République Algérienne démocratique et po
Ministère de L'enseignement Supérie
Et de la Recherche Scientifique

جامعة جيجل
مكتبة كلية العلوم والتكنولوجيا
رقم الجرد : 01691

Université de Jijel
Faculté des Sciences et Technologie
Département d'Electronique

Mémoire de fin d'étude

En vue de l'Obtention du Diplôme de Master
En Électronique
Spécialité : Analyse des Systèmes

Thème

Dissimulation des Images dans la Transformée en Ondelettes

Présenté par :

Mr : Frites Abdelhakim

Encadré par :

Mr : Taleb Ahcène

Promotion Juin 2014

Remerciements

Je voudrais remercier tout d'abord, **Allah**, pour être mon meilleur confident et pour me permettre de réaliser mes rêves.

La rédaction de ce mémoire est l'occasion pour moi de faire un bilan des deux années passées depuis l'obtention de la licence. Ces années ont été riches de rencontres et je mesure aujourd'hui la chance que j'ai eu d'étudié avec des personnes qui m'ont beaucoup appris tout en partageant avec eux de très bons moments.

Je tiens vivement à remercier mon directeur de recherche Mr : **Taleb Ahcène**, qui a supervisé ce travail de recherche. Son soutien, sa disponibilité, sa patience, sa compréhension, ainsi que ses conseils judicieux tant lors de mes recherches que lors de l'écriture de ce mémoire... Je lui dois beaucoup.

Je remercie l'ensemble des membres du **jury** qui m'ont fait l'honneur d'accepter de lire et de juger ce mémoire.

Mes remerciements sont adressés également au chef du département d'électronique Mr : **R. REMMOUCHE.**

Je ne saurais terminer sans remercier l'ensemble des collègues et amis qui m'ont aidé et supporté durant ces dernières années. Un grand merci à vous tous.

À mes proches d'ici et d'ailleurs.

Dédicaces

Je dédie ce travail :

A mes parents

A mes frères et mes sœurs

A mes amies

A mes collègues

Et

A toute la famille 'frites'

ABDELHAKIM

TABLE DES MATIÈRES

Remerciements i
Dédicaces ii
Liste des figures vi
Liste des tableaux viii
Introduction générale 1

Chapitre I :

Techniques de dissimulation De l'information : Généralités

I.1 Introduction 3
I.2 Techniques de dissimulation de l'information 3
I.2.1 Cryptographie 4
I.2.1.1 Principe de la cryptographie 4
I.2.1.2 Domaine de l'utilisation de la Cryptographie 5
I.2.2 La stéganographie 6
I.2.2.1 Qu'est que la stéganographie ? 6
I.2.2.2 Peut-on détecter ou empêcher l'usage de la stéganographie ? 7
I.2.2.3 Classification des schémas de stéganographie 7
I.2.2.4 Exemple de dissimilation d'images numériques [13] 8
I.2.3 Le Tatouage 9
I.2.3.1 Principe du tatouage 9
I.2.3.2 Contraintes du tatouage 10
I.2.3.3 Les applications du tatouage 10
I.2.3.4 Robustesse 12
I.2.3.5 Résistance aux attaques 13
I.2.3.6 protocoles de protection d'images numériques 13
I.3 Conclusion 14

Chapitre II :

Stéganographie et domaines d'insertions

II.1 Introduction 15

II. 2 La stéganographie 15

II. 2.1 La stéganographie informatique : principes et fondements théoriques 15

II .2.2 Schémas de stéganographie 17

II .2.3 Types de stéganographie 19

II.2.3.1 La stéganographie linguistique 19

II.2.3.2 La stéganographie technique 19

II.3 Objectifs de la stéganographie 21

II.4 Quelques applications classiques de la stéganographie 22

II.4.1 Une image peut en cacher une autre 22

II.4.2 Dissimuler un message dans un texte 23

II .5 Domaine d'insertion dans les images numérique 25

II .5.1 La stéganographie dans le domaine spatial 25

II .5.2 La stéganographie dans le domaine fréquentiel 26

II.5.3 La stéganographie dans le domaine multirésolution (ondelettes) 27

II .6 Les différentes classes de méthodes de stéganographie 29

II .6.1 Méthodes additives 30

II.6.2 Méthodes substitutives 31

II .7 Comparaison entre les méthodes substitutives et additives 32

II.8 conclusion 33

Chapitre III :

Ondelettes et stéganographie

III.1 Introduction 34

III.2 Histoire de la décomposition en ondelettes 34

III.3 Définition mathématique 34

III.4 Transformée en ondelettes 35

III.4.1 Transformée en ondelettes continue 36
III.4.2 Transformée en ondelettes discrète 36
III.4.3 L'Analyse multirésolution (AMR) 37
III.4.4 Généralisation aux images 38
III.5 Choix du domaine transformé 39
III.5.1 Introduction sur la transformation de Haar 39
III.5.1.1 La transformée 1D de Haar 39
III.5.1.2 La transformée 2D de Haar à 2 niveau 40
III .6 Stéganographie basée sur les ondelettes 41
III .7 Les attaquants actifs et stéganographie robuste 41
III .8 Conclusion 42

Chapitre IV :

Résultats et discussion

IV.1 Introduction 43
IV.2 Propriétés et avantages de la décomposition en ondelettes 43
IV.3 La méthode proposée 44
IV.3.1 Description de l'algorithme 44
IV.4 Moyens d'évaluation 47
IV.4.1 Le MSE (Mean Square Error) 47
IV.5 Outils d'évaluation 48
IV.4.2 Le PSNR (Peak Signal to Noise Ratio) 48
IV.6 Résultats de simulation 48
IV.6.1 Insertion additive 49
IV.6.2 Insertion substitutive 53
IV.6.3 Simulation d'attaques 55
IV.7 Conclusion 58
Conclusion générale 59
Bibliographie 60

LISTE DES FIGURES

Figure. I.1Chiffrement symétrique 4
Figure. I.2 Chiffrement asymétrique. 5
Figure I.3. Insertion et détection aveugle pour le tatouage d'image. 10
Figure I.4. Dans le cas de la protection des droits d'auteurs, la robustesse est capitale. Cette priorité est moindre pour l'authentification ou l'indexation. 13
Figure I.5 Application du tatouage pour le transfert d'images numériques sur internet 14
Figure I.1 Triangle représente caractéristiques d'un marquage. 17
Figure II.2 Problème classique de communication secrète. 18
Figure II.3 : La dégradation de l'image passe alors inaperçue et seul le logiciel adéquat permet de retrouver les données cachées [23]. 23
Figure.II.4 A gauche, image originale. A droite, image contenant un PDF de32Kb [28] 25
Figure II.5 (a) Décomposition à trois niveaux de l'image de Lena. (b) Décomposition spectrale. 28
Figure II.6 Transformée en Ondelette. 29
Figure II.7 Schéma d'une méthode additive. 31
Figure II.8 Principe de l'insertion par substitution. 32
Figure II.9 Détection et lecture de la signature par substitution. 32
Figure III.1 Décomposition pyramidale en première niveau de l'image Doaa_. 38
Figure IV.1. Schéma représentant la phase d'insertion d'image secrète. 45
Figure IV.2. Schéma représentant la phase de détection d'image secrète. 47
Figure IV.3 'Nature.bmp' (680x460) 48
Figure IV.4 'Doaa.JPG' (640x480) 48
Figure IV.5 'Logo-univ-Jijel.JPG'(191x180) 48
figure IV.6 'Avion sans pilote.JPG'(300x200) 48
Figure IV.7 'Logo-univ-Jijel.JPG' (680x460) 49
Figure IV.8 Processus d'insertion et différence entre image originale et stégo-image (PSNR égal à 44.89dB). 50
Figure IV.9 Processus d'insertion et différence entre image originale et stégo-image 51
(PSNR égal à 51.04 dB). 51
Figure IV.10 Schéma représentant la phase de détection de l'image secrète. 52

LISTE DES TABLEAUX

Tableau II.1 Comparaison entre les schémas additifs et les schémas substitutifs.....33
Tableau IV.1 Mesure objective de distorsion introduite par la compression JPEG. 56
Tableau IV.2 l'influence de bruit gaussien au stégo-image.....57

Introduction générale

Introduction générale

L'information est l'oxygène des temps modernes, Le développement rapide des ordinateurs et les technologies du réseau a conduit à une nouvelle ère de multimédia numérique. C'est particulièrement vrai dans le monde des affaires où, statistiquement, 80 % des actifs d'une entreprise prendraient désormais la forme de données informatiques [1]. Néanmoins, les entreprises le savent mieux que quiconque, cette inflation informationnelle s'accompagne d'un essor exponentiel de défis en matière de responsabilité : c'est là le revers de la médaille [2].

À la lumière de ce constat, donner une protection adéquate à l'information devient un enjeu primordial pour tous les acteurs économiques (entreprises, gouvernements, mais aussi les utilisateurs/consommateurs) et, bien entendu, pour les concepteurs de systèmes d'information. Avec toutes les nuances que suscite une telle affirmation, on peut dire que la protection de l'information se décline en deux axes principaux [3] : d'une part, la sûreté de l'information, qui consiste à protéger les données contre les perturbations ne provenant pas d'actes de malveillance (dégradations, pannes, etc.), d'autre part, la sécurité de l'information, qui consiste à protéger les données contre les actes de malveillance et qui peut se définir comme étant la « protection des ressources informationnelles d'une organisation face à des risques définis, qui résulte d'un ensemble de mesures de sécurité prises pour assurer la confidentialité, l'intégrité et la disponibilité de l'information traitée [4] ».

Pour assurer la sécurité d'une information, une possibilité est de la rendre « secrète », c'est-à-dire difficilement accessible ou inintelligible (par des moyens matériels, des mesures administratives ou techniques [5]), sauf pour la personne à laquelle elle est destinée : c'est là le domaine de la cryptographie. Mais Leonard de Vinci, qui s'y connaissait en matière de dissimulation, nous expliquerait volontiers que le meilleur moyen de protéger une information, c'est de la dissimuler, en faisant en sorte que personne – mis à part le destinataire – n'ait l'idée même de la chercher, n'imaginant pas qu'il peut y avoir, à un endroit donné, un « trésor » intéressant. On est là dans le domaine de la stéganographie, qui consiste à dissimuler (recouvrir) une information pour la faire passer inaperçue [6].

L'objet de ce projet de master est l'étude de dissimulation de données, appliquée aux images numériques. Une importance particulière a été attribuée à la dissimulation dans le domaine des ondelettes parce que c'est une technique relativement nouvelle et prometteuse.

Ce mémoire comporte quatre chapitres :

Le premier chapitre de ce mémoire sera consacré à l'introduction des notions de base sur les techniques de dissimulation d'information.

Le deuxième chapitre parlera de la stéganographie et les différents domaines d'insertions. Nous avons fait la distinction entre les deux schémas d'insertion : les schémas additifs et les schémas substitutifs.

Le troisième chapitre sera consacré à la transformée en ondelettes et son application à la dissimulation de l'information. Comme la transformée en ondelettes possède des propriétés inhérentes qui font d'elle un espace d'insertion attrayant, il a été choisi pour la partie expérimentale (chapitre 4).

Dans le quatrième chapitre, est présentée la partie expérimentale en l'occurrence l'implémentation d'algorithmes de dissimulation dans le domaine de la transformée en ondelettes, les résultats, et la discussion.

Enfin, on terminera par une conclusion générale, qui résume nos résultats ainsi que des perspectives pour d'autres travaux à venir.

Chapitre 1

Techniques de dissimulation de l'information : Généralités

I.1 Introduction

Les techniques de dissimulation de données (data hiding) permettent de transmettre des informations supplémentaires au travers de données hôtes. L'hôte actuellement à essentiellement muté vers le format numérique. La transmission, la manipulation et le stockage de documents numériques (texte, séquence audio ou vidéo) sont devenus une pratique quotidienne. L'évolution rapide de ces technologies numériques a suscité le développement de techniques fiables pour la protection des produits multimédias contre le piratage et la falsification.

Au cours de ce premier chapitre, nous allons donner un aperçu sur différentes techniques de dissimulation de données.

I.2 Techniques de dissimulation de l'information

Comme dis l'ancien dicton celui qui détient l'information détient le pouvoir. Le terme *information* n'est pas forcément d'une notion rigoureuse, mais plutôt un renseignement ou données qu'une personne ne souhaite pas divulguer.
Deux grandes tendances visent à protéger l'information :

- **Le chiffrement** dont l'objectif est de rendre l'information incompréhensible a une personne ne possédant pas une clef secrète : une personne surveillant le canal de communication par lequel transite le message sait qu'un échange a lieu, mais est ainsi incapable d'en interpréter le contenu.
- **La stéganographie** qui cherche plutôt à dissimuler la présence même d'informations pertinentes (secrètes) au sein d'un support (texte, audio, image, ou vidéo). Le support est choisi de caractère anodin, sans réel intérêt pour le destinataire et ne doit pas attirer des soupçons. Le message secret est caché de manière à passer inaperçu lors de la communication [7].

La cryptographie, la stéganographie et le tatouage sont des techniques destinées à insérer une information à caractère confidentiel lors de la transmission. Elles répondent toutes les trois à des problèmes de sécurité.

La cryptographie et la stéganographie ont été utilisées depuis longtemps à des fins militaire. Elles font partie les sciences du secret. Le tatouage de documents est un domaine beaucoup plus récent qui s'apparente à la stéganographie.

I.2.1 Cryptographie

I.2.1.1 Principe de la cryptographie

La cryptographie consiste à transformer un message pour qu'il devienne illisible ou indéchiffrable. Seule la connaissance d'une clef et du moyen de cryptage peut permettre de décoder le message afin de le rendre lisible. Cette technique permet de protéger le document pendant sa transmission. Mais, une fois le document décrypté, il ne présente plus aucune protection. Un des premiers procédés utilisés est celui par substitution, le message est crypté en substituant chaque lettre par une autre d'un alphabet décalé. La clef représentait le nombre de lettres de décalage [8].

Chiffrement symétrique

Le chiffrement symétrique consiste en l'échange d'une clef secrète entre les deux parties en communication (Alice et Bob). Lorsqu'Alice souhaite envoyer un message secret à Bob, elle crypte son message avec la clef secrète, et elle envoie le message à Bob. Une fois que ce dernier a reçu le message, il ne lui reste qu'à décoder le message grâce à cette même clef secrète.

Si, lors de la phase d'échange de messages, Eve en intercepte un, elle ne pourra le décoder sans l'aide de la clef secrète.

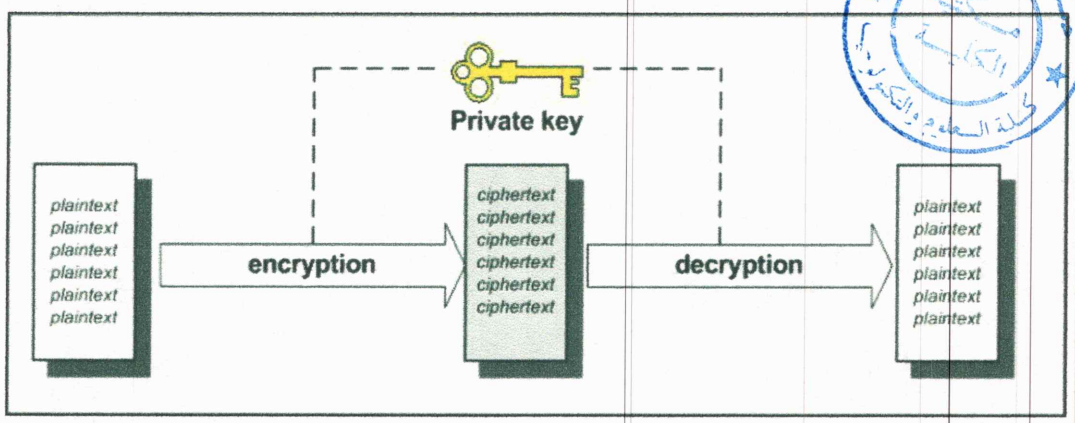


Figure. I.1 Chiffrement symétrique

Evidemment, le handicap majeur de cette méthode est que la clef secrète doit le rester ! Le problème se situe donc dans l'échange de cette clef entre Alice et Bob. Pour pallier à ce problème, d'autres procédés sont employés pour l'échange de clef secrète, c'est notamment l'utilisation qui est faite de la cryptographie à clef publique, et du chiffrement asymétrique.

Chiffrement asymétrique

Le chiffrement asymétrique repose quant à lui sur un système à double clef : une clef publique et une clef privée. Chacune des deux parties (Alice et Bob) possède donc une paire de clefs, une publique qu'elle publie, et une secrète qu'elle conserve précieusement. Ces deux clefs peuvent servir à coder comme à décoder. Dans notre cas, le message est crypté à l'aide de la clef publique et décodé à l'aide de la clef privée.

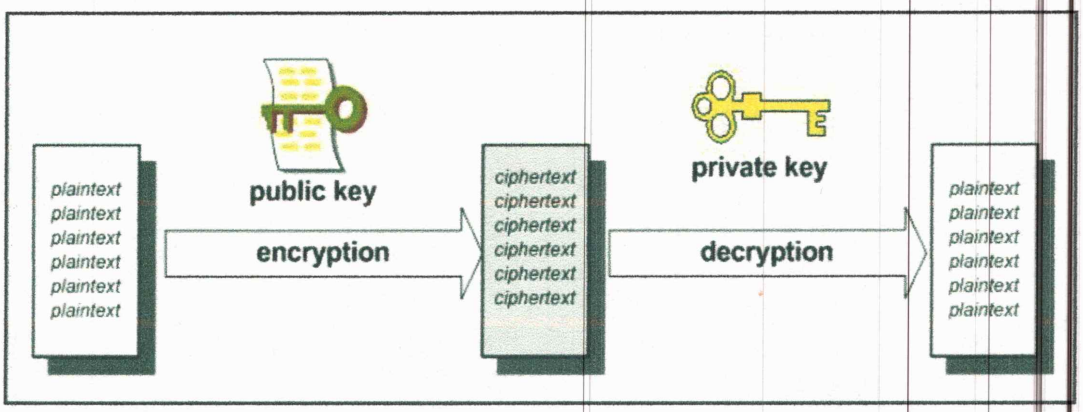


Figure. I.2 Chiffrement asymétrique.

L'algorithme de chiffrement asymétrique le plus fréquemment utilisé de nos jours est le RSA (Rivest – Shamir – Adelman), inventé en 1978. Cet algorithme est également utilisé pour la signature numérique mais nous ne développerons pas cet aspect.

I.2.1.2 Domaine de l'utilisation de la Cryptographie

De nos jours la cryptographie est une science étroitement liée aux systèmes de communication. Elle permet de multiples applications [9] :

1. Garantir l'intégrité des données une fonction de hachage peut être associée au document, elle assure qu'il est inchangé.
2. Assurer la confidentialité de données : seules des entités autorisées peuvent accéder aux données.
3. Permettre l'authentification des entités en communication : seules des entités autorisées peuvent accéder aux données.
4. Veiller à la non-répudiation de l'origine : l'information qui a été émise par une source ne peut être réfutée.

Le chiffrement de messages consiste à transformer une information à l'aide d'une convention secrète. La fonction de transformation constitue l'algorithme

cryptographique dont le secret réside dans des paramètres appelés clés. Lorsque l'on déchiffre le message, en connaissant ses clés on réalise l'opération inverse.

I.2.2 La stéganographie

I.2.2.1 Qu'est que la stéganographie ?

Le mot stéganographie vient du grec 'steganos' (caché ou secret) et 'graphy' (écriture ou dessin) et littéralement signifie : *écriture cachée.*

Durant l'ère médiévale, des pochoirs étaient superposés sur les messages pour pouvoir révéler les différents mots formant le message caché. En 1586, la police secrète de la couronne britannique a identifié des lettres qui contenaient un message dissimulé décrivant un complot contre la reine Elizabeth d'Angleterre. Le complot a pu être arrêté lorsque la police a inséré à l'une des lettres un message demandant les qualités des six personnes qui devaient accomplir le crime. A cette époque, certains postiers anglais avaient pour tâche d'enlever les formules de politesse des lettres ou encore de reformuler les télégrammes afin de détruire d'éventuels messages cachés. Durant la seconde guerre mondiale, la stéganographie était majoritairement représentée par l'utilisation d'encre invisible [10]. La stéganographie moderne utilise aussi comme réceptacle des documents numériques comme le texte, les images ou encore le son ou la vidéo.

La stéganographie étudie les techniques pour communiquer de l'information de façon cachée. L'adjectif caché ne signifie pas ici que l'information est visible mais codée, il s'agit alors de cryptographie. Ici, il signifie que la présence de l'information n'est pas perceptible parce que enfouie dans une autre information.

Pour résumer le problème de façon plus académique, utilisons une présentation proche de celle utilisée en cryptographie. Alice et Bop ont été arrêtés et emprisonnés. Ils désirent se communiquer des informations afin d'organiser leur défense lors du procès (ou leur évasion). Ils sont autorisés à communiquer quasi librement, avec la restriction que tous les messages seront lus par les responsables de la prison. Ils utiliseront la stéganographie pour communiquer leur plan.

Pour pouvoir communiquer de façon secrète, il faut d'abord pouvoir communiquer tout simplement. On attachera à des messages anodins, un message secret. Afin de décoder ce message, le correspondant doit connaitre un secret et/ou la technique pour déchiffrer extraire ce message. Il est évident que ce message caché peut être lui-même codé et/ou signé en utilisant

des méthodes cryptographiques. La stéganographie n'étant plus alors que la dernière étape de votre encodage. Celle-ci pouvant même être destinés à cacher votre usage de la cryptographie [11].

I.2.2.2 Peut-on détecter ou empêcher l'usage de la stéganographie ?

L'observateur qui soupçonne une communication cachée et celui qui veut l'empêcher ne sont ni l'un ni l'autre démuni de possibilités, même s'il est dur de lutter contre une technique inconnue. L'observateur peut comparer les propriétés statistiques de la communication soupçonnée avec celles d'une communication ne contenants pas de messages cachés. De trop grandes différences peuvent être l'indice d'une communication cachée ou n'être qu'une simple anomalie statistique. Une fois découverte, on peut essayer de retrouver le message caché en utilisant des techniques de cryptanalyse, c'est-à-dire les techniques pour casser des codes cryptographiques.

Pour interdire toute communication cachée il faut pouvoir intercepter et transformer ou interdire toutes les communications (car elles peuvent potentiellement servir de transport). Un firewall possède les propriétés appropriées pour ce genre de contrôle absolu des communications. Celui qui veut empêcher une communication cachée doit néanmoins, laisser passer le message clair tout en détruisant le message caché. Il peut aussi tout simplement détruire tout message suspect (voir tout message). Sinon, il est obligé de modifier le message tout en lui conservant son sens ou son aspect original.

Puisque le bruit de fond ou les basses fréquences sont des bonnes cachettes, il faudra y rajouter son propre bruit ou filtrer le bruit existant. Il s'agit donc d'une sorte de dégradation du message. On pourra aussi décoder/décompresser puis coder/compresser le message pour le débarrasser des cachettes utilisant les particularités de certain codage.

Bref, une lutte efficace contre la stéganographie est difficile à mettre en œuvre même s'il existe des pistes intéressantes [12].

I.2.2.3 Classification des schémas de stéganographie

Il est possible de présenter les techniques de stéganographie selon différentes classifications. On distingue alors six catégories :

1. Un système par substitutions : remplace les parties redondances du support par le message.

2. Les techniques par transformations : dissimulent l'information dans une transformée du support comme le domaine des ondelettes (TOD : Transformation Ondelette Discrète, la TCD : Transformation Cousins Discrète ou la TFD : Transformation Fourier Discrète).
3. Les techniques par étalement de spectre.
4. Les méthodes statistiques : modifient plusieurs statistiques du support (fréquences des lettres, distribution des pixels.) Cacher le message et le récupérer se fait en testant ces hypothèses.
5. Les techniques par distorsions : altèrent le support, la différence avec le support initial constituant alors le message.
6. Les méthodes par génération de support autour du message pour le dissimuler.

I.2.2.3 Exemple de dissimilation d'images numériques [13]

Comment cacher numériquement une image "sous" une autre ? Pour simplifier les explications, nous prenons l'exemple des images en niveaux de gris. Supposant que chaque pixel de l'image serait un nombre entre 0 et 1 où le niveau de gris 0 correspond au noir, et le 1 au blanc. Le niveau 0.5 sera un gris moyen, un pixel proche de 0 serait gris foncé, un pixel proche de 1 serait gris clair. L'image sera quant à elle, représentée par une matrice de pixels de *n* lignes et *m* colonnes (*nxm*). Prenons comme exemple une matrice de 3 lignes et 4 colonnes (les pixels de l'image correspondante sont fortement grossis) :

$$M=\begin{pmatrix} 0.2 & 0.5 & 1 & 0 \\ 0 & 0.25 & 0.75 & 0.5 \\ 0.25 & 1 & 0.4 & 0.85 \end{pmatrix}$$

Matrice

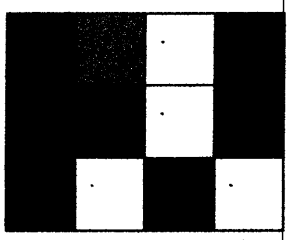


Image correspond

Mathématiquement, on peut décrire le camouflage d'une image "sous" une autre par une ***combinaison linéaire*** des deux matrices nxm correspondantes si les dimensions des deux matrices sont identiques et si A est la matrice de l'image "camouflant" et B la matrice de l'image camouflée, alors on peut calculer la matrice de l'image combinée par :

$$C = A + \left(\frac{1}{K}\right) * B \qquad (1.1)$$

Ou *K* est un nombre bien choisi. L'image B (qui sera peut-être légèrement différente de l'originale B) sera retrouvée par la formule :

$$B' = K(C - A) \qquad (1.2)$$

❖ **Remarque**

Les pixels très proches de 1 dans l'image A peuvent poser problème. En effet, en leur additionnant un certain nombre, ils risquent de dépasser 1.ils seront alors tronqués à 1. Cela a pour conséquence que, une fois l'image C déchiffrée, l'image B' sera légèrement altérée par rapport à B (voir l'exemple numérique ci-dessous).

$$C=\underbrace{\begin{pmatrix} 0.51 & 0.47 & 0.30 & 0.43 \\ 0.12 & 0.95 & 0.41 & 0.47 \\ 0.22 & 0.98 & 0.53 & 0.65 \end{pmatrix}}_{\mathbf{A}} + \frac{1}{10}\underbrace{\begin{pmatrix} 0.21 & 0.34 & 0.21 & 0.21 \\ 0.54 & 0.43 & 0.76 & 0.33 \\ 0.46 & 0.44 & 0.66 & 0.54 \end{pmatrix}}_{\mathbf{B}} = \underbrace{\begin{pmatrix} 0.531 & 0.504 & 0.321 & 0.451 \\ 0.174 & 0.993 & 0.486 & 0.503 \\ 0.266 & 1 & 0.596 & 0.704 \end{pmatrix}}_{\mathbf{C}}$$

$$B' = 10\underbrace{\begin{pmatrix} 0.531 & 0.504 & 0.321 & 0.451 \\ 0.174 & 0.993 & 0.486 & 0.503 \\ 0.266 & 1 & 0.596 & 0.704 \end{pmatrix}}_{\mathbf{C}} - 10\underbrace{\begin{pmatrix} 0.51 & 0.47 & 0.30 & 0.43 \\ 0.12 & 0.95 & 0.41 & 0.47 \\ 0.22 & 0.98 & 0.53 & 0.65 \end{pmatrix}}_{\mathbf{A}} = \underbrace{\begin{pmatrix} 0.21 & 0.34 & 0.21 & 0.21 \\ 0.54 & 0.43 & 0.76 & 0.33 \\ 0.46 & 0.20 & 0.66 & 0.54 \end{pmatrix}}_{\mathbf{B'}}$$

I.2.3 Le Tatouage

I.2.3.1 Principe du tatouage

Le schéma de tatouage d'image se décompose en deux opérations distinctes illustrées sur la figure I.3.

- **La phase d'insertion :** elle consiste à introduire une marque dans l'image en vue d'identifier son propriétaire (le nom de l'auteur ou de l'entreprise par exemple). Cette insertion peut se faire dans le domaine spatial ou dans le domaine transformé (transformé de Fourier, en cosinus discrète, en ondelette, etc.)

- **La phase de détection :** elle permet de retrouver la marque ou la signature insérée. Cette étape est souvent effectuée en aveugle, c'est-à-dire pas besoin de voir ou de savoir l'image originale pour pouvoir détecter la marque (utiliser l'image originale pour la détection donnerait un schéma plus lourd et pourrait poser des problèmes licites ou illicites.)

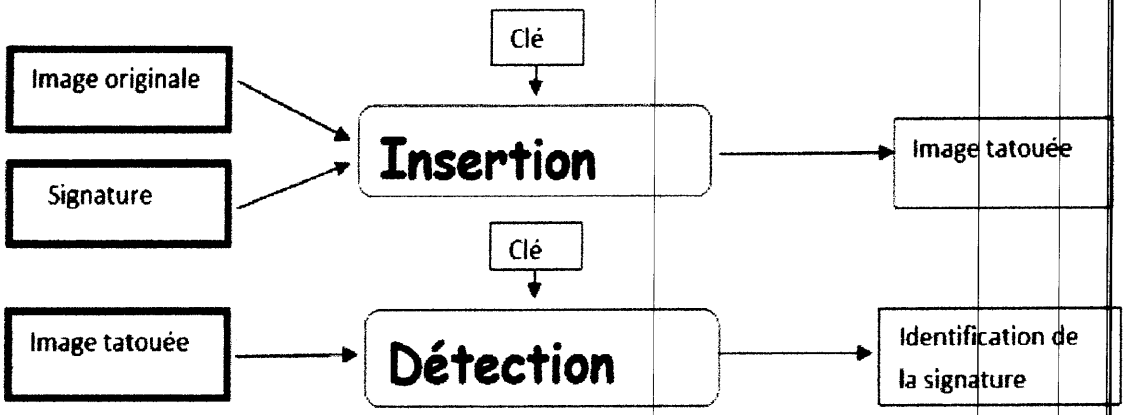


Figure I.3. Insertion et détection aveugle pour le tatouage d'image.

I.2.3.2 Contraintes du tatouage

Pour être performent et efficace, le tatouage doit vérifier les trois critères suivants :

- **Le rapport :** c'est la quantité d'information que l'on insère dans la marque par rapport à la quantité d'information contenue dans le support numérique. La tendance actuelle vise à insérer une quantité d'information au moins égale à 64 bits.
- **L'invisibilité :** c'est une condition nécessaire à tout algorithme de tatouage d'image. L'utilisation de marques psycho visuel tend de plus en plus à se généraliser, pour insérer une quantité d'information importante tout en gardant la marque invisible.
- **La robustesse :** c'est 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 marque du propriétaire. Ces techniques utilisées pour le piratage, combinent notamment : transformations géométriques, filtrages divers et attaques de type cryptographique.

I.2.3.3 Les applications du tatouage

a) Le tatouage et le problème du droit d'auteurs

La première application envisagée pour le tatouage de document est la protection des droits d'auteur. Le tatouage offre une alternative intéressante à la cryptographie car il permet de protéger l'image même lorsque celle-ci est diffusée.

Le but du tatouage consiste ici en l'insertion d'une signature numérique qui atteste de l'identité du dépositaire de l'image. Cette signature ne doit être connue que de la personne ou de l'organisme qui a tatoué l'image. Elle dépend donc d'une clef secrète qui permet son insertion et de sa signature.

Pour une application du copyright, la signature ne doit pas obligatoirement porter une information conséquente, car la détection de la signature peut elle-même attester l'appartenance de la signature.

b) L'authentification des documents numériques

L'information insérée au sein de l'image permet de certifier qu'une image n'a pas été modifiée [14]. On entre ici dans une problématique de contrôle d'intégrité des documents. Dans ce cas précis, la signature ajoutée est dite fragile, on parlera en anglais de « fragile watermarking ». Elle doit être détectée tant que l'image n'a pas été manipulée [15]. Le tatouage fragile est « évolué » lorsque la dégradation provoquée par la compression, la transformation géométrique ou bien encore le filtrage de l'image n'altère pas le tatouage, mais que l'ajout ou l'effacement d'objet dans l'image est détecté.

On peut distinguer deux catégories d'insertion de la signature en tatouage fragile :

- La marque insérée peut représenter le contenu grossier de l'image, la signature contient alors beaucoup d'informations.
- La marque insérée est simplement répandue à l'intérieur de l'image, la manipulation est révélée par une absence de détection.

c) Prévention de la redistribution non autorisée

L'objectif est de détecter les processeurs licites d'un document qui sont à l'origine de sa distribution illicite. Les exemples les plus courants de telles distributions sont les copies (gravées) de CD audio, ou encore la rediffusion de fichier audio au format mp3 sur les pages web personnelles. Une solution au problème de la redistribution non autorisée consiste à identifier séparément les acheteurs, en leur attribuant un numéro de série personnel.

d) Réglementation des copies de données multimédia

Le cryptage d'un document ne suffit pas à assurer la protection de la copie : la sécurité est assurée le long du canal de transmission qui relie le vendeur à l'acheteur sous certaine hypothèse de robustesse ; mais une fois décrypté, le document n'est plus protégé et rien n'empêche le client de la copier. Le tatouage peut s'appliquer à cette famille de problèmes. Des informations relatives à la copie et à l'utilisation sont encodées dans la marque : il peut s'agir d'autorisations du type « pas de copies », « une seule copie », « plus de copies disponibles », ou encore « copie sans restriction ». Le dispositif chargé de la lecture et/ou de la copie interroge le support en refusant de le lire ou de le copier si les données encodées ne le permettent pas. Ce

dispositif suppose la construction d'une nouvelle génération de lecteurs audio. Les lecteurs DVD de seconde génération (permettant de graver des données vidéo) devraient être équipés d'un tel système de tatouage.

e) Information sur le support

La marque peut contenir des données publiques informatives sur l'œuvre, de type auteur, titre, date, adresse électronique, etc. dans l'éventualité (très probable) ou cette application interviendrait en complément d'une protection de la propriété, il s'agirait non pas d'une seconde marque, mais d'informations supplémentaires insérées dans la première marque. On peut aussi envisager l'insertion d'une seconde marque entièrement publique, ce qui autoriserait le client à supprimer ces informations supplémentaires pour minimiser la taille des données stockées. Cette technique a été développée par digimarc [16] sur les images numériques qui sont alors appelées « smart image ». Ces images contiennent des adresses de pages internet permettant d'obtenir des renseignements de nature publicitaire sur l'image.

f) Indexation

On peut envisager l'utilisation du tatouage afin de faciliter l'accès aux banques de données. La marque n'aura pas besoin d'être robuste à de nombreux types d'attaques, puisqu'il ne s'agit plus de protection mais d'identification.

g) Suivi de document

La plupart des techniques définies ci-dessus peuvent être associées à des techniques de suivi de document. Un robot traqueur, Apple bot (bot est le diminutif usuel de robot : programme informatique automatique) explore, sans l'intervention de humaine, un réseau de données à la recherche de données portant une certaine marque de propriété. Cette application privilégie très nettement des algorithmes rapides, qui font appel au minimum de données possible, comme les algorithmes aveugles.

I.2.3.4 Robustesse

Il est utopique d'espérer qu'une marque insérée par tatouage contienne une quantité très importante d'information soit aussi robuste à une très grande variété de traitements. Il faut nécessairement faire un compromis entre le niveau de robustesse et la fonctionnalité du marquage. Le tatouage dédié à la protection des droits d'auteurs doit être aussi robuste que possible car la signature permet dans ce cas l'attester la propriété d'une image [17].

La robustesse du tatouage dédiée à l'authentification de document doit être contrôlée : la marque doit pouvoir révéler une manipulation de l'image mais peut demeurer insensible aux traitements classiques « innocent » comme le filtrage ou la compression. Dans le cas du tatouage pour l'indexation de documents, la priorité doit être accordée à la quantité d'information insérée qui doit être maximale. La robustesse de la signature n'est pas une charge prépondérante, bien que selon les cas la marque doit survivre à des conversions analogiques numériques ou encore à des transformations géométriques simples (rotations, translations).

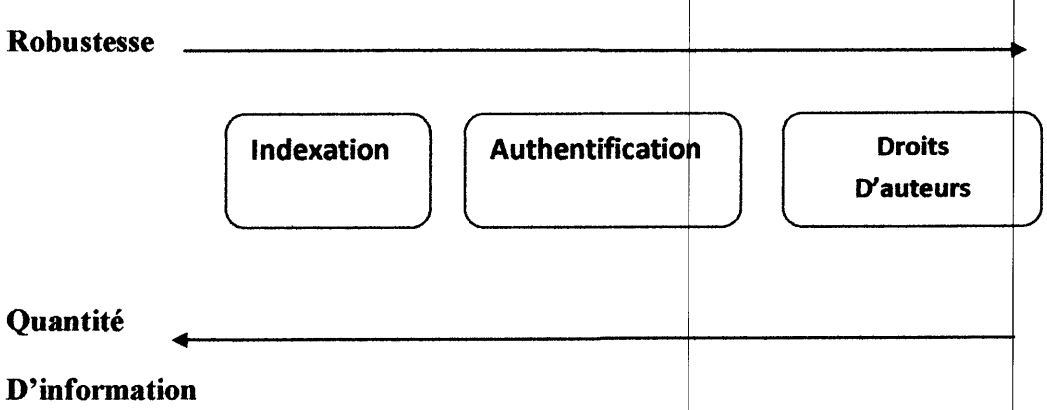


Figure I.4. Dans le cas de la protection des droits d'auteurs, la robustesse est capitale. Cette priorité est moindre pour l'authentification ou l'indexation.

I.2.3.5 Résistance aux attaques

Les applications demandant un grand degré de robustesse nécessitent aussi un grand degré de résistance aux attaques ou falsifications, car de plus que des transformations naturelles, le tatouage va subir l'attaque de pirates voulant effacer cette marque. Ces pirates sont supposés connaître l'algorithme de marquage et donc être en mesure de développer des attaques spécifiques à cet algorithme.

I.2.3.6 protocoles de protection d'images numériques

Les protocoles de tatouage d'images numériques sont fondés sur la participation de 'tierces parties de confiance'. L'étude menée dans le cadre des projets Octalis [18] et Aquamars [19] propose un protocole pour l'enregistrement des images sur Internet. Ce protocole met en jeux deux organismes de confiance : l'autorité d'enregistrement et l'autorité de tatouage. Il est présenté sur la figure I.5 ci-dessous :

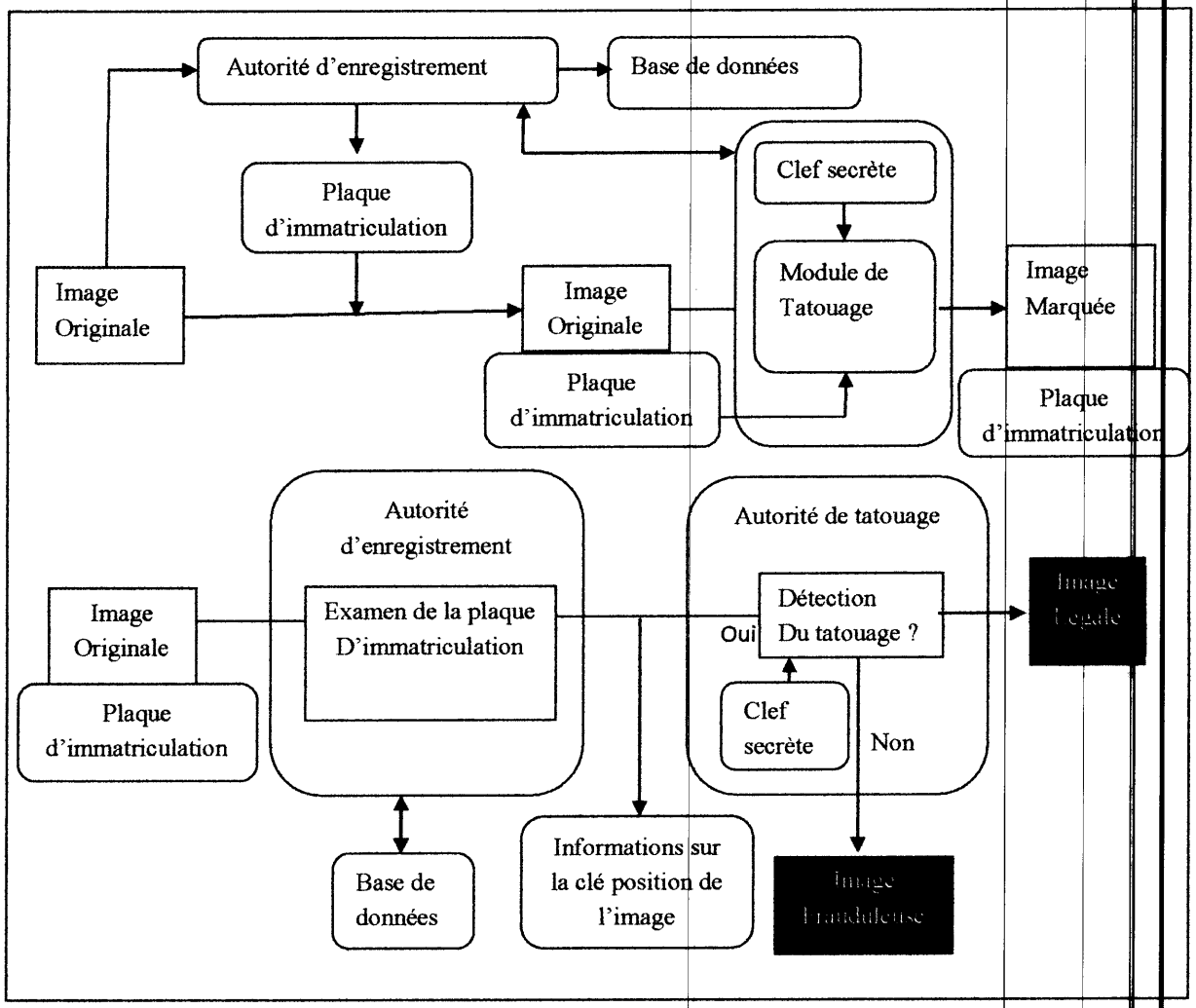


Figure I.5 Application du tatouage pour le transfert d'images numériques sur internet.

I.3 Conclusion

Au cours de ce chapitre, on a vu que l'information a toujours constitué une denrée prisée. Comment l'acquérir ? Comment la protéger ? Comment en vérifier la provenance et l'intégrité ? Avec l'évolution des technologies et des connaissances, les réponses à chacune de ces questions ont évolué. De nouvelles défenses ont contré de nouvelles attaques qui s'opposaient elles-mêmes à d'anciennes défenses. La stéganographie est un sujet encore peu étudié et faiblement médiatisé en tant que tel, mais qui va certainement connaitre ses heures de gloire dans un futur proche. Les liens entre la stéganographie et la télématique sont évidents et son usage sur l'internet semble promis à un bel avenir. Nous avons présenté les objectifs de dissimilation d'information. Selon les attentes, les contraintes d'imperceptibilité, de capacité et de robustesse varient. Cependant, comme ces besoins sont à l'encontre les uns des autres, un compromis est toujours nécessaire.

Chapitre 2

Stéganographie

et

domaines d'insertions

II.1 Introduction

Stéganographie se réfère à la science de la communication "invisible". Contrairement à la cryptographie, où l'objectif est de sécuriser les communications à partir d'un espion, les techniques de stéganographie s'efforcent de cacher la présence du message lui-même d'un observateur [20]. Compte tenu de la prolifération des images numériques, et du degré élevé de redondance présente dans une représentation numérique d'une image (malgré la compression), il y a eu un intérêt accru pour l'utilisation des images numériques dans le but de la stéganographie. Les simples techniques de stéganographie d'image essentiellement intègrent le message dans un sous-ensemble du plan LSB (bit le moins significatif) de l'image, éventuellement après chiffrement [21]. Les outils stéganographiques populaires basés sur LSB-encastrement varient dans leurs approches pour cacher des informations.

II. 2 La stéganographie

II. 2.1 La stéganographie informatique : principes et fondements théoriques

La stéganographie moderne doit beaucoup au modèle conceptuel du « problème du prisonnier » introduit en 1983 par Gustavus Simmons [22]. Le contexte est le suivant : incarcérés dans deux cellules séparées d'une prison de haute sécurité, Alice et Bob doivent communiquer par messages surveillés, c'est-à-dire que le message doit passer nécessairement par un gardien, afin d'élaborer un plan d'évasion. Marine et Alexandre doivent alors mettre en place un canal dit subliminal afin de dissimuler l'information qu'ils échangent dans un support qui n'éveille pas les soupçons du gardien. Si les schémas classiques de cryptographie ne permettent pas un tel canal, la stéganographie le permet. En effet, alors que dans le premier cas, l'échange de messages chiffrés suscitera la méfiance du gardien qui mettra fin à la communication entre les deux détenus et les contraindra certainement à divulguer leur clé de chiffrement, dans le second cas, Marine et Alexandre dissimuleront l'information compromettante dans un « message innocent » qui n'éveillera pas les soupçons du gardien. Comme le souligne Fabien Galand [23] : « *l'approche choisie peut dépendre du contexte dans lequel a lieu la communication ; le recours au chiffrement peut être interdit, ou bien les deux protagonistes peuvent vouloir dissimuler l'existence même de l'échange de messages confidentiels.*»

De ce modèle conceptuel, en apparence fort simple, se dégagent en réalité deux procédés distincts en matière de sécurisation de l'information :

- D'une part, la sécurisation de la communication (COMSEC). L'information est transmise, mais elle est incompréhensible : il s'agit là du domaine de prédilection de la cryptographie.

  Aussi, le potentiel attaquant saura qu'une information est communiquée, ce qui représente déjà souvent en soi une information importante, mais elle lui sera illisible, donc il sait qu'il ne sait pas !

- D'autre part, la sécurisation des transmissions (TRANSEC). L'information et la transmission de celle-ci sont dissimulées : il s'agit là d'un domaine dans lequel la stéganographie a une place. En l'occurrence, le potentiel attaquant, ne sachant pas qu'une information a été communiquée, ne cherchera pas à l'intercepter : il ne sait pas qu'il ne sait pas !

  Précisons à cet égard que la stéganographie pure, celle ne faisant intervenir aucune clé de chiffrement (l'information est alors transmise en clair, seul le procédé d'insertion étant secret), s'écarte de fait du fameux principe de Kirchhoff [24] qui veut que : « *la sécurité d'un crypto-système ne doit reposer que sur le secret de la clef* ». Toutefois, coupler stéganographie et cryptographie, ce qui est dans la pratique très courant [25], permet incontestablement de renforcer la sécurisation de l'information.

Dans le domaine de la dissimulation d'information, il faut trouver le juste équilibre entre :

- La capacité, c'est-à-dire la quantité d'informations que l'on peut incorporer dans un support.
- L'imperceptibilité, c'est-à-dire les chances que le stégo-médium soit détecté *innocent* (non stégo) par un attaquant.
- La robustesse, c'est-à-dire l'aptitude de préservation des données cachées face aux modifications, volontaires ou non, du stégo-médium (compression, filtrage, etc.)

Ce compromis est traditionnellement représenté par un triangle. En stéganographie, la capacité et l'imperceptibilité ont beaucoup d'importance, tandis que le tatouage ou l'empreinte privilégient, comme nous le verrons, la robustesse. Pour finir, notons que le processus complet de stéganographie repose sur deux opérations : d'une part, la dissimulation

en tant que telle, qui consiste à insérer l'information à cacher dans le médium ; d'autre part, l'extraction, qui vise à la récupérer. Le terme « détection » est également utilisé lorsqu'il s'agit simplement de vérifier la présence d'une information (par l'examen d'un signal, d'une caractéristique particulière du médium, etc.) dans le stégo-médium, sans pour autant l'extraire [26].

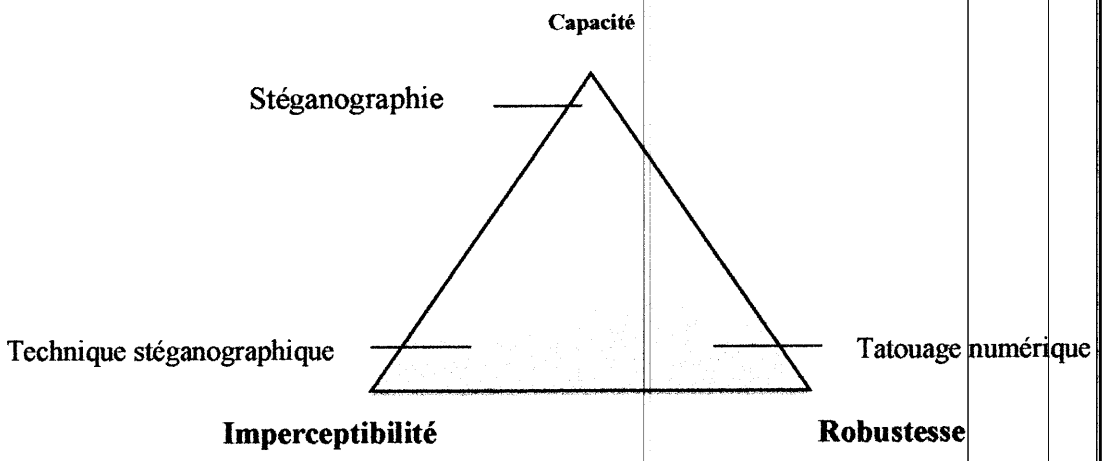


Figure I.1 Triangle représente caractéristiques d'un marquage.

II .2.2 Schémas de stéganographie

Un exemple classique d'écrivant une communication secrète a été proposée par J Simmons [27] comme le problème des prisonniers. Imaginons une prison, deux prisonniers Alice et Bob et une gardienne Eve. Comme dans toute prison, Alice et Bob sont enfermés dans deux cellules séparées. Alice et Bob sont autorisés à communiquer par messages surveillés, c'est-à-dire que le message doit passer nécessairement par la gardienne Eve, comme montre la figure II.2. Avant d'être enfermés, Alice et Bob ont partagé une *technique secrète* pour partager des informations sans provoquer le moindre signe de soupçon chez Eve. Alice et Bob ont l'idée de s'évader de la prison, grâce à leur *technique secrète*, Alice et Bob pourront communiquer leur plan d'évasion sans qu'Eve soit suspicieuse. La règle du jeu est donc la suivante : si Eve conclut qu'il y a une communication secrète, elle stoppe la communication ou alors laisse la communication s'il n'y a pas de communication secrète.

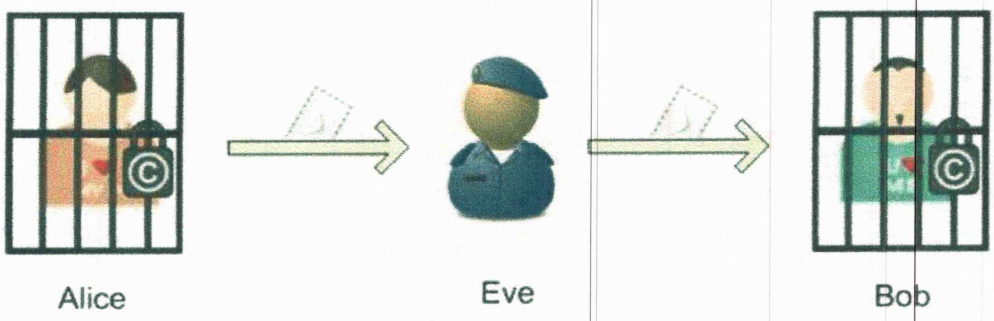


Figure II.2 Problème classique de communication secrète.

La fonction d'insertion (embedding), elle prend en paramètre un support ou medium de couverture et un message qu'on veut dissimuler, puis retourne un nouveau medium de couverture appelé stégo-médium ou stégo-objet. Le stégo-médium peut être intercepté par quelqu'un qui peut faire une modification ou non. Finalement, le stégo-objet est traité par une fonction d'extraction (fonction inverse à la fonction d'insertion) qui retourne le message original.

De la même façon qu'en cryptographie il existe plusieurs systèmes de stéganographie :

- **La stéganographie pure** : aucune entente préalable n'est nécessaire entre Alice et Bob, il suffit qu'ils utilisent le même algorithme de cryptage.

- **La stéganographie à clé secrète** : Alice et Bob conviennent d'une clé secrète servant à insérer et extraire le message.

- **La stéganographie à clé publique** : tout comme en cryptographie, Alice utilise la clé publique de Bob lorsqu'elle souhaite lui envoyer un message ; Bob, pour sa part, l'extrait le message à l'aide de sa clé privée.

En stéganographie, la clé détermine les portions de l'image ou sera caché le message. Il est possible de dissimulé des messages cryptés. Aussi La robustesse est peu importante en stéganographie car le médium ne sera pas modifié alors que l'imperceptibilité et la capacité sont très importantes.

II .2.3 Types de stéganographie

Il existe deux types de stéganographie :

- La stéganographie linguistique
- La stéganographie technique

II.2.3.1 La stéganographie linguistique

L'un des exemples les plus connu date de 1313, il s'agit de 3 sonnets écrits par Boccaccino dissimulés dans d'autres poèmes. Les lettres des 3 sonnets étaient les premières lettres des vers des autres poèmes.

La lettre de Georges Sand utilise une autre technique et la réponse d'Alfred Musset utilise une autre technique très connue « l'Acrostiche ». Les premiers mots de chaque ver forment une phrase.

II.2.3.2 La stéganographie technique

Nous allons maintenant parler plus précisément de la stéganographie technique. En effet, c'est la plus intéressante car elle permet de dissimuler des données dans plusieurs types de médias.

A. Dans du texte

Il s'agit du premier médium sur lequel ce type de cryptographie et été appliqué :

Voici différentes techniques :

- Trous sous les lettres importantes.
- Changement de type d'écriture (Francis Bacon).
- Utilisation de synonymes.
- Changement de règles de grammaires.
- Jeu sur les espaces.

Ces méthodes ont plusieurs inconvénients :

- Faible capacité - il est possible de l'augmenté mais l'imperceptibilité diminue alors.

Une variante moderne consiste à insérer les données dans le formatage (espacement des interlignes, taille de police) des documents électroniques mais ces techniques ne résistent pas à l'examen du code.

B. **Dans le son**

Cette technique est très délicate à mettre en œuvre car l'oreille humaine est beaucoup plus sensible que les yeux c'est pourquoi la stéganographie utilisent beaucoup plus les médiums images et vidéos. On peut cependant noter l'exemple du groupe de techno AphexTwin qui avait dissimulé une image dans l'une des pistes de son album.

C. **Dans les images**

Nous allons maintenant détailler les six grandes approches de stéganographie :

Un système par substitutions remplace les parties redondantes du support par le message.

- Les techniques par transformations dissimulent l'information dans une transformée du support, comme par exemple la transformée en cosinus discrète ou le domaine des ondelettes.
- Les techniques par étalement de spectre : les informations sont dissimulées dans toute l'image, et la perte de certaines informations doit pouvoir être compensée par les autres.
- Les méthodes statistiques modifient plusieurs statistiques du support (distribution des pixels, luminosité...) pour cacher le message et le récupérer en testant ces hypothèses.
- Les techniques par distorsions altèrent le support, la différence avec le support initial constituant alors le message.
- Les méthodes par génération de support : construisent un support autour du message pour le dissimuler.

Un exemple plus courant est d'insérer le message dans les bits les moins significatifs *'Least Significant Bit* ou (LSB)' : le bit le moins significatif de chaque composante de couleur est remplacé par celui de la donnée à cacher (Substitution). Pour décoder on récupère les bits de poids faibles. Une clé détermine les pixels dont les LSB seront modifiés.

Pour garantir une bonne imperceptibilité totale, seuls les pixels situés dans des zones de variation de couleurs seront modifiés.

En utilisant la DCT par exemple, la clé détermine deux coefficients dans le tableau 8*8 obtenu après DCT et modifie leurs valeurs de façon à ce que leur différence soit supérieure ou inférieure à un certain seuil pour coder le 1 ou le 0 binaire respectivement, puis on fait une DCT inverse pour retrouver l'image.

Pour décoder, on exécute le même processus mais la modification des coefficients est remplacée par un test sur le seuil de différence.

D. **Dans la vidéo**

Les techniques sont équivalentes à celles utilisées dans les images à la différence près que les vidéos sont souvent plus bruitées. Ceci facilite l'imperceptibilité des données dissimulées mais les rend aussi moins robustes.

II.3 Objectifs de la stéganographie

La stéganographie cherche à cacher un message secret dans un médium de sorte que personne ne puisse distinguer un médium vierge d'un stégo-médium. La nature de l'information dissimulée ne revêt pas d'importance : il peut tout aussi bien s'agir d'un texte en clair que de sa version chiffrée. Ce message n'a à *priori* aucun lien avec le stégo-médium qui le transporte.

Lorsqu'un attaquant tente uniquement de détecter si un message transite dans un médium sur un canal de communication, on dit de lui qu'il est *passif*. La plupart des solutions de stéganographie ne considèrent que ce type d'attaquant, au contraire des deux domaines suivants ou il est *actif* : l'attaquant sait alors que le stégo-médium contient une information et il tente de la modifier ou de la retirer.

Toutefois si le but de la stéganographie est de dissimuler un message sans éveiller l'attention humaine, avec la stéganographie informatique il faut également veiller à ne pas éveiller l'attention des logiciels d'analyse. Car si une image est soupçonnée de contenir un message stéganographique, on pourra toujours la soumettre à un logiciel chargé de traquer tout bruit de fond trop organisé et statistiquement non aléatoire : on peut alors facilement repérer un message stéganographique et effectuer une stéganalyse (tentative de récupération du message caché).

Il faut donc que le message à cacher soit en tout point comparable à une suite de bits aléatoires : pour cela une seule solution : *il faut préalablement crypter le message*.

II.4 Quelques applications classiques de la stéganographie

« *Le chemin est long par les préceptes et court par les exemples* », notait François des Rues dans son ouvrage *Les marguerites françaises*. Aussi, après avoir présenté les aspects techniques de la dissimulation à l'heure du numérique, nous proposons quelques illustrations de stéganographie appliquée à divers types de données numériques multimédia, en l'occurrence une image (A) et un texte (B). Nous verrons ainsi qu'en plus d'être une opération séduisante sur le plan technique, la stéganographie peut être relativement facile à mettre en œuvre.

II.4.1 Une image peut en cacher une autre

Franz Kafka, précurseur à bien des égards, relevait au début du XXème siècle : « *Le regard ne s'empare pas des images, ce sont elles qui s'emparent du regard* ». La stéganographie appliquée aux images numériques en est, aujourd'hui, une excellente preuve.

Il s'agit alors d'*encapsuler* un fichier secret dans un document hôte qui ne sera autre qu'une image. De la sorte, sans conséquence sur l'apparence, (l'image pourra être visionnée sans problème) l'image contiendra en fait un message caché.

Les méthodes pour cacher un message secret dans une image numérique sont multiples [28]. En l'occurrence, il s'agit de « rogner » sur les bits de chaque pixel d'une image et d'y ajouter le code binaire du fichier numérique secret. Considérant qu'un pixel d'image (« RGB » de l'anglais Red-Green-Blue) est souvent codé sur trois octets (soit 24 bits d'information) ce qui donne 16,8 millions de couleurs, on comprend aisément qu'une telle dégradation de l'image soit indiscernable à l'œil nu.

De nombreux logiciels permettent aujourd'hui de coder aisément des messages à l'intérieur d'une image. L'exemple valant bien souvent les meilleures explications, nous nous sommes soumis à l'exercice.

Image hôte

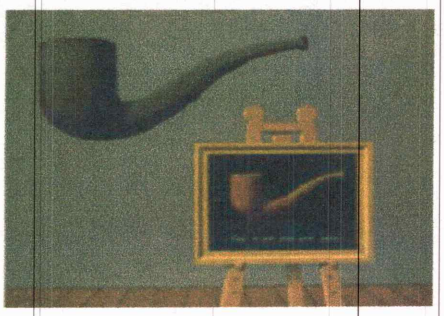


image à cacher

Image contenant le fichier secret

Figure II.3 : La dégradation de l'image passe alors inaperçue et seul le logiciel adéquat permet de retrouver les données cachées [28].

II.4.2 Dissimuler un message dans un texte

Quoique très anciennes et simples à mettre en œuvre, les techniques stéganographiques consistant à dissimuler un message dans du texte restent toujours d'actualité [29]. Ceci d'autant plus que la quantité de courriels échangés ne cesse de prendre un essor croissant.

Comme nous allons le voir, la dissimulation d'information dans du texte n'a pas grand-chose à voir avec l'image. En effet, alors que la dégradation de l'image pouvait passer inaperçue, l'altération d'un texte sera aisément discernable : soit le texte est identique à l'original, soit il ne l'est pas [28]. Dès lors, nous allons présenter une méthode qui tend vers un endommagement minimal du texte original.

<u>Méthodes des « espaces » en fin de phrases ou entre les mots :</u>

S'agissant de l'utilisation de cette méthode en fin de phrase, il faut toujours se définir un code à suivre.

EXEMPLE 1

Code à suivre : 0 espace en fin de phrase correspond à 0 ; 1 espace en fin de phrase correspond à 1.

Texte contenant le message secret tel que perçu :

René Magritte ou la trahison des images … Le peintre belge Magritte (1898-1967) est une figure marquante du mouvement réaliste. Il s'est fait remarquer notamment par son art du décalage entre le titre et le sujet représenté. La trahison des images est un de ses tableaux les plus célèbres. Il représente une pipe accompagnée de la légende suivante : « ceci n'est pas une pipe ». Son intention était de montrer que, même peinte de la manière la plus réaliste qui soit, un tableau qui représente une pipe n'est pas une pipe. On ne peut ni la bourrer ni la fumer. De même que « le mot "chien" ne mordras ».

Texte contenant le message secret où les espaces sont remplacés par « _ » pour davantage de lisibilité :

René Magritte ou la trahison des images_… Le peintre belge Magritte (1898-1967) est une figure marquante du mouvement réaliste. Il s'est fait remarquer notamment par son art du décalage entre le titre et le sujet représenté_. La trahison des images est un de ses tableaux les plus célèbres_. Il représente une pipe accompagnée de la légende suivante : « ceci n'est pas une pipe ». Son intention était de montrer que, même peinte de la manière la plus réaliste qui soit, un tableau qui représente une pipe n'est pas une pipe_. On ne peut ni la bourrer ni la fumer_. De même que « le mot "chien" ne mord pas ».

→ Nous avons codé dans notre message : 1 espace, 0 espace, 1 espace, 1 espace, 0 espace, 1 espace, 1 espace, 0 espace. **10110110 soit un octet de dissimulé.**

Comme vous pouvez le constater, il faut beaucoup de phrases pour coder un peu de texte (en l'occurrence, 8 phrases pour coder 1 octet) et une personne attentive aura vite fait de détecter les espaces. En revanche, cette méthode reste très simple à implémenter et il y a possibilité de la moduler à votre gré (par exemple, en rajoutant des espaces pour coder davantage de caractères sur moins de texte).

S'agissant de la méthode des espaces entre les mots, il faut là encore se définir au préalable un code à suivre.

II .5 Domaine d'insertion dans les images numérique

II .5.1 La stéganographie dans le domaine spatial

Dans le domaine spatial, la dissimulation du message est directement effectuée au niveau du codage des pixels. Une image peut être représentée à l'aide d'une matrice de pixels. Chaque pixel est représenté à l'aide de 1 à 32 bits. Ce nombre dépend de la représentation des couleurs utilisées. Les plus utilisées sont cependant 8 bits ou 24 bits Sur 8 bits, deux méthodes de codage sont utilisées. Dans le cadre d'une image en niveaux de gris, chaque pixel code directement le niveau de gris approprié. Dans celui d'une image couleurs, on utilise le mécanisme d'image indexée. Au sein de chaque pixel est codé une valeur correspondant à l'index de la couleur a utilisé dans la palette de couleurs définie.

Pour ce qui est du codage sur 24 bits, on utilise généralement le RGB (Red Green Blue) pour la représentation des couleurs. Chaque pixel est codé à l'aide d'un triplé de byte spécifiant chacune des composantes principales. Dans ce type de représentation, il est possible de dissimuler 3 bits par pixel (1 par composante) sans aucun impact visuel. Les résultats sont présentés dans la figure II.4.

Figure.II.4 A gauche, image originale. A droite, image contenant un fichier de format PDF de 32 Kb dissimulé [28].

Les fichiers généralement utilisé sont au format BMP.

Cette technique est très utilisée car elle est facile à mettre en œuvre. Elle permet de directement ajouter les données à l'image, sans avoir à passer par un mécanisme de

compression/décompression comme ce serait le cas pour la modification des coefficients DCT.

Sa propre implémentation devient très facile, cela permet de s'affranchir de l'utilisation d'un produit existant et par la même occasion, d'éviter la détection de signature étant attribuée à ce programme (technique encore très utilisée dans les outils de détection). De plus, il est possible de vraiment contrôler la manière dont seront dissimulées les données au sein du conteneur. Il sera possible de facilement implémenter des mécanismes permettant de déjouer les tentatives d'analyse statistiques.

L'inconvénient majeur provient des formats utilisés. Les images au format JPEG sont de loin, les plus répandue sur Internet. Le simple fait d'envoyé une image au format BMP peut attirer l'attention, et de ce fait, mettre à néant tous les efforts de dissimulation de données.

Ainsi, les outils permettant la dissimulation de données dans le format JPEG constitue une des meilleures solutions offertes. La prochaine section va en détailler l'idée générale.

II .5.2 La stéganographie dans le domaine fréquentiel

Le domaine fréquentiel (obtenu après une TCD ou une TFD), possède l'énorme avantage d'être l'espace de transformation qui est utilisé dans des nomes de communication, telles que JPEG pour les images fixes, ou bien MPEG2 pour les séquences vidéo, les schémas qui utilisent le domaine fréquentiel comme domaine d'insertion, peuvent être d'avantage robustes face aux opérations de compression, puisqu'ils utilisent le même espace que celui qui sert à la quantification et au codage de l'image.

La TCD à deux dimensions (2D) est définit mathématiquement par la formule suivante [30] :

$$S(u,v) = \frac{2}{N} C(u)C(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} s\,(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) - \cos\left(\frac{\pi v(2y+1)}{2N}\right) \qquad \text{(II.1)}$$

La transformée TCD-2D inverse (TCDI-2D) s'écrit :

$$s(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C\,(u)C(v)S(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) - \cos\left(\frac{\pi v(2y+1)}{2N}\right) \qquad \text{(II.2)}$$

Avec C(u)=1/$\sqrt{2}$ si u=0 et C(u)=1 autrement.

La Transformé de Fourrier Discrète (TFD) à 2D est définit par :

$$F(k_1,k_2) = \beta \sum_{n1=0}^{N1-1} \sum_{n2=0}^{N2-1} f\,(x_1,x_2) \exp\left(\frac{-i2\pi_1 k_1}{N_1} - \frac{i2\pi n_2 k_2}{N_2}\right) \quad \text{(II.3)}$$

Avec : β =($N_1, N_2)^{-1/2}$ et i=$\sqrt{-1}$

La TFD inverse à 2D s'écrit alors :

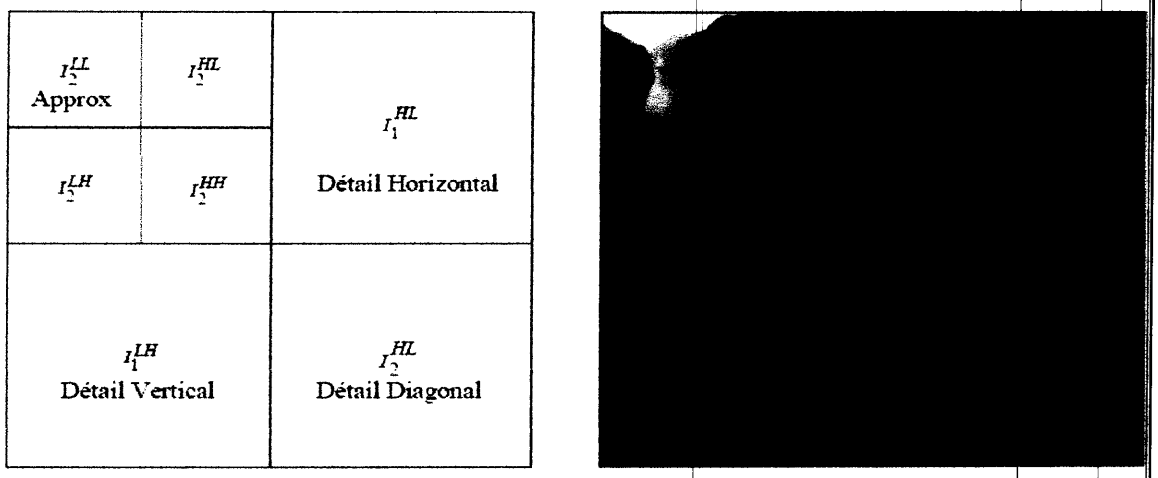
$$F(n_1,n_2) = \beta \sum_{k1=0}^{N1-1} \sum_{k2=0}^{N2-1} f\,(k_1.k_2) \exp\left(\frac{-i2\pi k_1 n_1}{N_1} - \frac{i2\pi k_2 n_2}{N_2}\right) \quad \text{(II.4)}$$

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), au contraire l'espace obtenu après la TFD possède des propriétés d'invariances qui peuvent être exploité pour détecter la marque après des transformations géométriques telles que la rotation, la translation et le changement d'échelle.

II.5.3 La stéganographie dans le domaine multirésolution (ondelettes)

• La transformée en ondelette

Grossièrement parlant, la transformée en ondelettes consiste en une décomposition spatio-fréquentielle multi-échelles d'une image. La figure II.5 montre la décomposition de l'image 'Nature.bmp' avec trois facteurs d'échelle. La bande de basse fréquence au facteur d'échelle le plus bas est située au coin haut gauche (LL2). Au même niveau de résolution, le block HL2 contient des informations sur la fréquence horizontale la plus haute et sur la fréquence verticale la plus basse. De même le block LH3 contient les informations sur la plus basse horizontale et la plus haute verticale bande de fréquences au facteur d'échelle le plus bas. Le block HH3 (diagonal) similairement, contient les informations sur les fréquences hautes verticales et horizontales à la même échelle. Le même processus est répété pour le niveau de résolution intermédiaire et pour le plus haut niveau de résolution.



(a) **(b)**

Figure II.5 (a) Décomposition à trois niveaux de l'image de 'Nature.bmp'.

(b) Décomposition spectrale.

Une façon de construire les différents niveaux de résolution est de monter en cascade des filtres et des processus de sous échantillonnage. Comme montrés dans la figure II.6 deux types de filtres orthogonaux H(w) et G(w) sont utilisés le premier est un filtre passe haut et le second est passe bas et qui sont définis par les équations :

$$H(\omega) = \sum_k h_k \exp(-jk\omega) \qquad \text{(II.5)}$$

Alors le processus itératif de décomposition est donné par :

$$c_{j-i,k} = \sum_n h_{n-2k} c_{j,n} \qquad \text{(II.6)}$$

$$d_{j-i,k} = \sum_n g_{n-2k} C_{j,n} \qquad \text{(II.7)}$$

Où le processus itératif de reconstruction est défini par :

$$c_{j,n} = \sum_n h_{n-2k} c_{j-1,k} += \sum_n g_{n-2k}\, d_{j-1,k} \qquad \text{(II.8)}$$

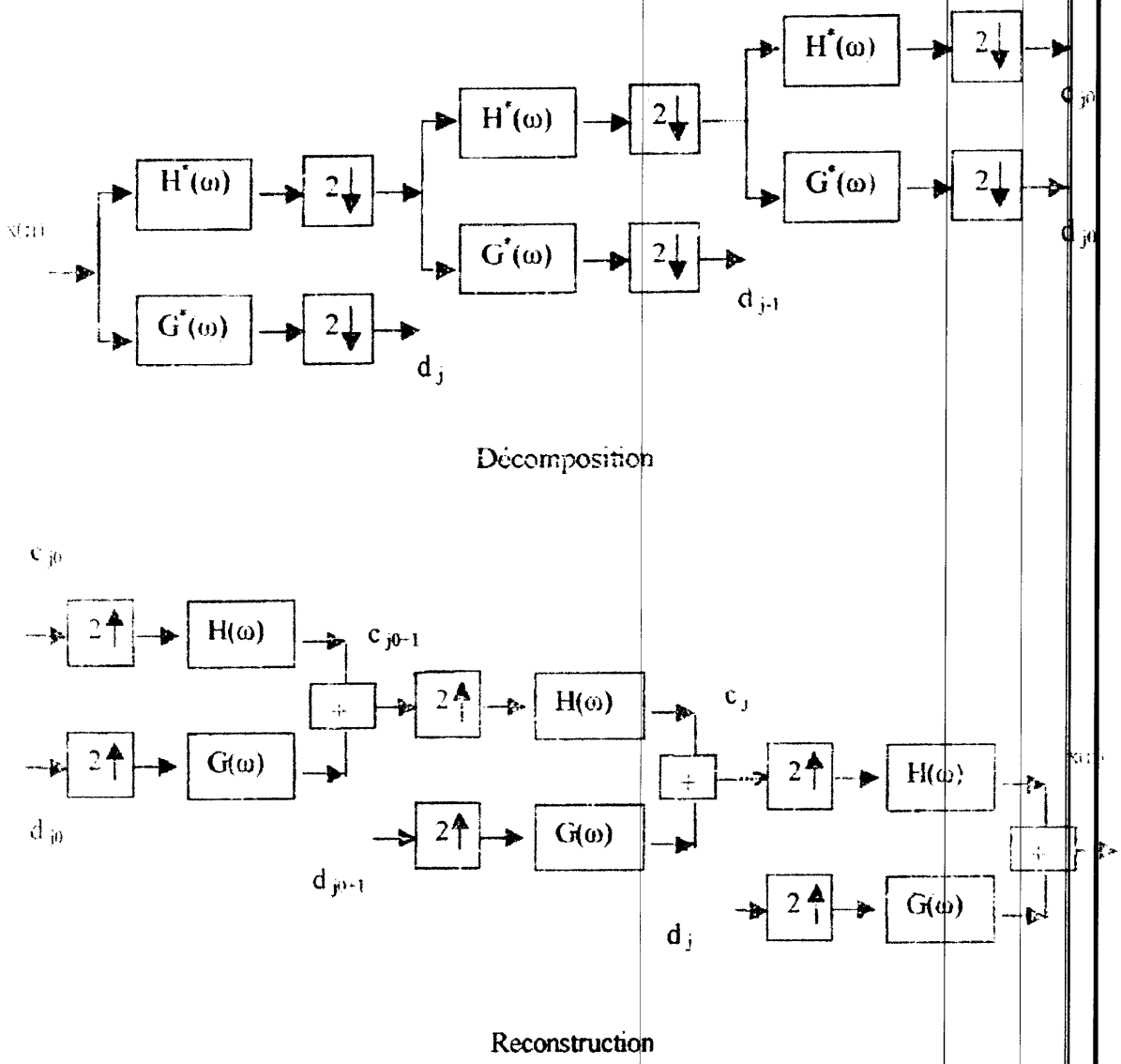


Figure II.6 Transformée en Ondelette.

Nous allons présenter plus loin quelques algorithmes utilisant le domaine multirésolution par ondelettes pour la stéganographie. Nous commençons par présenter différentes classes d'algorithmes et des exemples d'algorithmes appartenant à chaque classe.

II .6 Les différentes classes de méthodes de stéganographie

Traditionnellement, on classe les méthodes de stéganographie selon le domaine sur lequel ils agissent. On dispose alors essentiellement de méthodes spatiales, fréquentielles ou multi-résolutions. Néanmoins, un autre critère de séparation existe en fonction de la manière

dont est inséré le stéganographie : soit il est, ajouté au médium, soit il en remplace certains coefficients. Chaque espace de travail utilisé en stéganographie possède ses propres avantages et inconvénients [31].

Les méthodes agissant dans le domaine spatial modifient directement les valeurs des pixels. Comme aucun traitement initial n'est requis, ces algorithmes sont très rapides et permettent de travailler en temps réel. De plus, elles offrent souvent une bonne résistance aux opérations géométriques.

- **Le type de schéma d'insertion de la signature**

Dans un schéma additif, la marque est ajoutée sans modifier l'image originale, dans un schéma substitutif, on supprime dans l'image certaine de ses composantes, cette substitution formant le support de la marque.

- **Le choix de l'espace de travail**

La marque peut ait être insérée dans le domaine spatial, soit dans le domaine transformée (Transformation Cousins Discrète, Transformation Fourier Discrète, Ondelettes).

Pour décrire les différentes méthodes de stéganographie d'images, nous traitons séparément les méthodes additives et les méthodes substitutives.

II .6.1 Méthodes additives

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un bruit à l'image. La figure II.7 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque $W0$ qui est composée d'un bruit blanc modulant parfois un message M. La seconde étape est la pondération de cette marque grâce à la prise en compte de critères psychovisuels et de caractéristiques propres à l'image. La troisième étape est l'addition de la marque dans les valeurs de l'image. Cette incrustation peut se faire directement sur l'image (Dans le domaine spatial) ou dans un domaine transformé. Cette section nous permettra de donner un aperçu de ces différentes étapes à travers des exemples de schéma de stéganographie

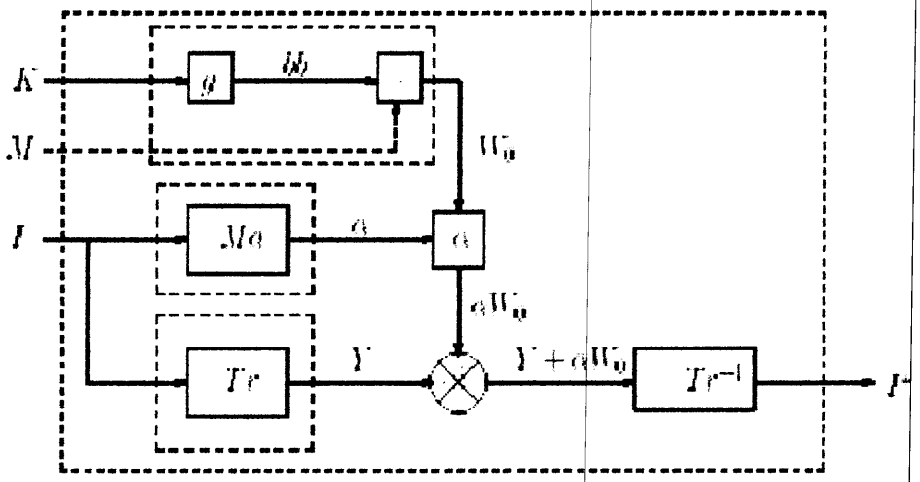


Figure II.7 Schéma d'une méthode additive.

La marque W0 est construite en modulant le message M par un bruit blanc bb de générateur K. W0 est ensuite pondéré par un gain α, issu du calcul d'un masque Ma psychovisuel. Cette marque est ajoutée à l'image ou à une transformée Tr.

II.6.2 Méthodes substitutives

➢ **Insertion de la signature**

Les schémas substitutifs peuvent se décomposer en quatre étapes :

1. Une clef associée à un générateur aléatoire permet de sélectionner les différentes composantes $C_k(I)$ de l'image. Ces composantes peuvent par exemple désigner des pixels de l'image, des coefficients issus de blocs TCD de l'image, ou encore des propriétés géométriques de l'image.

2. La signature à insérer est obtenue en appliquant une contrainte F sur $C_k(I)$ en fonction du massage à insérer $W(K)$ .cela peut être par exemple une relation d'ordre, un critère de similarité, ou encore une propriété géométrique de l'image

3. On procède ensuite à l'étape de substitution :

$$C_k(I_w) = F(C_k(I), W(K)) \qquad \text{(II.9)}$$

4. L'image tatouée est reconstruite à partir des composantes propres à la signature.

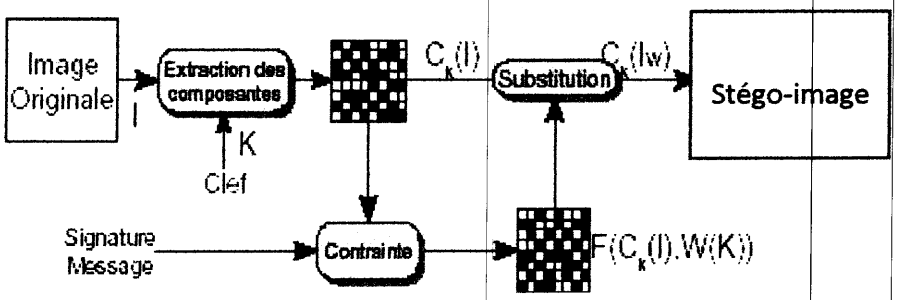


Figure II.8 Principe de l'insertion par substitution.

- **Détection de la signature et lecture du message**

La détection de la signature peut se décomposer en quatre étapes

1. la clef secrète permet d'extraire les composantes de stégo-image I_t soit : $C_k(I_t)$

2. le message inséré dans l'image à partir de la contrainte F utilisée lors de l'insertion de la signature.

3. la détection de la signature s'effectue en comparant le degré de similitude entre le préambule retrouvé et le préambule utilisée lors de l'insertion de la signature.

4. le message inséré est ensuite décodé.

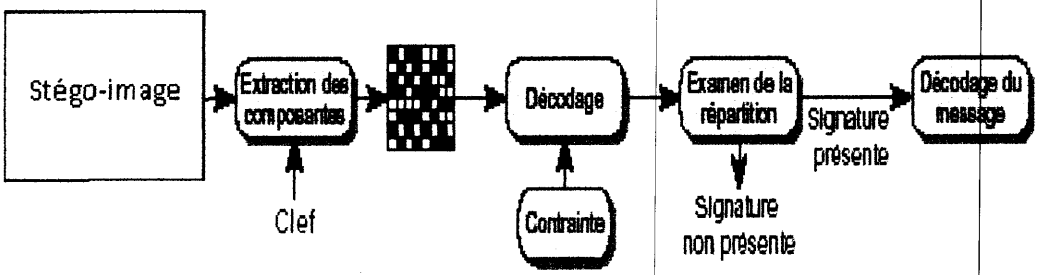


Figure II.9 Détection et lecture de la signature par substitution.

II .7 Comparaison entre les méthodes substitutives et additives

Le tableau III.1 présente les principales différences entre la classe des schémas additifs et la classe des schémas substitutifs :

	Additifs	**Substitutifs**
Capacité (sans attaques)	Faible	Maximale
Clef	Germe de la séquence aléatoire	Choix des sites
Insertion	Addition d'une séquence aléatoire	Substitution de caractéristiques de l'image
Détection	Corrélation	Analyse de la redondance
Amélioration de la détection	Estimation de W Utilisation De l'image originale	Code correcteur d'erreurs

Tableau II.1 Comparaison entre les schémas additifs et les schémas substitutifs.

II.8 conclusion

La stéganographie consiste à cacher un message dans un support "innocent". Elle peut, de surcroît, se combiner à la cryptographie, qui se charge de dissimuler le sens de la missive et non plus son existence. Le message secret s'abrite d'abord derrière son invisibilité.

En cas de découverte, il restera à le décoder. Un défi pour les services secrets qui, dans le cas du terrorisme, doivent réaliser ces deux opérations au plus vite pour que l'information recueillie ne soit pas obsolète.

Il faut savoir que si la stéganographie est très pratique, son utilisation informatique est détectable. Il ne faut pas oublier que cela est avant tout un code informatique. La sécurité de la stéganographie repose sur le fait que le message ne sera sans doute pas détecté.

Chapitre 3

Ondelettes et stéganographie

III.1 Introduction

Dans ce chapitre nous allons présenter une méthode basée sur des techniques plus modernes dans le domaine de traitement d'images, qui est la décomposition en ondelette. Celle-ci est apparue dans la dernière décennie.

Le but de présentation de cette méthode est de faire ressortir les procédures générales de traitement d'image. L'étude de cette méthode permet également de mieux comprendre comment dissimuler une information dans les images numériques ? On finira le chapitre par une conclusion sous forme d'analyse qui résumera ce qui a été vu dans le chapitre.

III.2 Histoire de la décomposition en ondelettes

Les ondelettes ont vu le jour lorsque certains sujets d'étude ont nécessité une analyse en fréquence et en temps. Au XIXe siècle, l'analyse de Fourier était la seule technique permettant la décomposition d'un signal et sa reconstruction sans perte d'information; malheureusement elle fournit une analyse en fréquence mais ne permet pas la localisation temporelle de changements abrupts, comme par exemple l'apparition d'une deuxième note de musique après qu'une première note ait été jouée. En 1909, Alfred Haar définit une fonction composée d'une courte impulsion négative suivie d'une courte impulsion positive, connue pour être la première ondelette (Ondelette de Haar). En 1946, Dennis Gabor, mathématicien Hongrois, inventa une transformation de fonction analogue a celle de Joseph Fourier, appliquée sur une fenêtre temporelle exprimée par une fonction gaussienne [32]. Finalement, le terme d'ondelette fut introduit dans le langage mathématique par Jean Morlet et Alex Grossmann en 1984. Terme initialement français, il fut traduit en anglais par *wavelet*, à partir des termes *wave* (onde) et le diminutif *let* (petite). Yves Meyer, reconnu comme un des fondateurs de la théorie des ondelettes, rassembla en 1986 toutes les découvertes précédentes (il en dénombra 16) puis définit les ondelettes orthogonales. La même année, Stéphane Mallat fit le lien entre les ondelettes et l'analyse multirésolution. Enfin, Ingrid Daubechies mit au point en 1987 des ondelettes bi-orthogonales appelées ondelettes de Daubechies, facilement implémentables, et utilisées dans le standard JPEG 2000.

III.3 Définition mathématique

En mathématiques, une ondelette (Ψ) est une fonction de carré sommable de l'espace de Hilbert $L^2(\mathbb{R})$, le plus souvent oscillante et de moyenne nulle, choisie comme outil d'analyse et de reconstruction multi-échelle. Les ondelettes se rencontrent généralement par familles

constituées d'une ondelette mère et de l'ensemble de ses images par les éléments d'un sous-groupe du groupe des transformations affines de $\mathbb{R}^n$.

On définit ainsi une famille $\psi_{s,\tau}$ (où $(s,\tau) \in \mathbb{R}^{+*} \times \mathbb{R}$) d'ondelettes à partir de l'ondelette mère :

$$\forall t \in \mathbb{R}, \psi_{s,\tau}(t) = \frac{1}{\sqrt{s}}\Psi\left(\frac{t-\tau}{s}\right) \qquad \text{(III.1)}$$

Par extension, des familles de fonctions sur des sous-variétés de $\mathbb{R}^n$ d'invariantes par un groupe de transformation localement isomorphe au groupe affine peuvent également être qualifiées de familles d'ondelettes.

III.4 Transformée en ondelettes

Les techniques basées sur les ondelettes sont actuellement de plus en plus fréquentes ou en cours d'investigation. Parmi celles-ci on peut citer celle de Kundur et Hatzinakos [33] et celle de Lin et Chang [34]. Le principe de la méthode proposée par Lin et Chang est de choisir, tout d'abord, un bruit pseudo-aléatoire et une ondelette de base, qui constituent le secret du système d'authentification. Puis, de décomposer l'image en 4 sous-bandes (LL, LH, HL et HH) en fonction de l'ondelette de base choisie au départ. L'étape suivante revient à substituer la sous-bande HH par le bruit pseudo-aléatoire et à effectuer ensuite la transformation en ondelettes inverse afin d'obtenir l'image marquée. Il est intéressant de noter que le fait de modifier uniquement la sous-bande HH (hautes fréquences) n'entraine pas de dégradations visibles.

Le processus d'authentification consiste alors à effectuer la même décomposition que lors de la phase d'insertion, puis à corréler la sous-bande HH obtenue avec le bruit pseudo-aléatoire. Si l'image n'a subi aucune manipulation, le résultat du test ressemblera à une matrice de points uniformément répartis. Dans le cas contraire, la distribution perdra son caractère uniforme dans les régions où l'image a été manipulée. Les auteurs font remarquer que cette méthode est « perméable » à certaines manipulations telles qu'un flou ou un rehaussement des contours, dans la mesure où les changements ne sont pas trop importants.

On distingue deux types de transformées en ondelettes suivant que le sous-groupe est discret ou continu.

III.4.1 Transformée en ondelettes continue

Analyser une fonction de carré sommable en ondelettes consiste à calculer l'ensemble de ses produits scalaires avec les ondelettes de la famille. Les nombres obtenus sont appelés coefficients d'ondelettes, et l'opération associant à une fonction ses coefficients d'ondelettes est appelée transformée en ondelettes.

On définit ainsi la transformée en ondelette continue d'une fonction $f \in L^2(\mathbb{R})$ par :

$$g(s,\tau) = \int_{-\infty}^{\infty} f(t)\psi_{s,\tau}(t)^* \, dt \qquad \text{(III.2)}$$

Où $\psi_{s,\tau}$ est une ondelette de la famille d'ondelettes, $*$ désigne le complexe conjugué, τ est le facteur de translation et s le facteur de dilatation.

Pour retrouver le signal f d'origine on utilise la transformée en ondelette continue donnée par :

$$f(t) = \frac{1}{C}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{1}{|s|^2} g(s,\tau)\psi_{s,\tau}(t) ds \, d\tau \qquad \text{(III.3)}$$

Où

$$C = \int_{-\infty}^{\infty} \frac{|\hat{\Psi}(\omega)|^2}{|\omega|} d\omega \qquad \text{(III.4)}$$

$\hat{\Psi}$ Étant la transformée de Fourier de l'ondelette mère Ψ.

III.4.2 Transformée en ondelettes discrète

On peut adapter la transformée en ondelettes dans le cas où l'on se trouve dans un ensemble discret. Cette technique est notamment utilisée dans la compression de données numériques avec ou sans perte. La compression est réalisée par approximations successives de l'information initiale du plus grossier au plus fin. On réduit alors la taille de l'information en choisissant un niveau de détail.

Il s'agit alors d'échantillonner s sur une échelle dyadique et τ. On écrit alors :

$$\psi_{m,n}[t] = s_0^{-m/2}\psi(s_0^{-m}t - n\tau_0). \qquad \text{(III.5)}$$

Où s_0 et τ_0 sont des constantes.

On définit ainsi la transformée en ondelettes discrète :

$$g[t] = \sum_{m\in\mathbb{Z}} \sum_{n\in\mathbb{Z}} \langle x, \psi_{m,n} \rangle \cdot \psi_{m,n}[t] \qquad \text{(III.6)}$$

III.4.3 L'Analyse multirésolution (AMR)

L'AMR d'un signal revient à le décomposer à différentes échelles, en approximations et en détails. Les espaces de projection 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 :

$$a_x(j,k) = \int_R x(t)\, 2^{-j/2} \varphi(2^{-j}(t-k))\, dt = \int_R x(t)\, \varphi_{j,k}(t)\, dt \qquad \text{(III.7)}$$

$$d_x(j,k) = \int_R x(t)\, 2^{-j/2} \psi(2^{-j}(t-k))\, dt = \int_R x(t)\, \psi_{j,k}(t)\, dt \qquad \text{(III.8)}$$

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* et *g* sont liés à ψ et φ par les deux relations suivantes :

$$\varphi(\frac{t}{2}) = g * \varphi(t) \qquad \text{(III.9)}$$

$$\psi(\frac{t}{2}) = h * \varphi(t) \qquad \text{(III.10)}$$

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

$$A_j = \sum_k a_x(j,k)\, \phi^*_{j,k}(t) \qquad \text{(III.11)}$$

$$D_j = \sum_k d_x(j,k)\, \psi^*_{j,k}(t) \qquad \text{(III.12)}$$

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

$$A_j = A_{j+1} + D_{j+1} \qquad \text{(III.13)}$$

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 :

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \qquad \text{(III.14)}$$

Les algorithmes que nous proposons utilisent la décomposition multirésolution basée sur l'ondelette de Haar.

III.4.4 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 III.1 montre la décomposition pyramidale résultante de l'image 'Doaa.bmp'. On obtient pour un niveau de décomposition j une imagette d'approximations $I^{LL}(m, n)$: (filtrage passe-bas lignes et colonnes) et trois imagettes de détails, $I^{HL}(m, n)$ (filtrage passe-haut lignes et passe-bas colonnes), $I^{LH}(m, n)$ (filtrage passe-bas lignes et passe-haut colonnes) et I^{HH} (m, n) (filtrage passe-haut lignes et colonnes) selon l'orientation fréquentielle horizontale, verticale et diagonale.

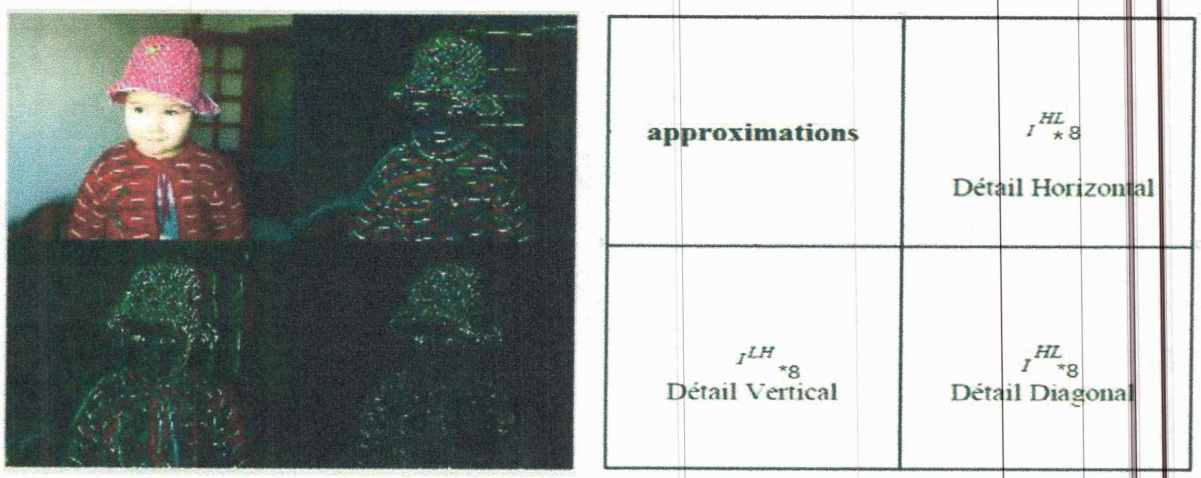


Figure III.1 Décomposition pyramidale en première niveau de l'image 'Doaa.bmp'.

III.5 Choix du domaine transformé

Les coefficients d'un paquet d'ondelettes correspondent à la contribution dans l'image de composantes fréquentielles prises à une certaine résolution. Dans un nœud donné, les coefficients représentent donc le comportement de toute l'image à la résolution et dans la bande de fréquence fixée par le nœud. Modifier un paquet d'ondelettes nous assurera donc la répartition de l'information de la marque sur toute l'image. La répartition fréquentielle des modifications se fera naturellement en sélectionnant plusieurs paquets. Une contrainte issue de la robustesse du schéma impose que les composantes choisies pour porter la marque doivent être perceptuellement significatives, ce qui signifie, pour notre méthode, que la construction de la base doit être motivée par ce critère : la meilleure base doit être composée de paquets représentant des contributions significatives de l'image. La dernière contrainte rappelée ci-dessus nous incite à construire une base possédant une structure riche, nous permettant d'obtenir un grand nombre de paquets.

III.5.1 Introduction sur la transformation de Haar

La transformation de Haar est l'une des transformations les plus simples en mathématiques ondelettes. Elle utilise des impulsions carrées pour rapprocher la fonction d'origine. Les fonctions de base pour les ondelettes de Haar à un certain niveau tous ressemblent à une impulsion unité déplacée le long de l'axe x. Elles sont appelés échelles dans la terminologie ondelettes.

Bien que cette définition est en fait assez simple en termes des équations abstraites qui viennent sur le moment où l'étude des transformations en ondelettes, Pour cet article, nous ignorons la définition formelle des transformations de Haar et les propriétés qu'ils fournissent. Au lieu de cela, nous montrons comment mettre en œuvre la transformation de Haar, et comment nous proposons de l'utiliser pour la stéganographie [35].

III.5.1.1 La transformée 1D de Haar

La transformée de Haar 1D fonctionne sur un ensemble de quatre pixels. La transformation d'un ensemble de pixels :

a	b	c	d	➡	A= (e + f)/2	B= (e - f)/2	C= (a - b)/2	D= (c - d)/2

Où $c = (a + b)/2$

et $f = (c + d)/2$

La transformation inverse est :

A + B + C	A + B - C	A - B + D	A + B - D

En généralisant à deux dimensions, nous prenons la transformée à 1D de Haar d'abord le long des lignes, puis même chose le long des colonnes de l'image. Si la largeur ou la hauteur ne sont pas des multiples de 4, alors, les frontières sont ignorées dans la transformation.

III.5.1.2 La transformée 2D de Haar à 2 niveau

La transformée 2D de Haar fonctionne aussi sur un ensemble de 4 pixels, mais est considéré comme 2D, car il y a un traitement supplémentaire sur un bloc de 2x2 après avoir terminé les transformations lignes et colonnes initiales. Donc la transformation 1D est généralisée à deux dimensions. De plus, après que le calcul soit terminé.

a	b	c	d	➡	A= (a + b)/2	B= (c - d)/2	C= (a - b)/2	D= (c - d)/2

e	f	➡	E= (a + b)/2	F= (a – b)/2

Le même calcul est fait pour la deuxième ligne de pixels, et ensuite à nouveau pour chaque colonne de ce bloc 2x2.

L'inverse est tout d'abord calculé pour chaque groupe de 4x4 pixels. Pour ce faire, nous prenons l'inverse pour les deux premières colonnes dans le bloc 2x2, puis prendre l'inverse pour les deux premières lignes dans le bloc 2x2. L'inverse est : Pour le E et F ci-dessus.

E+F	E-F

Enfin, l'inverse est prise pour chaque groupe de quatre pixels ; d'abord par des colonnes, puis par lignes, comme suit : Pour A, B, C et D ci-dessus.

A + C	A - C	B + D	B - D

IV.1 Introduction

La dissimulation de données dans les images numériques connait un intérêt croissant. L'application envisagée dans notre cas est de modifier imperceptiblement les données des images de façon à véhiculer secrètement une information. L'espace d'insertion engendré par la transformée en ondelettes parait adéquat, car l'exploitation des propriétés de la décomposition multirésolution permet une meilleur maniabilité des bandes susceptible d'abriter la marque

IV.2 Propriétés et avantages de la décomposition en ondelettes

Le choix des ondelettes pour la stéganographie est motivé par plusieurs facteurs ; on note essentiellement :

- ✓ Les recherches sur le système visuel humain (SVH) montrent que la rétine découpe une image en plusieurs canaux de fréquences d'une largeur de bande d'approximativement une octave chacune. Les signaux dans ces différents canaux sont traités indépendamment. De même, dans une décomposition multirésolution l'image est séparée en bandes de largeurs approximativement égales dans une échelle logarithmique. Par conséquent, il est estimé que l'utilisation de la transformée discrète en ondelettes (TOD) va permettre le traitement des composantes résultantes d'une manière indépendante sans interaction significativement perceptible entre eux. La représentation multirésolution permet ainsi le décodage séquentiel d'une basse résolution vers une haute résolution.
- ✓ Les dégradations introduites par codage dans le domaine des ondelettes sont moins prononcés que celles introduites par la TCD (compression JPEG) à des taux de compression égaux. De plus l'effet de blocs est clairement visible à des taux de compression JPEG élevés, car le codage est basé sur la TCD opérant indépendamment sur des blocs 8*8.
- ✓ La transformée en ondelette génère une structure de données connue sous une représentation échelle-espace. Les hautes fréquences du signal sont localisées précisément dans le domaine des pixels, alors que les basses fréquences sont localisées dans le domaine fréquentiel. La résolution spatiale de la transformée en ondelette augmente avec la fréquence. Donc, les contours aigus qui sont localisés spatialement, et qui ont un contenu haut fréquence important peuvent être vus dans les sous bandes de détail, et forment les contours des objets de l'image. Alors que la

résolution fréquentielle est indépendante de la fréquence dans le domaine de la TCD, elle est inversement proportionnelle à la fréquence dans le domaine des ondelettes.

- ✓ La représentation hiérarchique de l'image due à la caractéristique multirésolution de la transformée est particulièrement souhaitable pour l'application où l'image est transmise progressivement, lorsque de grandes quantités de données doivent être traitées, comme pour les applications vidéo ou pour les systèmes en temps réel.
- ✓ Comme expliqué plus haut, la haute résolution des sous bandes permet de localiser plus facilement des caractéristiques de l'image comme les contours et les zones texturées. Les schémas de stéganographie posent souvent la marque dans les coefficients les plus grands de la TOD, donc affectant principalement les régions, comme les contours et les textures, où le SVH et moins sensible.
- ✓ Le standard de compression et de codage le JPEG2000 est basé sur la TOD.

Ces propriétés importantes de la TOD nous ont encouragés à aborder la stéganographie dans le domaine des ondelettes. Nous allons présenter l'algorithme implémenté pour l'expérimentation.

IV.3 La méthode proposée

Dans notre travail, nous avons choisi comme domaine d'insertion le domaine de la transformée en ondelettes pour abriter le message secret.

L'algorithme global est décrit ci-dessous :

IV.3.1 Description de l'algorithme

On s'est proposé de cacher l'image dans l'image où une image secrète dans une image couverture n'attirant pas l'attention.

Le schéma appliqué se divise en deux phases : la phase d'insertion et la phase de sa détection.

Au niveau de la phase d'insertion, l'image couverture originale est transformée par décomposition en premier niveau (niveau 1) d'ondelette 2D de Haar, puis nous conditionnons l'image secrète en la redimensionnant de sort que le nombre de pixels de l'image secrète redimensionnée est égale au nombre de pixels de l'image originale, de la même façon ensuite, on effectue la transformation en ondelettes 2D de Haar de l'image secrète. Les détails de la transformée de l'image originale vont abriter l'approximation de l'image secrète. Pour se faire, on s'est proposé de cacher les coefficients de l'approximation dans les grands coefficients des détails de l'image couverture, car les grands coefficients des détails correspondent aux contours

et textures ou les petites modifications seront imperceptibles. On trie ces coefficients en ordre décroissant et en les modifiant suivant une fonction d'insertion de telle sorte à porter l'approximation de l'image secrète (en utilisons leurs indexes dans les détails). La Figure IV.1 représente la phase d'insertion d'image secrète.

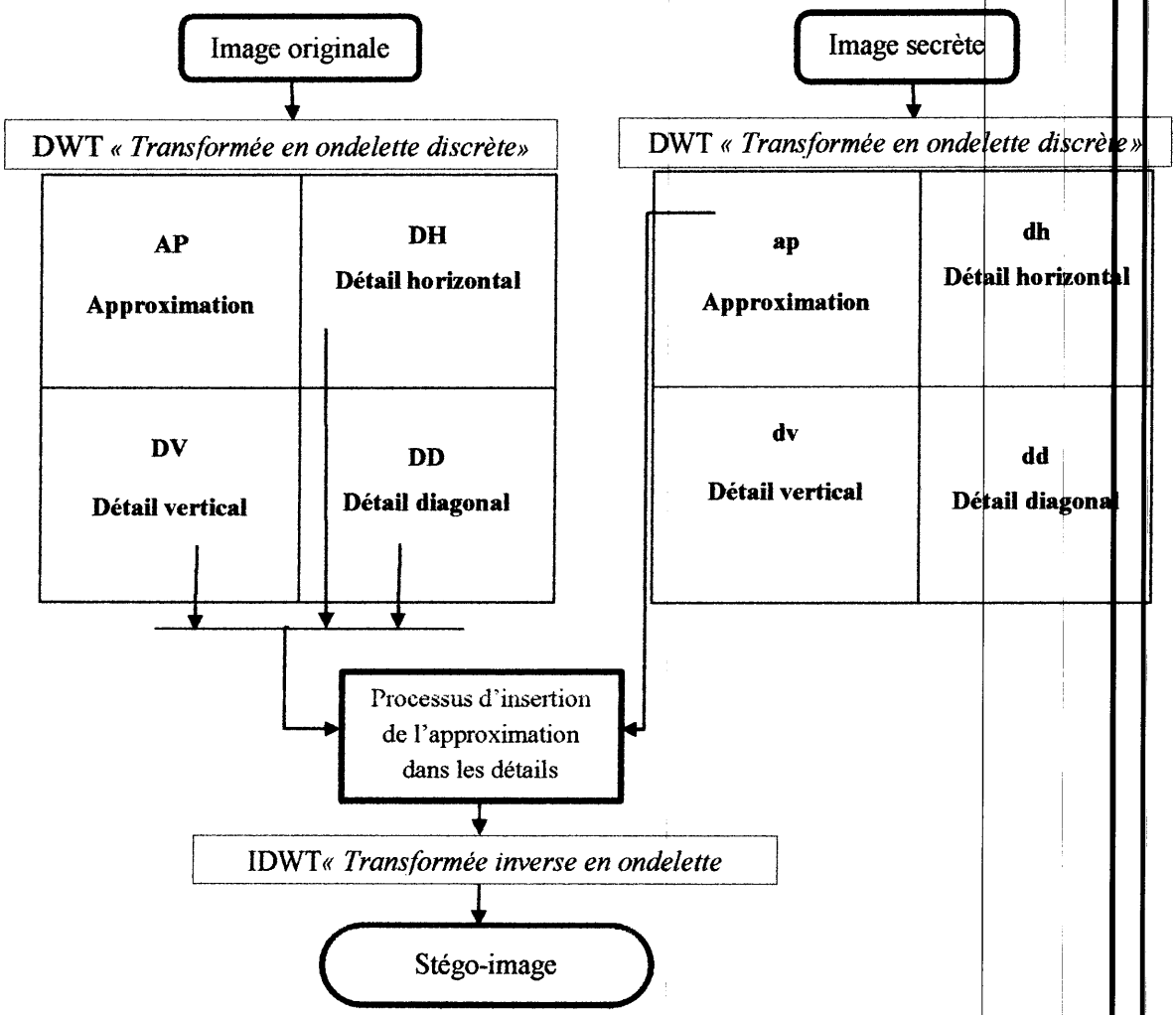


Figure IV.1. Schéma représentant la phase d'insertion d'image secrète.

On a testé dans la partie expérimentale les deux algorithmes d'insertion additif et substitutif suivants :

$$y_i = y_{io} + \alpha w_i \qquad \text{(IV.1)}$$

$$y_i = \alpha w_i \qquad \text{(IV.2)}$$

(IV.1) c'est la fonction d'insertion additive.

(IV.2) c'est la fonction d'insertion substitutive.

Où

- y_i : est le coefficient de stégo-image.
- y_{io} : est le coefficient élu pour porter l'image secrète.
- α : facteur de pondération.
- w_i : est l'élément de l'image à insérer.

Les nouveaux coefficients du stégo-objet sont donnés par les équations (IV.1) et (IV.2). Le stégo-image est reconstruite par la transformée inverse 2D de Haar.

Connaissant l'algorithme et la méthode d'insertion, le récepteur du stégo-image va tenter d'extraire l'approximation de l'image secrète. On suppose qu'on est dans le cas d'un schéma de détection non-aveugle, où le récepteur possède l'image couverture originale mais pas l'image secrète. Donc, il transforme le stégo-image et l'image couverture originale en ondelettes 2D de Haar. Comme les coefficients de l'approximation de l'image secrète sont éparpillés sur les grands coefficients triés en ordre décroissants de détails. Il doit recalculer les indexes des grands coefficients triés à partir de l'image couverture originale pour pouvoir retrouver les emplacements originaux dans l'image secrète. Les coefficients « différence » après soustraction des deux images transformées seront ainsi correctement rangés et représentent l'approximation de l'image secrète récupérée. Notez que les indexes des coefficients peuvent jouer le rôle d'une clef secrète.

Il est possible que le stégo-image transitant sur un canal de communication entre l'émetteur et le récepteur soit attaqué « modifié ». On a simulé quelques attaques pour évaluer la robustesse de l'algorithme. Le schéma de détection reste le même avec ou sans attaque. La Figure IV.2 représente la phase de détection d'image secrète.

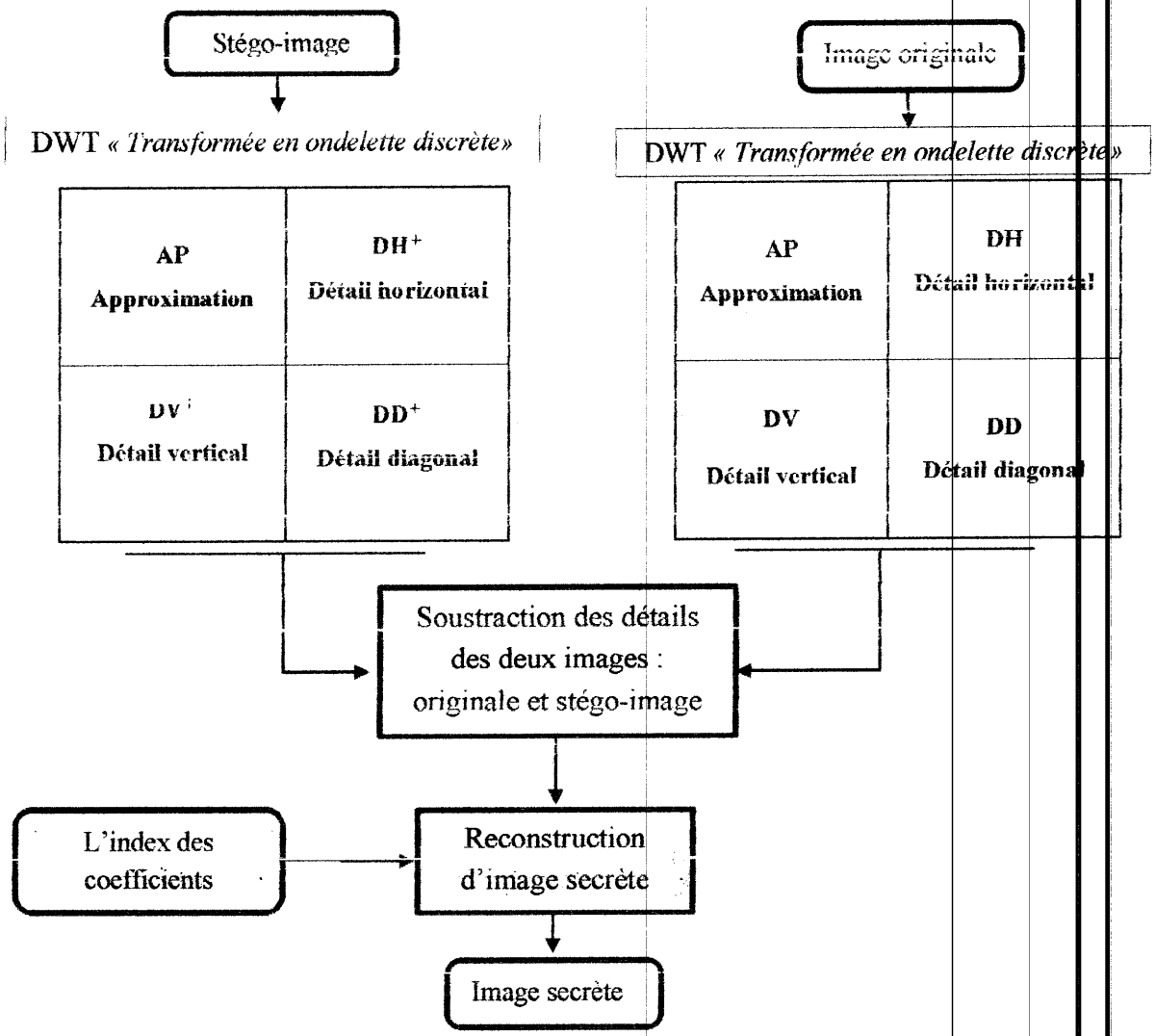


Figure IV.2. Schéma représentant la phase de détection d'image secrète.

IV.4 Moyens d'évaluation

IV.4.1 Le MSE (Mean Square Error)

La modification de l'image soit par l'insertion de la signature ou/et après une attaque dégrade la qualité de l'image. Le MSE est une métrique utilisée pour estimer cette perte d'information.

$$MSE = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left(I_{ij} - I_{ij}^{*}\right)^2}{nm} \qquad \text{(IV.3)}$$

I et I* sont respectivement l'image originale et stégo-image de taille (m×n) avec Iij et Iij* leurs composantes.

IV.5 Outils d'évaluation

IV.5.1 Le PSNR (Peak Signal to Noise Ratio)

La mesure de distorsion la plus fréquemment utilisée en traitement d'images est le PSNR (Peak Signal to Noise Ratio). En fait, le PSNR n'est rien d'autre qu'une conversion du MSE en dB.

$$\mathrm{PSNR} = 10\log10\,(\mathrm{Xmax}^2/\mathrm{MSE}) = 10\log10\,(255^2/\mathrm{MSE}) \qquad \text{(IV.4)}$$

Avec Xmax est la plus grande luminance des pixels de l'image.

IV.6 Résultats de simulation

Dans la partie expérimentale, l'approche proposée a été appliquée sur les images 'Nature.bmp' (640x460) figure IV.3 et l'image 'Doaa.JPG' (640x480) figure IV.4. Les images secrètes sont : le logo utilisé actuellement dans les correspondances internes de l'université de Jijel 'Logo-univ-Jijel. JPG (191x180) figure IV.5. L'image du drone 'avion sans pilote.JPG' (300x200) figure IV.6 sur internet a été aussi utilisée comme image secrète.

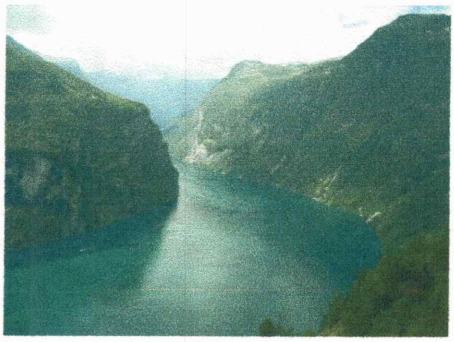


Figure IV.3 'Nature.bmp' (680x460)

Figure IV.4 'Doaa.JPG' (640x480)

Figure IV.5 'Logo-univ-Jijel.JPG' (191x180)

figure IV.6 'Avion sans pilote.JPG' (300x200)

La taille de l'image 'Logo_univ_Jijel' sera ajustée (redimensionnée) automatiquement de sorte qu'elle sera proprement contenue dans l'image importante ; sa nouvelle taille sera (680x460). L'image secrète redimensionnée est montrée dans la figure IV.7.

Figure IV.7 'Logo-univ-Jijel.JPG' (680x460)

Pour évaluer les performances de notre approche, nous avons procédé à une étude comparative entre deux schémas d'insertion : additif et substitutif.

IV.6.1 Insertion additive

a) Distorsions introduites par l'insertion de la marque

Nous allons appliquer le programme sur deux images couverture « Nature.bmp » et « Doaa.JPG » qui sont des images originales innocentes et « Logo-univ-Jijel.JPG » et « Avion sans pilote.JPG » comme images secrètes.

Cependant, pour mettre en évidence la décomposition et l'insertion et leur influence sur les images originales on va présenter un exemple où on a divisé l'approximation de l'image secrète redimensionnée verticalement en trois parties *égales.* Dans chaque détail est insérée une subdivision. En prenant en premier lieu un facteur de pondération $\alpha = 0.01$, le processus d'insertion et la différence entre l'image originale et stégo-image sont illustrés ci-dessous :

a.1. Cacher Logo-univ-Jijel dans l'image Nature

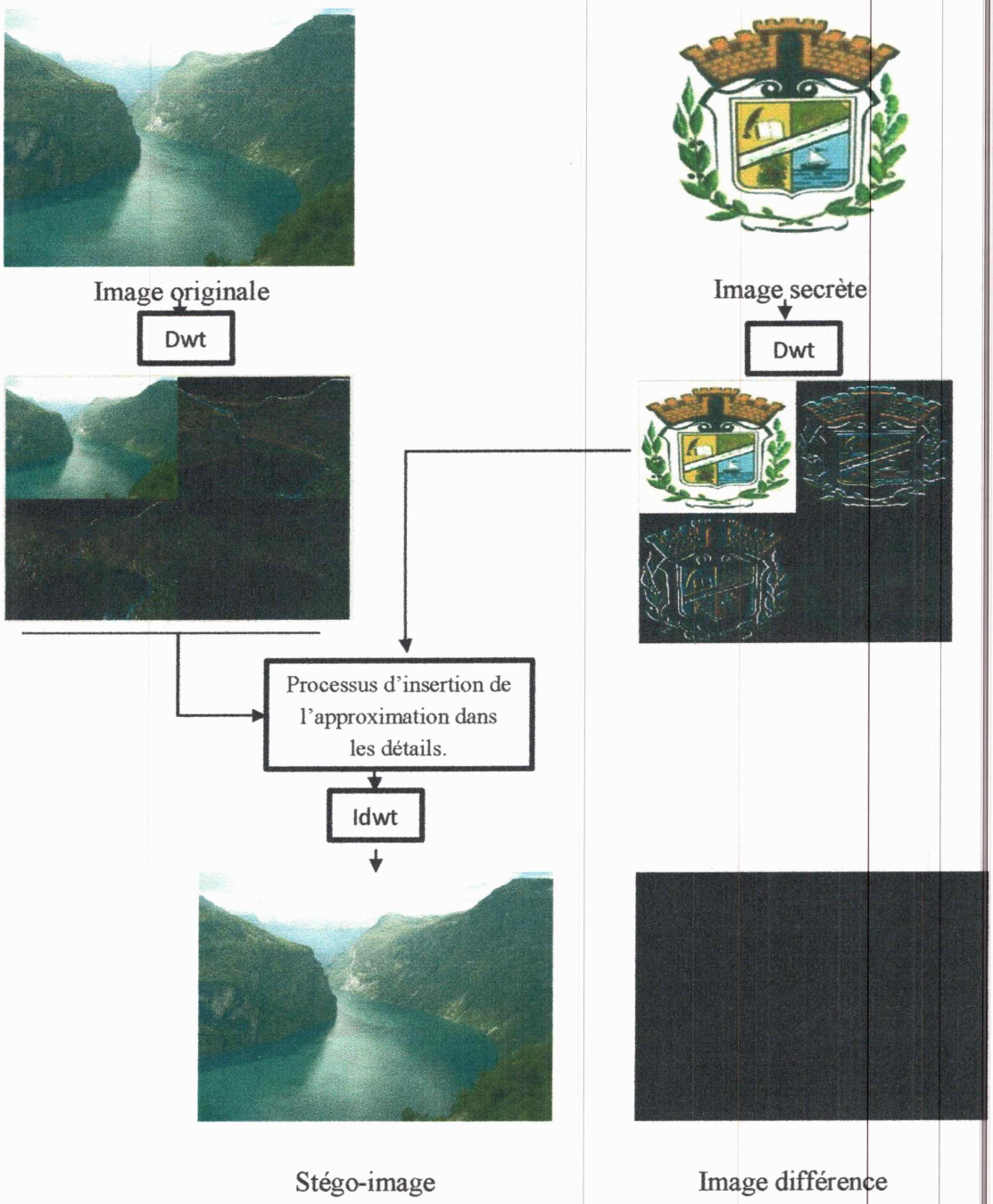


Figure IV.8 Processus d'insertion et différence entre image originale et stégo-image (PSNR égal à 44.89dB).

On peut remarquer que dans ce cas d'insertion additive sans attaques que la différence est imperceptible, et le PSNR avec $\alpha = 0.01$ est élevé (44.89dB).

b) Processus de détection de la marque en absence d'attaques

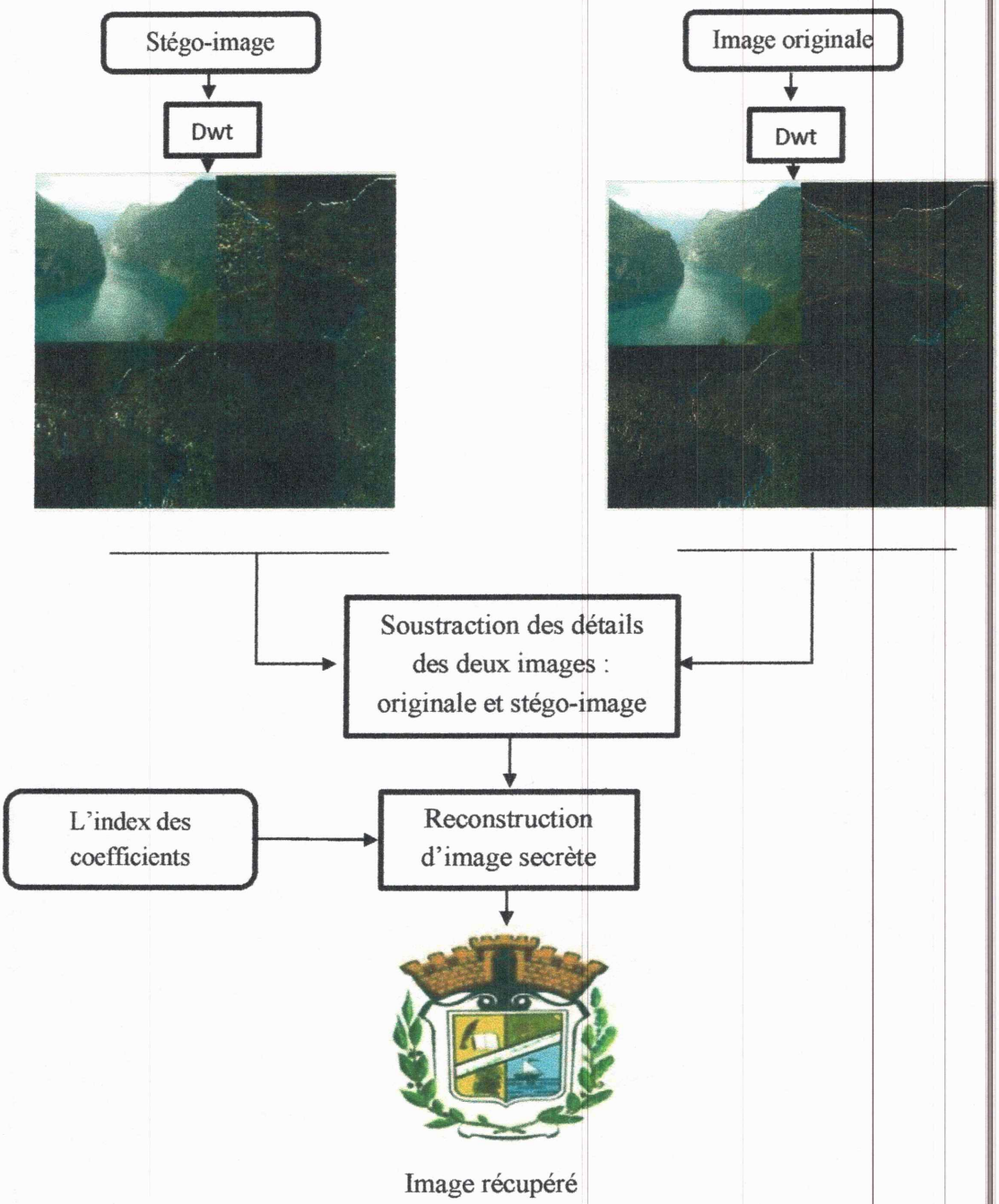


Figure IV.10 Schéma représentant la phase de détection de l'image secrète.

La marque «l'approximation de l'image secrète » est proprement récupérée dans le cas sans attaque. On a appliqué le même processus de détection sur le stégo-image Doaa et on a pu récupérer proprement l'image « Avion sans pilote ».

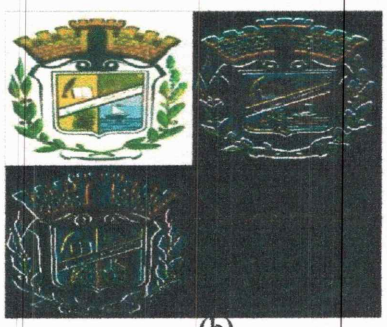
IV.6.2 Insertion substitutive

a) Distorsions introduites par l'insertion de la marque

On a pris pour cet exemple l'image couverture Nature et l'image secrète Logo-univ-Jijel avec le même facteur de pondération $\alpha = 0.01$ comme illustré ci-dessous :

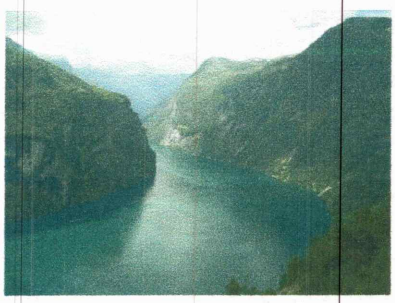
a.1. Cacher Logo-univ-Jijel dans l'image Nature

(a)

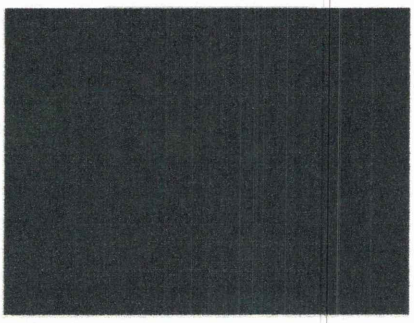


(b)

(c)



(d)



(e)

Figure IV.11 Insertion substitutive dans les coefficients d'ondelettes (a) Décomposition de l'image originale (b) Décomposition de l'image secrète, (c) Image original, (d) Stégo-image résultante, (e) Différence entre l'image original et stégo-image.

On remarque aussi que dans ce cas d'insertion substitutive avec α=0.01 la dégradation du stégo-image est imperceptible. Alors qu'ici on peut difficilement voir dans l'image différence (e) un relief du contour. Le PSNR a subit une très faible dégradation (41.63dB).

a.2. Cacher Avion sans pilote dans l'image de Doaa

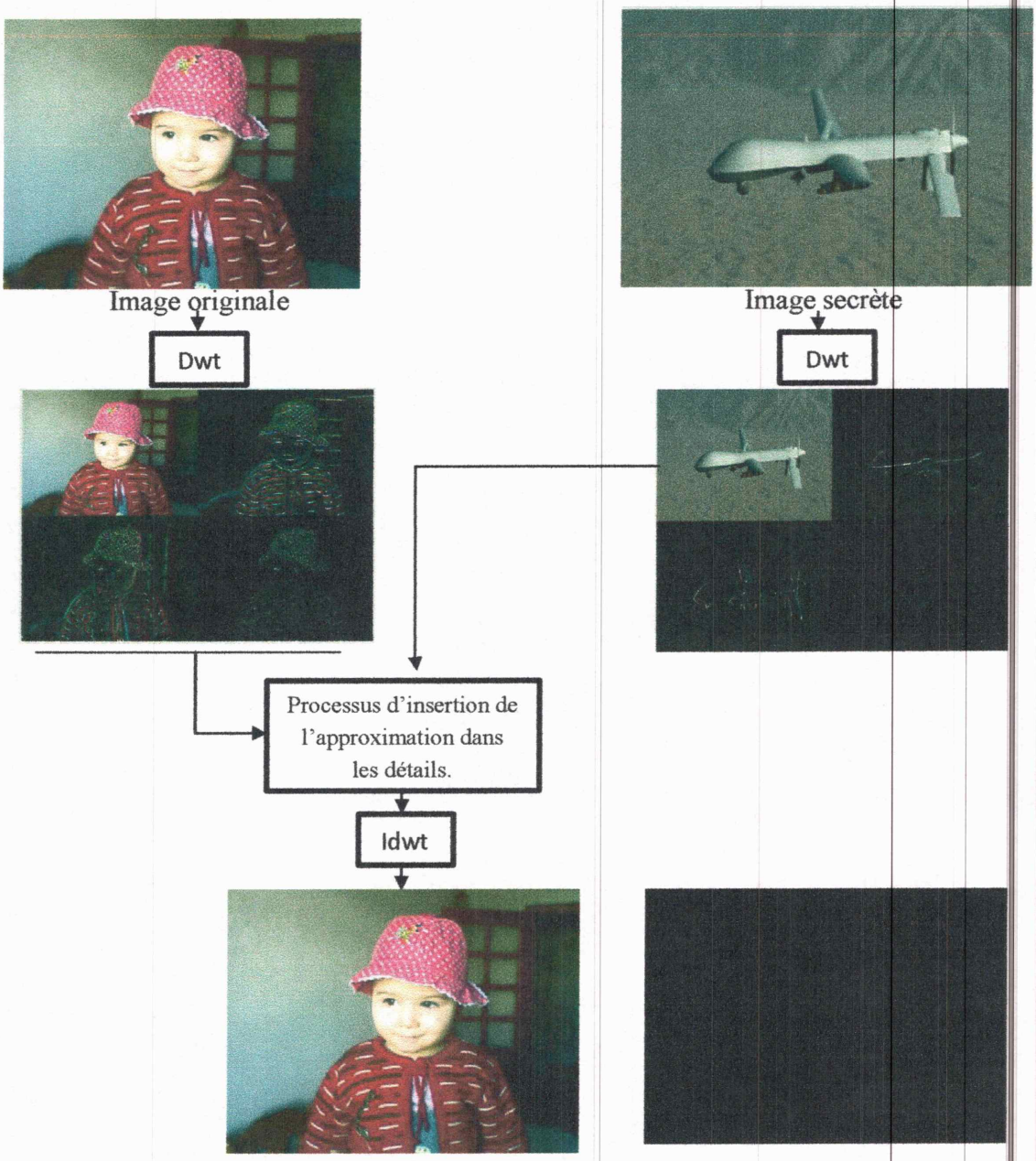
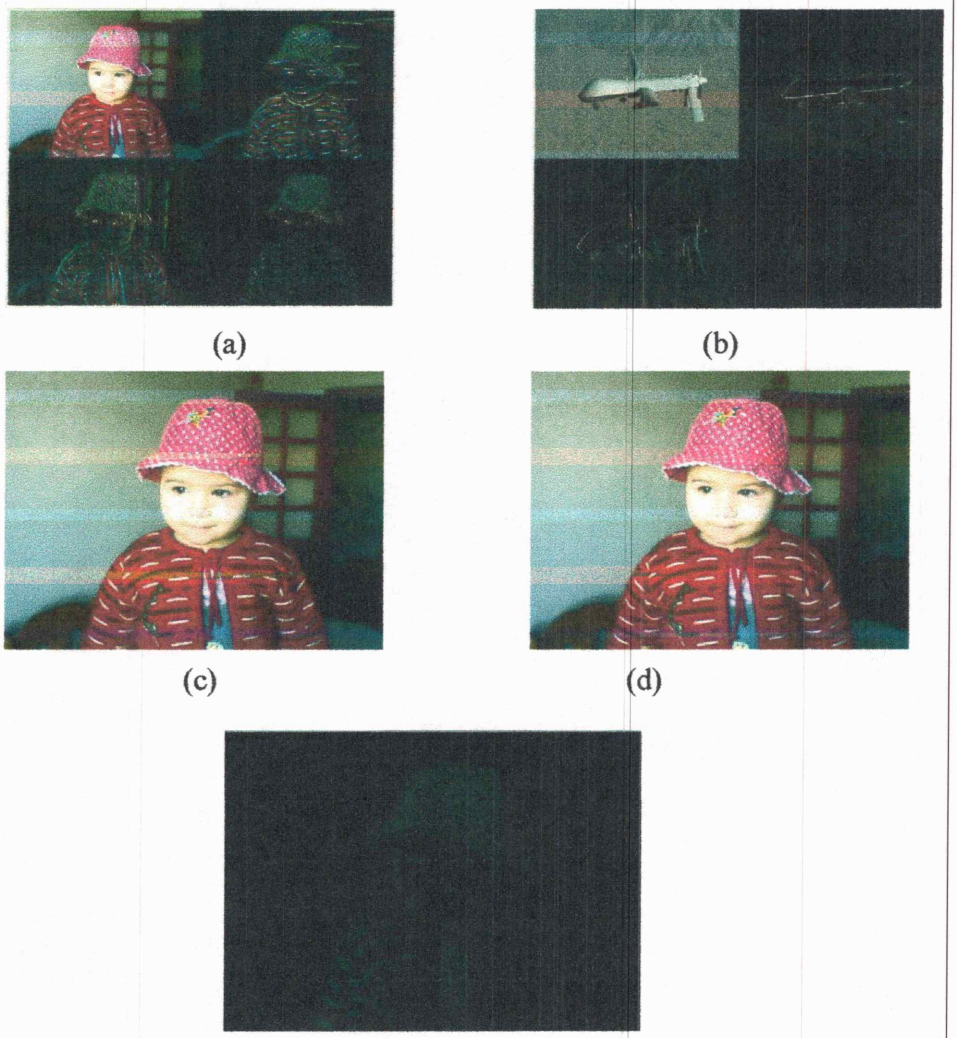


Figure IV.9 Processus d'insertion et différence entre image originale et stégo-image (PSNR égal à 51.04 dB).

On remarque aussi ici que la différence est toujours imperceptible avec un PSNR élevé.

a.2. Cacher Avion sans pilote dans l'image de Doaa



(a) (b)

(c) (d)

(e)

Figure IV.12 Insertion substitutive dans les coefficients d'ondelettes (a) Décomposition de l'image originale (b) Décomposition de l'image secrète, (c) Image original, (d) Stégo-image résultante (e) Différence entre l'image original et stégo-image.

On remarque toujours, avec α=0.01, la dégradation du stégo-image est imperceptible. La différence entre le stégo-image et l'image couverture est à peine visible dans les régions texturées. Le PSNR est aussi ici plus faible que celui pour le schéma additif (40.11dB).

b) Processus de détection de la marque en absence d'attaques

On calcule la différence des détails des deux images transformées stégo-image et couverture.

On calcule les indexes des grands coefficients d'ondelettes des détails à partir de l'image couverture pour pouvoir arranger les coefficients différence et reconstruire l'approximation de l'image secrète.

(a)

(b)

(c)

Figure IV.13 Extraction de la marque en absence d'attaques (a) Décomposition du stégo-image (b) Décomposition d'image originale (c) Image secrète récupéré.

L'approximation de l'image secrète est proprement récupérée dans le cas sans attaque. On a appliqué le même processus de détection sur le stégo-image Doaa et on a pu récupérer proprement l'image « Avion sans pilote ».

Dans la phase d'insertion et à partir des deux méthodes précédentes. Nous remarquons que le système visuel humain (mesure subjective) distingue pas la différence engendrée par le marquage, alors qu'on réalité il y a des différences entre ces deux méthodes (PSNR mesure objective).

IV.6.3 Simulation d'attaques

Nous avons considéré trois types d'attaques : la compression JPEG considéré comme un traitement innocent et introduction de bruits (traitement malveillant) « gaussien » et « Salt and Pepper ».

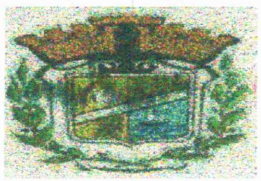
a) **Influence de la compression JPEG**

On a appliqué la compression JPEG sur les deux stégo-images 'Nature.bmp', 'Doaa.bmp'. la taille de ces images successivement (916 Ko, 900 Ko) avec différents facteurs de qualité Q (50, 70,100). Le tableau suivant représente le PSNR et la taille correspondant aux différents facteurs de qualité.

le facteur de qualité avec (PSNR et la taille) correspondant / Image	Q=50		Q=70		Q=100	
	PSNR (dB)	taille Ko	PSNR (dB)	taille Ko	PSNR (dB)	taille Ko
Image Nature	37.73	22.6	38.61	32.6	47.33	232
Image Doaa	35.76	25.1	36.65	35.2	43.32	208

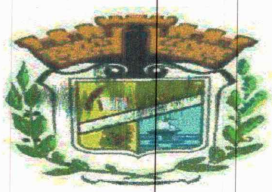
Tableau IV.1 Mesure objective de distorsion introduite par la compression JPEG.

Le PSNR de l'approximation de l'image secrète récupérée (Logo-univ-Jijel) après la compression JPEG avec différents facteurs de qualité est présentée dans la figure suivante :



PSNR=28.21dB pour (Q=50)

PSNR=33.58dB pour (Q=70)



PSNR=37.09dB pour (Q=100)

Figure IV.14 Représente le PSNR de l'approximation de l'image secrète récupérée après la compression JPEG avec différents facteurs de qualité.

Le tableau et les figures obtenues montrent l'influence de la compression JPEG sur les images secrètes extraites.

b) **Influence du bruit de type 'Salt and Pepper'**

On a appliqué un bruit de type **Salt and Pepper** avec une densité de bruit égale **0.05** sur les deux images 'image Nature' et 'image Doaa', les PSNR en dB sont montrés dans la suivantes :

Stégo-image après l'attaque

Avec PSNR= 38.92 dB

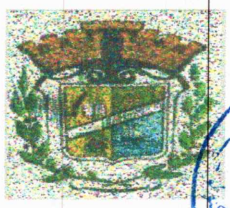


image secrète récupérée

avec PSNR= 29.05dB

Stégo-image après l'attaque

Avec PSNR= 40.52 dB

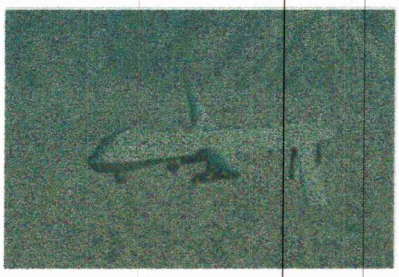


image secrète récupérée

avec PSNR= 26.90dB

Les images représentent l'influence du bruit 'Salt and Pepper' sur le stégo-image et l'image secrète extraite.

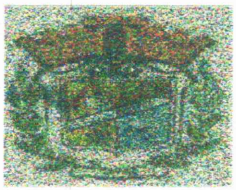
c) **Influence du bruit de type 'gaussien'**

On a appliqué un bruit gaussien de variance de 0.001, 0.002 et 0.003 et de moyenne nulle sur les deux images 'Nature' et 'Doaa'. les résultats PSNR en dB sont présentés dans le tableau suivant :

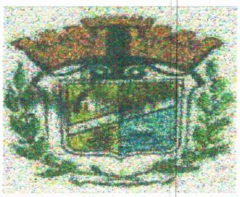
le bruit et PSNR qui convient / image	0.001	0.002	0.003
	PSNR (dB)	PSNR (dB)	PSNR (dB)
Image Nature	33.16	31.29	30.44
Image Doaa	34.01	32.03	31.16

Tableau IV.2 L'influence de bruit gaussien au stégo-image.

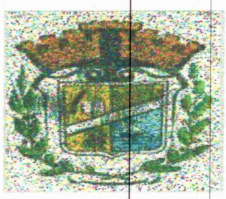
Le PSNR de l'approximation de l'image secrète récupérée (Logo-univ-Jijel) après là l'application de bruit de type gaussien avec différents variances est présentée dans la figure suivante :



PSNR=27.24dB
pour (v=0.003)



PSNR=29.12dB
pour (v=0.002)



PSNR=32.09dB
pour (v=0.001)

Figure IV.15 Représente le PSNR de l'approximation de l'image secrète récupérée après là l'application de bruit gaussien avec différents variances.

Les figures montrent l'influence du bruit gaussien sur les images secrètes extraites.

IV.7 Conclusion

Ce chapitre a montré que la communication invisible est possible dans l'ère informatique. Presque tout message possède le potentiel d'être une couverture pour les communications secrètes ; la composante de bruit (détail) des images numériques ou son numérique peut être modifiée.

Dans notre travail, les deux méthodes d'insertion additive et substitutive sont opérantes dans le domaine des ondelettes. L'une des méthodes donne de meilleurs résultats que l'autre c'est la méthode additive par quantification des coefficients de la transformée en ondelettes discrète. L'image originale est nécessaire pour l'étape d'extraction du stégo-image (stéganographie non aveugle). Les résultats montrent une robustesse de l'algorithme envers une variété de techniques de distorsion des images.

La distorsion introduite par l'insertion de la marque dans l'image originale n'est pas visible, soutenue par le choix des coefficients significatifs des sous bandent pour l'insertion de la marque, qui localise la position de la marque dans les contours et les textures de l'image, où l'œil humain est moins sensible.

Conclusion générale

Conclusion générale

Nous avons introduit ce travail en présentant et en définissant les objectifs stéganographiques d'images numériques. Nous avons passé un aperçu sur les différents moyens de dissimulation de l'information, en particulier dans un support multimédia. Différentes applications de dissimulation de l'information et les différentes propriétés requises pour chaque application ont été introduites.

Nous avons alors présenté la méthode implémentée dans ce projet. Elle consiste à représenter une image par une structure d'ondelettes. La marque sera implémentée en déformant cette structure. La transformée en ondelettes possède des propriétés inhérentes qui font d'elle un espace d'insertion attrayant. Pour respecter le cahier des charges, en particulier l'imperceptibilité de l'insertion sur le stégo-image, nous avons introduit la marque dans les grands coefficients des détails de la DWT et aucune dégradation perceptible n'a été constatée pour de petits facteurs de pondération α=0.01.

Nous avons simulé quelques types d'attaque sur le stégo-objet pour évaluer la robustesse de l'algorithme. On a pu récupérer l'image secrète dans tous les cas de figure, et la déformation subite par l'image secrète peut donner une indication sur le type d'attaque impliqué. Néanmoins, on n'a pas simulé les attaques géométriques dans notre travail.

Comme perspectives ouvertes par ce travail on peut envisager d'utiliser des ondelettes non-séparables, dont l'utilisation n'induit pas d'orientation particulière. A l'inverse, choisir des ondelettes dérivant des filtres proches de ceux utilisés par les modèles du SVH, nous permettrait une meilleure approche du compromis invisibilité/robustesse. On peut aussi envisager de calculer directement le masque psychovisuel dans le domaine des paquets d'ondelettes.

Une autre extension de ce travail concerne l'introduction d'une clef privée pour crypter encore le message secret. L'intérêt est d'ajouter un autre niveau de sécurité. Enfin, on peut envisager d'adapter la méthode de utilisée pour d'autres supports que les images fixes.

Bibliographie

Bibliographie

[1] Kimberly Kiefer et al, "*Information Security : A Legal, Business and Technical Handbook*", Chicago, ABA Publishing, 2004, p. 41.

[2] Stewart D. Personick et Cynthia A.Patterson, "*Critical Information Infrastructure Protection and the Law : An overview of Key Issues*", Washington, The National Academies Press, 2003, p. 46.

[3] Bruce Schneier, "*Beyond Fear*", New York, Copernicus Books, 2003, p. 12 ; Bruno Doucende, *Sécurité des Systèmes d'Information*, Livre blanc du groupe, 2004, p. 19.

[4] La disponibilité, l'intégrité et la confidentialité forment la « triade DIC » (*AIC Triad* en anglais), qui est au cœur de la notion de sécurité informationnelle. L'article 26 de la "*Loi concernant le cadre juridique des technologies de l'information*" reprend d'ailleurs ce principe en substance.

[5] Article 4.7.3 du "*Code type sur la protection des renseignements personnels*", CAN/CSA-Q830-96, annexe A à la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5.

[6] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, " Stéganographie : sécurité par dissimulation "," *Revue d'Information Scientifique et Technique*", vol. 16 n° 1, 2006, p. 102.

[7] I. Pitas and T. Kaskalis, "applying signature on digital image". In workshop on monlinear signal and image processing, page 460-463, neos Mamaras, june 1998.

[8] G.Dubertret. " Initiation à la cryptographie ".Vuibert, 1998.

[9] Patrik Bas, "Méthodes de tatouage d'image fondées sur le contenu" thèse de doctorat de l'INPG, Grenoble, 6 Octobre 2000.

[10] A. p. Petitcolas, R. J Anderson, and M. G. Kunh. Information hiding-a survery. *Proceegings of the IEEE,* 87(7) :1062-1078.

[11] "Security and Watermarking of Multimedia Contents II" de SPIE Electronics Imaging ,2328 jan 2000 -San Jose CAL. http://www.spie.org/info/ei.

[12] " IEEE Colloquium on Secure Image and Image Authentication ",10 April 2000 at IEEE Savoy Place in London –(GB). http//www.iee.org.uk/Events/e10apr00.htm.

[13] G. Dubertret. " Initiation à la cryptographie ". Vuibert, 1998.

[14] D. Kundur and D. Hatzinakos. "Digital watermarking for telltale tamper proofing and authentication ". *proceeding of the IEEE*, 87(7) :1167-1180, july 1999.

[15] M. Barni, F. Bartoloni, V. cappellini, A, lippi, and A. Piva. "A dwt-based technique for spatio-frequency masking of digital signatures". In Ping Wah wong and Edward J.delp, editors, ISBT/SPIE's 11th annual symposium, Electronic Imaging ,99 : "security and watermarking of multimédia contents", volume 3657 of spie proceedings, pages 31-39 san Jose, California USA, 23-29 January 1999.

[16] A. taleb, A. Bennia, A. Bouridane. "Adaptive Bit PlaneBased Authentication Digital warermarking". Conférence sur le genie électrique, CGE, Bordj El Bahri ,17 déc. 2002.

[17] Patrik Bas, " Méthodes de tatouage d'images fondées sur le contenu ", thèse de doctorat de L'IPG, Grenoble, octobre 2000.

[18] D. Augot, J-M. boucquereau, J-F. Delaigle,C. Fontaine, and E. Goray. "Secure delivery of image over open networks". Proceedings of the IEEE, 87(7) :1251-1266, July 1999.

[19] J.barda and E.Sigonnaud. "Spécification de systèmes pour les images fixes et animés". "Technical report", "réseau National de la recherche en télécomunication", projet Aquamars, Paris, August 1999.

[20] G. J. Simmons, Prisoners. "Problem and the Subliminal Channel (The), CRYPTO83 - Advances in Cryptology", August 22-24. 1984. pp. 51-67.

[21] N. F. Johnson, S. Katzenbeisser, "A Survey of steganographic techniques", in S. Katzenbeisser and F. Petitcolas (Eds.): *Information Hiding*, pp. 43-78. Artech House, Norwood, MA, 2000.

[22] Gustavus J. Simmons, " *The prisoner's problem and the subliminal channel* ", Plenum Press, 1983.

[23] Fabien Galand, " Construction de codes Zpk-Linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrement", thèse de doctorat en informatique, Université de Caen, 2004, p. 111.

[24] Auguste Kerckhoffs, "*La cryptographie militaire*", Journal des Sciences Militaires, 1883.

[25] Comme l'explique François Cayre, "*Les deux disciplines n'ont jamais été concurrentes, mais sont plutôt complémentaires*". François Cayre, " Cryptographie, stéganographie et tatouage : des secrets partagés ", *Interstices*, 2008.

[26] A. Ali-Pacha, N. Hadj-Saïd, A. Belgoraf et A. M'Hamed, préc. Note 11, p. 104.

[27]. J. Simmons, " The prisioner's problem and the subliminal chanel ", Plenum Press, 1983

[28] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf et A. M'Hamed, préc., note 11, p. 110.

[39].J. Barbier, préc. Note 15.

[30] Stefan Katzenbeisser. Fadien A. P. Petitcolas. " Information hiding Techniques for Steganography and Digital Watermarking ". Artech Hoose, 2000.

[31] .F. Merciol et S. Lefèvre, préc. Note 34.

[32] G. Dennis, " Theory of communication : Part 1 : The analysis of information ", *Journal of the Institute of Electrical Engineering*, London, vol. 93-3, n° 26, 1946, p. 429-457

[33] Kundur, D. & Hatzinkos, D. (1999). "Digital watermarking for tell tale tamper proofing and authentication. Proceedings", of IEEE, 87(7), pages 1167-1180.

[34] Lin, C.-Y., & Chang, S.-F. (2000). "Semi-Fragile Watermarking for Authenticating JPEG Visual Content. SPIE International Conference on Security and Watermarking of Multimedia Contents", San Jose, USA, vol. 3971, No 13, pages 140–151.

[35] Nicolaou, Alex. "A Wavelet Wading Pool" August, 1996.
http://www.cgl.uwaterloo.ca/~anicolao/wadingpool/WaveletWadingPool.html

[36] Smoot, S., and L. A. Rowe, "DCT Coefficient Distributions", in Proceedings of the SPIE 2657, Human Vision and Electronic Imaging, 1996, pp. 403–411.

[37] Machado, R., "EzStego, Stego Online, Stego", http://www.stego.com , 1997.

[38] Repp, H., "Hide4PGP", http : //www.rugeley.demon.co.uk/security/hide4pgp.zip, 1996.