Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahlab de Blida

Faculté des sciences

Département d'informatique

Mémoire Présenté par

Gacem Nassim

Belarbi Mohamed Abdou

En vue d'obtenir le diplôme de Master

Domaine : Mathématique et Informatique. MI

Filière : Informatique.

Option : Ingénierie des logiciels.

Titre : Tatouage robuste pour le traçage des utilisateurs illicites des vidéos distribuées.

Encadreur : Mme K.Ait Saadi

Organisme d'accueil : Centre de Développement des Technologies Avancée

Soutenue le : **devant le jury composé de :**

-M Mme Benstiti **Président**

-M Mr Sidemou **Examinateur**

-M Mme Toubalina **Examinateur**

- promotion 2012/2013 -

Dédicaces

Je dédie ce travail :

A la femme qui m'a depuis mon plus jeune âge encouragé, orienté, et soutenu avec patience durant toutes les épreuves que j'ai dues traverser et qui a toujours cru en moi

A ma très chère MAMAN ***NADJET***;

A l'homme qui a sacrifié sa personne pour pouvoir nous procurer tout besoin nécessaire pour une bonne éducation, bien-être et confort

A mon très cher PERE ***ARAB*** ;

A mes frères

Sami

Et

Mourad

Et ma très chère sœur

Sarah

Je le dédie spécialement à ma chère fiancée ***Zemieche Manel*** et à toute sa famille

A ma très chère tante ***Naciba*** et sa défunte fille ***Ahlèm*** (Paix soit sur son âme)

A mon binôme, ami et frère ***Abdou***, que la paix et la joie soient présentes au sein de sa famille

A mes très chers amis ***Mahmoud***, ***Aghilas*** et ***Racim*** et toutes leurs familles

A ma chère belle sœur ***Hind*** et à ma craquante et petite nièce ***Lyna***

Et à tous ceux que je porte dans mon cœur

GACEM NASSIM

Dédicaces

Je dédie ce travail :

A la femme qui m'a depuis mon plus jeune âge encouragé, orienté, et soutenu avec patience durant toutes les épreuves que j'ai dues traverser et qui a toujours cru en moi

A ma très chère MAMAN ***NADIA***;

A l'homme qui a sacrifié sa personne pour pouvoir nous procurer tout besoin nécessaire pour une bonne éducation, bien-être et confort

A mon très cher PERE ***KHALED*** ;

A mon frère ***SAMIR***

A ma sœur ***FATHIA***

A ma défunte sœur ***SOUMIA*** (Paix soit sur son âme)

A mes chers grands parents ***GACEM*** et ***HASSIBA***, à mon oncle ***MOHAMED*** , sa femme, mes tantes et à toute ma famille

A mes chers cousins et cousines ***LAMINE***, ***REDA***, ***MANEL*** et ***SERINE***

A mon binôme, ami et frère ***NASSIM***, que la paix et la joie soient présentes au sein de sa famille

A mes très chers amis ***Mahmoud***, ***Aghilas***, ***Athmen***, ***Nadjib***, ***Amel***, ***Hanna***, ***Farah***, ***Loubna*** et toutes leurs familles

Je le dédie spécialement à une personne importante à mes yeux ***Amina Louiza LACHEHEB***

A mes neveux et nièces ***Alla'a***, ***Aymen***, ***Soumia*** et ***Isra'a***

Et à tous ceux que je porte dans mon cœur

Mohamed Abdou BELARBI

Résumé

Résumé

Le tatouage numérique est une technique permettant d'insérer une marque servant d'empreinte digitale identifiant ainsi un utilisateur bien précis. Une des applications du tatouage numérique permet de tracer les contenus multimédias, ce qui garanti une protection contre une redistribution illicite de ces derniers. Cette application est le Fingerprinting, elle assure donc le traçage des copies des utilisateurs, honnêtes ou malhonnêtes soient-ils.

Dans cette thèse, nous avons utilisé la méthode de traçage des copies pirates des utilisateurs dans la norme de compression vidéo H.264/AVC. La marque utilisée comme empreinte est créée à l'aide du code de Tardos probabiliste amélioré qui sera insérée lors de la compression du média en utilisant la technique d'étalement du spectre. Le critère d'invisibilité de la marque sera assuré en suivant un concept de la psychophysique qui définit la limite en dessous de laquelle un individu ne parvient plus à différencier deux stimulations, c'est le seuil différentiel (Just Noticeable Difference JND). L'évaluation de la robustesse de la marque sera faite par l'utilisation de quelques attaques telle que les attaques par collusion linéaires et l'attaque de compression.

Mots clés : Tatouage numérique, Fingerprinting, code de Tardos amélioré, traçage des copies, norme de compression H.264/AVC, seuil différentiel.

Abstract

Digital watermarking is a technique to insert a mark for fingerprint thus identifying a specific user. One application of the watermark is used to draw the multimedia content, which guarantees protection against unauthorized redistribution thereof. This application is the fingerprinting, thus it ensures the tracing copies of users, honest or dishonest they are.

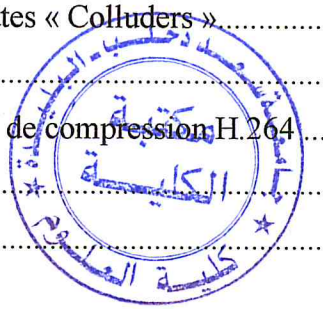
In this thesis, we used the method of tracing pirate copies of users in the H.264/AVC video compression standard. Used as the brand footprint is created using the improved probabilistic Tardos code which will be inserted during the compression of the media using the spread spectrum technique. The test invisibility of the mark will be provided following a concept of psychophysics that defines the boundary below which an individual can no longer differentiate between two stimuli, the differential threshold (Just Noticeable Difference JND). The evaluation of the robustness of the mark will be made by the use of some attacks such as collusion attacks and linear compression driver.

Keywords: watermarking, fingerprinting, code of Tardos improved tracing copies compression standard H.264/AVC, differential threshold.

SOMMAIRE

Sommaire

- **Liste des figures**



- **Liste des tableaux**

Introduction Générale

Introduction

L'évolution des technologies de capture et de transmission d'images et de vidéos numériques à la fin du XXème siècle a ouvert de grandes perspectives et possibilités de création et de manipulation des contenus visuels à la fois sur le plan scientifique et artistique offrent au public la possibilité d'échange des fichiers multimédias grâce à des outils tels que (Internet, CD/DVD, etc.). Néanmoins, cette formidable révolution technique a également engendrée des problèmes de sécurité en occurrence la copie et la distribution illégale de ces médias. Les principaux acteurs touchés sont les artistes, les maisons d'édition, l'économie et l'emploi de façon générale. On estime au niveau mondial à plus d'une vingtaine de milliards de dollars les pertes en matière de droits d'auteur [1]. Ainsi, les fournisseurs de contenues ont rapidement vu leurs ventes chuter de façon significative. Ces derniers sont donc très attentifs à toute nouvelle technologie qui améliorerait la gestion des droits numériques et d'empêcher la redistribution illégale de contenus multimédias protégés par le droit d'auteur. Dans cette optique, le tatouage numérique a été introduit au début des années 90 comme un mécanisme de sécurité complémentaire au cryptage. En effet, les données cryptées, une fois décryptées, seront accessibles. A ce moment précis, les données numériques ne sont plus protégées par le cryptage et peuvent être éventuellement copiées et redistribuées à grande échelle.

Le tatouage numérique a donc été introduit comme une seconde ligne de défense. L'idée de base consiste à protéger un document numérique en dissimulant un code de façon robuste et imperceptible.
Mais, cette technique n'est pas totalement robuste puisque des attaques ont été conçues pour la déjouer, d'où la nécessité de trouver une solution de traçabilité pour remédier aux éventuelles attaques.
Le but est d'élaborer un algorithme de tatouage robuste permettant de tracer les copies, l'utilisation illicites des vidéos compressées par le standard vidéo courant H.264 /AVC.
Le mémoire est organisé comme suit :

- Dans le premier chapitre, nous présenterons l'état de l'art décrivant les principes généraux du tatouage numérique, propriétés, et applications.

- Le second chapitre introduira la notion de traçage des copies pirates et la contribution du tatouage numérique dans cette application.

- L'apport du modèle psycho visuel dans le Watermarking (JND : Just Noticeable Difference) fera l'objet du troisième chapitre.

- Le quatrième chapitre parlera de l'implémentation des techniques citées dans les chapitres précédents à savoir le tatouage robuste, le code de Tardos amélioré et le modèle psycho-visuel pour réaliser une application pouvant tracer les utilisateurs malhonnêtes des vidéos compressés par la norme H.264/AVC qui sera introduite dans ce même chapitre.

- Le dernier chapitre clôturera ce mémoire par les tests et résultats obtenus après l'implémentation des différents traitements pour l'application ciblée. L'évaluation se fera du point de vue qualité visuelle et robustesse face aux différentes attaques de collusion linéaires.

Et ce mémoire sera achevé et terminé par une conclusion générale donnant ainsi quelques aspects de cette approche.

Chapitre I : Tatouage numérique

1. Introduction

La cryptographie était la technique la plus utilisée afin de sécuriser le partage et la transmission des contenus audio-visuels. Cependant, la sécurité des documents est assurée juste avant l'étape de déchiffrement, mais après cette étape, le contenu du document devient clair et visible sans aucune protection, donc il peut être manipulé, retransmis. C'est à ce manque de fiabilité que le tatouage numérique a été introduit, branche de la stéganographie qui signifie précisément « écriture cachée » ayant comme concept la dissimulation d'une marque d'une manière invisible dans un document donné.

Dans ce chapitre, nous allons définir le tatouage numérique, son principe, ses domaines d'application et citer quelque stratégies d'attaques pour l'application de la traçabilité.

2. Tatouage numérique

2.1. Définition

C'est une technique de marquage ayant pour principe d'insérer une signature invisible et permanente dans un contenu multimédia (audio, vidéo ou image) transitant par les réseaux, tel que Internet, afin de lutter contre la fraude et le piratage et d'assurer le droit de propriété intellectuelle. Chaque image possédera donc un code d'identification imperceptible et indétectable par tout système ignorant son mode d'insertion. Ce qui implique la dissuasion d'un éventuel pirate dans la mesure où cette marque peut être retrouvée dans chaque copie de l'image originellement tatouée. Cette dernière doit avoir la capacité à résister aux différentes attaques (Collision, etc.). La figure 1.1 décrit d'une manière générale les principaux processus du tatouage numérique [2] [3].

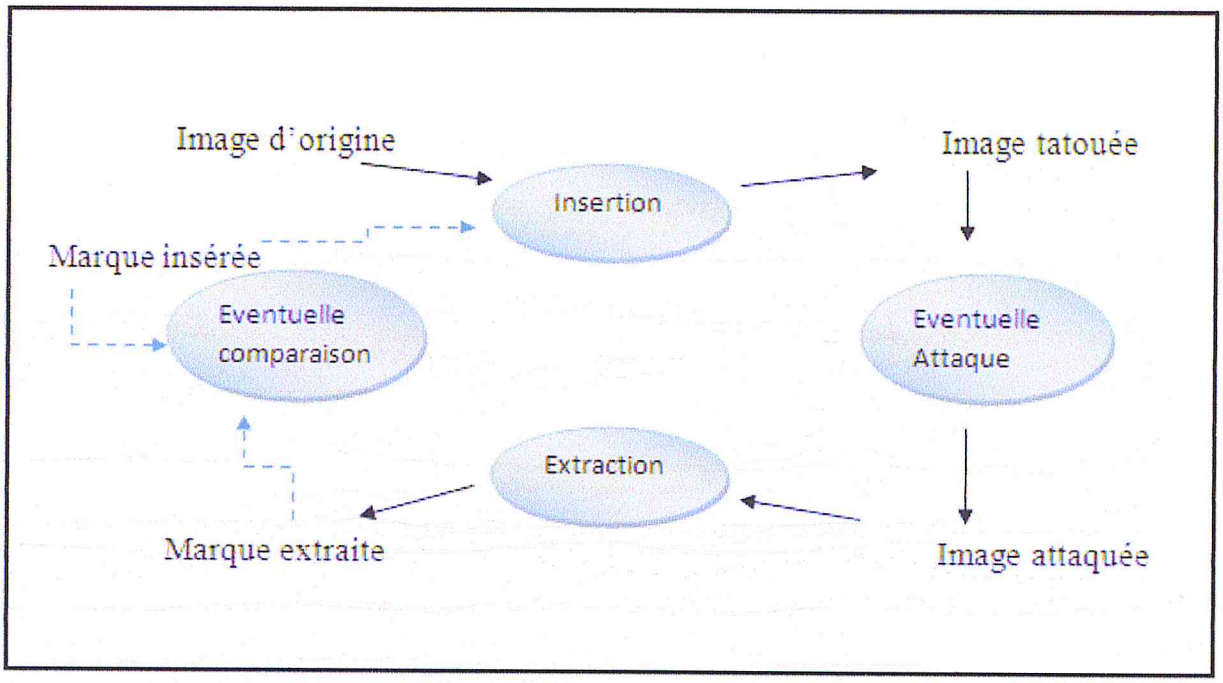


Figure 1.1 : Schéma général du processus de tatouage numérique

2.2. Propriétés du tatouage numérique

Il existe plusieurs propriétés du tatouage numérique qui diffèrent d'une application à une autre, mais les principales propriétés sont [4] :

- **2.2.1. Capacité :** Représente la quantité d'information insérée dans le signal haute dans une image. Cette quantité varie selon l'application [5].

- **2.2.2. Imperceptibilité :** Le tatouage numérique peut introduire des distorsions. L'idéal c'est que lesdites distorsions soient les plus faibles possibles afin que visuellement l'image tatouée reste identique ou presque à l'image originale [5].

- **2.2.3. Robustesse :** Le pouvoir de récupérer une marque qui a été insérée même après que l'image ou vidéo soit soumise à des attaques [5].

- **2.2.4. Sécurité :** Un système de tatouage numérique doit aussi assurer la sécurité en ayant un compromis entre les trois précédentes propriétés, mais

aussi garantir à ce que la marque soit robuste sans altérer l'image après d'éventuelles attaques [5]. La figure 1.2 montre les propriétés du tatouage numérique et leur liaison.

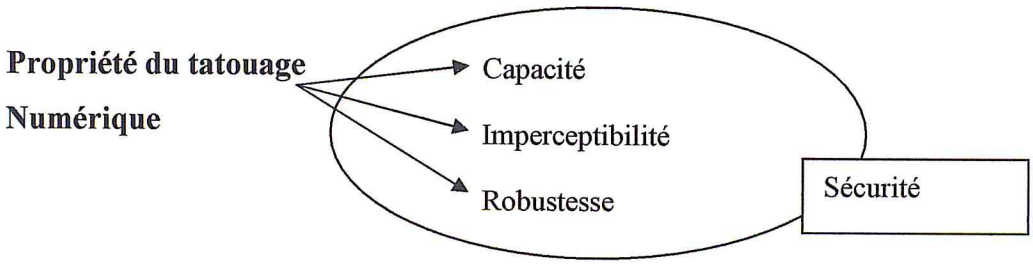


Figure 1.2 : Les propriétés du tatouage numérique

2.3. **Classification du tatouage numérique :** Le tatouage numérique est classifié par rapport aux critères suivant : Manière d'insertion, domaine d'insertion, robustesse et mode d'extraction [5] [6]. La figure 1.3 schématise la classification du tatouage numérique.

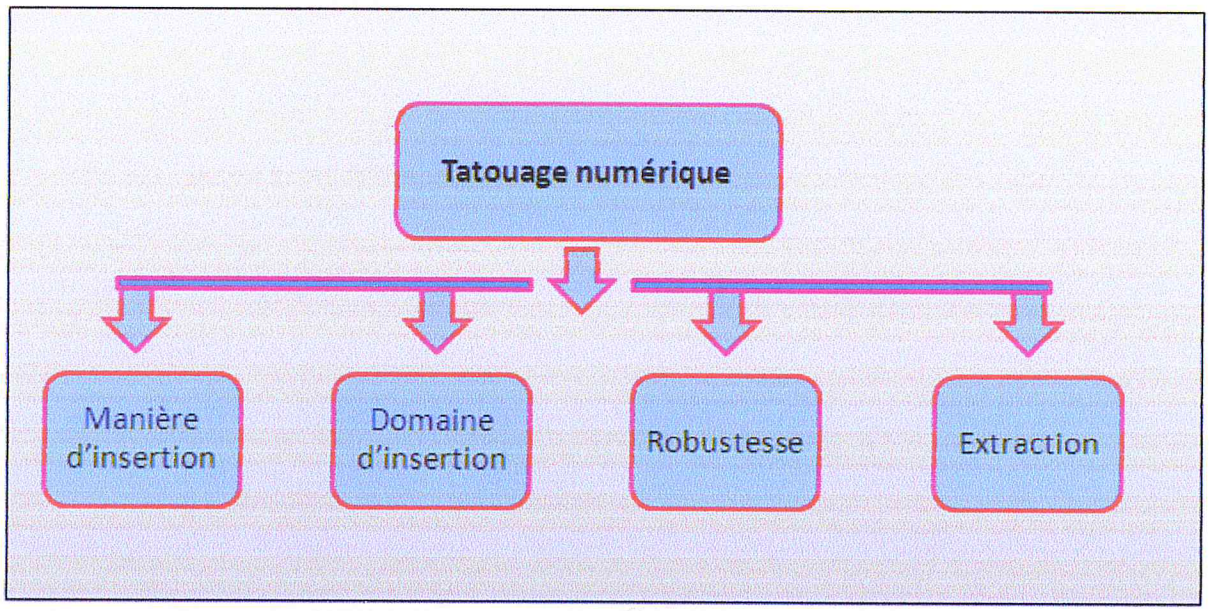


Figure 1.3 : Classification du tatouage numérique

2.3.1. Manière d'insertion

- **Schéma additif :** Le principe consiste en l'extraction des coefficients de l'objet d'origine à modifier, en suite le tatouer en ajoutant la marque à ces coefficients [4].

- **Schéma substitutif :** Le concept est que l'information à insérer est substituée à des caractéristiques de l'image. L'idée de base consiste à insérer une marque en modifiant le contenu structurel de l'image [4].

2.3.2. Domaine d'insertion

- **Domaine spatial :** Les algorithmes fonctionnant dans le domaine spatial modifient directement les valeurs des pixels de l'image. Comme aucun traitement initial n'est requis, ils sont très rapides et permettent de travailler en temps réel. Cependant, un tel schéma n'assure pas une robustesse face à la compression qui peut être considérée comme une attaque. Un faible taux de compression avec JPEG par exemple est capable de détruire la marque [4].

- **Domaine fréquentiel :** Ce domaine résulte après l'utilisation d'une TFD (Transformée de Fourier Discrète) ou d'une DCT (Transformée en Cosinus Discrète) ou la DWT (Compression par ondelette). Les techniques utilisant la DCT sont plus robustes face aux opérations de compression [4]. Le tatouage peut être appliqué d'une manière adaptative aux fréquences qui contiennent l'information importante de l'image d'origine évitant ainsi la perte des informations après la compression [4] [7].

Le tableau suivant (tableau 1.1) fournis une comparaison entre les deux précédents domaines [4] [7] :

Tableau 1.1 : Tableau illustrant une comparaison entre le domaine spatiale et le domaine fréquentiel

	Domaine spatiale	**Domaine fréquentiel**
Cout de calcule	Bas	Haut
Robustesse	Fragile	Robuste
Perception	Haute	Basse
Capacité	Haute (avec dépendance sur la taille de la marque)	Basse

- **Domaine compressé :** Ce domaine assure la préservation de l'information sans aucun accroissement de la taille du fichier [4]. Il est une résultante du domaine précédent (Domaine fréquentiel), les algorithmes sont appliquées directement sur le flux binaire compressé. La plupart de ces algorithmes utilisent le code de longueur variable (le VLC « Variable Length Code ») pour l'insertion [4] [7].

2.3.3. Robustesse : Les algorithmes de tatouage numérique peuvent être classifiés aussi selon leur robustesse. Il existe trois catégories : tatouage robuste, fragile et semi-fragile.

- **Tatouage robuste :** Les algorithmes de tatouage robuste ont été proposés pour pallier les problèmes de protection des droits d'auteurs, les recherches dans ce domaine persistent pour aboutir à un schéma aussi robuste que possible. Donc, l'idéal c'est d'arriver à insérer une certaine quantité d'information et d'assurer sa robustesse face à une grande variété de traitement. Lors de l'indexation, le niveau de robustesse est bas par contre la quantité d'information est plus importante. Cependant, c'est l'inverse pour ce qui est du traçage des documents, la robustesse est supérieure à la quantité d'information car la marque doit certifiée la propriété d'image [5].

  La figure 1.4 illustre l'interaction entre la robustesse et la quantité d'information par rapport à leur niveau.

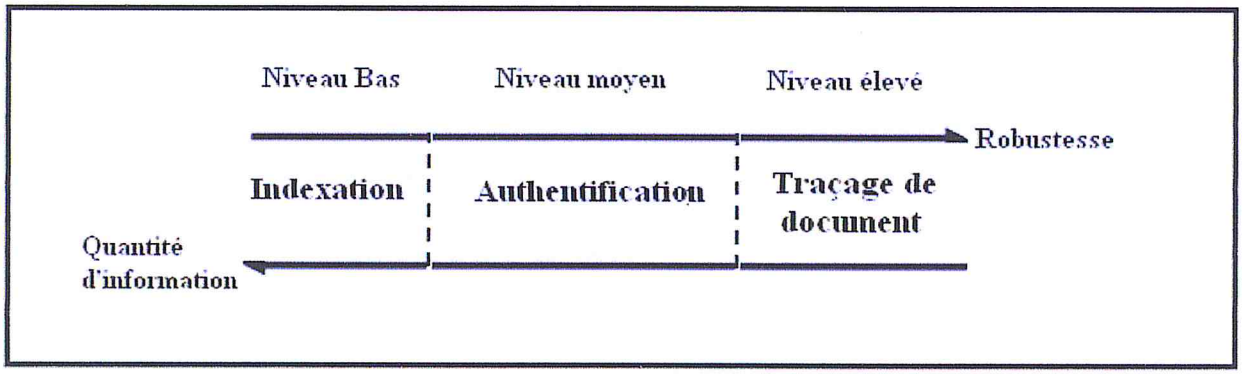


Figure 1.4 : Interaction entre la robustesse et la quantité d'information par rapport à leurs niveaux

- **Tatouage fragile :** On dit qu'un tatouage est fragile si la marque insérée au sein du document est détruite lorsqu'il subit n'importe quel traitement après avoir été tatoué [5].

- **Tatouage semi-fragile :** La différence entre le tatouage fragile et semi-fragile c'est qu'ici le tatouage peut faire face à certaines manipulations de l'image. Donc offre une sécurité meilleure que dans le tatouage fragile [5].

2.3.4. Mode d'extraction

Dans le mode d'extraction de la marque, on distingue trois catégories :

- **Extraction non aveugle :** C'est le cas ou la donnée d'origine est nécessaire à l'extraction. Ce système fonctionne en deux étapes : d'abord il compare le média marqué avec le média original, ensuite un algorithme de décision est appliqué pour répondre si oui ou non, la marque détectée correspond bien à la marque appliquée à l'origine. L'intérêt de ce marquage est très limité [8].

- **Extraction aveugle :** Ce mode d'extraction consiste en la mise en œuvre d'une méthode pour extraire la marque sans utiliser ni l'image d'origine ni la marque insérée. Donc la marque est récupérée à partir de l'image tatouée [8].

- **Extraction semi-aveugle :** Elle n'utilise pas la donnée originale, mais elle a besoin de la marque lors de l'extraction. Dans ce cas, il s'agit de répondre à la question : une marque précise est-elle dans l'image. La majorité des algorithmes de tatouage actuels utilisent ce mode fonctionnement [8].

2.4. Les différentes étapes d'un algorithme de tatouage

Il est important de séparer les différentes étapes d'un algorithme de tatouage, selon les étapes suivantes [3] :

- Dans un premier temps, on commence par générer la marque. Cette étape fait appel à des principes qui viennent aussi bien du monde de la cryptographie (chiffrement de la marque, utilisation de clef, etc.), que du monde du traitement du signal (étalement de spectre, canal de transmission, code correcteur, etc.) ;

- En suite vient la phase d'insertion. Chaque domaine possède ses particularités. Dans le monde de l'audio, on possède une bonne connaissance de l'aspect perceptif des bruits, ce qui permet d'optimiser au mieux l'insertion d'une marque robuste. Cette connaissance étroitement liée aux études de la perception humaine, n'est pas aussi précise dans le monde de l'image fixe ou encore dans celui de la vidéo, ce qui rend plus difficile l'optimisation de la phase d'insertion. L'insertion se fait rarement dans le domaine spatial.

La figure 1.5 montre d'une manière générale le processus d'insertion d'une marque.

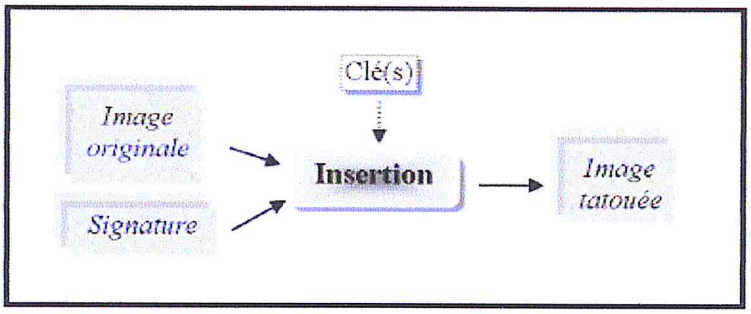


Figure 1.5 : Schéma général du processus d'insertion d'une marque

- Enfin vient la phase de détection. Cette étape est étroitement liée aux précédentes. En effet, pour extraire la marque, le dual de ces phases est souvent utilisé. Dans le cas ou la phase de détection n'est pas le dual de la phase d'insertion, on se base sur les propriétés de cette dernière pour réaliser la détection de la marque.

  La figure 1.6 montre d'une manière générale la détection d'une marque.

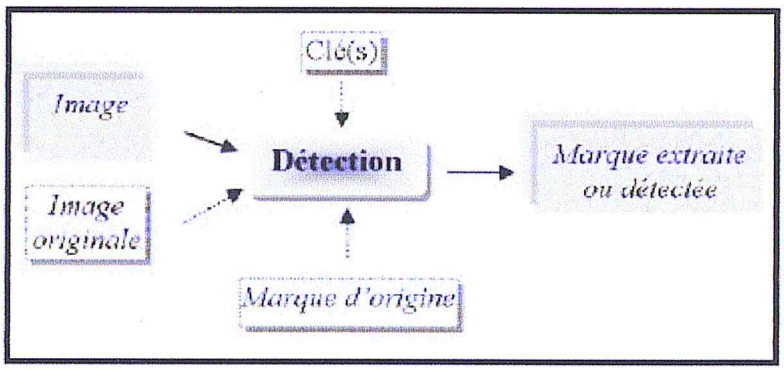


Figure 1.6 : Schéma général du processus de détection d'une marque

Pour mieux comprendre le principe du tatouage numérique, il faut connaitre les principales applications où il intervient.

2.5. Quelques applications utilisant le tatouage numérique

On peut classifier les applications du tatouage numérique en deux ensembles: l'un lié à la sécurité et nécessitant pratiquement toujours des schémas très robustes et très sûrs, l'autre lié à l'enrichissement et ne nécessitant pas nécessairement autant de robustesse ni de sûreté.

Il est évident que les applications liées à la sécurité sont celles qui ont le plus drainé d'« affaires». De nombreux industriels ont vu dans le tatouage une solution pour la protection des droits d'auteurs venant en soutien de la cryptographie pour sécuriser les médias comme l'image, le son, la vidéo. Ces industriels ont encouragé financièrement la recherche dans le domaine. Ce sont également les applications ayant les plus fortes contraintes d'invisibilité, de robustesse, de temps réel et de sûreté.

Les applications les plus connues d'un système de tatouage image ou vidéo sont les suivantes :

2.5.1. Gestion des droits numériques : La gestion des droits numériques, en anglais c'est « DRM, Digital Rights Management » peut être définie comme « la description, l'identification, la négociation, la protection, la surveillance et le suivi de toutes les formes d'usages». Elle concerne la gestion des droits numériques et le respect des droits numériques [3] [9].

2.5.2. L'authentification : L'authentification dans le tatouage numérique ne doit pas être confondue avec l'authentification de la cryptographie. Tandis que l'authentification en cryptographie désigne la vérification d'un message d'origine ou prouvant l'identité d'une personne, l'authentification dans le tatouage numérique se réfère à l'assurance de l'intégrité de l'image. Une image est dite authentique si elle n'a pas été modifiée. L'idée de base de cette application consiste à insérer une marque fragile dans une image qui sert à alerter l'utilisateur face à une éventuelle modification de l'image et localiser les zones manipulées [3] [9].

2.5.3. Protection de copyright : La protection de copyright est une application importante de tatouage numérique. Elle permet l'identification du teneur de droits d'auteurs et les protèges ainsi dans la distribution du contenu. Les marques robustes sont intégrées dans une image afin de protéger les droits du propriétaire. Il devrait être possible de détecter la marque en dépit de traitement d'image commun, les distorsions

géométriques, de compression d'images, et de nombreux autres types de manipulations d'images. Par conséquent, le retrait volontaire de la marque robuste devrait se traduire par une dégradation sévère de l'aspect visuel de l'image. La détection réussite de la marque peut identifier avec certitude le propriétaire [3] [9].

2.6. Application du tatouage au système de traçage des copies pirates

L'application qui peut nous servir d'exemple sur le tatouage numérique au système de traçage des copies pirates est la vidéo à la demande sur Internet (VoD : L'abréviation de « Vidéo on Demand »), le concept est simple, un serveur distribue des copies à un certains nombre d'utilisateurs (disant « n » utilisateurs), parmi eux se trouve des personnes malhonnêtes qui les utilisent à des fin malveillants (vente, redistribution, etc.) . Les propriétaires du document en question veulent connaitre l'identité des coupables. Pour se faire, un identifiant unique qui permet de tracer la source des copies pirates, ayant pour forme une séquence de « m » bits est cachée, enfouie dans chaque vidéo d'une manière imperceptible en utilisant une technique de tatouage robuste. Ayant comme résultat n documents perceptiblement conforment mais totalement différents. Si un utilisateur s'accapare du document et l'utilise à des fins malhonnêtes, il sera tracé grâce à l'identifiant tatoué dans le document qui le désignera comme étant le coupable, car l'identifiant est unique et propre à chaque utilisateur.

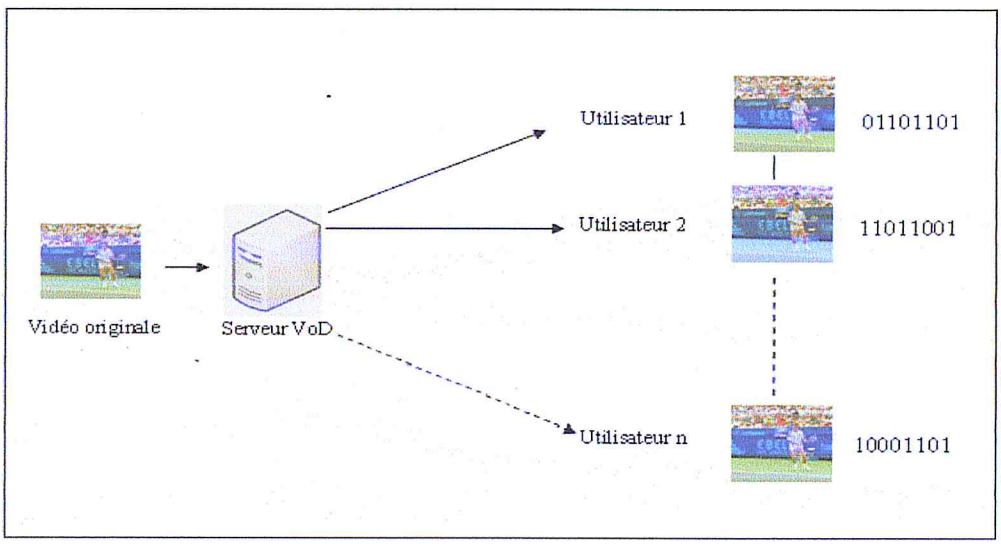


Figure 1.7 : Attribution et distribution de vidéo à l'aide d'un serveur VoD

La problématique rencontrée est celle ou plusieurs pirates sont présents et décident de s'allier à fin de créer une copie ayant un nouvel identifiant en mélangent celles qui leurs ont été adressées.

2.7. Les attaques

Les attaques, le plus souvent sont des traitements classiques qu'une personne effectue mais pas forcement en ayant des objectifs malveillants. Ils peuvent aussi être des traitements visant soit à brouiller soit à enlever la marque qui sers de protection de la vidéo. Les attaques peuvent être classifiées en deux familles, les attaques bienveillantes et les malveillantes [3].

- **Attaques bienveillantes :** C'est les traitements qui, initialement n'ont pas pour but et objectif d'empêcher la détection de la marque ou de provoquer sa destruction. Il peut s'agir des dégradations dues à une compression, à des filtrages (réduction de bruit), à un changement de résolution, au type de codage (progressif ou entrelacé). Un autre traitement couramment utilisé en vidéo est la conversion analogique/numérique, et inversement. Enfin, certaines distorsions géométriques peuvent être utilisées : flip vertical (couramment utilisé pour rendre les publicités non reconnaissable dans une séquence), cropping, perte d'une ligne ou d'une colonne, etc.

- **Attaques malveillantes :** De nombreuses attaques initialement développées pout l'image fixe peuvent être facilement adaptées à la vidéo puisque celle-ci ce n'est qu'une succession d'images. Elles ont pour objectif de rendre le tatouage inopérant, c'est le but principal des attaques malveillantes. Toutefois, une attaque malveillante qui a accompli sa mission devra produire un contenu à la fois privé de sa protection (la marque) et son exploitation est toujours possible.

Conclusion

Dans ce chapitre, nous avons introduit le tatouage numérique avec quelques notions de base, son principe, ses propriétés, différentes applications ainsi que quelques attaques.

Dans le prochain chapitre, nous aborderons l'application de traçage de traître en général et les différents codes anti-collusion utilisés.

Chapitre II : Traçage des copies pirates

1. Introduction

Avec le développement rapide de la technologie et l'utilisation croissante de l'outil Internet et la diffusion payante, impliquant ainsi l'apparition de la télévision numérique ou par satellite, la transmission vidéo par Internet, les lecteurs DVD etc…, ce qui a contraint le fournisseur à assurer la sécurité et la protection de ces fichiers ce qui, dans le cas contraire, posera un énorme problème à la gestion des droits d'auteurs. Cependant, l'utilisation d'une technique de transmission de fichiers codés à un certain nombre d'utilisateurs par le biais d'un canal de transmission public s'est avéré assez limité, car, si un utilisateur malveillant diffuse une copie d'une manière illégal, on sera en mesure de remonter à lui, mais, s'il décide de s'allier avec d'autres utilisateurs du même document pour forger une copie contenant un identifiant qui ne correspond à personne, sa serait difficile voir impossible de remonter aux utilisateurs coupables. Le traçage des copies pirates de ces utilisateurs(Fingerprinting) est une solution à cette problématique.

Dans ce chapitre, nous allons introduire la notion des systèmes de traçage de copies pirates, parler de l'attaque par collision, en suite, donner un aperçu d'une solution de traçage des copies pirates proposer par la communauté statistique.

2. Traçage des copies pirates

Le traçage de traitre existe depuis longtemps. Il y a plus d'un siècle, le cœur de métier de certaines sociétés était de vendre des tables de valeurs mathématiques ou physiques de 'grande précision', telle que les tables logarithmes, on en codait le nom des clients qui avait acheté la table. Exemple, un tatouage numérique personnalise les screeners qui sont des DVD de films récents voire pas encore sortis en salle, envoyés aux critiques professionnels ou aux membres de jurys tel celui de la cérémonie des Oscars [1]. En 2004, après enquête du FBI, la détection d'un tatouage a permis de condamner l'acteur Carmine Caridi, connu pour son rôle dans Le Parrain (Un film ayant marqué le septième art) à une amande de 600000 dollars après que son complice ai copié le contenu d'une soixantaine de screeners de Caridi pour les diffuser d'une manière illégale [1].

L'exemple précédent montre l'efficacité à tracer les coupables en appliquant la technique de traçage des copies pirates.

2.1. Définition du traçage des copies pirates

Traçage des copies pirates ou Fingerprinting est une technique destinée à tracer des copies d'un contenu en insérant un identifiant propre et unique à chaque utilisateur pouvant ainsi détecter et identifier les utilisateurs malhonnêtes.

Afin de mieux comprendre l'utilité des systèmes de traçage des copies pirates, il faut connaitre l'une des causes qui a amené à vouloir résoudre ce problème, l'attaque par collision [10].

La collision est une stratégie d'attaque connue depuis un certain temps déjà en cryptographie [10]: un groupe d'utilisateurs malveillants se rassemblent et mettent en commun ses informations ou connaissances sur le système de protection, quelles qu'elles soient pour générer des données non protégées. Ce type de comportement a été mentionné pour la première fois lors de la mise au point de protocoles pour diviser un secret entre plusieurs individus sans qu'aucun d'entre eux n'ait accès à l'ensemble du secret [11]. Un exemple typique est le partage de secret pour contrôler des actions critiques telles que l'ouverture de la porte d'un coffre fort particulier à la banque. Le client et le responsable de la banque ont tous les deux clés et les deux sont nécessaires pour ouvrir le coffre. Si une partie du secret (clé) manque, la porte du coffre reste fermée. A plus grande échelle, plusieurs clés contenant une partie du secret sont distribuées et il est nécessaire de rassembler au moins « k » clés différentes pour avoir accès à l'intégrité du secret. Dans ce contexte, les attaquants sont un groupe de « u » utilisateurs qui cherchent à construire de fausses clés ou à reconstruire l'intégralité du secret quand bien même « $u < k$ ». On retrouve aussi cette problématique de la collusion dans des schémas de distribution dynamique de clés [12] pour les sessions d'audio/vidéo conférences, vidéo à la demande, etc.

La figure 2.1 montre le rassemblement des utilisateurs malhonnêtes afin d'unir leur copies tatoués pour produire des documents ne contenant plus aucun tatouage.

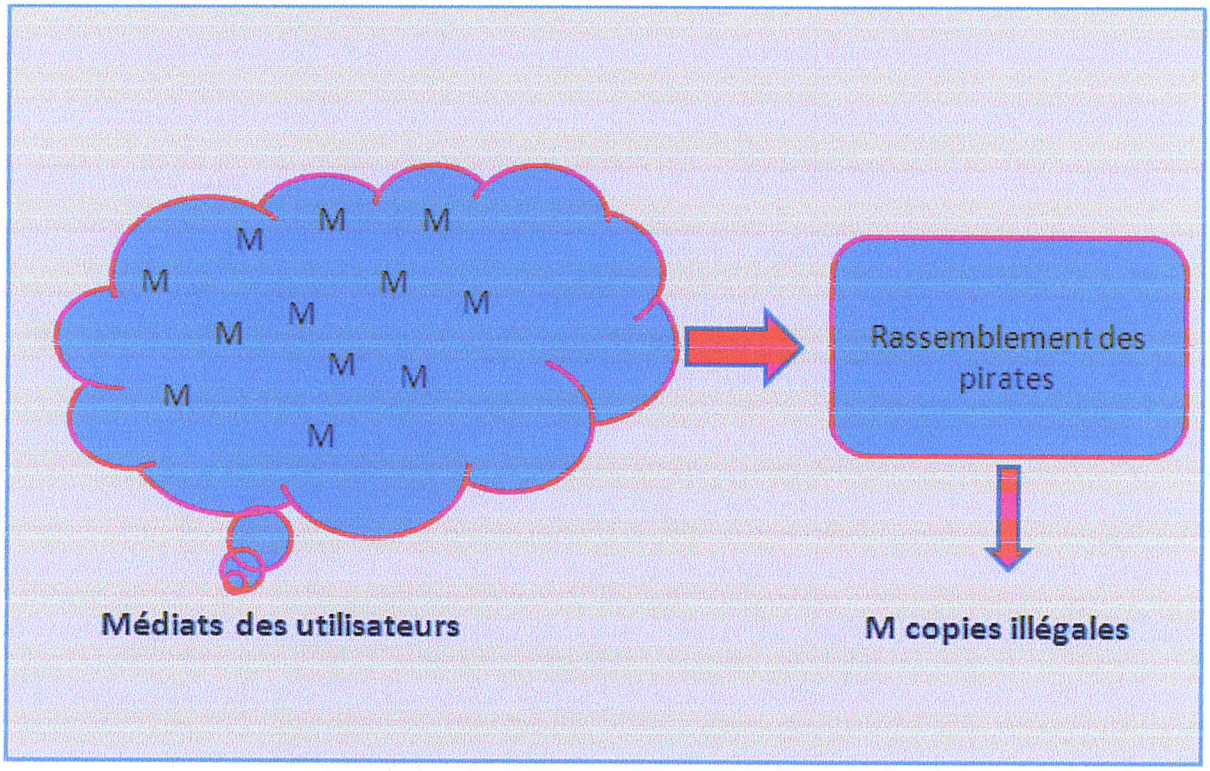


Figure 2.1 : Principe de l'attaque par Collusion

En tatouage numérique, les attaques par collision ont été évoquées pour la premières fois dans le contexte du suivi de copies [13]. Dans ce type d'application, les fournisseurs de contenus veulent distribuer un faible nombre de contenus à une très large audience. Ils désirent par conséquent avoir les moyens de pister une copie pirate jusqu'à la personne à l'origine de cette fuite. Dans ce but, au lieu de distribuer exactement le même film à tous les consommateurs, des copies sensiblement différentes sont assignées à chacun d'entre eux. Ainsi, chaque consommateur obtient une copie unique portant un identifiant qui lui est propre. Si un utilisateur isolé rend sa copie disponible sur Internet, il est alors possible de l'identifier en utilisant le tatouage. Face à cette menace, les attaquants sont tentés de se regrouper pour combiner leurs différentes copies et générer ainsi un nouveau document qui ne contiendrait plus de tatouage comme illustré dans la figure 2.1. Il existe principalement deux stratégies de collusion en tatouage :

- Soit les documents sont analysés pour estimer certaines propriétés du signal de tatouage qui pourraient être utilisées dans un second temps pour retirer le signal de tatouage ;
- Soit les documents sont combinés pour estimer directement le document original non tatoué.

Des parades ont déjà été proposées dans la littérature. Par exemple, des codes ayant certaines propriétés assurent que lorsque des documents tatoués sont combinés, certaines parties du tatouage demeurent inchangées [14]. Ces parties résiduelles sont alors examinées pour isoler et identifier de façon certaine au moins un des individus dans le groupe des attaquants.

2.2. Code anti collusion pour le traçage des copies pirates

- **Le code correcteur d'erreurs :** Le théorème le plus connu en traçabilité forte fait le lien entre le traçage de traitres et la théorie des codes correcteurs d'erreurs [15] : si « X » est un code correcteur d'erreurs (« n » mots de code de longueur « m »), de distance minimale « $d > m\,(1 - c^{-2})$ » alors « X » est un code c-traceable.

  Considérons le mot de code « x » d'un traitre donné. En mélangeant leurs mots de code, les utilisateurs forment une séquence pirate « y » qui peut être vue comme « x+e », c'est-à-dire le mot de code du traitre plus des erreurs. L'algorithme de décodage du code correcteur d'erreur enlèvera les erreurs et retrouvera le mot de code « x » du traitre. Si les traitres partagent les risques, un symbole sur « c » provient de « x », et il y a au plus « $m\,(1 - c^{-1})$ » erreurs. La condition sur la distance minimale assure qu'aucun innocent est plus proche de « y ». Cependant, décoder autant d'erreurs n'est pas à la portée de tous les codes correcteurs. Il faut employer des codes extrêmement redondants ou des concaténations de codes produisant des mots de code très longs. Si le théorème ci-dessus stipule que des codes correcteurs d'erreurs sont utiles en traçage de traitres, l'analogie avec un canal de transmission bruité n'est pas très convaincante et indique que ce n'est pas vraiment le meilleur outil [1].

- **L'approche statistique :** Devant l'importante complexité des codes à forte traçabilité, les cryptographes ont toléré des erreurs d'accusation. C'est la traçabilité faible. On distingue deux types d'erreurs [1]:

  - La probabilité « ε_1 » d'accuser des innocents à tort,
  - La probabilité « ε_2 » de rater des pirates.

  Le code est utile si on sait borner ces erreurs, et si les bornes sont très faibles.

  « ε_1 » est la probabilité la plus critique, typiquement de l'ordre de 10^{-6}. «ε_2 » est beaucoup plus grande, de l'ordre de 10^{-1} car on tolère que de temps en temps les

traitres nous échappent. Pour comparer deux codes, l'habitude est de travailler à une taille de collusion donnée « c », d'imposer les probabilités « ε_1 » et « ε_2 » et de comparer les longueurs « m » des mots de code nécessaire pour atteindre ce niveau de performance. Le meilleur code a la plus petite longueur.

- **Le code de Tardos :** Les codes de Tardos appartiennent aux codes à traçabilité faible. Ce sont des codes probabilistes. Il n'existe pas d'encodeur, et non plus de décodeur de ces codes. La génération de mots avec les mêmes paramètres peut donner des codes différents. Ces codes, contrairement aux codes correcteurs d'erreurs, ont été construits spécifiquement pour le Fingerprinting et atteignent la borne de longueur minimal ($m=O(c^2\log(1/\varepsilon_1))$) [16] [17]. La phase dite de décodage, qui n'en est pas vraiment une, ne donne pas en sortie un mot de code. Elle prend un mot du code en entrée avec le mot à décoder, et sort un score qui correspond à une mesure de l'implication de l'utilisateur concerné dans la création du mot à décoder. La figure 2.2 illustre cette différence.

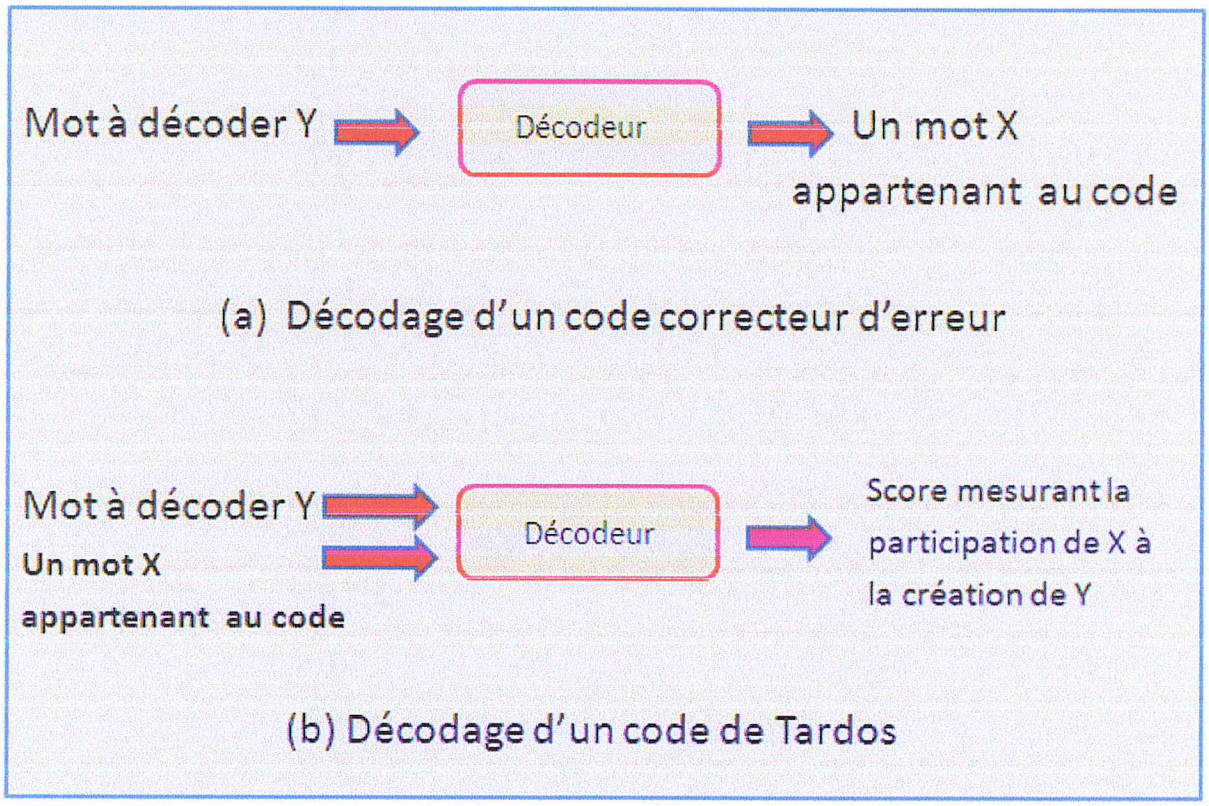


Figure 2.2 : Fonctionnement différent de la phase d'accusation selon l'utilisation d'un Code correcteur d'erreurs ou d'un code de Tardos.

➢ **Les codes présentés par Tardos [16] [17] [18]:** Dans la version proposée en 2003 par Gabor Tardos dans [18], les paramètres utilisées sont les suivants : « c » est le nombre de colluders, « $0 < \varepsilon_1 < 1$ et $k = [\log (1/ \varepsilon_1)]$, ε_1 étant la probabilité de fausse alarme, soit la probabilité d'accuser un utilisateur innocent. La longueur « m » dépend du nombre de colluders

$$m = 100\ c^2\ k = 100\ c^2 \log(\tfrac{1}{\varepsilon}) \qquad (2.1)$$

Soit « n », le nombre total d'utilisateurs.

Les mots de code distribués forment une matrice « n x m » binaire X. L'utilisateur « j » se voit associé le mot binaire $X_j = (X_{j1}, X_{j2}, \ldots X_{jm})$.

Initialisation : Pour générer cette matrice, « m » réels « $p_i \in [t, 1-t]$ » sont distribués indépendamment selon la façon suivante :

$$p_i = \sin^2 r_i \qquad (2.2)$$

Avec la valeur « r_i » prise uniformément dans l'intervalle $r_i \in [t', \pi/2-t']$ avec « $0< t'< \pi/4$ ».

$$\sin^2 t' = t \qquad (2.3)$$

On note $p= (p_1, \ldots, p_m)$.

Construction : Chaque élément de la matrice X est ensuite indépendamment tiré en suivant la probabilité « $P(X_{ji} = 1) = p_i$ ».

Chacun de ces « n » mots de code est caché dans la copie délivrée à l'utilisateur associé comme expliqué dans l'introduction.

	p_1	p_2	p_3	$\ldots$	p_m
X_1	1	0	1	$\ldots$	0
X_2	0	1	0	$\ldots$	1
X_3	1	1	0	$\ldots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
X_n	0	0	0	$\ldots$	1

Figure 2.3 : Construction des mots de code de Tardos

Les valeurs des différents paramètres ont été discutées dans différents articles. Une particularité du code de Tardos est que la distribution des scores (moyenne et variance) est la même quelque soit la stratégie utilisée par les colluders pour fabriquer la copie pirate.

La fonction de distribution est donnée sous la forme suivante :

$$\mathbf{f(p) : [t, 1\text{-}t] \rightarrow \mathbb{R}^{+}} \quad f(p) = \frac{1}{(2 \arcsin(1-2t)\, \pi \sqrt{p(1-p)})} \tag{2.4}$$

Cette fonction est symétrique par rapport à 0.5 et de telle sorte qu'il y a beaucoup de valeurs proches de 0 et de 1. On peut voir la fonction « f » sur la Figure 2.4.

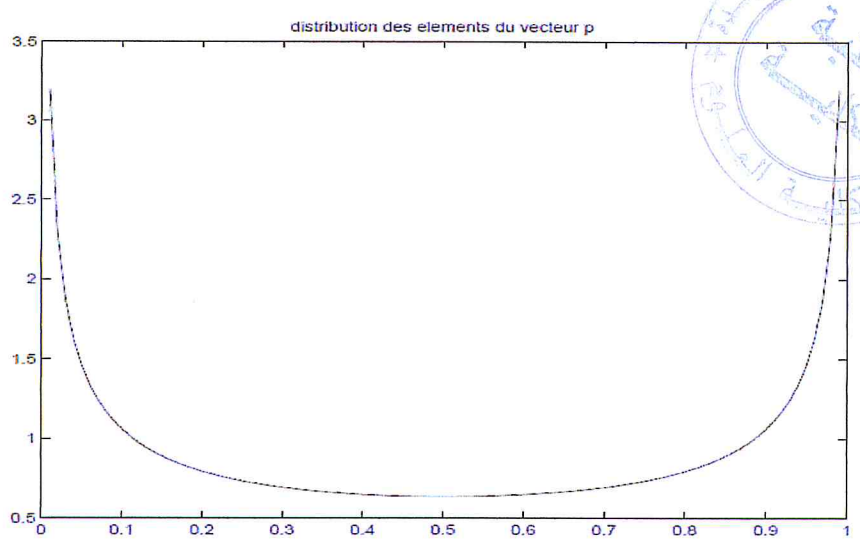


Figure 2.4 : Tracé de la fonction « f » représentant la distribution des probabilités

Accusation : On extrait la séquence « Y » de la copie pirate. Afin de savoir si l'utilisateur « j »est impliqué dans la production de la contrefaçon, on calcule un score d'accusation « S_j ». Si ce score est supérieur à un certain seuil « Z », alors on considère l'utilisateur « j » comme coupable. Une variante est d'accuser l'utilisateur le plus probablement coupable, ie, celui qui a le plus gros score. Le calcul des scores repose sur deux fonctions d'accusation, qui évaluent la corrélation entre la séquence « X_j », associée à l'utilisateur « j », et la séquence extraite « Y » :

$$S_j = \sum_{i=1}^{m} yi \,.\, U(Xji, pi) \tag{2.5}$$

Avec : X_{ji} qui représente le code de l'utilisateur j et Y_i représente le code de la vidéo pirate.

Nous notons $g_{yixi}(p_i)$ les fonctions U_{ji}. (Les scores d'accusation de B.Skoric)

$$U_{ji} = g_{10}(p_i) = -\sqrt{pi/(1-pi)} \quad \text{si } X_{ji} = 0 \tag{2.6}$$

$$U_{ji} = g_{11}(p_i) = \sqrt{(1-pi)/pi} \quad \text{si } X_{ji} = 1 \tag{2.7}$$

L'utilisateur « j » est accusé si « $S_j > Z$ », avec

$$Z = 20\ c\ k = 20\ c\ (\log(\tfrac{1}{\varepsilon})) \tag{2.8}$$

- **Code de Tardos Amélioré :** Tardos amélioré suit les mêmes étapes que ceux proposées par G. Tardos sauf une amélioration au niveau de l'accusation, précisément, au niveau du calcul des scores d'accusation.

  Voici la nouvelle formule du score d'accusation [19] :

$$S_j = \sum_{i=1}^{m} yi\ .\ U(Yi, Xji, pi) \tag{2.9}$$

Avec

Les fonctions d'accusation :

$$U(1,1,p) = g_{11}(p)\ ; \qquad U(0,0,p) = g_{00}(p) \tag{2.10}$$

$$U(1,0,p) = g_{10}(p)\ ; \qquad U(0,1,p) = g_{01}(p) \tag{2.11}$$

$$g_{11}(p) = g_{00}(1-p) = -g_{01}(p) = -g_{10}(1-p) = \sqrt{(1-pi)/pi} \tag{2.12}$$

Conclusion

Dans ce chapitre, nous avons défini le traçage des copies pirates et le code anti collusion de Tardos.

Le prochain chapitre parlera du modèle psycho-visuel JND (Just Noticeable Difference).

Chapitre III : L'apport du modèle psycho visuel dans le Watermarking

1. Introduction

Différentes études du système visuel humain ont été menées. Les objectifs principaux étaient la modélisation du SVH pour la visualisation des images en niveaux de gris, le codage d'images ou encore l'étude des dégradations et l'évaluation de la qualité. L'utilisation du modèle psycho-visuel dans une application de codage d'images visait à supprimer une certaine quantité d'information de l'image. L'adaptation du modèle visuel dans une application de tatouage se fait non pas par la recherche de l'information susceptible d'être supprimée, mais plutôt par la recherche du seuil de visibilité. L'obtention de ce seuil de perception permet d'optimiser conjointement les processus d'insertion et de détection de la marque en obtenant le meilleur compromis entre l'invisibilité et la robustesse de la marque. Un des principaux avantages de l'utilisation d'un modèle psycho-visuel pour le tatouage des images réside dans le fait que l'invisibilité de la marque est garantie sans toutefois devoir passer par des tests contraignants d'évaluation de la qualité des images tatouées

Parmi les modèles perceptuels utilisés dans le tatouage numérique, le JND (JND : Just Noticeable Difference) est le plus répondu, il vise à calculer un seuil qui permet de déterminer la quantité maximum de distorsion qu'il est possible d'introduire, sans que cela soit perceptuellement visible.

2. Le modèle JND

2.1. Définition : Le JND (Just Noticeable Difference) ou l'appellation en français est le seuil différentiel, est un concept de la psychophysique qui définit la limite en dessous de laquelle un individu ne parvient plus à différencier deux stimulations [20]. Le JND compte pour la plus petite différence détectable entre un regardant et le niveau secondaire d'un stimulus sensoriel particulier en psychophysique, qui est également connu sous le nom de limen de différence. Le modèle JND a donné une voie prometteuse pour modéliser la propriété de HVS (Système Visuel Humain) avec précision et efficacité à l'image de bon nombre de domaine de traitement d'images, telles que la compression d'image perceptive, l'évaluation de la qualité d'image, le tatouage ...

Le JND se base sur la psychophysique qui est une branche de la psychologie expérimentale qui cherche à déterminer les relations quantitatives qui existent entre un stimulus physique et la perception qu'on en a. La psychophysique s'intéresse aux sens physiologiques tels que la vue, l'ouïe, le toucher mais aussi à des sensations comme la perception du temps ou du mouvement [SW1].

2.2. Le JND basé sur la DCT 8x8 (Modèle de Watson)

Une des méthodes de calcul d'un masque perceptuel pour guider le marquage d'un bloc DCT de l'image est inspiré des travaux de Watson et est communément appelée le masque JND de Watson. Dans le domaine des études psycho-physiques, l'unité JND se définit comme étant le niveau de distorsion qui peut être perçu dans 50% des cas d'essais ou tests expérimentaux. Le modèle perceptuel de Watson tente d'incorporer des caractéristiques du système visuel humain dans la mesure perceptuelle de la distorsion tolérée par l'image. Trois caractéristiques du HVS sont prises en compte : la sensitivité fréquentielle, le masquage de la luminance et le masquage du contraste [21].

La sensitivité fréquentielle du HVS : le système visuel humain est très sensible aux changements dans les composantes fréquentielles basses et médianes de l'image. Watson définit une table de sensitivité fréquentielle t de taille 8x8 en lien avec les composantes fréquentielles des blocs DCT 8×8 de l'image (voir le Tableau 1). Chaque élément t(i,j) correspond au coefficient DCT B(i,j) et définit l'amplitude du changement qui produit une distorsion d'un JND dans l'image. Par exemple, t(0,1)=1.01 signifie que toute variation du coefficient B(0,1) dépassant l'amplitude 1.01 va provoquer une distorsion supérieure à un JND dans l'image. En observant la table t, on peut constater que les composantes fréquentielles basses et médianes ont des petites valeurs t(i,j), ce qui signifie que les changements dans ces composantes vont avoir un grand impact sur la quantité de distorsion perçue dans l'image [21].

Tableau 3.1 : La table de sensitivité fréquentielle *t* définie par Watson

1.40	1.01	1.16	1.66	2.40	3.43	4.79	6.56
1.01	1.45	1.32	1.52	2.00	2.71	3.67	4.93
1.16	1.45	2.24	2.59	2.98	3.64	4.60	5.88
1.66	1.52	2.59	3.77	4.55	5.30	6.28	7.60
2.40	2.00	2.98	4.55	6.15	7.46	8.71	10.17
3.43	2.71	3.64	5.30	7.46	9.62	11.58	13.51
4.79	3.67	4.60	6.28	8.71	11.58	14.50	17.29
6.56	4.93	5.88	7.60	10.17	13.51	17.29	21.15

- Le masquage de la luminance : Si l'intensité moyenne du bloc image considéré est très élevée, cette région sera alors capable d'absorber de plus grandes variations car une brillance élevée procure un effet de masquage des changements subis. Le bloc DCT correspondant peut alors subir des changements plus importants que ce qui est prévu dans

la table *t* sans être perceptibles. Pour tenir compte de ce phénomène, la table de sensitivité est alors ajustée pour donner lieu à un masque de luminance t_L défini sur toute l'image comme suit [21] : $T_L(i,j,k) = t(i,j) * \left(\frac{B(0,0,k)}{B_{0,0}}\right)^{aT}$ (3.1)

k étant le numéro du bloc 8×8, $B(0,0,k)$ le coefficient DC du *kième* bloc, $B_{0,0}$ la moyenne de tous les coefficients DC de tous les blocs de l'image et a_T une constante valant *0.649*.

- Le masquage du contraste: lorsqu'une composante fréquentielle a une énergie élevée, ceci a pour effet de réduire la visibilité d'un changement sur cette composante. La prise en compte de ce type de masquage donne lieu à un masque de seuils comme suit :

$$S(i,j,k) = \max\{t_L(i,j,k), |B(i,j,k)|^w t_L(i,j,k)^{1-w}\} \quad (3.2)$$

Où w est une constante qui vaut 0.7. Notons que chaque s(i,j,k) réfère à un seuil de variation que peut subir tout coefficient DCT individuel B(i,j,k) avant d'atteindre une distorsion visible d'un JND.

2.3. JND 16x16

Le JND 16x16 est venu comme extension au JND 8x8, il est destiné au bloc de taille 16x16, et gardant toujours les mêmes principes avec quelques différences [20].

Sa formule se base sur celle du JND 8x8 à la différence avec la taille du bloc 16x16.

$$T(k,n,i,j) = T_{basic}(k,n,i,j) \cdot F_{lum}(k,n) \cdot F_{contrast}(k,n,i,j) \quad (3.3)$$

Avec le $T_{BASIC}(k,n,i,j)$ qui est le seuil de base généré par le contraste spatial en fonction de la sensibilité (CSF Contrast Sensitivity Function).

$$T_{basic}(k,n,i,j) = \left(\frac{S}{\Phi i\, \Phi j}\right)\left(\frac{e^{c\omega ij}/e^{a+b\omega ij}}{\gamma+(1-\gamma)\cos^2 \Phi ij}\right) \quad (3.4)$$

Pour le JND 16x16 nous avons les constantes a, b et c prédéfinies [20]: a=1.88, b=0.165, c=0.16, s=0.25, et $\phi i, \phi j$ sont les facteurs de normalisation des pixels:

$$\Phi_m = \sqrt{1/N} \text{ si } m=0 \quad \text{où} \quad \sqrt{2/N} \text{ si } m>0 \quad \text{avec } N=4. \quad (3.5)$$

$$\varphi_{ij} = \arcsin\left(2 \cdot \omega i, 0\omega / \omega^2 ij\right) \quad (3.6)$$

$$\omega_{ij} = (1/2N)\left(\sqrt{((i/\theta x)^2 + (j/\theta y)^2)}\right) \quad (3.7)$$

$$\theta_x = \theta_y = 2 \arctan\left(1/(2 \times Rvd \times Ih)\right) \quad (3.8)$$

Θ_x et Θ_y sont les angles visuels horizontals et verticals respectivement. Où Rd indique le ratio de la distance de la hauteur de l'image, et Ph est la hauteur de l'image (en pixel).

$$F_{lum} = \begin{cases} (60 - Iave)/150 + 1 & si \quad Iave \leq 60 \\ 1 & si \quad 60 < Iave < 170 \\ (Iave - 170)/425 + 1 & si \quad Iave \geq 170 \end{cases} \quad (3.9)$$

- Iave est la moyenne de l'intensité des valeurs des contours dans un bloc (16x16).
- Classification selon la texture des blocs :

$$Block\_categ = \begin{cases} PLANE & si \quad \sum edge < 16 \\ EDGE & si \quad 16 \leq \sum edge \leq 52 \\ TEXTURE & si \quad \sum edge > 52 \end{cases} \quad (3.10)$$

- Avec $\sum edge$ (la densité des pixels appartenant au contour), est le nombre de position avec un contour supérieur à Iave [22].
- Le masque de contraste F_{cm} est calculé comme suit :

$$F_{contrast}(n,i,j) = \begin{cases} \Psi & si \quad (i^2 + j^2) \leq 2 \text{ dans les blocs smooth et edge} \\ \Psi . \left(\min\left(4, \max\left(1, (AC(n,i,j) / (T_{basic}(n,i,j) \times F_{lum}(n)))^{0.36}\right)\right)\right) & sinon \end{cases} \quad (3.11)$$

Avec

$$\Psi = \begin{cases} 1 & si \quad \text{pour les blocs smooth et edge} \\ 2.25 & si \quad \text{pour } (i^2 + j^2) \leq 2 \text{ pour les blocs texturés} \\ 1.25 & si \quad \text{pour } (i^2 + j^2) > 2 \text{ pour les blocs texturés} \end{cases} \quad (3.12)$$

Où AC (m,n,i,j) est la valeur du coefficient correspondant.

L'approche suivi pour calculer la densité de pixels appartenant au contours est l'approche Gradient. Son principe est comme suit :

- **Approche gradient:** pour la détermination des extrema locaux dans la direction du gradient.

Dans ce qui va suivre, considérons $I(x,y)$ une image:

Soit $G(x,y)$ le gradient de I au point (x,y) :

$$G(x,y) = (Ix(x,y),Iy(x,y)) \tag{3.13}$$

Soit D(I) le laplacien de I au point (x,y).

Dans les premières approches envisagées, l'extraction des points de contour s'effectue par sélection des points de norme de gradient élevée grâce aux deux étapes suivantes :

- **Calcul de la norme du gradient** : L'amplitude du gradient s'obtient alors par l'une des formules suivantes :

$$M(x,y)= \sqrt{(Gx(x,y)^2 + Gy(x,y)^2} \tag{3.14}$$

$$M(x,y)=|(Gx(x,y)+Gy(x,y)| \tag{3.15}$$

Conclusion

Dans ce chapitre, nous avons introduit la technique psycho-visuel JND définissant la limite en dessous de laquelle un individu ne parvient plus à différencier deux stimulations.

Dans le prochain chapitre, nous aborderons le traçage de traître à travers la proposition d'un système de tatouage intégré à H.264 et utilisant le code anti-collusion de Tardos et un modèle psycho-visuel JND pour contrôler la visibilité.

Chapitre IV : Implémentation Et Réalisation

Introduction

Dans les chapitres précédents, nous avons défini la technique de tatouage numérique (principe, concept, différentes applications ainsi que quelques attaques), le modèle psycho-visuel JND et les critères à respecter pour la l'application du traçage des copies.

Dans ce chapitre nous appliquons les connaissances acquises afin de développer une méthode permettant de sécuriser des vidéos H.264/AVC distribuées à la demande ou graver sur des supports tels que les DVD. Solution permettant de détecter les sources de redistribution illégales en utilisant le tatouage numérique robuste adaptative basée sur le modèle JND et comme code de traçabilité le code statistique de Tardos.

Un exemple d'application de tatouage numérique de la vidéo distribuée est le film Harry Potter 7 et les Reliques de la Mort qui est victime de son succès avec le téléchargement illégal proposé sur des serveurs de partage de fichiers comme Rapidshare, ou Megaupload, même dans les applications peer to peer qui sont souvent des fausses vidéos en streaming. Cependant, le vrai Harry Potter 7 épisode 1 de la Warner Bros dont les 36 premières minutes du film circule sur internet, possède un tatouage numérique. Cette empreinte numérique sur le film Harry Potter 7 permet à la Warner Bros d'identifier le pirate qui a partagé ce nouvel épisode d'Harry [SW2].

Mais avant de décrire les différents processus, nous introduirons quelques notions du standard H.264 qui représente le signal hôte dans le processus d'insertion.

La norme H.264/AVC

Le H.264 est une norme ouverte et sous licence compatible avec la plupart des techniques de compression disponible aujourd'hui. Un encodeur H.264 peut réduire la taille d'un fichier vidéo numérique de plus de 80% par rapport à la norme Motion JPEG et de 50% par rapport à la norme MPEG-4 Partie 2, sans que la qualité d'image ne soit compromise. Résultat : un fichier vidéo nécessite nettement moins d'espace de stockage et de bande passante sur le réseau. Ce qui le rend très utile pour les applications vidéo [25].

Principe du fonctionnement de la norme de compression H.264/AVC : [26] [27]

- **Phase encodage**

  La figure 4.1 illustre le fonctionnement de la phase encodage d'une vidéo via la norme H.264/AVC.

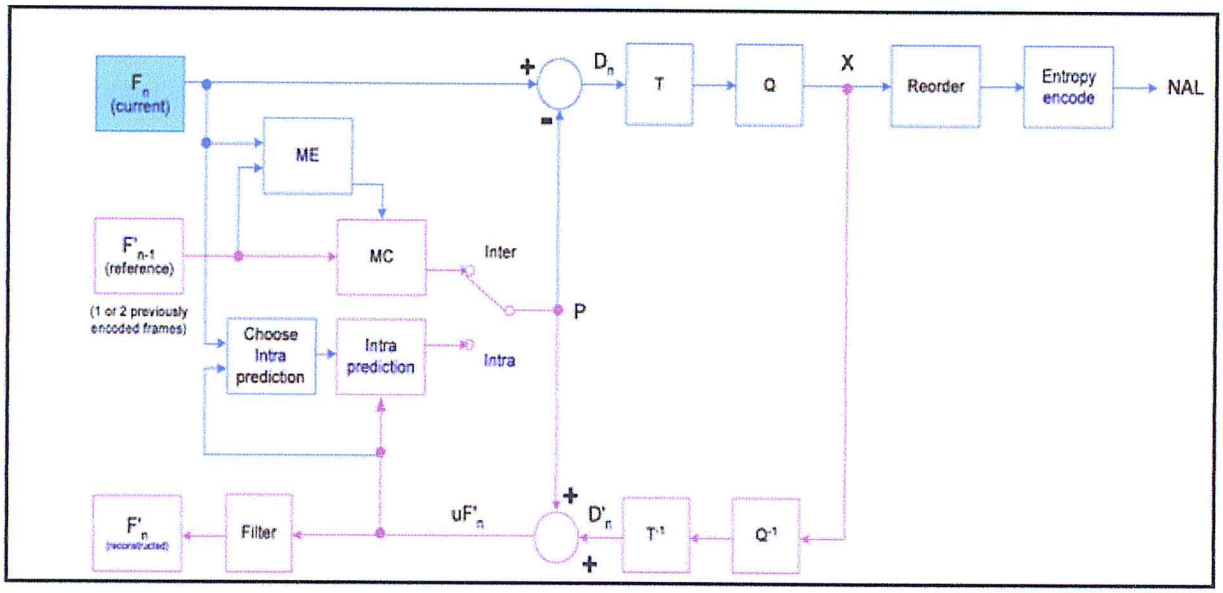


Figure 4.1 : Schéma d'encodage Vidéo via la norme H.264/AVC

L'image à l'entrée Fn du codeur est segmentée en blocs de pixels de taille 16x16 appelées macroblocs. Ces macroblocs sont alors prédits soit à l'aide de prédictions spatiales (Intra prédiction ou prédiction I) soit à l'aide de prédictions temporelles appelées aussi compensation de mouvement (MC) ou Inter prédiction (prédiction P).

Pour la première image, On ne peut pas utiliser la seconde méthode, seule la prédiction spatiale est possible dans la mesure où il n'y a pas d'autres images auxquelles se référer. Pour les autres images, les deux modes de prédictions pour chaque macrobloc peuvent être utilisés et on choisit le meilleur (Inter/Intra). A l'aide d'une DCT, le résiduel (Dn) résultant de cette prédiction subit une transformation (T) puis une quantification (Q) et codage à l'aide d'un codage entropique sans perte.

Notons aussi que ce résiduel est dé-quantifié (Q^{-1}) et dé-transformé (T^{-1}) afin de stocker l'image décodée uFn^{-1} pour l'utiliser lors du codage temporelle des prochaines images à coder. Afin de réduire les effets de bloc, uFn^{-1} est filtré par filtre de déblocage.

- **Phase décodage**

  Pour ce qui est du décodage, le même processus de codage est utilisé.

  Les macroblocs fournis par le NAL sont décodés et réarrangés pour obtenir les coefficients X à partir desquels sont obtenus les même D'n que le codeur. En utilisant les informations contenues dans le bitstream, le décodeur crée une prédiction P, l'ajoute à D'n et obtient uF'n. Après filtrage, l'image décodée F'n est retrouvée.

  La figure 4.2 montre le processus de décodage via la norme de compression H.264/AVC.

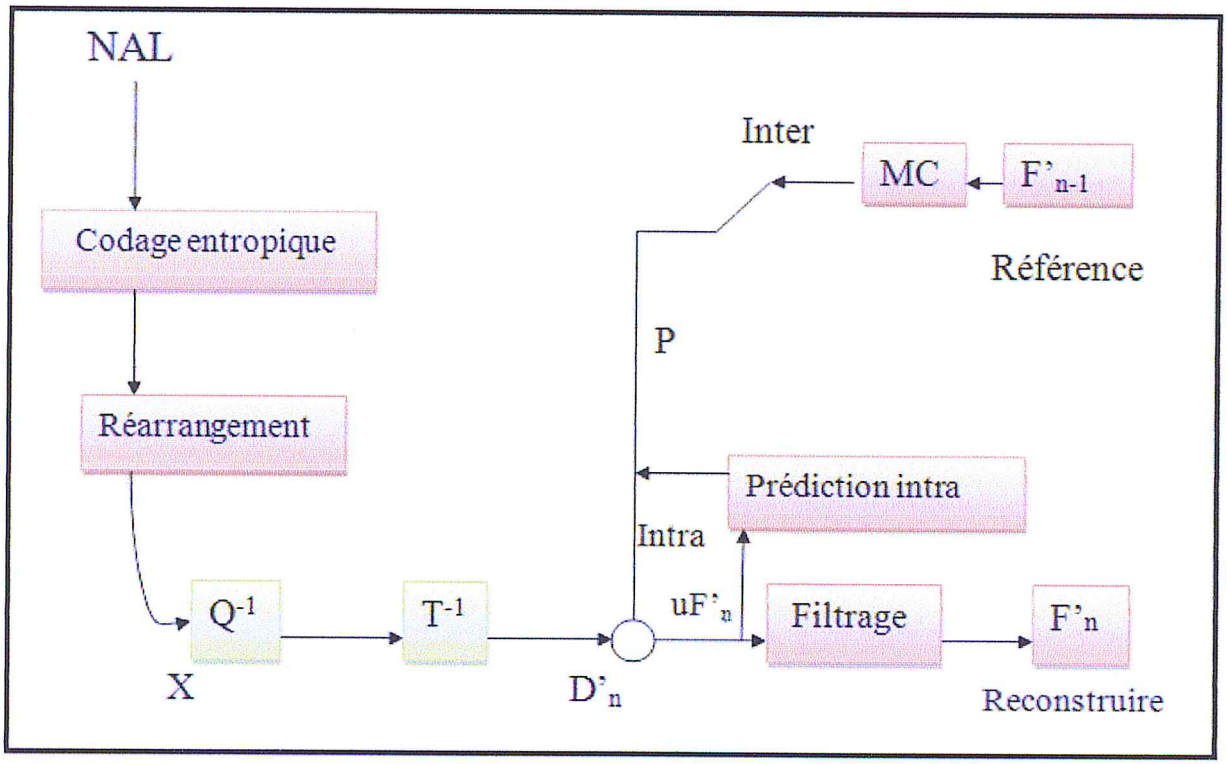


Figure 4.2 : Schéma de décodage vidéo via la norme H.264/AVC

- **Transformation et Quantification**

  La norme H.264/AVC spécifie les processus de transformation et de quantification qui sont conçus pour assurer de manière efficace le codage des données vidéo, afin d'éliminer tout décalage entre le codeur et le décodeur et minimiser la complexité des calculs [26].

- **Partitionnement d'une image en macrobloc**

Une image est segmentée en macroblocs, et ces macroblocs, selon leurs textures (images texturées ou homogènes) sont partitionnées en blocs (16x16, 8x8 et 4x4), la figure 4.3 montre les diverses partitions.

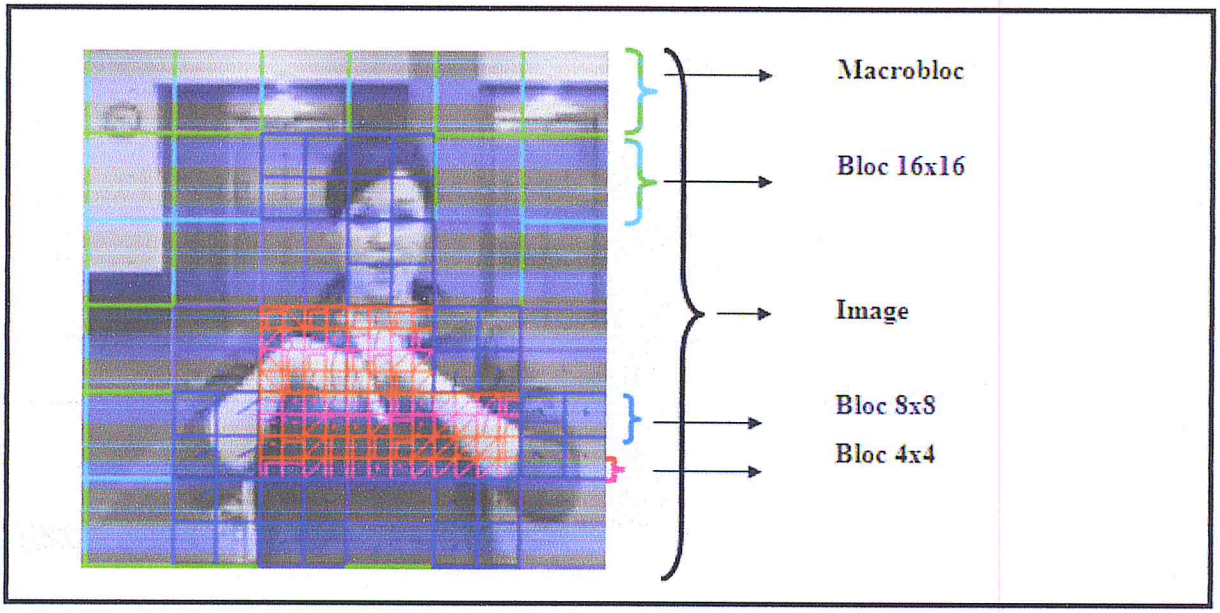


Figure 4.3: Partitionnement d'une image

1. **Etat de l'art de tatouage numérique pour le traçage des traîtres dans la norme H.264/AVC**

Différentes techniques de tatouage numérique ont été proposées pour la protection des vidéos compressées par la dernière norme de compression vidéo H.264/AVC. Mais pratiquement deux travaux ont été publiés dans la littérature pour l'application de traçage des copies des pirates dans la norme. La première a été publiée en 2010 par Shahid et al [35]. Ces derniers ont proposé une approche basée sur l'insertion du code de Tardos dans la vidéo au cours de processus de compression H.264/AVC. Plus précisément ce code est caché dans les coefficients transformés quantifiés selon une force de marquage fixe. La méthode a donné des résultats satisfaisants au point de vue détectabilité mais son inconvénient résidait dans la dégradation de qualité visuelle des vidéos tatouées. Pour remédier à cet inconvénient et limiter les distorsions d'insertion, Ait Saadi et al [6] ont proposé une méthode de tatouage adaptative basée sur les caractéristiques fréquentielles de la vidéo au cours de la compression. La marque était insérée dans les blocs de type intra_4x4 et inter_4x4 au niveau des coefficients continus DC. La méthode a amélioré la qualité visuelle des vidéos tatouées. Pour augmenter la robustesse et en même temps

garder la qualité de la vidéo taouée inchangée, dans ce mémoire nous proposant d'introduire un modèle psycho-visuel prenant en compte les caractéristiques spatiales et fréquentielles. Aussi pour augmenter le taux de détectabilité des pirates nous utiliserons le code anti-collusion amélioré de Tardos.

2. La solution proposée

La méthode proposée adopté un mécanisme d'insertion adaptative selon les étapes suivantes :

- Génération du code de Tardos.
- Insertion du code de Tardos.
- Extraction du code.
- Processus d'accusation.

2.1. Génération du code de Tardos

Afin d'identifier les utilisateurs et pour pouvoir les tracer en cas de présence d'individus malhonnêtes nous avons utilisé la version amélioré du code de Tardos (chap 3).

La longueur du code « m » est égal à

$$m = dm\, c^2 \log\left(\frac{1}{\varepsilon 1}\right) \qquad (4.1)$$

Avec « c » qui représente une estimation du nombre de pirate, ε_1 la probabilité d'accuser un innocent et dm qui est une constante définie par G. Tardos « dm=100 ».

2.2. Insertion du code de Tardos

L'insertion de la marque générée est faite pendant la compression après l'étape de quantification (figure 4.4). La marque est insérée dans les blocs de type intra_4x4 et au niveau des coefficients quantifiés AC (figure 4.5) en se basant sur les valeurs du JND pour contrôler la force de marquage.

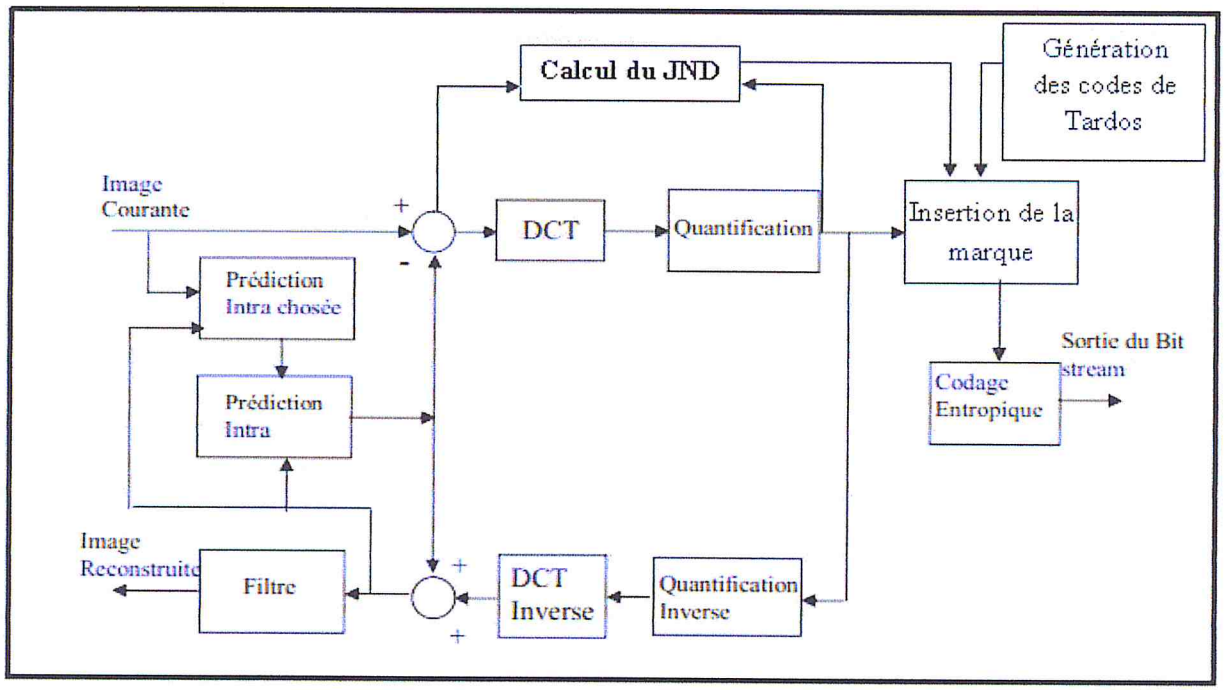


Figure 4.4 : Processus d'insertion de la marque avec le codeur H.264/AVC

DC	AC	AC	AC
AC	AC	AC	AC
AC	AC	AC	AC
AC	AC	AC	AC

Figure 4.5 : Les AC et les DC dans un bloc 4x4

- **Calcul de la force de marquage selon le JND**

  Nous avons utilisé le modèle JND basé sur les blocs de taille 4x4 [28] pour l'adapter aux blocs de type 4x4 du codeur. Le calcul de ce dernier se base sur les caractéristiques spatiales et fréquentielles. La figure 4.6 ci-dessous illustre le principe de calcul du modèle JND dans la norme H.264/AVC

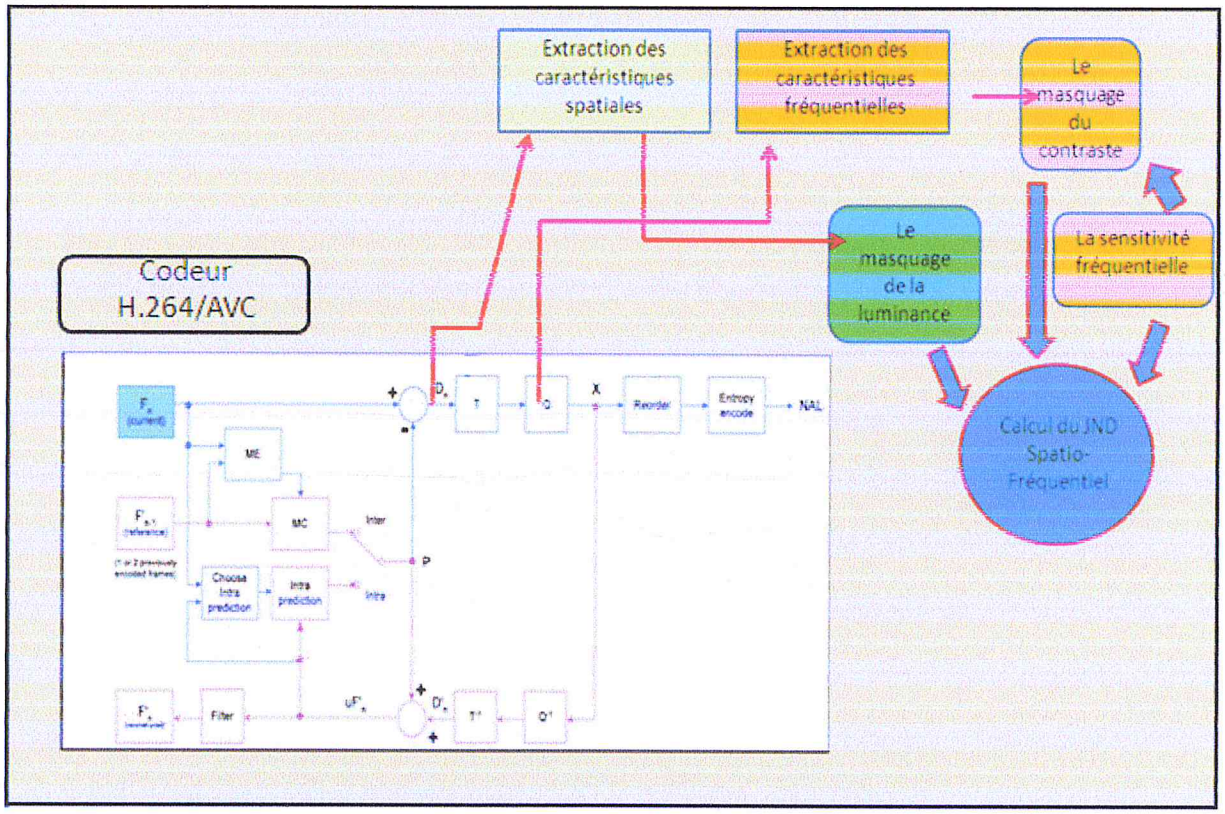


Figure 4.6 : Le schéma bloc du calcul du modèle JND dans la norme H.264/AVC

Le modèle JND spatio-fréquentiel se calcul en suivant les formules ci-dessous :

$$T_{JND}(k,n,i,j) = T_{BASIC}(k,n,i,j) \times F_M(k,n,i,j) \quad (4.2)$$

$$F_M(k,n,i,j) = F_{lum}(k,n) \times F_{contrast}(k,n,i,j) \quad (4.3)$$

Où k est le numéro de la trame dans les séquences vidéo, n est l'indice du bloc dans la k-iéme et i, j les indices des coefficients DCT dans un bloc de taille 4x4 avec $(0 \leq i \leq 3,\ 0 \leq j \leq 3)$.

$T_{JND}(k,n,i,j)$ est le seuil spatio-fréquentiel.

Le $T_{BASIC}(k,n,i,j)$ est le seuil de base généré par le contraste spatial en fonction de la sensibilité humaine au contraste (contrast sensivity function - CSF). Cette fonction permet de prendre en compte la sensibilité de l'oeil humain aux différentes fréquences spatiales pondérées par la fonction de sensibilité.

Le facteur de modulation $F_M(k,n,i,j)$ est un produit de la luminance $F_{lum}(k,n,i,j)$ et le contraste de masquage $F_{contrast}(k,n,i,j)$.

Le seuil de base $T_{BASIC}(k,n,i,j)$ est donné par la formule suivante :

$$T_{basic}(k,n,i,j) = \left(\frac{S}{\Phi i\, \Phi j}\right)\left(\frac{e^{c\omega ij}/_{e^{a+b\omega ij}}}{\gamma+(1-\gamma)\cos^2 \Phi ij}\right) \quad (4.4)$$

Où a = 1.33, b =0.11, c = 0.18, qui sont déterminés expérimentalement dans [29]

$$\Phi_m = \sqrt{1/N} \text{ si } m=0 \quad \text{où} \quad \sqrt{2/N} \text{ si } m > 0 \quad \text{avec } N = 4 \quad (4.5)$$

$$\omega_{ij} = \left(1/_{2N}\right)\left(\sqrt{((i/\theta x)^2 + (j/\theta y)^2)}\right) \quad (4.6)$$

$$\varphi_{ij} = \arcsin\left(2 \cdot \omega i, 0\omega /_{\omega^2 ij}\right) \quad (4.7)$$

$$\theta_x = \theta_y = 2 \arctan\left(1/_{(2 \text{ x Rvd x Ih})}\right) \quad (4.8)$$

$\phi i, \phi j$ sont les facteurs de normalisation des pixels.

Θ_x et Θ_y sont les angles visuels horizontal et vertical respectivement.

Avec I_h est la hauteur de l'image, et R_{vd} est le rapport entre la distance du lecteur et la hauteur de l'image.

Le facteur de luminance $F_{lum}(k,n)$ est le facteur d'adaptation de luminance relatif à la valeur de l'intensité moyenne du bloc :

$$F_{lum} = \begin{cases} 1+ [60 - I'(n,k)] / 150 & \text{si} \quad I'(n,k) \leq 60 \\ 1 & \text{si} \quad 60 < I'(n,k) < 170 \\ 1+ [I'(n,k) - 170] / 425 & \text{si} \quad I'(n,k) \geq 170 \end{cases} \quad (4.9)$$

Où I'(n,k) est l'intensité moyenne du n-ième bloc dans la k-ième image.

Le seuil de sensibilité au contraste détecte une variation de la luminance, vu comme une fonction dépendante de la luminance du fond. Ce seuil est calculé selon une classification du contenu des blocs de l'image. Pour cela, Les blocs DCT sont classifiés en trois types : Smooth (plane), edge (contour) et texture (bloc texturé) selon la formule suivante :

$$\text{Type Bloc} = \begin{cases} \text{Smooth} & \text{si} \quad \delta edge \leq \alpha \\ \text{Edge} & \text{si} \quad \alpha < \delta edge \leq \beta \\ \text{Texture} & \text{si} \quad \delta edge > \beta \end{cases} \quad (4.10)$$

$$\delta edge = \sum edge \,/_{N^2} \tag{4.11}$$

Avec δedge représente la densité des pixels appartenant aux contours et $\sum edge$ est l nombre de position avec un contour supérieur à Iave, α et β des constantes qui prennent les valeurs 0.1 et 0.2 respectivement. [30].

Le masque de contraste est donné comme suit :

$$F_{contrast}(n,i,j) = \begin{cases} \Psi & \text{si} \quad (i^2 + j^2) \leq 2 \text{ dans les blocs smooth et edge} \\ \Psi.\ \min\left(4, \max\left(1, \left(AC(n,i,j) / \left(T_{basic}(n,i,j) \times F_{lum}(n)\right)\right)^{0.36}\right)\right) & \text{sinon} \end{cases} \tag{4.12}$$

Avec

$$\Psi = \begin{cases} 1 & \text{si} \quad \text{pour les blocs smooth et edge} \\ 2.25 & \text{si} \quad \text{pour } (i^2 + j^2) \leq 2 \text{ pour les blocs texturés} \\ 1.25 & \text{si} \quad \text{pour } (i^2 + j^2) > 2 \text{ pour les blocs texturés} \end{cases} \tag{4.13}$$

Avec AC(n,i,j) est le coefficient DCT du n-iéme bloc.

Les conditions et restrictions d'insertion

Lors du choix des positions où se fait l'insertion, et pour éviter la détérioration de la vidéo, certaines restrictions sont appliquées :

- ✓ N'insérer que dans les blocs de type intra 4x4 (blocs – texturés). Dans un bloc homogène, c'est-à-dire les blocs de type Intra 16x16, la marque sera visible et la qualité d'image sera détériorée.
- ✓ Ne pas insérer si le coefficient tatoué est égal à « zéro » car la norme H.264 a une particularité, lors du décodage. Si le décodeur rencontre un coefficient nul, il mettra automatiquement les coefficients suivants à zéro ce qui provoquera la perte d'information (Marque sera incomplète lors de l'extraction).
- ✓ N'insérer que si le coefficient AC est supérieur ou égale au JND lui correspondant.

L'insertion

L'insertion est effectuée au cours de la compression selon le schéma suivant (figure 4.7).

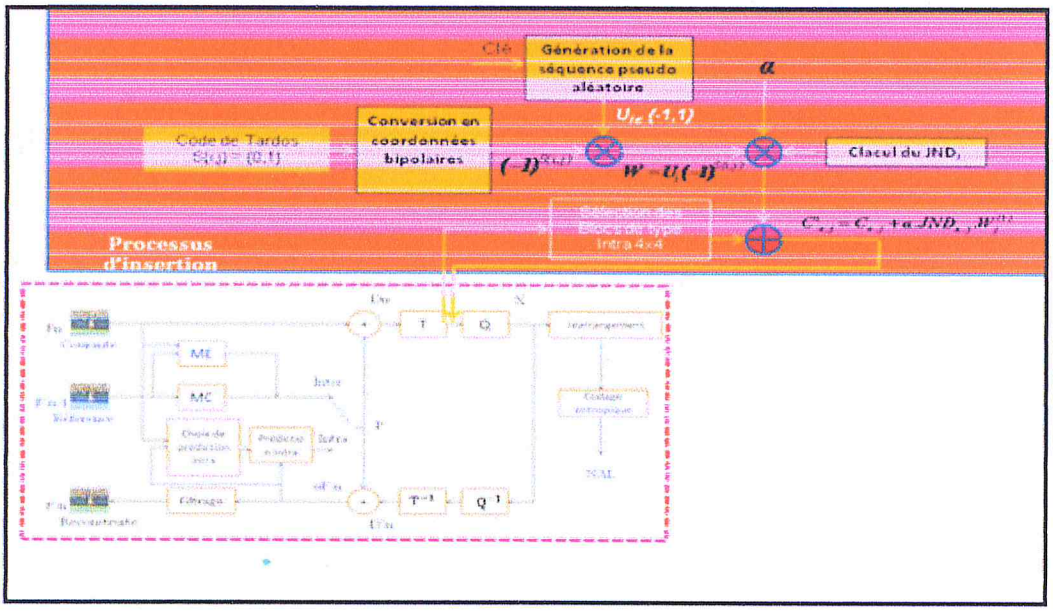


Figure 4.7 : Schéma synoptique d'insertion

Afin que notre tatouage soit robuste, nous avons choisi de répéter l'insertion du même bit dans tous les blocs d'un macrobloc en se basant sur les restrictions vues précédemment et la formule d'insertion suivante :

$$AC'(n,m,i,j) = AC(n,m,i,j) + \alpha \cdot JND(n,m,i,j) \cdot U_k \cdot W(r) \qquad (4.14)$$

Avec :

- (n,m) : Position du bloc dans le macrobloc.
- (i,j) : Position du AC dans le bloc.
- AC'() :Vecteur des coefficients AC tatoués.
- AC() : Vecteur des coefficients AC originaux.
- JND : Vecteur des valeurs du JND.
- U_k : La séquence gaussienne (clé).
- W(r) : est la marque bipolaire (-1,1).

Afin d'augmenter la sécurité d'insertion, le code de Tardos binaire (0,1) est converti en code bipolaire de valeur (-1, 1).

L'introduction de la séquence gaussienne *Ui* dans l'opération d'insertion est justifiée par le faite que beaucoup de techniques de tatouage robuste existantes dans la littérature offrant la robustesse [31] et la capacité sont basées sur la méthode d'étalement de spectre. D'autre part, il a été confirmé par de nombreux travaux que le tatouage basé sur l'étalement de spectre est résistant face à de nombreuses attaques, quand les marques sont de distribution gaussienne et sont statistiquement indépendantes, particulièrement aux attaques de collusion [32]. La figure 4.8 suivante résume le processus d'insertion dans un bloc donné.

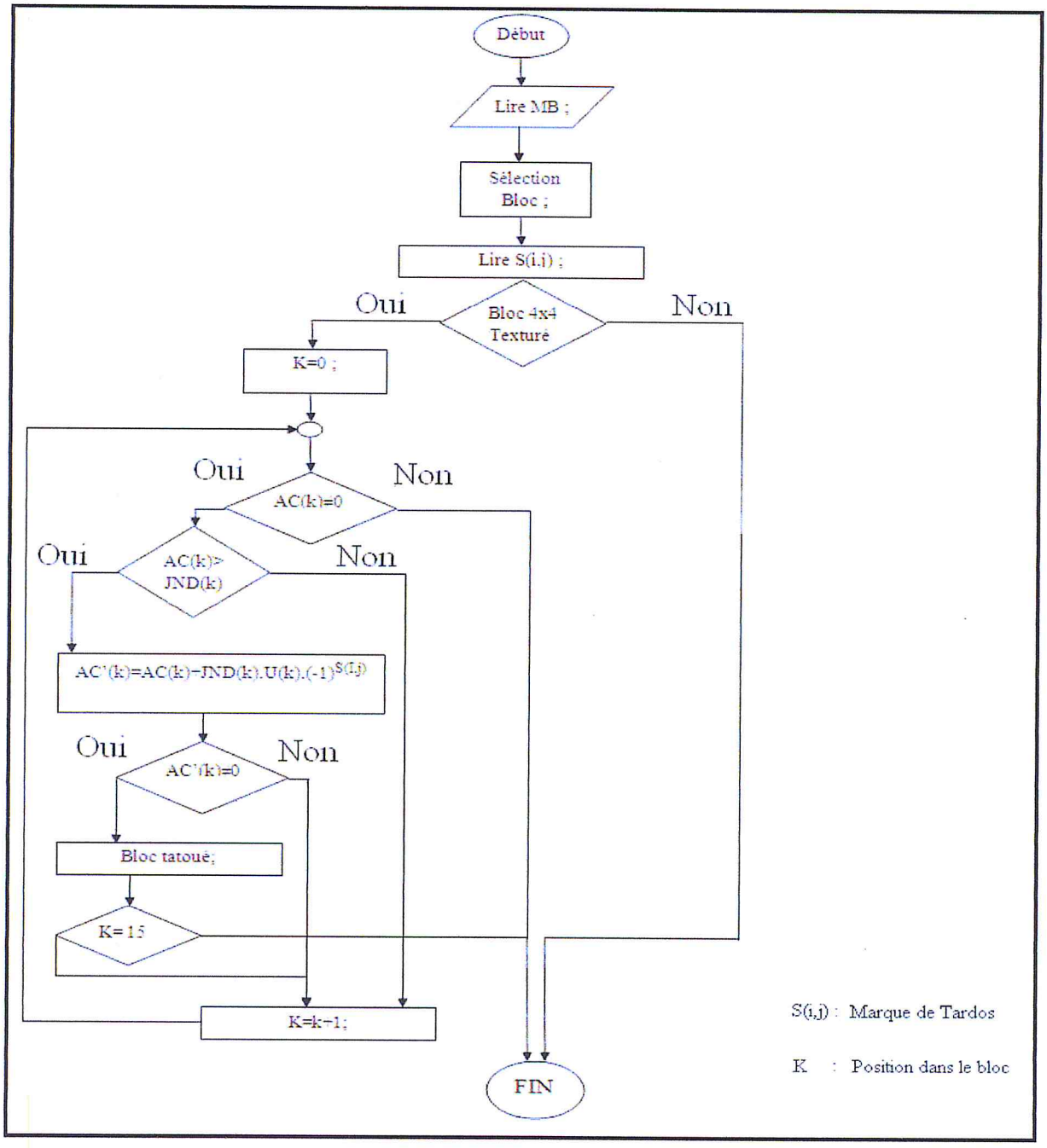


Figure 4.8 : Organigramme résumant les étapes de l'insertion.

2.3. Extraction du code

La détection de la signature est effectuée au niveau du décodeur H.264/AVC (comme illustrée dans la figure 4.9). Le processus de détection est semblable au processus d'insertion en suivant le schéma inverse.

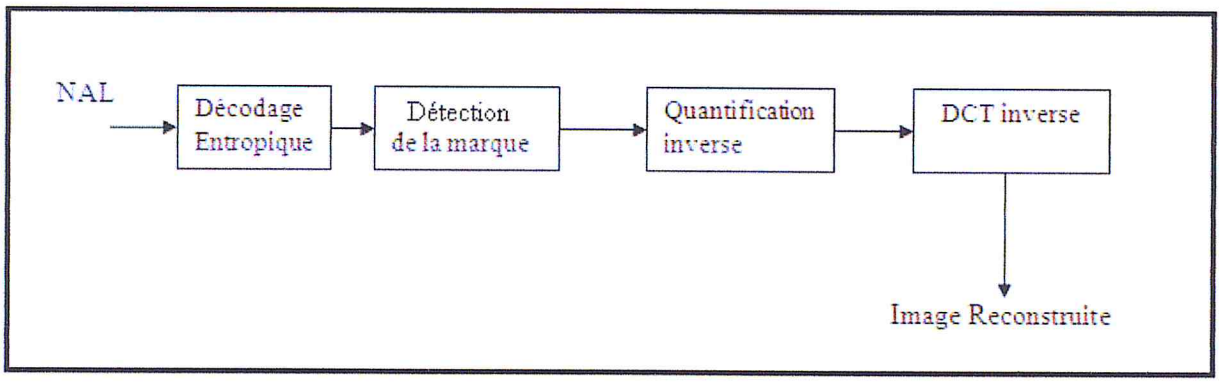


Figure 4.9 : Processus d'extraction d'une image via la norme H.264/AVC.

Le processus d'extraction suit les étapes suivantes :

- La sélection des positions d'extraction des macroblocs tatoués selon la clé (Gaussienne).
- L'extraction de la marque : la marque est extraite selon la formule suivante :

$$R(i,j) = A'(i,j) - A(i,j) \quad (4.15)$$

$$W(i,j) = \text{sign}\,(R\,(i,j)) \quad (4.16)$$

Avec :

W(i,j) est la marque insérée (si le W(i,j) est égale à « 1 », donc S(i,j) qui est la marque binaire est égale à « 0 », sinon, si le W(i,j) est égale à « -1 », donc S(i,j) qui est la marque binaire est égale à « 1 »)

$$\text{Si } W(i,j) = 1 \text{ alors } S(i,j) = 0 \quad (4.17)$$

$$\text{Sinon, si } W(i,j) = -1 \text{ alors } S(i,j) = 1 \quad (4.18)$$

2.4. Processus d'accusation

Tardos amélioré a été utilisé pour l'accusation. Il suit les mêmes étapes que celles proposées dans le code anti collusion standard de G. Tardos [18]. L'amélioration est au niveau de l'accusation, précisément, au niveau du calcul des scores d'accusation et du

seuil. Les scores sont calculés par rapport à la marque extraite de la vidéo piratée ainsi que les marques des utilisateurs déjà stockées dans une base de données (figure 4.10).

$$S_j = \sum_{i=1}^{m} yi \,.\, U(Yi, Xji, pi) \tag{4.19}$$

X_{ji} qui représente le code de l'utilisateur j et Y_i représente le code de la vidéo pirate.

Les fonctions d'accusations :

$$U(1; 1; p) = g_{11}(p) ; \tag{4.20}$$

$$U(0; 0; p) = g_{00}(p); \tag{4.21}$$

$$U(0; 1; p) = g_{01}(p); \tag{4.22}$$

$$U(1; 0; p) = g_{10}(p); \tag{4.23}$$

$$g_{11}(p)= g_{00}(1-p)= -g_{01}(p)= -g_{10}(1-p)=\sqrt{((1-p)/p)} \tag{4.24}$$

Nous avons utilisé comme seuil la médiane des scores :

$$Z = {(MaxSj + MinSj)}/{2} \tag{4.25}$$

La figure 4.10 montre les étapes du processus d'accusation. A partir d'une vidéo attaquée par un certain nombre de colluders (Utilisateurs malhonnêtes), une marque est extraite et comparée avec celles des utilisateurs déjà stockées dans une base de données. Le score de chaque utilisateur est calculé.
Les utilisateurs ayant un score supérieur au seuil Z sont accusés.

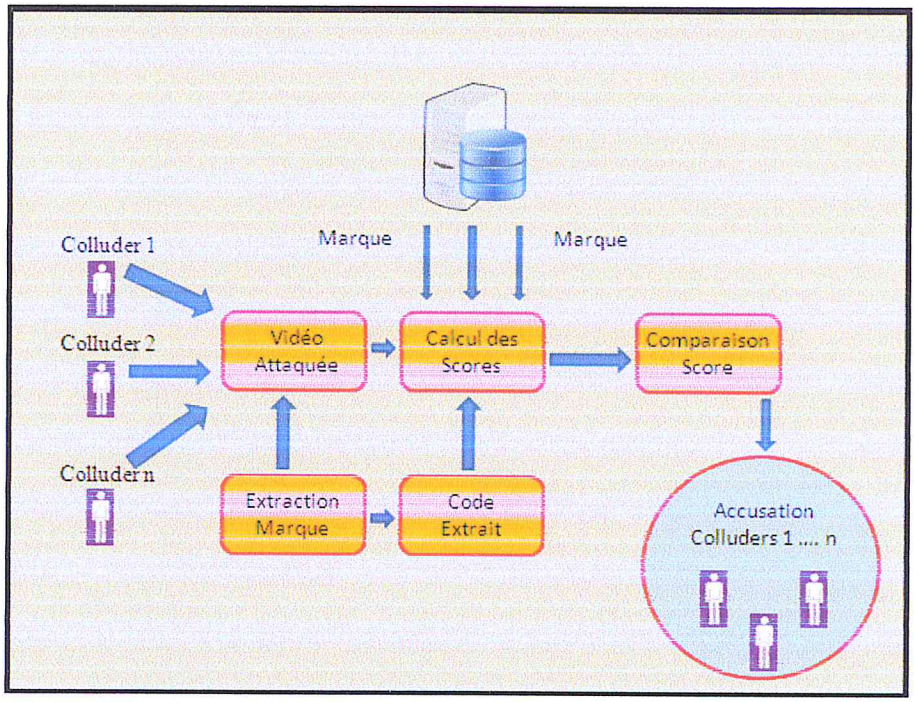


Figure 4.10 : Processus d'accusation

Conclusion

Dans ce chapitre, nous avons parlé du travail que nous avons accompli qui consiste à tracer les utilisateurs malveillants des vidéos compressées par la norme H.264/AVC en combinant une technique de tatouage numérique robuste basée sur le modèle psycho-visuel spatio-temporel JND 4x4 et le code anti collusion amélioré de Tardos.

Dans le prochain chapitre, nous allons présenter les tests et les résultats obtenus et l'application que nous avons conçus.

Chapitre V :
Tests
Et
Comparaisons

1. Introduction

Dans ce chapitre, nous allons exposer les résultats auxquels nous sommes parvenus en appliquant la méthode de tatouage vidéo implémentée.

L'efficacité d'un algorithme de tatouage, quelque soit son domaine d'application, ne peut être jugé qu'après une évaluation expérimental des performances. Des tests d'évaluation ont été effectués pour juger les performances de la technique de tatouage développée en termes d'invisibilité et robustesse face aux attaques de collusions. Nous avons effectué les tests d'évaluation sur les vidéos standard (benchemark) généralement utilisées dans les traitements vidéo : Stefan, Foreman, Football, Bus, City et Soccer. Les formats utilisées sont CIF (352x288), 4CIF (704x576) et HD 720p (1280x720). Nous avons utilisé la norme de compression vidéo H.264/AVC version 10.0 pour l'intégration de la solution proposée.

L'évaluation de la robustesse est effectuée face aux attaques de collusion linéaires.
Parmi celles-ci: [33]

$$P_{AVG}(j) = \sum_{k \epsilon Sc}(Yk(j)/k) \quad (5.1)$$

$$P_{MIN}(j) = MIN(Y_k(j))k \epsilon S_c \quad (5.2)$$

$$P_{MAX}(j) = Max(Y_k(j))\ k \epsilon S_c \quad (5.3)$$

$$P_{Med}(j) = med(Y_k(j))\ k \epsilon S_c \quad (5.4)$$

$$P_{MINMAX}(j) = (Y_{min}(j) + Y_{max}(j))/2 \quad (5.5)$$

$$P_{modNedg}(j) = Y_{min}(j) + Y_{max}(j) - Y_{med}(j) \quad (5.6)$$

P désigne le pixel manipulé.

2. Les paramètres d'entrés dans l'encoder.cfg de la norme H.264/AVC

La figure 5.1 Désigne les paramètres modifiés lors de la compression des vidéos au niveau de l'encoder.cfg.

```
###############################################################################################
# Files
###############################################################################################
InputFile              = "Nom de la vidéo.yuv"       # Input sequence  // Nom de la vidéo
InputHeaderLength      = 0      # If the inputfile has a header, state it's length in byte here
StartFrame             = 0      # Start frame for encoding. (0-N)
FramesToBeEncoded      = 6000      # Number of frames to be coded //Le nombre d'images qui doivent etre encodées Dans la vidéo
FrameRate              = 30.0   # Frame Rate per second (0.1-100.0)  // Le nombre d'image a encodé en une seconde
SourceWidth            = 352    # Frame width
SourceHeight           = 288    # Frame height      // Résolution de la vidéo
TraceFile              = "trace_enc.txt"
ReconFile              = "test_rec.yuv"
OutputFile             = "test.264"  // Nom de la vidéo retournée après compression
###############################################################################################
# Encoder Control
###############################################################################################
ProfileIDC             = 100  # Profile IDC (66=baseline, 77=main, 88=extended; FREXT Profiles: 100=High,
LevelIDC               = 40  # Level IDC   (e.g. 20 = level 2.0)

IntraPeriod            = 10 # Period of I-Frames (0=only first) //La periode de l'image
EnableOpenGOP          =  0  # Support for open GOPs (0: disabled, 1: enabled)
IDRIntraEnable         =  0  # Force IDR Intra  (0=disable 1=enable)
QPISlice               = 15  # Quant. param for I Slices (0-51)  // Pas de quantification
QPPSlice               = 15  # Quant. param for P Slices (0-51)
FrameSkip              =  0 # Number of frames to be skipped in input (e.g 2 will code every third frame)
ChromaQPOffset         =  0  # Chroma QP offset (-51..51)
```

Figure 5.1 : Paramètres d'entrée dans l'encoder.cfg de la norme H.264/AVC

Tableau 5.1 : Paramètres d'entrée dans l'encoder.cfg de la norme H.264/AVC

Paramètres	Description
InputFile	Le nom de la vidéo qu'on veut compresser
FrameToBeEncoded	Le nombre d'images qui doivent être encodées dans la vidéo
SourceWidth & SourceHeight	Résolution de l'image
IntraPeriod	La période entre deux images intra. La vidéo conférence entre dans l'intervalle [10,15], c'est pourquoi, on a donné la valeur 10 à ce paramètre
QPISlice & QPPSlice	Pas de quantification

3. Mesure de qualité

L'évaluation de la qualité visuelle est calculé selon le rapport signal sur bruit PSNR (pour Peak Signal to Noise Ratio). Ce dernier mesure, en échelle logarithmique des décibels, le rapport entre la puissance maximale d'un signal et la puissance du bruit affectant la fidélité de sa représentation.

Dans notre application, le PSNR est automatiquement généré par le codeur au cours de la compression sous le nom de fichier **« log.dat »**

4. Tests de génération des codes de Tardos

La génération des codes de Tardos est effectuée en prenant en considération les paramètres suivants :

- c : Désignant le nombre de colluders qui prendra la valeur « 20 ».
- n : Le nombre d'utilisateur prenant la valeur « 100 ».
- ε : Est la probabilité de fausse alarme prenant comme valeur 10^{-1}.

  Ces paramètres nous donnent un code de longueur « m= 92103 ».

Tableau 5.2 : La longueur du code de Tardos par rapport au paramètres n, c, ε

Nombre d'utilisateur « n »	Nombre de colluders « c »	La probabilité d'erreur « ε »	La longueur du code de Tardos « m »
100	20	10^{-1}	92103
100	20	10^{-3}	276311
10000	10	10^{-5}	115129

5. Tests de la qualité d'image après insertion

5.1. Tests et comparaison des PSNR et le Bitrate

Le tableau 5.3 montre les tests entre les valeurs du PSNR et bitrate des vidéos d'origine (sans insertion) et les valeurs du PSNR et bitrate des vidéos tatouées.

Tableau 5.3 : Comparaison PSNR et Bitrate

Video	PSNR (dB)		Bitrate (bpp)	
	Original	Après insertion	Original	Après insertion
Stefan_CIF	46.20	46.35	1015752	1342512
Foreman_CIF	46.37	46.47	689664	982768
Football_CIF	45.81	46.03	1132248	1477024
Bus_CIF	45.89	46.07	1075752	1426064
City 704x576	45.76	45.89	3534648	4737712
Soccer_4CIF	45.89	46.03	3475080	4558144

Les valeurs du PSNR qui représente la qualité de vidéo sont restées pratiquement inchangées (différence € [0,0.22] se qui est négligeable), se qui implique la non détérioration de la vidéo. Pour le taux de bits (bit par pixel), une augmentation (entre 32% et 41%) est remarquée après l'insertion (tableau 5.3). En comparant ces résultats obtenus avec ceux des travaux précédant [6], on remarque une amélioration au niveau des valeurs du PSNR (dans [6], la différence après l'insertion appartient à [0,2.6]).

5.2.Tests et comparaison entre les séquences avant et après l'insertion

Les figures 5.2, 5.3, et 5.4 montrent la qualité des séquences vidéo avant et après insertion.

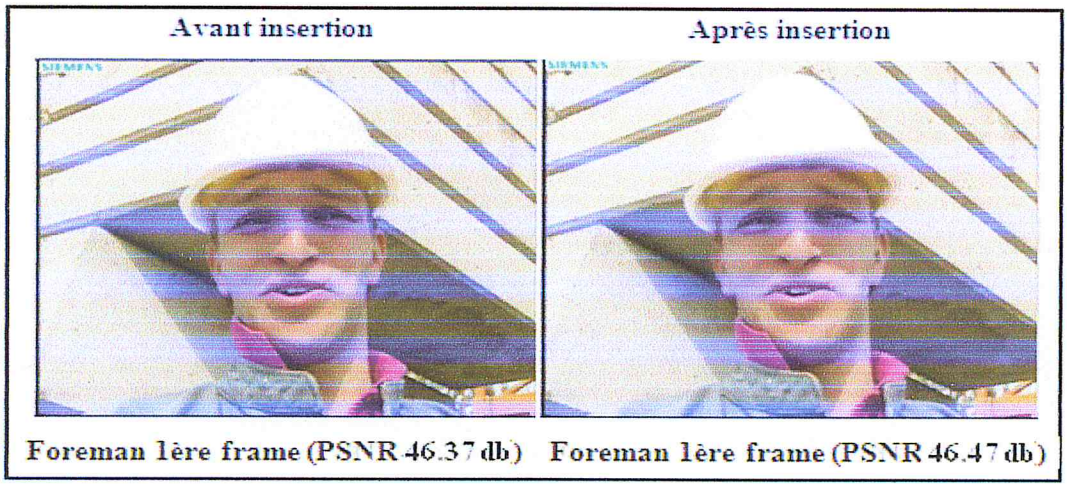


Figure 5.2 : Comparaison entre la séquence Forman avant et après l'insertion du point de vue qualité d'image.

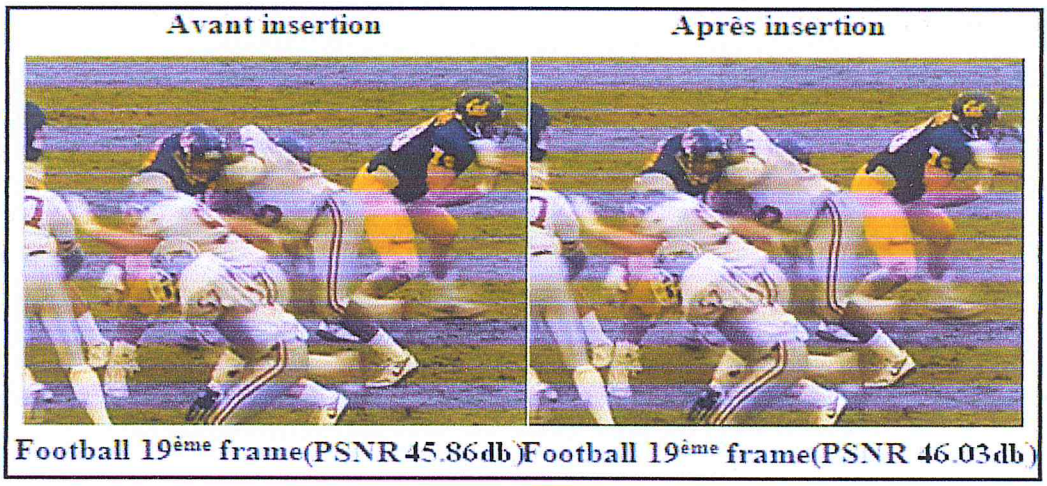


Figure 5.3 : Comparaison entre la séquence Football avant et après l'insertion du point de vue qualité d'image.

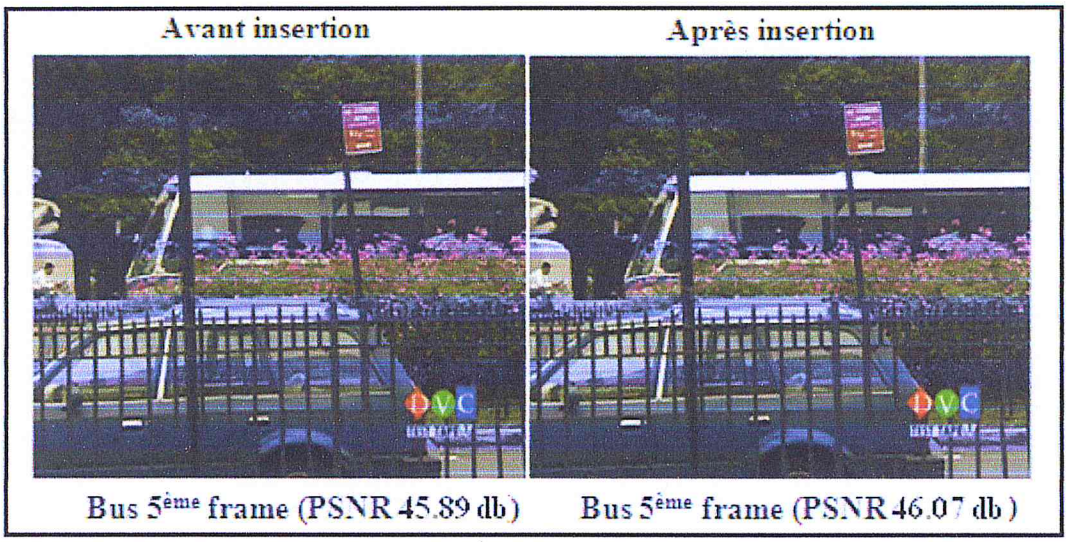


Figure 5.4 : Comparaison entre la séquence Bus avant et après l'insertion du point de vue qualité d'image.

Les figures (5.2, 5.3 et 5.4) montrent que la qualité des vidéos n'a pas diminué, ce qui confirme les résultats du PSNR.

5.3.Influence du pas de quantification sur la qualité et la capacité d'insertion

Le tableau 5.4 et les figures 5.5 et 5.6 montrent l'influence du pas de quantification QPI sur la qualité de la vidéo (PSNR) et le taux d'insertion dans une image. Les valeurs QPI ϵ [15, 20] sont les plus optimales.

Tableau 5.4 : Influence du pas de quantification sur PSNR et la capacité d'insertion

Pas de Quantification QPI	PSNR (dB)	Capacité d'insertion bits
35	33.46	0
30	35.32	7
25	39.27	60
20	42.39	126
15	46.37	219
10	50.17	302
8	51.32	310

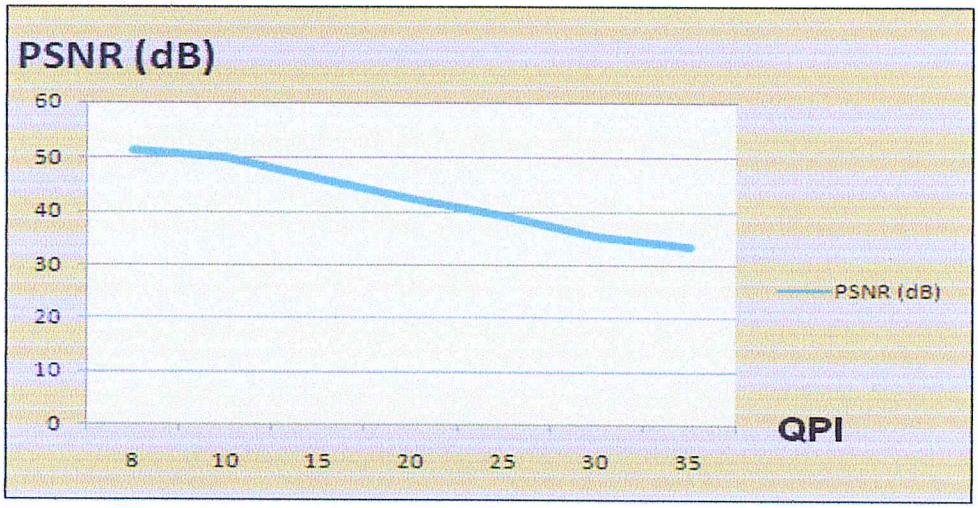


Figure 5.5 : Rapport entre le pas de quantification et le PSNR

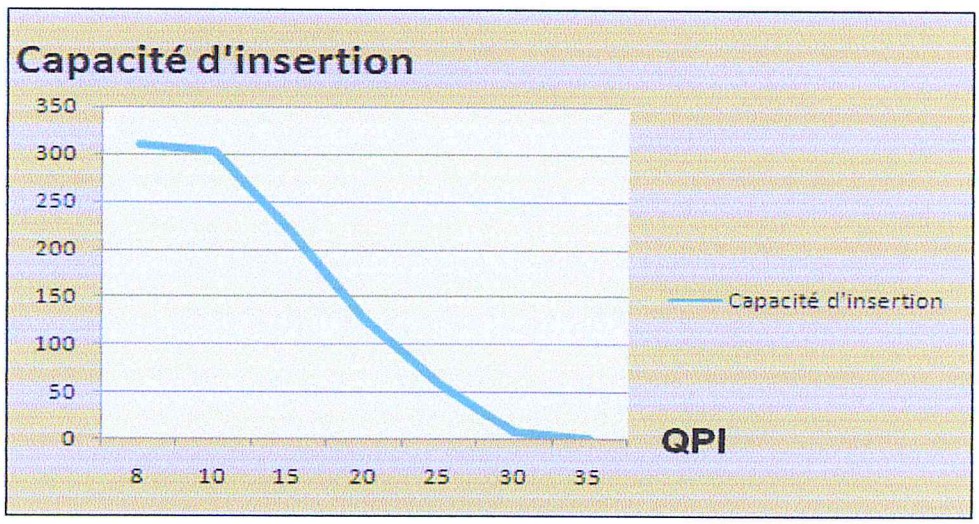


Figure 5.6 : Rapport entre le pas de quantification et la capacité d'insertion

6. Tests de la traçabilité des pirates

La robustesse face aux attaques linéaires est effectuée en utilisant l'application développée par Mohamed Amine Morsli au cours de [6] de son mémoire de master 2. Le tableau 5.5 illustre les résultats d'accusation par rapport au nombre de colluders et le type d'attaques.

On remarque qu'aucun innocent n'a été accusé par contre, le taux de détection des colluders est important concluant ainsi que les résultats obtenus sont satisfaisants.

.

Tableau 5.5 : Taux de détection des utilisateurs malhonnêtes par rapport à l'attaque et le nombre de colluders

Nombre de Colluders	Les colluders (Pirates) localisés pour les attaques suivantes					
	AVG	Min	Max	Median	MinMax	ModNeg
2	2	2	2	2	2	2
5	4	5	5	5	5	4
8	8	8	8	8	8	7
11	9	10	10	10	10	8
14	12	13	13	13	13	11
17	15	15	14	16	15	12
20	16	15	16	16	15	13

Le tableau 5.6 est un tableau comparatif entre les résultats obtenus lors des tests avec le code de Tardos amélioré, la technique JND et l'insertion au niveau des coefficients AC, avec ceux des travaux accomplis précédemment [6] (l'utilisation du code de Tardos simple et l'insertion au niveau des coefficients DC).

Tableau 5.6 : Tableau comparatif entre les résultats des nouveaux et précédents travaux.

Nombre de Colluders	Les colluders (Pirates) localisés pour les attaques suivantes											
	AVG		Min		Max		Median		MinMax		ModNeg	
Comparaison des nouveaux tests avec les précédents	PS	[6]	PS	[6]	PS	[6]	PS	[6]	PS	[6]	PS	[6]
2	2	2	2	2	2	2	2	2	2	2	2	2
5	4	4	5	5	5	5	5	5	5	5	**4**	**3**
8	8	8	8	8	8	8	8	8	8	8	7	7
11	9	9	10	10	10	10	10	10	**10**	**9**	8	8
14	12	12	13	13	13	13	**13**	**14**	**13**	**12**	**11**	**10**
17	15	15	15	15	14	14	16	16	**15**	**14**	12	12
20	16	16	15	15	**16**	**15**	16	16	**15**	**14**	13	13

PS : Solution Proposée

L'utilisation du modèle JND pour l'insertion au niveau des coefficients AC combiné avec le code de Tardos amélioré a permis une meilleure traçabilité des colluders et une meilleure robustesse par rapport aux attaques MinMax et ModNeg. Pour les autres attaques, le tableau comparatif (tableau 5.6) démontre que presque tous les nombres de colluders détectés sont égaux.

Conclusion

Dans ce chapitre, nous avons mentionné les différents tests et comparaisons du point de vue qualité d'image, de la génération des codes de Tardos et de la traçabilité des traitres. Les résultats obtenus par cette technique de tatouage sont bons puisqu'on a augmenté le taux d'insertion ce qui accroit la robustesse tout en gardant une bonne perceptibilité de la vidéo.

7. Présentation de l'application

Nous allons maintenant présenter l'application développée. La figure 5.7 montre la fenêtre principale de l'application permettant la communication entre l'utilisateur et l'application.

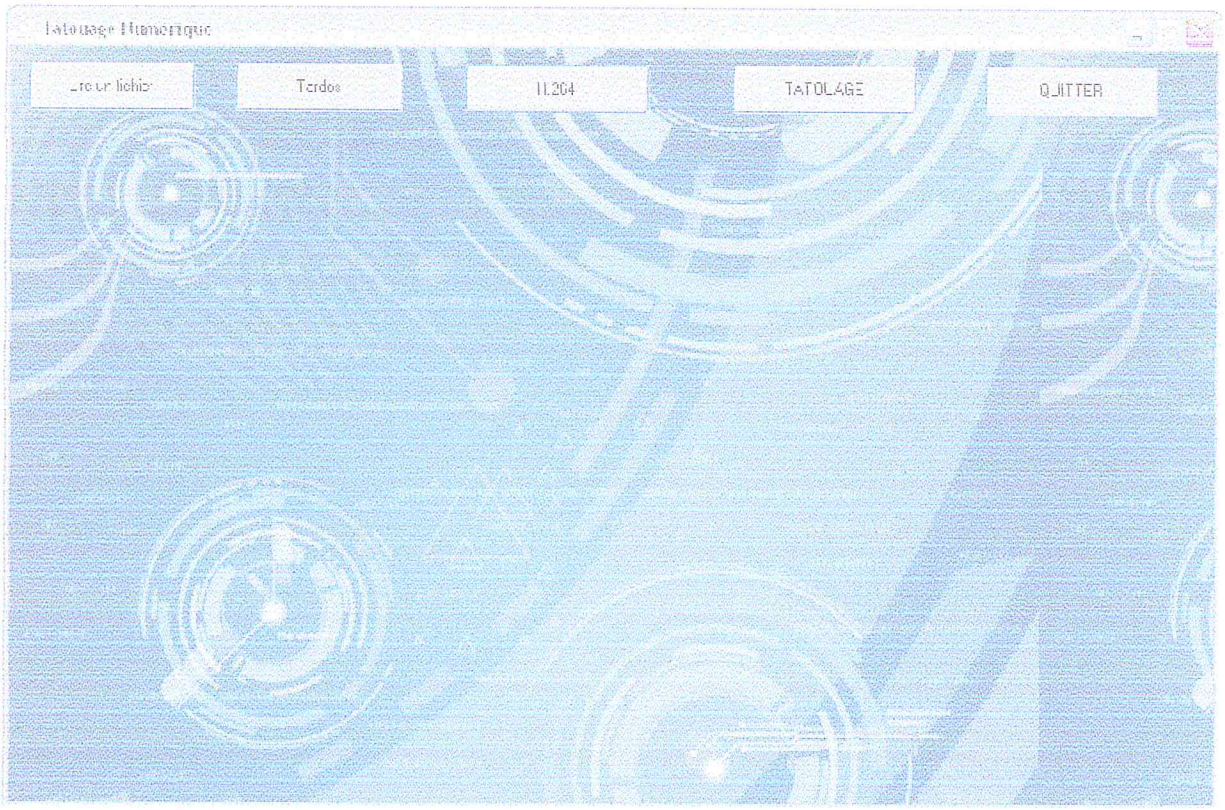


Figure 5.7 : Fenêtre principale de l'application

Dans cette fenêtre, on a utilisé les boutons suivants ayant chacun sa fonctionnalité :

- **Lire un fichier**

  Ce bouton donne accès à un logiciel pouvant lire des vidéos de format « YUV », la figure 5.8 montre l'apparition de ce logiciel lors du clic sur « Lire un fichier ».

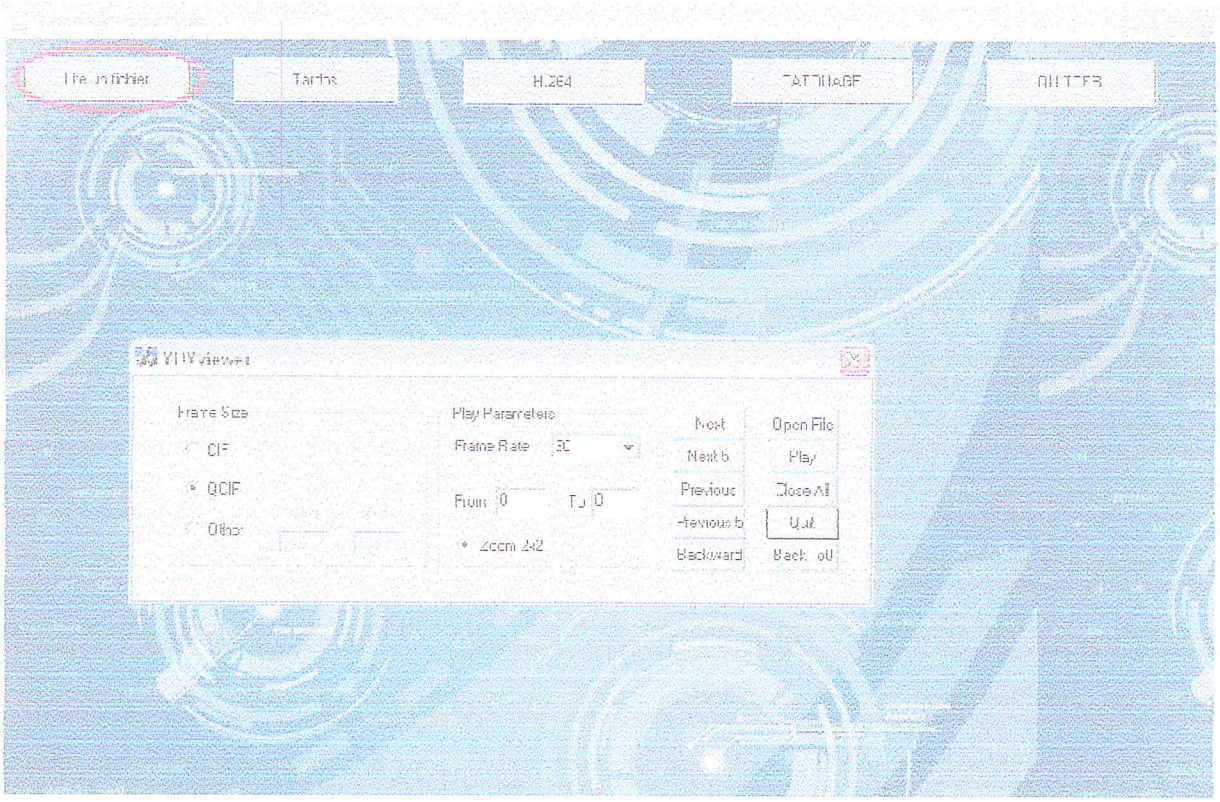


Figure 5.8 : Fonctionnalité du bouton Lire fichier donnant accès au logiciel YUV viewer

La figure 5.9 et 5.10 montre l'utilisation de YUV viewer pour ouvrir la séquence Stephan.

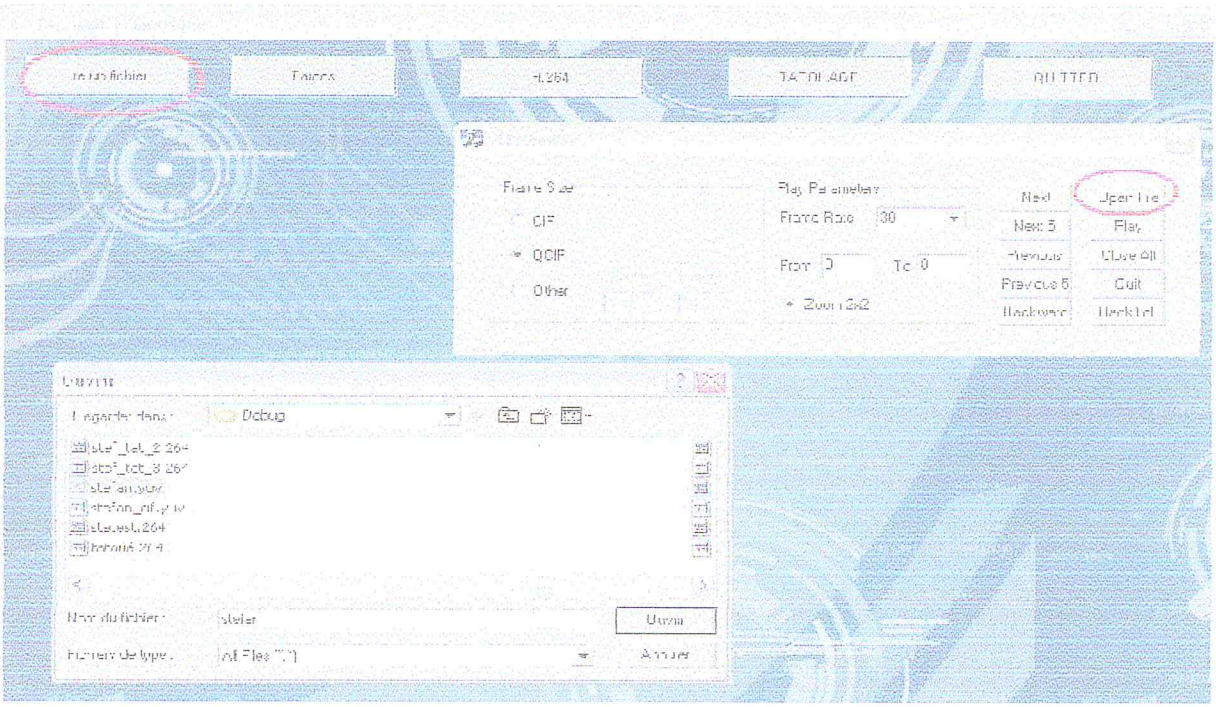


Figure 5.9 : Sélection de la séquence vidéo à visionner

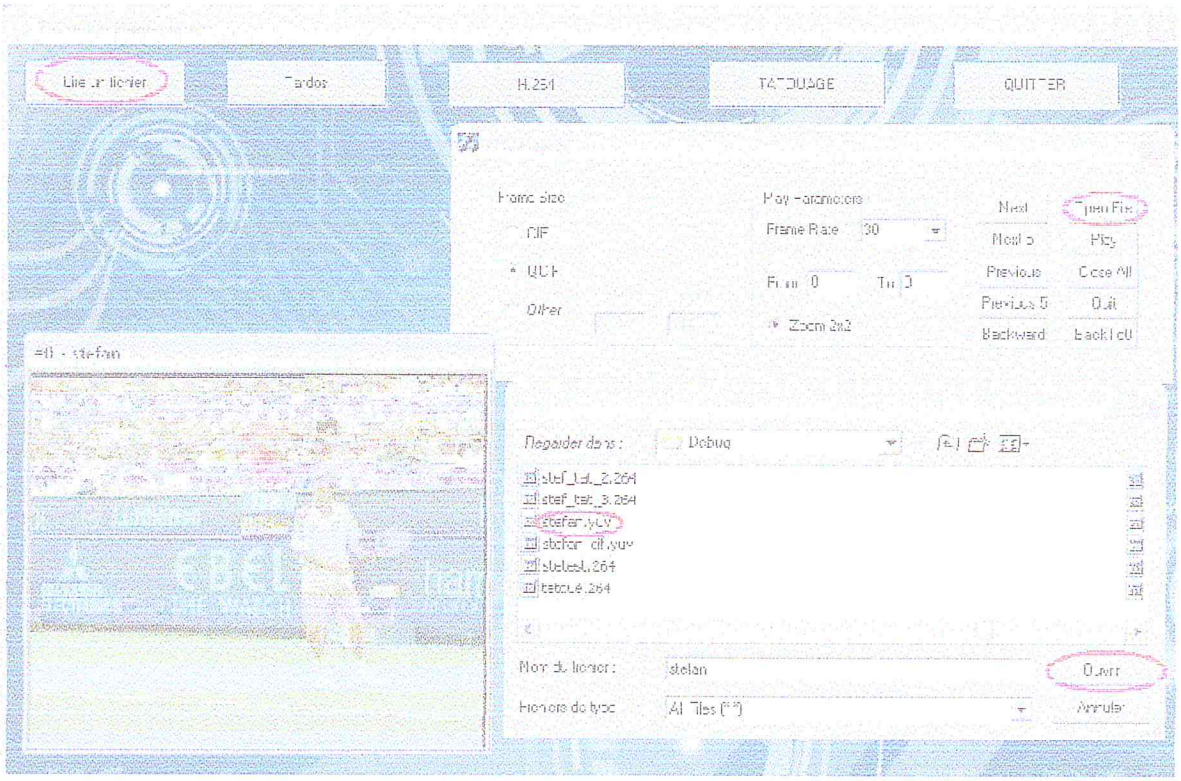


Figure 5.10 : Lecture de la séquence vidéo stefan.yuv de format QCIF

- **Tardos**

  Le *bouton Tardos permet d'accéder à la partie création des codes et accusation* d'éventuel utilisateur malhonnête. La figure 5.11 montre la fenêtre du code de Tardos.

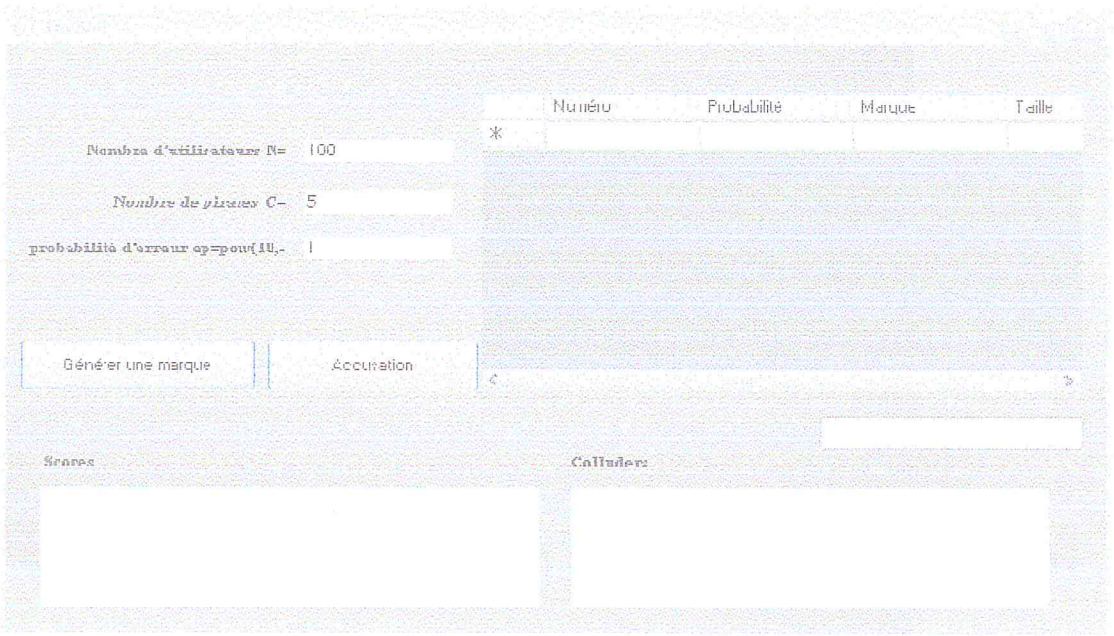


Figure 5.11 : Fenêtre accédant au code de Tardos

Le bouton « **Générer une marque** » permet de créer les codes à insérés pour chaque utilisateur en prenant en considération le nombre d'utilisateurs « N », le nombre de pirates « c » et la probabilité d'erreur ε.

La figure 5.12 montre le tableau des marques attribuées à chaque utilisateur.

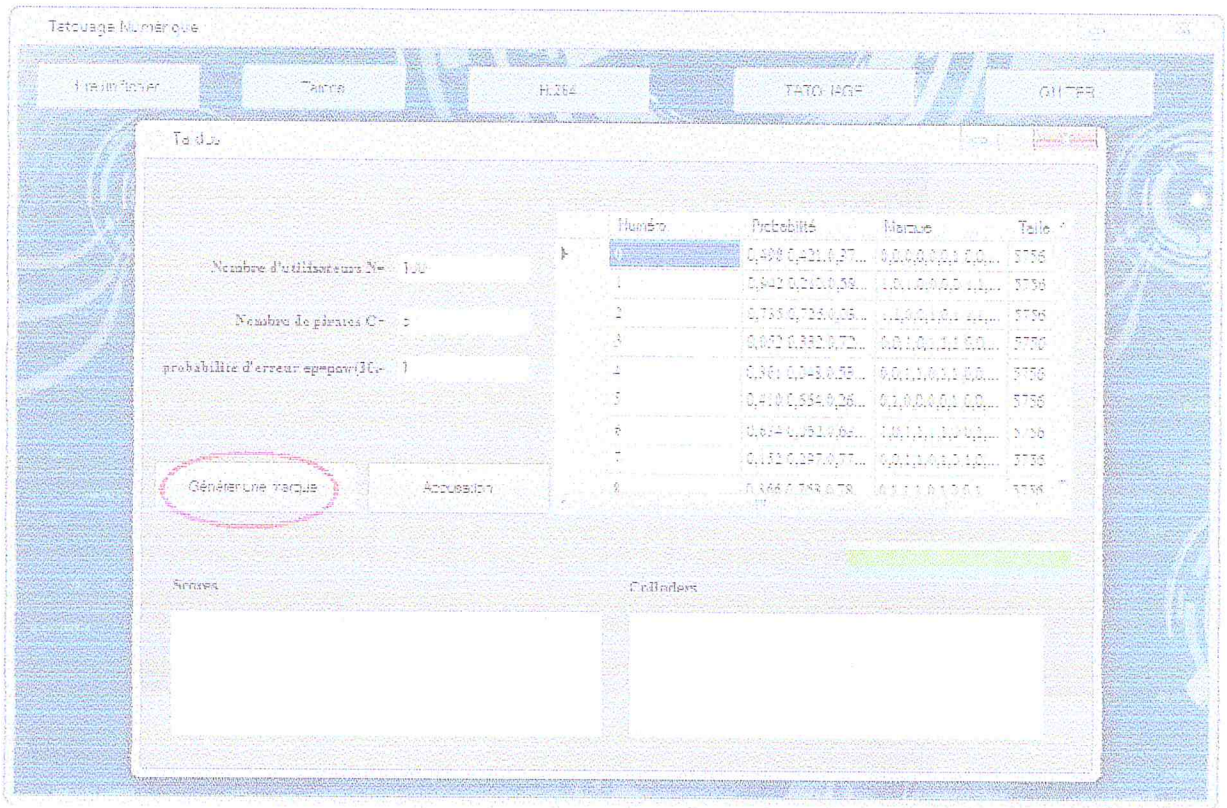


Figure 5.12 : Génération des codes de Tardos.

Le bouton « **Accusation** » fournis le score de tous les utilisateurs (Voir chap3) et la liste des pirates « Colluders ».

La figure 5.13 montre la liste des scores calculés pour chaque utilisateur et la liste des utilisateurs accusés.

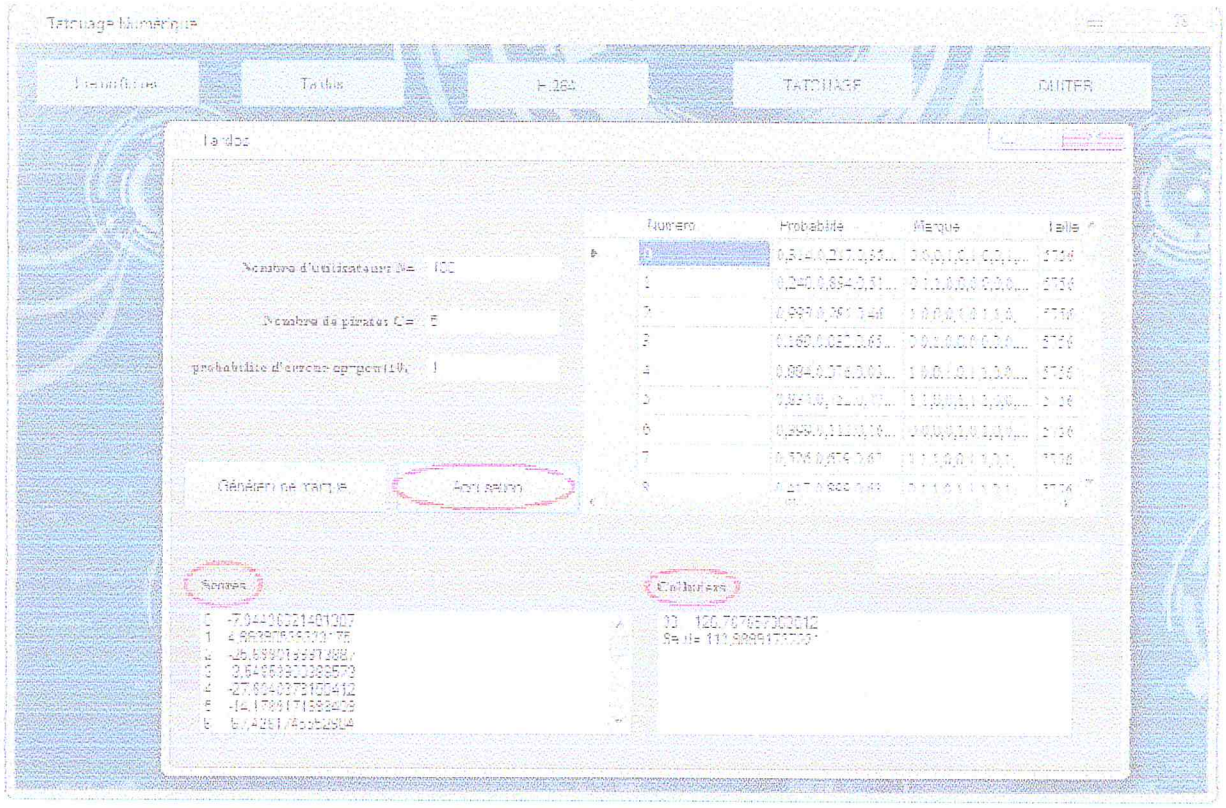


Figure 5.13 : Listes des scores des utilisateurs et la liste des pirates « Colluders »

- **H.264**

  Le bouton H.264 donne accès à deux choix, Compression ou Décompression, le premier permet de compresser une séquence vidéo à l'aide la norme de compression H.264 et le deuxième permet la décompression de ce contenu.

➢ **Bouton Compression**

La figure 5.14 montre la fenêtre qui s'affiche pour la compression d'une séquence vidéo en sélectionnant la séquence et en précisant les paramètres.

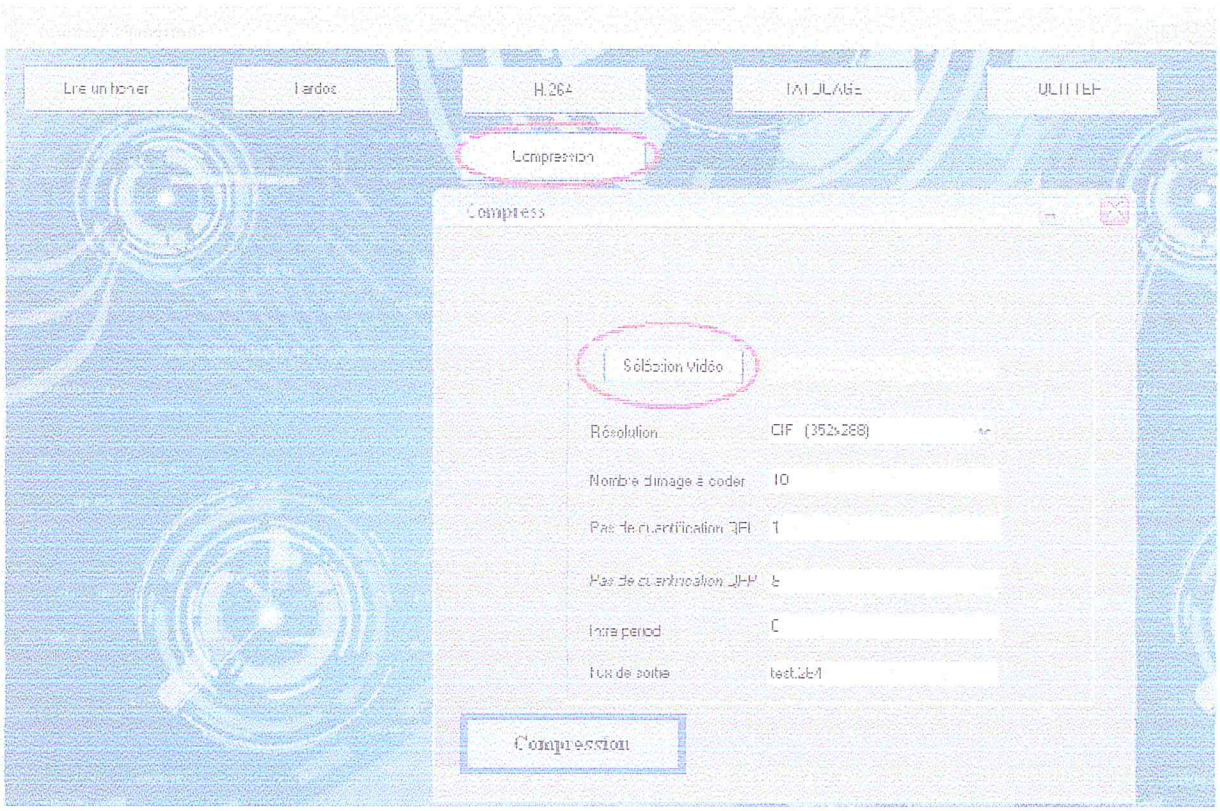


Figure 5.14 : Compression d'une séquence vidéo

Nous obtiendrons après la compression d'une séquence vidéo un flux de sortie ayant comme nom «test.264 ».

- **Bouton Décompression**

  Le bouton « Décompression » permet de décompressé une séquence vidéo via la norme de compression H.264.

  La figure 5.15 montre la fenêtre de décompression pour décompresser la séquence vidéo voulue.

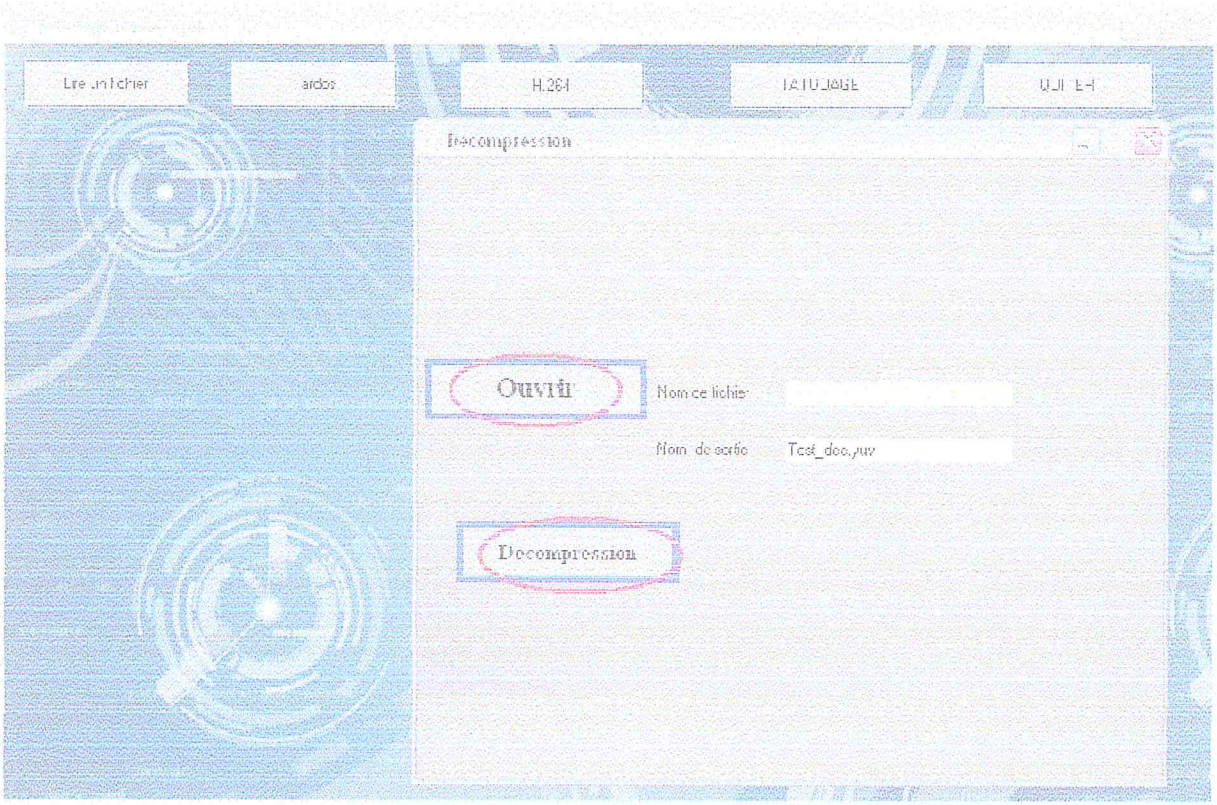


Figure 5.15 : Décompression d'une séquence vidéo via la norme de compression H.264

- TATOUAGE

  Ce bouton offre deux choix à faire, « Insertion ou Extraction », à l'aide de ces deux boutons, on insère et on extrait respectivement une marque d'une séquence vidéo suivant la technique de tatouage numérique.

➢ **Insertion**

Ce bouton permet d'insérer une marque propre à un utilisateur dans une séquence vidéo.

La figure 5.16 permet de voir la fenêtre d'insertion s'afficher avec les paramètres à entrés telle que le nom de la séquence vidéo où insérer le code, le nom de la vidéo après insertion, sélection de la clé, etc.

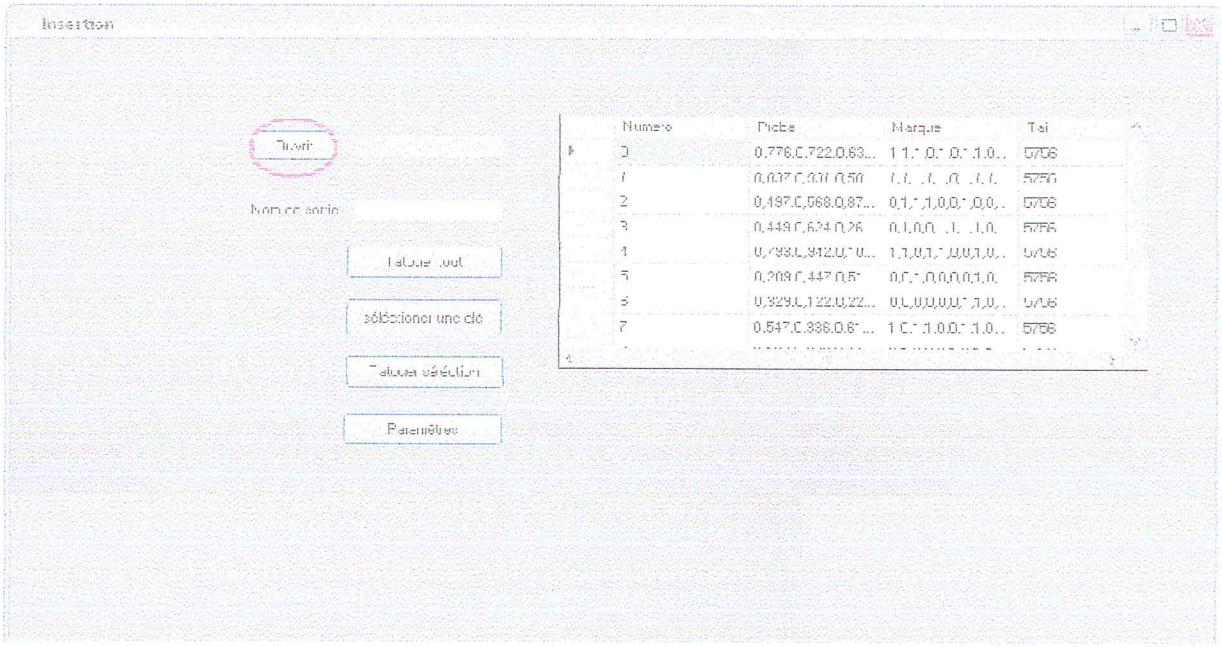


Figure 5.16 : Insertion d'une marque dans une séquence vidéo

- **Extraction**

  Ce bouton permet de sélectionner la séquence vidéo pour extraire la marque qu'a été insérée.

  La figure 5.17 montre la fenêtre d'extraction.

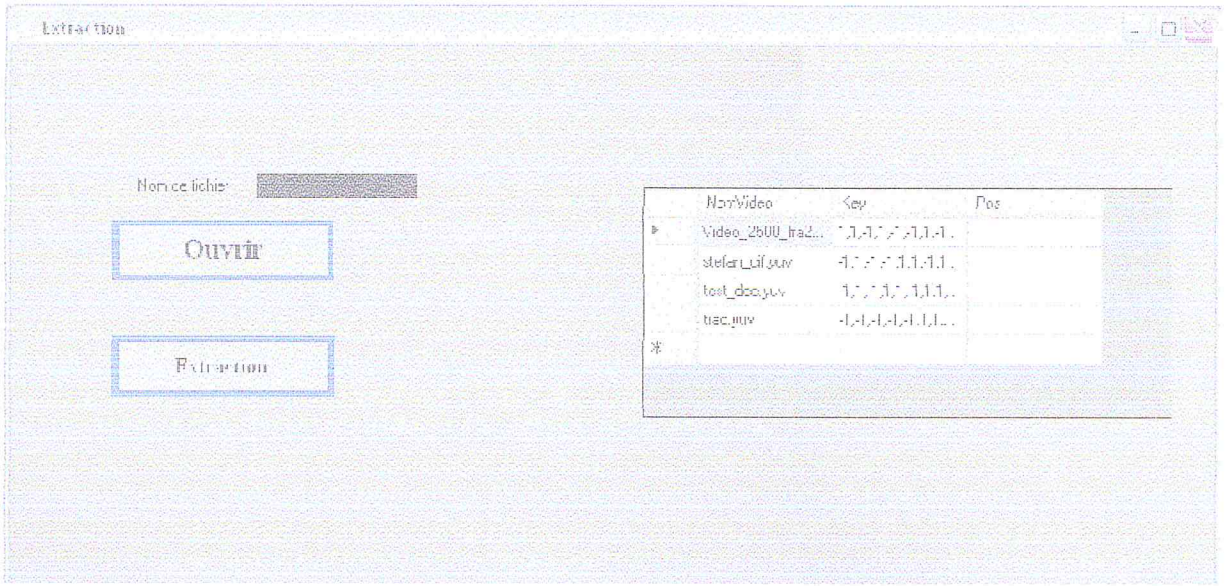


Figure 5.17 : Extraction de la marque d'une séquence vidéo

- **Quitter**

  Le bouton quitter sert à sortir de l'application.

Conclusion Générale

Conclusion générale

L'étude que nous avons menée sur le tatouage robuste pour le traçage des utilisateurs illicites des vidéos H.264/AVC distribuées à travers l'Internet comprend cinq chapitres. Le premier chapitre introduit la notion de tatouage numérique et sa contribution dans la protection du contenu. Le chapitre 2 expose la problématique de la diffusion des contenus des vidéos distribuées par internet ou sur les lecteurs DVD et la nécessité de protéger leur contenu par la technologie du tatouage robuste couplée à des codes anti collusion pour tracer et identifier les utilisateurs malveillants. Le chapitre 3 introduit l'apport du modèle psycho visuel dans le tatouage et plus particulièrement le modèle JND. Le chapitre 4, décrit en détails les différents modules implémentés de la solution de traçage des utilisateurs illicites du contenu H.264/AVC en utilisant un tatouage robuste basée sur le modèle JND et le code anti collusion amélioré de Tardos.

L'approche développée associant le tatouage robuste basé dur un modèle psycho-visuel JND couplé au code amélioré de Tardos a aboutis à des résultats concluants sur la qualité visuelle aussi bien que sur le critère de robustesse face aux attaques de collusion linéaires.

Les codes de Tardos sont résistants aux attaques de collusion, c'est-à-dire au groupement d'adversaires mettant leurs contenus numériques afin de forger une version pirate. Ils sont particulièrement attractifs par leur faible longueur et leur efficacité néanmoins nous proposons comme perspectives à ce mémoire de porter des améliorations au niveau du processus d'accusation et d'introduire d'autre variante permettant d'accuser plus de membres de la collusion. Ou bien introduire d'autres codes anti collusion qui ne nécessitent pas un stockage d'une base de données des codes distribuées.

Bibliographie

Bibliographie :

[1] : Teddy Furon, Thomas Security Lab, Cesson-Sévigné, France. « Le traçage des traitres ».

[2] : Christian REY, Jean-Luc Dugelay « An overview of watermarking algorithms for Image authentication».

[3] : Yann BODO « Elaboration d'une technique d'accès conditionnel par tatouage et embrouillage vidéo basée sur la perturbation des vecteurs de mouvement».

[4] : Drira Fadoua : « Tatouage d'image par technique multidirectionnelles et multi-résolution ».

[5] : Khaled Loukeaoukha, « Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective» thèse pour l'obtention du grade de philosophie Doctor. Université Laval.

[6] : Morsli Amine, Taibi Abd elhafid « Protection de contenu multimédia par le traçage des copies de pirates dans la norme de compression H.264/AVC » 2011.

[7] : M. El-Gayyar «Watermarking Techniques Spatial Domain Digital Rights Seminar», Media Informatics University of Bonn Germany, mai 2006.

[8] : A.Parisis, P.Carré, A.Trémeau, Laboratoir SIC, université de Poitiers « Introduction au tatouage d'images couleur »

[9] : Chaw-Seng WOO « Digital Image Watermarking Methods for Copyright Protection and Authetification ».

[10] : Gwenael Doerr et Jean-Luc Dugelay « Problématique de la Collusion en Tatouage Vidéo Collusion Issue in Vidéo Watermarking ».

[11] : A. Menezes, P. van Oorschot, et S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[12] : A. Eskicioglu. Multimedia security in group communications: Recent progress in key management, authentication and watermarking. ACM MultiMedia Systems, Special Issue on Multimedia Security, 9(3) :239–248, September 2003.

[13] : M. Wu, W. Trappe, J. Wang, et R. Liu. Collusion-resistant fingerprinting for multimedia. IEEE Signal Processing Magazine, 21(2) :15–27, March 2004.

[14] : D. Boneh et J. Shaw. Collusion secure fingerprinting for digital data. IEEE Transaction on Information Theory, 44(5) :1897–1905, September 1998.

[15] : Chor, B., Fiat, A., Naor, M., Pinkas, B. : «Tracing traitors. » IEEE Trans. Inform. Theory 44 (1998) 1897-1905.

[16] : Ana Cahrpentier : « Identification de copies de documents multimédias grâce aux codes de Tardos ».2011

[17] : C. Peikert, A. Shelat et A. Smith « Lower bounds for collusion-secure fingerptinting ». Page 472-478, 2003.

[18] : Gabor Tardos «Optimal Probabilistic Fingerprint Codes» 2003.

[19] : Ana Charpentier, Caroline Fontaine, Teddy Furon « Décodage EM du code de Tardos pour le fingerprinting ».

[20] : Just-Noticeable Difference Profile for Images Lin Ma and King N. Ngan Department of Electronic Engineering, The Chinese University of Hong Kong, Hong Kong SAR

[21] : Coxn I.J., Miller, M.L, Bloom, T.(2008). Digital watermarking and stéganographie (2 ed.) Morgan Kaufmann. Watson, A.B. (1993). Visually optimal DCT quantization matrices for individual images. Paper presented at the Data compression Conference (DCC).

[22] : Spatio-Temporal Just Noticeable Distortion Profile for Grey Scale Image/Video in DCT Domain Zhenyu Wei, Student Member, IEEE, and King N. Ngan, Fellow, IEEE

[23] : Hervé LE BORGNE, « Analyse de Scènes Naturelles par Composantes Indépendantes » institut national polytechnique de Grenoble, thèse pour obtenir le grade de docteur. Le 30 janvier 2004.

[24] : Spatio-temporal Just Noticeable Distortion Model Guided Video Watermarking 2009. Yaqing Niu1,2, Jianbo Liu1, Sridhar Krishnan2, and Qin Zhang1
1 Information Engineering School, Communication University of China, Beijing, China
2 Department of Electrical and Computer Engineering, Ryerson University, Toronto, Canada.

[25] : AXIS communications, document de synthèse « La compression vidéo H.264, nouvelle possibilité dans le secteur de la vidéosurveillance ».

[26] : Iain E. Richardson « The H.264 Advaced Video Compression Standard » ,deuxième édition (2010).

[27] : Thomas Wiegand, Gary J Sullivan, Senior Member, IEEE, Gisle Bjontegaard, and ajay Luthar, Senior Member, IEEE « Overview of the H.264/AVC Video Coding Standard »

[28] : Duyao Wang, Sujuan Huang, Guorui Feng, Shuozhong Wang : « Perceptual Differential energy watermarking for H.264/AVC» 3 juin 2011.

[29] : Wei ZY, Ngan KN (2009) Spatio-temporal just noticeable distortion profile for grey scale image/video in DCT domain. IEEE Trans Circuits Syst Video Technol 19(3):337–346.

[30] : Canny J (1986) A computational approach to edge detection. IEEE Trans Pattern Anal Mach Intell 8(6):679–698.

[31] : J. Sullivan, P. Topiwala and A. Luthra, "The H.264/AVC Advanced Video Coding Standard: Overview and Introduction to the Fidelity Range Extensions," SPIE Conference on Applications of Digital Image Processing XXVII, Special Session on Advances in the New Emerging Standard: H.264/AVC, 2004.

[32] : F. Hartung, J. Su, and B. Girod, "Spread Spectrum Watermarking: Malicious Attacks and Counter attacks," in Proc. SPIE: Security and Watermarking of Multimedia Contents, pp. 147–158, 1999.

[33] : Z.Shahid, M.chaumont and W.Puech, « Spread Spectrum-Based Watermarking For Tardos Code-Based Fingerprinting For H.264/AVC Video». Lirmm, umrcnrs 5506, university of Montpellier 2, France 2008.

[34] : Foued DERRAZ, Mohamed BELADGHAM, M'hamed KHELIF « Mesure Objective de la Qualité d'Image Médicale Dérivée de l'Index de Similarité Structurelle » Laboratoire de Génie Biomédicale –TLEMCEN-ALGERIE.

[35] : Z.Shahid, M.chaumont and W.Puech, "Spread Spectrum-Based Watermarking For Tardos Code-Based Fingerprinting For H.264/AVC Video". Lirmm, umrcnrs 5506, university of Montpellier 2, France 2008.

Sites web :

[SW1] : http://fr.wikipedia.org/wiki/Psychophysique

[SW2] : http://www.onsebuzz.com/divers/harry-potter-7-identification-du-piratage-grace-a-untatouage-numerique,201011191397.html.

Mots clés (Glossaire):

- Copyright : Est l'ensemble des prérogatives exclusives dont dispose une personne physique ou morale sur une œuvre de l'esprit originale.

- Filtre passe-bas : Est un filtre qui laisse passer les basses fréquences et qui atténue les hautes fréquences (fréquences supérieurs à la fréquence de coupure). C'est l'inverse du filtre passe-haut, les deux combinés forment un filtre passe-bande.
- TFD (Transformée de fourier discrète) : Est un outil mathématique de traitement de signal numérique.
- DCT (Transformée en Cosinus discrète) : Est un outil mathématique de traitement de signal numérique.
- La distance de Hamming : est une distance au sens mathématique du terme. À deux suites de symboles de même longueur, elle associe le nombre de positions où les deux suites diffèrent.
- Dual : Se dit de propriétés mathématique qui sont par deux et qui présentent un caractère de réciprocité.
- Mode Intra : L'image est encodée à partir d'un algorithme de prédiction spatiale, chaque macrobloc de l'image courante doit être encodé à partir de la texture de leurs voisins qui peut varier assez facilement.
- Mode Inter : désigne dans la compression vidéo une image ou une trame appartenant à un flux qui a été encodée à partir d'un algorithme de prédiction inter-trame. Elle dépend des images précédemment encodées afin de prédire la position des macroblocs d'origine.
- Composante DC : Le premier élément de chaque block (0,0)
- Composante AC : Le reste des éléments de chaque block (i=1---n, j=1---m).
- Labéliser : Attribuer une marque, nom,etc.