REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

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

MEMOIRE

Présentée Pour obtenir

LE DIPLOME DE MAGISTERE EN ELECTRONIQUE

Option : *TRAITEMENT DU SIGNAL*

Par

Mr : BOUDERBALA AHMED

Implémentation d'un algorithme de tatouage Vidéo robuste dans Le domaine compressé

Devant le jury :

Président :	CHAREF Abdelfetah	Professeur UMC.
Rapporteur :	KHAMADJA Mohammed	Professeur UMC.
Examinateurs :	BENNIA Abdelhak	Professeur UMC.
	HACHOUF Fella	M.C UMC.

Remerciements

Louange à dieu le miséricordieux, qui m'a permis d'accomplir ce travail.

Je tiens à remercier vivement mon directeur de mémoire :

Le professeur Mohammed KHAMADJA

D'avoir dirigé ce travail, ainsi pour toutes les facilités matérielles qu'il m'a accordé pour

L'accomplissement de ce travail.

Comme je tiens à remercier en particulier le docteur : Said BENYERBAH, pour m'avoir co-dirigé avec

compétence tout le log de ce travail, ainsi pour tous les efforts fournis à mon égard.

Je remercie le professeur : Abdelfetah CHAREF, d'avoir accepter de présider le jury, et également

le professeur : Abdelhak BENNIA , et le M.C : Hachouf Fella qui ont accepté

d'être membres du jury

Je remercie toute ma famille, ainsi que tous les amis et collègues, pour leur soutien

et encouragement au cours de mes études

Dédicace

grâce a dieu et par son aide j'arrive au bout de chemin laborieux a cet effet et par ce mémoire qui couronne la de la mon parcoure universitaire.

Je dédie ce modeste travail, résultat de toutes les années d'étude :

A mes très chers parents pour tout leur sacrifice, et pour tout leur encouragement durant toutes mes années d'étude.

A mes frères et mes sœurs.

A ma grande mère.

A toute la famille.

A tous mes amis de près ou de loin.

A tous mes camarades de la promotion.

Monsieur BOUDERBALA AHMED

Table des matières

Sommaire

Chapitre 2 : METHODE DE TATOUAGE VIDEO DEVELOPPEE

Chapitre 3 : RESULTATS DE SUMULATION

Liste de figures

Introduction générale

Les applications du traitement d'images sont multiples et interviennent dans de nombreux aspects de la vie courante et professionnelle. Avec l'ère de l'information, de l'internet haut-débit, de l'audiovisuel et du numérique, l'expansion et la circulation des supports multimédia ont beaucoup augmenté.

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

Le but de ce mémoire était d'élaborer un algorithme de tatouage vidéo. Cet algorithme est robuste contre les dégradations de traitement de l'image et invisible. C'est pour cette raison, Nous avons choisi d'utiliser les coefficients hautes fréquences de macro blocs dans l'image comme support pour développer notre algorithme. En marge du tatouage, nous avons donc étudié la qualité de la vidéo tatouée afin de proposer une méthode complète de tatouage des images vidéo.

Dans ce mémoire, nous aborderons les aspects de la protection des images vidéo. Plus précisément, ce mémoire est composé des chapitres suivants :
Dans le premier chapitre, nous présentons un état de l'art décrivant les principes généraux du tatouage ainsi que sur les algorithmes de base de tatouage vidéo.

Dans Le deuxième chapitre, nous présentons de manière détaillée, l'algorithme de tatouage que nous avons élaboré au cours de ce mémoire afin de pouvoir concevoir une protection complète, par la mise en oeuvre de ce procédé, d'une vidéo. Nous exposerons en premier lieu le principe fondamental de notre méthode, la mise en place d'une règle d'insertion permettant de garantir la sécurité du schéma proposé et de minimiser l'impact visuel de tatouage.

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

1. Introduction

Le tatouage des données numériques est une discipline récente. Cette technique permet une protection du média (image, vidéo, audio). Le tatouage des images de la vidéo consiste à insérer une marque de façon robuste et imperceptible [1].

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

Après avoir présenté les propriétés du tatouage, nous décrivons les processus d'insertion puis de détection de la signature et soulignons les contraintes auxquelles doit faire face un algorithme de tatouage. Et nous présentons ensuite les différentes techniques de tatouage existent. Et Nous soulignons l'importance du choix du domaine d'insertion.

Enfin, nous ajoutons à ces méthodes d'autres techniques qui rendent l'algorithme plus performant, nous distinguons les différentes méthodes d'insertion, avant la compression, durant la compression et après la compression. Et la catégorie des schémas qui permet une synchronisation de la signature lors de la détection, nous présentons notamment diverses attaques susceptibles d'empêcher la détection de la signature.

2. Principes généraux d'une méthode de tatouage d'image

Afin d'étudier les différents aspects du problème de tatouage, selon les applications particulières et ses exigences, nous devons clarifier le modèle général du tatouage. Un schéma classique de tatouage des images peut se décomposer en deux étapes fondamentales :

La phase d'insertion.

La phase de détection.

2.1. La phase d'insertion

La figure 1.1 présente le schéma d'implémentation de la marque [2]. L'insertion de la marque dans une image I permet d'obtenir une image tatouée notée I_W. L'espace d'insertion $T(I)$ peut être le domaine spatial on bien le résultat d'une transformation réversible qui facilite l'insertion comme la DCT (Discrete cosins transform), la Transformée de Fourier Discrète (TFD) ou encore une Transformation par Ondelettes (TOD). La signature insérée W, dépend d'une clé secrète K mais aussi du message $\{b_0, b_1, ..., b_{n-1}\}$ que l'on désire insérer. Cette signature peut être une séquence pseudo aléatoire possédant certaines propriétés (distribution gaussienne ou uniforme), une donnée binaire {-1, +1} ou bien une petite image (logo).

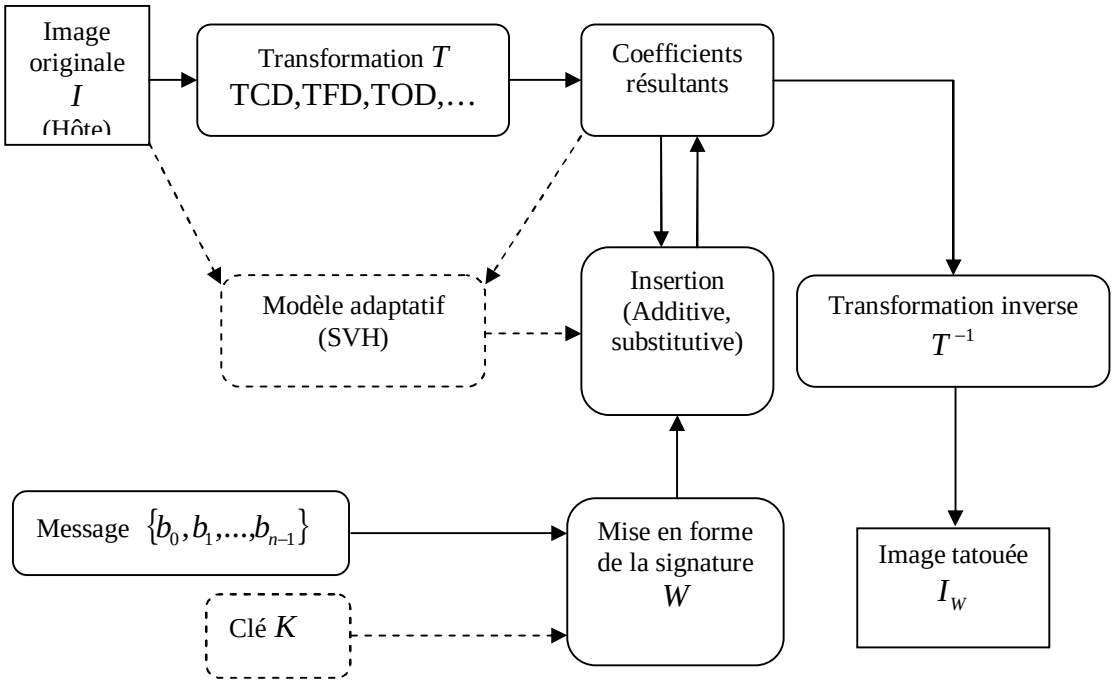


Figure 1.1 Schéma du processus d'insertion d'une signature.

L'utilisation d'un modèle psychovisuel adaptatif permet de contrôler et d'augmenter la force de la signature. Notons que par le choix d'un domaine fréquentiel approprié tout en choisissant seulement certains coefficients, beaucoup de systèmes visuels humains (SVH) [3] peuvent être effectués implicitement. Plus la transformation de l'image approche les propriétés du SVH, plus il est facile de mettre plus d'énergie dans l'image hôte sans produire une déformation perceptible.

2.2. Phase de détection

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

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

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

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

La figure 1.2 présente le processus de détection [2]. La marque extraite W' est comparée à la marque originale W par mesure de corrélation. La mesure de similitude la plus utilisée entre W et W' est la corrélation normalisée pour les séquences pseudo-aléatoires,

$$\delta = \frac{W'.W}{\|W'\|.\|W\|} \qquad (1.1)$$

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

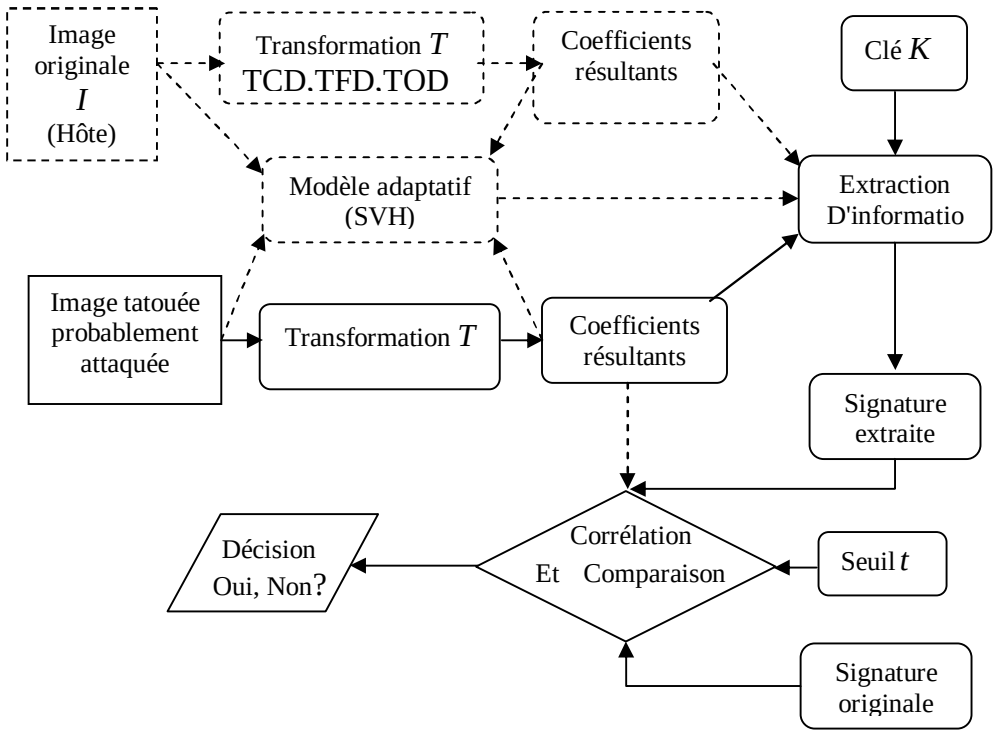


Figure 1.2 Schéma du processus de détection d'une signature.

3. Les contraintes d'un schéma de tatouage efficace

Que ce soit pour l'image fixe, pour l'audio ou pour la vidéo, le tatouage fait appel aux principes de base suivants [4]:

3.1 Robustesse

C'est la capacité que possède un algorithme de tatouage à résister aux attaques extérieures, qu'elles soient bienveillantes ou malveillantes. Pour la vidéo, il peut s'agir d'attaques simples comme le changement de format de compression, le changement de débit ou tout autre traitement classique (il s'agit ici de traitements bienveillants qui ne visent pas forcement à retirer la marque). On peut aussi avoir des attaques plus élaborés, qui ont pour seul but de retirer la marque, comme des attaques statistiques aveugles ou des attaques basées sur la connaissance de l'algorithme utilisé ([5] et [6]).

3.2 Capacité

C'est la quantité d'information (bits de tatouage) que l'on peut cacher au sein du média (image ou vidéo). Il paraît évident que plus on augmente la capacité, plus la signature sera

perceptible, et plus la robustesse diminuera (dans le cas où on veut retrouver exactement la marque).

3.2 Invisibilité

C'est l'impact que peut avoir la signature sur l'image ou la vidéo tatouées. Plus le marquage sera fort, plus elle sera visible (et inversement). Concevoir un algorithme de tatouage revient à trouver le meilleur compromis entre ces trois principes, en fonction de l'application visée.

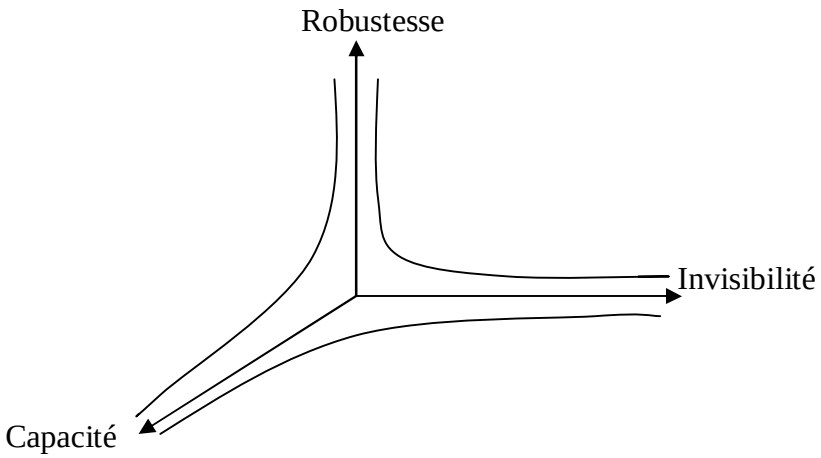


Figure 1.3 problématique des contraintes d'un schéma de tatouage.

4. Les applications du tatouage

Les applications classiques d'un système de tatouage vidéo sont les suivantes:

4.1 Protection de copyright

Le tatouage offre une alternative intéressante pour protéger l'image, même lorsque celle-ci est diffusée. La protection des droits d'auteur représente, quant à elle, l'application la plus courante aujourd'hui. L'objectif est d'insérer une information dans l'image ou vidéo source, typiquement le copyright du propriétaire, afin de prévenir toute revendication frauduleuse de propriété. Cette signature ne doit être connue que de la personne ou de l'organisme de tatouage. Elle dépend donc d'une clé secrète, qui permet son insertion et sa détection. Cette application nécessite la mise en place d'un algorithme de tatouage d'un niveau de robustesse très élevé.

4.2. Les Empreintes

Cette application est utilisée pour tracer les copies illégales de media (suivi des pirates). Ce type d'application engendre un marquage unique pour chaque copie distribuée (typiquement un numéro de série). Cependant, la distribution de copies composées de différentes marques, peut engendrer des problèmes de collusions [7]. Ainsi, les marques utilisées devront satisfaire un critère de sécurisation de collusions.

4.3. Protection contre la copie

Un souhait des distributeurs de multimédia est l'existence d'un moyen de protection contre la copie, afin d'interdire une circulation de media illégaux. Cependant, il est possible d'utiliser des marques spécifiant le statut de la copie de la donnée. Un exemple est le système DVD, dans lequel les données contiennent des informations de marquage. Exemple : Il existe deux types de DVD les conformes et les non conformes. Les lecteurs de DVD dits "non conformes" sont basées sur une norme qui ne souscrit pas au traité de protection des DVD. Un DVD sur lequel s'exerce les droits d'auteur, peut être lu et décrypté par un lecteur conforme. Il ne peut pas être lu par un lecteur non conforme, un problème survient lorsque le DVD crypté est attaqué, et qu'il devient possible de se procurer une copie décryptée de ce DVD. L'utilisation du tatouage permet de combler cette faille, en insérant des informations au sein du flux MPEG4. Les lecteurs non conformes sont capables de lire seulement les DVD illégaux, et les lecteurs conformes, les DVD légaux.

4.4. Contrôle de diffusion

On peut insérer une marque dans une publicité, afin d'en contrôler la diffusion. Cela peut également servir à réaliser une audiométrie.

4.5. Authentification de données

L'objectif est de détecter toutes modifications éventuelles des données, afin de pouvoir certifier si celles-ci ont été modifiées ou non.

4.6. Indexation

Le domaine de l'indexation des images consiste à classer de manière automatique des images selon leur contenu. Il permet de faciliter une recherche dans une base de données. Le tatouage d'un document permet ainsi d'insérer une information (contenant peu de bits) décrivant le contenu de l'image. Cela permet de qualifier sommairement l'image, ou d'insérer un pointeur vers une description plus complète.

4.7. Sécurité médicale

Insertion d'un "identifiant" confidentiel assurant la correspondance entre le patient et la radio, afin d'éviter toutes confusions.

5. LES TECHNIQUES DE TATOUAGE EXISTANTES

Les schémas de tatouage des images que l'on peut rencontrer dans la littérature scientifique sont très variés et peuvent sembler à première vue très différents les uns des autres. Cependant, les techniques de tatouage courantes peuvent être groupées selon ([8] et [9]) :

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

5.1 Domaines d'insertion du tatouage

Un des points clefs dans un algorithme de tatouage est l'espace d'insertion utilisé pour insérer la signature [9].

5.1.1 Le tatouage dans le domaine spatial

Cette approche consiste en la modification directe des pixels de l'image. Afin d'assurer l'invisibilité de la signature, cette modification doit rester limitée. Une des toutes premières approches utilisée consiste à insérer les bits du message dans les bits de poids faible de chaque pixel (least significant bits, LSB) [4]. Une autre approche, appelée patchwork [10], est la modification des propriétés statistiques de petites régions de l'images, comme la moyenne ou l'écart-type, le message étant représentée par exemple par la différence des ces propriétés entre deux régions adjacentes. On peut aussi inclure dans cette catégorie les techniques consistant à encoder le message dans l'histogramme de l'image, en modifiant les valeurs des pixels en conséquence. Ou bien le tatouage w peut être tout simplement ajouté aux pixels de l'image, avec une faible intensité. L'inconvénient des méthodes appliquées au domaine spatial est qu'elles sont en général peu robustes.

5.1.2 Le tatouage dans le domaine transformé

Il existe de nombreuses transformées, celles qui sont le plus couramment utilisées sont les suivantes :

– La transformée de Fourier discrète [11] : Cette dernière a largement été étudiée en tatouage puisqu'elle offre la possibilité de contrôler les fréquences du signal. Cela permet de choisir de façon adéquate les parties de l'image qui devront être marquées, afin d'obtenir un bon compromis entre visibilité et robustesse. Cette transformation est également utilisée pour fusionner la signature avec le medium, dans la phase de modulation, mais aussi utilisée pour diviser les images en bandes perceptuelles.

– La transformée en cosinus discrète [12]: Les règles de marquage opérant dans le domaine DCT sont souvent plus robustes à la compression JPEG et MPEG. Le créateur de signatures peut ainsi prévenir ces attaques plus facilement. De plus, les études menées concernant les distorsions visuelles sur la source à coder, contribuent à une meilleure prédiction de l'impact visuel d'une signature sur le medium. Enfin, insérer une signature dans le domaine compressé permet de réduire les temps de calcul.

– La transformée de Mellin Fourier [13] : La plupart des algorithmes de marquage rencontrent des problèmes lors de l'extraction de la signature, après que l'image tatouée ait subi une transformation géométrique affine. Or, la transformée de Mellin Fourier est basée sur la propriété de translation de la transformée de Fourier, qui mentionne que seule la phase est altérée par une translation. En restreignant l'espace de marquage à l'amplitude de la transformée de Fourier, le support de la signature devient insensible à toute translation de l'image.

– Le domaine ondelettes [14] : On retrouve les mêmes atouts dans la mise en place d'une signature dans le domaine des ondelettes que dans le domaine DCT pour JPEG, avec cependant un avantage supplémentaire provenant de la multirésolution. Cet aspect permet de réaliser en effet, une bonne distribution du message dans le médian en terme de robustesse et de visibilité.

– La division d'images en bandes perceptuelles [15]: Ce principe consiste à réaliser des processus itératifs, qui permettent de prendre en compte le modèle visuel humain afin de maintenir la signature en dessous d'un seuil de visibilité. Cet hypothèse est déjà utilisée en vidéo (une énergie localisée dans une bande de fréquence peut masquer une bande voisine, d'énergie plus faible, c'est le principe de masquage). L'idée de cette méthode repose sur l'hypothèse que le système visuel humain divise le stimulus visuel en plusieurs composantes. Chaque composante étant associée à 3 paramètres :

– la localisation dans le champ visuel.

– la fréquence spatiale (calculée à partir de l'amplitude de la transformée de Fourier).

– l'orientation (calculée à partir de la phase de la transformée de Fourier).

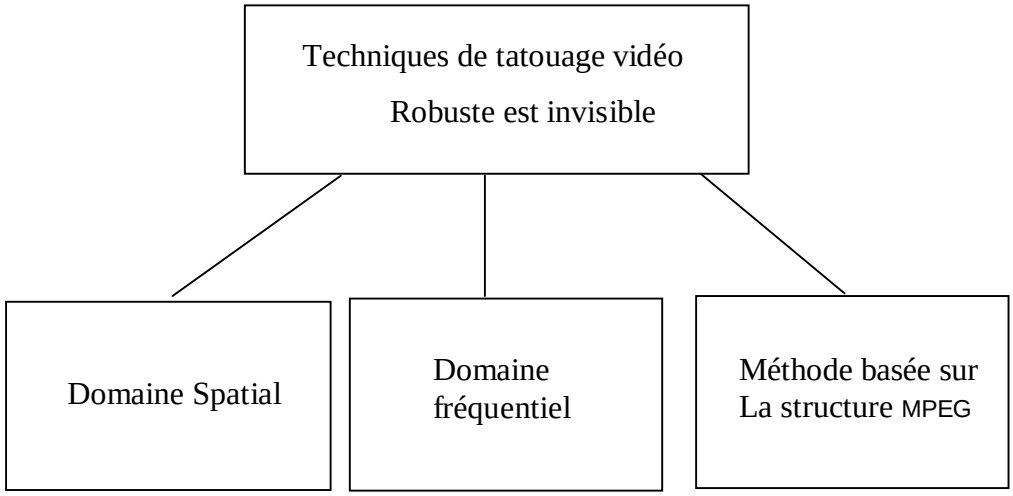


Figure 1.4 Classification des techniques de tatouage vidéo

5.2 Les méthodes additives

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un bruit à l'image [9]. La figure 1.5 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque W_0 qui est composée d'un bruit blanc bb de générateur K modulant parfois un message M . La seconde étape est la pondération de cette marque par un facteur a issu du calcul d'un masque psychovisuel *Ma*. La troisième étape est l'addition de la marque à l'image. Cette incrustation peut se faire directement sur l'image I (dans le domaine spatial) ou sur une transformée Tr de celle-ci (TFD, TCD, TOD,…etc.) pour obtenir l'image tatouée I^*.

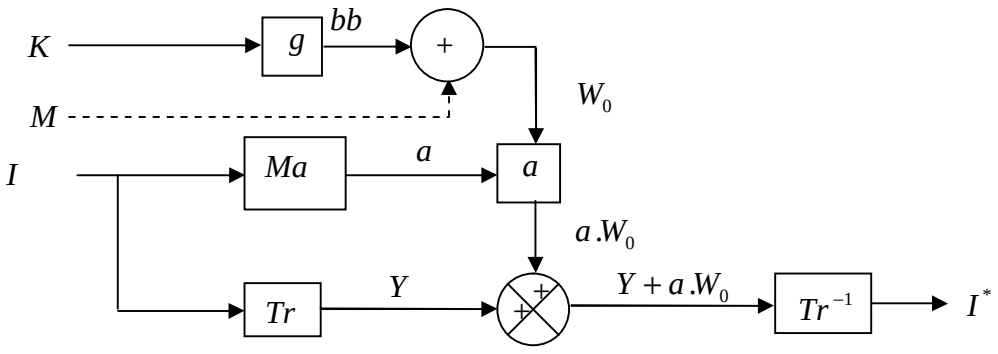


Figure 1.5 Schéma de tatouage d'une méthode additive.

5.3 Les méthodes substitutives

La classe des schémas substitutifs peut être représentée par des schémas où la signature n'est pas ajoutée mais substituée des composantes de l'image [9]. Une clé secrète *K* associée à un générateur aléatoire permet de sélectionner les différentes composantes $C_K(I)$ de l'image. Ces composantes peuvent désigner les pixels d'une image, ou une transformée de celle-ci (TCD, TFD,…etc.). La signature à insérer est obtenue en appliquant une contrainte (par exemple : un critère de similarité ou une relation d'ordre) sur $C_K(I)$ en fonction du message à insérer. On procède ensuite à l'étape de substitution.
L'image tatouée *I** est reconstruite à partir des composantes propres à la signature (figure 1.6).

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

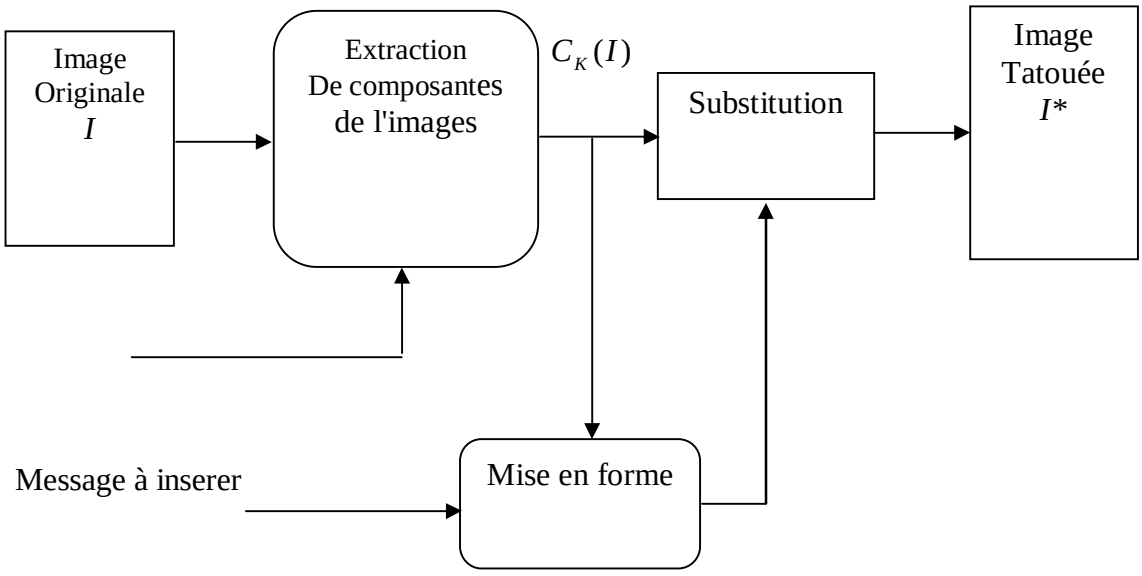


Figure 1.6 Principe de l'insertion par Substitution

6. ETAT DE L'ART DU TATOUAGE VIDEO

Dans un flux vidéo, il est possible de tatouer les images de type intra et inter [16]. De nombreux schémas développes peuvent être appliqués aux séquences vidéos. Ces dernières présentent cependant d'autres propriétés, qui peuvent être exploitées pour l'insertion de la signature :

- la taille brute d'une séquence vidéo est beaucoup plus importante que la taille d'une image fixe. L'espace d'insertion de la signature en est considérablement augmenté.
- la dimension temporelle du signal traité peut être utilisée pour l'insertion de la signature. Celle-ci peut, par exemple, être insérée dans le mouvement des différents objets de la séquence. Les séquences vidéo présentent également des contraintes différentes de celles des images fixes.
- la complexité du schéma de tatouage doit être faible. L'insertion et la détection de la signature doivent pouvoir s'effectuer en même temps, dans la plupart des applications. La contrainte de temps réel s'applique essentiellement à la phase de détection.
- le mouvement des objets augmente souvent la visibilité de la signature : ainsi, une signature "fixe" ajoutée sur un objet en mouvement, sera d'avantage perceptible que si l'objet est statique.
- le flux vidéo est souvent compressé de manière à réduire la taille originelle des séquences. L'insertion de la signature peut alors directement s'effectuer lors de la compression. L'insertion sur le format décompressé ne doit pas entraîner, après compression, une augmentation significative de la taille des données.
- la présence de la signature dans la séquence vidéo peut permettre d'autres attaques que celles liées aux images fixes. Si la signature est redondante dans la séquence, elle peut être estimée en calculant la moyenne des différentes images de la séquence. La signature doit pouvoir être détectée après une perte de synchronisation, produite par la sélection d'une séquence précise ou la perte d'images de la séquence. La section suivante présente un aperçu des différents schémas de tatouage appliqués à la vidéo.

6.1 Les différents algorithmes de tatouage vidéo

Nous allons, dans cette section, exposer différentes approches utilisées en tatouage vidéo. Comme nous allons le voir dans la suite, les schémas de tatouage sont indirectement liés aux schémas de codage. D'ailleurs, de nombreuses techniques de tatouage sont directement issues

des techniques de codage. Le domaine spatial présente l'avantage d'être peu coûteux en temps de calcul, puisqu'il n'est pas nécessaire de réaliser des transformations. Cependant, ce domaine ne permet pas de gérer aisément l'invisibilité. En outre, les domaines transformés sont utilisés en tatouage lors de l'insertion du système de tatouage dans un processus de codage ou lors de l'insertion de la marque dans un flux compressé. Le domaine DCT est le plus couramment utilisé. D'autres transformées (telle que la FFT 3D, [17]), sont plus marginales. Un algorithme du tatouage vidéo peut se décomposer en trois classes fondamentales :

– l'insertion de la signature sur le format décompressé.

– l'insertion de la signature durant la compression.

– l'insertion de la signature après la compression.

6.2 L'insertion de la signature avant la compression

Dans cette approche, la signature est insérée directement sur le flux vidéo décompressé ([18] et [19]), cette approche basée sur le domaine spatial comme nous allons la voir dans la partie suivante.

F. Hartung et B. Girod [20] proposent une méthode d'insertion dans le domaine non-compressé, basée sur une règle additive dans le domaine spatial. Une vidéo peut être analysée suivant plusieurs points de vue, le cas d'une succession d'images 2D (en occultant la dimension temporelle), ou comme étant un signal 2D + t, ou encore la considérer comme étant un signal 3D (dans ce cas la dimension temporelle n'est pas séparée des dimensions spatiales), ou enfin comme un signal 1D, comme présenté figure 1.7.

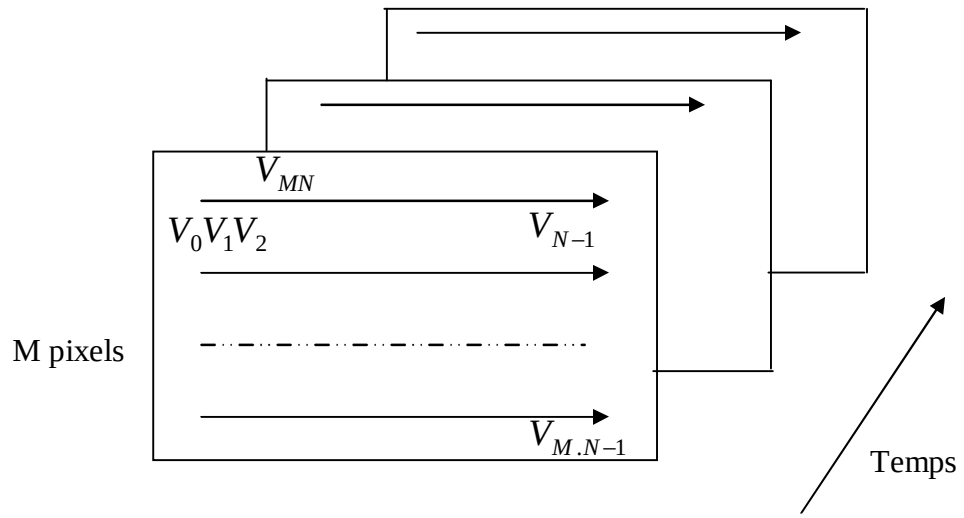


FIG 1.7 Représentation d'un signal vidéo en un signal 1D

- **Génération de la signature**

On souhaite insérer la signature suivante :

$$a_j, a_j \in \{-1, 1\}, j \in N \tag{1.2}$$

Cette signature est tout d'abord sur-échantillonnée d'un facteur c_r, afin de créer un signal redondant, permettant de le rendre plus robuste.

$$b_i = a_j,\ j.c_r \le i \le (j+1).c_r, i \in N \tag{1.3}$$

On module ensuite le signal obtenu par un bruit binaire pseudo-aléatoire, qu'on amplifie ensuite par un facteur a :

$$\begin{cases} p_i ; p_i \in \{1,-1\}, i \in N \\ w_i = a_i.b_i.p_i, i \in N \end{cases} \tag{1.4}$$

- **Insertion de la signature**

Le tatouage est ajouté de la façon suivante :

$$\bar{v}_i = v_i + a_i.b_i.p_i, i \in N \tag{1.5}$$

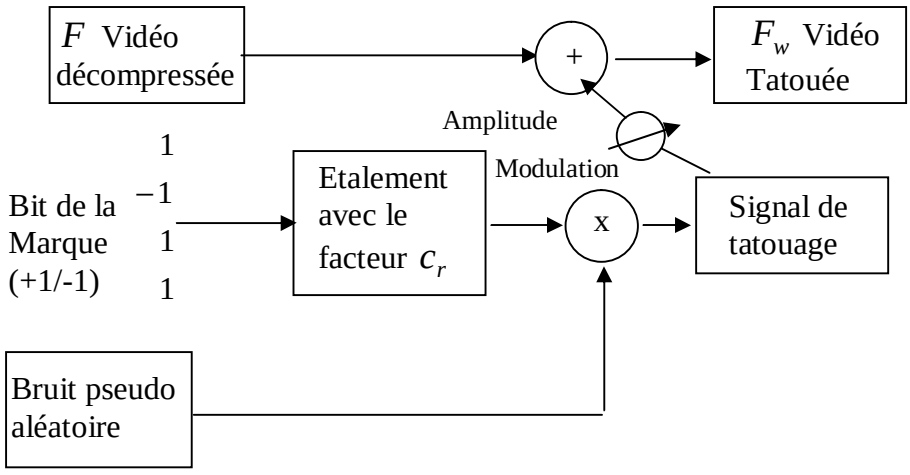


FIG 1. 8 Procédure d'insertion de Hartung

- **Extraction de la marque**

Pour l'extraction, la vidéo originale n'est pas nécessaire. Avant de commencer la détection, l'image est filtrée par un filtre passe bas. Le signal obtenu v_w est démodulé en le multipliant par le bruit utilisé lors de l'insertion de la signature. On calcule ensuite la corrélation entre la signature et le signal obtenu.

$$s_j = \sum_{i=j.c_r}^{(j+1).c_r-1} p_i.v_w \qquad (1.6)$$

L'inconvénient majeur de cette méthode, c'est que la signature ne doit pas entraîner, après la compression.

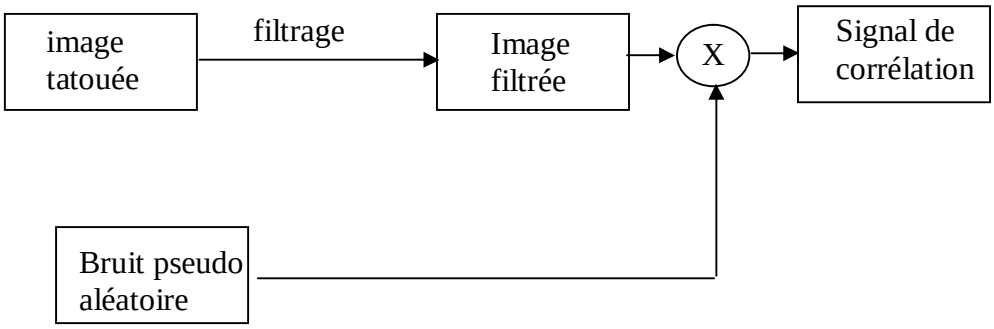


FIG. 1.9 Procédure d'extraction

6.3 L'insertion de la signature durant la compression

Nous allons, dans cette section, exposer différentes approches utilisées en tatouage vidéo durant la compression [21]. Il y'a beaucoup de méthodes utilisant l'approche d'insertion dans le domaine compressé. Ces dernières ont largement été utilisées puisqu'elles offrent la possibilité d'obtenir plus grande robustesse et aussi l'impact visuel sur la vidéo tatouée est très faible ainsi que l'insertion et la détection de la signature peuvent être effectuées en temps réel.

F. Hartung et B. Girod [20], dans leurs secondes approches, proposent un schéma de marquage qui s'applique directement au flux compressé en ne marquant que les images intra.

- **Insertion de la signature**

L'insertion se fait dans le domaine DCT, sur les images intra. Les blocs DCT de l'image et ceux correspondant à la signature sont ajoutés. Afin de ne pas augmenter le débit de la vidéo, seuls les blocs marqués dont la taille est inférieure ou égale au bloc original sont sélectionnés. La figure 1.10 explicite la procédure d'insertion.

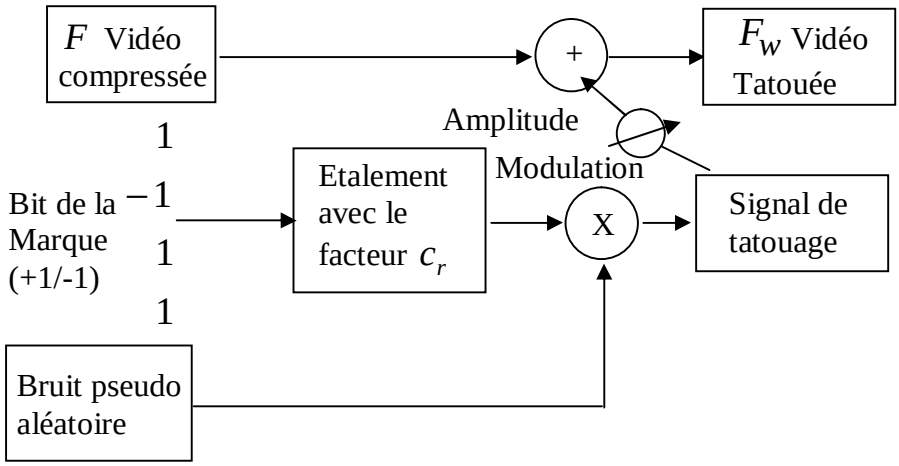


FIG. 1.10 Procédure d'insertion

6.3.1 Tatouage par la méthode de différence d'énergie

Le tatouage vidéo qui utilise la différence d'énergie est appelé (Differential Energy Watermarking DEW) [22]. En calculant la différence d'énergie entre certains groupes de blocs 8x8 de coefficients DCT dans les images intra on peut représenter le bit de la signature {1,-1}. La différence d'énergie est imposée par la suppression des coefficients DCT hautes fréquences des blocs. Les blocs 8x8 transformées dans une image intra sont sélectionnés aléatoirement en utilisant un code secret. Ce processus atteint deux objectifs, le premier est, on ne peut pas extraire la marque correctement sans utiliser la clef secrète. Deuxièmement, le processus est fait pour éviter un groupe des blocs non équilibré dont l'énergie existe.

L'algorithme de DEW a plusieurs paramètres réglables qui sont employés pour insérer la signature, et pour l'optimiser ou pour la capacité, la robustesse ou impact visuel [23], Les paramètres sont les suivants :

- **Le nombre des blocs 8x8 utilisé correspondent un bit de tatouage** : Ce paramètre est représenté par n dans la figure 1.11. Si plusieurs blocs sont utilisés pour insérer un bit de la marque, la capacité du tatouage réalisée est faible mais le tatouage devrait être plus robuste et la dégradation et très faible parce que la différence d'énergie est diffusée sur plusieurs blocs. L'énergie dans la région $S(c)$ montrée dans la figure (1.11) est doit être enlevée à chaque bloc DCT.
- **Calcule la différence d'énergie** : C'est la valeur minimale de $(E_A - E_B)$ comme illustrée dans la figure (1.11). Ce paramètre influé sur la robustesse et l'impact visuel de tatouage, si la différence d'énergie $(E_A - E_B)$ est grande, le tatouage inséré devrait être plus robuste, cependant, la qualité visuel est décroissante parce que plusieurs coefficient DCT doivent être enlevés.
- **Point minimal de coupure** : Ce paramètre est représenté par c dans la figure (1.11). il indique l'index du nombre des coefficients DCT particuliers dans un bloc de la taille 8x8 dans le parcours en zigzag (zigzag scanned). Si $(i < c)$ le coefficient DCT ne peut pas être enlevé pour forcer la différence d'énergie. Ainsi il peut être vu comme un limiteur ou paramètre précédent par détermination de combien coefficients DCT peuvent être enlevés pour forcer la différance d'énergie, La différence d'énergie est donnée par l'équation suivante :

$$E_A - E_B \tag{1.7}$$

Où $E_A = \sum (DCT\ \ dans\ 2)^2$ (1.8)

Et,

$$E_B = \sum (DCT\ \ dans\ 2)^2 \tag{1.9}$$

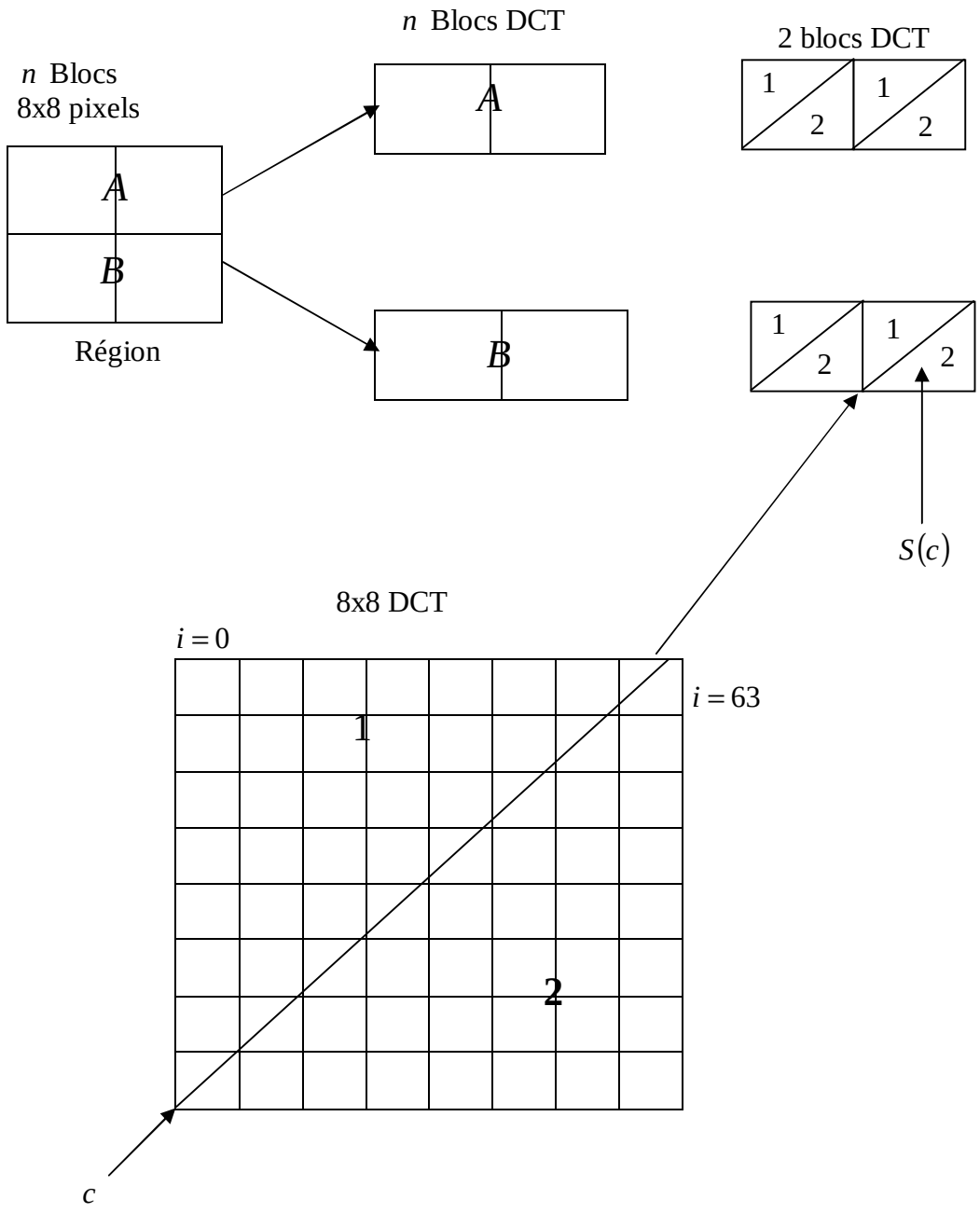


Figure 1.11 Procédure du tatouage par différence d'énergie

6.3.2 Méthode de tatouage adaptée à la norme H.264

Ta.Te Lu, Wei. Lun Hsu, and Pao. Chi Chang [24] proposent une méthode d'insertion dans le domaine compressé, basée sur une règle substitutive dans le domaine transformé DCT. Le principe de leur méthode consiste à insérer le tatouage seulement dans les images

intra du H.264, qui exploite l'erreur de prédiction de bloc 4x4 pour inclure le bit de tatouage. La méthode sera alors robuste aux attaques temporelles.

H.264 est une nouvelle norme avancée qui fournit plusieurs modes de prédiction des images intra et inter. L'image originale intra est divisée en macroblocs (MB_s) 16x16 avec chaque MB contient seize blocs 4x4. Pour chaque MB, l'erreur de prédiction de chaque bloc 4x4 est estimée pour avoir un minimum de taux-déformation (rate-distortion) ([25] et [26]). Afin de compresser la séquence vidéo et la signature insérée en même temps, l'algorithme de tatouage est intégré dans le codeur H.264, qui est illustrée dans la figure (1.12). Dans le codeur H.264, seulement les blocs de la taille 4x4 dans l'image I sont employés pour insérer le Tatouage.

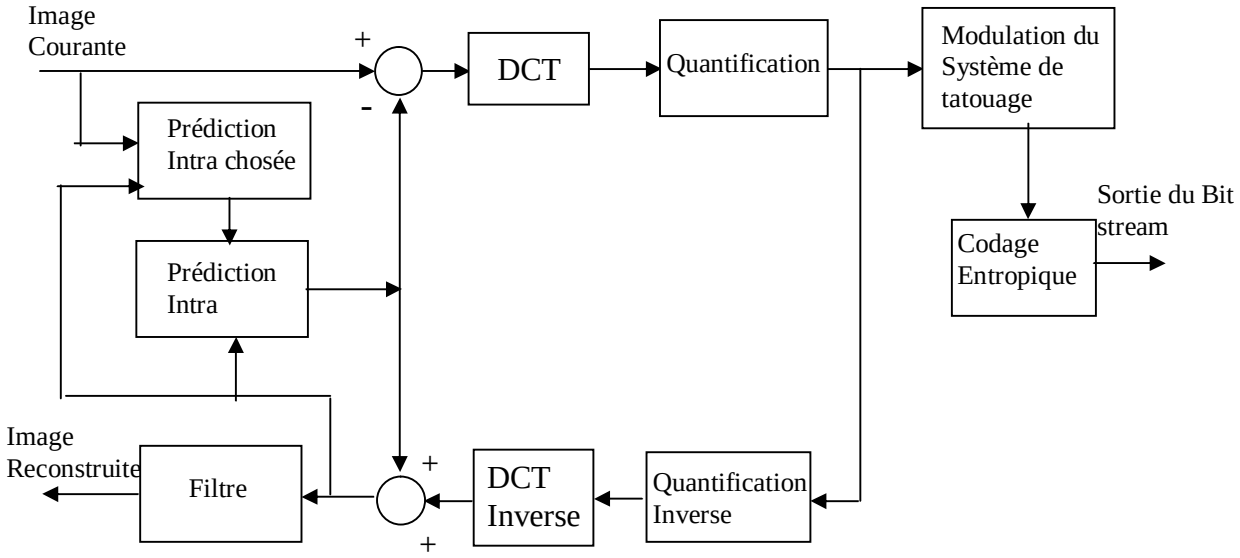


Figure 1.12 Codeur H.264 avec la marque insérée

- **Détection de la signature**

La détection de la signature est exécutée après le décodage entropique comme montré dans Figure (1.13). Les mêmes procédures d'insertion sont employées pour extraire la signature.

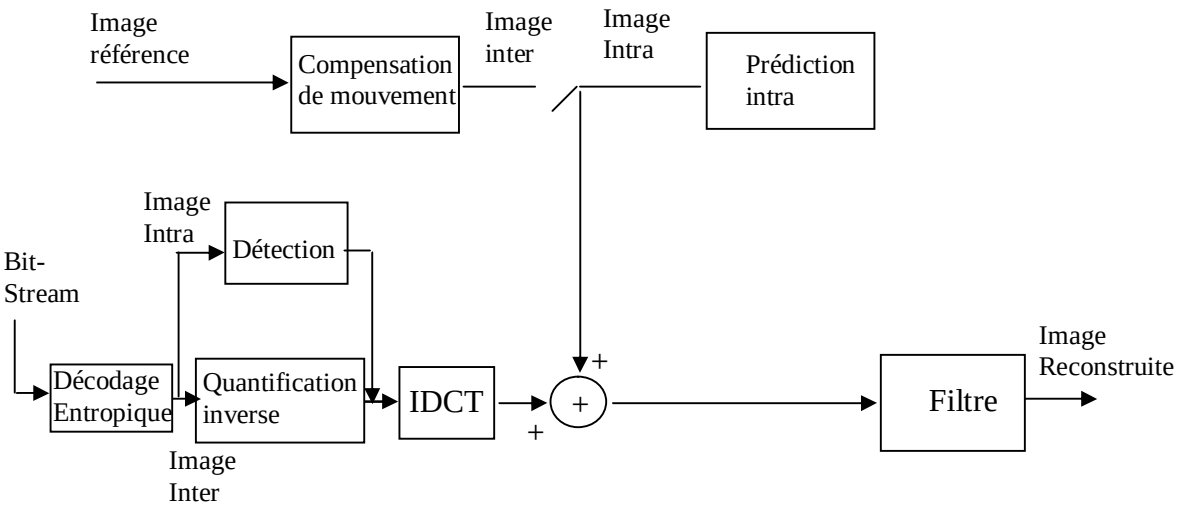


Figure 1.13 Décodeur H.264 avec l'extraction de la signature

6.3.3 Méthode de tatouage dans le domaine spatio-temporel

Koz. A, A.Alatan. A [27] proposent une méthode d'insertion dans le domaine spatio-temporel. La structure globale de leurs méthode de tatouage est donnée dans la figure 1.14 [28]. Dans cette structure, La séquence vidéo est séparée en images successives et transformée au domaine (u, v, z) par une transformation spatiale 2-D DCT suivi par une DFT (transform in the temporal direction).

Le signal de la vidéo de chaque bloc est dénoté comme $I_b(x, y, n)$, où x et y sont les cordonnées spatiales dans un bloc, n est le numéro de la trame, et b est représente le nombre du bloc. Le signal de la vidéo pour chaque bloc devrait être transformé en domaine (u, v, z) afin d'exploiter les seuils de contraste temporel. Pour ce faire, 2-D DCT (8x8) est appliquée au signal de contraste pour chaque trame et le signal résultant est dénoté comme $f_b(u, v, n)$. Puis, la DFT dans une seul dimension temporel de la vidéo est appliqué au signal résulte. Le signal de la transformée final est représente comme $F_b(u, v, z)$.

Puisque la méthode proposée devrait diffuser le tatouage sur tous les blocs de 8x8xK pixels, la séquence de tatouage est d'abord divisée dans les parties égales selon le nombre de blocs dans le sagement temporel. Puis, les éléments de la séquence de tatouage correspondant à chaque bloc sont inclus aux coefficients transformés $F_b(u, v, z)$. Afin de satisfaire l'invisibilité, la force de tatouage est limitée tels que sa valeur maximum n'excède pas les seuils temporels $T(u, v, z)$. La procédure d'insertion peut être récapitulée comme suit :

$$\left|F_b^{*}(u,v,z)\right| = \left|F_b(u,v,z)\right| + W_i T(u,v,z) \tag{1.10}$$

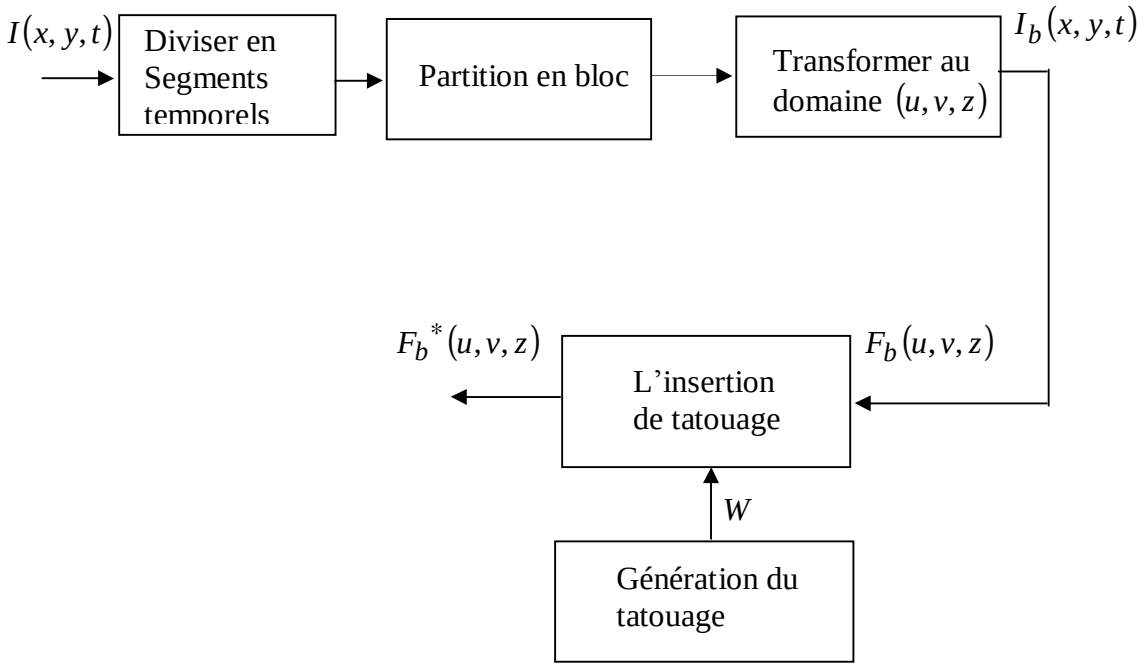


Figure 1.14 Structure globale de la procédure du tatouage

Les performances de la méthode proposée donnent une grande robustesse aux distorsions communes.

6.4 Insertion de la signature après la compression vidéo

Dans [29] les auteurs proposent un schéma d'insertion aveugle, après le processus de la compression du H.264. Un schéma fonctionnel de la méthode proposée est montré sur la figure 1.15. Cette méthode est basée sur un transcodeur, qui analyse le train binaire (bitstream) original du H.264, calcule un tatouage, insérer le tatouage et produit d'un nouveau train binaire du H.264. La première étape est un codage inverse d'entropie, qui extrait les signaux vidéo du train binaire du H.264. Dans l'étape suivante, une structure de la vidéo est analysée, les plus grandes parties de la structure contiennent des trames, Généralement les trames I, p et B sont employés. Selon le type, chaque trame est contient différents types des macroblocs. Les Macroblocs contiennent l'erreur de prédiction des vecteurs de mouvement et

des coefficients DCT. Le tatouage remplace les bits moins significatifs (LSB) des coefficients. Lors l'insertion, on change la distribution et le nombre de macro blocs Pour diminuer la dégradation. Une clef secrète est utilisée pour assurer la sécurité. Et en suite, le codage d'entropie de la vidéo est fait. Le résultat est un nouveau train binaire H.264 tatouée.

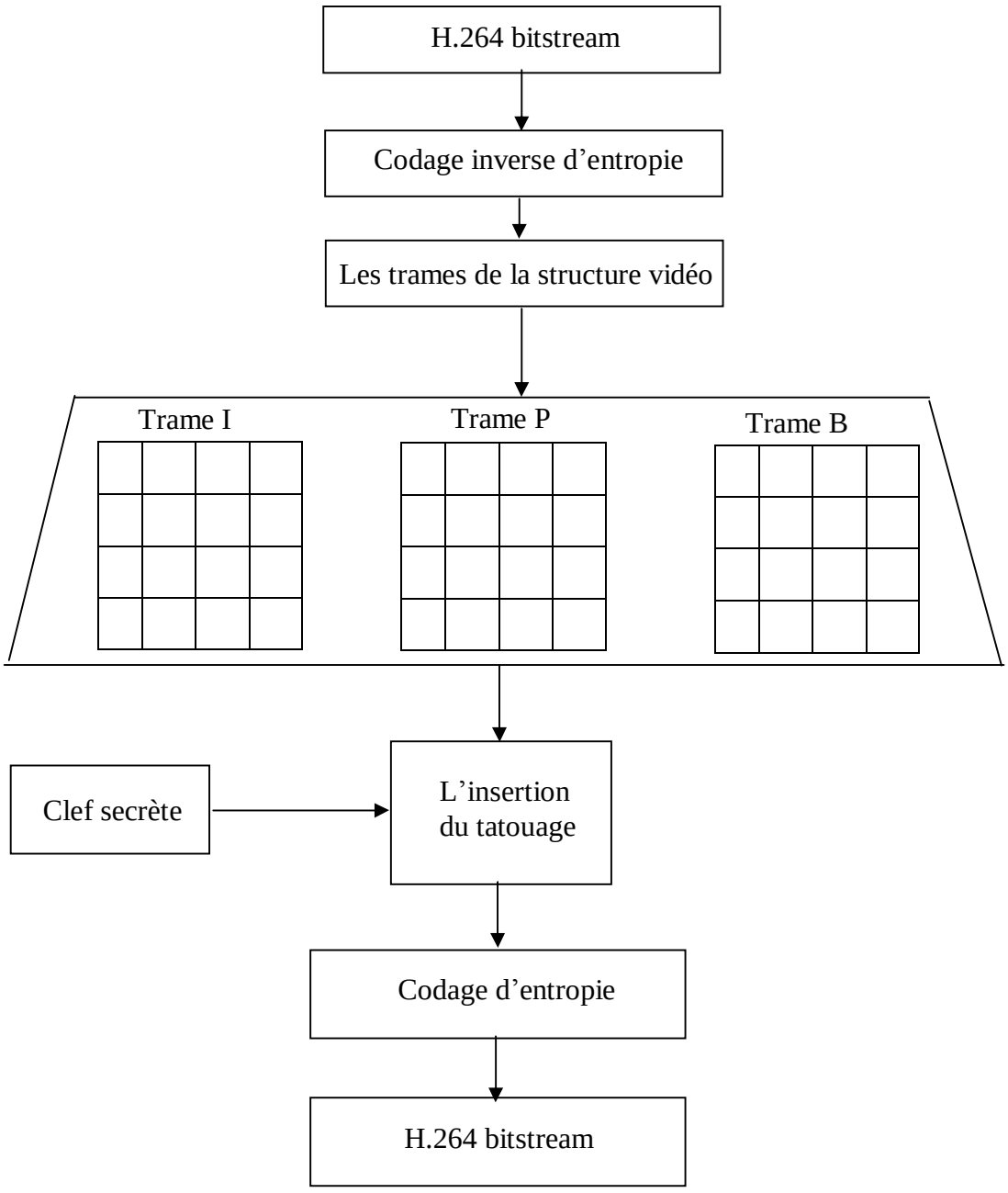


Figure 1.15 Schéma fonctionnel de la méthode proposée

Cette méthode, s'effectuée après la compression. Les coefficients résultants après l'opération de la déquantification sont généralement importants. Dans ce cas, il est claire que la modification de quelques coefficients importants pour le bit d'insérer le tatouage, diminue

la qualité de la vidéo tatouée, plus que le tatouage inséré est augmente plus que la qualité de la vidéo tatouée diminue, dans ce cas, la robustesse est faible. Les auteurs proposent cette méthode pour le but d'authentification la vidéo, c'est pour cette reason, ils n'ont pas besoin la robustesse.

7. Les attaques

La vidéo tatouée et distribuée peut subir diverses attaques, qui sont constituées par toutes les altérations qu'elle peut subir, intentionnelles ou non, et qui ont pour conséquence d'affaiblir le tatouage inséré ou d'en rendre la détection difficile. Les attaques considérées sont soit une dégradation ou un tatouage de l'image tendant à affaiblir le tatouage, soit des distorsions géométriques qui le désynchronisent. Par exemple l'impression sur papier est une attaque (généralement non intentionnelle) qui correspond à une conversion analogique. Dans ce cas l'image doit être renumérisée sur un scanner afin de pouvoir en lire le tatouage, et ce processus combine généralement une dégradation de la qualité (due surtout à la trame d'impression) et une rotation de la feuille qui est posée non alignée sur le scanner. Il existe beaucoup d'attaques contre les techniques de tatouage. Les attaques peuvent être dirigées soit contre le tatouage lui-même, soit contre le processus de détection du tatouage, soit contre les protocoles ou contre l'infrastructure de sécurité qui entoure le tatouage. Cependant ici deux catégories principales retiennent notre attention: les désynchronisations et les attaques basées sur le traitement du signal.

– Les désynchronisations correspondent aux distorsions géométriques que nous avons déjà vues; les déformations peuvent être globalement affines ou non, ou même peuvent varier localement. Elles ne détruisent pas le tatouage, mais rendent difficile la synchronisation du détecteur, d'où la nécessité de méthodes de compensation telle que celle que nous a détaillée.

– Les attaques basées sur le traitement du signal en revanche tendent à affaiblir ou à brouiller le tatouage, en considérant ce dernier comme un bruit à enlever; les filtres simples des logiciels d'édition d'images, l'addition de bruit ainsi que les techniques plus élaborées du type restauration d'image appartiennent à cette catégorie.

Travailler sur les attaques n'est pas seulement l'apanage des pirates, mais permet aussi d'élaborer des méthodes afin d'éprouver la robustesse des algorithmes de tatouage développés. Les premières attaques connues et largement utilisées à cette fin sont essentiellement des attaques par filtrage simple, ou des attaques de désynchronisation.

7.1 Attaques par collusion

Dans une approche par collusion, plusieurs utilisateurs se rassemblent pour accumuler différents documents tatoués. Ils les combinent ensuite pour obtenir des documents qui ne contiennent plus aucun signal de tatouage. Il existe principalement deux grandes familles d'attaques par collusion ([30] et [31]). D'une part, quand différentes versions tatouées de la même image sont disponibles, il suffit souvent de les moyenner pour obtenir une estimation de l'image originale non-tatouée. D'autre part, les utilisateurs peuvent amasser différentes images contenant le même tatouage. Dans ce cas, le but est d'estimer ce signal tatouage et de l'enlever par la suite de chaque image. Ces stratégies d'attaque prennent une nouvelle dimension lorsque de la vidéo est considérée car il n'est alors plus nécessaire que plusieurs utilisateurs se regroupent. Les trames de la vidéo fournissent en effet une large collection d'images tatouées : des images similaires dans les scènes fixes et des images différentes dans les scènes à forte activité.

7.2 Attaque par surmarquage

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

8. Conclusion

Nous avons présenté dans ce chapitre le contexte technique qui entoure le domaine du tatouage des images de la vidéo. La plupart des méthodes s'appliquent dans un domaine compressé. Seules, quelques techniques insèrent directement leur signature dans la vidéo décompressée. Pour le marquage dans l'espace compressé, les marques sont insérées dans les coefficients DCT, les vecteurs de mouvements ou dans la structure GOP.

Il existe deux types de marquage : les méthodes additives, qui ajoutent une marque au modèle et les méthodes substitutives, qui remplacent des composantes du modèle par une marque.

Notre but est de développer un algorithme de tatouage vidéo robuste aux attaques les plus communes. Dans notre travail, nous avons concentré sur les méthodes d'insertion durant la compression vidéo. Dans le chapitre suivant, nous allons exposer notre algorithme de tatouage vidéo basé sur l'insertion dans le domaine transformé DCT.

1. Introduction

L'algorithme que nous allons décrire dans ce chapitre est un système de tatouage vidéo basé sur le marquage des macro blocs dans les images compressées. Comme nous avons pu le voir dans l'état de l'art, il existe plusieurs algorithmes utilisent la même approche. Dans notre travail, nous avons inséré la signature dans le domaine compressé. Cependant, ce domaine apporte des difficultés et des contraintes supplémentaires, qu'il faudrait étudier plus précisément, afin de s'assurer de la robustesse et de l'invisibilité de l'algorithme. Nous allons maintenant étudier en détail l'algorithme que nous avons développé. Comme nous l'avons vu dans le chapitre1, un algorithme de tatouage robuste et efficace doit prendre en compte trois critères essentiels : l'invisibilité de la signature, la robustesse à diverses attaques (intentionnelles et non intentionnelles) lors de la détection et la capacité du schéma pour augmenter la quantité d'information que l'on peut cacher au sein de la vidéo. Donc, pour construire un algorithme de tatouage vidéo efficace, il faut dans les meilleurs des cas combiner les trois aspects (invisibilité, capacité et la robustesse) et parfois faire des compromis dans ce contexte, nous savons opté dans notre travail pour la conception d'un schéma de tatouage qui répond à ces trois contraintes. Nos principales contributions sont :

- l'énergie des coefficients hautes fréquences de l'objet vidéo a été exploitée pour insérer la signature, car cette énergie s'approche au mieux à la sensibilité de l'appareil visuel humain. Et d'autre part, notre signature est insérée de la même manière que des principales techniques utilisées en tatouage qui utilisent l'approche basée sur l'étalement de spectre.

- deux modes d'insertion sont utilisés pour marquer les images de la vidéo, qui ont le même principe d'insertion, le premier consiste à insérer la marque dans tous les blocs de l'image, le second consiste à insérer la marque dans seulement un ensemble des macro blocs.

2. Principe du schéma de tatouage

Dans ce chapitre nous développons la manière dont est construit notre schéma de tatouage l'algorithme fait partie de la classe des schémas substitutifs dans le domaine transformé DCT. L'insertion de la signature s'appuie sur l'exploitation des caractéristiques du SVH. Le marquage se fait sur la luminance. L'information de luminance est d'abord transformée dans le domaine

DCT (sur des blocs 8*X*8), les coefficients DCT modifiés a but d'insérer le bit de tatouage sont alors sélectionnés aléatoirement, puis, selon le bit de la signature à insérer $\{\pm 1\}$, une relation prédéfinie est imposée à ces coefficients. Deux paramètres sont alors déterminés, un paramètre de lissage (*smooth*), et un paramètre caractérisant les contours (*edge*). Le premier correspond au nombre de coefficients DCT non nuls après la quantification par la matrice utilisée dans le standard de la compression (H.264). Afin de réduire les artefacts au niveau des contours, un deuxième paramètre est déterminé, il correspond à la somme (en valeur absolue) des derniers coefficients *AC nuls*, dans le parcours en zigzag. Ces deux paramètres permettent d'adapter la force de la marque au contenu du bloc. Plus le paramètre de lissage est grand, plus il y a de composantes fréquentielles et, par conséquent, il sera possible de cacher plus d'informations.

Pour la détection, La séquence vidéo est décodée, et le processus inverse à l'insertion est appliqué : la séquence de position des blocs tatoués est générée et la marque est ensuite détectée, par le calcul de la corrélation entre la signature à examiner sa présence et les blocs marqués de l'image tatouée. L'amplitude de la valeur de corrélation est utilisée pour décider si la signature est présente ou non.

3. Processus d'insertion

Dans notre travail, on utilise deux mode d'insertion de la signature, dans le Premier mode : L'insertion se fait dans le domaine compressé, sur les coefficients DCT des images. La force d'insertion est différente, selon si l'on marque tous les macro blocs 8x8 d'une image, dans ce cas la force d'insertion est importante. Dans le second: Le principe d'insertion est le même que dans le premier mode (mais un ensemble de macro bloc 8x8 de l'image est marqué).

Nous détaillons dans cette section la construction du schéma d'insertion de la méthode proposée. La séquence vidéo est décomposée en plusieurs images, chaque image est divisée en 99 blocs de la taille 16x16 pixels, l'image appelée **QCIF** de format (176x144) est utilisée comme illustrée dans la figure (2.1). Chaque macro bloc est transformé par une transformation DCT, et il est quantifié par l'utilisation d'une matrice de quantification spécifique comme celle du standard H264. Puis, La signature est modulée dans le domaine transformé, pour ensuite être insérée aux coefficients non nuls sélectionnées par la convention proposée. Et après cette dernière étape les MB_s de l'image sont tatoués, et en utilisant une quantification et transformation inverses pour

rendre le MB sous forme originale, puis, on fait le codage entoptique pour avoir l'image tatouée, qui est illustrée par la figure (2.2).

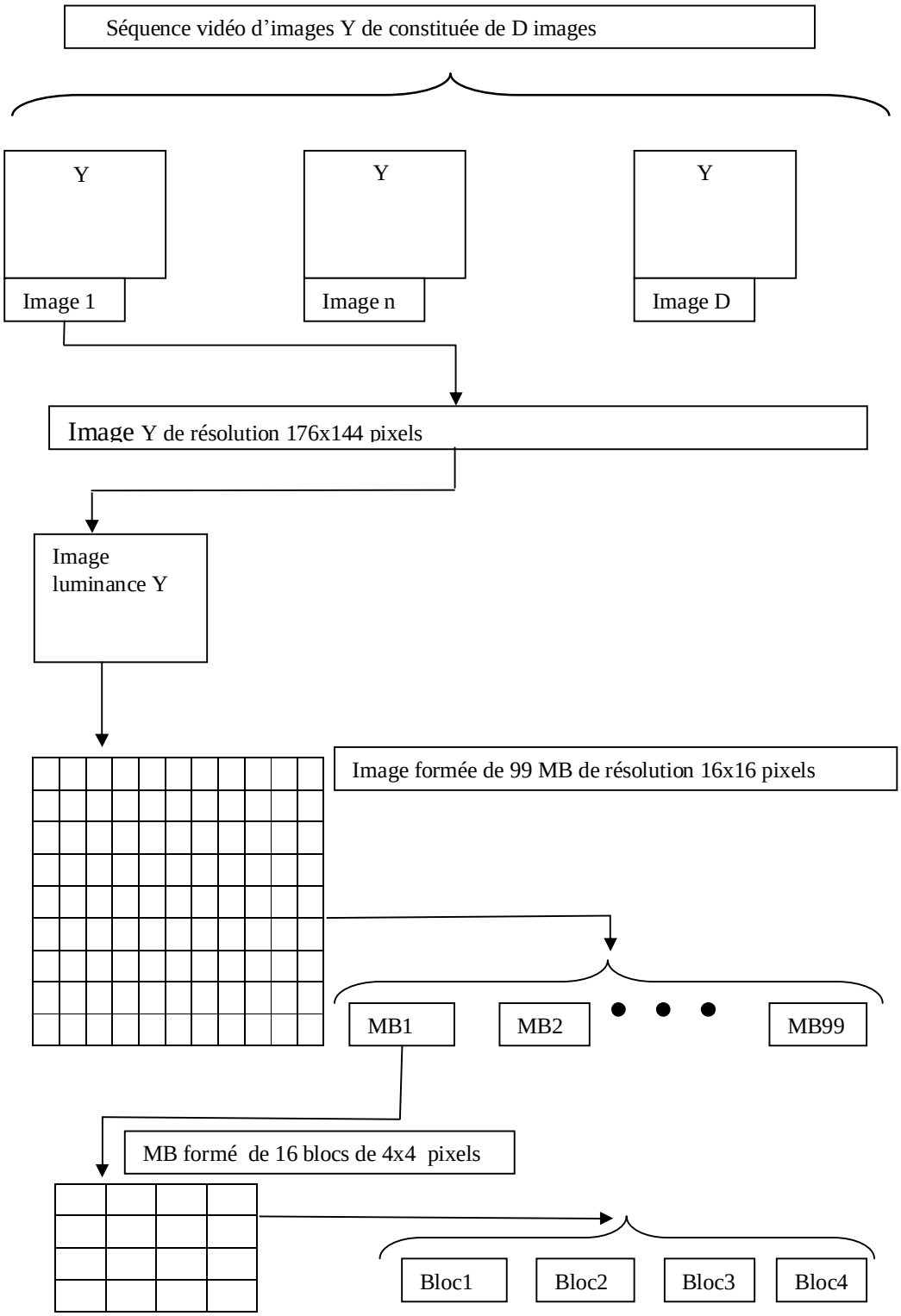


Figure 2.1 Processus de traitement d'une image de la séquence vidéo

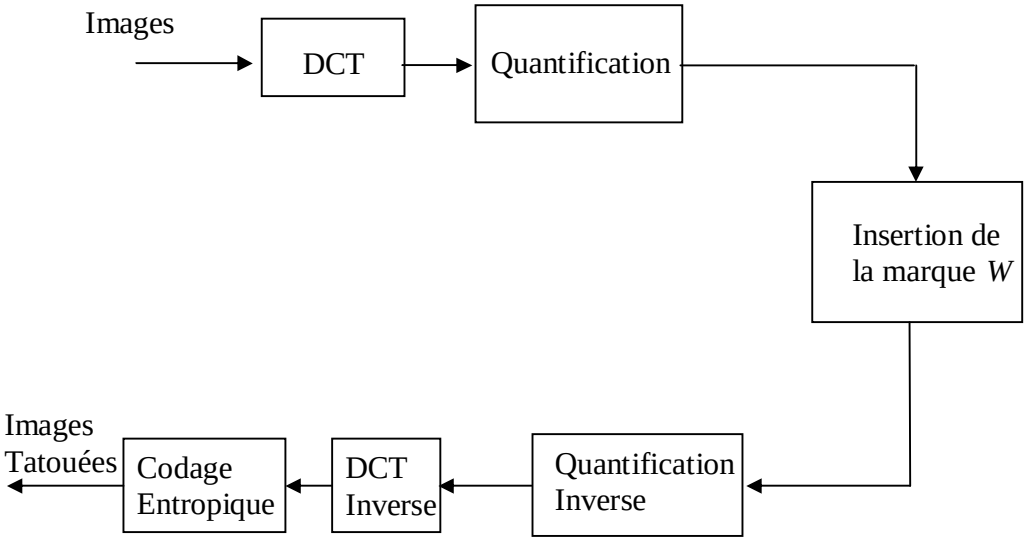


Figure2.2 Schéma récapitulatif du tatouage des images

3.1 Génération de la signature

Pour chaque image de la vidéo, une marque est générée. La marque est distribuée sur un signal 2*D* de même taille que les images de la séquence constituées de bloc 8*X*8, le bloc 8x8 correspond au signal de la marque est transformé dans le domaine DCT.

La séquence à insérer dans le domaine transformée (DCT) [32], elle est peut être choisi de plusieurs manières. Souvent, les séquences du tatouage utilisent un générateur de nombres pseudo-aléatoires, mais la signature peut être également obtenue par une application récursive des séquences chaotiques appropriées.

Dans le tatouage vidéo, plus souvent, les séquences du tatouage utilisent un générateur de nombres pseudo-aléatoires le système générateur pseudo-aléatoire a été employé pour le tatouage numérique, pour garantir la sécurité de la marque insérée. En effet, bien souvent, ce dernier est inclut directement dans le compilateur utilisé, et par conséquent, utiliser ce générateur revient à un simple appel de fonction, elle produit un générateur pseudo-aléatoire (PN) de suites binaires $\{\pm 1\}$, on utilise une séquence binaire pseudo-aléatoire à 396 bits aléatoires de longueurs de la même taille que l'image constituée par des macro blocs 8x8.

Notre signature binaire à insérer $W \in \{+1,-1\}^N$, où N correspond à la taille de la signature), et est obtenue à partir d'une valeur initiale (clef secrète), cette valeur secrète est utilisée pour initialiser le générateur pseudo-aléatoire.

$$w(k) = \begin{Bmatrix} 1 \\ ou \\ -1 \end{Bmatrix}, \text{ avec } k = 0...395 \qquad (2.1)$$

Où k est la taille de la séquence pseudo aléatoire PN, et W est le tatouage que nous voulons insérer.

3.2 Insertion de la signature

L'insertion se fait directement sur le flux compressé en sélectionnant des coefficients DCT hautes fréquences non nuls (AC_i transformés et quantifiés) d'un MB de la taille 8x8, puisque la quantification est une simple opération, il est souhaitable d'insérer le tatouage après quantification pour éviter l'effacement possible du tatouage. En outre, le codage et décodage entropique sont deux procédures rapides, et l'insertion et la détection de la signature peuvent être fiat en temps réel. La signature est diffusée sur de nombreuses fréquences de façon à ce que les coefficients modifiés soient faibles. La vidéo originale n'est pas nécessaire pour la détection. Cette méthode présente une capacité d'insertion satisfaisante ainsi qu'une facilité de mise en oeuvre appréciable. Nous insérons les bits du tatouage sur chaque macro bloc (MB) de la taille 8x8, en modifiant certains des derniers coefficient DCT hautes fréquences non nuls de chaque bloc 4x4. On Considère un macro bloc (16x16), Ce MB est divisé en quatre blocs 8x8, comme illustré dans la figure (2.3).

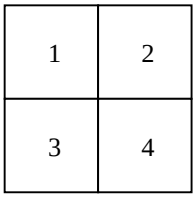


Figure 2.3 Représentation d'un macro bloc (16x16) dans un codeur vidéo

Le macro bloc peut être divisé en 16 blocs de 4x4.

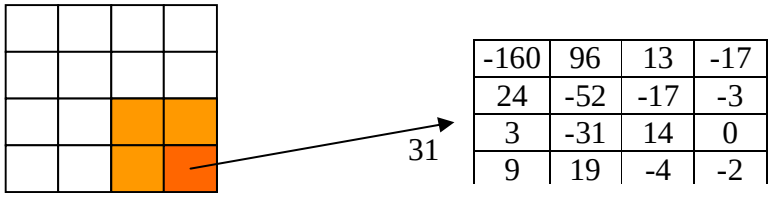


Figure 2.4 Un exemple d'un macro bloc codé par DCT dans H.264

Où chaque bloc 4x4 noté par $p(i, j)(0 \le i, j \le 3)$. Puis, chaque bloc $p(i, j)$ est transformé par :

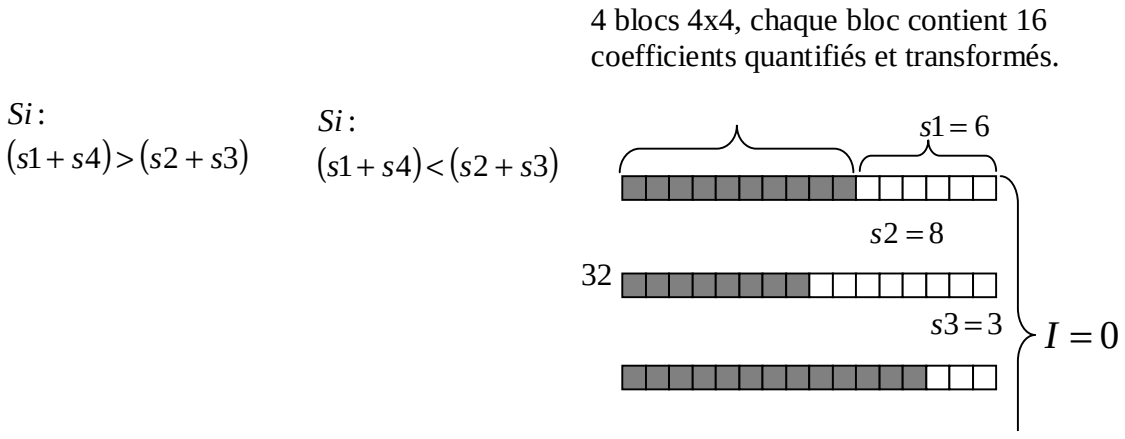
$$p(u,v) = \text{int}\, DCT\{p(i, j)\}, \qquad 0 \le u, v \le 3 \tag{2.2}$$

Où $\text{int}\, DCT\{p(i, j)\}$ représentent les coefficients DCT entiers. Les coefficients DCT entiers $p(u,v)$ de deux dimensions du bloc 4x4 peuvent être transformés par une matrice spécifique de balayage-zigzag en un signal d'une seule dimension, on peut avoir une séquence linéaire de 16 coefficients $P(k)$, où $k \in [0,15]$ indique la position du zigzag.

Après la quantification, les coefficients d'ordre supérieur (les derniers dans le balayage en zigzag) sont plus probablement nuls selon la restriction du bloc (texture) et sur la taille de pas de quantification. En considérant un bloc non tatoué comme montré dans la figure (2.4) du point de vue de ses coefficients moyennes fréquences.

3.3 La règle d'insertion

Un index I qui sert de l'indexation du MB de la taille 8x8 est utilisé, en associant à chaque MB l'une des trois valeurs de I {1, -1.0}, on trouve une image modélisée. On utilise une convention pour insérer le tatouage, cette convention est montrée dans la figure (2.5) ci-dessous. Les coefficients transformés et quantifiés $p(u,v)$ des blocs 1 à 4 dans un MB sont utilisés pour déterminer l'index I , si la somme des derniers coefficients nuls (hautes fréquences) des blocs 1 et 4 est supérieur à celle des blocs 2 et 3 l'index du MB est 1, dans le cas contraire l'index du MB est -1, également si toutes les sommes ou deux à deux sont égaux l'index est 0. L'insertion de la signature s'effectue en modulant le bit de tatouage à insérer dans un MB de la taille 8x8. L'exemple suivant, qui est illustré par la figure (2.5) montré la convention proposée. Dans cet exemple, l'index I est nul.



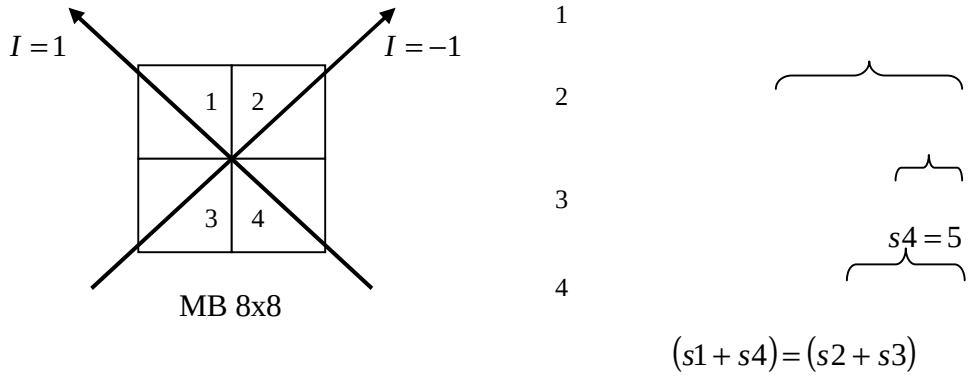
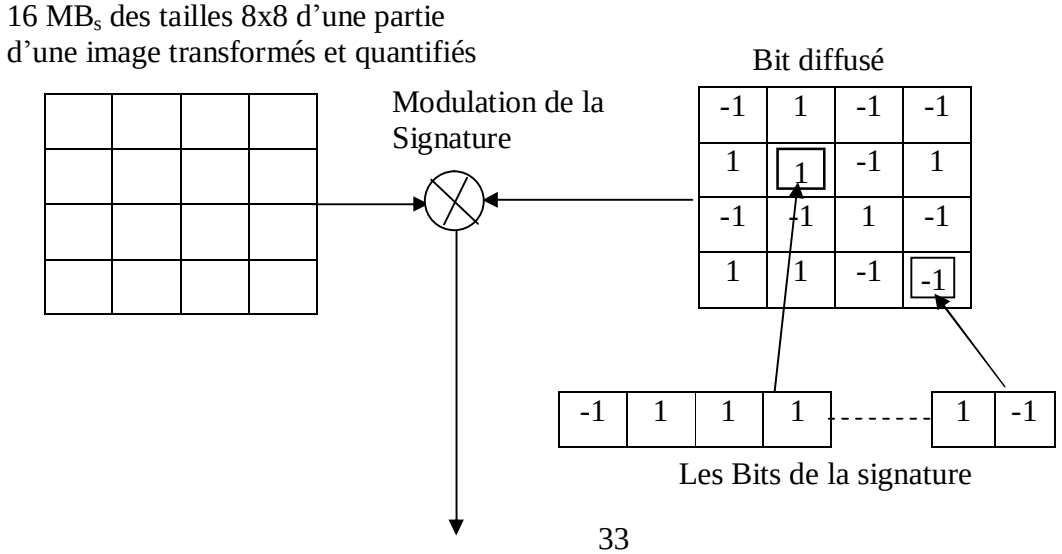


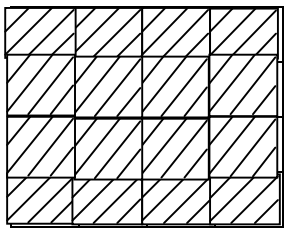
Fig. 2.5 La convention utilisée en tatouage

Où les coefficients dans les cases blanches situent à droite représentent les derniers coefficients DCT hautes fréquences nuls ($p(u_0, v_0) = 0$ où u_0, v_0, indiquent les positions des coefficients DCT hautes fréquences dans le parcours en zigzag). On exploit les coefficients hautes fréquences pour inclure les bits de la signature W, les bits sont inclus en mettant certains coefficients AC_i hautes fréquences non nuls à zéro de blocs 1 et 4 ou de blocs 2 et 3, ses coefficients modifiés doivent être non importants. En rassemblant aux index de macro blocs un signal aléatoire, le signal produit est de type :

1 1 -1 0 -1 -1 1 0 1 0 -1 -1 -1 0 1 -1 0 1 0....

Le nombre des chiffres de ce signal est égale le nombre des macro blocs de la taille 8x8 dans l'image. Ce signal peut être facilement modulé par un signal pseudo-aléatoire (PN), le bit de tatouage diffusé est {1, -1}, c-à-d une séquence pseudo-aléatoire est ensuite modulée aux coefficients DCT de chaque macro bloc, l'exemple représenté par la figure 2.6 illustre la modulation d'une signature constituée par 16 bits dans 16 MB_s de tailles 8x8.





MB 8x8 non tatoué

MB 8x8 tatoué

16 MB_s de la taille 8x8 transformés
et quantifiés, après tatouage

Figure 2.6 Illustration de tatouage inséré dans 16 MB_s d'une partie d'une image

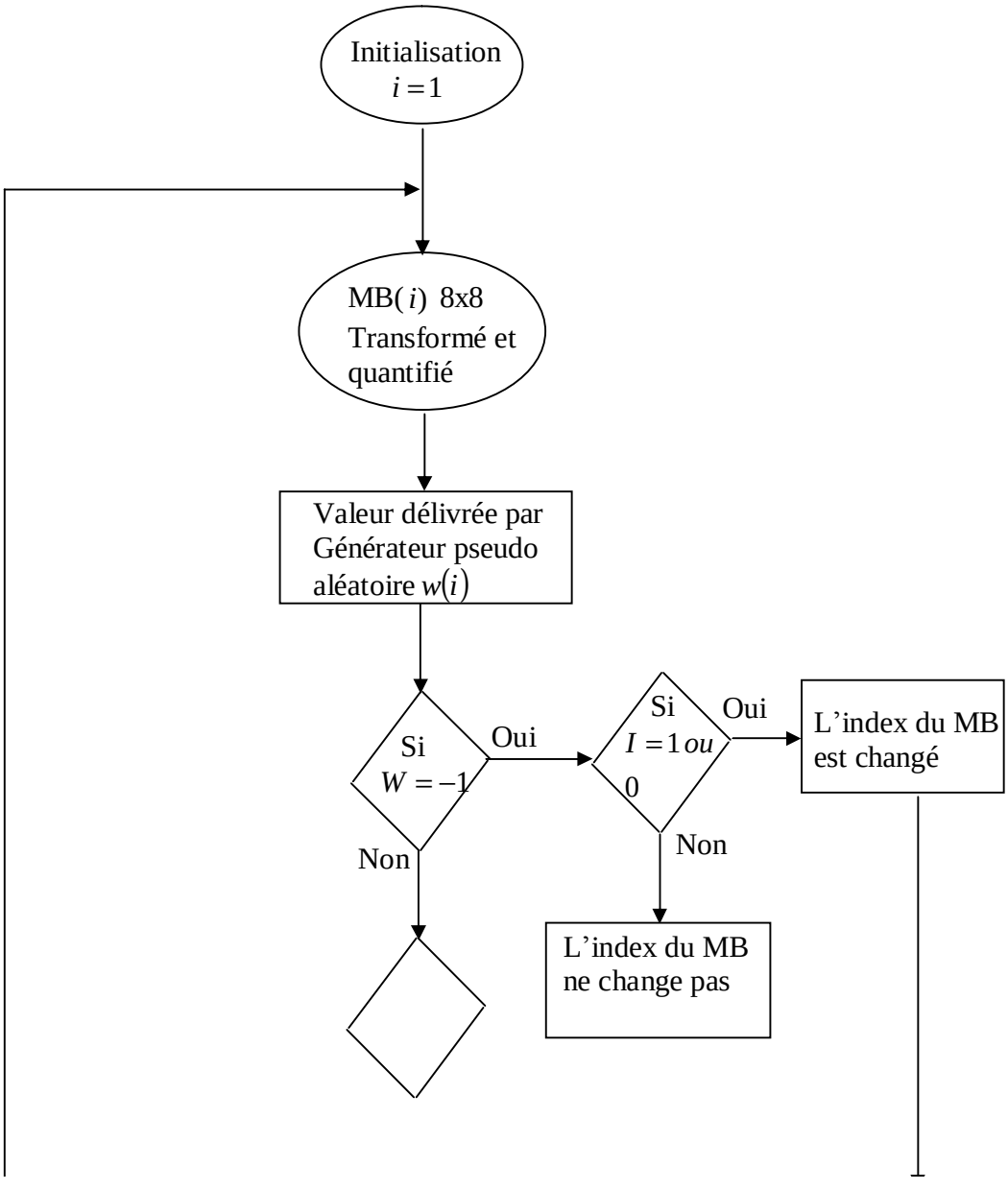
On peut simplifier la phase d'insertion sous forme des équations suivantes :
La variable I qui sert de l'indexation du MB de la taille 8x8 est formée comme suit:

$$I = \begin{cases} 1 & si \quad pour \quad (S_1 + S_4) > (S_2 + S_3) \\ -1 & si \quad pour \quad (S_1 + S4) < (S_2 + S_3) \\ 0 & ailleurs \end{cases} \tag{2.3}$$

Selon l'index I du MB et la valeur générée par le générateur pseudo aléatoire PN, la marque (W) est insérée par la formule suivante :

$$\begin{cases} si\ W = -1\ et \begin{cases} (I = 1\ ou\ 0)\ l'index\ I\ devient\ -1 \\ ou\ \ I = -1\ \ l'index\ I\ ne\ change\ pas \end{cases} \\ si\ W = \ 1\ \ et \begin{cases} (I = 1\ ou\ 0)\ \ l'index\ I\ ne\ change\ pas \\ ou\ \ I = -1\ \ l'index\ I\ devient\ 1 \end{cases} \end{cases} \tag{2.4}$$

Pour changer l'index I, les coefficients moyenne fréquences d'un MB de la taille 8x8 sont modifiés de sorte que l'inégalité ($(s1 + s4) > (s2 + s3)$ ou $(s1 + s4) < (s2 + s3)$) est changée


Initialisation
$i=1$
MB(i) 8x8
Transformé et
quantifié
Valeur délivrée par
Générateur pseudo
aléatoire $w(i)$
Si
$W=-1$
Oui
Non
Si
$I=1 ou$
0
Oui
Non
L'index du MB
est changé
L'index du MB
ne change pas

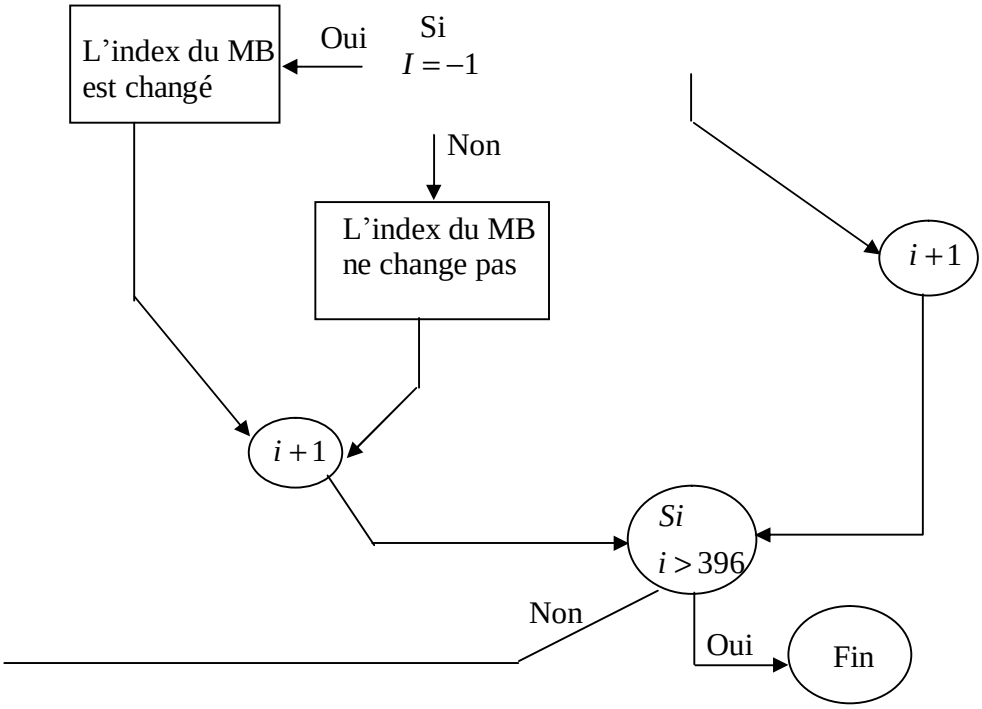


Figure 2.7 Organigramme d'insertion de la signature

4. Détection de la signature

La détection de la signature est formée après le décodage entropique comme illustrée dans la figure (2.8). Le processus de détection est semblable au processus d'insertion. La procédure de détection du tatouage est décrite comme suit:

La luminance d'une image tatouée est divisée en macro blocs de la taille 8x8, puis, et elle est transformée par DCT comme la phase d'insertion, chaque MB 8x8 est aussi divisé en 4 blocs 4x4, et on calcule les sommes $\{S_1, S_2, S_3, S_4\}$ de la même manière que le cas d'insertion pour déterminer l'index I du MB, les index de macro blocs obtenus est un signal aléatoire contient des valeurs (1,-1,0). Puis, la corrélation r entre les index de macro blocs tatoués et la séquence binaire pseudo aléatoire PN utilisée dans l'insertion dont on examine sa présence, est calculée comme suit :

$$r = \frac{1}{L}\sum_{i=0}^{L} W_i^p * W_i^* \qquad avec \quad L = 0,...395 \tag{2.5}$$

Où L est la taille de la signature, et W_i^p la i-ème valeur du tatouage insérée et W_i^* est i-ème valeur du tatouage détectée. Dans notre algorithme, et Pour une meilleure détection la valeur de la corrélation r est très proche à la valeur 396.

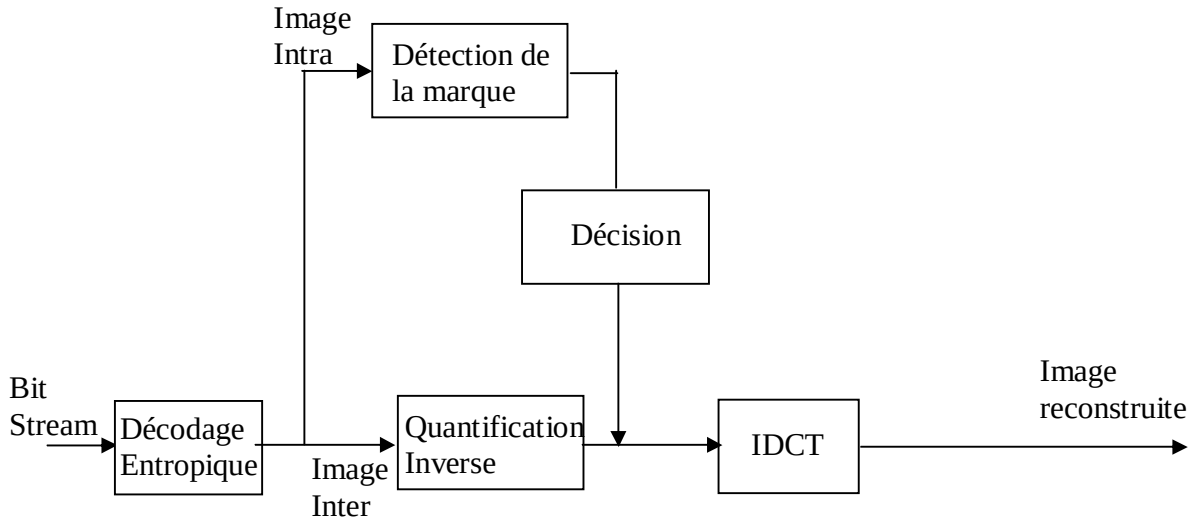
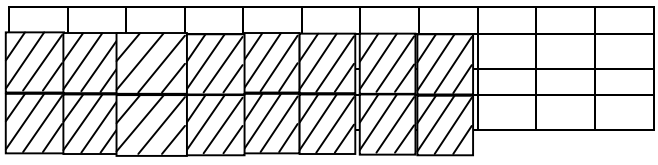
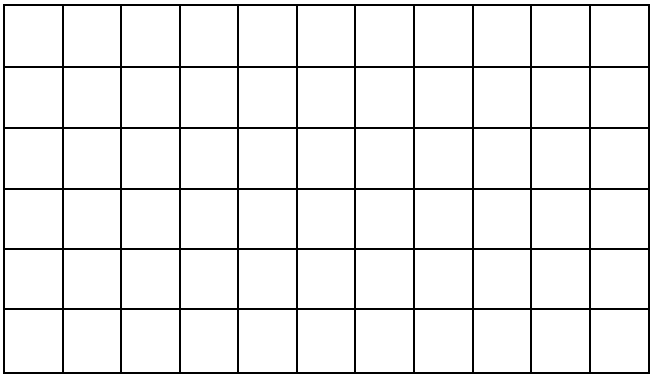


Figure 2.8 Détection du tatouage vidéo

5. Insertion de la signature dans un ensemble des MB_s dans l'image

Notre second mode d'insertion consistant à marquer seulement un ensemble des dans les images comme montrée dans la figure 2.9, la sélection des ensembles MB_s. Elle se faire de manière pseudo-aléatoirement. Afin de choisir judicieusement notre procédure de sélection, nous avons étudié la dégradation de la qualité de l'image tatouée. Dans ce mode, il est clair que la qualité de l'image tatouée est mieux que dans le cas précèdent puisque seulement un ensemble des blocs sont modifiés. Alors on peut dire que le tatouage résulte est devient robuste à diverses attaques. On doit noter que les bits de tatouage dans ce mode sont très petits.



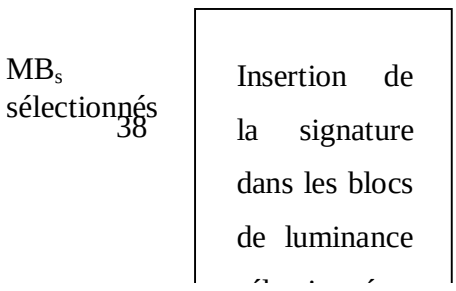


MB 16x16 tatoué (marqué)

MB 16x16 non tatoué (marqué)

Figure 2.9 Image QCIF du format (176x144) pixels tatouée

La méthode est basée sur la séparation de certaine partie de l'image utilisée en tatouage. Pour le tatouage à insérer, un ensemble de n macro blocs $8x8$ est choisi pseudo-aléatoirement à partir des images de la vidéo, et chaque bloc 8x8 est divisé en quatre sous ensembles de même taille 4x4. Le nombre n des macro blocs de la taille 8x8 choisi est de 64. Pour chaque sous ensemble, l'énergie des coefficients DCT hautes fréquences non nulles est calculée. Afin d'insérer un bit, l'énergie des coefficients hautes fréquences d'un des sous ensembles est réduite en mettant certains coefficients hautes fréquences non nuls à zéro, ces coefficients doivent être non importants dans l'images pour réduire l'impact visuel apparaît sur l'image tatouée. Et Pour faciliter la compréhension de l'approche, des blocs consécutifs sont utilisés plutôt que des blocs aléatoirement choisis.



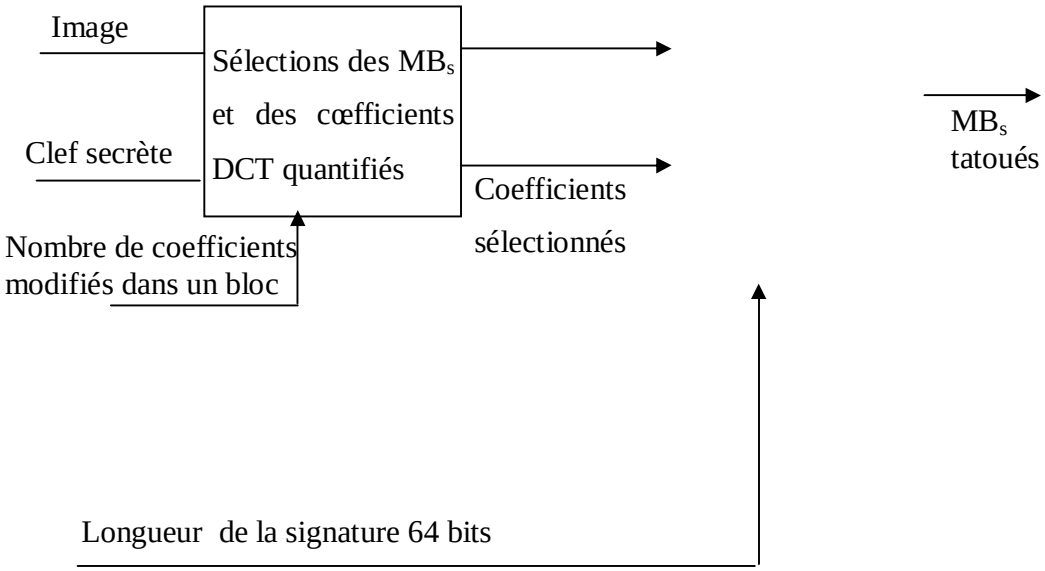


Figure 2.10 Insertion de la signature dans un ensemble de MB_s

5.1 L'extraction de la signature

La détection se fait par des mesures de corrélation. Les bits du tatouage peuvent alors être extraient, en sélectionnant le même ensemble de blocs, en le divisant en sous ensembles, et en comparant l'énergie des coefficients hautes fréquences non nulles de chaque sous ensemble.
Le processus de détection est semblable au processus d'insertion. La procédure de détection du tatouage est de la même manière comme montrée dans la section 4.

Les index de macro blocs obtenus est un signal aléatoire contient des valeurs (1,-1,0).Puis, la corrélation r entre les index de blocs tatoués et la séquence binaire pseudo aléatoire PN utilisée dans l'insertion dont on examine sa présence, est calculée comme suit :

$$r = \frac{1}{L}\sum_{i=0}^{L} I_i . PN_i \qquad avec \quad L = 0,...63 \tag{2.6}$$

Où L est la taille de la signature. Dans ce mode, et Pour une meilleure détection la valeur de la corrélation r est très proche à la valeur 64.

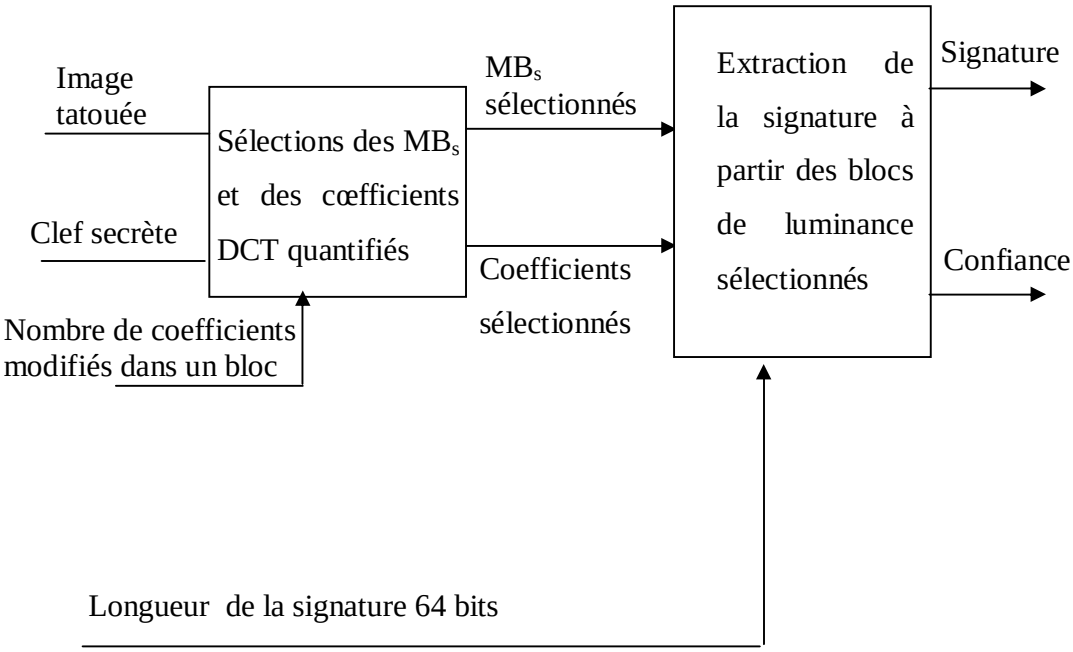


Figure 2.11 Extraction de la signature

6. Conclusion

Ce chapitre a été consacré au développement d'une méthode de tatouage des images vidéo numérique. Nous avons présenté une méthode complète. La modulation d'une signature pseudo aléatoire, la signature est initialisée par une valeur initiale secrète pour garantir la sécurité contre les pirates, et avec les coefficients issue d'une transformation DCT de blocs dans l'image a été adaptée et maximisée selon des caractéristiques de la vidéo et des considérations psychovisuelles afin d'optimiser le compromis invisibilité/robustesse. Nous avons utilisé deux modes d'insertion semblables, le premier consiste à insérer la signature dans tous les blocs de l'image, cependant, dans ce mode il y a un impact visuel sur les images tatouées. C'est pour cette raison que nous avons introduit le second mode qui consiste à insérer la signature dans un ensemble des blocs sélectionnés pseudo-aléatoirement pour améliorer la qualité des images de la vidéo tatouée, et pour augmenter la robustesse de notre algorithme de tatouage.

1. INTRODUCTION

Dans ce chapitre nous allons exposer les résultats auxquels nous sommes parvenus en appliquant la méthode de tatouage vidéo définie dans le chapitre précédant.

L'efficacité d'un algorithme de tatouage, quelque soit son domaine d'application, ne peut être jugé qu'après une étude statistique des résultats de tatouage obtenus. Le choix des séquences des images doit être fait parmi les images de test standard reconnues en traitement de l'image. Pour évaluer les résultats obtenus. En effet, plusieurs formats reconnus sont utilisés, pour la vérification de la mise en œuvre d'algorithme du tatouage, tels que, CIF, QCIF, ... Mais ceci semble moins important, nous choissions seulement le modèle du sous échantillonnage de la composante luminance Y (4 :2 :0).

Afin de minimiser l'impact visuel engendré par le marquage des macro blocs (MB_s) dans les images compressées de notre précèdent schéma. Et Pour améliorer la qualité des images compressées résultantes après le tatouage, nous allons utiliser deux mode d'insertion, le premier consiste à insérer la signature (tatouage) dans tous les macro blocs des images compressées, et le second consiste à marquer quelques MB_s dans les images compressées. Pour augmenter la robustesse contre diverses attaques, Nous allons évaluer les performances de la méthode de tatouage en terme d'invisibilité et on provoque les images compressées tatouées aux quelques attaques importantes pour juger la présence de la signature. Dans la dernière section, nous donnons quelques perspectives pour des travaux futurs.

2. PLATEFORME DE TEST

Dans le but d'évaluer les performances de notre méthode de tatouage des images de la vidéo, nous utilisons les séquences de test standard. On procède au tatouage d'une séquence vidéo des images dans luminance Y par le modèle de tatouage substitutif, Nous utilisons le format QCIF de résolution 176x144 la plus utilisée pour les faibles cadences. Nous considérons la variation du paramètre de quantification Qp (utilisé dans le standard H264) de 1 à 50.

Pour améliorer la robustesse de notre schéma de tatouage on utilise deux séquences de test, la première est la séquence 'carphone', la seconde est 'foreman'.

L'algorithme de tatouage et les attaques ont été effectués sous l'environnement C++, nous initialisons le générateur pseudo aléatoire plusieurs fois par une valeur secrète (clef secrète) pour juger la probabilité de fausses alarmes.

3. Tatouage de la séquence vidéo

Dans notre procédure, nous utilisons deux modes d'insertion de la signature, le premier consiste à insérer la marque dans tous les macroblocs (MB_s), le second consiste à insérer la marque dans quelques MB_s sélectionnés (dans notre expérience, 64 MB_s de la taille 8x8 sont employés pour insérer les bits de la signature).

3.1 Mode d'Insertion dans tous les MB_s de l'image

Dans notre travail, les séquences vidéo utilisées sont composent de plus 100 images dans la luminance Y, modèle 4 :2 :0 la résolution pour la luminance et format QCIF (176x144). Nous insérons la signature dans les images de ces séquences. La qualité d'image tatouée est obtenue pour différentes valeurs du paramètre de quantification Qp. La figure 3.1 montre la composantes Y de l'image 'CarPhone' obtenue avant le tatouage et après le tatouage en fonction Qp. Le tableau 3.1 montre les résultats que l'on obtient, sachant que la valeur de Qp varie de 1 à 50 par incrément de cinq. On peut remarquer que la valeur du *PSNR* diminue lorsque la valeur de Qp augmente, cela signifie qu'il faut choisir une valeur moyenne de Qp pour avoir une haute fidélité visuelle. Cependant, les résultats expérimentaux montrent que lorsque Qp est égale ou inférieure à 25 on peut détecter la signature parfaitement.

Qp	1	5	10	15	20	25	30	35	40	45	50
PSNR (dB) (Image compressée non tatouée)	50.86	50.78	48.97	46.05	42.76	39.27	35.46	31.79	28.09	24.08	21.4
PSNR (dB) (Image compressée tatouée)	50.81	50.52	47.56	44.03	40.06	36.8	32.92	29.6	26.6	24.09	21.22

Tableaux 3.1 Table des valeurs : Qp, Distorsion de l'image compressée non tatouée Et tatouée.

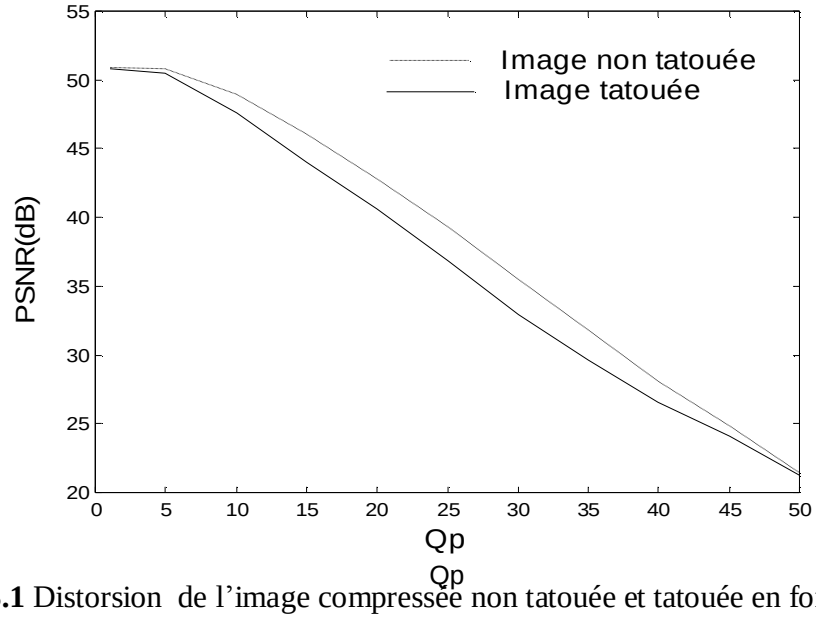


Figure 3.1 Distorsion de l'image compressée non tatouée et tatouée en fonction de Qp

Les relevés des valeurs sont donnés dans le tableau 3.1. La courbe typique de la distorsion de l'image compressée et de celle tatouée est donnée dans la figure 3.1, elle traduit l'impact de la variation du paramètre de quantification Qp sur la mesure de qualité PSNR, on constate que l'amélioration de la qualité de l'image tatouée, se traduite par une augmentation du PSNR, plus que la qualité de l'image tatouée est plus proche à celle de l'image compressée non tatouée, plus le tatouage est robuste.

Pour assurer la qualité de l'image tatouée à la reconstruction, on peut conclure que la distorsion est d'autant plus grande si les bits de tatouage inclus sont plus forts. Il faut garder un compromis entre les bits à insérer et la distorsion pour assurer au moins les qualités

Subjectives de l'image compressée reconstruite après l'opération du tatouage. Il faut mettre au point que, l'augmentation du paramètre de quantification provoque une diminution de la capacité du tatouage, ce qui augmente la distorsion, et la diminution du paramètre de quantification provoque une augmentation de la capacité du tatouage, en effet, on doit noter l'importance du paramètre de quantification Qp. Dans le compromis robustesse/invisibilité.

La première image de la composante Y reconstruite avant et après le tatouge de la séquence 'CarPhone', en fonction des trois valeurs du paramètre de quantification *Qp* {20, 30,40} est

donnée dans la figure 3.2. Pour cette image, nous voulons montrer l'effet du paramètre de quantification sur la qualité d'image compressée reconstruite (non tatouée et tatouée). A partir d'un Qp=30, on constate que la distorsion commence à être visible sur l'image reconstruite.

(a)

(b)

Image Y 'caphone' compressée (a), et sa version tatouée (b), Qp=20

(c)

(d)

Image Y 'caphone' compressée (c), et sa version tatouée (d), Qp=30

(e)

(f)

Image Y 'caphone' compressée (e), et sa version tatouée (f), Qp=40

Figure 3.2 Images Y ‘carphone’ compressées (a) et (c) et (e), et leurs versions tatouées Respectivement (b) et (d) et (f)

Dans cette partie, nous nous intéressons à l’amélioration de la robustesse de notre schéma d’insertion. Pour ce faire, on inclut la marque sur plusieurs images de 1 à 10 de la séquence ‘carphone’, cette procédure d’insertion de la même manière que la procédure précédente, les courbes représentées dans les figures (3.3 et 3.4) montrent respectivement la distorsion de dix images compressées non tatouées et tatouées pour un paramètre de quantification Qp est égale à 20. D’après les mesures de la distorsion qui sont présentées par le tableau 3.2, on peut constater que la différence entre les valeurs du PSNR des images compressées tatouées et des images compressées non tatouées est de plus de 2dB, cela implique qu’il y’a une dégradation sur les images tatouées, c’est pour cette raison, nous avons introduit un deuxième mode d’insertion comme nous allons la voir dans la section (3.2).

PSNR(dB) images compressées non tatouées	42.76	42.96	43.05	43.08	43.02	43.05	43.05	42.97	43.12	43.00
PSNR(dB) images compressées tatouées	40.6	40.5	40.87	40.7	40.86	40.74	40.6	40.68	40.75	40.6

Tableaux 3.2 Distorsion de dix images compressée non tatouées et tatouées, Qp=20. Pour La séquence ‘carphone’

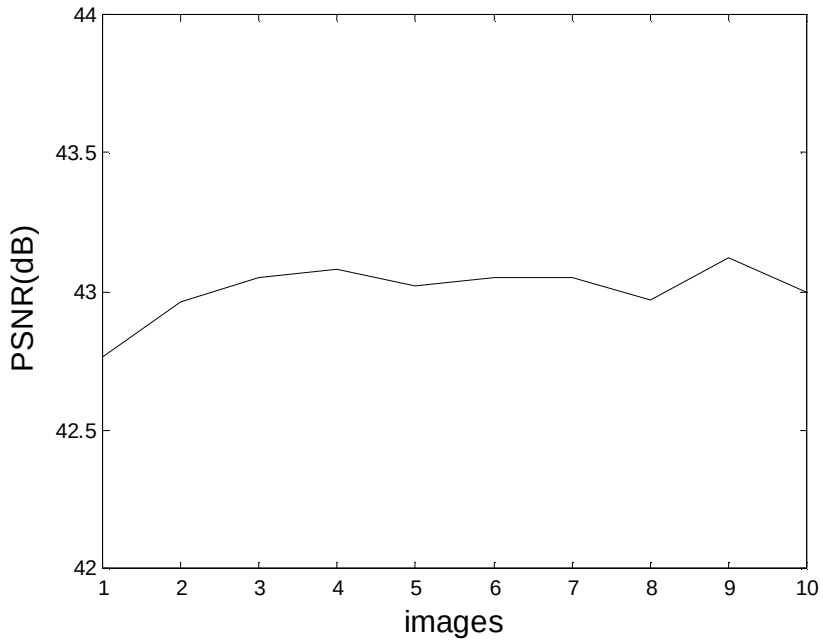


Figure 3.3 Distorsion des images compressées non tatouées, Qp=20. Pour 'Carphone'

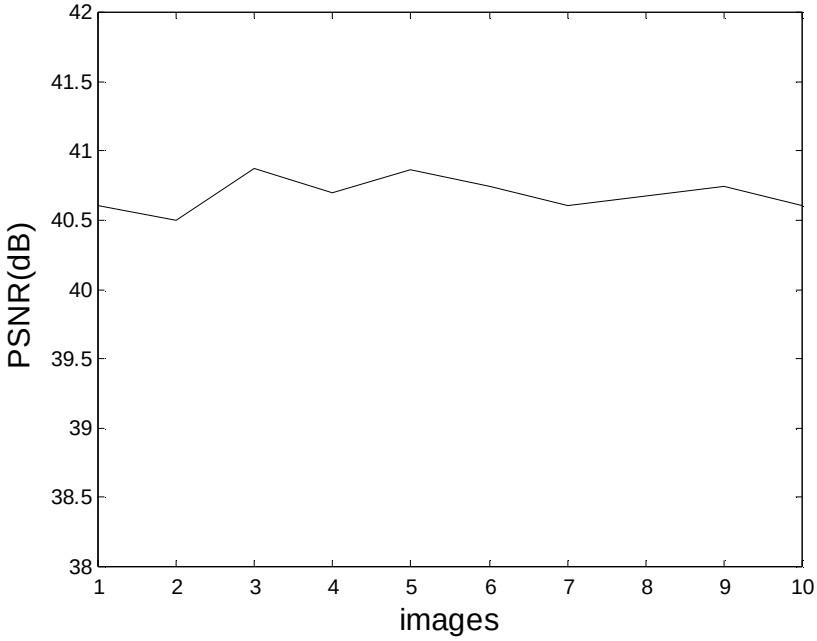


Figure 3.4 Distorsion des images compressées tatouées, Qp=20. Pour 'carphone'

La première image de la composante Y reconstruite aussi avant et après le tatouge de la séquence ‘foreman’, en fonction des trois valeurs de quantification *Qp* {20, 30,40} est donnée dans la figure 3.5. Pour cette image, nous voulons montrer l’effet du paramètre de quantification sur la qualité d’image compressée reconstruites (non tatouée et tatouée). A partir d’un Qp=30, on constate que la distorsion commence à être visible sur l’image reconstruite.

(a)

(b)

Image Y ‘foreman’ compressée (a), et sa version tatouée (b), Qp=20

(c)

(d)

Image Y ‘foreman’ compressée (c), et sa version tatouée (d), Qp=30

(e)

(f)

Image Y ‘foreman’ compressée (e), et sa version tatouée (f), Qp=40

Figure 3.5 Images Y 'foreman' compressées (a) et (c) et (e), et leurs versions tatouées Respectivement (b) et (d) et (f)

D'après les mesures de la distorsion qui sont présentées par le tableau 3.3, on peut constater que la différence entre les valeurs du PSNR des images compressées tatouées de la séquence du 'foreman' et des images compressées non tatouées est de plus de 2,5dB, cela implique qu'il y'a une dégradation sur les images tatouées.

PSNR(dB) images compressées non tatouées	42.04	42.08	41.99	42.05	42.01	41.96	41.98	42.04	41.95	41.95
PSNR(dB) images compressées tatouées	39.39	39.49	39.40	39.58	39.50	39.13	39.34	39.32	39.21	39.38

Tableaux 3.3 Distorsion de dix images compressée non tatouées et tatouées, Qp=20. Pour la séquence 'foreman'

3.2. Mode d'insertion dans un ensemble des MB_s de chaque image

Notre procédure d'insertion consistant à marquer seulement un ensemble de MB_s de la taille 8x8 dans les images pour réduire la dégradation subir sur les images tatouées dans le mode précédent, la sélection des ensembles MB_s. Elle se faire de manière pseudo-aléatoirement. Afin de choisir judicieusement notre procédure de sélection, nous avons étudié la dégradation de la qualité de l'image tatouée, d'après les résultats obtenus, ce mode donne les meilleurs résultats, et d'autre part, les pirates ne connaissent pas les positions des blocs marqués.

PSNR(dB) images compressées	42.76	42.96	43.05	43.08	43.02	43.05	43.05	42.97	43.12	43.00
PSNR(dB) images compressés tatouées	42.58	42.76	42.90	42.92	42.89	42.92	42.90	42.87	42.97	42.83

Tableaux 3.4 Distorsion de dix images compressée non tatouée et tatouées, Qp=20.

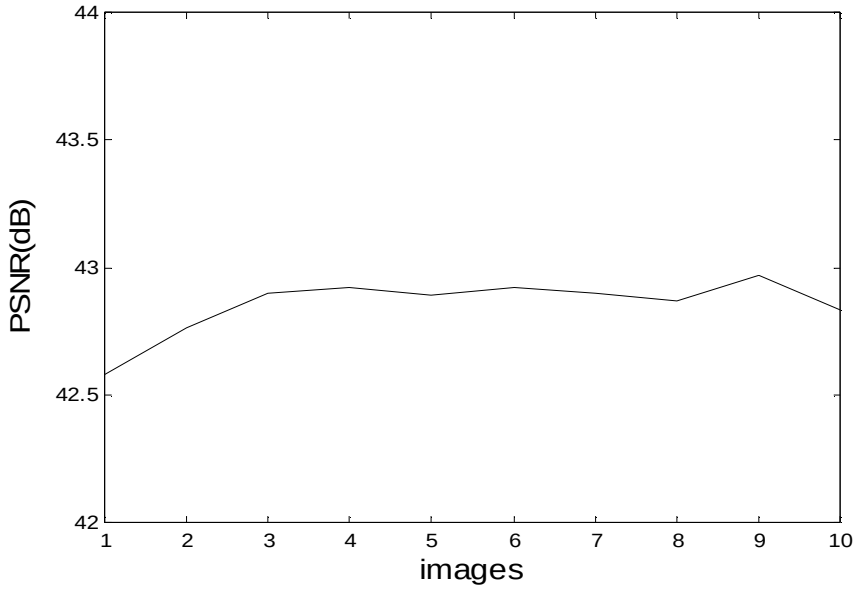


Figure 3.6 Distorsion des images compressées tatouées, Qp=20

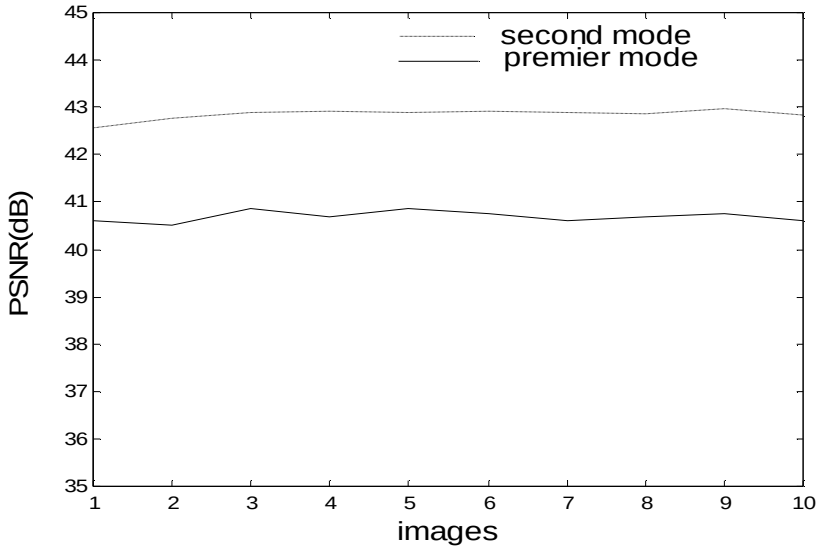


Figure 3.7 Comparaison entre deux modes d'insertion, Qp=20

Les relevés des valeurs sont donnés dans le tableau 3.4. La courbe de la distorsion des images compressées tatouées est donnée dans la figure 3.6, cette courbe montre la distorsion de dix

images compressées tatouées avec un paramètre Qp est égale 20, D'après les mesures de la distorsion qui sont présentées par le tableau 3.4, on peut constater que la différence maximale entre les valeurs du PSNR des images compressées tatouées et des images compressées non tatouées est de 0.17 dB, cela implique que la distorsion des images tatouées est très proche à celle des images compressées non tatouées, alors que, on peut conclure que ce mode d'insertion résiste à la distorsion, donc la robustesse à la distorsion est très élevée. La courbe de la distorsion des images compressées tatouées est montrée dans La figure 3.7, cette courbe montre la comparaison entre deux modes d'insertion dans les mêmes images tatouées, Les relevés des valeurs sont donnés dans le tableau 3.5. D'après la comparaison, on constate que la qualité des images compressées tatouées dans le second mode est mieux que celle du premier mode.

PSNR(dB) premier mode d'insertion	40.6	40.5	40.87	40.7	40.86	40.74	40.6	40.68	40.75	40.6
PSNR(dB) deuxième d'insertion	42.58	42.76	42.90	42.92	42.89	42.92	42.90	42.87	42.97	42.83

Tableaux 3.5 Distorsion de dix images compressées tatouées, Qp=20. Pour deux modes d'insertion dans la séquence 'carphone'

4. FIABILITE DE DETECTION ET UNICITE DE LA SIGNATURE

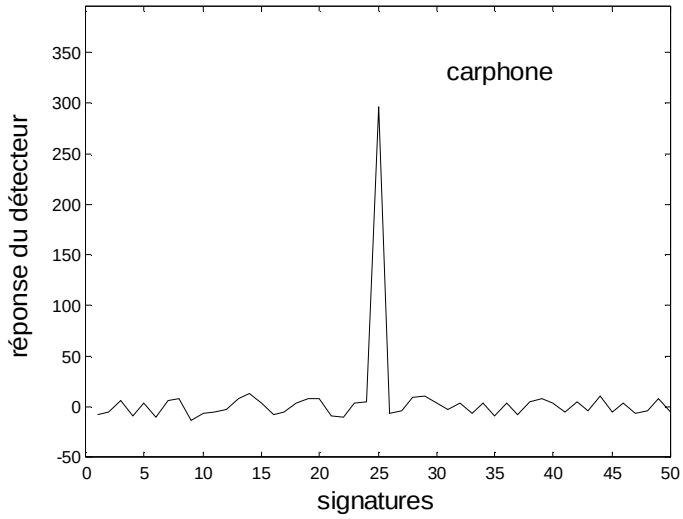
La phase de détection de la marque correspond à un processus dual à celui de l'insertion. La Détection est réalisée par une mesure de corrélation entre l'image déjà tatouée et la marque insérée (schéma de tatouage aveugle).

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

On peut représenter les performances du détecteur par un graphique. Les courbes (b) et (d) représentées dans la figure 3.8 montrent respectivement la corrélation entre l'image tatouée et la marque insérer r à 50 signatures générées pseudo aléatoirement (générées à partir d'une valeur initiale ou clef secrète) pour (a) 'carphone' et (b) 'foreman'. Notre signature implantée dans

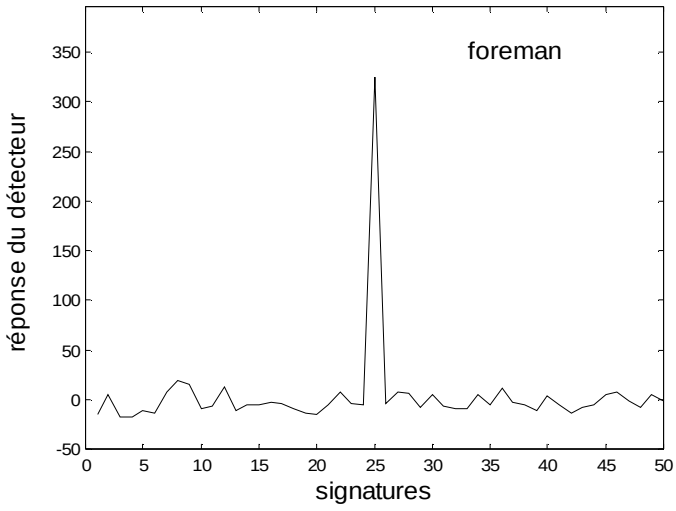
l'image apparaît en position 25. Aucune attaque n'a été portée à l'image. Les courbes montrent que l'on peut détecter parfaitement la signature dans les images tatouées sans équivoque, suggérant que l'algorithme a des taux de réponse de fausses alarmes (et faux négatifs) très bas.

(A)



(B)

(C)



(D)

Figure 3.8 Les images tatouées pour (a) ‘carphone’ et (c) ‘foreman’ , les réponses du détecteur à 50 signatures générées à partir d’une valeur initiale différente, la signature voulue est en position 25 des abscisses pour (b) ‘carphone’ et pour (d) ‘foreman’.

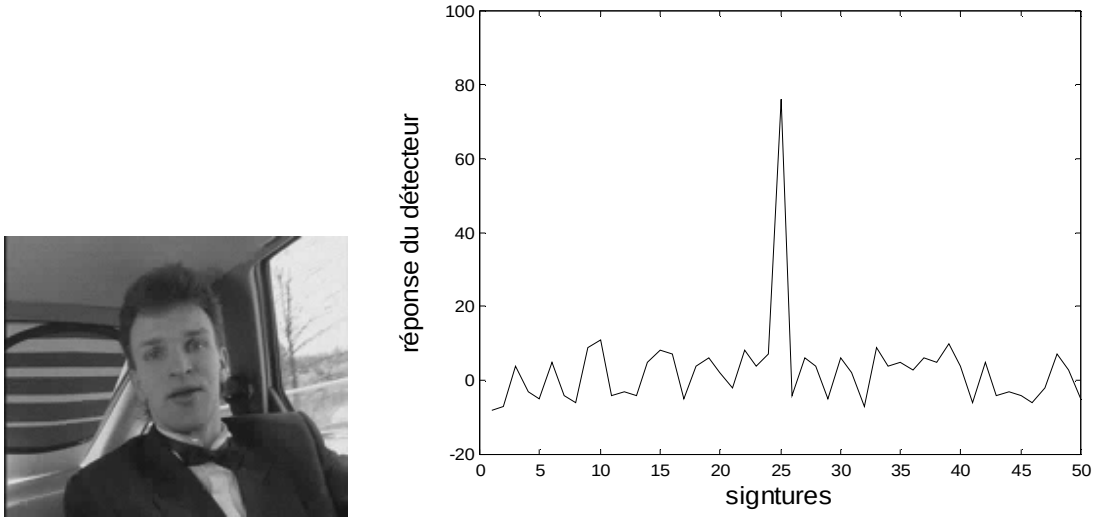
Puisque la détection est assurée, il reste maintenant à évaluer l'impact des attaques sur l'algorithme et les conséquences qu'elles peuvent avoir sur la détection.

5. ROBUSTESSE AUX DIVERSES ATTAQUES

Comme il s'avère impossible de considérer toutes les attaques possibles, nous avons décidé de restreindre notre domaine d'étude à l'ensemble de quelques attaques importantes.

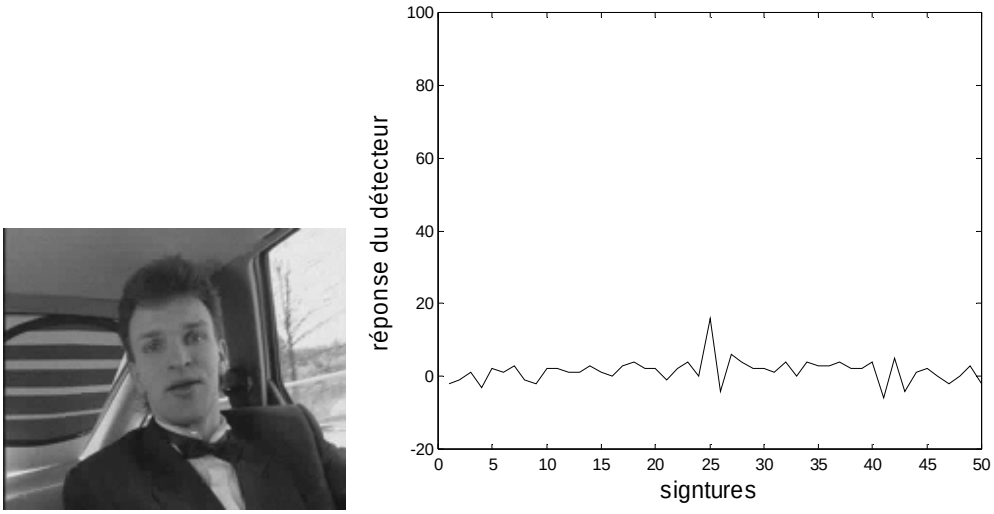
5.1. Robustesse à la variation du paramètre de quantification Qp

Nous avons éprouvé la robustesse de notre algorithme face à la variation du paramètre Qp, puisque la marque est insérée dans le domaine compressé, alors la réponse du détecteur r montrée dans la section 4 représente la détection d’une image tatouée avec un paramètre de quantification Qp=20 et il est aussi utilisé dans la phase d’insertion. On utilise ce paramètre pour juger la robustesse à son variation, lorsque que le paramètre de quantification QP augmente l’amplitude de la corrélation (réponse du détecteur r) diminue, a partir d’une valeur de paramètre de quantification QP supérieure ou égale à 30, l’amplitude de pic de corrélation r est presque nulle, alors la signature ne va pas être détectée, comme illustrer dans la figure 3.10. D’outre part, si on applique sur l’image tatouée une valeur du paramètre Qp inférieure à 20, on peut trouver une détection excellente, comme montrée dans la figure (3.11).



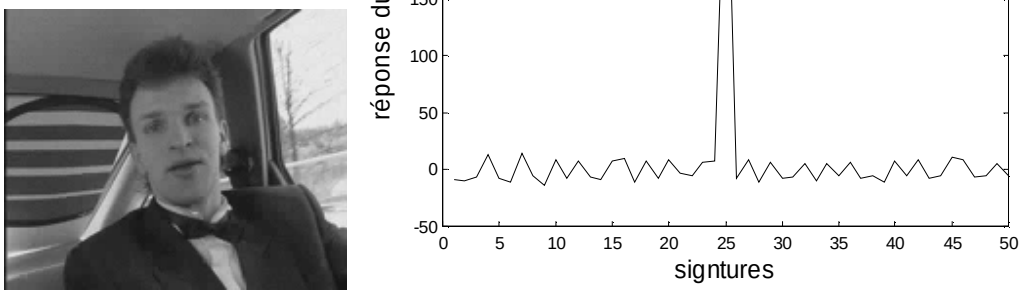
(A) (B)

Figure 3.9 Effet de la variation du paramètre de Qp quantification sur l'image tatouée ‘carphone’, la valeur du Qp vraie est de 25 (a), et la réponse du détecteur correspondante (b).



(A) (B)

Figure 3.10 Effet de la variation du paramètre de Qp quantification sur l'image tatouée ‘carphone’, la valeur du Qp vraie est de 30 (a), et la réponse du détecteur correspondante (b).



(A) (B)

Figure 3.11 Effet de la variation du paramètre de Qp quantification sur l'image tatouée ‘carphone’, la valeur du Qp vraie est de 10 (a), et la réponse du détecteur correspondante (b).

5.2. Robustesse au filtrage

Le filtrage consiste à appliquer une transformation (appelée *filtre*) à tout ou partie d'une image numérique en appliquant un opérateur. Nous avons décidé d'effectuer comme attaque deux types de filtrage :

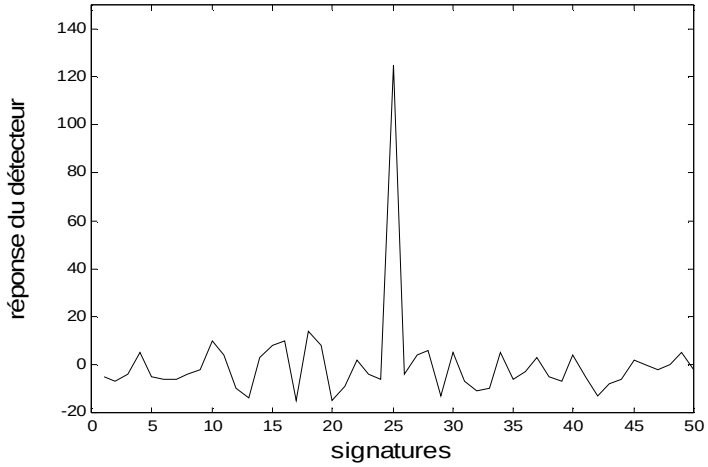
- le filtre passe-bas, consistant à atténuer les composantes de l'image ayant une fréquence haute (pixels foncés). Ce type de filtrage est généralement utilisé pour atténuer le bruit de l'image, un lissage apparaît sur l'image tatouée ‘corphone’ afin de réduire l'activité dans les zones texturées en utilisant ce filtre.

L'opération consiste à remplacer chaque pixel par la moyenne des pixels environnants. On Utilise ce que l'on appelle une matrice de convolution, qui par exemple dans le cas d'un filtre Passe bas 3x3 sera :

$$\frac{1}{9} x \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

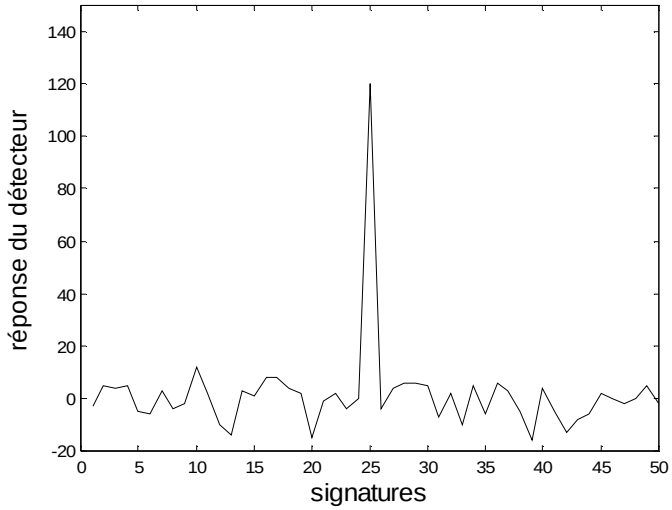
Il est possible d'utiliser d'autres matrices de convolution, par exemple la même Chose, mais prenant une zone plus grande, 9x9 par exemple. Le principe de calcul reste le même, en divisant la valeur obtenue par 81.

- Le filtre médian, est un type de filtre passe-bas dont le principe est de faire la moyenne des valeurs des pixels avoisinants. Le résultat de ce filtre est une image plus floue.



(A) (B)

Figure 3.12 Réponses du détecteur à 50 signatures générées aléatoirement après filtrage Passe-bas de l'image 'carphone' tatouée, notre signature apparaît en position 25.



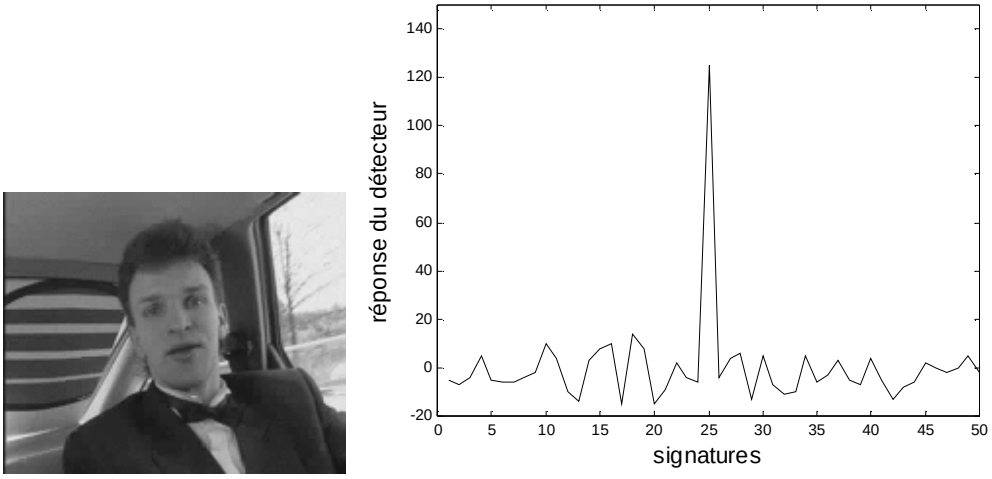
(A) (B)

Figure 3.13 Réponses du détecteur à 50 signatures générées aléatoirement après filtrage (filtre médian) de l'image "carphone" tatouée, notre signature apparaît en position 25.

La figure 3.12 (a) montre l'image ‘carphone’ tatouée après le filtrage par un filtre passe-bas. Il est clair que un lissage apparaît sur l'image tatouée ‘corphone’ et des dégradations se produisent éventuellement sur l'image tant que l’image est filtrée par un filtre passe bas. La figure 3.12 (b) représente la réponse du détecteur à 50 signatures générées aléatoirement, dont la signature présente dans l'image est incluse. Un pic clairement indique la présence de signature et démontre que le filtrage n'interfère pas avec notre processus.
La figure 3.13 (a) montre l'image ‘carphone’ tatouée après le filtrage, filtrée par un filtre médian. On voit bien qu’il y’a des dégradations se produisent éventuellement sur l'image tant que l’image est filtrée par un filtre médian. La figure 3.13 (b) représente la réponse du détecteur à 50 signatures générées aléatoirement, dont la signature présente dans l'image est incluse. Un pic clairement indique la présence de signature et démontre que le filtrage n'interfère pas avec notre processus.

5.3. Contamination par un bruit gaussien

Le bruit caractérise les parasites ou interférences d'un signal, c'est-à-dire les parties du signal déformées localement. Ainsi le bruit d'une image désigne les pixels de l'image dont l'intensité est très différente de celles des pixels voisins.
Nous avons également évalué la robustesse de l'algorithme en ajoutant un bruit gaussien à l'image tatouée. La variance du bruit utilisée dans la simulation varie entre [-6 6]. Sur la figure 3.14, on peut observer que le détecteur détecte la signature correctement, bien que la contamination par un bruit de variance de [-6 6] a causé à l'image une déformation intolérable. Notre algorithme de tatouage est tout à fait robuste à ce type de traitement.



(A) (B)

Figure 3.14 Effet de l'ajout du bruit gaussien de variance [-6 6] à l'image tatouée ‘carphone’ (a), et la réponse du détecteur correspondante (b).

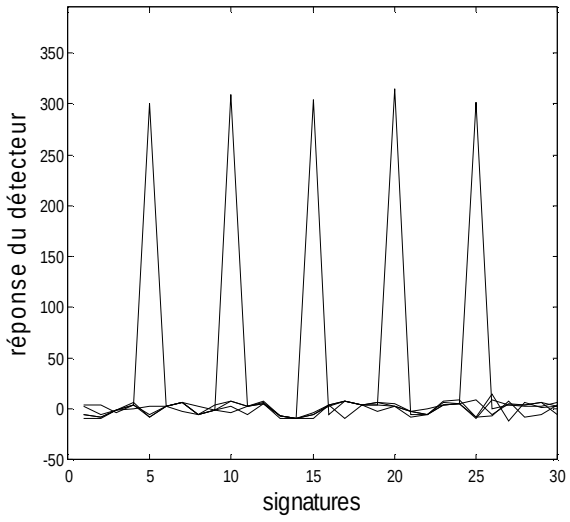
5.4. Attaque par surmarquage

Elle consiste à tatouer à nouveau une vidéo déjà tatouée. cette attaque peut être très dangereuse. Certains protocoles de tatouage se protègent en vérifiant, avant de distribuer une clef, que la vidéo proposée n'est pas tatouée. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection. Les pirates commencent par contourner l'interdiction au surtatouage : une image est dégradée jusqu'à ce que l'on puisse la sur tatouer (la première signature n'étant plus lisible). On ajoute aux images les images ainsi surtatouées. Les images résultantes portent alors les deux tatouages, mais le détecteur n'en lit qu'un, le nouveau : le pirate s'est donc approprié les images.

Les images (a) et (c) représentent respectivement ‘carphone’ et ‘foreman’ après cinq opérations de tatouage successives. Il est clair que des dégradations importantes se produisent éventuellement sur les images tant que le processus de tatouage est répété. Les courbes (b) et (d) représentées dans la figure 3.15 montrent respectivement les réponses du détecteur à 30 signatures générées aléatoirement, dont les cinq signatures présentes dans les images sont

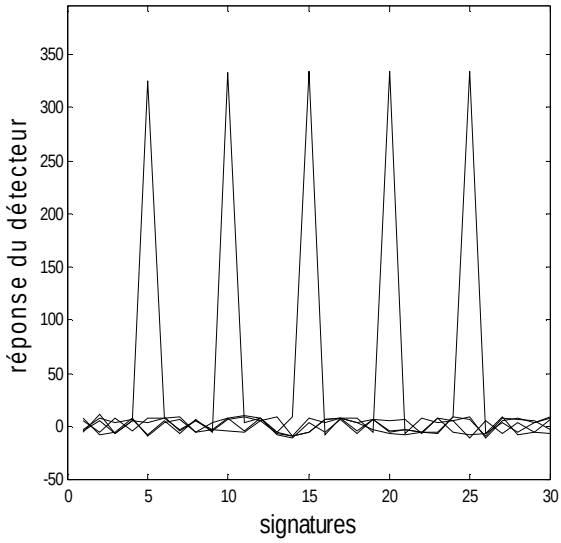
incluses. Cinq pics clairement indiquent la présence des cinq signatures et démontrent que le tatouage successif n'interfère pas avec notre processus.

(A)



(B)

(C)



(D)

Figure 3.15 Réponses du détecteur à 30 signatures générées aléatoirement après surmarquage de l'image ‘carphone’ (b) et de l’image ‘foreman’ (d).

6. Conclusion

Nous avons présenté dans ce chapitre les résultats obtenus pour la méthode de tatouage des images de la vidéo que nous proposons, ces résultats montrent que la méthode développée est particulièrement robuste aux dégradations de type traitement habituel de la vidéo (compression , filtrages et ajout du bruit). Ces résultats sont obtenus par analogie entre l’insertion dans le domaine transformé (DCT) et le modèle psychovisuel, qui prend en compte la sensibilité de l'oeil humain au bruit pour augmenter et adapter la capacité de la signature selon les caractéristiques locales de la vidéo. La qualité des images de la vidéo tatouée est obtenue à partir d'un critère subjectif. D’après les résultats obtenus des méthodes d’insertion utilisées, on constate une bonne performance de détection de la signature pour les deux modes d’insertion, sauf que dans le premier mode qui emploi tous les blocs de l’image pour inclure la signature, la capacité du tatouage est très élevée que le second mode.

CONCLUSION GENERALE

Généralement, les méthodes de tatouage vidéo utilisent le domaine compressé. Ces méthodes sont insérées dans les coefficients transformés et quantifiés dans les images successives de la vidéo.

Nous avons introduit ce travail en exposant les principes et les propriétés générales d'un processus de tatouage numériques. Et nous avons aussi exposé différentes approches utilisées en tatouage vidéo, un algorithme du tatouage vidéo peut se décomposer en trois classes fondamentales :

– l'insertion de la signature sur le format décompressé.

– l'insertion de la signature durant la compression.

– l'insertion de la signature après la compression.

La signature insérée dans le domaine décompressé porte l'inconvénient de n'est pas être présence, après la compression, le domaine utilisé dans cette approche est le domaine spatial, l'insertion dans ce domaine devrait être un tatouage aveugle ou semi-aveugle,de plus, cette méthode n'est pas robuste à les attaques géométriques. L'insertion dans le domaine compressé offre la possibilité d'obtenir plus grande robustesse et aussi l'impact visuel sur la vidéo tatouée est très faibles ainsi que L'insertion et la détection de la signature peuvent être s'effectuer en temps réel. L'insertion après la compression s'effectuée directement dans le bit stream de la vidéo, cette approche est utilisée rarement dans les algorithmes de tatouage vidéo au raison de la complexité de mise en œuvre de ces algorithmes.

Nous avons mis en œuvre une méthode complète permettant de certifier que le compromis invisibilité/robustesse du tatouage est garantit. Nous avons choisi l'approche basée sur l'insertion dans le domaine compressé, l'insertion suit un schéma d'étalement du spectre d'une séquence pseudo aléatoire dans le domaine transformé et quantifié dans les images vidéo. Ce domaine permet d'obtenir une meilleure prédiction de l'impact visuel d'une signature sur la vidéo tatouée et insérer une signature dans le domaine compressé permet de réduire les temps de calcul, et aussi permettant une meilleur approche du compromis invisibilité/robustesse. Une étude statistique du problème de détection nous a conduit à une amplitude de corrélation qui peut être calculé à posteriori sur l'image tatouée.

Cependant, notre méthode donne une dégradation sur l'image tatouée dans le cas où tous les macroblocs (MB_s) de la taille 8x8 de l'image sont tatoués. Pour remédier à ce problème, nous avons introduit un second mode d'insertion basé sur le marquage d'un ensemble de MBs.

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

A titre de perspectives, nous avons vue la possibilité de tatouer les images inter dans la vidéo (H.264). Le travail de la future s'appliquera la méthode proposée aux images inter du standard international de la compression (H.264), en exploitant le signal d'erreur de prédiction après compensation de mouvement pour empêcher l'effet de dérive présent dans le tatouage des images vidéo et discuter les attaques temporelles.

Références

[1] A. H. Tewfik and M.D. Swanson. "Data Hiding for Multimedia Personalization, Interaction And Protection". IEEE Signal Processing Magazine, Pages 41–44, 1997.

[2] A. Meerward, "Digital Image Watermarking in the wavelet transform domain", Diploma thesis, Salwburg University, January 2001.

[3] C. T. Hsieh and Y. K. Wu, "Digital Image Multiresolution Watermark Based on Human Visual System Using Error correcting Code", Tamkang journal of Science and Engineering, Vol. 4, No. 3, pp. 201-208,2001.

[4] Yann Bodo, Elaboration d'une Technique D'accès Conditionnel par Tatouage et Embrouillage Vidéo basée sur la Perturbation des Vecteurs de Mouvement, Thèse de doctorat de L'école National supérieur des télécommunications, 2004

[5] F. Deguillaume, G. Csurka, and T. Pun. Countermeasures for Unintentional and Intentional Video Watermarking Attacks. Ping Wah Wong and Edward J. Delp Eds, IS&T/SPIE's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, Vol. 3971 of SPIE Proceedings, San Jose, California USA, 23-28 January 2000. (Paper EI 3971-33).

[6] K. Su, D. Kundur, and D. Hatzinakos. A Content-Dependent Spatially Localized Video Watermark for Resistance to Collusion and Interpolation Attacks. In Proc. IEEE Int. Conf. On Image Processing, vol. 1, pp. 818-821, 2001.

[7] Y. Wu and R. Deng. Adaptive Collusion Attack to a Block Oriented Watermarking Scheme. Information and Communications Security, 5th International Conference, Huhehaote, China, October 10-13, 2003.

[8] C. S. Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual-Property", IDEA GROUP PUBLISHING, 2005.

[9] P. Bas, "Méthodes de Tatouage d'images fondées sur le contenu", Thèse de doctorat de L'INPG, Grenoble, Octobre 2000.

[10] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images", In IEEE Work-shop on Nonlinear Image and Signal Processing, pages 460-463, Noes Marmaras,Greece, June 1995.

[11] P. Bas, N. Le Bihan, and J-M Chassery. Color Image Watermarking Using Quaternion Fourier Transform. Proc of ICASSP , 2003, Hong Kong, China.
[12] B. Tao and B. Dickinson. Adaptive Watermarking In The DCT Domain. In Proc. Int. Conf. Image Processing (ICIP), Lausanne, Switzerland, Sept. 96.
[13] J.J.K. O'Ruanaidh and T.Pun. Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking. Signal Processing, Vol.66, No.3, May 1998, pp.303-317.
[14] D. Kundur and D. Hatzinakos. Digital Watermarking Using Multiresolution Wavelet Decomposition. Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.
[15] J. F. Delaigle, C. De Vleeschouwer, F. Goffin, and B. Macq. Low Cost watermarking based on a Human Visual Model. Lecture Notes in Computer Science, 1242, 1997.
[16] D. Ghosh, and K. Ramakrishna, "Watermarking Compressed Video Stream over Internet," The 9th Asia-Pacific Conference on Communications 2003 (APCC2003), Vol.2, pp.711-715, 2003.
[17] F. Deguillaume, G. Csurka, J.J.K. O'Ruanaidh, and T. Pun. Robust 3D DFT video watermarking. Electronic Imaging / Session : Security and Watermarking, 1999.
[18] F. Deguillaume, G. Csurka, J. O. Ruanaidh, and T. Pun. "Robust 3D DFT Video Watermarking," In Proceedings of Security and, San Jose, Vol.3657, pp. 113-124, 1999. Watermarking of Multimedia Contents, SPIE
[19] Jae Hyuck Lim, Dae Jin Kim, Hyun Tae Kim, Chee Sun Won. "Digital Video Watermarking Using 3D-DCT and Intra-Cubic Correlation," Security and Watermarking of Multimedia Contents III, Ping Wah Wong, Edward J. Delp III, Editors, Proceedings of SPIE Vol. 4314, 2001.
[20] F. Hartung and B. Girod. Watermarking Of Uncompressed and Compressed Video. Signal Processing, Vol. 66, pp. 283–301, 1998.
[21] D. Cross, B. G. Mobasseri, "watermarking for Self-Authentication of Compressed Video," IEEE ICIP, vol.2, pp. 913-916, 2002.
[22] I. Setyawan, R. L. Lagendijk, "Low Bit Rate Video Watermarking Using Temporally Extended Differential Energy watermarking (DEW) Algorithm," Proc. Security and Watermarking of Multimedia Contents III, vol. 4314, pp. 73-44, 2001.
[23] G.C. Langelaar, R. L. Lagendijk, Optimal Differential Energy Watermarking of DCT Transactions on Circuit and Systems for Video Technology, 2003.

[24] Lain E. G. Richardson, H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia, John Wiley & Sons Ltd Publishers, 2003 ISBN 0-470-84837-5

[25] T. Wiegand, G. J.Sullian, G. Bjontegaard, and A.Luthra, "Overview of the H.264 Video Coding Standard," IEEE Trans. Circuits Syst. Video Technol., vol. 13, pp. 560-576, July 2003.

[26] Ta.Te Lu, Wei. Lun Hsu, and Pao. Chi Chang, "Blind Video Watermarking for H.264," in IEEE CCECE, May 2006, pp. 2353-2356.

[27] Koz. A, A.Alatan. A, "Oblivious Spatio-Temporal Watermarking of Digital Video by Exploiting the Human Visual System," in IEEE TCSVT, March 2008. Vol 18, pp. 326-337.

[28] A. Koz and A. A. Alatan, "Oblivious Video Watermarking Using Temporal Sensitivity of HVS," in Proc. IEEE ICIP, 2005, vol. 1, pp. 961–964.

[29] Shipeng Li, F Pereira, H. Y. Shum, A. G. Tescher.H. "264/AVC Video Authentication Using Skipped Macroblocks For An Erasable Watermark," Proc. of SPIE, Vol. 5960, 2005.

[30] K. Su, D. Kundur, et D. Hatzinakos. A Novel Approach to Collusion Resistant Video Watermarking. Dans Security and Watermarking of Multimedia Contents IV, Volume 4675 de Proceedings of SPIE, Pages 491–502, Janvier 2002.

[31] G. Doerr et J.-L. Dugelay. Collusion Issue in Video Watermarking. Dans Security, Steganography and Watermarking of Multimedia Contents VII, volume 5681 de Proceedings of SPIE, pages 685–696, Janvier 2005.

[32] C.-P. Fan, "Fast 2-Dimensional 4x4 Forward Integer Transform Implementation for H.264/AVC," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 53, no. 3, pp. 174–177, Mar. 2006.

Abstract:

In this memory, we presented a novel blind video watermarking method based on the exploitation the coefficients of highs frequencies not zero in the block transform by DCT. The images intra (I) of international standard of the compression video (H264) are chosen to embed watermark**,** and then its luminance are divided into blocks of the size 8x8 and transformed by DCT. We used two ways to embed watermark, the first employs all blocks in image to insert watermark, the second employs certain block in image to insert the bits of watermark, for both ways of insertion, the watermark is inserted in the coefficients of highs frequencies not zero of blocks in images. During the detection process, the correlation between watermark and the highs frequency coefficients transformed not zero is computed to judge whether the frame has been embedded watermark. The experimental results indicate that the correlation curve peaks correspond at the watermarked images. The proposed watermarking method has strong robustness against some attacks such as image filtering, image compression, image statistical average and collusion attack, attack by on marking.

Résumé

Dans ce mémoire, nous avons présenté une nouvelle méthode de tatouage vidéo aveugle basée sur l'exploitation des coefficients hautes fréquences non nuls dans les blocs transformés par DCT. Les images intra (I) du standard international de la compression vidéo (H264) sont choisies pour insérer le tatouage, et alors leurs luminances sont divisées en blocs de la taille 8x8 et transformés par DCT. Nous avons utilisé deux manières pour insérer le tatouage, la première emploi tous les blocs dans l'image pour insérer le tatouage, la seconde emploi certains blocs dans l'image pour insérer les bits de tatouage, pour les deux manière d'insertion, le tatouage est inséré dans les coefficients hautes fréquences non nuls des blocs dans les images. Pendent le processus de détection, la corrélation entre le tatouage et les coefficients transformés hautes fréquences non nuls est calculée pour juger si l'image à été tatouée. Les résultats expérimentaux indiquent que l'amplitude des pics de corrélation correspond aux images tatouées. La méthode du tatouage proposée a une forte robustesse à quelques attaques connues telles que filtrage d'image, compression d'image, attaque par collusion, attaque par surmarquage.

ملخص :

في هده المذكرة، قمنا بتقديم طريقة جديدة لوشم صور الفيديو اعتمادا على استغلال المعاملات ذات التواتر العالي الغير معدومة الموجودة داخل المربعات المحولة بواسطة (DCT : Discrete Cosins Transform) بصفة عامة الفيديو . عبارة عن مجموعة من الصور المتعاقبة، بحيث أنه درجة الكثافة الضوئية لهده الصور مقسمة إلى مربعات ذات السعة 8*8 من المعاملات المحولة. لإدراج الوشم داخل صور الفيديو قمنا باستخدام نمطين، بحيث أنه في النمط الأول استعملنا كل المربعات الموجودة داخل الصورة لإدراج الوشم، بينما في الثاني استخدمنا فقط مجموعة من المربعات لإدراج الوشم، حيت أن كل منهما يعتمد على استغلال المعاملات ذات التواتر العالي الغير معدومة لهدف إدراج الوشم داخل صور الفيديو. خلال مرحلة الكشف عن الوشم، نقوم بحساب دالة التشابه بين الوشم في حد دانه و المعاملات المحولة لأجل معرفة هل الصورة موشومة أم لا. النتائج التجريبية توضح أن السعة العظمى لإشارة التشابه تتوافق مع الصور الموشومة، وكدالك نفس النتائج توضح أن الطريقة المقترحة لها مثانة عالية ضد بعض الهجمات المعروفة في معالجة الصورة مثل ترشيح الصور، ضغط الصور، الهجوم عن طريق تكرار الوشم...الخ. الغرض من هده الهجمات هو نزع الوشم المجود داخل صور الفيديو