République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études
En vue de diplôme de Master en informatique

Option : Réseaux et systèmes distribués (RSD)

Thème :

Développement d'une application de cryptage des vidéos en utilisant les alghorithemes de chiffrement RSA et 3-WAY en exploitant la bibliothèque FFMPEG

Réalisé par

- M^elle Berrezoug lilya wissem.
- M^elle ouadah meriem.

Présenté le : 26/06/2024.

- Mr Benmammar Badr (President).
- Mr Fekar Riyadh (Examinateur).
- Mr BENAISSA Mohamed Samir (Encadrant).

Année universitaire : 2023-2024


لا إله إلا الله محمد رسول الله

"Les compétences techniques sont importantes, mais elles ne sont rien sans la capacité de comprendre et de résoudre les vrais problèmes."

Margaret Hamilton.

Dédicace

On dédie ce travail,

A nos chers parents

A nos chers frères

A ceux qui comptent le plus pour nous

Cette réussite est aussi la vôtre. Merci à tous ceux

ont contribué à ce travail, de près ou de loin. Votre soutien

a été mon phare dans la nuit.

Remerciement

Tout d’abord, je tiens à remercier DIEU le tout Puissant de m’avoir donné le courage, la volonté, la force et la patience pour mener à terme ce travail.

En premier lieu, nous tenons à remercier chaleureusement toute l'équipe pédagogique du département d'informatique pour son soutien continu tout au long de notre parcours académique.

Nos remerciements les plus spéciaux vont à M. Benaissa, dont l'encadrement a été d'une valeur inestimable. Nous apprécions le temps qu'il nous a consacré, ainsi que ses conseils et remarques indispensables qui ont grandement enrichi notre travail.

Un grand merci est également adressé à nos professeurs du département d'informatique et aux membres du jury qui ont accepté de juger notre travail avec bienveillance.

Enfin, nous exprimons notre reconnaissance à toutes les personnes ayant contribué, de près ou de loin, à la réalisation de ce projet. Votre implication a été essentielle, et nous sommes reconnaissants de pouvoir partager le fruit de ce travail avec vous.

Table des matières

CHAPITRE 2 : Concepts de base/Chiffrement de vidéo numérique

CHAPITRE 3 : Les algorithmes de chiffrement RSA et 3-WAY/ Etude la bibliothèque FFMPEG.

CHAPITRE 4 : Test des résultats

TABLE DES FIGURE

Chapitre 1

Chapitre 2

Chapitre 3 :

Chapitre 4 :

LISTE DES TABLEAUX

Chapitre 2

Chapitre 3

Chapitre 4

Introduction générale

Depuis les temps anciens, la préoccupation fondamentale de l'humanité demeure la sécurité. L'évolution des réseaux informatiques et des communications par Internet, englobant divers types de données comme les messages textuels, les images et les fichiers volumineux tels que les vidéos, a sensiblement complexifié les défis liés à la sécurité ainsi que les solutions à y apporter. Actuellement, les vidéos numériques renferment une richesse d'informations considérable, jouant un rôle prépondérant dans les échanges contemporains. Elles sont utilisées de manière étendue dans des secteurs sensibles tels que les systèmes de visioconférence, le commerce électronique et les diffusions vidéo, accentuant ainsi la cadence des progrès dans les domaines de la communication audio et vidéo. Cependant, l'émergence de nouveaux défis, tels que les virus informatiques, les accès non autorisés aux données et la propagation de fausses informations, crée un besoin impérieux de sécurisation des informations. Ainsi, la sécurité des données devient une exigence cruciale, que ce soit pour le stockage ou la transmission et l'échange d'informations. Dans ce contexte, la cryptographie émerge comme l'une des méthodes les plus efficaces pour garantir la confidentialité et l'intégrité de ce type d'informations.

Divers algorithmes sont actuellement disponibles, proposant des alternatives et des méthodes de cryptage vidéo variées. La cryptographie symétrique, par exemple, utilise une seule clé pour le chiffrement et le déchiffrement des fichiers vidéo. D'autre part, les algorithmes asymétriques font appel à deux méthodes distinctes, l'une pour le chiffrement et l'autre pour le déchiffrement, formant ainsi une paire de clés fonctionnant de concert dans le processus de cryptage et de décryptage. L'objectif de ce mémoire est d'explorer et de comparer deux approches majeures de chiffrement, à savoir le chiffrement RSA (asymétrique) et le chiffrement 3-way (symétrique). Le second objectif de cette étude consiste à appliquer ces deux types de chiffrement sur des fichiers vidéo, puis à comparer les résultats obtenus en termes de sécurité, de vitesse de chiffrement et de qualité,

Notre mémoire est organisé en quatre chapitres distincts. Le premier chapitre fournit une introduction générale sur la cryptographie. Le deuxième chapitre se concentre sur les concepts fondamentaux des données visuelles comme des vidéos numériques. Le troisième chapitre traitera le fonctionnement de l’algorithme RSA et 3-WAY. Enfin, le dernier chapitre, nous présentons l’implémentation de notre application avec les différents résultats obtenues sur la qualité et la vitesse de l’opération de chiffrement avec les deux algorithmes RSA et 3-WAY.

Chapitre1
Généralité sur la cryptographie

Chapitre1 Généralité sur la cryptographie

1.1. Introduction

La cryptographie représente une discipline d'une grande ancienneté, comme en témoignent des recherches mettant en lumière l'utilisation par un scribe égyptien de hiéroglyphes non conformes à la langue pour rédiger un message. Au fil du temps et à travers l'histoire, la cryptographie a principalement servi des desseins militaires. De nos jours, les réseaux informatiques requièrent invariablement une composante de cryptographie en tant que mécanisme essentiel pour garantir la confidentialité des informations numériques. Ce chapitre expose les principes fondamentaux de la cryptographie.

1.2. Terminologie

- **C*ryptographie :*** étude des différents moyens pour transformer une donnés dans un format « Sécurisé ».
- ***Cryptanalyse :*** L'art de « casser » les algorithmes de chiffrement.
- **Cryptologie :** c'est un domaine qui permet de regroupe la cryptographie et cryptanalyse.
- ***Encodage :*** Transformer une donnés pour mieux la transporter***.***
- ***Clé de chiffrement :*** Elément qui permet de passer de l'état chiffré à non chiffré, il existe plusieurs types des clés : ``privé, sécrète, publique….. ``
- ***Texte clair :*** il s'agit un contenue « donnes » à sécuriser.
- ***Texte chiffré :*** cela correspond à l'issue du processus de chiffrement appliqué au texte en clair.
- ***Chiffrement :*** c'est la technique ou l'algorithme employé pour convertir un texte en clair en un texte chiffré.
- ***Déchiffrement* :** c'est la méthode ou l'algorithme utilisé pour convertir un texte chiffré en texte en clair.

- ***Décrypter :*** cela implique retrouver le texte en clair associé à un texte chiffré sans disposer de la clé utilisée pour le chiffrement. Ce terme devrait être réservé au contexte de la cryptanalyse.
- ***Crypter :*** à la lumière de la définition de "décrypter", on constate que le terme "crypter" n'a pas de signification particulière, et son utilisation devrait être évitée. De même, le mot "cryptage" n'a pas de même.
- ***Coder, décoder :*** il s'agit d'une méthode ou d'un algorithme visant à altérer la mise en forme d'un message sans introduire d'élément secret.**[1]**

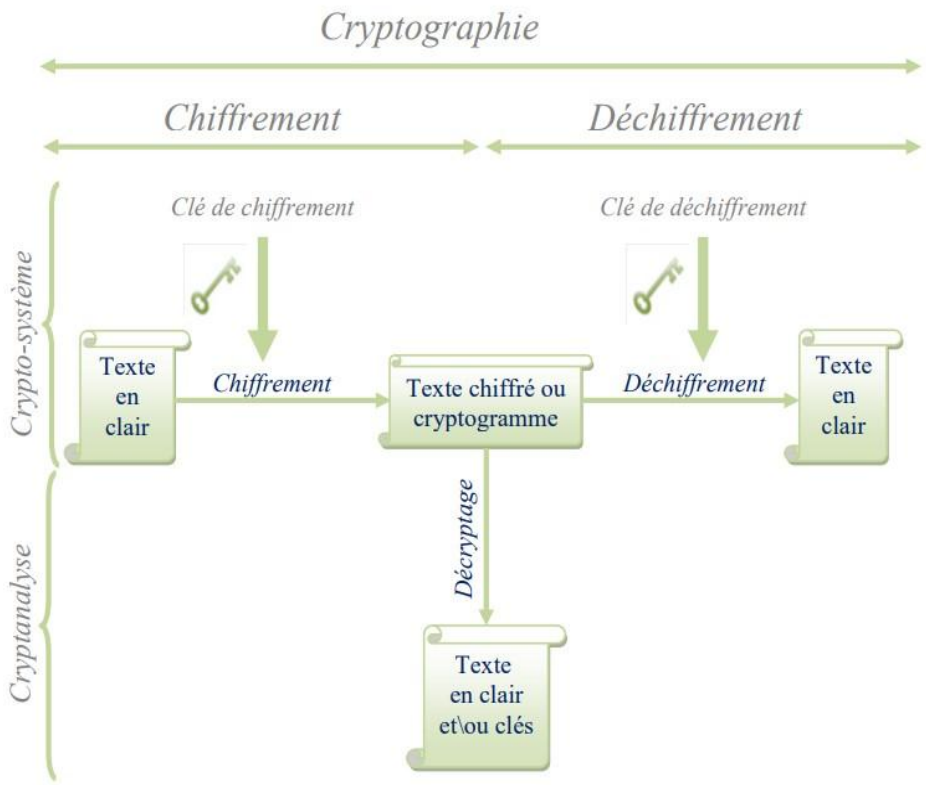


Figure I.1 Représente Organigramme du crypto-système proposé

1.3. L’historique de la cryptographie

L'évolution de la cryptographie est intrinsèquement liée à celle de l'écriture. Les premières De son utilisation remontent à 2000 ans avant Jésus-Christ en Égypte. Pendant des siècles, La cryptographie s'est basée sur deux principes fondamentaux :

- La permutation : consistant à modifier l'ordre des lettres dans le texte clair.
- La substitution : impliquant le remplacement d'une lettre par une autre dans un alphabet, que ce soit de manière mono-alphabétique ou poly-alphabétique.
- L'alphabet de César demeure l'exemple le plus célèbre de ce type de chiffrement, avec un décalage de 3 positions des lettres de l'alphabet. Ce n'est qu'en 1949 que Claude Shannon, dans le cadre de la théorie de l'information, formalise deux concepts cruciaux pour la construction de crypto-systèmes : la diffusion (chaque bit du texte clair doit influencer le plus grand nombre possible de bits du chiffré) et la confusion (la structure liant le chiffré et le clair doit être très complexe).

L'avènement des ordinateurs et des réseaux de télécommunications au cours des dernières décennies a libéré la cryptographie de ses applications strictement diplomatiques et militaires. La mondialisation de l'information a nécessité la création de systèmes cryptographiques communs réputés pour leur sécurité, car la puissance de calcul des ordinateurs personnels permet désormais à chacun de s'essayer à la cryptanalyse.

Dans ce contexte, en 1975, est apparu l'un des premiers grands algorithmes de cryptographie à clé secrète : le DES (Data Encryption Standard), fortement influencé par la théorie de l'information et choisi comme standard de chiffrement par le gouvernement américain en 1977. Depuis lors, la recherche en cryptographie n'a cessé de progresser, tant du côté de la clé publique que de la clé secrète. Notons notamment le choix, en octobre 2000, du nouveau standard de chiffrement américain pour le XXIe siècle : l'AES (Advanced Encryption Standard), en remplacement du DES**.[2]**.

L'avènement des ordinateurs et de l'Internet a propulsé la cryptologie dans une ère moderne. La grande avancée de ces dernières décennies a été la cryptographie à clés

publiques. L'avenir pourrait bien être celui de la cryptographie quantique, offrant une sécurité indéfectible.

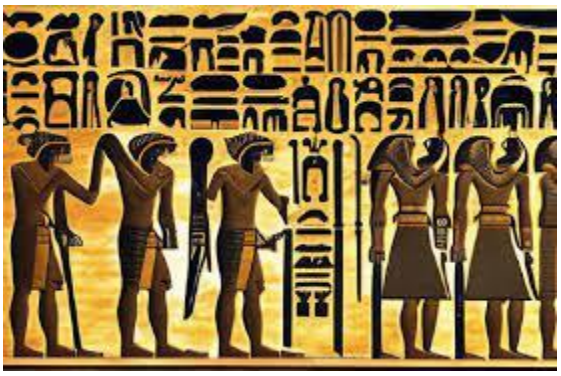


Figure I.2 Représente L'historique de la Cryptographie

1.4. Objectifs de la cryptographie

La cryptographie vise à résoudre quatre problèmes distincts :

- ***Confidentialité :*** Le texte chiffré doit demeurer lisible uniquement pour les destinataires autorisés, inaccessible à tout intrus.

  Deux mesures complémentaires doivent être mises en œuvre :

  - Restreindre et contrôler l'accès aux données.
  - Appliquer des méthodes de cryptage pour rendre les données compréhensibles. **[3]**

1-Avec le chiffrement par clé privée, une seule clé est utilisée pour le chiffrement et le déchiffrement. La condition préalable est l'échange sécurisé des clés entre les parties A et B.

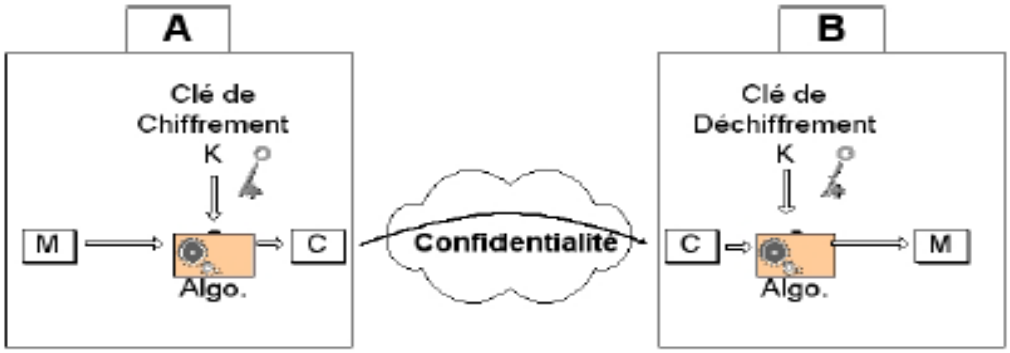


Figure I.3 Représente Confidentialité d'un système à clé privée

2- Dans un système de cryptographie à clé publique, chaque entité possède sa propre paire de clés.

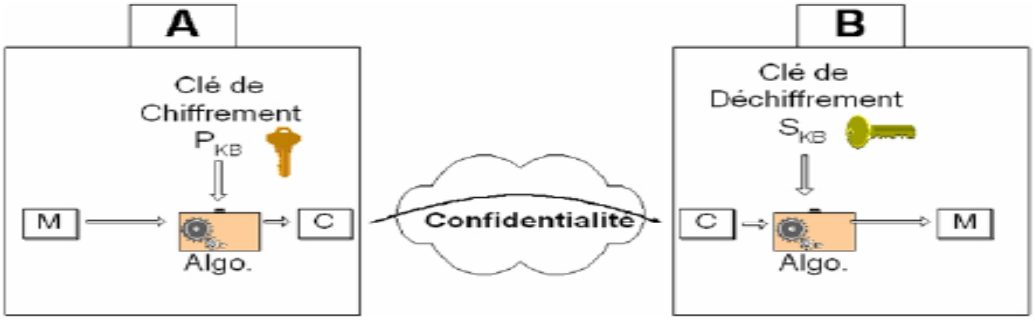


Figure I.4 Représente Confidentialité d'un système à clé publique

3- Dans le cas du cryptage hybride, le message est crypté à l'aide d'une clé privée, tandis que la sécurité de la clé est assurée par un système à clé publique.

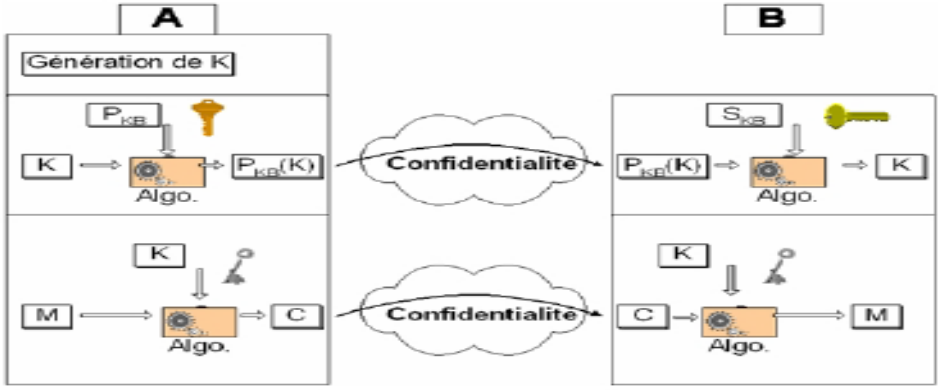


Figure I.5 Représente Confidentialité d'un système hybride

- ***Authentification*** : Le destinataire d'un message doit être en mesure de vérifier son origine, évitant ainsi toute usurpation par un tiers.

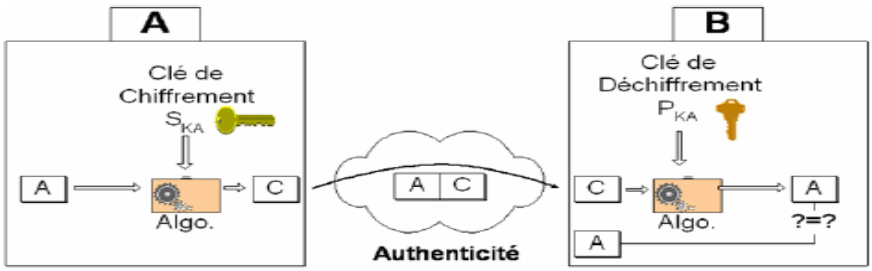


Figure I.6 Représente Authentification dans un système à clé publique

- ***Intégrité :*** Le destinataire d'un message doit pouvoir s'assurer qu'aucune altération n'a eu lieu pendant la transmission, empêchant tout intrus de substituer un faux message à l'original.

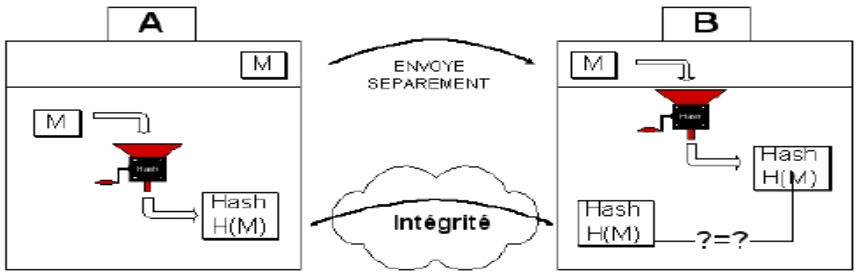


Figure I.7 Représente Vérification de l'intégrité par fonction dehachage

- ***Non répudiation :*** Un expéditeur ne doit pas avoir la possibilité de nier de manière injustifiée l'envoi d'un message par la suite.

Figure I.8 Représente La triade CIA

1.5. Définition de la Cryptologie

La cryptologie, qui englobe l'étude des systèmes cryptographiques (la science des codes secrets), peut être divisée en deux branches distinctes :

Cryptographie : ce domaine se concentre sur la préservation du secret.

Cryptanalyse : cette branche se consacre à la récupération du message d'origine sans une connaissance précise de l'ensemble du processus.

1.6. Définition de la cryptographie

Le mot cryptographie vient des mots en grec ancien kruptos signifiant « caché » et graphein signifiant « écrire », Le terme "cryptographie" englobe un ensemble de techniques visant à chiffrer des messages, La cryptographie des données consiste à brouiller le contenu des données, telles que le texte, l'image, l'audio, la vidéo, etc. pour rendre les données illisibles, invisibles ou inintelligibles lors de la transmission ou du stockage, appelé aussi chiffrement. L'objectif principal de la cryptographie est de protéger les données des attaquants non autorisés ou les individus. **[4]**

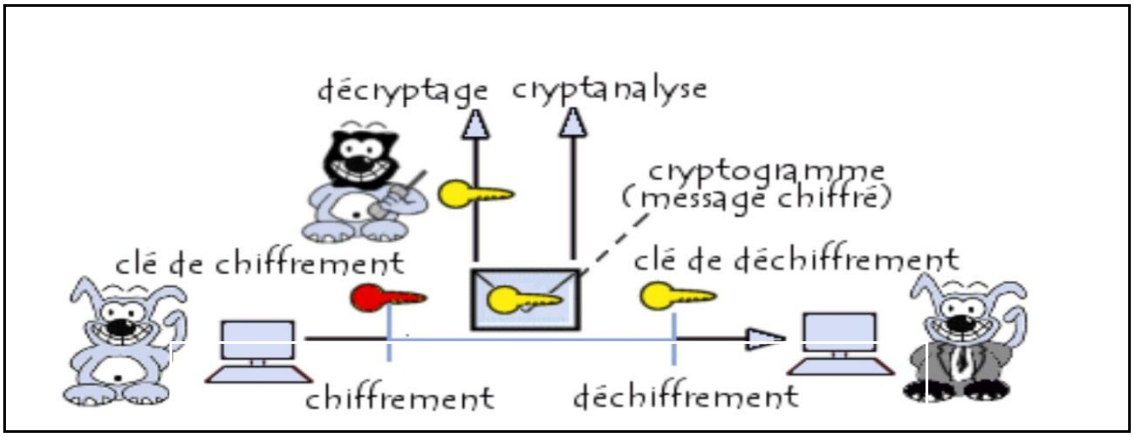


Figure I.9 Représente Le fonctionnement de la cryptographie

1.7. Types de cryptage

Les techniques de cryptages répartissent en deux catégories principales : Le chiffrement symétrique et le chiffrement asymétrique utilisant des clés. Avant d'explorer ces méthodes, il est nécessaire de clarifier le concept de clé, un concept qui sera fréquemment utilisé tout au long de ce chapitre.**[9]**

➢ 1.7.1. Cryptage par clé

Paramètre consistant en une séquence de symboles utilisés par un algorithme cryptographique pour modifier, confirmer, authentifier, crypter ou décrypter des données. En général, il existe deux catégories de clés :

- **1.7.1.1. Les clés symétriques**

Ce sont les clés utilisées à la fois pour le cryptage et le décryptage. Cette approche est communément appelée cryptage symétrique ou cryptage à clé secrète.

- **1.7.1.2. Les clés asymétriques**

Il s'agit des clés spécifiquement utilisées dans le cadre du chiffrement asymétrique, également Connu sous le nom de cryptographie à clé publique. Dans cette configuration, une clé distincte est utilisée pour les opérations de chiffrement et de déchiffrement.

Il existe également deux catégories de cryptage, en fonction du format des données :

➢ **1.7.2. Cryptage par bloc**

✓ Les données à crypter sont divisées en morceaux d'une taille fixe.

✓ Chaque bloc est crypté séparément.

✓ Ce processus de cryptage est relativement lent et nécessite beaucoup de mémoire et de puissance de calcul.

➢ **1.7.3. Cryptage à la volée**

✓ Les données à crypter sont un flux continu de bits ou de caractères.

✓ Ce processus est plus rapide, nécessite moins de ressources et est souvent réalisé à l'aide de matériel spécialisé.

✓ Il est souvent utilisé dans les flux audios et vidéo.

- **1.7.1.1 Cryptographie Symétrique**

Utilise la même clé pour le chiffrement et le déchiffrement.

Rapide et efficace pour le traitement de grandes quantités de données.

Figure I.10 Représente La Cryptographie Symétrique

Exemples d'algorithmes : AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES,3-WAY.

- **Le Data Encryption Standard (DES)**

  Est un exemple important de cryptographie par blocs. Il est largement utilisé pour crypter les codes PIN, les transactions bancaires, etc. Travaillant sur des blocs de 64 bits à la fois, DES utilise une clé d'entrée de 64 bits, dont le huitième bit sert de clé de contrôle de parité. En conséquence, la taille effective de la clé est réduite à 56 bits.

- **Advance Encryption Standard (AES)**

  En 1997, le NIST a lancé un appel à propositions en vue de définir une nouvelle norme destinée à succéder au DES. Le processus de sélection s'est conclu en novembre 2001 avec le choix du crypto système Rijndael, rebaptisé Advanced Encryption Standard (AES). Ce dernier opère sur des blocs de 128 bits, disposés en matrices 4 × 4 avec des entrées de 8 bits. L'algorithme offre la possibilité d'utiliser des longueurs de bloc et de clé variables. La spécification finale autorise toute combinaison de longueurs de clé de 128, 192 ou 256 bits, ainsi que de blocs de longueur 128, 192 ou 256 bits.

1.7.1.2. Cryptographie Asymétrique (ou Cryptographie à Clé Publique)

Utilise une paire de clés : une clé publique et une clé privée.

La clé publique est partagée, tandis que la clé privée reste secrète.

Principalement utilisée pour l'échange sécurisé de clés et la signature numérique.

Figure I.11 Représente La cryptographie Asymétrique

Exemples d'algorithmes : RSA, DSA (Digital Signature Algorithm), ECC (Elliptic Curve Cryptography).

- **RSA**

Est le premier algorithme qui peut être utilisé pour chiffrer des données et créer des signatures numériques. La sécurité de l'algorithme RSA repose sur la complexité de l'analyse des grands nombres. Deux grands nombres premiers sont utilisés pour générer les clés publique et privée. La difficulté supposée de récupérer le texte en clair à partir de la clé et du texte chiffré est comparable à la difficulté d'analyser le produit de deux grands nombres premiers.**[7]**

- **La cryptographie à courbe elliptique (ECC)**

La cryptographie à courbe elliptique englobe l'ensemble des primitives cryptographiques asymétriques pertinentes, incluant les signatures numériques et les algorithmes d'échange de clés. L'opération fondamentale de l'algorithme ECC consiste en la multiplication scalaire k*P, où k est un entier et P représente un point sur une courbe elliptique. **[8]**

1.8. L'Exigence du cryptage vidéo

Le cryptage vidéo est essentiel pour les raisons suivantes :

- Pour ne pas permettre la visualisation non autorisée des vidéos transmises, notamment celles provenant des caméras de vidéosurveillance des forces de l'ordre et envoyées à un centre de visualisation central.
- Assurer la protection des messages multimédias privés échangés, que ce soit sur des réseaux sans fil ou câblés.
- L'utilisation du cryptage vidéo est utile pour garantir la sécurité des vidéos utilisées dans des services tels que l'apprentissage par vidéoconférence.

- Assurer la protection des vidéos médicales contenant des informations confidentielles sur les patients, afin d'empêcher tout accès non identifié par des utilisateurs malveillants.**[5]**
- Assurer la sécurité des vidéos générées par diverses applications IoT, telles que les systèmes de surveillance dans les maisons et les usines.

1.9. Classification des algorithmes de cryptage vidéo

Afin de caractériser les propriétés des algorithmes de cryptage vidéosde manière distincte, nous choisissons ici une classification basée sur leur relation avec les algorithmes de compression vidéo. Cela conduit à une distinction entre les algorithmes de cryptage et de compression, où le cryptage et la compression sont combinés, et les algorithmes de cryptage qui fonctionnent indépendamment de la compression.

➢ 1.9.1. Algorithmes de crypto-compression

Le concept fondamental des algorithmes de crypto-compression repose sur l'application du cryptage à une étape spécifique de l'algorithme de compression, ce qui permet d'obtenir un résultat nettement différent d'un flux vidéo utilisant un algorithme de compression conventionnel. Cette méthode de codage peut être associée à l'une des trois étapes de codage, ce qui donne lieu à trois catégories d'algorithmes :

- Codage post-conversion.
- Codage après quantification.
- Cryptage en quantification.

➢ 1.9.2. Algorithmes de cryptage autonomes vis-à-vis de la compression

Au sein de cette catégorie d'algorithmes de cryptage, la compression et le cryptage sont réalisés de manière distincte. Le processus de cryptage peut être mis en œuvre avant ou après la compression.

➢ 1.9.3. Algorithmes de cryptage antérieurs à la compression

Les algorithmes de compression sont conçus pour minimiser les redondances présentes dans le texte en clair. D'un autre côté, les algorithmes de chiffrement dissimulent ces redondances grâce à des opérations cryptographiques. En optant pour une disposition où les algorithmes de chiffrement sont appliqués avant la compression, la quantité de redondance à compresser est considérablement réduite. Il est donc rare que les algorithmes de cryptage indépendants de la compression soient mis en œuvre avant cette étape.

➢ 1.9.4. Algorithmes de cryptage post-compression

Les algorithmes de cryptage post-compression tiennent compte des caractéristiques propres au flux vidéo compressé, telles que la distribution uniforme des valeurs d'octets dans ce dernier. Ces algorithmes peuvent alléger la charge de calcul du cryptage en choisissant généralement une partie spécifique du flux vidéo pour le cryptage, ou en cryptant l'intégralité du flux vidéo à l'aide d'un algorithme léger dédié**.[6]**

1.10. Approches utilisées pour le cryptage

➢ 1.10.1. Cryptage intégral

Les algorithmes de cryptage vidéo qui appliquent le cryptage à l'ensemble du flux binaire vidéo entrent dans cette catégorie. Cette catégorie d'algorithmes nécessite une puissance de calcul importante, ce qui se traduit par une vitesse d'exécution plus lente**.**

➢ 1.10.2. Chiffrement sélectif

Également connu sous le nom de cryptage partiel, il s'agit d'une sous-section du cryptage variable. Les algorithmes de cette catégorie effectuent un cryptage visé des octets dans les images vidéo. Comme ces algorithmes ne cryptent pas tout octet de données vidéo, la complexité du processus de cryptage s'en trouve réduite**.[5]**

1.11. La cryptanalyse

La cryptanalyse, un des principaux domaines d'activité, consiste à décrypter un message crypté sans connaître la clé de décryptage. Selon la quantité d'informations accessibles et le degré de contrôle que le cryptanalyste exerce sur le système, une pluralité d'attaques de cryptanalyse peut être utilisée. Il s'agit notamment d'une attaque par texte chiffré uniquement, d'une attaque par force brute qui repose sur une recherche exhaustive des clés, d'une attaque par texte en clair connu où le cryptanalyste a une certaine connaissance du texte en clair, d'une attaque par texte en clair choisi où le cryptanalyste peut influencer la boîte noire du système, et d'une attaque par texte chiffré choisi où le cryptanalyste alimente la boîte noire avec des textes chiffrés spécifiques pour obtenir la clé secrète ou une partie de cette clé. Ces stratégies mettent en évidence les différentes méthodes utilisées pour violer la sécurité des systèmes cryptographiques et soulignent l'importance de concevoir des systèmes résistants à ces attaques.

1.12. Conclusion

Dans ce chapitre, nous avons abordé l'histoire et la généralité de la cryptographie. Nous avonsprésentéla terminologie et l'objectif de la cryptographie, ainsi que la classification des systèmes de cryptographie. Nous avons également examiné des exemples de d’algorithmes de cryptage symétrique et asymétrique. Soulignant son rôle crucial dans la préservation de la confidentialité, de l'intégrité et de l'authenticité des données, renforçant ainsi la sécurité des systèmes informatiques moderne.

Chapitre 2
Concepts de base / Chiffrement de vidéo numérique

Chapitre 2 Concepts de base / Chiffrement de vidéo numérique

2.1. Introduction

Ce chapitre se penche sur les concepts fondamentaux du chiffrement de la vidéo numérique. Nous abordons les bases de la vidéo, les espaces couleur, la compression vidéo, et les redondances. Ensuite, nous explorons les différentes méthodes de compression et les normes telles que MPEG et H.261.En parallèle, nous introduisons le chiffrement vidéo, en examinant les types tels que le chiffrement total et sélectif. Nous discutons également de la relation entre le chiffrement et la compression vidéo, avec un aperçu des systèmes de crypto-compression.

2.2. Notions sur la vidéo

Une vidéo est constituée d'une séquence d'images fixes, chacune possédant trois caractéristiques distinctes

- Le nombre de bits alloué pour l'espace couleur (8 bits pour les images en noir et blanc et 24 bits pour les images en couleurs).
- Les dimensions exprimées par le nombre de colonnes et de lignes ou le nombre de pixels présents dans chaque image.
- La cadence d'images par seconde.

2.3. Les principes fondamentaux physiques et techniques

➢ 2.3.1. La vision

Humaine repose sur la réception d'un flux lumineux, composé de photons, par l'œil. Au sein de cet organe, les bâtonnets réagissent à l'intensité lumineuse (luminance ou Y), tandis que les cônes sont sensibles à la couleur (chrominance ou C). Le cœur combine ensuite ces informations pour former une représentation visuelle. Il est à noter que l'œil humain est plus sensible à l'intensité lumineuse (Y) qu'à la couleur (C).

➢ 2.3.2. La couleur

La vidéo utilise la méthode de synthèse additive pour produire des couleurs. Dans ce système, les trois couleurs primaires sont le rouge, le vert et le bleu (acronyme RVB). En mélangeant ces trois couleurs, il est possible de recréer toute la gamme des couleurs perceptibles par l'œil humain. Ainsi, l'écran vidéo est constitué d'une série de combinaisons de ces trois couleurs primaires. Lorsque ces combinaisons sont activées simultanément, elles génèrent l'image affichée.

- **2.3.2.1 Les espaces couleurs**

Les espaces colorimétriques sont des représentations des couleurs d'une image. Parmi ces espaces, on retrouve :

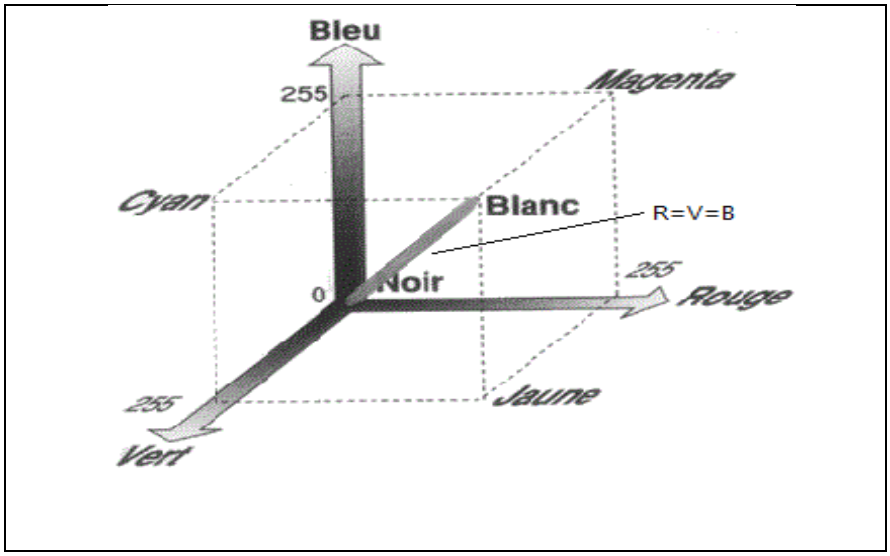


Figure II.1 Représentation des couleurs RVB

- **2.3.2.1.1. L'espace RGB (ou RVB)**

Dans l'espace colorimétrique RVB, chaque pixel est défini par trois valeurs représentant les proportions relatives de rouge (R), vert (V) et bleu (B). Ces trois couleurs primaires additives de la lumière permettent de coder chaque composante sur 8 bits, offrant ainsi la possibilité de créer plus de 16 millions de couleurs distinctes.

Figure II.2 Représente Espace colorimétrique RVB

- **2.3.2.1.2. L'espace YCrCb**

L'espace colorimétrique YCrCb représente les couleurs d'une image de manière plus efficace en séparant la luminance de la chrominance. La luminance (Y) est obtenue par une moyenne pondérée des composantes R, V et B, comme indiqué par l'équation :

$$Y = Kr\,R + Kb\,B + Kg\,G$$

Où Kr et Kb et Kg sont des facteurs de pondération. Dans cet espace, seules la luminance (Y) et les composantes de chrominance rouge et bleue (Cr, Cb) sont transmises. Il est possible de déduire la troisième composante de chrominance à partir des deux autres, simplifiant ainsi la transmission d'informations.**[10]**

- **2.3.2.1.3. L'espace YUV**

L'espace colorimétrique YUV est un modèle de couleur qui divise une image en trois composantes principales : Y (luminance), U (chrominance bleue) et V (chrominance rouge). La composante Y représente l'intensité lumineuse, tandis que les composantes U et V représentent la couleur. Cette séparation permet une compression plus efficace des données, notamment dans le domaine de la vidéo, tout en préservant la qualité visuelle. L'utilisation de l'espace YUV est courante dans diverses applications, offrant des avantages tels que la réduction de la bande passante nécessaire pour transmettre des vidéos.

➢ 2.3.3. Le signal

En vidéo, la caméra convertit la lumière en signaux électriques. Dans la vidéo analogique, ces signaux varient continuellement. Le processus est le suivant :

L'objectif de la caméra divise la lumière en trois composantes : rouge, verte et bleue, à l'aide de filtres dichroïques qui reflètent certaines couleurs et en laissent passer d'autres.

Dans les appareils photo professionnels, ces trois images sont projetées sur trois capteurs photo sensibles distincts, chacun contenant des centaines de milliers de points, généralement entre 400 000 et 700 000. Ces capteurs, appelés CCD (dispositifs à couplage de charge), capturent les images. Les appareils photo grand public sont souvent équipés d'un seul capteur CCD.

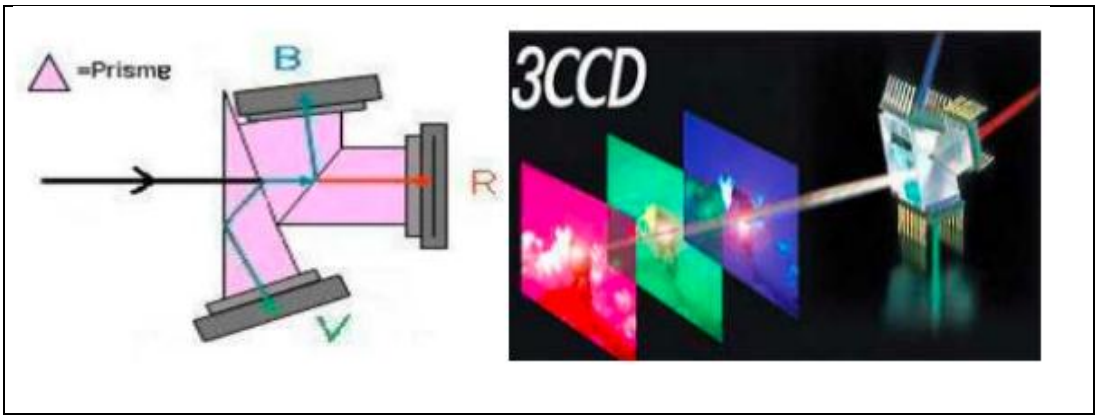


Figure II.3 Représente Schéma de principe d'un Capture Tri-CCD (charged coupled device)

2.4. Les caractéristiques d'un fichier vidéo

Définissent sa composition Ces attributs sont les suivants

- **La résolution** : la taille des pixels de l'image.
- **Le rapport hauteur/largeur** : la proportion entre la largeur et la hauteur de l'image.
- **Fréquence d'images** : la vitesse à laquelle les images sont capturées et reproduites.
- **Le débit binaire** : la quantité de données utilisée pour représenter l'audio ou la vidéo par seconde, mesurée en kilo-octets, méga-octets ou giga-octets par seconde. Un débit binaire plus élevé indique généralement une meilleure qualité.

- **Taux d'échantillonnage audio** : fréquence à laquelle le signal audio est mesuré lors de la conversion de l'analogique au numérique.

2.5. Définition de la compression

La compression désigne le processus d'élimination des redondances présentes dans les signaux tels que l'audio, les images ou les vidéos, dans le but de réduire la taille de stockage, la bande passante nécessaire à la transmission, et par conséquent, le temps de transmission. Pour la vidéo, les redondances statistiques et psycho visuelles sont distinguées. La compression se divise en deux catégories principales : la compression sans perte, permettant la récupération totale des données originales après décompression, et la compression avec perte, visant à atteindre des taux de compression élevés au détriment d'une perte d'information, notamment utilisée dans les domaines de la vidéo et de l'audio.

2.6. Les redondances statistiques

Les redondances statistiques se divisent en deux catégories : la redondance inter pixels et la redondance de codage. La redondance inter pixels concerne la corrélation entre les pixels d'une image individuelle et entre les images successives d'une séquence. On distingue la redondance spatiale, liée à la disposition des pixels dans une image, et la redondance temporelle, liée aux relations entre les images successives. La redondance de codage est la prévisibilité des données résultant des techniques de codage, pouvant être réduite grâce à des méthodes de compression efficaces.

➢ 2.6.1. La redondance spatiale

La redondance spatiale fait référence à la corrélation statistique entre les pixels à l'intérieur d'une trame d'image, également connue sous le nom de redondance intra-trame.

2.6.2. La redondance temporelle

La redondance temporelle se réfère à la corrélation statistique entre les pixels de trames successives dans une séquence vidéo, également désignée sous le nom de redondance inter trame.

2.6.3. La redondance de codage

La redondance de codage se distingue de la redondance de l'information, se concentrant plutôt sur la manière dont l'information est représentée. Éviter la redondance de codage revient à développer des techniques de codage plus efficaces pour compresser les données d'images et de vidéos. Parmi les méthodes utilisées, on trouve notamment deux techniques de codage à longueur variable : le Codage de Huffman et le codage arithmétique.

2.7. Compression sans pertes

La compression sans pertes vise à diminuer la taille d'une vidéo tout en permettant la reconstruction exacte de la vidéo d'origine. Pour atteindre cet objectif, différents types de codage sont employés, tels que le codage arithmétique, le codage de Huffman, ainsi que les codages reposant sur des dictionnaires. Ces méthodes de compression préservent l'intégralité des données, assurant ainsi la fidélité de la vidéo reconstituée par rapport à l'originale. **[12]**

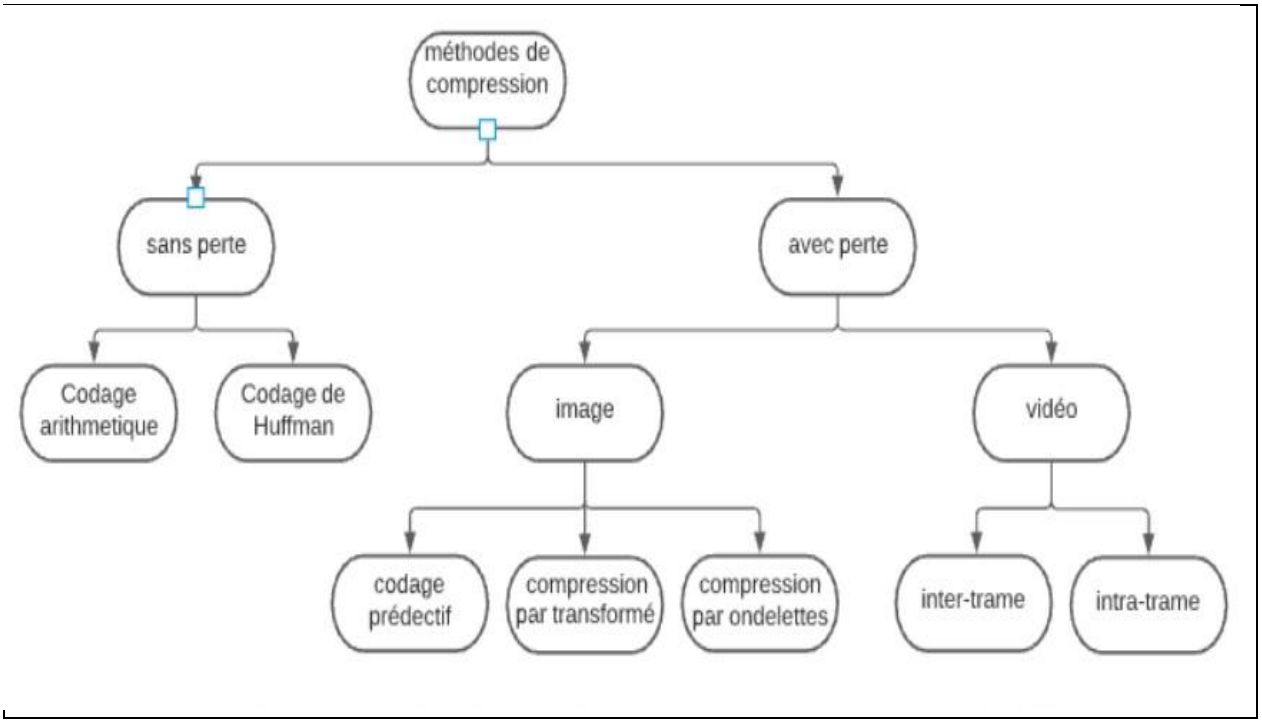


Figure II.4 Représente Classification des approches de compression pour image d'une vidéo **[21]**

➢ 2.7.1. Codage de Huffman

Le processus de codage de Huffman vise à réaliser une compression sans perte en subdivisant les données d'entrée en une séquence de symboles, simplifiant ainsi le processus de modélisation. Dans la plupart des applications de compression d'images et de vidéos, la taille de l'alphabet formé par ces symboles est généralement limitée à un maximum de 64 000 symboles. La construction du code de Huffman implique les étapes suivantes :

- **Tri des symboles par probabilités**

  Les symboles sont ordonnés en fonction de leurs probabilités d'occurrence. Pour construire le code de Huffman, il est essentiel de connaître a priori la fréquence d'occurrence de chaque symbole. En pratique, cette fréquence peut être estimée à partir d'un ensemble de données d'apprentissage représentatif des données à compresser sans perte.

- **Application d'un processus de contraction**

Les deux symboles avec les probabilités les plus faibles sont soumis à un processus de contraction. Supposons que ces symboles soient SN-1 et SN. Ils sont remplacés par un symbole hypothétique, HN-1, avec une probabilité d'occurrence égale à (PN-1) + PN. Ainsi, le nouvel ensemble contient N-1 symboles : S1, S2, ..., SN-2, HN-1.

- **Répétition du processus de contraction**

  Cette étape est répétée jusqu'à ce que le dernier ensemble n'ait qu'un seul membre. La procédure récursive du processus de contraction peut être assimilée à la construction d'un arbre binaire. À chaque étape, deux symboles sont fusionnés, formant ainsi une structure arborescente. À la fin du processus, tous les symboles deviennent des feuilles de cet arbre, et le mot de code attribué à chaque symbole est déterminé en parcourant l'arbre binaire de la racine au nœud correspondant au symbole.

➢ 2.7.2. Codage arithmétique

Le codage arithmétique représente une méthode de compression sans perte qui considère plusieurs symboles comme une unité de données unique, tout en préservant l'approche incrémentielle du codage symbole par symbole, comme dans le codage de Huffman. Contrairement au codage de Huffman, le codage arithmétique sépare le processus de codage de la modélisation, permettant ainsi une adaptation dynamique du modèle probabiliste sans influencer la conception du code.

Dans la théorie du codage arithmétique, chaque ensemble possible de donner se voit attribuer un unique mot de code. Chaque mot de code peut être envisagé comme un sous-intervalle semi-ouvert dans l'intervalle [0,1). En allouant une précision suffisante en termes de bits à chaque mot de code, il devient possible de distinguer un sous-intervalle de tout autre, facilitant ainsi le décodage précis de l'ensemble de données correspondant. Tout comme dans le cas des mots de code de Huffman, les ensembles de données les plus probables correspondent à des sous-intervalles plus vastes, nécessitant donc moins de bits de précision. **[13]**

2.8. Compression avec pertes

La compression avec pertes, comme JPEG, JPEG2000 et H.264, réduit la taille des fichiers en éliminant de manière permanente certaines informations redondantes. Cependant, cette méthode est irréversible et peut entraîner une légère altération de la qualité par rapport à l'original.

➢ 2.8.1. Le codage par transformation

Le codage par transformation est employé principalement pour éliminer les redondances spatiales dans les images en projetant les pixels dans un domaine de transformation avant la compression des données. Cette méthode tire avantage du fait que l'énergie d'image dans la plupart des scènes naturelles se concentre principalement dans la région des basses fréquences, représentée par quelques coefficients de transformation. Ces coefficients peuvent être quantifiés pour éliminer ceux qui ne sont pas significatifs, sans compromettre de manière significative la qualité de l'image reconstruite. Il convient de noter que ce processus de quantification est une opération avec perte, car les valeurs originales ne peuvent pas être préservées.

➢ 2.8.2. Transformée en cosinus discrète (DCT : Discrete Cosine Transform)

La base de toutes les normes de compression d'images et de vidéos repose sur le codage d'image par la Transformée en cosinus discrète (DCT). Dans ce système, le calcul fondamental consiste à transformer un bloc d'image N x N du domaine spatial au domaine DCT. Pour les normes de compression d'image, la valeur courante de N est 8. Le choix d'une taille de bloc 8 x 8 présente plusieurs avantages. D'un point de vue de l'implémentation matérielle ou logicielle, une taille de bloc de 8 x 8 n'engendre pas d'exigences de mémoire excessives, et la complexité de calcul d'une DCT 8 x 8 reste gérable sur la plupart des plates-formes informatiques. Du point de vue de l'efficacité de la compression, une taille de bloc supérieure à 8 x 8 ne conduit généralement pas à une amélioration significative de la compression, car la corrélation spatiale diminue lorsque le voisinage de pixels dépasse huit pixels.

- **2.8.3. Transformée en ondelette discrète (DWT : Discrete Wavelet Transform)**

La Transformée en ondelette discrète (DWT) repose sur le concept d'ondelette, définie comme une "petite onde" dont l'énergie est concentrée dans le temps, offrant ainsi un outil pour analyser des phénomènes transitoires, non stationnaires ou variables dans le temps. Les ondelettes possèdent des propriétés ondulatoires oscillantes tout en permettant une analyse simultanée du temps et de la fréquence.

2.9. Motion JPEG

Motion JPEG (MJPEG) représente une séquence vidéo numérique sous la forme d'une série d'images JPEG. Les avantages de cette approche sont similaires à ceux des images fixes JPEG, offrant une flexibilité en termes de qualité et de taux de compression. Cependant, le principal inconvénient de Motion JPEG réside dans son absence d'utilisation de techniques de compression vidéo avancées, ne permettant pas l'élimination des redondances temporelles. En conséquence, le taux de compression pour les séquences vidéo est généralement légèrement inférieur par rapport aux méthodes de compression vidéo plus avancées.

2.10. MPEG-1

La norme MPEG-1, développée par le groupe MPEG en 1988, définit des normes de compression vidéo et audio, développées dans le cadre de la norme ISO/IEC-11172. L'objectif principal du groupe est de développer des normes internationales pour la compression, la décompression, le traitement et le codage des images animées et des données audios, Elle implique également des techniques d'encodage efficace des séquences vidéo. Observez la séquence vidéo illustrée dans la figure 2.5.

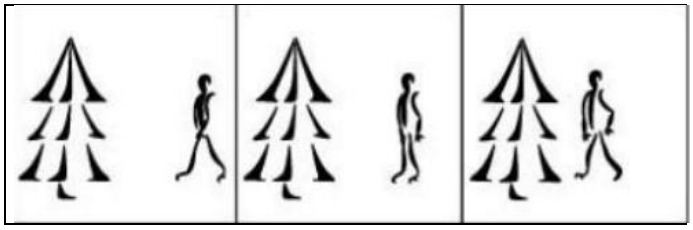


Figure II.5 Représente Une séquence vidéo JPEG de trois images

La séquence commence par l'image de gauche, suivie de l'image du centre et de l'image de droite. Pendant la lecture, la vidéo montre un homme se déplaçant de droite à gauche devant un arbre immobile. Dans Motion JPEG/Motion JPEG 2000, chaque image de la séquence est codée comme une entité distincte, ce qui garantit l'intégrité de la séquence originale. En revanche, dans le contexte de la vidéo MPEG, seules les parties nouvellement insérées de la séquence sont incluses, ainsi que des informations sur les éléments en mouvement. Pendant la transmission, afin d'optimiser l'utilisation de la bande passante, la séquence vidéo de la figure 2.1 se présente comme indiqué à la figure 2.2. Toutefois, il est important de noter que cette représentation ne s'applique que pendant la transmission et que, lors de la visualisation, la séquence retrouve son aspect initial.

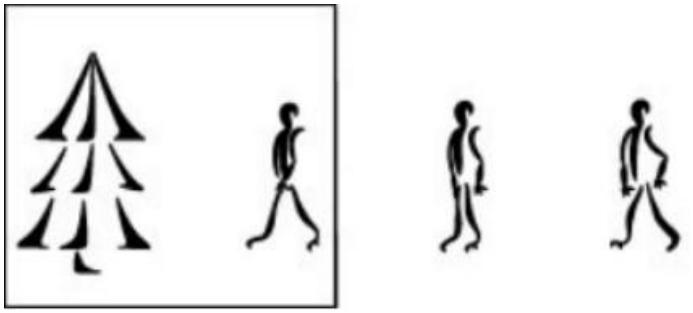


Figure II.6 Représente Une séquence vidéo MPEG de trois images

MPEG-1 se concentre sur des flux de bits d'environ 1,5 Mbps et a été développé à l'origine pour stocker de la vidéo numérique sur un disque compact. La vidéo numérique sur un disque compact. L'accent est mis sur le taux de compression plutôt que sur la qualité de l'image

2.11. MPEG-2

La norme MPEG-2 a été développée pour la diffusion télévisée et d'autres applications nécessitant des débits de données de 4 Mbps et plus. Cette norme offre une qualité d'image très élevée et prend en charge les formats vidéo entrelacés, avec des améliorations spécifiques pour la télévision haute définition (TVHD). Compatible avec MPEG-1, un décodeur MPEG-2 peut décoder les flux MPEG-1.

Sur le plan audio, MPEG-2 permet jusqu'à cinq canaux à bande passante complète (gauche, droite, centre et deux canaux arrière), ainsi qu'un canal d'amélioration des basses

fréquences, ou jusqu'à sept canaux pour des commentaires audio. La norme des systèmes MPEG-2 spécifie comment combiner différents flux audio, vidéo et de données privées en un seul flux multiplexé. Elle trouve des applications diverses dans les domaines de la diffusion, des télécommunications, de l'informatique et du stockage Bien que MPEG-2 offre des techniques avancées pour améliorer la qualité vidéo à un débit binaire donné, son principal inconvénient réside dans la complexité accrue des équipements nécessaires. Par conséquent, ces fonctionnalités ne sont pas idéales pour des applications nécessitant une surveillance en temps réel.

2.12. MPEG-4

Les fonctionnalités clés de MPEG-4, en ce qui concerne la compression vidéo, incluent le support pour des applications nécessitant encore moins de bande passante, telles que les unités mobiles, ainsi que des applications nécessitant une qualité extrêmement élevée avec une bande passante quasi illimitée, comme la production de films en studio. Contrairement à MPEG-2, les différences entre MPEG-4 et MPEG-2 sont principalement liées aux fonctionnalités non liées au codage vidéo, et donc moins pertinentes pour les applications de surveillance.
MPEG-4 utilise une approche asymétrique, où l'encodeur MPEG est complexe, exigeant une charge de calcul importante pour l'estimation de mouvement, tandis que le décodage est plus simple et peut être effectué par les processeurs de bureau actuels ou des puces de décodeur peu coûteuses. Le schéma de base de MPEG-4 consiste à prédire le mouvement d'une image à l'autre dans la direction temporelle, suivi de l'utilisation de la transformée en cosinus discrète (DCT) pour traiter la redondance dans les directions spatiales.

La prédiction de mouvement se fait dans le canal de luminance (Y) sur des blocs de 16x16, où l'encodeur recherche une correspondance étroite avec un bloc dans une trame précédente ou future. Les coefficients DCT résultants sont quantifiés, et la plupart des coefficients deviennent nuls. La quantification peut varier pour chaque bloc de 16x16 de Y et les blocs correspondants de 8x8 dans U et V. Les résultats, y compris les coefficients DCT, les vecteurs de mouvement et les paramètres de quantification, sont codés par Huffman à l'aide

de tableaux fixes. Les coefficients DCT utilisent un tableau de Huffman bidimensionnel où un code spécifie une longueur d'exécution de zéros et la valeur non nulle qui a terminé l'exécution. En outre, les vecteurs de mouvement et les composants DCT sont codés en DPCM.

2.13. H.261

H.261 est un algorithme de compression vidéo spécifiquement conçu pour les vidéoconférences, bien qu'il puisse être utilisé pour d'autres tâches de compression vidéo. Cette norme permet l'utilisation de multiples canaux de communication de 64 kbps chacun (P=1, 2, 3...30.), en accord avec la structure de données du RNIS. Le codage H.261 repose sur la Transformée en Cosinus Discrète (DCT), ce qui permet de coder intégralement certaines images (intra-trame) tout en codant les différences entre les autres images (inter-trame).
Les éléments clés du codeur source H.261 comprennent la prédiction, la transformation par blocs (passage du domaine spatial au domaine fréquentiel), la quantification et le codage entropique. Contrairement au codeur, le décodeur nécessite une prédiction, et la compensation de mouvement est considérée comme facultative. Une autre fonctionnalité dans la recommandation est le filtrage en boucle, appliqué aux données de prédiction pour réduire les erreurs significatives lors du codage inter-trame. Bien que le filtrage en boucle améliore considérablement la qualité vidéo, il requiert une puissance de traitement supplémentaire. Le fonctionnement du décodeur permet à différents Codecs conformes à la norme H.261 d'offrir des niveaux variables de qualité vidéo.

Standard	Applications	Bit rate
Motion-JPEG	Still image compression	Variable
MPEG-2000	Improved still image compression	Variable
MPEG-1	Video on digital storage media	1.5 mb/s
MPEG-4	Object based coding	Variable
H.261	Video conferencing Over ISDN	P × 64 kb/s
H.263	Video telephony over PSTN	33.6 kb/s
H.264	Improved video compression	10–100 kb/s

Tableau II.1 Représente Analyse comparative des normes de compression vidéo **[16]**

2.14. Normes de codage vidéo

Les normes de codage vidéo sont divisées en deux catégories principales, H.26x et MPEG-x, et ont émergé sous les auspices de deux entités distinctes : l'ITU-T pour les codecs H.26x, orientés vers les applications de télécommunication telles que la vidéoconférence et la téléphonie vidéo, et l'ISO/IEC pour les produits MPEG-x, conçus principalement pour répondre aux besoins de stockage vidéo (CD-ROM, DVD), de diffusion télévisuelle et de diffusion vidéo en continu (vidéo sur Internet).

Les recommandations de l'ITU-T ont été spécialement élaborées pour les applications de télécommunication, tandis que les normes MPEG ont été développées pour des applications plus larges, allant du stockage à la diffusion en continu. Bien que les deux comités de normalisation aient généralement travaillé de manière indépendante sur des normes distinctes, il y a des cas exceptionnels où leur collaboration a abouti à des normes communes, telles que H.262/MPEG-2 et H.264/MPEG-4 Partie 10 (v10).

La figure 2.8 récapitule l'évolution des normes de codage vidéo issues des deux organisations depuis le début en 1984 jusqu'à aujourd'hui. Elle illustre également l'évolution du codage d'images fixes résultant de la collaboration entre l'ITU-T et l'ISO/IEC.

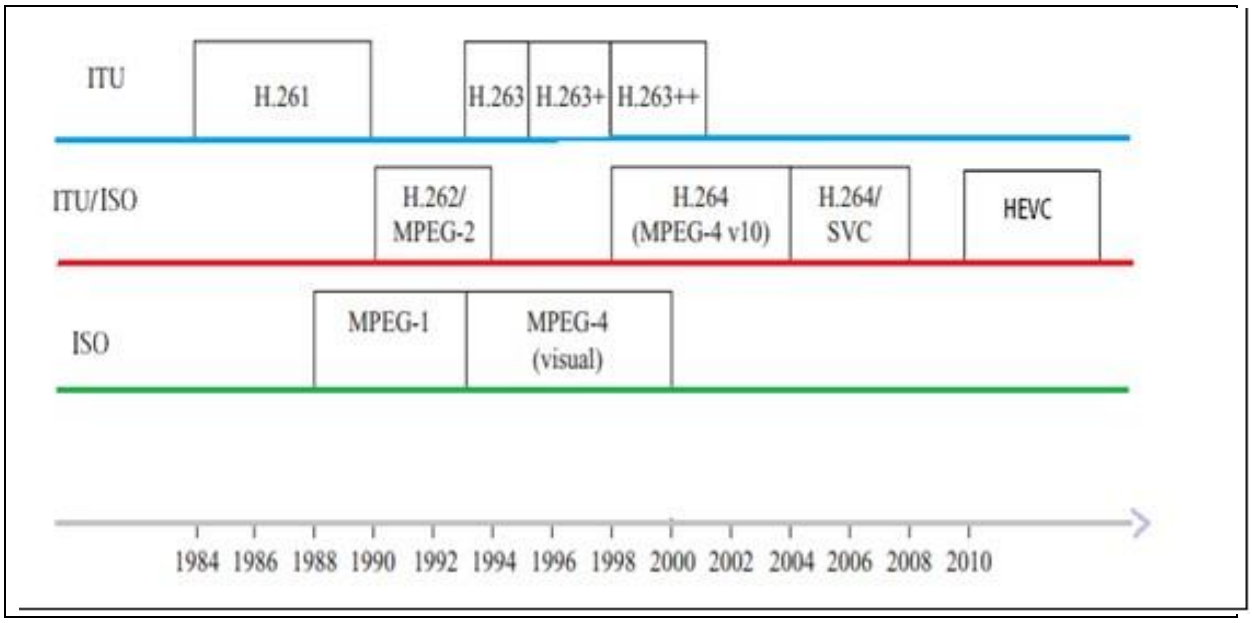


Figure II.7 Représente Evolution des normes de codage vidéo de l'ITU-T et de l'ISO / IEC comités

2.15. Chiffrement vidéo numérique

Comparativement à la communication textuelle, la communication vidéo présente plusieurs caractéristiques distinctes, notamment la gestion de volumes de données conséquents, des impératifs en temps réel, l'utilisation de codecs vidéo standardisés, des formats de compression de données normalisés, ainsi que des exigences de sécurité propres à cette application.

➢ 2.15.1. Classification du chiffrement vidéo

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

• 2.15.1.1. Chiffrement total (full encryption)

Le chiffrement total implique de chiffrer l'intégralité des données de l'information claire. Bien que rarement utilisé pour le chiffrement vidéo, il peut être appliqué en chiffrant chaque image individuellement dans une séquence vidéo en mode spatial/fréquentiel. Cependant, cette approche augmente considérablement le volume de la vidéo chiffrée. De même, si elle est utilisée pour chiffrer le flux binaire compressé, elle risque d'altérer le format. Pour cesraisons, le chiffrement total n'est généralement pas recommandé pour la protection des vidéos.

• 2.15.1.2. Chiffrement sélectif (sélective encryption)

Contrairement au chiffrement total, le chiffrement sélectif vise à chiffrer uniquement un sous-ensemble spécifique des données de l'image ou de la vidéo à crypter. Les données chiffrées sont sélectionnées en fonction de critères et de conditions variés. Souvent, ces critères de sélection sont des conditions assurant la confidentialité et la conformité au format de fichier compressé. Le chiffrement sélectif est fréquemment appliqué pendant

l'étape de compression pour obtenir un fichier conforme à la norme, avec une taille similaire ou identique au fichier non chiffré, tout en garantissant un niveau élevé de sécurité.

➢ 2.15.2. Chiffrement et compression vidéo

La figure 2.9 propose une classification des techniques de chiffrement de la vidéo, mettant en lumière la relation entre la compression et le chiffrement, qui se divise en deux catégories principales : les approches de chiffrement intégrées dans le processus de compression, également appelées systèmes de crypto-compression, et les approches de chiffrement indépendantes de toute étape décompression vidéo.

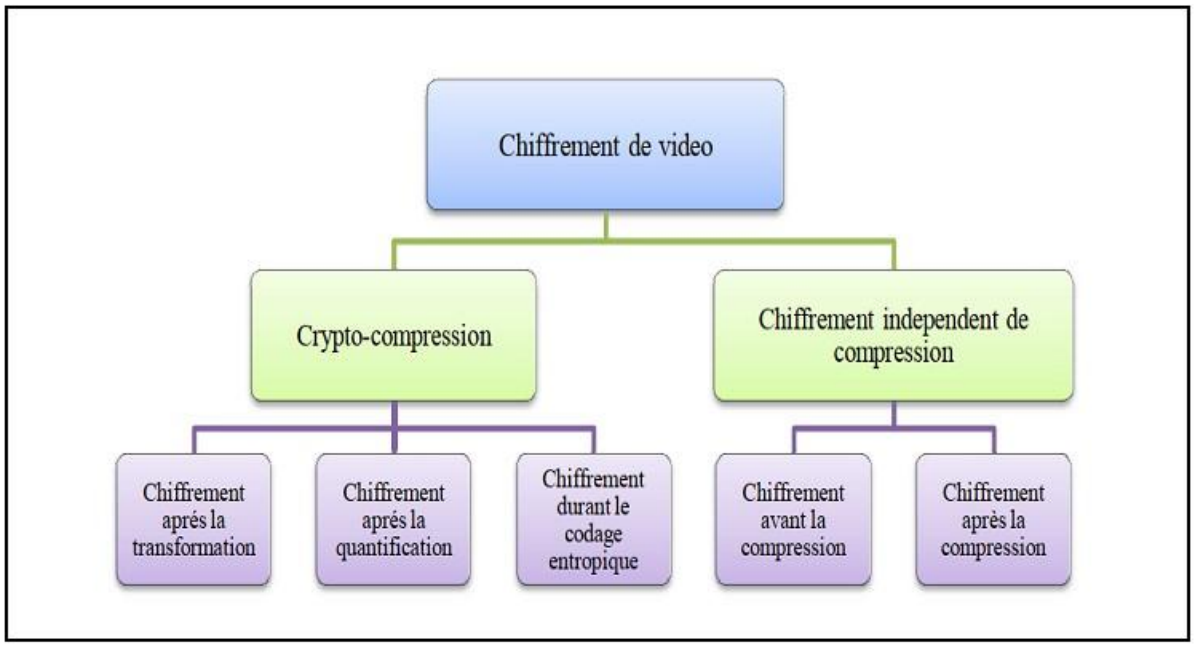


Figure II.8 Représente Taxonomie des techniques de chiffrement de vidéo numérique

- **2.15.2.1 Chiffrement indépendant de la compression**

Le chiffrement indépendant de la compression se divise en deux types

Chiffrement avant la compression

Les algorithmes de compression visent à réduire la redondance du texte brut d'entrée. Les algorithmes de chiffrement, utilisant des opérations cryptographiques, dissimulent la redondance inhérente du texte brut d'entrée. Par conséquent, si ces algorithmes de

chiffrement sont appliqués avant la compression, il reste beaucoup moins de redondance à comprimer. Cependant, cette approche est rarement utilisée de manière efficace avant la compression. Parmi les approches de chiffrement préalable à la compression, citons l'approche de Pazarci-Dipc et l'approche de chiffrement préservant la corrélation de la vidéo (CPEV - correlation-preserving encryption vidéo).

Chiffrement après la compression

Le chiffrement direct de la vidéo compressée peut compromettre le décodage de la vidéo cryptée, car le format du flux binaire ne serait plus conforme à la norme de codage établie. Des approches telles que SECMPEG et VEA ont réussi à chiffrer le flux binaire tout en préservant son format pour le décodage. Meyer et Gade Gast ont proposé un chiffrement sélectif pour la norme MPEG1 en 1995. Les parties sélectionnées pour la protection sont chiffrées à l'aide d'algorithmes de chiffrement classiques. Quatre niveaux de sécurité sont définis en fonction de la quantité de données à chiffrer

- ✓ Premier niveau : Chiffrement des entêtes de la couche de séquence et des entêtes des couches de tranches.
- ✓ Deuxième niveau : Chiffrement des coefficients de DCT de basse fréquence de chaque bloc dans chaque image intra.
- ✓ Troisième niveau : Chiffrement uniquement des blocs intra.
- ✓ Quatrième niveau : Chiffrement intégral du flux binaire de la vidéo compressée.

- **2.15.2.2. Les systèmes de crypto-compression pour la sécurité des vidéos**

Dans cette catégorie, l'opération de chiffrement est fusionnée avec une opération de compression et mises en œuvre de manière intégrée. Le chiffrement peut être appliqué à différents stades de la compression, que ce soit après la transformation fréquentielle, la quantification visuelle, ou même pendant le module de codage entropique.

Chiffrement après la transformation

Les données sujettes au chiffrement après la transformation fréquentielle de l'erreur résiduelle incluent les amplitudes et les signes des coefficients. Chaque norme de codage possède sa propre transformée appliquée, parmi lesquelles la transformée de DCT et ses améliorations sont les plus populaires.

- **Chiffrement après la quantification**

L'étape de quantification réduit l'espace des coefficients, suivant un mode de balayage tel que le mode en zigzag, qui commence par les coefficients de basses fréquences et termine par les coefficients de hautes fréquences, selon l'ordre défini par la norme de codage adoptée. Les données pouvant être chiffrées comprennent les amplitudes et les signes des coefficients quantifiés (QTCs) ainsi que l'ordre des QTCs.

- ***Chiffrement pendant le codage entropique***

Après la sortie et la standardisation de chaque norme de codage vidéo, la préservation de la taille du flux binaire crypté sans augmentation, tout en maintenant un format décodable conforme à la syntaxe de la norme, devient une préoccupation majeure. Cela représente un défi réel en termes de décidabilité des éléments syntaxiques après le chiffrement. Les approches de chiffrement pendant le codage entropique impliquent généralement la sélection et la protection sélective des éléments syntaxiques spécifiques, une pratique suivie par la plupart des méthodes présentes dans la littérature scientifique.

Les données à chiffrer varient selon le codage entropique adopté par la norme de codage vidéo. Par exemple, les normes MPEG utilisent des tables de Huffman avec des codes de type VLC, tandis que H.264 et ses extensions utilisent un codage adaptatif selon le contexte avec l'utilisation de CAVLC et CABAC.

2.16. Conclusion

La cryptographie demeure la solution privilégiée pour assurer la sécurité des médias multimédias. Idéalement, l'emploi de la cryptographie asymétrique est recommandé pour garantir la protection des vidéos. Dans la suite, nous explorerons plus en détail les algorithmes de chiffrement RSA et 3-WAY, ainsi que l'étude de la bibliothèque FFMPEG, afin de mieux comprendre leur rôle dans la sécurisation des données multimédias.

Chapitre 3

Les algorithmes de chiffrement RSA et 3-WAY/ Etude la bibliothèque FFMPEG.

Chapitre 3 *Les algorithmes de chiffrement RSA et 3-WAY/ Etude la bibliothèque FFMPEG.*

3.1. Introduction

La cryptographie tient une place prépondérante dans l'histoire de l'informatique, initialement réservée aux militaires et aux grandes entreprises. Aujourd'hui, elle est utilisée par toute personne, professionnelle ou privée, qui souhaite sécuriser la transmission de données. Bien qu'il existe de nombreuses méthodes de chiffrement, seules quelques-unes sont unanimement reconnues en termes de sécurité, parmi lesquelles l'algorithme RSA et 3-WAY jouit depuis longtemps d'une excellente réputation.

L'objectif de notre projet de fin d'étude est de développer une application de cryptage des vidéos basé sur une étude comparative entre les deux algorithmes RSA et 3-WAY selon la qualité et la vitesse de chiffrement.

3.2. Algorithme à clé publique RSA

➢ 3.2.1. Le principe :

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé actuellement, est le système RSA. Publié en 1977 par Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman de l'Instituions de technologie du Massachusetts, le RSA est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction "puissance".

➢ 3.2.2. L'algorithme de chiffrement

- ✓ Il est facile de fabriquer de grands nombres premiers p et q (+- 100 chiffres)
- ✓ Etant donné un nombre entier n = p.q., il est très difficile de retrouver les facteurs p et q

    - Création des clés

- ✓ La clé secrète : 2 grands nombres premiers p et q
- ✓ La clé publique : n = p*q ; un entier e premier avec (p-1)(q-1)

- Chiffrement

Le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :

$C = M^e \bmod n$

- Déchiffrement : il s'agit de calculer la fonction réciproque

$M=C^d \bmod n$

tel que $e.d = 1 \bmod [(p-1)(q-1)]$

Entrée : taille de la clé //exprimée en bits.
Sortie : la clé publique (N,E) et la clé privée (N,D)

1. Prendre deux nombres premiers **p** et **q** suffisamment grands (de taille à peu près égale).
2. Calculer **N = p*q,**
3. Calculer **α= (p-1) (q-1)**,
4. Choisir un nombre **E**tel que ***1 <E <α*** etle **PGDC *(e, α)=1***,
5. Prendre un nombre **E** qui n'a aucun facteur en commun avec **α**,
6. Calculer **D** tel que **D*E**modα=**1**.
7. **Return**N, E, D

III.2.2.2 Chiffrement :

Entrée : (N, E) et M // la clé publique et le texte en clair M avec M∈ [0.N-1].
Sortie : C // texte chiffré.

1. Calculer **$C=M^E \bmod N$**
2. **Return**C

III.2.2.3 Déchiffrement :

Entrée : (D, E) et C // la clé privée et le texte chiffré.
Sortie : M // texte clair.

1. Calculer**$M=C^D \bmod N$**
2. **Return**M

Figure III.1 Représente principe de chiffrement par RSA

3.2.3. Fonctionnement de RSA

Le fonctionnement du crypto système RSA est basé sur la difficulté de factoriser de grands entiers. Soit deux nombres premiers *p* et *q*, et *d,* un entier tel que *d* soit premier avec *(p-1) *(q-1)*). Le triplet *(p,q,d)* constitue ainsi la clé privée.La clé publique, représentée par le couple (n, e), est dérivée de la clé privée par les transformations suivantes :

$n = p * q$

$e = 1/d \bmod((p-1)(q-1))$

Pour garantir le succès du déchiffrement, le message M doit être premier avec la clé n. Cela se fonde sur le théorème d'Euler, stipulant que si M et n sont premiers entre eux, alors :

$M^{phi(n)} = 1 \bmod(n)$

Il est donc crucial que M ne soit pas un multiple de p, q, ou n. Une approche pour respecter cette condition consiste à fractionner le message M en segments Mi, de telle sorte que le nombre de chiffres dans chaque Mi soit strictement inférieur à ceux de p et q. Cette exigence suppose que p et q soient de grande taille, ce qui concorde avec la pratique courante, étant donné que la sécurité du RSA repose sur la complexité de la recherche de p et q, connaissant n, dans un délai raisonnable.

Phi(n) étant l'indicateur d'Euler, et valant dans le cas présent *(p-1) *(q-1).*

$n = p * q$

$e = 1/d \bmod((p-1)(q-1))$

Soit *M*, le message à envoyer. Il faut que le message *M* soit premier avec la clé.

En effet, le déchiffrement repose sur le théorème d'Euler stipulant que si *M* et *n* sont premiers entre eux, alors :

$M^{phi(n)} = 1 \bmod(n)$

Phi(n) étant l'indicateur d'Euler, et valant dans le cas présent *(p-1) *(q-1).*

Il est essentiel que M ne soit pas un multiple de p, q ou n. Une solution consiste à hacher le message M en Mi parties, en veillant à ce que le nombre de chiffres dans chaque Mi soit nettement inférieur à ceux de p et q. Cette condition suppose que p et q sont grands, ce qui est conforme à la pratique actuelle. En fait, la sécurité de RSA dépend de la complexité à trouver p et q, compte tenu de n, en un temps raisonnable, ce qui nécessite que p et q soient grands.**[23]**

EXEMPLE : CHIFFRER "SALUT"

1) processus A génère ses clés :

- Clé secrète : p = 61, q = 89 (Remarque : en pratique, p et q devraient être beaucoup plus grands, avec plus de 100 chiffres !)

- Clé publique : e = 5 (premier avec (60 * 88)), n = 61 * 89 = 5429

2) processus A diffusé sa clé publique (peut être publiée dans un annuaire, par exemple).

3) processus B, ayant obtenu le couple (n, e), sait qu'il doit l'utiliser pour chiffrer son message. Il convertit chaque lettre du mot "SALUT" en utilisant la position correspondante dans l'alphabet :

- S = 19, A = 1, L = 12, U = 21, T = 20

- SALUT = 19 1 12 21 20

4) Ensuite, processus B divise son message chiffré en blocs de même longueur, représentant chacun un nombre plus petit que n. Cette étape est cruciale pour éviter une simple substitution que l'on pourrait attaquer en analysant les fréquences.

- SALUT = 019 112 121 202

5) processus B chiffre chaque bloc (B) en utilisant la transformation C = B^e mod n (où Cest le bloc chiffré) :

- C1 = 19^5 mod 5429 = 5252

- C2 = 112^5 mod 5429 = 3303

- C3 = 121^5 mod 5429 = 2373

- C4 = 202^5 mod 5429 = 1371

Processus B obtient donc le message chiffré C : 5252 3303 2373 1371.

➢ 3.2.4. Sécurité de RSA

La résistance de RSA est basée sur certaines conditions de sécurité, en particulier :

- L'utilisation de valeurs assez élevées pour les paramètres e et d.

- Garder secrètes les valeurs de p et q. Garder secrètes les valeurs de p et q.
- Des longueurs de clés allant de 1024 bits à 2048 bits sont recommandées pour garantir que l'algorithme est suffisamment solide.
- Des études ont montré qu'un code RSA avec une clé de 1024 bits peut être craqué en huit mois, avec la coopération de 1600 ordinateurs conventionnels.**[18]**

➢ 3.2.5. Avantages et inconvénients du cryptage asymétrique (RSA)

- **3.2.5.1. Avantages**

✓ Gestion simplifiée avec une seule clé secrète à stocker.
✓ Particulièrement efficace pour faciliter l'échange de clés afin d'ouvrir un tunnel de communication sécurisé.

- **3.2.5.2 Inconvénients**

✓ Impact sur la vitesse de traitement en raison de sa lenteur.
✓ Absence d'authentification de la source.
✓ Vulnérabilité possible aux attaques de type "man-in-the-middle".**[2420]**

➢ 3.2.6. Les garanties du RSA

Nous avons vu que pour créer les clés, il fallait choisir deux grands nombres premiers

Les nombres premiers. Après un bref aperçu de la question, nous examinerons deux tests permettant de déterminer si un grand nombre est premier : L'un est aléatoire et l'autre est déterministe.

- **Quelques observations à propos des nombres premiers**

Les nombres premiers ont fait l'objet d'un certain nombre d'observations de la part de divers mathématiciens au fil des ans. Un exemple notable est le crible d'Ératosthène, datant de 240 avant J.-C., qui est une méthode déterministe consistant à diviser n par tous les entiers inférieurs à sa racine carrée. Toutefois, cette méthode perd de son efficacité pour les nombres plus importants en raison de sa complexité en O(√n). Les spécialistes estiment que seules les tâches traitées en temps polynomial sont considérées comme faciles. En 1640, Fermat a introduit des tests plus efficaces pour résoudre ce problème.

- **RSA assurerait quand même une sécurité importante**

Bien que ce pourcentage soit faible, il affecte la fiabilité des transactions en ligne, en particulier dans un contexte où des millions d'achats en ligne sont effectués chaque année. Cet algorithme est utilisé pour sécuriser de nombreux services en ligne tels que les services bancaires, le commerce électronique, le courrier électronique et les transactions en ligne. En pratique, lorsqu'un utilisateur se connecte à un site de commerce électronique, les transactions sont cryptées à l'aide de la clé publique du site, qui ne peut être décryptée que par le propriétaire du site qui possède la clé privée correspondante. Les clés publiques sont délivrées par les autorités de certification et sont intégrées dans le certificat numérique. En théorie, il est impossible de deviner le code de la clé privée et aucune paire de clés identiques n'a jamais été produite.

- **Mais difficile, voire impossible de les « casser »**

La robustesse du procédé RSA repose sur la complexité de l'analyse de n pour en déduire les valeurs de p, q et d. Cette notion d'inviolabilité repose plus sur l'expérience que sur la preuve formelle et n'est pas concluante pour certains spécialistes. Cependant, des progrès dans les méthodes d'analyse ou des avancées technologiques peuvent remettre en cause la sécurité des petites clés utilisées dans RSA. Cette question sera examinée plus en détail après avoir expliqué le principe de l'algorithme GNFS (General Number Field Sieve), qui a conduit au record de la plus grande clé déchiffrée.

3.3. Algorithme de chiffrement 3-way

En cryptographie, l'algorithme de chiffrement 3-Way a été créé en 1994 par Joan Daemen. Il est étroitement lié à BaseKing, étant toutes deux des variantes d'une même technique de chiffrement générale.

La particularité de 3-Way réside dans sa taille de bloc de 96 bits, qui diffère des tailles plus courantes comme 64 ou 128 bits. La clé utilisée a également une longueur de 96 bits. Cette taille provient de l'utilisation de trois mots de 32 bits dans l'algorithme, d'où le nom du chiffrement. À l'époque de sa création, les clés et les blocs de 96 bits étaient considérés comme suffisamment robustes, bien que les chiffrements modernes optent souvent pour des blocs de 128 bits et des clés de 128 bits ou plus.

3-Way fonctionne comme un réseau de substitution-permutation avec 11 tours.

3.3.1. Description de 3-WAY

La description de l'algorithme 3-Way est relativement simple. Pour chiffrer un bloc de texte en clair X, le processus se déroule comme suit :

1. Pour chaque itération i, où i varie de 0 à n-1, effectuer les opérations suivantes :
   - ✓ X = X XOR Ki
   - ✓ Appliquer la fonction theta sur X
   - ✓ X = Pi l (X)
   - ✓ Appliquer la fonction gamma sur X
   - ✓ X = Pi - 2(X) X
   - ✓ X = X XOR Kn+1
   - ✓ Appliquer à nouveau la fonction theta sur X

Le déchiffrement s'effectue de manière similaire en inversant les bits à l'entrée et à la sortie. Il est à noter que, jusqu'à présent, aucune tentative de cryptanalyse de l'algorithme 3-Way n'a abouti. De plus, l'algorithme n'est pas soumis à un brevet**. [25]**

➢ 3.3.2. Implémentation de l'algorithme 3 WAY

L'algorithme 3-Way met en œuvre des opérations sur des blocs de 96 bits avec une clé de même taille. Les fonctions utilisées dans l'algorithme sont les suivantes :

- ✓ La fonction theta(X) est une substitution linéaire, impliquant essentiellement une combinaison de décalages circulaires et d'opérations de OU exclusif.
- ✓ Les permutations Pi_1(X) et Pi_2(X) sont des opérations de permutation simples. Dans ce contexte, nous avons opté pour des permutations circulaires de 10 positions et de 1 position, respectivement, l'une étant l'inverse de l'autre.
- ✓ La fonction gamma(X) est une substitution non linéaire. Pour la mettre en œuvre, une approche simple consiste à combiner les trois mots en utilisant des opérations de OU exclusif, par exemple, en prenant le résultat du OU exclusif entre le premier mot et l'inverse du deuxième, puis en combinant le résultat avec un "ET logique" du troisième mot**. [21]**

➢ 3.3.3. Avantages et inconvénients du cryptage Symétrique (3-way)

• 3.3.3.1. Avantages de 3-way

Les avantages de 3-Way résident dans sa conception visant une efficacité élevée sur diverses plates-formes, allant des processeurs 8 bits au matériel spécialisé. De plus, l'algorithme présente des caractéristiques mathématiques élégantes, permettant l'exécution pratiquement -identique des opérations de décryptage et de chiffrement au sein des mêmes circuits.

3.3.3.2. Inconvénient de 3-way

Un inconvénient de 3-Way, similaire à son homologue BaseKing, réside dans sa vulnérabilité à la cryptanalyse de clé associée. Une démonstration réalisée par John Kelsey, Bruce Schneier et David Wagner a révélé que l'algorithme peut être compromis avec une requête de clé associée et environ 222 textes en clair sélectionnés.**[20]**

➢ 3.4. Définition de la bibliothèque ffmpeg

Une bibliothèque FFmpeg est un ensemble de fonctions et de routines programmées dans le cadre du projet FFmpeg, permettant d'effectuer des opérations de manipulation multimédia dans des applications logicielles. Ces bibliothèques fournissent une interface programmable pour l'encodage, le décodage, le transcodage, la lecture, l'écriture et la manipulation de divers formats de fichiers multimédias, tels que l'audio et la vidéo.

Voici quelques-unes des principales bibliothèques de FFmpeg :

- **Libavcodec**: Cette bibliothèque fournit des encodeurs et des décodeurs pour divers formats de fichiers audio et vidéo.
- **Libavformat** : Gère les opérations de multiplexage et de démultiplexage pour les conteneurs multimédias, ce qui permet de lire et d'écrire des fichiers multimédias dans différents formats.
- **Libavutil**: Cette bibliothèque contient des fonctions utilitaires utilisées par d'autres parties de FFmpeg.
- **Libswscale**: Fournit des fonctions de mise à l'échelle et de conversion de format de couleur pour les images vidéo.
- **Libavfilter** : Cette bibliothèque fournit des fonctions de filtrage pour appliquer des effets et des transformations aux flux audio et vidéo.
- **Libswresample** : Cette bibliothèque est utilisée pour rééchantillonner et convertir les formats audios.

Ces bibliothèques sont utilisées par les développeurs de logiciels pour intégrer des fonctions de traitement multimédia dans leurs applications, offrant des capacités avancées de lecture, d'écriture et de manipulation de contenus audio et vidéo.**[18]**

➢ 3.4.1. Les options de FFMPEG

Voici quelques options sur bibliothèque FFMPEG :

FFmpeg option	Explication
-i teapot.mp4	Sélectionne teapot.mp4 comme fichier d'entrée.
`-f image2pipe`	Indique à FFmpeg de convertir la vidéo en une séquence d'images (je crois !).
`-y`	Indique à FFmpeg d'écraser le fichier de sortie s'il existe déjà.
`-r 25`	Définit la fréquence d'images des données entrantes à 25 images par seconde.
`-vcodec mpeg4`	Indique à FFmpeg d'utiliser son encodeur « mpeg4 ».
`output.mp4`	Spécifie output.mp4 comme fichier de sortie.

Tableau 3.1 Représente Les options de la bibliothèque FFMPEG

➢ 3.4.2. Le rôle de la Bibliothèque FFMPEG

Les bibliothèques FFmpeg jouent un rôle important dans le fonctionnement de l'ensemble du projet FFmpeg. Elles sont utilisées pour intégrer des fonctionnalités de traitement multimédia dans d'autres applications logicielles. Voici quelques-uns des rôles clés des bibliothèques FFmpeg :

- **Traitement multimédia** : Les bibliothèques FFmpeg offrent des fonctionnalités pour le traitement des fichiers multimédia, y compris l'encodage, le décodage, le transcodage, la lecture, l'écriture, la conversion de format, etc.
- **Prise en charge des formats** : Elles prennent en charge une grande variété de formats de fichiers audio et vidéo et de conteneurs multimédias, ce qui permet aux applications d'interagir avec différents types de contenus multimédias.
- **Fonctions utilitaires** : Les bibliothèques FFmpeg contiennent des fonctions utilitaires pour des opérations courantes telles que la gestion des erreurs, la gestion de la mémoire, le calcul de l'horodatage, etc.

- **Intégration d'applications :** Les développeurs peuvent utiliser les bibliothèques FFmpeg pour intégrer des fonctionnalités multimédias dans leurs propres applications, telles que les lecteurs multimédias, les éditeurs vidéo, les convertisseurs multimédias, les systèmes de streaming, etc.
- **Personnalisation** : Les bibliothèques FFmpeg offrent un haut degré de flexibilité et de personnalisation, permettant aux développeurs de créer des applications avec des fonctionnalités spécifiques adaptées à leurs besoins.
- En résumé, les bibliothèques FFmpeg fournissent une infrastructure essentielle pour le traitement multimédia dans un large éventail d'applications, offrant des fonctionnalités avancées pour manipuler et interagir avec différents types de contenus audio et vidéo.

➢ 3.4.3. Les avantages et les inconvénients de bibliothèque ffmpeg

• 3.4.3.1. Les avantages de la bibliothèque ffmpeg

- **Polyvalence** : FFmpeg prend en charge un large éventail de formats de fichiers audio, vidéo et de conteneurs, ce qui le rend polyvalent pour le traitement multimédia.
- **Gratuit** abondance de ressources, de forums de discussion et de documentation pour obtenir de l'aide et des conseils.
- **Fonctionnalités avancées** : Les bibliothèques FFmpeg offrent un large éventail de fonctionnalités avancées pour le traitement multimédia, y compris l'encodage, le décodage, le transcodage, le streaming, le streaming, les filtres, et plus encore.
- **Intégration facile** : FFmpeg est conçu pour être facilement intégré dans d'autres applications grâce à ses bibliothèques bien documentées et à son API stable

  .
- **Gratuit et open source** : FFmpeg est un logiciel gratuit et open source, ce qui signifie qu'il est disponible gratuitement et que son code source peut être revu et modifié.
- **Grande communauté et support** : FFmpeg est largement utilisé et bénéficie d'une communauté active d'utilisateurs et de développeurs, ce qui signifie qu'il existe une

- **3.4.3.2. Les inconvénients de bibliothèque ffmpeg**

  - **Complexité** : En raison de sa puissance et de sa flexibilité, FFmpeg peut être complexe à utiliser, en particulier pour les utilisateurs novices ou pour des tâches simples.
  - **Gérer les dépendances** : FFmpeg a des dépendances et des exigences spécifiques en termes de configuration de la compilation, ce qui peut parfois causer des problèmes lors de l'intégration dans d'autres projets logiciels.
  - **Stabilité et mises à jour** : Bien que FFmpeg soit largement utilisé, sa stabilité et sa fréquence de mise à jour peuvent varier, ce qui peut entraîner des problèmes de compatibilité ou de performance dans certains cas.**[19]**

En résumé, les bibliothèques FFmpeg offrent une solution puissante et polyvalente pour le traitement multimédia, mais leur utilisation peut nécessiter une compréhension approfondie de leurs fonctionnalités et de leur intégration dans des projets logiciels.

3.5. Conclusion

Dans ce chapitre, nous avons présenté l'algorithme de cryptage à clé publique RSA et à clé privé 3-WAY. Nous prévoyons d'appliquer ces deux algorithmes de cryptage pour sécuriser des fichiers vidéo à l'aide de la bibliothèque FFMPEG.

Chapitre 4
Teste des résultats

Chapitre 4 Teste des résultats

4.1. Introduction

Dans ce chapitre, nous présenterons les résultats de l'implémentation des algorithmes RSA et 3-Way appliqués au cryptage vidéo. Le but est de comparer ces deux techniques de chiffrement en termes de performance, de sécurité et d'efficacité dans le contexte du cryptage vidéo.

Les algorithmes RSA et 3-Way ont été choisis pour leurs caractéristiques distinctes : RSA est un algorithme asymétrique bien connu pour sa robustesse et sa sécurité, tandis que 3-Way est un algorithme symétrique moins courant mais notable pour sa simplicité et sa rapidité. Dans notre implémentation, nous analyserons la vitesse et la qualité de l'opération de chiffrement des vidéosde ces deux algorithmes.

4.2 Présentation de l'Environnement et du Matériel et Outils Utilisés

➢ 4.2.1. Environnement de Développement

Pour cette étude, nous avons utilisé un environnement de développement comprenant le matériel et les outils logiciels suivants :

- **Matériel**

Caractéristique	**Détail**
Ordinateur de Développement	Hp
Processeur	Intel Core i5-9700K à 3,6 GHz
Mémoire vive (RAM)	16 Go DDR4
Stockage	SSD 512 Go
Carte Graphique	NVIDIA GeForce GTX 1660
Système d'exploitation	Windows 10

Tableau 4.1 Représente Les caractéristiques du matériel informatique utilisé

➢ 4.2.2. Outils et Logiciels Utilisés

Pour l'implémentation des algorithmes de cryptage ainsi que pour le développement des applications mobiles, nous avons utilisé les outils suivants :

- **Pour la Partie Java avec NetBeans**

- Langage de Programmation : Java
- IDE (Environnement de Développement Intégré) : NetBeans
- Bibliothèque Graphique : Java Swing

- **Pour la Partie Application Mobile avec Android Studio :**

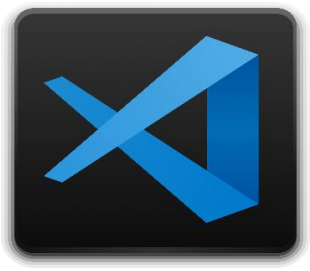
- Langages de Programmation : Java, XML
- IDE (Environnement de Développement Intégré) : Android Studio
- Framework UI : Android SDK (pour le développement d'interfaces utilisateur Android)
- Stockage et Gestion des Données : Utilisation de fichiers XML pour le stockage demétadonnées et de configurations dans l'application Android.

4.2.3. Configuration Logicielle

- Système d'Exploitation : Windows 10
- Versions des Outils

  NetBeans : Version 15

  Android Studio : Version 16
- Langage de Programmation : Java
- Framework Android : Android SDK



Cette configuration logicielle et ces outils nous ont permis de développer et d'implémenter efficacement les algorithmes de cryptage en Java avec NetBeans, ainsi que les applications mobiles Android avec Android Studio.

4.3. Installation Bibliothèque FFMPEG Sur Windows

Voici les étapes pour installer la bibliothèque FFmpeg sur Windows 10 sans détails :

- **Télécharger FFmpeg**

Aller sur FFmpeg Download page.

Télécharger la version pour Windows depuis un site tiers (comme gyan.dev).

- **Extraire le fichier**

Extraire le contenu du fichier ZIP téléchargé dans un dossier (par exemple, C:\ffmpeg).

- **Configurer le PATH**

Ouvrir "Variables d'environnement système".

Modifier la variable Path dans "Variables système".

Ajouter C:\ffmpeg\bin.

- **Vérifier l'installation**

Ouvrir l'invite de commandes.

Exécuter ffmpeg -version pour vérifier l'installation.

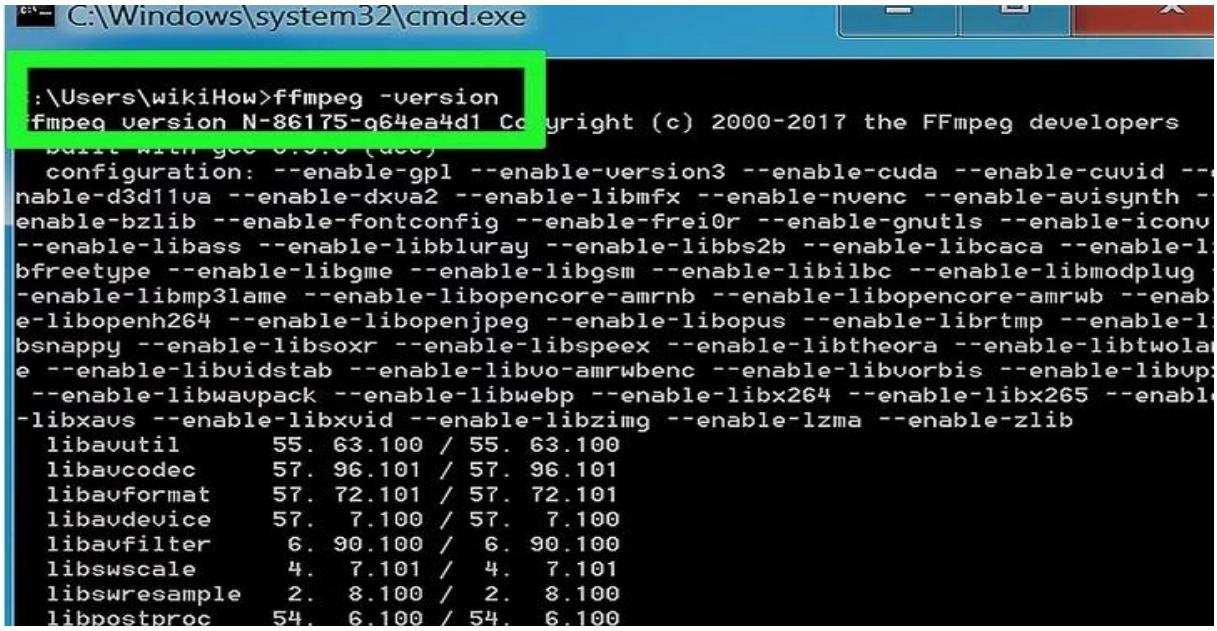


Figure IV.1 Représente Configuration de la bibliothèque FFMPEG

4.4. Présentation de l'application

➢ 4.4.1. Web

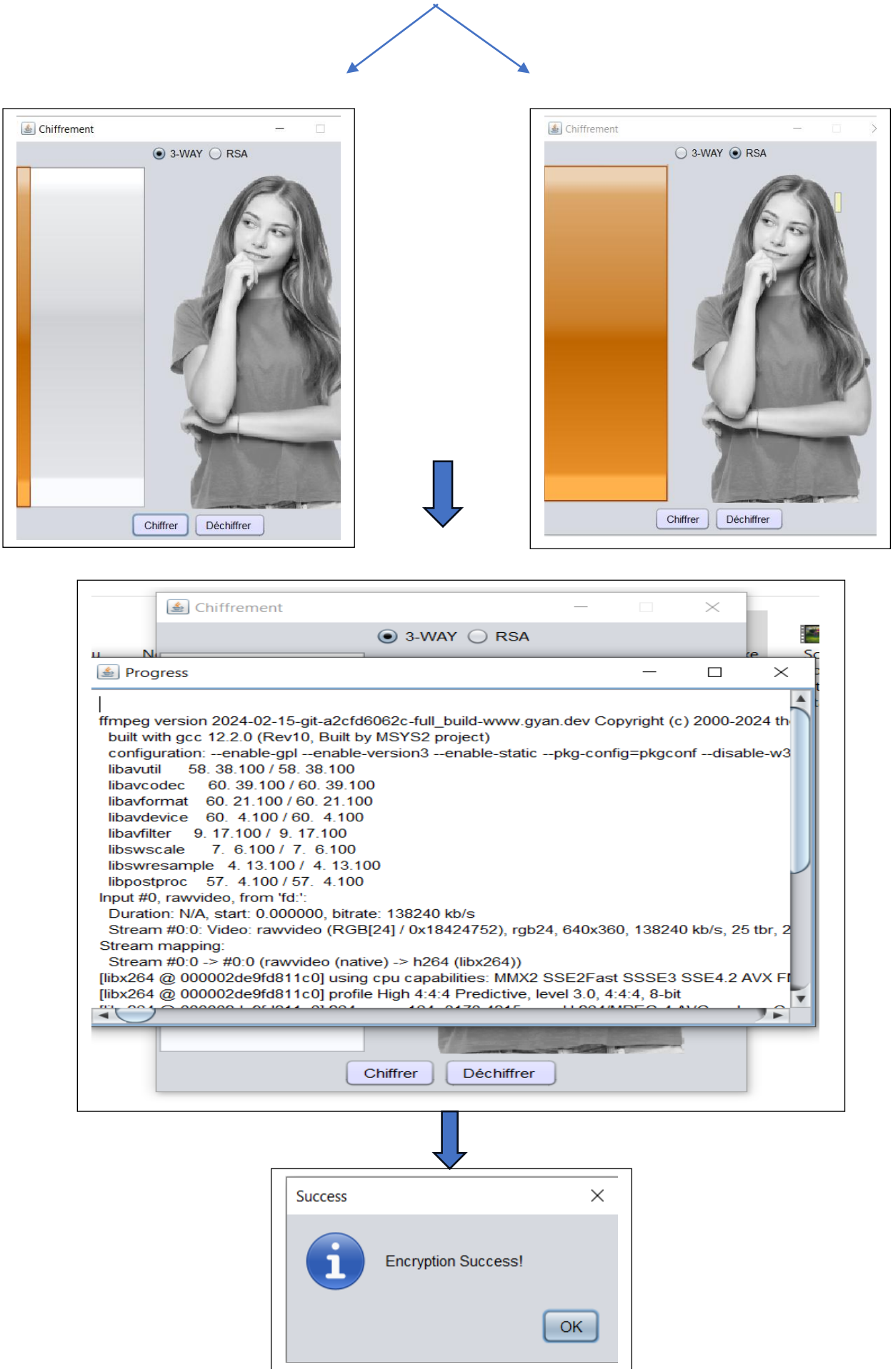
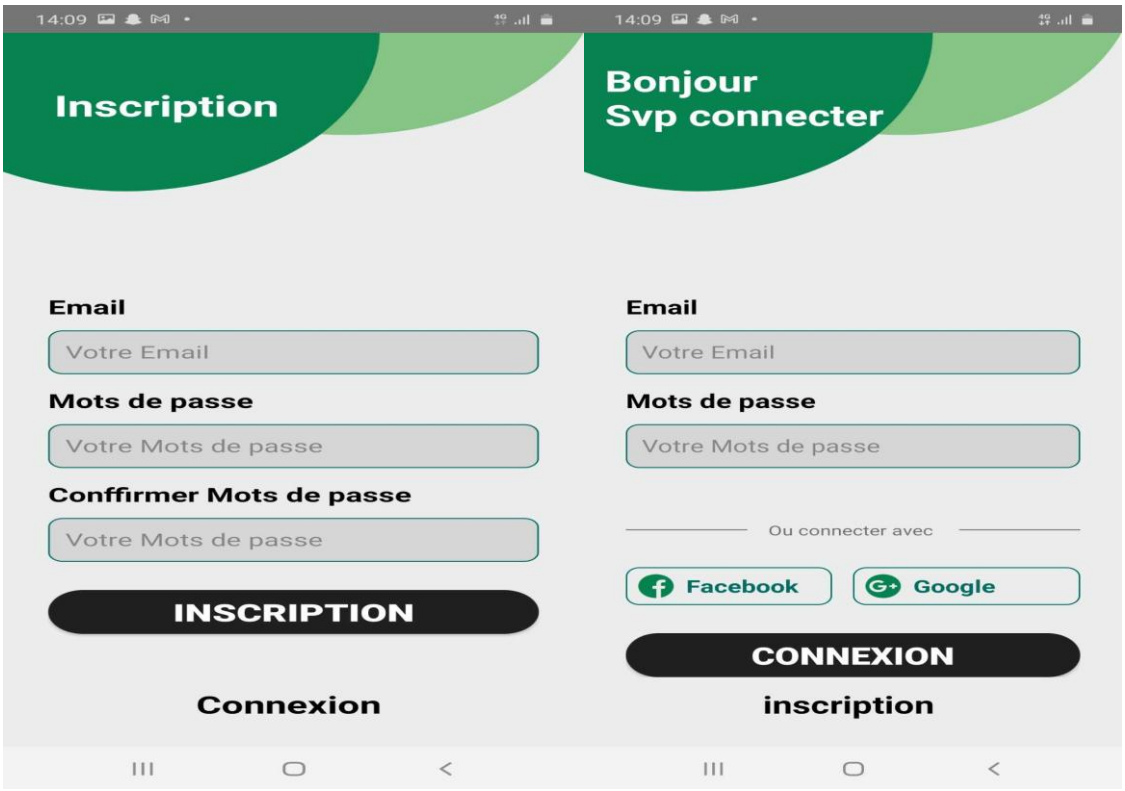


Figure IV.2 Présentation 1 de l'application

➢ 4.4.2 Mobile


14:09
Inscription
Email
Votre Email
Mots de passe
Votre Mots de passe
Conffirmer Mots de passe
Votre Mots de passe
INSCRIPTION
Connexion
14:09
Bonjour
Svp connecter
Email
Votre Email
Mots de passe
Votre Mots de passe
Ou connecter avec
Facebook
Google
CONNEXION
inscription


14:10
VIDÉOCRYPT
RSA ALGORITME
3-WAY ALGORITME
deconnecter

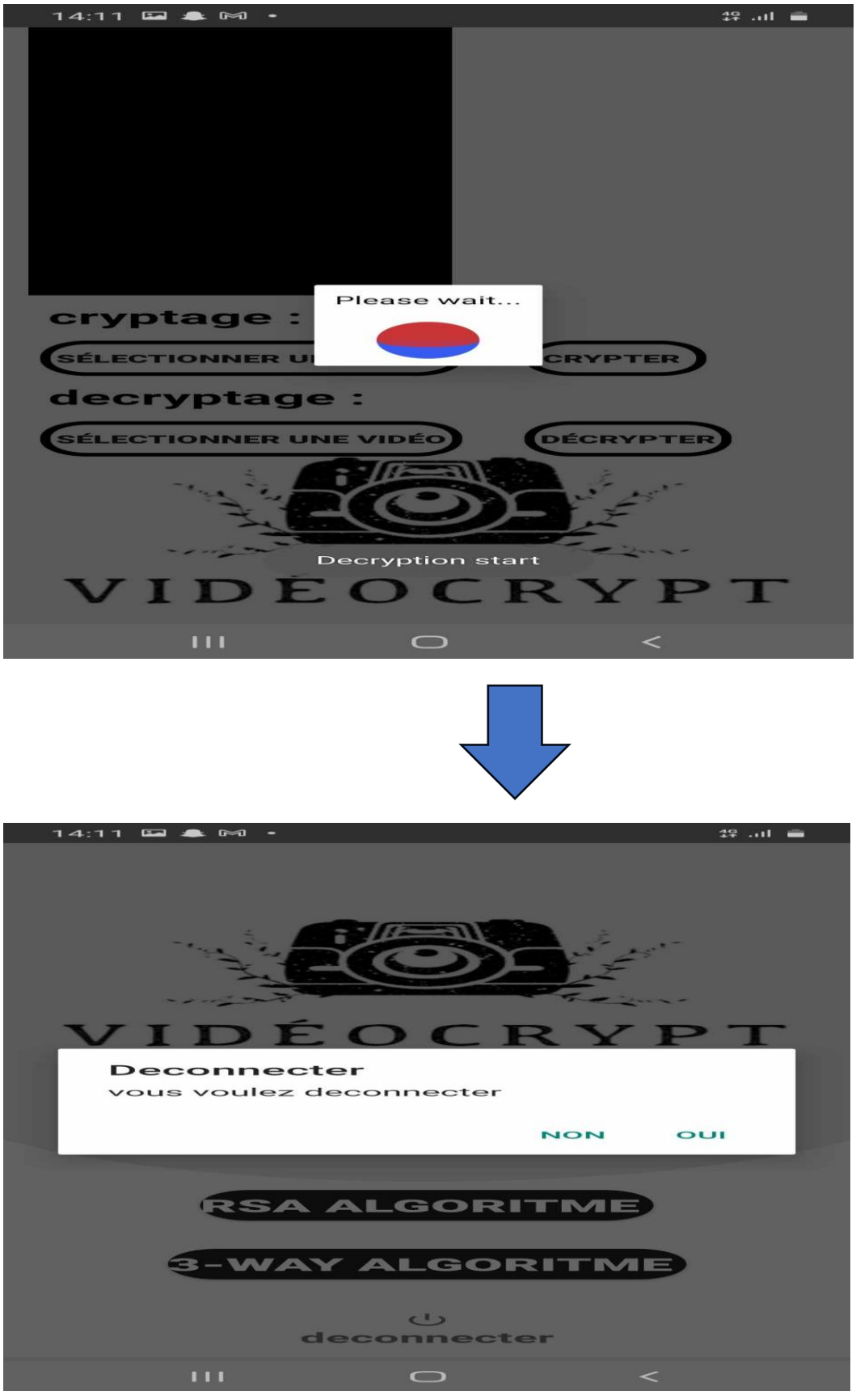


Figure IV.3 Présentation 2 de l'application

4.5. Étude Comparative des Algorithmes de Chiffrement RSA et 3Way

Temps / Vidéos	Type De Vidéos	Le Début	Le milieu	La FIN
Original				
Chiffrement Vidéo 01 :	Résultat RSA			
	Résultat 3-WAY			
Déchiffrement Vidéo 01 :	Résultat 3-WAY & RSA			

Tableau 4.2 Représente résultats Comparatifs du Chiffrement et Déchiffrement par RSA et 3Way (Vidéo 1)

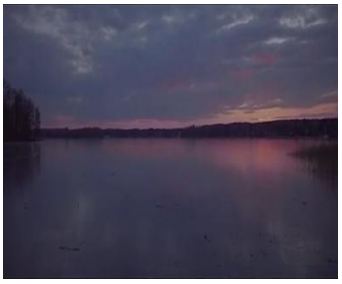
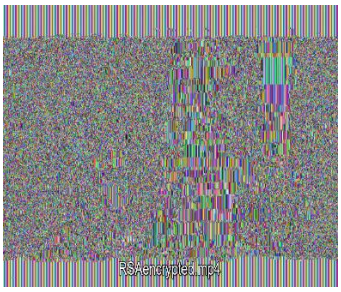
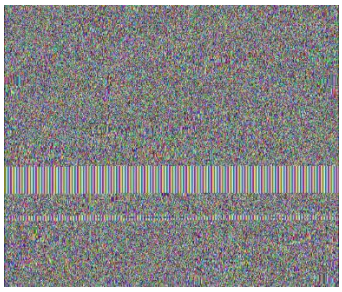
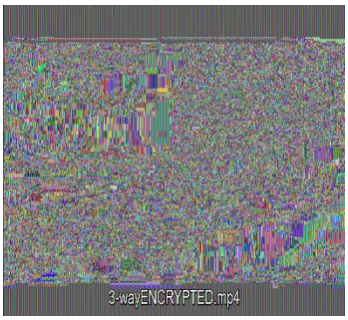
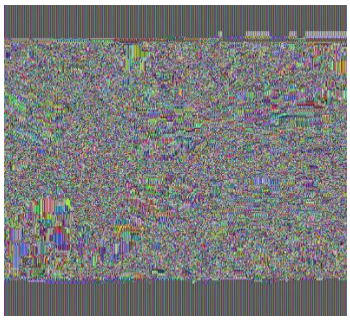
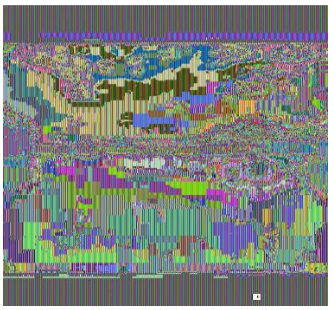
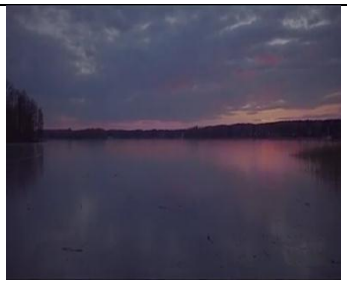
Temps / Vidéos	Type De Vidéos	Le Début	Le milieu	La FIN
Original				
Chiffrement Vidéo 02 :	Résultat RSA			
	Résultat 3-WAY			
Déchiffrement Vidéo 02 :	Résultat 3-WAY & RSA			

Tableau 4.3 Représente Résultats Comparatifs du Chiffrement et Déchiffrement par RSA et 3-Way (Vidéo 2)

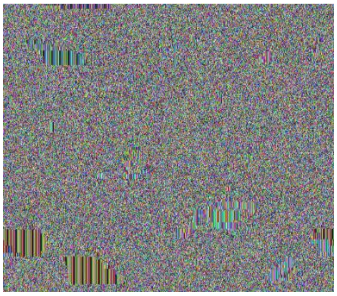
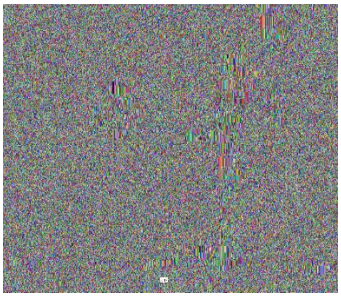
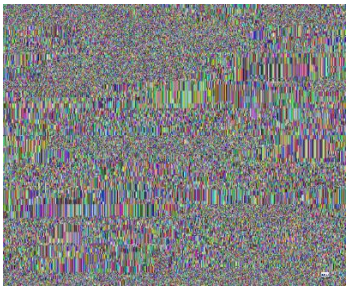
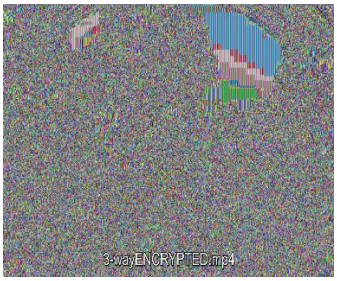
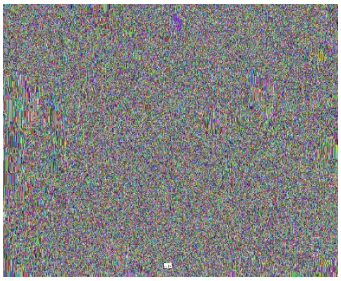
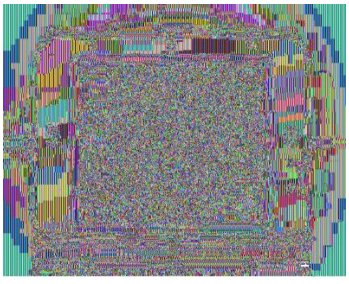
Temps / Vidéos	Type De Vidéos	Le Début	Le milieu	La FIN
Original				
Chiffrement Vidéo 03 :	Résultat RSA			
	Résultat 3-WAY			
Déchiffrement Vidéo 03 :	Résultat 3-WAY & RSA			

Tableau 4.4 Représente Résultats Comparatifs du Chiffrement et Déchiffrement par RSA et 3-Way (Vidéo 3)

	Le temps de chiffrement vidéo par RSA	Le temps de chiffrement vidéo par 3-WAY
Vidéo 1	10min	**5** min
Vidéo 2	6min	**3** min
Vidéo 3	8min	**4** min

Tableau 4.5 Représente temps de chiffrement de deux algorithmes RSA et 3-WAY

Remarque : D'après le résultat obtenu nous remarquons que le 3-WAY est plus rapide dans la vitesse du chiffrement par rapport à l'algorithme RSA.

- **Critères sur la qualité visuelle de l'opération de chiffrement :**

Entre 80 et 120 : Meilleures qualités (RSA)

Entre 60 et 80 : Bonnes qualités

Entre 40et 60 : Moyennes qualités (3-WAY)

Entre 0 et 40 : Faibles qualités

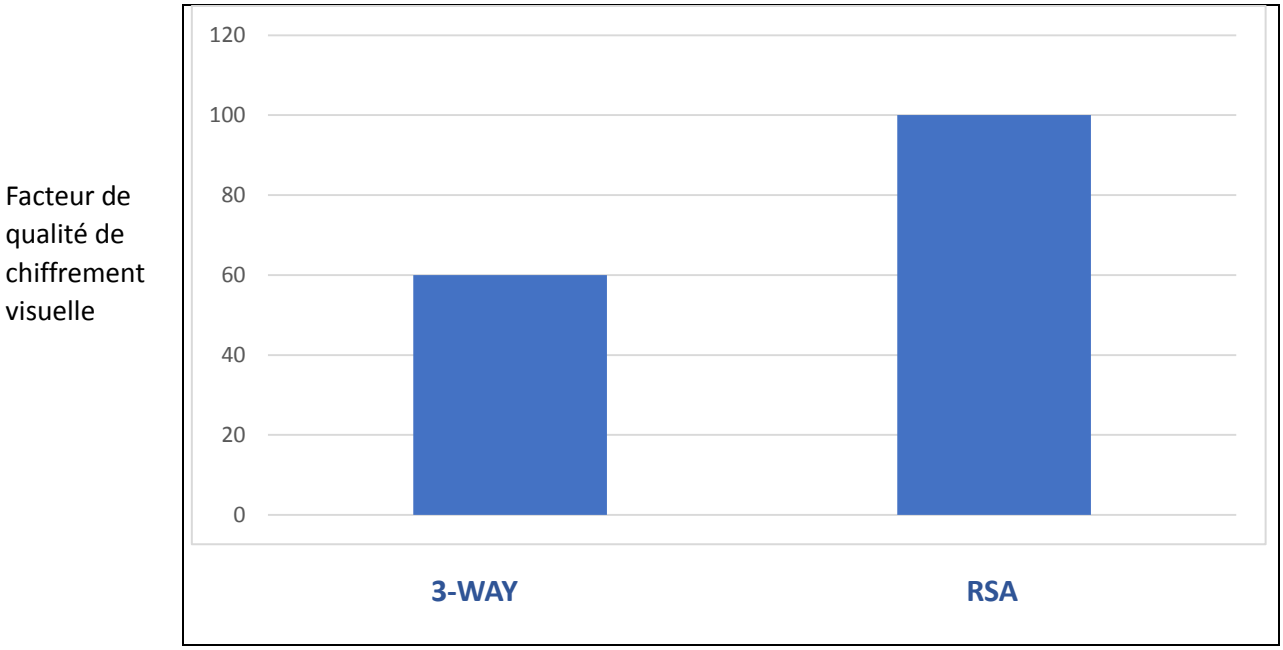


Figure IV.4 Représente Qualité de chiffrement de RSA et 3-WAY

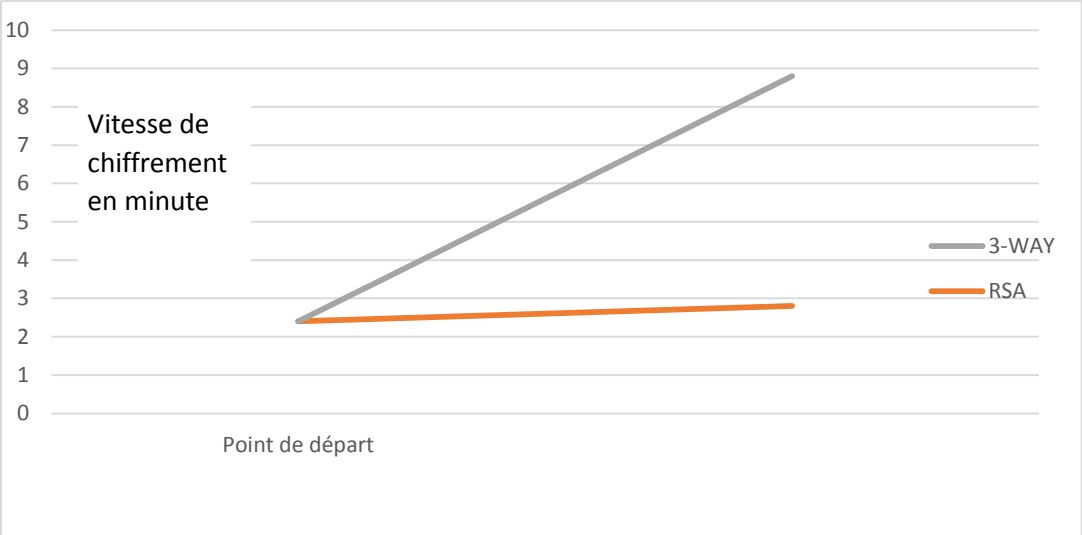


Figure IV.5 Représente la vitesse de chiffrement de RSA et 3-WAY.

4.6. Les caractéristiques des vidéos utilisées pour le RSA

Vidéo Original	**Nom de vidéo**	**Durée**	**Taille**	**Nbr frames**	**Le Temps d'exécution**
	Vidéo 01	10s	771Ko	360	10min
	Vidéo 02	15s	661 KO	250	6min
	Vidéo 03	30s	2.21 Mo	272	8 min

Tableau 4.6 Représente Caractéristique de vidéos utilisées et résultat de chiffrement par RSA

4.7. Les caractéristiques des vidéos utilisées pour le 3-WAY

Vidéo Original	**Nom de vidéo**	**Durée**	**Taille**	**Nbr frames**	**Le Temps d'exécution**
	Vidéo 01	10s	771Ko	360	5min
	Vidéo 02	15s	661 KO	250	3 min
	Vidéo 03	30s	2.21 Mo	272	8 min

Tableau 4.7 Représente Caractéristique de vidéos utilisées et résultat de chiffrement par 3-WAY

4.7. Conclusion

D'après les résultats que nous obtenus, nous remarquons que le cryptage RSA prend beaucoup de temps pour crypter une vidéo, alors que le cryptage 3-Way prend moins de temps. Nous également remarqué que le temps d'exécution augmente si le nombre frame augmente et si la longueur de la vidéo augmente. Mais en termes de qualité visuelle, nous remarqué qu'avec le cryptage RSA, la similarité de la vidéo affecte sur la qualité du cryptage. Lorsque vous prenez des vidéos avec une faible similarité, vous obtenez une meilleure qualité, tandis que RSA offre une meilleure qualité visuelle, mais son utilisation n'est plus recommandée aujourd'hui en raison de sa lenteur d'exécution.

D'après les différents tests que nous effectués, nous constaté que le cryptage 3-Way est toujours plus rapide et offre une qualité visuelle moyenne lors du cryptage. En particulier lors de la prise de vidéos à faible similarité. En revanche, le cryptage RSA, qui se caractérise par une qualité visuelle élevée, a une vitesse d'exécution très lente. Étant donné que le facteur vitesse est le plus important, le chiffrement 3-WAY est souvent préféré pour les applications pratiques, malgré sa qualité visuelle inférieure.

Conclusion Générale

Conclusion générale

Ce projet, réalisé dans le cadre de notre mémoire de fin d'études de niveau master, a permis d'appliquer nos compétences et connaissances acquises durant nos années d'études.

La croissance exponentielle de la quantité d'informations transitant sur les réseaux impose de crypter ces données pour assurer leur confidentialité et leur sécurité. Le cryptage est essentiel pour prévenir l'interception, la lecture ou la modification non autorisée des messages, ainsi que pour empêcher la création de messages erronés.

Nous avons utilisé la bibliothèque **FFMPEG** pour le traitement des vidéos, en particulier pour la lecture et la conversion des vidéos en entrée et en sortie. Cette bibliothèque est reconnue pour sa soliditéet sa fiabilité, étant utilisée par des logiciels et services tels que VLC et YouTube.

Nous avons comparé les algorithmes de cryptage **RSA et 3-Way** pour sécuriser les fichiers vidéo**. RSA** offre une sécurité élevée mais est plus lent, tandis que **3-Way** est plus rapide, bien que moins connu. Nos résultats montrent que l'utilisation combinée de ces méthodes peut offrir une solution efficace pour le cryptage vidéo, en utilisant RSA pour sécuriser les clés de session et 3-Way pour le cryptage rapide des vidéos.

Pour les recherches futures, nous recommandons d'explorer des optimisations supplémentaires des algorithmes **RSA** au niveau des paramètres **p** et **q** etpour**3-Way**, nous augmentons le nombre de bits de clés de chiffrement de 96 bits à 128 bits.

Ce mémoire a apporté une contribution précieuse au domaine du cryptage vidéo en fournissant des analyses détaillées et des recommandations pour les travaux futurs.

Références

[1]. Aicha TEKKOUK ,Etude et Implémentation d'une méthode cryptanalyse pour le chiffrement continu, mémoire de magister Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf ,2010.

[2]. KHIDER Ali et YAALA Mohamed implémentation de l'Algorithme de Cryptage AES sur un circuit FPGA,Université Dr. Yahia Farès de Médéa,2012-2013.

[3]. Mohand-Amokrane BIR et Lyes DAHMOUNI, Etude et implémentation d'algorithmesde chiffrement à clé secrète et à clé publique : Application au cryptage de la parole, mémoire de master, Université Mouloud Mammeri De Tizi-Ouzou,2018.

[4]. M. Abomhara, O. Zakaria, and O. O. Khalifa, "An Overview of Video Encryption Techniques," Int. J. Comput. Theory Eng., pp. 103–110, 2009, doi: 10.7763/ijcte. 2010.v2.123

[5]. Y. Negi Asstt Professor, "A Survey on Video Encryption Techniques," Int. J. Emerg. Technol. Adv. Eng. A Surv. Video Encryption Tech., vol. 9001, no. 4, pp. 234–237, 2008, [Online]. Available: www.ijetae.com.

[6]. F. Liu and H. Koenig, "A survey of video encryption algorithms," Comput. Secur., vol. 29, no. 1, pp. 3–15, 2010, doi: 10.1016/j.cose.2009.06.004.

[7]. X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proc. 6th Int. Forum Strateg. Technol. IFOST 2011, vol. 2, pp. 1118– 1121, 2011, doi: 10.1109/IFOST.2011.6021216.

[8]. M. Amara and A. Siad, "Elliptic Curve Cryptography and its applications," 7th Int. Work. Syst. Signal Process. their Appl. WoSSPA 2011, pp. 247–250, 2011, doi: 10.1109/WOSSPA.2011.5931464.

[9]. Bousalah Malika Et Tifour Yamina, Contribution à la conception d'un crypto systèmesymétrique flexible sur circuit FPGA, mémoire de master, Universite M'hamed Bougara De Boumerdes,2015-2016.

[10]. I. E. G. Richardson, Video codec design developing image and video compression systems. John Wiley and Sons, 2002.

[11]. K. S. Thyagarajan, Still Image and Video Compression with MATLAB. John Wiley and Sons, 2011.

[12]. V. Bhaskaran and K. Konstantinides, Image and Video Compression Standards: Algorithms and Architectures. Kluwer Academic Publishers, 1997.

[13]. L. E. Tresa and M. Sundararajan, “Comparative analysis of different wavelets in DWT for video compression,” 2014 Int. Conf. Circuits, Power Comput. Technol. ICCPCT 2014, pp. 1512–1517, 2014, doi: 10.1109/ICCPCT.2014.7054859.

[14]. S. Pandit, P. K. Shukla, A. Tiwari, P. K. Shukla, M. Maheshwari, and R. Dubey, “Review of video compression techniques based on fractal transform function and swarm intelligence,” Int. J. Mod. Phys. B, vol. 34, no. 8, pp. 1–21, 2020, doi: 10.1142/S0217979220500617.

[15]. X. Zhang, O. C. Au, J. Dai, C. Pang, and F. Zou, “New chroma intra prediction modes based on linear model for HEVC,” Proc. - Int. Conf. Image Process. ICIP, pp. 197–200, 2012, doi: 10.1109/ICIP.2012.6466829.

[16]. M. M. Nasralla, M. Razaak, I. Rehman, and M. G. Martini, “A Comparative Performance Evaluation of the HEVC Standard with its Predecessor H.264/AVC for Medical videos over 4G and beyond Wireless Networks,” 2018 8th Int. Conf. Comput. Sci. Inf. Technol. CSIT 2018, pp. 50–54, 2018, doi: 10.1109/CSIT.2018.8486153.

[17]. E. Doutsi, “Retina-inspired Image and Video coding,”, PhD thesis, Université Côte d’Azur, 2017.

[18]. Etude comparative entre les algorithmes cryptographiques appliqués sur des fichiers textes et des fichiers images (BMP) basé sur une simulation d’une attaque exhaustive – melle BENHAMOU Fatima, Melle DERRAR Ghizlane Ibtissam – 2006

[19]. FFmpeg est-il la meilleure bibliothèque C/C++ à utiliser pour enregistrer une vidéo brute, en mémoire, dans un format conteneur ? : r/ffmpeg (reddit.com)

[20]. Kelsey, J., Schneier, B., & Wagner, D. (1997). Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA. In International Conference on Information and Communications Security (ICICS), Lecture Notes in Computer Science, vol 1334. Springer, Berlin, Heidelberg.

[21]. Compression avec ou sans perte : Guide du débutant pour les deux formats, Kinsta, 2024-04-28.

Biblioweb

[23]. https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/
18 décembre 2015.

[24]. https://www.sealpath.com/fr/blog/types-de-chiffrement-guide/
14 juin 2022.

[25]. 03fr-rist14-2.pdf www.webreview.dz visité le 20/05/2024. Disponible sur :
http://www.webreview.dz/IMG/pdf/03fr-rist14-2.pdf

20 mai 2024.

Résumé :

Avec l'augmentation significative des données transitant sur les réseaux internationaux, le cryptage est devenu essentiel pour garantir la confidentialité et la sécurité des informations. Il est particulièrement nécessaire pour protéger les vidéos contre l'interception, la lecture non autorisée et les modifications malveillantes. Dans ce travail, nous avons étudié la cryptographie vidéo en utilisant deux algorithmes : RSA et 3Way. Pour mettre en œuvre ces algorithmes, nous avons utilisé la bibliothèque FFMPEG, réputée pour sa fiabilité en matière de traitement vidéo.

Notre étude se termine par une comparaison des résultats de ces deux algorithmes en termes de qualité de cryptage et de temps de traitement. Les résultats montrent les forces et les faiblesses de chaque méthode, fournissant un aperçu de l'utilisation optimale de RSA et 3Way dans la cryptographie vidéo.

Mot-clé : cryptographie vidéo, RSA, 3Way, confidentialité, sécurité des informations, interception, lecture non autorisée, FFMPEG, traitement vidéo, qualité de cryptage, temps de traitement, algorithmes de cryptage, protection des vidéos.

ملخص

مع الزيادة الكبيرة في نقل البيانات عبر الشبكات الدولية، أصبح التشفير ضرورياً لضمان سرية وأمن المعلومات. وهذا ضروري بشكل خاص لحماية مقاطع الفيديو من الاعتراض والتشغيل غير المصرح به والتعديل الخبيث. في هذا العمل، درسنا تشفير الفيديو باستخدام خوارزميتين المشهورة بموثوقيتها في معالجة الفيديو. تختتم دراستنا بمقارنة نتائج هاتين FFMPEG ولتنفيذ هذه الخوارزميات، استخدمنا مكتبة 3-WAY و RSA: ووقت المعالجة. تُظهر النتائج نقاط القوة والضعف في كل طريقة، مما يوفر نظرة ثاقبة RSAو 3-WAYالخوارزميتين من حيث جودة التشفير للاستخدام الأمثل لخوارزميات في تشفير الفيديو.

الكلمـــات المفتاحيـــة : متـــوازن، غيـــر متـــوازن، الســـرية، RSA ، 3-WAY ،مكتبـــة Ffmpeg.

Abstract

With the significant increase in data transiting international networks, encryption has become essential to guarantee the confidentiality and security of information. This is particularly necessary to protect videos from interception, unauthorized playback and malicious modification.

In this work, we studied video cryptography using two algorithms: RSA and 3Way. To implement these algorithms, we used the FFMPEG library, renowned for its reliability in video processing. Our study ends with a comparison of the results of these two algorithms in terms of encryption quality and processing time. The results show the strengths and weaknesses of each method, offering insight into the optimal use of RSA and 3-Way in video cryptography.

Keyword: video cryptography, RSA, 3Way, confidentiality, information security, interception, unauthorized playback, FFMPEG, video processing, encryption quality, processing time, encryption algorithms, video protection.