**République Algérienne Démocratique et Populaire**
**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

**Université Saâd DAHLEB. Blida**

**Faculté Des Sciences de l'Ingénieur**

**Département d'Electronique**

**Option : Communication**

## MEMOIRE DE MAGISTER

**Présenté par**
**Mr. Ahmed Zohair DJEDDI**

**THEME**

# MARQUAGE DES IMAGES FIXES

**Soutenu devant les membres du jury :**

| | | | |
|---|---|---|---|
| **Président : Mr** | **M. BENSEBTI** | Maître de conférence | Université Saad DAHLEB. Blida |
| **Examinateur : Mr** | **D. BERKANI** | Professeur | E.N.P El -harrach |
| **Examinatrice : M$^{me}$** | **A. BELHADJ-AISSA** | **Professeur** | U.S.T.H.B Bab-Ezzouar |
| **Examinateur : Mr** | **N. KHORISSI** | Chargé de cours | Université Saad DAHLEB. Blida |
| **Invitée : M$^{me}$** | **A. CHERFA** | Chargée de cours | Université Saad DAHLEB. Blida |
| **Rapporteur : Mr** | **A. GUESSOUM** | Professeur | Université Saad DAHLEB. Blida |

# *Remerciements*

*Je remercie Dieu le tout puissant de m'avoir donner après tend d'années passées, après mon obtention de mon diplôme d'ingénieur, la possibilité, la force et le courage de continuer mes études et de terminer ce modeste travail.*

*Grâce à dieu j'ai eu l'honneur de rencontrer* ***M$^{er}$ GUESSOUM Abderazzak*** *qui a acceptée avec plaisir de me diriger vers ce champ de recherche et qui a accepté d'encadrer ce travail.*

***M$^{er}$ GUESSOUM A.*** *m'a beaucoup aidé pondant toutes les étapes de mon travail avec ces directives, ces conseils et ces suggestions pour lesquelles je le remercie infiniment.*

*Je remercie* ***Mr M. BENSEBTI*** *de m'avoir aider et d'avoir accepter d'être le président de mon jury.*

*Je voudrais également remercier* ***M$^{er}$ D. BERKANI*** *professeur à l' E.N.P El-harrch ,* ***M$^{me}$ A. BELHADJ- AISSA*** *professeur à l'U.S.T.H.B. Bab- Ezzouar ,* ***M$^{er}$ N. KHORISSI*** *chargé de cours à l'université Saad DAHLEB de Blida ,* ***M$^{me}$ A. CHORFA*** *chargée de cours à l'université Saad DAHLEB de Blida d'avoir bien voulu me faire l'honneur de participer à mon jury.*

*Je voudrais également remercier mes amis* ***M$^{er}$ M. BERSALI*** *et* ***M$^{er}$ M. BOUCHENAFA*** *de leurs précieuses aides et de leur fort encouragement.*

*J'aimerais aussi saluer tous mes amis et collègues de travail et les remercier pour leurs encouragements, et je souhaite à tout le monde la réussite dans leurs vies.*

*Enfin, un remerciement particulier à mon père, ma mère, ma grande sœur, mes frères, mes sœurs et tous les membres de ma famille pour leurs encouragements continus.*

# Table des matières :

# *Introduction générale :*

L'information a toujours eu un rôle primordial dans l'histoire. Son contrôle est synonyme de pouvoir et de puissance. Elle peut être des données secrètes pendant une guerre, des schémas d'un produit industriel civil ou militaire ou tout simplement les dernières actualités d'un journal télévisé.

Par le passé, les données étaient transmises par manuscrit ou tout simplement par voix, elles sont actuellement transmises par des câbles ou des ondes. Elles peuvent parcourir des milliers de kilomètres en quelques secondes. Elles sont devenues volatiles et peuvent être interceptées et /ou reproduites.

Les documents numériques multimédia sont soumis au problème de piratage lors de leur transmission d'un point à un autre (interception) ou même quand ces derniers arrivent a leur destination (duplication) et ceci peut causer des problèmes économiques non négligeables aux distributeurs des produits multi média .

Le marquage des documents, appelé en anglais **Watermarking** (traduction en français : **filigrane ou tatouage numérique**), permet d'insérer dans un document numérique une signature non perceptible qui permet de résoudre les problèmes des droits d'auteurs. Dans le contexte du copyright la signature doit être inaltérable et contient une information.

Nous nous intéressons dans le cadre de ce travail au filigrane des images numériques fixes, nous établissons un classement des différents type de marquage suivant les domaines d'insertion de la marque, les méthodes d'insertion de la marque (additives ou substitutives) ou autres critères. Nous effectuons une étude détaillée d'au moins un algorithme connu de chaque type. Cette étude, contient les procédures de dissimulation de la marque, les procédures de détection et d'extraction de la marque et la robustesse de ces algorithmes contre les différents types d'attaques. En fin, nous terminerons ce travail par une comparaison entre ces algorithmes.

Dans le premier chapitre nous allons donner le cadre juridique dans le quel le marquage des produits multimédia intervient. Nous citerons ensuite les différents domaines d'utilisation du filigrane en précisant son utilité dans chaque domaine.

Dans le deuxième chapitre nous allons citer les différents critères utilisés dans les classifications des méthodes (algorithmes) de marquage des produits multimédia. Nous continuerons par donner une classification basée sur la méthode d'insertion de la marque

(l'opération utilisée lors de l'insertion) qui peut être additive ou substitutive. Nous donnerons des exemples d'algorithmes de chaque classe.

Dans le troisième chapitre, nous allons détailler un algorithme au moins , des différentes classes citées dans le chapitre II de ce travail. Dans cette étude, l'algorithme d'insertion de la marque et l'algorithme de détection et d'extraction du message sont détaillés. Nous allons réaliser des expériences montrant la robustesse de ces algorithmes vis-à-vis des différentes attaques contres ces derniers.

Nous allons terminer ce travail par une conclusion générale qui contient une comparaison entre les différents algorithmes.

# *CHAPITRE N°1*

# *Introduction Au Marquage Des Images Fixes*

# *1.1-Utilité du marquage :*

## *1.1.1-Introduction :*

Pour assurer la protection contre la copie illégale et la protection des droits de publication des signaux audio et vidéo numériques, deux techniques complémentaires sont en développement: cryptographie et tatouage. Des techniques de cryptographie peuvent être employées pour protéger des données numériques pendant la transmission d'un expéditeur à un récepteur. Cependant, après que le récepteur ait reçu et ait déchiffré les données, ces dernières ne seront plus protégées. Les techniques de tatouage peuvent compléter la cryptographie en incluant une marque imperceptible et secrète (un filigrane) directement dans les données originales. Ce signal de filigrane est inclus de telle manière qu'il ne puisse pas être enlevé sans affecter la qualité des signaux audio ou vidéo. Le signal de filigrane peut, par exemple, être utilisé pour la protection de droits de publication puisqu'il peut cacher des informations sur l'auteur dans les données. Le filigrane peut aussi être utilisé pour prouver la propriété devant un tribunal. Une autre application intéressante pour laquelle le filigrane peut être utilisé, il permet de déterminer la source des copies illégales au moyen de la technique d'empreinte digitale.

Dans ce cas-ci, le fournisseur des médias dissimule des filigranes dans les copies des données avec un numéro de série qui est lié à l'identité du client. Si des copies illégales sont trouvées, par exemple sur Internet, le propriétaire des droits intellectuels peut facilement identifier les clients qui ont brisés leurs accords de licence en fournissant les données aux tiers. Le signal de filigrane peut également être employé pour commander des dispositifs d'enregistrement numérique puisqu'il peut indiquer si certaines données peuvent être enregistrées ou pas. Dans un tel cas, les dispositifs d'enregistrement doivent être équipés de détecteurs de filigrane.

D'autres applications du filigrane sont à inclure:

Il peut être utilisé par un Système de surveillance automatisé pour la radio et la radiodiffusion de TV, ou pour l'authentification des données et la transmission des messages secrets. Chaque application du filigrane a ses propres conditions spécifiques. Néanmoins, les conditions les plus importantes, qui doivent être réunies par la plupart des techniques de filigrane, sont :

- ✓ Que le filigrane soit imperceptible sur les données dans lesquelles il est caché.
- ✓ Qu'il puisse contenir une quantité d'information raisonnable.
- ✓ Qu'il ne puisse pas être enlevé facilement sans affecter la qualité des données dans lesquelles il est dissimulé.

## *1.1.2-L'utilité du marquage :*

**D**ans les dernières années il y a eu une explosion dans l'utilisation et la distribution des données numériques des multimédias. Les ordinateurs individuels avec des connexions d'Internet ont pris les habitations par l'assaut, et ils ont fait de la distribution des données et des applications multimédia beaucoup plus faciles et plus rapides. Des applications de commerce électroniques et les services rapides en ligne sont développés. Même les équipements audio et vidéo analogiques dans les habitations sont en cours d'être changés par leurs successeurs numériques. En conséquence, nous pouvons voir les dispositifs de masse d'enregistrement numériques pour des données multimédia, accéder au marché des consommateurs d'aujourd'hui.

Bien que les données numériques aient beaucoup d'avantages par rapport aux données analogiques, les fournisseurs de service sont peu disposés à offrir leurs services en forme numérique parce qu'ils craignent la duplication et la diffusion sans restriction de leurs produits. À cause des violes possibles des droits de publication, la propriété intellectuelle du produit numériquement enregistré doit être protégée. Le manque d'un tel système de protection était la raison de l'introduction retardée du **(DVD)** (digital versatile disc).

Plusieurs compagnies des médias ont au commencement refusé de fournir leurs produits sous forme de **DVD** jusqu'à ce que le problème de la protection contre les copies illégales ait été adressé.

L'organisation mondiale de la protection intellectuelle, regroupant 171 états membres au jour du 17 avril 2000, a défini un cadre particulier de protection juridique des documents numériques. Un traité sur le droit d'auteur a été signé le 20 décembre 1996, entrant dans le cadre de la convention de berne révisée le 2 mars 1997.

Ce traité comporte un article sur les « informations relatives au régime des droits d'auteur de documents sous forme électronique »

**ARTICLE 12 : OBLIGATION RELATIVES A L 'INFORMATION SUR LE REGIME DES DROITS**

1. **les parties contractantes doivent prévoir des sanctions juridiques appropriées et efficaces contre toute personne qui accomplit l'un des actes suivants en sachant, ou, pour ce qui relève des sanctions civiles, en ayant des raisons valables de penser que cet acte va entraîner, permettre, faciliter ou dissimuler une atteinte à un droit prévu par le présent traité ou la convention de berne :**
   - **I) supprimer ou modifier, sans y être habilité, toute information relative au régime des droits se présentant sous forme électronique ;**
   - **II) distribuer, importer aux fin de distribution, radiodiffuser ou communiquer au public, sans y être habilité, des oeuvres ou des exemplaires d'œuvres en sachant que des informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifier sans autorisation .**
2. **dans le présent article, « l'expression sur le régime des droits »s'étend des informations permettant d'identifier l'œuvre, l'auteur de l'œuvre, le titulaire de tout droit sur l'œuvre ou des informations sur les conditions et modalités d'utilisation de l'œuvre, et de tout numéro ou code représentant ces informations, lorsque l'un quelconque de ces éléments d'information est joint a l'exemplaire d'une œuvre ou apparaît en relation avec la communication d'une œuvre au public.**

Les représentants de l'industrie d'électronique grand public et de l'industrie des films cinématographiques ont accepté de chercher la législation au sujet des dispositifs numériques d'enregistrement visuel. Recommandations décrivant les manières qui protégeraient la propriété intellectuelle et les droits des consommateurs ont été soumises au congrès des USA et eurent comme conséquence la Loi des droits de publication des données Numériques, **Millénium** , qui a été signée par le Président Clinton le 28 octobre 1998.

Un filigrane peut être utilisée dans :

**Protection des droits de publication:** Pour la protection de la propriété intellectuelle, le propriétaire des données peut dissimuler un filigrane représentant l'information sur les droits de publication dans ses données. Ce filigrane peut permettre au propriétaire de prouver sa propriété devant un tribunal quand quelqu'un viole ses droits de publication.

**Empreinte digitale:** Pour déterminer la source des copies illégales, le propriétaire peut employer la technique d'empreinte digitale. Dans ce cas-ci, le propriétaire peut cacher différents filigranes dans les copies des données qui sont fournies à différents clients. L'empreinte digitale peut être comparée à inclure un numéro de série, qui est lié à l'identité du client, dans les données. Elle permet au propriétaire intellectuel d'identifier les clients qui ont brisé leur accord de licence en fournissant les données aux tiers.

**Protection contre la copie illégale:** L'information stockée dans un filigrane peut commander directement les dispositifs d'enregistrement numérique pour la protection contre la copie illégale. Dans ce cas-ci, le filigrane représente l'interdiction de copier et les détecteurs de filigrane dans l'enregistreur déterminent si les données peuvent être enregistrés ou pas.

**Surveillance d'émission:** En dissimulant des filigranes dans des spots publicitaires un système de surveillance automatisé peut vérifier si les spots sont diffusés en tant que contracté. Non seulement des films publicitaires mais également tous les produits TV peuvent être protégés par la surveillance des émissions. Les nouvelles peuvent avoir une valeur de plus de 100,000USD par heure, ce qui les rend très vulnérables à la violation des droits de propriété intellectuelle. Un système de surveillance d'émission peut vérifier tous les canaux d'émission et informe les stations de TV selon les résultats.

**Authentification de données:** Les filigranes fragiles peuvent être employés pour vérifier l'authenticité des données. Un filigrane fragile indique si les données ont été changées et il fournit l'information sur les localisations des endroits où les données ont été changées.

Les techniques de tatouage ne sont pas seulement employées pour la protection des données. D'autres applications sont à inclure:

**Indexation:** Indexation du courrier visuel où des commentaires peuvent être inclus dans le contenu visuel. Indexation des films et des nouvelles où on peut insérer des marqueurs et des commentaires qui peuvent être employés par des moteurs de recherche.

**Sûreté médicale:** Inclure la date et le nom du patient dans les images médicales pourrait être une mesure de sécurité utile **[1]**.

**Dissimulation de données secrètes:** Des techniques de tatouage peuvent être employées pour la transmission des messages privés et secrets. Puisque les divers gouvernements limitent l'utilisation des services de chiffrage, les gens peuvent cacher leurs messages dans d'autres données.

## *1.2- Les Conditions du marquage :*

Chaque application du marquage a ses propres conditions spécifiques. Par conséquent, il n'y a aucun ensemble de conditions qui peut être réuni par toutes les techniques de marquage. Néanmoins, quelques directions générales peuvent être données pour la plupart des applications mentionnées ci-dessus:

**Transparence :** Dans la plupart des applications l'algorithme de marquage doit insérer la marque tels que ceci n'affecte pas la qualité des données originales. Une marque est vraiment imperceptible si les humains ne peuvent pas distinguer les données originales des données avec la marque insérée **[2].** Cependant, même la plus petite modification dans les données originales peut être détectable quand celles-ci sont comparées directement aux données marquées. Puisque les utilisateurs des données marquées normalement n'ont pas accès aux données originales, ils ne peuvent pas effectuer cette comparaison. Par conséquent, il peut être suffisant que les modifications dans les données marquées soient inaperçues tant qu'ils ne seront pas comparés aux données originales.

**La capacité du marquage :** La quantité de l'information qui peut être stockée dans une marque dépend de l'application du marquage. Pour la protection des copies, une capacité d'un bit est habituellement suffisante. Selon une proposition récente pour la technologie du marquage des produits audio de la fédération internationale de l'industrie Phonographique, (IFPI), la capacité minimale pour un marquage audio devrait être 20 bits par seconde, indépendamment du type du niveau du signal . Cependant, ce minimum est très ambitieux et devrait être abaissé seulement à quelques bits par seconde. Et pour la protection des droits de propriété intellectuelle, il semble raisonnable que la marque doit être d'une taille de 60 bits (approximativement 10 chiffres) suivant l'ISBN, la numérotation standard internationale du livre, ou l'ISRC, code standard international d'enregistrement, (approximativement 12 lettres alphanumériques).

**Robustesse:** Un marquage fragile qui peut servir à prouver l'authenticité des données originales ne doit pas être robuste contre les techniques de traitement ou des changements intentionnels des données originales, puisque la disparition de la marque montre que ces données originales ont été modifiées et ne sont plus authentiques. Cependant, si un marquage est employé pour une autre application, il est souhaitable que ce marquage reste toujours dans les données originales, même si la qualité des données marquées est dégradée, intentionnellement ou involontairement. Les exemples des dégradations involontaires sont

des applications impliquant le stockage ou la transmission des données, où des techniques de compression sont appliquées aux données pour réduire leurs tailles et pour augmenter l'efficacité. Le marquage doit être robuste contre d'autres traitements innocents tels que : le filtrage, la conversion (analogique / numérique) et (numérique / analogique), le recadrage d'image, le changement d'échelles et autres.

D'autres traitements destinées à enlever la marque sont développés tel que la comparaison entre plusieurs copies avec différentes marques comme dans le cas de la technique d'empreinte digitale.

Dans tous les cas. Il ne devrait y avoir aucune manière dont la marque peut être enlevée ou changé sans dégradation suffisante de la qualité perceptuelle des données originales afin de les rendre inutilisables.

**Sécurité:** La sécurité des techniques de marquage peut être interprétée comme la sécurité des techniques de chiffrage [1], on devrait supposer que la méthode employée pour chiffrer les données est connue à une partie non autorisée, et que la sécurité doit se situer dans le choix d'une clef. Par conséquent une technique de marquage est vraiment sécurisée si la marque est indétectable même en sachant exactement les algorithmes de dissimulation et d'extraction de cette marque.

# *CHAPITRE N°2*

# *Classification Des Algorithmes De Marquage*

# 2.1-introduction :

Dans cette partie, nous essayons de donner les différents paramètres permettant d'effectuer un classement des algorithmes de marquages ensuite nous citerons quelques algorithmes appartenant aux classes les plus importantes.

On rencontre dans la littérature scientifique plusieurs algorithmes de marquage qui peuvent apparaître à première vue très différents, le domaine d'insertion de la marque, les méthodes utilisées pour détecter les messages ou encore la catégorie d'attaques visées sont autant de paramètres qui permettent de distinguer les différents algorithmes.

# 2.2-Paramètres de classification :

La majorité des algorithmes existants peuvent être classés suivant les critères suivants :

- ✓ Les localités où la marque est inséré : L'utilisation du HVS (Human visual system) model visuel humain est adressé.
- ✓ Le domaine où l'algorithme opère : Par exemple, un algorithme peut modifier directement l'image dans le domaine spatial pour dissimuler un message, ou il peut faire une transformation vers d'autres domaines (Par exemple, DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) ou Ondelettes), insérer la marque et appliquer la transformée inverse correspondante.
- ✓ Codage de la marque.
- ✓ La formation du signal composite : comment la marque est dissimulée à l'intérieur de l'image originale .la marque peut être ajoutée tout simplement à l'image ou l'image doit subir des transformations pour dissimuler ou détecter la présence de la marque.
- ✓ Comment la marque est détectée et extraite de l'image marquée : étant donnée que la marque possède une faible puissance comparée à celle du signal hôte le détecteur travaille dans un environnement de faible rapport signal sur bruit .il existe plusieurs méthodes où la performance du décodeur peut être améliorée. même pour les cas où l'image marquée a été modifiée par une personne malveillante.

On peut résumer ces critères dans la figure (figure 2.1) :

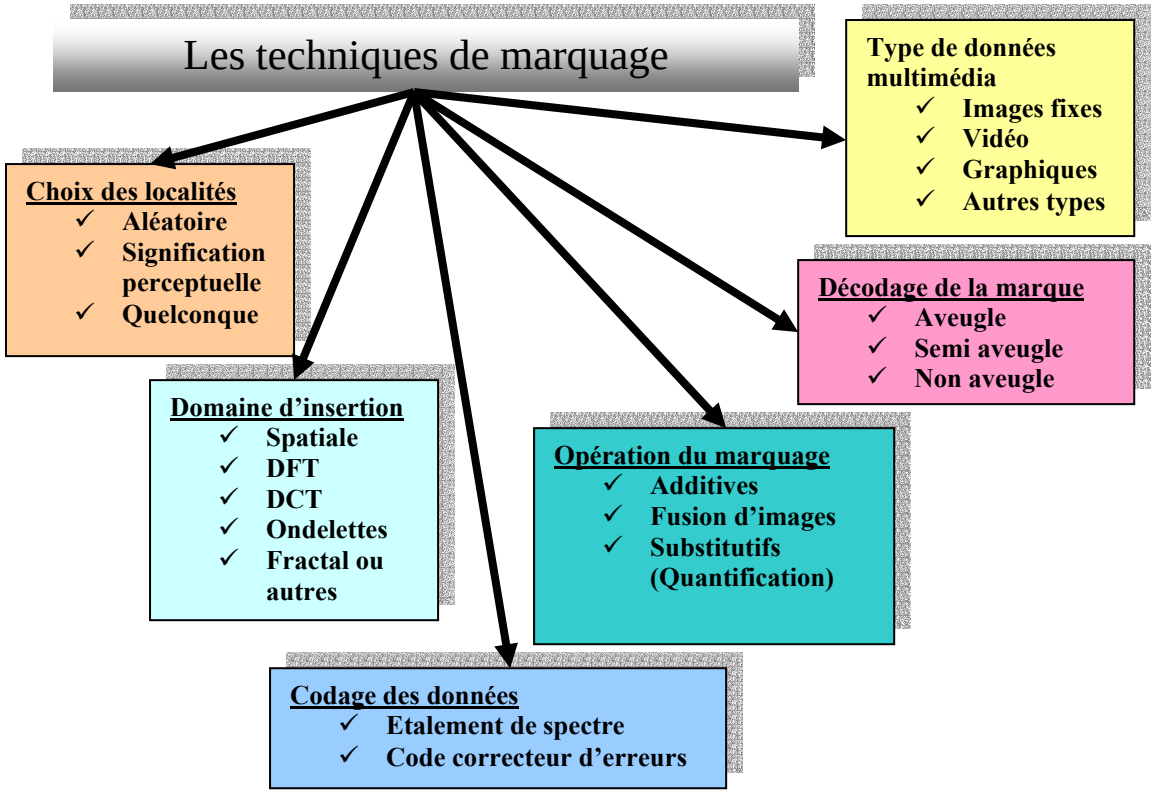



**Figure 2.1 : critères pour la classification des schémas**

On remarque que ces algorithmes sont partagés essentiellement en deux grandes classes.

**1- classe des algorithmes additifs :** où la signature est ajoutée à une composante de l'image pour être ensuite détectée par corrélation (ou marquage basée sur la corrélation).

**2- classe des algorithmes substitutifs :** pour lesquels la signature prend la place d'une composante de l'image (ou marquage non basée sur la corrélation)

# *2.3-Les algorithmes additifs:*

Ces algorithmes sont appelés aussi « *les techniques de marquage basées sur la corrélation* ». Dans ces algorithmes la marque, qui représente le signal, est ajoutée directement au bruit représenté par une composante de l'image.

La difficulté majeur, dans ce contexte là, est qu'il faut mettre en forme le signal d'une manière nous permettant la détection de la marque (signal) malgré la présence de l'image (bruit).

## *2.3.1- Insertion de la marque :*

Dans ces cas l'insertion de la marque suit plusieurs étapes.

1- des composantes sont extraites de l'image originale ***I*** .par composantes nous entendons l'image elle-même (l'intensité ou une des composantes de la couleur généralement le bleu) ou bien le produit d'une transformation fréquentielle (DCT, DFT) ou multi résolution (Ondelettes).ces composantes peuvent être réordonnées en utilisant une clef secrete ***K*** cette opération ayant pour but de brouiller le domaine d'insertion. Les composantes extraites forme alors le vecteur $C_K(I)$

2- une marque de base que nous nommerons $W_b(K)$, est ensuite générée. cette séquence est construite à l'aide d'un générateur aléatoire et dépend également de la clef secrète ***K***.

3- un message binaire $M=\{b_1,\ldots,b_n\}$, $b_i \{0 ; 1\}$ peut éventuellement être modulé par la séquence aléatoire $W_b$. c'est le principe de l'étalement de spectre**.** on obtient alors le vecteur $W(K)$**.**

4- la marque $W(K)$ est ajoutée aux composantes de l'image $C_K(I)$ pour obtenir les composantes $C_K(I_W)$ de l'image marquée :

$$C_K(I_W) = C_K(I) + W(K) \qquad (2.3.1)$$

Afin d'alléger les notations, nous posons par la suite

$$Y=C_K(I_W),\ W=W(K) \quad et \quad C_K(I)=I \quad donc \quad Y=W+I$$

5- l'image marquée est reconstruite à partir des composantes $C_K(I_W)$**.**

## *2.3.2- Détection de la marque :*

Deux hypothèses seulement sont utilisées pour décider si l'image contient ou non une marque.

1- $\mathbf{H_0}$ : Traduit la présence du bruit seulement (l'image) sans le signal (la marque).

2- $\mathbf{H_1}$ : Traduit la présence du bruit (l'image) et du signal (la marque).

$$H_1 : Y=I+W \quad (2.3.2) \quad \text{et} \quad H_0 : Y=I \quad (2.3.3)$$

Le bruit est souvent considéré comme étant Gaussien avec une moyenne nulle et qui représente dans ce cas l'image **[2]**.

En appliquant la corrélation entre $Y$ et $W$ on peut obtenir une information révélatrice sur la présence ou l'absence de la marque.

$$r =< W ; Y >= \sum_{i,j} W_{i,j} Y_{i,j} \quad (2.3.4)$$

Si la marque est présente ($H_1$) :

$$r(H_1) = <W ; I+W> = <W ; I> + <W ; W> \approx <W ; W> \quad (2.3.5)$$

Si la marque n'est pas présente ($H_0$) :

$$r(H_0) = <W ; I> << r(H_1) \quad (2.3.6)$$

La procédure de détection de la marque peut alors être représentée par les étapes suivantes :

1- Extraction des composantes marquées.
2- Génération de la séquence aléatoire de base $W_b$ à partir de la clef secrète $K$.
3- Calcul de la corrélation entre les composantes marquées et la séquence de base.
4- Décodage du message.

Durant le processus de détection, un seuil $S$ est habituellement utilisé pour décider si la marque est détectée ou non. Si la corrélation dépasse un certain seuil, le détecteur annonce que l'image $Y$ contient la marque $W$ sinon l'image ne contient aucune marque.

$$r > S, \quad W \text{ est détectée} \qquad et \qquad r < S, \quad W \text{ n'est pas détectée.}$$

Afin d'augmenter la performance de la corrélation un pré filtrage peut être appliquée à l'image, l'utilisation d'un filtre passe haut rend possible l'élimination d'une partie des composantes propres à l'image et diminue sa contribution dans le calcul de la corrélation et ainsi l'augmentation de la valeur de cette dernière **[3] [4] [5]**. Par exemple l'utilisation d'un simple filtre (FIR) $F_{edge}$, ou $F_{edge}$ est comme suite :

$$F_{edge} = \begin{bmatrix} -1 & -1 & -1 \\ -1 & 10 & -1 \\ -1 & -1 & -1 \end{bmatrix} / 2 \qquad \textbf{(2.3.7)}$$

## *2.3.3- Algorithmes additifs dans le domaine spatial :*

Dans cette partie nous présentons quelques algorithmes de marquage additifs dans le domaine spatial.

## *2.3.3.1-La première catégorie d'algorithmes*

La figure 2.2 représente le schéma des algorithmes de marquage de la première catégorie. Les procédures de marquage consistent à générer une marque, faire une mise en forme de la marque et ajouter ensuite le résultat à l'image pour avoir l'image marquée.

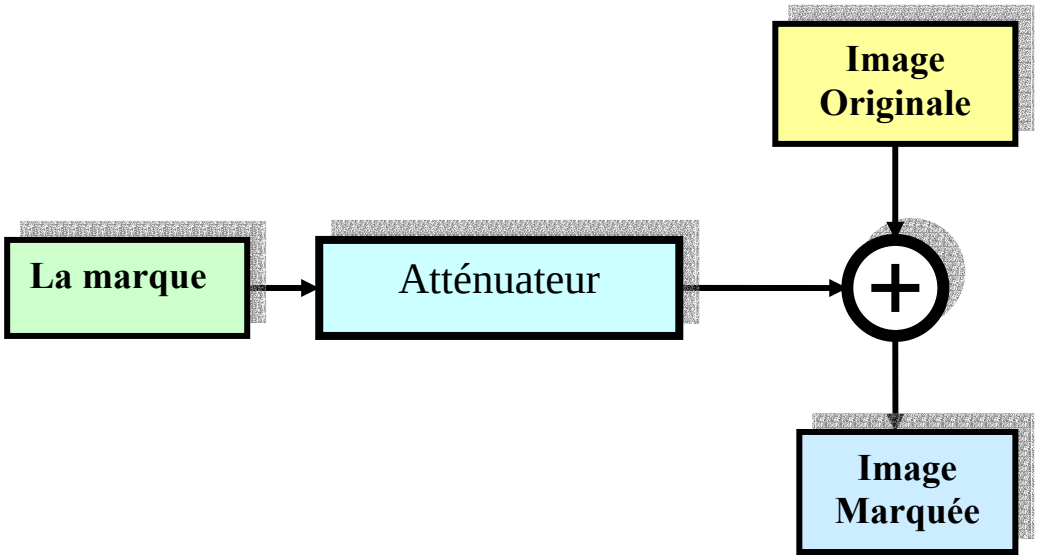



**Figure 2.2 : schéma des algorithmes de la première catégorie**

## *A- Techniques de marquages basés sur l'étalement de spectre dans le domaine spatial :*

Les premiers auteurs qui ont utilisé la technique d'étalement de spectre dans le marquage des images sont Tirkel et *al* **[6] [4]**.

Leur technique consiste à ajouter des M- séquences sur les bits de poids faibles de l'image .la détection de la marque est effectuée en calculant la corrélation entre l'image marquée et les M -séquences.

Les différents pics de la corrélation traduisent la présence de la marque et la position de ces pics indique les lettres du message transmis.

Hartung et Girod ont développé un algorithme similaire qui permet d'insérer un message de plusieurs bits au sein d'une image ou d'une séquence d'images **[7]**.

Chaque bit à insérer est associé a une valeur (-1) s'il est égal à (0) et (+1) s'il est égal à (1) , et est étalé sur une fenêtre .le signal résultant à la même taille que l'image . Il est ensuite modulé par une séquence aléatoire et pondéré par un masque qui représente l'activité de l'image : la pondération est ainsi plus faible sur les zones homogènes que sur les zones texturées. La séquence obtenue est ensuite ajoutée à l'image.

Pour effectuer la détection du message il faut calculer la corrélation entre la séquence aléatoire et chaque fenêtre de l'image marquée ce qui donne tous les bits du message, le bit est (1) si la corrélation est positive et il est (0) si elle est négative. Un filtrage de l'image marque améliore nettement les performance de la corrélation (estimation de la marque par un filtre passe haut).

Langelaar et *al* ont développé un autre algorithme similaire mais plus robuste contre la compression JPEG .Il consiste à dissimuler un message de quelques centaines de bits à l'intérieur d'une image de dimensions (X, Y) devisée en blocs de 8x8 pixels.

Chaque bit du message est dissimulé à l'intérieur d'un bloc des valeurs de la luminance de l'image .La largeur et la hauteur des blocs doivent être des multiples de « 8 » ainsi que les cordonnées de leurs coins supérieur gauche pour être compatible à la compression JPEG et ainsi robuste contre cette dernière.

La détection de la marque est réalisée par le calcul de la corrélation de chaque bloc avec la séquence aléatoire utilisée lors de la dissimulation. Les règles utilisées dans la dissimulation et la détection du message sont les mêmes que celles qui sont utilisées par la technique précédente.

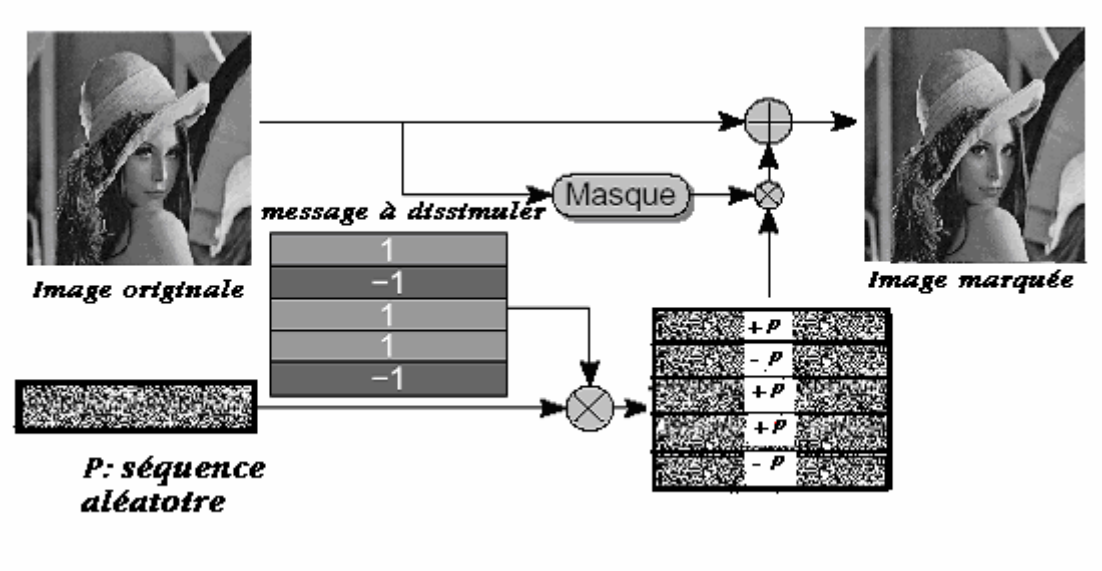



**Figure 2.3 Algorithme de Hartung et Girod**

Pour rendre cette technique plus robuste contre la compression JPEG les auteurs ont appliqué une distorsion aux blocs en réalisant leurs transformations DCT (Discrete Cosine Transform), et en faisant une quantification des coefficients avec un certain facteur de qualité Q et à la fin en calculant l'inverse de la DCT **[8]** .

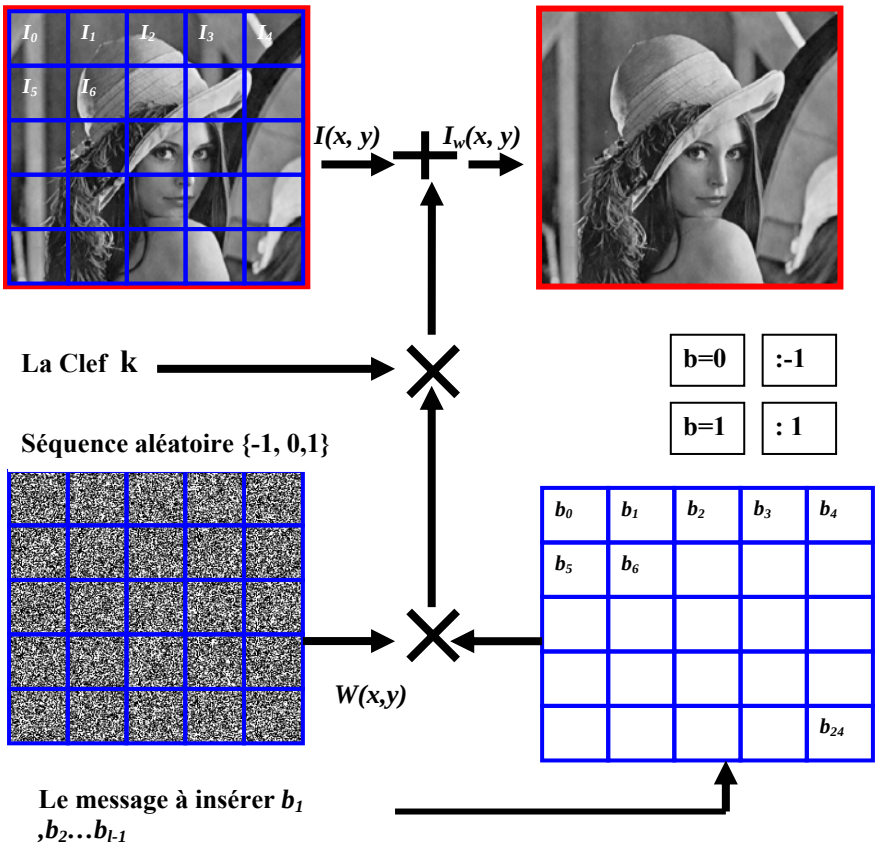



**Figure 2.4 Procédure de marquage par l'algorithme de langelaar**

## *B- Technique du « patchwork » :*

Bender et *al* **[9]**. Proposent une technique similaire à l'insertion de la marque par étalement de spectre. Cette technique consiste a générer un ensemble bidimensionnel de bits de mêmes dimension que l'image où le nombre des « uns » (ensemble $A_1$) est égal au nombre des « zéros » (ensemble $A_2$), ensuite affecter à chaque pixel de l'image le bit correspondant .Chaque pixel de l'image est ensuite modifié de la façon suivante :

- Si $p_{i,j} \in A_1 : p'_{i,j} = p_{i,j}$ .
- Si $p_{i,j} \in A_2 : p'_{i,j} = p_{i,j} + \alpha$ .

La détection se fait en calculant la différence entre la moyenne des pixels appartenant a l'ensemble $A_2$ et la moyenne des pixels appartenant a l'ensemble $A_1$. La marque est détectée si cette différence dépasse un certain seuil. Cette technique a été étudiée en détail par Pitas et kaskalis **[10] [2] [11] [12]**.

## *2.3.3.2-La deuxième catégorie d'algorithmes :*

Le schéma de la deuxième catégorie d'algorithmes est illustré dans la figure 2.5, l'amélioration principale par rapport à la première catégorie est que dans ce cas l'image originale est utilisée pour générer un masque perceptuel. Le message est généré selon ce masque, il est intense dans les régions où il va être invisible et moins intense dans les autres régions.

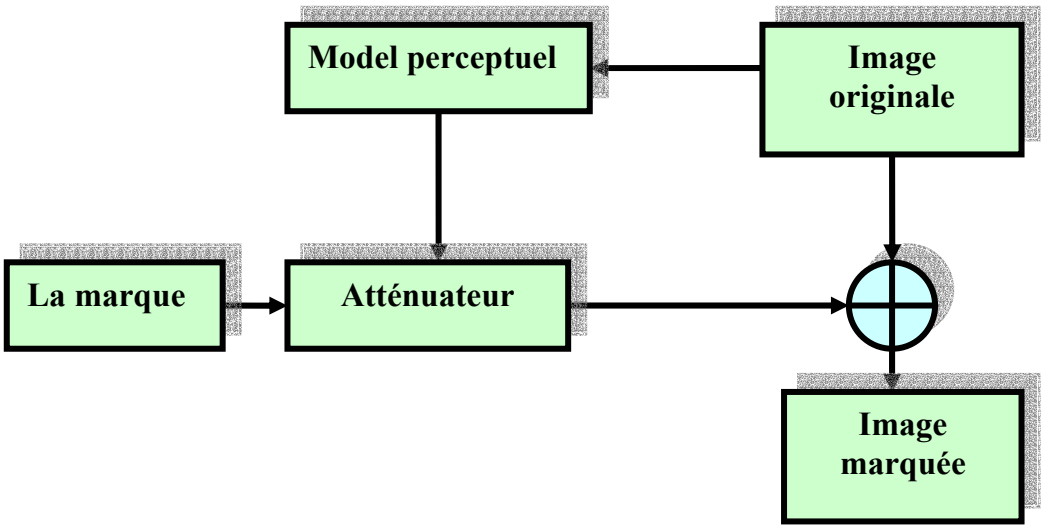



**Figure 2.5 : Schéma des algorithmes de la deuxième catégorie**

L'un des algorithmes appartenant a cette catégorie et celui qui est développé par Goffin **[13]**. La marque est filtré par un filtre passe bas, modulée en fréquence, masquée et ensuite ajoutée a l'image originale. Le processus de masquage utilise le phénomène de grillage.

La détection est accomplie par la démodulation. Un calcul de corrélation est comparé à un seuil.

Une différente méthode est proposée par Kutter **[14]**, l'auteur propose de marquer la composante bleue de la luminance. Il a été démontré que le HVS (Human visual system) est moins sensible aux changements de la composante bleue de l'image qu'aux changements des composantes vert et rouge. Kutter a dissimulé un nombre binaire à travers une modulation d'amplitude dans le domaine spatial .un seul bit est dissimulé dans une position (*i, j)* choisie aléatoirement en ajoutant ou retranchant, selon la valeur du bit, une valeur proportionnelle à celle de la composante bleue, donc modification de la composante bleue de l'image.

## *2.3.3.3-La troisième catégorie d'algorithmes :*

Le schéma de la troisième catégorie d'algorithmes est illustré dans la figure 2.6.

L'amélioration par rapport à la deuxième catégorie d'algorithme se réside dans le fait que toutes les caractéristiques de l'image sont utilisées afin de générer une marque avec un maximum de robustesse. Bien qu'elle soit schématiquement simple, elle comporte des avantages importants par rapport aux autres techniques de marquage. La principale distinction et que cette fois l'image n'est pas considérée comme un bruit additif. Etant donné que cette idée est très récente il n'y a pas beaucoup d'algorithmes qui sont classés dans cette catégorie.

Cox a présenté un algorithme de la catégorie III qui fonctionne comme suit. L'image et la marque toutes les deux sont traitées comme des vecteurs. Le codeur emploie la connaissance du vecteur image « r0 » pour calculer une région S (r0) dans laquelle des contraintes de visibilité sur l'image sont satisfaites. L'algorithme de marquage consiste à choisir une région.

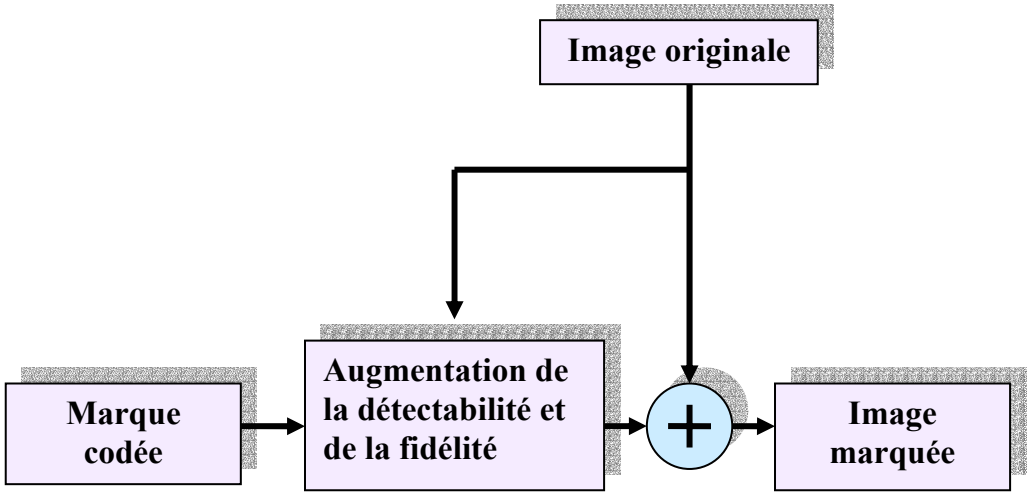



**Figure 2.6 : schémas de la troisième catégorie d'algorithmes**

## *2.3.4- Algorithmes additifs dans le domaine fréquentiel :*

## *2.3.4.1-Insertion dans le domaine TCD :*

À ce point, seulement des méthodes dans le domaine spatial ont été étudiées. Le marquage additif peut également être effectué dans le domaine des fréquences. Les plus populaires transformées sont la DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform), et les ondelettes. Il y a plusieurs motivations pour le marquage dans un domaine de transformation. Premièrement certaines transformées sont intrinsèquement robustes à certaines transformations. Par exemple il est facile de réaliser des marquages dans le domaine de la DFT (Discrete Fourier Transform) qui sont robustes contre le recadrage (cropping).

Deuxièmement, les algorithmes de compression les plus populaires fonctionnent dans les domaines des transformées, par exemple JPEG dans le domaine de la DCT (Discrete Cosine Transform) et EZW dans le domaine des ondelettes. En assortissant le domaine du marquage avec le domaine de la compression il est possible d'optimiser un algorithme de dissimulation de sorte qu'il soit optimal en ce qui concerne une technique donnée de compression. En conclusion, la fonction de marquage doit être spécifiée pour chaque domaine de transformation.

1- Dans **[15]** Cox insère une marque se composant d'une séquence de nombres aléatoires x = x1,..., x2 d'une distribution normale. La marque est insérée dans le domaine de la DCT (Discrete Cosine Transform) de l'image par l'une de trois méthodes:

$$v_i' = v_i + \alpha x_i \quad . \qquad \textbf{(2.3.9)}$$

$$v_i' = v_i(1 + \alpha x_i) \qquad \textbf{(2.3.10)}$$

$$v_i' = v_i e^{\alpha x_i} \quad . \qquad \textbf{(2.3.11)}$$

Où **α** représente la force du marquage les $v_i$ sont les coefficients DCT (Discrete Cosine Transform) de l'image originale. La plus intéressante approche est la deuxième.

L'image originale est nécessaire pour détecter la marque. En utilisant les coefficients de la corrélation normalisée, on mesure la similitude entre la marque détectée obtenue en calculant la différence entre les coefficients DCT (Discrete Cosine Transform) de l'image marquée et l'image originale $X^*$, et les coefficients de l'image originale $X$ .cet algorithme sera étudié en détail ultérieurement au chapitre 3.

$$sim(X, X^*) = \frac{XX^*}{\sqrt{X^*X^*}} \qquad \textbf{(2.3.12)}$$

2- dans piva et al. **[16]** les auteurs utilisent la même technique d'insertion que celle de cox mais sans l'utilisation de l'image originale pour la détection de la marque.

La marque est insérée selon la formule suivante :

$$y_i = x_i + \alpha |x_i| w_i \qquad \textbf{(2.3.13)}$$

La détection de la marque s'effectue en évaluant la corrélation :

$z = \frac{YW}{M}$ **(2.3.14)** , Où M est le nombre de coefficients marqués.

## *2.3.4.2- Algorithmes additifs dans le domaine multi résolution:*

Barni et *al.* Ont présenté un algorithme de marquage dans le domaine de la transformée par ondelette. La détection de la marque dans cet algorithme se fait sans l'utilisation de l'image originale contrairement à d'autres algorithmes ou l'image originale est nécessaire

pour la détection de la marque **[17] [18] [19]**.La marque est dissimulée, sous la forme d'une séquence pseudo aléatoire, dans les trois, sous bandes de détails du premier niveau de la décomposition. Cet algorithme sera étudié en détail au chapitre 3.

# *2.4- Les algorithms substitutifs:*

**D**ans cette classe la marque n'est pas ajoutée à l'image mais substituée à des composantes de l'image.

## *2.4.1 Insertion de la marque :*

Les algorithmes substitutifs peuvent se décomposer en quatre étapes.

1- Une clef secrète ***K*** associée à un générateur aléatoire permet de sélectionner les différentes composantes $\mathbf{C_K\ (I)}$ de l'image.

2- La signature insérée est obtenue en appliquant Une contrainte $f$ sur $\mathbf{C_K\ (I)}$ en fonction du message à insérer ***W (K)***.

3- Substitution $C_K(I_w) = f(C_K(I), W(K))$ . **(2.4.1)**

4- Reconstruction de l'image à partir des $\mathbf{C_K\ (I_w)}$**.**

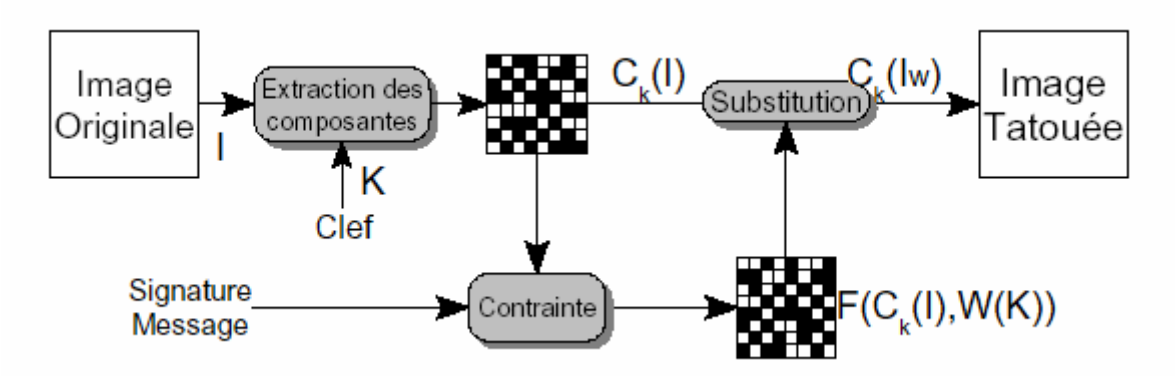



**Figure 2.7 : schéma substitutif d'insertion de la marque**

## *2.4.2 Détection de la marque :*

Un préambule composé d'une séquence pré définie peut être inséré dans l'image pour être utilisé lors de la détection.

La détection de la marque ce décompose en trois étapes :

1- Extraction des composantes marquées de l'image à l'aide de la clef ***k.***
2- Comparaison du degré de similitude entre le préambule retrouvé et le préambule utilisé lors de l'insertion.
3- Décodage du message.

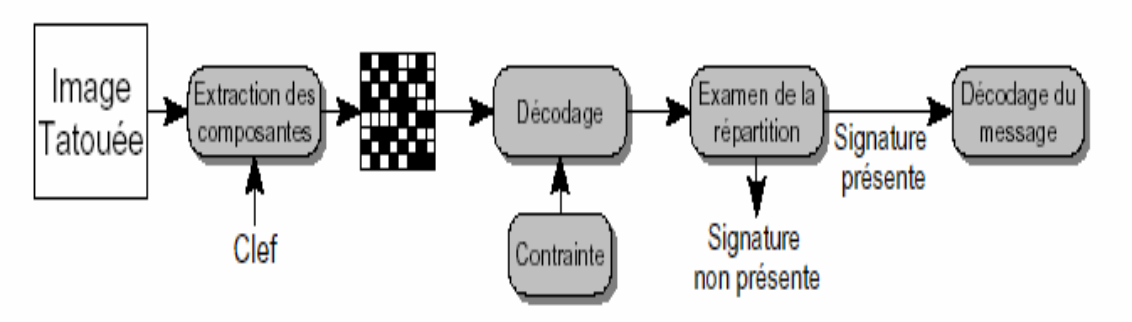



**Figure 2.8 décodeurs d'un substitutif**

## *2.4.3- Algorithmes substitutifs dans le domaine spatial :*

### *2.4.3.1- Changement du bit le moins significatif :*

L'exemple le plus simple d'une technique de marquage substitutif dans le domaine spatial est la modification du bit le moins significatif. Chaque pixel dans une image, en niveaux de gris, est représenté par un nombre à 8 bits. Puisque les bits les moins significatifs ne contiennent pas des informations visuellement significatives, ils peuvent facilement être remplacés par une énorme quantité de bits de marquage. Donc il suffit de remplacer ces bits par le message à dissimuler.

Des algorithmes plus sophistiqués de marquage qui se servent des modifications du LSB peuvent être trouvés dans **[4]**, **[20]**, **[21]**, **[22]** et **[23]**. Ces techniques de marquage ne sont pas très sécurisées et pas très robustes aux techniques de traitement d'image parce que les bits les moins significatifs sont facilement remplaçables par des bits aléatoires, retirant ainsi les bits de la marque.

## *2.4.4-Algorithmes substitutifs dans le domaine fréquentiel :*

### *2.4.4.1- Modification des coefficients DCT :*

Dans **[24]**, **[25]**, **[26]** et **[27]** les auteurs ont proposé des méthodes de marquage qui ajoutent une marque sous forme de chaîne binaire dans le domaine des blocs DCT (Discrete Cosine Transform) de taille 8x8. Pour marquer une image, l'image est divisée en blocs 8x8. Les coefficients DCT des blocs sont calculés ensuite, deux ou trois sont choisis dans chaque blocs sur la bande des fréquences moyennes. Les coefficients choisis sont quantifiés en utilisant la table de quantification JPEG par défaut **[28]** et un facteur de qualité JPEG relativement bas. Les coefficients choisis sont alors adaptés de telle manière que leurs grandeurs forment un certain rapport. Les rapports entre les coefficients choisis composent 8 ensembles (combinaisons), qui sont divisés en 3 groupes. Deux groupes sont utilisés pour représenter les bits ' 1 ' ou ' 0 ' de la marque, et le troisième groupe représente les ensembles inadmissibles. Si les modifications qui sont nécessaires pour maintenir un ensemble désiré deviennent trop grandes, le bloc est marqué comme inadmissible. Par exemple, si un bit de la marque à la valeur ' 1 ' doit être inclus dans un bloc, le troisième coefficient devrait avoir une valeur plus inférieure que les deux autres coefficients.

| **Dissimulation d'un bit dans trois coefficients DCT** | | | |
|---|---|---|---|
| $S_i$ | **C1** | **C2** | **C3** |
| **1** | **H** | **M** | **L** |
| **1** | **M** | **H** | **L** |
| **1** | **H** | **H** | **L** |
| **0** | **M** | **L** | **H** |
| **0** | **L** | **M** | **H** |
| **0** | **L** | **L** | **H** |
| **ignorer ce bloc** | **H** | **L** | **M** |
| **ignorer ce bloc** | **L** | **H** | **M** |
| **ignorer ce bloc** | **M** | **M** | **M** |

Un bit est inséré dans un bloc en modifiant l'ordonnancement d'un triplet de TCD {C1, C2, C3}

Un bit égal à '1' est inséré en modifiant les valeurs C1, C2, C3 pour obtenir :

$$\begin{cases} C1 > C3 + Cte \\ C2 > C3 + Cte \end{cases} \qquad \textbf{(2.4.2)}$$

Un bit égal à '0' est inséré en modifiant les valeurs C1, C2, C3 pour obtenir :

$$\begin{cases} C1 + Cte < C3 \\ C2 + Cte < C3 \end{cases} \qquad \textbf{(2.4.3)}$$

## *2.4.4.2- Quantification des coefficients DCT :*

Cette méthode est développée par Bors et Pitas **[29]** , **[30]** et **[31]** ou la marque est introduite dans les coefficients DCT (Discrete Cosine Transform) de la bande des moyennes fréquences et qui n'est pas un message mais un ensemble de paramètres utilisé dans un réseaux gaussien classificateur et de contraintes.

L'image originale n'est pas utilisée lors de la détection de la marque.

Les auteurs envisagent deux types de contraintes :

**1-** La première correspond en une quantification scalaire, le pas de la quantification dépend de la marque.

$$FxW = Cte \qquad \textbf{(2.4.4)}$$

- $\boldsymbol{F}$ est le vecteur des coefficients DCT .et $W$ est un vecteur qui dépend de la signature .le calcul de $F$ s'effectue par minimisation des moindres carrés.

**2-** La deuxième contrainte correspond à une quantification vectorielle appliquée sur certains coefficients TCD des blocs sélectionnés. Cela revient à choisir le vecteur $F$ tell que :

$$\left\| \boldsymbol{F} - \boldsymbol{W}_k \right\|^2 = \min_{i=1}^{H} \left\| \boldsymbol{F} - \boldsymbol{W}_i \right\|^2 \qquad \textbf{(2.4.5)}$$

$\boldsymbol{W_i}$ étant un ensemble de vecteur provenant de la signature.

La détection se fait en étudiant la répartition des blocs sélectionnés satisfaisant la contrainte utilisée lors de l'insertion.

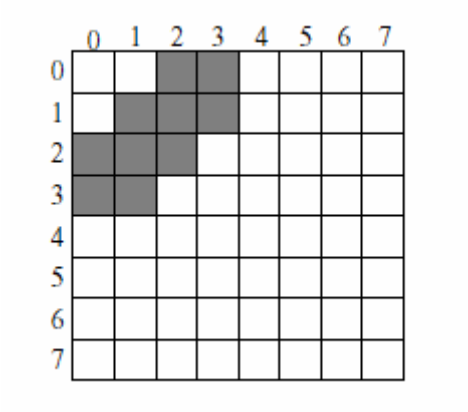



**Figure 2.9 Les coefficients de moyennes fréquence utilisée**

## *2.4.4.3-Seuillage des coefficients DCT :*

Langelaar et al. **[32]** et **[33]** Ont développé un algorithme qui consiste à insérer une série de bits. Chaque bit est inséré dans *n8x8* blocs DCT (Discrete Cosine Transform). Diviser ces *n*8x8 blocs DCT de l'image originale en deux ensembles A et B en utilisant une fonction aléatoire qui dépend d'une clef.

Pour les blocs de l'ensemble A on calcule la somme de l'énergie des coefficients (à partir d'un nombre k) $E_A(k)$ .

$$E_A(K) = \sum_{b} \sum_{j=k}^{64} c_{b,j}^2 \qquad (2.4.6)$$

Faire le même calcul pour l'ensemble B $E_B(k)$ .L'énergie dans un sous espace est donc enlevée.

$$E'_B := 0 \quad \text{Si} \quad s_i = 1$$
$$E'_A := 0 \quad \text{Si} \quad s_i = 0$$

$S_i$ étant le bit à insérer. Ainsi on change la différence d'énergie.

$$D = E'_A - E'_B = E'_A - 0 = +E'_A \quad \text{Si} \quad s_i = 1$$
$$D = E'_A - E'_B = 0 - E'_B = -E'_B \quad \text{Si} \quad s_i = 0$$

L'énergie est enlevée par l'élimination des coefficients de **k** jusqu'à zéro.

La valeur de k est calculée de telle sorte que pour un maximum de k on à $E_A(k) > D$ et $E_B(k) > D$ .

Pour la détection deux fréquences de coupure sont calculées :

$$\mathbf{K_A} = \text{ valeur maximale pour laquelle } \sum_{b} \sum_{j=k}^{64} c^{2}{}_{b,\,j} > D$$

Faire le même calcul pour $K_{B,}$ ainsi le bit dissimulé peut être lue :

| | |
|---|---|
| **Si $K_A < K_B$** | **$S_i$=1.** |
| **Si $K_A = K_B$ et $E_A(k_A) < E_B(k_B)$** | **$S_i$=1.** |
| **Si $K_A = K_B$ et $E_A(k_A) > E_B(k_B)$** | **$S_i$=0.** |
| **Si $K_A > K_B$** | **$S_i$=0.** |

Le message détecter peut être comparé au message dissimuler au départ.

## *2.4.5-Algorithmes substitutifs dans le domaine multi résolution :*

## *2.4.5.1- Quantification des coefficients ondelettes :*

Kundur et Hatzinakoz ont proposé un algorithme de marquage basé sur la quantification des coefficients d'ondelettes ou l'image originale n'est pas nécessaire pour la détection de la marque.

L'algorithme commence par faire la transformation en ondelette de l'image originale jusqu'au niveau de détail k. un triplet de coefficients $\left\{C_K^H, C_K^V, C_K^D\right\}$ est sélectionné aléatoirement pour dissimuler un bit du message .les éléments de ce triplet sont ensuite ordonnés par ordre croissant $C_k^{n_1} \le C_k^{n_2} \le C_k^{n_3}$ la différence entre les valeurs minimales et maximales des coefficients permet de calculer le pas de quantification**Δ.**

$$\Delta = \frac{c_k^{n_3} - c_k^{n_1}}{2Q - 1} \qquad \textbf{(2.4.7)}$$

**Q** est une constante permettant de régler le degré de visibilité de la marque.
Le coefficient est modifié suivant la règle illustrée dans la figure suivante.

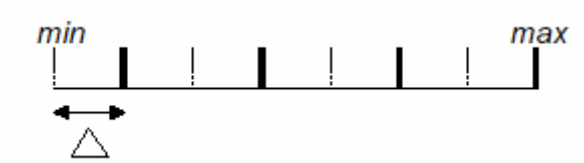



**Figure 2.10 : échelle de quantification des coefficients d'ondelette**
Les valeurs min et max sont respectivement la plus grande et la plus petite valeur du triplet

- pour insérer un bit '**1**' la valeur de $C_K^{n2}$ est quantifiée en prenant la valeur du trait gras le plus proche.
- pour insérer un bit '**0**' la valeur de $C_K^{n2}$ est quantifiée en prenant la valeur du trait pointillé le plus proche.

L'extraction de la marque se fait en utilisant la séquence aléatoire pour localiser les coefficients marqués.

# *2.5- Conclusion:*

Les classes des algorithmes de marquage sont très variées. La recherche dans ce domaine ne fait que commencer, les chercheurs essayent de trouver de nouvelles techniques de marquage en variant les domaines d'insertion de la marque, ou les méthodes utilisées pour le marquage. Cette évolution est réalisée en essayant d'utiliser toutes les techniques existantes dans les domaines de la cryptographie, de la communication, de la sécurité informatique ou autres domaines tel que le domaine des mathématiques (les statistiques). Il s'agit d'essayer les techniques anciennes ou les toutes nouvelles techniques. Le but essentiel est de trouver un algorithme qui soit robuste contre toutes les attaques possibles, existantes ou qui peuvent être développées. Un algorithme de marquage, où la marque doit être invisible et indétectable. Un algorithme de marquage où la taille, de la marque, soit suffisamment grande pour porter les informations nécessaires pour réaliser les buts du marquage.

Dans le chapitre suivant nous allons détailler quelques algorithmes et montrer l'évolution des techniques citer dans ce chapitre .Des résultats seront présentés montrant la robustesse des algorithmes.

# *CHAPITRE N°3*

# *Algorithmes Et Résultats*

# 3.1-Introduction :

**D**ans ce chapitre nous allons détailler quelques algorithmes des différents types de marquage et déterminer leur robustesse contre les différentes attaques.

# 3.2-Algorithmes dans le domaine spatial:

**L**es algorithmes suivants travaillent dans le domaine spatial ce qui veut dire qu'il n'y a pas de temps supplémentaire pour le calcul d'une transformée. Les valeurs des luminances des pixels ou les valeurs des trois composantes rouge, verte ou bleue sont directement manipulées. Nous allons commencer par le cas les plus général et le plus commun pour montrer les procédures suivies pour la dissimulation et l'extraction d'un message à l'intérieur d'une image numérique et montrer ensuite les paramètres influants sur la robustesse de ces algorithmes en effectuant plusieurs expériences.

## 3.2.1- Algorithme de base :

***Les auteurs :*** les méthodes basées sur cette techniques sont développées par plusieurs auteurs. Schyndel **[4]** ,Bender **[9]** ,Pitas **[10]** , Bruyndonckx **[34]**,Caroni **[35]** , Hartung **[36]** , Langelaar **[5]** ,Pitas **[2]**, Smith **[37]** , wolfgang **[38]** , Langelaar **[8]** ,Wolfgang **[39]** ,Zeng **[40]** , **[41]** ,Wolfgang **[42]** ,Wolfgang **[43]** , kalker **[44]** .

***Détecteurs :*** dans ces algorithmes les détecteurs n'ont pas besoin de l'image originale pour détecter la présence de la marque, c'est-à-dire ces algorithmes sont du type aveugle , par conséquent l'image originale n'est pas utilisée pour l'extraction du message.

***La marque :*** la marque est une séquence pseudo aléatoire formée des éléments $\{-1,0,1\}$ ou seulement $\{-1,1\}$, les nombres réels (fractionnaires) peuvent être utilisés.

***Les sites :*** tous les pixels de l'image sont utilisés pour dissimuler un bit. Pour augmenter la capacité de dissimulation, l'image est divisée en plusieurs blocs.

***Le marquage :*** le marquage (figure 3.1) est basé sur l'équation suivante

$$I_W(x,y) = I(x,y) + K.W(x,y) \quad \textbf{(3.2.1)}$$

Où $I_W(x,y)$ est un pixel de l'image marquée, $I(x,y)$ est un pixel de l'image originale,

$W(x, y)$ Élément de la séquence aléatoire et $K$ coefficient de visibilité de la marque.

1- Générer une séquence pseudo aléatoire avec une **clef =10** figure 3.3 de longueur égale au nombre de pixels de l'image originale figure 3.2.
2- Multiplier cette séquence « sous forme d'une matrice de dimensions égales aux dimensions de l'image originale « **Lena** » par un facteur **k**.
3- Ajouter la matrice résultante à l'image originale « **Lena** » pour obtenir l'image marquée figure 3.4.

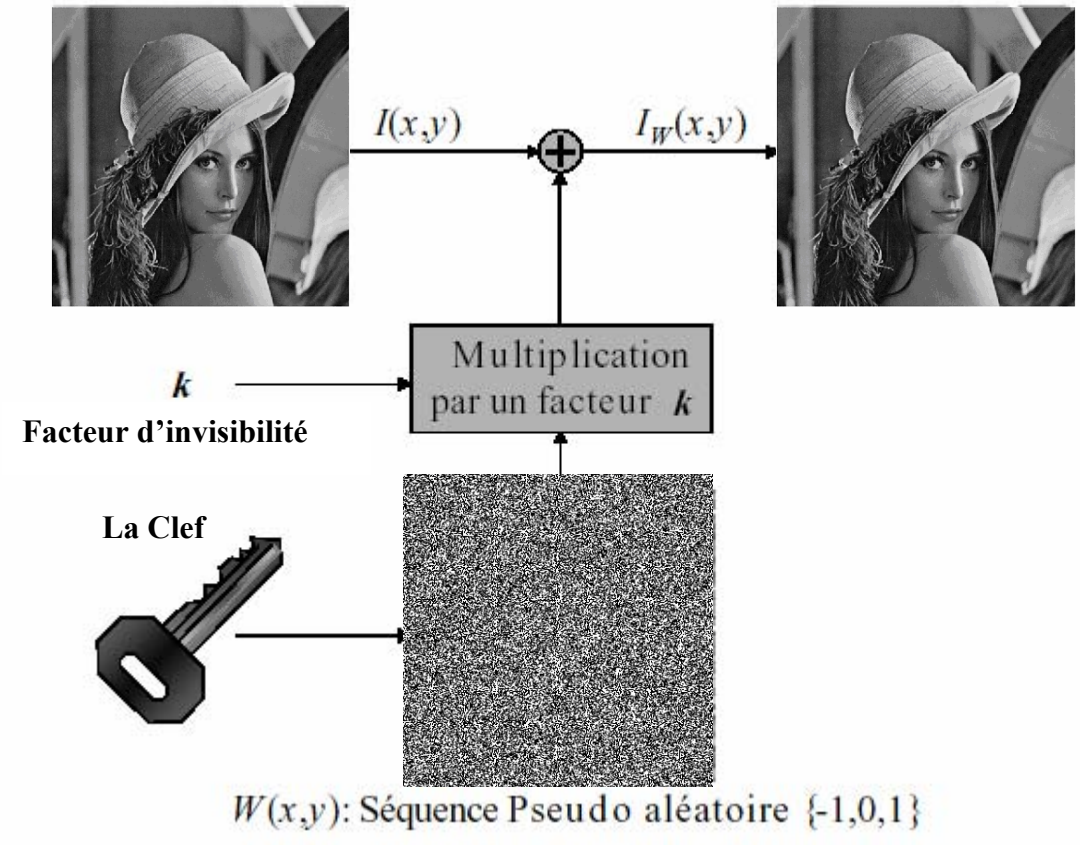
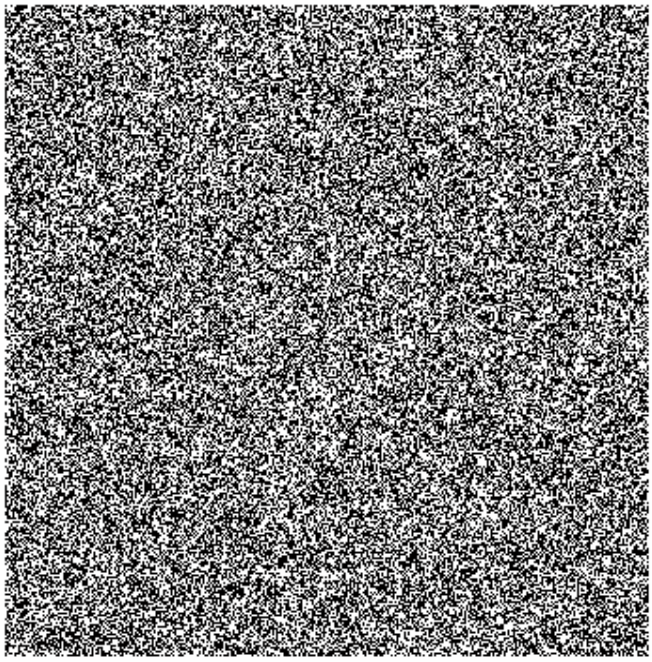



**Figure 3.1 : algorithme de base dans le domaine spatiale.**

image originale

**Figure 3.2 Image originale (hôte).**



Séquence aléatoire

**Figure 3.3 Séquence pseudo aléatoire (La marque).**
**Générée avec un seed=10.**

Image de lenna marquée

**Figure 3.4 image marquée par une séquence aléatoire de seed=10.**

***Détection :*** la détection se fait par un calcul de la corrélation entre l'image marquée et une séquence pseudo aléatoire identique a celle qui est utilisée lors de la dissimulation. Si $W(x,y)$ est constitué de deux nombres $\{-1,1\}$, et si le nombre des « 1 » est égal « -1 » on peut estimer la corrélation comme suite :

$$R = \frac{1}{Z}\sum_{i=1}^{Z} I'_{WI}(x,y)W_i(x,y) = \frac{1}{Z}\sum_{i=1}^{Z/2} I'_{Wi}W_i^{+} + \frac{1}{Z}\sum_{i=1}^{Z/2} I'_{Wi}W_i^{-} = \frac{1}{2}\left\{\mu\left[I_W^{'+}(x,y)\right] - \mu\left[I_W^{'+}(x,y)\right]\right\} \quad (3.2.2)$$

Où **Z=NxM** le nombre de pixels de l'image marquée. Et $^{+,-}$ indiquent les ensembles des pixels où les éléments correspondants de la séquence aléatoire sont respectivement positifs (+1) ou négatifs (-1). $I'_{WI}(x,y)$ Valeur de la luminance au point ***i*** et $W_i(x,y)$ élément de la séquence aléatoire correspondant.

Cette corrélation est maximale si la séquence aléatoire utilisée est la même que celle qui est utilisée lors de la dissimulation du message on peut facilement montrer ce fait par l'expérience suivante.

***Experience1 : figure(3.5)***

1- On réalise une dissimulation suivant l'algorithme de marquage décrit précédemment avec une clef égale à **10**.
2- On calcule les coefficients de corrélation en utilisant une clef qui varie entre **15** et **0**.
3- On trace le diagramme en bars représentant le coefficient de corrélation en fonction de la valeur de la clef de la séquence aléatoire.

**Remarques :**

- ✓ **Il est claire que le coefficient de corrélation calculé en utilisant la clef 10 (la même utilisé lors du marquage) est nettement plus grand que les autres coefficients.**
- ✓ **Les autres coefficients ne sont pas forcement nuls. Ce qui nécessite, pour une meilleure détection, l'établissement d'un seuil de détection.**

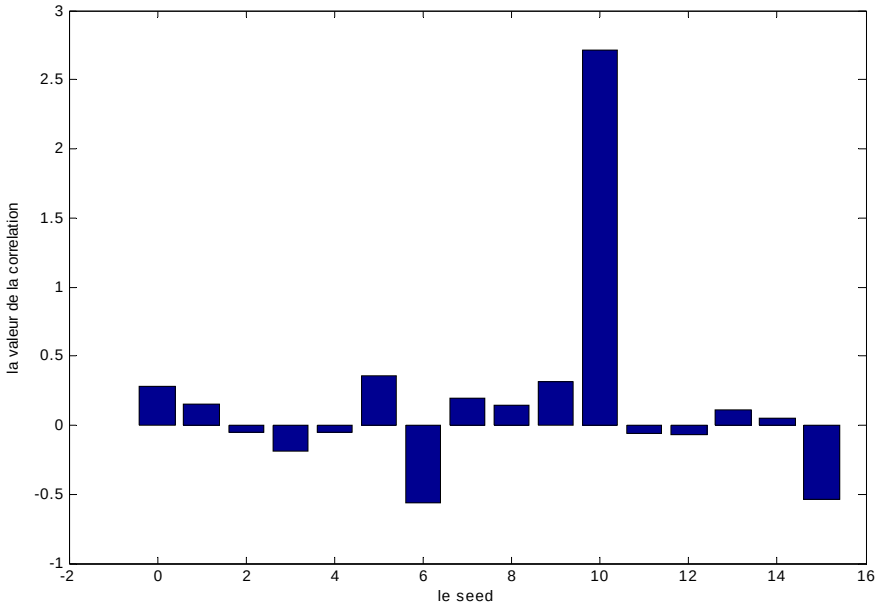



**Figure 3.5 variation de la valeur du coefficient de corrélation en fonction de la clef de la séquence pseudo aléatoire**

***Le seuil de détection :*** si la corrélation $R_{xy}$ dépasse un certain seuil $T$ le détecteur détermine que l'image $Iw(x,y)$ contient une marque $W(x,y)$.

$$R_{xy} > T \rightarrow W(x,y) \text{ est détectée.}$$
$$R_{xy} < T \rightarrow \text{pas de } W(x,y) \text{ détectée.} \quad \textbf{(3.2.3)}$$

***Filtrage :*** étant donné que le contenu de l'image peut être interféré avec la marque, spécialement dans les composantes basses fréquences, la fiabilité du détecteur peut être augmenté en appliquant un filtrage à l'image marquée avant la corrélation **[3]**, **[4]**, **[5]** .cela diminue la contribution de l'image dans le calcul de la corrélation .par exemple, l'utilisation d'un simple filtre détecteur de contour FIR $F_{edge}$ est suffisant.

$$F_{edge} = \begin{bmatrix} -1 & -1 & -1 \\ -1 & -10 & -1 \\ -1 & -1 & -1 \end{bmatrix} / 2 \qquad \textbf{(3.2.4)}$$

Les résultats expérimentaux que nous allons présenter ultérieurement dans ce chapitre montrent que l'application de ce filtre avant le calcul de la corrélation diminue d'une façon significative la probabilité d'erreurs même si la qualité visuelle de l'image est sérieusement affectée**[5]** , **[8]** .

### *Dissimulation d'un message :*

Jusqu'à présent nous avons vu comment marquer une image par un signal pseudo aléatoire c'est-à-dire utiliser toute l'image pour dissimuler un message d'un bit où on peut considérer que la présence de ce signal indique que le message est « 1 », et son absence indique que le message est « 0 ».

Une image est vue comme un bruit gaussien qui perturbe le signal *W* .en plus, l'image marquée peut être considérée comme un canal de transmission perturbé par un bruit Gaussien sur lequel un message est transmis. Dans ce cas-ci, la transmission fiable du message est théoriquement possible si son taux de l'information n'excède pas la capacité du canal, qui est donnée par **[45]** :

$$C_{ch} = W_b \log_2\left(1+\frac{\sigma_W^2}{\sigma_I^2}\right) \quad , \quad \textbf{bit/pixel} \qquad \textbf{(3.2.5)}$$

Ici, l'unité de $C_{ch}$ est le nombre de bits du message par le nombre des pixels de l'image et la bande passante $W_b$ est égale à un cycle par pixel .Toutefois, pour un système pratique **[37]** :

$$C_{ch} = W_b \log_2\left(1+\frac{\sigma_W^2}{\alpha.\sigma_I^2}\right), \quad \textbf{bit/pixel} \qquad \textbf{(3.2.6)}$$

Ici, $\alpha$ est un petit facteur qui est inférieur à 3 et supérieur a 1.Puisque le rapport signal sur bruit est nettement inférieur à 1, l'équation **3.2.6** peut être approximée à :

$$C_{ch} \approx \frac{1}{\ln 2}\left(\frac{\sigma_W^2}{\alpha.\sigma_I^2}\right), \quad \textbf{bit/pixel} \qquad \textbf{(3.2.7)}$$

Selon cette équation, il devrait être possible de stocker beaucoup plus d'information dans une image qu'un seul bit en utilisant la technique de base décrite dans la section précédente. Par exemple, un signal comprenant les nombres entiers {-*k*, *k}* ajoutés à l'image de 512x512 de Lena (le schéma 3.2.1) peut comporter approximativement 50, 200 ou 500 bits de données pour $k$ = 1.2 ou 3 respectivement et pour $\alpha = 3$.

Il y a plusieurs manières d'augmenter la capacité de la technique de base. La manière la plus simple de dissimuler une série de bits $b_0, b_1, ..., b_{n-1}$ dans une image : est de diviser l'image $I$ en $n$ images secondaires $I_0, I_1, ..., I_{n-1}$ et de marquer chaque image secondaire suivant la technique de base. Là où chaque marque représente un bit du message **[37]**, **[5]** et **[8]**. Ce procédé est représenté sur la figure **3.6.**

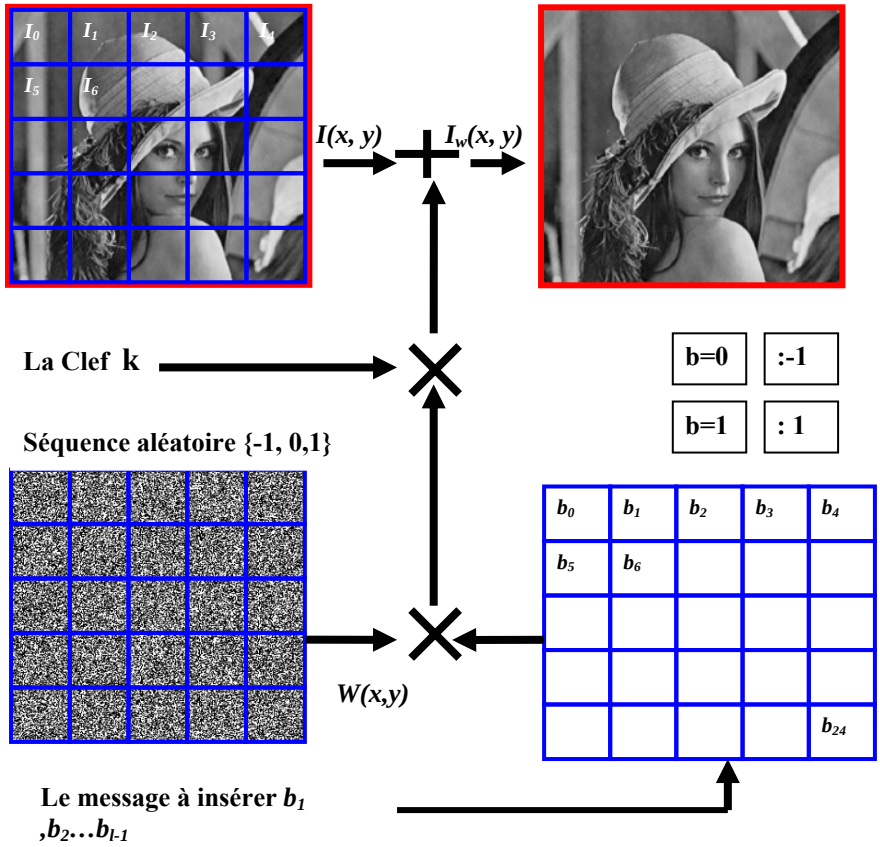



**Figure 3.6 dissimulation d'un message formé de 25 bits**

En utilisant l'équation **3. 2.7** nous pouvons calculer le nombre de Pixel $P$ requis ,par image secondaire, pour la détection fiable d'un simple bit dissimulé dans cette image secondaire:

$$P = \frac{\alpha \sigma_I^2 \ln 2}{\sigma_W^2} \text{ Pixels} \qquad \textbf{(3.2.8).}$$

Un bit du message peut être représenté de plusieurs manières. Une séquence pseudo aléatoire *RP* peut être ajoutée si le bit du message est égal à un, et on laisse l'image inchangée si le bit du message égal zéro. Dans ce cas-ci, le détecteur calcule la corrélation entre l'image secondaire et le modèle pseudo aléatoire et assigne la valeur « 1 » au message détecté si la corrélation excède un certain seuil T autrement on assume que le bit du message est « 0 ».

L'utilisation d'un seuil peut être évitée en ajoutant deux séquences pseudo aléatoires différentes $RP_0$ et $RP_1$ pour la dissimulation des deux bits du message 0 et 1. Le détecteur calcule maintenant la corrélation entre l'image secondaire et les deux séquences. La valeur du bit correspondant à la séquence qui donne la corrélation la plus élevée est assignée au bit du message. Dans **[37]** les deux modèles sont choisis de telle manière qu'ils diffèrent seulement dans le signe, $RP_0 = - RP_1$ Dans ce cas-ci, le détecteur doit calculer seulement la corrélation entre l'image secondaire et l'une des deux séquences; le signe de la corrélation détermine la valeur du bit du message.

Pour étudier l'effet du pré filtrage dans le détecteur, le facteur k de visibilité et le nombre de Pixel *P* par bit du message sur la robustesse du marquage, nous réalisons les expériences suivantes. Nous ajoutons d'abord une marque à une image avec la méthode de **[37]**. Après, nous compressons l'image marquée à l'aide de l'algorithme de compression JPEG **[28]**, où Q est le facteur de qualité de l'algorithme de compression est rendu variable. En conclusion, le message est extrait à partir de l'image compressée et comparée avec le message original dissimulé dans l'image.

### *Expérience 2* :

La première de ces trois expériences montre l'effet de l'application d'un pré filtrage (donné par Equation **3.2.4)** avant la détection du message qui est dissimulé avec un facteur d'invisibilité $k = 2$, et un nombre **P = 32x32** pixels par bit de message( taille des blocs). Sur la (figure **3.7)** les pourcentages d'erreurs provoquées par la compression JPEG sont tracés :

- ✓ pour un détecteur qui utilise ce pré filtrage
- ✓ et pour un détecteur sans pré filtrage.

On peut clairement voir que le pré filtrage augmente la robustesse du marquage d'une manière significative.

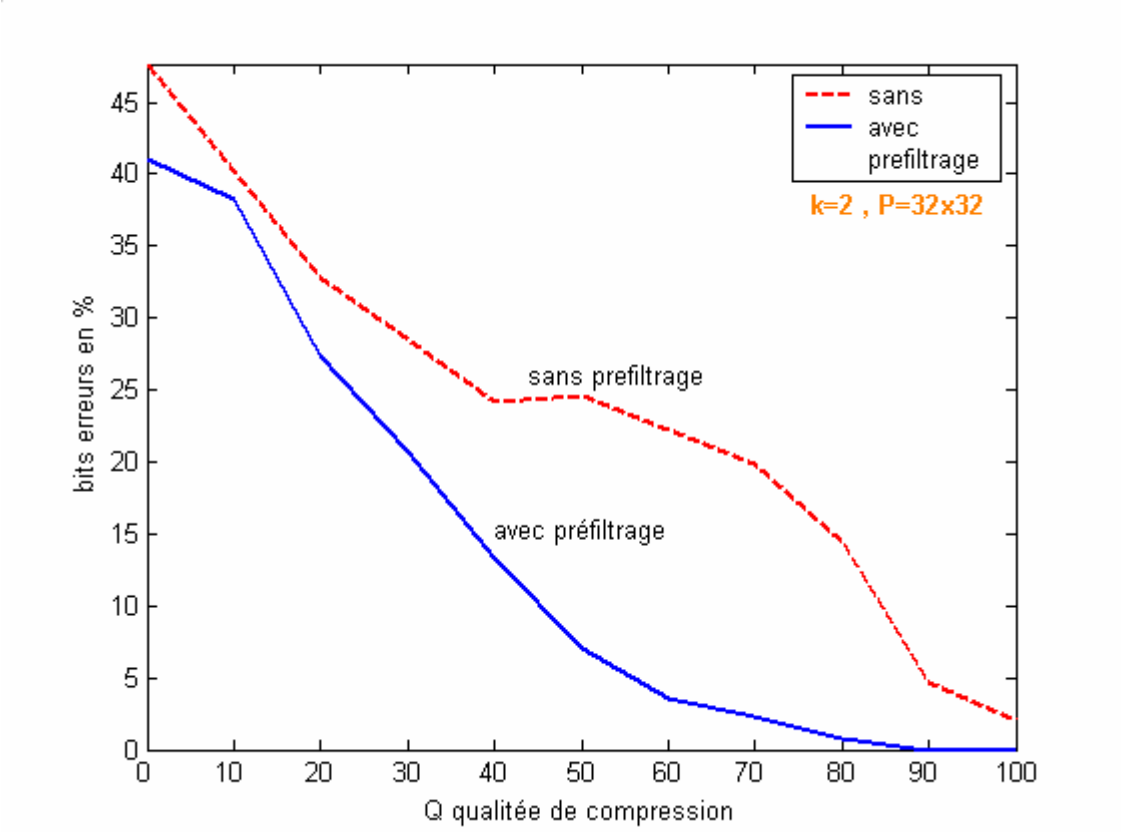



**Figure 3.7 variation du pourcentage des erreurs de détection en fonction de la qualité de compression de deux détecteurs l'un avec un pré filtrage et l'autre sans pré filtrage**

### *Expérience 3 :*

La deuxième expérience montre l'effet de l'augmentation du coefficient d'invisibilité k sur la détection pour un message dissimulé avec le nombre **P = 32x32** pixels par bit du message (taille des blocs), et détecté à l'aide d'un pré filtrage. De la figure **3.8** il découle que la robustesse du filigrane peut être améliorée sensiblement en augmentant le coefficient d'invisibilité k.

### *Expérience 4 :*

La troisième expérience montre que l'influence du nombre de Pixels *P* par bit du message sur la robustesse d'un marquage effectué avec un coefficient d'invisibilité $k = 2$ est détecté en utilisant un pré filtrage. De la figure **3.9** il découle que si on diminue la capacité du marquage (augmenter la taille des blocs) la robustesse du marquage augmente.

Une autre manière d'augmenter la capacité de la technique de base c'est l'utilisation de la technique d'étalement de spectre" Direct Séquence Code Division Multiple Access (DS-CDMA)" **[46]**, **[47]**, **[7]**, cette technique sera détaillée dans la partie suivante.

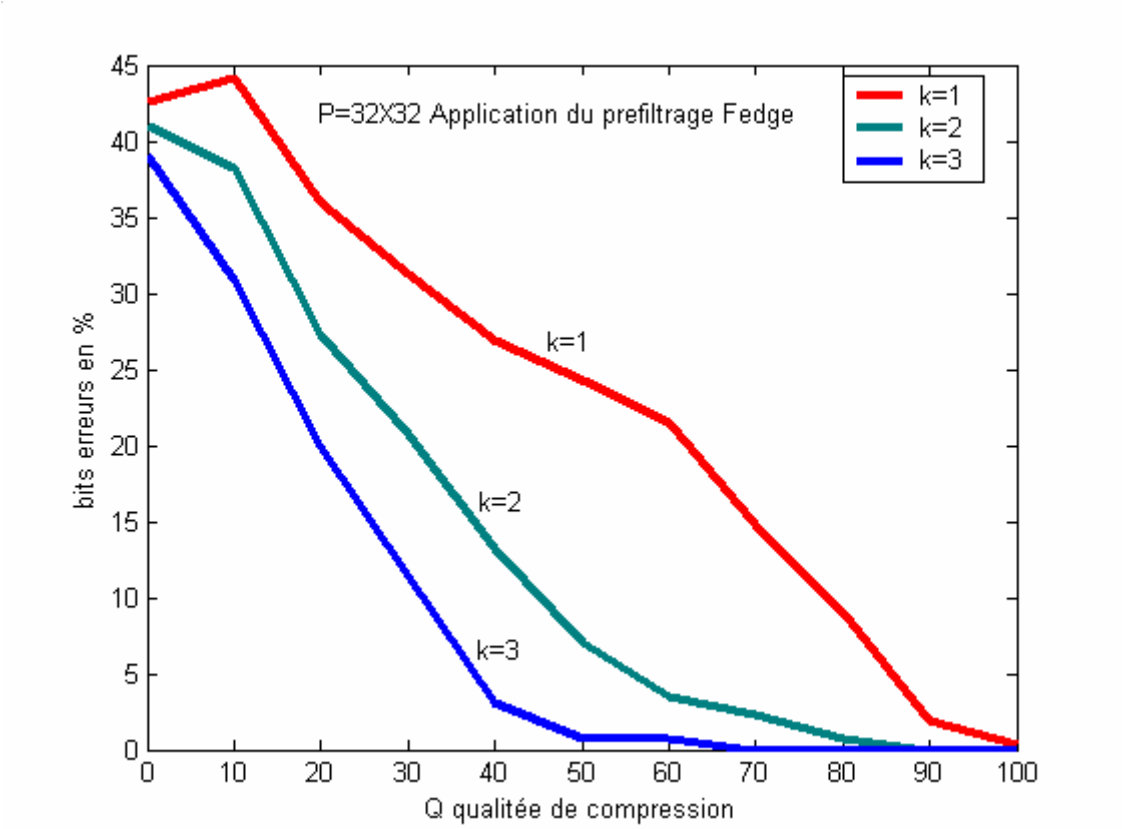



**Figure 3.8 l'effet de la variation du coefficient d'invisibilité k sur la robustesse du marquage**

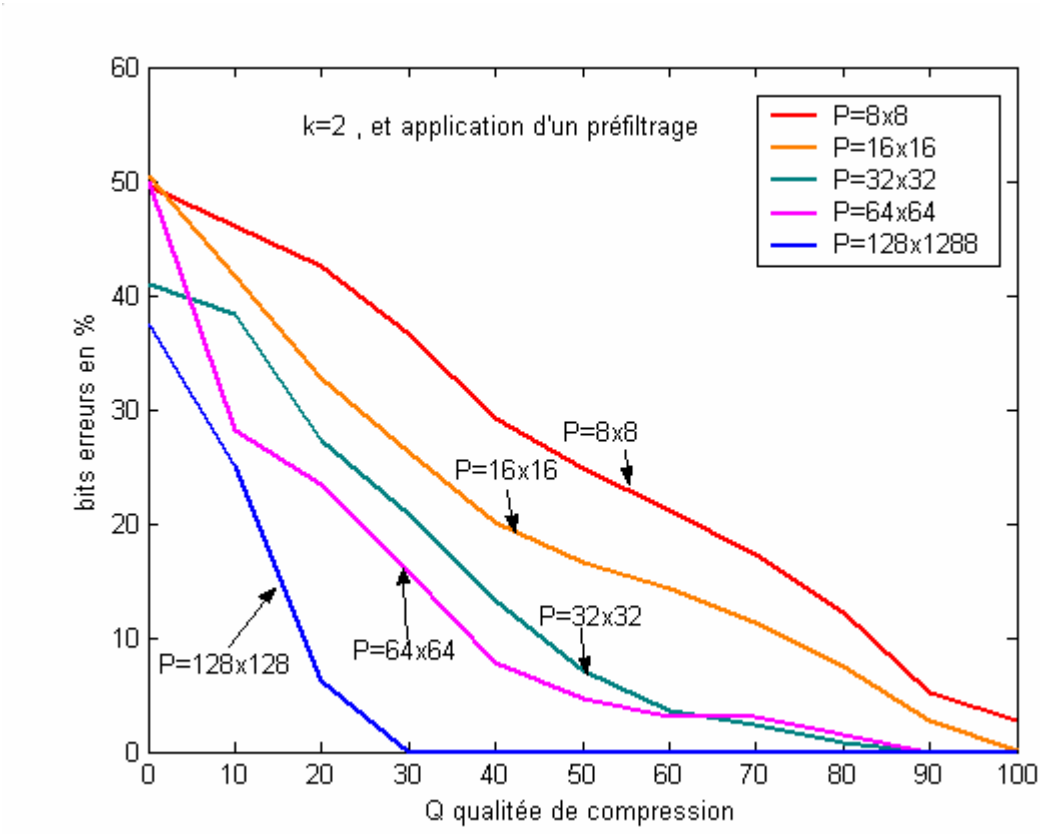



**Figure 3.9 variation de l'erreur de la détection en fonction de la taille des blocs**

## *3.2.2- Algorithme CDMA :*

***Les auteurs* :** cet algorithme est développé par F. Hartung et B. Girod **[7]** et amélioré par langelaar (**TDMA**) (Time Division Multiple Access) ensuite par Patrick Bas (**CDMA**) (Code Division Multiple Access).

***Détecteur* :** le détecteur n'a pas besoin de l'image originale pour détecter le message.

***La marque :*** est un ensemble de séquences aléatoires formés des éléments $\{-1,0,1\}$ ou seulement $\{-1,1\}$, les nombres réels (fractionnaires) peuvent être utilisés.

***Les sites :*** tous les pixels de l'image sont utilisés pour dissimuler un bit. Pour augmenter la capacité de dissimulation l'image est divisée en plusieurs blocs, et plusieurs couches.

***Le marquage :***

Cet algorithme appartient à la classe des algorithmes additifs et permet d'insérer et de détecter un message constitué de plusieurs bits. Le schéma de dissimulation du message est illustré dans la figure **3.10.**

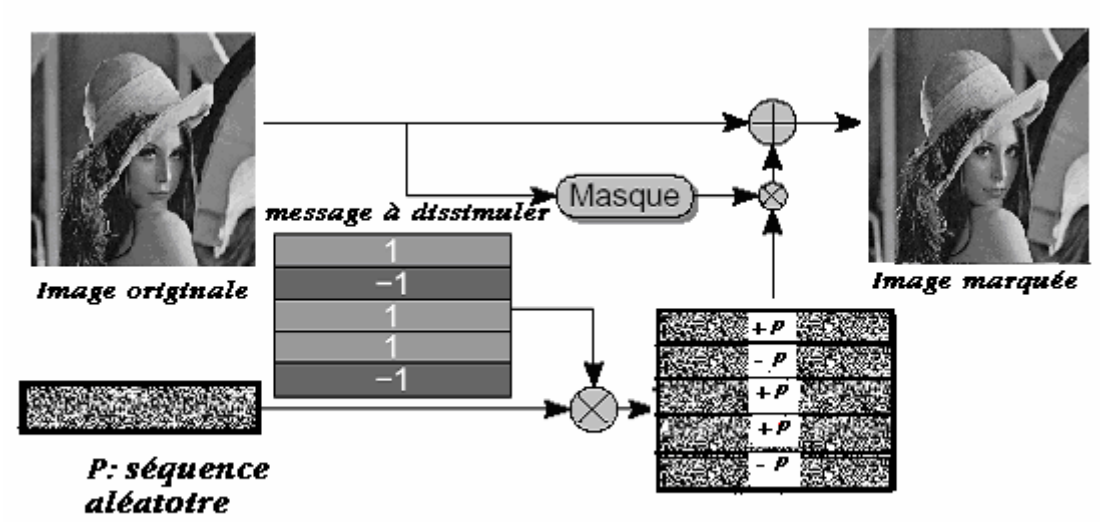



**Figure 3.10 schéma de marquage suivant l'algorithme de Hartung et Girot**

La technique CDMA (Code Division Multiple Access) est utilisée en communication numérique pour acheminer, dans un même canal et de manières simultanées, des signaux appartenant à des utilisateurs différents. Les signaux occupent tous la même bande de fréquence. Chaque utilisateur est identifié par une séquence aléatoire appartenant à la catégorie des M- séquences le message convoyés par l'utilisateur est modulée par la séquence aléatoire. Le signal transmis dans le canal est composé de la somme des signaux de chaque utilisateur. Le system CDMA permet d'augmenter ou de réduire le nombre d'utilisateur sans

configurer le système de transmission. Cette technique se différencie de la technique TDMA (Temporelle Division Multiple Access), utilisée par la technologie GSM, qui utilise une division temporelle pour différencier les utilisateurs figure 3.11.

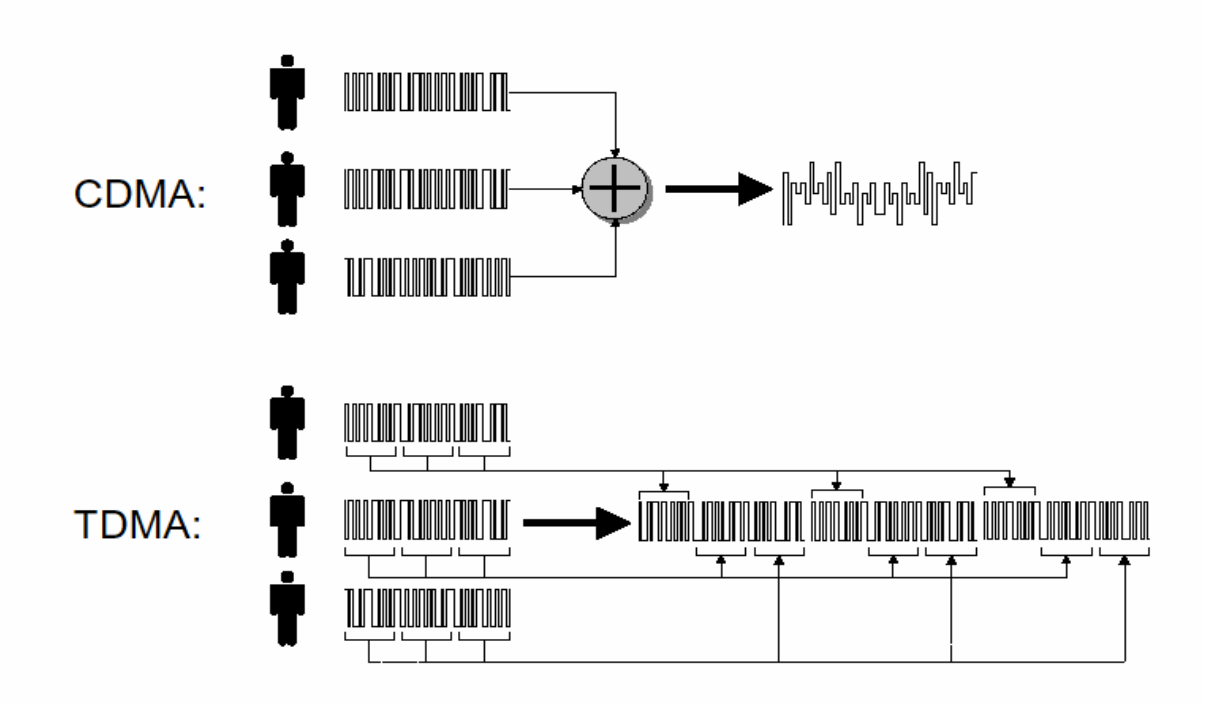



**Figure 3.11 Le schéma de comparaison entre les deux techniques CDMA et TDMA**

Cette technique et appliquée au marquage d'images numériques, et qui permettent de dissimuler un message de plusieurs bits au sein d'une seule image (un seul bloc) on allouant une partie du message à chaque séquence (utilisation de plusieurs séquences).l'idée est de généraliser l'algorithme apporté par Hartung et Girot en insérant une marque constituer de plusieurs séquences aléatoire (appelées couches).l'utilisation d'une telle stratégie dégage deux avantages :

1. la superposition des séquences permet d'augmenter la surface des blocs B (le nombre de pixels par blocs augmente) représentant chaque bit d'information.
2. la visibilité de la marque par pixel est définie comme étant le rapport entre l'écart type de la marque et la surface des blocs, décroît lorsque le nombre des couches augmente.

| | Variance | Ecart-Type | Surface | Visibilité / pixel |
|---|---|---|---|---|
| 1 couche | 1 | 1 | $N^2/64$ | $64/N^2$ |
| 2 couches | 2 | $\sqrt{2}$ | $N^2/32$ | $32\sqrt{2}/N^2$ |
| 4 couches | 4 | 2 | $N^2/16$ | $32/N^2$ |
| 8 couches | 8 | $2\sqrt{2}$ | $N^2/8$ | $16\sqrt{2}/N^2$ |

**Tableaux 3.1 la visibilité par pixel décroît en fonction du nombre de couches**

L'utilisation d'un algorithme multicouche entraîne une augmentation des valeurs maximales de la séquence résultante. Si la séquence aléatoire d'un algorithme monocouche n'est composée que de -1 et +1 une séquence constituée par superposition de 8 séquences (8 couches) peut avoir des valeurs appartenant à l'ensemble $\{\pm 8,\pm 6,\pm 4,\pm 2,0\}$. Par contre les valeurs crêtes apparaissent avec des probabilités plus faibles que celles proches de 0.

| Coefficient ajouté | +/-8 | +/-6 | +/-4 | +/- 2 | 0 |
|---|---|---|---|---|---|
| Probabilité | 1/256 | 8/256 | 28/256 | 56/256 | 70/256 |

**Tableaux 3.2 probabilité d'apparition des différents éléments d'une séquence à 8 couches**

### *Exemple :*

Ici, à chaque bit $b_i$ du message, on associe une séquence pseudo aléatoire indépendante *RPi*, de même taille que l'image. Cette séquence dépend de la valeur du bit, Ici nous employons la séquence *+RPi* si *bi* représente un 0 et *– RPi* si *bi* représente un 1. L'addition de toutes les séquences forme la marque à dissimuler. Avant d'ajouter la marque à une image, nous pouvons amplifier la marque par un facteur de gain ou la limiter à un certain rang. L'exemple suivant emploie 7 séquences pseudo aléatoires différentes pour inclure les 7 bits 0011010 du message.

```
RP0:-1 1 1-1-1 1-1-1 1 1-1   b0:0  →  +RP0:-1 1 1-1-1 1-1-1 1 1-1
RP1: 1 1-1-1 1-1-1 1 1-1 1   b1:0  →  +RP1: 1 1-1-1 1-1-1 1 1-1 1
RP2: 1-1-1 1-1-1 1 1-1 1-1   b2:1  →  -RP2:-1 1 1-1 1 1-1-1 1-1 1
RP3:-1-1 1-1-1 1 1-1 1-1-1   b3:1  →  -RP3: 1 1-1 1 1-1-1 1-1 1 1
RP4:-1 1-1-1 1 1-1 1-1-1 1   b4:0  →  +RP4:-1 1-1-1 1 1-1 1-1-1 1
RP5: 1-1-1 1 1-1 1-1-1 1 1   b5:1  →  -RP5:-1 1 1-1-1 1-1 1 1-1-1
RP6:-1-1 1 1-1 1-1-1 1 1 1   b6:0  →  +RP6:-1-1 1 1-1 1-1-1 1 1 1 +
                                       W  :-3 5 1-3 1 3-7 1 3-1 3
```

**Figure 3.12 Exemple de marquage base sur la technologie CDMA pour un message de 7 bits**

On peut extraire chaque bit du message en calculant la corrélation entre la séquence aléatoire et le bloc marqué. Si la corrélation est positive la valeur 0 est affectée au bit $b_i$ du message et si elle est négative une valeur 1 est affectée au message.

$W$ : -3 5 1 -3 1 3 -7 1 3 -1 3

$I$ : 98 98 97 98 97 96 97 96 95 94 94 +

$I_W$ : 95 103 98 95 98 99 90 97 98 93 97

$$E[(RP_0-E[RP_0])\cdot(I_W-E[I_W])] = +15.6 \rightarrow b_0=0$$
$$E[(RP_1-E[RP_1])\cdot(I_W-E[I_W])] = +16.4 \rightarrow b_1=0$$
$$E[(RP_2-E[RP_2])\cdot(I_W-E[I_W])] = -26.4 \rightarrow b_2=1$$
$$E[(RP_3-E[RP_3])\cdot(I_W-E[I_W])] = -3.1 \rightarrow b_3=1$$
$$E[(RP_4-E[RP_4])\cdot(I_W-E[I_W])] = +21.6 \rightarrow b_4=0$$
$$E[(RP_5-E[RP_5])\cdot(I_W-E[I_W])] = -23.6 \rightarrow b_5=1$$
$$E[(RP_6-E[RP_6])\cdot(I_W-E[I_W])] = +0.4 \rightarrow b_6=0$$

**Figure 3.13 Exemple d'extraction de la marque (CDMA)**

## *L'algorithme :*

L'algorithme de dissimulation se décompose des étapes suivantes :

1. génération de la séquence multicouche. le nombre des couches peut varier de 1(une seule couche, qui est le cas classique) à 8 couches .au delà de 8 couches les valeurs maximales deviennent plus importantes et la signature devient visible figure 3.14. dans notre exemple on a réalisé un marquage à 8 couches et 64 bits par couche figures 3.15 et 3.16.

Image marquée en utilisant 2 couches

Image marquéeen utilisant 20 couches

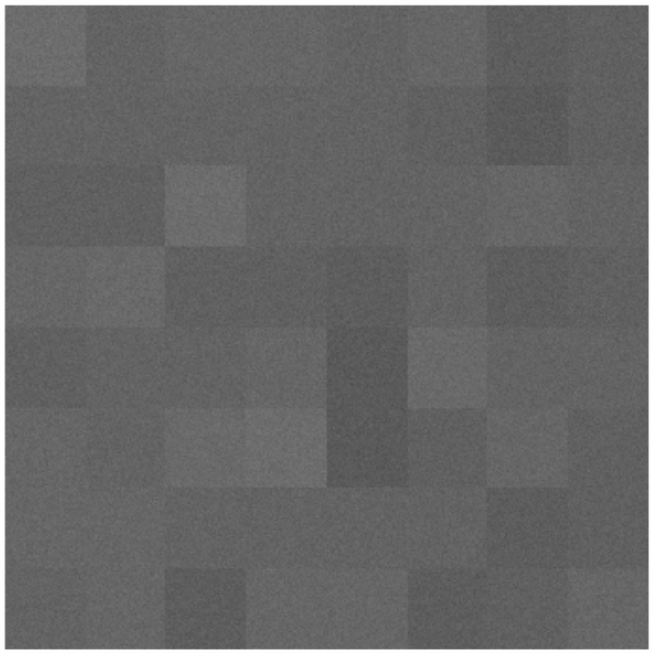
**Figure 3.14. À gauche l'image de Lena marquée en utilisant 2 couches et celle de droite en utilisant 20 couches (détérioration de la qualité d'image).**

2. la séquence aléatoire W est pondérée par un masque psycho visuel calculé en fonction de la variance de l'image originale pour obtenir la séquence $W_P$ .Le masque peut être obtenu en calculant les variances locales de l'image considérées au voisinage 5x5 .

$$W_P(i,j) = W(i,j).M(i,j) \qquad (3.2.9)$$

Image marquée en utilisant 8 couches

**Figure 3.15 images de Lena marquée en utilisant 8 couches (en remarque que la marque commence à être visible)**



La séquence à 8 couches

**Figure 3.16 une séquence aléatoire à 8 couches ,64 bits par couche**

3. la séquence obtenu est alors multipliée par un coefficient de visibilité **K** qui permet de régler la puissance de la marque .il conditionne la robustesse du marquage mais aussi la visibilité de la signature.

$$W_C(i,j) = k.W_P(i,j) \qquad \textbf{(3.2.10).}$$

4. la séquence $W_C$ est ajoutée à l'image originale pour former l'image marquée.

$$I_W = I + W_C \qquad \textbf{(3.2.11).}$$

Toutes ces étapes sont illustrées dans le schéma de la figure 3.17.

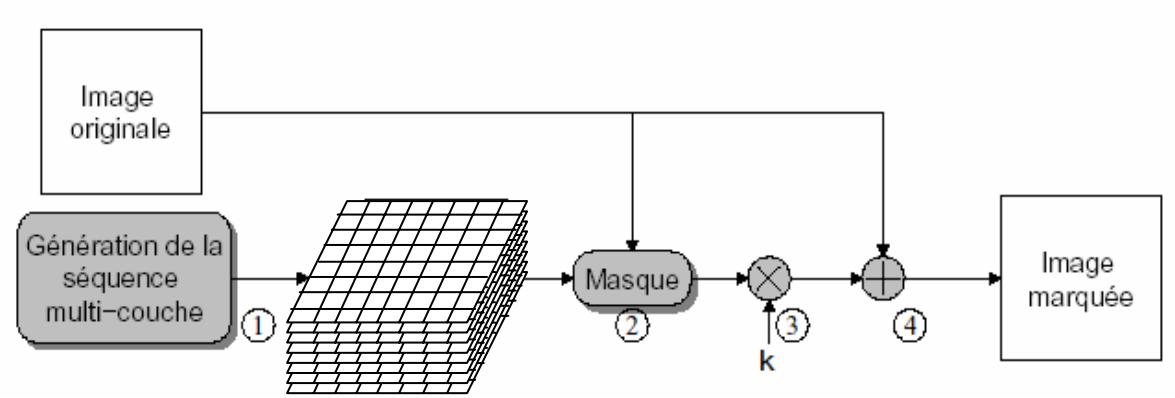



**Figure 3.17 principe de dissimulation d'un message suivant l'algorithme CDMA**

### *La détection :*

Puisque cet algorithme est additif la détection se fait par le calcul de la corrélation entre l'image marquée et la séquence aléatoire. Cette détection ce divise en plusieurs étapes figure 3.18.

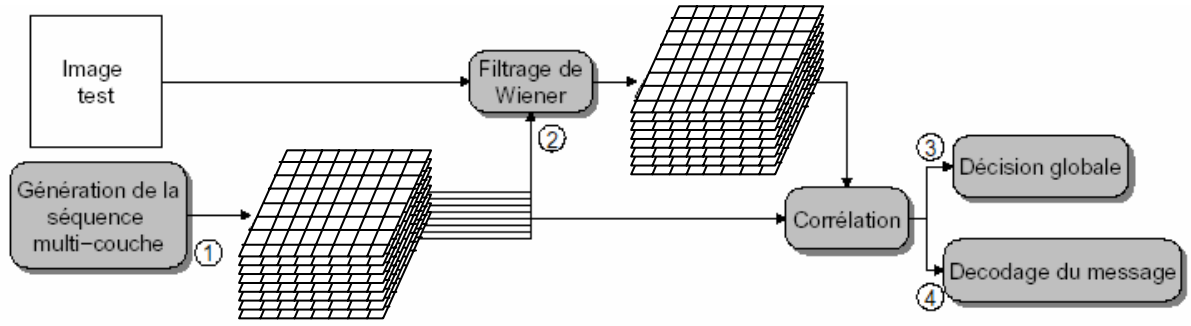



**Figure 3.18 Principes de détection de la marque et extraction du message pour l'Algorithme CDMA.**

1. La séquence aléatoire multicouche est générée comme lors de l'étape de la dissimulation du message.
2. On applique un pré filtrage à l'image marquée pour améliorer la détection.
3. On applique une détection globale qui permet de confirmer la présence de la signature.
4. Si la détection est positive, on procède à la lecture du message.

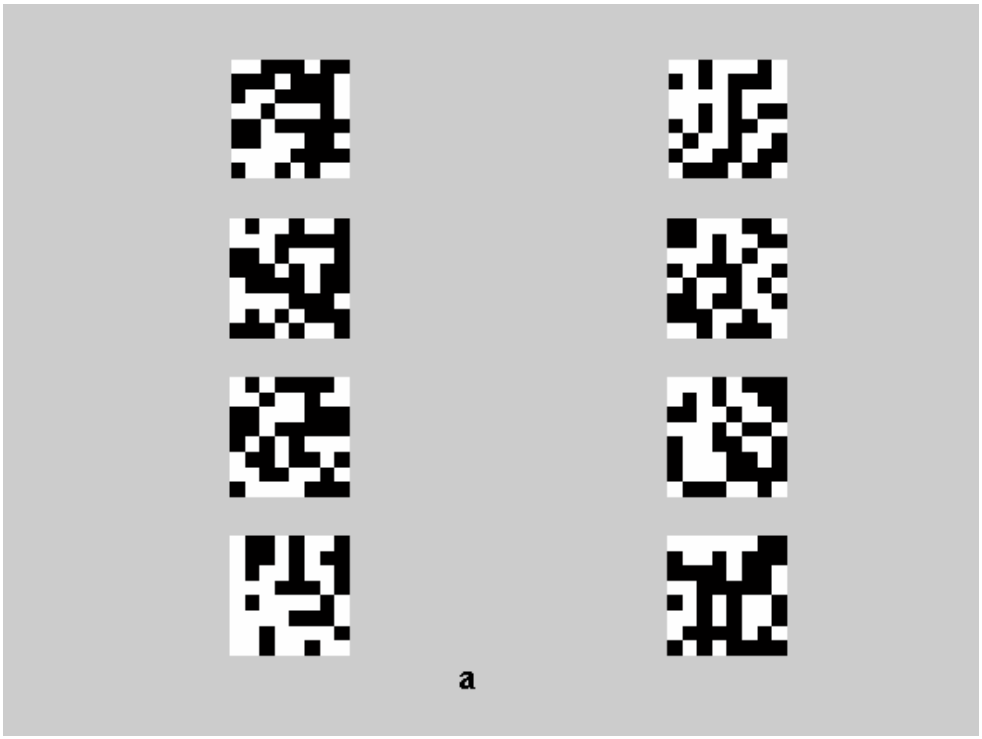



**Figure 3.19.a les 8 couches d'un message dissimulé**

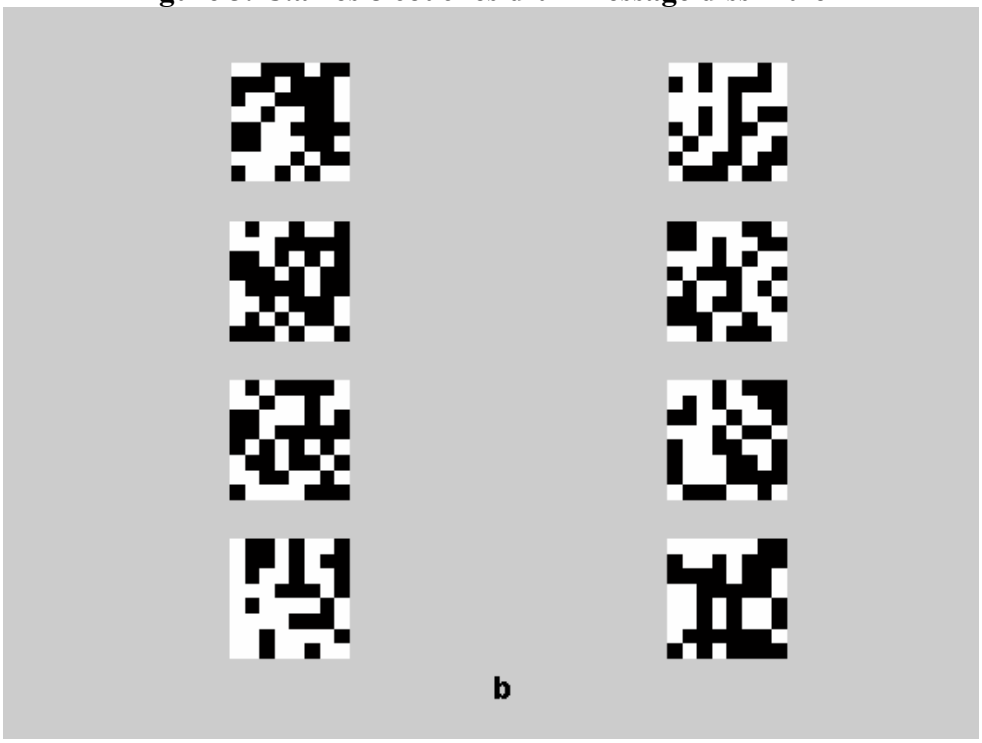



**Figure 3.19.b. les 8 couches du message détecté**

Sur les deux images de la figure **3.19**, les 8 couches d'un message formé de 8x8x8 bits sont représentées dans la figure **3.19.a** chaque couche contient 8x8 bit du message . Ce message est pris aléatoirement et le nombre total des bits est 512bits qui peut être un message (texte), logo ou une autre image. Un message d'une telle taille est impossible à être dissimulé sans l'utilisation de la technique CDMA (Code Division Multiple Access).

Dans la deuxième partie de la figure **3.19** (partie **b**) le message détecté est représenté de la même manière que le message d'origine. On remarque, par comparaison, qu'il y a des erreurs de détection sur quelques bits.

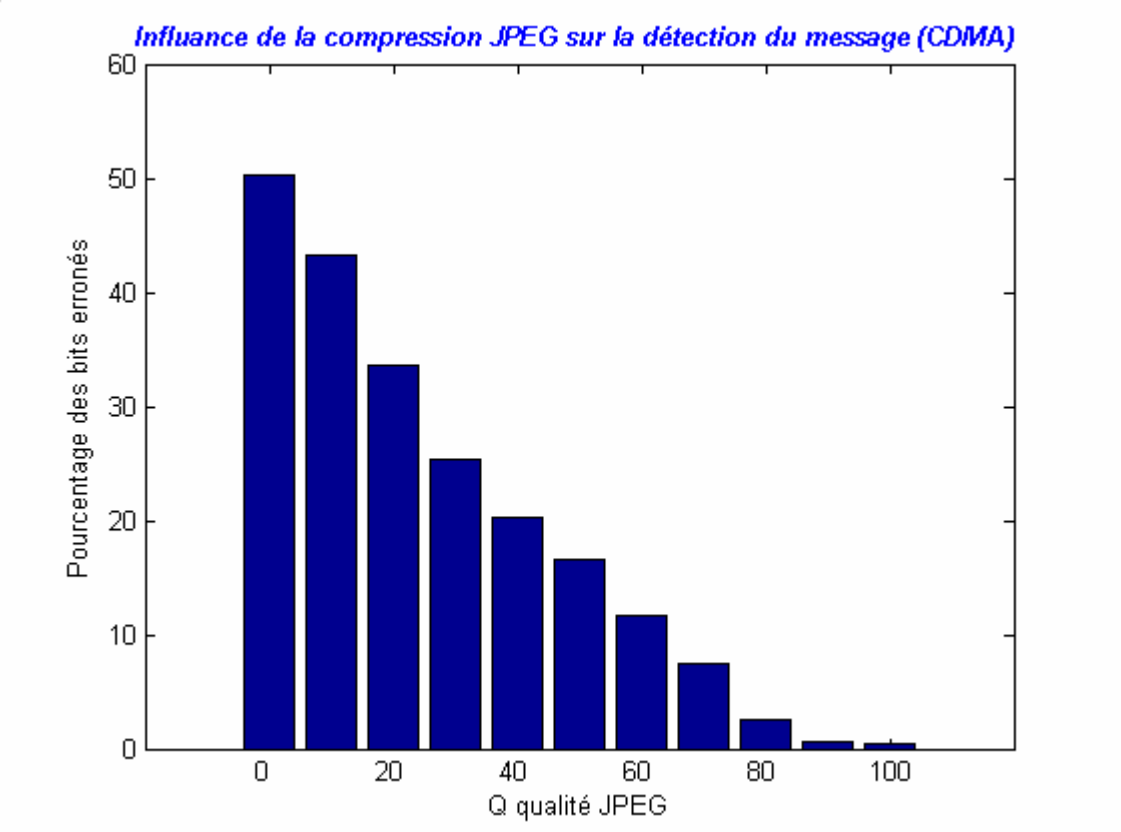



**Figure 3.20 pourcentages des bits erronés en fonction de la qualité Q de la compression JPEG**

La figure 3.20, montre que pour une compression d'un facteur de qualité supérieur à 50% l'erreur sur la détection est très petite et permet aisément de déchiffrer le message après la détection, si le message est une autre image ou logo cella nous donne une très bonne qualité d'image à la réception. Notons que pour une compression de l'image marquée d'un facteur de qualité inférieur à 50%, commence déjà à donner une très mauvaise qualité d'image qui ne nécessite pas une protection, étant donné quelle ne sera plus utilisable.

Pour montrer l'amélioration que peut apporter la technique CDMA, par rapport à la technique de base, nous avons réalisé une expérience où on a dissimulé le même message en utilisant les deux techniques. Une détection du message ensuite est réalisée en comptabilisant le nombre de bits erronés figure 3.21.

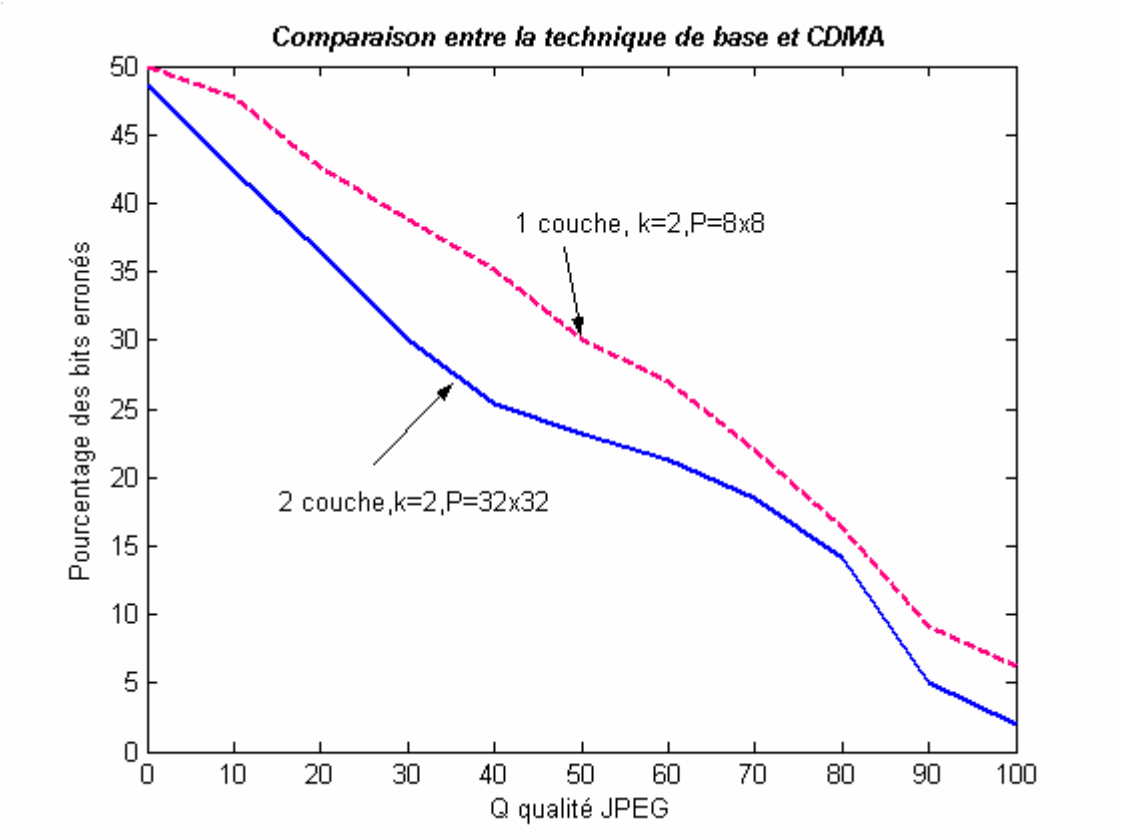



**Figure 3.21 Comparaison entre la technique de base et la technique CDMA.**


**Figure 3.22 à gauche l'image de Lena marquée par la technique CDMA et compresser (Q=30%), et à droite la même image marquée par la technique de base et compressée (Q=50%), les deux images donnent après extraction du message le même taux d'erreurs.**

Le message, dissimulé, a une taille de 512 bits. Dans le premier cas tout le message se trouve sur une seule couche dans des blocs de 8x8 pixels. Dans le deuxième cas la technique utilise deux couches chaque bits est dissimulé dans un bloc de 32x32 pixels.

On remarque de la figure 3.21 que la robustesse de la technique CDMA est plus grande que celle de la technique de base pour toutes les valeurs de Q (qualité de la compression JPEG).

## *3.2.3- Algorithme de KUTTER :*

***Les auteurs :*** cet algorithme a été développé par Martin Kutter, Frédéric Jordan et Frank Bossen **[14]**.

***Détecteur :*** l'image originale n'est pas nécessaire pour la détection de la marque et l'extraction du message.

***La marque :*** est un message constitué de plusieurs bits rendus redondant en les répétons plusieurs fois .deux bits sont ajoutés au début du message (zéro et un) .ces deux bits sont utilisés dans la phase d'extraction du message.

***Les sites :*** cet algorithme manipule la composante bleue des pixels constituants l'image .et cela donnes N x M positions possibles pour dissimuler un bit du message .ces positions sont visitées en effectuant un scanning en zigzag de toute l'image figure 3.23. Ce scanning est adopté pour rendre le marquage indépendant des dimensions de l'image. Le choix des sites est effectué aléatoirement mais pas qualitativement.

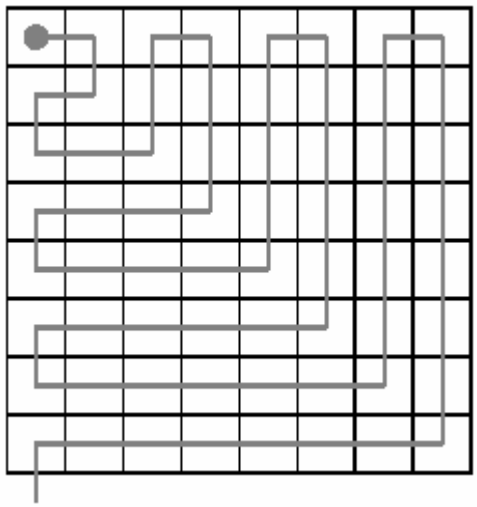


**Figure 3.23 .Scanning des positions possibles pour la dissimulation des bits dans l'algorithme de kutter**

### *Le marquage :*

Pour dissimuler un bit $S_i$ d'un message dans une image $I=\{R, G, B\}$ suivant l'algorithme de kutter, on modifie la valeur de la composante bleue d'un pixel $p\ (i, j)$ d'une fraction de la

valeur de sa luminance 3.2.12. Ce pixel est choisi aléatoirement et dépend d'une clef secrète *K* (utilisée comme une valeur initiale d'un générateur des séquences pseudo aléatoire).

$$L = 0.299R + 0.587G + 0.114B \,. \qquad \textbf{3.2.12.}$$

Suivant la formule suivante :

$$B_{ij} \leftarrow B_{ij} + (2s-1)L_{ij}q \,. \qquad \textbf{3.2.13.}$$

**q est le coefficient d'invisibilité de la marque.**

Ce qui signifie que si le bit du message est égal à « 1 » on effectue une modification sur la composante bleue de l'image sinon le pixel est laissé intact d'une part, et d'autre part avant d'effectuer cette opération un nombre aléatoire $\alpha$ est généré et comparé à un seuil $\delta$, qui représente la probabilité de présence de la marque, et le pixel est marqué suivant les règles suivantes :

- ✓ **Si $\alpha < \delta$ on procède au marquage de la position *(i, j)*.**
- ✓ **Si $\alpha > \delta$ on ne marque pas la position *(i, j)* et on passe a la position suivante.**
- ✓ **Chaque bit est dissimulé Cr fois pour rendre le marquage plus redondant.**

**Où $0 \le \alpha \le 1$ et $\delta$ est un réel choisit entre 0 et 1.**

## *Expérience1 :*

Dans cette expérience nous avons procédé à la dissimulation d'un message, constituée de 100 bits dont le premier bit est « 0 » et le deuxième est un « 1 », dans l'image de Lena figure 3.24. En utilisant les paramètres suivants :

- ✓ **Mess=[0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 1 1 0 1 0 0 0 1 1 1 1 1 ] ,le message dissimulé.**
- ✓ **q = 0.1, coefficient d'invisibilité.**
- ✓ **$\delta$ = 0.55 probabilité de dissimulation.**
- ✓ **Cr = 1000, répétition du marquage de chaque bit du message.**
- ✓ **Image hôte = Lena (512x512) soit N=512 et M=512.**

Image original

**Figure 3.24 Image originale (Lena 512x512 pixels)**

Image marquée avec repetition 1000 fois

**Figure 3.25 Image marquée en utilisant l'algorithme de kutter.**

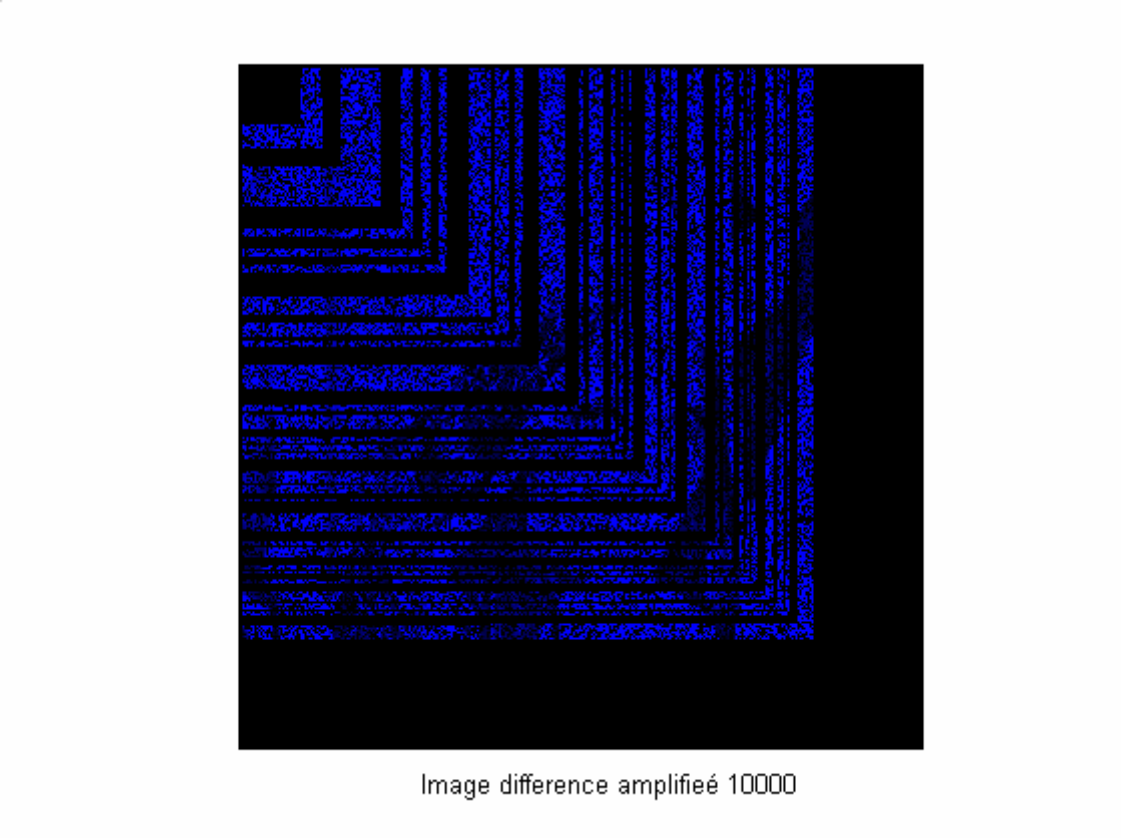



**Figure 3.26. La différence entre l'image originale et l'image marquée**.

De la figure 3.26 on remarque que le marquage d'une image commence par le coin supérieur gauche suivant le scanning décrit précédemment, et que les zones marquées sont celles qui correspondent aux bits « 1 » du message. En plus la silhouette de Lena montre que le marquage est proportionnel à la luminance de l'image et la couleur bleue des pixels de cette image signifie que seulement la composante bleue de l'image originale est modifiée.

### *Détection :*

Le détecteur essaye d'extraire une marque reconstituée $S''$ à partir d'une image probablement marquée $I''$ .

Pour extraire un bit $S''_K$ , d'un message dissimulé, de la position $(x, y)$ on compare la valeur actuelle de la composante bleue de ce pixel $b''(x, y)$ avec une prédiction de cette valeur $\hat{b}''(x, y)$. Les valeurs de la composante bleue du voisinage sont utilisées pour le calcul de la prédiction. Dans cet algorithme on utilise un voisinage en forme de croix de dimension trois **c=3**.

$$\hat{b}''(x,y) = \frac{1}{4c}\left(-2b''(x,y)\sum_{i=-c}^{+c} b''(x+i,y) + \sum_{k=-c}^{+c} b''(x,y+k)\right) \quad \textbf{3.2.14.}$$

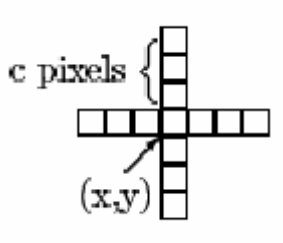



**Figure 3.27. Forme de voisinage utilisée pour le calcule de prédiction**

pour chaque bit on calcule la prédiction Cr fois étant donnée qu'on a marqué ce bit Cr fois au paravent. C'est la moyenne de la différence entre les valeurs prédites et les valeurs locales qui est considérée.

$$\sigma_k'' = 1/i\sum_{l=1}^{i}[\hat{b}''(x_l,y_l) - b''(x_l,y_l)]$$

Sachant que les deux premiers bits sont respectivement $S_0 = 0, S_1 = 1$.on peut calculer le seuil de détection $\sigma = \frac{\sigma_0'' + \sigma_1''}{2}$ qui sera utilisé pour la détection de tous les autres bits suivant la formule 3.2.15.

$$S_k'' = \begin{cases} 0 \ si \ \sigma_k'' < \sigma \\ 1 \ si \ \sigma_k'' > \sigma \end{cases} \qquad \textbf{3.2.15.}$$

Ainsi tout le message est détecté.

Sur la figure 3.28 les valeurs des prédictions $\sigma_k''$ sont représentées .il est claire que les valeurs correspondantes aux bits « 1 » du message sont au dessus de la droite $\sigma_k'' = \sigma$ et celles qui correspondent aux bits « 0 » du message sont au dessous de cette droite .

***Expérience 2 :*** afin de montrer la robustesse de cet algorithme contre la compression JPEG on procède au marquage de l'image originale de Lena. Une détection du message est réalisée après chaque compression en variant le coefficient de qualité de compression Q de 0 à 100 avec un pas de 10.Une comparaison est effectuée, entre le message original et le message détecté pour chaque valeur de Q, afin de déterminer le nombre de bits erronés. On trace la courbe de l'erreur de détection en fonction de la qualité de compression figure 3.29.

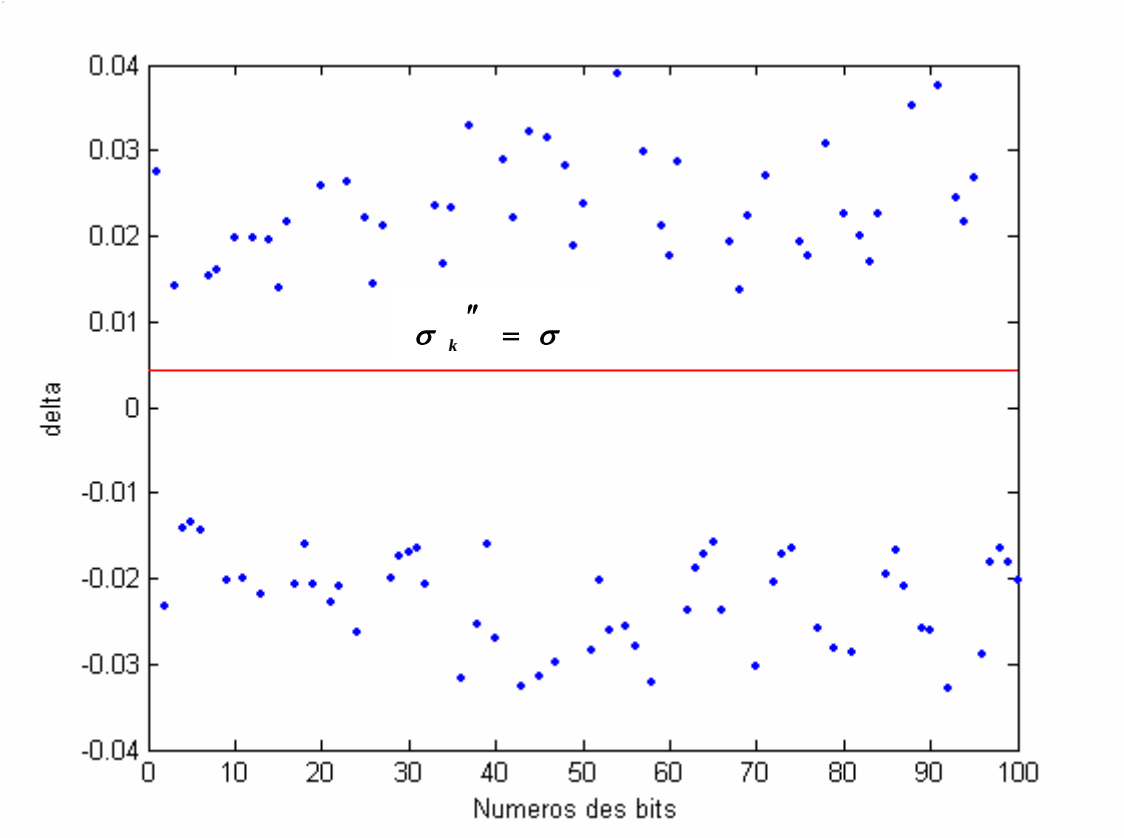



**Figure 3.28. Représentation des $\sigma_k''$ valeurs des prédiction en de tous les bits du message**

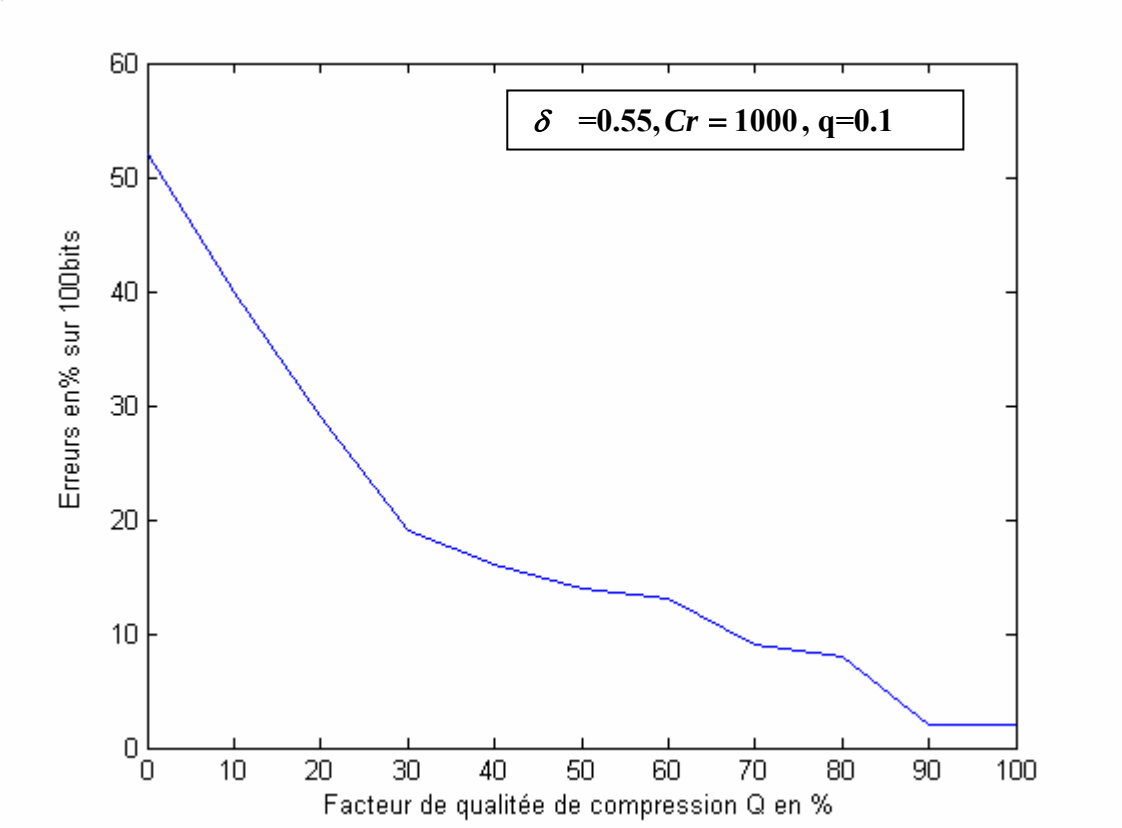



**Figure 3.29. Influence de la compression JPEG sur la détection du message.**

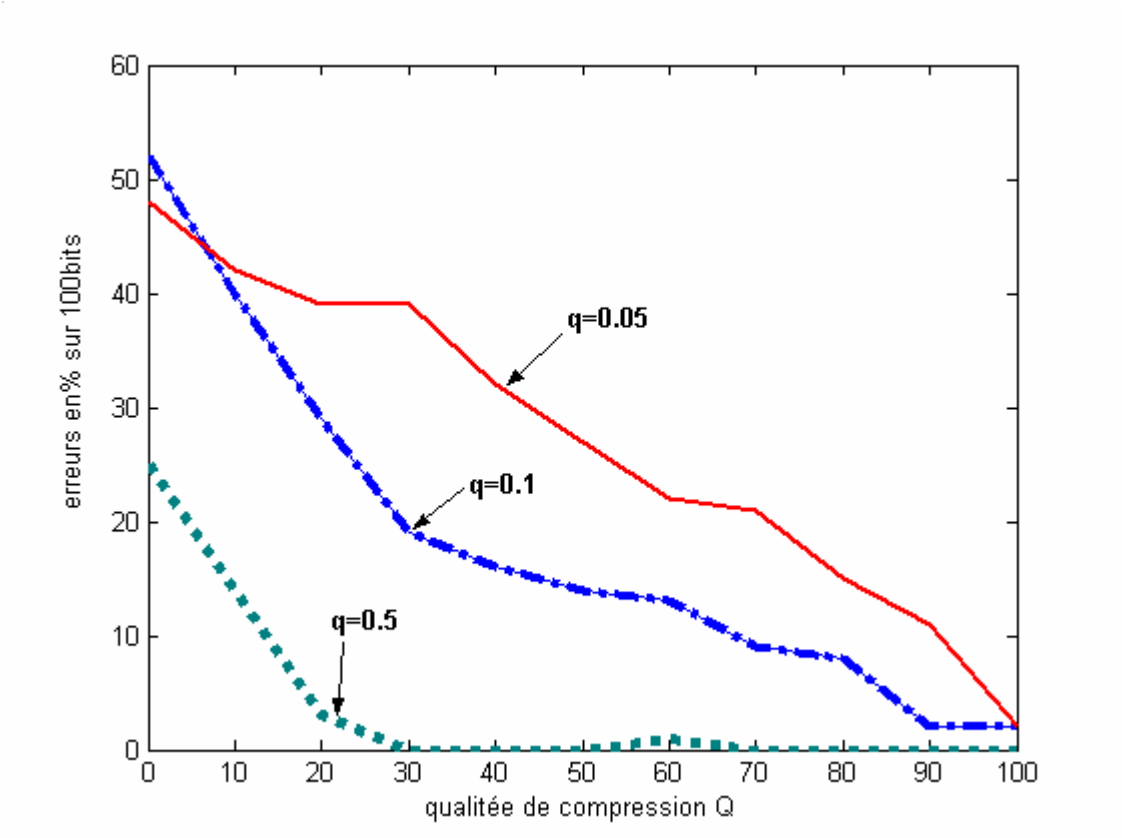



**Figure 3.30.influence du coefficient d'invisibilité q sur la robustesse contre la compression JPEG**

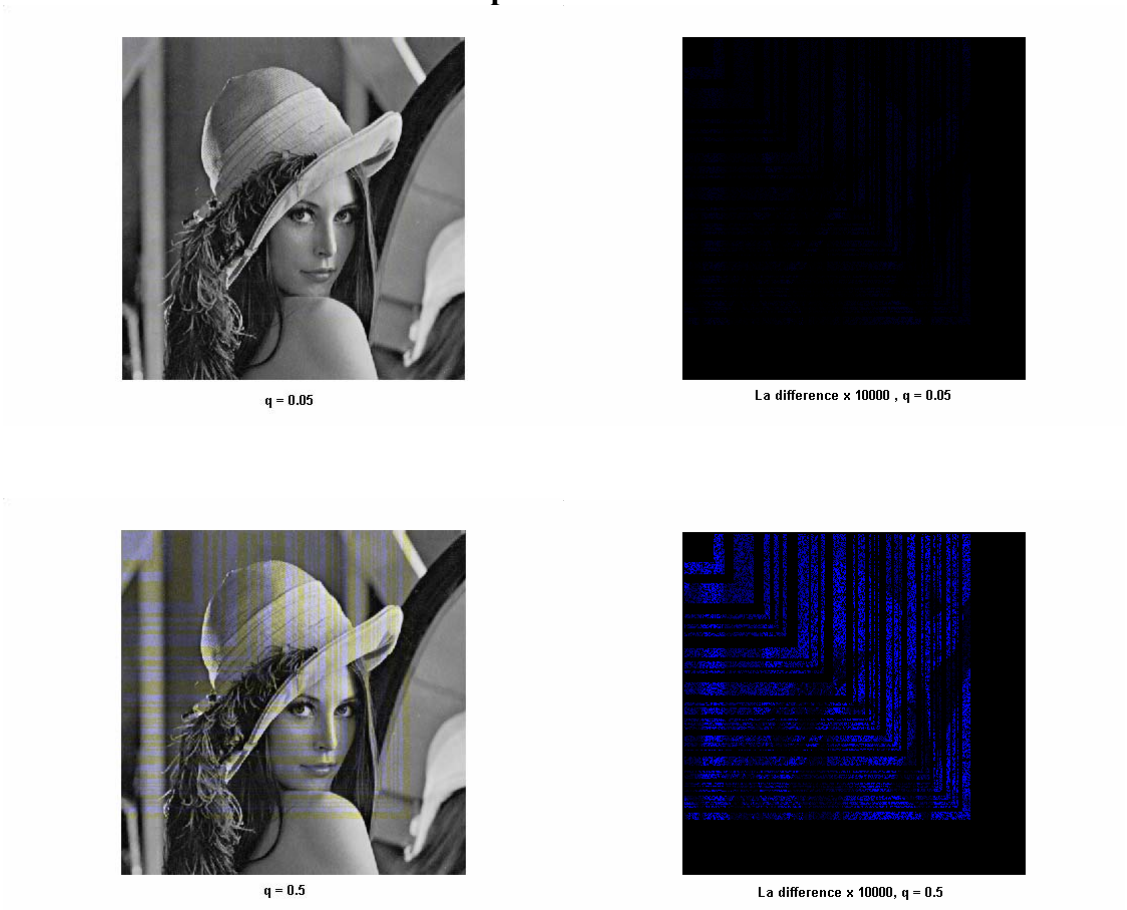



**Figure 3.31.influence de q sur la qualité de l'image marquée**

On remarque que la détection du message se fait avec une faible erreur (<20%) tant que la qualité de compression est (>30%) qui est un très bon résultat. car, au dessous de cette valeur l'image commence a être inutilisable et par conséquent les raisons du marquage disparaissent.

***Expérience 3 :*** pour déterminer l'influence du coefficient d'invisibilité de la marque q on effectue plusieurs marquage en variant ce dernier .sur la figure 3.30 trois valeurs de q sont utilisées 0.05, 0.1 et 0.5 pour tracer les courbes (nombre de bits erronées en fonction de la qualité de compression Q).cette figure montre que si on augmente ce coefficient la robustesse de l'algorithme contre la compression JPEG augmente mais de la figure 3.31 ce coefficient influe aussi sur la visibilité de la marque (augmentation de la visibilité).Ce qui est contradictoire au critères du marquage . Pour cela : il faut faire un compromis entre la robustesse de l'algorithme et la visibilité de la marque. La valeur q = 0.1 est plus ou moins acceptable.

***Expérience 4 :*** sur la figure 3.32 sont tracées les courbes des erreurs des détections en fonction du coefficient de qualité de compression Q correspondantes aux différentes valeurs de Cr (le nombre de répétition de marquage Cr =1, 10, 100, 400, 600,1000 et 1400).on remarque que pour de faibles valeurs de Cr l'algorithme de kutter est moins robuste contre l'attaque par compression JPEG .par contre, cet algorithme devient plus robuste pour de fortes valeurs de Cr ce qui montre l'utilité de la répétition du marquage de chaque bit.

Ce nombre est aussi lié aux dimensions de l'image et à la valeur de $\delta$ (la probabilité de dissimulation qui diminue les positions possibles de la dissimulation si elle est faible).

***Expérience 5 :*** l'algorithme de kutter pressente une robustesse contre l'attaque par rotation. L'utilisation des deux bits « 0 » et « 1 » au début de chaque message dissimulé est utilisée pour déterminer l'angle de la rotation qu'a subie l'image marquée, en calculant la différence entre les deux valeurs $\sigma_0''$ et $\sigma_1''$ qui doit être maximale si on effectue une rotation de même angle vers le sens inverse. Dans la figure 3.33 la différence $\sigma_0''$ - $\sigma_1''$ est calculée en balayant toutes les valeurs possibles de rotation (de -180° à +180°) d'une image marquée et pivotée d'un angle égal a 10° figure 3.34 .on remarque que cette différence est maximale pour un angle égal à -10° ce qui signifie que cette image est marquée et pivotée de 10°. Après la détection de cet angle il est facile ensuite de détecter le message dissimulé.

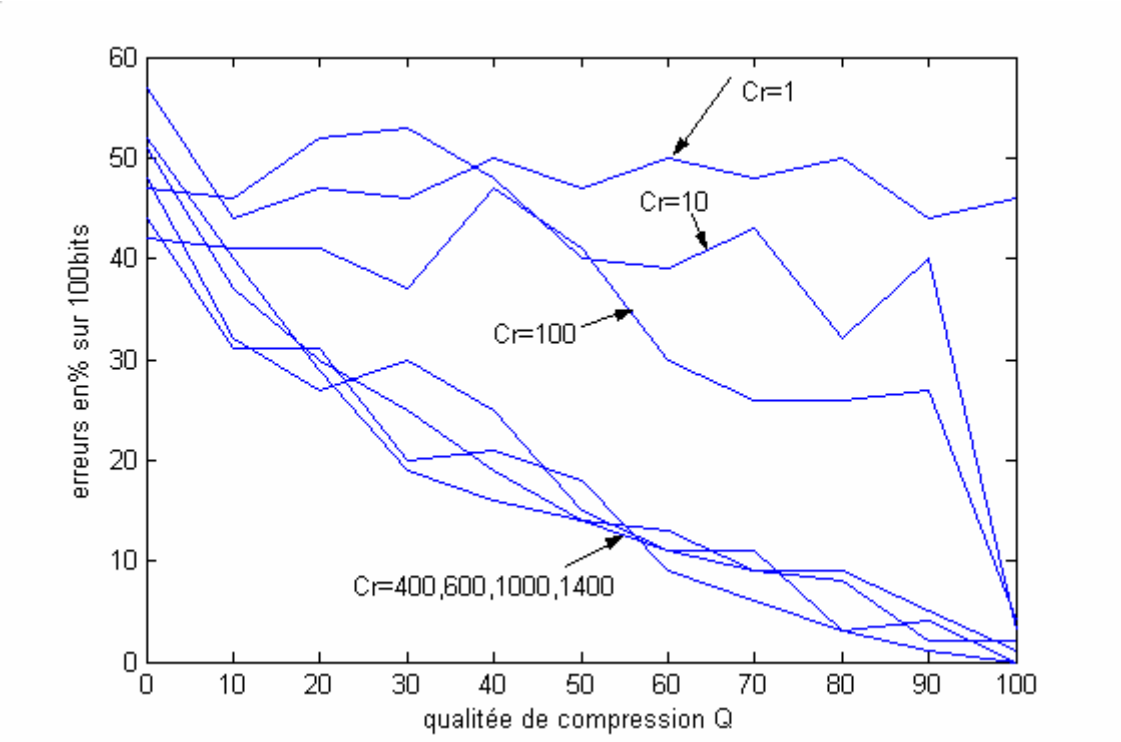



**Figure 3.32. Influence du nombre de répétition du marquage de chaque bit**

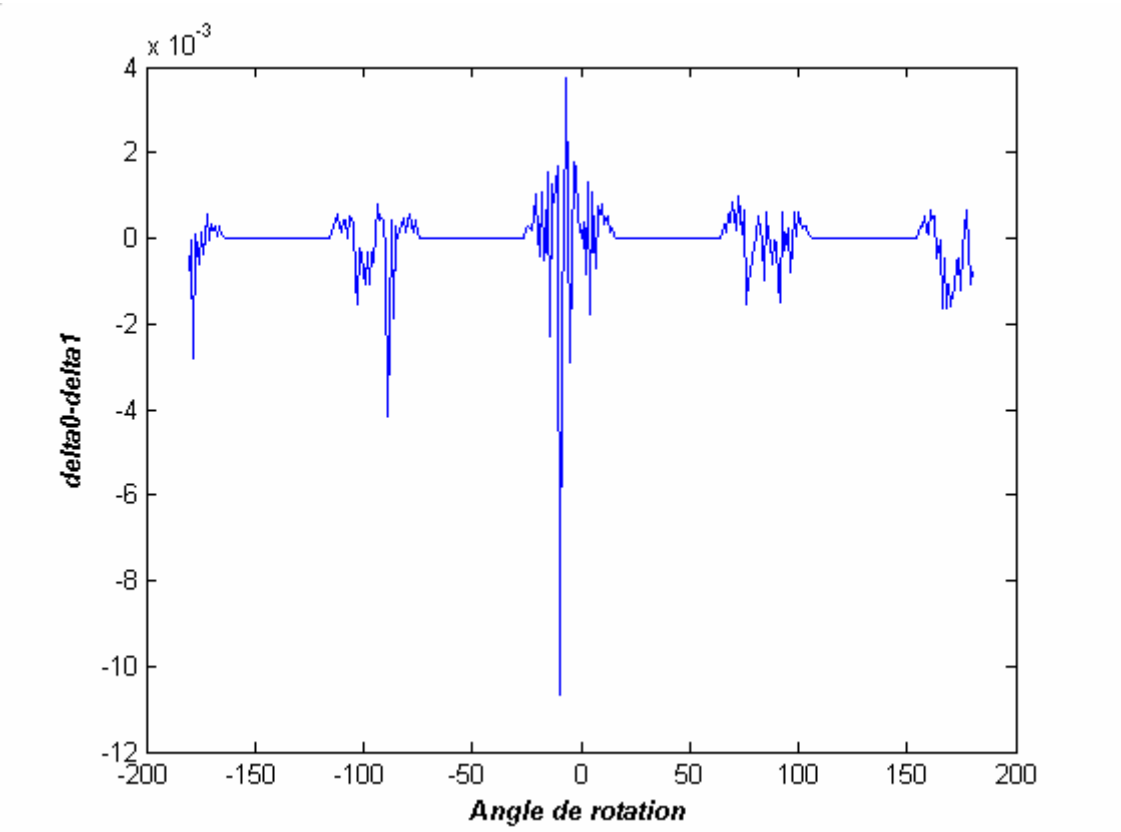



**Figure 3.33. Détection de l'angle de rotation utilisée comme attaque contre l'algorithme de kutter**

**Figure 3.34. Image de Lena marquée et pivotée de 10°**

## *3.2.4- Algorithme LSB :*

***Les auteurs :*** Des algorithmes de marquage plus sophistiqués qui se servent de la modification du LSB (les bits les moins significatifs) peuvent être trouvés dans **[4]**, **[19]**, **[20]**, **[21]** et **[23]**.

***Détecteur :*** l'image originale est nécessaire pour la détection de l'image (ou message) dissimulé, ou bien la connaissance du nombre et des positions des bits utilisés pour le marquage.

***La marque :*** le message dissimulé peut être une image ou un texte sous la forme d'une série de bits (binaires).

***Les sites :*** cet algorithme utilise un ou plusieurs bits de la valeur de la luminance de chaque pixel de l'image originale (en niveaux de gris) comme des sites de marquage.

***Le marquage :*** Le marquage se fait en suivant les étapes suivantes :

1. Lecture de la valeur de la luminance du pixel (x, y) de l'image originale.

2. Annuler les NB bits les moins significatifs de cette valeur.
3. Lecture de la valeur de la luminance du pixel (x, y) correspondant de l'image à dissimuler.
4. Faire un décalage à droite de cette valeur de 8-NB bits.
5. Faire la somme des deux valeurs résultantes.

En résumé, il s'agit de remplacer les NB bits moins significatifs de l'image originale par les NB bits les plus significatifs de l'image a dissimulée figure 3.34b

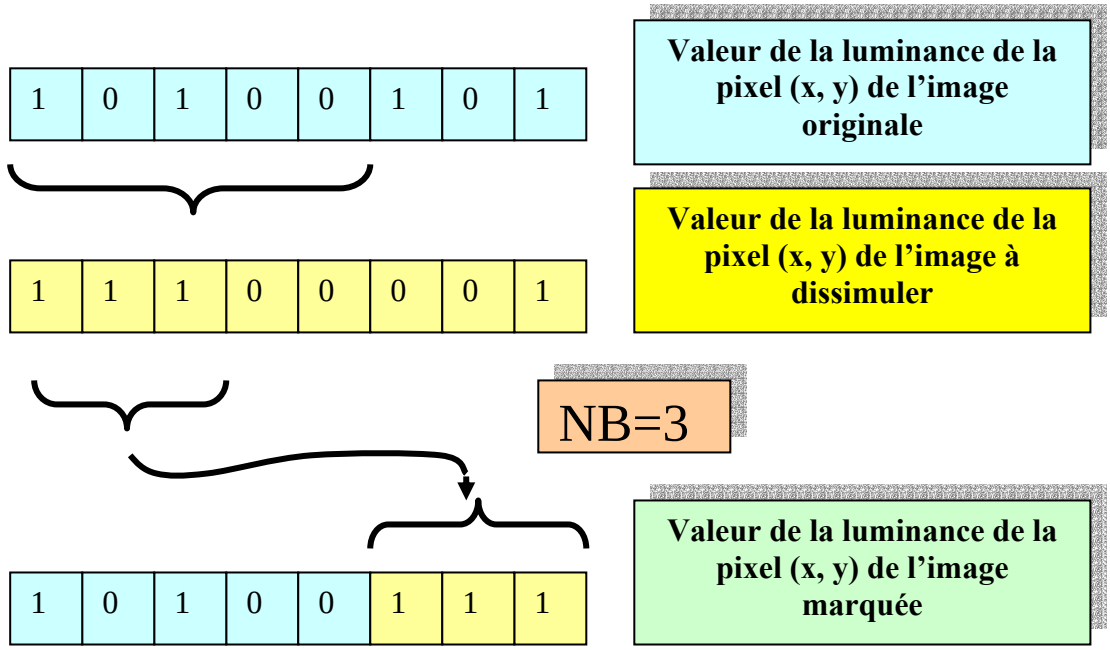
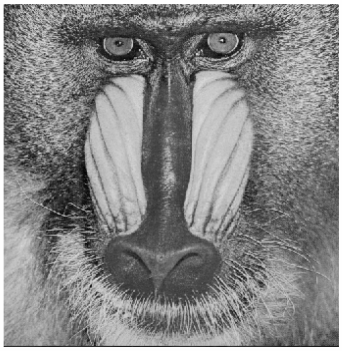



**Figure 3.34b Algorithme LSB**

Ces techniques de dissimulation ne sont pas très sécurisées et pas très robustes contre les techniques de traitement parce que les bits les moins significatifs peuvent être facilement remplacés par une séquence aléatoire, enlevant ainsi les bits dissimulés.

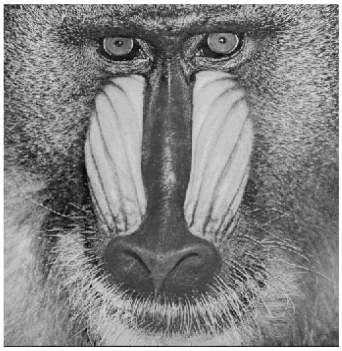
### *Détection :*

La détection du message se fait en effectuant un décalage à gauche de 8-NB bits. Plus NB est grand, plus la qualité de l'image extraite est meilleure, plus le message dissimulé est visible sur l'image marquée. Il faut faire donc un compromis entre la visibilité de la marque et la qualité de l'image extraite en choisissons la bonne valeurs de NB figure 3.35.



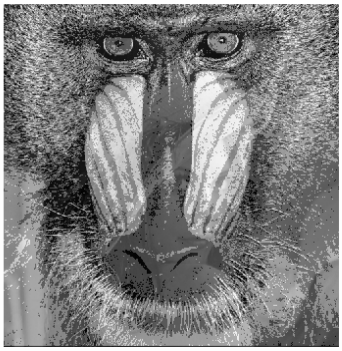
a - Image marquée avec NB=1

a - Image marque NB=1



b - Image marquée NB=2

b - Image marque NB=2



c - Image marquée avec NB=6

c - Image marque NB=6

d - Image marquée avec NB=7

d - Image marque NB=7

**Figure 3.35.Images marquées a gauche et les images extraites à droite**

# 3.3- Algorithmes dans le domaine fréquentiel :

Les techniques décrites dans la section précédente peuvent également être appliquées dans d'autres domaines non spatiaux. Chaque domaine possède des avantages et des inconvénients. Dans **[48]** la phase de la transformée de Fourier discrète (DFT) est utilisée pour dissimuler une marque, car les phases des coefficients de la DFT sont plus importantes que les amplitudes pour l'intelligibilité d'une image. La dissimulation d'une marque dans les composantes les plus importantes d'une image améliore la robustesse du marquage, la présence de la marque dans ces composantes importantes de l'image signifie une dégradation sévère de la qualité de l'image pour retirer la marque. La deuxième raison d'utiliser les phases des valeurs de la DFT est qu'elle est bien connue de la théorie de communication, et que souvent la modulation de phase possède l'immunité contre le bruit supérieur en comparaison avec la modulation d'amplitude **[48]**.

Beaucoup de techniques de marquage utilisent la modulation d'amplitude de DFT en raison de sa propriété de translation invariable **[49]**, **[50]**, **[51]**, **[52]**, **[53]**, **[46]** et **[47]**. Puisque les translations cycliques de l'image dans le domaine spatial n'affectent pas L'amplitude de la DFT, la marque dissimulée dans ce domaine sera une translation invariable et, au cas où une technique CDMA (Code Division Multiple Access) serait utilisée, elle est même légèrement résistante au recadrage. En outre, la marque peut directement être dissimulée dans la bande des moyennes fréquences les plus importantes.

Enfin le filigrane peut facilement être dépendant du contenu de l'image en modulant les coefficients d'amplification en fonction des amplitudes de la DFT $| I(u\ v) |$.

## 3.3.1- Algorithme de base (DFT) :

***Les auteurs :*** cette technique à été utilisée par plusieurs algorithmes Alexander Herrigel **[49]** et **[50]**, Shelby Pereira **[51]**, J.J.K. Ó Ruanaidh **[52]**, **[53]**, **[46]** et **[47],** I.J. Cox **[54]**.

***Détecteur :*** l'image originale est nécessaire pour la détection du message. La détection se fait par calcul de la similitude.

***La marque :*** dans sa version la plus simple cet algorithme utilise une série de nombres réels. En pratique, on génère une marque avec des éléments qui suivent une distribution $N(0,1)$ (ou $N(\mu,\sigma^2)$ représente une distribution normale avec une moyenne $\mu$ et une variance $\sigma^2$ ).

***Les sites :*** toutes les valeurs des modules de la DFT sont des sites possibles .de préférence et pour les raisons évoquées précédemment les modules de la DFT représentant les Moyennes fréquences sont souvent utilisées figure 2.9.

***Le marquage :*** le marquage se fait de la manière suivante figure 3.36:

- ✓ Calculer les coefficients DFT de l'image.
- ✓ Insérer la marque suivant la formule suivante :

$$\left| I_w(u,v) \right| = \left| I(u,v) \right| .(1 + \alpha . W(u,v)) \qquad 3.3.1$$

De préférence on choisit les plus grands coefficients.

- ✓ Calculer la transformée de Fourrier inverse IDFT.

$I_{x,y}(u,v)$ : Les coefficients DFT (modules) de l'image originale.

$I_{W_{x,x}}(u,v)$ : Les coefficients DFT (modules) marquées.

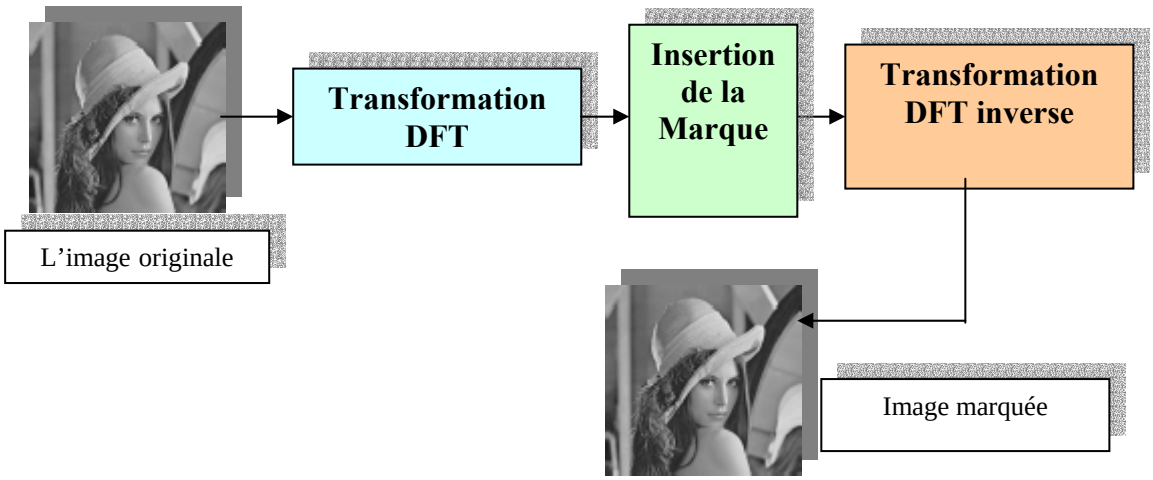



**Figure 3.36 marquage dans le domaine fréquentiel.**

Ici, *W (u, v)* est une séquence pseudo aléatoire a 2-dimension.et $\alpha$ représente le facteur d'amplification de la marque. Maintenant, la modification d'un coefficient de la DFT (Discrete Fourier Transform) n'est pas fixe mais proportionnelle à l'amplitude du coefficient de la DFT. Les plus petits coefficients de la DFT sont à peine affectés, tandis que les plus grands coefficients de DFT sont affectés plus sévèrement grâce à la formule de marquage 3.3.1.

Puisque la marque est principalement dissimulée dans les plus grands coefficients de la DFT, les composantes les plus significatives de l'image, la robustesse du filigrane est grande.

Notez que la symétrie des coefficients de Fourier doit être préservée pour s'assurer que les données de l'image seront très bien évaluées après la transformation inverse et le retour au

domaine spatial. Si le coefficient | $I$ ($u$, v) | dans une image de N $x$ M pixels est modifié selon l'équation 3.3.1. Sa contre- partie | $I$ ($N$ - $u$, $M$ - v) | doit être modifié de la même manière.

**(a)** **(b)**

**Figure 3.37 a- image de Lena fortement marquée et b- la différence $I - I_W$**

***La détection :*** la détection et l'extraction de la marque se fait de la maniéré suivante.

- ✓ Calcul des coefficients de la DFT (modules) de l'image marquée.
- ✓ Calcul de la différence entre les modules des coefficients de la DFT de l'image marquée et les modules des coefficients de l'image originale correspondants pour avoir le message dissimulé $\boldsymbol{X}^*$.
- ✓ Mais par raison de la transformation de Fourier, de Fourier inverse et des attaques possibles le message détecté ne peut être égal au message dissimulé (algébriquement).pour cela un calcul de similitude est obligatoire pour faire une comparaison entre les deux messages 3.3.2.

$$sim(\boldsymbol{X}, \boldsymbol{X}^*) = \frac{\boldsymbol{X}.\boldsymbol{X}^*}{\sqrt{\boldsymbol{X}^*.\boldsymbol{X}^*}} \qquad \textbf{3.3.2.}$$

Sur la figure 3.38 est représenté la réponse du détecteur pour 1000 signaux générés par une clef variante de 1 à 1000.les valeurs des similitudes sont toutes faibles sauf pour la valeur 100 avec laquelle est généré le signal dissimulée dans l'image. Dans cet exemple tous les modules des coefficients de la DFT de l'image sont utilisés, $\alpha$ =0.1 et le message dissimulé est un signal pseudo aléatoire d'une distribution normale $\boldsymbol{N(0,1)}$ et généré avec une clef (100).

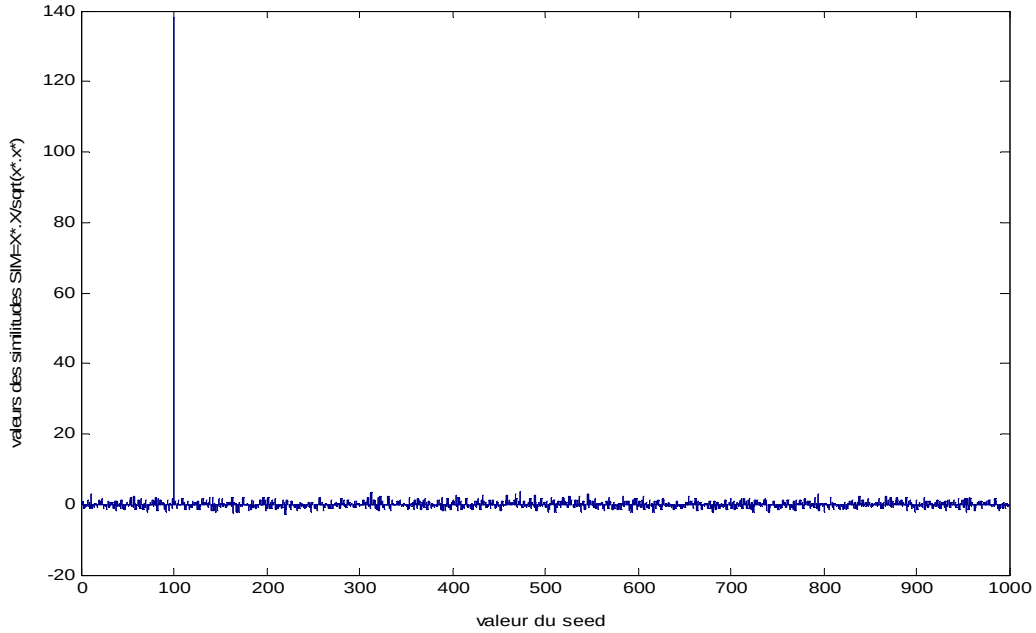



**Figure 3.38. Réponse du détecteur à une image marquée avec une clef =100.**

## *3.3.2- Algorithme de COX (DCT) :*

***Les auteurs :*** Cet algorithme a été développé par Ingemar J. Cox, Joe Kilian, Tom Leighton et Talal Shamoon. **[17] [55]**.

***Détecteur :*** l'image originale est nécessaire pour la détection du message. La détection se fait par calcul de la similitude.

***La marque :*** cet algorithme utilise une série de nombres réels. En pratique, en génère une marque dont les éléments suivent une distribution $N(0,1)$ (ou $N(\mu,\sigma^2)$ représente une distribution normale avec une moyenne $\mu$ et une variance $\sigma^2$ ).une distribution alternative peut être utilisée tel que, choisir uniformément les éléments de la marque entre, $\{1,-1\}$ $\{0,1\}$ ou $[0,1]$.

***Les sites :*** toutes les valeurs des modules de la DCT sont des sites possibles .de préférence les ***n*** plus grands modules des coefficients DCT sont utilisés.

***Le marquage :*** le marquage se fait en réalisant l'extraction des ***n*** plus grands coefficients DCT de valeurs $V = v_1,...,v_n$ de l'image **D**, dans lesquels on insert la marque $X = x_1,...,x_n$ pour obtenir une nouvelle séquence de coefficients marquée $V' = v_1',...,v_n'$ .on remet en place ensuite $V'$ dans l'image à la place de $V$ pour obtenir l'image marquée figure 3.39.

L'insertion de $\boldsymbol{X}$ dans $\boldsymbol{V}$ pour obtenir $\boldsymbol{V'}$ se fait par l'une des trois formules suivantes 3.3.3

$$\textbf{1-} \quad v_i^* = v_i + \alpha . x_i$$

$$\textbf{2-} \quad v_i^* = v_i (1 + \alpha . x_i) \qquad \textbf{3.3.3}$$

$$\textbf{3-} \quad v_i^* = v_i (e^{\alpha . x_i})$$

$\alpha$ est le coefficient d'amplification de la marque, on remarque que la force du marquage est proportionnelle aux valeurs des coefficients de la DCT dans les deux dernières équation 2 et 3. L'équation ne peut pas être approprié dans le cas où les valeurs de $\boldsymbol{V}$ varient entre $\mathbf{10^6}$ (Additionner 100 dans ce cas n'est pas suffisant pour constituer une marque) et **10** (Additionner 100 dans ce cas provoque une distorsion de cette valeur), pour cela la marque doit être ajouter d'une manière proportionnelle à la valeur du coefficient DCT.

L'insertion basée sur les deux dernières formules est plus robuste contre une telle différence d'échelle.

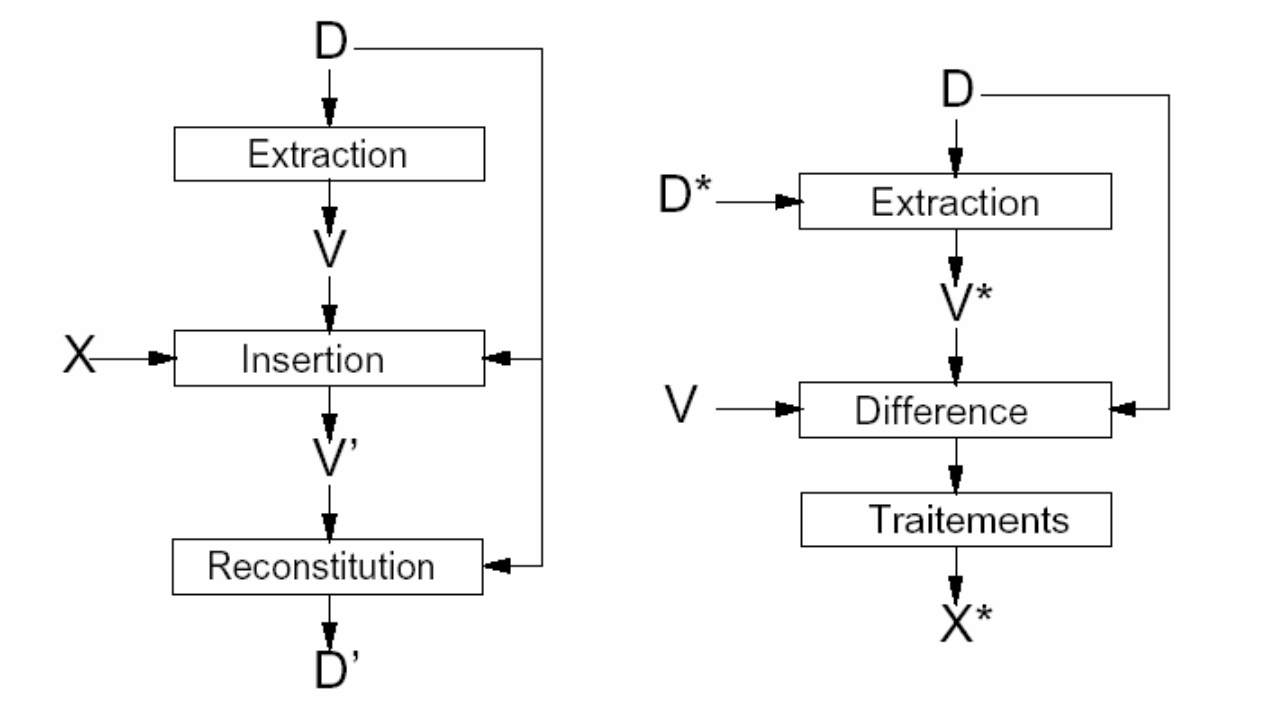
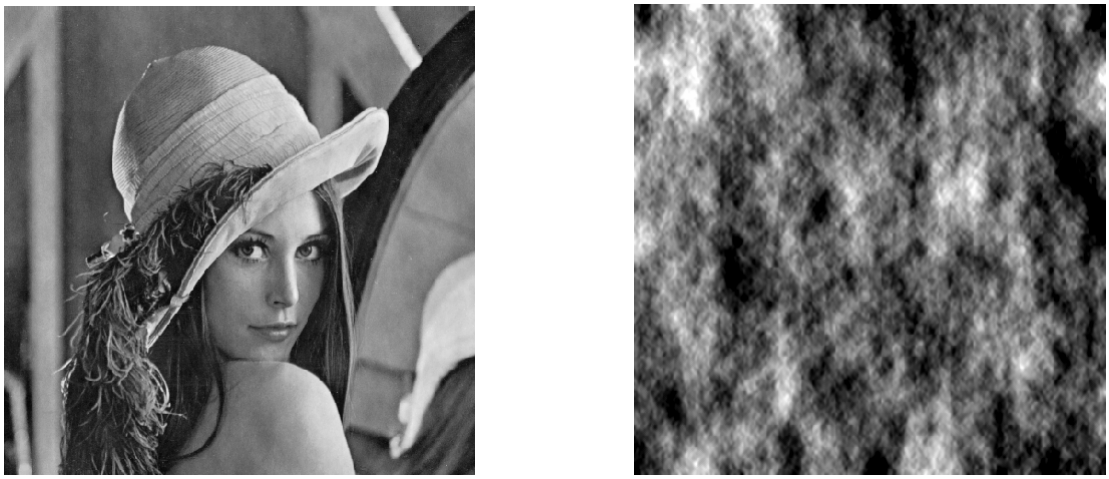



**Figure 3.39 Insertion et extraction d'une marque suivant l'algorithme de COX**.

***La détection :*** l'image marquée **D'** peut subir une attaque volontaire ou involontaire et devient une image modifiée $\mathbf{D}^*$. Sachant **D** et $\mathbf{D}^*$, une marque altérée $\boldsymbol{X}^* = x_1 + ... + x_n$ peut être extraite, en calculant la différence des modules des coefficients DCT (originaux et altérés), et comparée ensuite à la marque originale $\boldsymbol{X}$ par des méthodes statistiques.

On extrait $X^*$, en commençant par l'extraction de $V^* = v_1^* + ... + v_n^*$ la série des modules des coefficients DCT de $\mathbf{D}^*$ correspondant aux plus grand modules des coefficients DCT de **D** en utilisant les informations connues sur **D**.



**(a)** **(b)**

**Figure 3.40. L'image de Lena marquée $\alpha$ = 0.1 et la différence entre l'image marquée et l'image originale.**

Il est peu probable que la série extraite $\mathbf{X}^*$ soit identique à la série **X**. pour cela on mesure la similitude entre les deux séries $\mathbf{X}^*$ et **X** :

$$sim(X, X^*) = \frac{X.X^*}{\sqrt{X^*.X^*}}.$$

$sim(X, X^*)$ ne peut pas dépasser la valeur 6 si $X^*$ n'est pas similaire a X. donc, si l'image ne comporte qu'une seule marque avec une seule clef cette valeur ne dépasse 6 qu'une seule fois. Sur la figure 3.41 sont représentés les valeurs des similitudes en fonction de 1000 valeurs différentes de la clef utilisées pour générer 1000 marques différentes.

L'image utilisée est celle de Lena, marquée par une série X généré en utilisant une clef égale à 100.il est claire que pour toutes les autres séquences la valeur de la similitude ne dépasse pas 6 et est égale à 86, 48 pour la clef 100.

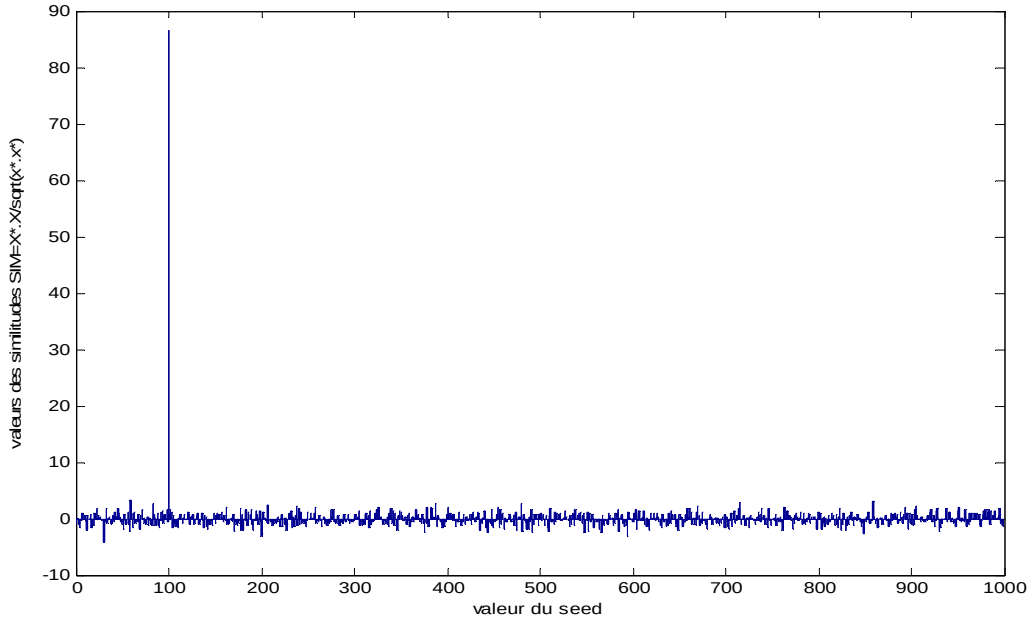



**Figure 3.41 la réponse du détecteur est unique pour un marquage unique**

***Expérience 1 :*** pour déterminer la robustesse de l'algorithme contre la compression JPEG, après avoir marquer une image, on réalise des versions compressées de cette image avec différents facteurs de qualité Q. on observe ensuite la réaction du détecteur pour chaque version Tab 3.3.3.

| Qualité | 5% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Similitude | 15.61 | 29.95 | 54.92 | 70.53 | 77.46 | 80.76 | 83.04 | 84.16 | 85.76 | 87.07 | 86.70 |

Le détecteur donne de très bons résultats figure 3.43. même pour de faibles valeurs de Q figure 3.42.

***Expérience 2 :*** l'algorithme de Cox est robuste contre l'attaque par filtrage .on applique un filtre passe bas B à l'image marquée figure 3.44.

$$\boldsymbol{B} = \begin{bmatrix} \mathbf{0.25} & \mathbf{0.25} \\ \mathbf{0.25} & \mathbf{0.25} \end{bmatrix} \qquad \mathbf{3.3.4.}$$

Le détecteur donne une très grande valeur de similitude (33.68) figure 3.46.

**Figure 3.42 Lena marquée et compressée (Q=5%, Q=1%)**

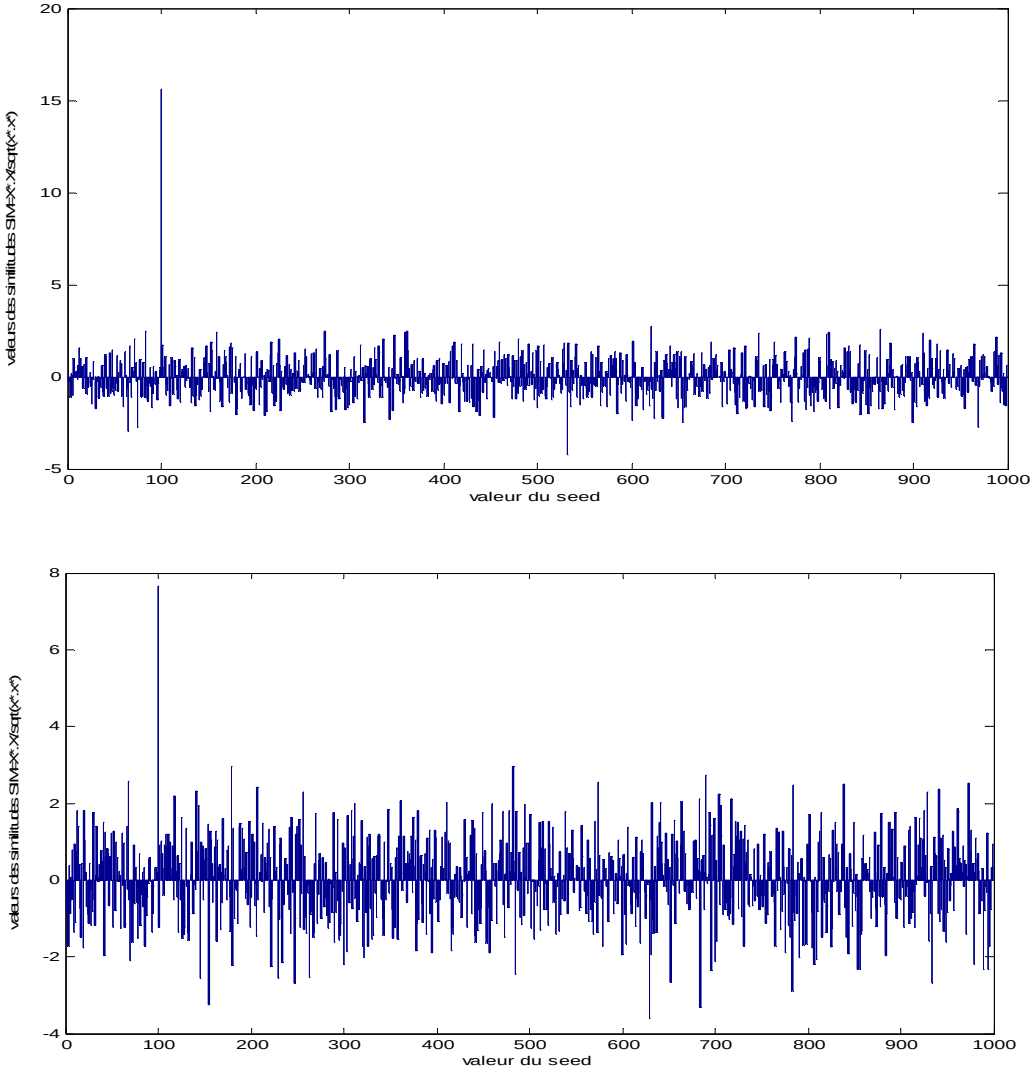



**Figure 3.43. Réponse du détecteur à une image marquée et compressée Q=5% et Q=1%**

**Figure 3.44 Image de Lena filtrée**

**figure 3.45 redimensionner à 50%**

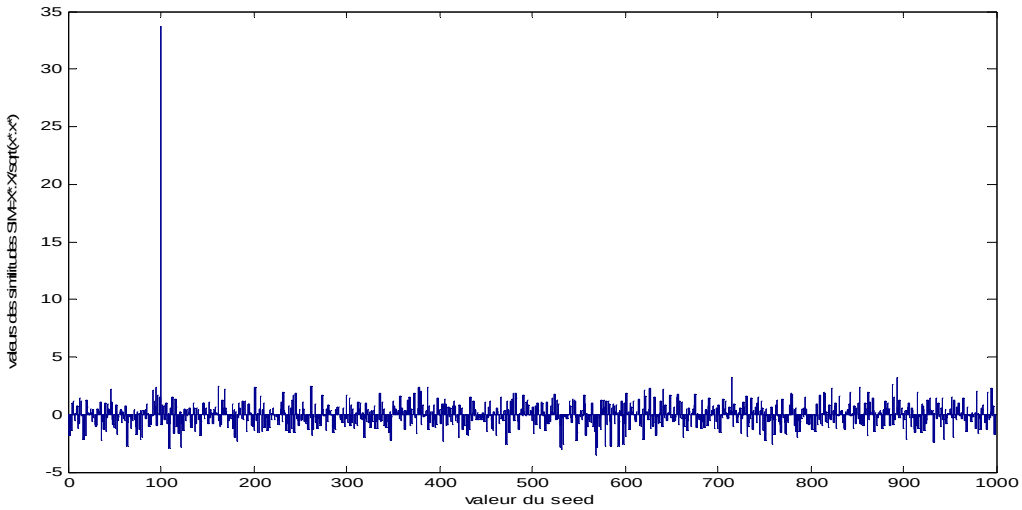



**Figure 3.46 réponse du détecteur à l'image de Lena marquée et filtrée**

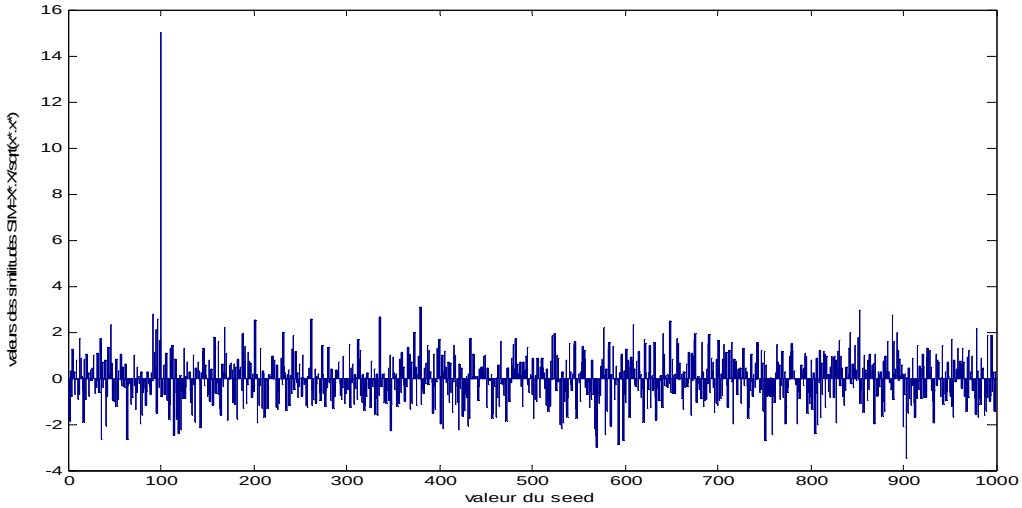



**Figure 3.47 .réponse du détecteur à l'image de Lena marquée et filtrée redimensionnée à 50% puis a 200%**

***Expérience 3 :*** en effectuant un changement d'échelle de 50% de l'image marquée avec un filtrage passe bas, et un deuxième changement d'échelle de 200% pour restituer les dimensions initiales de l'image, l'image marquée perd de ces détails fins, et la marque devient de plus en plus altérée .

L'algorithme de COX présente une robustesse contre ce type d'attaque. La figure 3.45 représente l'image de Lena redimensionnée a 50% et filtrée par un filtre passe bas. La réponse du détecteur est représentée sur la figure 3.47 où la similitude, pour la clef égale à 100, est égale à (15.00).

***Expérience 4 :*** cette expérience montre la robustesse de l'algorithme de COX contre l'attaque par découpage de parties de l'image marquée (recadrage). On découpe l'image marquée en ne laissant que le quart central figure .les parties découpées sont remplacées ensuite par les parties correspondantes de l'image originale pour avoir des meilleurs résultats .

**(a)** **(b)**

**Figure 3.48 (a)- quart central de l'image de Lena marquée (b)-l'image découpée complétée par l'image originale**

Cette expérience montre que même dans le cas d'une perte de 75% de l'image marquée la détection de la marque reste possible. La réponse du détecteur dans ce cas donne une similitude égale à (28.41) figure 3.50.

***Expérience 5 :*** la robustesse de l'algorithme de COX contre le (dithering) ( tramage à diffusion d'erreur d'image) est démontrée dans la figure 3.52 .on réalise une version tramée avec diffusion d'erreur de l'image de Lena marquée 3.51. La réponse du détecteur donne la valeur (43.74).

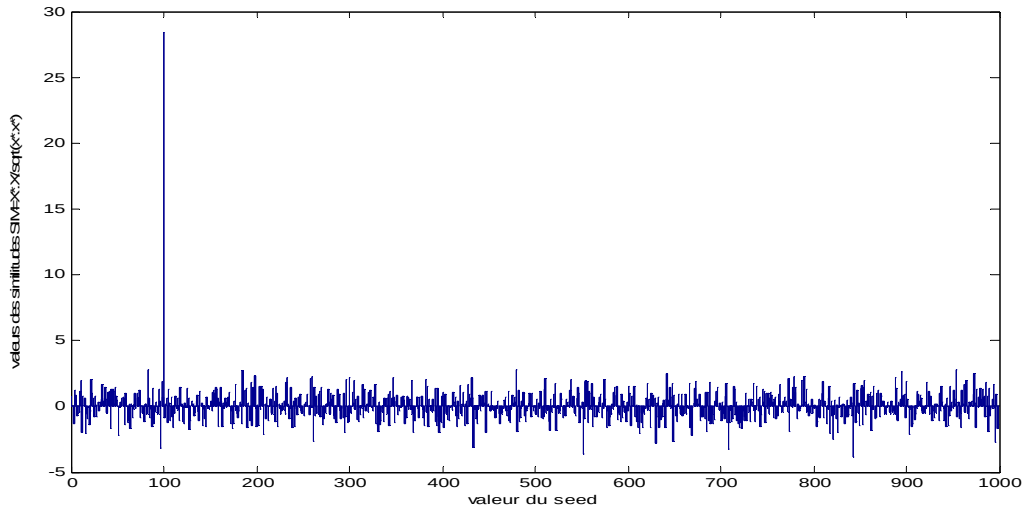



**Figure 3.50 la réponse du détecteur à un quart d'une image marquée**.

**(a)** **(b)**

**Figure 3.51 (a) version originale de Lena (b) version tramée avec diffusion d'erreur et marquée.**

# *3.4-Algorithmes dans le domaine multi résolution:*

Si les techniques de marquage peuvent exploiter les caractéristiques du model visuel humain (HVS), il est possible de dissimuler une marque, avec plus d'énergie, dans une image, qui rend le marquage plus robuste. De ce point de vue, la transformation discrète par ondelettes (DWT) est un outil très attirant, parce qu'il peut être employé comme une version de calcul efficace pour les modèles fréquentiels du système HVS **[56]**. Par exemple, il s'avère que l'oeil

humaine est moins sensible au bruit dans les bandes de haute résolution et dans les bandes de DWT (Discrete Wavelet Transform) ayant sur l'orientation de 45 ° (c.-à-d. *des bandes* HH).

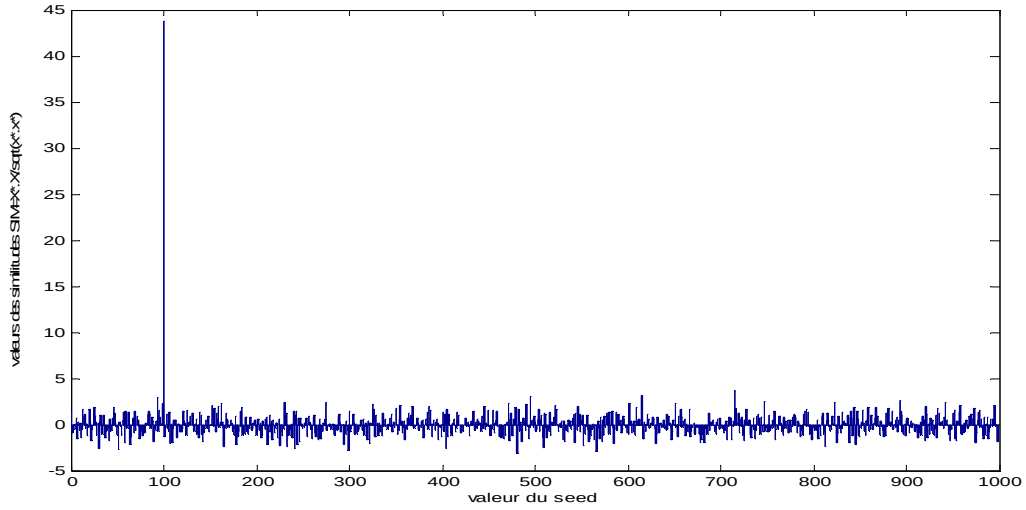



**Figure 3.52. Réponse du détecteur à une version marquée et tramée avec diffusion d'erreur de Lena.**

En outre, le codage DWT (Discrete Wavelet Transform) des images, tel que (EZW), sont inclus dans les normes de compression d'image et de vidéo, telles que JPEG2000 **[18]**. En dissimulant une marque dans le même domaine que la compression nous pouvons augmenter la robustesse des techniques de marquage. Beaucoup d'approches appliquent les techniques de base décrites au début de cette section aux coefficients DWT des bandes de haute résolution $LH_1$, $HH_1$ et $HL_1$ (figure 3.53) **[56]**, **[29]**, **[17]**, **[57]** et **[19]**.

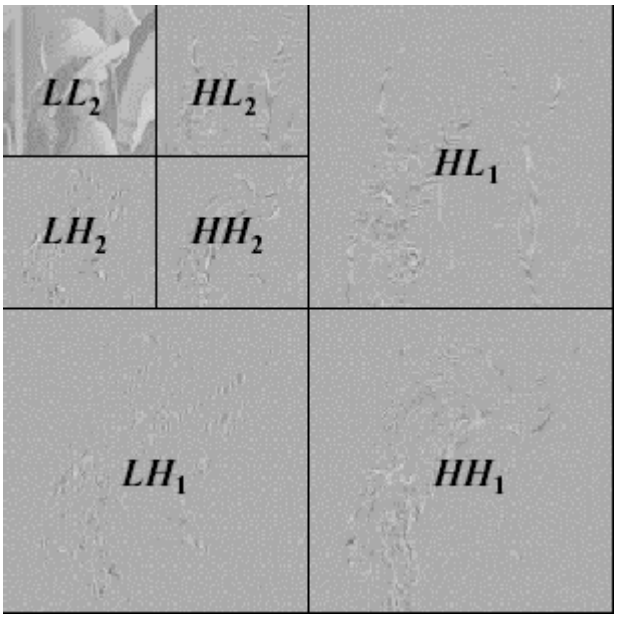



**Figure 3.53. Décomposition DWT d'une image**

## *3.4.1- Algorithme de KUNDUR (DWT) :*

***Les auteurs :*** cet algorithme est développé par Deepa Kundur et Dimitrios Hatikanos **[19]**.

***Détecteur :*** l'image originale est nécessaire pour la détection du message. La détection se fait par le calcul de la corrélation normalisée entre la marque détectée et la marque originale.

***La marque :*** la marque est une série de bits $\{-1,1\}$ et couvre tous les sites possibles. Cette série forme une matrice à deux dimensions $2X_S \times 2Y_S$ où $2X_S$ et $2Y_S$ sont plus petites que $X$ et $Y$ d'au moins d'un facteur de $2^M$ $(M \geq 1)$.

***Les sites :*** la marque est dissimulée dans tous les coefficients des bandes de détail du niveau $L$ où ils sont groupés en rectangles de même dimension que la marque : une marque $R^i_{k,l}$ est dissimulée dans chaque rectangle.

***Le marquage :***

- ✓ Le premier niveau de la DWT de la marque est calculée (seulement les détails de l'image sont utilisée nom pas les approximations).
- ✓ Les bandes du $L$ eme niveau de la DWT de l'image sont ensuite calculées et segmentées en rectangles $R^i_{k,l}$ figure (3.54)

$$R^i_{k,l} = \left\{ r^i_{k,l}(x,y) = f_{k,l}(X_{i,k,l} + x, Y_{i,k,l} + y) \right\} \qquad \textbf{3.4.1.}$$

Où

$$x \in \{0,...,2X_S\} \quad \text{Et} \quad y \in \{0,...,2Y_S\}$$

Où $(X_{i,k,l}, Y_{i,k,l})$ et le coin supérieur gauche du rectangle dans le domaine DWT.

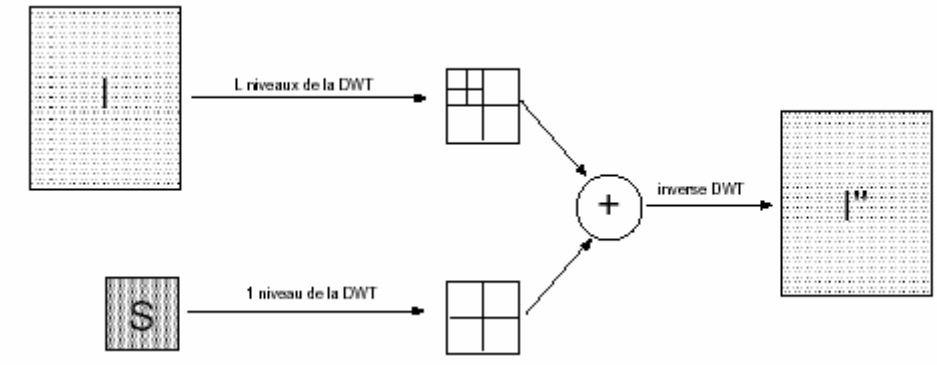



**Figure 3.54. Le marquage suivant l'algorithme de kundur**

- ✓ Pour chaque rectangle l'importance $S^i_{k,l}$ (la mesure de l'importance perceptuelle) est calculée suivant la formule 3.4.2.

$$S_{k,l}^{i} = \sum_{\forall(u,v)} C(u,v)\left|F_{k,l}^{i}(u,v)\right|^{2} \qquad \textbf{3.4.2.}$$

Où $\boldsymbol{C}$ est la matrice de la sensitivité du contraste calculée à l'aide de la formule3.4.3

$$C(u,v) = 5.05e^{-0.178(u+v)}\left(e^{0.1(u+v)} - 1\right) \qquad \textbf{3.4.3.}$$

Et $F_{k,l}^{i}(u,v)$ est la transformée de Fourier discrète des composante de l'image $r_{k,l}^{i}(x,y)$.

✓ La dissimulation se fait à l'aide de la formule 3.4.4.

$$g_{k,l}(x,y) = r_{k,l}^{i}(x,y) + \delta_{k,l}\sqrt{S_{k,l}^{i}}\,w_{k,l}(x,y) \qquad \textbf{3.4.4.}$$

Les paramètres de l'utilisateur $\delta_{k,l}$ pour $l = 1,...,L$ sont des réels positifs qui déterminent la relation entre la visibilité de l'image et la robustesse de la marque contre la distorsion du signal à chaque niveau de résolution, et il est calculé à l'aide de la formule suivante 4.1.5.

$$\delta_{k,l} = \frac{\alpha}{\max_{tous(x,y)}\sqrt{S_{k,l}^{i}}} \qquad \textbf{3.4.5}$$

**(a) (b) (c)**

**Figure 3.55. (a) image marquée (b) la matrice marque (c) la différence entre l'image originale et l'image marquée à l'aide de l'algorithme de KUNDUR x100**

***La détection :*** les auteurs n'ont pas détaillé les procédures de détection et l'extraction de la marque mais en suivant les démarches suivis lors de la dissimulation (car cette algorithme utilise l'image originale pour l'extraction de la marque) on peut extraire une marque altérée de l'image marquée.

Une corrélation normalisée 3.4.6 est utilisée pour comparer la marque originale avec la marque détectée (estimée) et ainsi on peut confirmer la détection de la marque figure 3.56.

$$\rho(w,\phi) = \frac{\sum_{\forall(x,y)} w(x,y)\phi(x,y)}{\sqrt{\sum_{\forall(x,y)} w^2(x,y)}\sqrt{\sum_{\forall(x,y)} \phi^2(x,y)}} \qquad 3.4.6$$

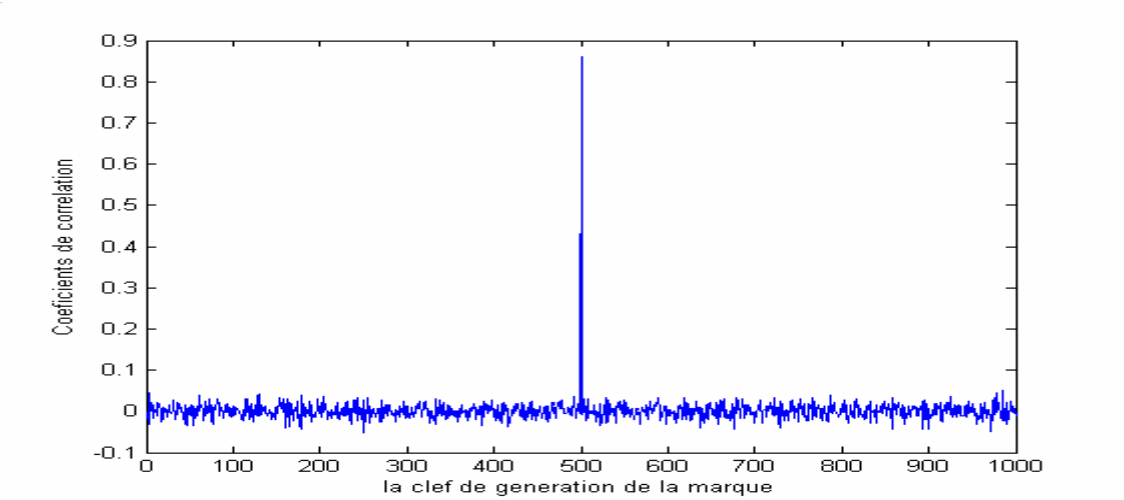



**Figure 3.56. Réponse du détecteur pour une image marquée à l'aide de l'algorithme de kundur**

***Expérience 1 :*** on a effectué cette première expérience pour déterminer la robustesse de cet algorithme contre la compression JPEG.

L'expérience consiste à marquer une image suivant l'algorithme de Kundur et de compresser l'image marquée avec différents coefficients de qualité de compression Q.

Les versions compressées de l'image sont soumises au détecteur pour calculer les coefficients de corrélations des estimations de la marque avec la marque originale figure 3.57.

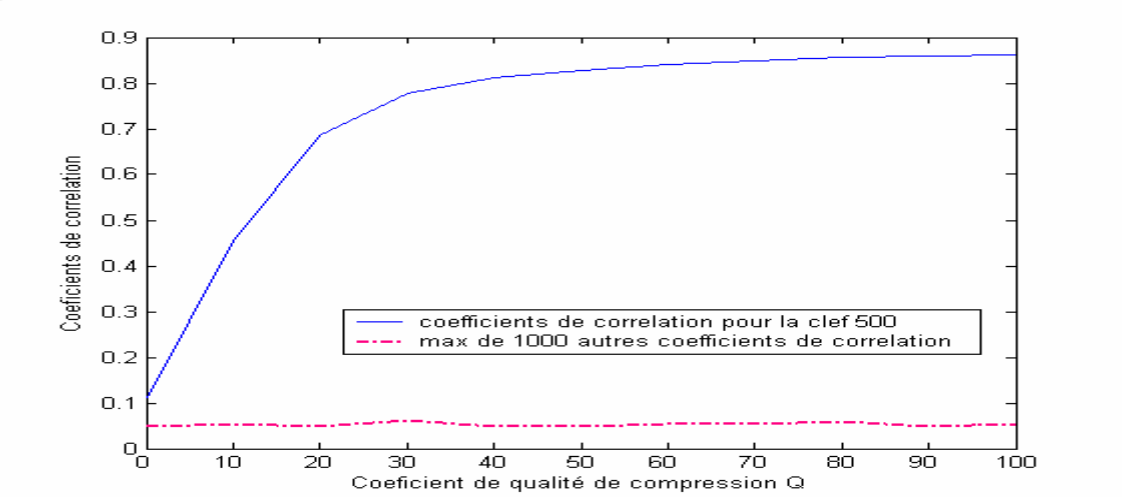



**Figure 3.57. Coefficient de corrélation en fonction de la qualité de compression Q et le maximum de 1000 coefficients de coefficient autre que celui de la détection.**

Sur cette figure est représentée, aussi, le maximum des valeurs de 1000 coefficients de corrélations (autres que celui de la détection) en fonction de la qualité de compression.

Cette figure montre que pour de très faibles coefficients de qualité de compression la marque reste détectable.

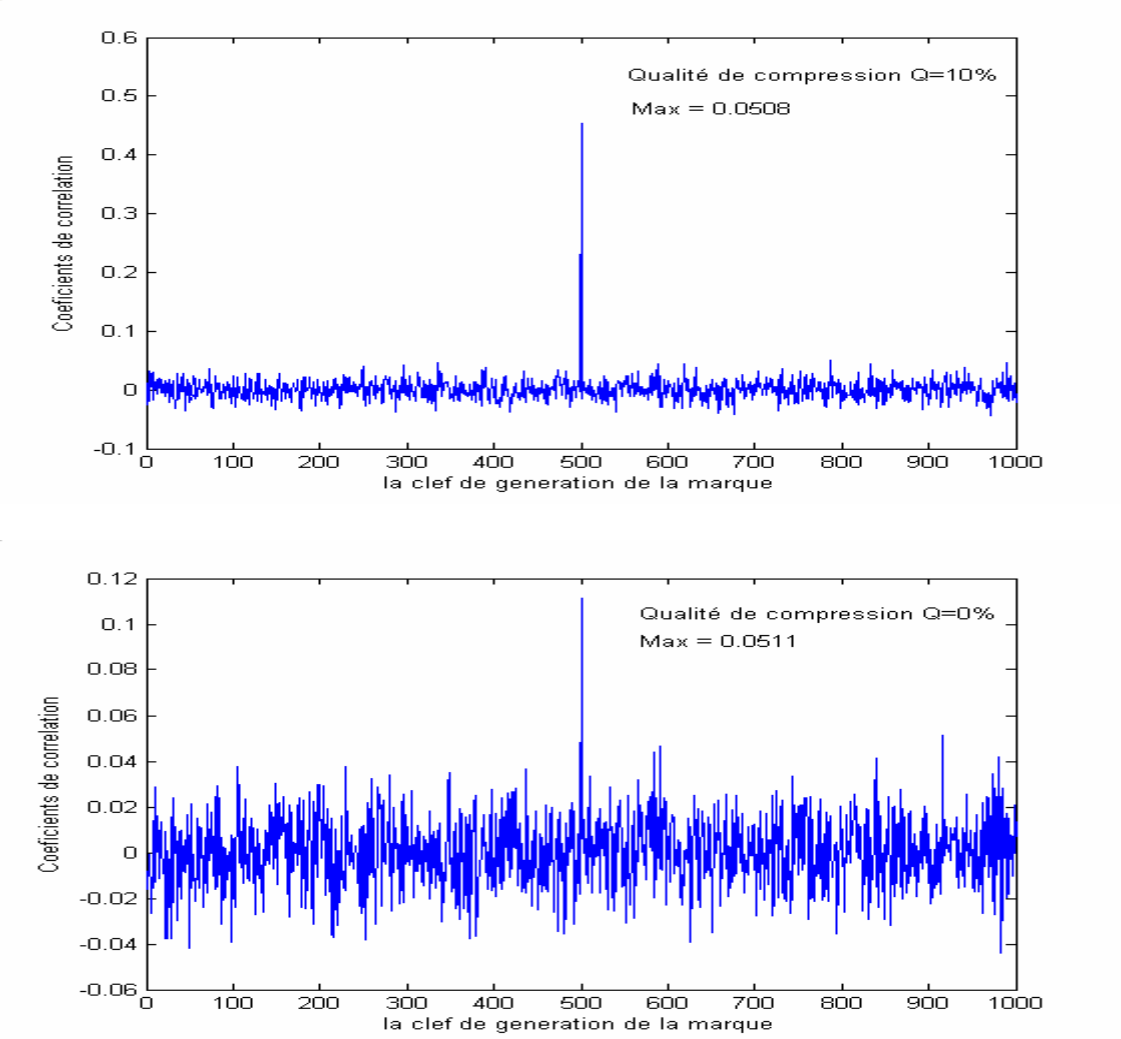



**Figure 3.58. Réponse du détecteur pour une version marquée et compressée Q=10% et Q=0%**

Sur la figure 3.58 sont représentées les réponses du détecteur à 1000 séquences aléatoires, y compris la réponse à la séquence aléatoire qui représente la marque originale (clef = 500) pour les deux coefficients de qualités de compression Q = 10% et 0%.

Le détecteur donne :

| Qualité de compression | 0% | 10% |
|---|---|---|
| Coefficients de corrélation | 0.1112 | 0.4534 |
| Maximum obtenu pour 1000 autres séquences aléatoires | 0.0511 | 0.0508 |

**(a)** **(b)**

**Figure 3.59 (a) image originale (b) version filtrée de l'image marquée**

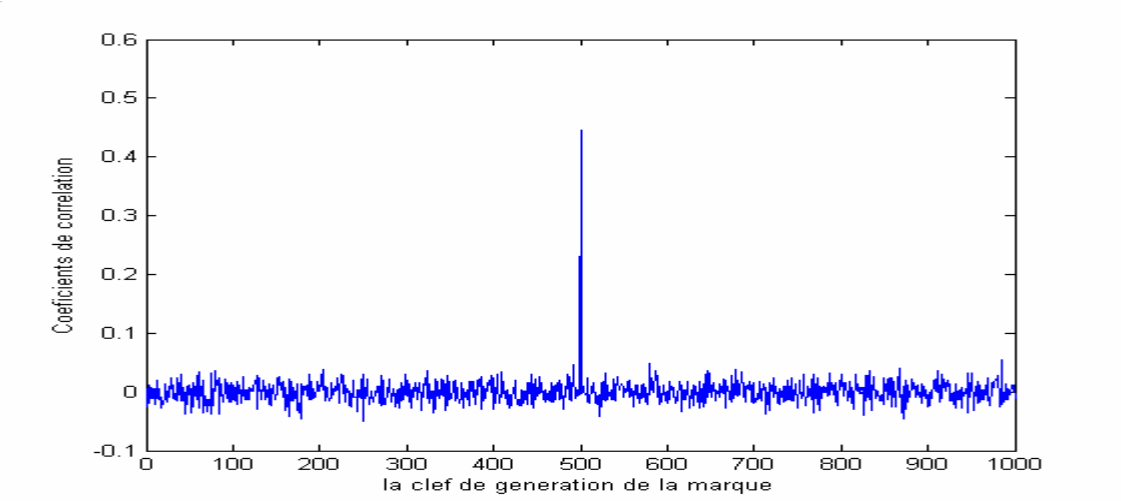



**Figure 3.60. Réponse du détecteur à une image marquée et filtrée.**

***Expérience 2 :*** l'algorithme de kundur est robuste contre l'attaque par filtrage .on applique une filtre passe bas B à l'image maquée figure 3.59.

$$B = \begin{bmatrix} 0.25 & 0.25 \\ 0.25 & 0.25 \end{bmatrix}$$

Le détecteur donne une valeur du coefficient de corrélation (0.4457) figure 3.60.le maximum des coefficients de corrélation pour 1000 autres séquences est 0.0542. La marque reste toujours détectable car la valeur du coefficient de corrélation est nettement supérieure des autres coefficients de corrélation.

**Figure 3.61. Image de Lena originale et une version redimensionnée à 50%**

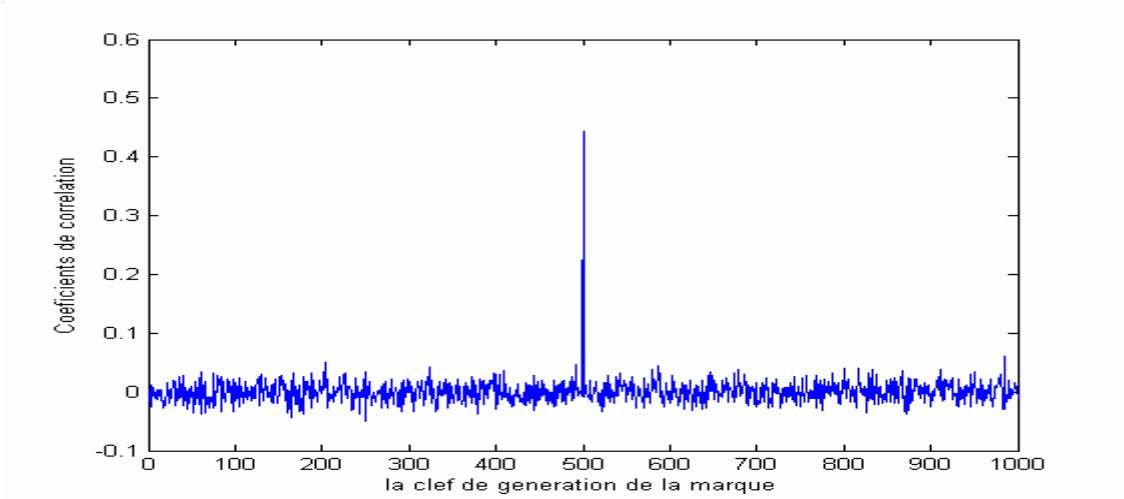



**Figure 3.62. Réponse du détecteur à une version redimensionnée de l'image marquée**

***Expérience 3 :*** en effectuant un changement d'échelle de 50% de l'image marquée , et en effectuant un deuxième un changement d'échelle de 200% pour restituer les dimensions initiales de l'image, l'image marquée perd de ces détails fins, et la marque devient de plus en plus altéré .

L'algorithme de kundur présente une robustesse contre ce type d'attaque. La figure 3.61 présente l'image de Lena redimensionnée à 50%. La réponse du détecteur est représentée sur la figure 3.62 où le coefficient de corrélation, pour la clef égale à 500, est égal à (0.4427), très supérieur du maximum des coefficients de corrélation de 1000 autres séquences (0.060). Cela signifie que la marque reste détectable après ce type d'attaques.

***Expérience 4 :*** cette expérience montre la robustesse de l'algorithme de kundur contre l'attaque par découpage des parties de l'image marquée (recadrage). On découpe l'image

marquée en ne laissant que le quart central figure 3.63.les parties découpées sont remplacées ensuite par les parties correspondantes de l'image originale pour avoir des meilleurs résultats .

**(a)** **(b)**

**Figure 3.63 (a)- quart central de l'image de Lena marquée (b)-l'image découpée complétée par l'image originale**

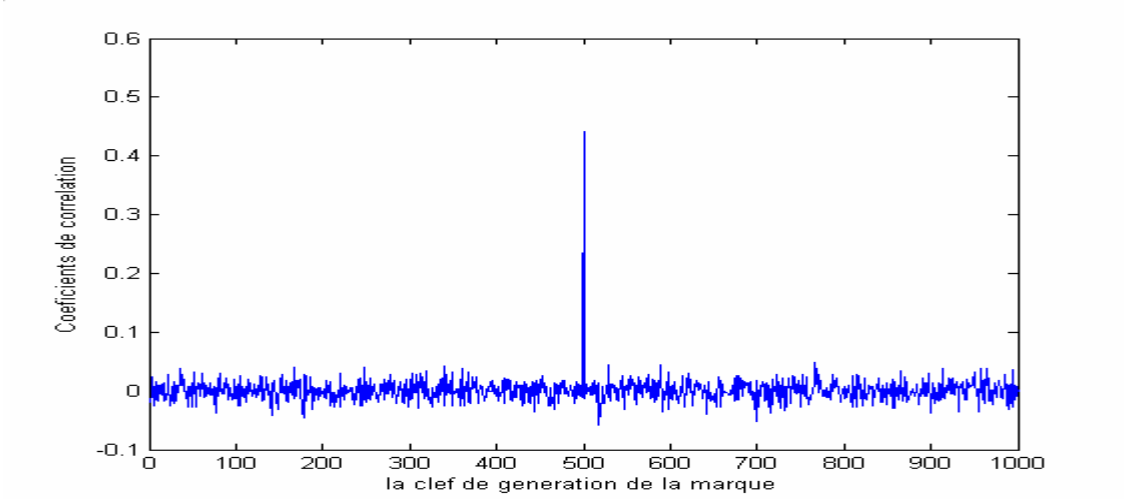



**Figure 3.64 la réponse du détecteur à un quart d'une image marquée.**

Cette expérience montre que même dans le cas d'une perte de 75% de l'image marquée la détection de la marque reste possible. La réponse du détecteur dans ce cas donne un coefficient de corrélation égale à (0.4415), très supérieur du maximum des coefficients de corrélation de 1000 autres séquences (0.0581) figure (3.64).

***Expérience 5 :*** la robustesse de l'algorithme de kundur contre (dithering) le tramage à diffusion d'erreur d'image est très faible ,figure 3.66.on réalise une version tramée avec diffusion d'erreur de l'image de Lena marquée 3.65. La réponse du détecteur donne la valeur (0.0815), très proche du maximum des coefficients de corrélation de 1000 autres

séquences (0.0567) cela montre que cet algorithme n'est pas très robuste contre ce type d'attaque.

**Figure 3.65. Versions tramée avec diffusion d'erreur de Lena marquée.**

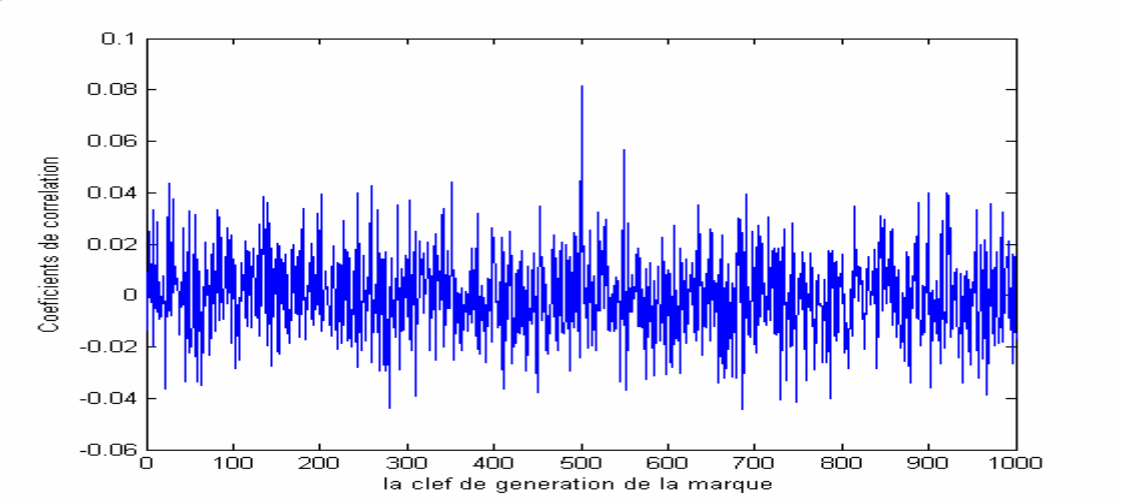



**Figure 3.66. La marque est à peine détectable.**

# *3.5-Conclusion :*

Les résultats présentés dans ce chapitre montrent l'influence du domaine d'insertion sur la robustesse des algorithmes ainsi que les techniques utilisées pour synchroniser les algorithmes. Les algorithme du domaine spatial sont très utilisées dans le marquage des séquences vidéo car leur temps de marquage est court grâce l'économie du nombre d'opérations de calcul .L'algorithme de cox est plus robuste contre la compression JPEG car il utilise la DCT comme domaine d'insertion qui est utilisé aussi par la compression JPEG. Chaque algorithme a ces propres avantages et ces propres inconvénients.

# *Conclusion*

**N**ous avons présenté dans ce travail les domaines d'utilisation du filigrane, et l'importance de cette technologie dans le domaine de la production et la distribution des données multimédia, car sans un moyen de protection contre le piratage et contre les violations des droits d'auteur les producteurs de ces produits ont refusé de mettre leurs produits sous forme numérique et les distribuer électroniquement (via Internet par exemple).
Nous avons vue aussi que cette technologie n'entre pas seulement dans le domaine de la protection mais aussi dans le domaine de la confidentialité tel que leur utilisation dans l'imagerie médicale pour conserver la confidentialité des malades, leur utilisation dans la transmission des messages secrets.
Le domaine de l'indexation des données multimédia est aussi inclu et qui permet de diminuer le temps de recherche et de trie. En bref il permet d'automatiser le traitement de ce type de données.

**D**ans le deuxième chapitre nous avons présenté les différentes classes d'algorithmes qui ont marqué l'évolution du marquage numérique des images fixes.
Si au départ les algorithmes de marquage étaient de type additif, ils ont ensuite évolué vers des algorithmes opérants par substitution et sont devenus de plus en plus performant.
L'augmentation de la robustesse des algorithmes est liée à

- ✓ La prise en considération des différentes attaques que peut subir ces algorithmes.
- ✓ La prise en considération des différents algorithmes de traitement d'images qui peuvent être considérés comme des attaques involontaires.
- ✓ La prise en compte du contenu de l'image, qui à permis d'augmenter la puissance de la signature, à travers des méthodes basées sur le système visuel humain, ou encore de synchroniser la détection de la signature après une transformation géométrique (cas des algorithmes auto synchronisants).

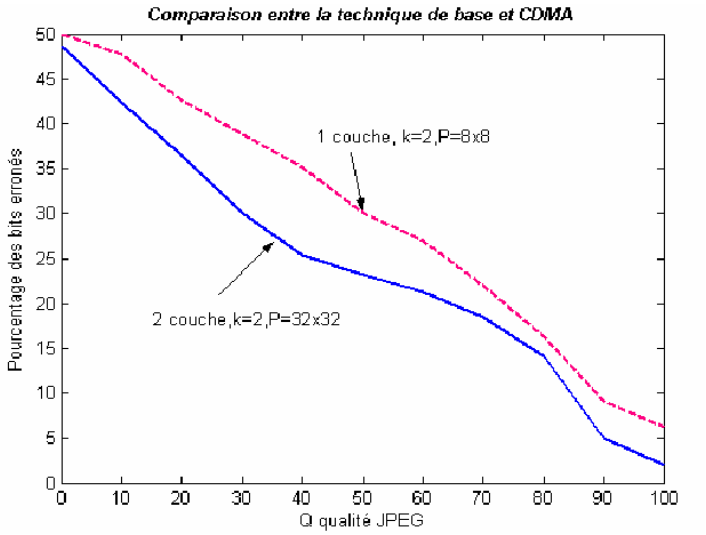
Dans ce travail nous n'avons pas cité tous les algorithmes existants, il existe plusieurs autres algorithmes qui sont destinés à des fins précises telles que l'impression. D'autres algorithmes ont été destinés vers des fins commerciales, par conséquent ils n'ont jamais été publiés.

**D**ans le troisième chapitre nous avons détaillé plusieurs algorithmes en essayant de couvrir le maximum de classes présentées dans le chapitre II. Dans la première partie de ce chapitre nous avons vu l'un des premiers algorithmes réalisés dans le domaine spatial qui

consiste à ajouter des M- séquences aux bits les moins significatifs des valeurs de la luminance des pixels de l'image .Ce marquage peut facilement être attaqué en modifiant, ou tout simplement en éliminant, les deux ou trois bits les moins significatifs de l'image marquée. En effet, même si le coefficient d'invisibilité de la marque est égal à 3, qui est le cas extrême, le changement causé par la marque ne peut que difficilement dépasser le troisième bit de la valeur de la luminances des pixels. Mais cela ne veut pas dire que cet algorithme n'est pas utilisable, il peut être utilisé comme marquage fragile pour prouver l'authentification des documents.

Par la suite, nous avons détaillé deux autres algorithmes qui ont apporté des modifications et des améliorations au premier algorithme.

- ✓ Le premier : utilise la technique TDMA (Time Division Multiple Access) pour augmenter la capacité du marquage qui était un bit seulement dans toute l'image et la taille des blocs permet une meilleure robustesse contre la compression JPEG.
- ✓ Le deuxième : utilise la technique CDMA (Code Division Multiple Access) et présente une meilleure capacité de marquage et une meilleure robustesse contre la compression JPEG.




Ces algorithmes sont parmi les premiers réalisés dans le domaine spatial. Ils ont été la base de plusieurs autres algorithmes. Plusieurs auteurs ont modifié ces algorithmes afin de les rendre plus robustes ou d'une plus grande capacité. Chaque auteur déclare lors de la publication de son article que son algorithme est le plus robuste et qu'il résiste à une telle attaque ou une autre, mais d'autres auteurs prouvent rapidement le contraire.

L'algorithme suivant, celui de Kutter, est un peu différent des autres car il permet de marquer des images en couleurs en modifiant la composante bleue de l'image. Le choix des sites est fait aléatoirement et ce sont les bits du message qui sont dissimulées directement. La détection dans ce cas se fait par un calcul de la similitude. L'algorithme de Kutter est plus robuste et possède un moyen de synchronisation après une attaque par rotation.

Le dernier algorithme de la première partie (LSB) est aussi parmi les premiers basés sur la substitution des composantes de l'image dans le domaine spatiale. La capacité est très grande, à un point où on peut dissimuler une image dans une autre. En effet chaque pixel de l'image peut dissimuler au moins un bit ce qui n'était pas le cas pour les algorithmes précédents qui utilise un ensemble de pixels pour dissimuler un seul bit. L'inconvénient de cet algorithme est qu'il n'est pas robuste, car il peut être attaqué par élimination des bits les moins significatifs.

Dans la deuxième partie du troisième chapitre nous avons détaillé deux algorithmes qui opèrent dans le domaine fréquentiel. Le premier utilise la DFT comme domaine d'insertion et représente le principe du marquage dans le domaine fréquentiel. Le deuxième est celui de COX qui utilise la DCT (Discrete Cosine Transform) comme domaine d'insertion. Les deux algorithmes sont de type non aveugle. La détection du message nécessite la connaissance du message originale.

L'algorithme de COX présente une robustesse remarquable contre l'attaque par compression JPEG .En effet, on a vue que pour une compression maximale le message reste toujours détectable et cela est due à la concordance du domaine d'insertion de la marque et l'algorithme d'attaque JPEG qui utilise la transformé DCT (Discrete Cosine Transform). Cet algorithme est robuste contre plusieurs types d'attaque tels que le recadrage (cropping), le filtrage, le redimenssionnement et le dithering d'image.

La dernière partie du chapitre III comporte un algorithme utilisant un autre domaine d'insertion qui est la transformée par ondelette DWT. Cet algorithme présente une robustesse similaire à celle de COX contre l'attaque par la compression JPEG, le recadrage (cropping), le filtrage, le redimenssionnement de l'image, mais il est moins robuste contre le dithering.

**E**n fin, chaque algorithme est destiné vers une utilisation bien précise et il utilise un domaine d'insertion bien précis ce qui limite sa robustesse à un nombre limité d'attaques.

**D**ans notre travail, on a implémenté toutes ces méthodes et on les a analysés du point de vue de leur robustesse et de l'influence de leurs paramètres.

# *Perspectives*

Le marquage des documents est encore un domaine de recherche très récent et les solutions, qu'il offre en matière de sécurité, sont actuellement confrontées au problème de la robustesse des algorithmes qui sont utilisés. Contrairement aux techniques de cryptographie éprouvées depuis plusieurs décennies et largement utilisées de nos jours .la limitation de l'emploi du marquage à la résolution des problèmes de droit d'auteurs peut paraître, en comparaison avec la cryptographie, marginale et incertain. La cryptographie est une science qui est déjà mure, les algorithmes utilisés sont réputée inviolables. Les deux disciplines ne répondent pas aux mêmes objectifs, le marquage permet une libre et une transparente circulation aux données sur les réseaux.

Le domaine de marquage d'image est un domaine de recherche fertile actuellement. De nouveaux algorithmes sont publiés avec un rythme ascendant. Il est donc un domaine en pleine période de croissance et il ne possède encore pas la robustesse que peuvent procurer les outils de nature cryptographique.

La robustesse est liée au domaine d'insertion de la marque qui de préférence doit concorder avec le domaine où exerce l'attaque. Donc, un robuste algorithme doit opérer dans tous les domaines utilisés dans le traitement d'image. Un tel algorithme peut résoudre le problème de la robustesse ou du moins il diminue l'influence des domaines d'insertion sur la robustesse des algorithmes.

Une deuxième approche peut être entamée, la réalisation d'un algorithme dans un domaine indépendant des domaines où opèrent les attaques contre le marquage.

La robustesse d'un algorithme dépend aussi de la synchronisation des détecteurs après une attaque (géométrique). Pour cela la recherche s'oriente aussi vers des algorithmes auto synchronisant.

# *Bibliographie*

**[1]** Ross J. Anderson, Fabien A.P. Petitcolas, “On the Limits of Steganography. IEEE Journal of Selected Areas in Communications”, 16(4):474-481, May 1998, Special Issue on Copyright & Privacy Protection, ISSN 0733-8716.

**[2]** I. Pitas, “A Method For Signature Casting On Digital Images”, Proceedings ICIP-96, IEEE International Conference on Image Processing, Volume III pp. 215-218, Lausanne, Switzerland, 16-19 September 1996.

**[3]** G. Depovere, T. Kalker, J.-P. Linnartz, “Improved Watermark Detection Using Filtering Before Correlation”, Proceedings of 5th IEEE International Conference on Image Processing ICIP'98, Chicago, Illinois, USA, Vol I, pp. 430-434, 4-7 October 1998.

**[4]** R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, "A Digital Watermark", Proceedings of the IEEE International Conference on Image Processing, volume 2, pages 86-90, Austin, Texas, USA, November 1994

**[5]** G.C. Langelaar, J.C.A. van der Lubbe, J. Biemond, “Copy Protection for Multimedia Data Based on Labeling Techniques”, 17th Symposium on Information Theory in the Benelux, Enschede, The Netherlands, 30-31 May 1996.

**[6]** A. Z. Tirkel, G. Rankin, R. Schyndel ,C.F. Osborne,” Electronic Water Mark” in Digital Image Computing, Technology and Applications (DICTA’93),Macquarie University, Sidney, 1993, pp. 666–673.

**[7]** F. Hartung and B. Girod, "Watermarking of Uncompressed and Compressed Video», Signal Processing, Vol. 66, no. 3, pp. 283-301, (Special Issue on Copyright Protection and Control, B. Macq and I. Pitas, eds.), May 1998.

**[8]** G.C. Langelaar, J.C.A. van der Lubbe, R.L. Lagendijk, “Robust Labeling Methods for Copy Protection of Images” , Proceedings of SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose (CA), USA, February 1997.

**[9]** W. Bender, D. Gruhl, N. Morimoto, “Techniques for Data Hiding”, Proceedings of the SPIE, Vol. 2420 pp 165-173, Storage and retrieval for image and Video Databases III, San Jose CA, USA, 9-10 February 1995.

**[10]** I. Pitas, T.H. Kaskalis, “Applying Signatures On Digital Images”, Proceedings of IEEE Workshop on Nonlinear Signal and Image Processing, pp. 460-463, Neos Marmaras, Greece, 20-22 June 1995.

**[11]** N. Nikolaidis I. Pitas, “Robust Image Watermarking In Spatial Domain“.Signal Processing, vol. 66 no. 3 pp. 385–403, May 1998, European Association for Signal Processing (EURASIP).

**[12]** N. Nikolaidis and I.Pitas, “Copyright Protection Of Images Using Robust Digital Signatures”, Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-96), vol. 4, pp. 2168-2171, Atlanta, USA, May 1996.

**[13]** F. Go_n, J. F. Delaigle, C. De Vleeschouwer, B. Macq, and J. J. Quisquater. “A Low Cost Perceptive Digital Picture Watermarking Method “. In I. K. Sethin and R. C. Jain, editors, Storage and Retrieval for Image and Video Database V, volume 3022, pages 264_277, San Jose, California, U.S.A., February 1997. The Society for Imaging Science and Technology (IS&T) and the International Society for Optical Engineering (SPIE), SPIE.

**[14]** M. Kutter, F. Jordan, F. Bossen, “Digital Signature of Color Images using Amplitude Modulation” , Proceedings of SPIE Electronic Imaging '97, Storage and Retrieval for Image and Video Databases V, San Jose (CA), USA, February 1997.

**[15]** I. Cox, J. Killian, T. Leighton, and T. Shamoon. “Secure Spread Spectrum Watermarking For Images, Audio And Video“. In Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96, pages 243_246, Lausanne, Switzerland,1996.

**[16]** A. Piva, M. Barni, F. Bartolini, V. Cappellini, “DCT-based Watermark Recovering Without Resorting To The Uncorrupted Original Image” , Proceedings of ICIP 97, IEEE International Conference on Image Processing, Santa Barbara, California, October 1997.

**[17]** D. Kundur, D. Hatzinakos, "A Robust Digital Image Watermarking Scheme Using Wavelet-Based Fusion," Proceedings of ICIP 97, IEEE International Conference on Image Processing, Santa Barbara, California, October 1997.

**[18]** W. Zhu Z. Xiong Y. Zhang ,“Multiresolution Watermarking For Image And Video: A Unified Appraoch“

**[19]** X.-G. Xia, C.G. Boncelet, G.R. Arce, “A Multiresolution Watermark for Digital Images”, Proceedings of ICIP 97, IEEE International Conference on Image Processing, Santa Barbara, California, October 1997.

**[20]** Tuomas Aura, “Invisible Communication”, Proceedings of the HUT Seminar on Network Security '95, Espoo, Finland, November 6, 1995.

**[21]** Tuomas Aura, “ Practical Invisibility In Digital Communication” , Proceedings of the Workshop on Information Hiding, Cambridge, England, May 1996, Lecture Notes in Computer Science 1174, Springer Verlag 1996.

**[22]** K. Hirotsugu, “An Image Digital Signature System With ZKIP For The Graph Isomorphism”, Proceedings ICIP-96, IEEE International Conference on Image Processing, Volume III pp. 247-250, Lausanne, Switzerland, 16-19 September 1996.

**[23]** Jiri Fridrich, Miroslav Goljan, “Protection of Digital Images Using Self Embedding”, submitted to The Symposium on Content Security and Data Hiding in Digital Media, New Jersey Institute of Technology, March 16, 1999.

**[24]** E. Koch, J. Zhao, “ Towards Robust and Hidden Image Copyright Labeling”, Proceedings IEEE Workshop on Non-lineair Signal and Image Processing, pp. 452-455, Neos Marmaras (Thessaloniki Greece), June, 1995.

**[25]** J. Zhao, E. Koch, “ Embedding Robust Labels into Images for Copyright Protection” ,Proceedings of the International Congress on Intellectual Property Rights forSpecialized Information, Knowledge and New Technologies, Vienna, Austria, August 21-25 1995.

**[26]** E. Koch, J. Rindfrey, J. Zhao, “Copyright Protection for Multimedia Data” , Proceedings of the International Conference on Digital Media and Electronic Publishing, Leeds, UK, 6-8 December 1994.

**[27]** S.Burgett, E.Koch, J.Zhao, “Copyright Labeling of Digitized Image Data”, IEEE Communications Magazine, pp. 94-100, March 1998.

**[28]** W. B. Pennebakker , J. L. Mitchell, “The JPEG Still Image Data Compression Standard”, Van Nostrand Reinhold, New York, 1993.

**[29]** F.M. Boland, J.J.K. Ó Ruanaidh and C. Dautzenberg, “Watermarking Digital Images for Copyright Protection” , IEE Int. Conf. on Image Processing and Its Applications, pp 326-330, Edinburgh, Scotland, July 1995.

**[30]** A.G. Bors, I.Pitas, “ Embedding Parametric Digital Signatures in Images”,EUSIPCO-96, Trieste, Italy, vol. III, pp. 1701-1704, September 1996

**[31]** A.G. Bors, I.Pitas, “ Image Watermarking Using DCT Domain Constraints” , IEEE International Conference on Image Processing (ICIP'96), Lausanne, Switzerland, vol. III, pp. 231-234, 16-19 September 1996

**[32]** G.C. Langelaar, R.L. Lagendijk, J. Biemond “Real-time Labeling Methods for MPEG Compressed Video” , 18th Symposium on Information Theory in the Benelux, Veldhoven, The Netherlands, 15-16 May 1997

**[33]** G.C. Langelaar, “Conditional Access to Television Service”, Wireless Communication, the interactive multimedia CD-ROM, 3rd edition 1999, Baltzer Science Publishers, Amsterdam, ISSN 1383 4231.

**[34]** O. Bruyndonckx, Jeans - Jacques Quisquater, And Benoit M. Macq .spatial method for copyright labeling of digital images . Proceedings IEEE Workshop on Non-lineair Signal and Image Processing, pp. 456-459, Neos Marmaras (Thessaloniki Greece), June, 1995

**[35]** G. Caronni, "Assuring Ownership Rights for Digital Images", Proceedings of Reliable IT Systems, pp. 251-263, VIS '95, Vieweg Publishing Company, Germany,1995.

**[36]** F. Hartung and B. Girod: “Digital Watermarking of Raw and Compressed Video” ,Proceedings SPIE 2952: Digital Compression Technologies and Systems for Video Communication, pp 205-213, October 1996 (Proc. European EOS/SPIE Symposium on Advanced Imaging and Network Technologies, Berlin, Germany)

**[37]** J.R. Smith, B.O. Comiskey, “Modulation and Information Hiding in Images” ,Preproceedings of Information Hiding, an Isaac Newton Institute Workshop,University of Cambridge, UK, May 1996

**[38]** R.B. Wolfgang and E. J. Delp, "A Watermark for Digital Images", Proceedings of the IEEE International Conference on Image Processing, Volume III pp. 219-222, September 16-19, 1996, Lausanne, Switzerland.

**[39]** R.B. Wolfgang and E.J. Delp, "A Watermarking Technique for Digital Imagery: Further Studies," Proceedings of the International Conference on Imaging Science, Systems, and Technology, Las Vegas, USA, June 30 - July 3, 1997.

**[40]** W.Zeng, B. Liu, “On resolving Rightful Ownerships of Digital Images by Invisible Watermarks” , Proceedings of ICIP 97, IEEE International Conference on Image Processing, Santa Barbara, California, October 1997.

**[41]** Jiri Fridrich, “Robust Bit Extraction From Images” , submitted to IEEE ICMCS'99 Conference, Florence, Italy, 7-11 June 1999

**[42]** R. B. Wolfgang and E. J. Delp, "Overview of Image Security Techniques with applications in Multimedia Systems," Proceedings of the SPIE Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways, Vol. 3228, pp. 297-308, Dallas, Texas, USA, November 2-5, 1997.

**[43]** Raymond B. Wolfgang, Edward J. Delp, “ Fragile Watermarking Using the VW2D Watermark” Electronic Imaging ’99, The International Society for Optical Engineering, Security and Watermarking of Multimedia Contents, Vol 3657, San Jose, CA, USA, 25-27 January 1999.

**[44]** Ton Kalker, Geert Depovere, Jaap Haitsma, Maurice Maes, “A Video Watermarking System for Broadcast Monitoring” , Proceedings of SPIE ELECTRONIC IMAGING '99, Security and Watermarking of Multimedia Contents, January 1999, San Jose (CA), USA.

**[45]** C.E. Shannon, W.W. Weaver, " The Mathematical Theory of Communications" , The University of Illinois Press, Urbana, Illinois, 1949

**[46]** Joe J. K. Ó Ruanaidh, Shelby Pereira, "A Secure Robust Digital Image Watermark" Electronic Imaging: Processing, Printing and Publishing in Color, SPIE Proceedings, (SPIE/IST/Europto Symposium on Advanced Imaging and Network Technologies), Zürich, Switzerland, May 1998

**[47]** Joe J. K. Ó Ruanaidh, Thierry Pun, "Rotation, Scale And Translation Invariant Spread Spectrum Digital Image Watermarking", Signal Processing, Vol. 66, no. 3, pp. 303-317, (Special Issue on Copyright Protection and Control, B. Macq and I. Pitas, eds.), May 1998.

**[48]** J.J.K. Ó Ruanaidh, W.J. Dowling, F.M. Boland, "Phase Watermarking of Digital Images", Proceedings of the IEEE International Conference on Image Processing, Volume III pp. 239-242, Lausanne, Switzerland, September 16-19, 1996.

**[49]** Alexander Herrigel, Holger Petersen, Joseph O' Ruanaidh, Thierry Pun, Pereira Shelby, "Copyright Techniques for Digital Images Based On Asymmetric Cryptographic Techniques" , Workshop on Information Hiding, Portland, Oregon, USA, April 1998.

**[50]** Alexander Herrigel, Joe J. K. Ó Ruanaidh, Holger Petersen, Shelby Pereira and Thierry Pun, " Secure copyright protection techniques for digital images" , In David Aucsmith ed., Information Hiding, pp. 169-190, Vol. 1525 of Lecture Notes in Computer Science, Springer, Berlin, 1998.

**[51]** Shelby Pereira, Joe J. K. Ó Ruanaidh, Frédéric Deguillaume, Gabriella Csurka and Thierry Pun, Template based recovery of Fourier-based watermarks using log-polar and log-log maps, In IEEE Multimedia Systems 99, International Conference on Multimedia Computing and Systems, Florence, Italy, 7-11 June 1999.

**[52]** J.J.K. Ó Ruanaidh, F.M. Boland, O. Sinnen, "Watermarking Digital Images for Copyright Protection" , Electronic Imaging and the Visual Arts 1996, Florence, Italy, February 1996.

**[53]** Joseph J. K. Ó Ruanaidh, Thierry Pun, "Rotation, Scale And Translation Invariant Digital Image Watermarking" Proceedings of ICIP 97, IEEE International Conference on Image Processing, pp. 536-539, Santa Barbara, CA, October 1997

**[54]** I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", Technical Report 95 - 10, NEC Research Institute, Princeton, NJ, USA, 1995.

**[55]** I.J. Cox, J. Kilian, T. Leighton and T. Shamoon, "A Secure, Robust Watermark for Multimedia" , Preproceedings of Information Hiding, an Isaac Newton Institute Workshop, Univ. of Cambridge, May 1996.

**[56]** Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Lippi, Alessandro Piva, “A DWT-Based Technique For Spatio-Frequency Masking Of Digital Signatures” , Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents, vol. 3657, San Jose, CA, January 25 - 27, 1999.

**[57]** J.J.K. Ó Ruanaidh, W.J. Dowling, F.M. Boland, “Watermarking Digital Images for Copyright Protection”, IEE Proceedings Vision, Image- and Signal Processing, 143(4) pp. 250-256, August 1996.

**[58]** O. Rioul and M. Vetterli, “Wavelets and signal processing," IEEE Signal Processing Magazine, vol. 8, pp. 14{38, October 1991.

**[59]** Y. T. Chan, Wavelet Basics. New York: Kluwer Academic Publishers, 1995.

# *Annexes :*

## A. Synthèse de la transformée discrète par ondelettes (DWT) :

**D**ans cette annexe, brièvement, nous considérons et décrivons la notation générale utilisée pour la 2-D DWT. Le lecteur est orienté vers **[58, 59]** pour une description complète de la DWT. La DWT se rapporte au cadre du temps discret pour mettre en application la transformée orthonormal par ondelettes. Puisque nous sommes principalement concernés par des images dans ce travail nous employons le terme (espace) au lieu du (temps) en traitant la 2-D transformée par ondelettes. La transformation décompose un signal en fonctions de bases qui sont des dilatations et des translations de la fonction du signal désignée sous le nom d' *ondelette de base*.

Si la superposition spectrale entre les composantes de la fonction de base est petite, les coefficients des ondelettes fournissent une estimation du contenu fréquentiel du signal localisé à la bande de fréquence et à l'orientation correspondante.

De même, étant donné que l'ondelette de base est localisé dans l'espace, les coefficients fournissent une image de l'évolution spatiale du contenu fréquentiel.

La figure A.1 donne un exemple de la DWT de l'image de Lena. Comme il peut être vu, l'image est décomposée en une image secondaire de basse résolution et des détails de résolutions plus élevées. Le L-eme niveau de la DWT d'une image produit une séquence de ***3L*** images secondaires (sous bandes) de détail correspondant aux détails horizontal, vertical et diagonal pour chacun des ***L*** niveaux de résolutions et une approximation brute au niveau de la résolution le plus rude. Les différentes orientations de fréquence des images secondaire (sous bandes) de détail sont représentées par la variable ***o*** pour lesquelles ***o*** = 1, 2, 3 correspondent, respectivement, au détail horizontal, diagonal et vertical. Le niveau de résolution est représenté par la variable l où la plus grande valeur de l correspond à un niveau de résolution le plus brut (c.-à-d., une plus grande échelle). Ainsi, les coefficients de détail pour un niveau ***L*** de la DWT d'une image f sont donnés par le $f_{o,l}$ (m, n) où ***o*** = 1, 2,3, et ***l*** = 1, 2,…, ***L*** et (m, n) correspond à l'emplacement spatial dans la ***l***-eme résolution.

L'approximation brute est représentée par $f_{4,L}$ (m, n).

La figure A.2 élucide la terminologie. Chaque image secondaire $f_{o,l}$ est composée des Pixels représentants les valeurs des coefficients pour divers (m, n).


**Figure A.1: Exemple du DWT sur l'image de Lena. (a) L'image originale de Lena, (b) modules des coefficients de DWT de l'image dans (a) pour $L = 3$. Les coefficients ont été normalisés de sorte que les plus grands modules de chaque image secondaire semble blanche**

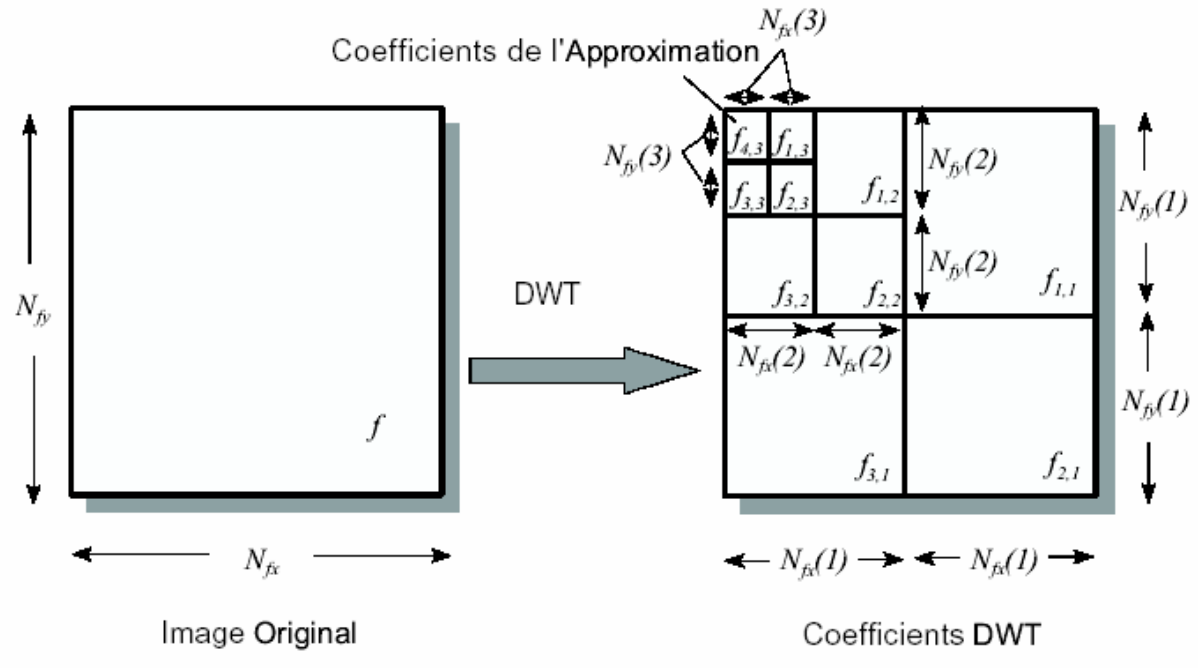



**Figure A.2: Notation utilisée pour les coefficients de la DWT. Le *L*-eme niveau de la décomposition discrète par ondelettes est composé des coefficients $f_{o,l}$ (m, n) où $o = 1, 2, 3$ correspond aux détails horizontal, diagonal et vertical, respectivement et au $l = 1, 2, \ldots, L$ est le niveau particulier de résolution.**

# B. La Transformée de Fourier Discrète :

Une image peut être considéré comme une fonction discrète à valeurs réelles $I(x,y)$ définie sur un repère cartésien de nombres entiers, telle que

$$I(x,y) \mid 0 \le x \le N-1 \wedge 0 \le y \le M-1$$

On considère le cas particulier d'une image carrée (*M =N),* la transformée de Fourier discrète bidimensionnelle *de* $I(x,y)$ est définie comme suite

$$F(u,v) = \frac{1}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} I(x,y)e^{-j\frac{2\pi}{N}(ux+vy)}$$

Où les éléments de $F(u,v)$ sont des nombres complexes
Et la transformée inverse de Fourier discrète est

$$I(x,y) = \frac{1}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F(u,v)e^{-j\frac{2\pi}{N}(ux+vy)}$$

Soit la notation du module et de la phase de la transformée

$$M = |F(u,v)|$$

$$\Phi = \angle F(u,v)$$

## Propriétés intéressantes de la DFT :

Cette section présente quelques propriétés de base d la DFT liés aux transformations géométriques dans le domaine spatial (c.-à-d. translation, rotation et recadrage).

**A. Translation :**

Puisque $F(u,v)$ et $I(x,y)$ sont des fonctions périodiques de période $N$, les relation suivantes s'imposent :

$$F(u,v) = F(u+N, v+N)$$

$$I(x,y) = I(x+N, y+N)$$

De plus, de la symétrie du spectre de la DFT on peut démontrer que

$$|F(u,v)| = |F(-u,-v)|$$

Maintenant, un décalage de $I(x,y)$ dans le domaine spatial se traduit par un décalage linéaire de la phase de la DFT

$$F(u,v)e^{-j\frac{2\pi}{N}(au+bv)} \leftrightarrow I(x+a, y+b)$$

Notez que puisque $F(u,v)$ est périodique, il est évident que des variations dans le domaine spatial, où les translations causent un enveloppement de l'image sur elle même Ceci est désigné sous le nom d'une translation circulaire.

Il est claire de l'équation précédente que le décalage dans le domaine spatial de l'image n'affecte que la phase de la DFT et laisse le module intact. Ceci montre que le spectre de la DFT est invariant.

**B. Rotation :**

Si on représente les cordonnées de la DFT et de l'image en leurs représentation polaire

$$x = r\cos\theta$$

$$y = r\sin\theta$$

$$u = \omega\cos\phi$$

$$v = \omega\sin\phi$$

En appliquant ces formules, les représentation de $F(u,v)$ et $I(x,y)$ deviennent $F(w,\phi)$ et $I(r,\theta)$, si on fait une rotation de l'image d'un angle $\theta_0$ cella cause une rotation de même angle au spectre de la DFT de l'image.

$$I(r,\theta+\theta_0) \leftrightarrow F(\omega,\phi+\theta_0)$$

**C. Changement d'échelles** :

Un changement d'échelles dans le domaine spatial cause un changement d'échelles inverse dans le domaine fréquentiel :

$$I(ax,by) \leftrightarrow \frac{1}{|ab|}F\left(\frac{u}{a},\frac{v}{b}\right)$$

# C. Transformation DCT : transformée en cosinus discrète bidimensionnelle :

La clé du processus de compression est la **DCT** (**D**iscrete **C**osine **T**ransform). La **DCT** est une transformée fort semblable à la **FFT** : la transformée de Fourier rapide (***F**ast **F**ourier **T**ransform*), travaillant sur un signal discret unidimensionnel. Elle prend un ensemble de points d'un domaine spatial et les transforme en une représentation équivalente dans le domaine fréquentiel. Dans le cas présent, nous allons opérer la **DCT** sur un signal en trois dimensions. En effet, le signal est une image graphique, les axes **X** et **Y** étant les deux dimensions de l'écran, et l'axe des **Z** reprenant l'amplitude du signal, la valeur du pixel en un point particulier de l'écran. La **DCT** transforme un signal d'amplitude (chaque valeur du signal représente l' "amplitude" d'un phénomène, ici la couleur) discret bidimensionnel en une information bidimensionnelle de "fréquences".

L'écriture de la **DCT** est :

$$F(u, v) = \frac{2}{N} c(u).c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Img(x, y).\cos\left[\frac{\pi}{N} u\left(x + \frac{1}{2}\right)\right].\cos\left[\frac{\pi}{N} v\left(y + \frac{1}{2}\right)\right]$$

La transformation inverse est donnée par :

$$Img(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u).c(v).F(u, v).\cos\left[\frac{\pi}{N} u\left(x + \frac{1}{2}\right)\right].\cos\left[\frac{\pi}{N} v\left(y + \frac{1}{2}\right)\right]$$

Où $\begin{cases} c(0) = (2)^{-1/2} \\ c(w) = 1 \text{ pour w } = 1,2,\ldots,N-1 \end{cases}$

Le calcul de la **DCT** ne peut pas se faire sur une image entière d'une part parce que cela générerait trop de calculs et d'autre part parce que le signal de l'image doit absolument être représenté par une matrice carrée. Dès lors, le groupe **JPEG** impose la décomposition de l'image en blocs de 8 pixels sur 8 pixels. La méthode de compression sera donc appliquée indépendamment sur chacun des blocs. Les plus petits blocs en bordure devront être traités par une autre méthode.

La **DCT** est donc effectuée sur chaque matrice 8x8 de valeurs de pixels, et elle donne une matrice 8x8 de coefficients de fréquence: l'élément (0,0) représente la valeur moyenne du bloc, les autres indiquent la puissance spectrale pour chaque fréquence spatiale. La **DCT** est conservative si l'on ne tient pas compte des erreurs d'arrondis qu'elle introduit.

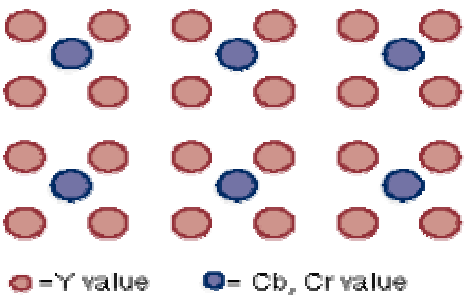
Lorsqu'on travaille avec le signal *Img*(*x*,*y*), les axes ***X*** et ***Y*** représentent les dimensions horizontales et verticales de l'image. Lorsqu'on travaille avec la transformée de cosinus discrète du signal *DCT*(*i*,*j*), les axes représentent les fréquences du signal en deux dimensions

# D. La Compression JPEG :

JPEG signifie Joint Photographic Expert Group. L'orientation principale de cette méthode de compression est donc la photographie. La compression JPEG est une compression avec pertes, ce qui lui permet, en dépit d'une perte de qualité un des meilleurs taux de compression (jusqu'à 20:1 à 25:1 sans perte notable de qualité). Elle est bien plus efficace lorsqu'elle est utilisée sur des images photographiques (qui comportent de nombreux pixels de couleurs différentes) que sur des images géométriques, contrairement à la méthode RLE.
La méthode JPEG utilise une variante de la transformée de Fourier, la transformée en cosinus (Discrete Cosine Transform ou DCT). Tout d'abord, la méthode de compression JPEG sépare l'image en blocs de 8x8 pixels. Par la suite, on applique à chacun des blocs la transformation en cosinus, qui transforme l'ensemble valeurs du domaine spatial en son équivalent dans le domaine temporel.

Cette opération ne compresse pas le fichier.

Puis vient la phase de quantification : au sein de ces blocs, on ne travaille pas sur les couleurs (codage Rouge/Vert/Bleu) mais sur la luminance et la chrominance. La **chrominance** est composée de la teinte et de la saturation et correspond à la couleur d'un pixel. La **luminance** correspond à l'intensité lumineuse du pixel. Au niveau de la perception humaine, la luminance est plus importante que la chrominance : l'oeil perçoit mieux les variations de luminosité que les variations de couleur. Cette caractéristique permet de réduire la taille des informations stockées lors de la compression : avec un simple codage Rouge/Vert/Bleu, on utilise trois matrices de la taille de l'image (en pixels), et on code les informations au sein de ces matrices. Le JPEG convertit les informations de couleur en information luminance/chrominance. On peut alors utiliser une matrice luminance de la taille de l'image et des matrices chrominances (teinte et saturation) deux fois plus petites : lors de l'affichage on aura une précision d'un pixel pour la luminance et de deux pixels pour la chrominance. Ceci ne sera pas perceptible pour l'oeil humain.

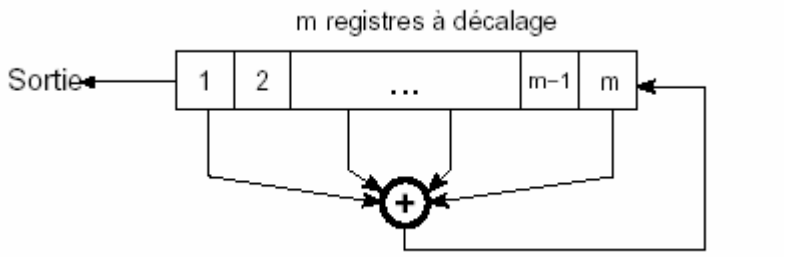


Cette transformation engendre des pertes, variables selon le type d'image source. On applique enfin un codage de Huffman : c'est la phase de codage statistique. Le résultat obtenu est alors la forme compressée de l'image initiale.


Schéma de l'algorithme de la compression JPEG

# D. Les M- Séquences :

Les M- Séquences, signifiant « maximum lenght shift register sequence » sont souvent utilisées pour représenter des séquences aléatoires. Ces séquences sont de longueur $L = (2^m - 1)$ bits et sont générées à partir de $m$ registres à décalage avec bouclage comme illustré dans la figure suivante :




**Principe du générateur MLBS**

Les registres qui sont bouclés dépendent des coefficients de polynômes « premiers ». Ces séquences sont périodiques de période $L$ .elle contiennent chacune $(2^m - 1)$ éléments égaux à (+1) et $(2^{m-1} - 1)$ éléments égaux à (-1).

La fonction d'auto corrélation $R_c(m)$ des M- Séquences est une caractéristique importante. Le calcul s'effectue de la manière suivante :

$$R_c(m) = \sum_{n=1}^{L} c_n c_{n+m} = \begin{cases} L & Si \quad m = 0 \\ -1 & Si \quad m \neq 0 \end{cases}$$

Pour N grand on obtient la propriété suivante :

$$R_c(0) >> R_c(n), n \neq 0$$

Cette propriété permet de localiser facilement la séquence aléatoire même si celle-ci est perturbée par un bruit additif important.