REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA

FACULTE : MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT :D''INFORMATIQUE

N° :……..

DOMAINE : Mathématiques et Informatique

FILIERE : Informatique

OPTION : Réseaux et Technologies de l'Information et de la Communication

Mémoire présenté pour l'obtention

Du diplôme de Master Académique

Par: CHENENE BOUBAKEUR

Intitulé

CHIFFREMENT DES VIDÉOS NUMÉRIQUES

Soutenu devant le jury composé de :

Ghribi Hayet	**Université de M'sila**	**Président**
CHIKOUCHE Noureddine	**Université de M'sila**	**Rapporteur**
Sahraoui Mohamed	**Université de M'sila**	**Examinateur**

Année universitaire : 2018 /2019

Dédicace

Je dédie ce modeste travail :

À tous les membres de ma famille pour leur soutien continu et je leurs souhaite bonne santé et long vie

À tous mes amis,

À tous mes enseignants qui ont fait leurs possibles pour nous donner le maximum d'informations concernant notre étude

surtout la responsable de la classe RTIC M Saudi lalia

Enfin, à toutes celles et tous ceux qui ont contribué de près ou de loin à l'accomplissement de ce travail.

Chenene Boubakeur

Remerciements

Avant tout on tient notre remerciement à notre Dieu tout puissant de nous avoir donné la foi, la force et le courage pour achever ce modeste travail

Je remercie mon encadreur Dr Chikouche Noureddin, de sa méthodologie et l'exactitude de ses précieux conseils

Je souhaite remercier tous les personnes qui m'ont aidé d'une façon directe ou indirecte à la réalisation de ce mémoire.

Merci infiniment

Chenene Boubakeur

Table des matières

CHAPITRE 2 : CRYPTOGRAPHIE ET CHIFFREMENT VIDEO NUMERIQUE

CHAPITRE 3 : TRAVEAUX EXISTANTS

CHAPITRE 4 : APPROCHE PROPOSEE ET IMPLEMENTATION

Liste de Figures

Liste des tableaux

INTRODUCTION GÉNÉRALE

Les technologies de réseau hautes performances ont rendu les applications multimédia en réseau de plus populaires. Vidéo sur demande, télévision Internet, visiophonie et vidéo. Les conférences sont des exemples typiques. Dans les réseaux ouverts, la confidentialité est l'une des principales préoccupations des utilisations commerciales et de communication multimédia. Dans une vidéoconférence d'affaires comme exemple, seuls les membres participants sont autorisés à recevoir les données audio et vidéo pour protéger la confidentialité de la négociation. Ce problème est généralement traité par cryptage. Seules les personnes autorisées peuvent accéder au contenu multimédia.

Il existe un certain nombre d'algorithmes disponibles qui fournissent différentes alternatives et approches en matière de cryptage vidéo. Les méthodes telles que les chiffrements symétriques utilisent une seule clé pour le cryptage ainsi que le décryptage du fichier vidéo. Sur l'autre part, les algorithmes asymétriques utilisent deux méthodes différentes, l'une pour le cryptage et l'autre pour le décryptage. Le processus de cryptage utilise une clé alors que le processus de décryptage utilise une clé différente. Ces deux clés forment une paire de clés qui travaillent ensemble main dans la main pour effectuer le processus de cryptage et de décryptage. Les techniques existantes telles que les chiffrements symétriques fournissent simplicité dans la conception au détriment de la sécurité tandis qu'asymétrique les chiffrements offrent une meilleure sécurité au prix du temps. Les deux techniques ont des avantages les uns sur les autres mais quand arrive à un code de preuve complet, les deux chiffrements ne sont pas en mesure de à la hauteur des attentes. La motivation derrière de la recherche, le travail réside dans le fait qu'il existe très peu de cryptage vidéo techniques disponibles qui pourraient fournir une meilleure sécurité au cout très peu de temps, réduisant également la complexité de la conception dans une grande mesure.

Problématique et objectif

Les méthodes existantes pour sécuriser les données vidéo reposent principalement sur de lourds algorithmes de traitement du signal qui nécessitent beaucoup de bande passante et prend beaucoup de temps pour effectuer le cryptage entrainant des retards de communication. Par contre, pas un seul algorithme de cryptage est suffisamment sécurisé pour fournir un complètement résultat sans faille et sans perte. La plus part des algorithmes symétriques sont plus rapides mais plus facile à percer, alors que les algorithmes asymétriques sont plus sécurisés mais prend plus de temps. Notre objectif est de créer un système qui crypte la vidéo rapidement

et conserve la qualité de l'image après le décryptage tout en préservant sa confidentialité après la transmission à une autre personne. Par l'utilisation des algorithmes cryptographique moderne.

Organisation du mémoire

Nous avons structuré notre mémoire en quatre chapitres :

Dans le premier chapitre nous allons commencer par de parler des types de vidéo et son caractéristique (Couleur d'espace, format …etc.), Après, nous allons passer à la compression de l'information vidéo en expliquant les diverses étapes de compression liées. Aussi, on va citer quelques normes de compression vidéo normalisées à partir des deux groupes de normalisation IEC/ISO et ITU-T.

Dans le deuxième, nous allons commencer par donner des définitions et vocabulaires relatives au domaine de la cryptographie moderne. Tout en restant même , on abordera également les algorithmes de chiffrement symétrique, asymétrique et hybride en citant quelques algorithmes classiques et populaires. Après, on passera aux techniques de chiffrement appliquées pour la protection de la vidéo numériques. Ces techniques dépendent inévitablement de la norme de codage de vidéo, et elles peuvent être appliqué avant, durant, ou après la compression. Finalement, on terminera par une conclusion.

Dans le troisième chapitre nous allons parler sur les derniers recherches dans le domaine de cryptage vidéo.

Dans le dernier chapitre, on va implémenter et développé une application qui crypté la vidéo par une nouvelle technique. Puis on va terminer par une conclusion générale.

CHAPITRE 1

CONCEPTS DE BASE DES VIDEOS

1. Introduction

En raison de l'importance des vidéos numériques et de la valeur des informations qu'elles contiennent, dans ce chapitre nous allons commencer par parler des types de vidéo et de ses caractéristique (Couleur d'espace, format …etc.), Après, nous allons passer à la compression de l'information vidéo en expliquant les diverses étapes de compression qui lui sont propres. Aussi, on va citer quelques normes de compression vidéo normalisées depuis les deux groupes de normalisation IEC/ISO et ITU-T. Finalement, on terminera avec une conclusion.

2. Types de vidéo

Il existe deux types de vidéo : vidéo analogique et vidéo numérique.

2.1. Vidéo analogique

La vidéo analogique, représentant l'information comme un flux continu de données analogiques, destiné à être affichées sur un écran de télévision , basé sur le principe du balayage qui propose deux types :balayage entrelacé et balayage progressif (voir la figure 1). Il existe plusieurs normes pour la vidéo analogique. Les trois principales sont : PAL ,NTSC ,SECAM. [1]

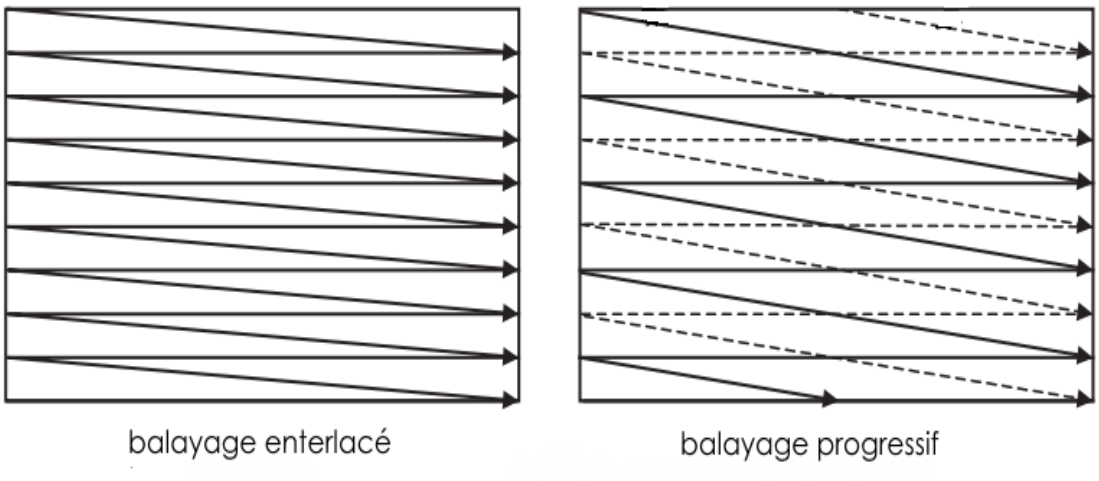

Figure 1.1 : les types de balayage

2.2. Vidéo numérique

La vidéo numérique est une séquence animée d'images fixes qui permet de représenter la même information ou la même scène temporellement, Chaque séquence vidéo est caractérisée par des propriétés spatiales qui décrivent chaque image comme la résolution, l'espace de couleur choisi, le format de sous échantillonnage de couleur (pour le système YCrCb), et la résolution temporelle qui indique le nombre d'images par seconde *fps* (Frame per second). [2]

3. Couleur de l'espace

Une image numérique représente un tableau d'échantillons en deux dimensions, chaque échantillon étant appelé pixel. La précision détermine le nombre de niveaux d'intensité pouvant être représentés et est exprimée par le nombre de bits / échantillon. Selon la précision, les images peuvent être classées en :

- Images binaires, représentées par 1 bit / échantillon
- Infographie, représentée par 4 bits / échantillon
- Images en niveaux de gris, représenté par 8 bits / échantillon,
- Images en couleur, représentées par 16, 24 bits ou plus / échantillon.

Selon la théorie trichrome, la sensation de couleur est produite en excitant sélectivement trois classes de récepteurs dans l'œil. [3]

3.1. Représentation RVB (Rouge-Vert -Bleu)

Dans un système de représentation des couleurs RVB, illustré à la **figure 1.2**, une couleur est produite en ajoutant trois couleurs primaires : rouge, vert et bleu . La ligne droite, où R = G = B, spécifie les valeurs de gris allant du noir au blanc.

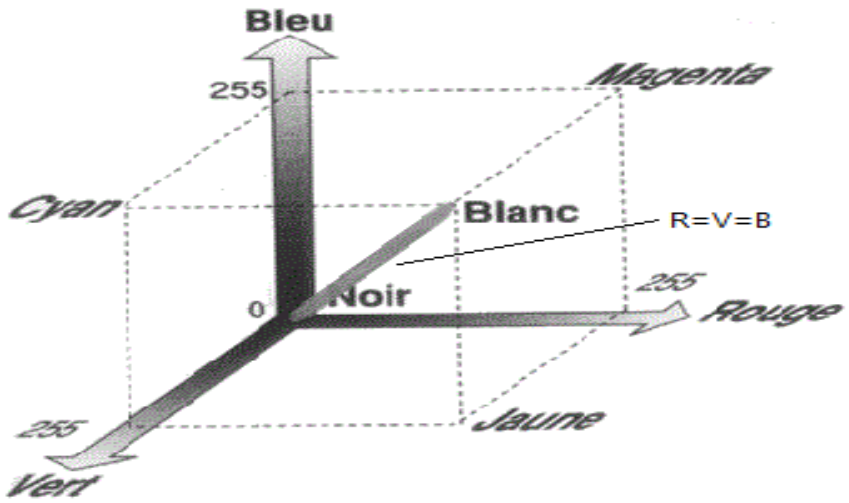

Figure 1.2 : Représentation des couleurs RVB

3.2. Représentation YUV (luminance /chrominance)

Une autre représentation des images en couleur, décrit la luminance et la chrominance composants d'une image. La composante de luminance noté Y fournit une version en niveaux de gris de l'image représente par l'équation (1.1), tandis que deux composants de chrominance U et V donnent des informations supplémentaires qui convertissent l'image en niveaux de gris

à une image de couleur par les équations (1.2), (1.3). La représentation YUV est plus naturelle pour la compression d'images et de vidéo. L'exacte transformation de la représentation RVB à YUV, spécifiée par la norme CCIR 601.

$$Y = 299R + 0.587G + 0.114B \quad (1.1)$$

$$U = 0.564(B-Y) \quad (1.2)$$

$$V = 0.713(B-Y) \quad (1.3)$$

3.3. Représentation YCbCr

Le format YCbCr, est utilisé de manière intensive pour la compression d'images. Dans Le format YCbCr, Y est identique à celui d'un système YUV. Toutefois, les composants U et V qui représentent la chrominance sont mis à l'échelle et zéro signés pour produire respectivement Cb et Cr, comme les équations (1.4) et (1.5).

$$Cb = U/2 + 0.5 \quad (1.4)$$

$$Cr = V/1.6 + 0.5 \quad (1.5)$$

De cette manière, les composantes de chrominance Cb et Cr sont toujours comprises dans la plage [0,1]. [3]

4. Formats d'échantillonnage

La Figure 1.3 montre trois modèles d'échantillonnage pour Y, Cb et Cr :

- Échantillonnage 4 : 4 : 4 signifie que les trois composantes (Y, Cb et Cr) ont la même résolution et qu'il existe donc un échantillon de chaque composante à chaque position de pixel.
- Échantillonnage 4 : 2 : 2 (parfois appelé YUY2), les composantes de chrominance ont la même résolution verticale que la luminance mais la moitié de la résolution horizontale. La vidéo 4 : 2 : 2 est utilisée pour une reproduction des couleurs de haute qualité.
- Le format d'échantillonnage 4 : 2 : 0 (« YV12 »), Cb et Cr ont chacun la moitié de la résolution verticale de Y. Le terme «4 : 2 : 0 » est plutôt déroutant car les chiffres n'ont pas réellement une interprétation logique et semblent avoir été choisis historiquement comme 'Code' pour identifier ce schéma d'échantillonnage particulier et le différencier de 4 : 4 : 4et 4 : 2 : 2.

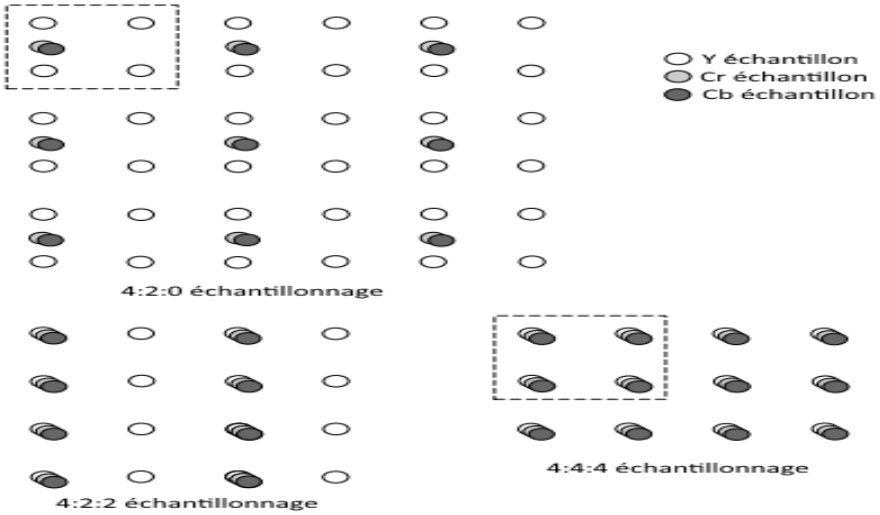

Figure 1.3 : Profils d'échantillonnage 4 : 2 : 0, 4 : 2 : 2 et 4 : 4 : 4**.** [4]

5. Formats vidéo numériques

Le groupe de spécialistes de l' UTI (SGXV) a recommandé trois formats. Ils sont : le standard input format (SIF), Common interchange format (CIF), et la version à faible débit de CIF appelé quart CIF (QCIF) [5]. (voir Table 1.1), ces formats décrivent un ensemble complet de formats vidéo numériques qui sont largement utilisés dans les applications mobiles.

Description	SIF	CIF	QCIF
Résolution horizontale (Y) pixels	352	360(352)	180(176)
Résolution verticale (Y) pixels	240/288	288	144
Résolution horizontale (Cr, cb) pixels	176	180(176)	90(88)
Résolution verticale (Cr, cb) pixels	120/144	144	72
Bits/pixel (bpp)	8	8	8
Mode d'affichage	Progressif	Progressif	Progressif
Trames par seconde (fps)	30	30, 15, 10, 7.5	30, 15, 10,7.5

Table 1.1 : Les différents formats de la vidéo numérique

La Figure 1.4 représente des autres formats pour la transmission d'images numériques issues de la télévision à tube comme la définition standard (SD), elle se compose de 720x576 pixels. Ce format est utilisé par les DVD. Et pour 720p, il est utilisé dans le cas de la Haute Définition (HD) mais dit intermédiaire. Il comprend 1280x720 pixels. Il est surtout utilisé par les services de VOD (Vidéo à la demande), Full HD l'autre définition de la HD. Ce format comporte 1920x1080 pixels. Autre que les téléviseurs qui la propose, il est aussi utilisé par le

Blu-Ray, Quad HD ou Ultra HD ou 4K une définition comprenant 4 fois plus de pixels que la Full HD. Elle se compose de 3840x2160 pixels. Le format cinéma se compose lui de 4096x2160 et enfin 8K Ce format propose une définition ayant 16 fois plus de pixels que la Full HD et 4 fois plus de pixels que la 4K. Il est équivalent à 7680x4320 pixels.

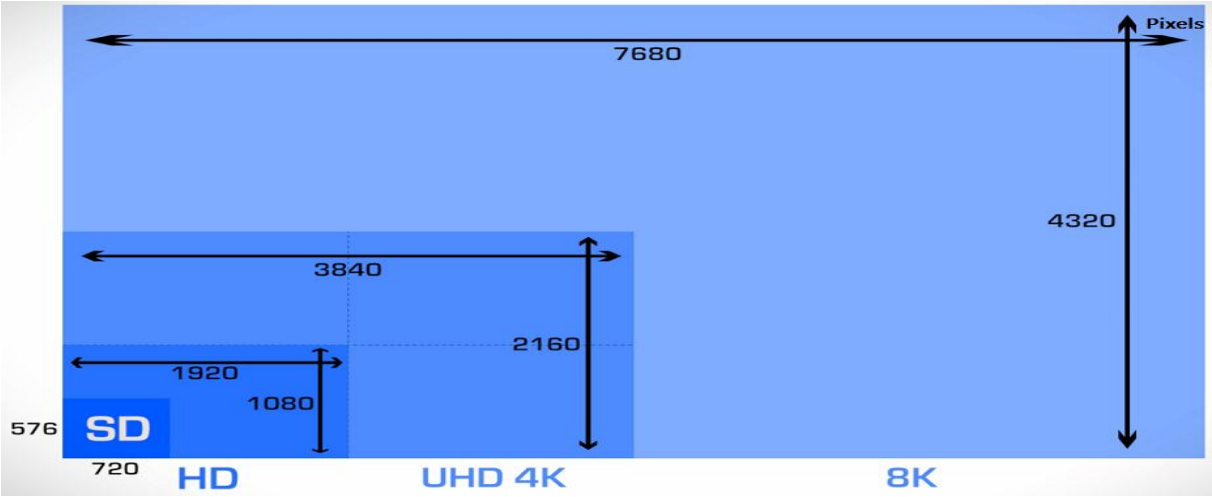

Figure 1.4 : L'évolution des formats de la vidéo numérique : de SD au 8K**.** [6]

6. Conteneurs de références

Les vidéos numériques sont contenues dans des fichiers qui sont appelés des conteneurs. Reconnaissable par leur extension de fichier (voir la Table 1.2).

Conteneur	**Extension**
Audio Video Interleave	.avi
MPEG 1/2/4	.mpg , .mpeg
Matroska	.mkv , .mka , .mks
QuickTime	.mov
3gp	.3gp , .3g2
Transport Stream	.ts
Flash Video	.flv

Table 1.2 : Conteneurs de vidéo.

7. Compression vidéo numérique

La compression vidéo est le processus de conversion d'un signal vidéo en un format qui utilise moins d'espace de stockage ou de bande passante de transmission. Vu la vidéo exigences

de transmission et de stockage (jusqu'à 270 Mbits / s pour la définition standard et 1,5 Gbit / s pour la haute définition), la compression vidéo est une technologie essentielle pour des applications telles que la télévision numérique (transmission terrestre, par câble ou par satellite), optique stockage / reproduction, télévision mobile, vidéoconférence et diffusion vidéo en continu sur Internet [7].

7.1. Types de compression

Il existe deux types de compression la compression avec perte et la compression sans perte :

7.1.1. 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. [8] et à-partir des méthodes de compression sans perte il ya codage en longueur, codage huffman, méthode Lempel-Ziv-Welche (LZW).

7.1.2. Compression avec perte

Le type de compression le plus couramment utilisé pour la vidéo car il fournit des taux de compression beaucoup plus élevés. Il y a bien sûr un compromis : plus le taux de compression est élevé, plus la qualité de la vidéo compressée est mauvaise. Les codecs avec perte ne conviennent pas aux données informatiques, mais sont utilisés en MPEG car ils permettent des facteurs de compression plus importants que les codecs sans perte.

7.2. Redondance vidéo

La compression est obtenue en supprimant les informations redondantes de la vidéo. Il existe quatre principaux types de redondances qui sont généralement explorés par les algorithmes de compression : [7]

- **Redondance perceptuelle** : l'informations de la vidéo qui ne peuvent pas être facilement perçues par l'observateur humain et qui, par conséquent, peuvent être supprimées sans altération significative de la qualité de vidéo.
- **Redondance temporelle** : les pixels des images vidéo successives présentent une grande similitude. Ainsi, même si le mouvement a tendance à modifier la position des blocs de pixels, il ne modifie pas leurs valeurs et donc leur corrélation. (Comme **figure** 1.5 (b)). On l'appelle aussi redondance inter-codage.

- **Redondance spatiale** : il existe une corrélation significative entre les pixels situés autour du même voisinage dans une image (comme **figure** 1.5 (a)). On l'appelle aussi redondance intra-codage.
- **Redondance statistique** : Ce type de redondance est lié à la relation statistique dans les données vidéo (bits et octets).

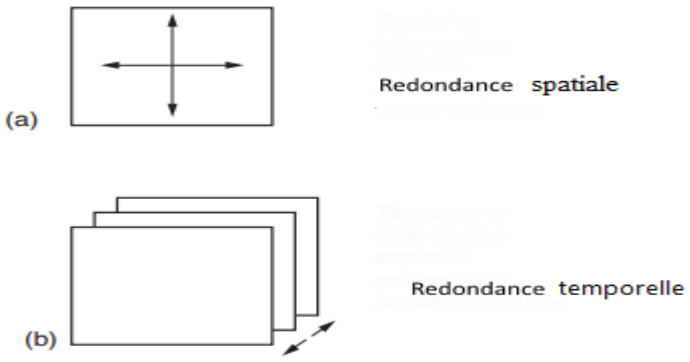

Figure 1.5 : Redondances dans la vidéo a) Redondance spatiale b) Redondance temporelle

7.3. Vidéo MPEG

The Motion Pictures Expert Group (MPEG) [9]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. [10]. Une vidéo MPEG est composée d'une séquence de groupe d'images (GOP), L'avantage majeur du MPEG par rapport aux autres formats de codage vidéo et audio est que les fichiers MPEG sont beaucoup plus petits que d'autres représentations, pour la même qualité. Ceci est dû au fait que MPEG utilise des techniques de compression très sophistiquées. La Transformation de Cosinus essentiellement Discrète (DCT) - nous allons détailler dans l'élément suivant - est utilisée pour la compression et la clé pour obtenir un taux de compression vidéo plus élevé consiste à exploiter la similitude entre les images d'une séquence vidéo. L'idée de base de la compression vidéo MPEG est de supprimer la redondance spatiale et la redondance temporelle, Il existe trois types de frame dans la compression MPEG : Les I frames, dites Intra Frames, ou key frames Les P frames, dites Inter Frames, Delta Frames, ou prédiction frames Les B frames, ou Bidirectionnel frames.

- **I frames :** Les trames I sont appelées images intra-codées, sans aucune référence à d'autres images. Chaque image est divisée en tranches puis en macroblocs, comme le montre dans la **figure 1.6**. Chaque macrobloc est compressé à l'aide de DCT suivi d'une quantification et codage à longueur variable. La sortie du flux codé est appelée flux MPEG.

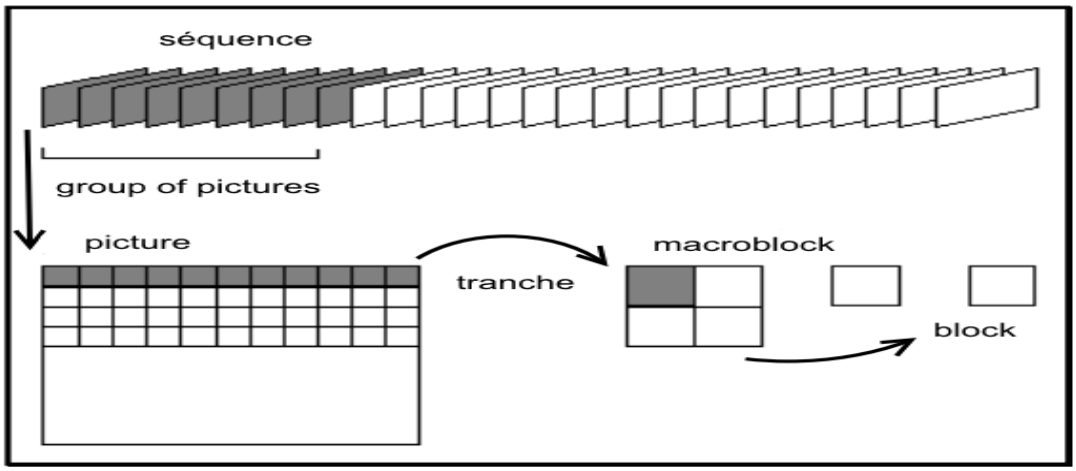

Figure 1.6 : Une vidéo MPEG est une séquence de groupe d'images (GOP). Chaque image est divisée en tranches et chaque tranche est ensuite divisée en macroblocs. [11]

- **P et B Frames :** Les trames P sont des trames inter codées qui sont codées de manière prédictive à l'aide des trames I ou P précédentes. Cadres B sont codés de manière bidirectionnelle à partir des trames I et / ou P précédentes et suivantes. À partir de la **Figure 1.7**, nous pouvons voir que la trame pour la prédiction en arrière suit la trame prédite. Cela nécessiterait de suspendre le décodage des images B jusqu'à ce que la prochaine image P ou B apparaisse dans le flux. Cependant, l'affichage ordre n'est pas l'ordre de codage. Les trames apparaissent sur le flux de données MPEG dans un ordre tel que la référence les cadres précèdent les cadres de référence. La séquence de trames ci-dessus est transférée dans l'ordre suivant : I P B B B P B B B. La tâche du décodeur est de réorganiser les images reconstruites. Les cadres P et B sont constitués du déplacement par rapport aux trames I correspondantes et aux signaux d'erreur résiduels.

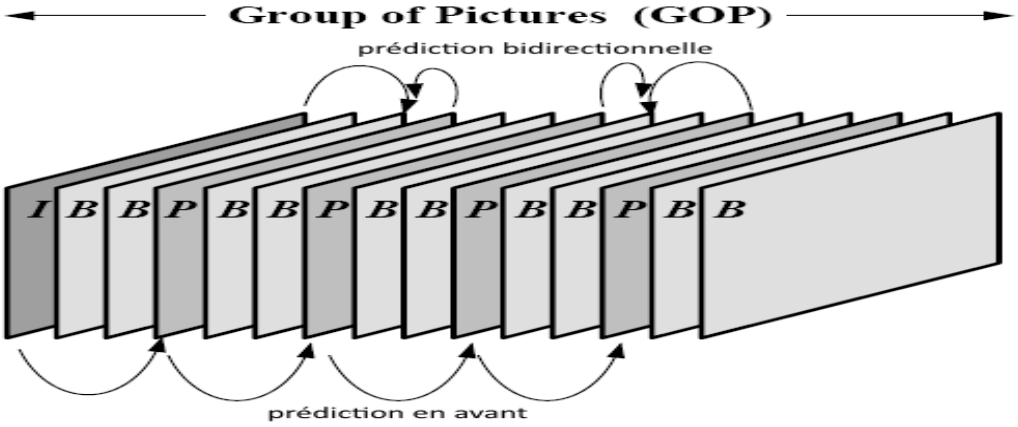

Figure 1.7 : Exemple de groupe d'images avec l'ordre d'affichage. [12]

7.4. Codage MPEG

Le codage MPEG comprend les quatre étapes illustrées à la **figure 1.8**. Avant cela, la vidéo est convertie de l'espace colorimétrique RVB en YUV et en échantillonnage réduit dans le domaine UV. La raison pour YUV à Le sous-échantillonnage dans le domaine UV vise à minimiser la résolution des composantes de couleur.

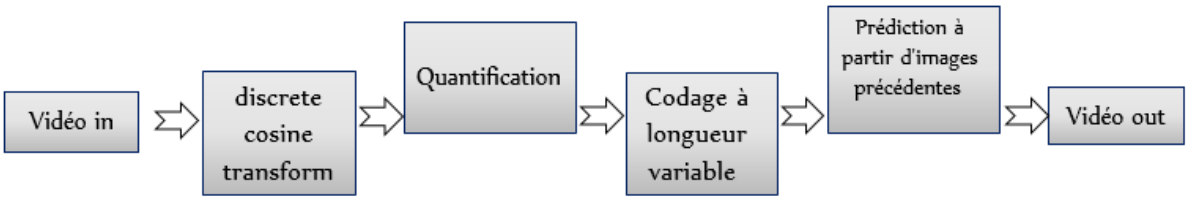

Figure 1.8 : Étapes de codage typiques utilisées dans la compression MPEG

7.4.1. DCT : une Discrete Cosine Transform exprime une séquence finement composée des points de données en termes d'une somme des fonctions cosinus oscillant à différentes fréquences. Les DCT sont importants pour des nombreuses applications en sciences et en ingénierie, de la compression avec perte d'audio et d'images (où de petites composants haute fréquence peuvent être éliminés). Il est choisi de facto dans la plupart des normes MPEG transformer car il a été prouvé être une approximation de la transformée optimale K-L au premier ordre de Markov modèle source [13]. La taille de la transformation 2D est de 8 * 8. DCT est utilisé pour la compression spatiale en MPEG et il convertit du domaine spatial au domaine de fréquence.

7.4.2. Quantification : la principale opération avec pertes dans l'ensemble du processus de compression MPEG. Comme en conséquence, la plupart des composantes de fréquence supérieure sont arrondies à zéro et la plupart des autres deviennent de petits nombres positifs ou négatifs, qui prennent beaucoup moins de bits à stocker.

7.4.3. Codage à longueur variable : Après le processus de quantification, les coefficients DCT sont codés en entropie. C'est une forme spéciale de la technique de compression de données sans perte. Il s'agit d'arranger les coefficients de manière « en zigzag ». Celles-ci sont ensuite codées à l'aide de l'algorithme RLE (Run-Length Encoding) qui regroupe les fréquences ensemble, en insérant des zéros de codage de longueur, puis en utilisant le codage de Huffman sur ce qui reste.

7.4.4. Prédiction à partir d'images précédentes : Ceci n'est rien d'autre qu'une estimation / compensation de mouvement. Il est adopté décorréler la redondance temporelle. Cette compression est utilisée pour les images P et B. Dans ce la différence entre le macrobloc en

cours et le macrobloc de meilleure correspondance (macrobloc de prédiction) dans le cadre de référence sont pris et envoyés comme les données résiduelles (erreur de prédiction). Notez que Les données résiduelles sont à nouveau décorrélées spatialement avec la transformation 2D après la décorrélation temporelle prédite par le mouvement. Le macrobloc de meilleure correspondance est décrit avec des vecteurs de mouvement qui sont en réalité sémantiques des données, pas des données de pixels, décrivant le décalage entre le macrobloc actuel et sa meilleure correspondance macrobloc dans le flux binaire.

8. Normes de codage vidéo

Les normes de codage vidéo ont évolué sous deux noms de marque, H.26x et MPEG-x. Les codecs H.26x sont recommandés par le secteur de la normalisation des télécommunications de l'ITU-T. Les recommandations de l'ITU-T ont été conçus pour les applications de télécommunication, telles que la vidéo conférence et téléphonie vidéo. Les produits MPEG-x sont l'œuvre de l'organisation internationale de normalisation et de la Commission électrotechnique internationale, (ISO / IEC). Les normes MPEG ont été conçus principalement pour répondre aux besoins de stockage vidéo (par exemple, CD-ROM, DVD), diffuser la télévision et la diffusion vidéo en continu (par exemple, la vidéo sur Internet). Pour la plupart des pièces, les deux comités de normalisation ont travaillé indépendamment sur des normes différentes. Il existe cependant des exceptions où leur travail commun a abouti à des normes telles que H.262 / MPEG-2 et H.264 / MPEG-4, partie 10 (v10). La figure 9 résume les évolutions des normes de codage vidéo des deux organisations et leurs efforts communs depuis le début en 1984 jusqu'à maintenant. La figure 11 montre également l'évolution du codage d'images fixes dans le cadre des travaux conjoints de l'ITU-T et de l'ISO / IEC. [14]

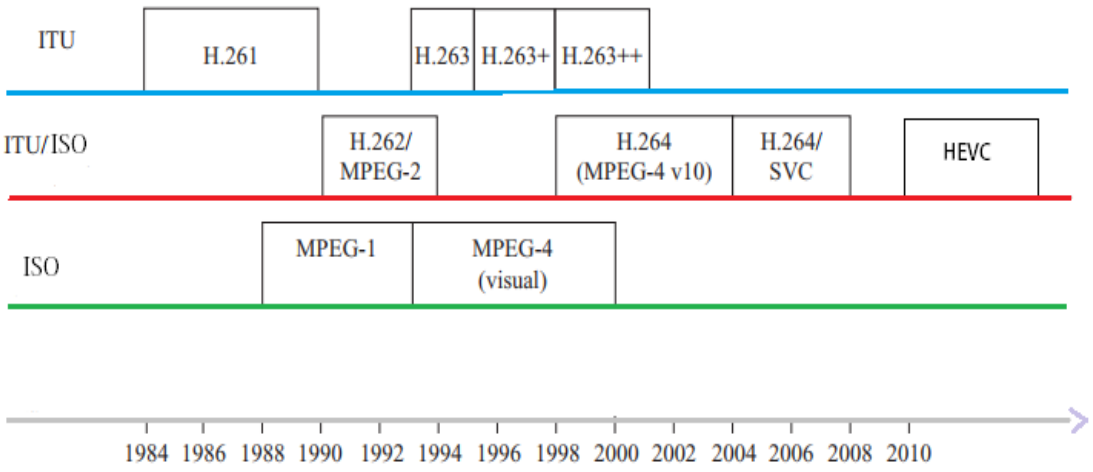

Figure 1.9 : Evolution des normes de codage vidéo de l'ITU-T et de l'ISO / IEC comités.

❖ **La norme H.264 / MPGE 4**

H.264 / MPEG-4 AVC est une norme de compression vidéo récemment mise au point conjointement par le comité de normalisation VCEG de l'ITU-T et les comités de normalisation MPEG ISO / IEC. La norme promet une compression beaucoup plus élevée que celle possible avec les normes antérieures. Il permet un codage très efficace de la vidéo non-entrelacée et entrelacée. Même à des débits binaires élevés, il offre une qualité visuelle plus acceptable que les normes antérieures. En outre, la norme prend en charge les flexibilités en matière de codage ainsi que l'organisation de données codées susceptibles d'accroitre la résistance aux erreurs ou aux pertes. [15] AVC signifie Advanced Vidéo Coding, la Table 1.2 spécifier les caractéristiques de la norme.

Catégorie	Description
Type de frame	Pour la norme h.264/avc on retrouve les mêmes types d'images que dans les normes précédentes (I, P ou B)
Division de macrobloc	La norme H.264/AVC prend en charge cinq types de tranches : tranches de type **I (Intra)**, les tranches de type **P (prédictif)**, les tranches de type **B (Bi-prédiction)** et enfin les tranches de types **SP (commutation P)** et **SI (commutation I)**.
Prédiction	La norme H264/AVC propose sept modes de prédictions. La prédiction d'un macrobloc peut être effectuée en le considérant dans son intégralité ou en le divisant en sous-blocs. Ainsi, pour le signal de luminance nous distinguons les partitions **16_16, 16_8, 8_16, 8_8, 8 _ 4, 4 _ 8 et 4 _ 4**. Les deux composantes de chrominance peuvent aussi être partitionnées en sous-blocs allant de **8 _ 8** échantillons jusqu'à **2 _ 2** échantillons
Quantification	La norme H264/AVC applique sur les coefficients de la transformée une quantification avec 52 niveaux de quantification. Pour chaque niveau un paramètre de quantification QP (quantization parametre) est associé. Le choix du pas est important pour un bon réglage du débit. Par la suite, les coefficients de chaque bloc de 4*4 sont ordonnés en appliquant le balayage en zigzag.
Le codage entropique	Le codage entropique peut être réalisé de deux manières différentes : -CAVLC (Context-Adaptive Variable Length Coding) : est une alternative pour le codage des tables de coefficients de transformation. -CABAC (Context- Adaptive Binary Arithmetic Coding) : est une combinaison d'une technique adaptative de codage arithmétique binaire qui permet un degré élevé d'adaptation et une réduction plus importante de redondance

Filtre anti-blocs	La H264/AVC définit un filtre de « déblocage » adaptatif en boucle qui a pour but de minimiser la visibilité des artefacts dus aux codages par blocs. Ce filtre réduit le débit binaire et offre une meilleure qualité d'image qu'avant filtrage.

Table 1.3 Les caractéristique de la norme h.264/avc.

9. Conclusion

Dans ce chapitre, nous avons parlé des vidéos et de ses types, les méthodes de compression et de codage des vidéos numériques, les normes des compressions vidéo.

Dans le prochain chapitre, nous allons parler de la cryptographie en général, et plus particulièrement du chiffrement des vidéos.

CHAPITRE 2

CRYPTOGRAPHIE ET CHIFFREMENT VIDEO NUMERIQUE

1. Introduction

Suite au développement rapide ces dernières années des technologies de l'information Et la communication et les infrastructures réseaux filaires et sans fil, la cryptographie est devenue, depuis quelques décennies, un véritable enjeu de société. Dans ce chapitre nous allons parler sur la cryptographie et la classification des algorithmes de cryptage, en citant quelques algorithmes classiques et populaires. Puis, on passera aux techniques de chiffrement appliquées pour la protection de vidéo numérique.

2. Définition de la cryptographie

La cryptographie est l'art de rendre inintelligible, de crypter, de coder un message à ceux qui ne sont pas habilités à en prendre connaissance, c'est est un ensemble des principes, méthodes et techniques dont l'application assure le « crypter » et le « décrypter » des données cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est pas en possession de la clé à utiliser pour le déchiffrer. La signification de « crypter » et « décrypter » est donnée successivement comme suit :

- **Crypter :** brouiller l'information, la rendre "incompréhensible".
- **Décrypter :** rendre le message compréhensible.

3. Objectifs de sécurité

La sécurité sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

▪ **La confidentialité** : consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.

▪ **L'intégrité** : Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Un intrus ne doit pas être capable de faire passer un faux message pour légitime.

▪ **L'authentification :** consiste à assurer l'identité d'un utilisateur, c.-à-d. de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

▪ **La non répudiation**

La non répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction .

4. Classes de cryptographie

La **figure 2.1** illustre les différentes classes de crypto systèmes :

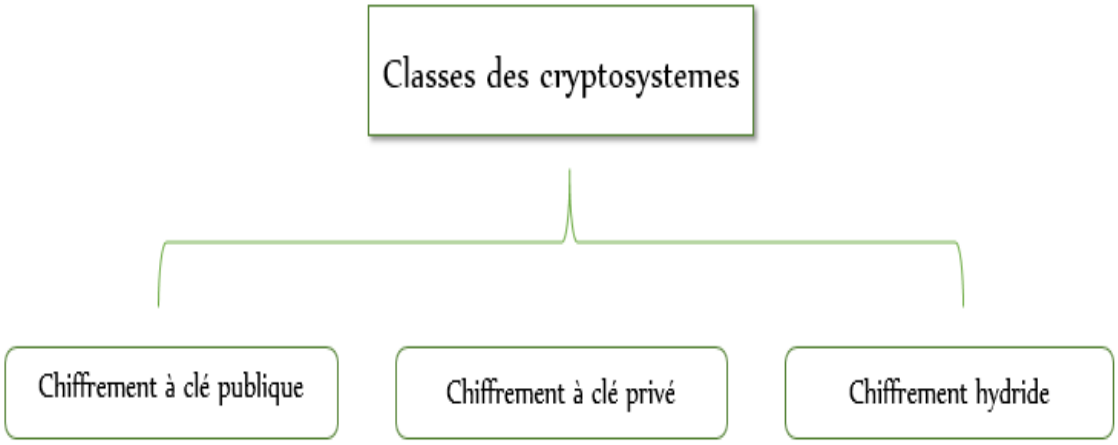

Figure 2.1 : Les systèmes de chiffrement moderne.

4.1. Cryptographie à clé privé (ou *cryptographie* symétriques)

Les cryptographies symétriques utilisent la même clé pour le chiffrement et le déchiffrement (ou la clé de déchiffrement est facilement dérivée de la clé de chiffrement (voir **figure 2.2**). Les algorithmes symétriques sont de deux types :

- Les algorithmes de **chiffrement par flot**, qui agissent sur le texte en clair un bit à la fois.
- Les algorithmes de **chiffrement par blocs**, qui consistent à diviser le texte clair en blocs de taille fixe (généralement 64 ou 128 bits) et chiffrent un bloc à la fois avec la même clé.

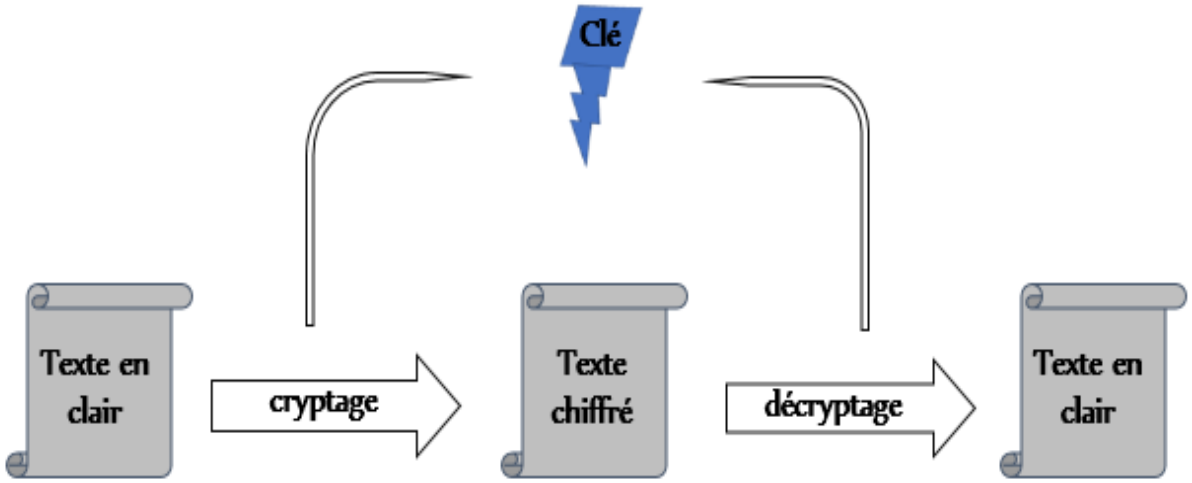

Figure 2.2 : Chiffrement symétrique.

Parmi les algorithmes de chiffrement symétrique on trouve : DES, AES, IDEA,3DES…etc.

4.1.1. DES (Data Encryption Standard)

DES est un algorithme qui a été le standard de chiffrement symétrique entre 1977 et 2001. Le DES est basé sur un schéma de Feistel. Cet algorithme fonctionne par blocs de texte claire de 64 bits en utilisant une clef de 56 bits (la clef compte 64 bits mais parmi lesquels 1 bit sur 8 est utilisé comme bit de partie), DES a une clé plus petite qui est moins sécurisée et plus lent par rapport à AES a une grande clé secrète comparativement plus sûre et plus rapide. En plus le DES a fait l'objet de très nombreuses attaques.

4.1.2. AES (Advenced Encryption Standard)

Le AES est lancé par NIST (National Institute of Standards and Technologies) le 2 octobre 2000 pour remplacer Triple DES et DES. Remplace désormais celui de Rijndael (dont le nom est basé sur les noms de ses deux inventeurs, **Joan Daemen** et **Vincent belges Rijmen**).

Techniquement, le chiffrement AES opère sur des blocs de 128 bits (plain text P) qu'il transforme en blocs cryptés de 128 bits (C) par une séquence de Nr opérations ou "rounds", à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de rounds diffère : respectivement 10, 12 et 14 rounds [16]. Pour la version 128 bits de l'AES Chaque bloc subit une séquence de transformations que nous résumons à travers les points suivants :

- Au débit ajouter une opération XOR entre P et K puis en en injectant le résultat S0, dans un cycle de 10 tours.
- Chaque tour d'AES-128 *r* calcule son état de sortie *Sr* en appliquant successivement

  quatre transformations :

  - **ByteSub** : les 128 bits sont répartis en 16 blocs de 8 bits (16 octets), qui sont ensuite placés dans une matrice de 4×4. Chaque octet est transformé par une fonction non linéaire S (S-box) conçu pour résister à la cryptanalyse linéaire et différentielle.
  - **ShiftRow :** les lignes de cette matrice sont soumises à une rotation vers la droite où l'incrément pour la rotation varie selon le numéro de la ligne. La 2ème ligne est décalée d'une colonne, la 3ème ligne de 2 colonnes, et la 4ème ligne de 3 colonnes.
  - **MixColumn** : chaque colonne est transformée par combinaisons linéaires des différents éléments de la colonne. Cela revient à multiplier la matrice 4×4 par une autre matrice 4×4.

- **AddRoundKey** : une clé dite de tour est générée à partir de la clé secrète par un sous algorithme dit de cadencement. Cette clé de tour est ajoutée par un « ou exclusif » au dernier bloc obtenu.

- Le chiffré est finalement défini comme étant la sortie du dixième et dernier tour qui a pour différence de ne pas comporter d'opération MixColumns. [17] [18] [16]

Le déchiffrement consiste en appliquer les opérations inverses dans chacune des étapes (Inv-SubBytes, InvShiftRows, InvMixColumns). AddRoundKey (à cause du XOR) est son propre inverse. On réitère ce processus le nombre de tour-1. Pour le dernier tour on exclut l'opération InvMixColumns ; et comme dans le chiffrement pas d'opération InvMixColumns dans le dernier tour. (voir Figure 2.3).

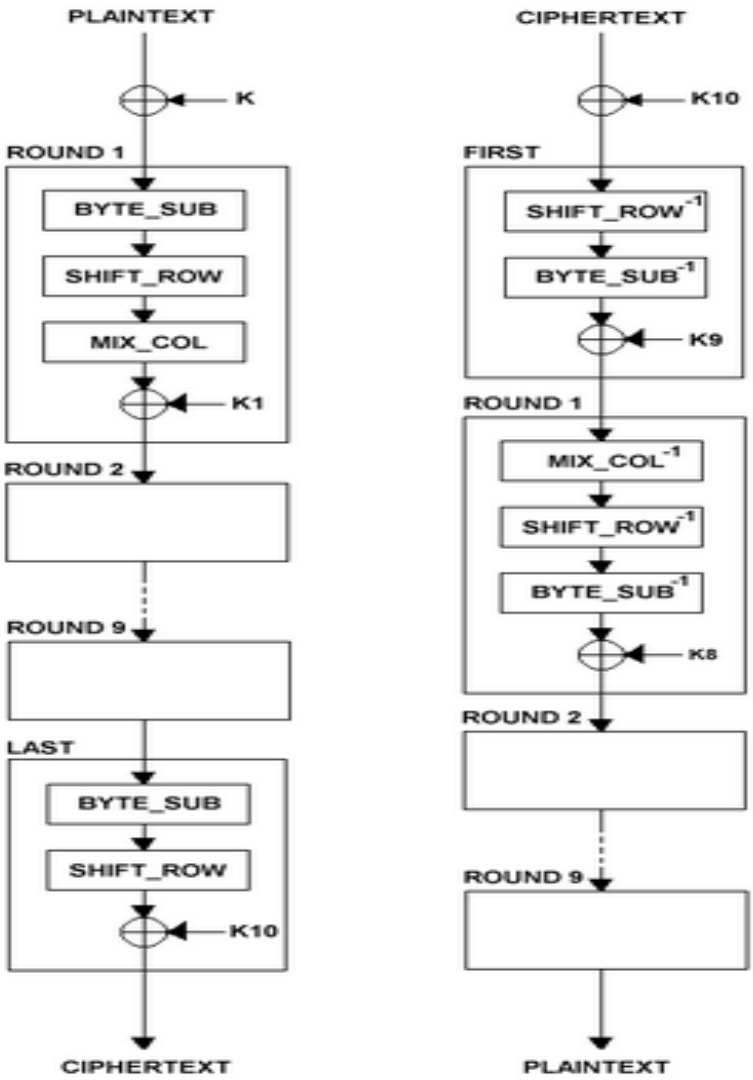

Figure 2.3 Schéma chiffrement et déchiffrement de l'AES [16].

4.1.3. Modes de chiffrement

Que ce soit pour le DES et AES, les clefs sont des longueurs fixées. Or les messages peuvent être de longueur quelconque bien sûr. Il faut donc initier des chiffrements par blocs de taille fixe correspondants aux tailles des clefs. Pour cela 4 modes de chiffrement par blocs sont possibles : ECB, CBC, CFB et OFB. [19]

- **Mode ECB, Electronic Code Book :** Le mode du "carnet de codage électronique" est le mode le plus simple. Le message, M, est découpé en blocs, $(m_i)_{i \geq 1}$, et chaque bloc est crypté par : $c_i = E(m_i)$; un bloc du texte en clair se chiffre, indépendamment de tout, en un bloc de texte chiffré. L'avantage de ce mode est qu'il permet le chiffrement en parallèle des différents blocs composant un message. [20] Et à partir à ses inconvénients est sensible à des « attaques par répétition » par ce que Les répétitions du texte en clair ne sont pas masquées et se retrouvent sous la forme de répétitions de textes chiffrés.
- **Mode CBC, Cipher Block Chaining :** en mode de "chiffrement avec chaînage de blocs" (Cipher Block Chaining), chaque bloc de texte en clair est combiné par ou exclusif avec le bloc chiffré précédent avant d'être chiffré. Le premier bloc du texte en clair est, quant à lui, combiné avec un bloc appelé vecteur d'initialisation. L'utilisation d'un vecteur d'initialisation différent pour chaque message permet de s'assurer que deux messages identiques (ou dont les premiers blocs sont identiques) donneront des cryptogrammes totalement différents. [21]

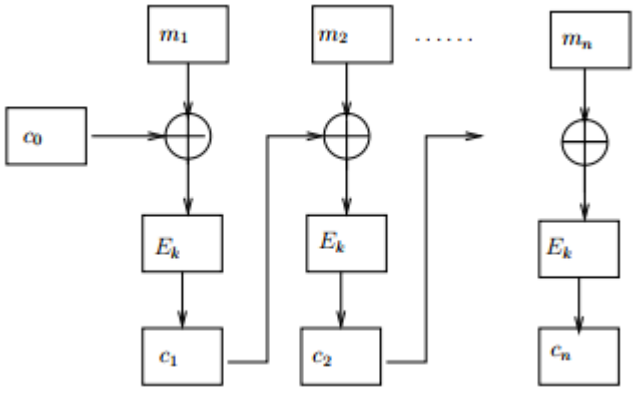

Figure 2.4 : Diagramme du mode CBC [19]

- **Mode CFB, Cipher FeedBack :** Dans ce mode le chiffrement par bloc a transformé à un chiffrement par flot, le flux de clé est obtenu en chiffrant le précédent bloc chiffré [22]comme la figure 2.5.

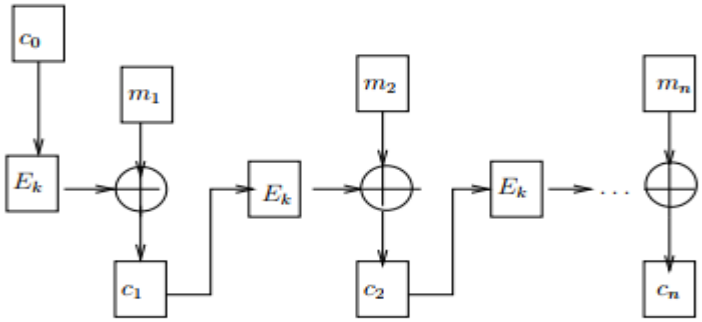

Figure 2.5 : Diagramme du mode CFB [19].

- **Mode OFB, Output FeedBack** : Est une variante de mode CFB. La clé est modifiée à chaque itération et combinée avec la clé suivante.

4.2. *Cryptographie à clé* publique (ou *cryptographie* asymétriques)

Avec La cryptographie asymétriques, les clefs de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre. On peut donc rendre l'une des deux publique tandis que l'autre reste privée. C'est pourquoi on parle de chiffrement à clef publique. Si la clef publique sert au chiffrement, tout le monde peut chiffrer un message, que seul le propriétaire de la *clef privée* pourra déchiffrer. On assure ainsi la confidentialité. Certains algorithmes permettent d'utiliser la clef privée pour chiffrer. Dans ce cas, n'importe qui pourra déchiffrer, mais seul le possesseur de la clef privée peut chiffrer. Cela permet donc la signature de messages. La Figure 2.6 présent le chiffrement asymétrique [21] .

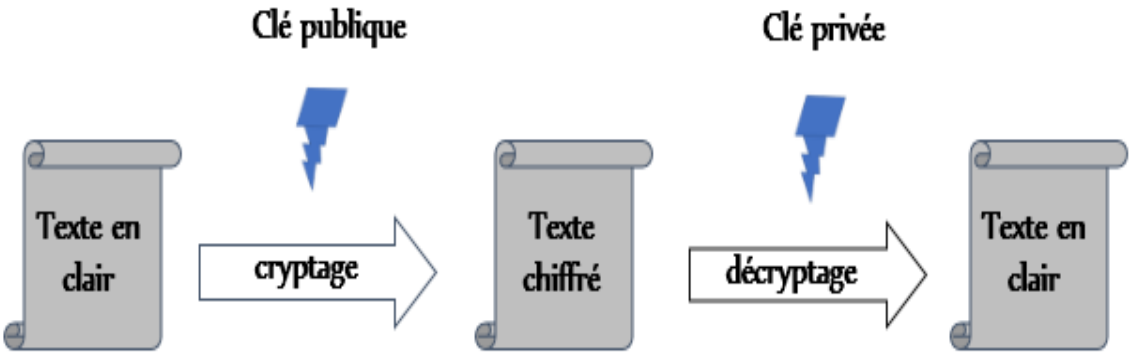

Figure 2.6 : Chiffrement asymétrique.

De manière générale, les algorithmes à clef publique reposent sur des problèmes mathématiques dans le domaine des théories de nombres, tels que factorisation des nombres (RSA) et logarithme discrete (El Gamal, ECC). Ces algorithmes ne résistent pas les attaques

quantiques. Tandis que, les algorithmes à clé publique de type post-quantum résistent ce type d'attaque, tels que les crypto systèmes NTRU et McEliece. La figure 2.7 illustre la classification des crypto systèmes asymétriques.

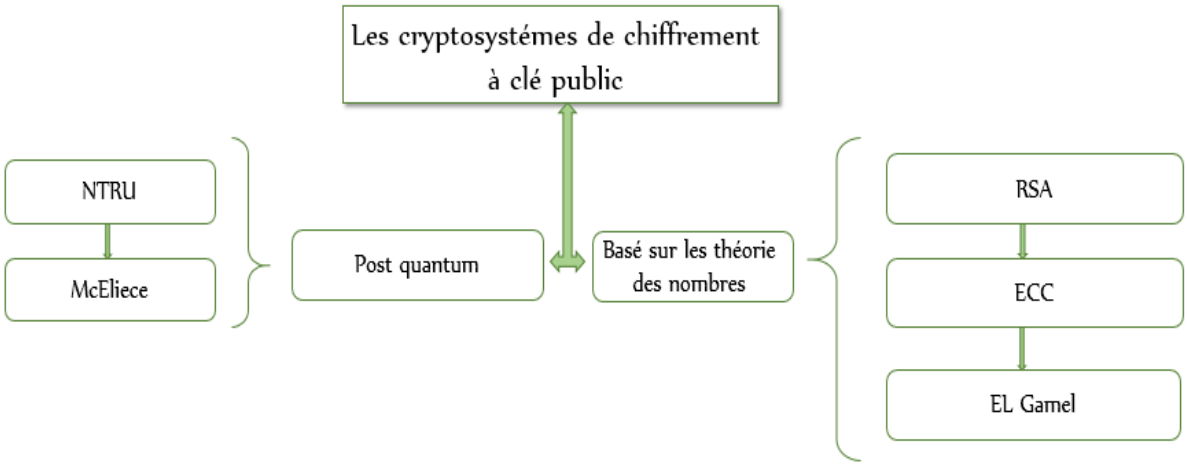

Figure 2.7 : Crypto-systèmes de chiffrement asymétrique (clé publique).

4.2.1. Les crypto-systèmes basé sur les théories des nombres

- **RSA**

Le crypto système RSA, inventé en 1977 par R. Rivest, A. Shamir et L. Adleman. La sécurité de RSA est basée sur la difficulté de factoriser les grands nombres entiers et la difficulté d'extraire la racine *n*-i`eme d'un entier modulo un grand nombre entier dont la factorisation est inconnue. [23] En effet, ce problème possède une faiblesse qu'il ne résiste pas aux algorithmes quantiques, comme celui de Shor qui permet de factoriser rapidement et donc monter une attaque de nature mathématique contre le crypto système RSA, ce qui signifie que si l'attaque est quantitative, toutes les clés RSA tomberaient [24] .

- **ECC**

Le crypto système ECC, the Elliptic Curve Cryptography, inventé indépendement en 1985 par N. Koblitz et V.S. Miller. La sécurité de ce crypto système est basée sur le problème du logarithme discret elliptique : Etant donné deux points P et Q d'une courbe elliptique E, déterminer un entier n tel que $nP = Q$. parmi les inconvénients des courbes elliptiques est que leur théorie est complexe et récente [25] , Le facteur de différenciation clé entre l'ECC et RSA est la taille de la clé comparée à la force de chiffrement. Comme le montre le graphique ci-dessus, l'ECC peut fournir la même force de chiffrement qu'un système basé sur l'algorithme

RSA, mais avec des clés beaucoup plus courtes. [26], ECC sont également sensibles aux percées quantiques.

4.2.2. Crypto système post quantum

La cryptographie quantique consiste à utiliser les propriétés de la physique quantique pour établir des protocoles de cryptographie qui permettent d'atteindre des niveaux de sécurité qui sont prouvés ou conjecturés non atteignables en utilisant uniquement des phénomènes classiques (c'est-à-dire non-quantiques). Un exemple important de cryptographie quantique est la distribution quantique de clés, qui permet de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information. Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles. Elle ne doit pas être confondue avec la cryptographie post-quantum qui vise à créer des méthodes de cryptographie résistante à un attaquant possédant un calculateur quantique [27]. Parmi les crypto-systèmes de cette type MCEliece et Ntru.

- **McEliece**

Le crypto système de **McEliece** inventé en 1978 par Robert McEliece. Ce système, reposant sur un problème difficile de la théorie des codes, n'a pas rencontré de véritable soutien dans la communauté cryptographique. L'une des principales raisons de cet état de fait est la taille de la clé. Pourtant, le crypto système de McEliece quelque avantage :

- La rapidité du chiffrement.
- Reposer sur un problème très différent des algorithmes asymétriques usuels.
- Le crypto système de McEliece résiste à ce jour à toute tentative de cryptanalyse [28]

- **NTRU**

Le crypto système NTRU, inventé entre 1996 et 1998 par J.H. Silverman, J. Hofistein et J. Pipher. La sécurité de NTRU est basée sur le problème du plus court vecteur non nul d'un réseau. Le nom NTRU en hommage à leur groupe de travail "Number Theorists Research Units".

- **Création des clefs**

« Choisit p et q deux entiers p << q, pose :

$R_q = \frac{\mathbb{Z}/q\mathbb{Z}[X]}{(X^n-1)}$, $R_p = \frac{\mathbb{Z}/p\mathbb{Z}[X]}{(X^n-1)}$ …… (3.1)

« Choisit un polynôme $f \in Rp$ tel que ($fp = f^{-1} mod\ p$)) et ($fq = f^{-1} mod\ q$)

« Choisit aléatoirement un polynôme $g \in Rp$ et calcule h=$g \times fq\ mod\ q$

« Clé publique *(Rp, Rq, h)*, clé privée *(fp =f−1 mod p , f)* , g est à écraser

- **Chiffrement**

« Prend la clé publique *(Rp,Rq,h)*

« Choisit un message $m \in Rp$

« Choisit un polynôme aléatoire $r \in Rp$ et calcule ($c = m + p.\ r \times h\ mod\ q$) qui est le chiffré.

- **Déchiffrement**

« Prend sa clé privée ($fp = f^{-1} \bmod p\ ;\ f$) ;

« Calcule $f\,c = fm + p{:}rg \bmod q$, (on suppose que $fm + p{:}rg \bmod q = fm + p{:}rg$)

« calculi ($f\,c \bmod q$) $\bmod p = fm \bmod p$

« calculi fp ($f\,c \bmod q$) $\bmod p = fp\ fm \bmod p = m \bmod p = m$

NTRU permet un cryptage et décryptage beaucoup plus rapides et une implémentation plus simple (toute l'arithmétique est effectuée en petit nombre) que RSA et ECC. La NTRU n'est pas seulement un crypto système à clé publique rapide, elle est également résistante aux technologies quantiques. [29]

4.3. Cryptographie hybride

La cryptographie hybride consiste, comme son nom l'indique, en une association des deux techniques de chiffrement précédentes où on code tout d'abord les données avec une clé privée dite *clé de session*, ensuite cette clé est chiffrée à l'aide d'une clé publique classique. Dans cette politique de cryptage le choix de chiffrer la clé d'une manière publique au lieu de chiffrer les messages est dû au fait que, la clé est souvent de petite taille par rapport aux données à chiffrer, donc, elle consomme beaucoup moins de temps lors de son chiffrement par rapport aux données. Ensuite, il ne reste qu'à transmettre le package contenant les données cryptées avec une clé privé, chiffrée de son tour avec une clé publique. Ainsi, les performances seront améliorées en associant la rapidité des systèmes de chiffrement symétriques et la bonne sécurisation des systèmes de chiffrement asymétriques. [30].

5. Chiffrement vidéo numérique

Par rapport à la communication textuelle, la communication vidéo se caractérise par un certain nombre de particularités, telles que la taille importante des données, les exigences en temps réel, l'utilisation de codecs vidéo normalisés, les formats de compression de données normalisés et les exigences de sécurité spécifiques à l'application.

5.1. Classification de chiffrement des vidéos

Il existe deux types principaux pour le chiffrement vidéo : chiffrement total et sélectif.

5.1.1. Le chiffrement total (full encryption)

Ce type de chiffrement consiste à encrypter toutes les données de l'information claire, il est rarement employé pour le chiffrement de vidéo, car s'il est appliqué pour chiffrer chaque image séparément de la séquence vidéo en mode spatial / fréquentiel, il conduira à accroitre le volume de vidéo chiffrée De même, s'il est appliqué pour chiffrer le flux binaire compressé, il va endommager son format. Grace à ces raisons, il est déconseillé de protéger la vidéo au moyen de ce type de chiffrement [2].

5.1.2. Le chiffrement sélectif (selective encryption)

Contrairement au chiffrement total, le chiffrement sélectif tente à chiffrer seulement un sous ensemble des données de l'image ou la vidéo à crypter. Les données chiffrées sont sélectionnée selon des critères et des conditions très variés. Mais le plus souvent, Les critères de sélection sont juste des conditions qui garantissent la confidentialité et la conformité de format de fichier compressé. Le chiffrement sélectif est appliqué souvent durant l'étape de compression afin d'obtenir un fichier conforme à la norme avec une taille proche ou identique au fichier clair, avec un haut niveau de sécurité. [2].

5.2. Chiffrement et compression vidéo

La **figure 1.8** illustre la taxonomie des techniques de chiffrement de vidéo , la relation entre la compression et le chiffrement est définir par deux classes primaires : des approches de chiffrement qui s'effectuent conjointement durant la compression ou ce qu'on appelle les systèmes de crypto-compression, et des approches de chiffrement qui ne dépendent pas d'aucune étape de compression vidéo [30] [2].

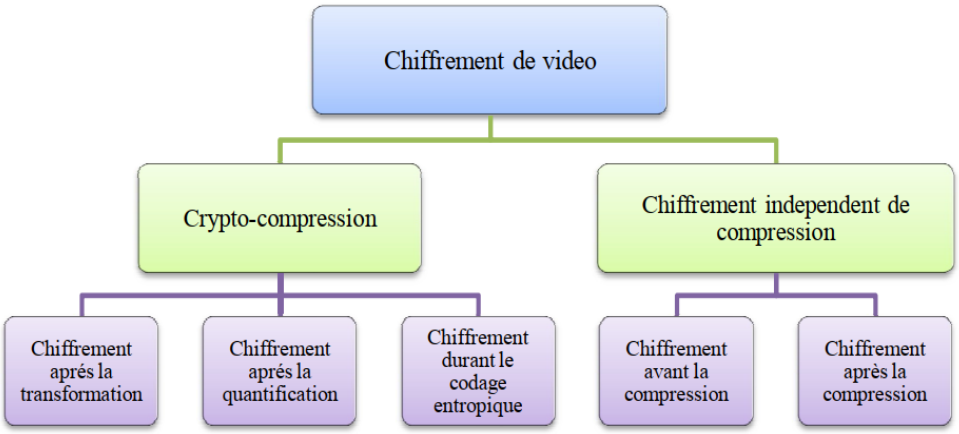

Figure 1.8 : Taxonomie des techniques de chiffrement de vidéo numérique.

5.2.1. Chiffrement indépendant de compression

Il existe deux types pour le chiffrement indépendant de compression :

❖ **Chiffrement avant la compression**

Les algorithmes de compression ont l'intention de réduire autant que possible la redondance de plaintext d'entrée. Les algorithmes de chiffrement cachent la redondance inhérente de plaintext d'entrée qui utilise des opérations cryptographiques. En conséquence, il y a beaucoup moins de redondance pour comprimer si ces algorithmes de chiffrement sont placés avant compression. Par conséquent, les algorithmes du chiffrement sont rarement rendus effectifs avant compression. Parmi les algorithmes de chiffrement se plaçant avant la compression, on trouve l'approche de Pazarci-Dipc ¸ et l'approche de chiffrement à base de préservation de corrélation de vidéo CPEV (correlation-preserving encryption video) [30] [2].

❖ **Chiffrement après la compression**

Le chiffrement naïf de la vidéo compressée peut altérer le décodage de la vidéo cryptée, car le format de flux binaire ne sera pas conforme avec la norme de codage convenue. Certaines approches comme SECMPEG et VEA ont réussi à chiffrer le flux binaire tout en préservant son format pour le décodage. Meyer et Gadegast ont proposé un chiffrement sélectif pour la norme MPEG1 en 1995. Les parties sélectionnées pour la protection sont chiffrées par des algorithmes de chiffrement conventionnels. Selon la quantité de données à être cryptée, quatre niveaux de sécurité sont définis :

- Premier niveau qui s'applique pour le chiffrement d'entêtes de la couche de la séquence (sequence layer), et les entêtes des couches de tranches.
- Deuxième niveau qui permet de chiffrer les coefficients de DCT de basse fréquence de chaque bloc dans chaque image intra.
- Troisième niveau qui permet de chiffrer seulement les blocs intra.
- Quatrième niveau qui permet de chiffrer entièrement le flux binaire de la vidéo compressée.

5.2.2. Les systèmes de crypto-compression pour la sécurité de vidéos

Dans ce type l'opération de chiffrement est combinée avec une opération de compression, et elles sont implémentées Le chiffrement peut être s'appliquer à n'importe quel stage de compression : après la transformation fréquentielle, après la quantification visuelle, et durant le module de codage entropique. [30] [31]

❖ **Chiffrement après la transformation**

Les données à chiffrer après la transformation fréquentielle de l'erreur résiduelle sont les amplitudes et les signes des coefficients. Chaque norme de codage dispose de son propre transformée appliquée. Le plus populaire est la transformée de DCT et ses améliorations. [30] [2]

❖ **Chiffrement après la quantification**

La quantification est l'étape qui permet la réduction de l'espace de coefficients. Ces derniers seront balayés et parcourus selon un mode de balayage. Le mode en zigzag est le plus populaire car il commence par les coefficients de basses fréquences, et il termine par les coefficients à hautes fréquences dont l'ordre de chaque QTC est déterminé selon la norme de codage adoptée. Les données possibles à chiffrer sont : les amplitudes et les signes de QTCs, et aussi l'ordre de QTCs [30] [2]

❖ **Chiffrement durant le codage entropique**

Après la sortie et la standardisation de chaque norme de codage vidéo, la préservation de la taille de flux binaire crypté sans augmentation, et avoir un format conforme décodable selon la syntaxe de la norme, occupe une préoccupation majeure pour la communauté cryptographique, car elle représente un défi réel à surmonter. Elle repose sur l'étude de la décidabilité des éléments syntaxiques après le chiffrement. Le choix de ces éléments syntaxiques et sa protection par un chiffrement sélectif sont des étapes communes suivies par la majorité

d'approches de chiffrement durant le codage entropique existantes dans la littérature scientifique.

Les données à crypter varient selon le codage entropique adopté par la norme de codage vidéo. Les normes de MPEG utilisent quant à eux, des tables de Huffman, où dans ce cas, chaque table se compose en codes de type VLC. H.264 et ses extensions utilisent un codage adaptatif selon le contexte par l'emploi de CAVLC et CABAC [30] [2] .

6. Conclusion

La cryptographie est la solution la plus utilisée pour sécuriser les Multimédia. Idéalement, il est préférable d'utiliser la cryptographie asymétrique pour protéger les vidéos.

Chapitre 3

TRAVEAUX EXISTANTS

1. Introduction

Ces dernières années, la sécurité vidéo est devenue la cible de nombreux algorithmes cryptographiques, Dans ce chapitre nous allons présenter les articles plus récents qui concerne le cryptage des vidéos numériques.

2. Iyer et all.

Iyer et all [32] ont proposé une approche pour sécuriser les vidéos basées sur la cryptographie hybride. Ils utilisent des fichiers texte intermédiaires au lieu de la vidéo cadres ou images. Il convertit le flux vidéo original en un fichier texte en le réduisant en un équivalent base64. Ce fichier texte est ensuite soumis à un double cryptage, c.-à-d. ECC et AES (voir le chapitre 2 élément 4.2.1 et 4.1.2) fournissent une double sécurité. Le processus de cryptage vidéo est illustré dans la Figure 3.1.

- **Les étapes de processus de cryptage**
  1- Lire la vidéo d'entrée de l'utilisateur.
  2- Convertissez la vidéo en un fichier texte au format Base64.
  3- Générer des clés publiques et privées ECC et l'AES clé symétrique.
  4- Cryptez le fichier Base64 avec la clé publique ECC.
  5- Chiffrer le fichier obtenu à l'étape précédente avec le Clé symétrique AES.
  6- Créez un code QR qui contient fichier crypté final, la clé AES et la clé privée ECC.

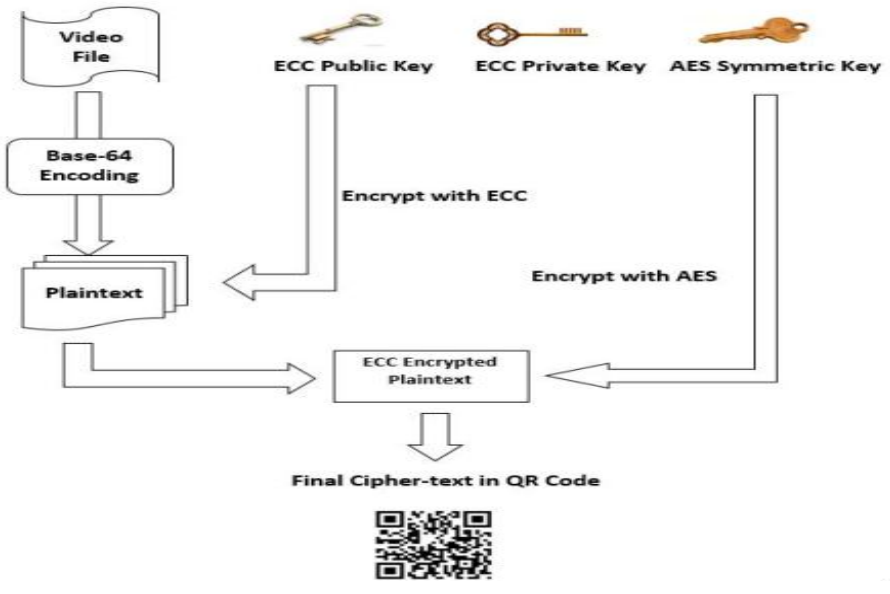

Figure 3.1 : Processus de cryptage vidéo

Le processus global de décryptage vidéo fonctionne exactement dans le sens inverse .et présenter dans la figure 3.2.

- **Les étapes de processus de décryptage vidéo**
  1- Lire le code QR.
  2- Extraire la clé symétrique AES
  3- Extrayez le texte chiffré du code QR.
  4- Appliquer le déchiffrement AES
  5- Extrayez la clé privée ECC du code QR.
  6- Appliquer le déchiffrement ECC.
  7- Reconvertissez le fichier intermédiaire en fichier multimédia d'origine à l'aide du déchiffrement Base64.

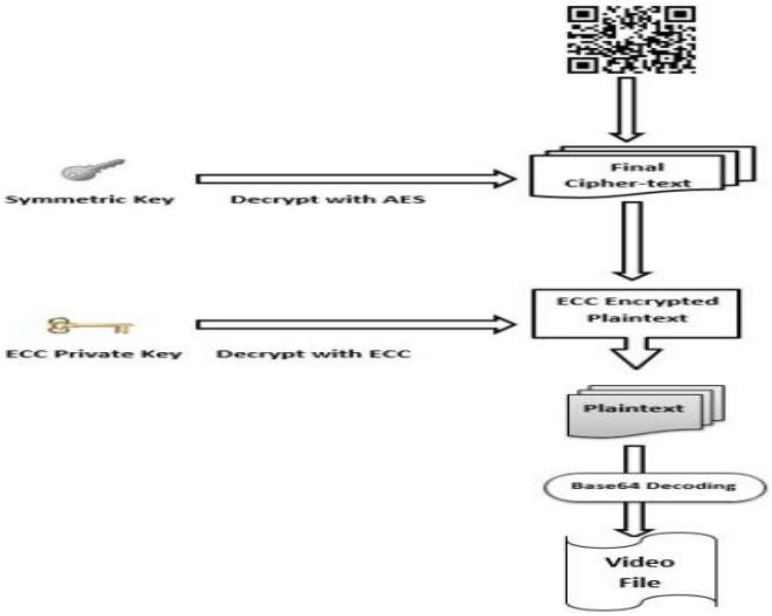

Figure 3.2 : Processus de décryptage vidéo

Généralement, le schéma proposé utiliser deux algorithmes de types différents, le premier algorithme est asymétrique (ECC) et le second est AES, un algorithme de chiffrement symétrique. Le premier algorithme est utilisé pour chiffrer la vidéo après sa transformation en un plaintext avec la base 64 et le deuxième est utilisé pour chiffrer le résultat de chiffrement de premier algorithme. Le schéma nous donne de meilleurs résultats à propos de la vitesse et de la précision. Le schéma repose sur la collecte de la vidéo cryptée et des clés des deux algorithmes dans le code QR afin de l'envoyer à l'autre partie, ces résultats n'aboutissent à rien car la propriété QR n'est pas protégée et tout le monde peut accéder aux clés et effectuer l'opération inverse.

3. **Dumbere et Janwe** [33]

Dumbere et Janwe ont proposé un schéma pour crypter une vidéo par l'algorithme a clé privée AES. Le schéma est basé sur l'extraction des images de vidéo et sur le chiffrement de chaque image à part, la figure 3.2 illustre le schéma proposé.

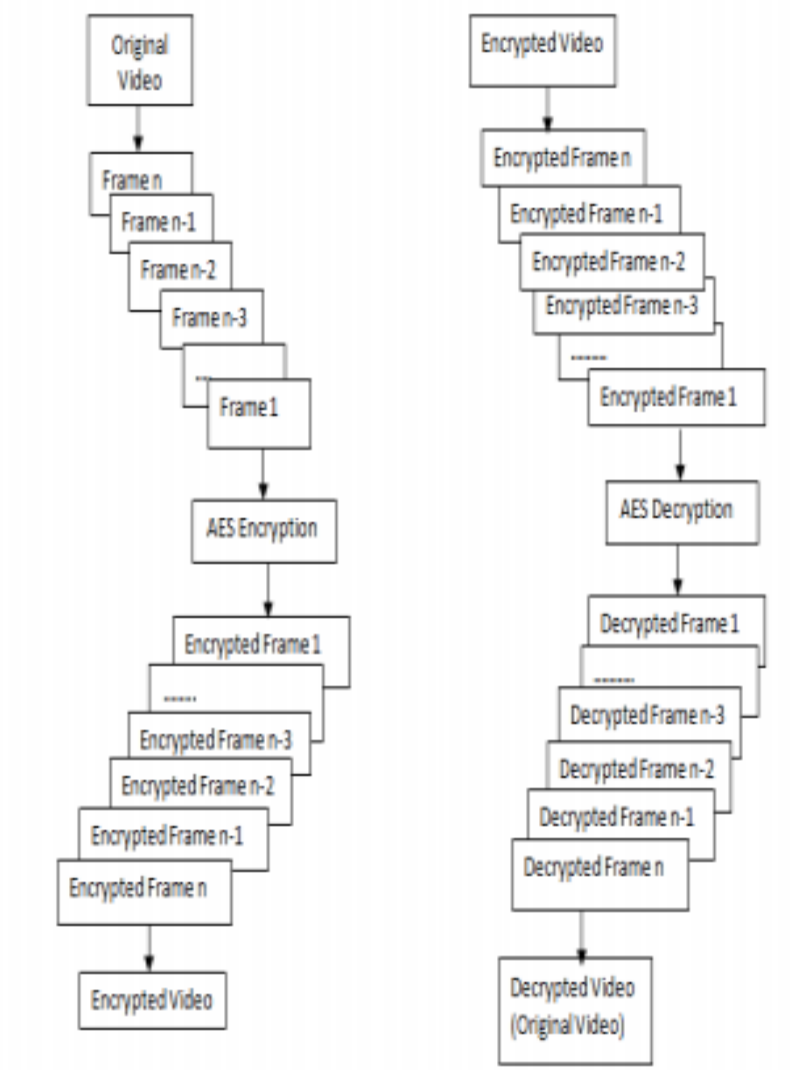

Figure 3.2 : Cryptage vidéo à l'aide de l'algorithme AES

Le schéma utilise les mêmes processus de cryptage et de décryptage pour les textes et les images. Il utilise également la même taille des clés et des nombres de rounds (voir chapitre 2 élément 4.1.2),

L'avantage de ce schéma est de fournir une protection contre la plupart des attaques. Cependant, elle prend du temps et réduit la qualité de l'image après le déchiffrement.

4. Dilkash et all [34]

Une autre approche de cryptage vidéo proposée par Dilkash et all basée sur le cryptage pixel. Le cryptage des pixels est effectué en mélangeant et en manipulant valeurs de pixel. Les positions des valeurs de pixels sont modifiées en fonction d'une séquence aléatoire générée. Le déchiffrement est effectué en commençant par mélanger les valeurs de pixel, puis en effectuant une manipulation inverse des valeurs de pixel individuelles pour obtenir le fichier vidéo d'origine.

❖ **La fonction de chiffrement**

- Extraire les images de la vidéo
- Créer une séquence aléatoire qui doit être égale au nombre d'éléments d'une image.
- L'étape suivante c'est le déplacement de pixel .il se produit en calculant la médiane de la plage (0 à 255), ensuite, les valeurs des pixels augmentent ou diminuent en fonction de la médiane (voir la figure 3.3).
- Utiliser la séquence aléatoire générée plus tôt pour mélanger la position des valeurs de pixel.
- Ajouter la séquence aléatoire à un fichier, La taille du fichier est égale à la taille de l'image
- Générer un ensemble fini des nombres aléatoires.
- Divise le fichier en nombre de sous-ensembles (de plage fixe) par l'utilisation de nombre aléatoire comme des indices de départ de chacun de ces sous-ensembles.
- Les nombres aléatoires utilisés sont ajoutés au fichier.
- Enfin les positions des pixels sont mélangées dans leurs sous-ensembles

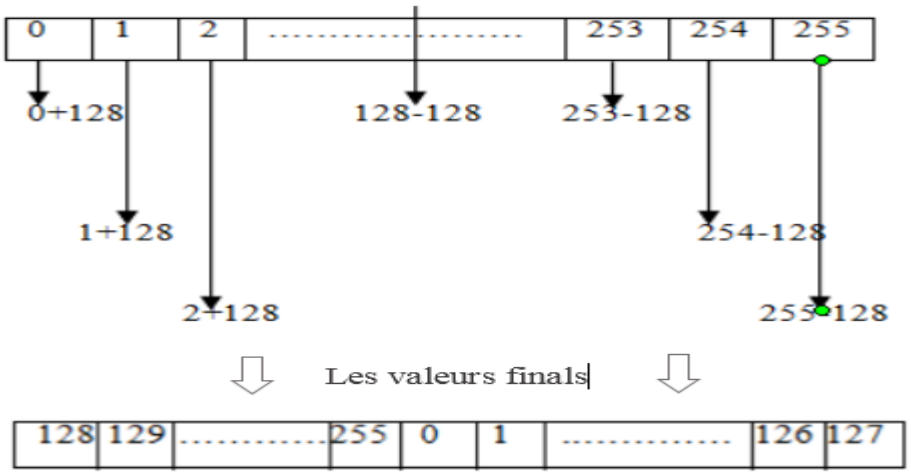

Figure 3.3 : La médiane de plage (0 à 255).

❖ **Pseudo-code pour le chiffrement**

```
Soit N le nombre d'images de la vidéo.
while j<N
 img=getsnapshot(vid);
 img_size=size(img);
 img1=zeros(img_size(1),img_size(2),img_size(3));
  if(j==0)
        idx=randperm(numel(img));
  end;

for a = 1:img_size(1)
     for b=1:img_size(2)
           for c=1:img_size(3)
img1(a,b,c) = img(a,b,c);
          end;
     end;
end;
for a =1:img_size(1)
      for b=1:img_size(2)
            for c=1:img_size(3)
if(img1(a,b,c)>=128)
      img1(a,b,c)=img1(a,b,c)-128;
       else if(img1(a,b,c)<128)
              img1(a,b,c)=img1(a,b,c) +128;
        end;
end;
img(a,b,c)= img1(a,b,c);
           end;
      end;
end;
shuffled_im=reshape(img(idx),size(img));
aviobj=addframe(aviobj,shuffled_im,shuffled_im);
j=j+1;
end;
```

Dans cette approche (Dilkash et all), ils n'ont pas parlé de la manière de générer la séquence aléatoire utilisé pour mélanger les pixels de l'image et les pixels de fichier. En plus, le mélange des pixels est aléatoire, Donc la qualité d'image après le décryptage est faible. L'approche proposée chiffre rapidement la vidéo et convient au cryptage en temps réel. Par contre, son chiffrement d'un fichier qui contient la séquence aléatoire est très complexe.

5. Chadha et all [35]

Ce schéma propose un algorithme de cryptage vidéo. Il utilise la séquence RSA et Pseudo Noise (PN), destiné aux applications nécessitant des transferts d'informations vidéo sensibles. Il est principalement conçu pour fonctionner avec des fichiers encodés à l'aide du codec AVI (Audio Vidéo Interleaved), la figure 3.4 présente le processus de cryptage et de décryptage.

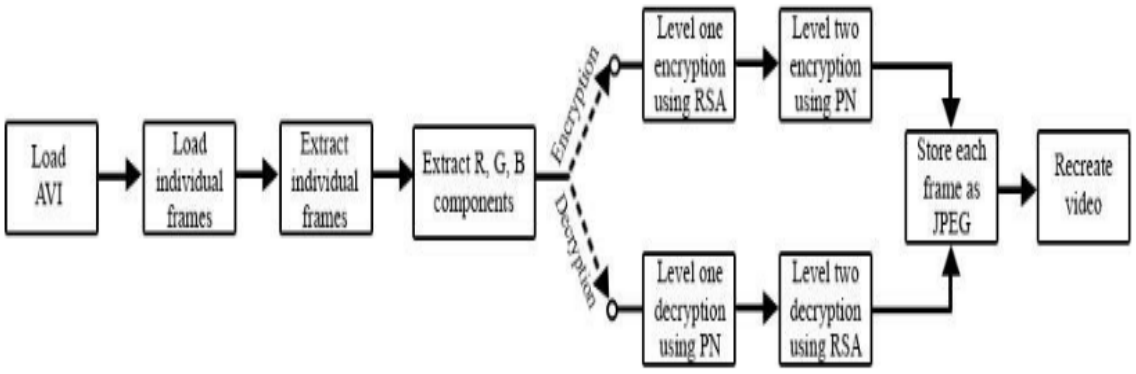

Figure 3.4 : Processus de cryptage et de décryptage.

❖ **La fonction de chiffrement**

- Charger Le fichier AVI.
- Extraire Les images du fichier chargé une par une.
- Après le processus d'extraction, les images sont chargées.
- Séparez les composants RVB de chaque image.
- Les trames RVB sont cryptées individuellement à l'aide de l'algorithme RSA.
- Crypter les trames RVB le 2 $^{-ème}$ fois par « pseudo random sequence noise ».
- Les composants RVB cryptés sont ensuite combinés en un fichier JPG.
- Les étapes 3 à 6 sont répétées pour toutes les images extraites.
- Le résultat est obtenu après utilisation de toutes les images stockées pour créer un fichier vidéo avec chaque image cryptée stockée en tant qu'image individuelle de la vidéo.

Le déchiffrement se produit à l'inverse de chiffrement, le schéma proposé présente une méthode de chiffrement à double couche qui permet d'obtenir une ressemblance visuelle nulle et une sécurité élevée, en oubliant pas que celle-ci prend du temp et déchiffre d'une manière complexe.

6. Conclusion

Dans ce chapitre, nous avons parlé des méthodes les plus importantes et les plus récentes pour le cryptage des vidéos. Dans le prochain chapitre, nous allons parler de notre schéma et comment développer une méthode pour crypter la vidéo numérique.

CHAPITRE 4

APPROCHE PROPOSEE ET IMPLEMENTATION

1. Introduction

Le cryptage vidéo est important pour assurer sa confidentialité lors de sa transmission sur des réseaux non sécurisés et pour son stockage. De nombreux algorithmes ont été suggérés pour le cryptage vidéo. Mais, presque tous ces algorithmes sont moins sécurisés, dans ce chapitre nous allons proposer un nouvel schéma pour garantir la confidentialité et l'authenticité de la vidéo.

2. Notre approche

Notre approche est basée sur l'hybridation entre deux algorithmes, le premier est de type symétrique (AES). Et le deuxième de type post quantum l'algorithme (NTRU), l'AES est utilisé pour chiffrer la vidéo, et l'NTRU est utilisé pour chiffrer la clé AES. Pour le scénario de transmission vidéo, l'expéditeur chiffre la vidéo et la clé et les envoie au destinataire, et pour accéder à la vidéo, le destinataire doit déchiffrer la clé AES avant de déchiffrer la vidéo.

Dans le Schéma proposé, il existe trois étapes dans le cas de chiffrement (Voir la **figure 4.1**) :

Etape 1 : utiliser l'algorithme AES avec le mode CBC pour crypter la vidéo.
Etape 2 : utiliser la clé publique de crypto système NTRU pour chiffrer la clé sécrète de l'AES.
Etape 3 : collecter la vidéo cryptée et la clé symétrique cryptée et les envoyer au destinataire

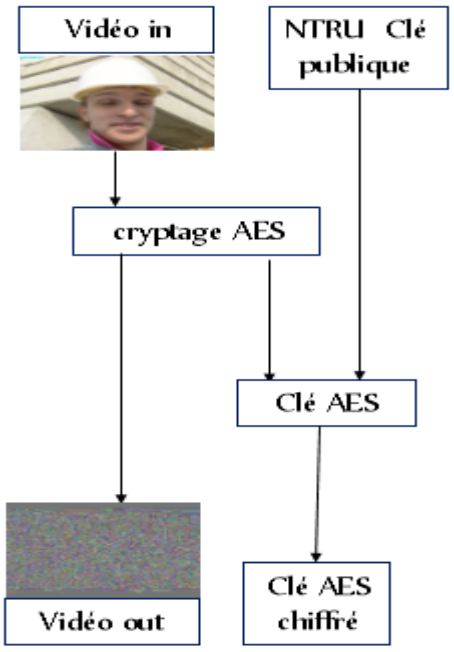

Figure 4.1 : Le système proposé pour le chiffrement

Le déchiffrement se compose également de trois étapes, mais dans l'ordre inverse (Voir la **figure 4.2**) :

Etape 1 : après la réception nous avons séparé la vidéo cryptée de la clé symétrique chiffrée.

Etape 2 : utiliser la clé privée de cryptosystème NTRU pour déchiffrer la clé AES.

Etape 3 : utiliser la clé symétrique pour déchiffrer et accéder à la vidéo.

Le but principal de ce chiffrement c'est de garantir la confidentialité de l'information vidéo après l'envoie.

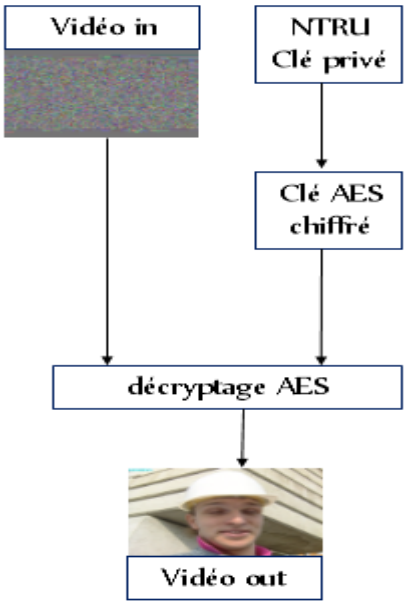

Figure 4.2 : Le system proposé pour le déchiffrement

2.1. Fonctions cryptographiques utilisées

Nous avons divisé notre approche en deux fonctions, la première est le cryptage et le décryptage vidéo, et la seconde est le cryptage et le décryptage de la clé AES.

2.1.1. Cryptage /décryptage de la vidéo

- Charger Le fichier AVI.
- Lire une image à la fois.
- Crypter chaque image individuellement par l'algorithme AES.
- Générer la clé de chiffrement de l'algorithme AES de taille 128 bits.
- Afficher le vidéo chiffré.

Le décryptage se compose également les mêmes étapes, mais dans l'ordre inverse. La Figure 4.3 illustre le cryptage/décryptage de la vidéo.

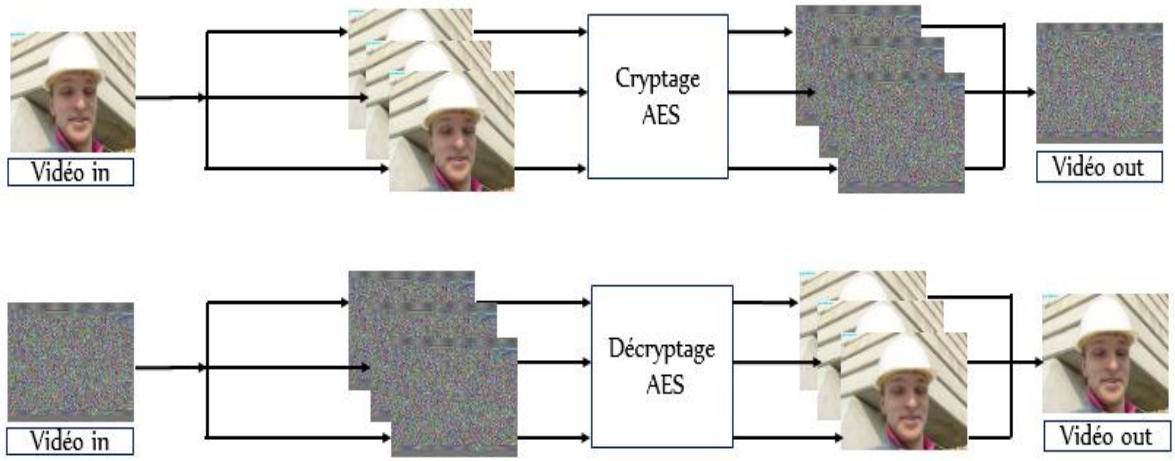

Figure 4.3 : Cryptage et décryptage de vidéo

Nous avons utilisé 38 frames de vidéo **carphone.avi** avec une résolution de 176 * 144 (qcif format),1.41mb taille et 3s longueur. La Figure 4.4 illustre des mages prises à différents moments de la vidéo (début, centre, finale).

Figure 4.4: Images prises à différents moments de la vidéo.

Les Figures 4.5 et 4.6 illustre le cryptage et le décryptage des images prises à différents moments de la vidéo.

Figure 4.5: Les images prises à différents moments de la vidéo après le cryptage

Figure 4.6: les images prises à différents moments de la vidéo après le décryptage

2.1.2. Cryptage / décryptage de la clé AES

La figure 4.3 présenter la cryptage/décryptage de la clé AES par la crypto-system a clé publique NTRU.

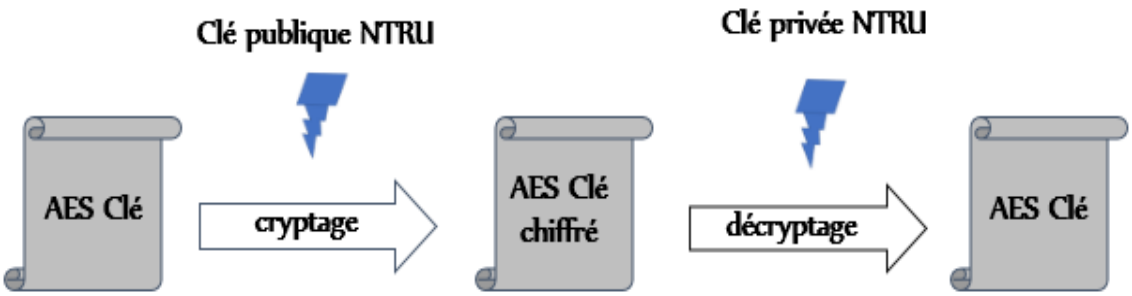

Figure 4.7 : Cryptage et décryptage de la clé AES.

Nous avons pris la clé AES comme une chaine et crypté par le crypto-system NTRU. Nous avons choisi le *APR2011_743_FAST* un ensemble de paramètres qui donne 256 bits de sécurité mais utilise des polynômes de forme produit et f = 1 + pF. Parmi les paramètres utilisés :

N : nombre de coefficients polynomiaux

q : module

df : nombre d'uns dans le polynôme privé f

dm0 : nombre minimum acceptable de -1, de 0 et de 1 dans le polynôme m 'lors de la dernière étape de cryptage

db : nombre de bits aléatoires à ajouter au message

c : un paramètre pour la fonction de génération d'index

Nous avons utilisé NTRU en raison de ses fonctionnalités telles que la facilité à générer des clés, une vitesse élevée, une utilisation réduite de la mémoire et non affecté par les attaques quantiques.

3. Implémentation

3.1. Environnement d'application

Nous avons utilisé les deux environnement MATLAB et JAVA pour l'implémentation de notre approche.

- MATLAB : « matrix laboratory » est un langage de programmation de quatrième génération émulé par un environnement de développement du même nom ; il est utilisé à des fins de calcul numérique. Développé par la société The MathWorks, Matlab permet de manipuler des matrices, d'afficher des courbes et des données et de mettre en œuvre des algorithmes. Nous avons utilisé le Matlab pour le chiffrement / déchiffrement de la vidéo. [36]
- JAVA : L'environnement d'exécution Java (abr. JRE pour Java Runtime Environment), parfois nommé simplement « Java », est une famille de logiciels qui permet l'exécution des programmes écrits en langage de programmation Java (orienté objet), sur différentes plateformes informatiques. Il est distribué gratuitement par Oracle Corporation, sous forme de différentes versions destinées aux systèmes d'exploitation Windows, Mac OS X et Linux2, toutes conformes aux Java Spécification Requetés (JSR). [37]

3.2. Bibliothèques

- La bibliothèque de fonctions mathématiques MATLAB : Il s'agit d'une vaste collection d'algorithmes de calcul allant des fonctions élémentaires comme la somme, le sinus, le cosinus et l'arithmétique complexe, à des fonctions plus sophistiquées comme la matrice inverse, les valeurs propres matricielles, les fonctions de Bessel et les transformées de Fourier rap.
- Ntru-1.2 : Une implémentation Java du crypto système à clé publique NTRU, constituée du schéma de chiffrement NTRUEncrypt et du schéma de signature NTRUSign

3.3. Environnement matériel

L'application a été créa depuis un PC LENOVO G50 :

- Mémoire : 8192 MB RAM.
- Processeur : Intel ® Core^{TM} i3 4005U CPU @ 1.70 GHZ.

- Système d'exploitation : Windows 7 Ultimat 64 bits
- Carte Graphique : 44000 Family.

4. Résultats expérimentaux

Dans cette section, nous présentons les différents résultats expérimentaux de notre approche.

- **L'histogramme**

L'histogramme d'une image fait référence à un graphique du pixel valeurs d'intensité. L'histogramme est un graphique montrant le nombre de pixels dans une image à différentes valeurs d'intensité trouvé dans l'image.

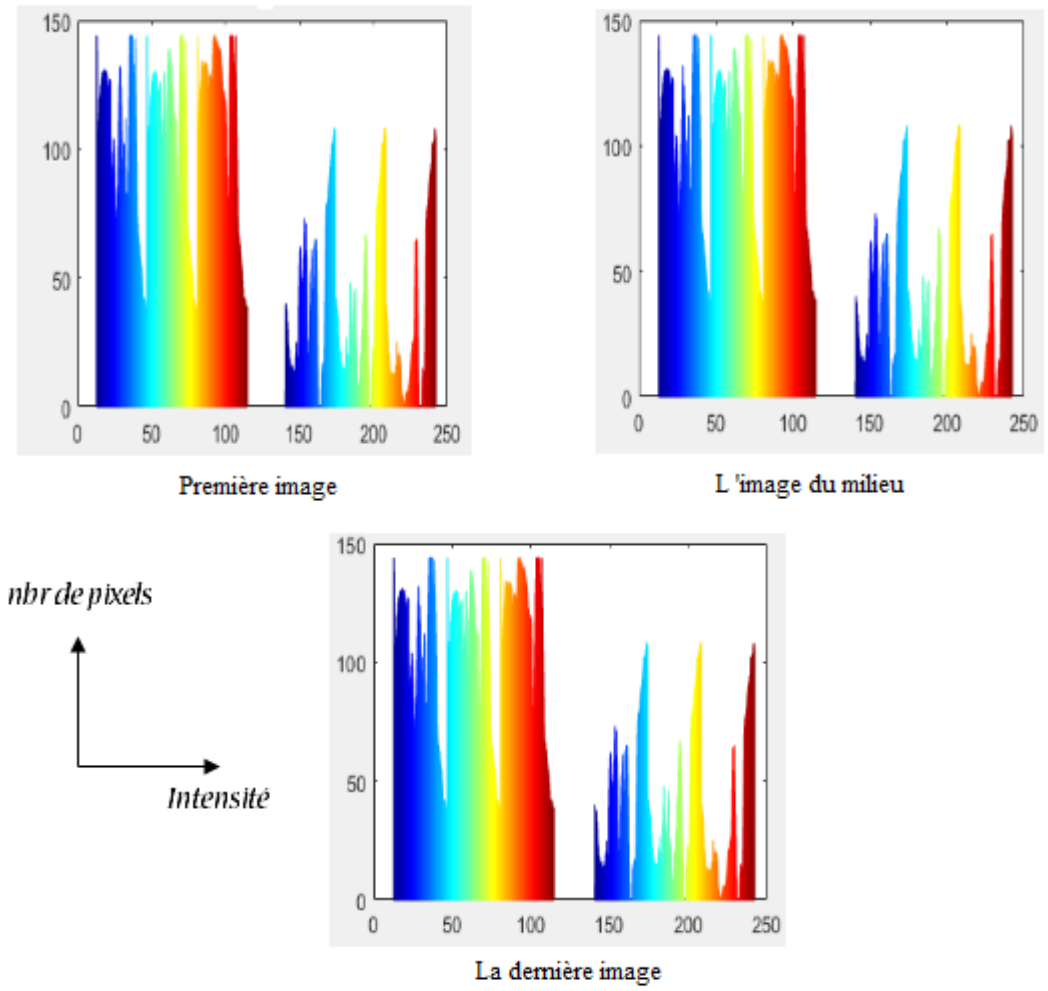

Figure 4.8: L'histogramme des images prises à différents moments de la vidéo original.

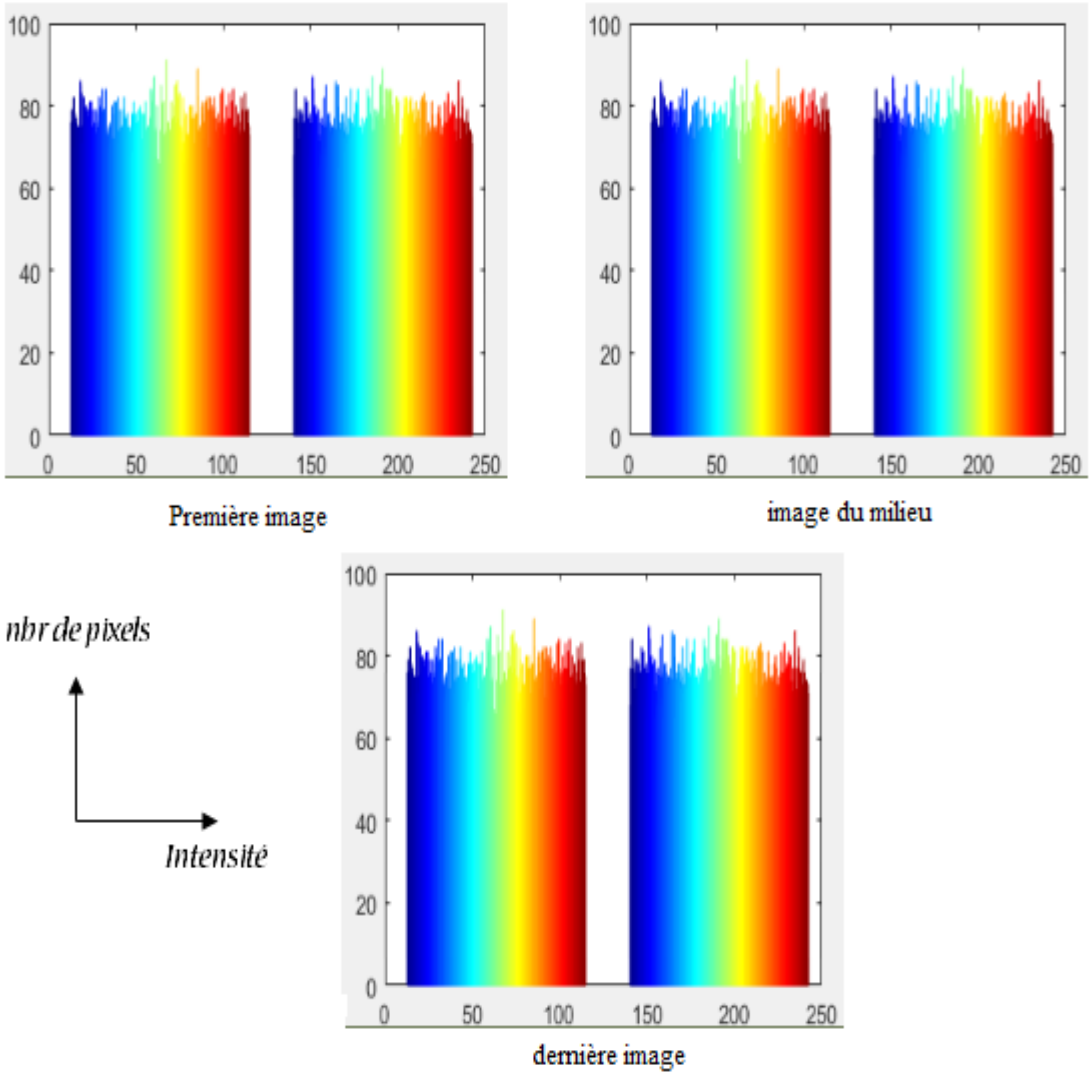

Figure 4.9: L'histogramme des images prises à différents moments de la vidéo après le cryptage.

- **PSNR (peak signal-to-noise ratio)**

Est calculé à l'aide de l'erreur quadratique moyenne (MSE) qui devrait idéalement être aussi faible que possible pour un déchiffrement sans perte. Le PSNR est calculé comme suit :

$$PSNR = 10.\log10\ (M2 / MSE) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (4.1)$$

Où M = valeur maximale possible du pixel de l'image.

Pour notre approche la valeur PSNR de l'original vidéo est 5.66654 et le valeur PSNR de la valeur après le décryptage est 3.21172

- **SSIM (**Structural Similarity Index)

Le principe est d'évaluer la dégradation en fonction du contexte local du défaut ; il est fait une pondération de 3 paramètres : Luminance, Contraste et Contours, la formule de calcul de la méthode et le suivant :

$$SSIM(x,y) = \left(\frac{(2\mu_x\mu_{\hat{x}} + C_1)(2cov_{x\hat{x}} + C_2)}{(\mu_x^2 + \mu_{\hat{x}}^2 + C_1)(\sigma_x^2 + \sigma_{\hat{x}}^2 + C_2)}\right) \quad \text{.....(4.2)}$$

μ_x est la moyenne de x.

$\mu_{\hat{x}}$ est la moyenne de $\hat{x}$.

σ_x^2 est la variance de x.

$\sigma_{\hat{x}}^2$ est la variance de $\hat{x}$.

$cov_{x\hat{x}}$ est la covariance de x et $\hat{x}$.

$C_1=(K_1L)^2$; avec $k_1=0.01$ et L : nombre d'échelons de Luminance.

$C_1=(K_2L)^2$; avec $k_2=0.03$ et L : nombre d'échelons de Luminance.

Les Figure 4.8 et 4.9 illustrent la valeur SSIM de la vidéo originale et après le décryptage.

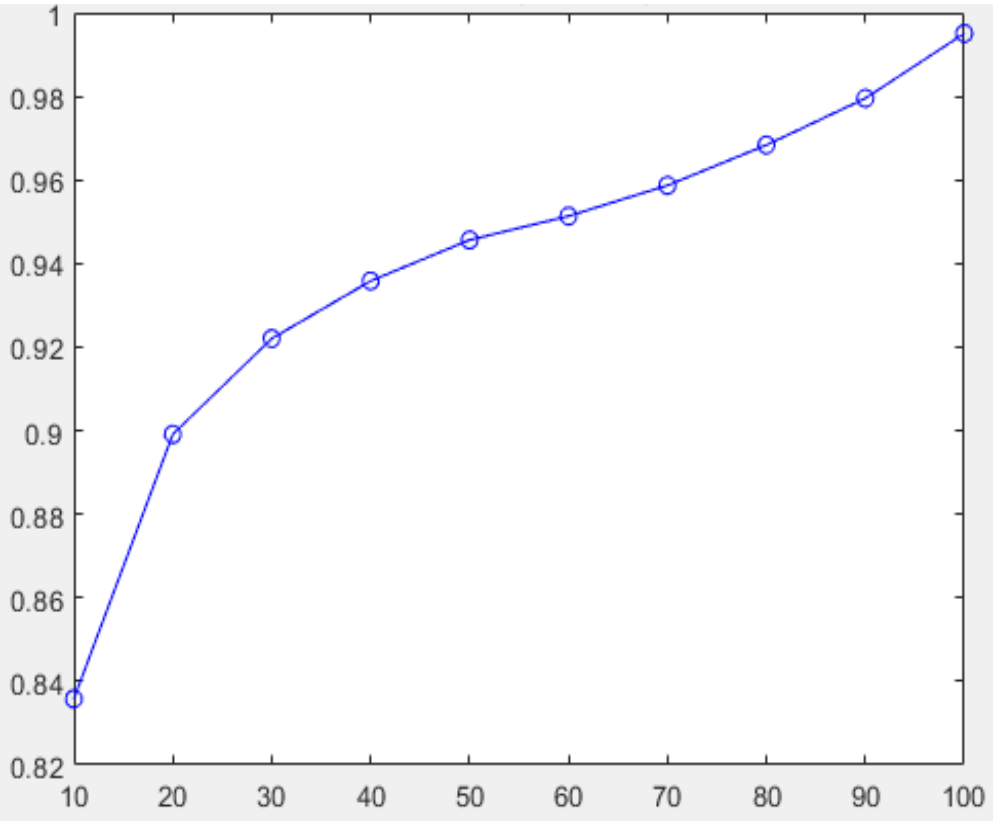

Figure 4.10:la valeur SSIM de vidéo original

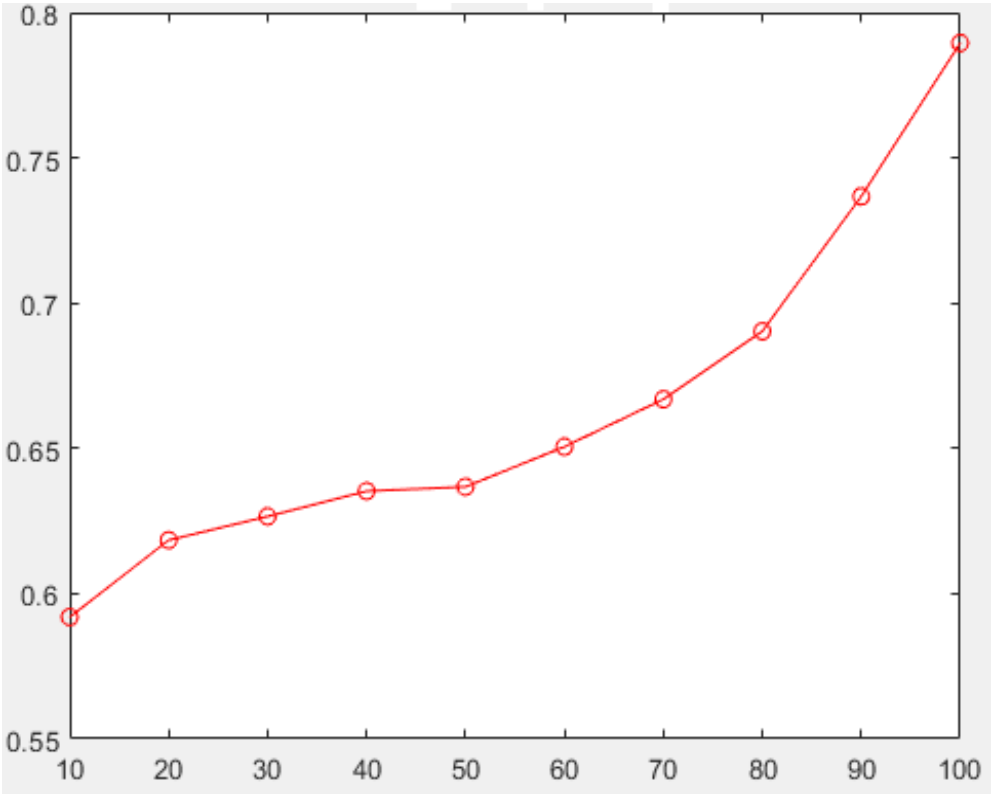

Figure 4.11 : la valeur SSIM de vidéo après le décryptage.

5. Discussion

A partir de la Table 4.1, nous observons qu'il existe des changements dans les déférents caractéristique du fichier vidéo, par exemple la taille de vidéo original est 1.41Mb par contre la taille de fichier vidéo après le chiffrement est 2.81Mb.

	Vidéo original	**Vidéo chiffré**	**Vidéo déchiffré**
Taille (Mb**)**	1.41	2.81	2.74
Nombre de frame	38	37	36
Longueur (s**)**	3.17	1.23	1.20
Taux de frame (fps**)**	12	30	30

Table 4.1 : les analyses du vidéo avant et après le chiffrement.

Nous remarquons également que la longueur de la vidéo a changé et est liée directement au taux des frames. Plus taux des frames est élevé, plus la longueur est courte, Outre les modifications apportées à la vidéo après le processus de cryptage et de décryptage. Les graphiques montrent que la précision n'a pas été beaucoup affectée par le retour au facteur SSIM. La même chose est vraie pour l'index PSNR.

Par conséquent l'histogramme d'image chiffrée est très uniforme après le cryptage, voire, l'attaquant il ne peut pas extraire l'information à partir de l'histogramme de l'image cryptée.

Notre approche est utilisée les algorithmes cryptographiques AES et NTRU, ces deux types sont restant les attaques quantiques, par contre l'approche utilisé par Chadha et all [35], elle s'utilisé l'RSA et Pseudo Noise, le type RSA ne résiste pas les attaques quantiques selon l'algorithme de shor. [38]

Dans une petite comparaison entre notre approche avec une autre approche utilisant AES et RSA, nous avons conclu que notre approche était plus rapide (voir la Table 4.2) avec une assurance totale de la confidentialité de la vidéo.

	AES /RSA	AES/NTRU
Chiffrement vidéo	79.88	79.88
Déchiffrement vidéo	67.40	67.40
Génération des clés (Publique et privé)	2	1
Chiffrement et Déchiffrement Clé symétrique	1	0.7
Total	150.28	148.98

Table 4.2 : Temps d'exécution de deux approches (s).

6. Conclusion

Dans ce chapitre nous avons présenté notre approche, qui dépend sur l'hybridation entre deux algorithmes, pour sécuriser les vidéos numériques.

Nous avons utilisé l'algorithme de cryptage symétrique AES pour crypter le vidéo et l'algorithme NTRU pour crypter la clé symétrique. Enfin, nous avons discuté des résultats obtenus.

CONCLUSION GÉNÉRALE

De nos jours, de plus en plus les vidéos numériques sont transférées ou stockées sur les réseaux informatiques. Avec le temps, la confidentialité de vidéo numérique est devenue indispensable. Au cours de ce mémoire, nous avons proposé un schéma de sécuriser le vidéo basé sur l'hybridation entre deux algorithmes, le premier algorithme de cryptographie symétrique AES, qui utilisé pour chiffrer la vidéo, et le deuxième algorithme NTRU, est schéma cryptographique post-quantum, qui utilisé pour crypter la clé symétrique. Le but principal de ce chiffrement c'est de garantir la confidentialité de l'information vidéo après l'envoie.

Les résultats expérimentaux montrent que notre approche dispose un niveau élevé de sécurité et d'efficacité.

Finalement les comparaisons avec les approches existants, montrent que l'approche proposé offre des performances très favorables.

Comme perspective à ce travail, nous allons améliorer notre approche sur le chiffrement sélectif.

Bibliographie

[1] Comment ça marche, www.commentcamarche.net/contents/1493. consulté le 13 02 2019.

[2] O. Mokhtar, thèse Doctorat, sécurité et compression de l'information multimédia, 2015.

[3] R. Westwater, B. Furht, Real-Time Video Compression Techniques and Algorithms, 1997.

[4] I. E. G. Richardson, H.264 and MPEG-4 Video Compression, Aberdeen, UK: The Robert Gordon University, 2003.

[5] Basic Concepts and Techniques of Video Coding and the H.261 Standard.

[6] wikiversity, https://fr.wikiversity.org/wiki/Formats_vidéo. consulté le 15 02 2019.

[7] F. D. Rango, Digital Vidéo,InTech, 2010.

[8] K. Sayood, Introduction to data compression, 500 Sansome Street, Suite 400, San Francisco, 2006.

[9] MPEG, http://www.chiariglione.org/mpeg, consulté le 13 02 2019.

[10] D. L. Gall, MPEG: A video compression standard for multimedia application, ACM, pp. 48-58, 1991.

[11] Vbrick,https://www.vbrick.com/doc/VBDNA/v41/GettingStarted/wwhelp/wwhimpl/js /html /wwhelp.htm?href=4_Streaming_Basics.html,consulté le 13 02 2019

[12] Y. Tan, D. D. Saur, S. R. Kulkami, P. J. Ramadge, Rapid estimation of camera motion from compressed video with application to video annotation, IEEE Transactions on Circuits and Systems for Video Technology, n°110, p. 133–146, 2000.

[13] J. Watkison, The MPEG Handbook, Focal Press, 2005.

[14] M. Ghanbari, Standard Codecs Image compression to advanced video coding, vol. 3rd Edition, The Institution of Engineering and Technology, 2011.

[15] A. Puria, X. Chen ,A. Luthra, Video coding using the H.264/MPEG-4 AVC compression standard,SienceDirect, pp. 1701-1713, 1993.

[16] Securite info, https://www.securiteinfo.com/cryptographie /aes.shtml, consulté le 13 02 2019

[17] A. Wurcker, Thèse Doctorat, Etude de la sécurité d'algorithmes de cryptographie embarquée vis-à-vis des attaques par analyse de la consommation de courant, 2015.

[18] S. Ismahane, Thése Doctorat, Sécurisation évolutionnaire du transfert d'images, 2012.

[19] J. Dumas, E. Tannier, J. Roch et S. Varrette, Théorie des codes : Compression , Cryptage, Correction, 2007.

[20] A. Uhl, A. Pommer, Image and Video Encryption From Digital Rights Management to Secured Personal Communication, Springer, 2005.

[21] Labouret, http://www.labouret.net/crypto/#212, consulté le 13 02 2019.

[22] N. Smart, Cryptography Made Simple, 2015.

[23] A. Nitaj, NTRU et ses variantes, sécurité et applications, Laboratoire de Mathématiques Nicolas Oresme Université de Caen.

[24] N. GAMA ,Thése Doctorat, Géométrie des nombres et cryptanalyse de NTRU, 2008.

[25] A. BOUMSO, Thése Doctorat, Méthode exploratoire de distribution des clé de cryptage pour les communications de groupe dans un réseau mobile ad hoc, 2006.

[26] Informatique news, https://www.informatiquenews.fr/lecc-une-alternative-aux-cles-rsa-36516, consulté le 13 02 2019

[27] Cryptographie quantique, https://fr.wikipedia.org/wiki/Cryptographie_quantique, consulté le 13 02 2019.

[28] fr academic ,https://fracademic.com/dic.nsf/frwiki/472618 , consulté le 13 02 2019.

[29] S. Singh, S. Padhye, Generalisations of NTRU cryptosystem,Security Comm. Networks, pp. 6315-6334, 2016.

[30] W.BIROUK,Mémoire de majister , Sécurisation des données sensibles sur téléphone mobile / dispositif d'assistant numérique personnel (PDA), 2007.

[31] F. Liu, H.Koenig , A survey of video encryption algorithms, Sience Direct, vol. Volume 29, n° 1Issue 1, pp. 3-15, February 2010.

[32] S.C. Iyer , R.R Sedamkar ,S. Gupta, A Novel Idea of Video Encryption using Hybrid Cryptographic Techniques,ScienceDirect, n° 179, p. 293 – 298, 2016 .

[33] D. M. Dumbere, N. J. Janwe, Video Encryption Using AES Algorithm, IEEE, pp. 332-337, 2014.

[34] N. Dilkash, A.Gupta ,A.Jain, Real Time Video Encryption for Secure Multimedia Transfer: A Novel Approach, IJESC, vol. Volume 8 Issue No.4, pp. 17077-17080, 2018.

[35] A. Chadha, S. Mallik, A. Chadha, R. Johar, M. ManiRoja,Dual-Layer Video Encryption using RSA Algorithm, IJCA, vol. Volume 116 –No. 1, pp. 33-40, 2015.

[36] wikipedia ,https://fr.wikipedia.org/wiki/MATLAB, consulté le 13 02 2019.

[37] wikipedia,https://fr.wikipedia.org/wiki/Environnement_d27exC3A9cution_Java ,consulté le 28-06-2019.

[38] medium, J. Hui,https://medium.com/@jonathan_hui/qc-cracking-rsa-with-shors-algorithm-bc22cb7b7767. Consulté le 11 07 2019.

ملخص

مع النمو السريع في استخدام الفيديو الرقمي في العديد من التطبيقات، تعد حماية بيانات الفيديو السرية من الوصول غير المصرح به مجالًا مهمًا جدًا للبحث. في هذه الرسالة النهائية، اقترحنا طريقة أمان فيديو محسّنة، استنادًا إلى التهجين بين خوارزميتي تشفير، الخوارزمية الأولى عبارة عن خوارزمية تشفير متماثلAES ، تستخدم لتشفير الفيديو. الخوارزمية الثانية هيNTRU ، وهي خوارزمية تشفير ما بعد الكم، ويتم استخدامها لتشفير المفتاح المتماثل. بالإضافة إلى ذلك، قمنا بتطبيق نهجنا وناقشنا النتائج التجريبية المختلفة. نهجنا هو أكثر أمنا مقارنة مع النهج الأخرى التي شملتها الدراسة.

Abstract

With the rapid growth in the use of digital video in many applications, protecting confidential video data from unauthorized access is a very important area of research. In this final thesis, we proposed an improved video security approach, based on the hybridization between two cryptographic algorithms, the first algorithm is a symmetric cryptographic algorithm AES, which used to encrypt the video. The second algorithm is NTRU, is a post-quantum cryptographic algorithm, it is used to encrypt the symmetric key. In addition, we implemented our approach and discussed the different experimental results. Our approach is more secure compared to other approaches studied.

Résumé

Avec la progression rapide de l'utilisation des vidéos numériques dans de nombreuses d'applications, la protection des données de vidéo confidentielles contre les accès non autorisés est un domaine de recherche très important. Dans ce mémoire de fin d'étude, nous avons proposé une approche améliorée de sécurisation des vidéos, qui basée sur l'hybridation entre deux algorithmes cryptographiques, le premier algorithme est un algorithme cryptographique symétrique AES, qui utilisé pour chiffrer la vidéo. Le deuxième algorithme est NTRU, est un algorithme cryptographique post-quantum, il est utilisé pour crypter la clé symétrique. De plus, nous avons implémenté notre approche et nous avons discuté les différents résultats expérimentaux. Notre approche est plus sécurisée par rapport d'autres approchés étudiées.

Mot clé : cryptage vidéo, cryptographie hybride, AES, NTRU, AVI.