République Algérienne Démocratique Et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique

Université Abou Bakr Belkaid– Tlemcen

Faculté des Sciences

Département d'Informatique

Mémoire de fin d'étude en vue d'obtention du diplôme de Master en informatique

Option : Réseau et système distribue (RSD)

Etude et comparaison entre les variantes de l'algorithme RSA pour le cryptage des fichiers vidéo en utilisant la bibliothèque Ffmepg

Réalisé par :

- ***Boudilmi Ghizlen Zoubida***
- ***Benmoulay Elcherif Rania***

Encadré par :

BENAISSA MOHAMED

Présenté le 4 juillet 2022 devant le jury composé de :

Président : **M. Mana Mohammed**

Examinateur : **M. Bambrik Ilyas**

Encadrant : **M. Benaissa Mohamed**

Année Universitaire 2021 / 2022

Remercîment

On offre notre grande gratitude à Allah qui nous a aidé à faire ce travail.

Tout en exprimant notre profonde gratitude à nos parents pour leurs encouragements, leurs soutiens et pour leurs sacrifices.

Nous remercions notre encadrant M Benaissa Mohammed pour les ses efforts, de nous avoir aidé, conseillé, encouragé et corrigé.

Nous remercions les membres de jury d'avoir accepté d'examiner notre travail.

Nous remercions aussi tout le corps enseignant au sein du département de l'informatique qui a contribué à notre formation universitaire.

Enfin, nous remercions tous ceux de près ou de loin qu'ont contribué à la réalisation de ce travail, trouvant ici notre sincère reconnaissance.

Dédicace

Je dédie ce modeste travail, à mes parents, à ma source de générosité

Et de patience tout au long de ma carrière scolaire. Que Dieu vous

protèges, vous prêtes bonne santé et longue vie.

A mes frères et sœurs et sa petite famille, qui m'ont toujours indiqué

La bonne voie et qui ont su m'aider.

Aux personnes qui m'ont accompagné durant mon cursus

universitaire,

À mes amies pour ses encouragements Permanents, et son soutien

Table Des Matières

Chapitre 2 Conceptede base des vidéos

Chapitre 3 Principe de fonctionnement RSA

chapitre 4 Tests et résultats de l'opération de chiffrement par rsa

Liste Des Tableaux

Liste Des Figures

Introduction Générale

L'utilisation large des images et des vidéos numériques dans divers applications apporte une attention particulière à la sécurité et aux problèmes de confidentialité aujourd'hui.

La cryptographie est parmi les méthodes les plus efficaces pour établir la confidentialité et l'intégrité des données visuelles comme les vidéos et les images, jusqu'à, maintenant divers algorithmes de cryptage ont été proposés et largement utilisé comme DES, RSA, etc.
Ils sont utilisés pour le texte et les données binaires.

Il est difficile de les utiliser directement dans le chiffrement vidéo car les vidéos numériques sont caractérisées par la redondance élevée, la forte corrélation et la taille volumineuse.
Et cela nécessite des traitements en temps réel.

Nous nous sommes intéressés dans notre projet de fin d'étude au développement d'une application de cryptage des vidéos en utilisant l'algorithme asymétrique RSA et la bibliothèque FFMPEG.
Le but principal de notre travail est de tester l'efficacité et l'influence des paramètres p et q de l'algorithme RSA sur la qualité et la vitesse de l'opération de chiffrement des vidéos.

Le contenu de ce mémoire est organisé comme suit :

Dans **le premier chapitre**, nous décrivons des généralités sur la cryptographie,
nous aborderons également les algorithmes de chiffrement symétrique, asymétrique et hybride en citant quelques algorithmes classiques et populaires.

Dans **le deuxième chapitre**, nous parlerons des concepts de bases des vidéos et de certains algorithmes modernes de chiffrement des vidéos.

Dans **le troisième chapitre**, nous décrivons le principe et la structure de fonctionnement de

l'algorithme RSA qui est utilisé dans le cryptage des vidéos en utilisons la bibliothèque FFMPEG

Dans **le dernier chapitre**, nous entamons la partie de tests et de résultats obtenue de l'opération de chiffrement par l'algorithme RSA en se basant sur la variation des valeurs p et q et leur

influence sur la qualité et la vitesse de cryptage des vidéos.

Chapitre 1

Introduction à la Cryptographie

1.Introduction à la Cryptographie

1.1 Introduction

Aujourd'hui grâce au développement des technologies d'internet la communication et le partage de multimédia devient plus facile et rapide, mais avec la progression de la cybercriminalité qui facilite l'accès légal et illégal au œuvres protégées, la sécurité des vidéos numérique est devenu un sujet important dans le monde de la communication donc la sécurité des systèmes d'information et la meilleure solution pour protéger les ressources multimédia , et parmi les techniques de la sécurité informatique le cryptage.

La cryptographie c'est l'ensemble des techniques utilisant des clés pour chiffrer les données et assurer la confidentialité, il y a deux types de chiffrement :

Premièrement, **chiffrement symétrique** : les algorithmes à clé secrète consiste a utiliser la même clé par l'émetteur et le récepteur pour chiffrer et déchiffrer les données mais le problème principal de ces algorithmes est qu'il y a toujours un risque d'attaque exhaustive pour retrouver la clé.

Deuxièmement, le **chiffrement asymétrique** : les algorithmes à clé publique utilisent deux clés différentes tel que : une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

Les algorithmes de chiffrement des vidéos nécessitent une large bande passante et beaucoup de temps de cryptage donc le but de notre mémoire c'est d'étudier le chiffrement des vidéos en utilisant l'algorithme à clé publique RSA.

1.2 *L'historique de la cryptographie*

La cryptographie existe depuis l'antiquité, on cherche à envoyer des messages sans que des personnes extérieures ne puissent les intercepter, historiquement elle est restée pendant très longtemps un art, pour devenir une science et avec l'apparition de l'informatique, son utilisation se démocratise de plus en plus **[1].**

La cryptographie est basée sur deux principes :

- La transposition : changer l'ordre des lettres des messages initiaux.
- La substitution : consiste à substituer dans un message chacune des lettres de l'alphabet par une autre (du même alphabet ou éventuellement d'un autre alphabet).

La substitution utilise deux types :

- Substitution poly alphabétique.
- Substitution mono alphabétique.

1.2.1 Substitution mono alphabétique

Elle consiste à remplacer une même lettre par une et une seule lettre (symbole, motif) dans la totalité du texte, la première technique cryptographique de substitution est associée à César **[2].**

1.2.2 Substitution poly-alphabétique

Consiste à rendre de plus en plus compliqué une cryptanalyse de substitution mono-alphabétique pour éviter de chiffrer une lettre par une et une seule lettre.

Le meilleur moyen est de chiffrer une même lettre par différents symboles ou lettres (poly alphabétique).**[2]**

1.2.3 Chiffre de César

César a réalisé la toute première substitution admise par les historiens.

L'idée de César était de chiffrer avec un décalage de lettres sur 3 positions.

Son principe est très simple : il remplace le A par D, le B par E, …

Exemple : le message salut devient : vdoxw.

L'inconvénient de ce chiffrement est de permettre aux ennemis de découvrir facilement le message transmis **[1].**

1.2.4 Chiffre de Vigenère

Son principe utilise le chiffre de César différent d'une lettre à l'autre de sorte à remplacer la même lettre par différentes lettres (possible de chiffrer différentes lettres par la même).

Chiffrement: Choisir un mot quelconque comme clé. Le reproduire autant de fois que nécessaire sous le texte clair, utiliser la table de Vigenère pour trouver le texte chiffré (intersection de la lettre du texte clair et la lettre de la clé **[12].**

1.3 Chiffrement symétrique

C'est l'un des plus anciens techniques de chiffrement qui consiste utilisé une clé partagée entre l'émetteur et le destinataire des données pour chiffrer et déchiffrer les messages.
Parmi les avantages de chiffrement à clé secrète : facile à mettre en place et simple à utiliser, mais l'inconvénient que la clé est partagé donc il y a le risque d'être piraté

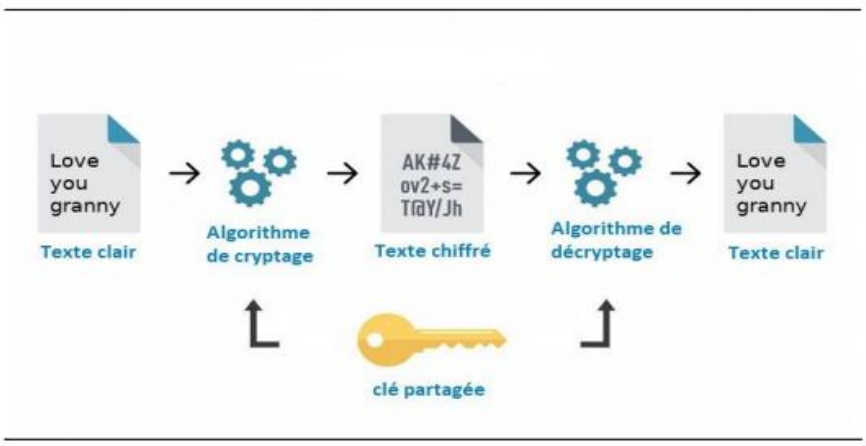


Figure 1.1 Schéma qui illustre le chiffrement symétrique **[3].**

On peut diviser le chiffrement symétrique en 2 catégories :

1.3.1 Chiffrement par bloc

Consiste à découper le message en bloc de bits de taille fixe et chiffrer en additionnant bit par bit avec la clé

1- Remplacer les caractères par un code binaire.
2- Découper cette chaine en blocs de longueur donnée.
3- Chiffrer un bloc en additionnant bit par bit a une clef.
4- Déplacer certains bits de blocs.
5- Recommencer éventuellement un certain nombre de fois l'opération 3 et passer au bloc suivant jusqu'à ce que tout le message soit chiffré.

Parmi les algorithmes les plus connus :

a. XOR (ou exclusif)

Son principe et très simple on peut crypter une vidéo en additionnant le premier pixel de l'image de la vidéo au premier pixel de l'image clé, exemple : **[4]**

XOR	0	1
0	0	1
1	1	0

Tableau 1.1 Tableau de XOR

1er pixel de l'image originale	01110011
1er pixel de l'image clé	10100101
XOR	
1er pixel de l'image cryptée	11010110

Tableau 1.2 Tableau de chiffrement d'une image

b. DES (data encryption standard)

Algorithme créé en 1977, il utilise une clé de taille 56bits **[13].**

Cet algorithme change un bit dans le texte en clair, il a un impact important sur les bits de texte chiffré.

La diffusion casse la répétition du texte en clair dans le texte chiffré, par exemple deux lettres doubles ne doivent pas être placées côte à côte après cryptage **[5].**

c. Blow Fish

Algorithme de chiffrement connu en 1999, il utilise un bloc de 64 bit et une clé de 32-448 bit il est rapide et plus sécurisé.

1.3.2 Chiffrement par flot

Le chiffrement par flot est classé parmi l'une des deux grandes catégories de chiffrements modernes utilisant une clé.

Son grand avantage

Il est utilisé généralement dans le chiffrement des communications téléphoniques (RC4, A5/1), il utilise le chiffrement symétrique, le texte peut être d'une taille arbitraire **[4].**

a. RC4

La clef RC4 permet d'initialiser un tableau de 256 octets elle répète la clef autant de fois que nécessaire pour remplir le tableau, par la suite, des opérations simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc… le but de cryptage rc4 est de mélanger autant que possible le tableau, finalement on obtient une suite de bits pseudo aléatoires qui peuvent être utilisés pour chiffrer les données via un XOR **[14].**

b. le chiffrement Bluetooth _e0

Est utilisé par le protocole Bluetooth pour protéger les échanges de données, une suite aléatoire créée sur laquelle on effectue un XOR avec les données.

La clef a une longueur qui est généralement fixée à 128 bits mais sa taille est variable.

À chaque itération, un bit est créé à 4 registres à décalage de longueurs différentes et deux états internes de 2 bits chacun. À chaque horloge, les registres sont décalés et les deux états sont mis à jour en utilisant l'état courant, l'état précédent et les valeurs présentes dans les registres à décalage. 4 bits sont extraits des quatre registres à décalage et sont additionnés.

L'algorithme effectue un XOR entre cette somme et la valeur du registre de 2 bits, le premier bit ainsi obtenu est la sortie pour le chiffrement **[15].**

E0 se divise en trois parties :

- Préparation de la clé.
- Génération du flux.
- Chiffrement.

1.4 Chiffrement asymétrique

Le cryptage à clé publique évite le partage d'un secret entre les deux interlocuteurs puisque, chaque utilisateur dispose d'un couple de clés : une clé secrète connue de lui seul et une clé publique qu'il met en général à disposition de tous dans un annuaire. Ces deux clés, en plus d'être distinctes, elles ne peuvent se déduire l'une de l'autre. Alors, pour envoyer un message confidentiel à x, y crypte le message clair à l'aide de la clé publique de x, ce dernier, à l'aide de la clé secrète correspondante, sera le seul en mesure de déchiffrer le message reçu **[6].**

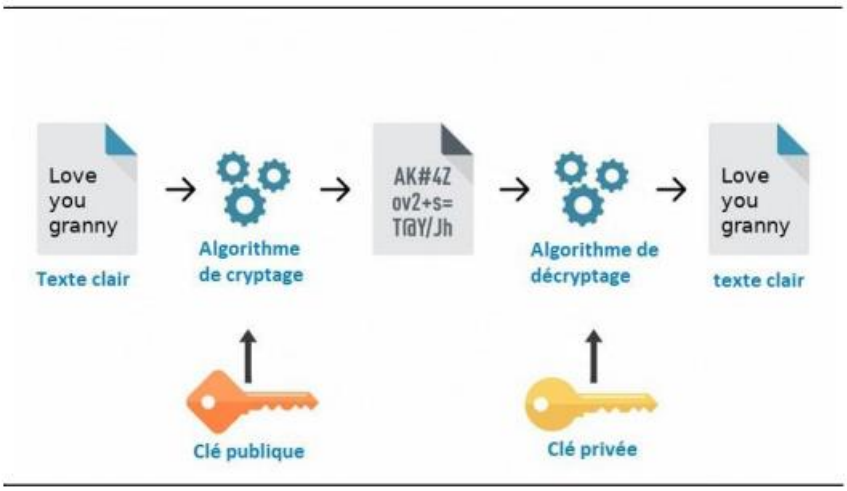


Figure 1.2 Schéma illustre le chiffrement asymétrique **[12]**

1.4.1 RSA

Cet algorithme a été créé en 1976 par Diffie et Hellamn qui ont introduit une approche pour les systèmes à clé publique et ont contesté les chercheurs de concevoir des algorithmes répondant aux exigences, le défi a été relevé par un algorithme proposé par Ron Rivest, Adi Shamir, Len Adleman (RSA) en 1978 au MIT.

RSA est un chiffrement par bloc dans lequel le texte brut et le texte chiffré sont des entiers compris entre 0 et m-1 pour un certain m, typiquement m a 1024 bits (m <1024) ou 309 chiffres décimaux **[7].**

1.5 Cryptographie hybride

Est un système de cryptographie basé sur deux grandes familles de systèmes cryptographiques : la cryptographie asymétrique et la cryptographie symétrique.

Principe :

A génère une clé secrète. il crypte cette clé avec la clé publique de B, l'information est envoyée à B par un canal non sécurisé.

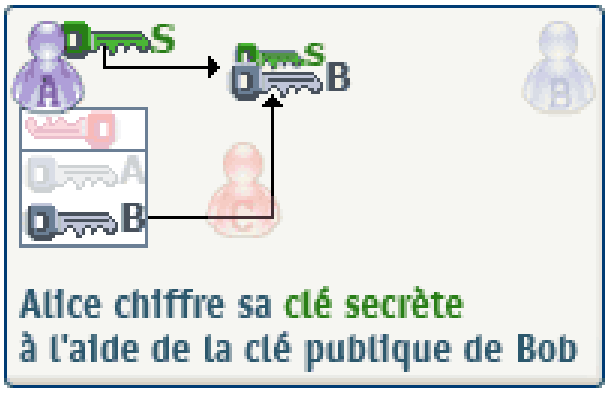


Figure 1.3 : Schéma qui illustre le chiffrement a clé secrète **[8]**

L'espion ne peut intercepter l'information car il ne possède pas la clé privée de B.

B décrypte l'information à l'aide de sa clé privée, et possède ainsi la clé secrète générée par A.

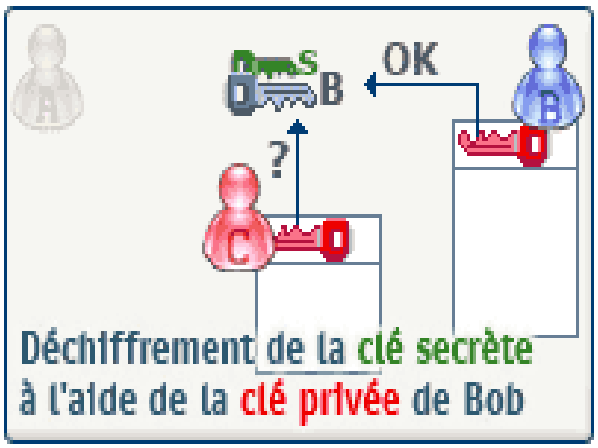


Figure 1.4 : Schéma qui illustre le déchiffrement a clé secrète **[8]**

A et B peuvent s'échanger des informations cryptées et décryptées à l'aide de la clé secrète.

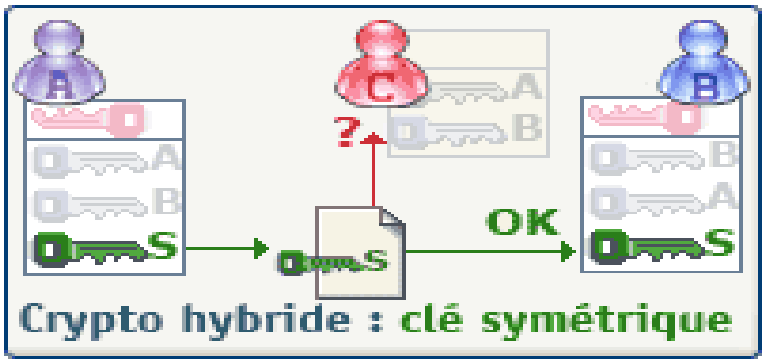


Figure 1.5 : Schéma qui illustre le cryptage hybride **[3]**

Chapitre 2

concept de base des vidéos

2. concept de base des vidéos

2.1 Introduction

La vidéo est constituée d'images qui apparaissent en continu à un certain rythme, l'œil humain se caractérise par sa capacité à distinguer environ 20 images par seconde, ainsi, en montrant plus de 20 images par seconde, l'œil peut être amené à croire l'image animée.
On décrit la fluidité d'une vidéo par le nombre d'images par seconde (en anglais frame rate), exprimé en FPS (frames per second, en français frames per second).

D'autre part, la vidéo au sens multimédia du terme est généralement accompagnée de son, c'est-à-dire accompagnée de données audio.

2.2 Type de vidéo

2.2.1 Vidéo Analogique

Représentant la donnée comme un flux continu de données analogiques, destinées à être affichées sur un écran de télévision (basé sur le principe du balayage).

Les trois principales des normes des vidéos analogique sont : PAL, NTSC, SECAM.

Le format PAL/SECAM (ligne de phase alternée/couleur continue avec mémoire) utilisé en Europe pour Hertz TV permet d'encoder la vidéo sur 625 lignes (seules 576 lignes sont affichées car 8% des lignes sont utilisées pour la synchronisation).

25 images par seconde avec un rapport d'aspect de 4:3 (c'est-à-dire un rapport d'aspect de 4:3).

Ou à 25 images par seconde, beaucoup de personnes perçoivent un battement dans l'image. Donc, étant donné qu'il n'était pas possible de transférer plus d'informations en raison de la limitation de bande passante, il a été décidé d'intercaler les images, c'est à dire transférer premièrement les lignes paires, puis les lignes impaires, le terme "champ" désigne la "demi-image" formée soit par les lignes impaires soit par les lignes paires.

L'ensemble constitué par exactement deux champs est appelé trame entrelacée.

Lorsqu'il n'y a pas d'entrelacement le terme de trame progressive est utilisé **[16].**

La norme NTSC : (National Télévision Standards Committe), utilisée aux Etats-Unis et au Japon, utilise un système de 525 lignes entrelacées à 30 images/seconde (donc à une fréquence de 60Hz).

Comme dans le cas du PAL/SECAM, 8% des lignes servent à synchroniser le récepteur. Alors, le NTSC affiche un format d'image 4:3, la résolution réellement affichée est de 640x480.

2.2.2 Vidéo Numérique

La vidéo numérique consiste à afficher une série d'images numériques. S'agissant d'images numériques affichées à un débit précis, il est possible de connaître le débit nécessaire à l'affichage de la vidéo, c'est-à-dire le nombre d'octets affichés (ou transférés) par unité de temps. Par conséquent, le débit binaire (en octets par seconde) requis pour afficher la vidéo est égal à la taille de l'image multipliée par le nombre d'images par seconde.

Considérons une image truecolor (24 bits) définie comme 640 x 480 pixels.

Pour afficher correctement une vidéo avec cette définition, il faut afficher au moins 30 images par seconde, soit un débit égal à : 900ko*30=27 mo/s

2.3. La compression des vidéos

La compression vidéo est le processus de conversion d'un signal vidéo dans un format qui utilise moins d'espace de stockage ou de bande passante de transfert.

La compression est une technologie fondamentale pour des applications telles que la télévision numérique (transmission terrestre, câble ou satellite), stockage/reproduction optique, télévision Mobile, visioconférence et streaming vidéo sur Internet **[9].**

Il existe deux types de compression, la compression avec perte et la compression sans perte.

2.3.1 Compression sans perte

Avec cette technique, les données sont compressées sans perte de données.

Comme leur nom l'indique, les techniques de compression sans perte n'impliquent aucune perte d’informations.

Si les données sont compressées sans perte, les données d'origine peuvent être récupérées exactement à partir de là, la compression sans perte est généralement pour les applications qui ne tolèrent aucune différence entre les données d'origine et la reconstruction de données.

2.3.2 Compression avec perte

C’est le type de compression vidéo le plus courant, car il fournit un taux de compression plus élevé, bien sûr, il y a un compromis : des taux d'intérêts plus élevés, plus la qualité de la vidéo compressée est faible.

Codec avec perte ne convient pas aux données informatiques, mais il est utilisé dans MPEG car il permet des facteurs de compression plus élevés que les codecs sans perte.

2.4 Classification des algorithmes de cryptage de vidéo numérique

Nous classons les algorithmes de cryptage de vidéo numérique en quatre catégories principales **: [10]**

2.4.1 Cryptage total

Dans cette classe, tout le contenu de la vidéo est d'abord compressé puis cryptée à l'aide des Algorithmes traditionnels tels que DES, RSA, IDEA, AES, etc.
Cette technique n'est pas adaptée à la vidéo en temps réel, applications dues au calcul lourd et à la vitesse lente.

2.4.2 Cryptage sélectif

Ces algorithmes chiffrent sélectivement les octets des images vidéo, étant donné que ces algorithmes ne cryptent pas chaque octet de données vidéo, et cette technique réduit la complexité.

2.4.3 Cryptage basé sur la permutation

Les algorithmes de cette classe utilisent des algorithmes de permutation principalement différents pour brouiller ou chiffrer le contenu vidéo, pas besoin de brouiller chaque octet. Certains algorithmes utilisent des listes organisées comme clé pour chiffrer le contenu vidéo.

2.4.4 Cryptage perceptif

Ce type de cryptage nécessite que la qualité des données audio et vidéo ne soit pas seulement partiellement réduite par le cryptage, c'est-à-dire que les données multimédias cryptées soient encore partiellement visibles. dans la technologie de protection vidéo traditionnelle appelée cryptage complet, tous le contenu est d'abord compressé, puis entièrement crypté à l'aide du flux binaire compressé cryptage standard, la technologie n'est pas adaptée aux applications en temps réel en raison de la latence élevée et de la complexité du calcul. le chiffrement sélectif gère qui ne le fait pas, seul un sous-ensemble des données est crypté. le but du cryptage sélectif est de réduire la quantité de données à chiffrer tout en conservant un niveau de sécurité adéquat.

2.5 Couleur de l'espace

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

- Images binaires (0,1), représentées par 1 bit / échantillon,
- Infographie, représentée par 4 bits / échantillon,
- Images en niveaux de gris, représenté par 8 bits / échantillon,
- Images en couleur, représentées par 16, 24 bits ou plus / échantillon.

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

2.5.1 Représentation RVB (Rouge-Vert -Bleu)

Dans un système de représentation des couleurs RVB, illustré à la **figure 2.1**, une couleur est produite en ajoutant trois couleurs primaires : rouge, vert et bleu.

La ligne droite, où R = G = B, spécifie les valeurs de gris allant du noir au blanc **[11].**

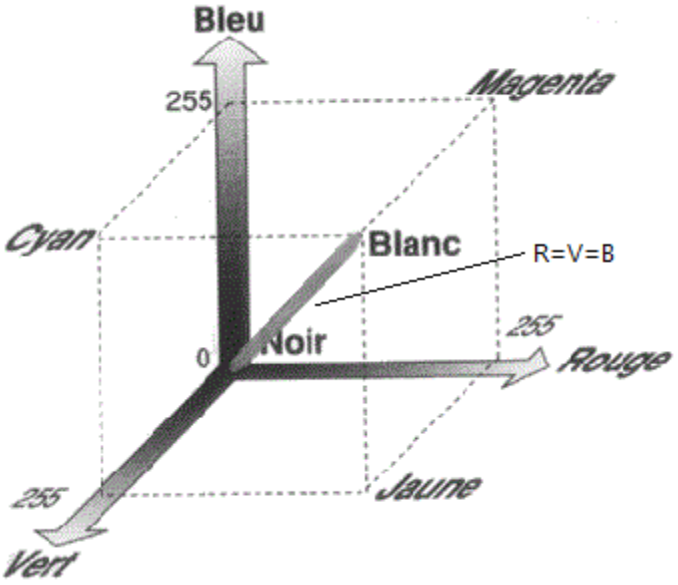


Figure 2.1 : Représentation des couleurs RVB

2.5.2 Représentation YUV (luminance /chrominance)

Une autre représentation des images en couleur, décrit la luminance et la chrominance composante d'une image, la composante de luminance noté Y fournit une version en niveaux de gris de l'image représente par l'équation (1.1), tandis que deux composants de chrominance U et V donnent des informations supplémentaires qui convertissent l'image en niveaux de gris à une image de couleur par les équations (1.2), (1.3), la représentation YUV est plus naturelle pour la compression d'images et de vidéo, l'exacte transformation de la représentation RVB à YUV, spécifiée par la norme CCIR 601 **[11].**

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

U = 0.564(B-Y) (1.2)

V = 0.713(B-Y) (1.3)

2 .5.3 Représentation YCbCr

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

Cb = U/2 + 0.5 (1.4)

Cr = V/1.6 +0.5 (1.5)

De cette manière, les composantes de chrominance Cb et Cr sont toujours comprises dans la plage[0,1]. **[11]**

Chapitre 3

principe de fonctionnement RSA

3. principe de fonctionnement RSA

3.1 Introduction

Dans ce qui suit nous allons citer une très grande évolution du chiffrement dans la cryptographie : le chiffrement RSA qui est utilisé pour la cryptographie a clé public d'où cette technique a été inventée en 1977 par Rivest, Shamir et Adleman.

Elle est basé sur le chiffrement asymétrique (qui est un cryptage où l'algorithme de chiffrement n'est pas le même que celui du déchiffrement, et où les clés utilisées sont différentes). Ce chiffrement est très utilisé dans le commerce électronique et l'échange de données confidentielles sur internet, pour but d'assurer la confidentialité et l'authenticité.

3.2 principe de fonctionnement du RSA

Le cryptage RSA est utilisé pour communiquer des clés symétriques pour échanger les informations de façon confidentielle.

A communique la clé publique à B et garde la clé privée pour elle, B envoie une clé symétrique cryptée à A avec le chiffrement RSA en utilisant la clé publique.

A décrypte la clé symétrique grâce à sa clé privée.

Cette phase basée sur 2 étapes

- Génération des clés
- Cryptage et décryptage

Exemple :

B veut envoyer un message secret à A.

Le processus se décompose ainsi :

1- A prépare une clé publique et une clé privée (génération de clés).

2- B utilise la clé publique de A pour crypter son message (cryptage).

3- A reçoit le message crypté et le déchiffre grâce à sa clé privée (décryptage).

3.2.1 Génération des clés

- Choisir au hasard p et q, deux nombres premier entre eux, on garde p et q secrets.
- Calcul le produit n = p*q, le module de chiffrement.
- Calculer φ(n) = (q - 1) *(p - 1) ,(avec φ(n) est une fonction qui représente la quantité de nombres premier dans l'ensemble {1,…,n}.
- Choisir un entier naturel au hasard e premier avec φ(n) et inférieur strictement à φ(n), (exposant de chiffrement);
- Calculer d l'entier naturel, l'inverse de e modulo φ(n), et inférieur strictement à φ(n), appelé exposant de déchiffrement .

d peut se calculer efficacement par l'algorithme d'Euclide étendu,

e est premier avec φ(n) donc selon le théorème il existe deux entiers k et d tels que e*d = 1 + k * φ(n), c.-à-d. que e*d ≡ 1 [φ(n)]

(n, e) ou (e, n) représente la clé publique du chiffrement

d représente la clé privée **[17]**

Exemple de génération de clé :

1- A choisit 2 nombres premiers au hasard p=11 q=5 ;

2- A calcule le produit n=11*5=55

3- A calcul $\varphi(n)$=10*4=40

4- A prend e = 7, tel que e est premier avec 40 d'où la clé publiques (7,55)

5- A cherche la clé privée d donc il faut résoudre l'équation précédente de notre exemple à l'aide de l'algorithme de Bézout-Euclide on aura :

- 40=5*7+5
- 7=1*5+2
- 5=2*2+1

Alors :

- 5-2*2=1
  5-2*(7-1*5)=1
- 3*5-2*7=1
  3*(40-5*7)-2*7=1
- 3*40-17*7=1
  7^{-1} [40] = -17 [40]= 23

la clé privée vaut d=23

3.2.2 Cryptage et décryptage

B veut envoyer un message à A, donc il dépose son message dans la boîte aux lettres d'A, A la seule qui pourra ouvrir sa boîte et consulter le message, la clé publique est symbolisée par la boite aux lettres, tout le monde peut y déposer un message, la clé qui ouvre la boîte aux lettres est la clé privée.

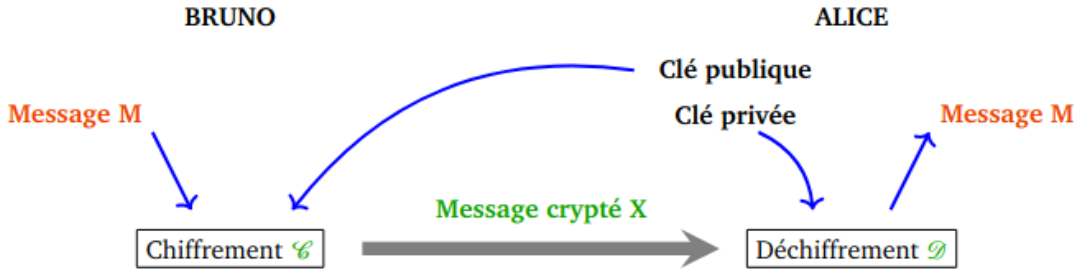


Figure 3.1 : Schéma qui illustre le chiffrement et le déchiffrement RSA **[18]**

a. Cryptage

B veut envoyer un message à A, il doit procéder comme suit :

1) il prend connaissance de la clé publique (e, n) de A.

2) il transforme chaque lettre du texte en clair en un équivalent numérique adéquat (le code ASCII par exemple), il partage les chiffres de ce message en blocs de même taille.

3) il encrypte chaque bloc séparément en calculant c ≡ m^e mod n.

4) il envoie chaque bloc à A.

Exemple :

B veut envoyer un message m= « salut » secret à A. il chiffre son message selon la procédure suivante :

L'exemple précédent la clé publique de A est : (7,55)

Donc B traduit les lettre du message selon le tableau suivant

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tableau 3.1 : tableau d'affectation des lettres en chiffres

M = « salut » transforme en M= 18 00 11 20 19

Il regroupe ce nombre en tranches de chiffres strictement inférieurs à n = 55 :

M= 18 00 11 20 19

M= m0 m1 m2 m3 m4

Pour chacun des nombres inférieurs à n =55, ils seront codés en utilisant la clé privée.

Il s'agit donc pour B d'élever chaque nombre à la puissance 7 et d'en prendre le reste par la division par 55, on obtient le code :

c =115 971 081 171 16

enfin il envoie chaque bloc à A.

b. Décryptages

A reçoit le message de B, à partir de p et q, qu'elle l'a gardé secret, et la clé de déchiffrement.

Chaque bloc sera déchiffré par l'équation suivante :

Mi = c^d mod n

c =115 971 081 171 16 Elle trouve m = salut.

3.3 La bibliothèque FFMPEG

FFmpeg est une collection de logiciels libres destinée au traitement de flux audio ou vidéo (enregistrement, lecture ou conversion d'un format à un autre).

Cette bibliothèque est utilisée par de nombreux autres logiciels ou services comme VLC, iTunes ou YouTube.

Développé sur GNU/Linux, FFmpeg peut être compilé sur la plupart des systèmes d'exploitation, y compris Windows.

Le projet est distribué sous licence libre, GPL 2+ ou LGPL 2.1+

en fonction des options de compilation du projet.

Le nom FFmpeg est constitué du nom du groupe de travail MPEG et des deux F provenant de l'abréviation de « fastforward » (« avance rapide ») en anglais **[19].**

Chapitre 4

Tests et résultats de chiffrement par RSA

4.Tests et résultats de chiffrement par RSA

4.1 Introduction

Aujourd'hui, RSA est un système universel servant de nombreuses applications.

Il est utilisé pour les transactions sécurisées sur Internet et il est implémenté dans de nombreuses normes informatiques, c'est donc le crypto-système asymétrique le plus utilisé aujourd'hui dans le monde.

Notre objectif dans ce chapitre est de faire une simulation par le crypto-système RSA le chiffrement des vidéos numériques en modifiant les paramètres de l'algorithme, on va aussi discuter les résultats qui seront basés sur deux critères importants : c'est la vitesse et la qualité visuelle de l'opération de chiffrement appliqué sur les vidéos.

4.2. processus de chiffrement

Notre travail est divisé en deux parties, le premier est le cryptage vidéo et le second est le décryptage.

4.2.1 Cryptage de la vidéo

- Charger les fichiers MP4.
- Diviser la vidéo en images et lire une seule image à la fois.
- Extraire les frames de chaque image à l'aide de FFmpeg et les chiffrer avec RSA
- Afficher la vidéo chiffrée.

4.2.2 Décryptage de la vidéo

On va faire les même étapes de chiffrement mais avec la vidéo cryptée : donc c'est l'opération inverse du cryptage

- Diviser la vidéo cryptée en images et lire une seule image à la fois.
- Extraire les frames de chaque image à l'aide de ffmpeg et les déchiffrer avec RSA.
- Afficher la vidéo déchiffrée.

4.3 Environnement de développement

4.3.1 Environnement logiciel

Nous avons développé notre approche dans l'environnement Linux avec la distribution Ubuntu 20.04 et nous avons utilisé le compilateur GCC sous Linux pour implémenter notre application. Le code source de notre application est écrit en langage C.

Nous avons également utilisé la bibliothèque ffmpeg sous Linux, qui est une bibliothèque riche en fonctionnalités qui peut exploiter et traiter des données multimédia telles que des images, des vidéos et des sons.

4.3.2 Environnement matériel

L'application a été développée sur un PC (Laptop ASUS modèle : Latitude E5450) ayant les caractéristiques suivantes :

→Processeur : Intel (R) Core (TM) i3-6006U CPU @ 2.00GHz 1.99 GHz.

→Mémoire RAM installée: 4,00 Go.

→Système d'exploitation : Windows 10 Professionnel 64 bit.

4.4 Les vidéos utilisées

Vidéos			
Nom	Video1	Video2	Video 3
Format	**MP4**	MP4	MP4
Taille	3.8Mb	3.5Mb	3.8Mb
Nombre de frame	150	360	907
Durée	5s	12s	30s

Tableau 4.1 : Caractéristique de vidéos utilisées

4.5 Les résultats de la simulation :

La vidéo originale :

Vidéo1 :

Début **milieu** **fin**

Figure 4.1 : Des images prises à différents moments de la vidéo1**.**

Vidéo2 :

Début **milieu** **fin**

Figure 4.2 : Des images prises à différents moments de la vidéo2.

Vidéo 3

Début **milieu** **fin**

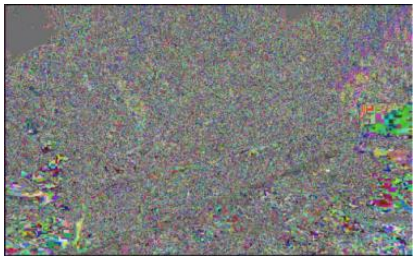
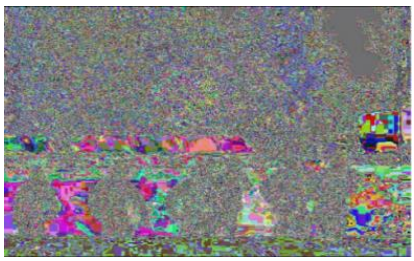
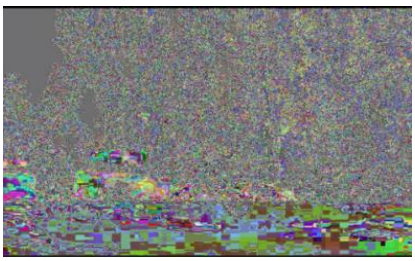
Figure 4.3 : Les images prises à différents moments de la vidéo3.

Les vidéos après le chiffrement

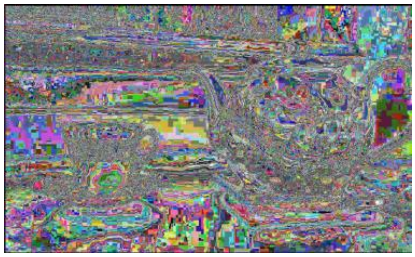
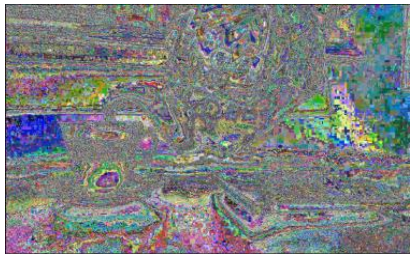
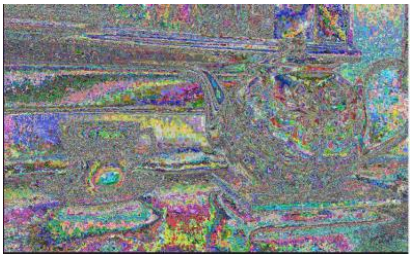
	N1	p	Q	Temps chiffrement
Video1	253	23	11	13s
Video2				1mn30s
Video 3				2mn51s

Video1 :

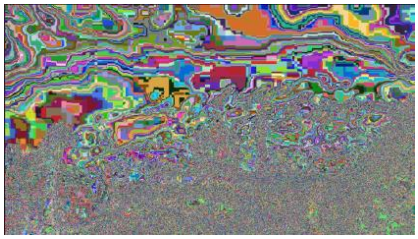
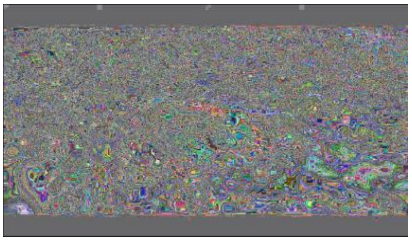
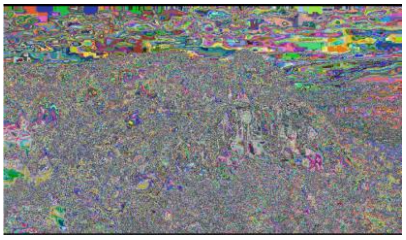
Début **milieu** **fin**

Video2 :

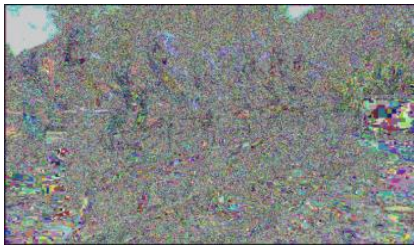
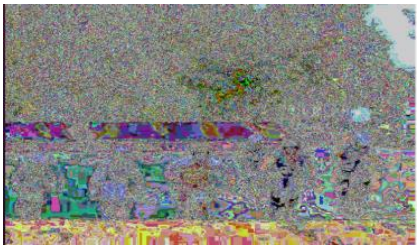
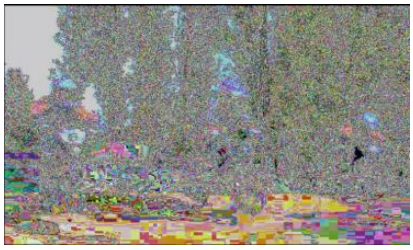
Video 3

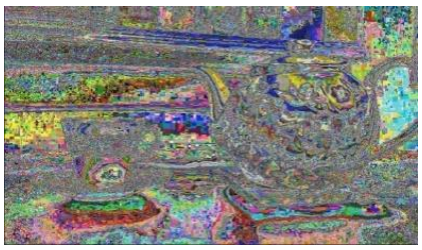
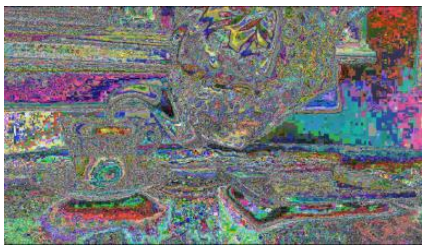
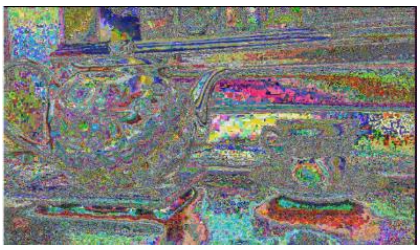
	N2	P	Q	Temps chiffrement
Video1	2701	37	73	22s
Video2				2mn19s
Video 3				6mn10s

Video1 :

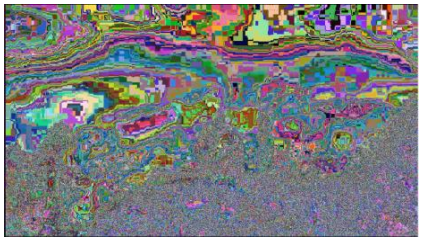
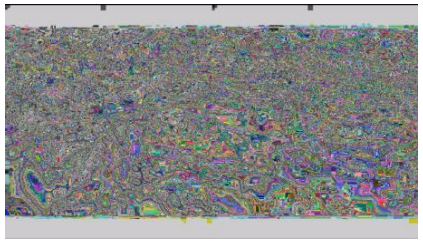
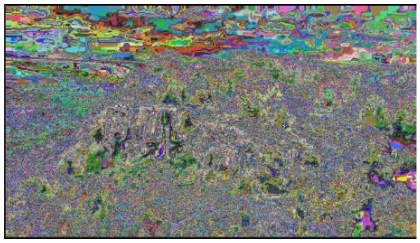
Début **milieu** **fin**

Video2 :

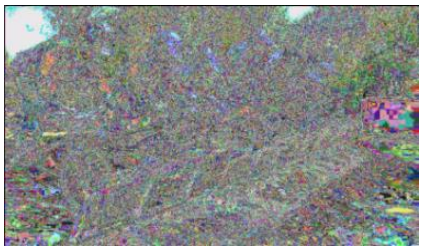
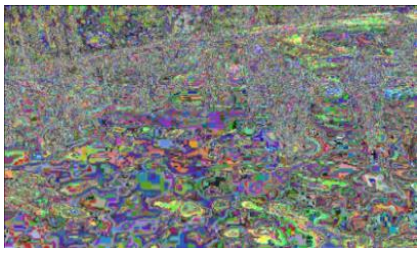
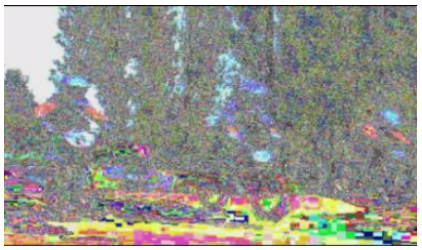
Video3

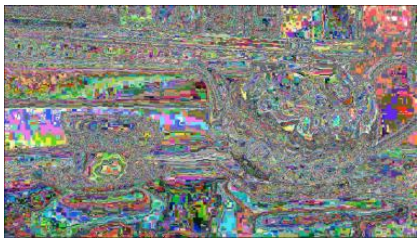
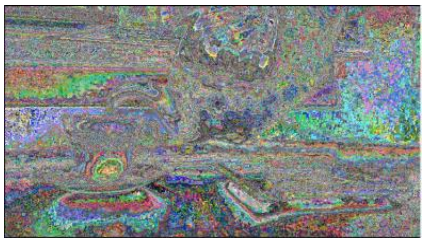
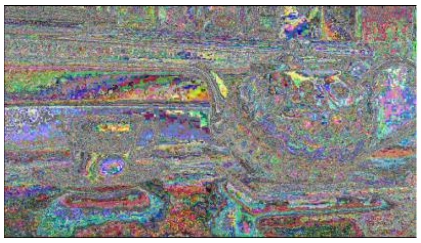
	N3	p	q	Temps chiffrement
Video1	43 733	101	433	29s
Video2				3mn25s
Video3				8mn53s

Video1 :

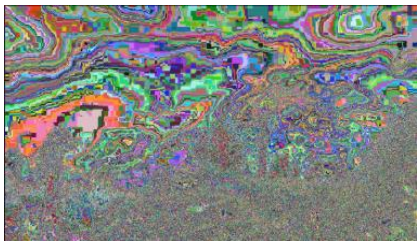
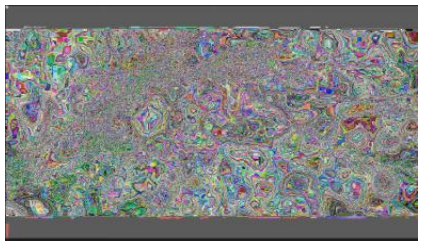
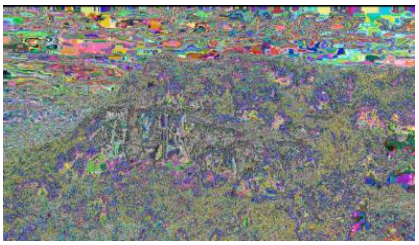
Début **milieu** **fin**

Video2 :

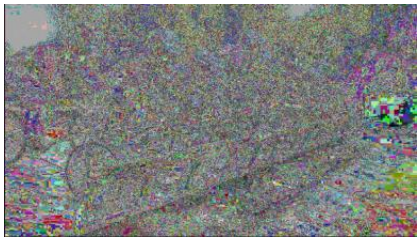
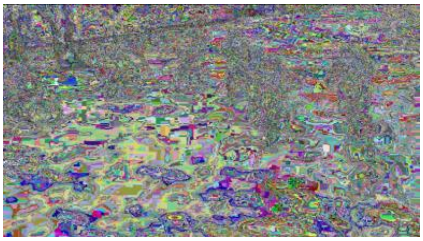
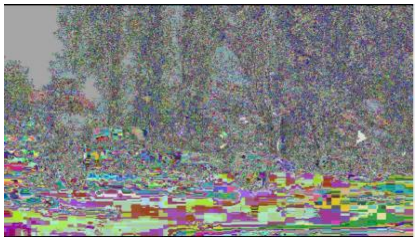
Video 3

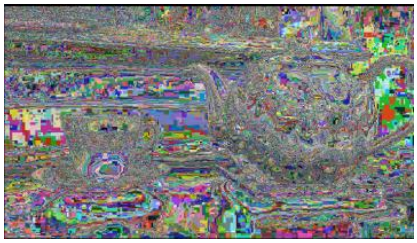
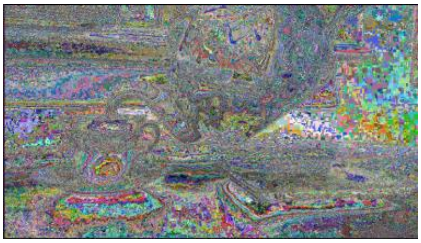
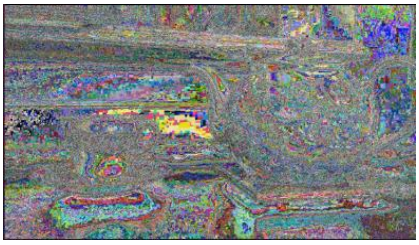
	N4	P	Q	Temps chiffrement
Video1	3 958 307	1009	3923	21s
Video2				2mn30s
Video3				6mn26s

Video1 :

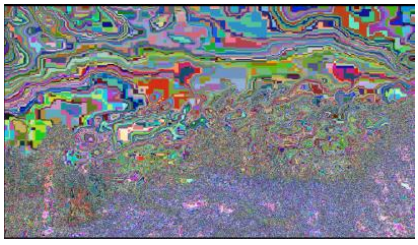
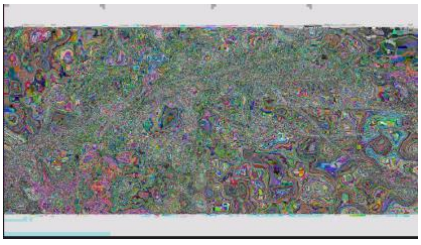
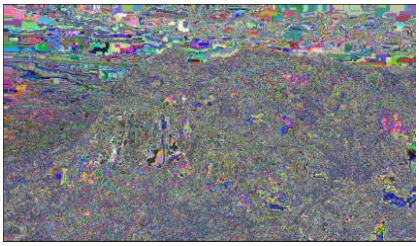
Début **milieu** **fin**

Video2 :

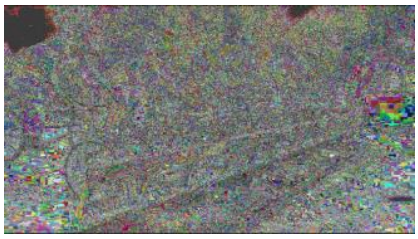
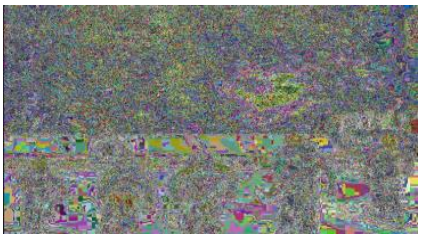
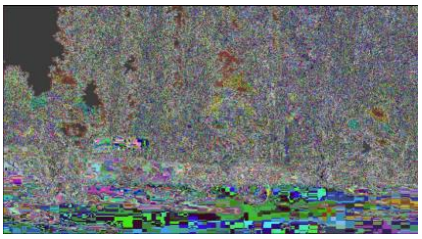
Video 3

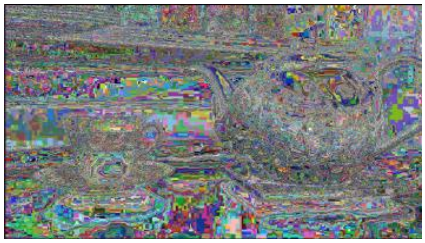
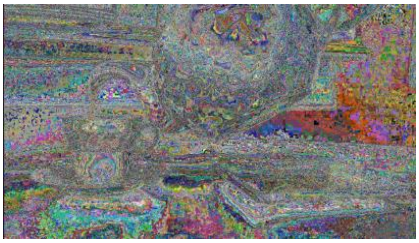
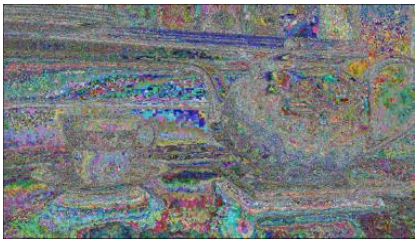
	N5	p	Q	Temps chiffrement
Video1	51 250 499	6607	7757	22s
Video2				2mn30s
Video 3				6mn37s

Video1

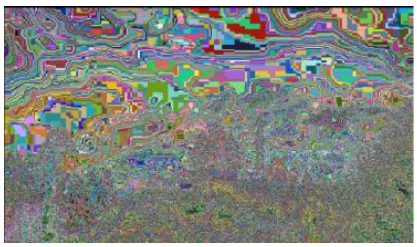
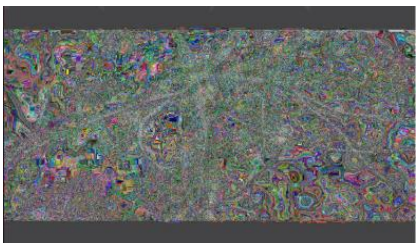
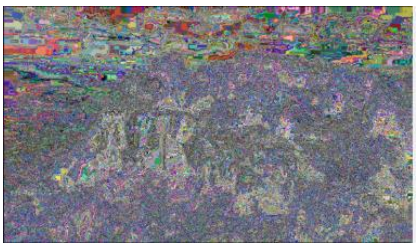
Début **milieu** **fin**

Video 2

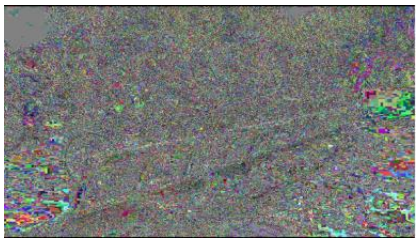
Video 3

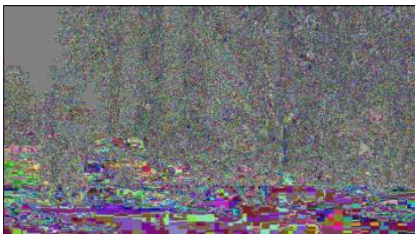




	N6	p	Q	Temps chiffrement
Video1	74 028 533	8219	9007	22s
Video2				2mn30s
Video 3				6mn37s

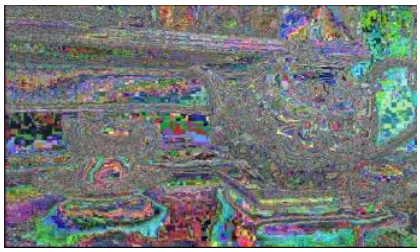
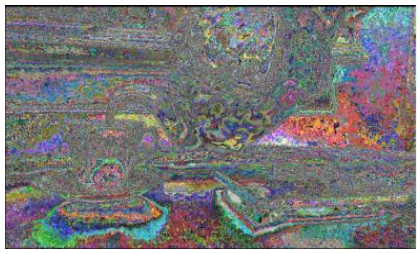
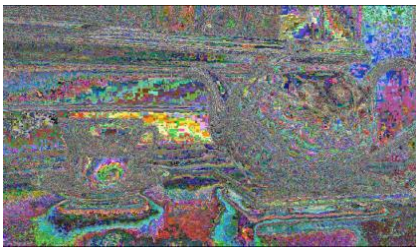
Video1

Début **milieu** **fin**

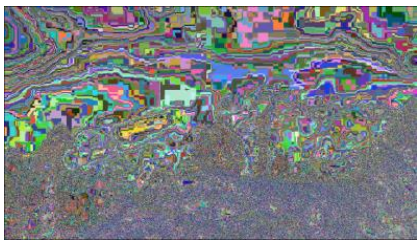
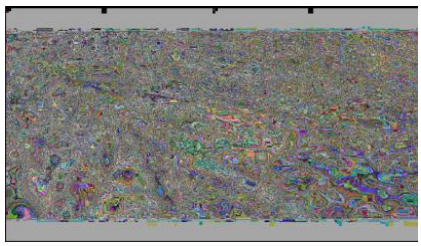
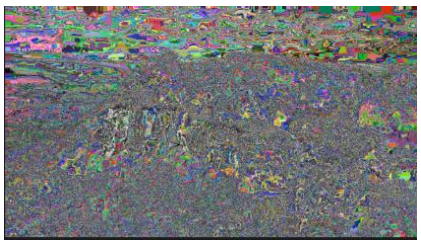




Video 2

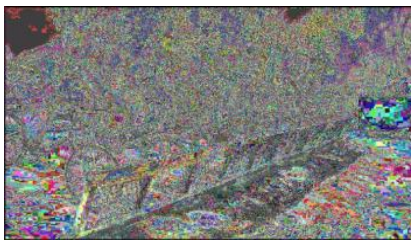
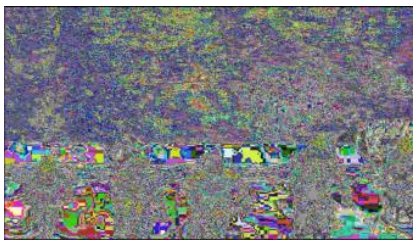
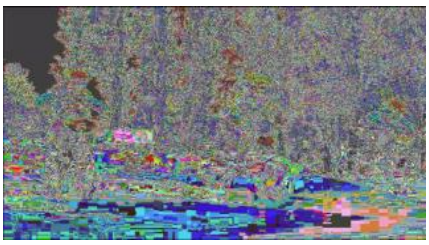
Video 3

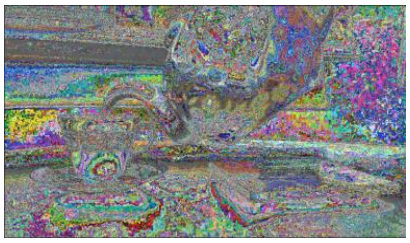
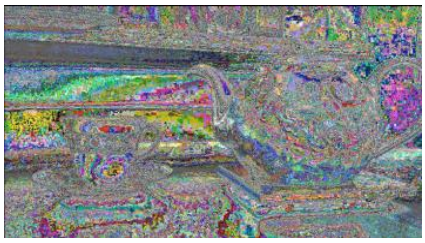
	N7	p	q	Temps chiffrement
Video1	144 571	10039	14401	46s
Video2	639			5mn13s
Video 3				13mn17s

Video 1

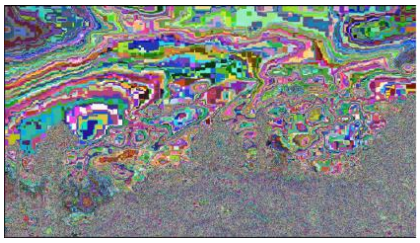
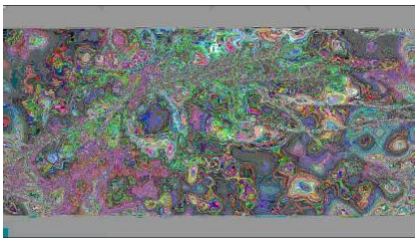
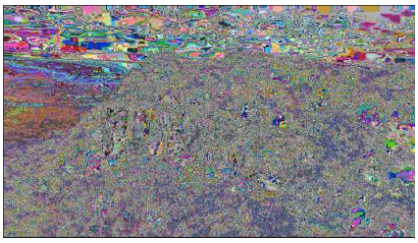
Début **milieu** **fin**

Video 2 :

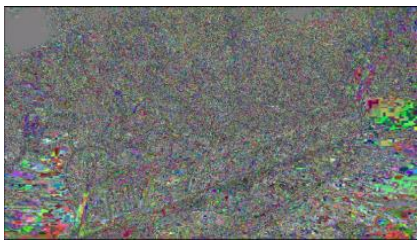
Video3

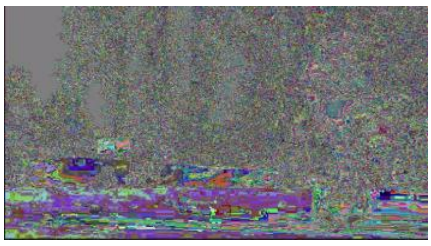




	N8	p	Q	Temps chiffrement
Video1	999 962 000 357	999979	999983	21s
Video 2				2mn30s
Video 3				6mn16s

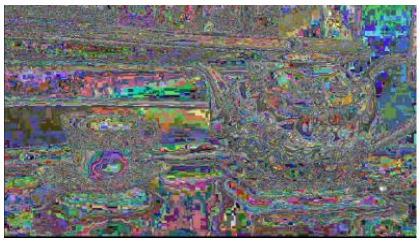
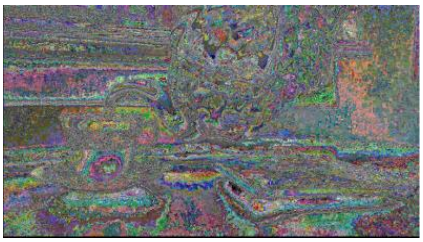
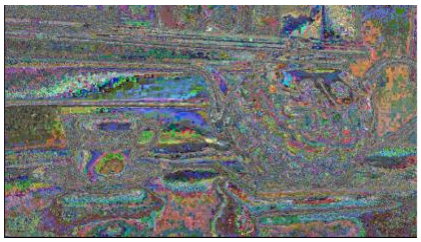
Video 1

Début **milieu** **fin**

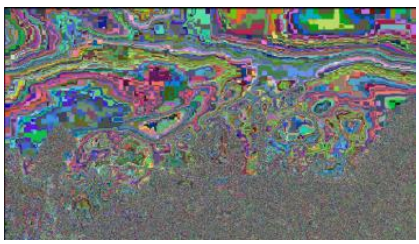
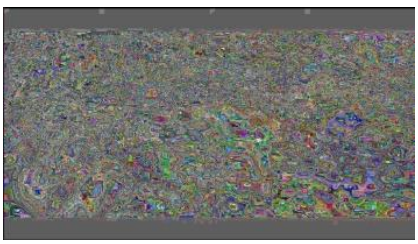
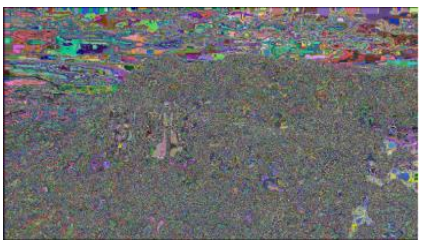




Video 2

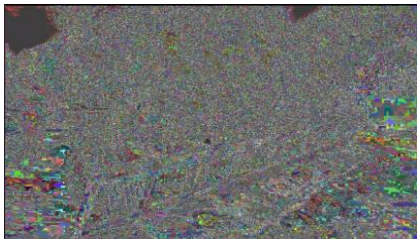
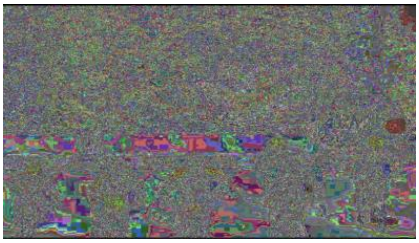
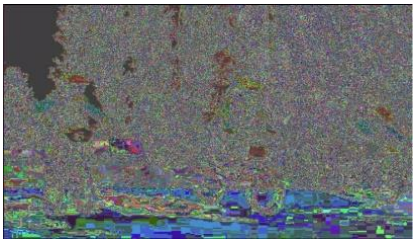
Video 3

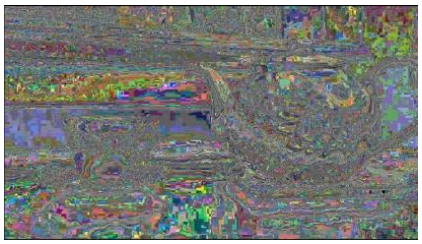
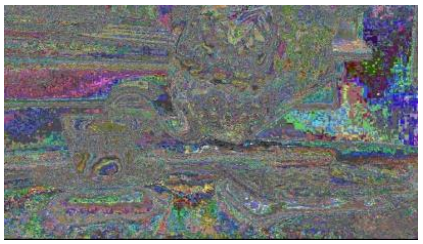
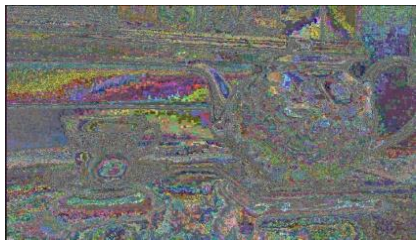
	N9	p	Q	Temps chiffrement
Video1	**75457886450**	**8685319**	**8687981**	**47s**
Vidéo 2	**939**			**5mn 16s**
Vidéo 3				**12mn35s**

Vidéo 1

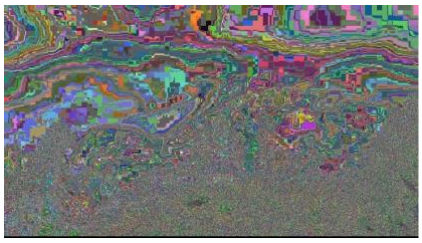
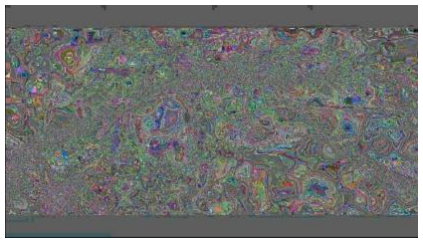
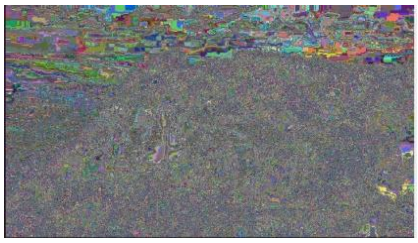
Début **milieu** **fin**

Vidéo 2

Vidéo 3

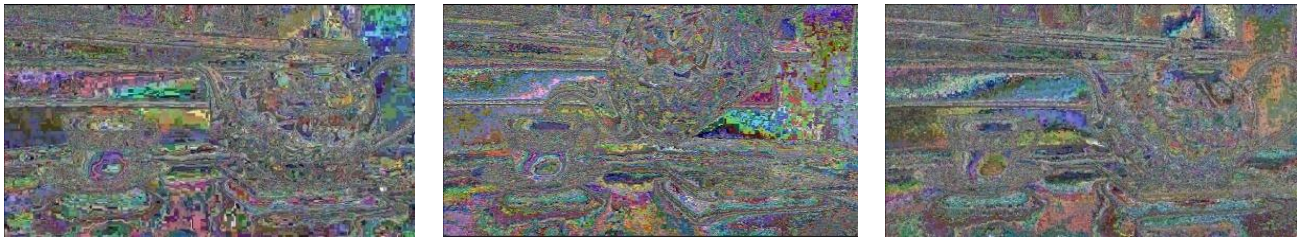




	N10	p	Q	Temps chiffrement
Vidéo 1	**106654591771**	**10327363**	**10327379**	**23s**
Vidéo2	**577**			**2mn26s**
Vidéo 3				**6mn3s**

Vidéo 1

Début **milieu** **fin**

Vidéo 2



Vidéo 3

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

  Entre 80 et 100 meilleures qualités

  Entre 50 et 80 bonnes qualités

  Entre 30 et 50 moyennes qualités

  Entre 10 et 30 faibles qualités

	N1	N2	N3	N4	N5	N6	N7	N8	N9	N10
Video1	10	10	20	25	40	45	50	65	75	85
Video2	10	10	15	20	30	35	40	55	65	75
Video3	10	15	25	30	45	55	60	70	80	90

Tableau 4.2 : La qualité de chiffrement visuelle des vidéos

On a vidéo 1 : similarité moyenne

Vidéo 2 : similarité faible

Vidéo 3 : similarité élevée

Graphe de la qualité de chiffrement des vidéos

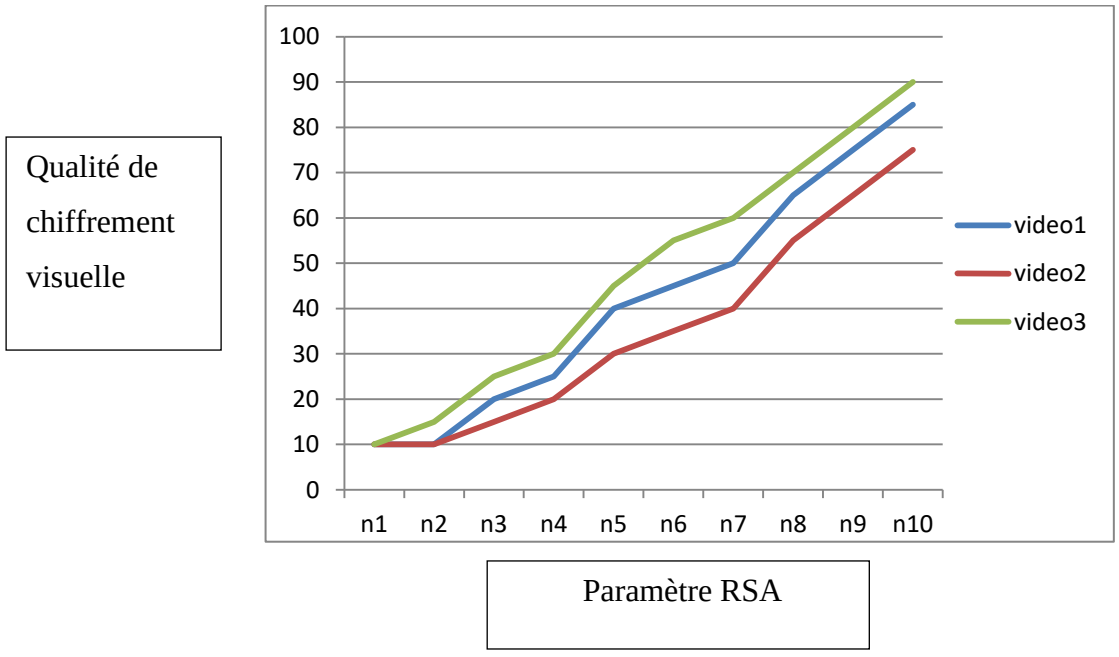


Figure 4.4 : La qualité de chiffrement des vidéos

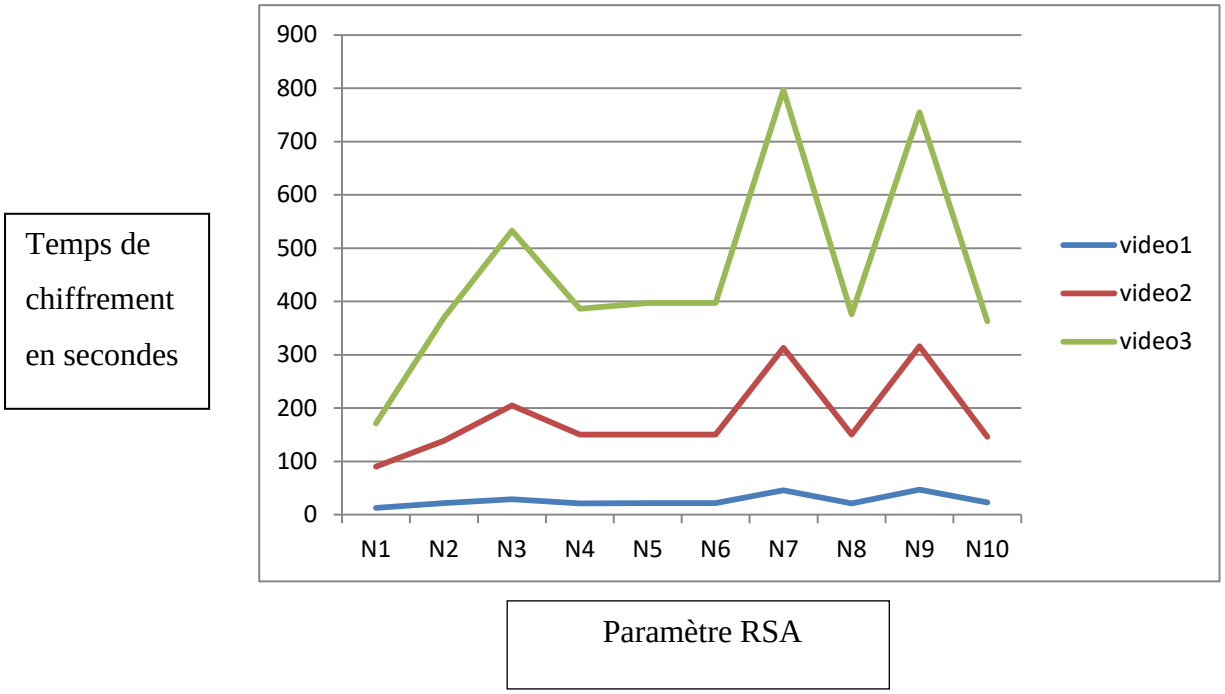


Figure 4.5 : Comparaison temps de chiffrement de video1, video2 et video3.

D'après les résultats obtenus nous remarquons que la taille de N affecte la qualité de chiffrement des vidéos , de sorte que lorsque nous avons utilisé une petite valeur de N on voit toujours la trace de la vidéo originale dans la vidéo chiffrée, donc il faut choisir de grandes valeurs pour les deux clés (p, q) pour avoir un meilleur résultat.

Nous remarquons également que la similarité de la vidéo affecte la qualité de chiffrement et lorsqu'on prend des vidéos avec similarité faible, on obtient une meilleure qualité, et pour cela la qualité de chiffrement de vidéo 2 est plus faible par rapport à vidéo 1 et vidéo 3 car elle est dotée d'une similarité élevée.

Et lorsque nous augmentons le nombre de frames, le temps de chiffrement augmente.

Conclusion Générale

Ce travail a été réalisé dans le cadre de projet de fin d'études de master au sein du département d'informatique de l'université de Tlemcen, auquel nous avons appliqué toutes les compétences et connaissances acquises durant nos années d'étude.

Dans le monde actuel, la croissance de quantité d'informations transitant les réseaux internationaux impose de les crypter pour assurer la confidentialité et la sécurité.

C'est peut-être le problème le plus important d'Internet, en clair, le cryptage permet d'éviter l'interception, la lecture ou la modification d'un message en clair, ainsi que la fabrication d'un message factice.

Le transfert de données visuelles comme les vidéos dans un système de communication comme internet a besoin d'être sécurisé et protégé contre les utilisateurs non autorisés à faire des modifications dans le contenu, C'est dans ce contexte que se situe notre travail qui consiste à crypter des vidéos en utilisant l'algorithme RSA et la bibliothèque FFMPEG.

Le problème qui se pose dans notre travail est comment peut-on concevoir un système de chiffrement efficace par l'algorithme RSA pour assurer la sécurité de ce type de données visuelles ?

Dans notre travail, nous avons étudié le problème de cryptage des vidéos par l'algorithme de chiffrement RSA, en exploitant la puissance de la bibliothèque FFMPEG dans le traitement des images, cela nous a permis de faire une étude sur les performances, et découvrir l'influence des valeurs p et q de l'algorithme RSA sur la qualité et la vitesse de l'opération de chiffrement.

D'après les résultats obtenus nous remarquons que la taille de N= (p*q) affecte sur la qualité de chiffrement des vidéos, de façon que lorsque nous avons utilisé une petite valeur de N on a remarqué l'indifférence de la trace de la vidéo originale dans le vidéo chiffrée donc il faut choisir des grandes valeurs pour les deux clés (p, q), pour obtenir un meilleur résultat de l'opération de chiffrement, Nous remarquons également que la similarité de la vidéo affecte la qualité de chiffrement et lorsqu'on prend des vidéos avec similarité faible on obtient une meilleure qualité, et lorsque nous augmentons le nombre de frames, le temps de chiffrement augmente

Comme perspectives pour ce travail, nous allons nous intéresser par le facteur de rapidité de chiffrement tout en conservant un niveau des performances dans la génération automatique des paramètres p et q.

Dans les contributions futures, nous souhaitons aller plus loin, utilisant de nouvelles idées comme : introduire le traitement parallèle dans le chiffrement des vidéos de grande taille.

Résumé :

L'utilisation large des images et des vidéos numériques dans divers applications apporte une attention particulière à la sécurité et aux problèmes de confidentialité aujourd'hui.
La cryptographie est parmi les méthodes les plus efficaces pour établir la confidentialité et l'intégrité des données visuelles comme les vidéos et les images.. Jusqu'à, maintenant divers algorithmes de cryptage ont été proposé et largement utilisé comme DES, RSA, etc. ils sont utilisés pour le texte et les données binaires.
Dans notre travail, nous avons étudiés le problème de cryptage des vidéos par l' algorithme de chiffrement RSA en exploitant la puissance de la bibliothèque FFMPEG dans le traitement des images. Cela nous a permis de faire une étude sur les performances et l'influence des valeurs p et q de l'algorithme RSA sur la qualité et la vitesse de l'opération de chiffrement.
Mot clés: Cryptage des vidéos, algorithme RSA, Bibliothèque FFMPEG.

ملخص:

.يجلب الاستخدام الواسع للصور ومقاطع الفيديو الرقمية في مختلف التطبيقات اهتمامًا خاصًا لقضايا الأمان والخصوصية اليوم

يعد التشفير من أكثر الطرق فعالية لإثبات سرية وسلامة البيانات المرئية مثل مقاطع الفيديو والصور.حتى الآن ، تم اقتراح

.خوارزميات تشفير مختلفة واستخدامها على نطاق واسع مثل RSA, DESإلخ. يتم استخدامها للنص والبيانات الثنائية

درسنا في عملنا مشكلة تشفير الفيديو بخوارزميات التشفير RSA من خلال استغلال قوة المكتبةFFMPEG في معالجة

الصور. سمح لنا ذلك بدراسة الأداء وتأثير القيمPوQالخوارزمية على جودة وسرعة عملية التشفير

الكلمات الرئيسية: تشفير الفيديو ،الخوارزميةRSA ، المكتبةFFMPEG

.

abstract :

The wide use of digital images and videos in various applications bringsparticular attention to security and privacy issues today.

Cryptography is among the most effective methods to establishconfidentiality and integrity of visual data likevideos and images. Untilnow, variousencryptionalgorithms have been proposed and widelyusedlike DES, RSA, etcthey are used for text and binary data.

Résumé

In ourwork, we have studied the problem of videoencryption by RSA encryptionalgorithms by exploiting the power of the FFMPEG library in image processing. This allowed us to study the performance and the influence of the p and q values of the RSA algorithm on the quality and speed of the encryptionoperation.

keywords: Videoencryption, RSA algorithm, FFMPEG library.

Les Références Bibliographiques

[1]SINGH Simon ,Histoire des codes secrets ,2d.J.C.Lattés ,1999.

[2] Brigitte Collard ,la cryptographie dans l'antiquité gréco-romaine ,2004

[3] yousfisalma,houiti hala,Technique d'encryption efficace dédiée pour une donnée volumineuse,université EchahidHammaLakdhar- EL OUED 2020/2021

[4] Karam Fouad, Imouloudene Salah Eddine , Transfert sécurisé des données visuelles (images) dans un réseau intranet selon l'architecture client/serveur, Université Abou Bakr Belkaid– Tlemcen,2015.

[5] Daniel Barsky ,Cours de Cryptographie ,2005/2006

[6] Souici Ismahane, cryptographie Nouvelle Algorithme de chiffrement évolutionnaire basé occurrences (ACEO), université de Guelma , 2008/2009

[7] A. Canteaut and F. Lévy-dit Véhel, ―La cryptographie moderne,‖ Revue Armement, 2001.

[8] R. Westwater ,B.Furht ,Real-Time Vidéo compression Technique ans Algorithms,1997

[9] DJEMAI Nadia, OTMANI Nassima,Etude et implementation des algorithmes de chiffrement appliqué au cryptage de video,2021

[10] J. Shah, D. Saxenaetal., ―Videoencryption : A survey,‖arXivpreprintarXiv :1104.0800,2011.

[11] Chenene Boubakeur, Chiffrement des vidéos numériques, Université Mohamed Boudiaf.M'sila, 2018 /2019.

Webographie

[12] https://slideplayer.fr/slide/10199363/, dernière visite mai 2022

[13] https://fr.wikipedia.org/wiki/Data_Encryption_Standard, dernière visite mai 2022

[14] https://fr.wikipedia.org/wiki/RC4, dernière visite mai 2022

[15] https://www.itespresso.fr/securite-bluetooth-cle-chiffrement-210157.html, dernière visite mai 2022

[16]https://www.commentcamarche.net/contents/1493-introduction-a-la-video-numerique ,dernière visite mai 2022

[17] https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/,dernière visite mai 2022

[18] https://www.apprendre-en-ligne.net/crypto/rsa/index.html,dernière visite mai 2022

[19] https://chowdera.com/2021/12/202112221132483451.html,derniere visite mai 2022