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

UNIVERSITE IBN KHALDOUN - TIARET

MEMOIRE

Présenté à :

FACULTÉ MATHEMATIQUES ET INFORMATIQUE
DÉPARTEMENT D'INFORMATIQUE

Pour l'obtention du diplôme de :

MASTER

Spécialité : Réseaux et Télécommunication

Par :
TAOUCHE Mohamed
KOUFI Brahim

Sur le thème

Protection de vidéo numérique par tatouage fragile

Soutenu publiquement le 09 / 12 / 2020 à Tiaret devant le jury composé de :

Mr OUARED Abdelkader	Grade	*Maitre de conférences*	Président
Mr OUAMRI mokhtar	Grade	*Maitre de conférences*	Encadreur
Mr LAAREDJ Zohra	Grade	*Maitre de conférences*	Examinateur

Remerciements :

Avant tout, nous remercions notre Dieu de nous avoir aidés à faire notre thème de fin d'étude et Merci à nos parents qui nous soutiennent bien.

Au terme de ce travail, nous tiens à exprimer notre profonde gratitude et nos sincères Remerciements à notre tuteur de notre projet de fin d'étude Monsieur ouamri mokhtar qui a accepté d'encadrer nos travaux.

Nous tenons à remercier vivement les jurys de leur extrême empressement d'évaluer notre travail. Qu'ils ont accepté de venir à évaluer notre travail.

Nous voudrions remercier également tous nos amis.

Nos profonds remerciements vont à nos camarades.

Nos plus vifs remerciements s'adressent aussi à tout le cadre professoral et administratif De l'Université Ibn khaldoun Tiaret.

Nos remerciements vont enfin à toute personne qui a contribué de près ou de loin à L'élaboration de ce travail.

* Et Merci *

Glossaire des Acronymes :

AVI	Audio Vidéo Interleave
B-FRAMES	Bi-directionalpredicted-FRAMES
BMP	bitmap
CODEC	Coder-Decoder
DCT	Discretecosinetransform
DWT	Discretewavelettransform
GIF	GraphicsInterchange Format
GOB	Group of Blocks
GOP	Group of Photos
HEVC	High EfficiencyVideoCoding
HVC	High VideoCoding
I-FRMES	Intra-FRAMES
JPEG	Joint Photographic Experts Group
LZW	Lempel-Ziv-Welche.
MPEG	Moving Picture Experts Group
MP4	MPEG-4
P-FRAMES	Predicted-FRAMES
PNG	Portable Network Graphics
TIFF	Tagged Image File Format
W	Watermark
I	Image
K	Key

Table de matières:

Liste des figures :

Introduction générale

Introduction générale

Ces derniers temps, avec le développement de la technologie de réseau, la protection des données multimédia devient de plus en plus importante. En raison de leur nature numérique, les données multimédia peuvent être dupliquées, modifiées, transformées et diffusées très facilement. La distribution plus rapide des données sur le réseau via les images, l'audio et la vidéo devient une ressource commune afin que toutes les données puissent être facilement transférées à l'autre personne en un seul clic. En raison de sa portabilité, la tendance du piratage et de la duplicité s'approche rapidement de l'Everest de nos jours. Le producteur d'origine du fichier ne sait même pas que le fichier créé par lui est disponible gratuitement via Internet et même s'il le sait, rien ne peut être fait. Ainsi, le développement récent de la technologie de tatouage numérique peut résoudre ce problème. Le filigrane est le processus pour masquer certaines données appelées filigrane ou étiquette dans les données d'origine. Un tatouage vidéo similaire intègre des données dans la vidéo à des fins d'identification, d'annotation et de droit d'auteur.

Ce mémoire est composé de quatre chapitres :

Dans le premier chapitre, on va présenter des notions de base sur la vidéo numérique.

Dans le deuxième chapitre, nous allons présenter un état de l’art en décrivant les principes généraux du tatouage ainsi que sur les algorithmes de base de tatouage vidéo.

Le troisième chapitre va décrire de manière détaillée l’algorithme de tatouage que nous avons élaboré au cœur de ce mémoire en terminant par manifester les résultats obtenus et les performances de la méthode de tatouage vidéo proposée.

Chapitre 1

Vidéo numérique

I.1 Introduction :

Les applications du traitement de vidéo sont multiples et interviennent dans de nombreux aspects de la vie courante et professionnelle.

La compression des données est souvent appelée codage, où le codage est un terme très général englobant toute représentation spéciale des données qui satisfait un besoin donné. Comme la compression des fichiers, l'objectif de la compression des médias est de réduire la taille du fichier et d'économiser de l'espace disque. Cependant, les algorithmes de compression des médias sont spécifiques à certains types de médias, tels que les fichiers image, audio et vidéo.

Dans ce chapitre, nous commençons tout d'abord par des notions de bases sur le vidéo et en donne un aperçu sur les méthodes de compression d'une manière général.

I.2 Définition de vidéo numérique :

La vidéo numérique est une collection d'images qui sont également espacées dans le temps.

I.3 Compression :

I.3.1 Compression en générale :

I.3.1.1 Définition de la compression :

En général, la compression des données consiste à prendre un flux de symboles et à les transformer en codes. La compression est effectuée par un programme qui utilise une formule ou un algorithme pour déterminer comment réduire la taille des données pour guanier l'espace de stockage.

La compression de données est également appelée codage source ou réduction de débit est le processus de modification, d'encodage ou de conversion de la structure des bits de données de manière à consommer moins d'espace sur le disque. Il permet de réduire la taille de stockage d'une ou plusieurs instances ou éléments de données.

L'objectif de la compression des données est de représenter une source d'information aussi précisément que possible en utilisant le plus petit espace de stockage.

I.3.1.2 Concepts de compression :

Il y a deux concepts de compression importants sont une compression à perte et sans perte :

I.3.1.2.1 Compression avec pertes :

Les techniques de compression à perte impliquent une certaine perte d'information, et les données qui ont été compressées à l'aide de techniques à perte ne peuvent généralement pas être récupérées ou reconstruites exactement. En contrepartie de l'acceptation de cette

distorsion dans la reconstruction, nous pouvons généralement obtenir des rapports de compression beaucoup plus élevés que ce qui est possible avec une compression sans perte [1]

I.3.1.2.2 Compression sans perte :

Avec la compression sans perte, les données sont compressées sans perte de données.

Les techniques de compression sans perte, comme leur nom l'indique, ne comportent aucune perte d'information. Si les données ont été compressées sans perte, les données d'origine peuvent être récupérées exactement à partir des données compressées. La compression sans perte est généralement utilisée pour les applications qui ne tolèrent aucune différence entre les données originales et les données reconstruites. [1]

Exemples de méthodes sans perte :

• codage en longueur, codage Huffman, méthode Lempel-Ziv-Welche (LZW).

I.3.1.3 Techniques de compression de base :

Compression de longueur ou RLE.

Codage des mots clés.

Codage adaptable de Huffman et algorithmes de LempelZiv.

DCT (transformée en cosinus discrète).

Compression par fractales.

Transforme d'ondelettes.

I.3.2 La compression d’image :

La compression d'image est une application de compression de données qui encode l'image originale avec quelques bits [2]. Les trois des plus courants formats de compression incluent JPEG, GIF et PNG. La compression JPEG, qui est couramment utilisée pour les photos numériques, intègre un algorithme de compression à perte qui se rapproche des couleurs proches et supprime les variations de couleur imperceptibles par l'œil humain. La compression GIF réduit la palette de couleurs d'une image à 256 couleurs ou moins, ce qui fournit un moyen efficace de représenter chaque couleur dans l'image. La compression PNG utilise un algorithme de compression sans perte qui filtre les données d'image et prédit des couleurs de pixels en fonction d'autres pixels proches. Bien que chacun de ces algorithmes fonctionne de différentes façons, ils peuvent être utilisés pour réduire la taille d'une image non compressée.

I.3.3 Compression de vidéo

Les algorithmes de compression vidéo ont un grand nombre d'applications allant de la vidéo conférence à la vidéo à la demande aux téléphones vidéo. Les normes de compression vidéo (telles que MPEG -1, 2, 4, 7) et les normes de téléconférence (telles que H.26X) sont des algorithmes essentiels utilisés dans ces applications et d'autres applications multimédia, dont la performance est très critique compte tenu des débits de données élevés Sont communs aux applications vidéo.

I.3.3.1 Définition

Le codage vidéo est le processus de compression et de décompression d'un signal vidéo numérique.[3]

Les technologies de compression vidéo sont en train de réduire et de supprimer les données vidéo redondantes afin qu'un fichier vidéo numérique puisse être envoyé efficacement sur un réseau et stocké sur des disques d'ordinateur. Avec des techniques de compression efficaces, une réduction significative de la taille du fichier peut être obtenue avec peu ou pas d'effets néfastes sur la qualité visuelle. La qualité de la vidéo, cependant, peut être affectée si la taille du fichier est encore abaissée en augmentant le niveau de compression pour une technique de compression donnée

Le but de la compression de la vidéo numérique c'est de prendre moins d'espace de stockage et de bande passante de transmission.

I.3.3.2 Vidéo codecs

Un codec est une norme de compression. La vidéo ou l'audio brut est compressé lors de l'encodage et décompressé (décodé) lors de la lecture. MP3 est un codec audio - une norme de compression que les lecteurs MP3 savent décoder, et les encodeurs MP3 savent comment encoder. Certains des plus importants sont H.264, HEVC, MPEG-2, Theora, VP8, VP9, JPEG2000, DivX, XviD et la famille WMV (vidéo) et MP3, AAC, Vorbis et la famille WMA (audio).

Un format est un conteneur de fichiers contenant un ou plusieurs codecs : vidéo, audio ou même des données. Le format du conteneur contient des informations sur les pistes de vidéo, audio et données qu'il détient.

I.3.3.3 Principes de compression vidéo

- La vidéo est simplement une séquence d'images numérisées et il est également appelé images animées.
- Une séquence vidéo peut être encodée avec l'algorithme JPEG frame by frame et cette approche est appelée Motion JPEG.

• En plus de la redondance spatiale présente dans chaque image, une redondance considérable est souvent présente entre les images successives.

• Les cadres sont classés comme 1 de 3 types de trame basiques (I-, Pand B-frames) et encodés différemment.

I.3.3.3.1 I-Frames (intra frame):

• Les images I sont codées indépendamment à l'aide de l'algorithme JPEG.

• Les images I sont insérées dans le flux de sortie relativement fréquemment.

• Les images I sont utilisées comme points d'accès pour l'accès aléatoire et la fonctionnalité FF / FR dans le flux de bits

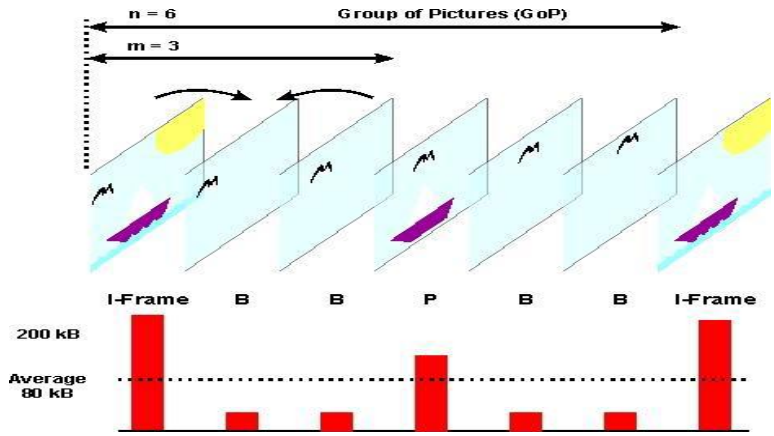


Figure 1 : image représente le diagramme d'I-Frame

I.3.3.3.2 P-Frames :

• Les cadres sont partitionnés en blocs de taille 16x16 (macro blocs).

• Pour encoder une trame P, le contenu de chaque macro bloc dans la trame cible est comparé sur un pixel par pixel avec le contenu de la trame de référence pour trouver un bloc de même taille identique.

• Le cadre de référence peut être un cadre P ou I.

• Le décalage (x, y) du macro bloc étant encodé et le bloc le mieux adapté est connu sous le nom de vecteur de mouvement.

• Ce processus de recherche de vecteur de mouvement est connu sous le nom d'estimation de mouvement.

• Une prédiction de la trame cible est réalisée avec la trame de référence en fonction des vecteurs de mouvement obtenus.

• La différence entre la trame prédite et la trame cible réelle est connue sous le nom d'erreur de prédiction.

• Compensation de mouvement : Des bits supplémentaires sont nécessaires pour coder l'erreur de prédiction afin de compenser la différence si nécessaire.

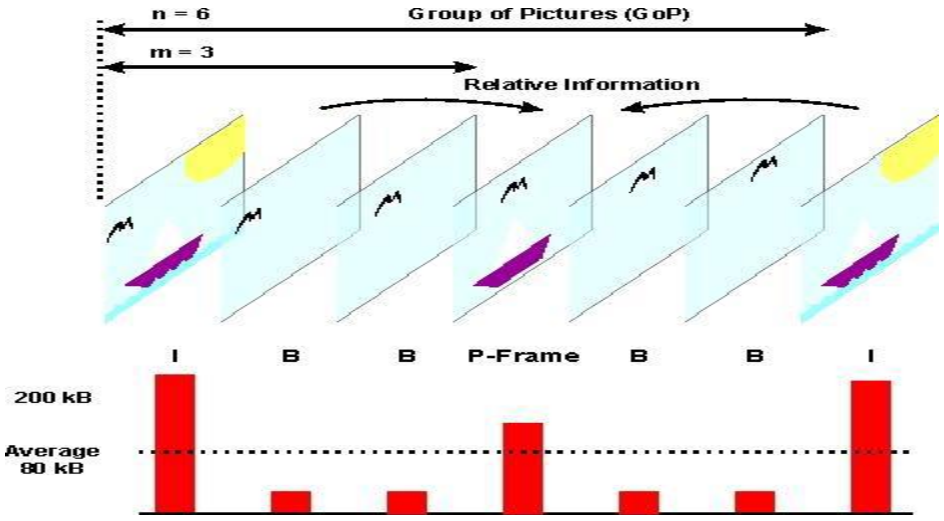


Figure 2 : image représente le diagramme de P-Frame

I.3.3.3.3 B-Frames :

• Pour encoder une trame B, tout mouvement est estimé en référence à la fois I ou P-frame immédiatement précédente et la trame P ou I immédiatement réussie.

• Les images B fournissent le plus haut niveau de compression.

• Les images B ne sont pas impliquées dans le codage d'autres images et ne propagent donc pas d'erreurs.

• Le nombre de trames entre les I-frames successifs est connu sous le nom d'un groupe d'images (GOP).

• Le nombre de trames entre un cadre P et le cadre I ou P immédiatement précédent s'appelle la plage de prédiction.

• L'ordre de codage et de transmission des cadres est modifié pour minimiser le temps requis pour décoder les images.

• Un quatrième type de cadre connu sous le nom de PB-frame a également été défini. Deux cadres voisins P et B sont codés comme s'ils étaient un cadre unique.

• Un 5ème type de cadre connu sous le nom de D-frame a été défini pour une utilisation dans les applications vidéo / vidéo à la demande.

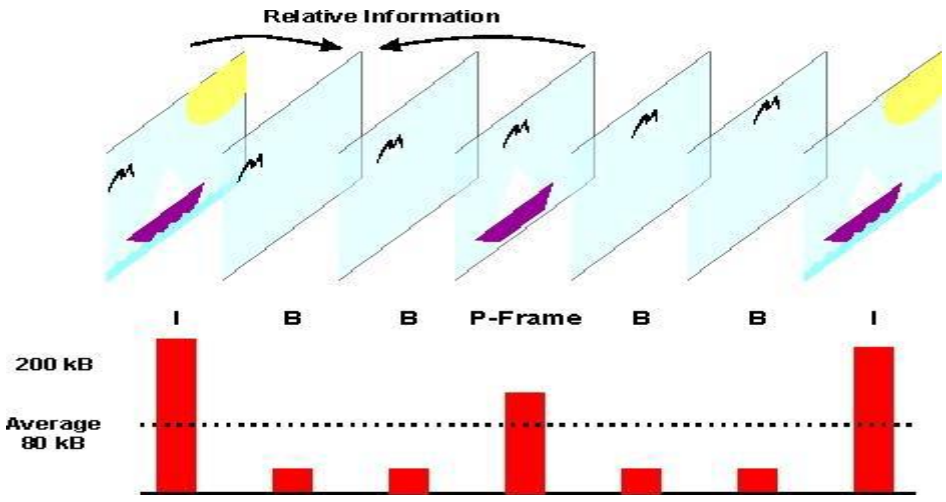


Figure 3 : image représente le diagramme de B-Frame

I.3.3.3.4 Format bit Stream basic :

• Type : type de trame, I, P ou B.

• Adresse : identifie l'emplacement du macro bloc dans le cadre.

• Valeur de quantification : la valeur de seuil utilisée pour quantifier tous les coefficients DCT dans le macro bloc.

• vecteur de mouvement : vecteur codé.

• Bloc présent : indique quel bloc dans le macro bloc est présent.

• Les chiffres typiques des rapports de compression.

• I-frames : 10 ~ 20 : 1.

• P-frames : 20 ~ 30 : 1.

• Cadres B : 30 ~ 50 : 1.

I.3.4 Format H.261

H261 est la norme internationale de compression vidéo la plus utilisée pour la vidéoconférence. Cette norme ITU (était CCITT) décrit les méthodes de codage et de décodage vidéo pour la composante d'image animée d'un service audiovisuel aux taux de p * 64 Kbps où p se situe dans la plage de 1 à 30. Les cibles standard et est réellement adapté pour Applications utilisant des réseaux à commutation de circuits comme canaux de transmission. [4]

Il supporte uniquement les frames I-frame et P-frame.

• Format de codage :

• Type : indique si le macro bloc est codé ou inter-codé

• Adresse : identifie l'emplacement du macro bloc dans le cadre

• Valeur de quantification : la valeur de seuil utilisée pour quantifier tous les coefficients DCT dans le macro bloc.

• vecteur de mouvement : vecteur codé

• Modèle de bloc codé : indique quel bloc dans le macro bloc est présent

• Code de début d'image : indique le début d'une nouvelle image.

• Référence temporelle : un horodatage pour le décodeur pour synchroniser les informations vidéo avec les informations audio.

• Type d'image : indique si la trame est codée en tant que cadre I ou P.

• Code de début GOB : est un marqueur de resynchronisation qui est utilisé pour la resynchronisation en cas d'erreur.

• Le groupe de bloc (macro) (GOP) est une structure composée de macro blocs 3x11.

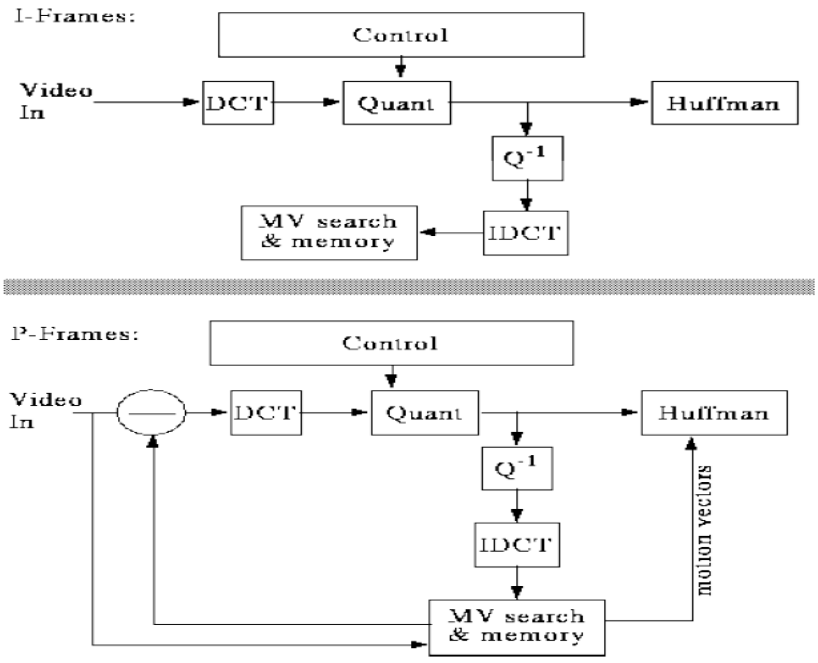


Figure 4 : la Structure bit Stream du format H261.

I.3.5 Format H.263

H.263 a été conçu pour des applications de codage à très faible débit. H.263 utilise la structure DCT à blocs compensés pour le codage. [5]

H.263 est une norme de compression vidéo de téléconférence développée par l'UIT, conçue pour des services de vidéo conversationnelle à faible débit.

• H.263 a été défini par l'UIT-T pour l'utilisation dans une gamme d'applications vidéo en temps réel sur les réseaux sans fil et les RTPC.

• Les applications comprennent la téléphonie vidéo, la visioconférence, la surveillance de la sécurité, les jeux interactifs, etc.

• La norme H.263 dispose d'un certain nombre d'options de codage avancées par rapport à H.261:

• Balayage progressif avec un taux de rafraîchissement de 15 ou 7,5 fps.

• Support I-, P-, B- et PB-frames.

• Les vecteurs de mouvement, si nécessaire, sont autorisés à pointer hors de la zone du cadre.

• Des schémas tels que le suivi des erreurs, le décodage indépendant des segments et la sélection de l'image de référence sont inclus dans la norme qui vise à minimiser les effets des erreurs sur les GOB voisins.

• Le schéma de dissimulation d'erreur est incorporé dans le décodeur pour masquer l'erreur du spectateur.

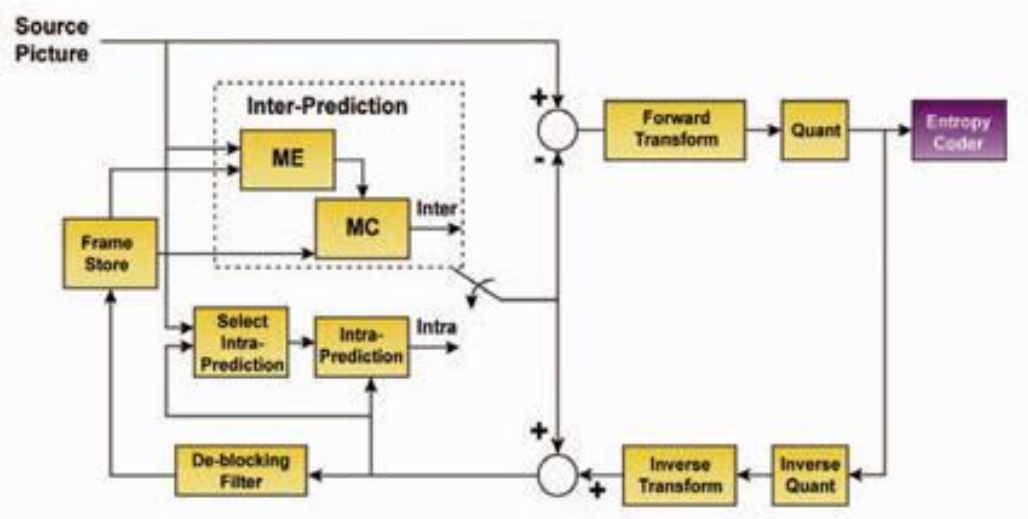


Figure 5 : codeur source du format H.263

I.3.6 Format H264 /AVC

La norme de codage vidéo avancée H.264 / MPEG-4 (H.264 / AVC) est la norme de codage vidéo la plus récente développée conjointement par le Groupe d'experts du codage vidéo UIT-T (VCEG) et le groupe d'experts ISO / IEC Moving Picture (MPEG). [6]

H.264, actuellement l'un des codecs vidéo fréquemment utilisés, est une compression populaire pour la vidéo HD. Étant donné que H.264 peut atteindre des vidéos de haute qualité dans des débits binaires relativement bas, il est couramment utilisé dans les caméscopes AVCHD, HDTV, Blu-ray et HD DVD. MP4 (.mp4) est l'un des formats vidéo codés H.264.

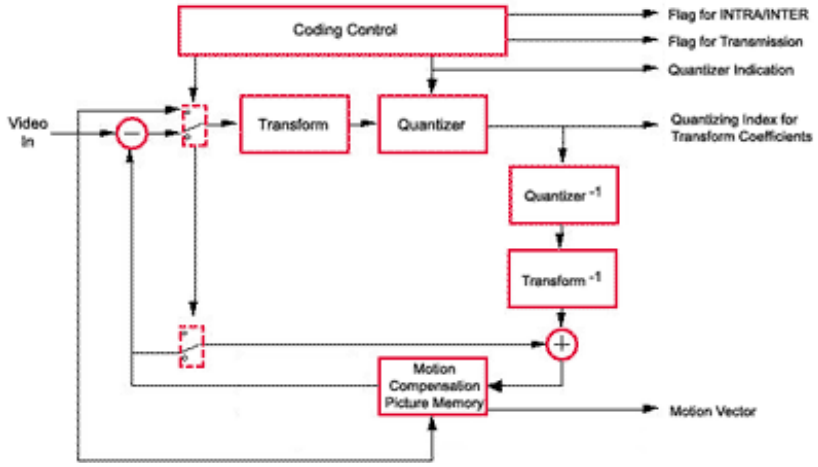


Figure 6 : Diagramme de bloc de codeur H.264.

I.3.7 Format H265/ HEVC

La norme de codage vidéo haute efficacité (HEVC) est le plus récent projet vidéo commun du Groupe d'experts du codage vidéo UIT-T (VCEG) et des organisations de normalisation MPEG (ISO / IEC Moving Picture Experts Group), travaillant ensemble dans un partenariat connu sous le nom de L'équipe collaborative conjointe sur le codage vidéo (JCT-VC) [7]. Il prend en charge les résolutions jusqu'à 8192 × 4320, y compris 8K UHD

HEVC a été développé dans le but de fournir deux fois l'efficacité de compression de la norme précédente, H.264 / AVC. Bien que les résultats d'efficacité de la compression varient en fonction du type de contenu et des paramètres du codeur, à des débits binaires de distribution vidéo typiques du consommateur, HEVC est généralement capable de compresser la vidéo deux fois plus efficacement qu'AVC.

• À un niveau identique de qualité visuelle, HEVC permet de compresser la vidéo vers un fichier qui est environ la moitié de la taille (ou la moitié du débit) d'AVC, ou lorsqu'il est comprimé sur la même taille de fichier ou débit que AVC, HEVC offre une qualité visuelle nettement meilleure.

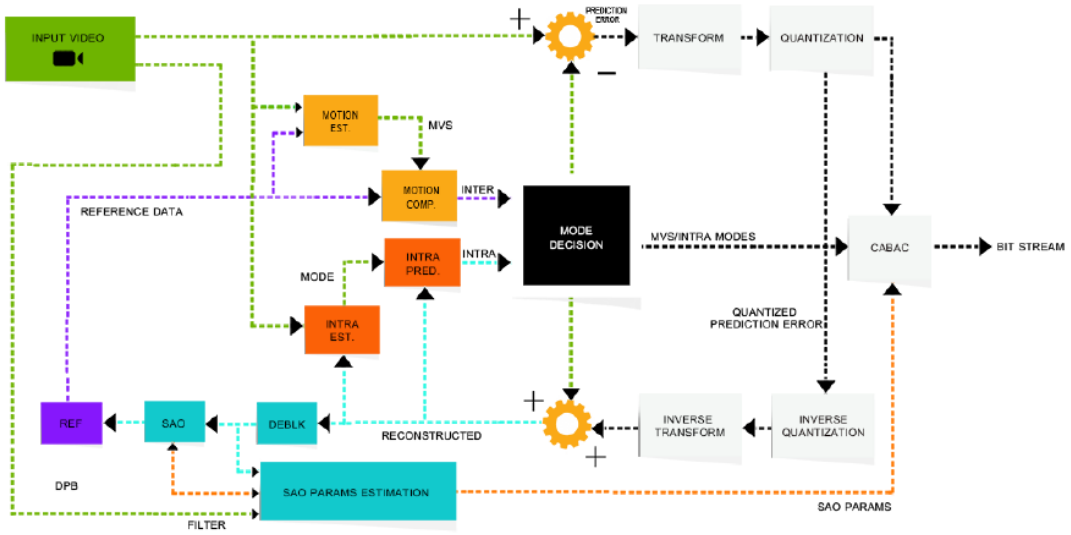


Figure7 : Schéma de principe du codeur HEVC.

I.3.8 Formats MPEG

The Motion Pictures Expert Group (MPEG) a été formé par l'ISO pour formuler un ensemble de normes relatives à une gamme d'applications multimédia impliquant l'utilisation de la vidéo avec le son. [8]

I.3.8.1 Format MPEG-1 :

La norme de compression vidéo MPEG est une norme de compression vidéo en couches, basée sur DCT qui se traduit par un flux vidéo compressé de qualité VHS qui a un débit d'environ 1,5 Mbps à une résolution d'environ 352x240. [9], [10]

• Technique de compression vidéo similaire à celle de H.261.

• Balayage progressif avec un taux de rafraîchissement de 30Hz (pour NTSC) et 25Hz (Pour PAL)

• Support I-, P- et B-frames.

• Les images I doivent être utilisées pour les différentes fonctions d'accès aléatoire associées aux magnétoscopes.

• Amélioration par rapport à H.261:

1. Une nouvelle couche appelée tranche est ajoutée dans la structure du flux afin que le décodeur puisse se resynchroniser plus rapidement en cas d'erreur.

2. supportent les B-frames.

3. plus grande fenêtre de recherche de vecteurs de mouvement et une résolution plus fine de sa représentation.

• Les chiffres typiques des rapports de compression

• I-frames : 10 : 1

• P-frames : 20 : 1

• B-frames : 50 : 1

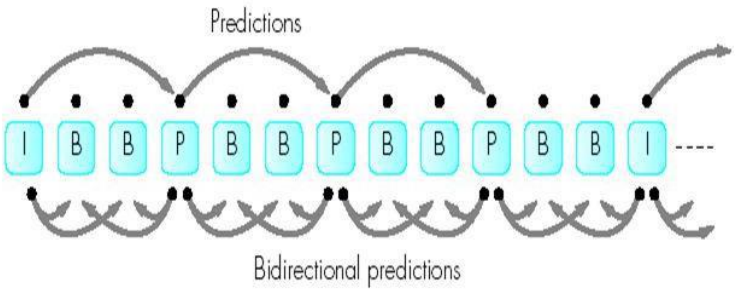


Figure 8 : frame de séquence MPEG-1

I.3.8.2 Format MPEG-2

Fondamentalement, le MPEG-2 peut être considéré comme un super-ensemble de la norme de codage MPEG-1 et a été conçu pour être compatible en arrière vers MPEG-1 - chaque décodeur compatible MPEG-2 peut décoder un flux de bits MPEG-1 valide. [11].

Le but original était une compression 10 fois meilleure que H.261

Les objectifs sont passés à

•Courbes de bits flexibles pour différentes capacités de récepteur

•L'interactivité basée sur le contenu avec le flux de données.

•L'indépendance du réseau (utilisé pour Internet, sans fil, etc.).

•Représentations basées sur des objets.

I.3.8.3 Format MPEG-4

MPEG-4 utilise des techniques similaires à M-JPEG, en ce qui concerne la mise en séquence. Il compare essentiellement deux images compressées, enregistre l'image et enregistre uniquement la différence à partir de chaque image séquentielle supplémentaire, comme le mouvement, ce qui permet d'économiser du temps, de l'espace mémoire et une puissance de traitement.[12]

Un taux de compression plus élevé fait partie des avantages de MPEG-4. Il peut synchroniser l'audio et la vidéo, et est idéal pour la visualisation en temps réel. MPEG-4 a été conçu pour prendre en charge les applications à faible bande passante.

Les inconvénients de MPEG-4 incluent une qualité d'image inférieure (M-JPEG), et il est autorisé, ce qui permet aux téléspectateurs d'avoir des frais supplémentaires. Il prend en charge un nombre réduit de caméras, comme les caméras mégapixels.

I.4 Protection

I.4.1 La cryptographie

Signifie « écriture secrète ». La cryptographie est une méthode largement utilisée pour protéger le contenu numérique des médias. Le message est chiffré avant la transmission et déchiffré côté récepteur à l'aide d'une clé. Personne ne peut accéder au contenu sans avoir la vraie clé. Il existe deux types de cryptographie

1. Cryptographie à clé symétrique
2. Cryptographie à clé asymétrique

En cryptographie à clé symétrique, la même clé (clé secrète) est utilisée à la fois pour le chiffrement et le déchiffrement. La clé secrète doit donc être transférée entre les expéditeurs et le récepteur via un support sécurisé. Si cela est possible, les données réelles peuvent être transférées via ce support lui-même. Si supposons que n nombre d'utilisateurs doivent envoyer des données sécurisées à n nombre d'utilisateurs, l'utilisation de la clé secrète sera (n * (n-1)) / 2.

En cryptographie à clé asymétrique, deux clés appelées clé publique et clé privée. Chaque utilisateur possède une clé privée et une clé publique. La clé publique est utilisée pour crypter les données et la clé privée est utilisée pour décrypter les données. Dans le processus de cryptage, l'expéditeur doit utiliser la clé publique du récepteur pour crypter les données. Et le récepteur doit utiliser sa propre clé privée pour décrypter les données. Il n'y a donc pas de transmission de clés et l'entretien des clés est également réduit.

I.4.2 La stéganographie

Signifie « écriture de couverture ». La stéganographie est la science qui implique la communication de données secrètes dans un support multimédia approprié, par exemple des fichiers image, audio et vidéo. Elle est toujours non visible. En stéganographie, le message est intégré dans les médias numériques plutôt que de le chiffrer de telle manière que personne, à l'exception de l'expéditeur et du destinataire prévu, ne réalise même qu'il existe un message caché. Le message caché dans la couverture ne peut être détecté que par la personne possédant la clé réelle. Ainsi, la stéganographie concerne la couverture de la communication point à point entre deux parités. C'est pourquoi les méthodes de stéganographie ne sont généralement pas robustes contre la modification des données, ou n'ont qu'une robustesse limitée.

I.5 Conclusion

Dans ce chapitre, nous avons décrit les différentes normes de compression y compris la compression d'images et de vidéo. La protection de flux multimédia véhiculés sur les réseaux ou transmis et utilisés en/hors lignes exige des techniques de protection de droits d'auteurs et de contrôle d'intégrité. Dans le prochain chapitre nous allons présenter une solution de protection du contenu numérique appelée le tatouage numérique en décrivant ainsi ses propriétés et son domaine d'utilisation.

Chapitre 2

Tatouage numérique

II.1 Introduction

En raison du développement rapide d'Internet, les utilisations des données multimédias comme l'audio, l'image et la vidéo deviennent très populaires. La transmission de contenus numériques est une tâche facile mais le maintien de la propriété est difficile, car différentes techniques ont été proposées. L'une des principales techniques de protection sténographique du droit d'auteur est le tatouage numérique. Le concept du tatouage numérique est dérivé une filigrane vidéo est utilisé pour fournir une authentification pour le contenu vidéo. Les différentes techniques de tatouage vidéo ont été développées, mais ces techniques ne résistent qu'aux attaques de base non résistantes aux attaques de traitement vidéo telles que la perte de trame, la permutation de trames et la moyenne et l'ajout de bruit, etc.

Dans ce chapitre, nous présenterons le principe du tatouage numérique des images/video ainsi que quelques-unes de ses applications, et les différentes étapes qui conduisent à l'insertion de la marque. Ensuite nous décrirons quelques représentations de l'image dans le domaine spatial et fréquentiel, et aussi les différentes applications possibles du tatouage numérique pour les vidéos.

II.2 Définition du tatouage numérique

Le tatouage numérique ou watermarking est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement message, est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte. [13]

II.3 Différences avec la cryptographie

En cryptographie, l’objectif n’est pas de dissimuler des informations dans d’autres, mais plus simplement de rendre l’information que l’ont désiré transmettre complètement illisible à toute personne ne possédant pas la donnée nécessaire à son décodage. De plus en cryptographie si le message primaire est modifié, il devrait être impossible de le recouvrer, tandis qu’en sténographie, le message secondaire est supposé rester accessible et ce même après de multiples recopies et manipulations diverses du message primaire [13].

II.4 Propriété de tatouage

On distingue généralement deux classes du tatouage : visible et invisible.

II.4.1 Tatouage visible

Le tatouage visible est très simple. Il est équivalent à l'estampage d'un watremark sur le papier, et pour cette raison il est appelé parfois estampage numérique. Le tatouage visible altère le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photo ajoutent un watermark visible en forme de copyright (©) aux versions de prévisualisation (basse résolution) de leurs photos. Ceci afin d'éviter que ces versions ne se substituent aux versions hautes résolutions payantes.

Le tatouage visible est un sujet à controverse. Il y a une branche de chercheurs qui disent que si le watermark est visible, alors elle peut être facilement attaquée. Néanmoins, nous trouvons des applications qui demandent que le watermark soit visible, c'est le cas du logo des sociétés dans les programmes télévisuels [14].

Figure 9 Exemple d'un tatouage visible .

Figure 10 Exemple d'un tatouage visible

II.4.2 Tatouage invisible

En revanche, le tatouage invisible est un concept beaucoup plus complexe. Le tatouage invisible modifie le signal d'une manière imperceptible par l'utilisateur final. Pour reprendre l'exemple de l'agence de photo, les photos hautes résolutions vendues par l'agence possèdent elles au contraire un watermark invisible, qui ne dégrade donc pas le contenu visuel, mais qui permet de détecter l'éventuelle source d'un vol. Le message caché par le tatouage peut être un identifiant de l'acheteur par exemple. En cas d'utilisation non-autorisée, l'agence peut alors se retourner contre l'acheteur.

Le tatouage invisible est l'approche la plus développée qui attire la plupart des chercheurs. La majorité des techniques concernant la protection des propriétés intellectuelles suivent cette branche.

Dans ce qui suit, nous nous concentrons sur cette dernière catégorie, et le mot « Tatouage » est pris au sens du tatouage invisible [15].

Figure 11 Exemple d'un tatouage invisible

II.5 Caractéristiques du tatouage numérique

Le tatouage est une technique consistant à incorporer des données cachées dans les informations du système multimédia de manière visible, comme les informations d'image, vidéo, audio et texte à des fins d'identification et de droit d'auteur. Les principales caractéristiques du tatouage numérique sont donc nécessaires pour concevoir une vidéo tatouée robuste qui sont :

II.5.1 Robustesse

La robustesse représente la capacité du tatouage à résister aux dégradations du document tatoué. Ces modifications définissent l'ensemble des attaques qu'elles soient

intentionnelles ou non intentionnelles. Le premier type d'attaques vise à supprimer la marque insérée dans un document, tandis que le deuxième type d'attaque n'a pas pour objectif de supprimer la marque mais plutôt l'altérer. Selon le critère de robustesse on distingue trois types du tatouage numérique :

- Tatouage robuste : Un système de tatouage est dit robuste, si la détection de la marque est effective même si le document tatoué a été altéré ou attaqué. Un système de tatouage robuste doit résister aux opérations licites effectuées sur le document numérique (compression, conversion analogique-numérique, filtrage, etc.) et celles illicites (attaques malveillantes des pirates).
- Tatouage fragile : Dans le tatouage fragile, la marque est très sensible aux modifications du document tatoué. Cette technique sert à prouver l'authenticité et l'intégrité d'un document tatoué. Une technique de tatouage fragile devrait détecter (avec une forte probabilité) toute altération du document tatoué. Une comparaison de la marque extraite et de la marque originale est effectuée afin d'identifier si le document est manipulé ou pas.
- Tatouage semi-fragile : Il combine les caractéristiques du tatouage robuste et fragile pour avoir une situation intermédiaire, dans laquelle la marque est robuste pour un ensemble défini de dégradations, et fragile à d'autres.

II.5.2 Imperceptibilité :

L'image tatouée devrait ressembler à l'image originale à l'œil normal. Le spectateur ne peut pas détecter qu'un tatouage y est intégré.

II.5.3 Sécurité :

Une personne non autorisée ne peut pas détecter, récupérer ou modifier le tatouage intégré.

II.5.4 Capacité :

La quantité d'informations intégrées doit être suffisamment importante pour identifier de manière unique le propriétaire de la vidéo.

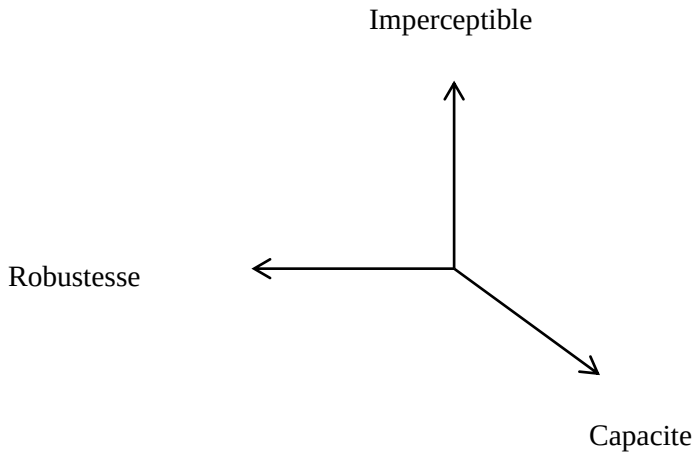


Figure 12 Contraintes du tatouage numérique

II.6 Modèle générique du tatouage

Le schéma du tatouage numérique est résumé dans la figure 2.8. Le système typique du tatouage numérique comprend deux sous-systèmes : le sous-système d'insertion du watermark (appelé aussi la phase de codage) et le sous-système de détection/extraction (appelé aussi la phase de décodage). Le sous-système d'insertion (Embedding) comprend en entrée un watermark W, un document hôte (porteur) I et une clé secrète K spécifique au tatoueur. Cette dernière est utilisée pour renforcer la sécurité de tout le système. La phase d'insertion génère en sortie un document tatoué Iw. Cette phase est modélisée par la fonction suivante :

$Iw = E(I,W,K)$ (2.1)

Le document tatoué IW est ensuite copié et attaqué, ce qui est modélisé par la transmission dans un canal soumis à bruit. Le document reçu est appelé I*w. La réception du document consiste en deux parties : d'une part la détection du watermark et d'autre part, s'il est présent son décodage (extraction).

La phase de (détection/extraction) prend en entrée le document tatoué et éventuellement attaqué I*w, la clé K et éventuellement le document original I et/ou le watermark originel W. La phase de détection consiste à prouver la présence d'un watermark en utilisant une mesure de confidentialité ρ. Elle est modélisée par la fonction :

$\rho = D(I^*w, K,..)$ (2.2)

La phase d'extraction consiste à calculer une estimation W ′ de W. Elle est modélisée par la fonction :

W ′ = D (I∗w ,K,..) (2.3)

- I et W sont des paramètres optionnels pour la fonction D.

Pour un système de tatouage typique, plusieurs conditions doivent être satisfaites :

- Le watermark W ′ doit être détecté à partir de Iw avec/ou sans la connaissance explicite du I.
- Si Iw n'est pas modifié (attaqué), alors W ′ correspond exactement à W [7].

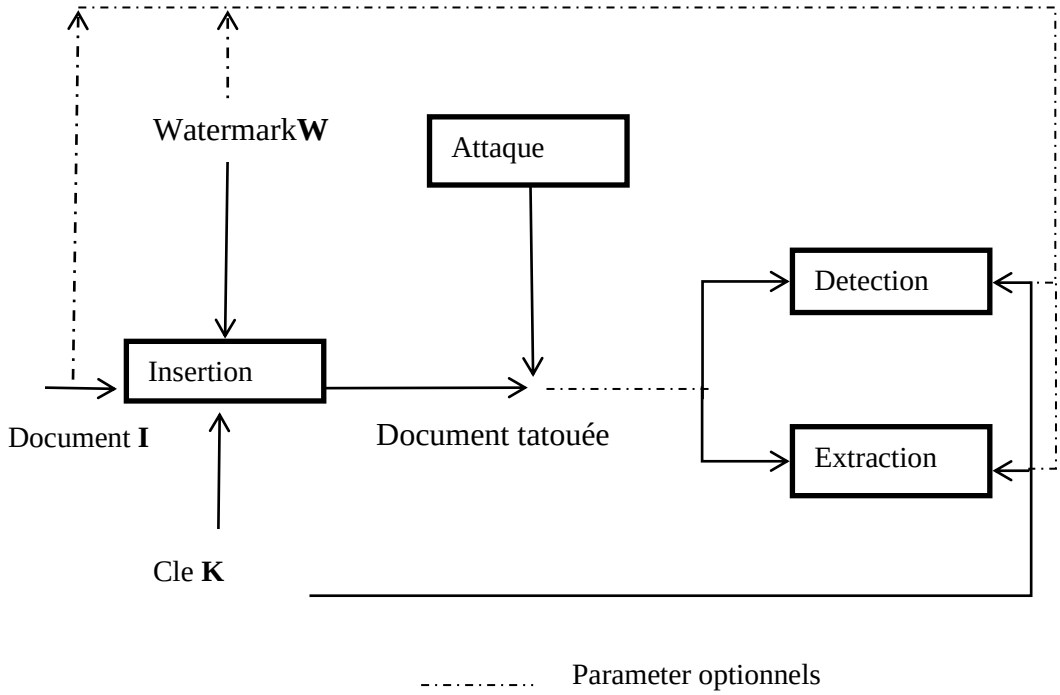


Figure 13 Modèle générique d'un système du tatouage .

– Pour un tatouage robuste, si Iw est attaqué, W ′ doit correspondre à W, afin de donner un jugement clair de l'existence du watermark.

– Pour un tatouage fragile, W ′ doit être partiellement ou totalement différente à W, après des petites modifications de Iw.

II.7 Applications du tatouage vidéo

Le tatouage numérique est utilisé dans diverses applications, dont certaines :

II.7.1 Identification du contenu et tatouage numérique :

Dans cette technique, le tatouage numérique permet une identification efficace du contenu en fournissant une identité numérique unique à toutes les formes de contenu

multimédia d'une manière qui persiste avec le contenu partout où il peut voyager. Tatouage numérique facilement intégré dans le contenu sans interférer avec le plaisir du consommateur. Il est imperceptible pour l'homme, mais facilement détecté et compris par les ordinateurs, les réseaux et une large gamme d'appareils numériques courants.

II.7.2 Protection du droit d'auteur :

Ces dernières années, la protection du droit d'auteur du numérique est devenue un problème grave en raison du développement rapide de la technologie. Le tatouage est l'une des alternatives au problème de protection des droits d'auteur. Dans cette technique, un tatouage est ajouté au signal vidéo qui transporte des informations sur l'expéditeur et le récepteur.

II.7.3 Surveillance de la diffusion

Dans cette technique, le propriétaire du contenu incorpore le tatouage avant la transmission. Le tatouage est extrait par le site de surveillance qui est installé dans la zone de transmission

II.7.4 Contrôle de copie :

Tatouage dans le contrôle de copie

- combiner chaque enregistreur de contenu avec un détecteur de filigrane.
- Lorsqu'un filigrane d'interdiction de copie est détecté, l'appareil d'enregistrement refuse de copier.

II.7.5 Altération des images :

Une autre application est l'authentification du contenu des images. Le but de cette application est de détecter toutes les alternatives et modifications apportées à une image.

II.8 Classification selon le domaine d'insertion

Les techniques courantes décrites dans la littérature peuvent être regroupées en deux principales classes : techniques travaillant dans le domaine spatial et techniques travaillant dans le domaine fréquentiel.

II.8.1 Domaine Spatial

Dans les techniques spatiales, le watermark est inséré en modifiant directement les valeurs de pixels de l'image hôte. Ce sont des méthodes simples et peu couteuses en temps de calcul. Elles sont consacrées aux tatouages en temps réel demandés dans des environnements de faible puissance. Certaines techniques dans le domaine spatial peuvent être robustes aux attaques de type transformations géométriques.

Plusieurs méthodes, proposées dans la littérature, modifient les bits de poids faible LSB de l'image hôte. L'invisibilité du watermark est obtenue par l'hypothèse que les données contenues dans les bits LSB sont visuellement insignifiantes.

II.8.2 Domaine Fréquentiel

Les méthodes présentées précédemment permettent en général de retrouver le watermark en faisant la différence entre l'image originale et l'image tatouée. Cela leur confère un sérieux désavantage : une personne qui voudrait attaquer ces images et qui se serait procurée une image originale, ou bien plusieurs personnes mettant en commun leurs images tatouées peuvent détruire le watermark. Des algorithmes incluant le watermark non pas directement dans l'image, mais dans une transformée de l'image seront à cet égard plus robustes, et permettent en plus de choisir les pixels qui seront plus résistants à certains types d'attaques.

Le tatouage dans le domaine fréquentiel est obtenu après l'utilisation de l'une des transformées comme la DFT (transformée de Fourier discrète), la DCT (transformée en cosinus discrète), DWT (la transformée en ondelettes) ou d'autres transformées.

II.9 Conclusion

Dans ce chapitre, différents types de techniques de tatouage sont revisités et les propriétés spécifiques dans divers domaines ont été discutés et les applications importantes du tatouage sont répertoriées. Cependant, la faiblesse des algorithmes existants comprend :

Le filigrane vidéo n'est pas robuste aux attaques telles que la perte d'images, la moyenne et l'analyse statistique, l'échange et l'ajout de bruit.

Chapitre 3

Approche proposée

Et

Résultats expérimentaux

III.1 Introduction

La notion d'intégrité est un concept très répandu dans le domaine de sécurité de multimédia. Elle permet d'assurer que le contenu informatif des données reçu soit rigoureusement identique à celles émises. Les approches de tatouages fragiles visent à détecter toutes modifications appliquées au document multimédia tatoué quel que soit son type (image, audio, vidéo,). En cas d'images et de vidéos numériques, ces modifications peuvent être classées sous forme d'attaques. Parmi les attaques courantes, on trouve :

- L'ajout d'un bruit gaussien ou non,
- Le filtrage linéaire (ex. : passe-haut ou passe-bas),
- Le filtrage non linéaire (ex. : filtrage médian),
- La compression (ex. : JPEG, MPEG, JPEG2000...),
- La quantification,
- La permutation,
- La rotation,
- Le zoom,
- Le décalage spatial ou temporel,
- La suppression ou l'ajout d'échantillons ou de pixels,
- Le moyennage des données,
- Le moyennage de différentes copies avec différentes marques,
- La conversion numérique - analogique puis analogique numérique -
- Puis re-numérisation d'une image via un scanner).

Dans ce chapitre, nous allons appliquer une approche de tatouage d'images connu sous le nom Koch & Zhao sur une séquence vidéo claire. Cette approche permet d'insérer la marque en utilisant la transformée en cosinus discrète. Après avoir présenté cette approche, nous allons l'évaluer par la soumettre à différentes attaques et de calculer des métriques objectives comme le PSNR et SSIM.

III.2 Transformée en cosinus discrète :

La DCT offre un bon compromis entre la capacité de regroupement d'informations et la complexité de calcul. La propriété de compactage d'énergie la plus importante du DCT est largement utilisée pour représenter une image

DCT est plus rapide et peut être implémenté dans les opérations O (n log n). Le DCT permet à une image d'être divisée en différentes bandes de fréquences, ce qui facilite beaucoup l'intégration des informations de filigrane dans les bandes de fréquences moyennes d'une image. Les bandes de fréquences moyennes sont choisies de manière à éviter les parties les plus visuelles importantes de l'image (basses fréquences) sans se surexposer à l'élimination par compression et attaques de bruit (haute fréquence). Le DCT transforme un signal ou une image du domaine spatial au domaine fréquentiel. Le schéma de filigrane basé sur DCT est le plus robuste à la compression avec perte.

La DCT est une fonction de transformation très populaire utilisée dans le traitement du signal. Il transforme un signal du domaine spatial au domaine fréquentiel. En raison de la bonne performance, il a été utilisé dans la norme JPEG pour la compression d'image. DCT a été appliqué dans de nombreux domaines tels que la compression de données, la reconnaissance de formes, l'image traitement, et ainsi de suite. La transformée DCT et sa manière inverse peuvent être exprimées comme suit :

$$F(u,v) = \frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} f(j,k)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}], \quad (1)$$

$$f(j,k) = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} C(u)C(v)F(u,v)\cos[\frac{(2j+1)u\pi}{2n}]\cos[\frac{(2k+1)v\pi}{2n}], \quad (2)$$

where

$C(w) = 1/\sqrt{2}$ when $w = 0$

$C(w) = 1$ when $w = 1,2,3,\ldots\ n-1$

En tant qu'image transformée par le DCT, elle est généralement divisée en m ´ m bloc. En général, un bloc se compose toujours de 8´8 composants. Le bloc les coefficients sont indiqués dans la figure (6).

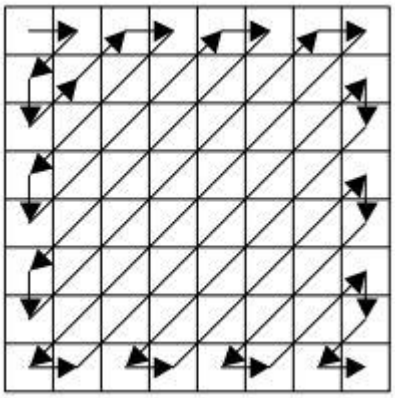


Figure 14 : Le coefficient de bloc DCT et le zig-zag

Le coefficient supérieur gauche est la valeur DC tandis que le coefficient d'autres représentent des composants AC. La permutation de balayage en zigzag est implicite distribution d'énergie de haute à basse ainsi que de basse fréquence à haute fréquence de la même manière. Les yeux humains sont plus sensibles au bruit dans les basses fréquences bande supérieure à une fréquence plus élevée. L'énergie de l'image naturelle est concentrée dans le bas gamme de fréquences. Le filigrane caché dans la bande de fréquence supérieure peut être jeté après une compression avec perte. Par conséquent, le filigrane est toujours intégré dans la plage de bande inférieure de l'image hôte transformée par DCT est une sélection parfaite. Les coefficients de bande inférieure du bloc DCT sont décrits comme sur la figure 15.

	1	5	6				
2	4	7					
3	8						

Figure 15 : Les huit coefficients de bande inférieure

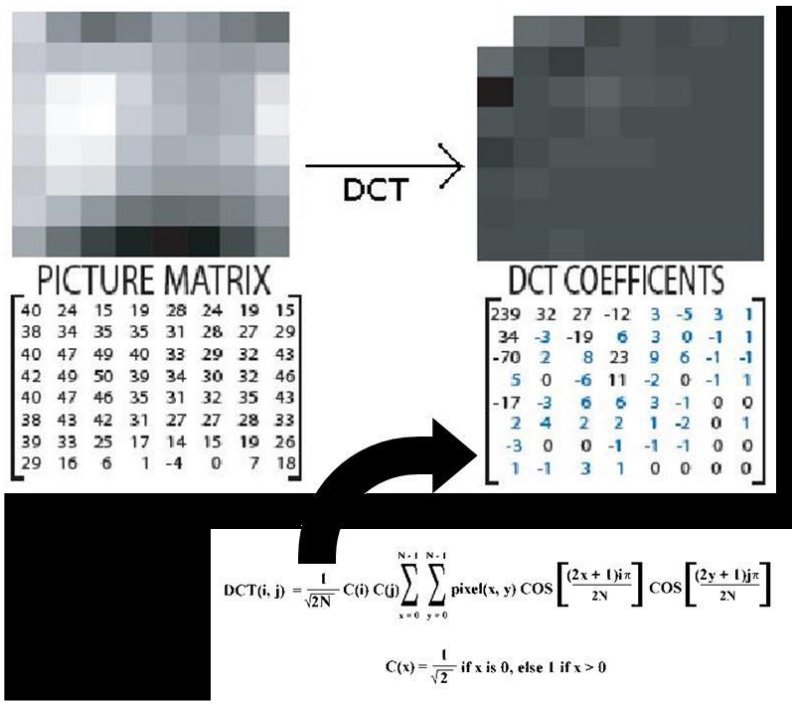


Figure 16 : Transformation de la matrice d'image 8 x 8 aux coefficients DCT

III.3 Techniques de tatouage vidéo

Le procédé de tatouage peut être soit directement inséré dans les données vidéo, soit intégré pendant le processus de codage ou implémenté après compression sur les données vidéo. Nous allons maintenant discuter brièvement de certaines techniques courantes de tatouage vidéo.

L'approche de Koch & Zhao consiste tout d'abord à diviser l'image à tatouer en un certain nombre de carrés ou blocs de 8x8 pixels, puis à effectuer la transformée en cosinus de ces blocs. Les bits de la marque sont alors insérés sur les moyennes fréquences, sachant que la modification des basses fréquences modifierait trop l'image et que les hautes fréquences sont enlevées et remises à zéro par la plupart des techniques de compression qui emploient la quantification pour réduire la taille de l'image ou la vidéo à comprimer. La clé de codage utilisée correspond à l'emplacement des blocs marqués, et est nécessaire pour décoder le tatouage. Par contre, l'algorithme d'extraction n'a besoin ni du support non marqué, ni de la marque ; autrement dit, l'extraction n'a besoin que de l'image ou la vidéo tatouée.

III.3.1 Algorithme d'insertion

1. Soit une séquence de k bits $(b_1, \ldots, b_k)$ à cacher dans l'image
2. Sélectionner dans l'image (selon une clé secrète) k blocs B $(B_1, \ldots, B_k)$ de taille 8x8.
3. Calculer les coefficients DCT $(a_{11}, \ldots a_{88})$ de chaque bloc sélectionné, si nécessaire.
4. Pour i allant de 1 à k :
   Soient (a_{kl}) et (a_{mn}) deux des coefficients DCT du bloc B_i, et b_i le bit à cacher
   - Si $\{(b_i = 1)$ et $(a_{kl})_i > (a_{mn})_i\}$ ou $\{(b_i = 0)$ et $(a_{kl})_i < (a_{mn})_i\}$, alors ne rien faire.
   - Sinon modifier les valeurs de $(a_{kl})_i$ et $(a_{mn})_i$ pour que la relation précédente soit vérifiée.
5. Calculer la DCT inverse à partir des valeurs ainsi modifiées afin d'obtenir l'image marquée, et revenir dans le domaine spatial, si besoin est.

Figure 17 Algorithme d'insertion Koch &Zhao

III.3.2 Algorithme d'extraction

1. Retrouver les blocs marqués grâce à la clé secrète.
2. Calculer les coefficients DCT associés aux blocs sélectionnés.
3. Comparer les valeurs des coefficients DCT afin de déterminer si le bit concerné du message était un "0" ou un "1".

Figure 18 Algorithme d'extraction Koch &Zhao

III.4 Résultats expérimentaux

L'approche présentée précédemment est proposée pour le tatouage d'images numériques. Comme la vidéo numérique sous ses différentes normes de codage (mpeg1, mpeg2, avi, …) est une séquence d'images numérique, nous avons tenté de l'appliquer pour chaque trame de la séquence. Pour cela, nous avons suivre un certain nombre d'étapes pour le tatouage d'une vidéo numérique comme le montre la figure 19.

III.4.1 Procédure de tatouage vidéo

1. Extraire les trames (frames) de cette vidéo
2. choisir une séquence de trames à partir de l'ensemble extraite.
3. Extraire la composante luminance en convertissant l'espace de couleur des trames tatoués en niveau de gris.
4. Appliquer l'approche de Koch & Zhao pour chaque trame.
5. Regrouper les trames tatouées pour avoir la vidéo tatouée.

III.4.2 Procédure d'extraction de la marque

1. Prendre la vidéo tatouée

2. Extraire les frames que nous avons déjà tatoués

3. Pour chaque image tatouée, extraire la composante de luminance.

4. Deviser chaque image en blocs de 8 * 8 pixels.

5. Appliquer la transformée de Dct pour chaque bloc.

6. Formez toutes les colonnes dans un tableau N *M (N et M sont les dimensions de la marque) et trouvez la différence entre les blocs.

7. Si Différence> = 0, définissez la valeur du bloc de la marque sur 0 et

Si Différence <0, définissez la valeur du bloc de la marque sur 1

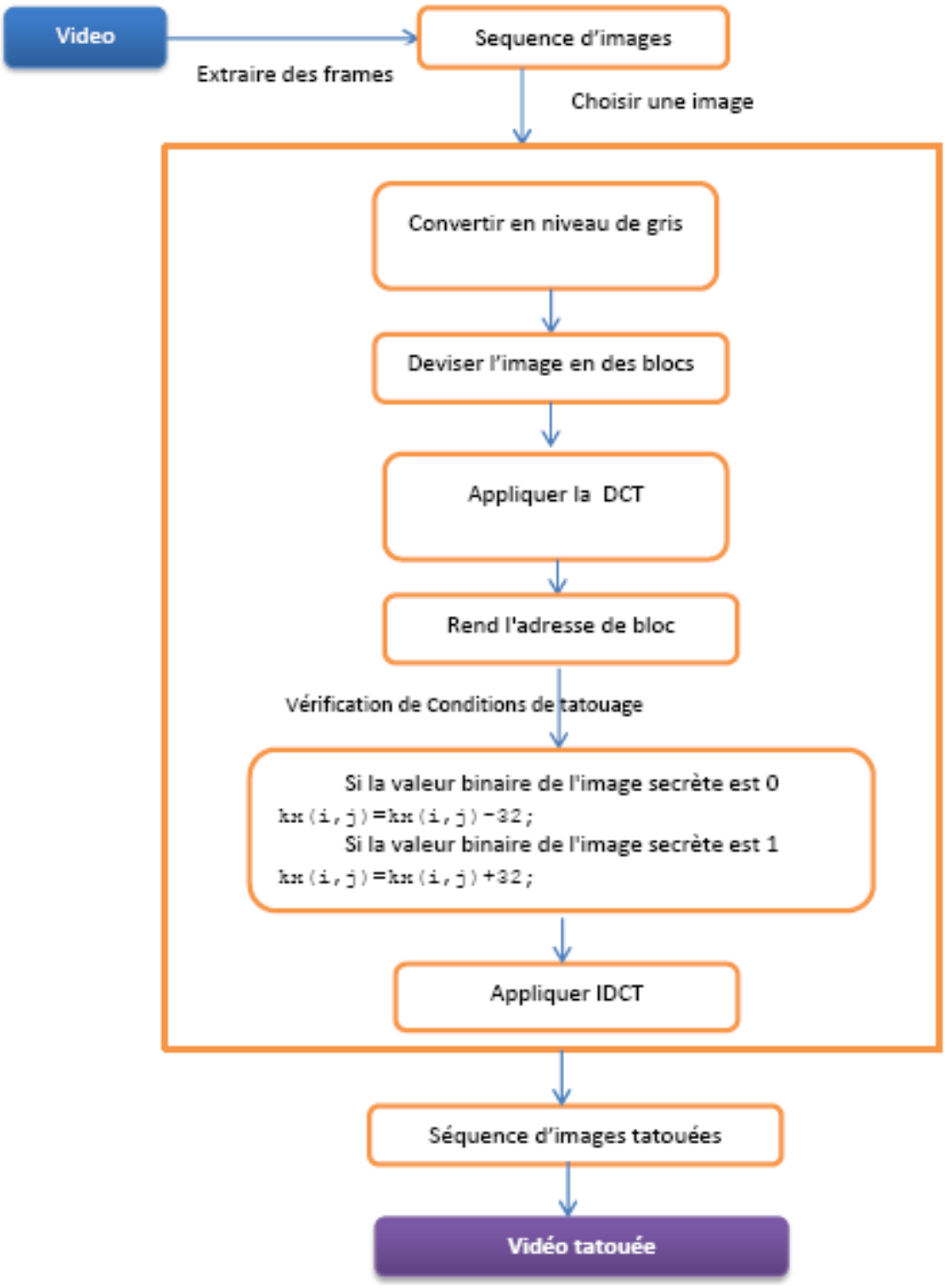


Figure 19 Procédure de tatouage vidéo

III.4.3 Implémentation et interfaces :

Nous avons implémenté notre approche en Matlab, où nous avons créé une interface principale permettant de choisir entre l'insertion ou l'extraction de la marque (figure 20, 21, 22).

.

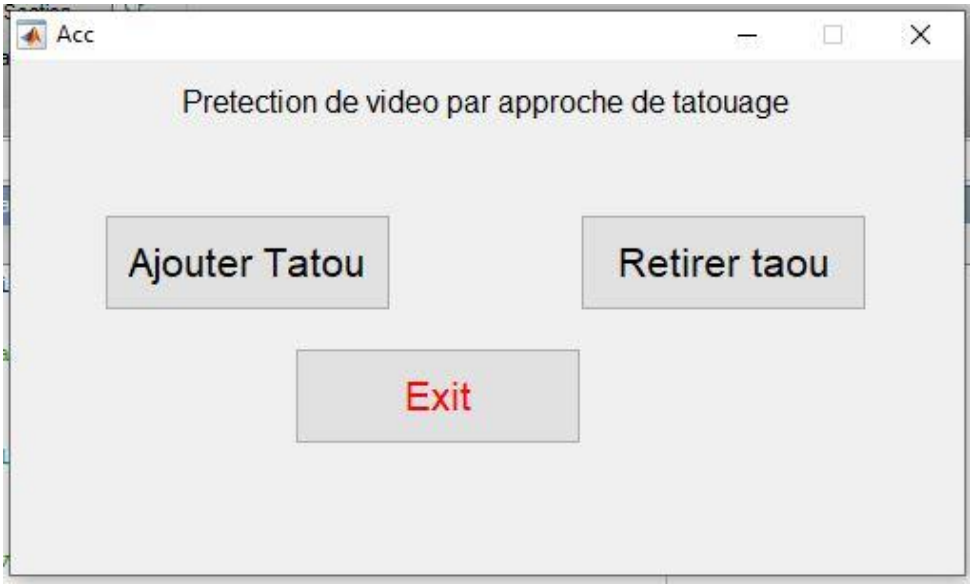


Figure 20 interface principale

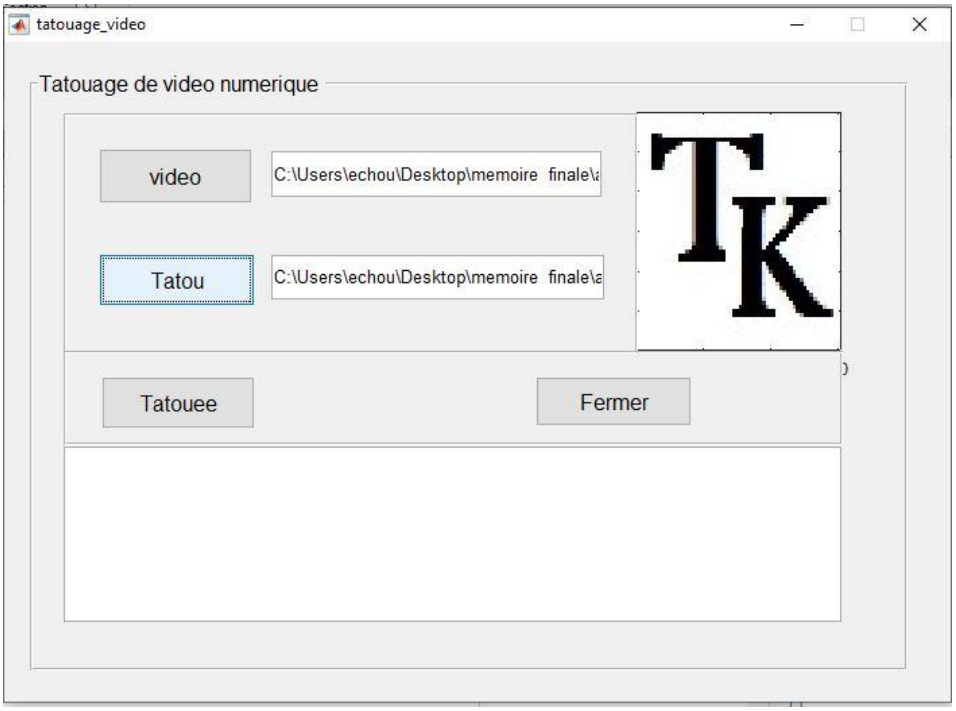


Figure 21 interfaces d'insertion de la marque

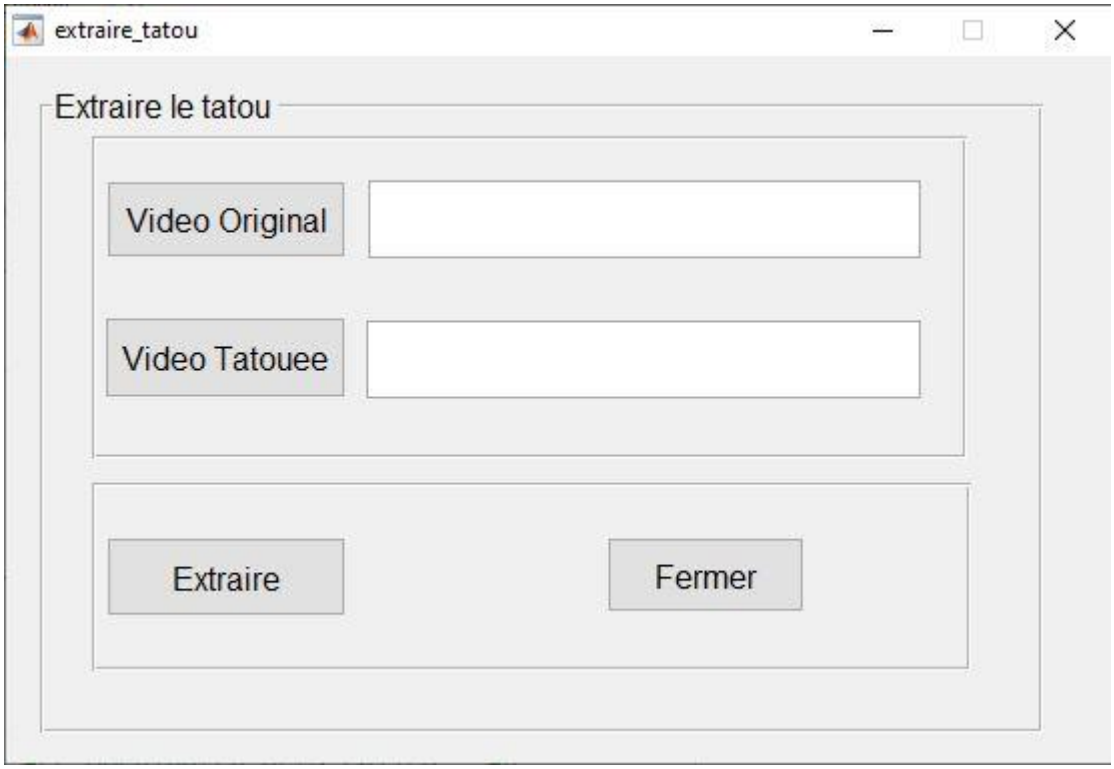


Figure 22 interfaces d'extraction de la marque.

III.4.4 Qualité visuelle de l'approche proposée

La vidéo choisie pour le tatouage comprend plus de 450 trames, la figure 23 montre le résultat de tatouage de notre séquence ou nous avons appliqué le tatouage à la composante de luminance uniquement, la marque est une séquence binaire de 32×32 bits donc elle est de 1024 bits.

(a)

(b)

(c)

Figure 23 (a) trame claire, (b) trame tatouée, (c) la marque.

La marque est invisible après le tatouage et la qualité visuelle est fortement proche de celle de la trame en claire.

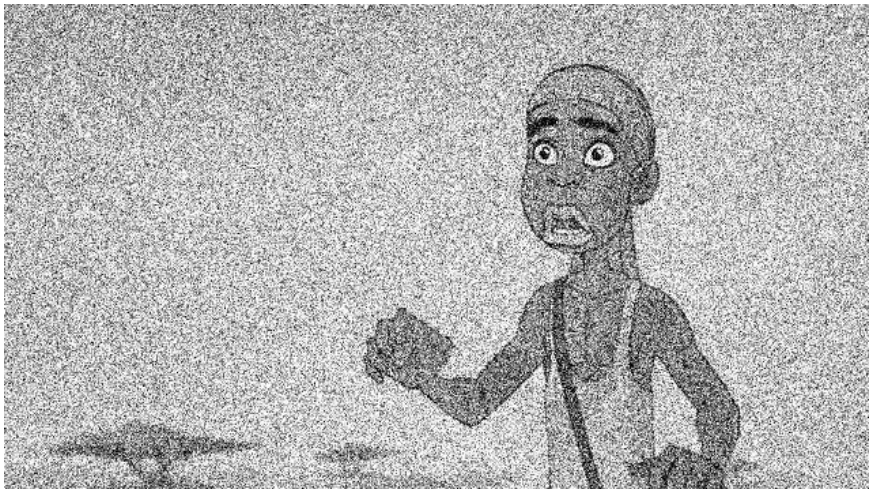
III.4.5 Authentification d'intégrité

Après avoir tatouée la vidéo, nous avons modifié la vidéo tatouée afin de vérifier si l'approche choisie détecte ces modifications. Si la marque n'a pas subir aucune modification, on déduit que l'approche à échouée à détecter ces attaques.

III.4.5.1 Bruit gaussien

Nous avons appliqué un bruit gaussien blanc à la vidéo tatoué de variance égal à 0.01, nous avons trouvé que la marque est modifiée comme le montre la figure 24.

(a)



(b)

(c)

Figure 24 (a) trame claire, (b) trame tatouée et affectée un bruit gaussien, (c) la marque extraite.

III.4.5.2 Rotation

Chaque image de la vidéo tatouée a été subi à une rotation de 3 degrés, nous avons Trouvé que la marque a été modifié et changé carrément.

(a)

(b)

Figure 25 (a) trame tatouée pivotée de 3 degrés, (b) la marque extraite.

III.4.5.3 Changement d'échelle

Nous avons appliqué dans cette expérience un changement d'échelle 2x à la vidéo Tatouée. La marque extraite diffère totalement de celle en claire comme la montre là Figure 26.

Figure 26 : la marque extraite après le changement d'échelle à 2x.

III.4.5.4 Compression

Dans cette expérience, nous avons comprimé chaque image de la vidéo en format JPEG avec un taux de compression de 10%. La marque extraite diffère aussi de la marque originale comme la montre là

Figure 27 : La marque extraite pour une vidéo compressée à un taux de 10%.

III.5 Conclusion :

Dans ce chapitre, nous avons présenté l'algorithme de tatouage fragile proposé appliqué à la composante de luminance (niveaux de gris) d'images de la séquence vidéo afin d'authentifier et de vérifier l'intégrité de vidéos numériques.

Nous avons trouvé qu'après l'implémentation, l'approche proposés offre des résultats prometteurs en termes de perceptibilité et de fragilité par rapport des attaques conventuelles à savoir l'ajout de bruit blanc, compression, rotation, …

Conclusion générale

Conclusion générale

Dans ce mémoire nous avons décrit notre approche qui répond à l'objectif que nous nous sommes fixés. Les solutions proposées sont certainement incomplètes mais laissent entrevoir de nombreuses perspectives. Citons dans ce qui suit les principales pistes que nous proposions pour donner une suite de développement de notre travail :

- Hybrider l'approche avec des techniques d'étalement de spectre pour rendre le tatouage robuste ou semi-fragile.
- Spécifier la bande de basses/moyennes fréquences à l'avance afin de rendre plus fragile cette approche aux attaques de modification de la vidéo tatouée.
- Incorporer l'approche de tatouage dans un processus de codage afin de concevoir un système de tatouage-compression.

Références bibliographies :

[1] Selmi Mohammed El-Amin, Yala Mohammed. « Synthèse et étude comparative sur les méthodes de compression vidéo » Mémoire de Master 2. Université Abou Bakr Belkaid. Tlemcen, Algérie 2017.

[2] Wei-Yi Wei, « An Introduction to Image Compression » Institut supérieur d'ingénierie de la communication Université nationale de Taiwan, Taipie, Taiwa, ROC

[3] Iain E. Richardson, « THE H.264 ADVANCED VIDEO COMPRESSION STANDARD », 2EME Edition, 2003

[4] Jerry D. Gibson, Toby Berger, Tom Lookabaugh, Dave Lindbergh and Richard L. Baker. « Digital Compression for Multimedia: Principles and Standards», Morgan Kaufmann; 1ER edition 15/01/1998.

[5] K. R. Rao, J. J. Hwang, « Techniques and standards for image », video and audio coding, 1996 Prentice Hall, p563

[6] Thomas Wiegand and Gary J, « Sullivan The H.264/AVC Video Coding Standard», IEEE MAGAZINE DE TRAITEMENT DES SIGNAUX MARS 2007.

[7] B. Bross, W.-J. Han, G. J. Sullivan, J.-R. Ohm, and T. Wiegand, High Efficiency Video Coding (HEVC) Text Specification Draft 9, document JCTVC-K1003, ITU-T/ISO/IEC Joint Collaborative Team on Video Coding (JCT-VC), Oct 20

[8] Didier Le Gall,MPEG:A video compression standard for multimedia application, vol 34 N°4, Avril 1991.

[9] Joan Mitchell, William B. Pennebaker, Chad, E. Fogg and Didier J. Legall, « MPEG video compression standard», Éditions international de Thompson, p470

[10] Didier LeGall, « MPEG: a video compression standard for multimedia applications», Communications of the ACM, Avril 1991, Vol 34, N° 4, p13.

[11] Thomas Sikora. “MPEG Digital Video Coding Standards”, R.Jurgens,1ER Edition, Berlin.

[12] L. Chiariglione (Convenor), "MPEG-4 project description", Document ISO/IEC JTC1/SC29/WG11 N1177, Réunion MPEG de Munich, Jan 1996.

[13] Hetatache Karima, « Développement d’algorithmes de tatouage d’images basés sur la SVD et les transformées discrètes », Mémoire de Magister université ferhat abbas-setif UFAS (ALGERIE),2014.

[14] Cédric Piovano & Julien Pugliesiimages, Le Tatouage Ou WATERMARKING, 2014.

[15] Imen Trabelsi, Halima Maamri « Tatouage numérique fragile pour l’authentification d’images ». Mémoire de Master université de Biskra, 2016.

Résumé :

La plupart d’algorithmes de tatouage sont soit un tatouage robuste pour la protection des droits d'auteur, soit un tatouage fragile pour la détection de falsification. Ce mémoire propose un algorithme de tatouage vidéo fragile qui a la capacité de détecter des attaques malveillantes dans le domaine fréquentiel. L’approche implémentée permet d’insérer la marque dans le domaine fréquentiel de chaque trame de la séquence vidéo où nous avons exploité la sensibilité des moyennes \hautes fréquences de la transformée de cosinus discrète appliquée à la composante luminance de chaque trame vidéo. Les résultats expérimentaux révèlent que l'algorithme implémenté atteint un taux de détection élevé contre un large éventail d'attaques de falsification telles que le filtrage, la transformation géométrique et compression.

Abstract :

Most watermarking algorithms are either a robust watermarking for copyright protection or a fragile watermarking for tampering detection. This thesis proposes a fragile video watermarking algorithm which has the capacity to detect malicious attacks in the frequency domain. The implemented approach allows inserting the mark in the frequency domain of each frame of the video sequence where we have exploited the sensitivity of the medium high frequencies of the discrete cosine transform applied to the luminance component of each video frame. The experimental results reveal that the implemented algorithm achieves a high detection rate against a wide range of tampering attacks such as filtering, geometric transformation and compression.