression

Les algorithmes de compression sont particulièrement dangereux pour les processus de tatouage puisque leur objectif est exactement l'opposé de celui du tatouage. On veut en effet, par l'utilisation de ces algorithmes ne garder de l'image que les composantes basse-fréquence essentielles à leur compréhension (une signature invisible n'est évidement pas essentielle). Si un algorithme de tatouage veut être robuste aux schémas de compression, il doit posséder une composante basse-fréquence qui sera conservée après la compression.

b) Les opérations de rehaussement, de lissage

Le rehaussement des images s'effectue en augmentant les composantes hautes fréquence de l'image. Les composantes hautes fréquences de la signature sont alors accentuées. Le lissage des images atténue la composante haute fréquence de l'image qui devient alors plus floue. Les composantes hautes fréquences de la signature sont dégradées.

c) Les transformations géométriques usuelles

L'édition des images nécessite constamment de modifier leur géométrie, on peut vouloir effectuer un fenêtrage, un changement d'échelle, un zoom, une translation, ou encore appliquer une rotation sur l'image. Ces transformations géométriques désynchronisent dans la plupart des cas le détecteur qui ne retrouve plus la signature (bien que celle-ci soit présente).

d) Les conversions analogiques/numériques

La numérisation de l'image à l'aide d'un scanner par exemple peut provoquer de légères déformations géométriques. Ce procédé va donc à la fois dégrader la signature et provoquer une perte de synchronisation de la signature.

6.2. Les attaques intentionnelles

Les attaques les plus pénalisantes dans cette situation sont celles qui visent à désynchroniser la marque avant la phase de détection. L'attaque est dite efficace lorsque la signature est indétectable ou lorsque la décision au sujet de l'authenticité de la signature est ambiguë.

a) Attaque par copiage

L'attaque par copiage consiste à recopier une marque obtenue préalablement (par exemple par estimation) sur une image non marquée. Le détecteur validera alors la nouvelle image comme étant tatouée. Cette attaque s'applique naturellement aux problèmes d'intégrité, puisqu'elle rend possible la présentation de faux qui seront authentifiés par le détecteur.

b) Attaque "jitter"

Elle consiste à inverser, à supprimer ou à remplacer certaines linges ou colonnes de l'image numérique. Cette attaque est très efficace face à des schémas de type étalement de spectre.

c) Attaque "mosaïque "

Elle consiste à diviser l'image en différentes parties. A cause de la division, la détection ne pourra pas être effectuée sur toute l'image mais seulement sur les parties séparées de l'image. Elle permet d'invalider la détection sans pour autant supprimer la marque.

d) Attaque"random bending"

Elle consiste à appliquer des déformations géométriques aléatoires sur l'image tatouée. Des petits seuillages sont effectués sur les zones planes de l'image pour dégrader la marque dans ces zones.

e) Attaque "surmarquage"

L'attaque par surmarquage vise à tatouer à nouveau une image déjà tatouée. Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse.

7. BANCS DE TESTS

Les techniques proposées pour le tatouage sont nombreuses, et pour chacune d'entre elles telle ou telle qualité est vantée par ses concepteurs. Travailler sur les attaques permet d'éprouver l'efficacité de ces méthodes. Malheureusement, il est actuellement encore très difficile de comparer équitablement les différentes techniques entre elles. Il est donc nécessaire de définir des tests comparatifs (benchmarks) standardisés.

7.1. Stirmark

Le banc de test Stirmark [34] est une première proposition d'un tel benchmark et reste toujours le plus célèbre. Il s'agit d'un logiciel appliquant une série d'attaques standards, composées de filtres simples (filtre passe-bas, quantification, addition de bruit Gaussien, etc.), et de distorsions géométriques (transformations affines, distorsions locales aléatoires). Ce banc de tests est extrêmement efficace et très peu d'algorithmes de tatouage d'images y sont robustes. L'attaque est quasiment invisible et pourtant elle est très efficace notamment grâce aux petites déformations géométriques non affines.

7.2. Checkmark

Voloshinovskiy et al. [31] proposent des attaques qui prennent en compte le contenu de l'image, à la différence de Stirmark. Le contenu de l'image est identifié grâce au SVH. Dans le but d'évaluer les dégradations dues au tatouage, le banc de test utilise le WPSNR qui prend en compte le contenu de l'image pour juger de la visibilité de la signature. Ce banc de test améliore celui proposé par Peticolas: plus d'attaques efficaces sont proposées et les algorithmes de tatouage ne sont pas testés seulement pour leur robustesse mais aussi pour leur qualité visuelle.

7.3. Certimark

Cependant, les attaques de Stirmark ne sont pas représentatives des attaques qu'un pirate peut utiliser. C'est pourquoi le projet européen Certimark (CERTification for waterMarking techniques) propose de créer de nouveaux benchmarks standardisés, incluant des attaques plus puissantes. Ce projet devrait aider au développement de méthodes de tatouage particulièrement robustes. En offrant des protocoles de tests standardisés, il permettra également aux différentes classes d'utilisateurs de connaître les performances des méthodes de tatouage, par là-même de mieux choisir la plus appropriée (et d'accroître leur confiance dans cette technologie).

8. Conclusion

Nous avons présenté dans ce chapitre le contexte technique qui entoure le domaine du tatouage d'image numérique. Contrairement à de nombreux domaines scientifiques, le tatouage est associé à un éventail extrêmement large de contraintes. Le"cahier des charges" n'est pas figé, et il est donc impossible de certifier qu'un algorithme puisse faire face à toutes les contraintes possibles. Chaque année, des chercheurs proposent à la fois des schémas appelés "robuste" mais aussi de nouvelles attaques permettant d'ôter la robustesse d'autres schémas.

1. INTRODUCTION

Comme nous l'avons évoqué dans le chapitre précédent, un algorithme de tatouage robuste et efficace doit prendre en compte trois critères essentiels : l'invisibilité de la signature, la robustesse face aux divers attaques (intentionnelles et non intentionnelles) lors de la détection et la sécurité du schéma pour assurer la confidentialité de l'information cachée. Donc, pour construire un algorithme de tatouage efficace, il faudra dans le meilleur des cas combiner les trois aspects (invisibilité, sécurité et robustesse) et parfois faire des compromis Dans ce contexte, nous avons opté dans notre travail pour la conception d'un schéma de tatouage qui répond à ces trois contraintes. Nos principales contributions sont :

- L'exploitation de l'analogie présentée par la TOD et les modèles du SVH pour dissimiler robustement la signature. En particulier, un modèle dérivé d'une technique de compression des images [17] estimant le sensibilité de l'oeil humain au bruit, est employé pour moduler et adapter la signature selon les caractéristiques locales de l'image.

- L'introduction du chaos pour augmenter la sécurité du schéma proposé.

- L'utilisation de la mise en correspondance des images (le recalage) qui nous permet de compenser les éventuelles transformations géométriques subies par l'image tatouée. une technique d'estimation de mouvement différentielle est employée pour estimer six paramètres affines qui nous renseignent sur le cisaillement, la rotation, la translation et le changement d'échelle.

2. PRINCIPE DU SCHEMA DE TATOUAGE

Dans ce chapitre nous développons la manière dont est construit notre schéma de tatouage L'algorithme fait partie de la classe des schémas additifs dans le domaine des ondelettes. L'ajout de la signature s'appuie sur l'exploitation des caractéristiques du SVH. La signature est une séquence chaotique binaire $\{\pm 1\}$ qui est ajoutée aux coefficients des trois sous-bandes de détail du premier niveau de la TOD de l'image. Chaque valeur binaire est multipliée, avant d'être ajoutée, par une fonction de pondération qui est obtenue à partir

de la fonction de sensibilité au bruit utilisée dans le système de compression [17] pour contrôler d'une manière adaptative le pas de quantification. De cette façon à chaque coefficient, le maximum des distorsions visiblement tolérables est ajouté. La construction de la fonction de sensibilité est principalement basée sur l'analyse du degré d'activité de l'image dans le voisinage du pixel à modifier.

Pour la détection, la corrélation est calculée entre la marque à examiner sa présence et les coefficients marqués. La valeur de la corrélation est comparée à un seuil pour décider si la signature est présente ou non. Un seuil optimum est théoriquement établi pour minimiser la probabilité de fausses alarmes.

Enfin, pour faire face au problème de perte de synchronisation après une transformation géométrique, un algorithme de recalage issu d'une technique d'estimation différentielle de mouvement est utilisé. La transformation est d'abord formulée comme étant purement affine. Ensuite, une contrainte de lissage est imposée à tous les paramètres géométriques localement estimés ; ceci nous permet de modéliser une large gamme de transformations géométriques afin de les inverser avant la phase de détection.

3. LA TRANSFORMEE EN ONDELETTES DISCRETE

La transformée en ondelettes a été intensivement étudiée, et elle a gagné l'intérêt des chercheurs de tatouage au cours des dernières années. L'intérêt de cette transformée repose sur les analyses en terme psychovisuel du SVH et sur l'aspect multi-échelles qui est propice à une répartition plus robuste du tatouage [1]. Dans cette partie, nous nous sommes volontairement limités aux notions nécessaires à la compréhension de la méthode décrite dans la suite du Mémoire.

Afin de simplifier les notations, nous considérerons dans un premier temps un signal à une seule dimension pour présenter les différentes notions sur les ondelettes puis nous généraliserons le propos au cas bidimensionnel.

3.1. La Transformée en Ondelettes Continue (TOC)

3.1.1. La Transformée de Fourier à Court Terme (TFCT)

La Transformée de Fourier (TF) est un outil permettant de connaître le comportement fréquentiel d'un signal. En utilisant cette transformation, on perd toute information relative au temps. Si les propriétés du signal ne varient pas beaucoup par une translation dans le temps (c.-à-d., un signal *stationnaire*), cet inconvénient n'est pas très important. Cependant, la plupart des signaux intéressants contiennent de nombreuses caractéristiques non stationnaires ou transitoires, ces caractéristiques sont souvent la partie la plus importante du signal, et l'analyse de Fourier n'est pas convenable pour les détecter. Pour remédier à cela, et dans le cadre des signaux à énergie finie ($x(t) \in L^2(R)$), on utilise un outil *temps- fréquence*: on restreint l'existence du signal autour d'un instant *t*, grâce à une fenêtre d'analyse $g(t-t)$ centrée sur cet instant, puis on prend sa transformée de Fourier :

$$T_x(f,t) = \int x(t)\, g(t-t)\, e^{-i2p\, f t}\, dt = \int x(t)\, g^*_{f,t}(t)\, dt \qquad (2.1)$$

On fait alors glisser cette fenêtre le long du signal, ce qui permet d'en mesurer le contenu spectral au cours du temps. On appelle cette transformation la **Transformée de Fourier à Court Terme**, on la note **TFCT**

La TFCT ne représente pas l'ensemble des *représentations temps-fréquence* mais elle permet d'en illustrer le principe et l'une des propriétés fondamentales : quelles que soient les dynamiques présentes dans le signal, elles sont analysées avec la même précision absolue. En pratique, on a souvent des signaux composés de parasites d'activité de courte durée, contenant des hautes fréquences, superposées à des composantes basses fréquences de longues durées. Il s'avère alors nécessaire de disposer d'une grande résolution temporelle dans les hautes fréquences afin de déterminer les instants d'occurrence de ces parasites, tandis que dans les basses fréquences, une bonne résolution fréquentielle aura l'avantage de mieux caractériser les composantes de longues durées.

L'analyse par ondelettes représente la prochaine étape logique : une technique de fenêtrage avec des régions à tailles variables.

3.1.2. La Transformée en Ondelettes Continue

La Transformée en Ondelettes Continue réalise une projection du signal sur un ensemble de fonctions appelées classiquement "ondelettes" et dont la construction diffère de celle de la TFCT : on remplace la variable de fréquence *f* par celle d'échelle *a*. Partant d'une fonction ψ, *l'ondelette mère*, de $L^2(R)$ de moyenne nulle, la famille des ondelettes translatées dans le temps et dilatées en échelle associée à ψ est définit comme suit ,

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \tag{2.2}$$

Elle définit l'espace bidimensionnel : le plan *temps-échelle*, dans lequel l'information du signal $x(t)$ va être représentée. La Transformée en Ondelettes Continue (TOC) peut alors être définie par le calcul du *coefficient de ressemblance* $TOC_x(a,b)$ entre le signal $x(t)$ et l'ondelette $\psi_{a,b}(t)$:

$$x(t) \;\mathbf{a}\; TOC_x(a,b) = \int_R x(t)\,\frac{1}{\sqrt{a}}\,\psi\left(\frac{t-b}{a}\right)dt \quad \text{où} \quad a \in R^+ - \{0\},\ b \in R \tag{2.3}$$

La famille des coefficients $TOC_x(a,b)$ est appelée la Transformée en Ondelettes Continue. Cette transformation est inversible, à condition que l'ondelette mère vérifie la condition, dite d'admissibilité :

$$\int |\Psi(f)|^2 \frac{df}{f} = K_\psi < +\infty \tag{2.4}$$

La formule d'inversion de cette transformée est donnée par la relation suivante :

$$x(t) = \frac{1}{K_\psi}\int_R\int_R TOC_x(a,b)\frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right)\frac{da\ db}{a^2} \tag{2.5}$$

3.2. La Transformée en Ondelettes Discrète (TOD)

La Transformée en Ondelettes Discrète (TOD) est donc obtenue par échantillonnage des coefficients d'échelle et de temps :

$$TOD_x(j,k) = TOC_x(a = 2^j, b = k2^j),\ (j,k) \in Z^2 \tag{2.6}$$

Cette transformée peut être inversée par :

$$x(t) = \sum_{j \in Z} \sum_{k \in Z} TOD_x(j,k)\ \psi_{j,k}(t) \tag{2.7}$$

Où $$\psi_{j,k}(t) = 2^{-j/2}\psi(2^{-j}(t-k)), (j,k) \in Z^2 \tag{2.8}$$

3.3. L'Analyse Multi-Résolution (AMR)

L'AMR d'un signal revient à le décomposer à différentes échelles, en approximations et en détails. Les espaces de projections du signal sont entièrement caractérisés par la donnée de deux filtres (*h* : passe haut, et *g* : passe bas). Ces filtres permettent le calcul rapide des coefficients de la transformée en ondelettes discrète via un algorithme itératif.

Pour un signal $x(t)$ à énergie finie, Les coefficients d'approximations et de détails sont définis par :

$$a_x(j,k) = \int_R x(t)\, 2^{-j/2}\varphi(2^{-j}(t-k))\, dt = \int_R x(t)\ \varphi_{j,k}(t)\, dt \tag{2.9}$$

$$d_x(j,k) = \int_R x(t)\, 2^{-j/2}\psi(2^{-j}(t-k))\, dt = \int_R x(t)\ \psi_{j,k}(t)\, dt \tag{2.10}$$

La fonction φ est appelée *fonction d'échelle* car elle permet de passer d'un espace d'approximation à un autre, c'est à dire d'une échelle à une autre.

Les deux filtres *h*, *g* sont liés à ψ et φ par les deux relations suivantes :

$$\varphi(\frac{t}{2}) = g * \varphi(t) \tag{2.11}$$

$$\psi(\frac{t}{2}) = h * \varphi(t) \tag{2.12}$$

L'approximation et le détail du signal $x(t)$ à la résolution 2^{-j} peut être obtenus par :

$$A_j = \sum_k a_x(j,k)\ f^*_{j,k}(t) \tag{2.13}$$

$$D_j = \sum_k d_x(j,k)\ \psi^*_{j,k}(t) \tag{2.14}$$

L'approximation du signal à un niveau *j* correspond à une approximation plus grossière complétée par le détail :

$$A_j = A_{j+1} + D_{j+1} \tag{2.15}$$

Pour assurer les deux opérations de décomposition et de reconstruction, la condition d'orthogonalité de base pour les deux filtres $H(w)$ et $G(w)$ est nécessaire [3] :

$$\left|H(w)\right|^2 + \left|G(w)\right|^2 = 1 \qquad (2.16)$$

3.4. Généralisation aux images

La généralisation de l'AMR aux signaux bidimensionnels ne pose aucune difficulté d'ordre théorique si l'on utilise des ondelettes séparables pour chaque dimension *m* et *n*. En pratique, pour calculer les coefficients d'approximations et de détails d'une image *I*, nous utilisons la généralisation de l'algorithme présenté au paragraphe précèdent. Chaque étape de cet algorithme est appliquée successivement aux lignes puis aux colonnes de l'image. La figure 2.1 montre la décomposition pyramidale résultante de l'image Lena. On obtient pour un niveau de décomposition *j* une imagette d'approximations $I_j^{LL}(m,n)$: (filtrage passe-bas lignes et colonnes) et trois imagettes de détails, $I_j^{HL}(m,n)$ (filtrage passe-haut lignes et passe-bas colonnes), $I_j^{LH}(m,n)$ (filtrage passe-bas lignes et passe-haut colonnes) et $I_j^{HH}(m,n)$ (filtrage passe-haut lignes et colonnes) selon l'orientation fréquentielle horizontale, verticale et diagonale.

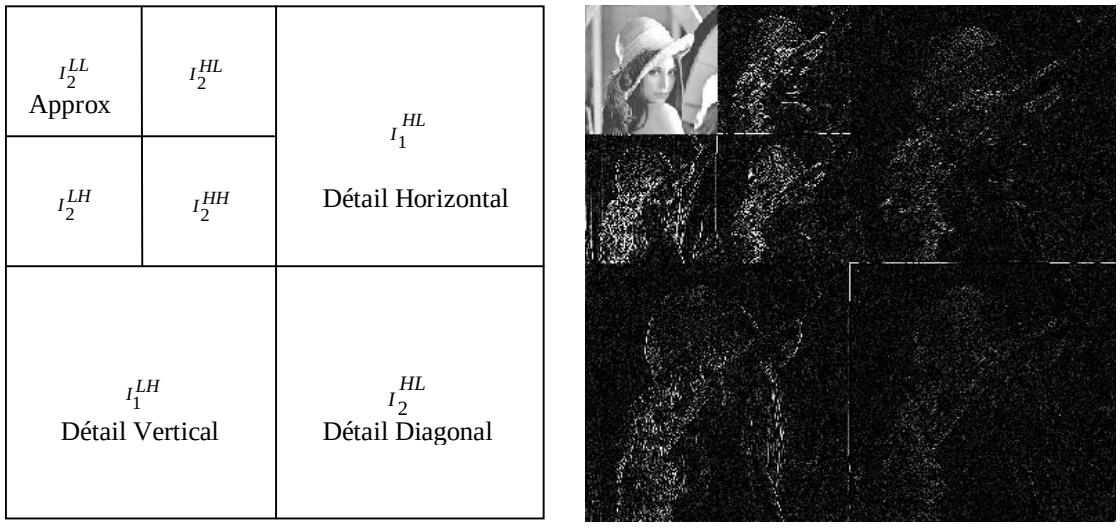


Figure 2.1 La décomposition pyramidale en deux niveaux de l'image Lena.

4. PROCESSUS D'INSERTION DE LA SIGNATURE

Nous détaillons dans cette section la construction du schéma d'insertion de la signature proposé. Notre algorithme fait partie à la classe des schémas additifs aveugles dans le domaine multirésolution. L'ajout de la signature s'appuie sur une étude psychovisuelle de l'image.

L'image originale est premièrement décomposée en utilisant la TOD en quatre niveaux, nous dénotons I_j^q la sous-bande au niveau de résolution : j=1,2,3,4 et avec orientation $q = \{LL, LH, HL, HH\}$ (figure 2.2). En particulier, pour notre implémentation, la paire bi-orthogonale CDF '9/7' (Cohen-Daubechies-Fauraue '9/7') [14] a été utilisée pour décomposer l'image originale. Cette paire a été adoptée dans la compression d'empreintes digitales par le standard de l'FBI et également dans le nouveau standard JPEG2000 [34].

Les filtres passe-haut d'analyse et de synthèse $H(z)$ et $\overline{H}(z)$, respectivement; et les filtres passe-bas correspondants $G(z)$ et $\overline{G}(z)$ sont donnés par [34] :

$$\begin{aligned} H(z) &= h_4(z^4 + z^{-4}) + h_3(z^3 + z^{-3}) + h_2(z^2 + z^{-2}) + h_1(z+1) + h_0 \\ G(z) &= g_3(z^3 + z^{-3}) + g_2(z^2 + z^{-2}) + g_1(z+1) + g_0 \\ \overline{H}(z) &= \overline{h}_3(z^3 + z^{-3}) + \overline{h}_2(z^2 + z^{-2}) + \overline{h}_1(z+1) + \overline{h}_0 \\ \overline{G}(z) &= \overline{g}_4(z^4 + z^{-4}) + \overline{g}_3(z^3 + z^{-3}) + \overline{g}_2(z^2 + z^{-2}) + \overline{g}_1(z+1) + \overline{g}_0 \end{aligned} \tag{2.17}$$

Où:

$$\begin{aligned} h_0 &= \overline{g}_0 \approx 0.852698679009, & g_0 &= \overline{h}_0 \approx 0.788485616614, \\ h_1 &= -\overline{g}_1 \approx 0.377402855613, & g_1 &= -\overline{h}_1 \approx -0.418092273333, \\ h_2 &= \overline{g}_2 \approx -0.110624404418, & g_2 &= \overline{h}_2 \approx -0.040689417620, \\ h_3 &= -\overline{g}_3 \approx -0.023849465019, & g_3 &= -\overline{h}_3 \approx 0.064538882646, \\ h_4 &= \overline{g}_4 \approx 0.037828455507, \end{aligned}$$

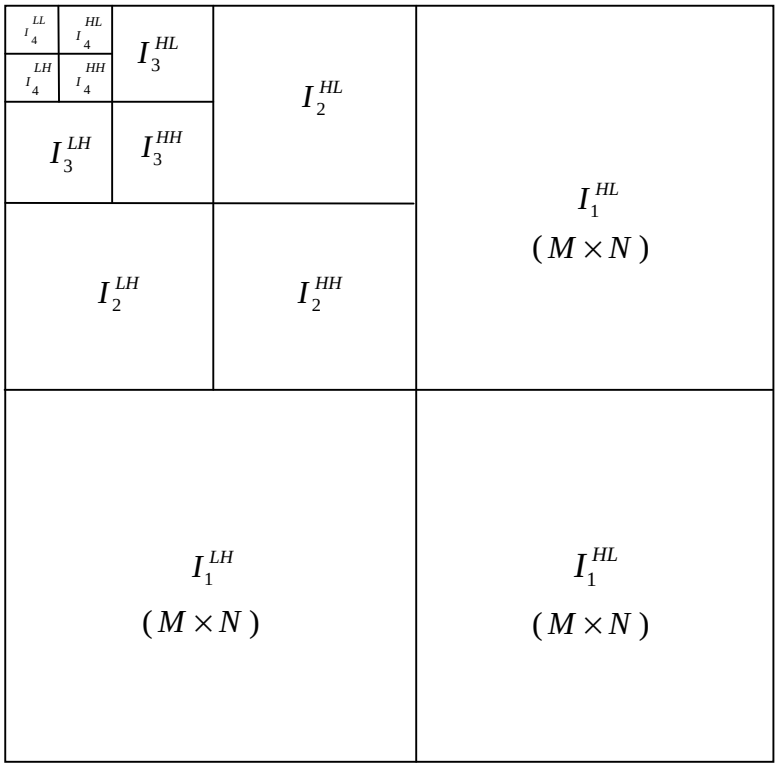


Figure 2.2 Décomposition pyramidal d'une image en 4 niveaux de résolution obtenus après TOD.

4.1. Génération de la signature

La séquence à insérer dans le domaine des ondelettes peut être choisi de plusieurs manières. Souvent, les séquences du tatouage utilisent un générateur de nombres pseudo-aléatoires [11], mais la signature peut être également obtenue par une application récursive des séquences chaotiques appropriées.

Ces dernières années, les systèmes chaotiques ont été employés pour le tatouage numérique, pour augmenter la sécurité. Les caractéristiques les plus attractives du chaos dans la dissimilation de l'information sont sa sensibilité extrême aux conditions initiales et l'étalement des orbites sur l'espace entier [12]. Ces caractéristiques spéciales font que les systèmes chaotiques sont d'excellents candidats pour le cryptage et le tatouage [32].

Pour notre algorithme, nous avons utilisé l'équation logistique [12] définie par l'équation (2.17) avec la condition initiale i_x (la clé secrète de notre méthode) pour générer une séquence chaotique *X*.

$$x_{k+1} = m\, x_k (1 - x_k) \tag{2.18}$$

Où $0 \le m \le 4$. Lorsque $3.5699456 < m \le 4$, le système est dans un état chaotique. Toutes les séquences produites par ce système sont très sensibles aux conditions initiales, dans le sens que deux séquences logistiques générées à partir des états initiaux différent sont statistiquement non corrélées. D'ailleurs, toutes les orbites de l'équation logistique sont concentrées dans l'intervalle [0,1].

Notre signature binaire à insérer $W \in \{+1,-1\}$ est obtenue en appliquant un seuillage sur la séquence chaotique *X*, mentionnée ci-dessus, comme suit :

$$w(k) = \begin{cases} 1 & \text{si } x(k) > 0.5 \\ -1 & \text{si } x(k) \le 0.5 \end{cases}, \text{ avec } k = 1...3MN \tag{2.19}$$

Où $2M \times 2N$ est la dimension de l'image originale, et $3MN$ est longueur de la séquence chaotique *X*, et elle est égale au nombre total des coefficients des trois sous-bandes de détail du premier niveau $\{I_1^{HL}, I_1^{LH}, I_1^{HH}\}$ où nous voulons insérer la signature. De plus, nous arrangeons cette séquence en 2-D, pour balayer ces trois sous-bandes .

4.2. Insertion de la signature

Les coefficients des trois sous-bandes de détails du premier niveau sont modifiés selon les formules suivantes :

$$\tilde{I}_1^{LH}(i,j) = I_1^{LH}(i,j) + a\,.\,p^{LH}(i,j).w(i.N + j) \tag{2.20}$$

$$\tilde{I}_1^{HL}(i,j) = I_1^{HL}(i,j) + a\,.\,p^{HL}(i,j).w(M.N + iN + j) \tag{2.21}$$

$$\tilde{I}_1^{HH}(i,j) = I_1^{HH}(i,j) + a\,.\,p^{HH}(i,j).w(2M.N + i.N + j) \tag{2.22}$$

Où a est le paramètre d'invisibilité global introduit pour contrôler la force de la signature, Il est clair que ce facteur intervient directement dans les performances de robustesse du

schéma. Plus le tatouage est 'fort', plus il est visible et plus il est robuste à certaines attaques (comme l'ajout de bruit). Le compromis proposé par notre schéma de tatouage est de calculer pour chaque coefficient de coordonnées (i, j) la fonction de pondération perceptuelle maximum $p(i, j)$ considérant la sensibilité locale de l'image au bruit. Les dégradations dû au tatouage seront alors ajustés à la limite de perceptibilité humaine. Nous détaillons au paragraphe suivant le critère psychovisuel permettant d'assurer l'imperceptibilité et la robustesse de notre méthode.

4.3. Le calcul de la fonction perceptuelle de pondération

Notre idée est de maximiser et d'adapter la force de tatouage a pour chaque coefficient des trois sous-bandes de détail du premier niveau en pondérant l'insertion de la signature par une fonction perceptuelle $p(i, j)$ dépendant des caractéristiques de l'image et de critères psychovisuels. La force de la signature sera augmentée dans les zones texturées à hautes fréquences, et elle sera diminuée dans les zones homogènes à basses fréquences.

Le calcul de cette fonction de pondération perceptuelle $p(i, j)$ est fondé sur une particularité du système visuel humain (SVH) appelée masquage présentée par Lewis et Knowles [17] où ils ont abordé le problème de quantification des coefficients de la TOD pour la compression : ils ont proposé d'adapter le pas de quantification de chaque coefficient selon la sensibilité locale de l'oeil au bruit.

L étude de ces auteurs est fondée sur les caractéristiques perceptuelles du SVH suivantes :

- **Luminosité d'arrière plan** : le SVH est moins sensible au bruit pour les arrières plans de forte et de faible luminosité. Les coefficients de la version basse fréquence de l'image I_4^{LL} peuvent être utilisés pour fournir les valeurs de la luminosité d'arrières plans.

- **Masquage selon la résolution et la direction :** la sensibilité de l'œil humain au bruit dans les bandes de haute résolution est faible, et varie selon l'orientation de ces bandes : le SVH est plus sensible aux motifs horizontaux et verticaux, plutôt qu'aux motifs à 45^0 (c.-à-d., $q = HH$, dans notre cas).

- **Masquage par les textures** : la sensibilité au bruit diminue s'il y a une haute activité au voisinage du coefficient. L'énergie des coefficients basse fréquence peut indiquer le niveau de l'activité de textures.

- **Masquage spatial où proximité du contour** : relie la sensibilité au bruit à la distance et à la taille du contour. Comme les coefficients que nous traitons sont supposés faire partie d'un contour, la localité spatiale de chaque niveau fournit les informations de distance, tandis que l'énergie des coefficients basse fréquence indique la taille du contour. La sensibilité diminue pour une taille de contour croissante et aux distances décroissantes à partir du contour.

En se basant sur ces considérations, le pas de quantification $q_l^q(i,j)$ de chaque coefficient $I_l^q(i,j)$ est le produit de trois termes, $\Theta(l,q)$, $\Lambda(l,i,j)$ et $\Xi(l,i,j)$:

$$q_l^q(i,j) = \Theta(l,q).\Lambda(l,i,j).\Xi(l,i,j)^{0.2} \tag{2.23}$$

Où la signification de chaque terme dans cette équation est expliquée ci-dessous.

Commençant l'analyse de $q_l^q(i,j)$ par le premier terme de l'expression (2.23). Pour prendre en compte le changement de la sensibilité perceptive au bruit selon la sous-bande (en particulier selon l'orientation et le niveau de détail), on pose :

$$\Theta(l,q) = \begin{Bmatrix} \sqrt{2}, & siq = HH \\ 1, & autrement \end{Bmatrix} \cdot \begin{Bmatrix} 1.00, \text{ si } l = 1 \\ 0.32, \text{ si } l = 2 \\ 0.16, \text{ si } l = 3 \\ 0.10, \text{ si } l = 4 \end{Bmatrix} \tag{2.24}$$

Le deuxième terme $\Lambda(l,i,j)$ prend en considération la luminosité locale basée sur les valeurs des niveaux de gris de la version basse fréquence de l'image I_4^{LL} (l'approximation au $4^{ème}$ niveau). Lewis et Knowles supposent que l'œil est moins sensible au bruit dans les régions de forte luminosité, ils ont proposé de calculer ce facteur de la manière suivante :

$$\Lambda(l,i,j) = 1 + L(l,i,j) \tag{2.25}$$

Où
$$L(l,i,j) = \frac{1}{256} I_4^{LL}\left(1 + \left\lfloor \frac{i}{2^{4-l}} \right\rfloor, 1 + \left\lfloor \frac{j}{2^{4-l}} \right\rfloor\right) \tag{2.26}$$

En se basant sur la considération que l'oeil humain est moins sensible au bruit dans les régions de forte luminosité ainsi que dans les régions de faible luminosité, nous avons modifier le facteur $L(l,i,j)$ comme suit :

$$L'(l,i,j) = \begin{cases} 1 - L(l,i,j), & \text{si } L(l,i,j) < 0.5 \\ L(l,i,j), & \textit{autrement} \end{cases} \tag{2.27}$$

Finalement, le troisième terme,

$$\Xi(l,i,j) = \sum_{k=1}^{4-l} \frac{1}{16^{k-1}} \sum_{q \in \{LH, HL, HH\}} \sum_{x=0}^{1} \sum_{y=0}^{1} \left[I_{k+l-1}^{q}\left(y + \frac{i}{2^{k-1}}, x + \frac{j}{2^{k-1}}\right)\right]^2 \times \textit{Var}\left\{ I_4^{LL}\left(1 + y + \frac{i}{2^{4-l}}, 1 + x + \frac{j}{2^{4-l}}\right) : x = 0,1; y = 0,1 \right\} \tag{2.28}$$

donne une mesure d'activité de textures au voisinage du pixel. En particulier, ce terme est composé par le produit de deux contributions : la première est la valeur quadratique moyenne locale des coefficients de la TOD dans toutes les sous-bandes de détail, tandis que la seconde est la variance locale de la sous-bande d'approximation I_4^{LL}. Ces deux contributions sont calculées dans un petit voisinage 2×2 correspondant à l'endroit (i,j) du pixel. Puisque la première contribution représente la distance à partir des contours, tandis que la seconde donne une mesure de texture, nous avons décidé de multiplier les deux termes, selon la considération que l'oeil est moins sensible dans les régions texturées, mais plus sensible proches des contours .

Le fait que $q_l^q(i,j)$ est choisi comme pas de quantification pour Le coefficient de la TOD à l'endroit (i,j), la quantification linéaire à mi-pas [17] implique que les dégradations ayant une valeur inférieure à $q_l^q(i,j)/2$ sont supposées imperceptibles.

Donc, nous avons choisis de mettre la fonction de pondération perceptuelle $p^q(i,j)$ pour les coefficients des trois sous-bandes $\left\{I_1^{HL}, I_1^{LH}, I_1^{HH}\right\}$comme suit :

$$p^q(i,j) = q_1^q(i,j)/2 \tag{2.29}$$

L'utilisation de ce modèle psychovisuel en tatouage d'images nous permet de répondre à deux contraintes : l'invisibilité de la signature est garantie, et Le compromis invisibilité-robustesse est optimisé.

5. PROCESSUS DE DETECTION DE LA SIGNATURE

Comme nous l'avons vu dans le chapitre précédent, les transformations géométriques provoquent une perte de synchronisation empêchant la détection de la signature. Il est extrêmement difficile d'obtenir un schéma robuste à toutes les catégories de transformations géométriques possibles. Certains schémas permettent d'identifier une transformation affine grâce à l'insertion de mires artificielles à l'intérieur de l'image, mais ils ne sont pas robustes aux transformations locales de l'image. D'autres schémas [5] utilisent le contenu de l'image pour apporter des repères liés à celle-ci. Les limites de ces méthodes sont atteintes lorsque la transformation géométrique appliquée est trop importante. La robustesse et les performances de ces schémas sont fortement liées au contenu de l'image que l'on doit traiter. Une autre stratégie pour faire face au problème de perte de synchronisation après une transformation consiste à trouver un espace d'insertion qui soit invariant à cette transformation comme la Transformée en Ondelettes Complexes [18].

Ici, nous avons introduit un algorithme de recalage des images [21] en appliquant une technique d'estimation différentielle de mouvement définie dans [22] pour établir une relation géométrique entre l'image originale et l'image tatouée géométriquement déformée, Un modèle affine à six paramètres est employé pour estimer le cisaillement, la rotation, la translation et le changement d'échelle. Cette technique nous permet de compenser les éventuelles transformations géométriques subies par l'image.

5.1. Présentation de l'algorithme de recalage

5.1.1. Définition

Le terme recalage est synonyme d'expressions telle que mise en correspondance ou alignement [19]. Il consiste essentiellement à établir une relation géométrique entre les objets représentés par deux images : l'image source (test) et l'image cible (référence). On peut aussi le définir comme le processus qui aligne deux images géométriquement [15].

La majorité des méthodes de recalage des images comporte habituellement les principaux éléments suivants [19] :

§ *L'identification et l'extraction des caractéristiques géométriques communes* : caractéristiques que l'on appelle des primitives ou attributs et qui peuvent être des points, des lignes, des surfaces, contours/bords,…etc.

§ *Le choix d'une transformation* (au sens mathématique) qui aligne deux images, locale ou globale. Une transformation est dite « globale » si elle s'applique à toute l'image, et « locale » si elle s'applique à des sous-régions de l'image qui ont alors chacune leur propre transformation.

§ *Le type de transformation* : rigide, non rigide, affine ou projective. Dans le recalage rigide global, seules les translations et les rotations sont admises. Les distances entre les points et les angles entre les lignes ne changent pas pendant le recalage .Les méthodes affines de recalage transforment des lignes parallèles en lignes parallèles. Les transformations projectives conservent les lignes. Les méthodes de recalage non rigide font intervenir des transformations plus générales.

§ *Un critère de similarité* qui modélise l'interaction entre les variables à estimer (paramètres de la transformation), et les données observées (attributs à mettre en correspondance défini dans le premier critère).

§ *L'optimisation* : une fois le problème formalisé, on recherche à estimer les meilleurs paramètres de transformation par une méthode d'optimisation dont le rôle est crucial.

Pour développer notre algorithme de recalage, nous avons essayé de trouver un compromis entre une technique souple et efficace. Afin d'éviter les diverses erreurs impliquées dans la sélection des attributs géométriques de l'image, nous avons choisi l'approche basée sur l'intensité présentée dans [20] [21] [22], rappelée ci-dessous.

Géométriquement, les transformations géométriques sont modelisées avec une transformation affine locale et une contrainte de lissage globale. Six paramètres sont simultanément estimés pour chaque pixel, nous permettant de capturer les déformations non-*linéaires* dans la géométrie.

Nous utilisons une métrique d'erreur standard MSE (Mean Square Error) sur les valeurs d'intensité. La minimisation implique deux étapes. D'abord une fonction erreur linéaire est minimisée en utilisant le critère des moindres carrés. Cette fonction d'erreur est alors augmentée avec une contrainte de lissage non-linéaire, et la solution des moindres carrés est employée pour procéder à une minimisation itérative non-linéaire. Une technique différentielle multi-échelles est utilisée pour réaliser cette procédure qui nous permet de capturer les transformations à grande et à petite échelle.

5.1.2. Formulation

Nous formulons le problème de recalage de l'image dans un cadre différentiel [22]. Cette formulation est empruntée de divers domaines d'estimation de mouvement.

a) Modèle affine local

Soit $I(x, y, t-1)$ l'image originale (référence) et $I(\hat{x}, \hat{y}, t)$ l'image tatouée ayant subi une transformation géométrique (test). La dénotation entre les deux images est adoptée avec un paramètre temporel *t*. Nous considérons la déformation comme un mouvement entre deux images de la même scène pris en deux instants différents.

Nous supposons que les intensités entre les images sont conservées, et que la transformation géométrique entre les images peut être modélisée localement par une transformation affine,

$$I(x,y,t) = I(m_1 x + m_2 y + m_5, m_3 x + m_4 y + m_6, t-1) \quad (2.30)$$

Où m_1, m_2, m_3, m_4 sont les paramètres affines linéaires, et m_5, m_6 les paramètres de translation. Ces paramètres sont estimés localement pour chaque petit voisinage spatial. Afin d'estimer ces paramètres, nous définissons la fonction d'erreur quadratique à minimiser suivante :

$$E(\vec{m}) = \sum_{x,y \in \Omega} [I(x,y,t) - I(m_1 x + m_2 y + m_5, m_3 x + m_4 y + m_6, t-1)]^2 \quad (2.31)$$

Où $\vec{m} = (m_1 \ldots m_6)^T$, et Ω dénote un petit voisinage spatial. Puisque cette fonction d'erreur est non-linéaire dans ses inconnues. Elle ne peut pas être minimisée analytiquement. Pour simplifier la minimisation, nous approximons cette fonction d'erreur en utilisant une expansion tronquée de premier ordre en séries de Taylor [22] :

$$E(\vec{m}) \approx \sum_{x,y \in \Omega} [I_t(x,y,t) - (m_1 x + m_2 y + m_5 - x) I_x(x,y,t) - (m_3 x + m_4 y + m_6 - y) I_y(x,y,t)]^2 \quad (2.32)$$

Où $I_t(.), I_x(.), I_y(.)$ sont les dérivées spatiotemporelles de $I(.)$. Noter que cette fonction d'erreur quadratique est maintenant linéaire dans son inconnue $\vec{m}$, et que l'expansion de séries de Taylor est plus précise pour les petits mouvements.

Cette fonction d'erreur peut être exprimée d'une manière plus compacte sous forme vectorielle :

$$E(\vec{m}) = \sum_{x,y \in \Omega} \left[k - \vec{c}^T \vec{m}\right]^2 \quad (2.33)$$

Où le scalaire *k* et le vecteur $\vec{c}$ sont donnés par :

$$k = I_t + x I_x + y I_y \quad (2.34)$$

$$\vec{c} = (xI_x \;\; yI_x \;\; xI_y \;\; yI_y \;\; I_x \;\; I_y)^T \tag{2.35}$$

Elle peut maintenant être minimisée analytiquement en différenciant par rapport à $\vec{m}$:

$$\frac{dE(\vec{m})}{d\vec{m}} = \sum_{x,y\in\Omega} -2\vec{c}\left[k - \vec{c}^T\vec{m}\right] \tag{2.36}$$

Mettant le résultat égal à zéro, et résolvant pour $\vec{m}$,

$$\vec{m} = \left[\sum_{x,y\in\Omega} \vec{c}\,\vec{c}^T\right]^{-1}\left[\sum_{x,y\in\Omega} \vec{c}\,k\right] \tag{2.37}$$

Cette solution suppose que le premier terme $\left[\sum_{x,y\in\Omega} \vec{c}\,\vec{c}^T\right]^{-1}$, une matrice 6×6, est inversible.

b) Contrainte de lissage globale

Jusqu'ici, nous avons supposé que les paramètres du modèle affine sont constants dans un petit voisinage spatial, équation (2.33).

Il y a un compromis naturel dans le choix de la taille de ce voisinage. Il est plus probable que la matrice $\left[\sum_{x,y\in\Omega} \vec{c}\,\vec{c}^T\right]^{-1}$ dans l'équation (2.37) sera inversible lorsque on choisi une région large. Cependant, il est plus probable que la supposition de la constance du mouvement sera maintenue lorsque on choisit une petite région. Nous pouvons remplacer la supposition de constance avec une supposition de lissage. C'est-à-dire, on suppose que les paramètres $\vec{m}$ du modèle changent légèrement à travers l'espace [22].

Nous commençons par une fonction d'erreur :

$$E(\vec{m}) = E_L(\vec{m}) + E_g(\vec{m}) \tag{2.38}$$

qui combine la contrainte de lissage, $E_L(\vec{m})$, avec la contrainte de la transformation géométrique précédente:

$$E_g(\mathbf{m}) = \sum_{x,y \in \Omega} \left[k - \mathbf{c}^T \mathbf{m}\right]^2 \tag{2.39}$$

Avec k et $\mathbf{c}$ donnés par les équations (2.34) (2.35).

Le nouveau terme d'erreur quadratique $E_L(\mathbf{m})$ incorporant la contrainte de lissage est

$$E_L(\mathbf{m}) = \sum_{i=1}^{6} l_i \left[\left(\frac{\partial m_i}{\partial x}\right)^2 + \left(\frac{\partial m_i}{\partial y}\right)^2\right] \tag{2.40}$$

Où l_i est une constante positive qui contrôle la pondération relative donnée à la contrainte de lissage sur le paramètre m_i.

La dérivée de $E_g(\mathbf{m})$ est donnée par :

$$dE_g(\mathbf{m}) / d\mathbf{m} = -2\mathbf{c}\left[k - \mathbf{c}^T \mathbf{m}\right] \tag{2.41}$$

Pour calculer la dérivée de $E_L(\mathbf{m})$, nous utilisons d'abord les dérivées discrètes approximatives de m_i par rapport à x et y :

$$\frac{dm_p(i,j)}{dx} = m_p(i,j) - m_p(i+1,j) \tag{2.42}$$

$$\frac{dm_p(i,j)}{dy} = m_p(i,j) - m_p(i,j+1) \tag{2.43}$$

Nous pouvons maintenant exprimer l'erreur de lissage d'un paramètre particulier m_p comme suit :

$$\begin{aligned} E_L(m_p(i,j)) &= l_p\left[\left(\frac{\partial m_p(i,j)}{\partial x}\right)^2 + \left(\frac{\partial m_p(i,j)}{\partial y}\right)^2\right] \\ &= l_p\left[(m_p(i,j) - m_p(i+1,j))^2 + (m_p(i,j) - m_p(i,j+1))^2\right] \end{aligned} \tag{2.44}$$

La dérivée de cette erreur de lissage par rapport à m_p peut être maintenant écrite comme :

$$\begin{aligned}\frac{dE_L(m_p(i,j))}{dm_p(i,j)} &= 2l_p[m_p(i,j)-m_p(i+1,j)]+2[m_p(i,j)-m_p(i,j+1)] \\ &= 4l_p m_p(i,j)-2l_p[m_p(i+1,j)+m_p(i,j+1)] \\ &= 4l_p[m_p(i,j)-\overline{m}_p(i,j)] \end{aligned} \quad (2.45)$$

Où $\overline{m}_p(i,j)=(m_p(i+1,j)+m_p(i,j+1))/2$, est la moyenne locale de m_p autour du pixel (i,j). En utilisant la notation vectorielle, nous pouvons succinctement représenter la dérivée de lissage comme suit :

$$\frac{dE_L(\vec{m})}{d\vec{m}} = 2L(\bar{\vec{m}}-\vec{m}) \quad (2.46)$$

Où $\bar{\vec{m}}$ est la composante moyenne de $\vec{m}$ sur un petit voisinage spatial, et L une matrice diagonale 6×6 avec l_i ses éléments diagonaux. Mettant $dE_b(\vec{m})/d\vec{m}+dE_L(\vec{m})/d\vec{m}=0$, et résolvant pour $\vec{m}$ à chaque emplacement de pixel se traduit par un système linéaire énorme qui est compliqué à résoudre.

Au lieu de cela, $\vec{m}$ est estimé de la façon itérative suivante [21] :

$$\vec{m}^{(j+1)} = \left(\vec{c}\,\vec{c}^{\,T}+L\right)^{-1}\left(\vec{c}\,k+L\,\bar{\vec{m}}^{(j)}\right) \quad (2.47)$$

Le premier estimé $\vec{m}^{(0)}$ est déterminé à partir de la solution obtenue dans la section précédente (4.2.2. (a)).
A l'itération (j+1) $\bar{\vec{m}}^{(j)}$ est estimé à partir de l'estimé précédant, $\vec{m}^{(j)}$.

5.2. Détails pour une implémentation réussie

La formulation donnée dans les deux sections précédentes est relativement simple. Cependant, il y a quelques détails qui sont critiques pour une implémentation réussie.

Premièrement, la fonction d'erreur donnée par l'équation (2.33) est seulement une approximation de la fonction d'erreur réelle donnée par l'équation (2.31), pour simplifier la minimisation, l'estimation à partir de la fonction d'erreur approximative est améliorée en utilisant la forme itérative du modèle de Newton-Raphson [21]. En particulier, à chaque itération, nous estimons les paramètres affines entre l'image test (image tatouée ayant subit une transformation géométrique) et l'image originale (de référence), et nous déformons l'image test suivant ces paramètres estimés. Une nouvelle transformation est estimée entre la nouvelle image teste déformée et l'image originale. Cinq itérations peuvent améliorer considérablement l'estimée finale $\hat{\vec{m}}$.

Deuxièmement, Les dérivées spatiotemporelles exigées ont un support fini, ce qui limite la quantité de mouvement qui peut être estimée. Un schéma pour passer d'un état grossier à un état fin est adopté afin de faire face aux grands mouvements. Une pyramide [20] est d'abord construite pour les deux images, originale et test, la mise en correspondance entière est estimée au niveau le plus grossier. Cette estimée est employée pour déformer l'image test au prochain niveau de la pyramide. Une nouvelle estimée est calculée à ce niveau, et le processus se répète à chaque niveau de la pyramide. Les transformations à chaque niveau de la pyramide sont accumulées produisant une seule transformation finale.

Le calcul des dérivées spatiotemporelles est une étape cruciale. Les dérivées des images sont souvent calculées comme une différence entre les valeurs de voisinage du pixel. Telles différences sont en général des faibles approximations et mènent aux erreurs substantielles. Pour calculer ces dérivées, un ensemble de filtres spécifiquement conçus pour la différentiation multidimensionnelle est utilisé [20]. Ces filtres améliorent d'une manière significative la mise en correspondance résultante.

5.3. Détection de la signature

Pour la détection, la corrélation r entre les coefficients tatoués et la séquence binaire chaotique dont on examine sa présence, est calculée :

$$r = \frac{1}{3MN}\sum_{i=0}^{M}\sum_{j=0}^{N}\tilde{I}_1^{LH}(i,j).w(iN+j)+\tilde{I}_1^{HL}(i,j).w(MN+iN+j)+\tilde{I}_1^{HH}(i,j).w(2MN+iN+j) \quad (2.48)$$

Où $3MN$ est la longueur de la signature et $2M \times 2N$ Les dimensions de l'image.

Cette corrélation est ensuite comparée à un seuil T_r choisi de telle façon à minimiser la probabilité de fausses alarmes (probabilité de faux positifs) de détection.

Pour déterminer T_r le critère de *Neyman-Pearson* est adopté [13]: au lieu de minimiser la probabilité d'erreur globale, nous minimisons la probabilité de faux négatifs sachant une probabilité de fausses alarmes donnée. De cette manière la robustesse contre les attaques est augmentée et la détection est accomplie sans aucune connaissance de a .
Etant donné une image $\tilde{I}$ et une signature *W*, seulement trois cas sont possibles.

Cas A: l'image $\tilde{I}$ n'est pas tatouée.

Cas B: l'image $\tilde{I}$ est tatouée par une signature *Z* différente de *W*.

Cas C: l'image $\tilde{I}$ est tatouée par la signature *W*.

Pour appliquer la théorie statistique de décision, nous devons faire quelques suppositions sur les variables aléatoires qui forment la variable d'observation r . Nous supposons que la signature W est une séquence des variables aléatoires indépendantes de moyenne nulle, et également indépendante par rapport aux coefficients de la TOD. Pour les coefficients tatoués de la TOD, nous supposons qu'ils sont des variables aléatoires indépendantes de moyenne nulle. Par l'exploitation du théorème de la limite centrale, nous pouvons également supposer que r est normalement distribué. Sous ces hypothèses, il est facile de démontrer [13] que les valeurs moyennes dans les trois cas A, B, et C sont :

$$\begin{aligned} &\textbf{Cas A}: \ m_{r_A} = 0 \\ &\textbf{Cas B}: \ m_{r_B} = 0 \\ &\textbf{Cas C}: \ m_{r_C} = \frac{a}{3MN}\sum_{i=0}^{M}\sum_{j=0}^{N}E\left[p^{LH}(i,j)\right]+E\left[p^{HL}(i,j)\right]+E\left[p^{HH}(i,j)\right] \end{aligned} \quad (2.49)$$

Cette corrélation est comparée au seuil T_r : si $r > T_r$, la signature est présente, sinon le détecteur indique l'absence de celle-ci.

Pour estimer la probabilité de fausses alarmes

$$P_f = \text{Prob}\,(r > T_r \,|\, \text{Cas A}.ou.\text{Cas B}) \tag{2.50}$$

On doit calculer la variance de la variable aléatoire r dans le cas A et le cas B.

Il est facile d'obtenir pour le cas A que :

$$s_{r_A}^2 = \frac{s_w^2}{(3MN)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} E\left[\left(I_1^{LH}(i,j)\right)^2\right] + E\left[\left(I_1^{HL}(i,j)\right)^2\right] + E\left[\left(I_1^{HH}(i,j)\right)^2\right] \tag{2.51}$$

En outre, pour le cas B :

$$\begin{aligned} s_{r_B}^2 = {} & \frac{s_w^2}{(3MN)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} E\left[\left(I_1^{LH}(i,j)\right)^2\right] + E\left[\left(I_1^{HL}(i,j)\right)^2\right] + E\left[\left(I_1^{HH}(i,j)\right)^2\right] + \\ & \frac{a^2 s_w^4}{(3MN)} \sum_{i=1}^{M} \sum_{j=1}^{N} E\left[\left(p^{LH}(i,j)\right)^2\right] + E\left[\left(p^{HL}(i,j)\right)^2\right] + E\left[\left(p^{HH}(i,j)\right)^2\right] \end{aligned} \tag{2.52}$$

Il est clair que le deuxième cas est le plus mauvais, parce qu' une grande variance donne une grande probabilité d'erreur.

Donc, la probabilité de fausses alarmes est donnée par :

$$P_f \le \frac{1}{2} erfc\left(\frac{T_r}{\sqrt{2 s_{r_B}^2}}\right) \tag{2.53}$$

À titre d'exemple, lorsque on fixe $P_f = 10^{-8}$, on trouve

$$T_r = 3.97\sqrt{2 s_{r_B}^2} \tag{2.54}$$

Notant que $s_x^2 = s_x^4 = 1, E[I_1^q(i,j)] = E[w_1^q(i,j)] = 0$, et que $w_1^q(i,j)$ ne dépend pas de $I_1^q(i,j)$ ainsi que de $p^q(i,j)$, ce qui donne

$$s_{r_B}^2 = \frac{1}{(3MN)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} E\left[\left(\tilde{I}_1^{LH}(i,j)\right)^2\right] + E\left[\left(\tilde{I}_1^{HL}(i,j)\right)^2\right] + E\left[\left(\tilde{I}_1^{HH}(i,j)\right)^2\right] \tag{2.55}$$

Dans la pratique, l'estimée impartialle de s_{r_B} suivant est employée :

$$s^2_{r_B} \approx \frac{1}{(3MN)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(\tilde{I}_1^{LH}(i,j)\right)^2 + \left(\tilde{I}_1^{HL}(i,j)\right)^2 + \left(\tilde{I}_1^{HH}(i,j)\right)^2 \quad (2.56)$$

Ce dernier résultat est très important, parce qu'il implique que le seuil T_r peut être calculé *à posteriori sur* l'image tatouée. Par conséquent, la détection de la signature peut être effectuée sans aucune connaissance de la valeur du paramètre a , qui peut être donc adaptée parfaitement à chaque image.

6. Conclusion

Ce chapitre a été consacré au développement d'une méthode de tatouage d'images numériques. Nous avons présenté une méthode complète. La modulation d'une signature chaotique, à condition initiale secrète avec les coefficients issue d'une décomposition mutirésolution de l'image, a été adaptée et maximisée selon des caractéristiques de l'image et des considérations psychovisuelles afin d'optimiser le compromis invisibilité/robustesse. Cependant, la méthode souffre de ne pas être robuste aux transformations géométriques asynchrones. C'est pour cette raison que nous avons introduit l'outil de recalage souvent utilisé en imagerie pour remédier à cet inconvénient.

CONCLUSION

Nous avons introduit ce travail en exposant les principes et les propriétés générales d'un processus de tatouage d'images numériques qui nous ont conduits à en établir le cahier des charges pour un tatouage robuste et efficace.

Pour respecter ce cahier des charges, nous avons mis en œuvre une méthode complète permettant de certifier que le compromis invisibilité/robustesse du tatouage est garantit. L'insertion suit un schéma d'étalement du spectre d'une séquence chaotique dans la transformée en ondelettes de l'image. Cette transformée permet de séparer différentes résolutions de l'image en meilleur accord avec un masque psychovisuel permettant une meilleur approche du compromis invisibilité/robustesse. Une étude statistique du problème de détection nous a conduit à un seuil optimum qui peut être calculé à posteriori sur l'image tatouée.

Cependant, notre méthode souffre de ne pas être robuste aux transformations géométriques asynchrones. Pour remédier à ce problème, nous avons introduit un outil de recalage issu d'une technique d'estimation différentielle de mouvement pour recouvrer les éventuelles déformations géométriques subies par l'image.

La suite de notre travail visait à analyser les performances de la méthode développée face à un ensemble d'attaques. Les résultats obtenus sont satisfaisants, puisqu'ils démontrent la robustesse du schéma face à une grande variété d'attaques.

Les perspectives ouvertes par ce travail porte sur la nécessité de construire des schémas qui tiennent en compte les différentes caractéristiques de l'image (points, régions, objets). L'utilisation de ces attributs permet de marquer séparément les différents éléments de l'image et de lier la signature au contenu de l'image, mais aussi d'obtenir des schémas auto-synchronisants. De plus, le temps de calcule nécessaire à l'insertion et la détection de la signature est considérablement réduit, mettant ces schémas de meilleurs candidats pour le tatouage de la vidéo qui constitue encore un challenge, car il ajoute des contraintes de traitement en temps réel d’un important flux de données. Par conséquent les standards actuels de la vidéo numérique devront intégrer des algorithmes de tatouage efficaces, notamment qui évitent une décompression complète du flux vidéo.

1. INTRODUCTION

Dans ce chapitre nous allons exposer les résultats auxquels nous sommes parvenus en appliquant la méthode de tatouage définie dans le chapitre précédant. Nous allons évaluer ici les performances de la méthode de tatouage en terme d'invisibilité et de robustesse face aux diverses attaques. Dans la dernière section, nous donnons quelques perspectives pour des travaux futurs.

2. PLATEFORME DE TEST

Dans le but d'évaluer les performances de notre méthode de tatouage, nous l'appliquons sur l'image "Lena" de taille 512×512 donnée par la figure 3.1. Cette image, codée avec 256 niveaux de gris, est classiquement utilisée en traitement d'image. Elle a une distribution fréquentielle moyenne. C'est une image très contrastée, elle comporte des angles vifs et des espaces texturés ainsi que des zones homogènes. Ce choix est judicieux à deux égards :

- Les images codées sur 256 niveaux de gris sont la base de travail de la plupart des algorithmes de traitement d'images.
- En tatouage d'image, la solution de facilité consiste à travailler directement sur la luminance de l'image. Les schémas développés en niveaux de gris peuvent alors s'appliquer sur la luminance des images couleurs. Cependant, un choix judicieux de l'espace couleur, comme espace d'insertion, permet d'augmenter les propriétés psychovisuelles de l'insertion de la signature.

L'algorithme de tatouage et les attaques ont été effectués sous l'environnement Matlab 6.5, et nous avons utilisé l'ondelette 'CDF9/7' pour calculer la TOD. La probabilité de fausses alarmes adoptée est égale à 10^{-8} [34].

Figure 3.1 Image Lena.

3. MESURE DE QUALITE

La notion de qualité intervient deux fois dans le cahier des charges d'un processus de tatouage. Il faut d'une part que l'image tatouée soit de la même qualité que l'image originale. D'autre part, les attaques auxquelles doit être robuste le tatouage, doivent conserver la qualité de l'image. Cette notion de qualité permet donc de caractériser les attaques et de restreindre leur ensemble afin d'étudier la robustesse de l'algorithme de tatouage.

La mesure de distorsion la plus populaire en traitement d'images, pour quantifier numériquement la qualité d'une image, est tout simplement le *PSNR*. Il est mesuré en dB à partir de la relation suivante :

$$PSNR_{dB} = 10\log_{10}\left(\frac{M * N * 255^2}{\sum_{i,j}(\tilde{I}(i,j) - I(i,j))^2}\right) \tag{3.1}$$

Où $I(i,j)$ est l'image originale, et $\tilde{I}(i,j)$ est l'image tatouée, les deux images étant de taille [$M \times N$].

Le *PSNR* quantifie l'intensité de la signature. Cependant, il ne s'adapte pas aux caractéristiques de l'image : la signature est en effet plus visible dans les zones peu texturées (à variance faible) et moins visible dans les zones plus texturées (à variance élevée). Pour quantifier plus efficacement la visibilité de l'image nous avons utilisé le *WPSNR* (Weighted *PSNR* : *PSNR* pondéré) [31] qui prend en considération le contenu de l'image pour juger de la visibilité de la signature. Le *WPSNR* est issu du *PSNR* mais il est plus pénalisant quand la signature est insérée dans les zones homogènes qui sont les plus pénalisantes pour la visibilité, et moins pénalisant quand la signature est insérée dans les zones texturées. Le *WPSNR* est donné par :

$$WPSNR_{dB} = 10\log_{10}\left(\frac{M * N * 255^2}{\sum_{i,j} NVF(i,j) * (\tilde{I}(i,j) - I(i,j))^2}\right) \tag{3.2}$$

NVF (Noise Visibility Function) est la fonction de visibilité du bruit, basée sur une modélisation stochastique de l'image et du bruit, dont la valeur sera faible pour les contours et les textures, et forte dans les régions uniformes. Cette fonction est donnée par la relation suivante :

$$NVF(i,j) = \frac{1}{1 + CS * VarLocale(i,j)} \tag{3.3}$$

Où *CS* est la sensibilité de contraste donnée par :

$$CS = \frac{CS_0}{Max(VarLocale(i,j))},\ CS_0 = 150. \tag{3.4}$$

et *VarLocale* : est la variance locale de l'image calculée sur un petit voisinage de taille 3×3 suivant un modèle gaussien non-stationnaire .

4. DEGRADATION

Afin d'évaluer les performances générales de l'algorithme proposé avec les divers valeurs du paramètre d'invisibilité a , nous avons effectué plusieurs expériences sur l'image "Lena" en modifiant la valeur de a . Le tableau 3.1 montre les résultats que l'on obtient,

sachant que la valeur de a varie de 0.01 à 2. On peut remarquer que la valeur du *WPSNR* diminue lorsque la valeur de a augmente, cela signifie qu'il faut choisir une petite valeur a pour avoir une haute fidélité visuelle. Cependant, les résultats expérimentaux montre que lorsque a est égale ou inférieure à 0,01 on ne peut pas détecter la signature correctement.

a	0.01	0.1	0.3	0.6	1	1.5	2
WPSNR	54.72	54.22	49.06	43.66	39.36	35.88	33.40
r	0.3658	0.4874	1.2517	2.4910	4.1651	6.2536	8.3385
T_r	0.0649	0.0652	0.0682	0.0777	0.0967	0.1257	0.1557
Détection	Echec	OK	OK	OK	OK	OK	OK

Tableau 3.1 Relations entre a , *WPSNR*, r et T_r , ($P_f = 10^{-8}$).

L'augmentation de la force du tatouage semble donner de bons résultats en terme de robustesse. Cependant, ce choix donne de mauvais résultats en terme d'invisibilité. Donc, nous avons choisis $a = 0.6$ pour garder un bon compromis entre les deux aspects robustesse/invisibilité. La figure 3.2 présente les résultats que l'on obtient en insérant une séquence chaotique binaire $\{-1,+1\}$ de taille $3\times 256\times 256$ dans l'image "Lena" avec la condition initiale $i_{séq} = 0.1564$, $m = 4$ et $a = 0.6$. La taille de la séquence a été choisie de telle sorte à balayer les trois sous-bandes de détails du premier niveau de la TOD de l'image.

Bien que l'on ne perçoive pas de détériorations, le *WPSNR* est assez faible (43.66 dB). La signature insérée est imperceptible, même lorsque on alterne l'image originale et l'image tatouée, ce qui prouve l'efficacité de la TOD et l'utilisation du masque psychovisuel pour dissimuler la signature. En particulier, l'efficacité de la fonction de pondération perceptuelle peut être appréciée de la figure 3.3 où la différence absolue entre l'image originale et tatouée est amplifiée par un facteur de 15 de façon à rendre les modifications visibles. Il est évident que la signature est surtout cachée dans les régions de haute activité (zones texturés) et autour des bords.

(a) **(b)**

Figure 3.2 Image originale "Lena" (a), et sa version tatouée (b).

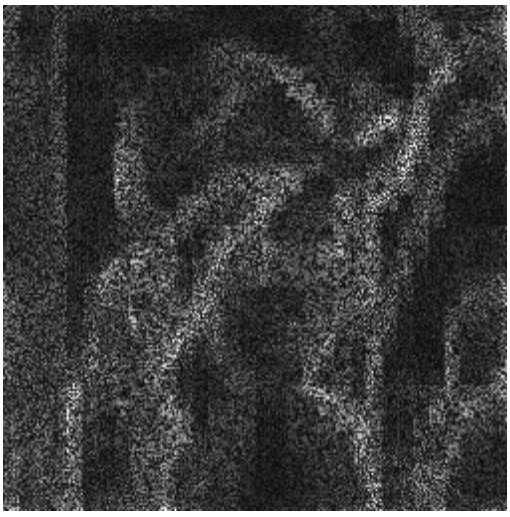


Figure 3.3 La différence absolue entre l' image originale et l' image tatouée amplifiée 15 fois.

5. FIABILITE DE DETECTION ET UNICITE DE LA SIGNATURE

Un algorithme de tatouage d'images doit pouvoir détecter la signature insérée dans l'image, mais il doit aussi pouvoir la différencier vis-à-vis d'autres signatures différentes appelées couramment fausses alarmes. Cette distinction doit être la plus évidente possible, dans le but d'éviter tout litige.

On peut représenter les performances du détecteur par un graphique. La figure 3.4 présente la réponse du détecteur r à 1000 signatures chaotiques générées aléatoirement (générées à partir des conditions initiales différentes). Notre signature implantée dans l'image apparaît en position 200. Aucune attaque n'a été portée à l'image. Les courbes montrent que l'on peut détecter parfaitement la signature dans les images tatouées sans équivoque, suggérant que l'algorithme a des taux de réponse de fausses alarmes (et faux négatifs) très bas.

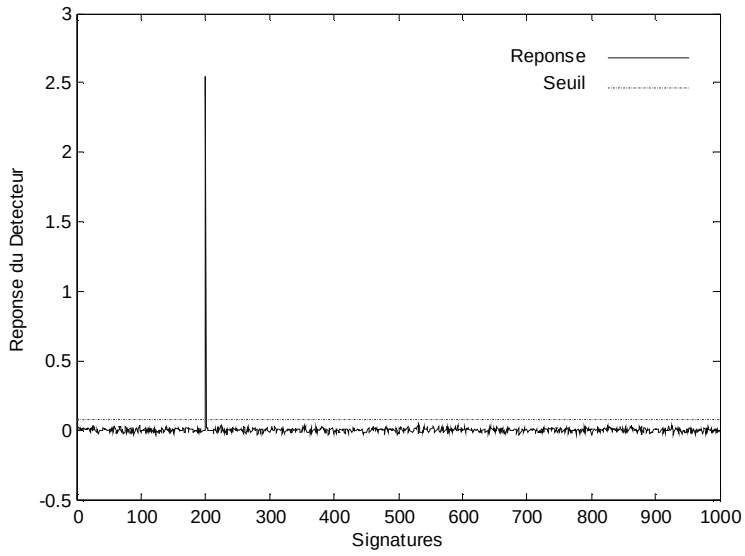


Figure 3.4 La réponse du détecteur à 1000 signatures générées à partir des conditions initiales différentes, la signature voulue est en position 200 des abscisses.

Puisque la détection est assurée, il reste maintenant à évaluer l'impact des attaques sur l'algorithme et les conséquences qu'elles peuvent avoir sur la détection.

6. ROBUSTESSE AUX DIVERSES ATTAQUES

Comme il s'avère impossible de considérer toutes les attaques possibles, nous avons décidé de restreindre notre domaine d'étude à l'ensemble de quelques attaques présentées dans le banc de test Checkmark [31].

6.1. Robustesse à la compression JPEG

Nous avons éprouvé la robustesse de notre schéma face à la compression JPEG, comme première expérience. La compression JPEG est encore actuellement l'algorithme de compression le plus largement utilisé.

La compression JPEG avec une qualité décroissante est appliquée sur l'image tatouée, et 1000 signatures différentes (parmi elles notre signature) sont examinées pour la détection. Sur la figure 3.5, la réponse du détecteur à la signature incorporée est tracée en fonction du facteur de qualité. Sur le même graphe, nous avons représenté la deuxième réponse la plus élevée du détecteur (c.-à-d., la réponse la plus élevée parmi celles produites par le détecteur lorsque les 999 fausses signatures sont examinées).

La réponse du détecteur demeure au-dessus du seuil de détection jusqu'à ce qu'un facteur de qualité de 10% soit atteint, La deuxième réponse la plus élevée du détecteur reste toujours en dessous du seuil.

La figure 3.5 montre que l'impact de la compression JPEG sur les performances du détecteur est assez faible pour un facteur de qualité supérieur à 10%. En dessous, la signature ne va pas être détectée. La figure 3.6 représente l'image "Lenna" tatouée obtenue après une compression JPEG de 20% de qualité. L'image est fortement dégradée et des effets de blocs et des artefacts apparaissent nettement ce qui réduit sa qualité commerciale. Cependant, La détection est excellente et la signature est reconnue sans aucune erreur. Ces excellents résultats sont obtenus grâce à l'utilisation de la TOD pour exploiter et modéliser les différentes propriétés de masquage du (SVH).

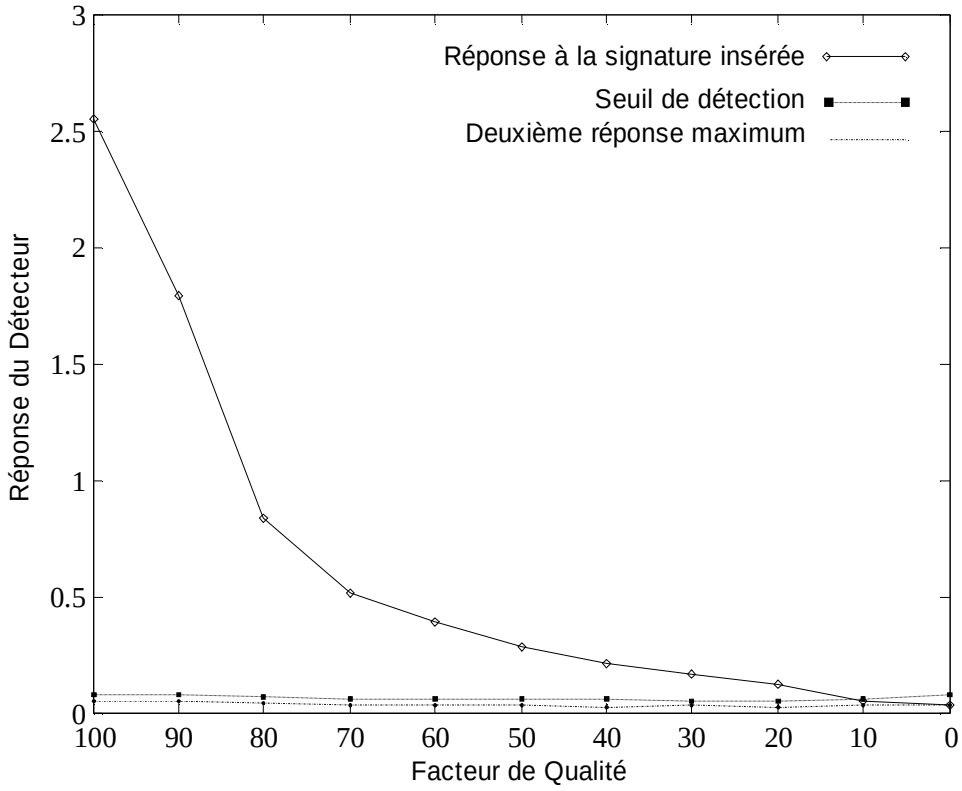
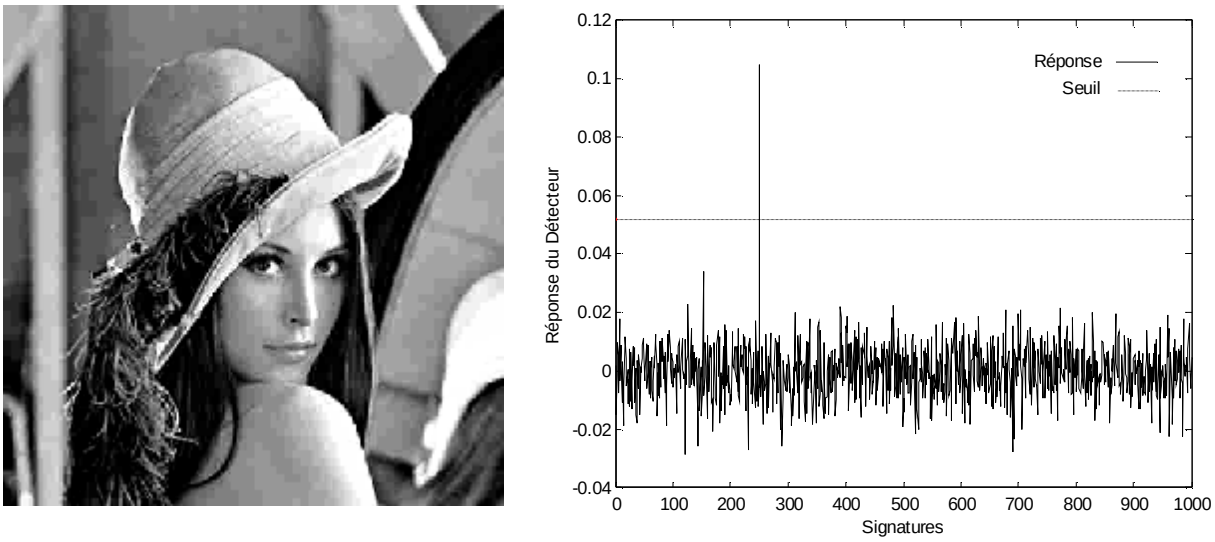


Figure 3.5 Réponse du détecteur en fonction du facteur de qualité.



(a) **(b)**

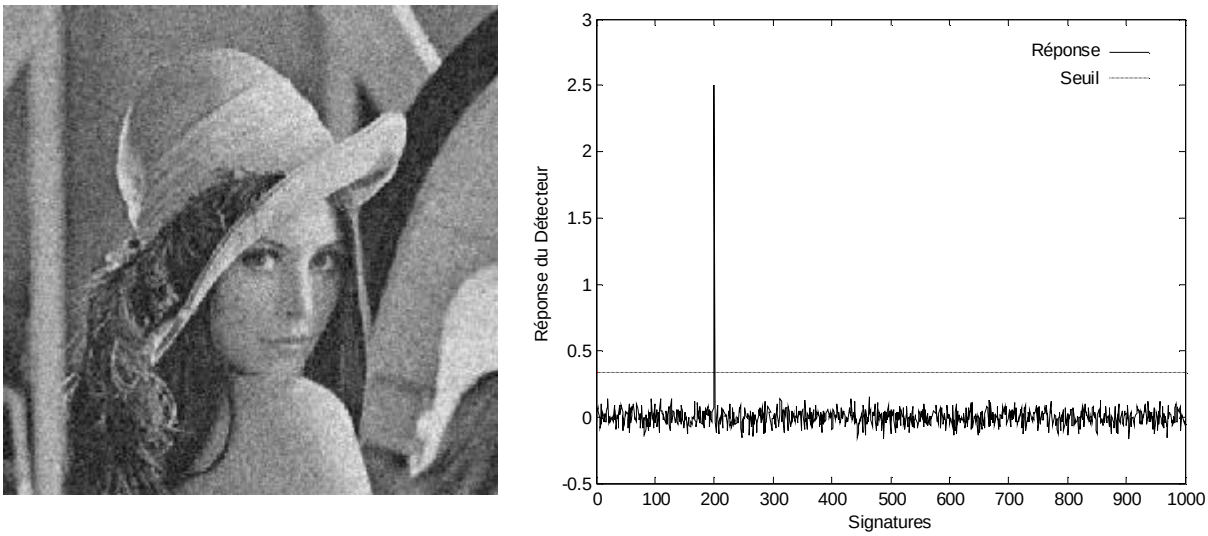
Figure 3.6 Effet de la compression JPEG sur l'image tatouée "Lena" pour un facteur de qualité de 20%(a), et la réponse du détecteur correspondante (b).

6.2. Contamination par un bruit gaussien

Nous avons également évalué la robustesse de l'algorithme en ajoutant un bruit gaussien à l'image tatouée. La variance du bruit utilisée dans la simulation varie de 10^{-5} à 10^{-2}. Le tableau 3.2 montre la réponse du détecteur à la signature insérée après l'ajout d'un bruit gaussien centré en faisant varier sa variance. Sur la figure 3.7, on peut observer que le détecteur détecte la signature correctement, bien que la contamination par un bruit de variance de 0.01 a causé à l'image une déformation intolérable. Notre schéma est tout à fait robuste à ce type de traitement.

Variance	Réponse r	seuil T_r	Décision
10^{-5}	2.5253	0.0786	OK
10^{-4}	2.5220	0.0843	OK
10^{-3}	2.5139	0.1286	OK
10^{-2}	2.5066	0.3316	OK

Tableau 3.2 Influence du bruit sur la détection.



(a) **(b)**

Figure 3.7 Effet de l'ajout du bruit gaussien centré de variance 0.01 à l'image tatouée "Lena"(a) , et la réponse du détecteur correspondante(b).

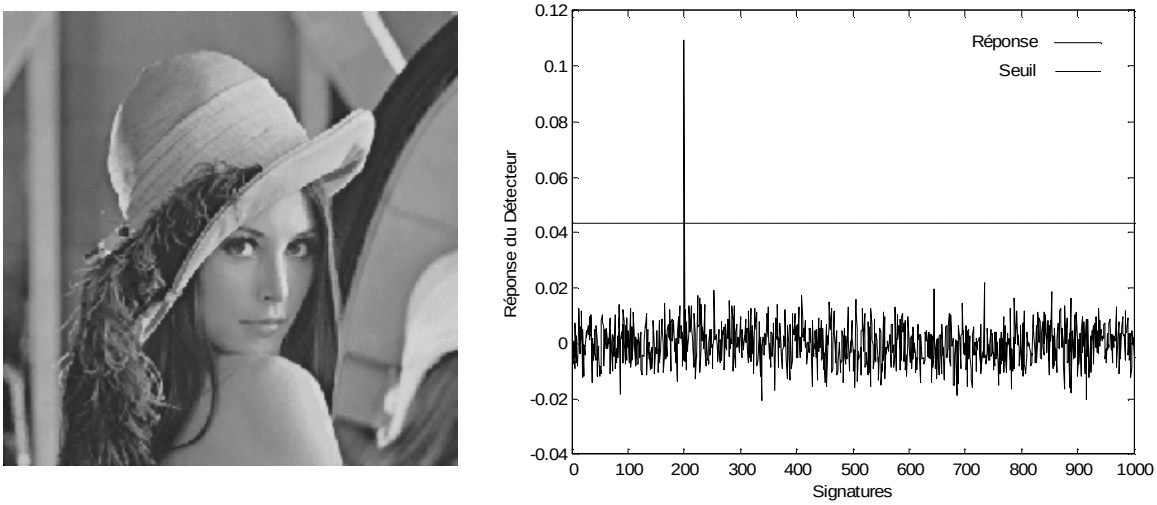
6.3. Robustesse au filtrage

Nous avons décidé d'effectuer comme attaque trois types de filtrage :

- Un lissage sur l'image tatouée "Lena" afin de réduire l'activité dans les zones texturées en utilisant un filtre Médian.
- Un rehaussement pour que l'image devienne plus contrastée et les détails davantage prononcés en utilisant un filtre passe haut de taille 3×3, $H=\frac{1}{4}\begin{bmatrix} 0 & -1 & 0 \\ -1 & 8 & -1 \\ 0 & -1 & 0 \end{bmatrix}$.
- Débruitage adaptatif par filtre de Wiener 5×5: ce type d'attaque concernent souplement les attaques sur les schémas d'étalement de spectre utilisant une signature de bruit blanc. Il vise à estimer la signature à partir du filtre de Wiener puis la soustrait après l'avoir multipliée au préalable par un facteur force, l'image résultante sera proche de l'image originale.

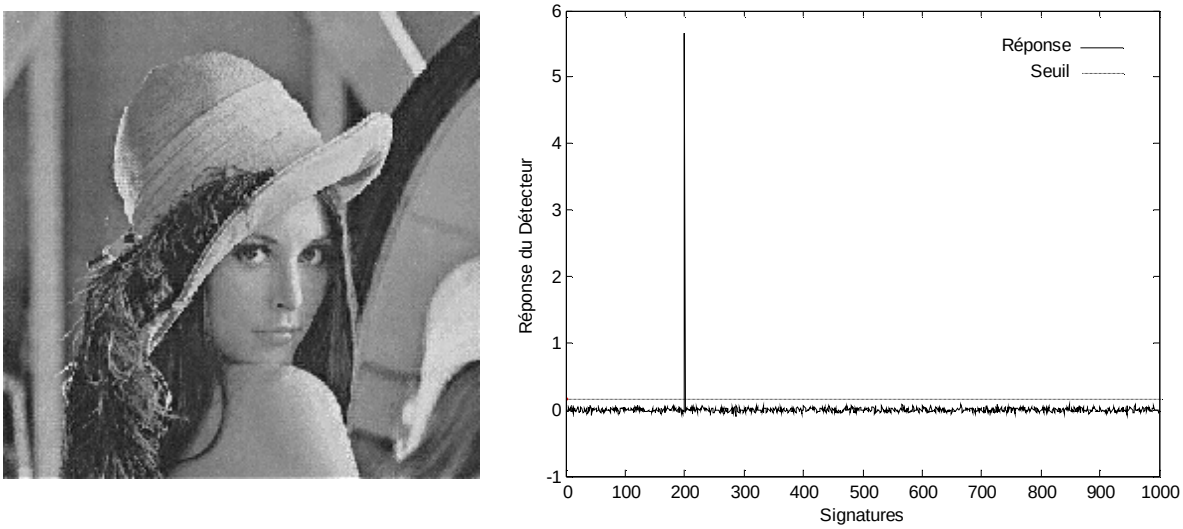
Les figures (3.8) (3.9) (3.10) montrent l'image Lena obtenue après tatouage pour les différents filtrages mentionnés ci-dessus et la réponse du détecteur correspondante.

Comme nous pouvons le voir, les transformations sont assez visibles. Nous estimons que les résultats obtenus sont satisfaisants, et l'utilisation de ces filtres n'influe pas sur la robustesse de notre schéma.



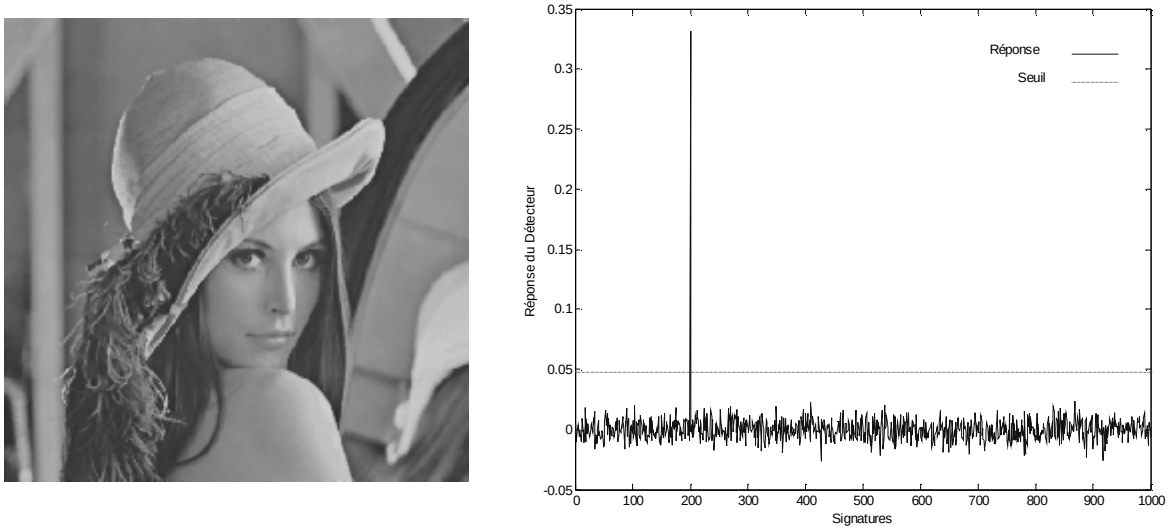
(a) **(b)**

Figure 3.8 Réponses du détecteur à 1000 signatures générées aléatoirement après filtrage Médian de l'image" Lena" tatouée,notre signature apparaît en position 200.



(a) **(b)**

Figure 3.9 Réponses du détecteur à 1000 signatures générées aléatoirement après filtrage Passe-haut de l'image" Lena" tatouée,notre signature apparaît en position 200.



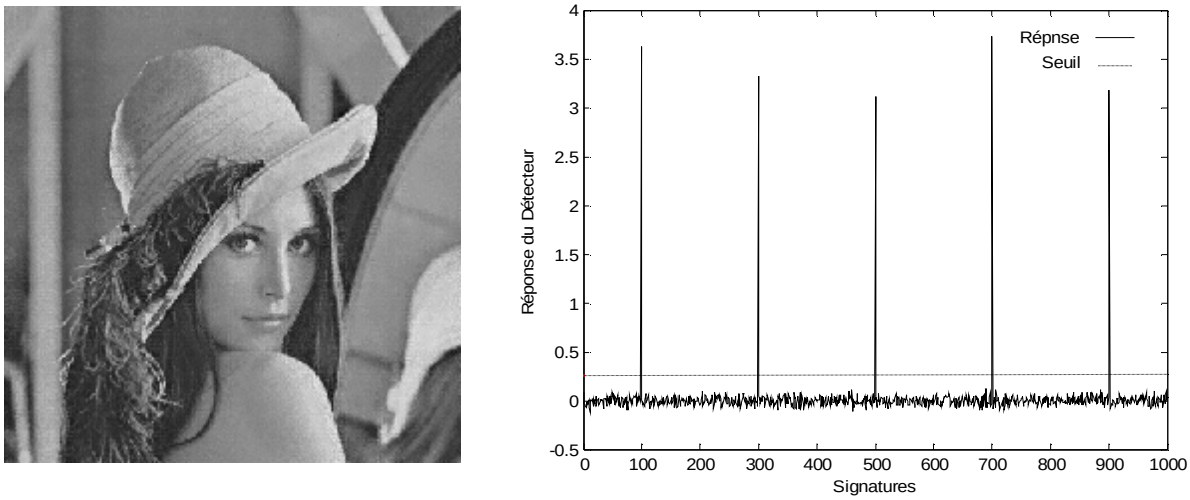
(a) **(b)**

Figure 3.10 Réponses du détecteur à 1000 signatures générées aléatoirement après filtrage Wiener de l'image" Lena" tatouée,notre signature apparaît en position 200.

6.4. Attaque par surmarquage

Elle consiste à tatouer à nouveau une image déjà tatouée. Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse. Certains protocoles de tatouage se protègent en vérifiant, avant de distribuer une clef, que l'image originale proposée n'est pas tatouée. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection. Les pirates commencent par contourner l'interdiction au surtatouage : une image est dégradée jusqu'à ce que l'on puisse la sur tatouer (la première signature n'étant plus lisible). On ajoute à l'image originale l'image ainsi surtatouée (en diminuant son amplitude pour que les dégradations n'apparaissent plus). L'image résultante porte alors les deux tatouages, mais le détecteur n'en lit qu'un, le nouveau : le pirate s'est donc approprié l'image.

La figure 3.11 (a) montre l'image "Lena" après cinq opérations de tatouage successives. Il est clair que des dégradations importantes se produisent éventuellement sur l'image tant que le processus de tatouage est répété. La figure 3.11 (b) représente la réponse du détecteur à 1000 signatures générées aléatoirement, dont les cinq signatures présentes dans l'image sont incluses. Cinq pics clairement indiquent la présence des cinq signatures et démontrent que le tatouage successif n'interfère pas avec notre processus.



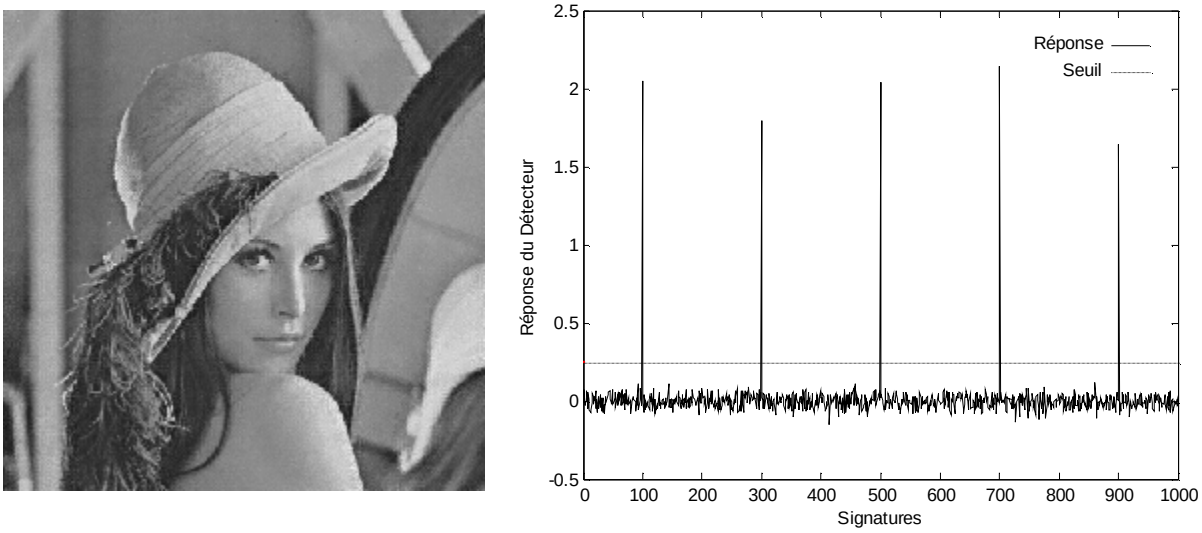
(a) **(b)**

Figure 3.11 Réponses du détecteur à 1000 signatures générées aléatoirement (incluant les cinq signatures spécifiques) après un surmarquage de l'image" Lena".

6.5. Attaque par collusion :

L'attaque dite de collusion a lieu lorsque plusieurs utilisateurs sont en possession de la même image portant différentes signature. La mise en commun de ces images permet de nombreuses opérations : moyenne, recherche de propriétés statistiques communes dans différents domaines, recherche d'informations sur la localisation de la signature. Décrivons une attaque par moyenne : l'image résultante de la moyenne des images tatouées en circulation aura la même qualité que ces dernières. Elle contiendra toutes les signatures, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les signatures.

Dans une expérience similaire à la précédente, on prend cinq images tatouées séparément et on les moyenne pour former la figure 3.12 (a) afin de simuler l'attaque par collusion. La figure 3.12 (b) représente la réponse du détecteur à 1000 signatures générées aléatoirement, dont les cinq signatures présentes dans l'image sont incluses. De nouveau, Cinq pics indiquent clairement la présence des cinq signatures et montrent qu'une simple attaque par collusion basée sur le moyennage de quelques images est inefficace.



(a) **(b)**

Figure 3.12 Réponses du détecteur à 1000 signatures générées aléatoirement (incluant les cinq signatures spécifiques) après collusion de l'image" Lena".

6.6. Robustesse aux transformations géométriques

La méthode proposée est donc robuste aux attaques de type traitement d'images. Ce résultat n'est pas suffisant puisque les attaques géométriques, comme les translations et les rotations sont beaucoup plus néfastes. Le processus de tatouage par ondelettes est particulièrement sensible aux transformations géométriques. En effet, du fait des décimations successives de l'image, la décomposition en ondelettes n'est pas invariante à la translation. C'est pourquoi, le tatouage proposé n'est pas robuste aux transformations géométriques.

Une des solutions pour parer une attaque géométrique est d'effectuer la transformation inverse pour resynchroniser l'image. Comme nous l'avons proposé dans le chapitre précédent, un algorithme de recalage issu d'une technique d'estimation différentielle de mouvement est utilisé pour faire face à ce problème. La transformation est d'abord formulée comme étant purement affine. Ensuite, une contrainte de lissage est imposée à tous les paramètres géométriques localement estimés ; la transformation affine *A* qui nous permet de modéliser les diverses transformations géométriques entre l'image originale et l'image tatouée est définie par les six paramètres à estimer: $m_1, m_2, m_3, m_4, m_5, m_6$.

Sous forme matricielle: $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} m_5 \\ m_6 \end{bmatrix}$. La transformation linéaire représentée par la matrice $\begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$ peut décrire des changements d'échelle, des rotations, et des "cisaillements". Le vecteur $\begin{bmatrix} m_5 \\ m_6 \end{bmatrix}$ correspond aux translations.

Pour notre algorithme de recalage, une pyramide à quatre niveaux est construite pour les deux images (originale et tatouée après transformation géométrique). Chaque niveau de la pyramide est obtenu en convoluant le niveau précédent à l'aide du filtre passe-bas séparable [0.05 0.25 0.4 0.25 0.05], suivi d'une réduction d'un facteur de deux. Le niveau le plus fin comprend l'image originale. A chaque niveau de la pyramide une seule transformation globale affine est d'abord estimée comme dans la section 4.2.2 (a) du chapitre précédent, avec Ω, la fenêtre spatiale d'intégration, définie pour être l'image entière. Le paramètre local affine $\vec{m}$ est d'abord estimé, avec $\Omega = 5 \times 5$. Cet estimé de $\vec{m}$

est employé pour amorcer les itérations de lissage, équation (2.41). Dans chaque itération, $l_i = 10^{11}$, i=1…6, et $\overline{m}_i$ est calculé par convolution avec le noyau 3×3: [1 4 1 ; 4 0 4 ; 1 4 1] /20 [21]. Après quarante itérations (boucle intérieure, itérations de lissage), la source est déformée suivant l'estimée finale. Ce processus est répété cinq fois (boucle externe, itérations de séries de Taylor). L'estimée finale est employée comme première estimée au prochain niveau plus fin selon cette estimée. Ce processus est répété à chaque niveau de la pyramide. Afin de réduire au minimum l'effet de bords (du à l'interpolation), nous accumulons les cartes géométriques successivement estimées et nous appliquons une seule carte géométrique à l'image tatouée à chaque niveau. La plupart des paramètres décrits ci-dessus ont été empiriquement choisis mais généralement conformes aux paramètres utilisés dans la littérature d'estimation de mouvement.

Les dérivées spatiotemporelles sont estimées comme suit. Les images sont premièrement pré-filtrées dans le temps (en employant le filtre [0.5 0.5]). La dérivée par rapport à *x* est ensuite estimée en pré-filtrant d'abord le résultat par rapport à *y* (à l'aide du pré-filtre [0.223755 0.552490 0.223755]), suivie d'une différentiation par rapport à x (à l'aide du filtre [-0.453014 0.0 0.0453014]). De même, la dérivée par rapport à y est estimée en pré-filtrant d'abord le résultat par rapport à x (à l'aide du pré-filtre [0.223755 0.552490 0.223755]), suivie d'une différentiation par rapport à y (à l'aide du filtre [-0.453014 0.0 0.453014]). La dérivée par rapport au temps est estimée en pré-filtrant d'abord dans l'espace (par rapport à x et y) à l'aide du pré-filtre ([0.223755 0.552490 0.223755]), suivie de l'application du filtre [0.5 -0.5] au résultat dans le temps.

Afin de visualiser la carte de recalage estimée, la technique du *flot optique* est utilisée. Cette approche représente la carte de recalage à un sous-ensemble de points discrets avec un vecteur de translation. Le vecteur à chaque endroit du pixel source décrit l'amplitude et la direction à l'endroit du pixel cible correspondant.

6.6.1. Robustesse au Fenêtrage (Cropping)

Le fenêtrage d'images (c.-à-d. la sélection d'une portion de l'image) mérite une discussion séparée, puisque c'est un traitement très courant (c'est l'une des opérations les plus populaires, habituellement non malveillante, qui peut être appliquée à une image) et parce qu'il présente quelques particularités qui le rendent différent des autres déformations géométriques. Nous avons donc éprouvé notre schéma face à ce traitement.

Nos expériences sur le fenêtrage sont principalement destinées à l'évaluation de la robustesse du tatouage suite à la perte d'information due à l'enlèvement d'une partie de l'image, La figure 3.13 représente les résultats obtenus après ce traitement lorsque l'on choisit de conserver (80% à10%) de la taille de l'image tatouée (l'opération de fenêtrage est effectuée de manière automatique en conservant une portion centrale de l'image). 1000 signatures différentes (parmi elle notre signature incorporée) sont examinées pour la détection. Sur le même graphe, nous avons représenté la deuxième réponse la plus élevée du détecteur (c.-à-d., la réponse la plus élevée parmi celles produites par le détecteur lorsque les 999 fausses signatures sont examinées). La réponse du détecteur demeure au-dessus du seuil de détection jusqu'à ce qu'un fenêtrage de 10% soit atteint, La deuxième réponse la plus élevée du détecteur reste toujours au-dessous du seuil.

La figure 3.14 montre l'effet d'un fenêtrage de 40% sur l'image "Lena". Bien qu'une grande portion de l'image ait été supprimée, nous obtenons de bons résultats.

Les résultats que nous avons obtenus sont tout à fait impressionnants, puisqu'ils démontrent la robustesse de notre algorithme proposé face au fenêtrage. Une explication possible de ces résultats est que, notre détecteur est basé sur la corrélation entre la signature et les coefficients de la TOD hôtes. Ainsi que la signature est étalée sur toute l'image, et que n'importe quelle partie de l'image contient assez de détails pour permettre une détection réussie.

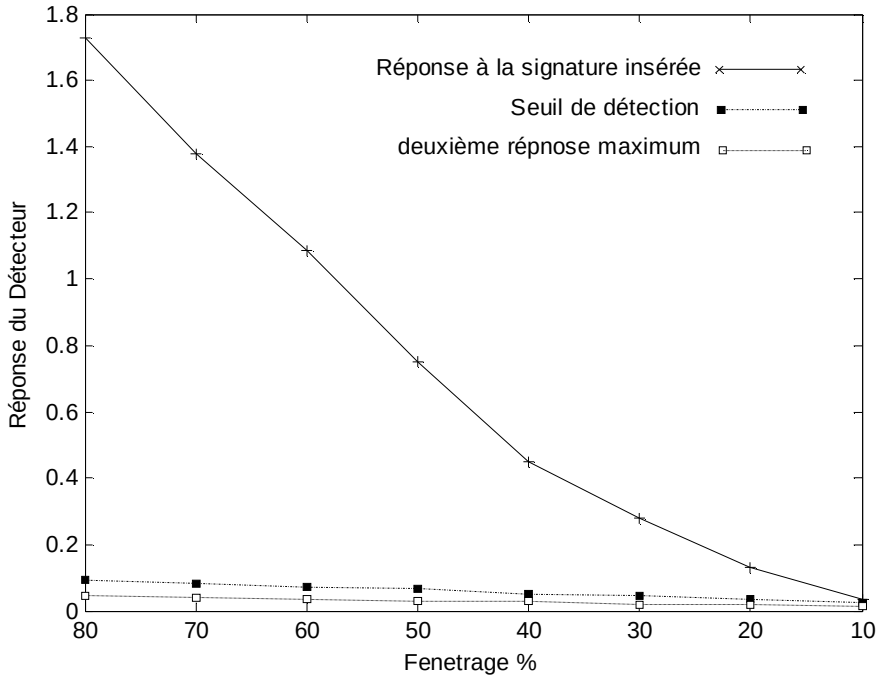
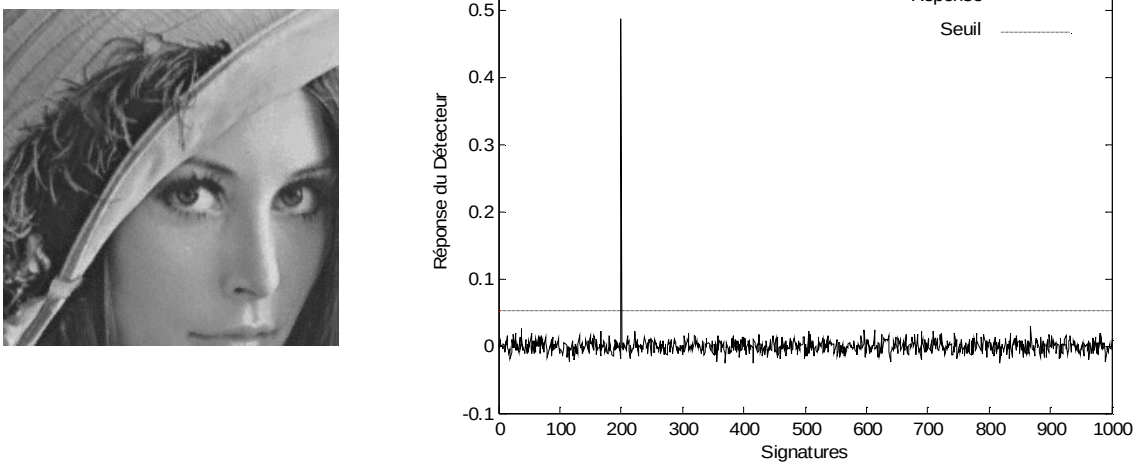


Figure 3.13 Réponse du détecteur après fenêtrage.



(a) **(b)**

Figure 3.14 Réponse du détecteur à 1000 signatures générées aléatoirement après fenêtrage de 40% de la taille de l'image" Lena" tatouée,
notre signature apparaît en position 200.

6.6.2. Robustesse aux rotations

Nous avons évalué la robustesse de notre schéma face à des rotations de 6 angles différents. Le tableau 3.3 montre la réponse du détecteur r après recalage de l'image pour chacun des angles de rotation.

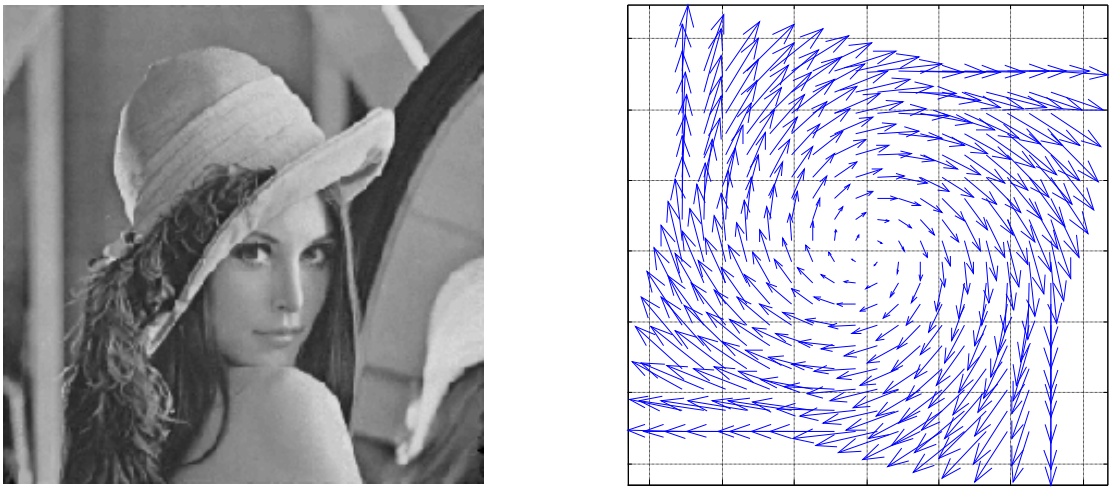
Angles	Réponse r	Seuil T_r	MSE avant recalage	MSE après recalage	Décision
5^0	0.0039	0.0009	0.1750	0.0410	OK
10^0	0.0037	0.0010	0.2210	0.0452	OK
20^0	0.0035	0.0009	0.2666	0.0516	OK
45^0	0.0032	0.0009	0.3075	0.0885	OK
60^0	0.0005	0.0009	0.3107	0.2360	Echec
90^0	-0.0001	0.0012	0.2890	0.2677	Echec

Tableau 3.3 Robustesse de notre schéma face à des rotations de $5^0, 10^0, 20^0, 45^0, 60^0$ et 90^0.

Sur la figure 3.15 nous avons représenté l'image Lena originale et l'image Lena tatouée après l'application d'une rotation de 20^0. La figure 3.16 montre l'image résultante après recalage et le flot optique de la carte de recalage estimée.

(a) **(b)**

Figure 3.15 Image Lena tatouée avant (a) et après (b) une rotation de 20^0.



(a) **(b)**

Figure 3.16 Image Lena tatouée après recalage (a), et le flot otique de la carte de recalage estimée correspondant (b).

Les résultats du tableau 3.3 montre que notre schéma de tatouage est robuste pour des rotations de faibles angles (de 0^0 à 45^0), les rotations d'un angles supérieur à 45^0 rendent la détection de la signature impossible. Ce problème est du en grande partie aux limitations inhérentes aux filtres de dérivation et de l'approximation des séries de Taylor de notre système de recalage. Cette approche est fondamentalement limitée par l'importance de l'angle de rotation, et les distorsions provoquées ne peuvent pas toujours être identifiées et révélées même en employant la stratégie de la pyramide.

6.6.3. Robustesse aux changements d'échelle

Nous avons testé notre schéma lorsque l'image Lena subit un changement d'échelle. Le tableau 3.4 donne le comportement du détecteur après une homothétie de facteur 0.75, 0.6 puis de 0.50.

homothétie de facteur	Réponse r	Seuil T_r	MSE avant recalage	MSE après recalage	Décision
0.75	0.0019	0.0005	0.2968	0.0317	OK
0.60	0.0007	0.0004	0.3871	0.0386	OK
0.50	0.0002	0.0003	0.4089	0.0420	Echec

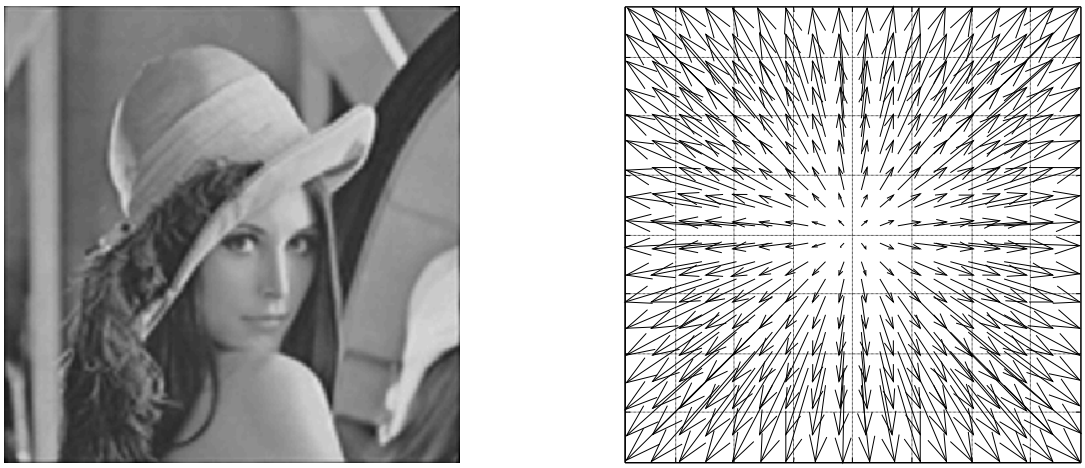
Tableau 3.4 Robustesse du schéma après des homothéties de facteur 0.75, 0.60 et 0.50.

Sur la figure 3.17 nous avons représenté l'image Lena originale et l'image Lena tatouée lorsque elle subit une homothétie d'un facteur de 0.5. La figure 3.18 montre l'image résultante après recalage et le flot optique de la carte de recalage estimée correspondante.

Il est clair que les détails les plus fins ont été perdus dans le processus de changement d'échelle. Cela doit être prévu puisque le re-dimensionnement d'une image exige une opération de filtrage spatiale passe-bas.

Avec les résultats obtenus, on peut remarquer que notre schéma est robuste pour des changements d'échelles ≥ 0.6. Lorsque le facteur d'homothétie devient important (<0.6), la détection de la signature est plus incertaine.

Figure 3.17 Image Lena tatouée avant et après une homothétie de facteur 0.7.



(a) **(b)**

Figure 3.18 L'image Lena tatouée attaquée après recalage (a), et le flot otique de la carte de recalage estimée correspondant (b).

6.6.4. Robustesse à la translation

Nous avons également évalué la robustesse de notre schéma face aux translations diagonales de 5, 10, 20 pixels (*dx*=*dy*= 5, 10, 20). Le tableau 3.5 montre la réponse du détecteur r après recalage de l'image Lena tatouée translatée. Sur la figure 3.19 nous avons représenté l'image Lena originale et sa version tatouée lorsque elle subi une translation de 10 pixels. La figure 3.20 montre l'image résultante après recalage et le flot optique de la carte de recalage estimée correspondant.

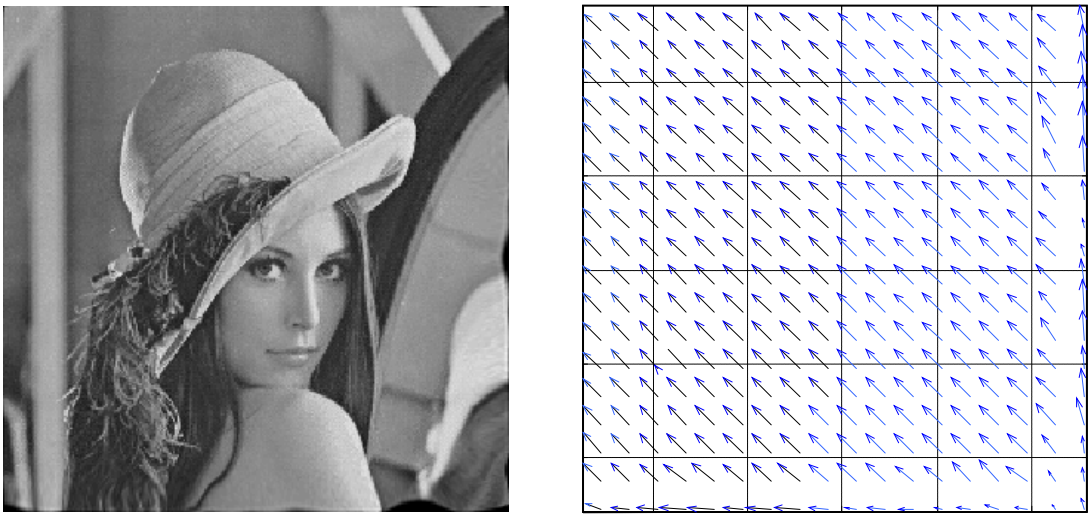
Avec les résultats obtenus (tableau 3.5), on peut remarquer que notre schéma est robuste à la translation.

Translation (Pixels)	Réponse r	Seuil T_r	MSE avant recalage	MSE après recalage	Décision
5	0.0108	0.0010	0.1628	0.0288	OK
10	0.0102	0.0010	0.2117	0.0408	OK
20	0.0089	0.0009	0.2637	0.0541	OK
30	0.0072	0.0008	0.2864	0.0623	OK

Tableau 3.5 Robustesse du schéma après translation.

(a) **(b)**

Figure 3.19 Image Lena tatouée avant (a) et après (b) une translation de 10 pixels.



(a) **(b)**

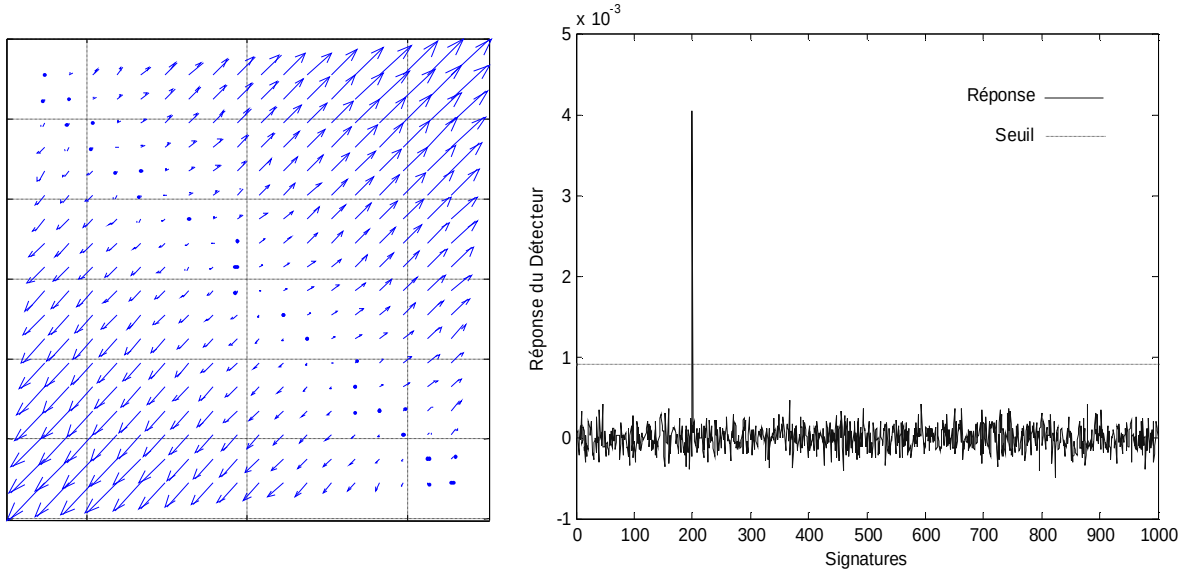
Figure 3.20 L'image Lena tatouée attaquée après recalage (a), et la carte de recalage estimée correspondant (b).

6.6.5. Robustesse au cisaillement

Nous avons testé notre schéma lorsque l'image "Lena" subi un cisaillement. La figure 3.21 donne le comportement du détecteur après un cisaillement 10% suivant X et Y.

(a) **(b)**

Figure 3.21 Image Lena tatouée après une cisaillement de 10 % (a) et ça version après recalage (b).



(a) **(b)**

Figure 3.22 Le flot optique de la carte de recalage estimée (a), et la réponse du détecteur correspondante (b).

Avec les résultats obtenus sur la figure 3.22, on peut remarquer que notre schéma est robuste au cisaillement.

7. Conclusion

Nous avons présenté dans ce chapitre les résultats obtenus pour la méthode de tatouage que nous proposons, ces résultats montrent que la méthode développée est particulièrement robuste aux dégradations de type traitement d'image (compression JPEG, filtrages et ajout du bruit). Ces résultats sont obtenus grâce à l'analogie présentée par la transformée en ondelettes et le modèle psychovisuel utilisé, qui prend en compte la sensibilité de l'oeil humain au bruit pour augmenter et adapter la force de la signature selon les caractéristiques locales de l'image. La qualité des images tatouées est obtenue à partir d'un critère subjectif. Cette méthode est très proche de celles utilisées en tatouage psychovisuel puisque elle est basée sur les mêmes modélisations du Système Visuel Humain.

Cependant, du fait des décimations successives, la décomposition pyramidale de l'image est non-invariante à la translation et la rotation, et l'algorithme souffre de n'être pas robuste aux transformations géométriques asynchrones. Pour remédier à ce problème, nous

avons montré que l'utilisation de algorithme de recalage développé au chapitre précédent peut compenser une large gamme de transformations géométriques affines.

Notre étude nous a permis de souligner que les limites de cette méthode sont atteintes lorsque la transformation géométrique appliquée est trop importante.

Liste de figures